Einfluss der Funktionalen Sicherheit auf die Bordnetzentwicklung

Dr. Peter Grabs, Dr. Frederic Holzmann — Intedis GmbH&Co. KG
Dr. Wolfgang Langhoff — LEONI Bordnetz-Systeme GmbH

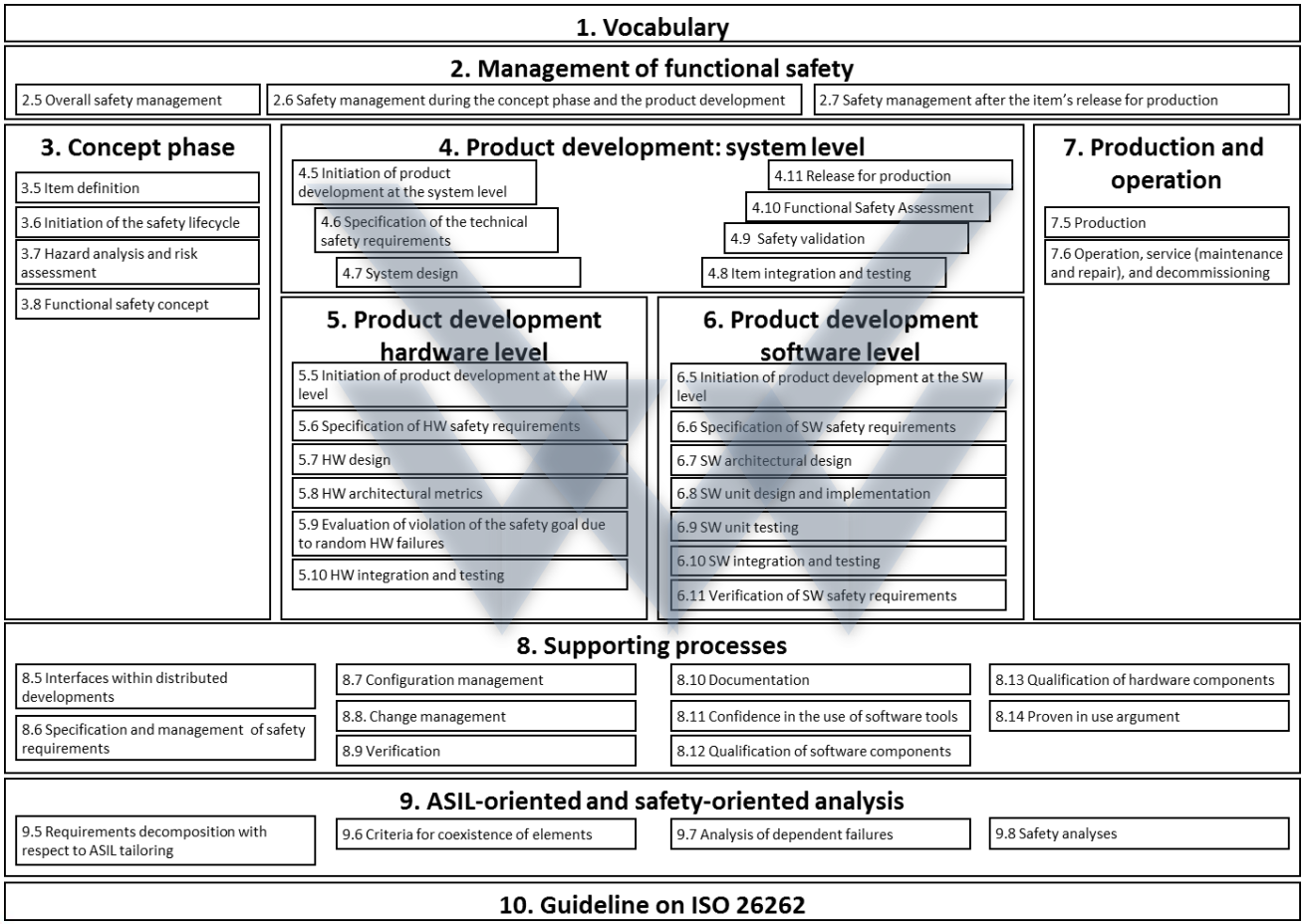
Outline

- System development according ISO 26262
- How to treat wires?
- Example from the real life
- Look into the glass bowl
- Summary

intedis

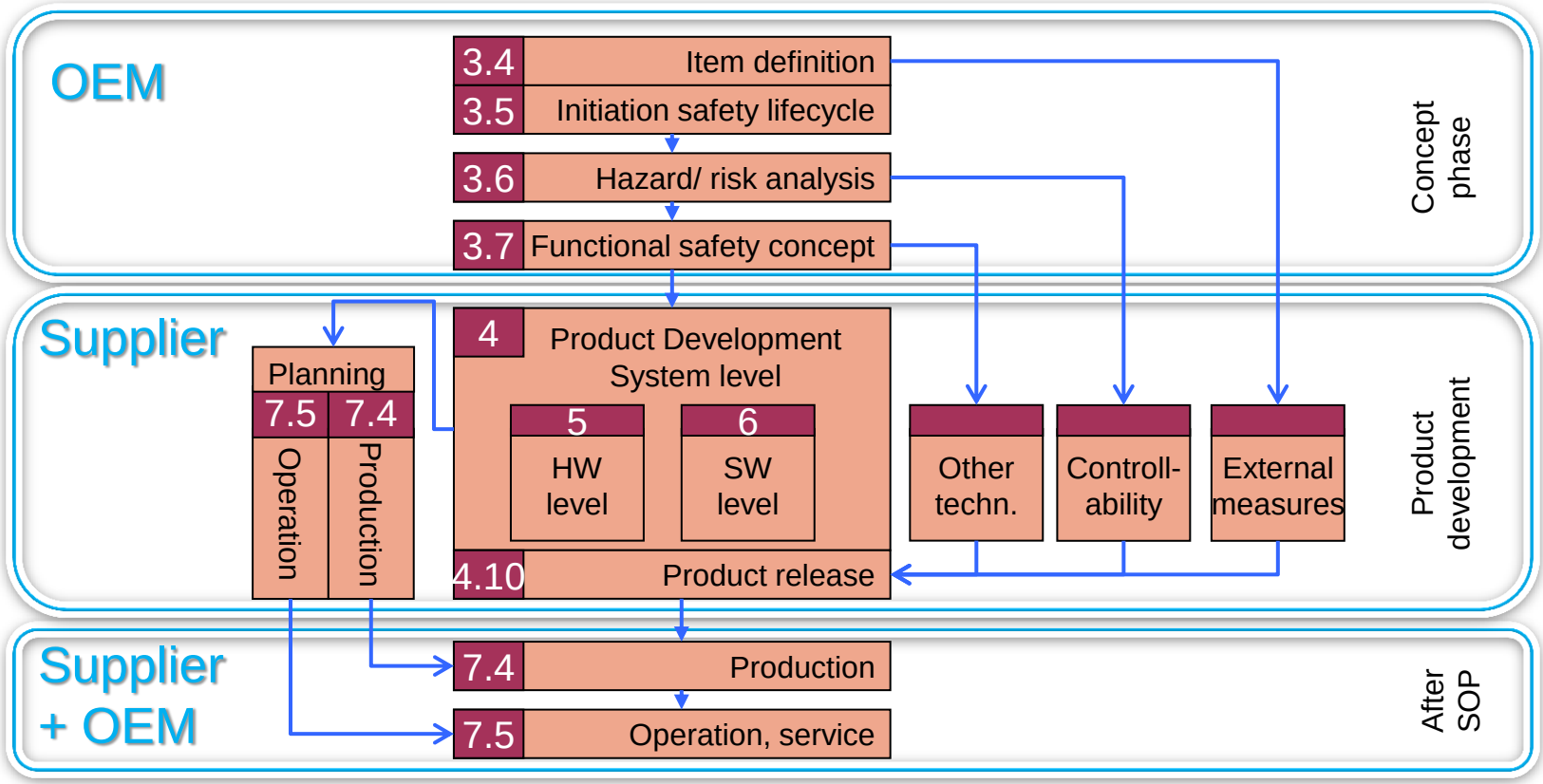
ISO 26262

ISO 26262 … applies to all activities during the safety lifecycle of safety-related systems comprised of **electrical, electronic and software components**.



Overall Automotive Safety Lifecycle according to ISO 26262

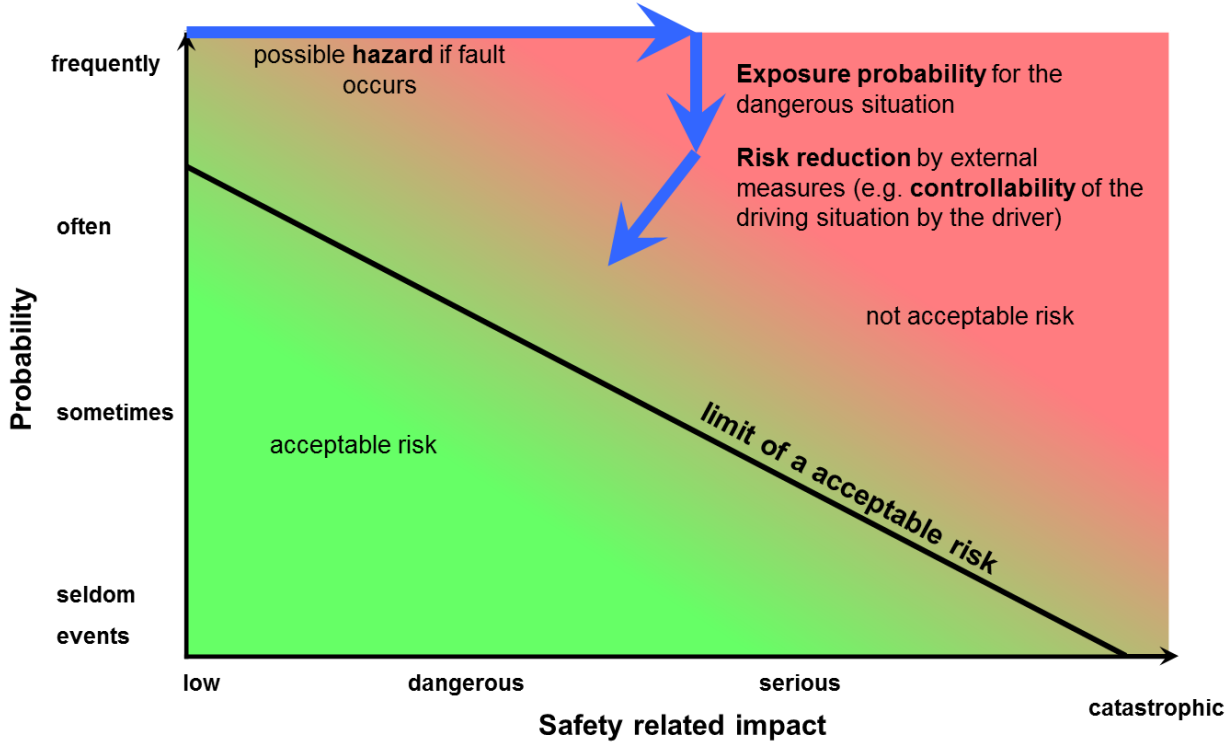
- The safety lifecycle is shared between OEM and supplier



Concept phase activities (HRA)

HRA = Hazard analysis and risk assessment

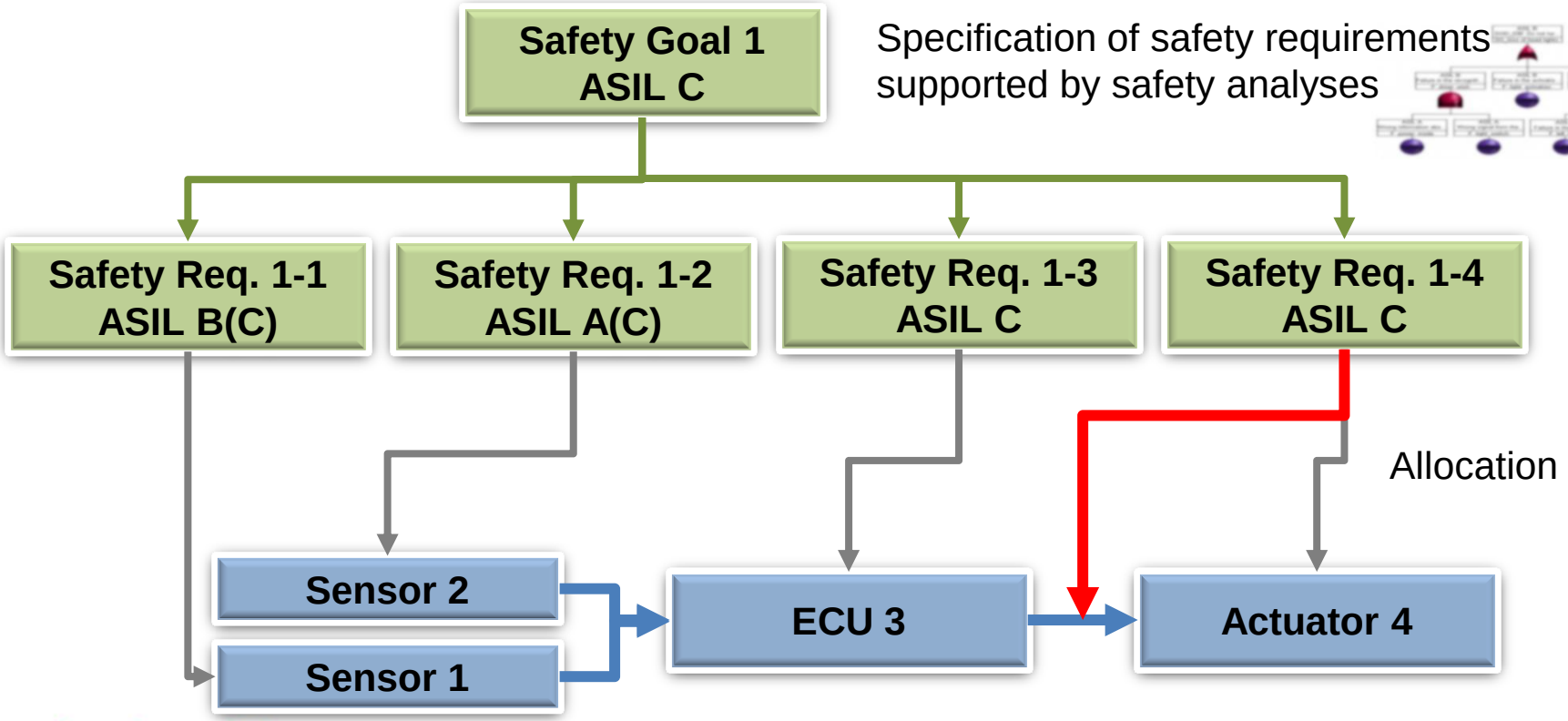
- Method to **identify and categorize hazardous events** of items and to **specify safety goals and ASILs** related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk. (ISO 26262-1)
- Basing on the **item definition**



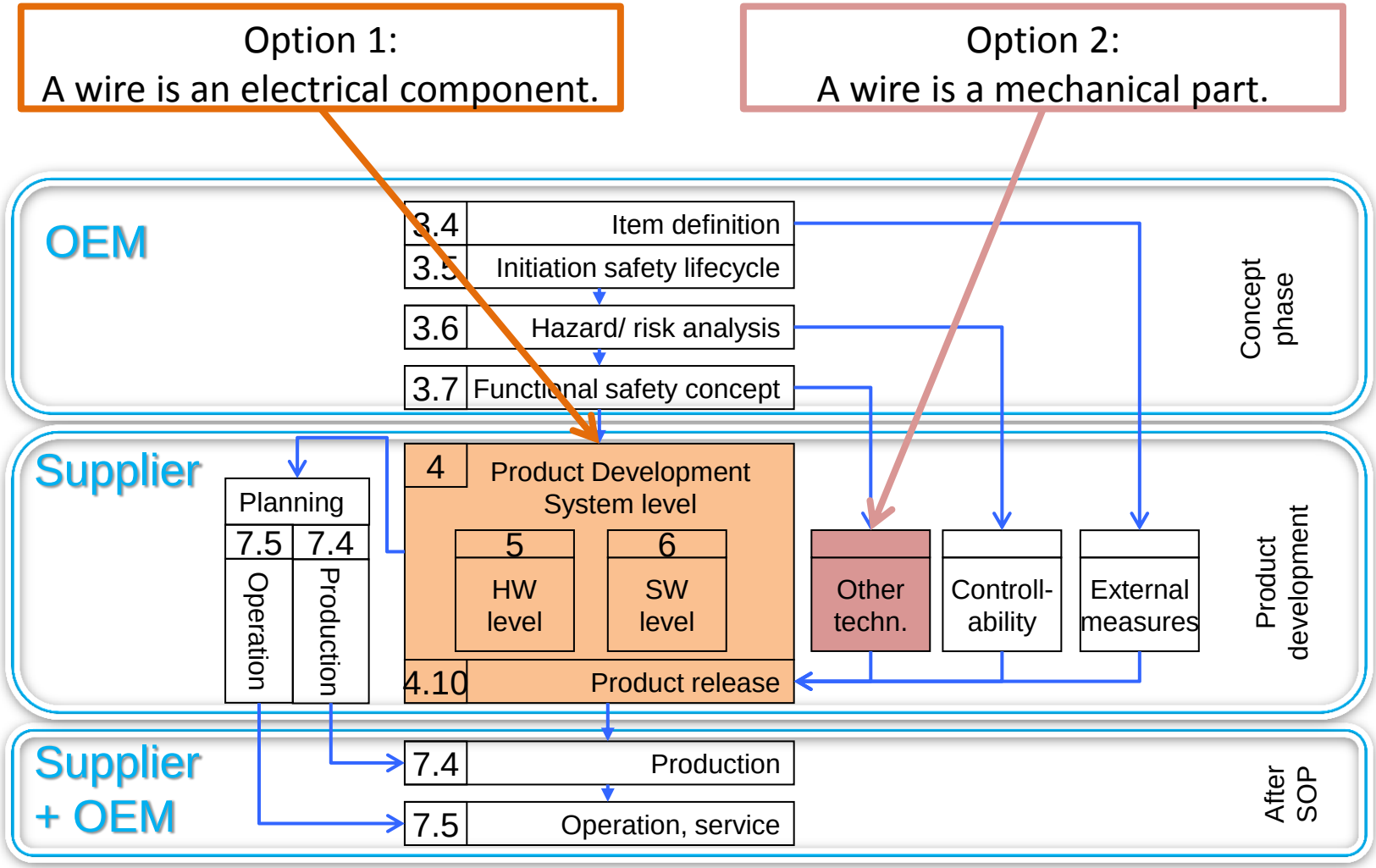
Concept phase activities (FSC)

FSC = Functional safety concept

- specification of the functional safety requirements, with associated information, their **allocation to architectural elements**, and their interaction necessary to achieve the safety goals. (ISO 26262-1)



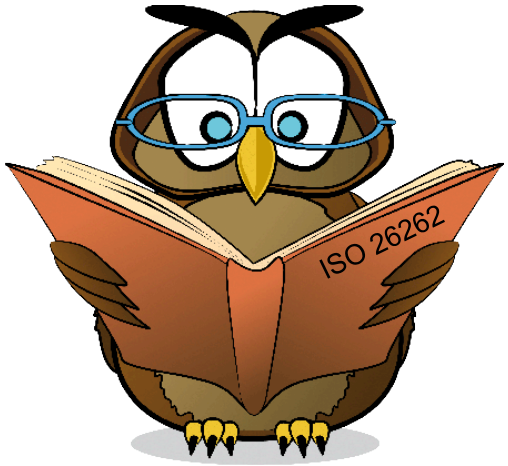
How to handle safety requirements for wires?



Option 1: Electrical Component

- Within the scope of ISO 26262

  → Read the standard



- Most requirements of ISO 26262 not applicable to wires (e.g. ISO 26262-6: SW development)
- ISO 26262-8 clause 13 offers a way to handle safety related wires according ISO 26262.

intedis

Classes of Parts / Components acc. ISO 26262-8: cl.13

Activity	Hardware part or component			
	Safety-related basic hardware part	**Safety-related intermediate hardware part**	**Safety-related intermediate hardware component**	**Safety-related complex hardware component**
	(e.g. resistors, transistors)	(e.g. gray code decoder)	(e.g. fuel pressure sensor)	(e.g. ECU)
Standard qualification	Applicable	Applicable	—	—
Qualification in accordance with Clause 13	—	Applicable	Applicable	—
Integration/test in accordance with ISO 26262-5	—	Applicable[a]	Applicable[a]	Applicable
Integration/test in accordance with ISO 26262-4	—			Applicable

[a] The hardware part or component will be integrated in accordance with ISO 26262-4, or ISO 26262-5, or both ISO 26262-4 and ISO 26262-5, depending on its level.

Standard qualification is sufficient

- “to address general functional performance, conformity of production, environmental endurance and robustness”

intedis

Option 2: Mechanical part

- To be treated as **“Other technologies”**

ISO 26262-3: 8.4.3.2 If the functional safety concept is to rely on elements of other technologies, then the following shall apply: …

c.) The implementation of functional safety requirements by elements of other technologies shall be ensured through specific measures that are outside the scope of ISO 26262.

d.) No ASIL should be assigned to these elements.

- Implementation of requirements is verified:

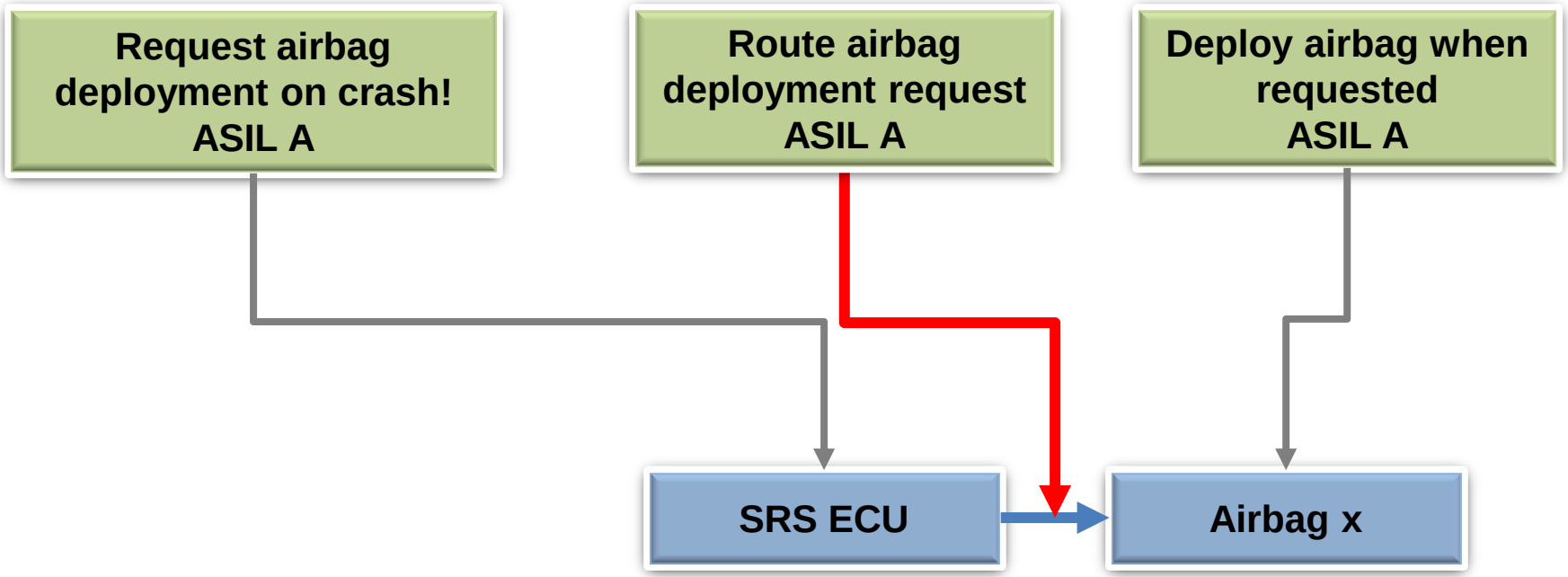
ISO 26262-8: 9.2 … to ensure that they comply with their requirements.

Both options lead to similar requirements!

intedis

Example: Airbag

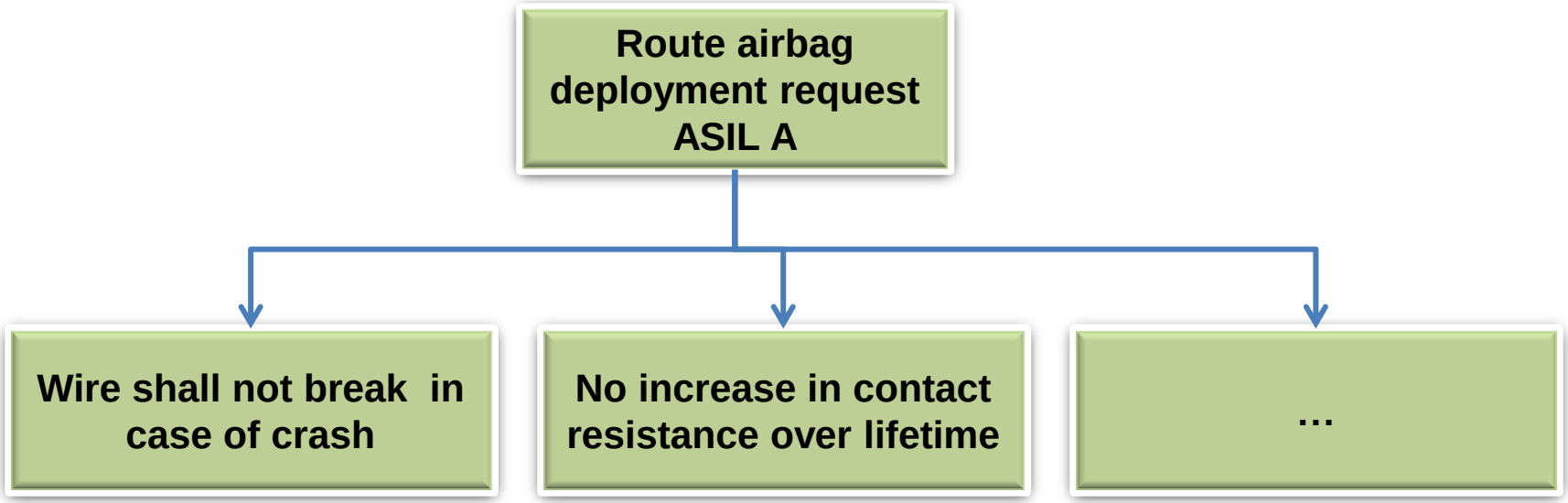
- SRS has a very standardized safety concept
- Typical safety goals:
  - No unintented airbag deployment! ASIL D
  - **Deploy airbag when needed!** **ASIL A**



intedis

Example: Airbag (2)

- What is the meaning of this safety requirement?

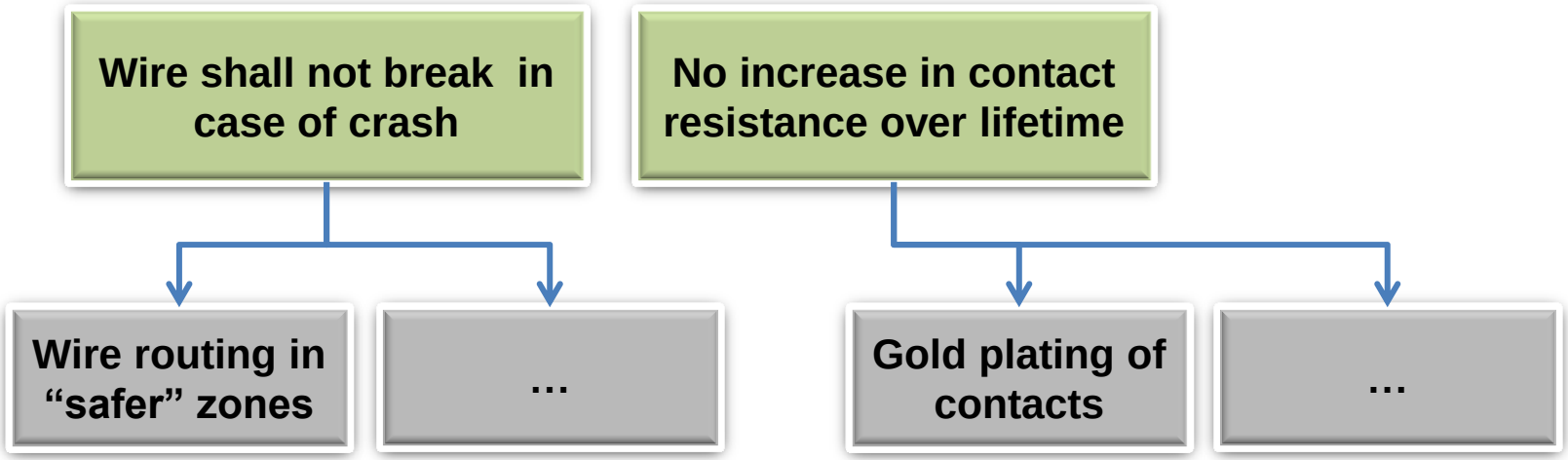


- Breakdown of the high level safety requirement
  - Supported by analyses (FTA, FMEA, …)
  - Considering test results
  - Solving real life issues

intedis

Example: Airbag (3)

- What does this mean for the wiring harness supplier



- Use technical know-how to define measures that fulfill the safety requirements!
- Prove effectiveness of these measures!

→ Verification against requirements under the relevant environmental conditions

intedis

Standardized approach possible?

- State of the art for airbag wires with ASIL A safety requirements is this:
  - “safe” routing
  - Gold plated contacts
  - ….
- How about a reverse argument?

  - These technical requirements are sufficient to comply with ASIL A safety requirements!

NO!!!!!!

- **The technical requirements have to be defined according to the safety requirements!!**

intedis

A look into the glass bowl

- Currently only a limited number of vehicle functions impose safety requirements on the availability of the function.
- This may change in the future!!!

- Concepts as drive-by-wire or autonomous driving will drastically change this!

- This includes a paradigm change from assistance to function for several functions, e.g. electrically powered steering.

- The problem will be to identify the right technical requirements to achieve a sufficient safety level.

intedis

Example: Steering in autonomous driving

- Consider a highly automated driving scenario on a highway
- Driver is in the car but not focused on the traffic
- Studies indicate a transfer time of ~ 5 sec.[1] till driver takes back control.

- What about the power supply for the EPS?
  - If the power supply fails, the car will not be steered for the next ~5 sec.

  - This is a huge time for steering!!!

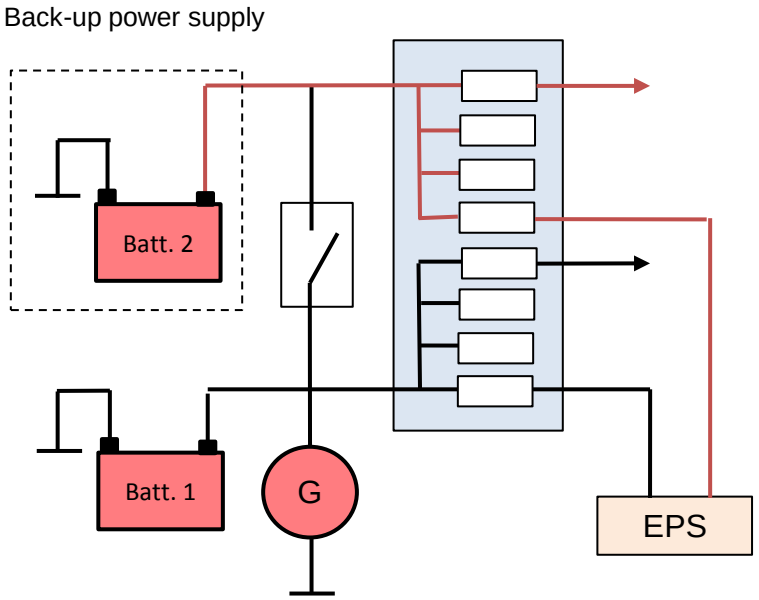
- How to overcome this issue?
- How to support the quantitative evaluation?

[1] Hackenberg, Bennewald, Othersen VW; Bongartz Carmeq "Licht oder Sound? Evaluation von diffusen Modalitäten zur Fahrerunterstützung während des teilautomatischen Fahrens", VDI Kongress 'Elektronik im Fahrzeug', Baden-Baden, Germany, 16th – 17th November 2013

intedis

Example: Steering in autonomous driving (2)

- Could be solved on architectural level:



- Could be solved on technology level:
  - New reliable wire technologies, e.g. self-healing wires
  - Improved crimping technologies
  - Robust connectors
  - …

intedis

Summary

- Development activities are distributed between OEM and supplier
  - Exchange of information between the parties necessary
- ASIL is not a useful attribute for wiring harness development.
  - Safety requirements have to be transformed into technical requirements
  - Compliance to the technical requirements has to be shown
- Future will bring even more topics like this!

Life remains interesting for us! ☺

intedis

Intedis GmbH & Co. KG
Max-Mengeringhausen-Straße 5
97084 Würzburg
Germany

P +49 (0)931 6602 0
F +49 (0)931 6602 35555
M info@intedis.com
W www.intedis.com