Safety over EtherCAT
Overview

EtherCAT Technology Group

EtherCAT® Technology Group

Safety over EtherCAT

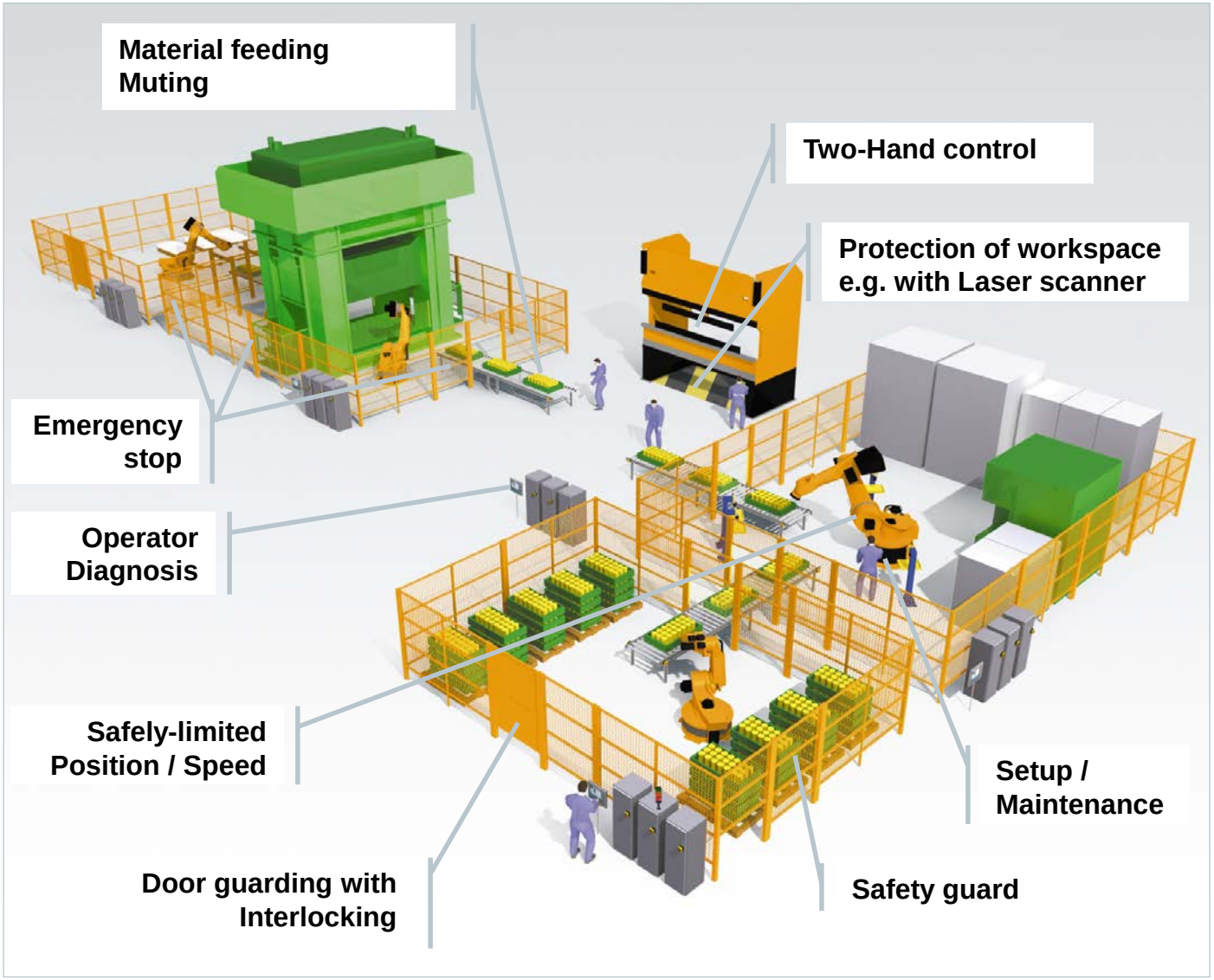
- Requirements
- Safety over EtherCAT Technology
  - Architecture
  - Definitions
  - State Machine
  - Telegram
  - Summary
- Conformance
- Applications

Safety in industrial automation

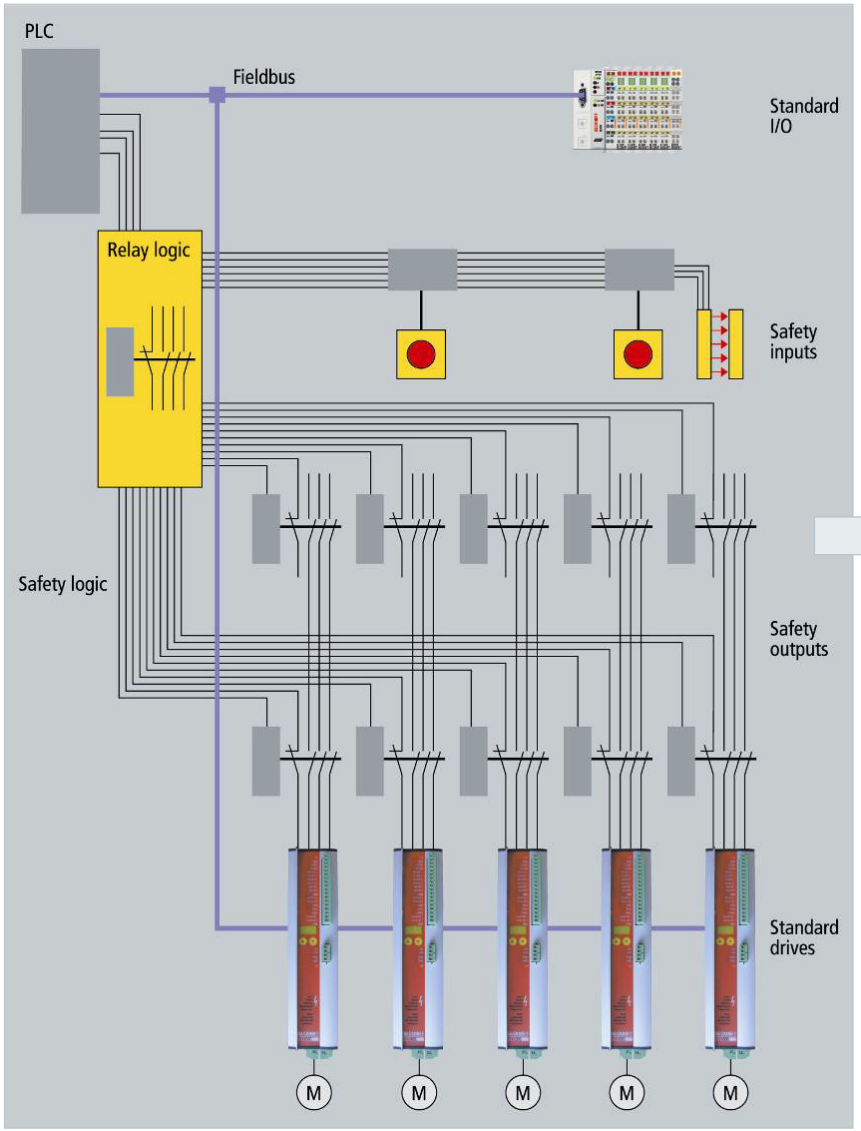
- Functional Safety
  - Protection against malfunction of machines
  - Protection of the machine operator against dangerous movements

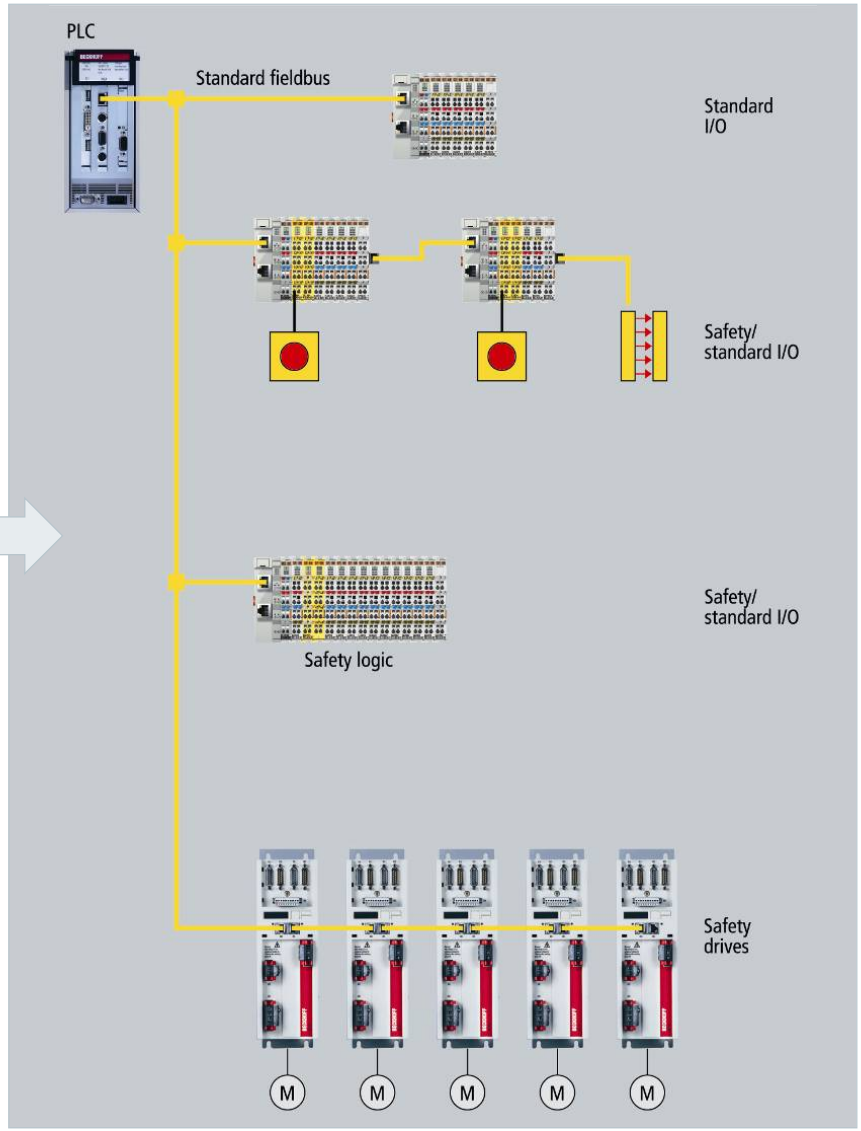
- Safety functions (Examples)
  - Monitoring of the workspace of a machine
    - Door guarding (with interlocking)
    - Protection with light curtain / laser scanner
  - Safe feeding of material
    - Muting
- Safe movement with manual intervention
  - Two-Hand control
  - Emergency Stop
  - Safe operating stop
  - Safely-limited speed

Safety in industrial automation



Modern safety concepts





Advantages of Safetybus systems

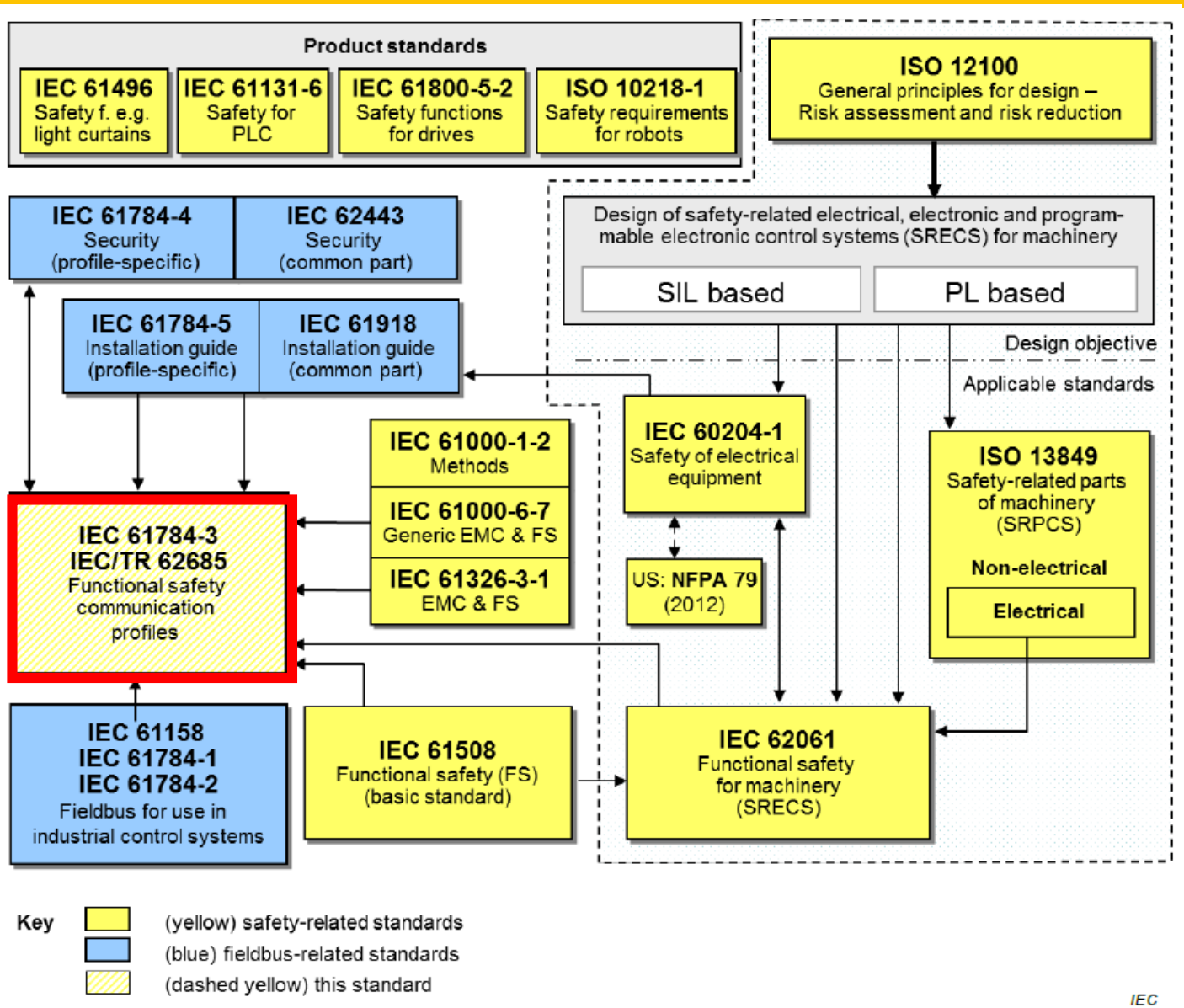
- Fast reaction
  - applicable for high dynamic drive architecture
- Simplified System
  - better clarity
  - simple cabling
  - simple extension of the system
  - better diagnosis
  - and therefore: higher safety
- Pre-tested safety functions within the devices according to the legal standards
- Lower costs

International standardization

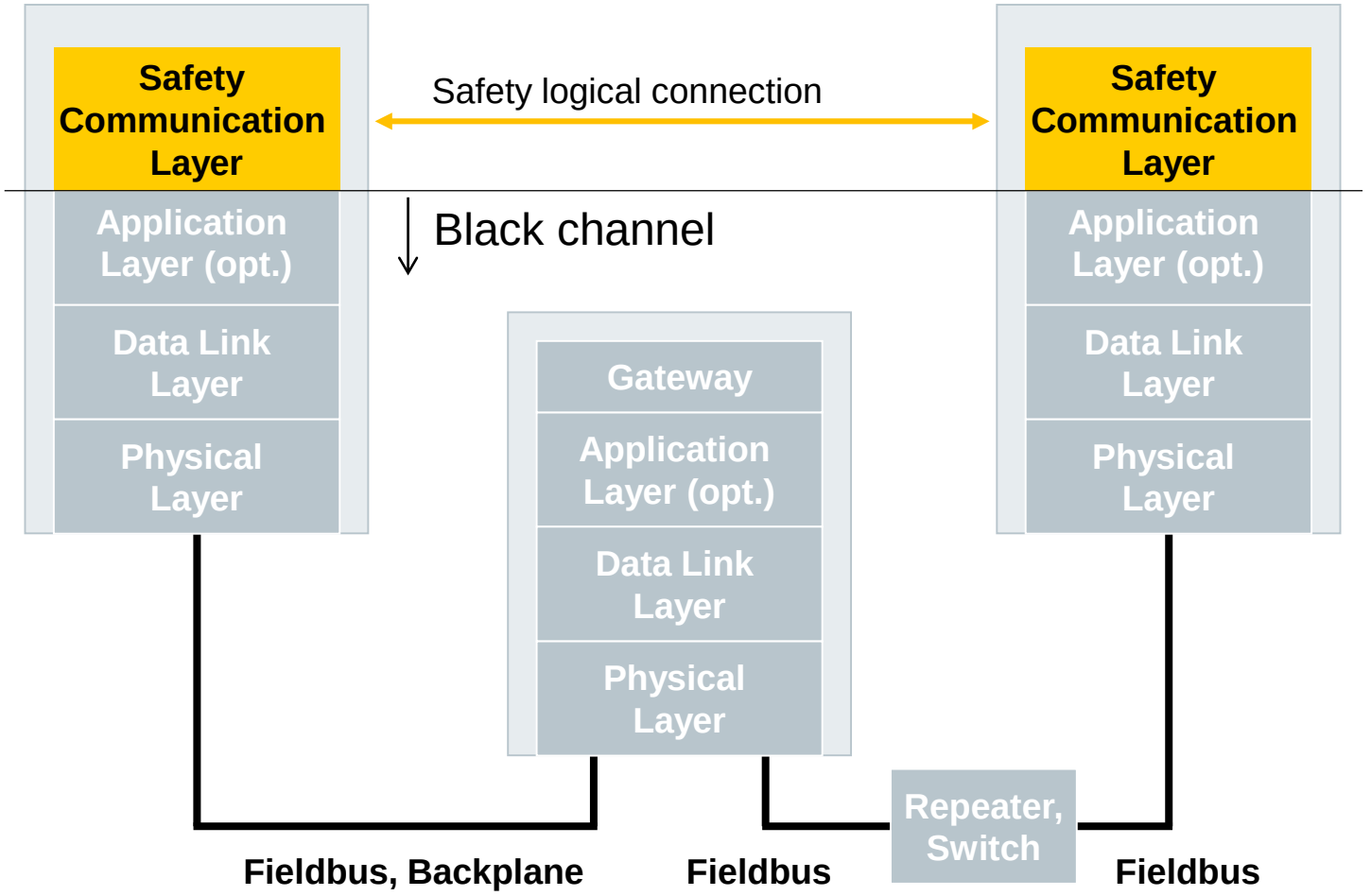
- German approach: BGIA Test principles GS-ET-26
  - Test principles of the German Institute for Occupational Safety and Health
  - Bus systems for the transport of safety-related messages
  - Assessment requirements of the BGIA to evaluate safety bus systems
  - Basis of the IEC 61784-3

- IEC 61784-3
  - DIGITAL DATA COMMUNICATIONS FOR MEASUREMENT AND CONTROL
    Part 3: **Profiles for functional safety communications in industrial network** - General rules and profile definitions
  - Based on Black Channel approach (see below)

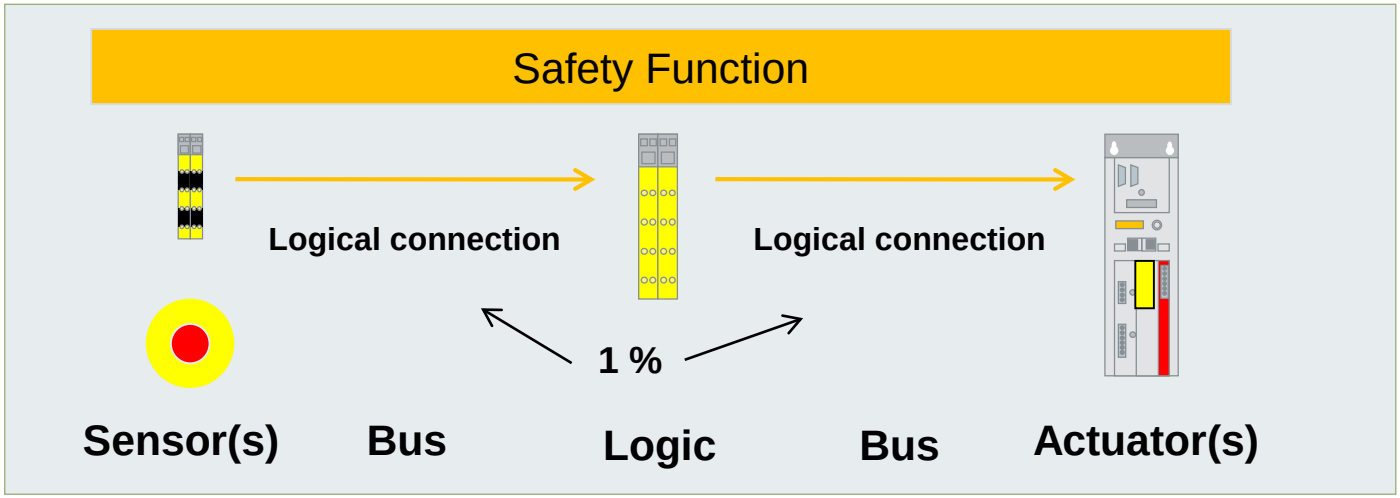
IEC 61784-3



IEC 61784-3
Functional safety communication model



Safety function decomposition



- Probability of failure for the safety function, according to IEC 61508:

  $PFH_{SafetyFunction}$ < 10^{-8}…10^{-7}/h for SIL 3

- The IEC 61784-3 highly recommends that the safety communication channel does not consume more than 1 % of the maximum PFD or PFH of the target SIL for which the functional safety communication profile is designed:

  $PFH_{LogicalConnection}$ < 10^{-9}/h for SIL3

$PFH_{SafetyFunction} = PFH_{Sensor} + PFH_{Logic} + PFH_{Actor} + PFH_{LogicalConnection}$

Safety-over-EtherCAT

- Safety-over-EtherCAT defines a safe communication layer, to transfer safe process data between Safety-over-EtherCAT devices.

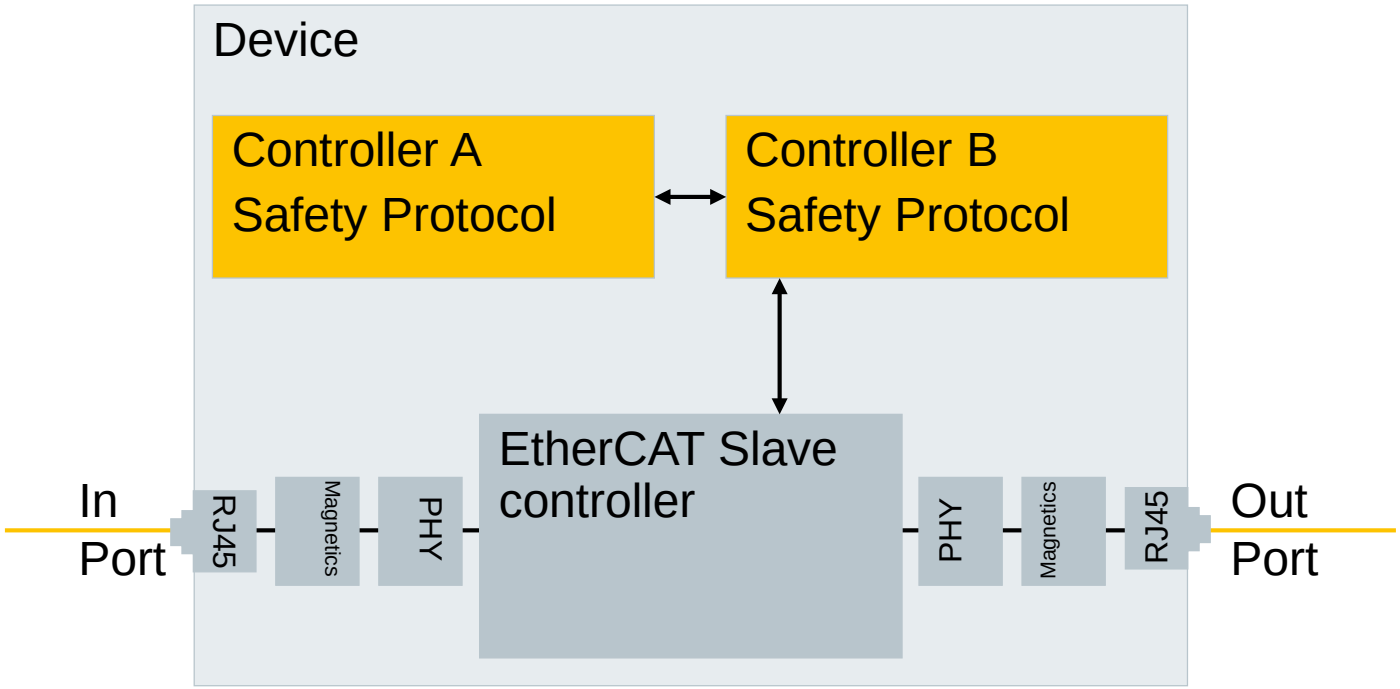
- FSoE is an open technology
  - Supported by EtherCAT Technology Group (ETG)
  - Part of IEC 61784-3 international standard

- The protocol is approved by an independent Notified Body (TÜV Süd Rail GmbH).

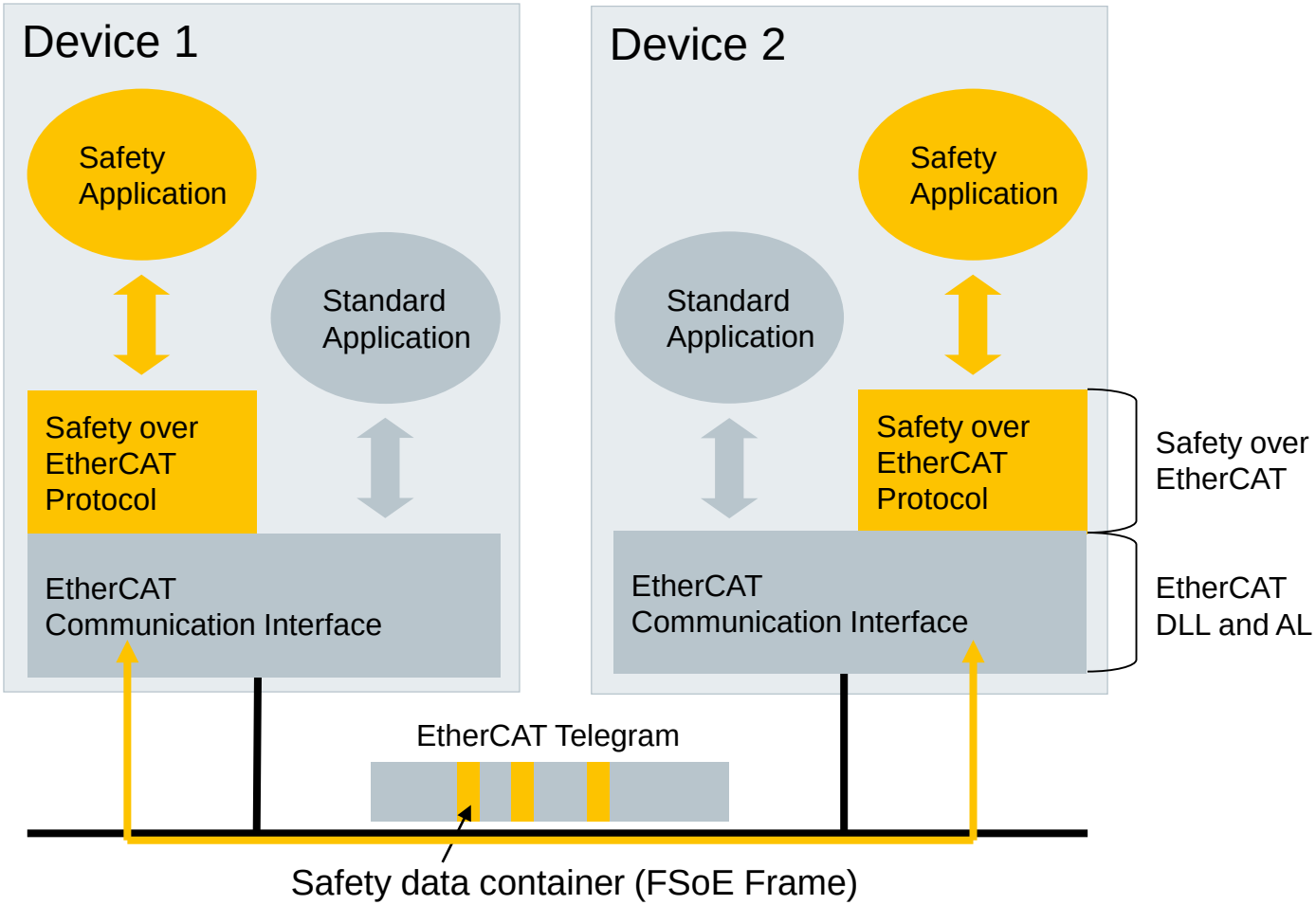
Safety over EtherCAT®

FSoE – Typical Hardware Architecture

- 1-channel standard communication system
- Redundant hardware for safety protocol and safety-related application



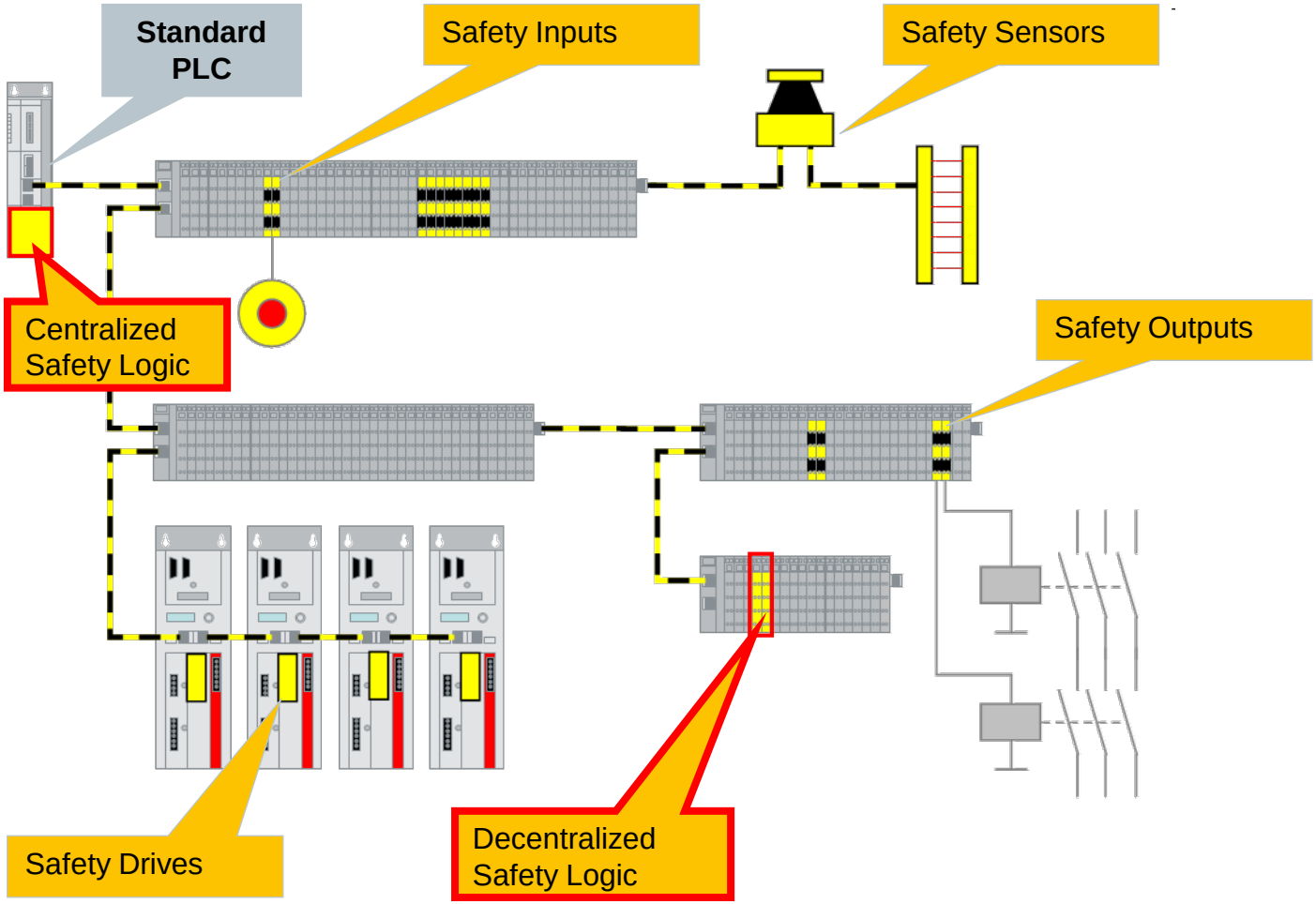
FSoE – Software Architecture



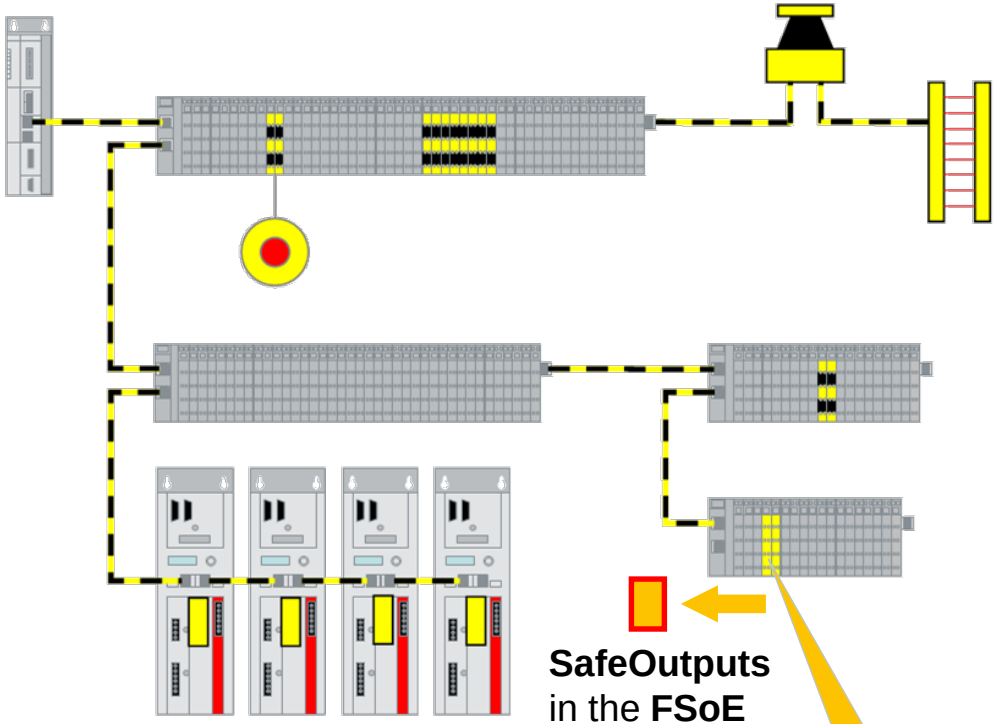
EtherCAT is used as a “black channel”.
It contains safety and standard information.

Safety over EtherCAT | System Example

- Centralized or decentralized Safety-Logic
- Standard PLC routes the safety messages



FSoE – Master / Slave Connection



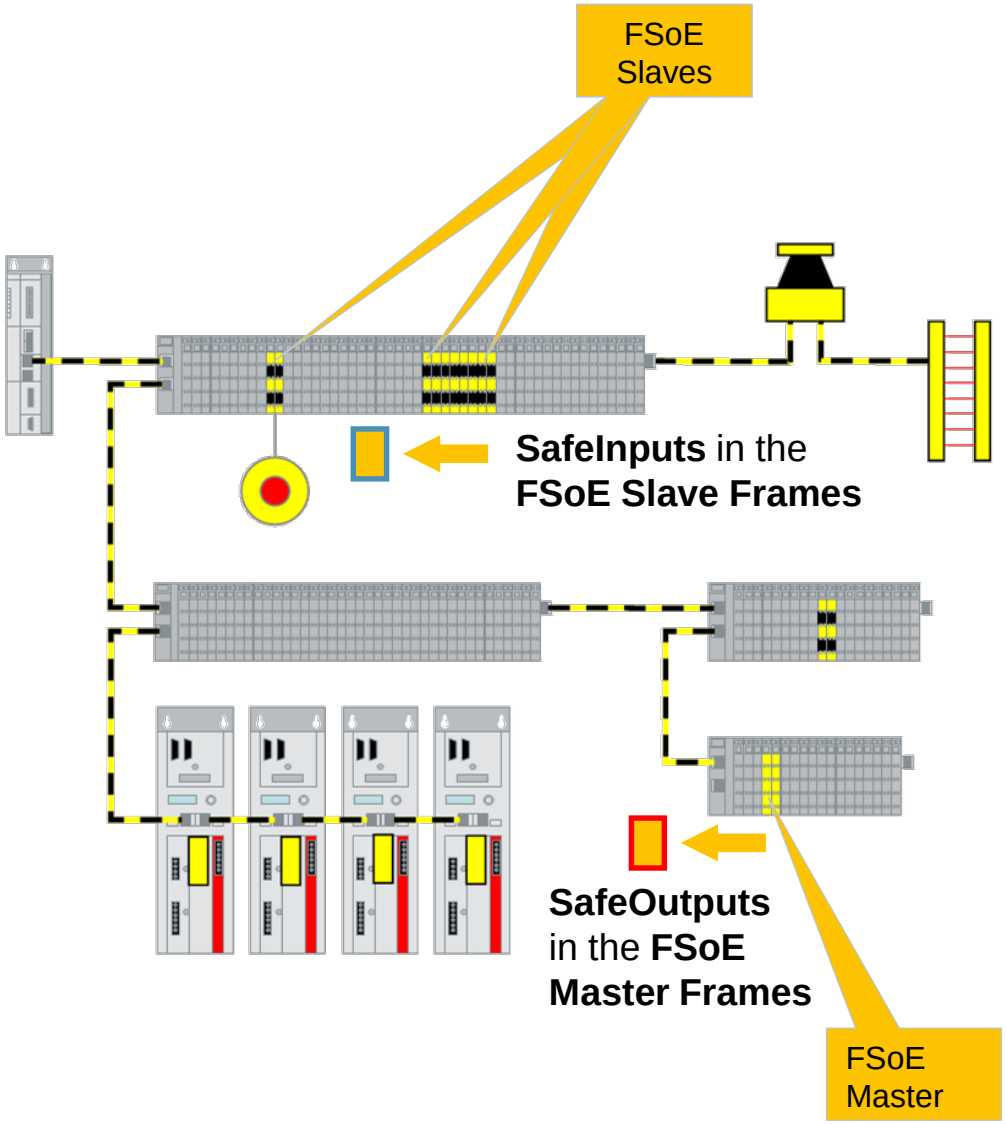
FSoE Master

Master of an FSoE Connection. The FSoE Master initiates the safety communication.

The FSoE Master sends an **FSoE Master Frame**, that contains the **SafeOutputs**.

An FSoE Master can handle one or more FSoE Slaves.

FSoE – Master / Slave Connection



FSoE Slave

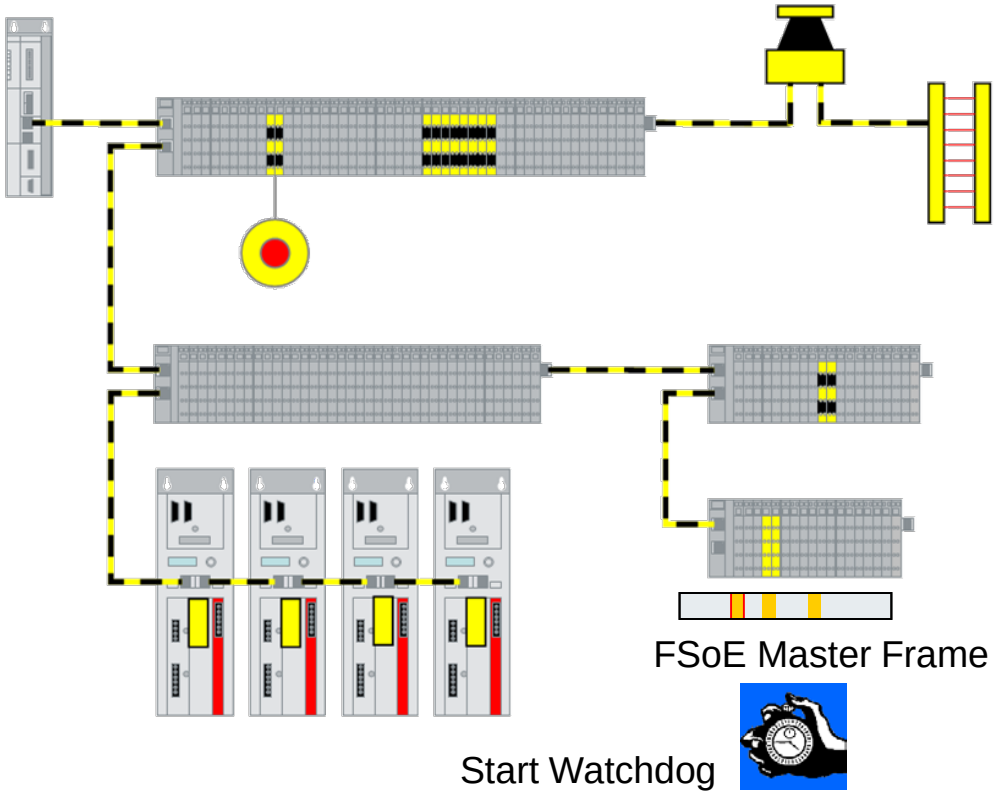
Slave of an FSoE Connection.

The FSoE Slave sends the **FSoE Slave Frame**, after receiving a valid FSoE Master Frame.

The FSoE Slave Frame contains the **SafeInputs**.

An FSoE Slave is assigned to one FSoE Master.

FSoE – Communication Cycle



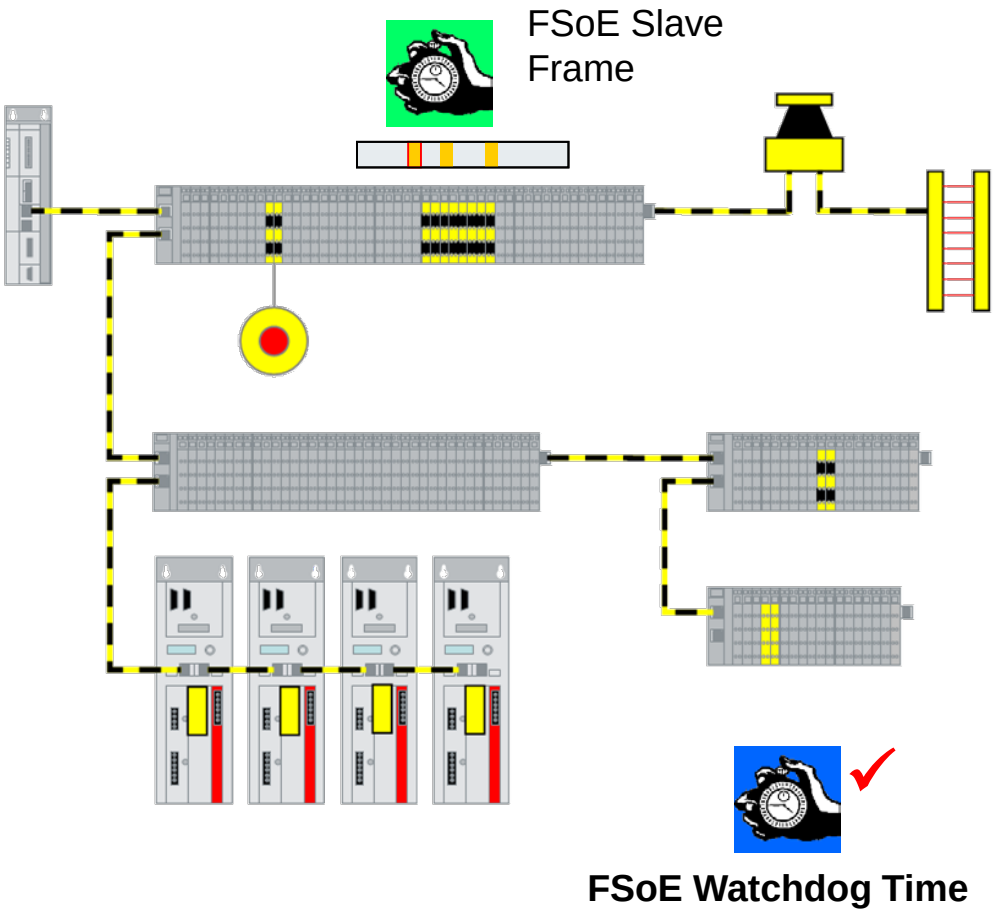
FSoE Cycle

The FSoE Cycle consists of an FSoE Master Frame, that is confirmed by the FSoE Slave Frame.

The FSoE Master sends the FSoE Master Frame to the FSoE Slave.

With sending the frame the FSoE Master starts a Watchdog-Timer.

FSoE – Communication Cycle



FSoE Cycle

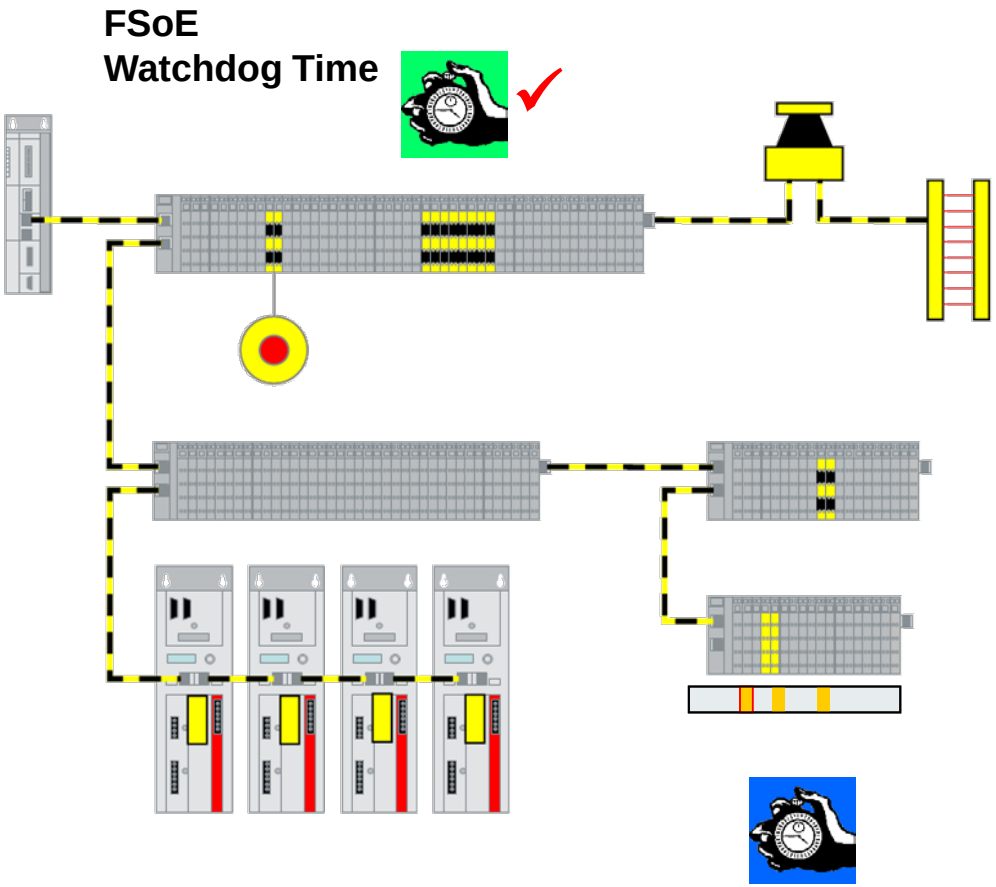
The FSoE Cycle consists of an FSoE Master Frame, that is confirmed by the FSoE Slave Frame.

The FSoE Master sends the FSoE Master Frame to the FSoE Slave.

With sending the frame the FSoE Master starts a **Watchdog-Timer**.

Only after receiving a valid FSoE Slave Frame, the FSoE Master generates the next FSoE Master Frame and starts a new FSoE Cycle.

FSoE – Watchdog Time

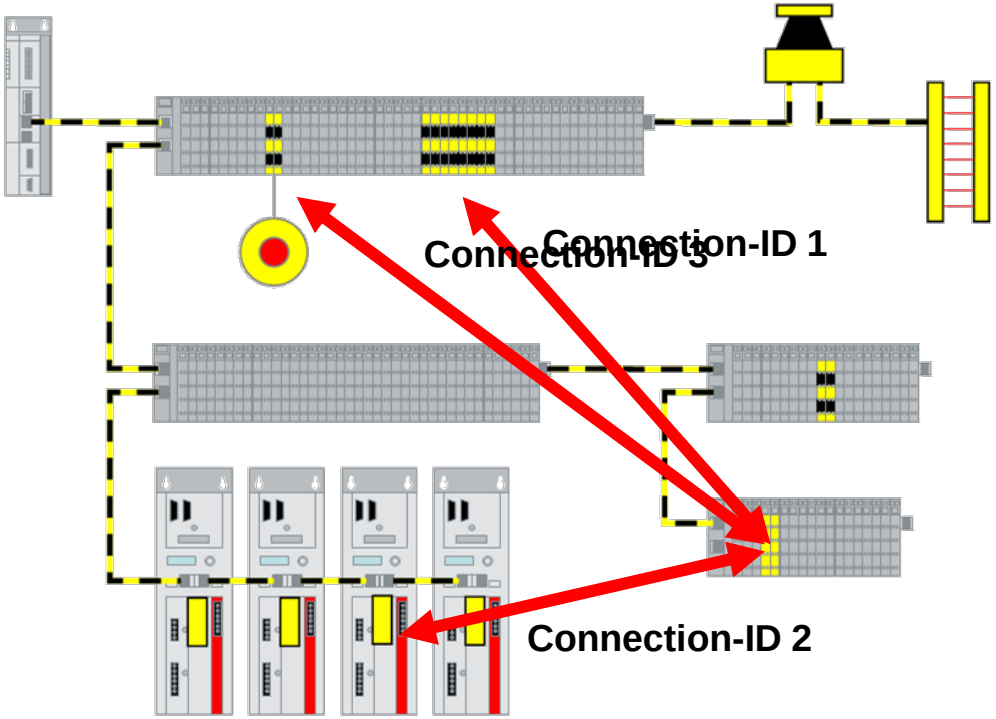


FSoE Watchdog Time

Each device monitors that the partner device responses within the safety configured **FSoE Watchdog Time**.

If the Watchdog Time exceeds, the device switches to the state “Reset”.

FSoE – Connections



FSoE Connection

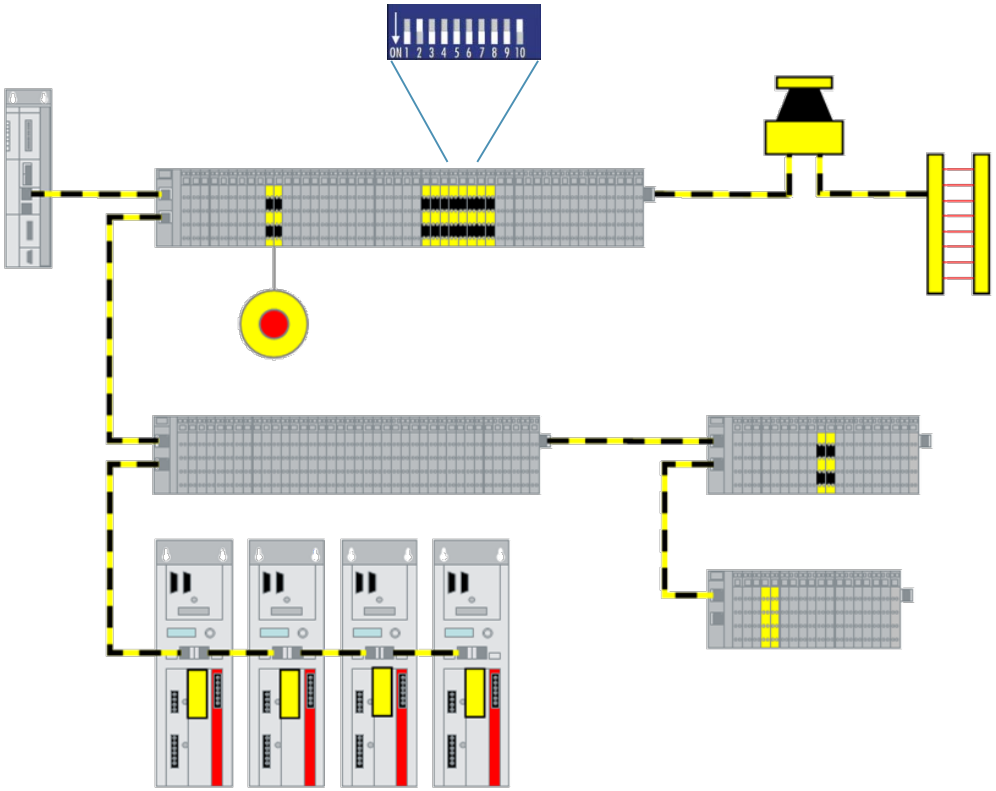
The **FSoE Connection** is a logically connection between one FSoE Master and one FSoE Slave.

It is a system-unique **Connection-ID**.

The uniqueness has to be checked by a safe configurator.

FSoE – FSoE Slave Address

FSoE Slave Address



FSoE Slave Address

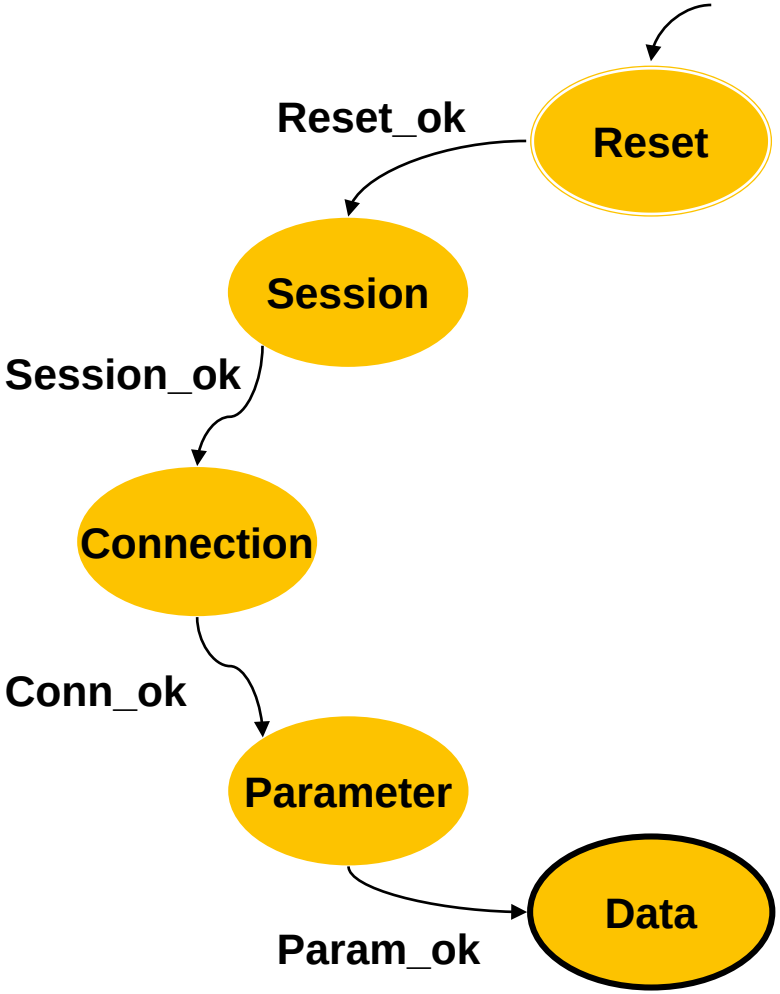
Next to the Connection-ID each FSoE Slave has a system-unique 16-Bit **FSoE Slave Address**.

This address can be adjusted for the device, e.g. with a DIP-Switch.

The FSoE Slave Address is used for the unique addressing of the device.

Up to 65,535 devices can be addressed.

FSoE State Machine per Connection



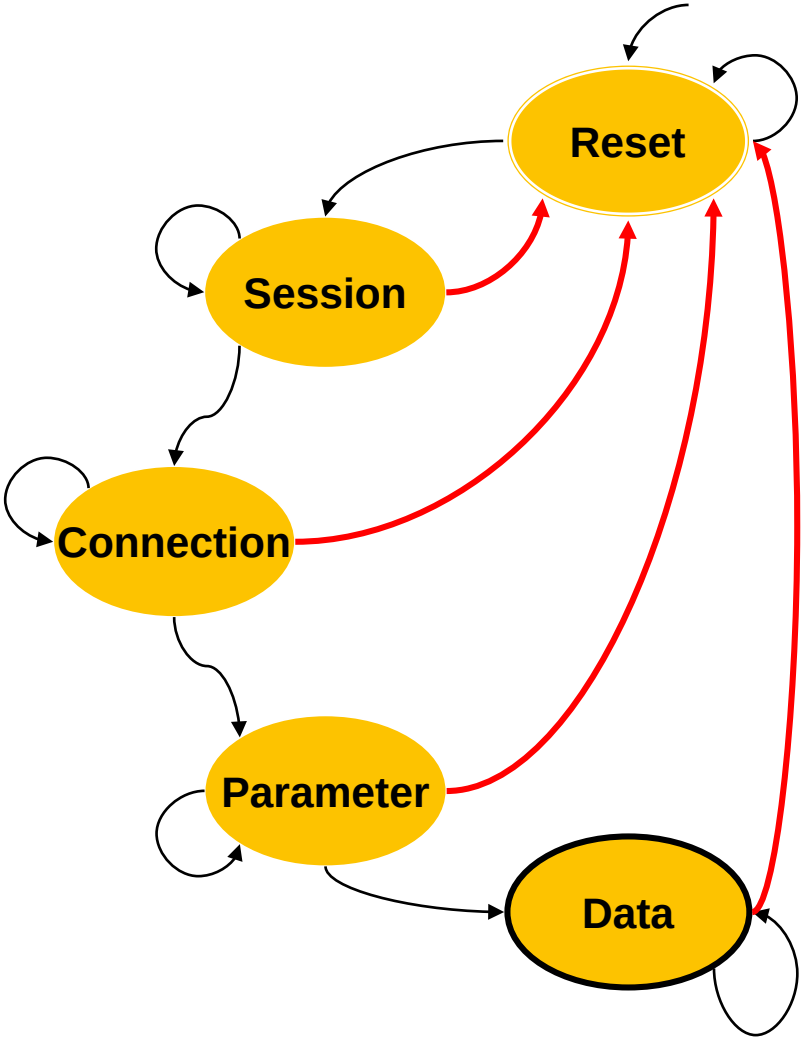
For each FSoE Connection an FSoE State Machine exists in the FSoE Master and in the FSoE Slave.

The FSoE Master handles one State Machine per FSoE Slave.

After Power-On the FSoE Master and the FSoE Slave are in state Reset.

Only in state Data the safe State of the Outputs can be left.

FSoE State Machine – Error behavior

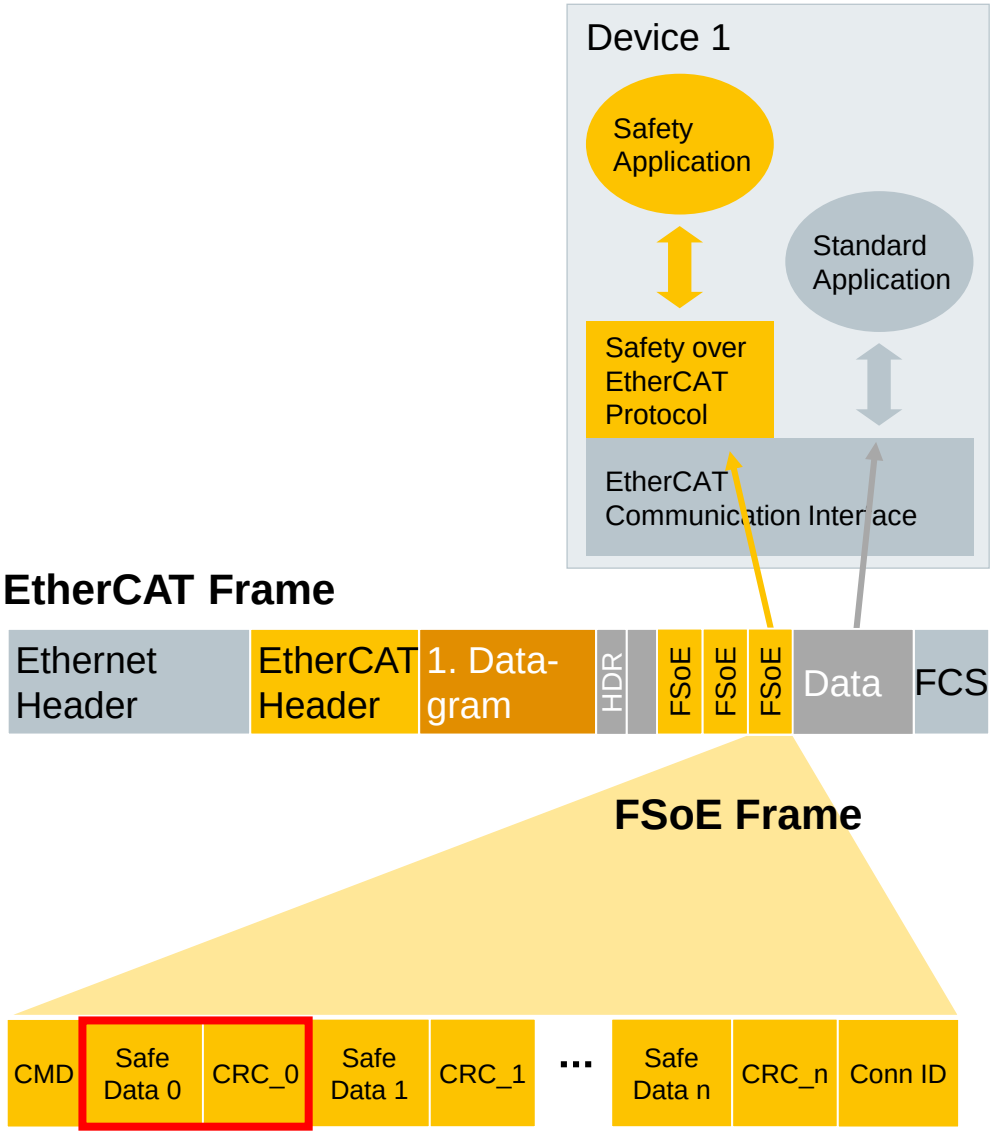


In case of an FSoE Connection error the devices change to the Reset state.

Examples

- FSoE Watchdog expires
- CRC checks fails
- FSoE Reset telegram received

Safety over EtherCAT: Software Architecture



FSoE Frame

The FSoE Frame is embedded as a Container in the process data of the device.

Each device detects a new FSoE Frame, if at least one Bit in the FSoE Frame is changed.

Every 2 Byte SafeData are checked by a 2 Byte CRC.

The maximum number of SafeData is therefore not restricted by the protocol.

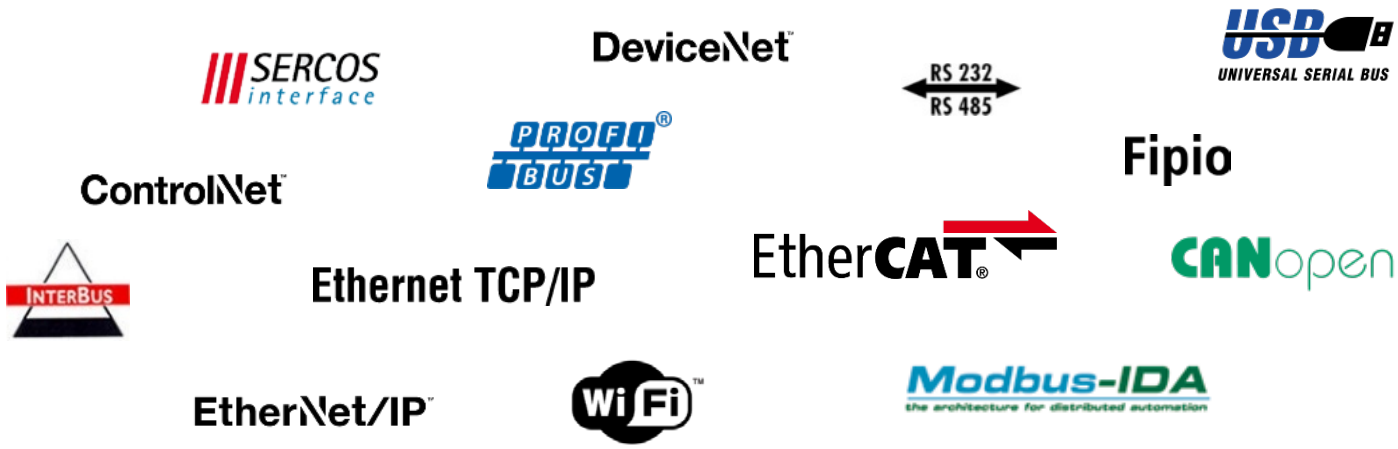
Safety measures for Safety over EtherCAT

Error \ Measure	Sequence Number	Watchdog	Connection ID	CRC Calculation
Unintended repetition	☑			☑
Loss	☑	☑		☑
Insertion	☑			☑
Incorrect sequence	☑			☑
Corruption				☑
Unacceptable delay		☑		
Masquerade		☑		☑
Repeating memory errors in Switches	☑			☑
Incorrect forwarding between segments			☑	

Safety over EtherCAT – Features

- The FSoE specification has no restrictions according to:
  - Communication layer and interface
  - Transmission speed
  - Length of safe process data

- Routing via unsafe gateways, fieldbuses or backbones is possible, even wireless.



Safety over EtherCAT – Features

- FSoE Frame is mapped in the cyclic PDOs
  - Minimum FSoE Frame-Length: 6 Byte
  - Maximum FSoE Frame-Length: Depending on the number of safe process data of the Slave Device
  - Therefore the protocol is suitable for safe I/O as well as for functional safe motion control
- Confirmed transfer from the FSoE Master to the FSoE Slave and vice versa.
- Safety-related Device Parameter can be downloaded from the Master to the Slave at Boot-Up of the FSoE Connection.
  - Watchdog time
  - Device specific safety-related Parameter for Slave application

Safety over EtherCAT – Features

- Probability of failure PFH < 10^{-9}/h
  - Based on Bit Error Probability of 10^{-2} of underlying communication channel

→no restrictions for device manufacturers and end user

- The protocol is developed according to IEC 61508 Safety Integrity Level (SIL) 3
- The protocol is approved by TÜV Süd Rail GmbH (Notified body)
- Certified products with Safety-over-EtherCAT are available since 2005.
- Safety-over-EtherCAT is part of IEC 61784-3 Functional safety fieldbuses

Safety over EtherCAT – Open Solution

- FSoE is disclosed within the ETG.5100 and part of IEC 61784-3 Functional Safety Fieldbuses
  - FSoE is recommended Chinese Standard GB/T 36006-2018
- Safety over EtherCAT Implementation Support
  - Support for planning, implementation and certification
- FSoE Conformance Test
  - Test cases to approve conformance for FSoE Master and FSoE Slave devices are available and approved
  - FSoE Conformance Test Tool for FSoE Slave devices approved by TUV
- Implementations of several vendors already exist

Safety over EtherCAT - Vendors

*as of 12/2019

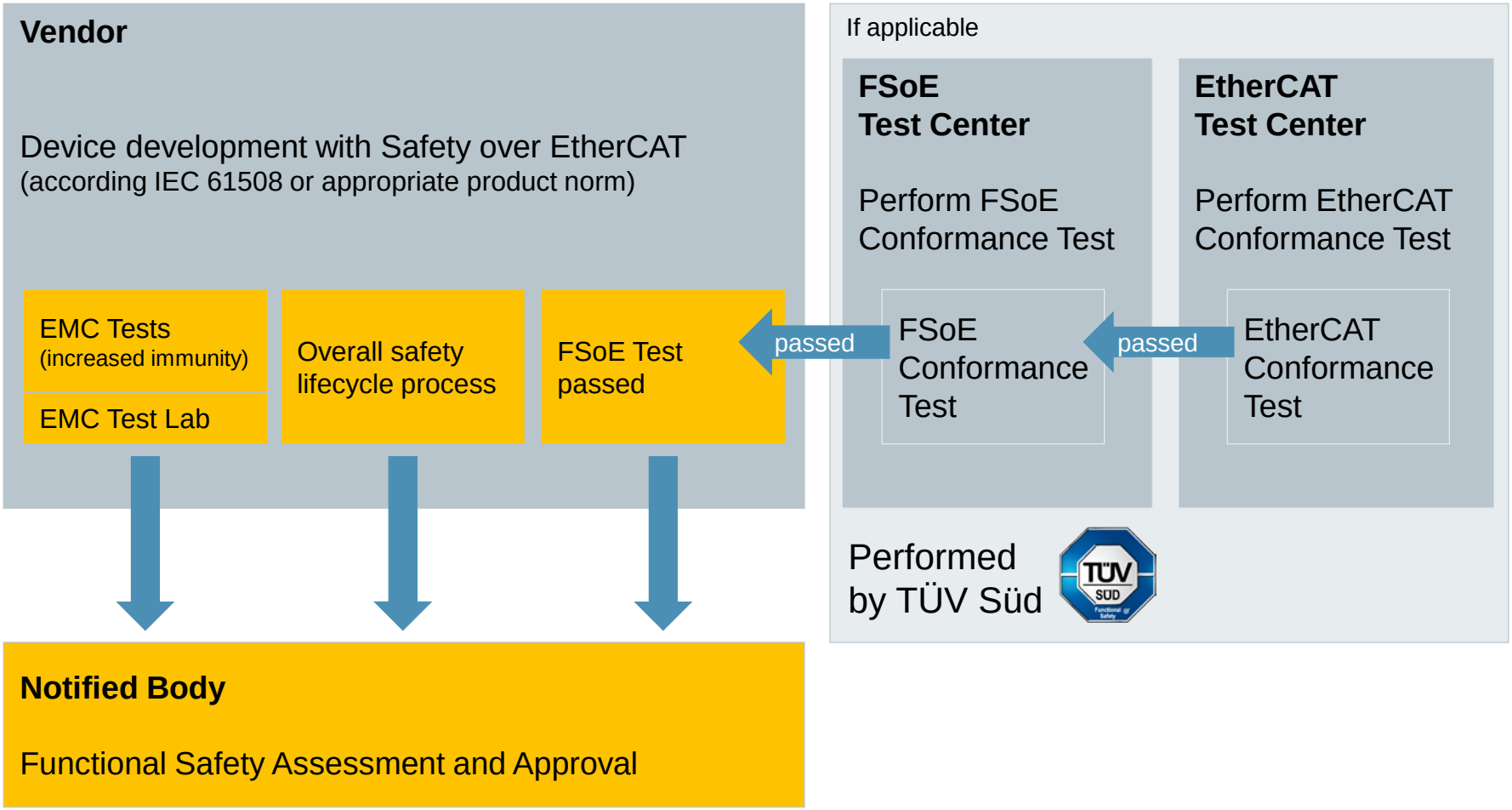
Safety over EtherCAT®

Safety over EtherCAT Conformance

- ETG.9001 Safety over EtherCAT Policy
  - defines FSoE conformance testing rules and policies

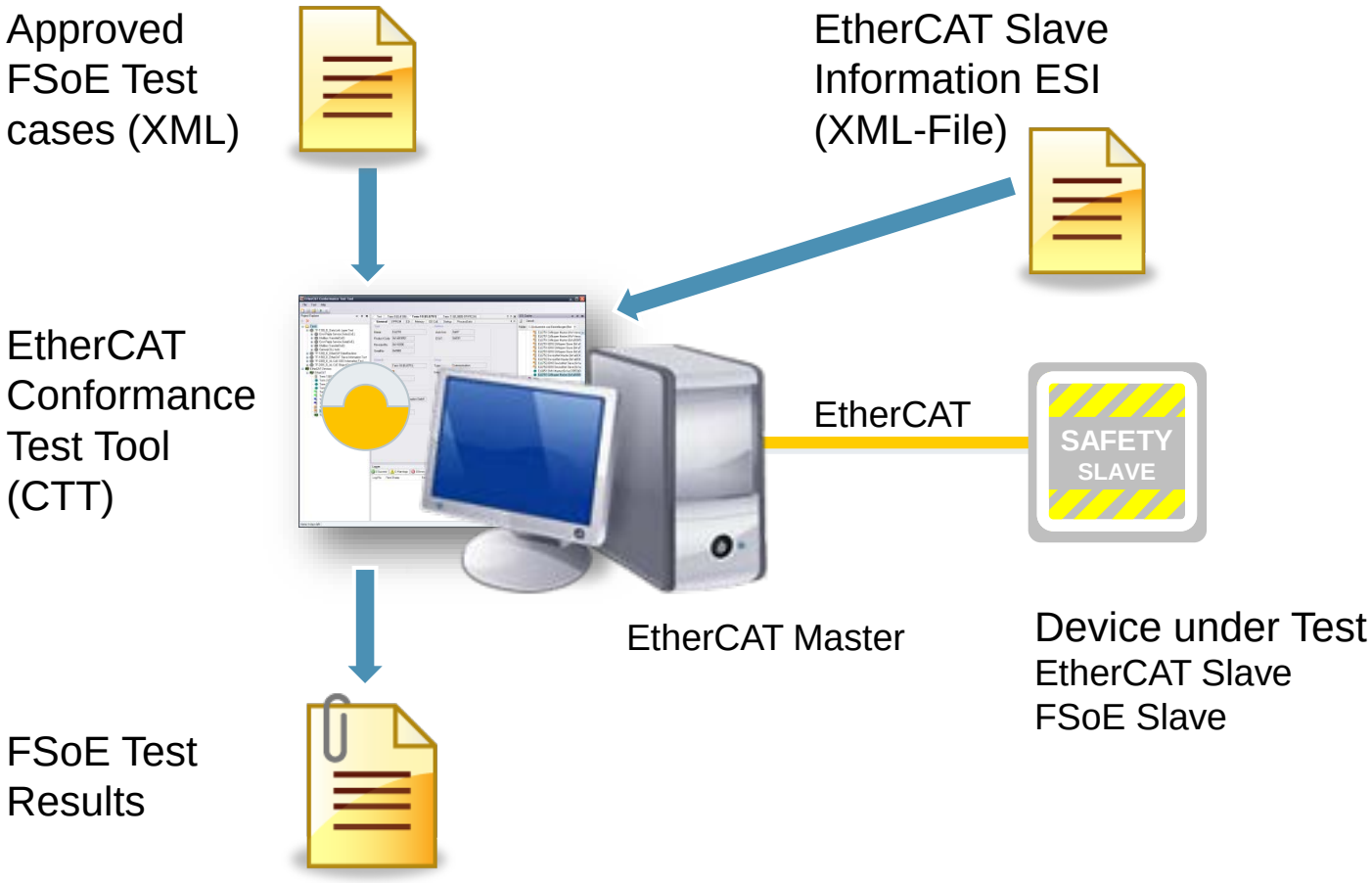
- FSoE Devices shall fulfil following requirements:
  - Compliance to
    - IEC 61508 and / or relevant sector / product standards
    - IEC 61784-3 general part
    - ETG.5100 Safety over EtherCAT Specification
    - EtherCAT Conformance Test Policy (if applicable)
  - Passing Functional Safety Assessment and approval of the FSoE Device by a Notified Body

Device Assessment and Approval

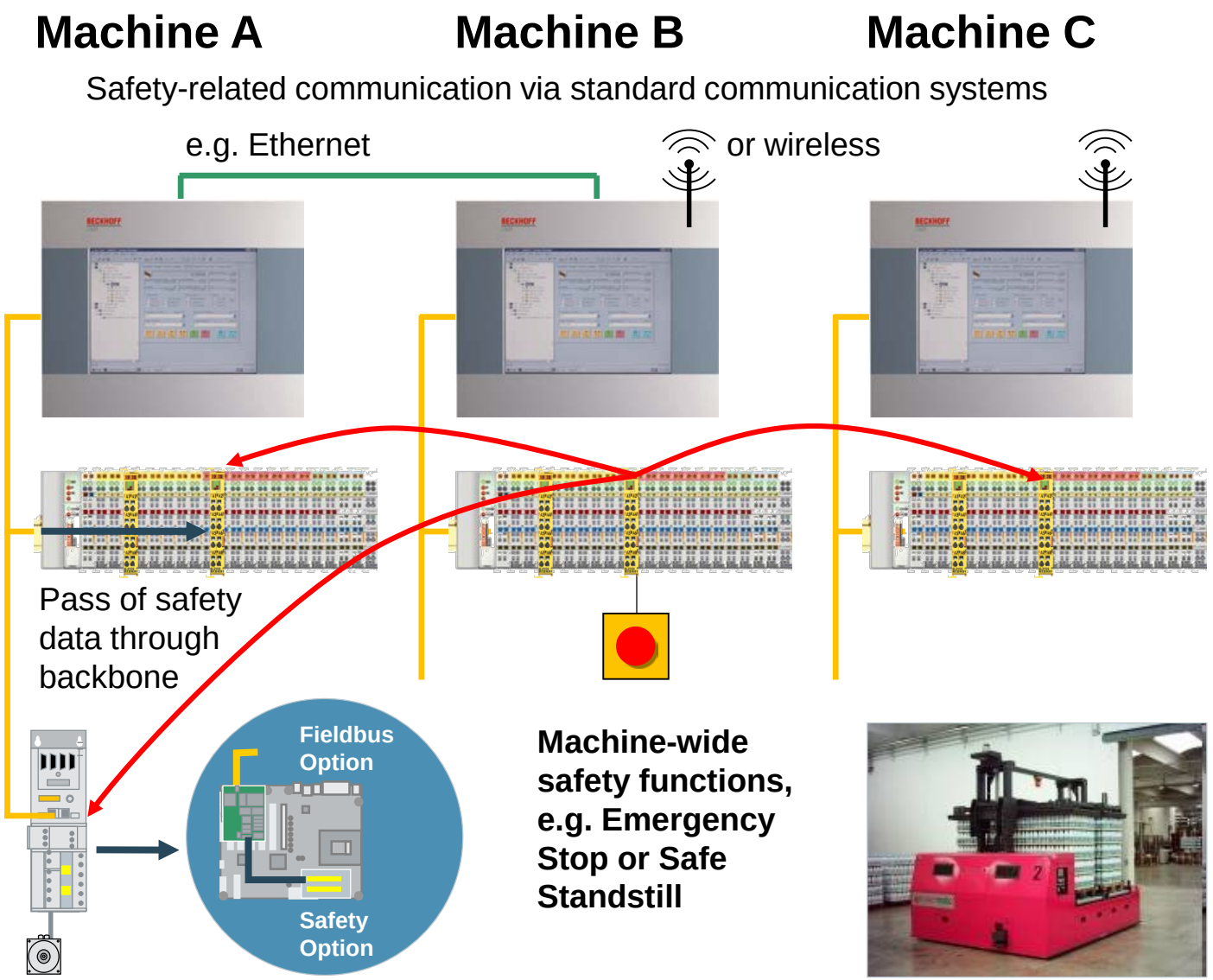


Process according to ETG.9100 FSoE Policy

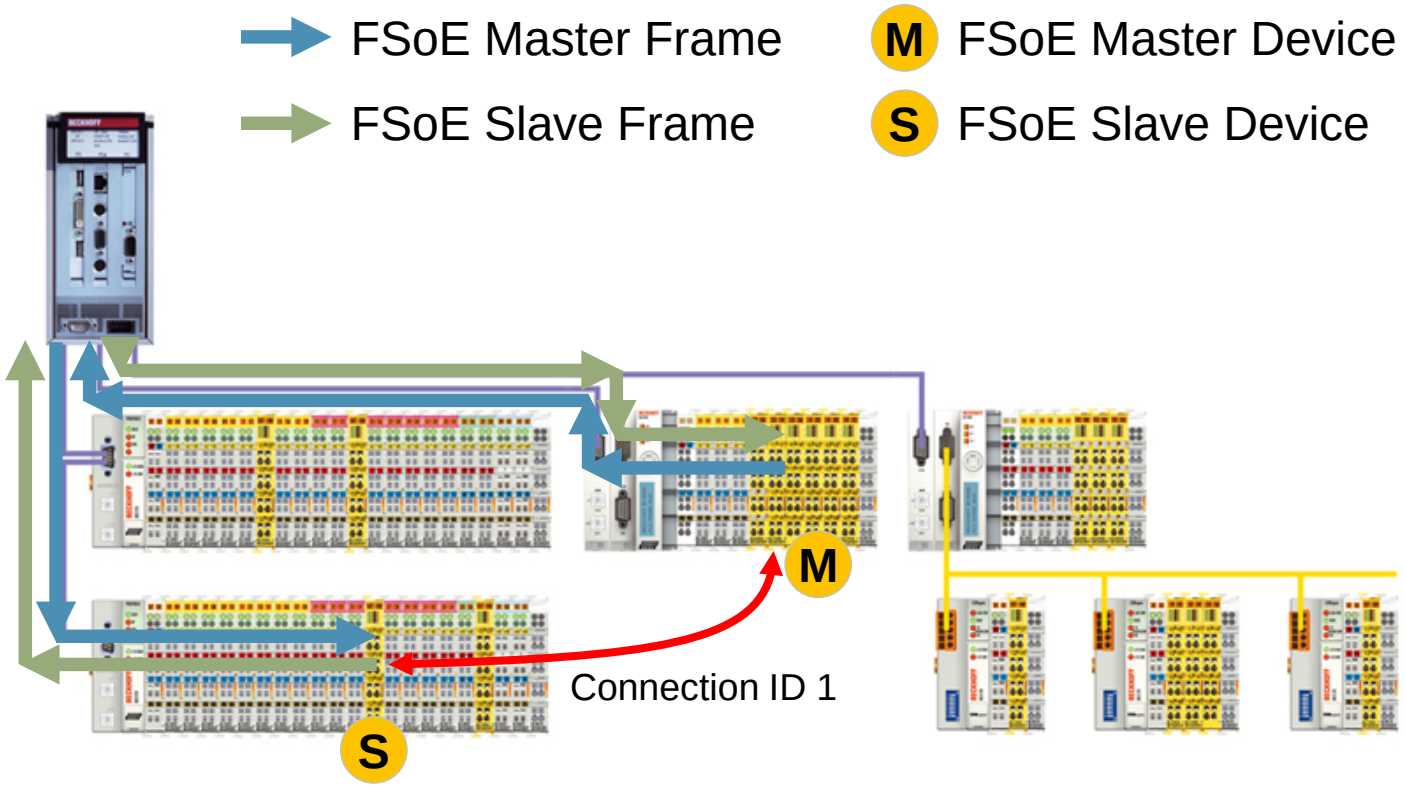
FSoE Conformance Test Tool



System aspects

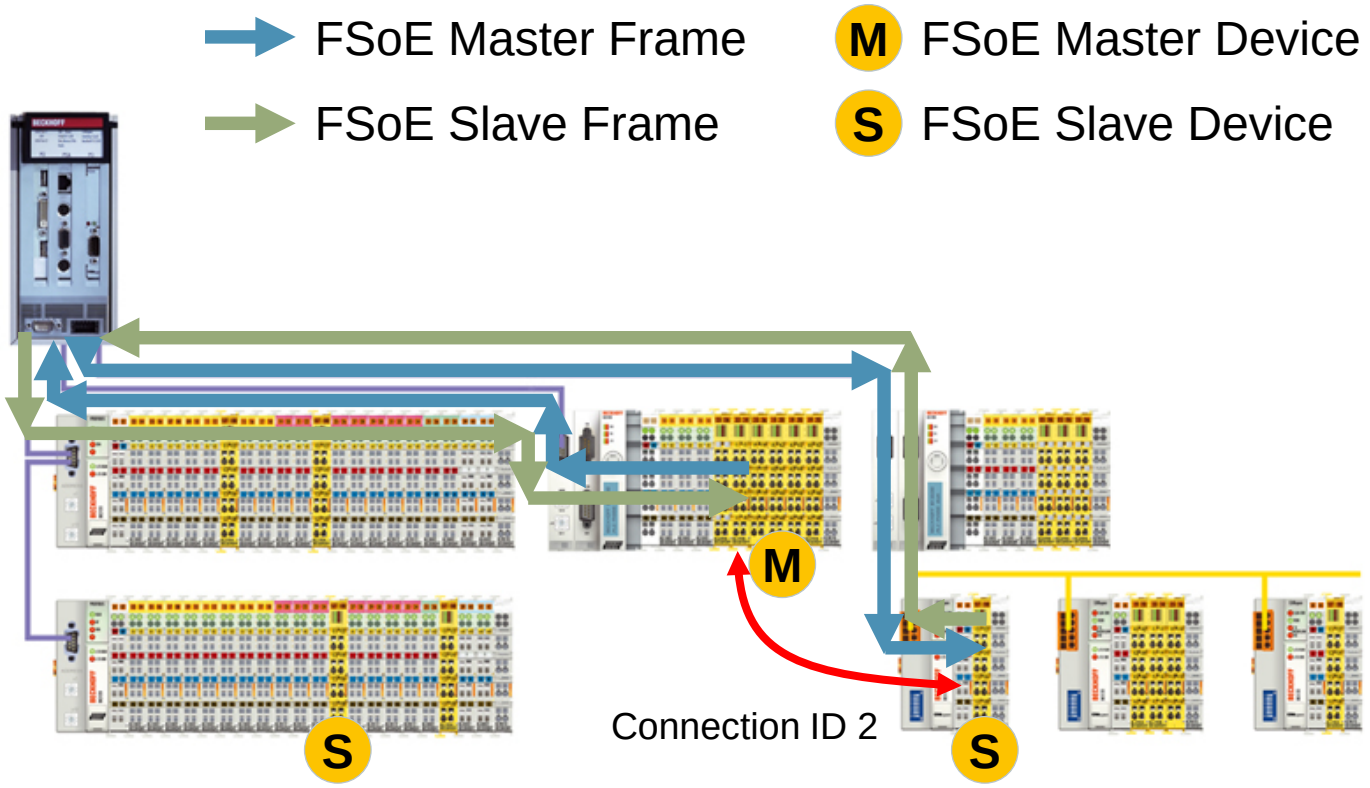


Safety for modern automation



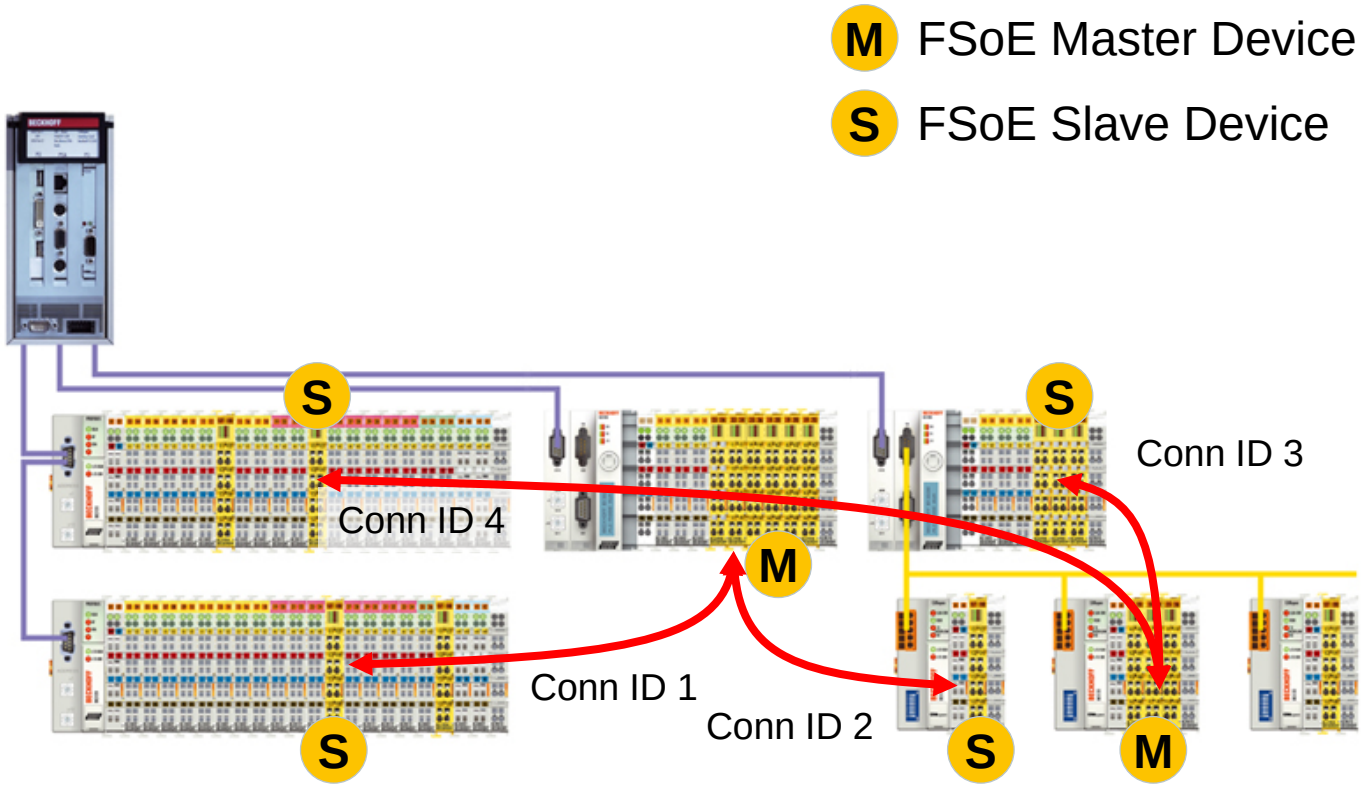
- Configured Master-Slave Connections
- Communication is routed via standard PLC

Safety for modern automation



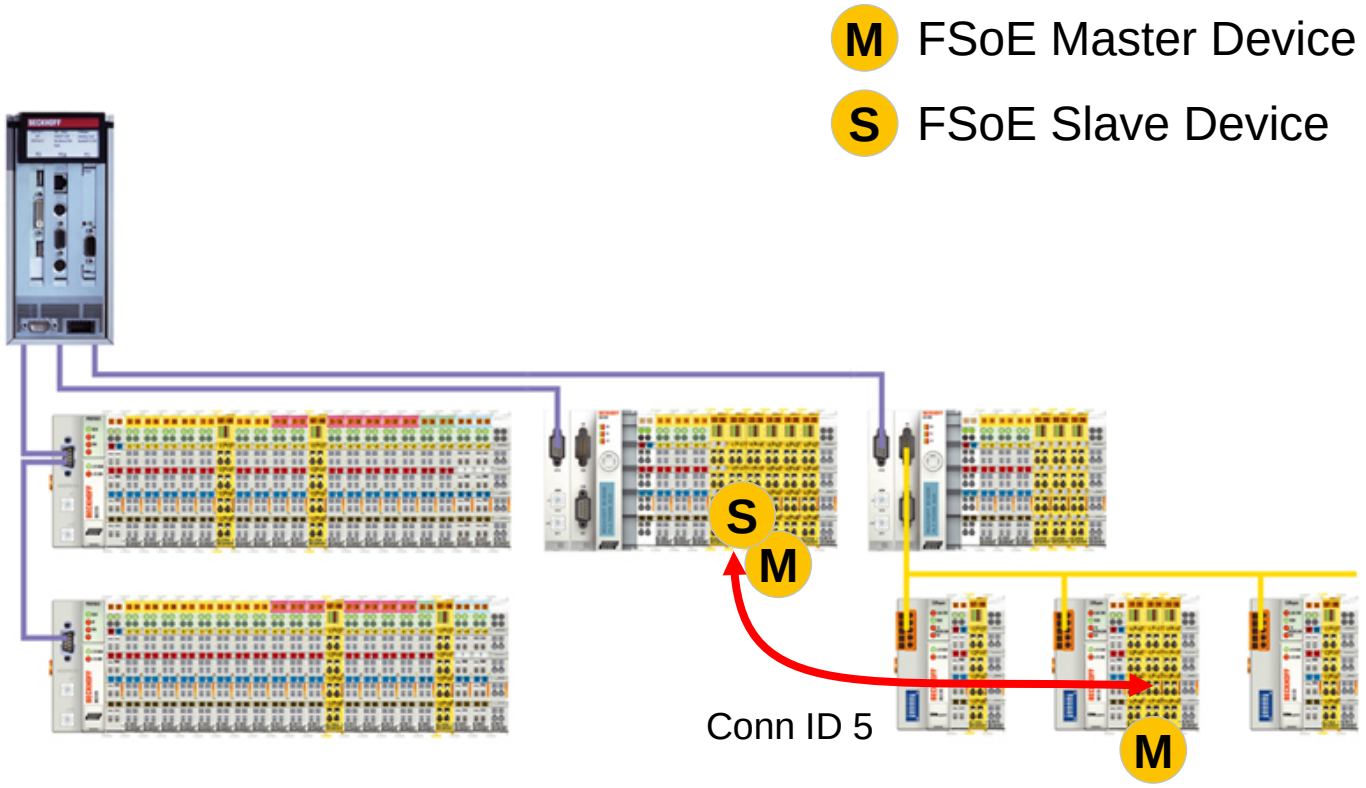
- Configured Master-Slave Connections
- Communication is routed via standard PLC

Safety for modern automation



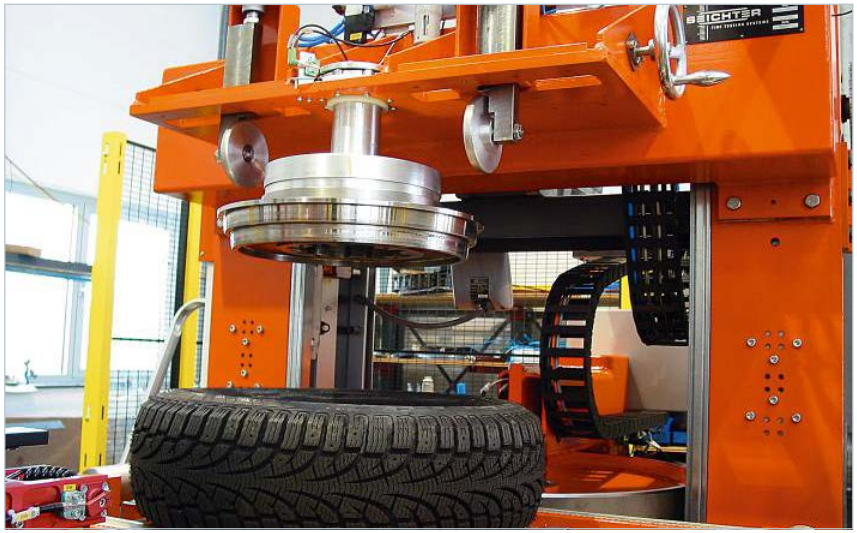
- Several Master in one network
- Safety groups with group-switch-off possible

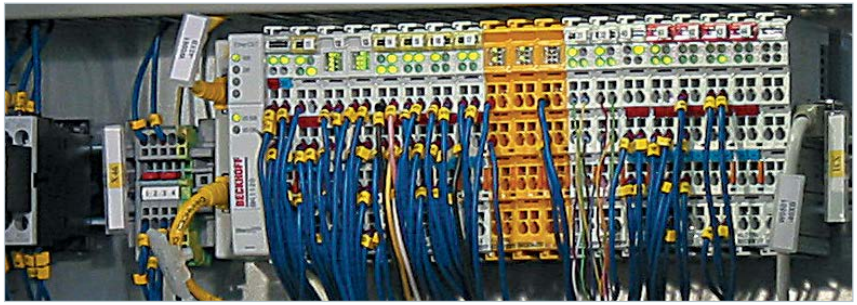
Safety for modern automation



- “Master–Master” communication via Master&Slave implementation in the device
- Unique Conn-ID necessary!
- Used for machine chaining

Application | Tire and wheel testing machine



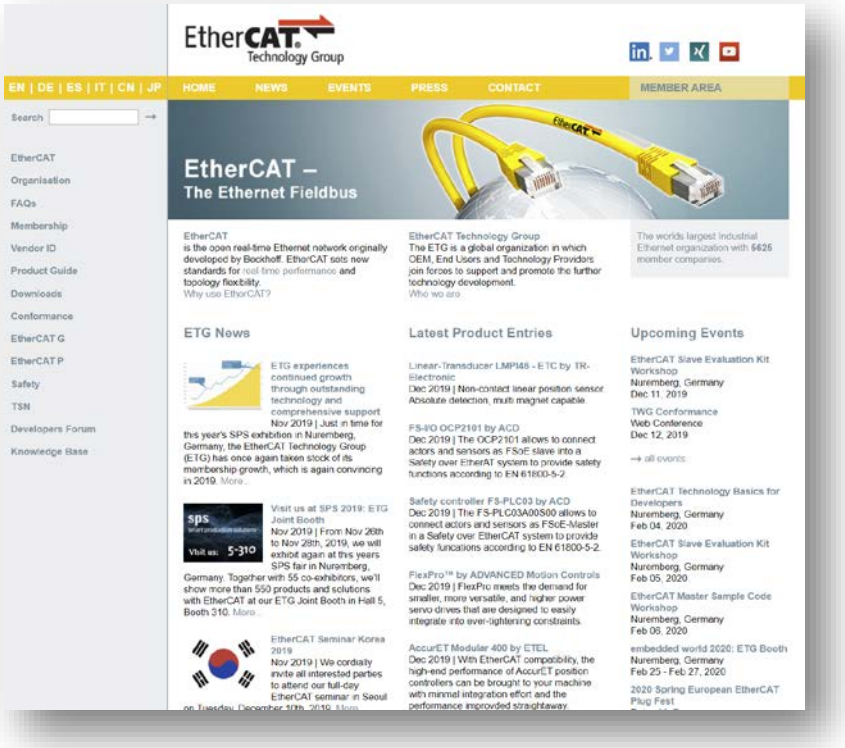


Application | Tire and wheel testing machine

- Advantages for the costumer:
- Integration of Safety functions in the TwinSAFE system
  - Emergency stop
  - Safety fence monitoring
- Small switch box directly at the safety fence
- Optimum interaction between standard automation and safety technology
  - Reduced engineering and hardware costs
  - Simplified wiring
  - Modifications are easy to implement
- Only one tool needed for Standard and Safety functions
  - TwinSAFE software editor conveniently integrated in the TwinCAT system

Safety over EtherCAT

www.ethercat.org



EtherCAT Technology Group
Dr. Guido Beckmann
g.beckmann@ethercat.org