

Overview Safety over EtherCAT

EtherCAT Technology Group

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

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

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- **BGIA Test principles GS-ET-26**
 - Test principles of the German Institute for Occupational Safety and Health
 - Scope: Bus systems for safety related communication
- **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

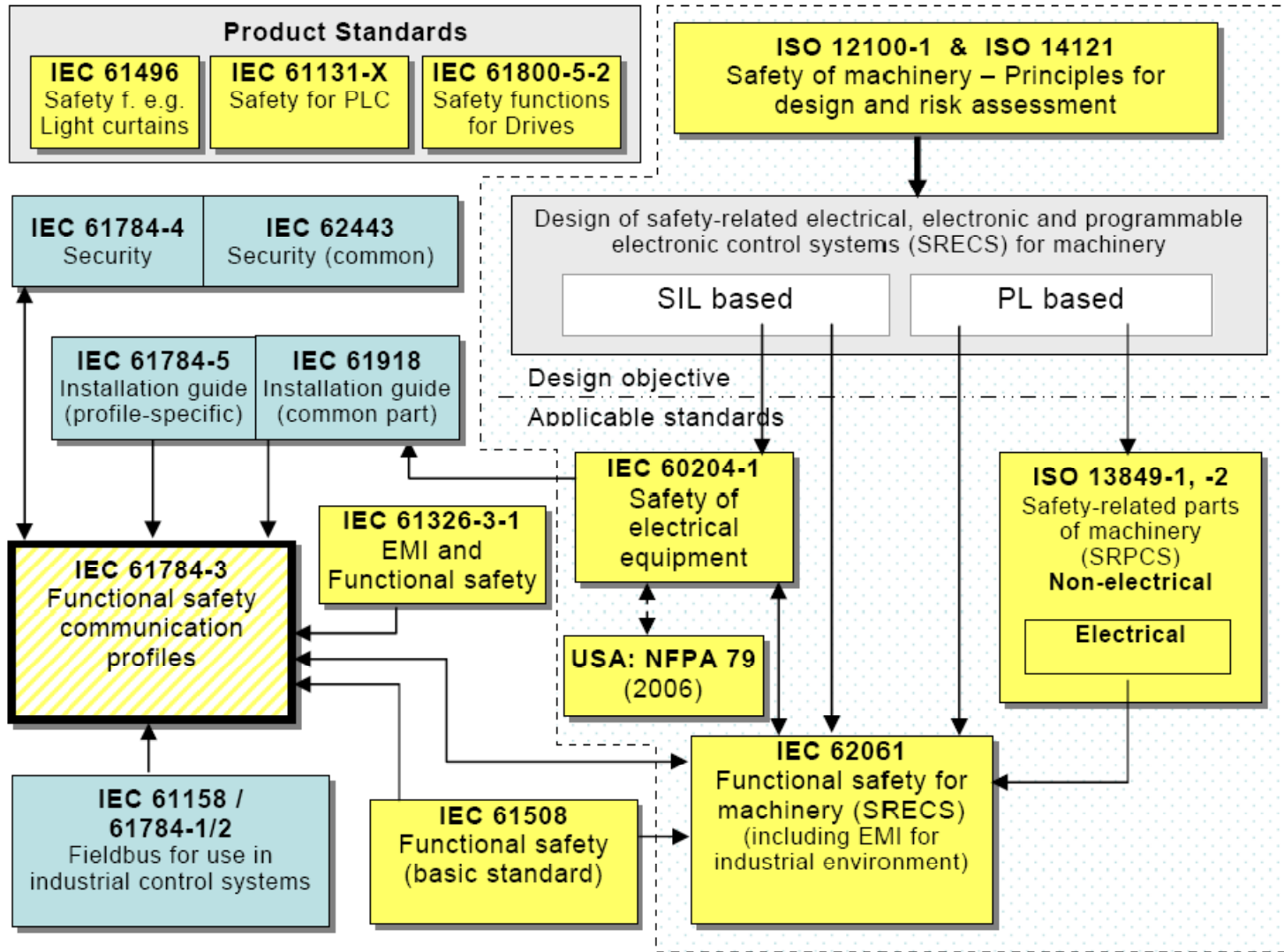
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



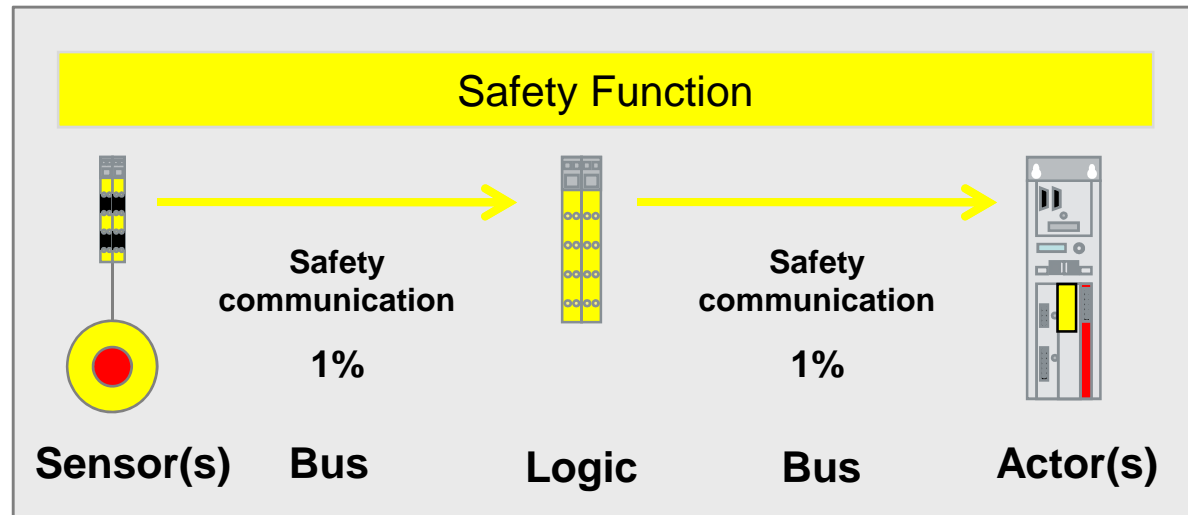
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- Probability of failure for the safety system:
 - $PFH_{\text{Safetyfunction}} = PFH_{\text{Sensor}} + PFH_{\text{Logic}} + PFH_{\text{Actor}} + 2x PFH_{\text{Bus}}$
 $< 10^{-8} \dots 10^{-7} / \text{h}$ for SIL 3 (IEC 61508)
- 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:
 - $PFH_{\text{Bus}} < 10^{-9} / \text{h}$ for SIL 3
- More than 100.000 years communication without an undetected Error!

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- **Safety over EtherCAT** (FSoE) defines a safety communication layer for the transportation of safety process data between safety over EtherCAT devices.
- FSoE is an open technology within the EtherCAT Technology Group (ETG).
- The protocol is approved by an independent Notified Body (TUV Sued Rail GmbH).

Safety over
EtherCAT[®]

Requirements

Safety over EtherCAT

- Architecture

- Definitions

- State Machine

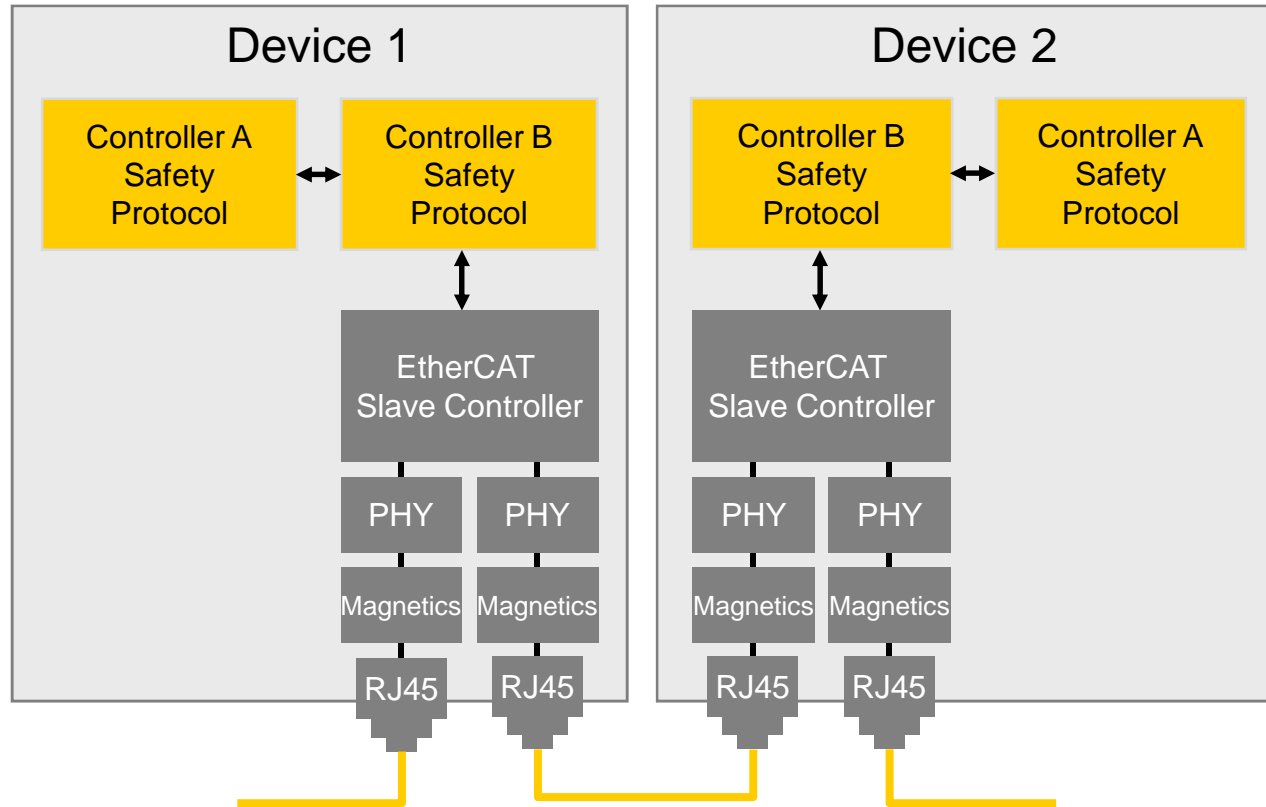
- Frame Structure

- Summary

Conformance

Applications

- 1-channel communication system
Model A according to IEC 61784-3 Annex A



Requirements

Safety over EtherCAT

- Architecture

- Definitions

- State Machine

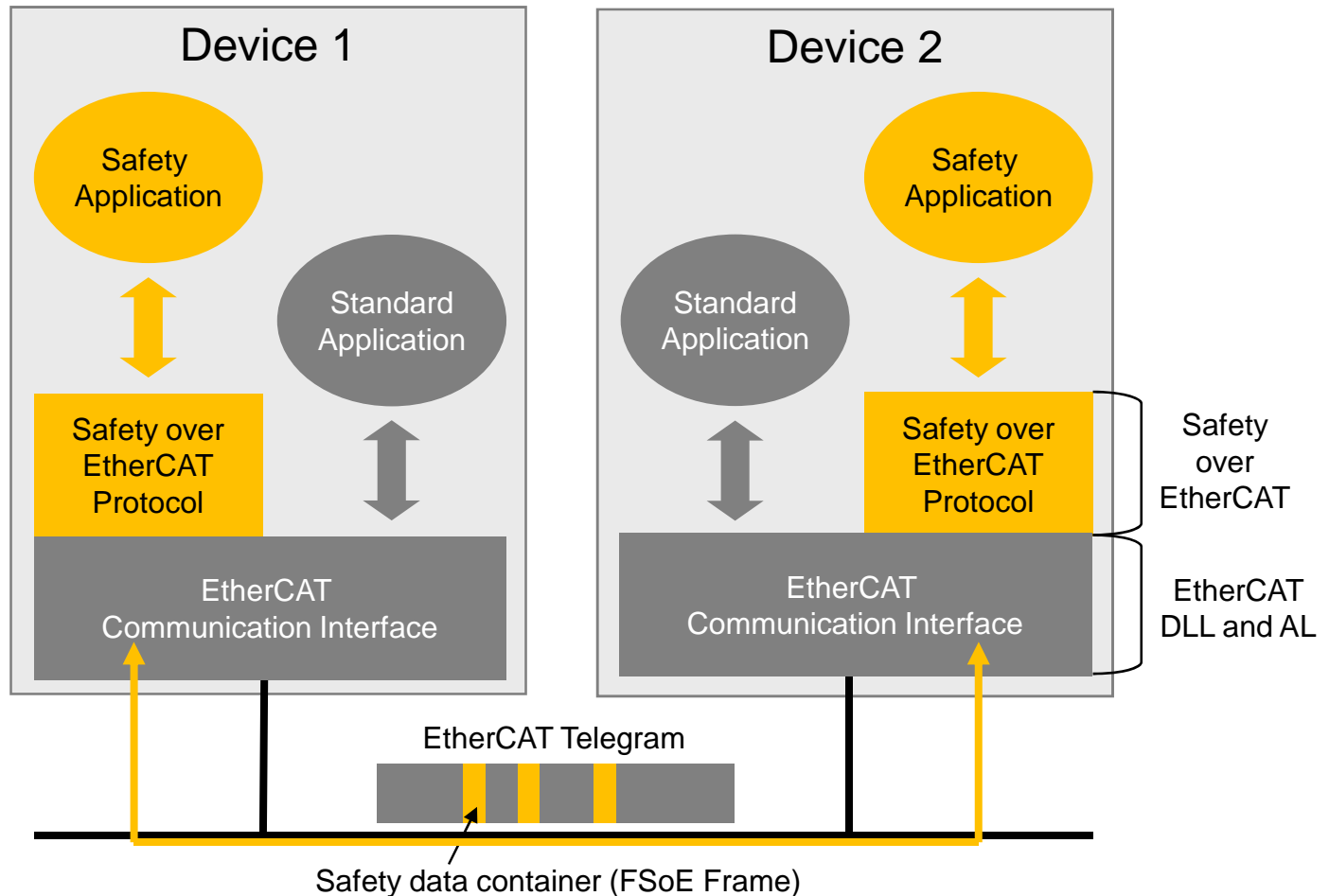
- Frame Structure

- Summary

Conformance

Applications

- Black channel approach with safety and non-safety data on the same bus



Requirements

Safety over EtherCAT

- Architecture

- Definitions

- State Machine

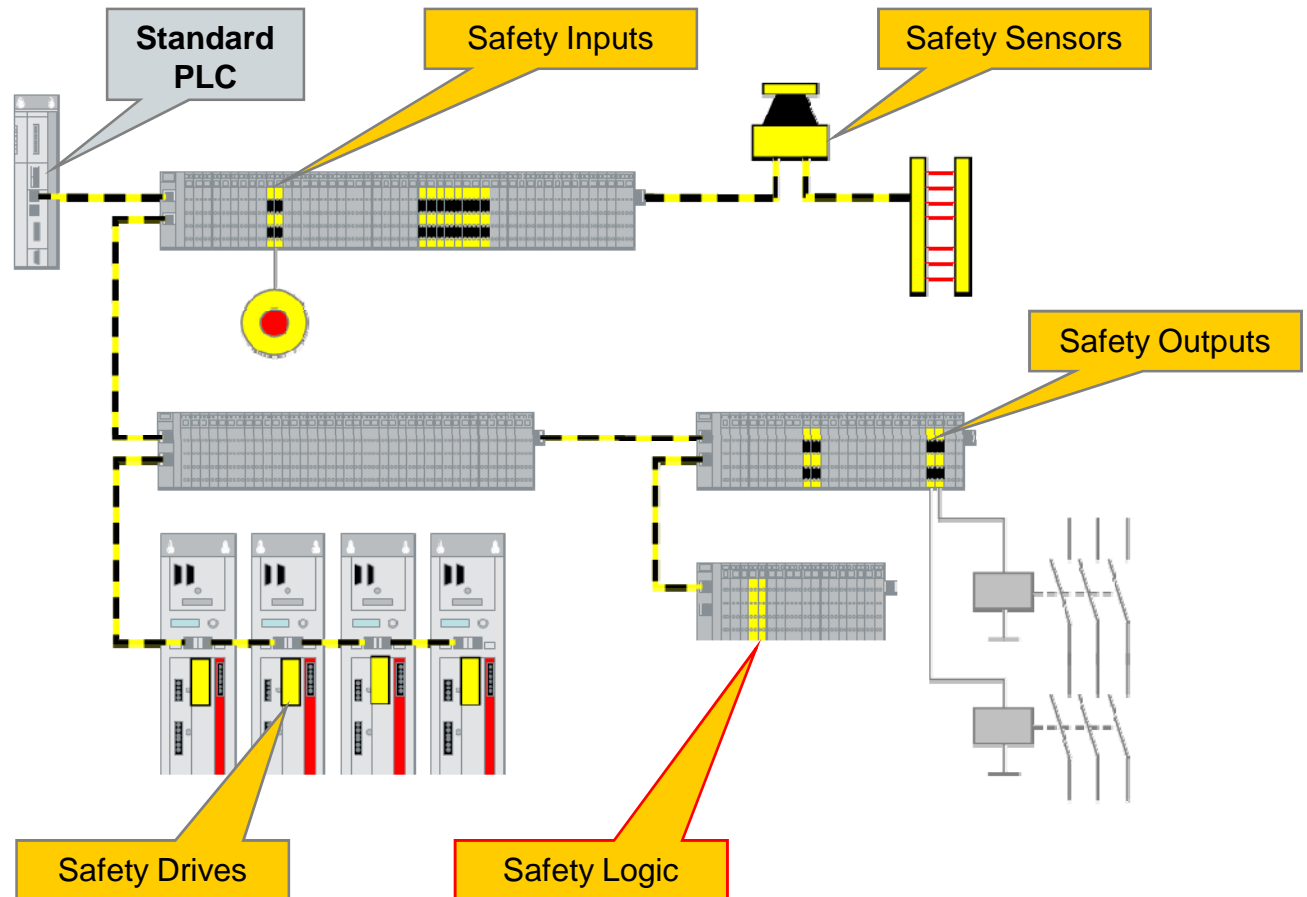
- Frame Structure

- Summary

Conformance

Applications

- Decentralized Safety-Logic
- Standard PLC routes the safety messages



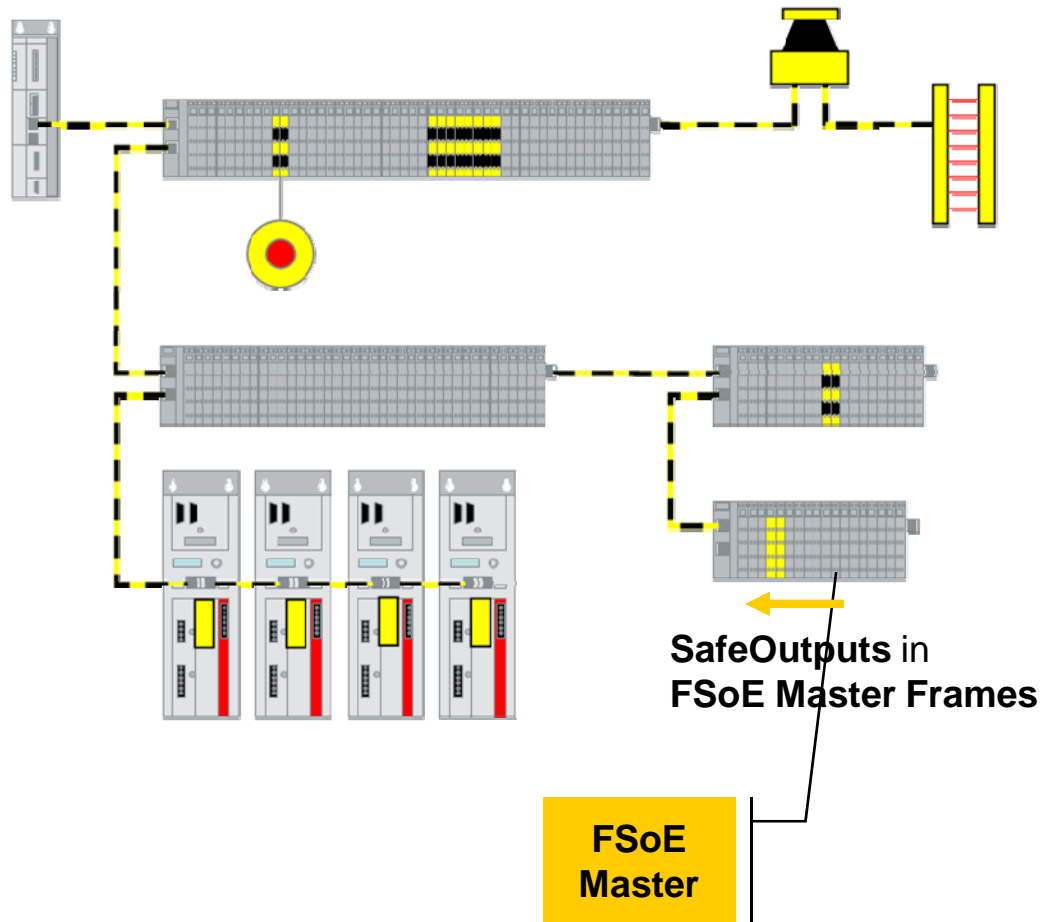
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Master

Master of a FSoE Connection. The Master initiates the communication.

The FSoE Master sends a **FSoE Master Frame**, which contains the **SafeOutputs**.

A FSoE Master can manage one or many FSoE Slaves.

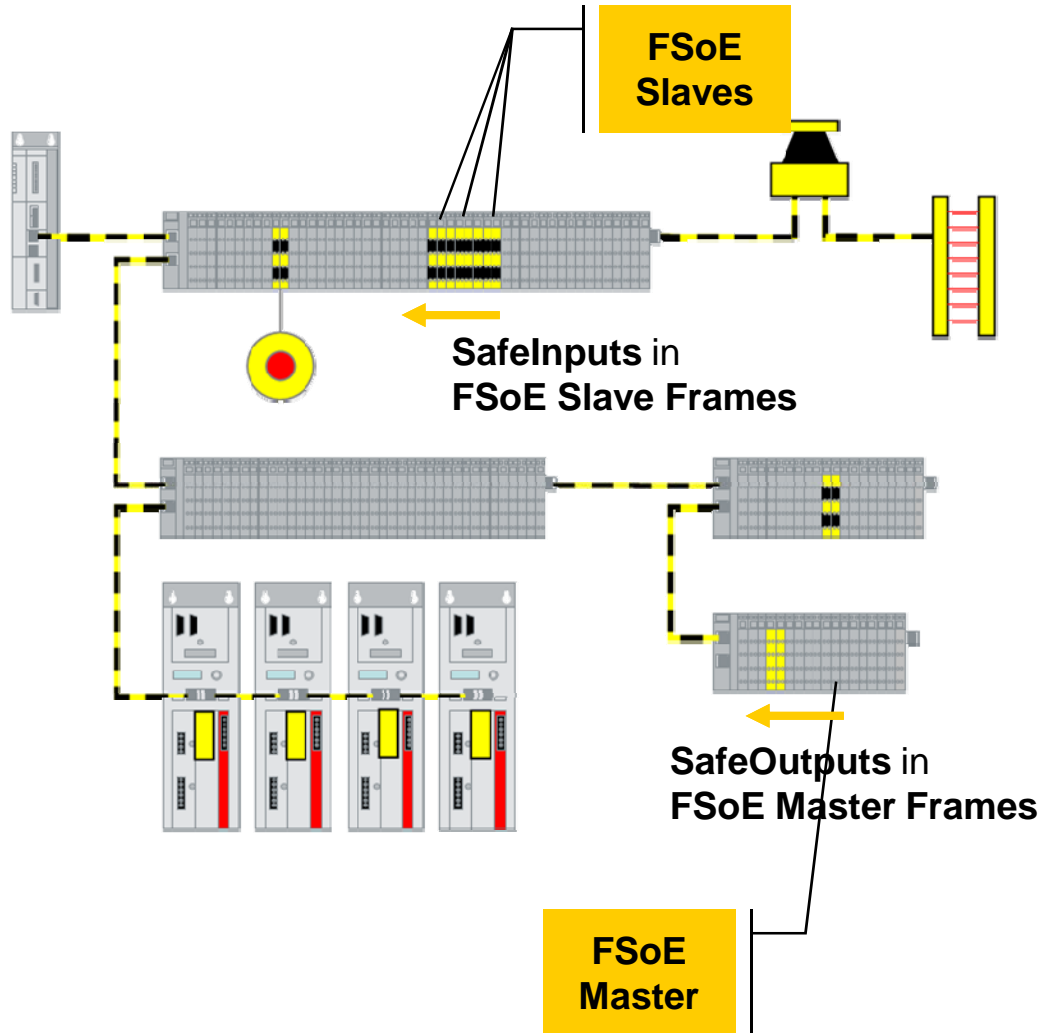
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Slave

Slave of a FSoE Connection.

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

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

A FSoE Slave belongs to one FSoE Master.

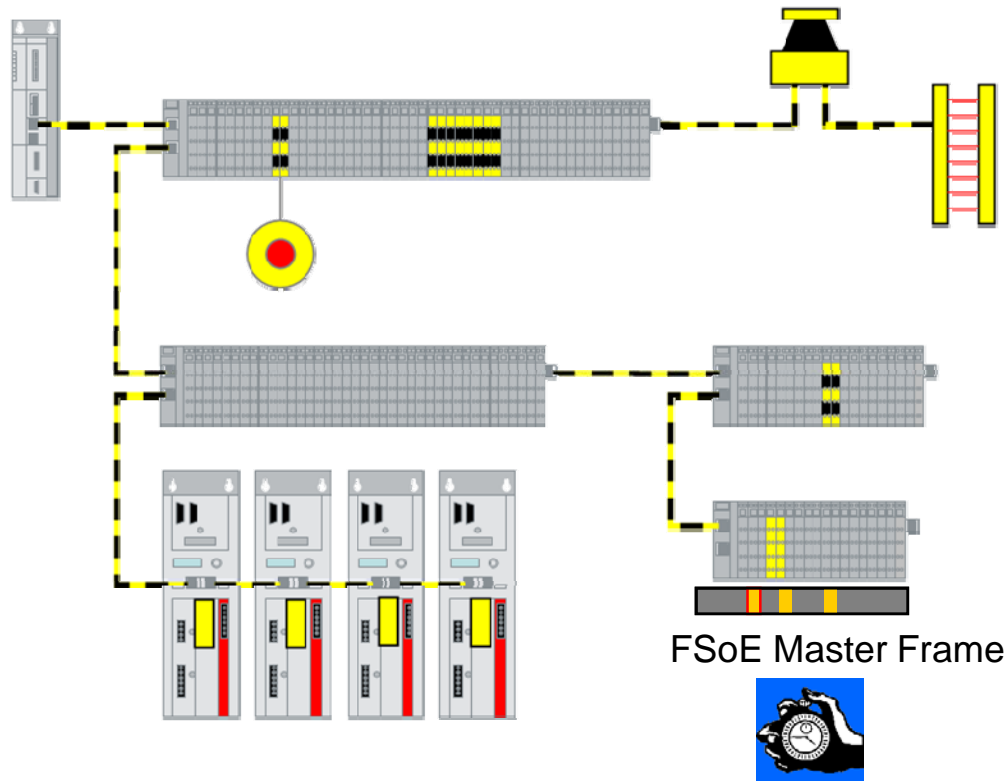
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Cycle

The FSoE Cycle consists of the FSoE Master Frame confirmed by a FSoE Slave Frame.

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

With sending the FSoE Master Frame the Master starts a Watchdog-Timer for guarding the FSoE Slave

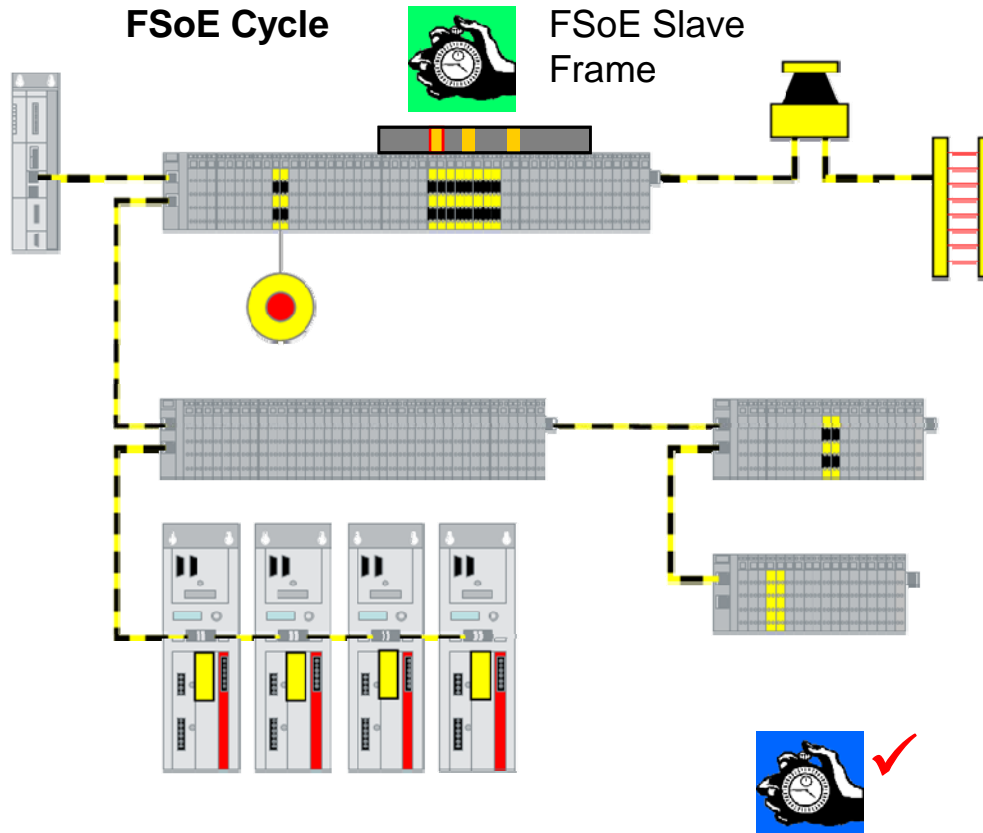
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Cycle

The FSoE Cycle consists of the FSoE Master Frame confirmed by a FSoE Slave Frame.

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

With sending the FSoE Master Frame the Master starts a Watchdog-Timer for guarding the FSoE Slave

The FSoE Master only generates a new FSoE Master Frame after receiving a valid FSoE Slave Frame. This starts a new cycle.

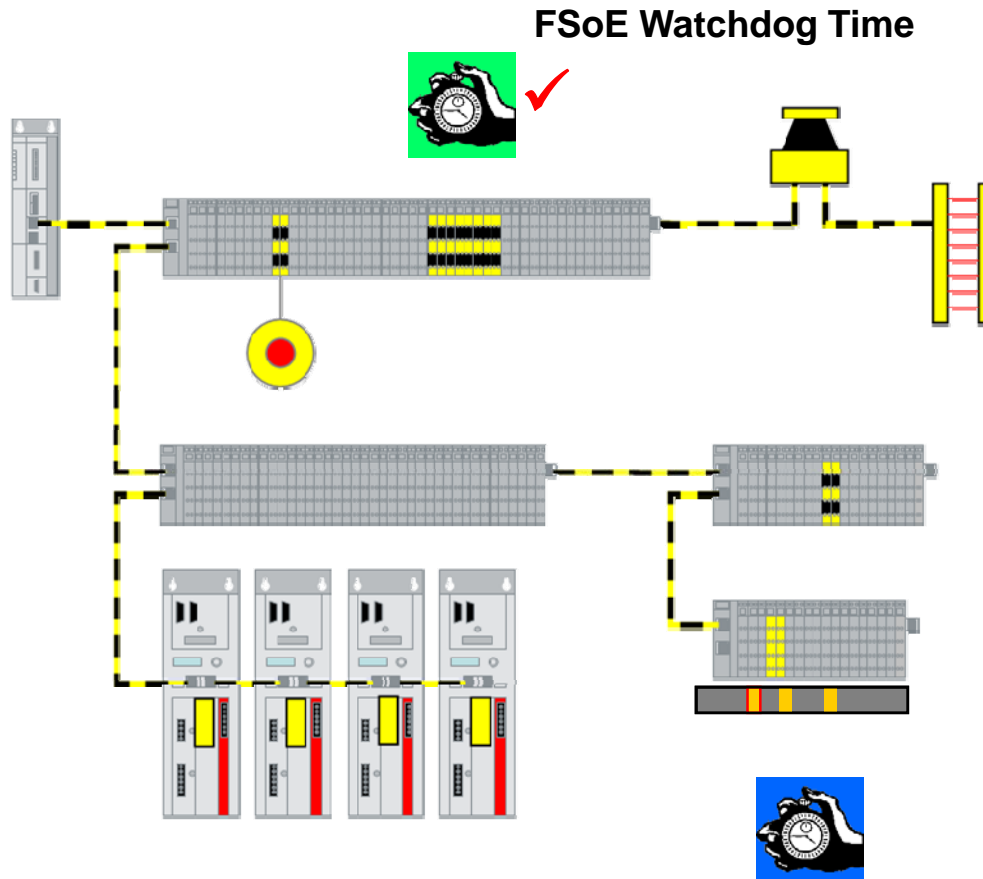
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Watchdog Time

Every device guards that the partner sends a new FSoE Frame within the configured **FSoE Watchdogzeit**

If the Watchdog expires, the devices change to the Reset State.

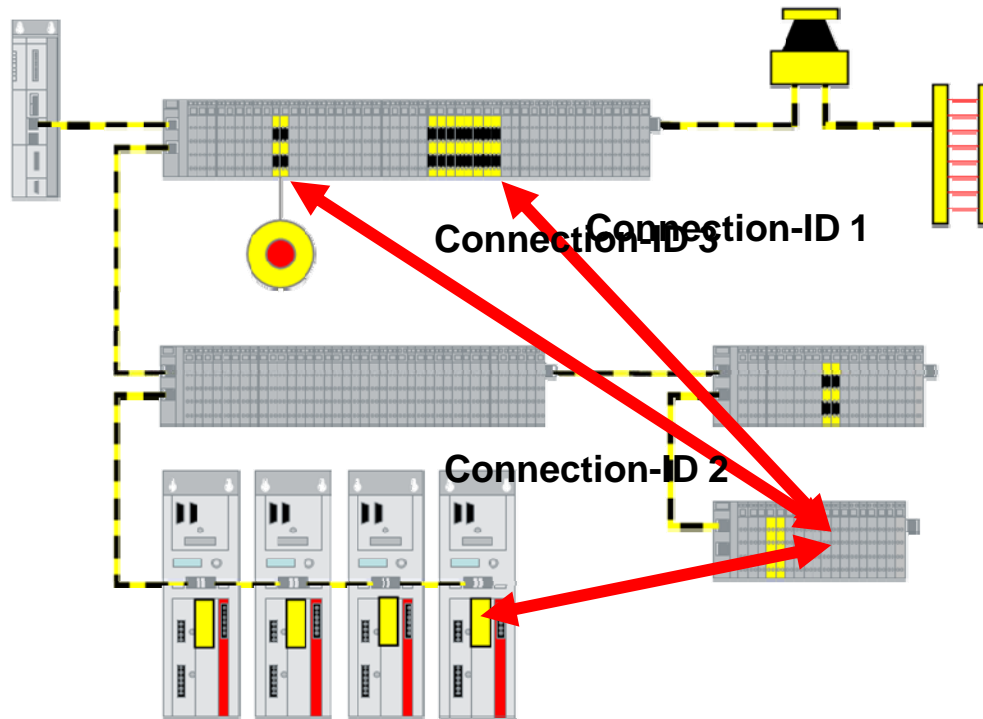
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Connection

The FSoE Connection is a logical connection between an FSoE Master and an FSoE Slave.

It shall be a unique **Connection-ID** in the system. This must be checked within the configuration.

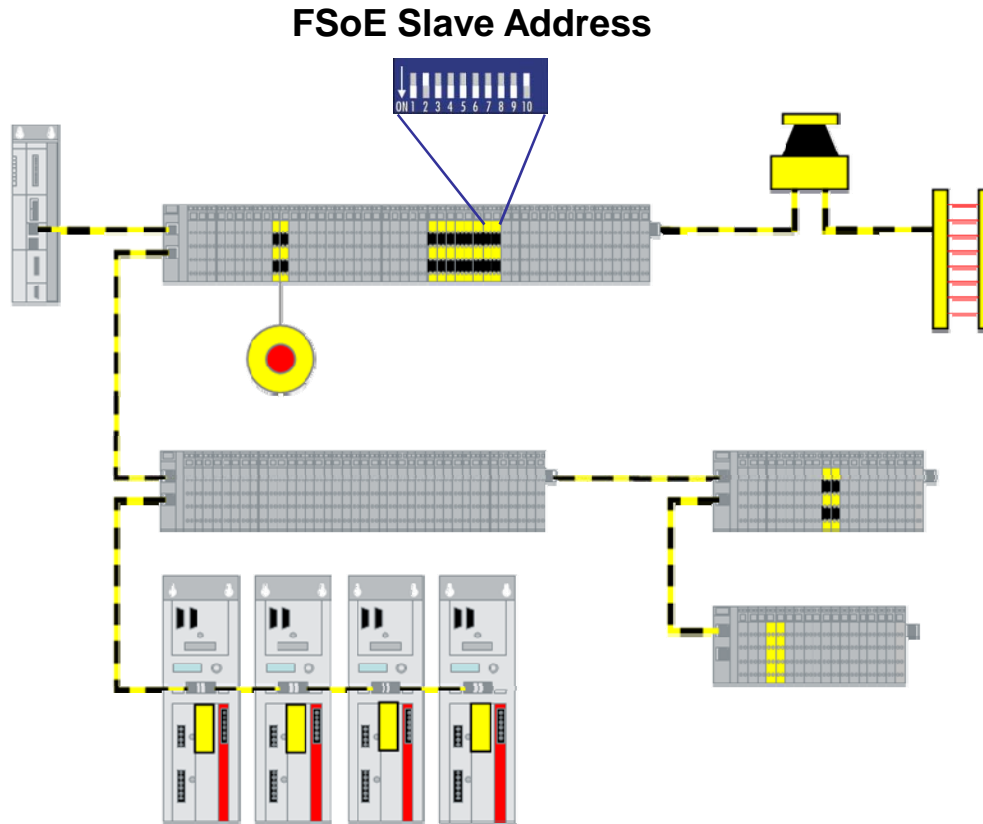
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



FSoE Slave Address

Beside the Connection-ID every FSoE Slave has in the scope of the system a unique 16-Bit **FSoE Slave Address**

This address can be adjusted at the Device, e.g. via a DIP-Switch.

Up to 65.535 Devices can be addressed.

FSoE State Machine per Connection

Requirements

Safety over EtherCAT

- Architecture

- Definitions

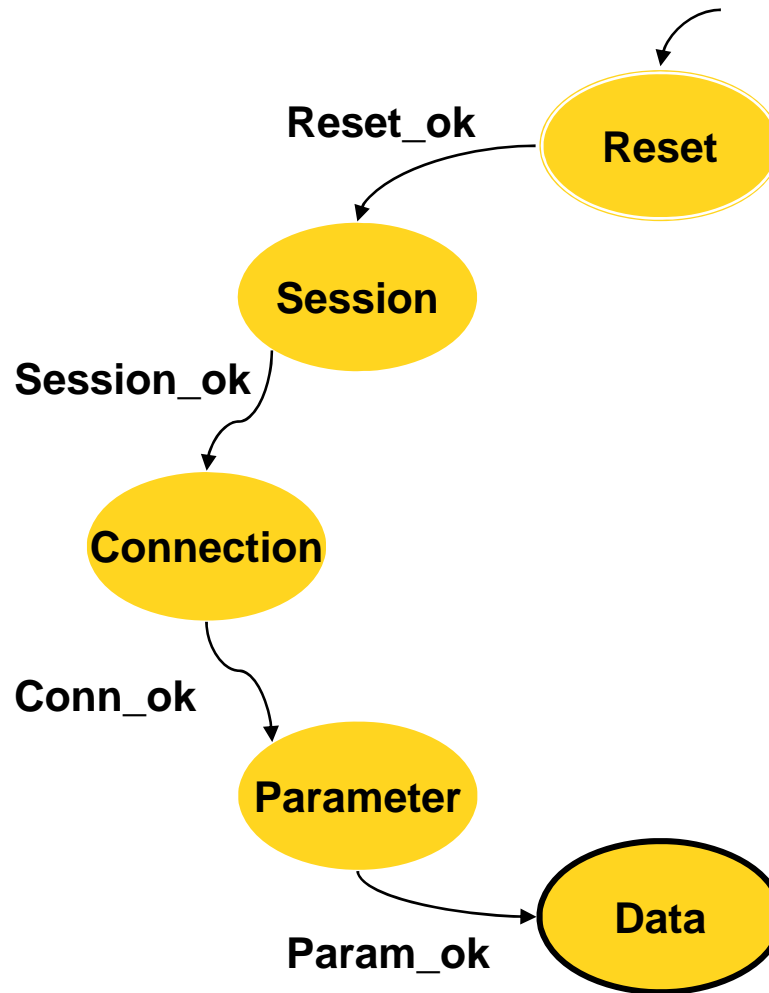
- State Machine

- Frame Structure

- Summary

Conformance

Applications



- Every FSoE Connection is handled by an FSoE State Machine.
- The FSoE Master manages a
- single FSoE State Machine per FSoE Slave.
- After Power-On the FSoE Master and the FSoE Slave are in the State Reset.
- The Safe Outputs can only be set in the state Data.

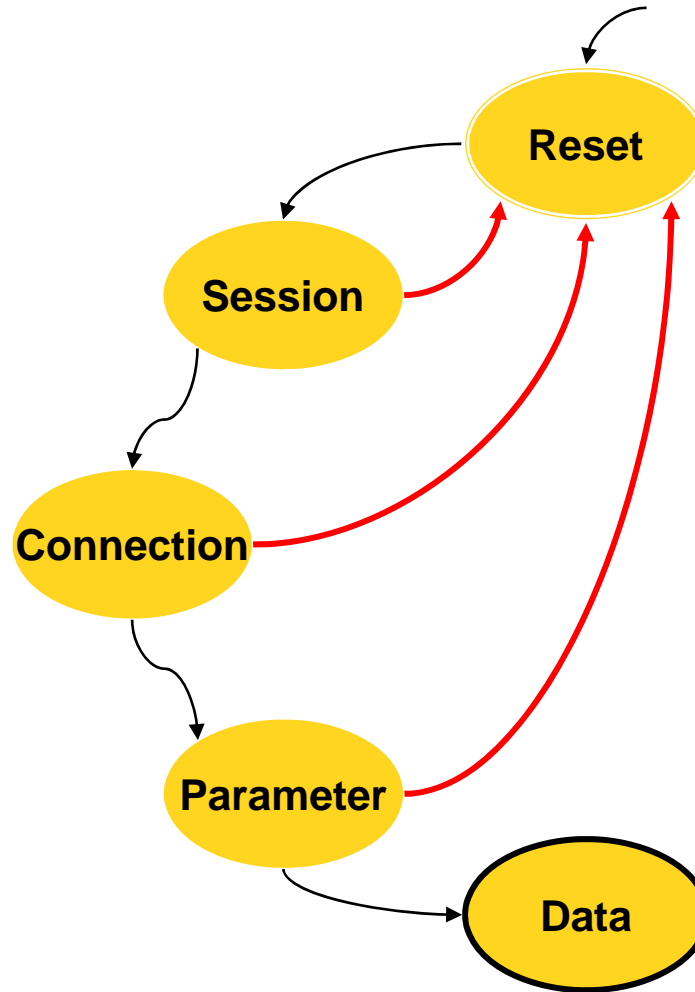
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- In case of an error the devices change to the Reset state.
- Master:
An internal detected Error (communication error or application error)
- Slave:
An internal error is detected or after receiving a Reset telegram from the Master

Requirements

Safety over EtherCAT

- Architecture

- Definitions

- State Machine

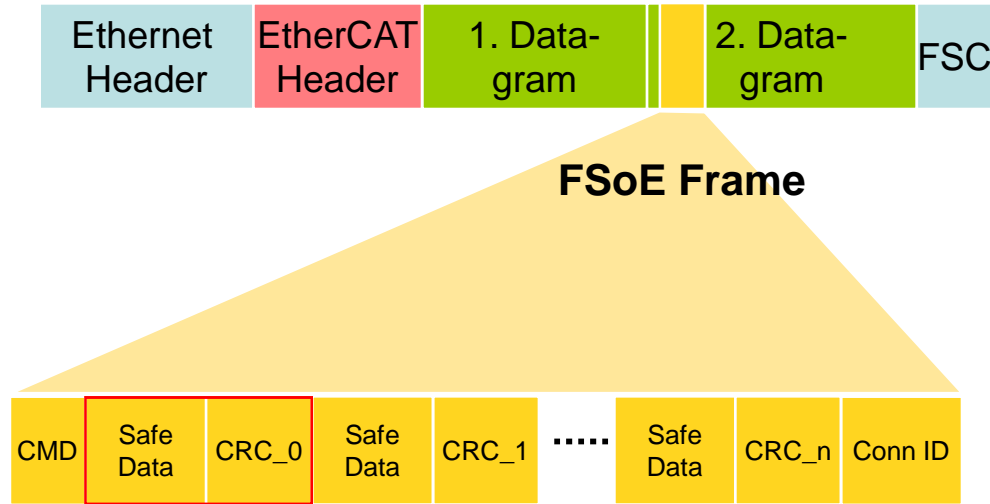
- Frame Structure

- Summary

Conformance

Applications

Ethernet-Telegram



FSoE Frame

The FSoE Frame is mapped 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.

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

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

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- The FSoE specification has no restrictions according to:
 - Communication layer and interface
 - Transmission speed
 - Length of safe process data
- Routing via unsafe gateways, fieldbus systems or backbones is possible.



Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- Residual Error Probability $R_{(p)} < 10^{-9}/h$
- 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 submitted to IEC 61784-3 Functional safety fieldbuses
 - Release date 2010

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- 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.
- Safe Device Parameter can be downloaded from the Master to the Slave at Boot-Up of a FSoE Connection

Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- Protocol test for the devices
 - Connection via EtherCAT Interface
 - Black box Test
- Test suite available for device manufactures
 - Test suite can be used during device development
 - No special Hardware necessary
- Independent Test Laboratory for confirmation of conformity

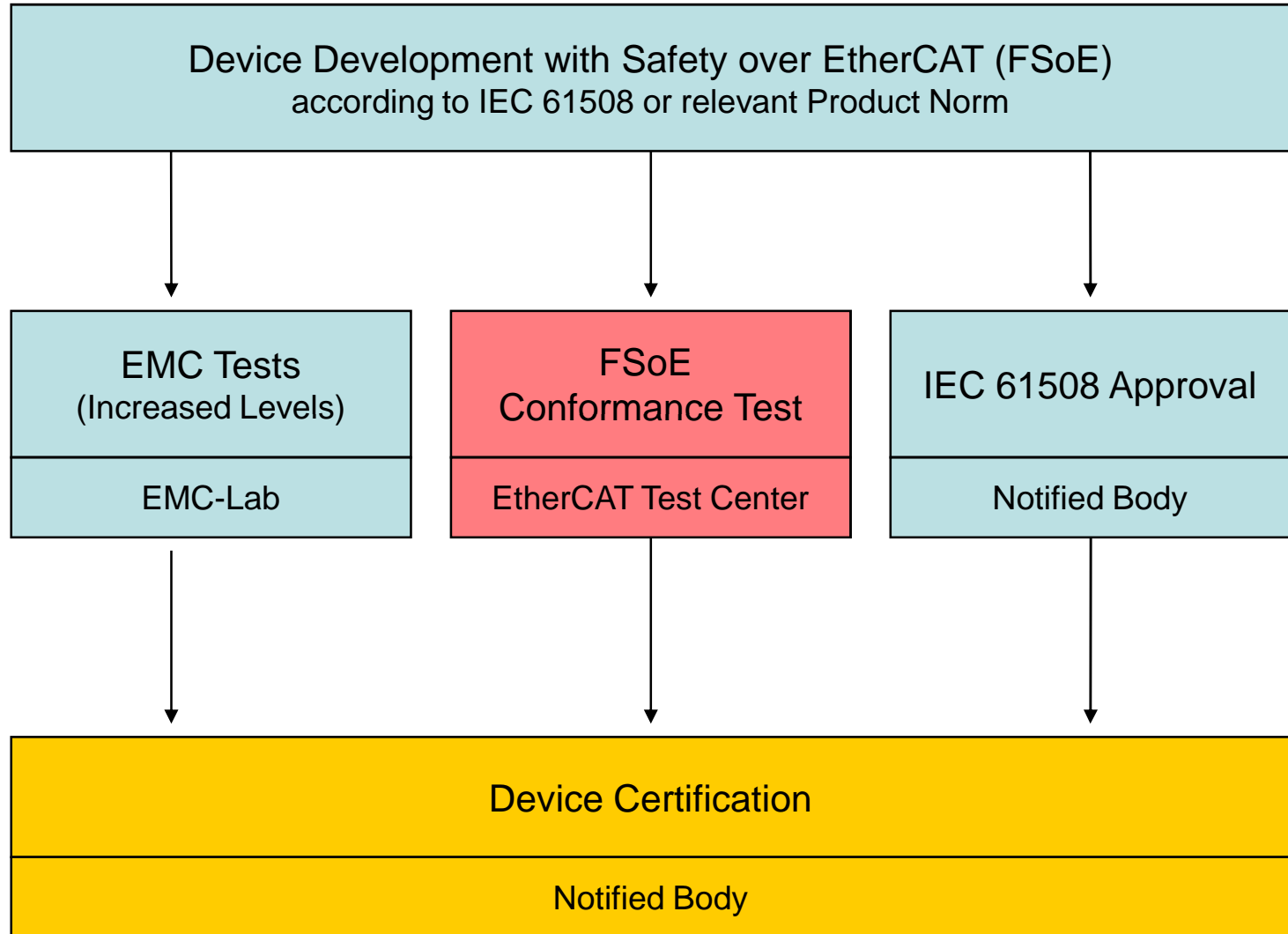
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



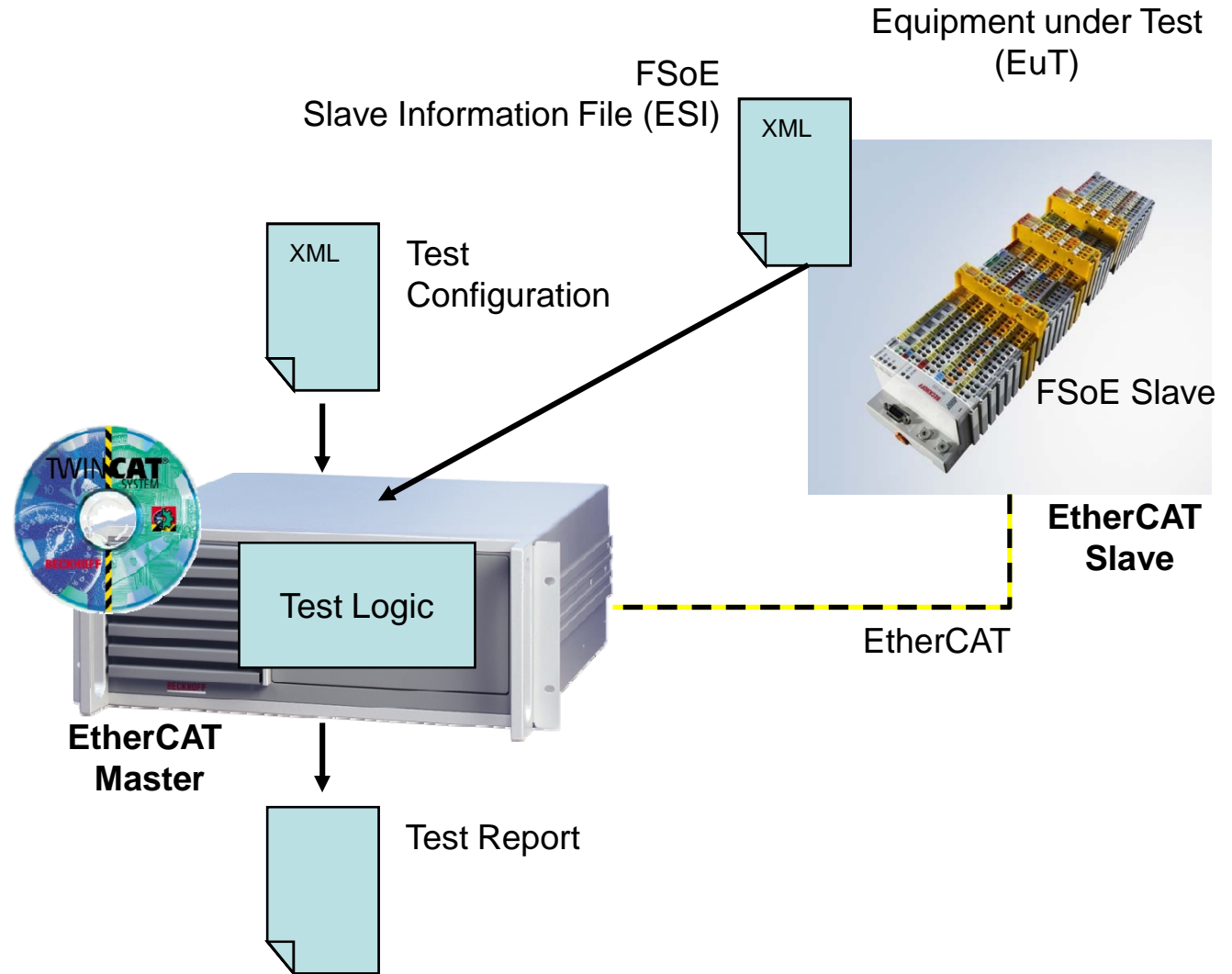
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



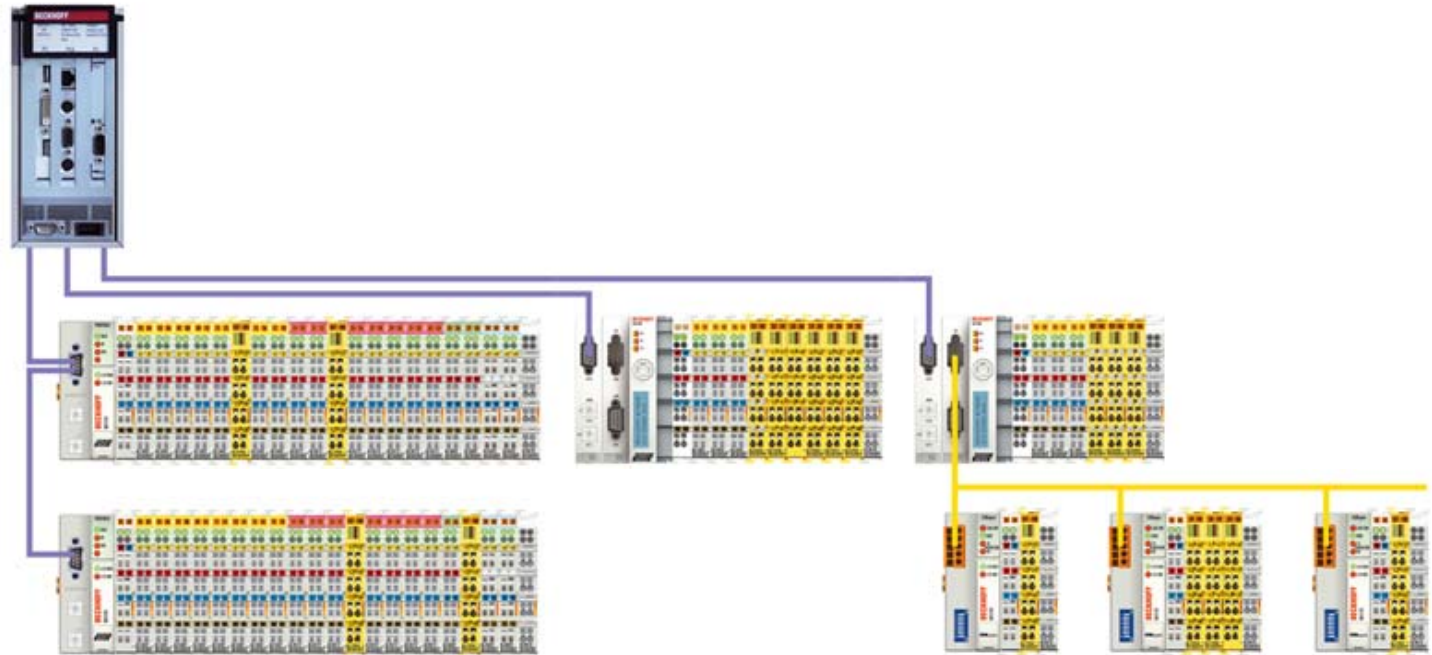
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- Mixed network for standard and safety functions
- Standard network with a decentralized safety island
- Separate networks for standard and safety functions

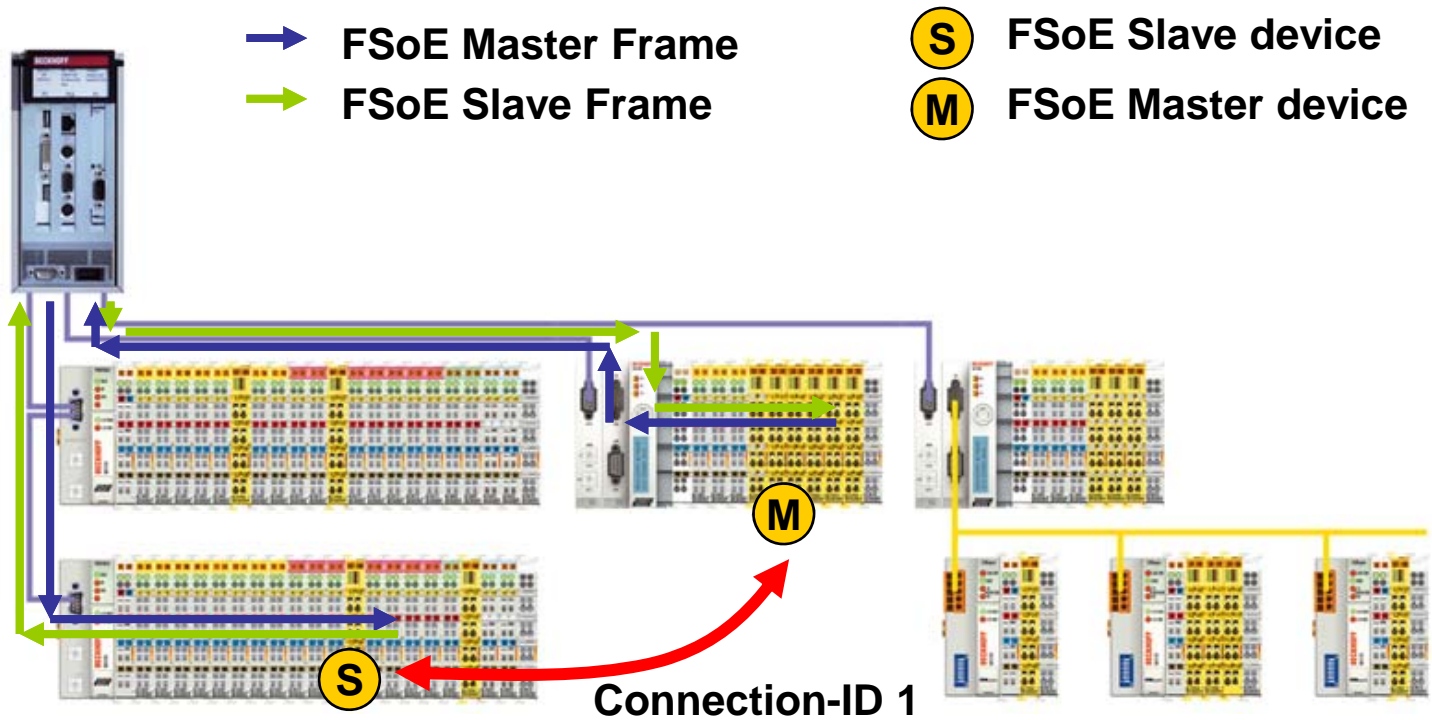
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- Configured Master-Slave Connections
- Communication routed via Standard-PLC

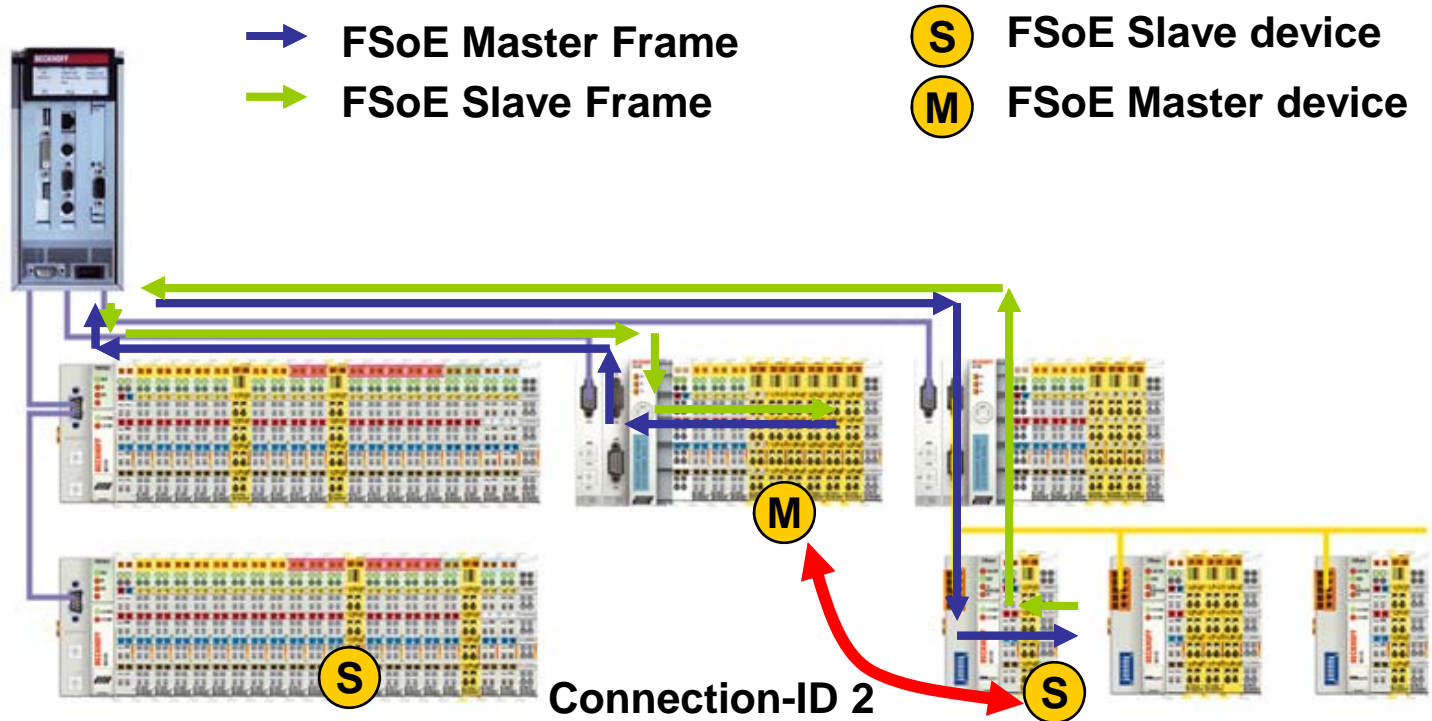
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- Configured Master-Slave Connections
- Communication routed via Standard-PLC

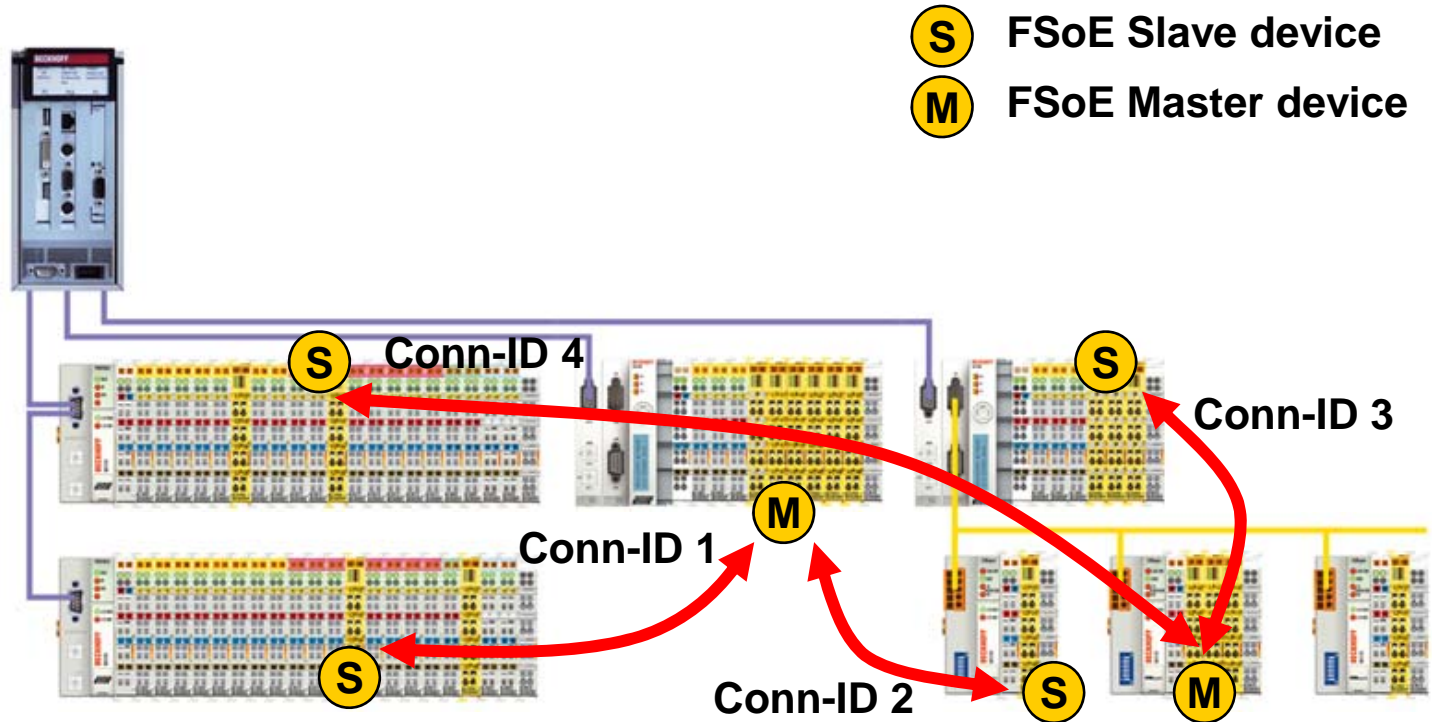
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- Multi Master networks
- Safety groups with group failsafe possible.

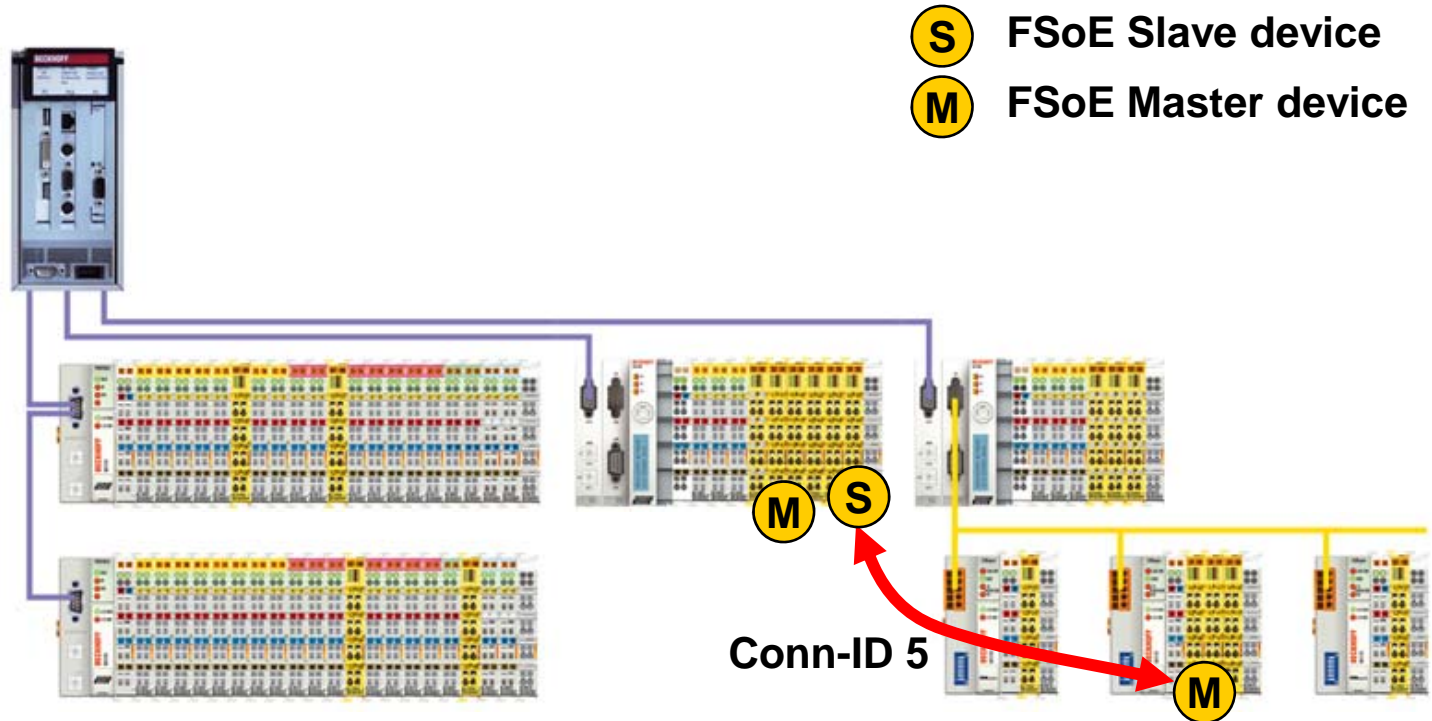
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



- "Master-Master" Communication possible with Master & Slave implementation in the Master device
- Unique Conn-ID
- Used for plant concatenation

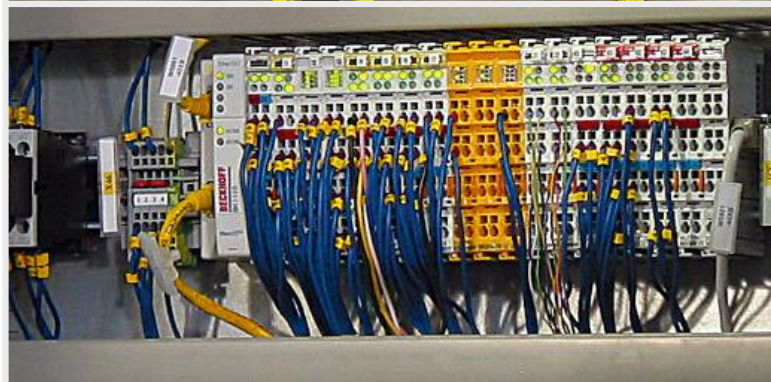
Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications



Requirements

Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

- Advantages for the customer:
- 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

Requirements

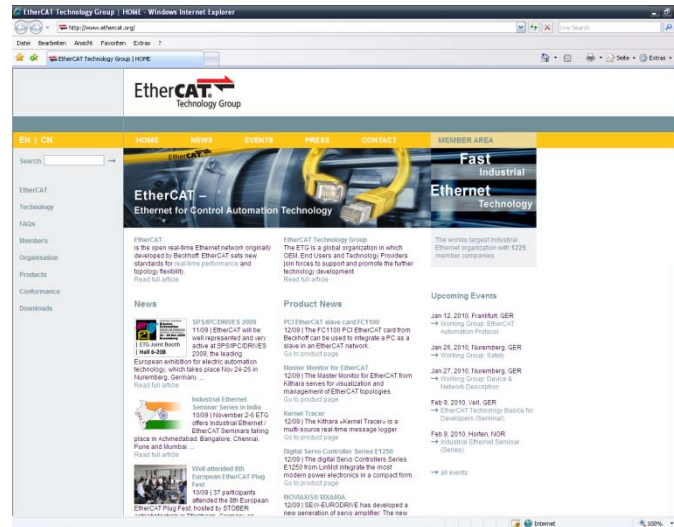
Safety over EtherCAT

- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

www.ethercat.org



EtherCAT Technology Group

Dr. Guido Beckmann

Ostendstr. 196

90482 Nuremberg, Germany

g.beckmann@ethercat.org