Relationship between Mobile Maschinery and ISO26262

Safety challenges for machinery in mixed environments and steps to resolving them from an assessment point of view

27. May 2021

Mehr Wert.
Mehr Vertrauen.

TÜV SÜD at a glance

150+
YEARS OF QUALITY, SAFETY & SUSTAINABILITY

1 000+
LOCATIONS WORLDWIDE

€ 2.4
BILLION IN ANNUAL REVENUE

24 000+
EMPLOYEES*

42 %
OF REVENUE OUTSIDE GERMANY^

574 000
CERTIFICATES

100 %
INDEPENDENT & IMPARTIAL

1-STOP
SOLUTIONS PROVIDER

*As of 2017-12-31
^Based on clients' locations
Note: Figures have been rounded off.

2. TÜV SÜD Rail: Offering a comprehensive suite of services

Automation

Training and consulting services

- Support for the implementation of functional safety requirements
- Training courses (EN 61508, ISO 13849, ISO26262, risk analysis, system design and analysis, FMEA / FTA, probabilistic, safety-relevant software)

Testing services

- System analysis
- Software analysis
- Environmental simulation and electromagnetic compatibility test
- Electrical safety test
- Hardware analysis / probabilistic methods
- Optical tests

Certification services

- Certification of electronic systems according to functional safety standards
- EC type examination and certification for safety devices according to the Machinery Directive 2006/42/EC Annex IV
- Certification of applications
- Certification of company functional safety system

Our Expert

Nikola Mitov
Expert Functional Safety at TÜV SÜD

Background:

- Nikola has worked over 6 years in Munich as a software architect.
- He has more than 5 years of experience in functional safety projects related to the automotive industry with main focus on system and software architecture for Battery Electric Vehicles (BEV) and Internal Combustion Engine (ICE) Vehicles.
- He has worked as a functional safety software architect during the development of powertrain functions for autonomous driving.
- Nikola joined TÜV SÜD in 2019 and acts as an assessor for projects related to IEC 61508, ISO 26262 and ISO 13849.

Agenda

1. Current Status Mobile Maschinery
2. Challenges “on Roads”
3. On-Road Functions

Status

We know the machine and the components quite well

Standards

We know the standards to apply:

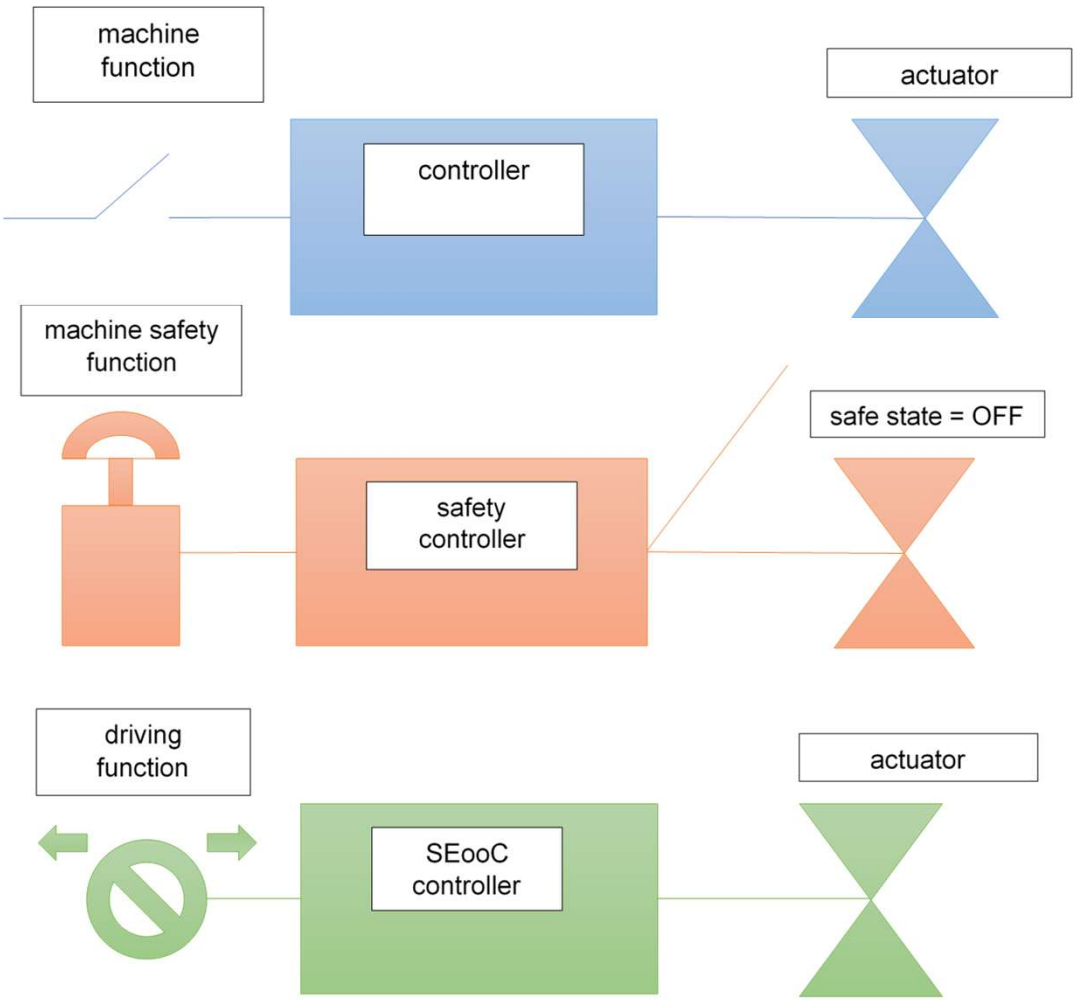
- ISO 3691 Industrial trucks
  Safety requirements
- EN12999
  Cranes – Loader cranes
- EN 13000
  Cranes –Mobile cranes
- ISO 15998 / 19014
  Earth-moving machinery
- EN 16590/ISO 25119
  Tractors and machinery
  for agriculture and forestry
- …

Controller Architecture

We know architectures for the machine functions

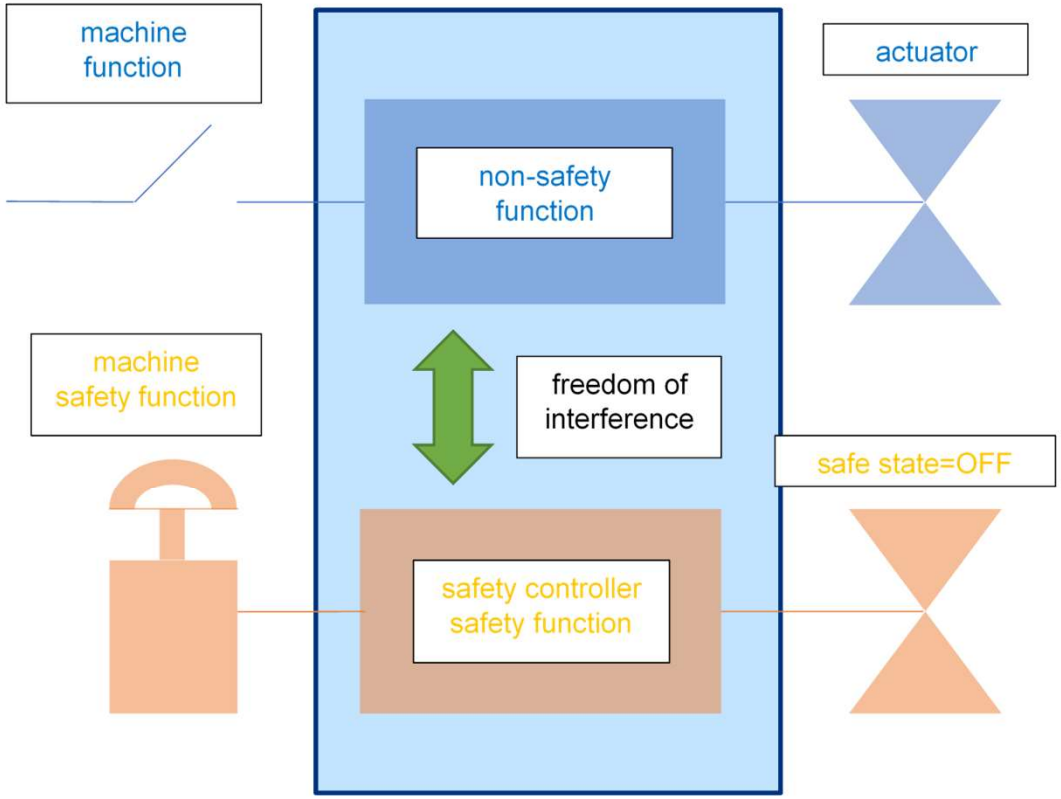
- EN ISO 13849-1 PIr
- IEC 61508 SIL

- Very often: on-road drive function



Controller Architecture

- Integration safety/ non-safety ongoing
- Less controllers to be mounted and maintained



Agenda

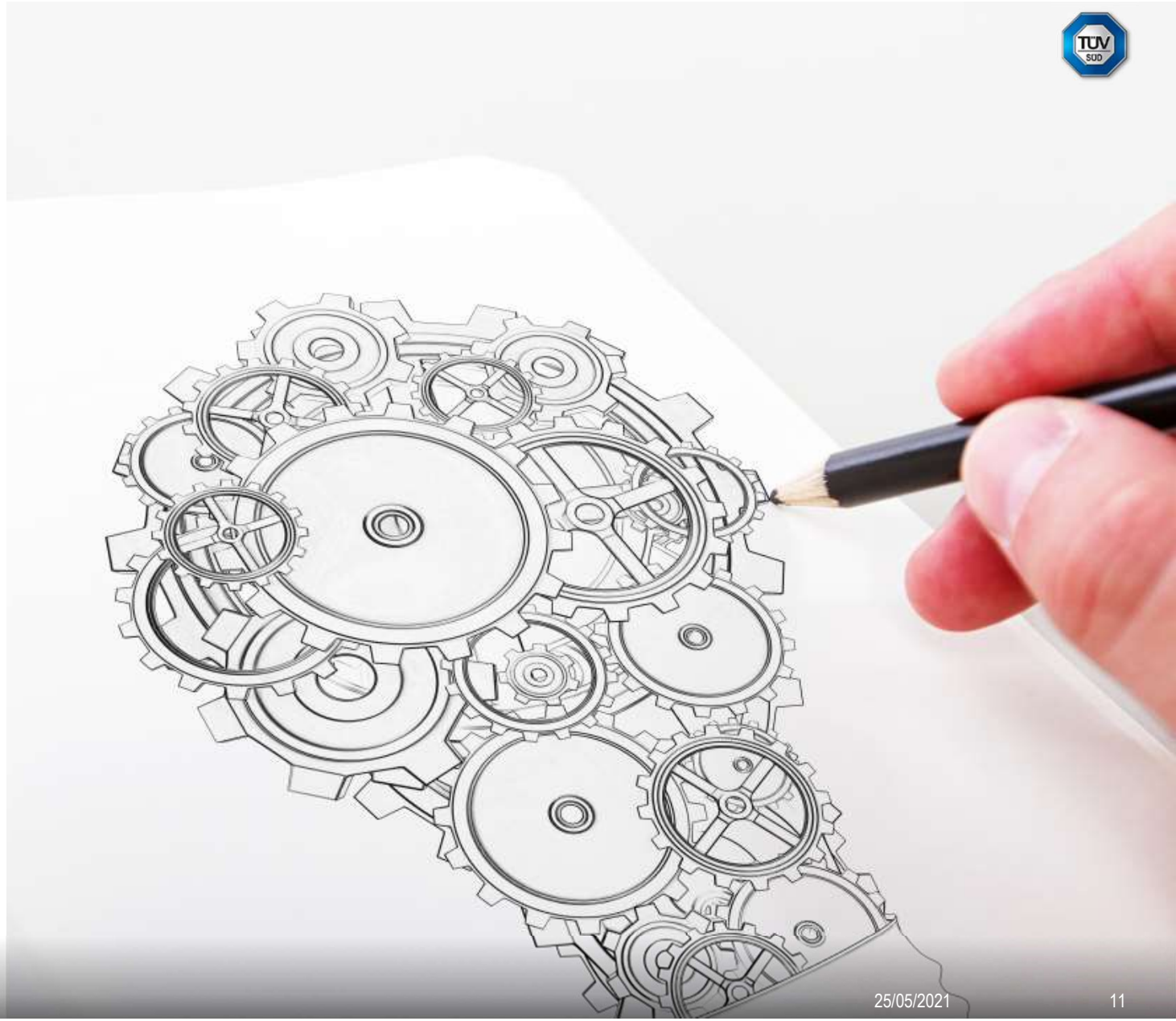
1. Current Status Mobile Maschinery
2. Challenges “on Road”
3. On-Road Functions

General

- Rising (safety) functionality
- Rising complexity
- Human centric design
  Usability vs. Responsibility

Example:

- Touchpad = high usability
- Touchpad for emergency stop?



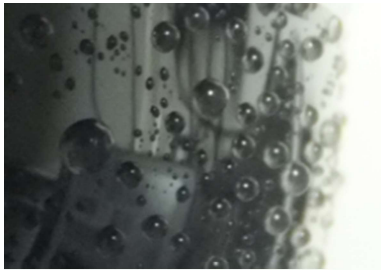
Sensors

- Environmental conditions influence accuracy of sensors and even sensoring principles
- Self-calibration?
- AI-learning based on such data?

Sensor principles

- Optical scanners offer well known safety features
- Sensor principle has to cope with robustness\false-trips if used outdoors

Increased Robustness

Sunlight	Droplets	Particles	Fog
			
Detection Principle	**Mounting position**	**Algorithm**	**Fog adaption**

Augmented Reality

- 3D container bar detection
- Obstacle detection
- Approach assistance via touchscreen
- Safety

Checkpoint:

- **Rising complexity → New development skills needed**
  - More precise definition / specification of (safety) requirements
  - Increasing interaction of HW/SW/Mechanics
  - Stricter process orientated development necessary

Checkpoint:

- **Rising complexity → New development skills needed**
  - More precise definition / specification of (safety) requirements
  - Increasing interaction of HW/SW/Mechanics
  - Stricter process orientated development necessary

- **Increasing software-based functions → Enhanced development processes needed**

Checkpoint:

- **Rising complexity → New development skills needed**
  - More precise definition / specification of (safety) requirements
  - Increasing interaction of HW/SW/Mechanics
  - Stricter process orientated development necessary

- **Increasing software-based functions → Enhanced development processes needed**

- **Rising complexity of Man-Machine-interface → User-centric design for safety needed**
  - One of the most important points: is the user still able to control a machine?
  - Shall he be? Or shall we rely more on hidden autonomous functions?
  - Can the user react: what is the purpose of a super-safe but unused emergency stop button?

Checkpoint:

- **Rising complexity → New development skills needed**
  - More precise definition / specification of (safety) requirements
  - Increasing interaction of HW/SW/Mechanics
  - Stricter process orientated development necessary

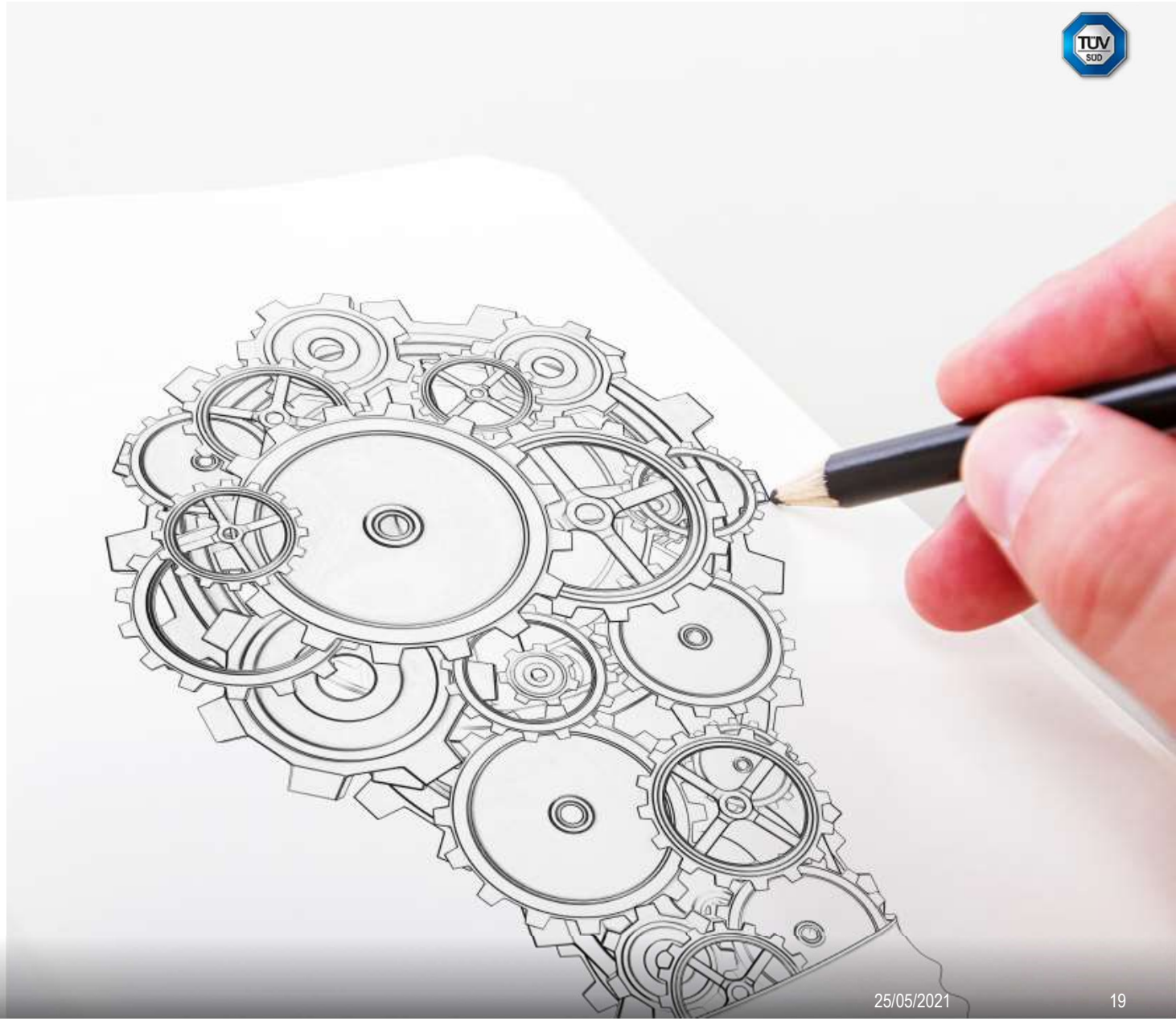
- **Increasing software-based functions → Enhanced development processes needed**

- **Rising complexity of Man-Machine-interface → User-centric design for safety needed**
  - One of the most important points: is the user still able to control a machine?
  - Shall he be? Or shall we rely more on hidden autonomous functions?
  - Can the user react: what is the purpose of a super-safe but unused emergency stop button?

- **Increasing need of computing power**
  - CPU \ Memory \ Interfaces \ Reaction times \ Bandwidth in networks and radio

Upcoming Enhancement of functions

- Semi-automatic execution
- Fully autonomous execution
- Mixed environments
- On-road



Agenda

1. Current Status Mobile Maschinery
2. Challenges “on Road”
3. On-Road Functions

On-Road

- ISO 26262-functions interface with machine functions
- Active machine functions while driving in public
  - Slow unloading
  - Positioning with VR glasses
  - Steer-by-Wire On-Road
  - Autonomous Functions
- ISO26262-compliance required?

On-Road

ISO 26262 Edition 2

- Part 8 "**supporting processes**" defines interfaces between manufacturers/suppliers using different functional safety standards

On-Road

ISO 26262 Edition 2

- Part 8 "**supporting processes**" defines interfaces between manufacturers/suppliers using different functional safety standards
- Standards like ISO 25119, machinery directive, ISO 13849-1, IEC 61508 are explicitly mentioned
- Ed.2 of ISO 26262 was released 12/2018

ISO 26262 Ed. 2 approach

"Clause 16 applies when body builder equipment developed according to another standard is integrated into a base vehicle developed according to ISO 26262."

ISO 26262 Ed. 2 approach

"Clause 16 applies when body builder equipment developed according to another standard is integrated into a base vehicle developed according to ISO 26262."

Part 8 Chapter 16 Integration of safety-related systems
not developed according to ISO 26262

ISO 26262 Ed. 2 approach

"Clause 16 applies when body builder equipment developed according to another standard is integrated into a base vehicle developed according to ISO 26262."

Part 8 Chapter 16 Integration of safety-related systems
not developed according to ISO 26262

We are allowed to claim ISO 26262 compliance based on other safety standards if the **focus is clearly on mobile machine as use case!**

Restrictions

- Not suitable for pure automotive developments
- The Maschine usage itself has to be the main Use-Case
- Steering and Control
  - Power?
  - Programing Environment?
  - Clear deduction between Safety/non-safety?

How to start – a workflow suggestion

Define use cases

How to start – a workflow suggestion

Define use cases

↓

Compare machine manufacturer needs

↓

How to start – a workflow suggestion

Define use cases

↓

Compare machine manufacturer needs

↓

Share information

↓

How to start – a workflow suggestion

Define use cases

Compare machine manufacturer needs

Share information

Compare methods & failure rates

How to start – a workflow suggestion

Define use cases

Compare machine manufacturer needs

Share information

Compare methods & failure rates

Safety case

Define Use Case

- Main application ≠ Driving on the road
- Physical conditions such as:

  Rotating cabin

  No direct steering is possible

  – ISO 26262-8 Ed. 2 chapter 16.4.2
  – “A rationale shall be given in the integrator safety case that **justifies the application of this clause**. EXAMPLE The supplier follows the safety standard ISO 13849.”

Compare Needs/Criteria

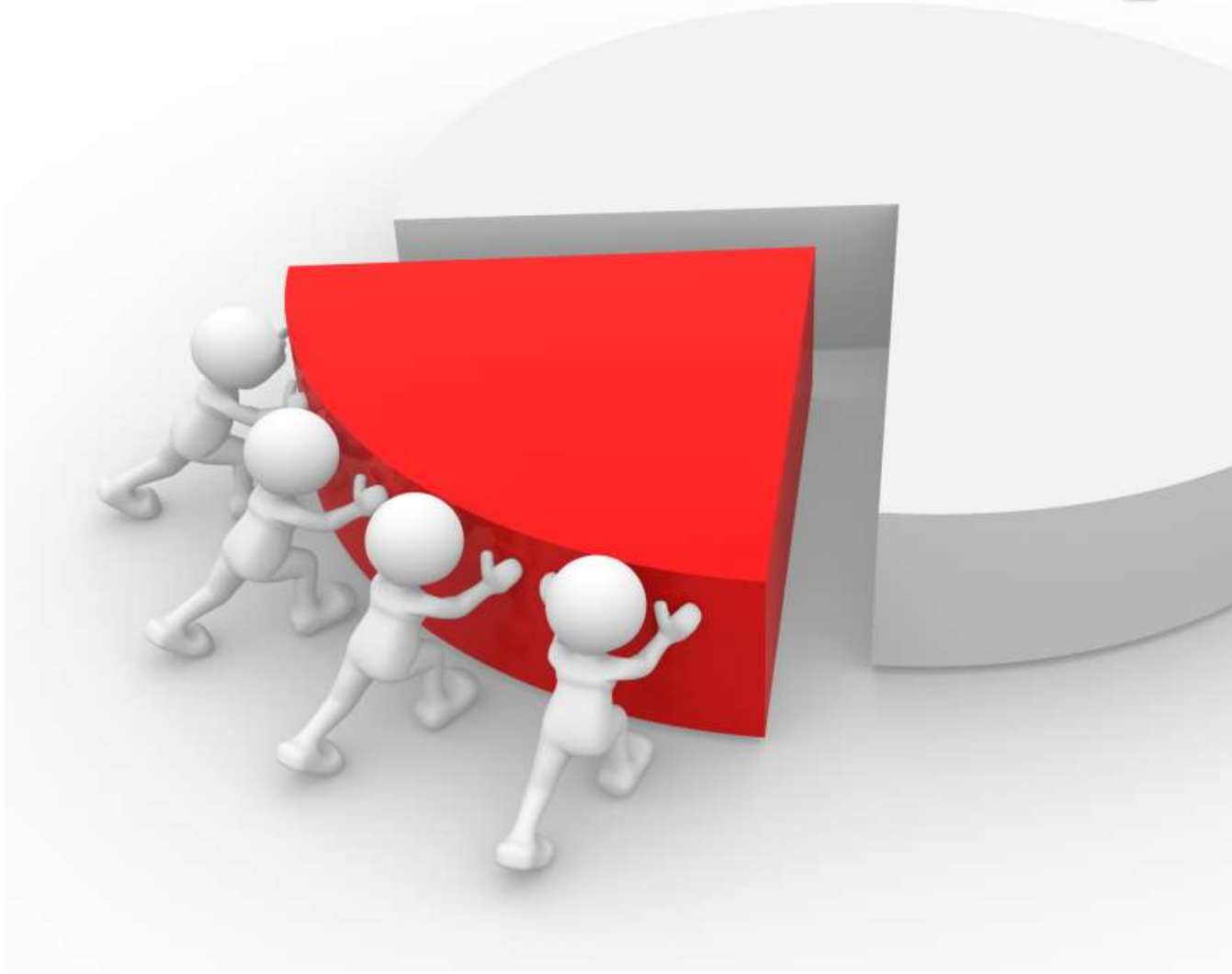
The homologation concept
must match the used components:

- ISO 26262-8 Ed. 2 chapter 16.4.3
- “The integrator shall define the criteria to argue that the safety-related system that has been developed to another safety standard meets the required level of functional safety.
  EXAMPLE 1 A mapping between ASIL and PL
  (Performance Level as used in ISO 13849)”

Share Information

Information needs to be shared between the integrator and the supplier

- ISO 26262-8 Ed. 2 chapter 16.4.3
- “The integrator shall define the criteria to argue that…”
  “NOTE The criteria address the design **process**, the product **design**, **qualification** measures and **approval** process.”



Compare Methods and Failure Rates

Methods and values must be compared

– “EXAMPLE 2 Comparison of requirements regarding applied methods and requested failure rates of different safety standards.”
  - FMEDA
  - multiple point failures (latent fault matrix)
  - SW Tables IEC 61508 und
  ISO 26262-SW-measures

Agreement?

– ISO 26262-8 Ed. 2 chapter 16.4.4
"The integrator and supplier shall agree on the relevant set of measures to verify that the criteria are met.

EXAMPLE A set of measures can be:
— availability of the specification …
— evidence …by test report
— …analysis …by FMEA, FTA, …
—…suitable for its intended use
—...adequate approval process by PPAP
— …life testing, environmental testing, testing beyond specification limits, robustness testing;
— analysis of field data"

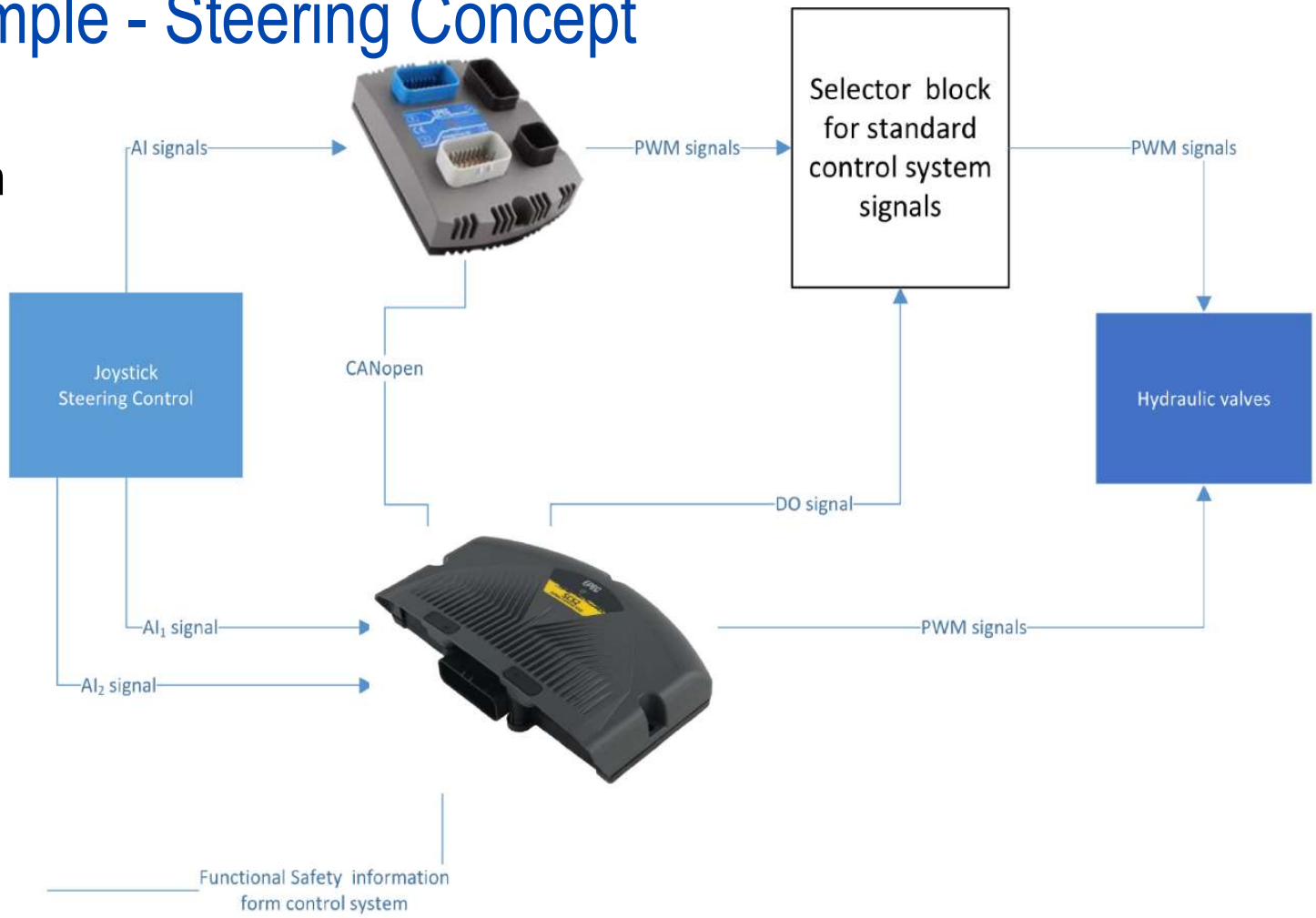
Safety Case

Summarized of existing(enhanced) and new documents

- ISO 26262-8 Ed. 2 chapter 16.5 Work products
- “16.5.1 Safety rationale resulting from requirements 16.4.2 to 16.4.4”

Mobile Machinery Example - Steering Concept

- No loss of steering function with a single failure
- Performance Level needed
- Conform to
  ISO 19014-1
  ISO 5010
  ISO 13849-1



Summary Use of generic standards

Machinery standards currently point to ISO EN 13849-1
The used approach to Functional Safety can be incompatible for functions like e.g.

- Algorithms
- Autonomous Functions
- Artificial Intelligence (AI)

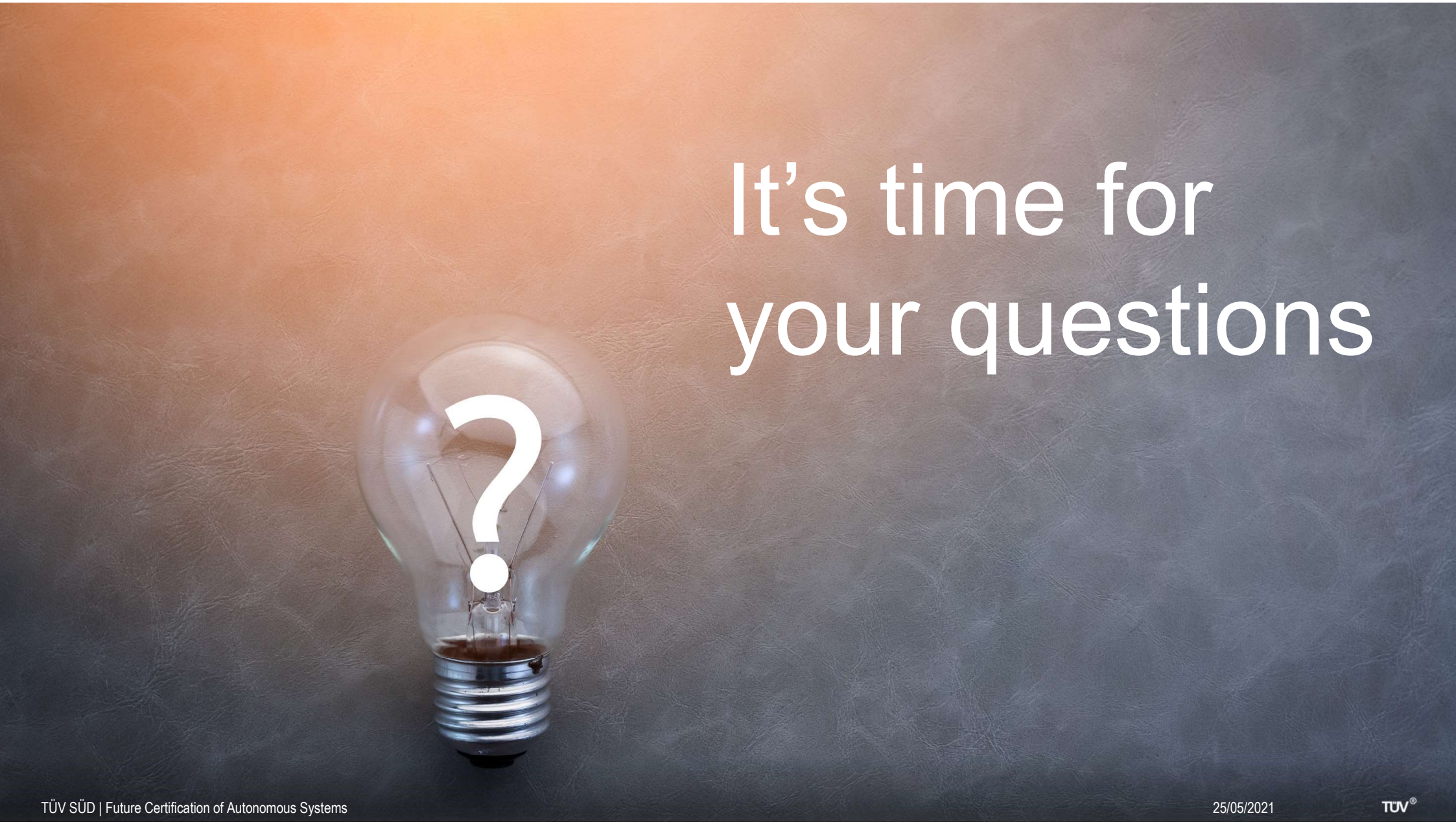
What we need:

- Different criteria than Category or Performance Level
- Process oriented working style
- Strictly requirement oriented approach and use cases
  (V&V at a final machine will not find all potential failures)

This is more like IEC 61508 or ISO 26262

Summary: A bit further down the road…

- AI
- „Smart“ Automation


It’s time for
your questions