

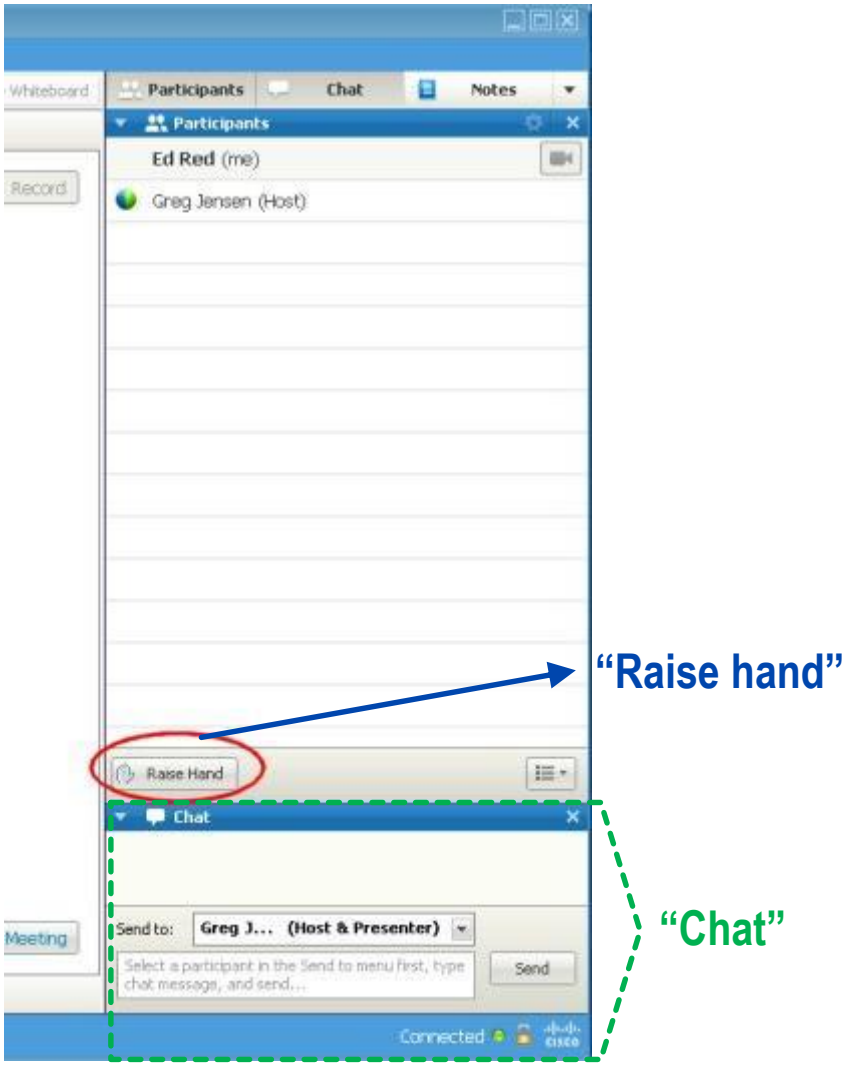
Safety-related Motor Drives and 2nd Edition of IEC 61800-5-2

Use and Design

08 May 2017

Choose certainty.
Add value.

Housekeeping



- Everyone will automatically be placed on "mute mode once the session begins to reduce background noise.
- Please send in any questions you may have through the WebEx **"Q&A"** function to the host. The questions will be answered at the end of the session.
- Alternatively, you can also use the WebEx "Raise hand" function during the "Q&A" session to ask any questions.
- The session will be recorded and made available for download.

Our Expert: Dr. Thomas Maier

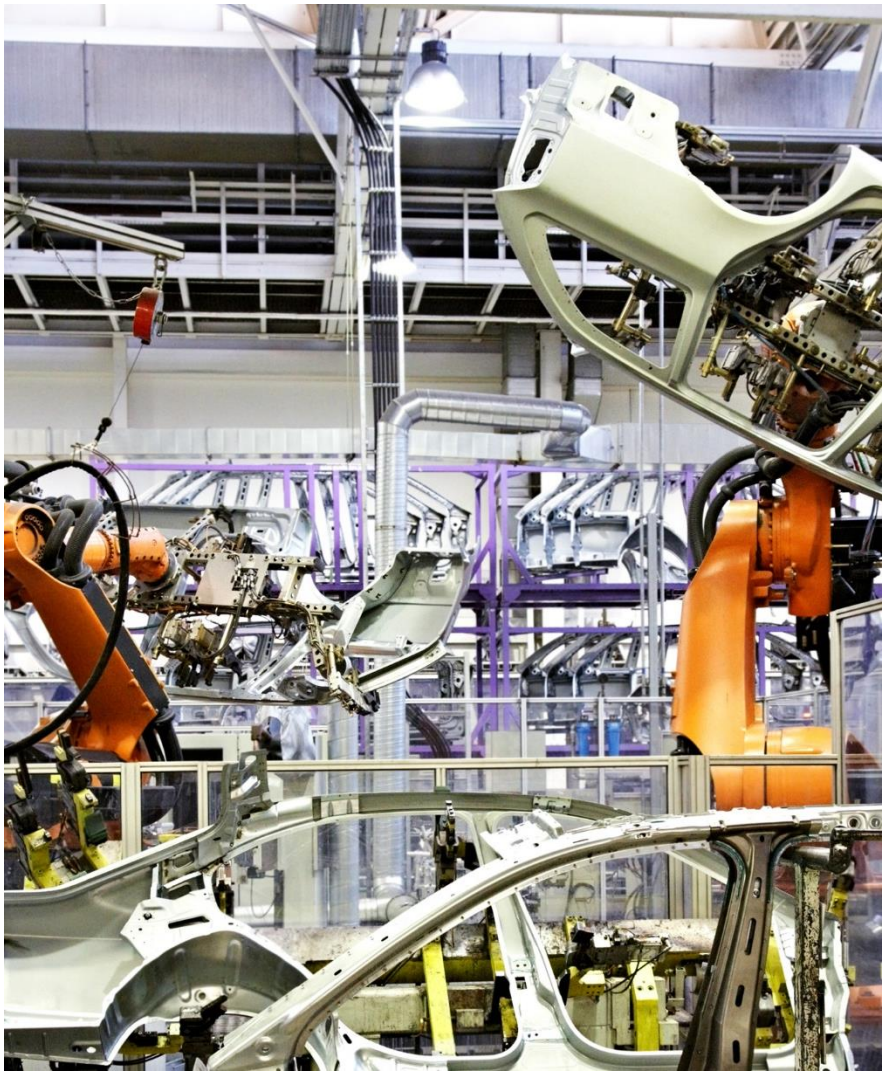


Dr. Thomas Maier
Business Development Manager at TÜV SÜD Rail since July 2016

Background:

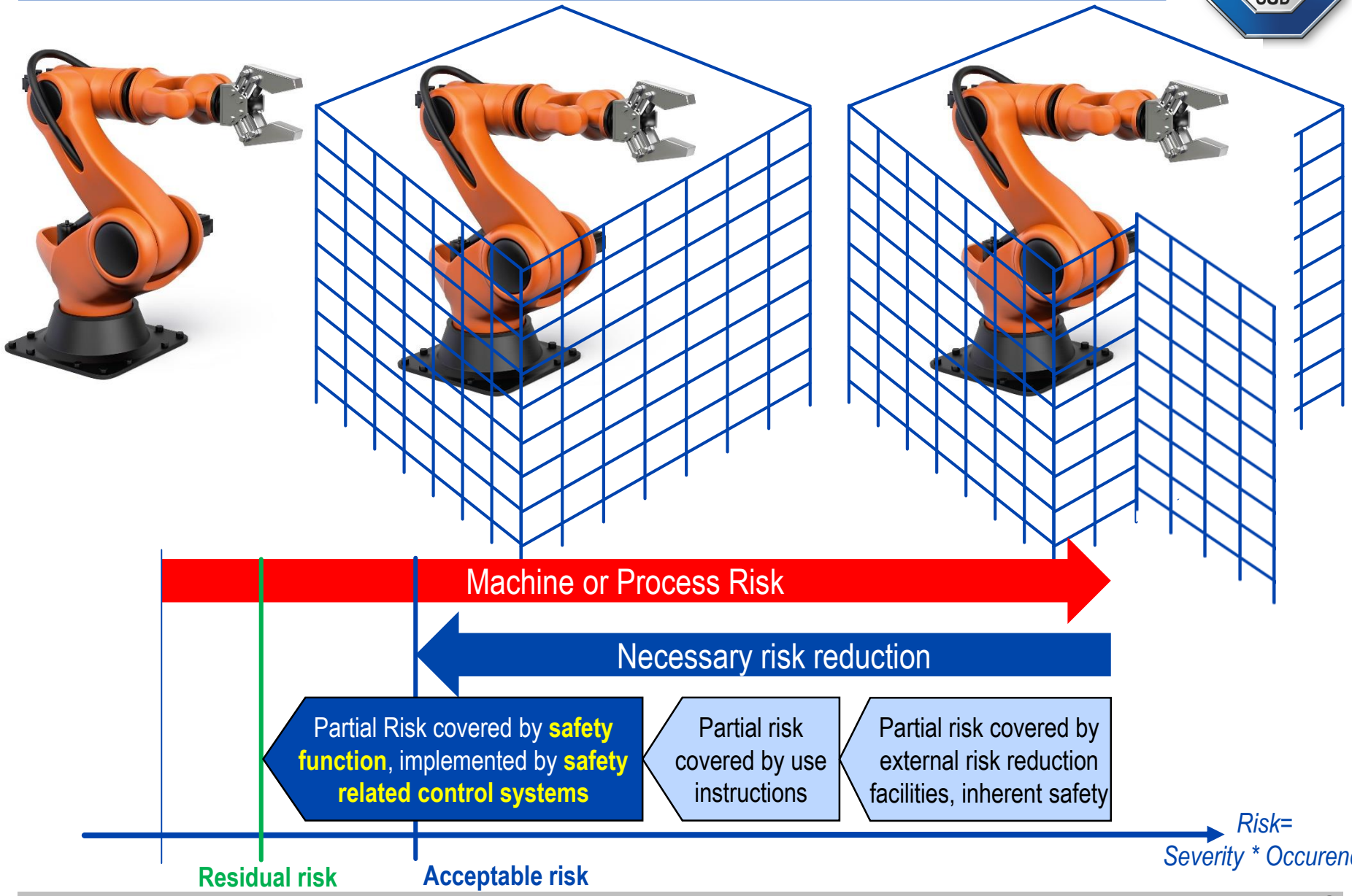
- 6 years at UL, principal engineer for functional safety
- 8 years with Danfoss Drives, functional safety in motion control.
- 3 years at LM Ericsson A/S: software processes and tools, CMMi, UML and SDL
- 3 years at Daimler-Benz: system safety and functional safety of drive-by-wire systems and in avionics.
- 4 years at the Joint Research Centre of the European Commission: system & software safety in fusion technology.
- International standardization (ISO 26262, ISO 13849 & IEC 62061, IEC 61800-5-2, IEC 61508 maintenance, UL 1998).
- Dr.-Ing. from University of Stuttgart

Agenda

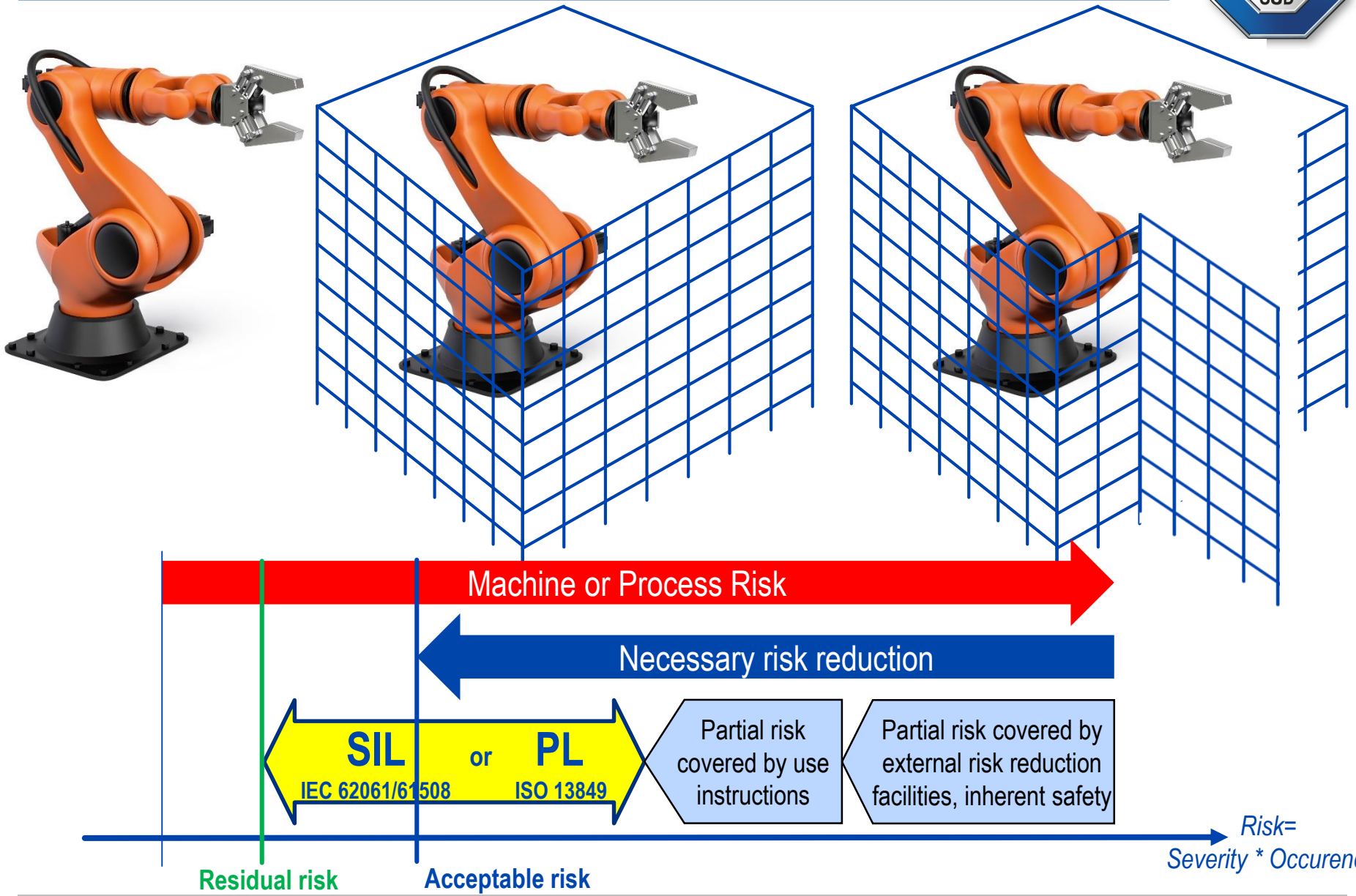


1. What is functional safety (FS)
2. FS standards and regulations
3. Scope and contents of IEC 61800-5-2 - User perspective
4. Application examples for STO, SS1, SLS
5. Implementation-related contents - Manufacturer perspective
6. Future standardisation efforts

Functional Safety



Functional Safety



Measurement of Safety Performance

… the required safety performance is dependent upon the risks.

SIL (Safety Integrity Level) or PL (Performance Level) are discrete levels of safety performance.

Main parameter of a SIL, PL is a probability of dangerous failure per hour (PFH):

PL (ISO 13849)	PFH target values	SIL (IEC 61508/IEC 62061)
a	≥ 10^{-5} to < 10^{-4}	no correspondence
b	≥ 3 x 10^{-6} to < 10^{-5}	1
c	≥ 10^{-6} to < 3 x 10^{-6}	1
d	≥ 10^{-7} to < 10^{-6}	2
e	≥ 10^{-8} to < 10^{-7}	3

This is not the only parameter of a SIL or PL! They address also:

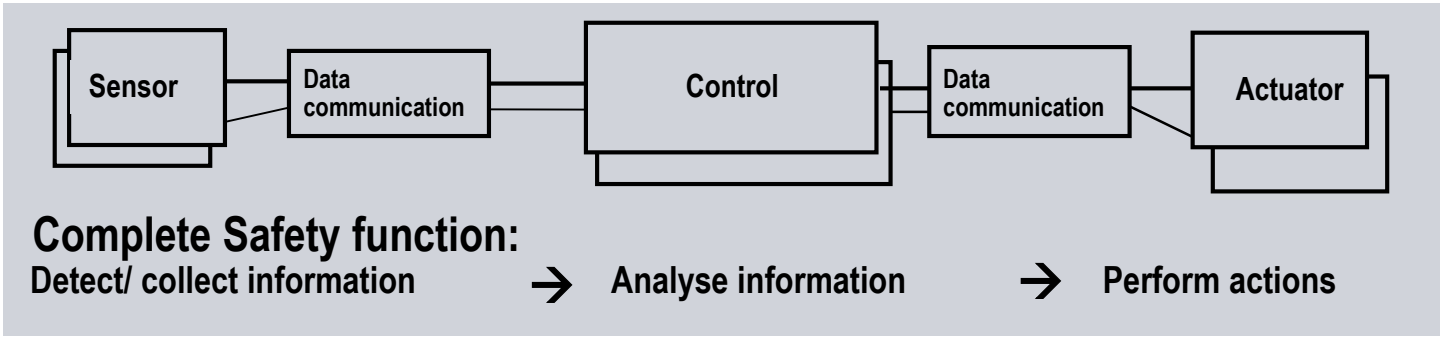
- Hardware Architecture in terms of
  - Redundancy („HFT“, „Category“)
  - Diagnostic Capabilities („SFF“, „DC“)

Control
of random hardware failures
(shorts, open, couplings, value change, functional failures, …)

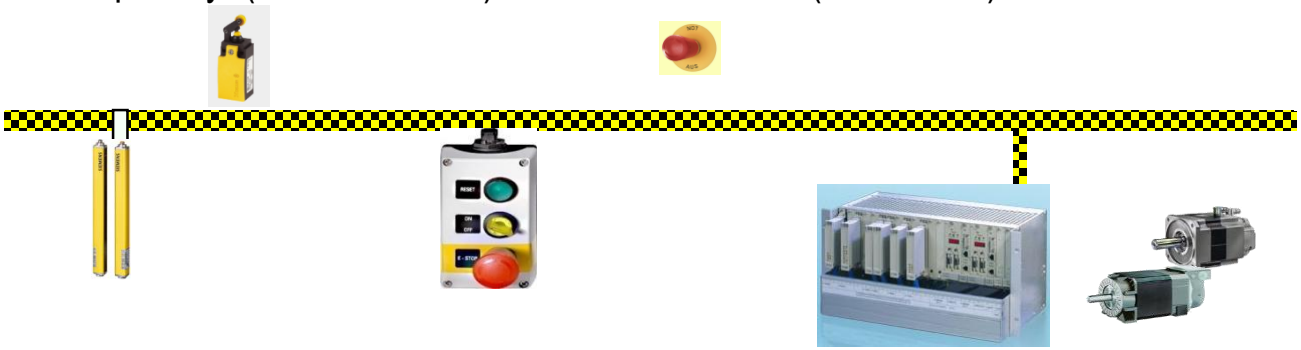
- Systematic capability
  - Processes, methods, tools
  - Environmental immunity (EM, …)

Avoidance
of systematic failures
(design faults, installation faults, environmental impacts, …)

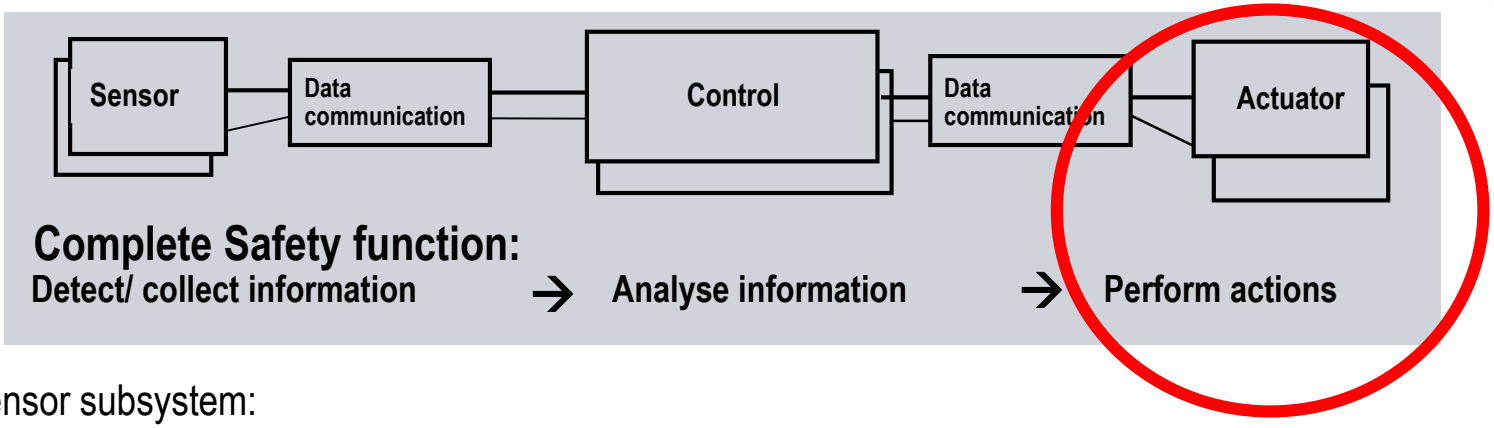
Safety function and safety-related system



- SIL / PL applies (initially) to a complete safety function, implemented by a cpmplete safety-related control system
- A safety-related control system consists of subsystems (typically sensor, control, actuator, possibly also data communication) with their safety sub-functions
- Each subsystem contributes to the overall PFH (PFHsystem = Σ PFHsubsys$_i$)
- Each subsystem must have architectural integrity and systematic integrity in accordance with SIL ("weakest link rule")
  - "SIL Capability" (IEC 61800-5-2) or "SIL Claim Limit" (IEC 62061) of sub-functions and subsystems



Functional safety standards at subsystem/sub-function level

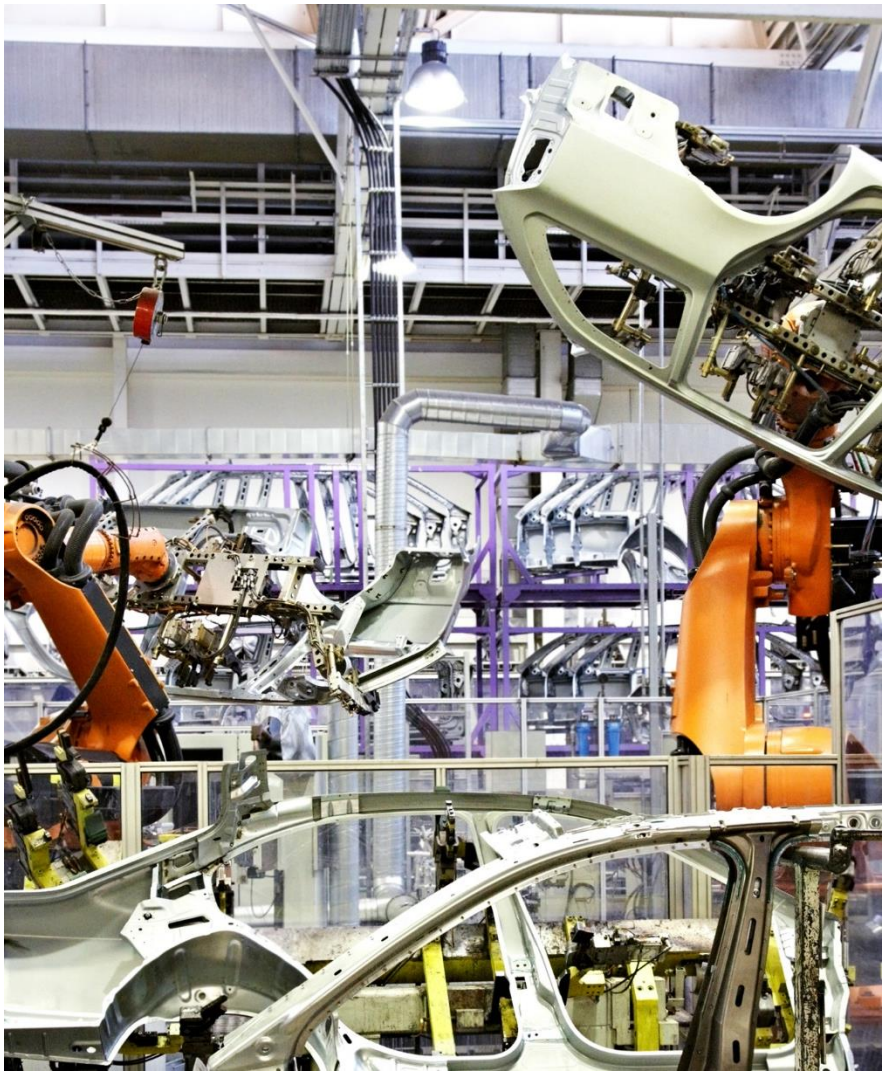


- Sensor subsystem:
  - eg. IEC 61496 (light curtains)
- Control subsystem:
  - eg. IEC 61131-6 (Safety PLC's)
- Actuator subsystem:
  - eg. IEC 61800-5-2 (Safety-related motor drives ("PDS(SR)")
- Data communication subsystem:
  - eg. IEC 61784-3

IEC 61800-5-2
Safety-related motor drives
(may include portions of safety-related data comm and control logic)

- IEC 62061, ISO 13849, and generally IEC 61508, can also be applied on subsystem-level!
  - In particular if no subsystem-level FS standard exists (eg for safety-related encoders, valves, …)
  - Subsystem manufacturers usually declare compliance in addition to the applicable subsystem standard
    - Compliance with further application-level FS standards is often declared (IEC 61511, EN 50156, …)

Agenda



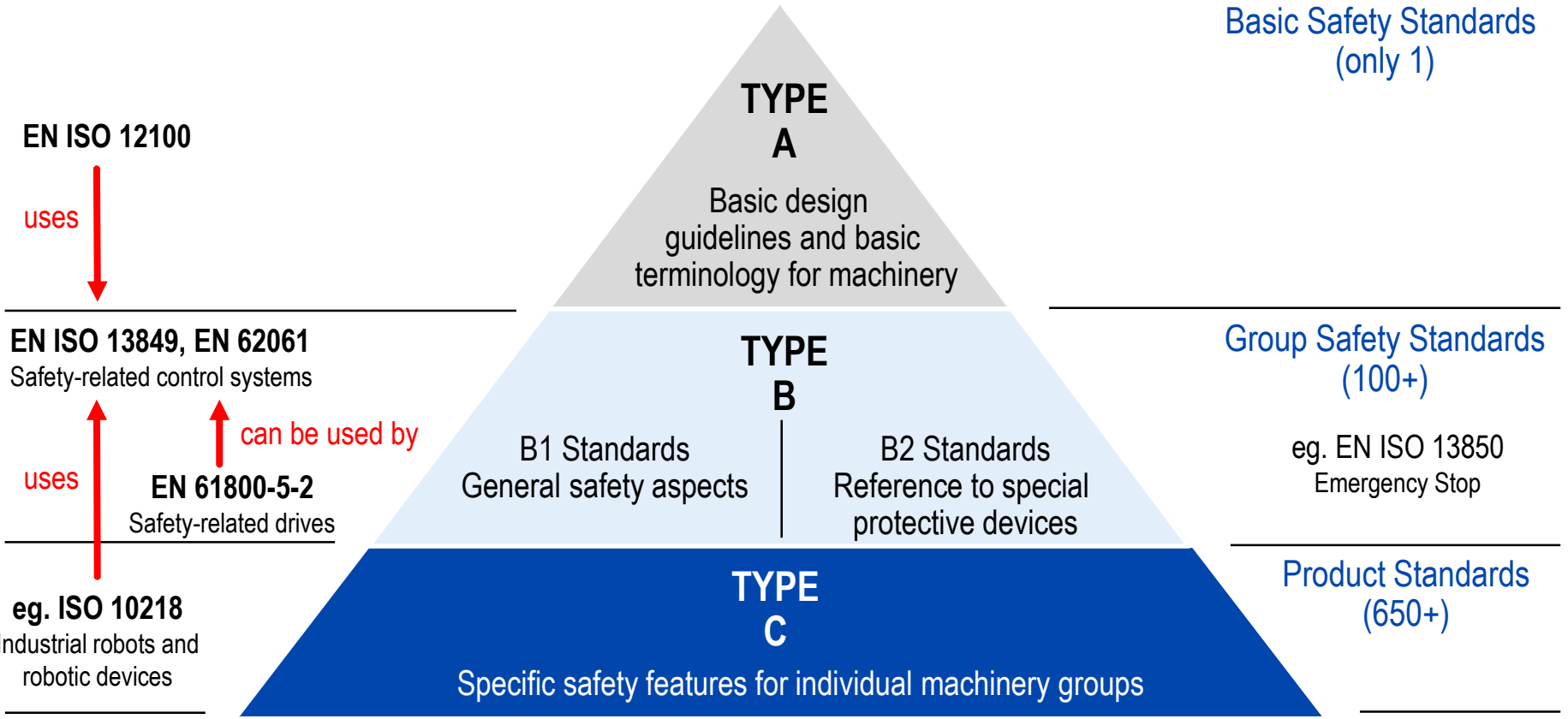
1. What is functional safety (FS)
2. FS standards and regulations
3. Scope and contents of IEC 61800-5-2 - User perspective
4. Application examples for STO, SS1, SLS
5. Implementation-related contents - Manufacturer perspective
6. Future standardisation efforts

EU Machinery Directive and Harmonised Standards

Basic Safety Requirements (EC Treaties)

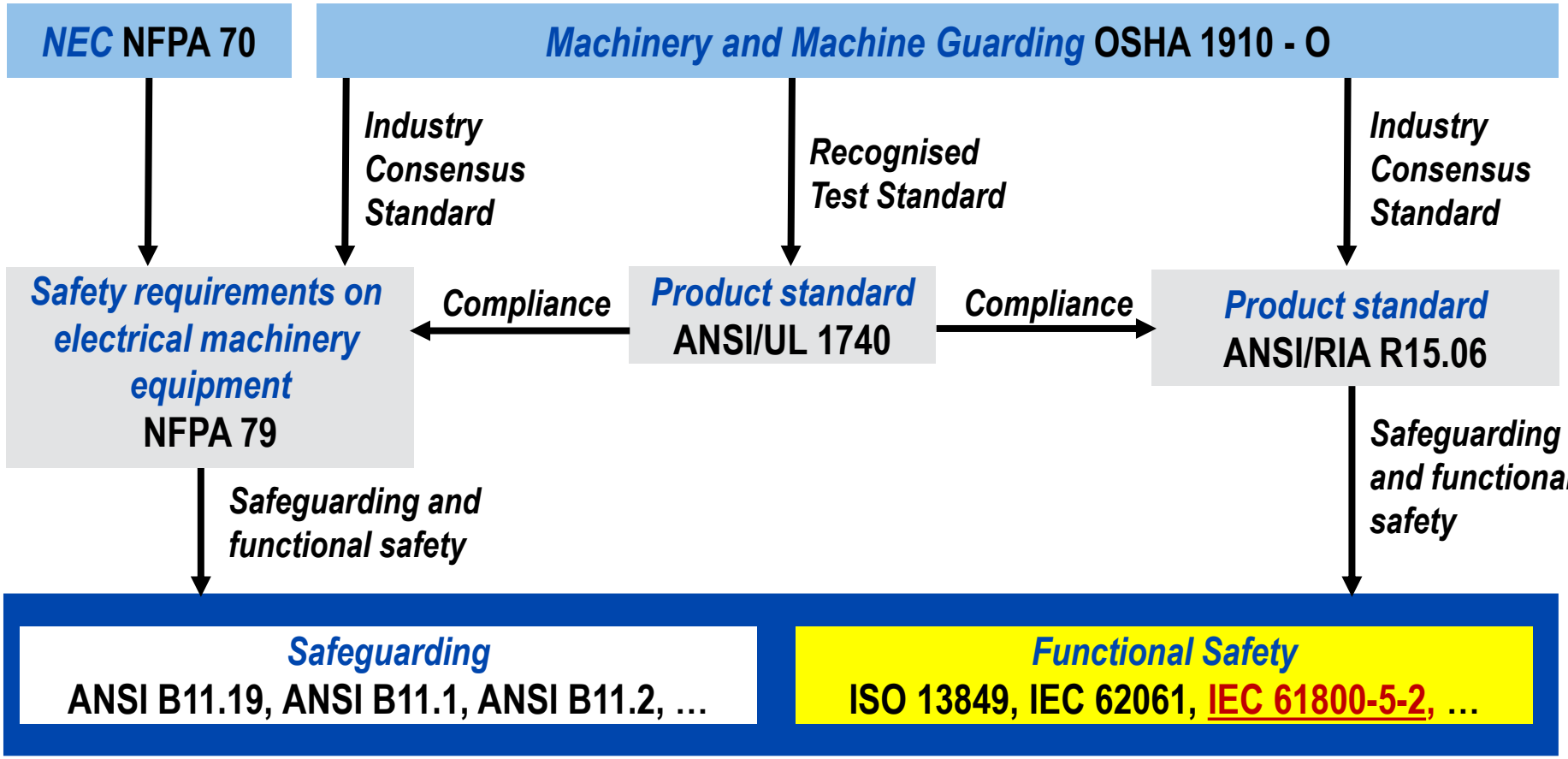
Machinery Directive 2006/42/EC

Harmonised Standards, Presumption of Conformity



US Regulations and Standards (example: robotics)

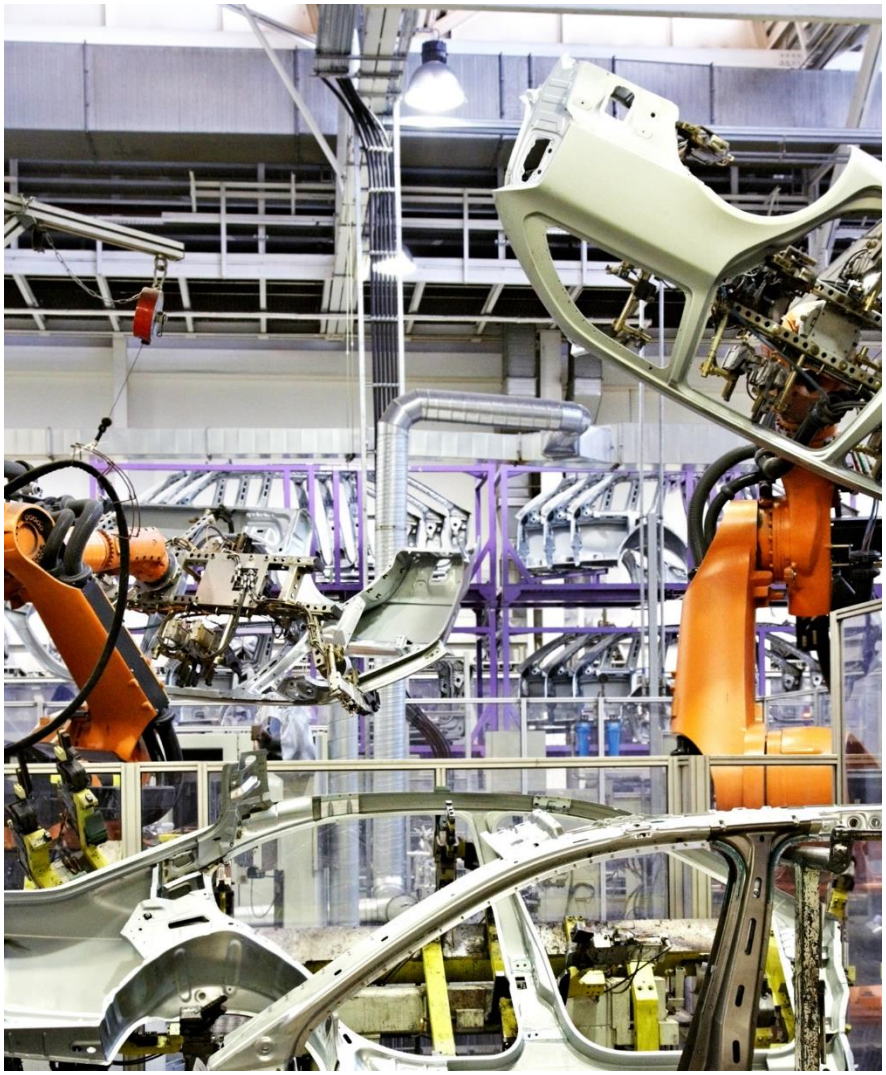
Key standard for machine safety: **NFPA 79**



IEC 61800-5-2 (Ed.1.0) references in NFPA 79:2015

- **9.2.5.4.1.4*** Where a Category 0 or Category 1 stop is used for the emergency stop function, it shall have a circuitry design (including sensors, logic, and actuators) according to the relevant risk as required by Section 4.1 and 9.4.1. Final removal of power to the machine actuators shall be ensured and shall be by means of electromechanical components. Where relays are used to accomplish a Category 0 emergency stop function, they shall be non retentive relays.
- *Exception: Drives, or solid state output devices, designed for safety related functions shall be allowed to be the final switching element, when designed according to relevant safety standards.*
- **A.9.2.5.4.1.4** IEC 61508 and **IEC 61800-5-2** give guidance to the manufacturer of drives on how to design a drive for safety related functions.
- **9.4.3.4* Use in Safety-Related Functions.**
  - **9.4.3.4.1** Software- and firmware-based controllers to be used in safety-related functions shall be listed for such use.
  - **9.4.3.4.2** Control systems incorporating software- and firmware-based controllers performing safety-related functions shall be self-monitoring and conform to all of the following:
    - (1) In the event of any single failure, the failure shall:
      - (a) Not lead to the loss of the safety-related function(s)
      - (b) Lead to the shutdown of the system in a safe state
      - (c) Prevent subsequent operation until the component failure has been corrected
      - (d) Prevent unintended startup of equipment upon correction of the failure
    - (2) Provide protection equivalent to that of control systems incorporating hardwired/hardware components
    - (3) Be designed in conformance with an approved standard that provides requirements for such systems
- **A.9.4.3.4** IEC 62061, ISO 13849-1, and ISO 13849-2 provide requirements for the design of control systems incorporating the use of software- and firmware-based controllers to performing safety-related functions. IEC 61508 provides requirements for the design of software- and firmware-based safety controllers**. IEC 61800-5-2** and IEC 61508 give guidance to the drive manufacturer on the design of drives intended to provide safety functions.

Agenda



1	What is functional safety (FS)
2	FS standards and regulations
3	Scope and contents of IEC 61800-5-2 - User perspective
4	Application examples for STO, SS1, SLS
5	Implementation-related contents - Manufacturer perspective
6	Future standardisation efforts

Scope of IEC 61800-5-2:2016

- Requirements for the design and development, integration and validation of **safety-related power drive systems (PDS(SR)).**
- Basis for manufacturers and suppliers of *PDS(SR)*s to indicate to users the safety performance for their equipment.
- Facilitate incorporation of a *PDS(SR)* into a safety-related system in compliance with IEC 61508, IEC 61511, IEC 62061 or ISO 13849.
- High demand or continuous mode of operation
- Limited to maximally SIL 3 per IEC 61508

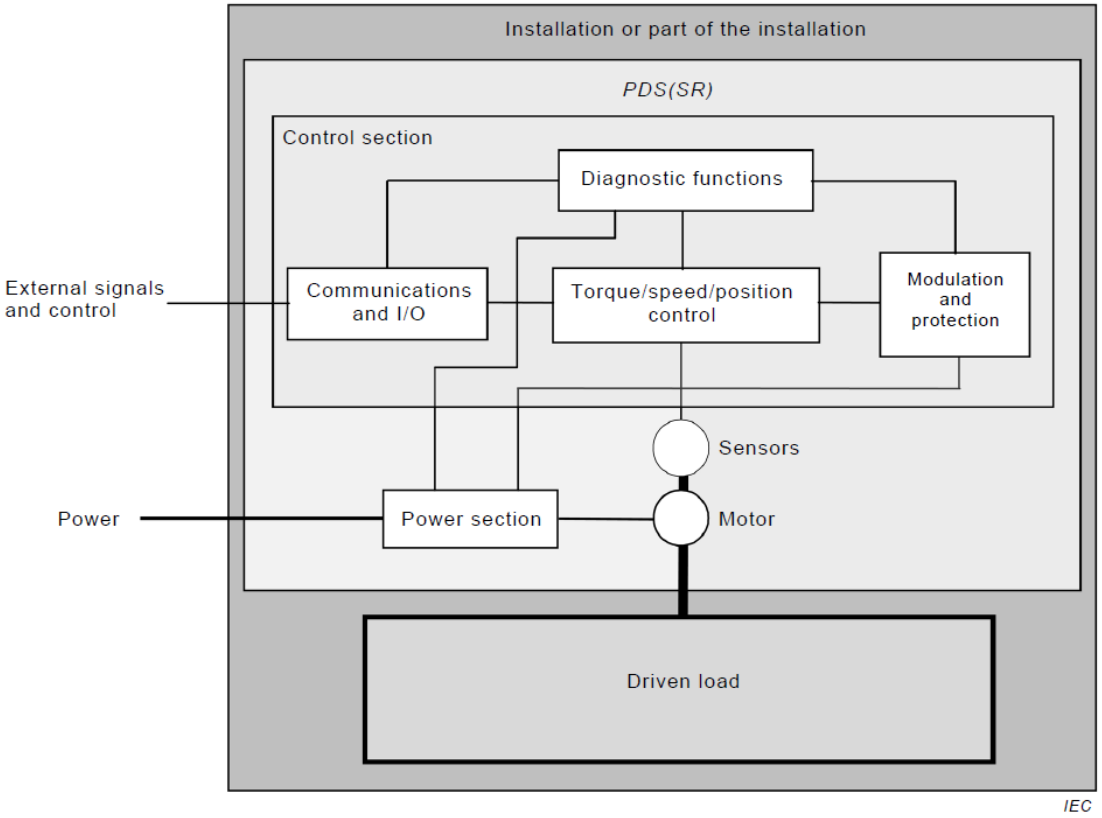


Figure 1 – Installation and functional parts of a *PDS(SR)*

Important contents – user perspective (blue: new in 2nd ed)

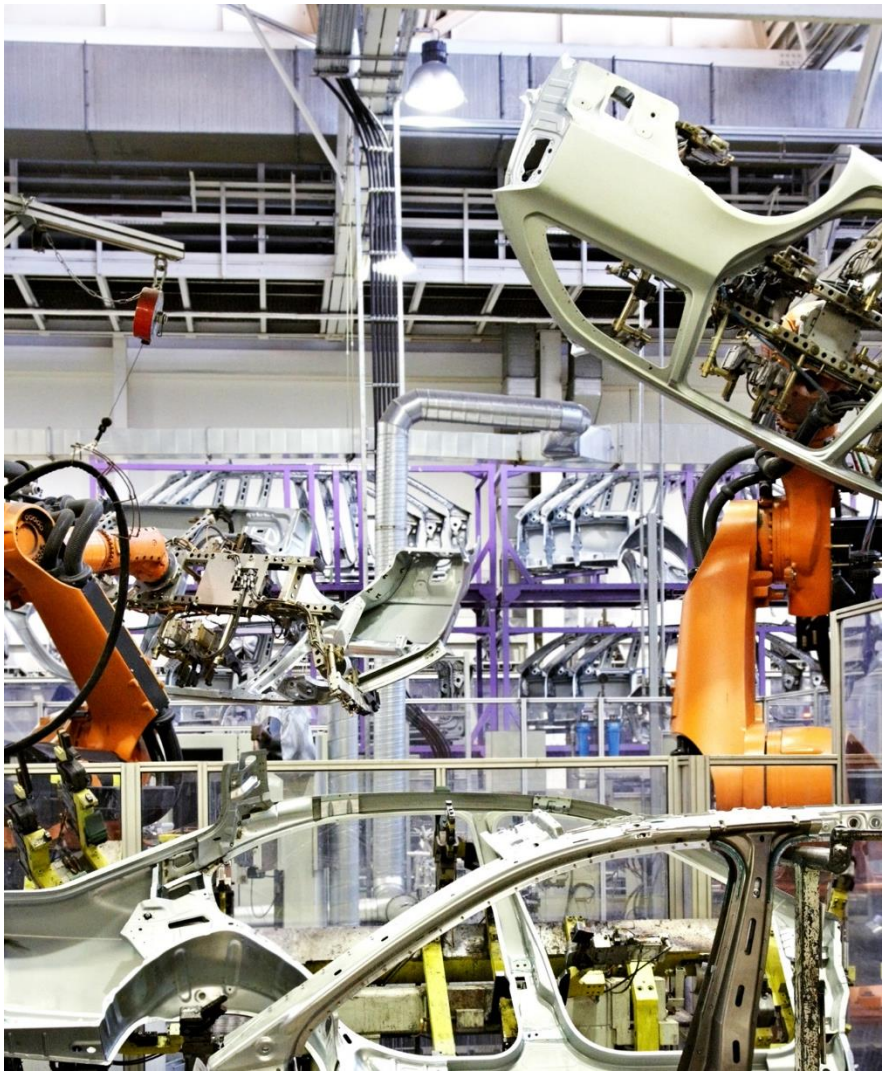
(Selection – list is not complete)

- Designated safety sub-functions:
  - Stopping functions STO, SS1(-d, -r, -t), SS2
  - Monitoring functions, based on safety-related …
    - … speed information: SLS, SDI, SLA, …
    - … position information: SLP, SLI, SOS, …
  - Output functions: SBC (Safe brake control)

- Relationship to ISO 13849 fortified:
  - Awareness that some type C standards currently refer to ISO 13849-1. In this case, *PDS(SR)* manufacturers may be requested to provide category and PL to facilitate the integration in the safety-related control systems.
  - „category“ and „performance level“ defined

- Diagnostic test intervals when HFT=1 and testing requires disrupting the application
  - one test per year for SIL 2, PL d / category 3;
  - one test per three months for SIL 3, PL e / category 3;
  - one test per day for SIL 3, PL e / category 4.

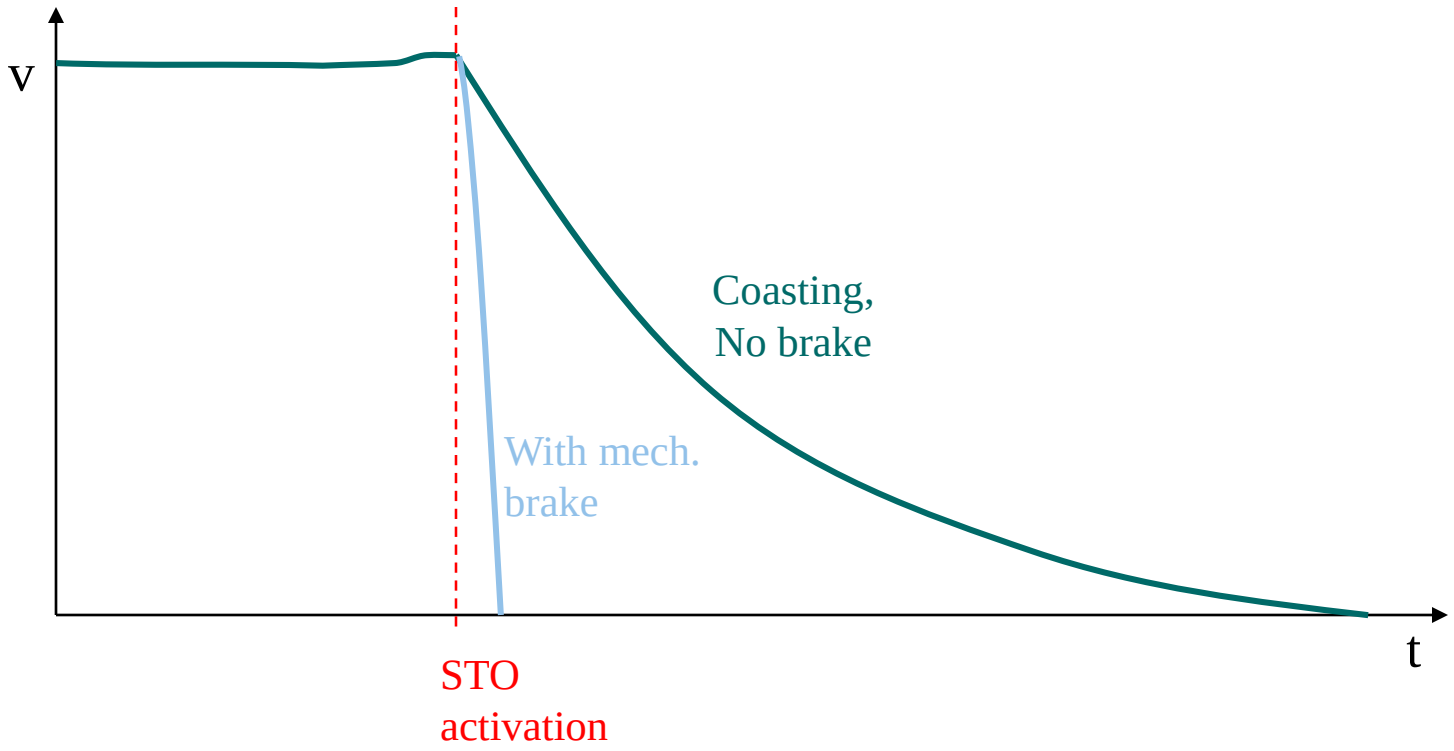
Agenda



1. What is functional safety (FS)
2. FS standards and regulations
3. Scope and contents of IEC 61800-5-2 - User perspective
4. Application examples for STO, SS1, SLS
5. Implementation-related contents - Manufacturer perspective
6. Future standardisation efforts

Safe Torque Off (STO)

"This function prevents force-producing power from being provided to the motor"

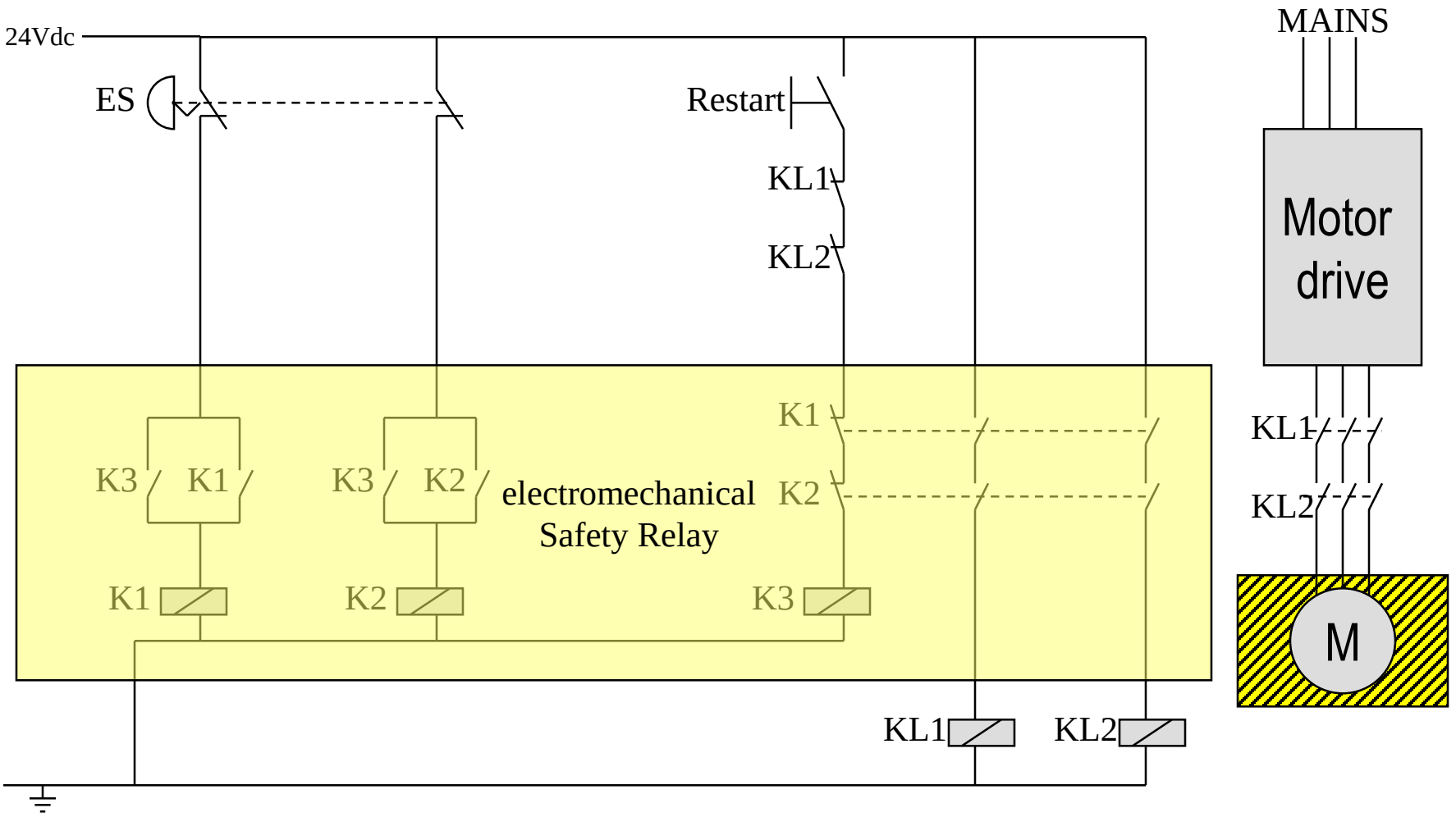


Application of “Safe Torque Off”

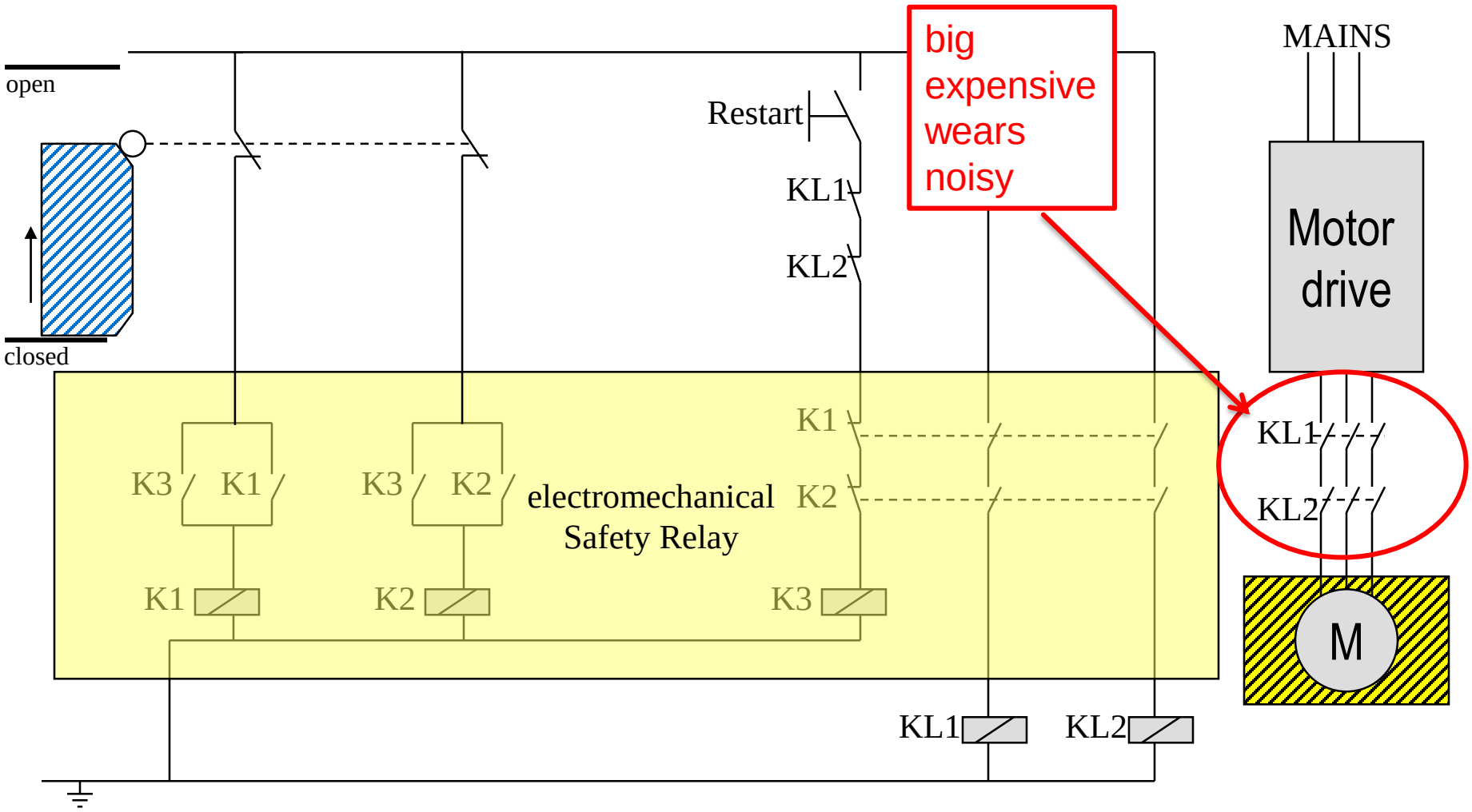


- Machine safety
  - ➢ To realise a Stop Category 0 (per IEC 60204-1, NFPA 79), which in turn is the basis for implementing
    - Emergency stop
    - Prevention of unintended or unexpected start up
- Elevators
  - ➢ To prevent hazardous movements
    - per A17.1 in USA and EN 81 in EU

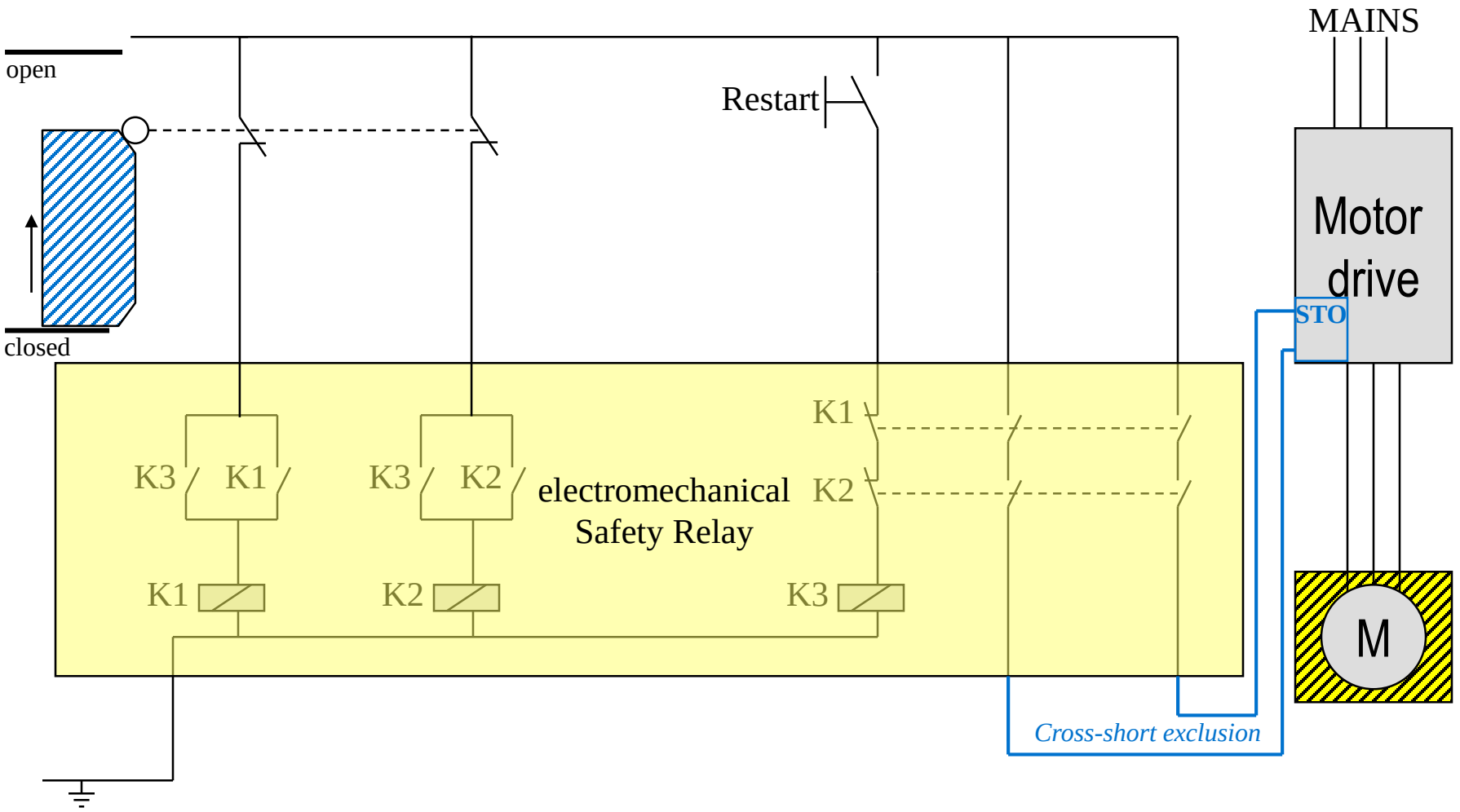
Emergency stop / STO, “conventional” functional safety



Unintended start-up prevention/STO, “conventional” functional safety

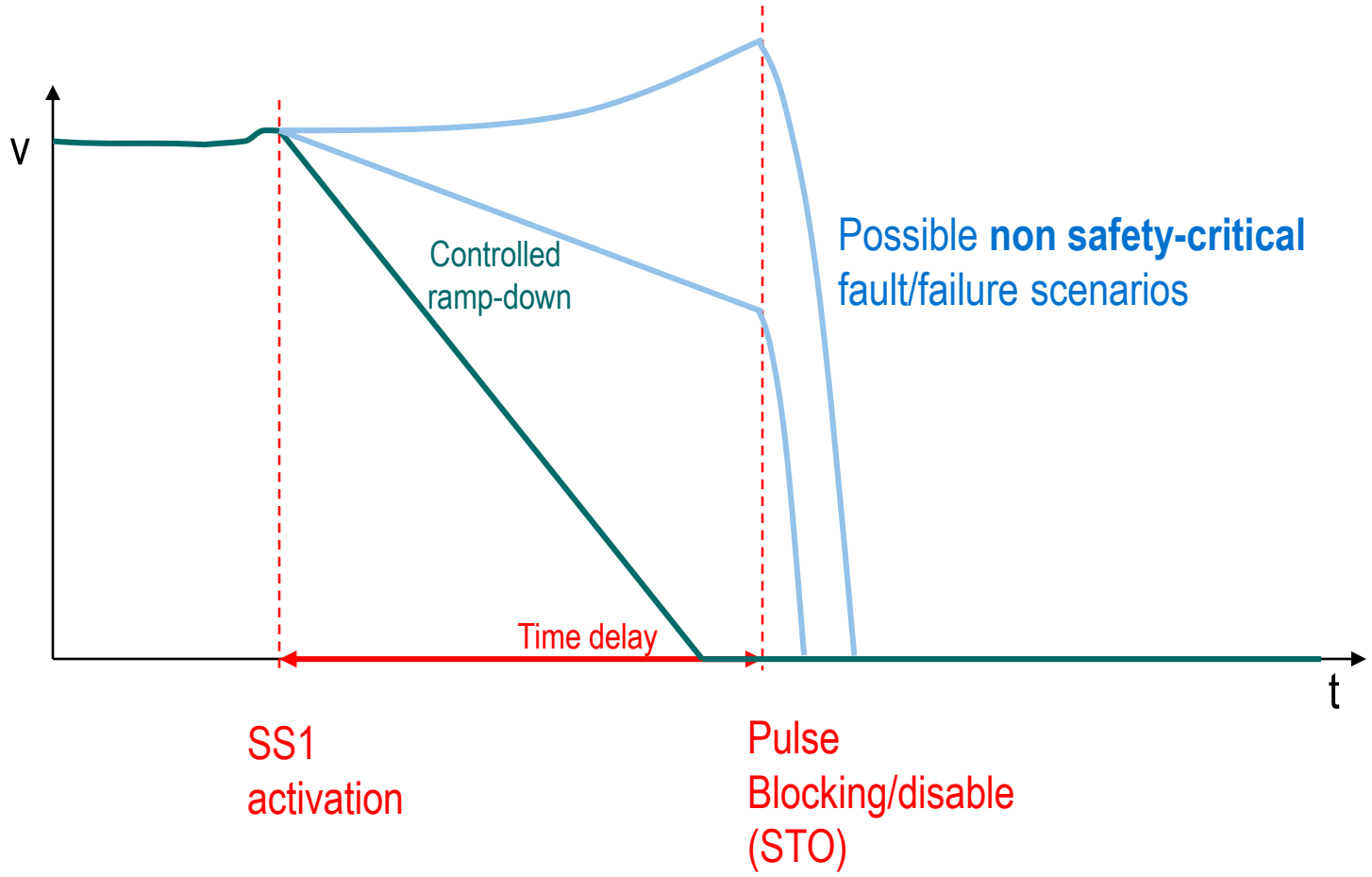


Unintended start-up prevention/STO integrated in motor drive (“safe pulse blocking”, electronic circuits)

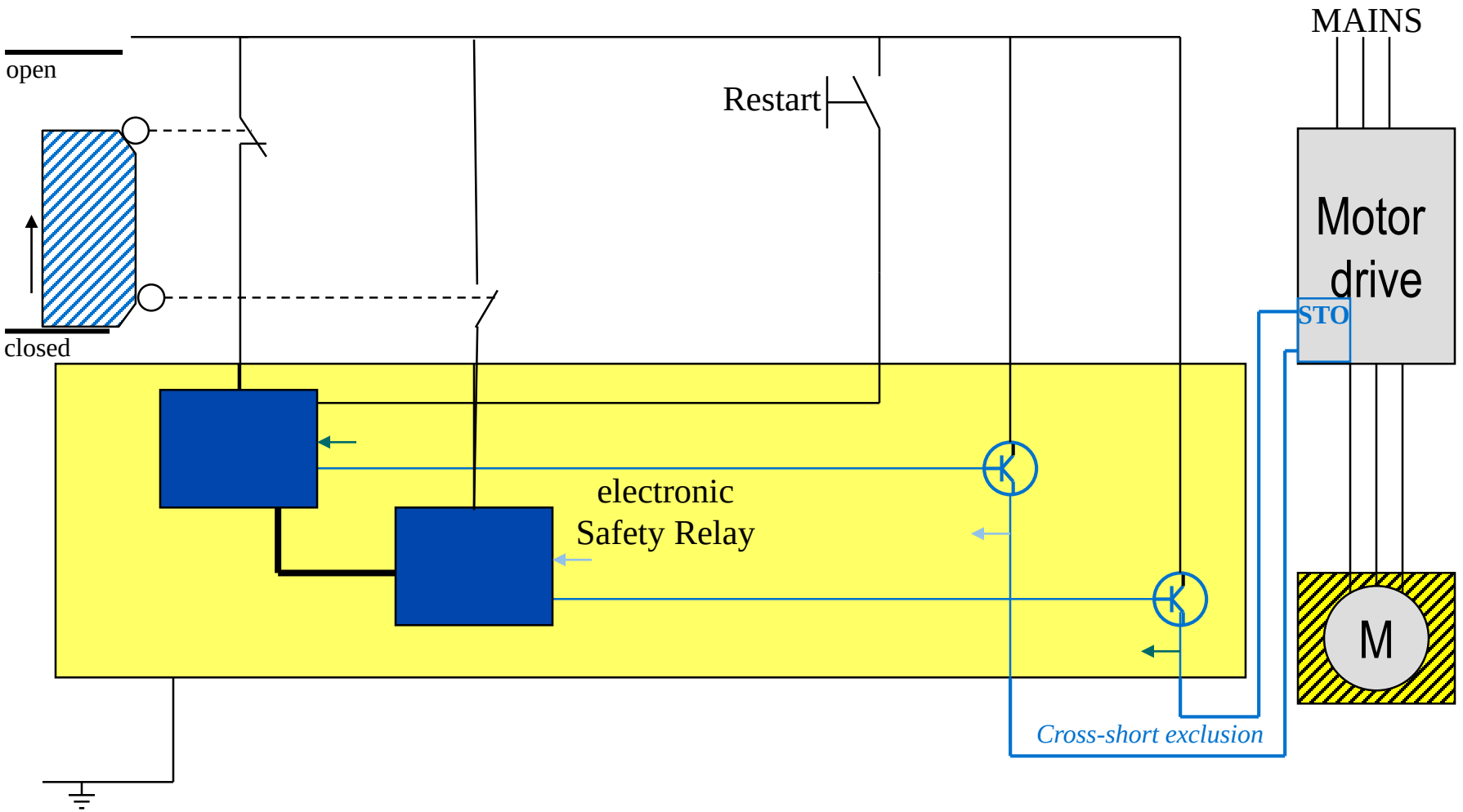


Safe Stop 1-t (SS1-t)

"Initiates the motor deceleration and performs the STO function after an application specific time delay."



Example: electronic safety relay to implement safety-related timer

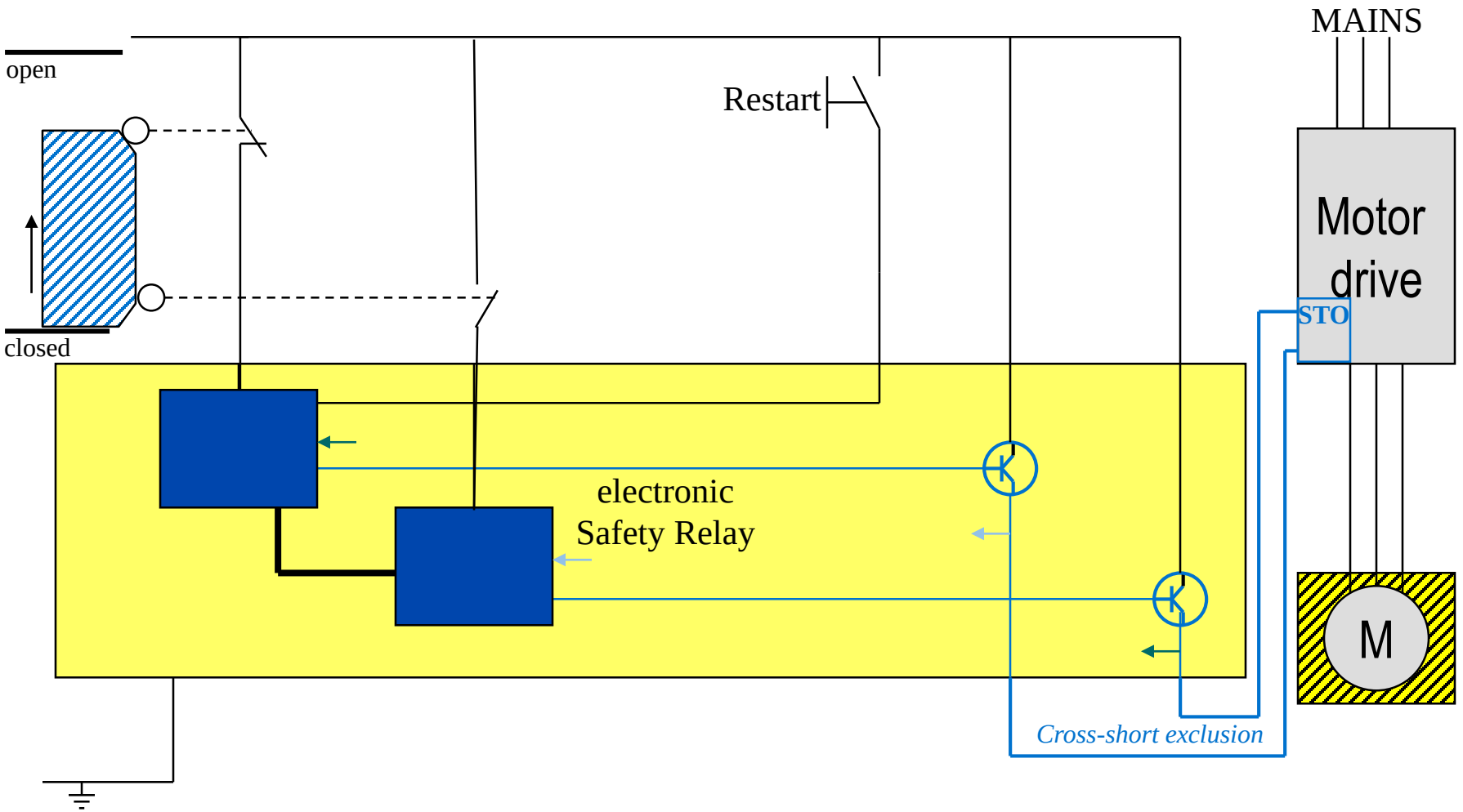


Application of Safe Stop 1

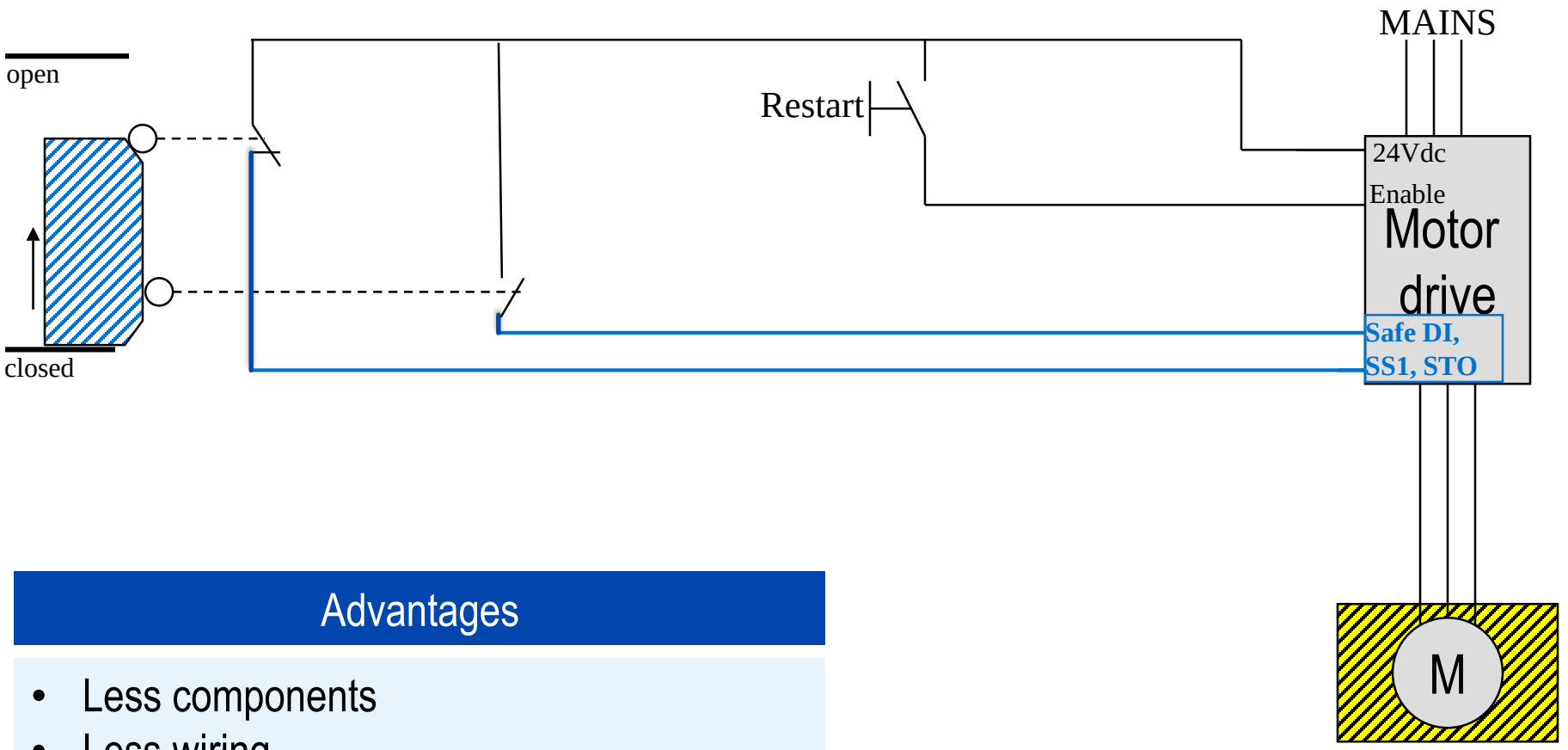


- Machine safety
  To realise a Stop Category 1 (per IEC 60204-1), which in turn can be the basis for implementing
  - Emergency stop
    - Advantage:
      - » avoid a too abrupt stop, protection of equipment, goods
      - » avoid a too slow stop, e.g. for paper machines, printing machines
      - » Limitations: failure to ramp-down must not mean a risk!
  - Operational safety-related stopping,
    - e.g. safety doors or ESPE that are regularly passed through as part of normal operating procedures
      - » Increased acceptance of safety functions => increased work place safety

Example: electronic safety relay to implement safety-related timer



Safety-related Digital Input, SS1, and STO integrated

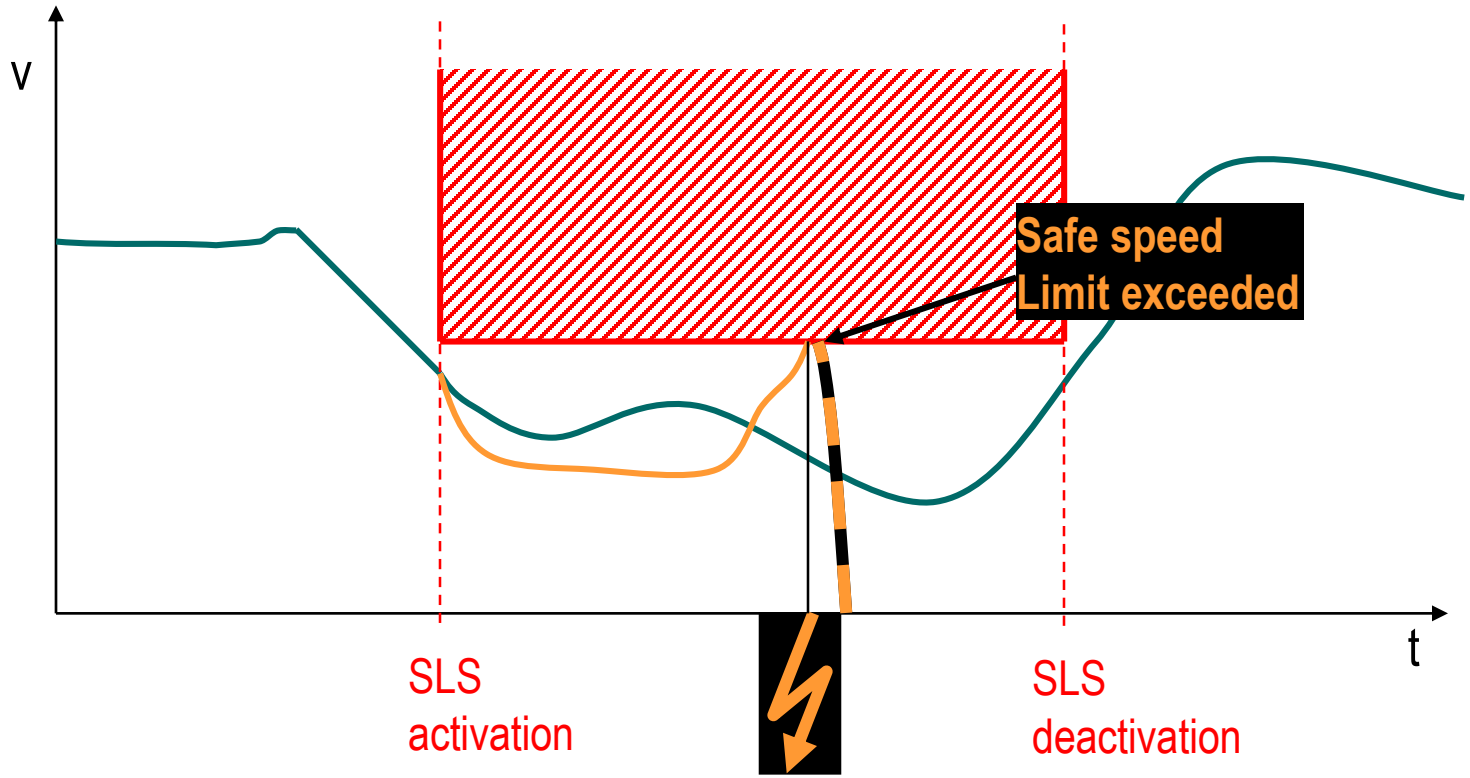


Advantages

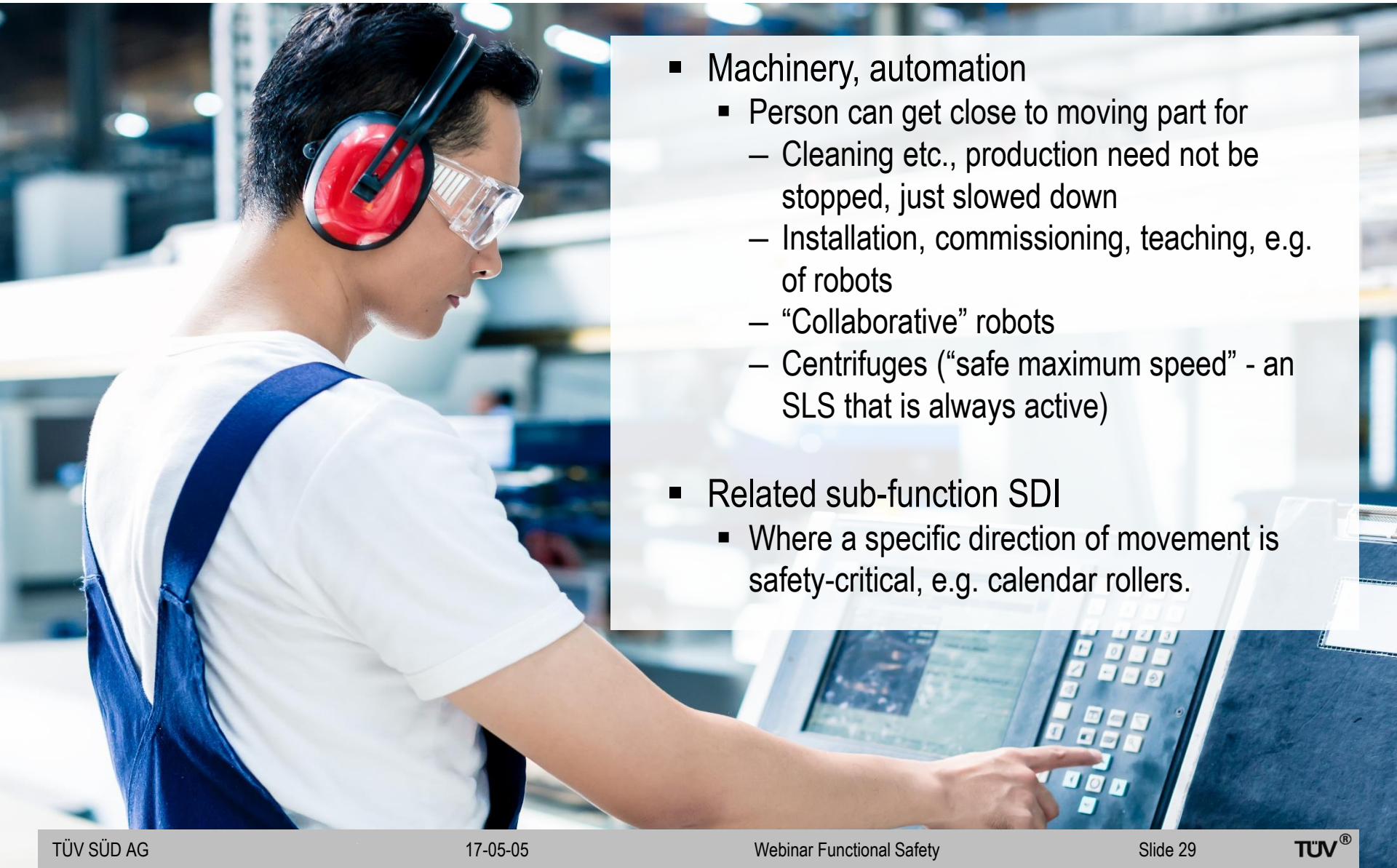
- Less components
- Less wiring
- Less maintenance

Safely limited speed

"Prevents the motor from exceeding the specified speed limit"

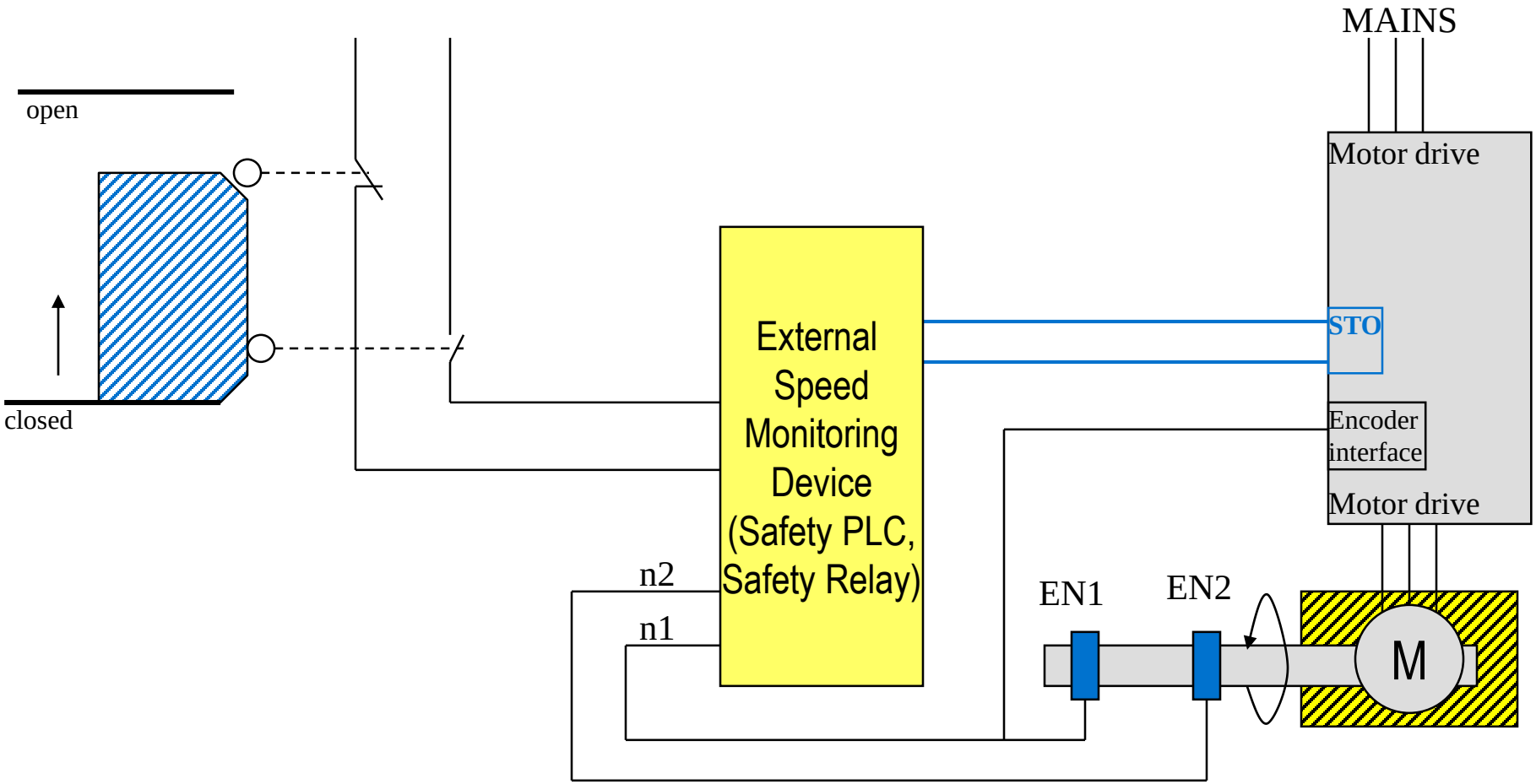


Application of Safely Limited Speed

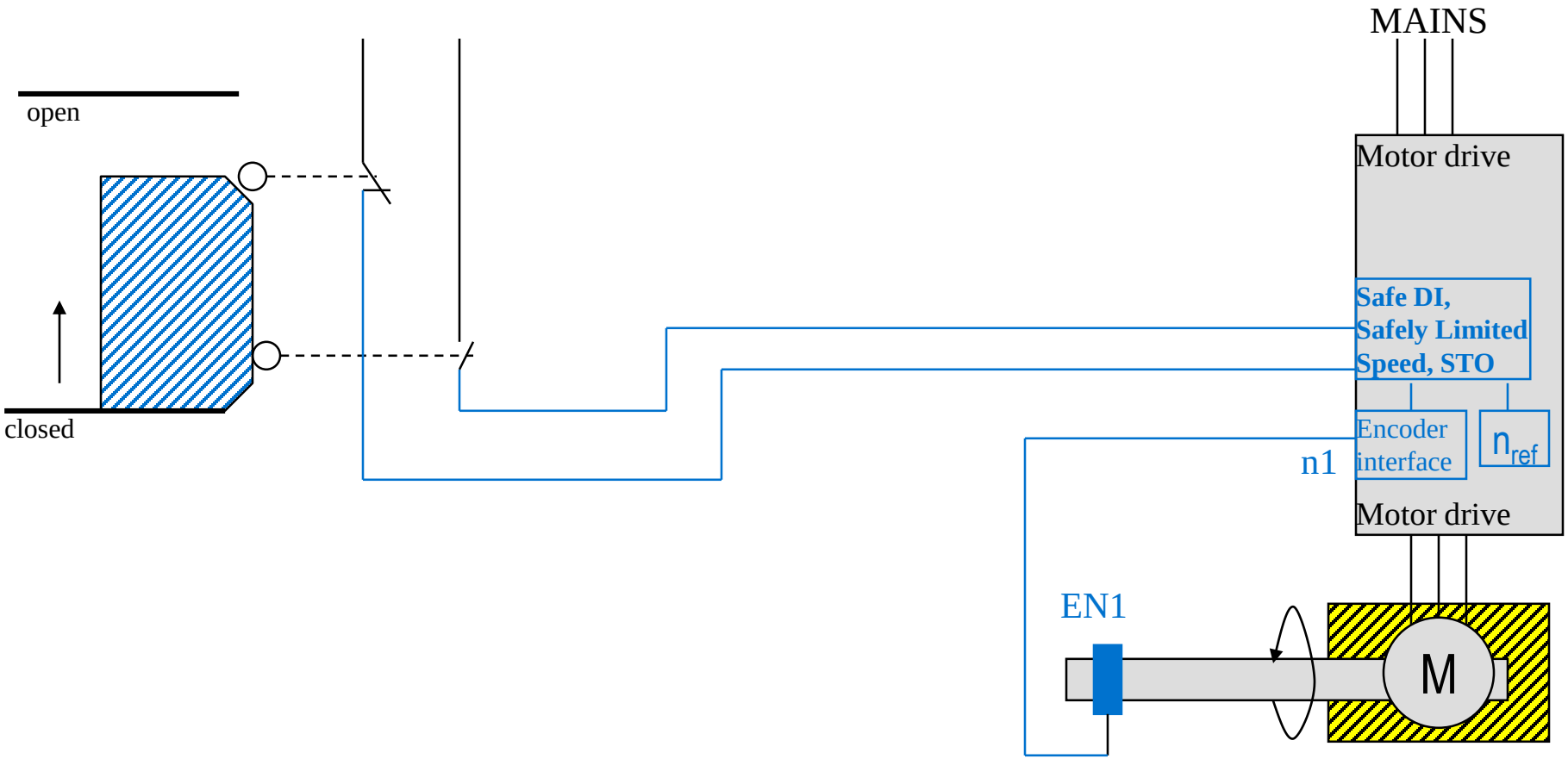


- Machinery, automation
  - Person can get close to moving part for
    - Cleaning etc., production need not be stopped, just slowed down
    - Installation, commissioning, teaching, e.g. of robots
    - “Collaborative” robots
    - Centrifuges (“safe maximum speed” - an SLS that is always active)
- Related sub-function SDI
  - Where a specific direction of movement is safety-critical, e.g. calendar rollers.

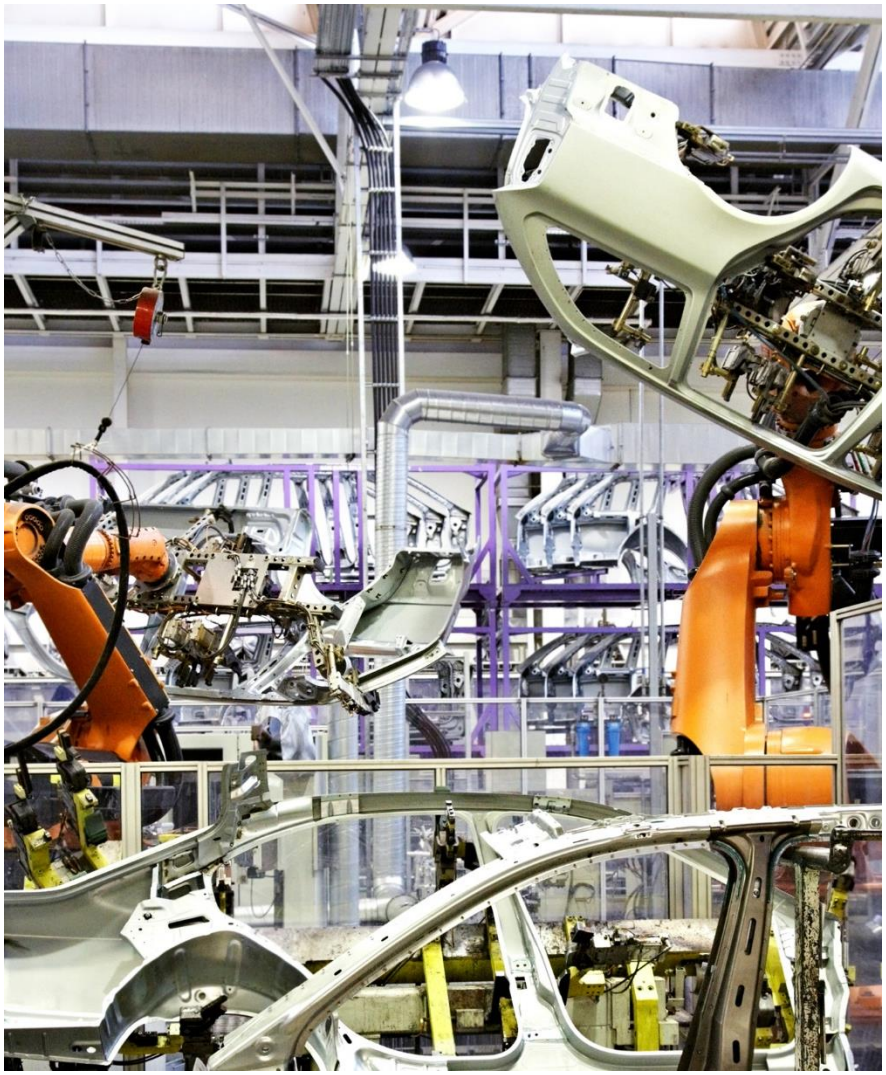
Safely Limited Speed (SLS), drive with STO, external safe speed monitoring device



Safely Limited Speed, integrated in drive



Agenda

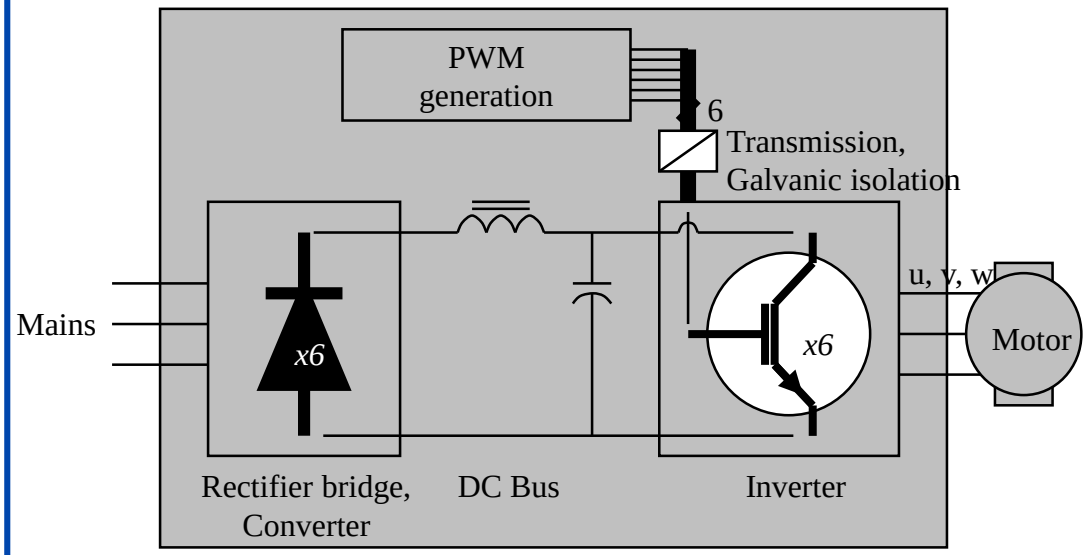


1	What is functional safety (FS)
2	FS standards and regulations
3	Scope and contents of IEC 61800-5-2 - User perspective
4	Application examples for STO, SS1, SLS
5	Implementation-related contents - Manufacturer perspective
6	Future standardisation efforts

STO by electronic pulse blocking: failure considerations

- Conclusions from research by BIA* [Zinken 1994]
  - ➢ Pulse patterns necessary to generate rotating field in motor, require complex circuits. Will not be generated “by accident”, e.g. by component failures (even multiple) or EMI.
  - ➢ This is NOT the case for circuits controlling (i.e. enabling, disabling) the pulse pattern generation
    - These circuits must be designed in accordance with the required SIL Capability requirements

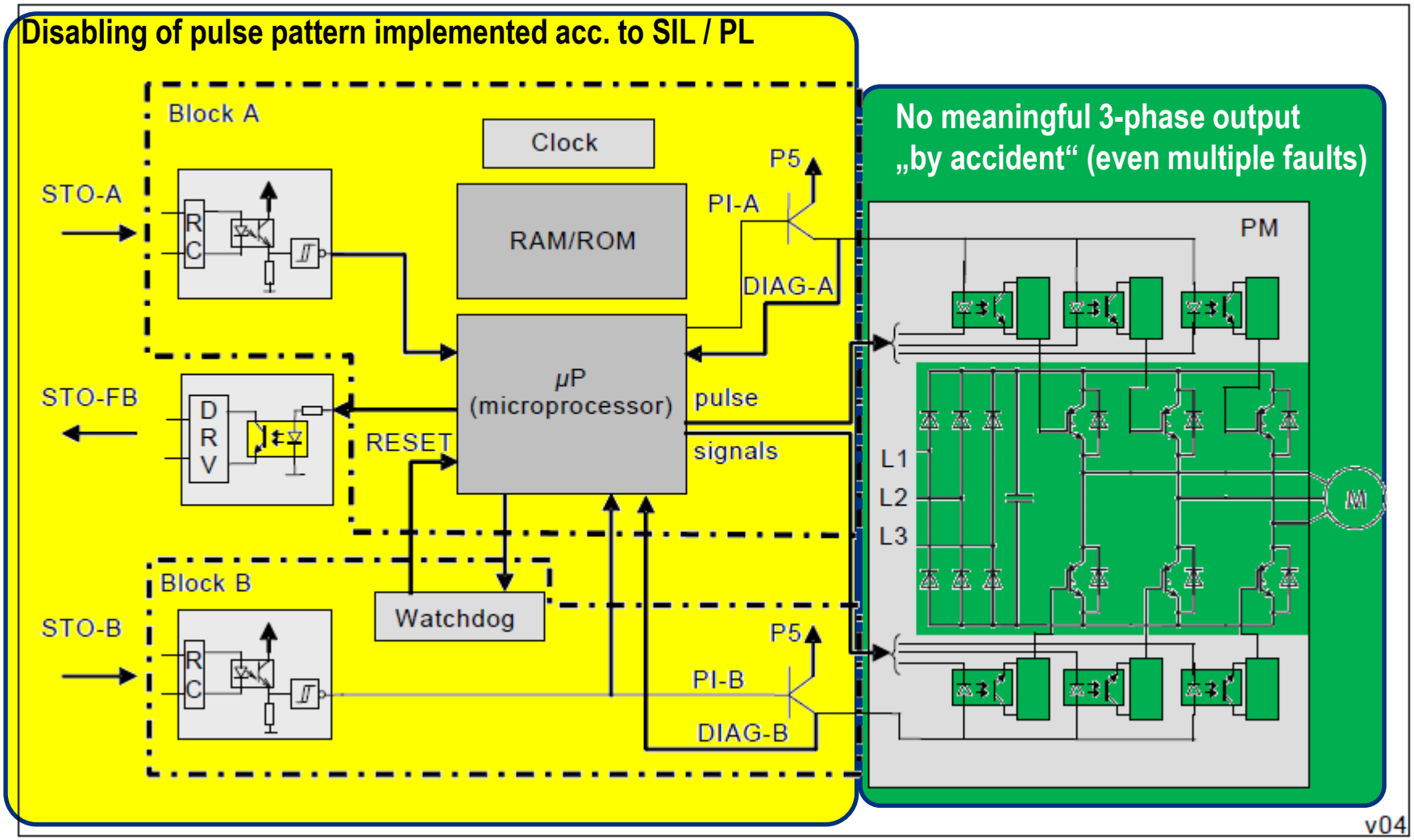
Basic structure for motor drive (VFD)



Zinken, E., “Vermeidung von unerwartetem Anlauf bei stromrichtergespeisten Antrieben”, Antriebstechnik 33 (1994) Nr. 10, S. 50-53, 4 Lit., 7 Abb.

*Today IFA, formerly BGIA and BIA

Example safety architecture

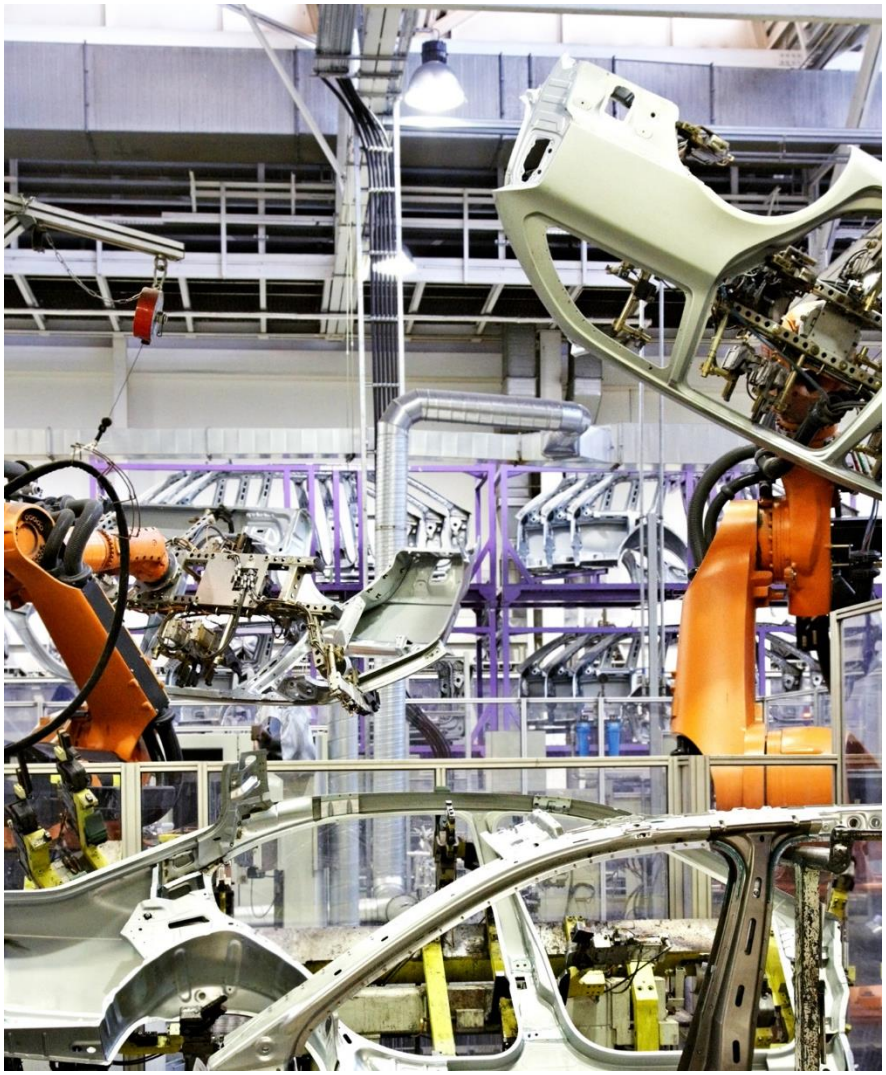


Important contents – manufacturer perspective (blue: new in 2nd.ed)

(Selection – list is not complete)

- Functional safety management tailored to the needs of a sub-system
  - Guidance in „Sequential task list“ in Annex A - improved
- Hardware and software requirements by reference to IEC 61508:2010
  - ➢ also to IEC 61508-2 Annex E for on-chip HFT and Annex F in case ASICs, FPGA are used
- Safety manual requirements: references to Annexes D of IEC 61508-2, -3, plus additional requirements.
- Requires a safety system architecture specification
- If HFT = 0 and exclusions of dangerous faults, then the maximum *SIL capability* limited to SIL2
  - ➢ *Unless* tables D.1, D.3, D.5, D.6, D.7 and D.8 apply, then SIL3.
  - ➢ (The “safety relay clause” of 1st edition has been removed)
- Tests: All safety sub functions shall be tested for immunity to EM, thermal, and mechanical stresses.
  - ➢ Safety sub-function shall be in operation during vibration test.
  - ➢ EM immunity requirements directly in the standard (Annex E)
- Relationship to ISO 13849 fortified
  - ➢ References throughout document to relevant clauses of ISO 13849-1 and ISO 13849-2

Agenda



1	What is functional safety (FS)
2	FS standards and regulations
3	Scope and contents of IEC 61800-5-2 - User perspective
4	Application examples for STO, SS1, SLS
5	Implementation-related contents - Manufacturer perspective
6	Future standardisation efforts

Safety-related encoders

NEW WORK ITEM PROPOSAL 22G/339/NP

- **Motivation and Objectives for new standard**
  - Encoder requirements found to be lacking in IEC 61800-5-2
- **Title of proposal**
  - Adjustable speed electrical power drive systems - Safety requirements for encoders - Functional, Electrical and Environmental
    - *Presumably 61800-5-3*
- **Scope**
  - a product standard, on functional safety, electrical safety, and environmental conditions.
  - Basis for manufacturers to declare safety performance
  - Facilitate incorporation into safety-related control systems per IEC 61508, IEC 62061, IEC 61511, ISO 13849, …
  - Maximally SIL 3

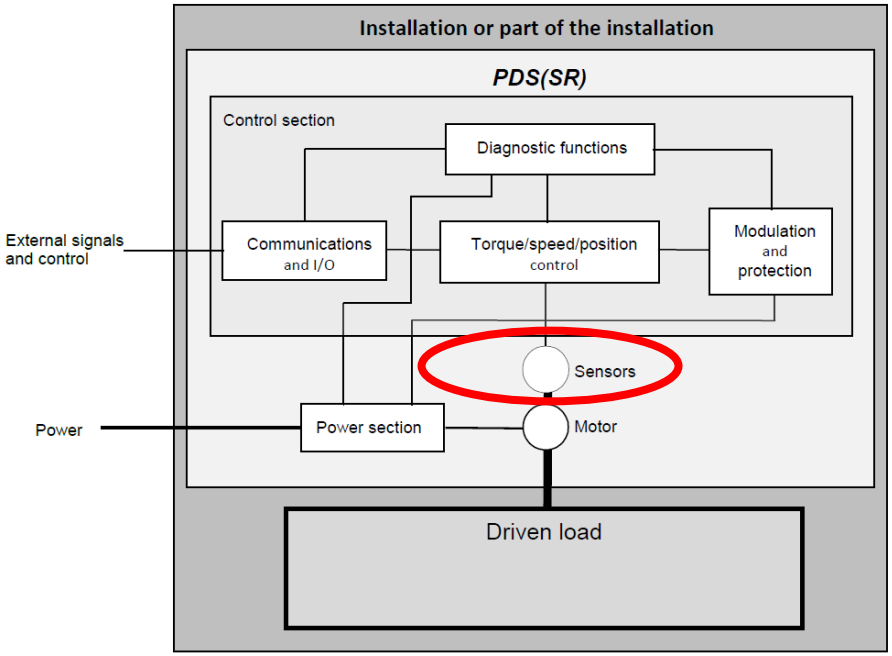
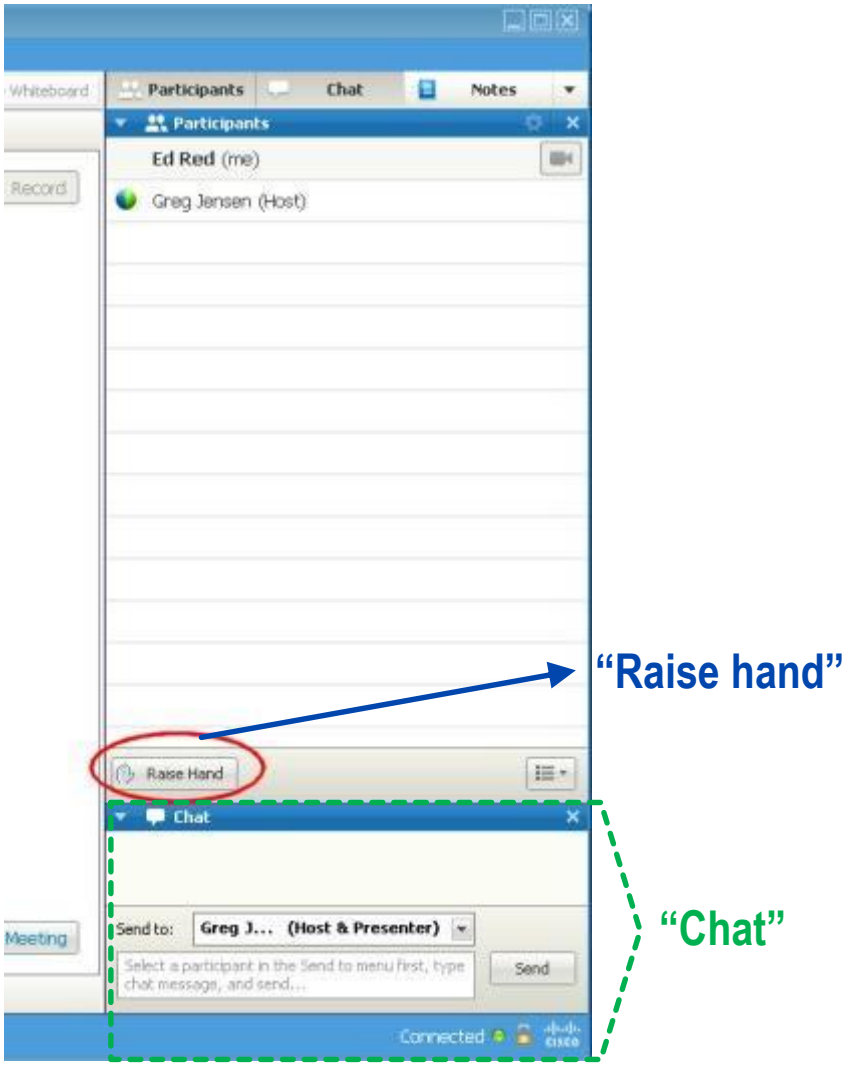


Figure 1 – Installation and functional parts of a *PDS(SR)* including the encoder (sensor)

Any questions?



- Please send in any questions you may have through the WebEx **"Q&A"** function to the moderator i.e. Thomas Adler
- Or use the WebEx "Raise hand" and we will unmute your line.

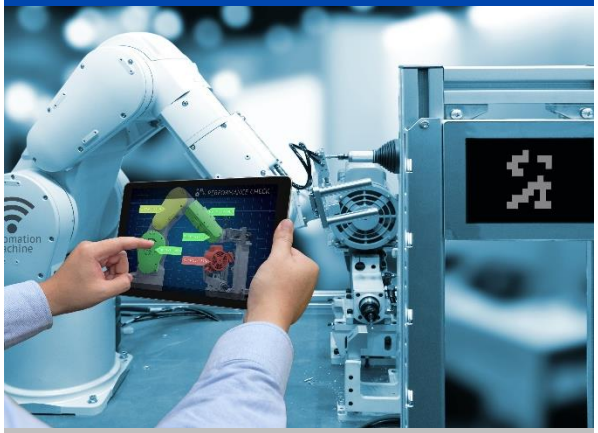
Stay updated!

Register for our industry E-ssentials



- Rail
- Automotive
- Consumer Products & Retail
- Healthcare & Medical Devices
- Chemical, Oil and Gas
- Power & Energy
- Real Estate & Infrastructure

Download our Functional Safety White Paper

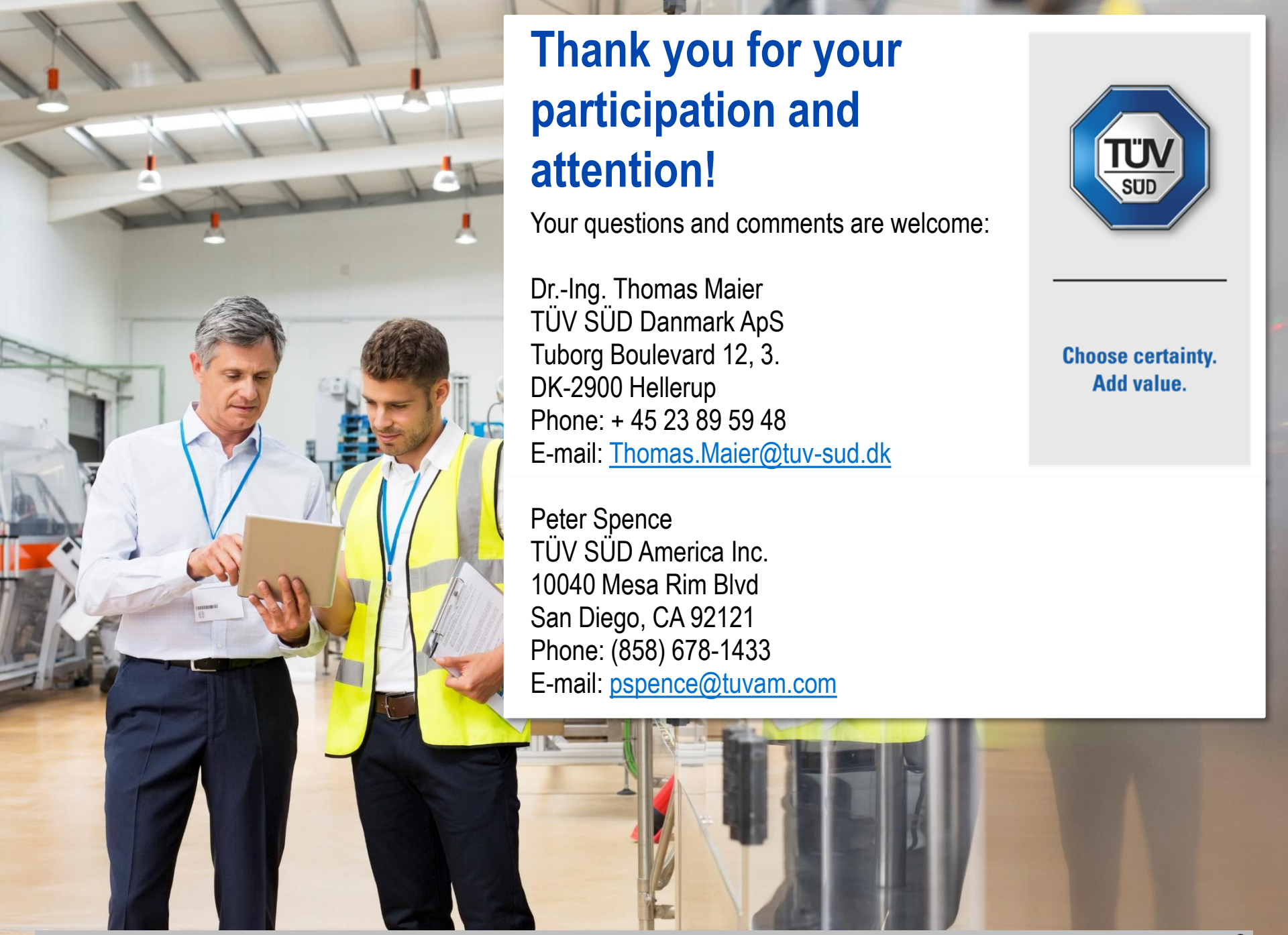


- Read more about "Functional safety for a digital world - Smart solutions from chip design to whole system design"

Find our more about our Functional Safety offers



- Learn more about our Functional Safety services
- Apply for one of our Functional Safety trainings



Thank you for your participation and attention!

Your questions and comments are welcome:

Dr.-Ing. Thomas Maier
TÜV SÜD Danmark ApS
Tuborg Boulevard 12, 3.
DK-2900 Hellerup
Phone: + 45 23 89 59 48
E-mail: Thomas.Maier@tuv-sud.dk

Peter Spence
TÜV SÜD America Inc.
10040 Mesa Rim Blvd
San Diego, CA 92121
Phone: (858) 678-1433
E-mail: pspence@tuvam.com

Choose certainty.
Add value.