Safe and Dynamic Driving
Designing for active interventions (Functional safety)
Agenda

1. Legal Demands
   1.1 Product liability
   1.2 Motivation

2. Introduction into Functional Safety
   2.1 What is Functional Safety
   2.2 Unreasonable Risks, hazards & malfunctions of E/E-Systems
   2.3 Implications
   2.4 Risk reduction

3. ISO 26262
   3.1 Standards for Functional Safety
   3.2 Scope and Limitation ISO26262

4. Example Application of Functional Safety
   4.1 Example Situation: Traffic jam on highway
   4.2 Conclusion
## Agenda

### 1 Legal Demands

1.1 Product liability

1.2 Motivation

### 2 Introduction into Functional Safety

2.1 What is Functional Safety

2.2 Unreasonable Risks, hazards & malfunctions of E/E-Systems

2.3 Implications

2.4 Risk reduction

### 3 ISO 26262

3.1 Standards for Functional Safety

3.2 Scope and Limitation ISO26262

### 4 Example Application of Functional Safety

4.1 Example Situation: Traffic jam on highway

4.2 Conclusion
Legal demands
Product Liability

› Product liability law
  › Supplier will be **liable** for **damages** as a result from **malfunction** of his product, that means personal injury or damage to property

› The supplier has to consider
  › Technical solutions which are **state of the art**
  › Product development processes according to safety relevance

› As a result it shall be assured
  › to **prevent** any **danger for life and health**
  › to prevent consequences for companies image
  › to prevent financial consequences for the producer
  › to **prevent** consequences for **involved persons**
    › Managing Directors, Line Managers, Engineers etc.
From Product Liability Law to state of the Art products

› On Country Authority Level shown with example of Germany

<table>
<thead>
<tr>
<th>LAWS</th>
<th>OBLIGATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law of Product Liability GPSG</td>
<td>Kodex zur Ausführung des Geräte- und ProduktSicherheits Gesetzes (GPSG) bei Straßenfahrzeugen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STANDARDS / RULES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262 in accordance with ISO 15504 (SPICE/ ASPICE) (functional safety for passenger vehicles)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive products according state of the art and current state of sciences</td>
</tr>
</tbody>
</table>

General Product Liability (2001/95/EG – European Norm)

Automotive Performance

Automotive Measures

Products

KBA-Kodex

KBA · KraftfahrBundesAmt
Motivation to apply ISO 26262

› **State of the art design is the legal required base for functional safety.** Best way to comply is to show compliance to the international standard ISO 26262 Road vehicles - Functional Safety

› ISO 26262 is considered as the current state of technology and reflects the minimum standard for the safety of a product

› A standard describes the opinion of the majority of experts for a specific product area
  - applied technical solutions and processes for product development and production of competitive products
  - necessary frame conditions
  - minimum requirement for products in the interest of Safety and Environment

› The non-compliance with a standard (such as ISO 26262) itself bears the **high risk that it will be considered as wrongdoing of the company**, leading to a liability of the company in a product liability case / incident.
Agenda

1 Legal Demands
   1.1 Product liability
   1.2 Motivation

2 Introduction into Functional Safety
   2.1 What is Functional Safety
   2.2 Unreasonable Risks, hazards & malfunctions of E/E-Systems
   2.3 Implications
   2.4 Risk reduction

3 ISO 26262
   3.1 Standards for Functional Safety
   3.2 Scope and Limitation ISO26262

4 Example Application of Functional Safety
   4.1 Example Situation: Traffic jam on highway
   4.2 Conclusion
Functional Safety

› Safety:
  absence of unreasonable risk of physical injury, of damage to the health of people, of damage to the environment.

› Risk:
  combination of the probability of occurrence of harm and the severity of that harm.

› Hazard:
  potential source of harm.

› E.g. in electric power steering systems ‘self steering’ is a hazard.
Functional Safety

Safety in use

Hazards emanating from the vehicle when operating as intended (without failure)

Functional Safety

Hazards emanating from the vehicle in case of failure

Security

Hazards emanating from human attacks to the vehicle
Scope of Functional Safety

› Functional safety:
  › Absence of unreasonable risk
  › due to hazards
  › caused by malfunctioning behaviour
  › of E/E systems.

› (Source: ISO 26262-1)
Definition

Unreasonable risk
due to hazards
caused by malfunctioning behaviour
of E/E systems
Unreasonable risk

› unreasonable risk:
  › „risk judged to be unacceptable in a certain context according to valid societal moral concepts”

› Every technical system has a risk to fail
› Society knows about this and accepts a certain amount of risk
  › (or claims to accept the risk until it occurs)

› Zero risk is usually not achievable
Due to hazards

› due to hazards:
  › “Potential source of physical injury or damage to the health of persons”

› Does not include:
  › Protections against financial risk
  › Protections against bad performance
  › Protections against unsatisfied customers

  › Less than required by laws and jurisdiction
  › Less than required by company management
Caused by malfunctioning behavior

› **caused by malfunctioning behavior:**

› Dangers by systems, working as intended, currently not in scope of ISO 26262

› (in discussion as safety of intended use [2nd release])

› **Examples:**

› Use of cruise control in serpentines

› It was never task of cruise control to decelerate before curves
Of E/E Systems

› of E/E systems
  › “System that consists of electrical and/or electronic elements, including programmable electronic elements“
  › Software/hardware controlling energy, information or material flow
  › Not regarded:
    › Hydraulics
    › High-voltage (Electric Shock),
    › Temperature (Fire),
    › Smoke
  › But: If software/hardware error may cause hazard, it is in scope!
    › Wrong controlling of engine might lead to fire of Diesel Particle Filters
    › Failed supervision of high-voltage due to system errors
Implication

- **Fault** can lead to **Error**
  - E/E System
  - Malfunction
  - Effect
  - Elementary on Technical level

- **Error** can lead to **Failure**
  - Based on implementation

- **Failure** can lead to **Hazard**
  - Depends on function
  - Depends on UseCase of Item

- **Hazard** can lead to **Harm**
  - Depends on UseCase of Item
  - Risk of

**Symptom**
- Open circuit
- Wrong variable declaration
- Loss of data
- Wrong data calculation
- Wrong data processing
- Loss function
- Function impaired
- Unintended acceleration
- Loss of braking
- Wrong steering
- Collision on highway
- Destabilization on country road
Risk Reduction

Fault
- Open circuit
- Wrong variable declaration
- Loss of data

Error
- Wrong data calculation
- Wrong data processing

Failure
- Loss function
- Function impaired

Hazard
- Unintended acceleration
- Loss of braking
- Wrong steering

Harm
- Collision on highway
- Destabilization on country road

Risk Reduction through E/E-Systems

Risk Reduction through functionality/operation

Risk Reduction through scope

Use Case versus Safety
Risk reduction

› Goal: perform risk reduction to achieve tolerable risk
Summary

› Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. It describes a state in which a vehicle function does not cause any intolerable endangering states, which are resulting from:

› specification, implementation or realisation errors,
› failure during operation period,
› reasonably foreseeable operational errors,
› reasonably foreseeable misuse.

Reduce risk to the acceptable level
# Agenda

<table>
<thead>
<tr>
<th>1</th>
<th>Legal Demands</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Product liability</td>
</tr>
<tr>
<td>1.2</td>
<td>Motivation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Introduction into Functional Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>What is Functional Safety</td>
</tr>
<tr>
<td>2.2</td>
<td>Unreasonable Risks, hazards &amp; malfunctions of E/E-Systems</td>
</tr>
<tr>
<td>2.3</td>
<td>Implications</td>
</tr>
<tr>
<td>2.4</td>
<td>Risk reduction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>ISO 26262</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Standards for Functional Safety</td>
</tr>
<tr>
<td>3.2</td>
<td>Scope and Limitation ISO26262</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>Example Application of Functional Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Example Situation: Traffic jam on highway</td>
</tr>
<tr>
<td>4.2</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
ISO 26262
One of many: Standards for Functional Safety

› Derivates from Generic Standard
  (Examples)

- **DO-178**
  - **Aerospace**
  - Road vehicles – Functional safety

- **ISO 26262**
  - **Automotive**
  - Generic
    - Functional safety of electrical/electronic/programmable electronic safety-related systems

- **IEC 61508**
  - **Generic**

- **IEC 50156**
  - **Firing**

- **EN 50129**
  - **Train**

- **IEC 61513**
  - **Nuclear Plants**

- **IEC 61511**
  - **Process Industry**

- **IEC 60601**
  - **Medicine**

- **IEC 62061**
  - **Machines**
Scope and limitations ISO 26262

› ISO 26262 is intended to be applied to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t.

› ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems including interaction of these systems.

› It does not address:

  › hazards as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behaviour of E/E safety related systems.

  › unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities

  › the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (for example active and passive safety systems, brake systems, steering systems).
Scope and limitations ISO 26262
Scope and limitations ISO 26262

› Conclusion:

› IEC 61508 as generic standard for functional safety applicable to all E/E-System

› ISO 26262 tailoring of IEC 61508 standard for E/E-Systems installed in series production passenger cars
# Agenda

1. **Legal Demands**
   - 1.1 Product liability
   - 1.2 Motivation

2. **Introduction into Functional Safety**
   - 2.1 What is Functional Safety
   - 2.2 Unreasonable Risks, hazards & malfunctions of E/E-Systems
   - 2.3 Implications
   - 2.4 Risk reduction

3. **ISO 26262**
   - 3.1 Standards for Functional Safety
   - 3.2 Scope and Limitation ISO26262

4. **Example Application of Functional Safety**
   - 4.1 Example Situation: Traffic jam on highway
   - 4.2 Conclusion
Application of Functional Safety

Example Situation: Traffic jam on highway
Application of Functional Safety

Example Situation: Traffic jam on highway

- Information content about the road ahead:
  - Weather conditions
  - Road conditions
  - Traffic scenarios

- Collected by the road user ahead
- Or by infrastructure, data on backends etc.
Application of Functional Safety

Example Situation: Traffic jam on highway

- Provided over the air to other traffic participants

- End of Traffic jam

- Road conditions

- Weather

8th ETSI Workshop on Intelligent Transport Systems (ITS), 8-10 March 2016
Public

9 March 2016
P. Blueher, © Continental AG
Application of Functional Safety

Example Situation: Traffic jam on highway

› Scenario: Standing vehicles at the end of traffic jam + quickly approaching vehicle

› Use Case: Warn all following traffic participants about traffic jam

› Faults: 1. HW or SW bug in E/E-System or
2. Signal runtime too long

› Malfunction: Traffic jam warning takes too long/received too late

› Hazard: No braking of vehicle

› Harm: Collision with end of traffic jam

→ Safety Goal: Avoid loss of braking leading to front collision within a fault tolerant time of 100ms.
Application of Functional Safety

Example Situation: Traffic jam on highway

Weather

Road conditions

Traffic jam

Electro-magnetic interferences

Signal runtime faults

E/E faults

t0 t1 t2
Application of Functional Safety

Example Situation: Traffic jam on highway

➢ Typical Faults:
  • HW/SW fault in E/E-systems of vehicle i.e. open circuits or false data declaration
  • HW/SW fault in E/E-systems of backend i.e. open circuits or false data declaration
  • HW/SW fault in E/E-systems of mobile phone tower i.e. open circuits or false data declaration
  • Electro-magnetic interferences due to radiation etc.
  • Systematic faults i.e. incorrect signal runtime

➢ Failure models:
  • Add, Change, delay, loss, mascarading, re-ordering, repetition of a message
Application of Functional Safety

Example Situation: Traffic jam on highway

› **Result:**

› Safety measures for message required

› Safety measures to be tailored according to designed use cases

› Safety measures against sporadic faults:

  › for message content: CRC, Checksum, Alive Counter

  › provide limited manipulation detection within car environment

  › will not help for bad nominal performance (design does not fulfil use case)

› Safety measure against systematic faults like false signal runtime:

  › smart development: How long does a signal from sender to receiver and why?

  › Event triggered versus deterministic

  › robust development process & methods
Application of Functional Safety

Example Situation: Traffic jam on highway

› Conclusion:

› **Independent Department / Organization for Functional Safety needed**

› **For each use case**

  › **Definition of system limit and scope required**

  › **Followed by a safety analysis of system**

  › **Choice of appropriate detection and mitigation measures**
Questions?
Thank you for your attention!
Safe and Dynamic Driving towards Vision Zero