Übersicht der Technologie Safety over EtherCAT

EtherCAT Technology Group

Safety over EtherCAT

- Safety over EtherCAT Technologie
  - Architektur
  - Begriffe
  - State-Machine
  - Telegrammstruktur
  - Zusammenfassung
- Konformitäts-Test
- Anwendungsmöglichkeiten
  - Master-Master
  - Konfiguration
  - Diagnosemöglichkeiten

Funktionale Sicherheitstechnik

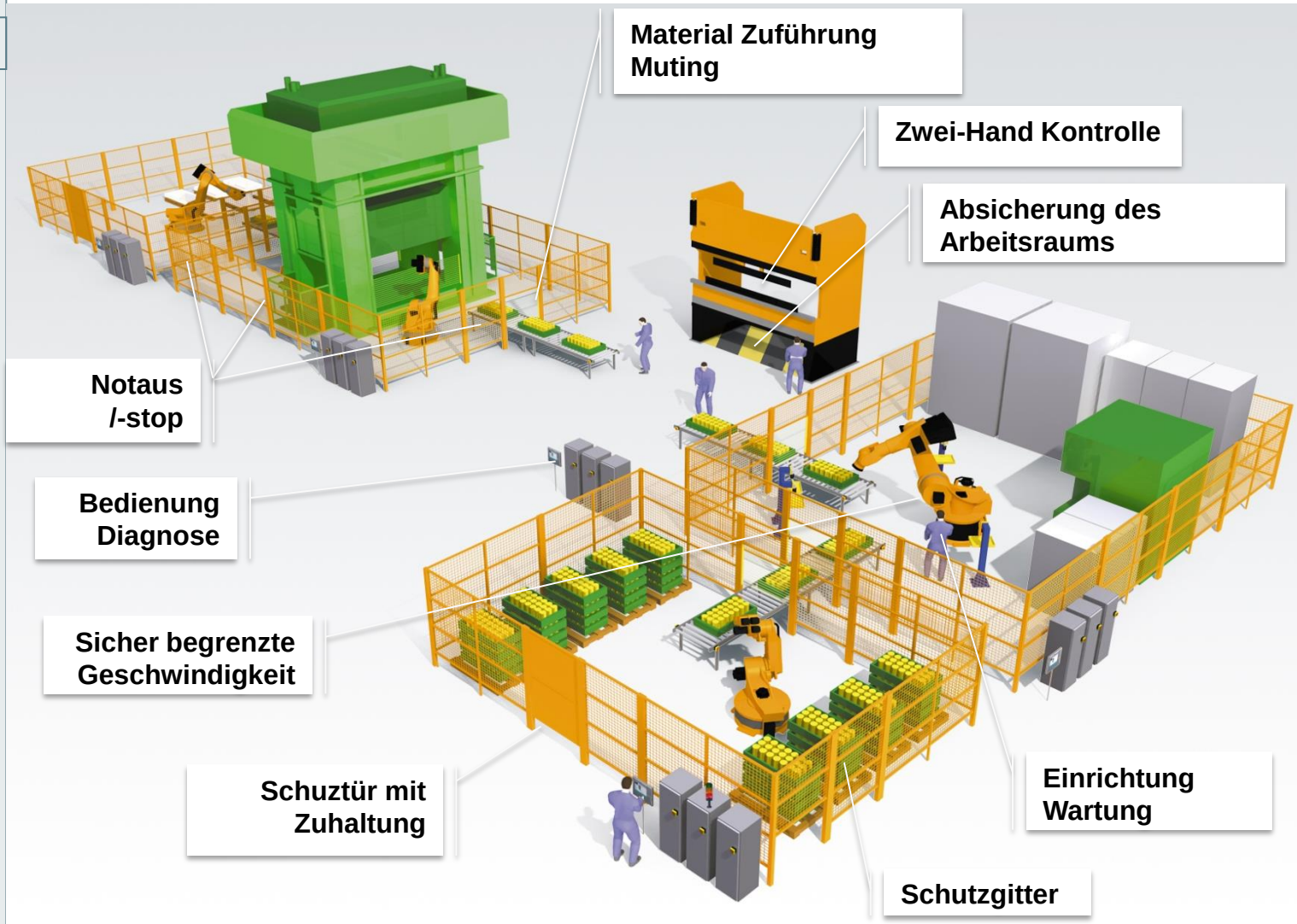
Anforderungen

Safety over EtherCAT

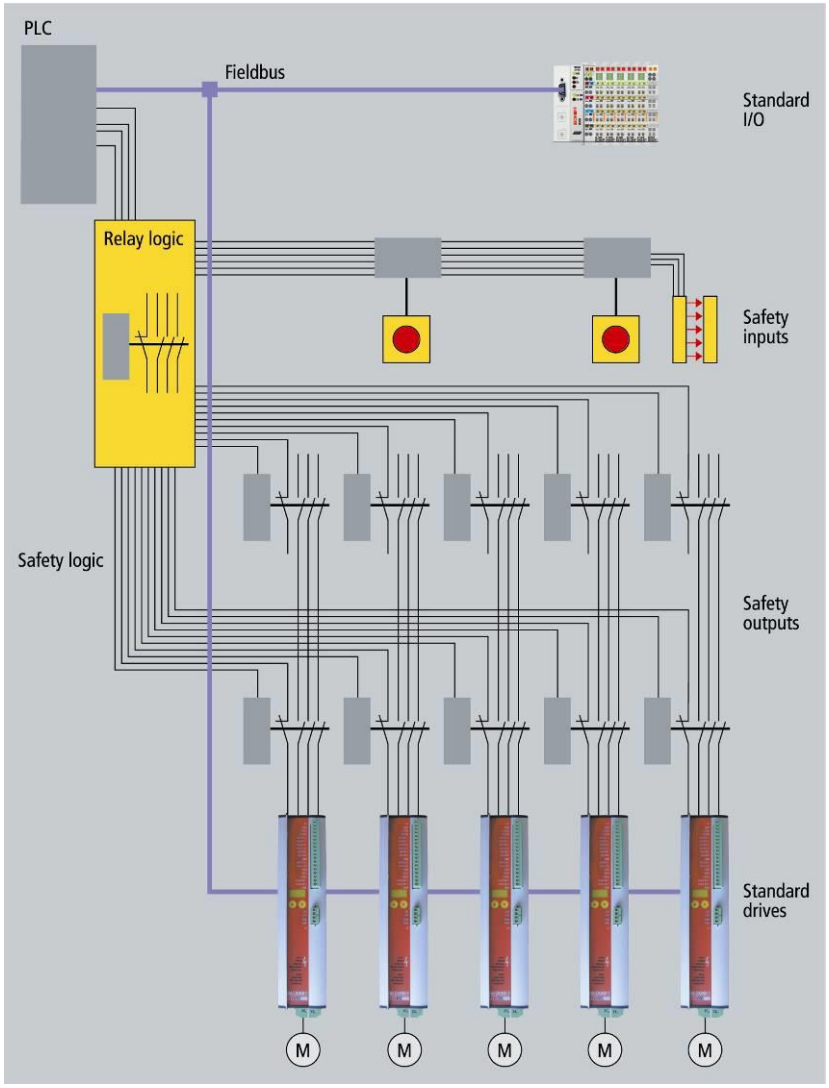
- Architektur
- Definitionen
- State-Machine
- Telegrammstruktur
- Zusammenfassung

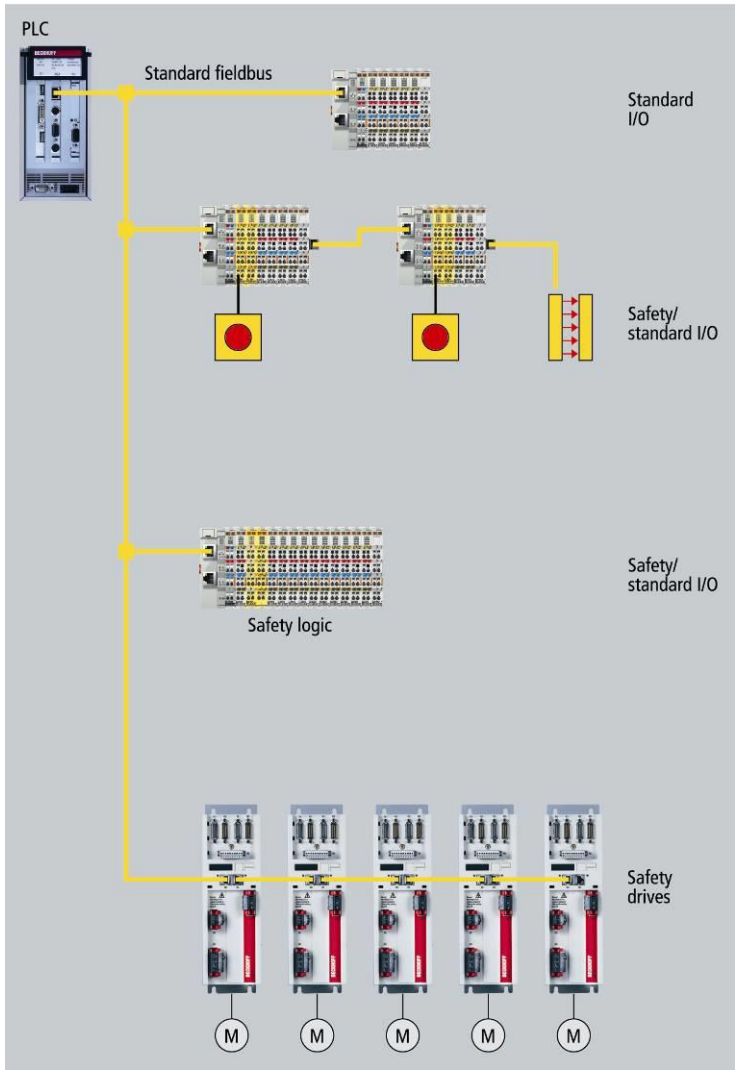
Konformität

Anwendungen



Moderne Sicherheitskonzepte





Vorteile sicherer Bussysteme

- Schnelle Reaktion
  - Anwendbar auch für hoch dynamische Antriebsapplikationen
- Vereinfachtes System
  - Bessere Übersichtlichkeit
  - Vereinfachte Verkabelung
  - Einfache Erweiterung des Systems
  - Bessere Diagnose
  - und damit: Höhere Sicherheit!
- Vorgetestete Sicherheitsfunktionen der Geräte entsprechend der geforderten Standards
- Niedrigere Kosten!

Normen zu Sicherheitsbussystemen

- BGIA Prüfgrundsatz GS-ET-26
  - Prüfgrundsatz des IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung) zur Bewertung von sicheren Bussystemen
  - Grundlage der 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 definition

IEC 61784-3

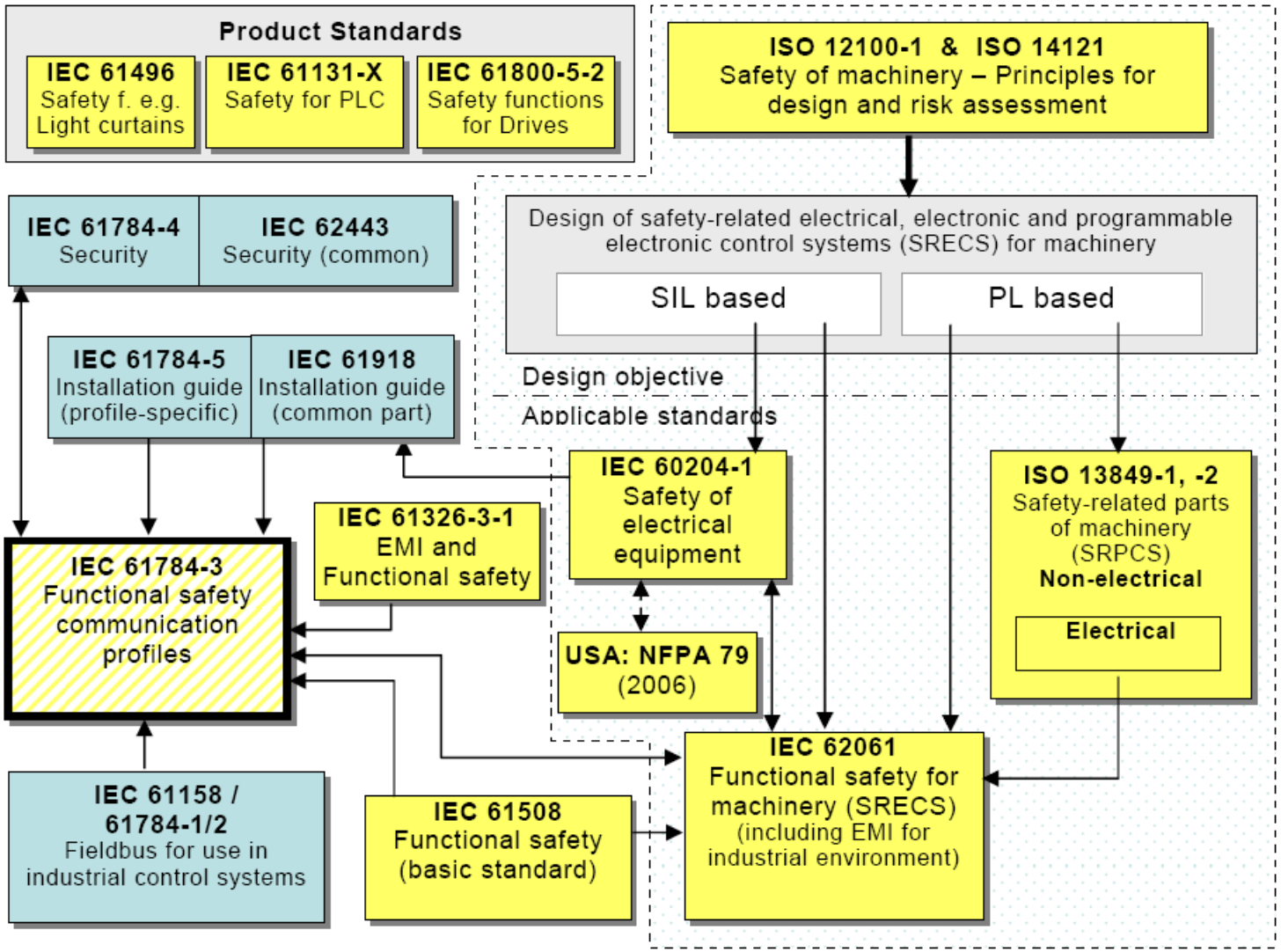
Anforderungen

Safety over EtherCAT

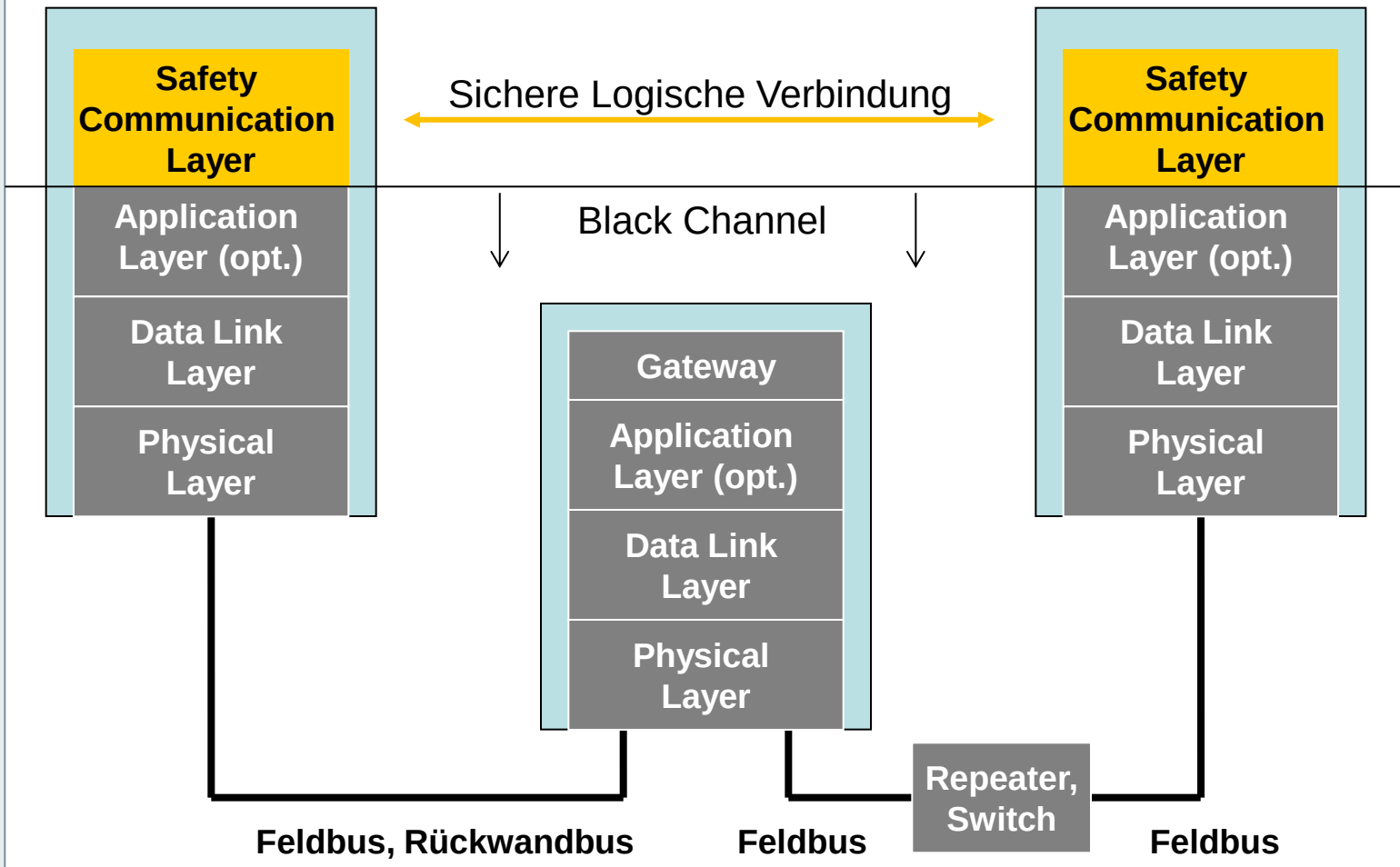
- Architektur
- Definitionen
- State-Machine
- Telegrammstruktur
- Zusammenfassung

Konformität

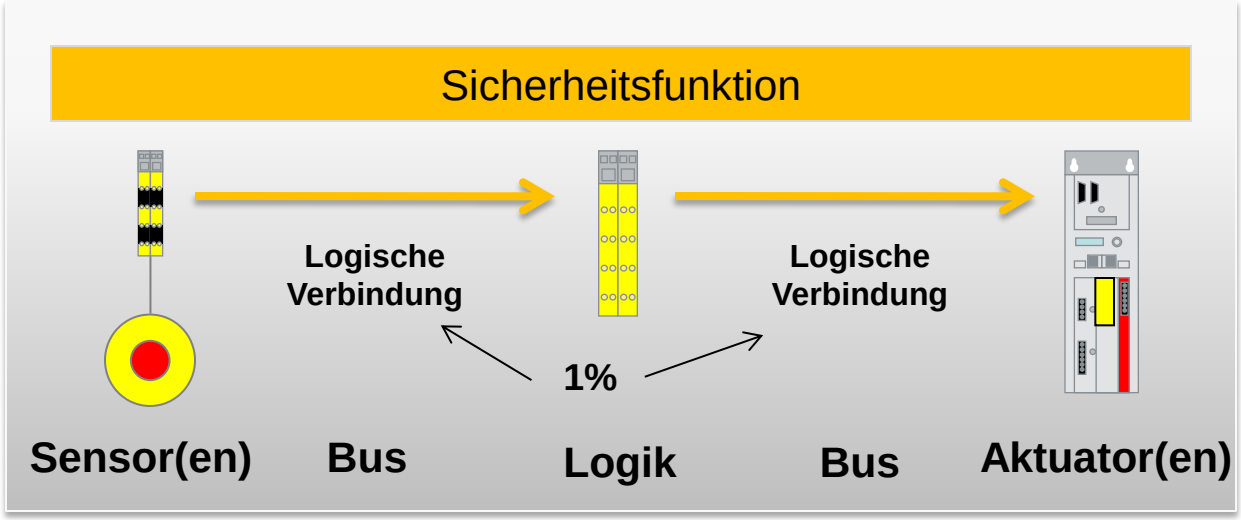
Anwendungen



IEC 61784-3 – Black Channel Ansatz



Verteilung der Restfehlerrate



- Restfehlerrate der Sicherheitsfunktion im gesamten System:
  - $PFH_{Safetyfunktion}$ $< 10^{-8}…10^{-7}$ /h bei SIL 3 (IEC 61508)

- In der IEC 61784-3 wird gefordert, dass auf den Kommunikationskanal nicht mehr als 1% der Restfehlerrate entfällt.
  Das entspricht einer zulässigen Restfehlerrate von:
  - PFH_{Bus} $< 10^{-9}$ /h für SIL 3

- Mehr als 100.000 Jahre Datentransport ohne unerkannten Fehler!

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

Safety over EtherCAT

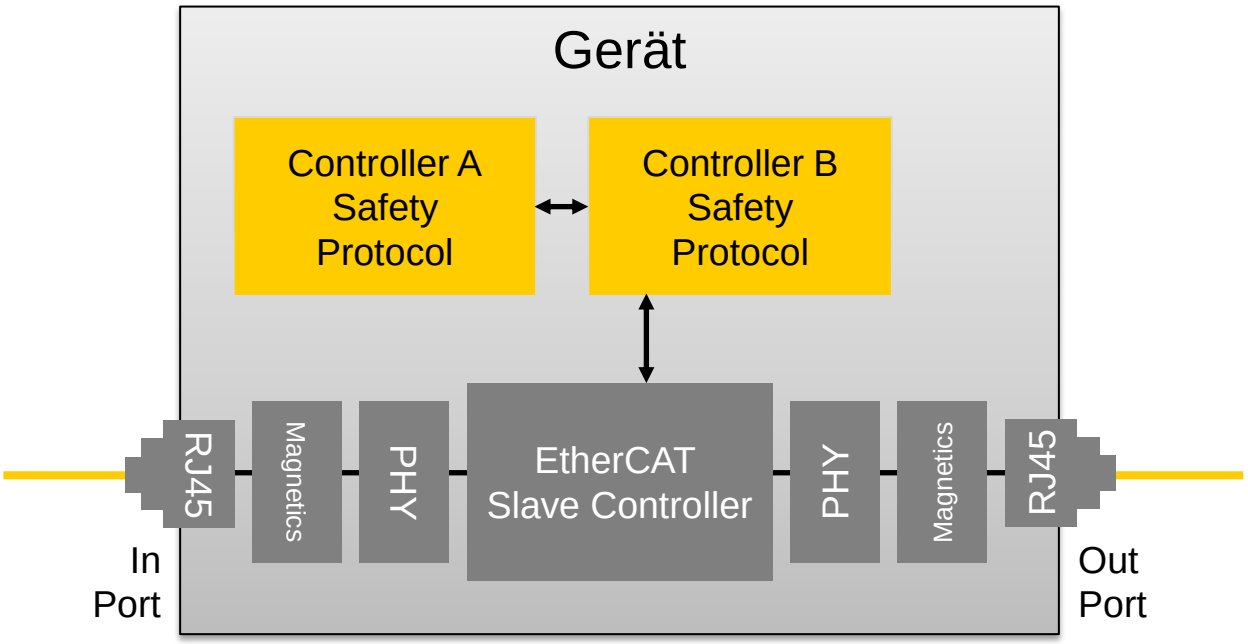
- **Safety over EtherCAT** (FSoE) bezeichnet einen sicheren Kommunikationslayer, mit dem sichere Prozessdaten zwischen Safety over EtherCAT Geräten übertragen werden können.

- FSoE ist eine offene Technologie
  - Support von der EtherCAT Technology Group (ETG)
  - Internationaler Standard innerhalb der IEC 61784-3

- Einhaltung des Safety-Integrity-Level SIL3 ist vom TÜV Süd Rail GmbH bestätigt

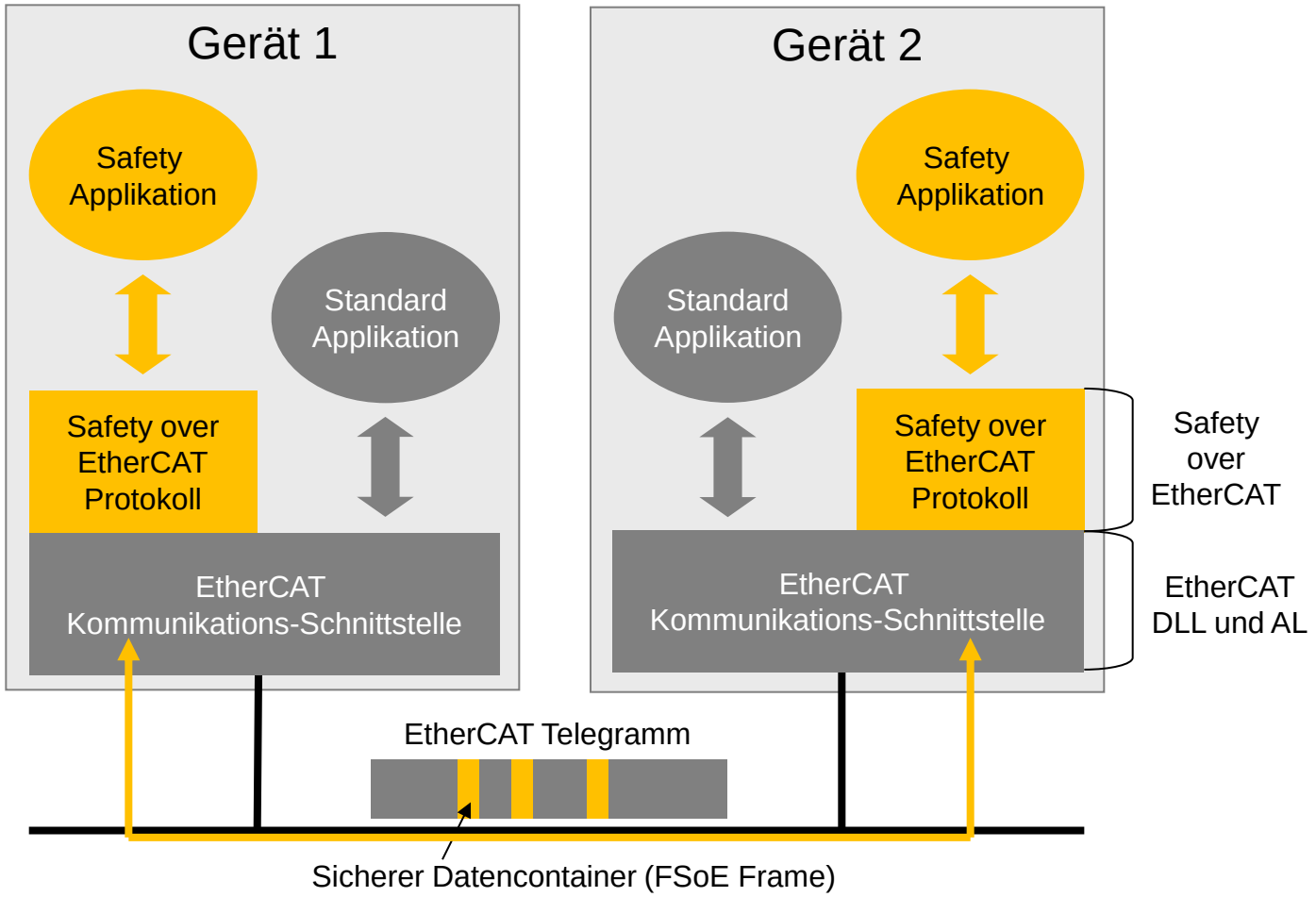
Safety over EtherCAT | Hardware Architektur

- Einkanaliges Standard-Kommunikations-System
- Redundante Hardware für die sicherheitsrelevante Applikation und das Sicherheitsprotokoll



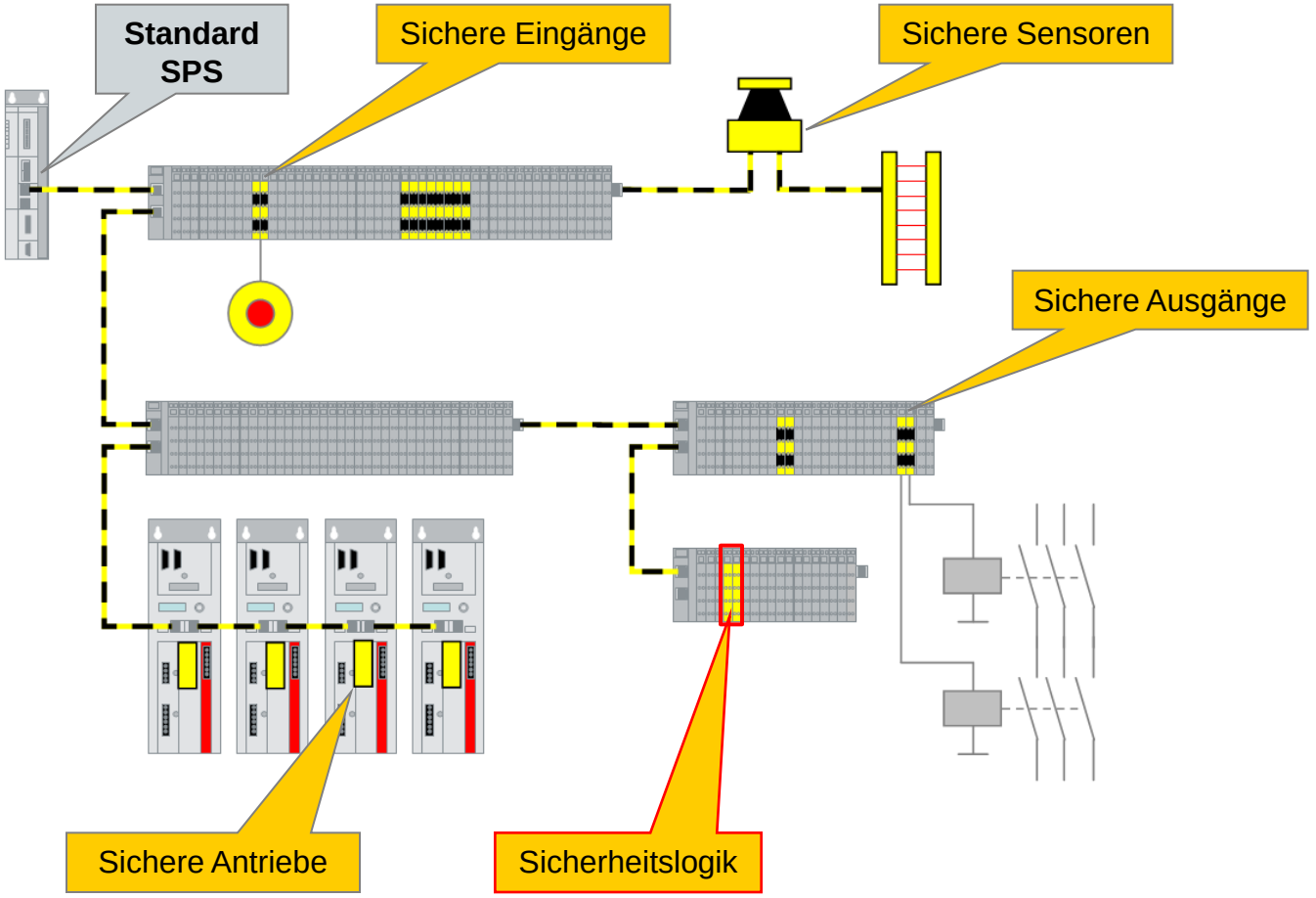
Safety over EtherCAT | Software Architektur

- EtherCAT wird als „schwarzer Kanal“ betrachtet, enthält sichere und Standard-Daten.

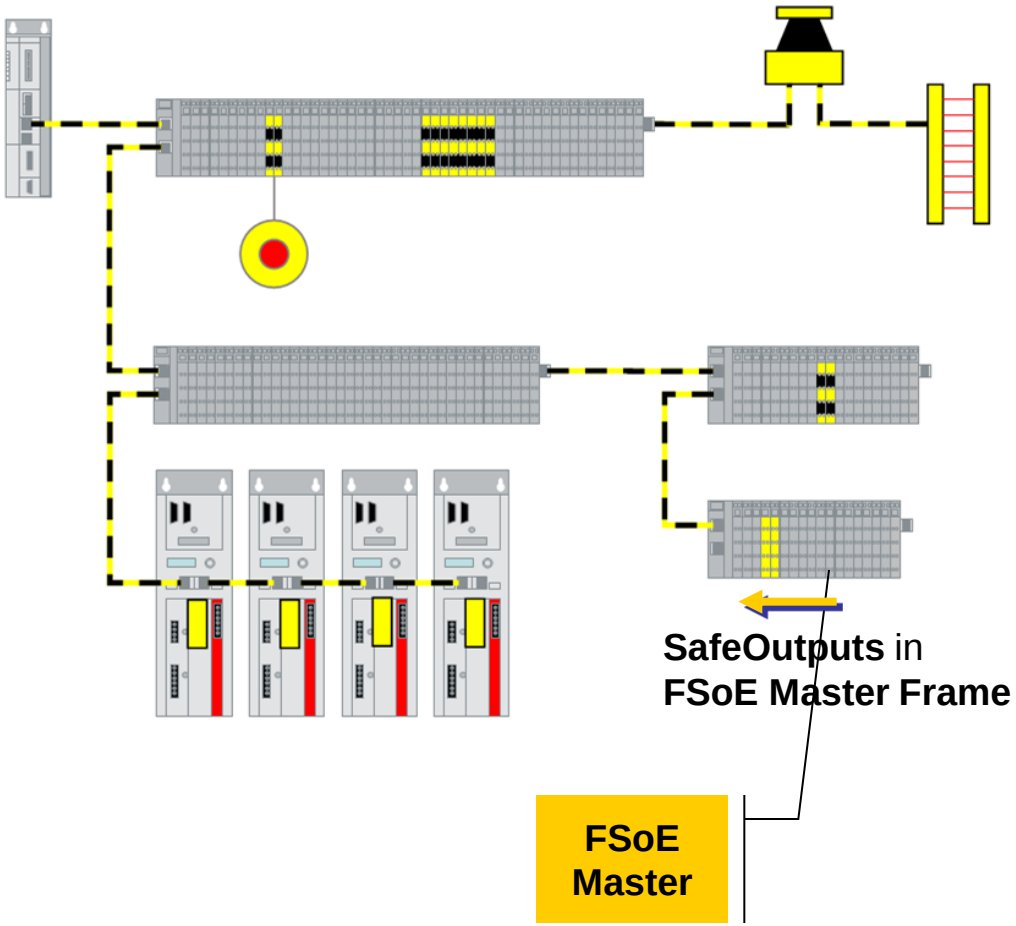


Safety over EtherCAT | Systembeispiel

- Dezentrale Sicherheits-Logik
- Standard SPS sorgt nur für Datenaustausch



FSoE | Master / Slave Verbindung



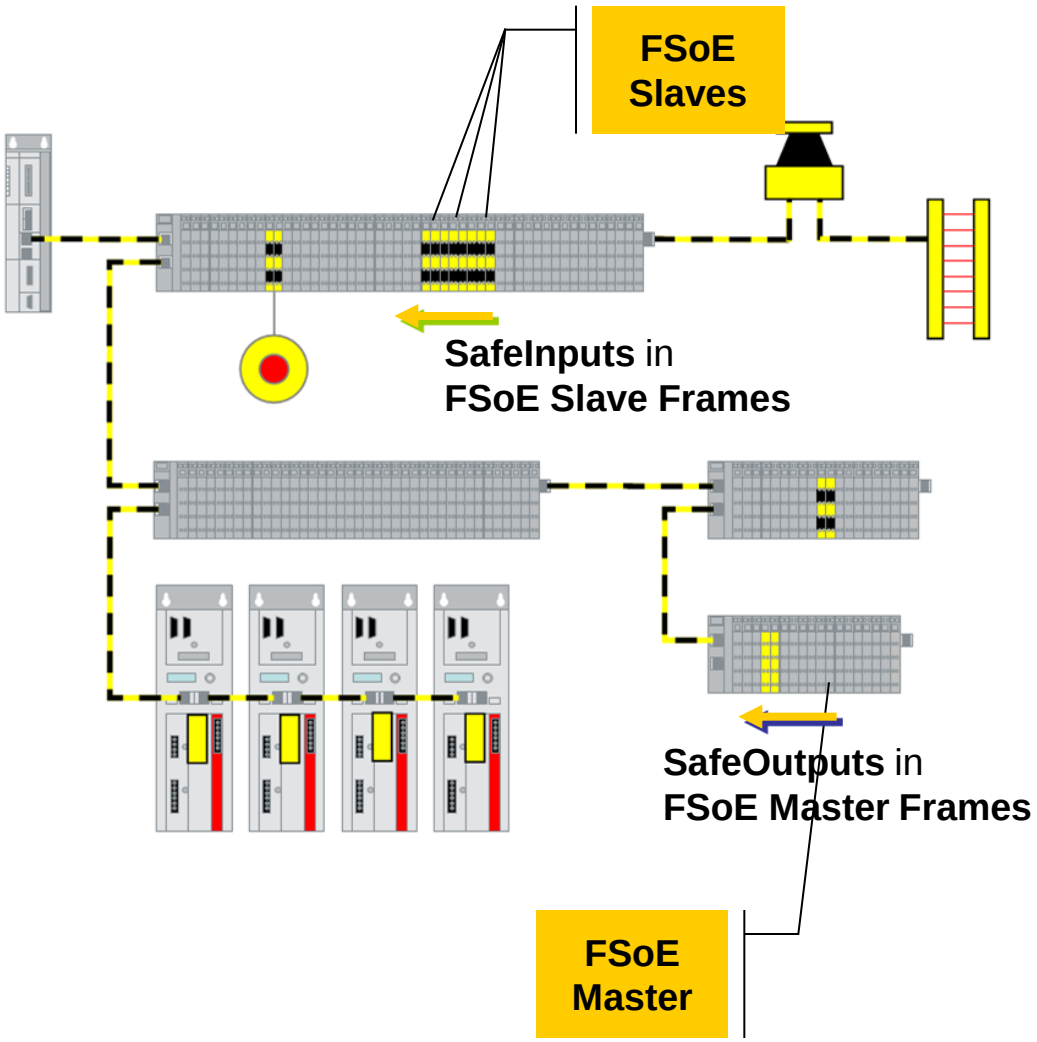
FSoE Master

Verbindungsmaster einer FSoE Connection. Der Master initiiert die Kommunikation.

Der FSoE Master sendet einen **FSoE Master Frame**, er enthält die **SafeOutputs**.

Ein FSoE Master kann einen oder mehrere FSoE Slaves verwalten.

FSoE | Master / Slave Verbindung



FSoE Slave

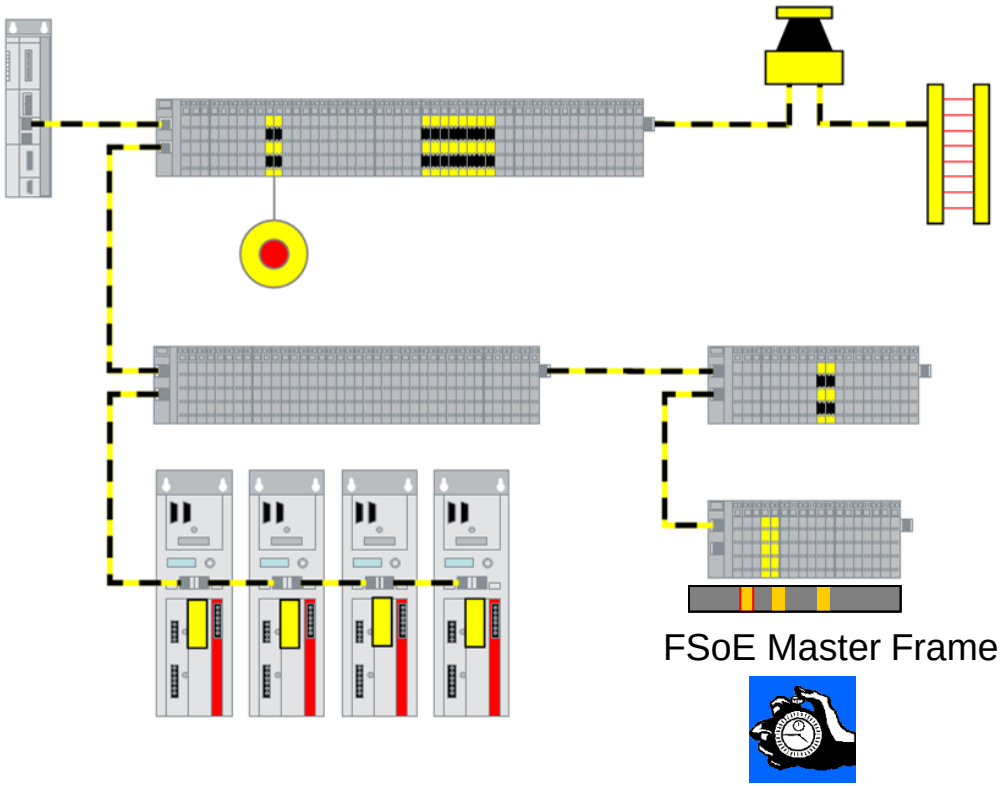
Verbindungsslave einer FSoE Connection.

Der FSoE Slave sendet einen **FSoE Slave Frame**, wenn er vom FSoE Master einen gültigen FSoE Master Frame erhalten hat.

Der FSoE Slave Frame enthält die **SafeInputs**.

Ein FSoE Slave ist genau einem FSoE Master zugeordnet.

FSoE | Kommunikationszyklus



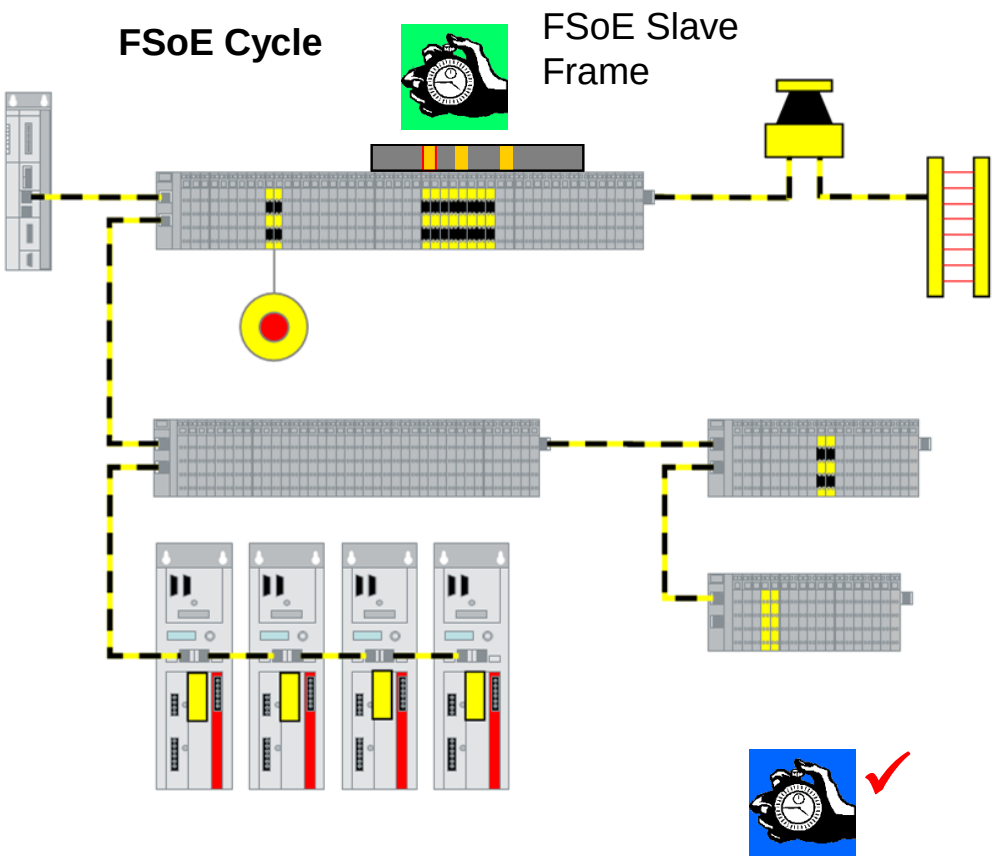
FSoE Cycle

Der FSoE Cycle besteht aus einem FSoE Master Frame, der von einem FSoE Slave Frame bestätigt wurde.

Der FSoE Master schickt einen FSoE Master Frame an den FSoE Slave.

Dabei startet er einen Watchdog-Timer zur Überwachung

FSoE | Communication Cycle



FSoE Cycle

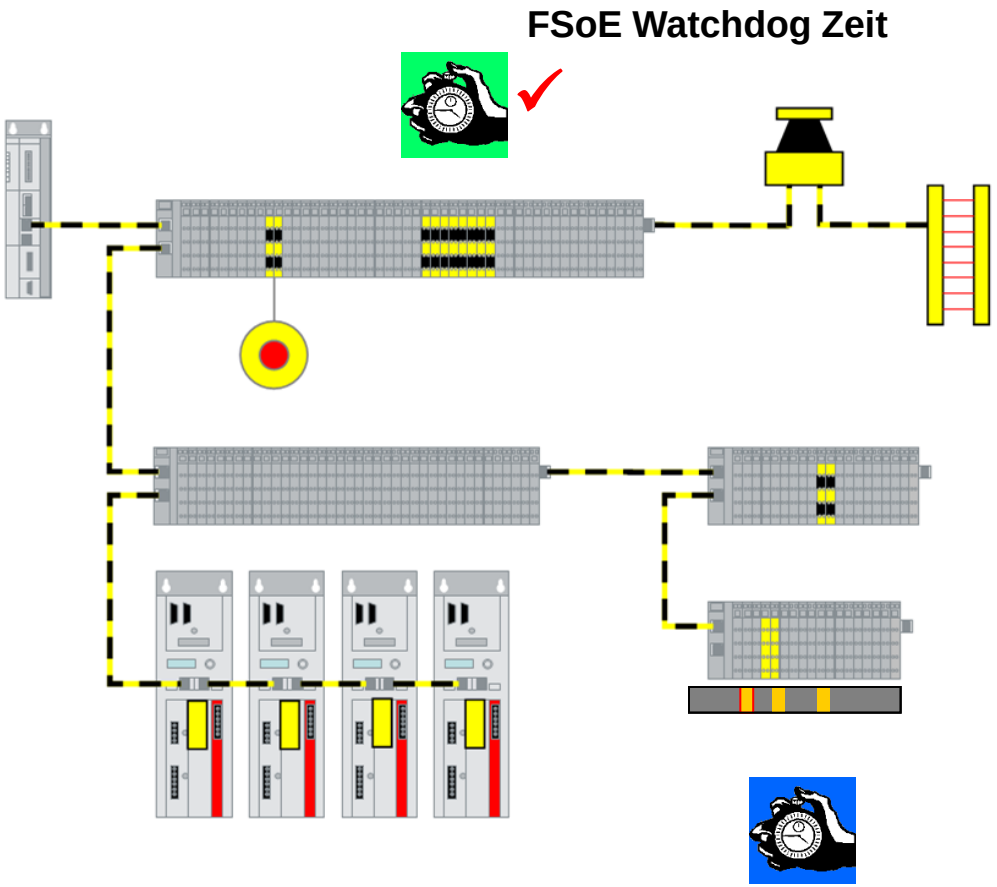
Der FSoE Cycle besteht aus einem FSoE Master Frame, der von einem FSoE Slave Frame bestätigt wurde.

Der FSoE Master schickt einen FSoE Master Frame an den FSoE Slave.

Dabei startet er einen Watchdog-Timer zur Überwachung

Erst nachdem er einen gültigen FSoE Slave Frame zurück bekommen hat, generiert er den nächsten FSoE Master Frame und startet damit einen neuen FSoE Cycle.

FSoE | Watchdog Zeit

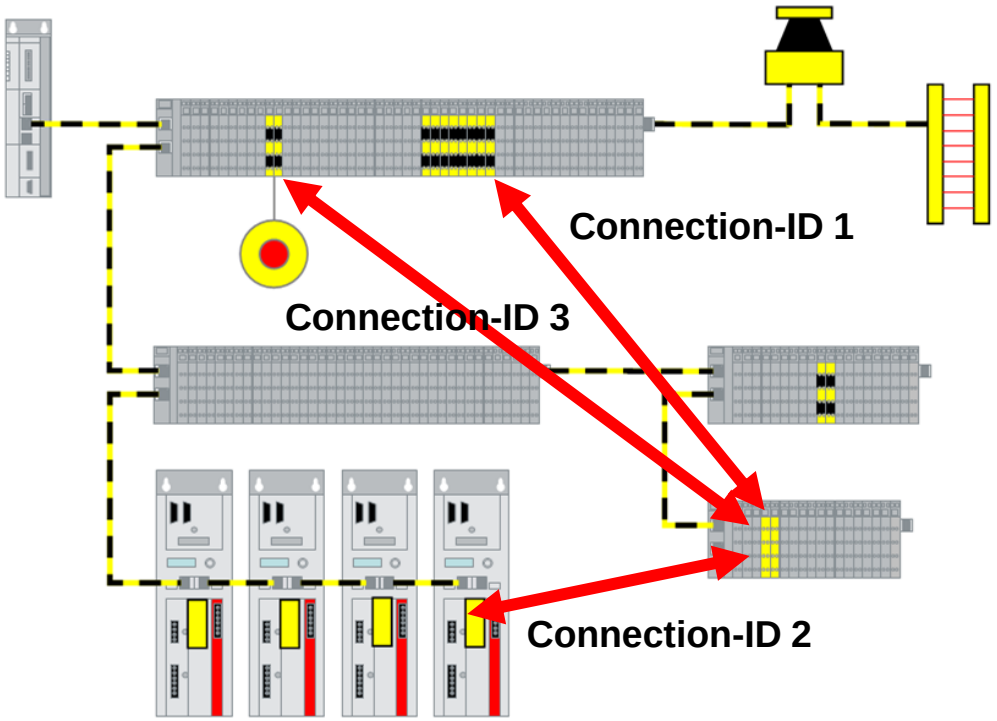


FSoE Watchdog Zeit

Jeder Teilnehmer überwacht, dass der Partner innerhalb der sicher parametrierten **FSoE Watchdogzeit** einen neuen FSoE Frame verschickt.

Läuft der Watchdog ab, dann wechselt der Teilnehmer in den Zustand Reset.

FSoE | Verbindungen



FSoE Connection

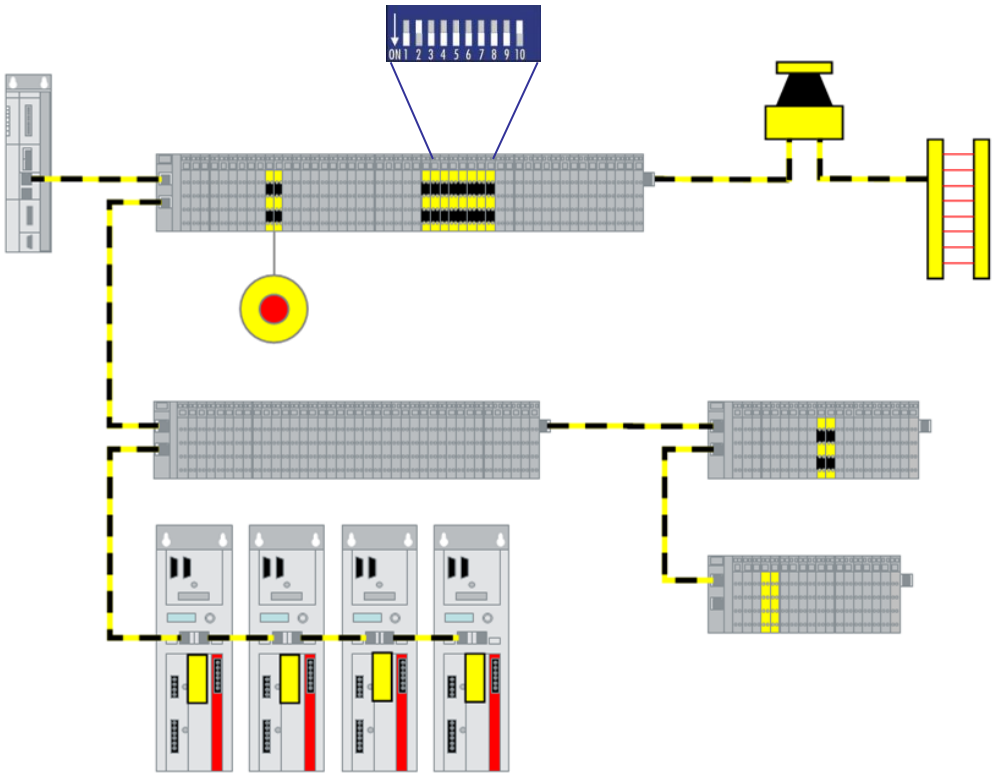
Bezeichnet eine logische Verbindung zwischen einem FSoE Master und einem FSoE Slave.

Es handelt sich um eine systemweit eindeutige **Connection-ID**.

Die Eindeutigkeit muss von einem sicheren Konfigurator oder Verifier überprüft werden.

FSoE | Eindeutige Adressierung

FSoE Slave Adresse



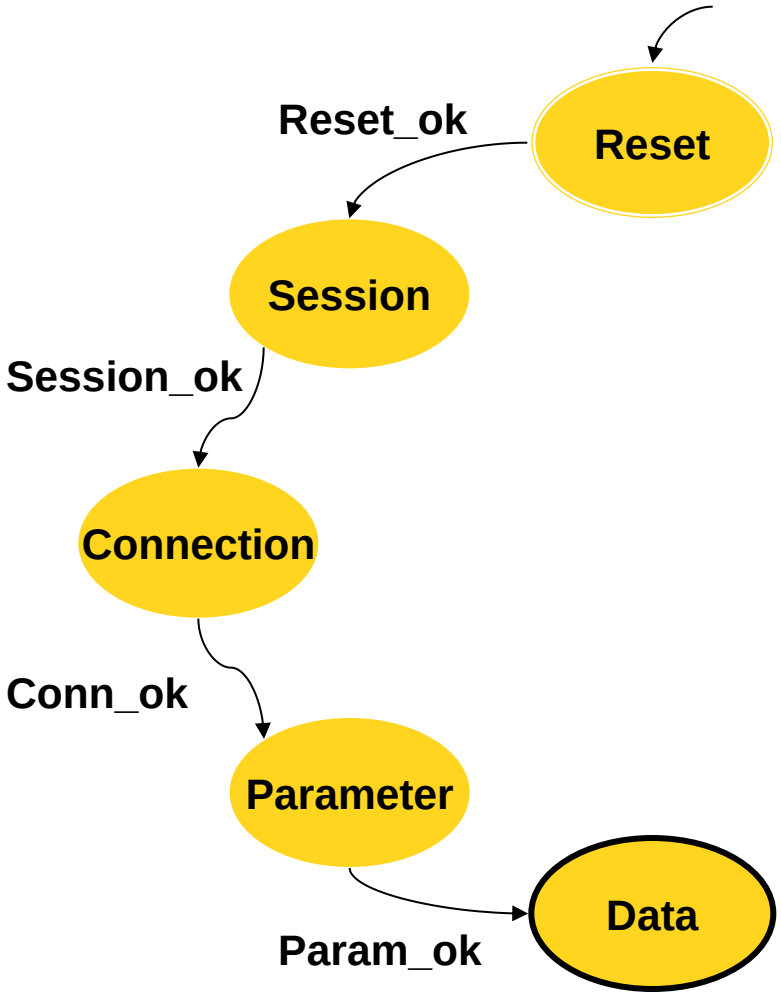
FSoE Slave Adresse

Neben der Connection-ID besitzt jeder FSoE Slave eine systemweit eindeutige 16-Bit FSoE Slave Adresse

Diese kann am Gerät eingestellt werden. Beispielsweise durch einen DIP-Schalter

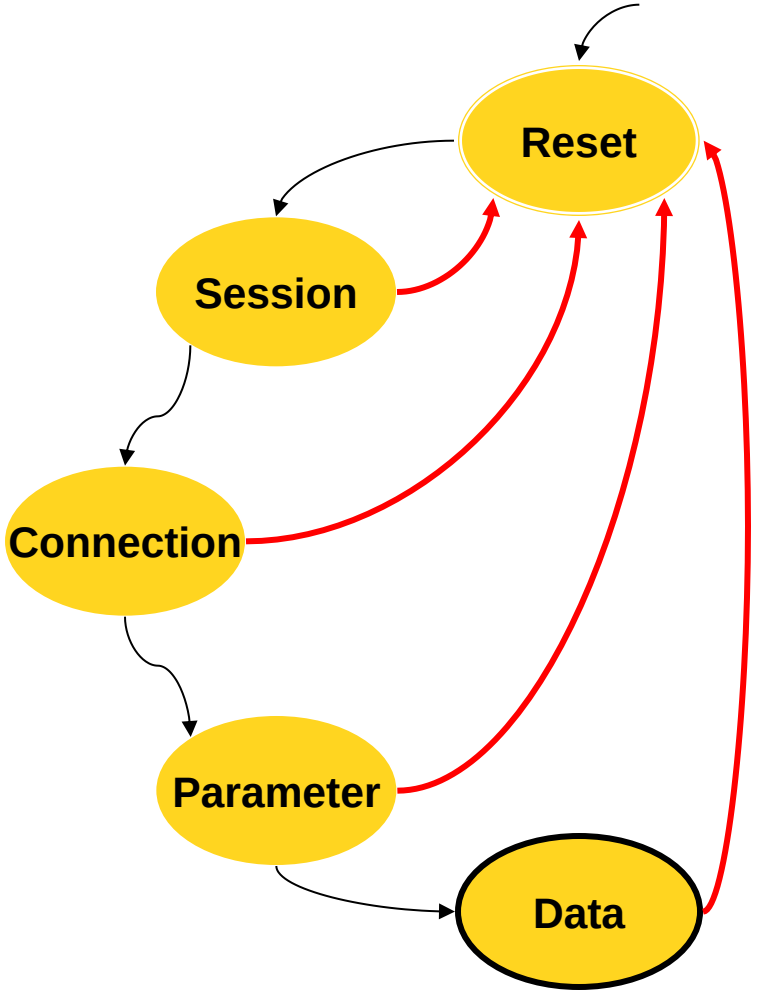
Es können 65.535 Teilnehmer in einem System unterschieden werden.

FSoE Zustandsmaschine je Connection



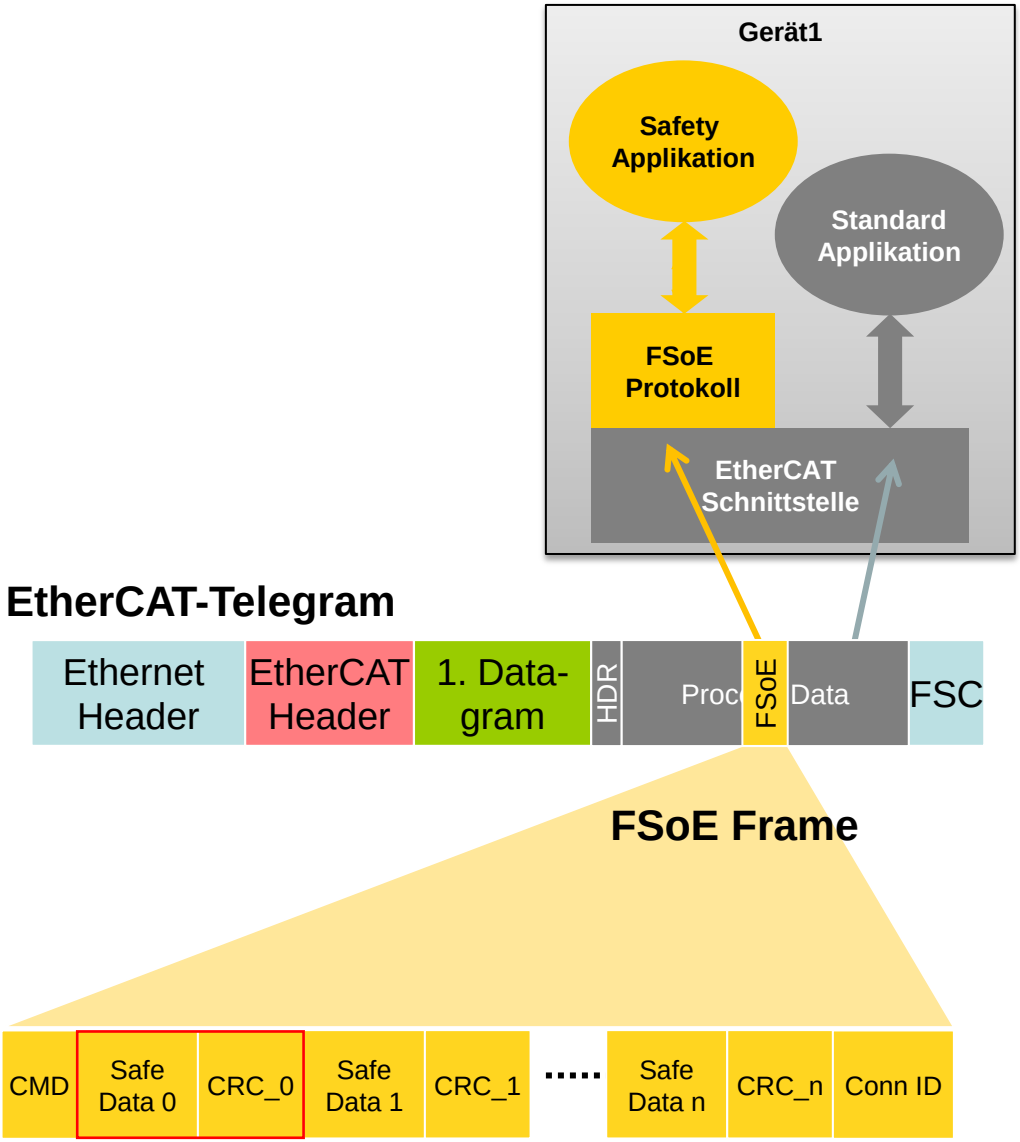
- Für jede FSoE Connection existiert eine FSoE Zustandsmaschine im Master und im Slave.
- Der FSoE Master verwaltet eine Zustandsmaschine pro FSoE Slave.
- Nach einem Power-On befinden sich FSoE Master und FSoE Slave im Zustand Reset.
- Nur im Zustand Data kann der sichere Zustand der Ausgänge verlassen werden.

FSoE Zustandsmaschine | Fehler



- Im Fehlerfall erfolgt ein Wechsel in den Reset-Zustand
- Master:
  Bei einem intern erkannten Fehler des Masters (Kommunikationsfehler oder Applikationsfehler)
- Slave:
  Bei einem intern erkannten Fehler des Slave
  oder
  bei einem Reset-Tgm. vom Master

Safety over EtherCAT | Telegrammstruktur



FSoE Frame

Der FSoE Frame wird als Container in die Prozessdaten des Teilnehmers gemappt.

Jeder Teilnehmer erkennt einen neuen FSoE Frame, wenn sich mindestens ein Bit gegenüber dem letzten FSoE Frame geändert hat

Je 2 Byte SafeData wird eine 2 Byte CRC übertragen

Es können *n* sichere Datenbytes (**SafeData**) übertragen werden

Safety over EtherCAT | Fehlerbeherrschung

Maßnahmen / Fehler-annahmen	Sequenz Number	Watchdog	Connection ID	CRC Berechnung
Wiederholung	☑			☑
Verlust	☑	☑		☑
Einfügung	☑			☑
Falsche Reihenfolge	☑			☑
Datenverfälschung				☑
Verzögerung		☑		
Maskerade		☑		☑
Wiederkehrende Speicherfehler	☑			☑
Falsche Weiterleitung			☑	

Safety over EtherCAT | Eigenschaften

- Die FSoE Spezifikation enthält keine Einschränkungen bezüglich:
  - Kommunikationsmedium
  - Übertragungsrate
  - Länge der sicheren Prozessdaten

- Routing via unsichere Gateways, Feldbusse oder Backbones ist möglich, sogar funk-basiert.

Safety over EtherCAT | Eigenschaften

- Das Protokoll ist entwickelt nach IEC 61508
  - Restfehlerrate $R_{(p)} < 10^{-9}/h$
  - Geeignet für den Einsatz in Geräten bis SIL 3
  - Keine Einschränkungen bzgl. des unterlagerten Kommunikationsprotokolls
- Die Protokoll Spezifikation durch den TÜV SÜD Rail GmbH geprüft und bestätigt.
- Vollständig zertifizierte Produkte mit Safety over EtherCAT Technologie sind seit 2005 verfügbar
- Das Protokoll ist in der IEC 61784-3 „Functional safety fieldbuses“ international standardisiert

Safety over EtherCAT | Eigenschaften

- FSoE Frame wird bei EtherCAT in den zyklischen PDOs eingebettet.
  - Minimale FSoE Frame-Länge: 6 Byte
  - Maximale FSoE Frame-Länge: Abhängig von der Anzahl der sicheren Nutzdaten des Slave-Gerätes
  - Das Protokoll ist damit geeignet für sichere I/O als auch für sichere Antriebe
- Bestätigter Transfer vom FSoE Master zum FSoE Slave und umgekehrt.
- Sichere Geräteparameter werden im Hochlauf einer Master-Slave Connection übertragen.
  - Watchdog Zeit
  - Gerätespezifische sicherheitsrelevante Parameter für die Slave Applikation

Safety over EtherCAT | offene Technologie

- FSoE ist offengelegt in der ETG.5100 und Teil der IEC 61784-3 Functional Safety fieldbuses
- Implementierungssupport über die ETG
  - Support bei der Planung, Implementierung und Zertifizierung
- FSoE Conformance Test
  - Test-Cases zum Nachweis der Konformität von FSoE Master und FSoE Slave Geräten sind verfügbar und durch den TÜV abgenommen
  - FSoE Conformance Test Tool für den automatischen Test von FSoE Slave Geräten ist ebenfalls vom TÜV abgenommen.
- Implementierungen von verschiedenen Geräteherstellern sind verfügbar

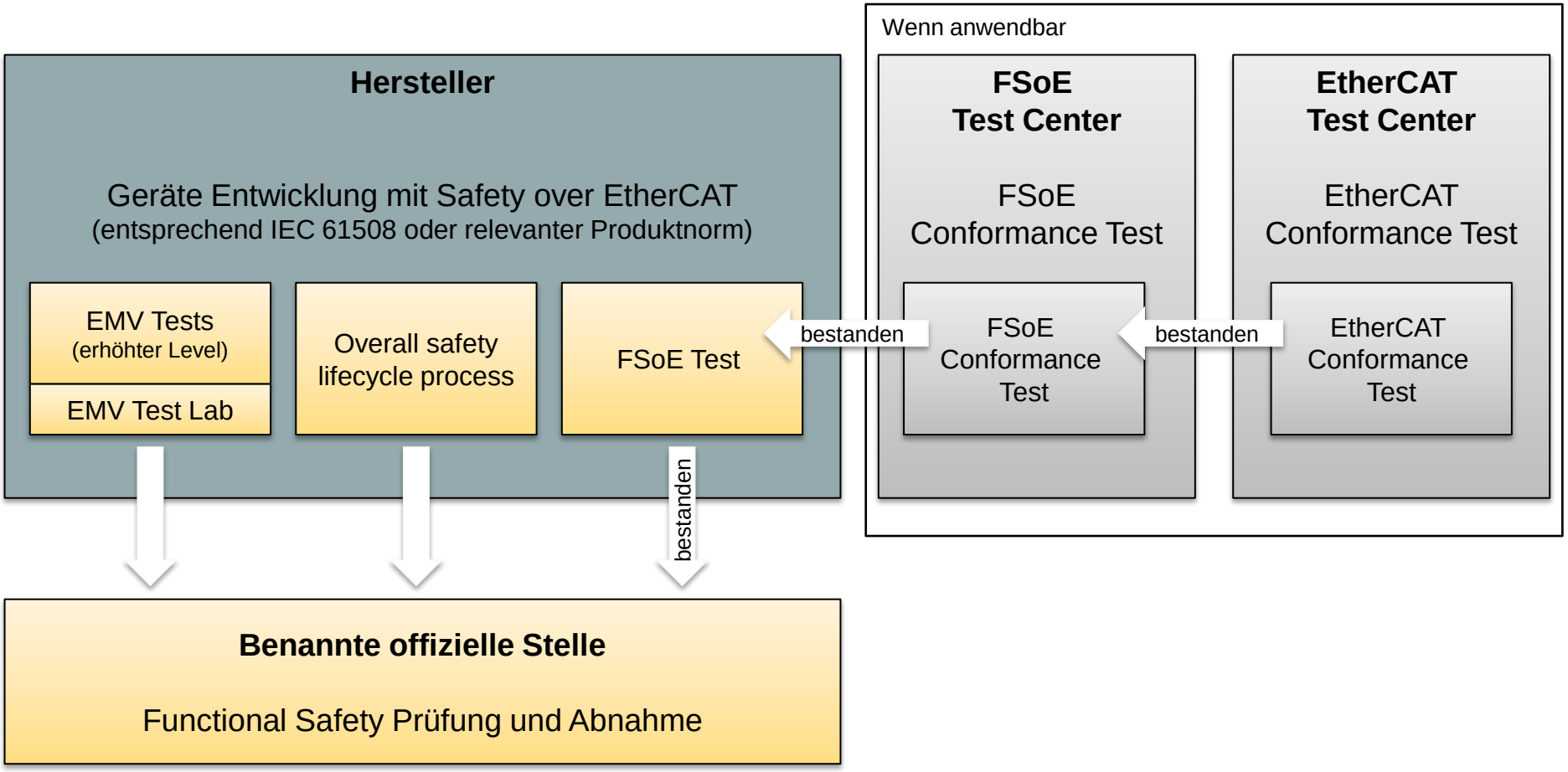
Safety over EtherCAT Hersteller

(Hersteller, die FSoE Geräte anbieten oder angekündigt haben. 03/2014. Nicht alle Produkte sind bereits verfügbar.)

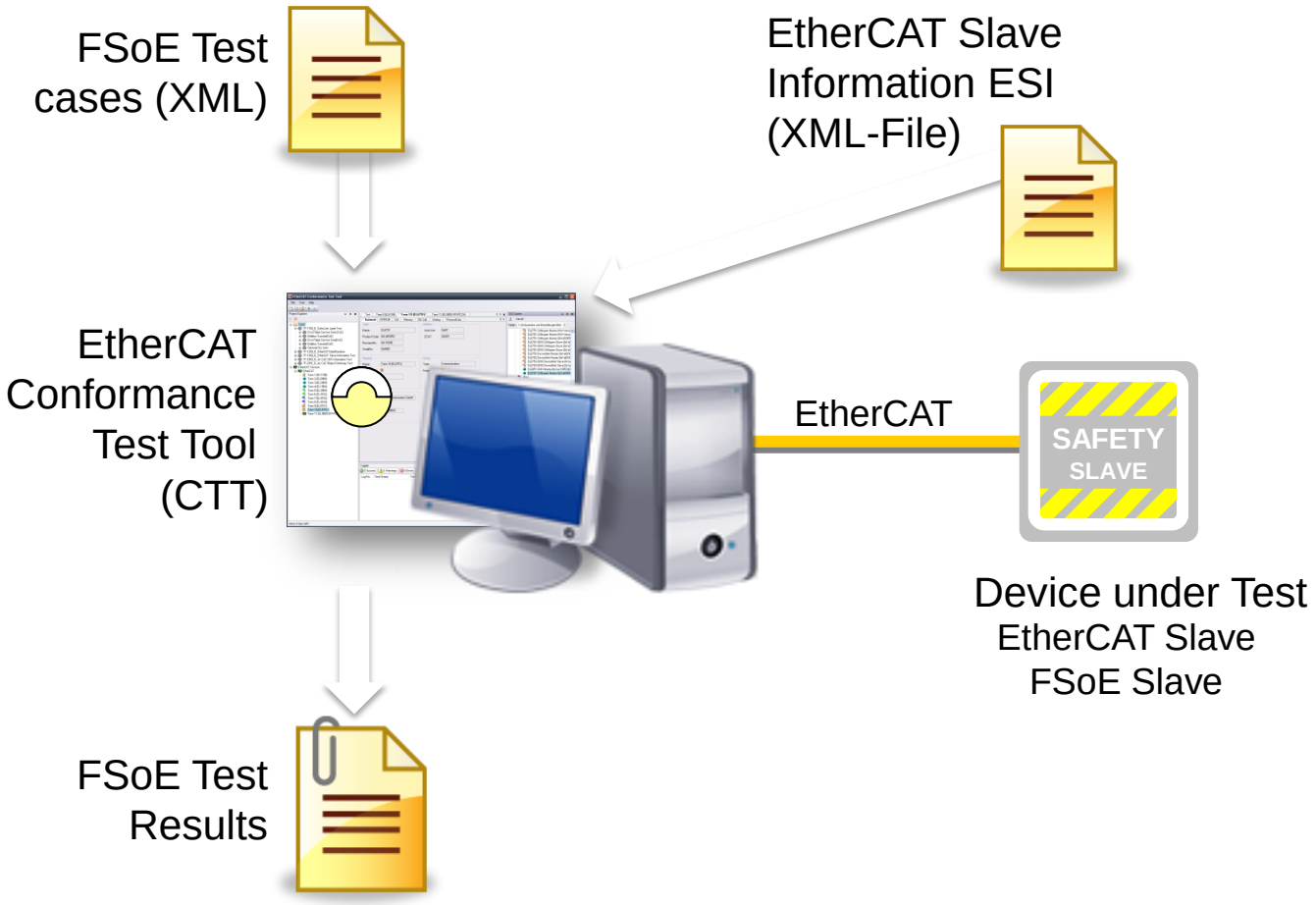
Safety over EtherCAT | Konformitäts-Test

- ETG.9001 Safety over EtherCAT Policy
  - Spezifiziert die FSoE Konformitätsregeln
- FSoE Geräte müssen die folgenden Eigenschaften einhalten:
  - Einhaltung der Standards
    - IEC 61508 und/oder relevanter Sektor / Produkt stanards
    - IEC 61784-3 Allgmeiner Teil
    - ETG.5100 Safety over EtherCAT Spezifikation
    - EtherCAT Conformance Test Policy (wenn anwendbar)
  - Functional Safety Abnahme des Gerätes durch eine Benannte Stelle (z.B. TÜV, IFA)

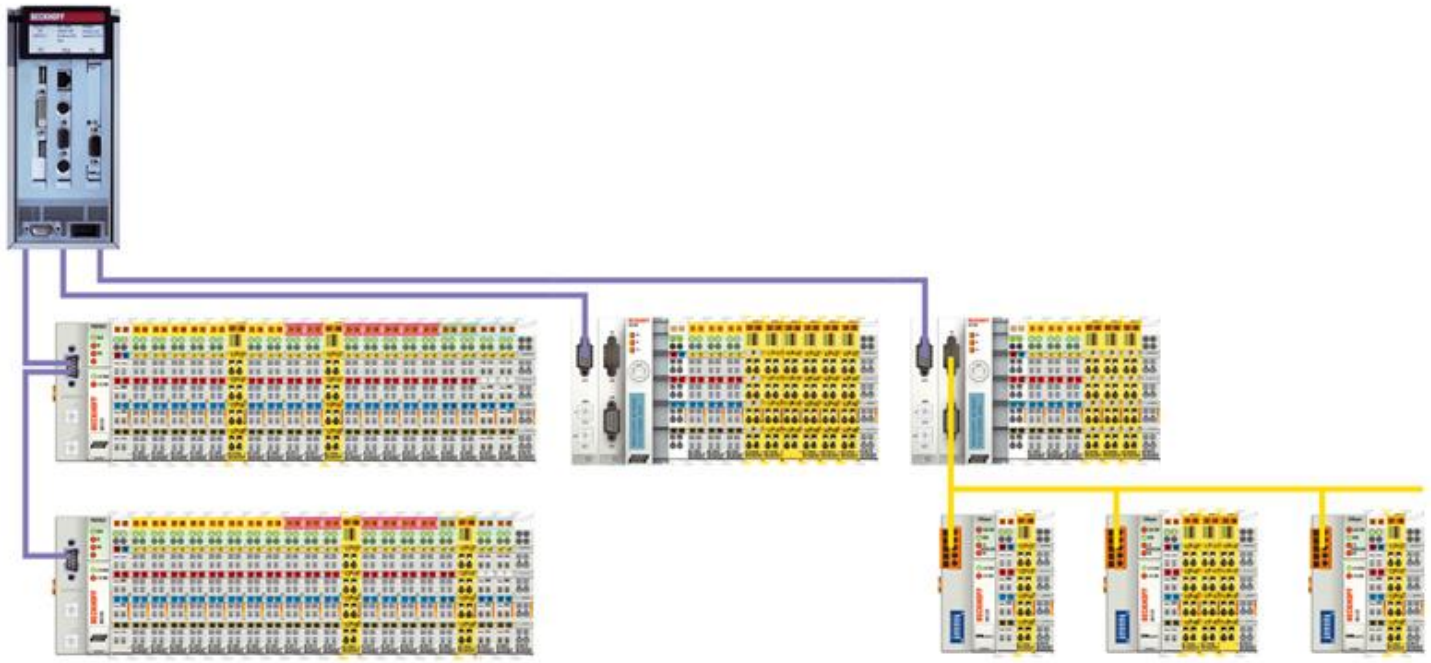
Geräte Prüfung und Abnahme



FSoE Conformance Test Tool | FSoE Slave

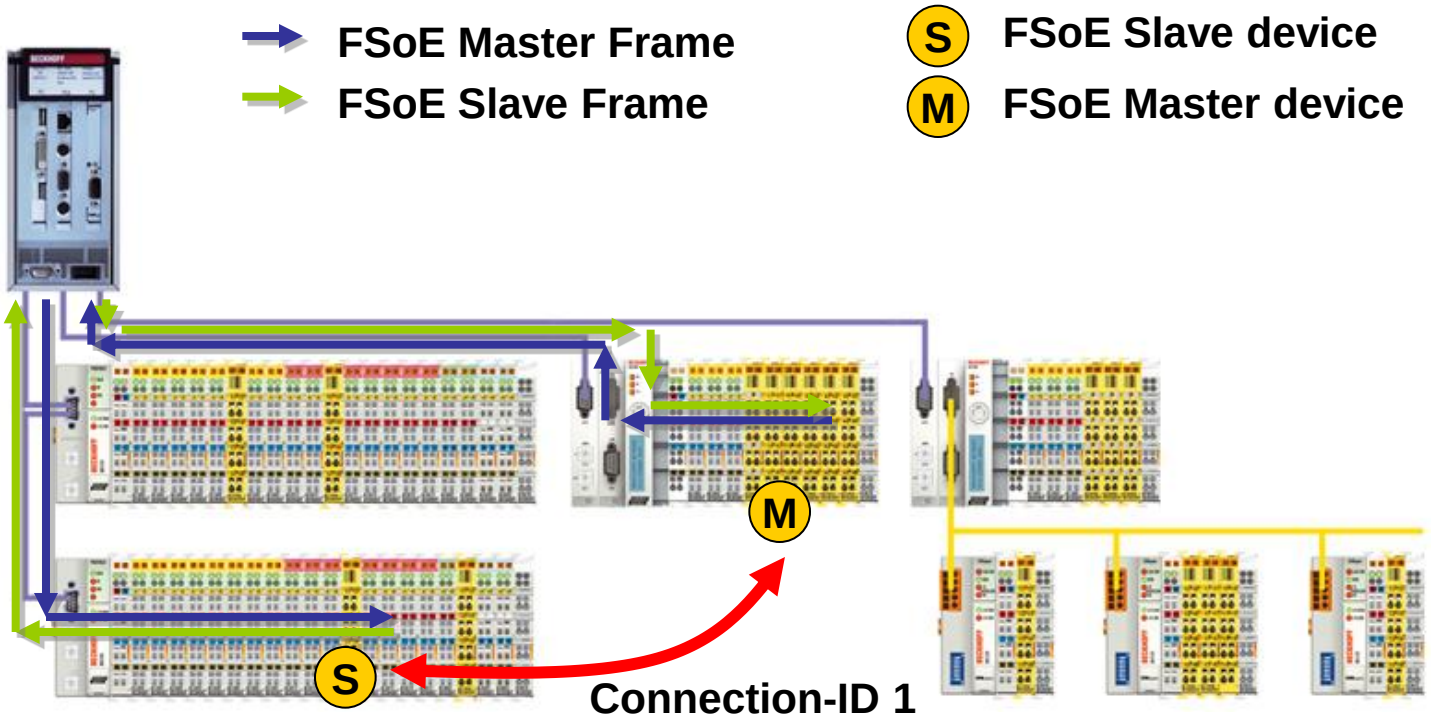


Sicherheitstechnik in der modernen Automation



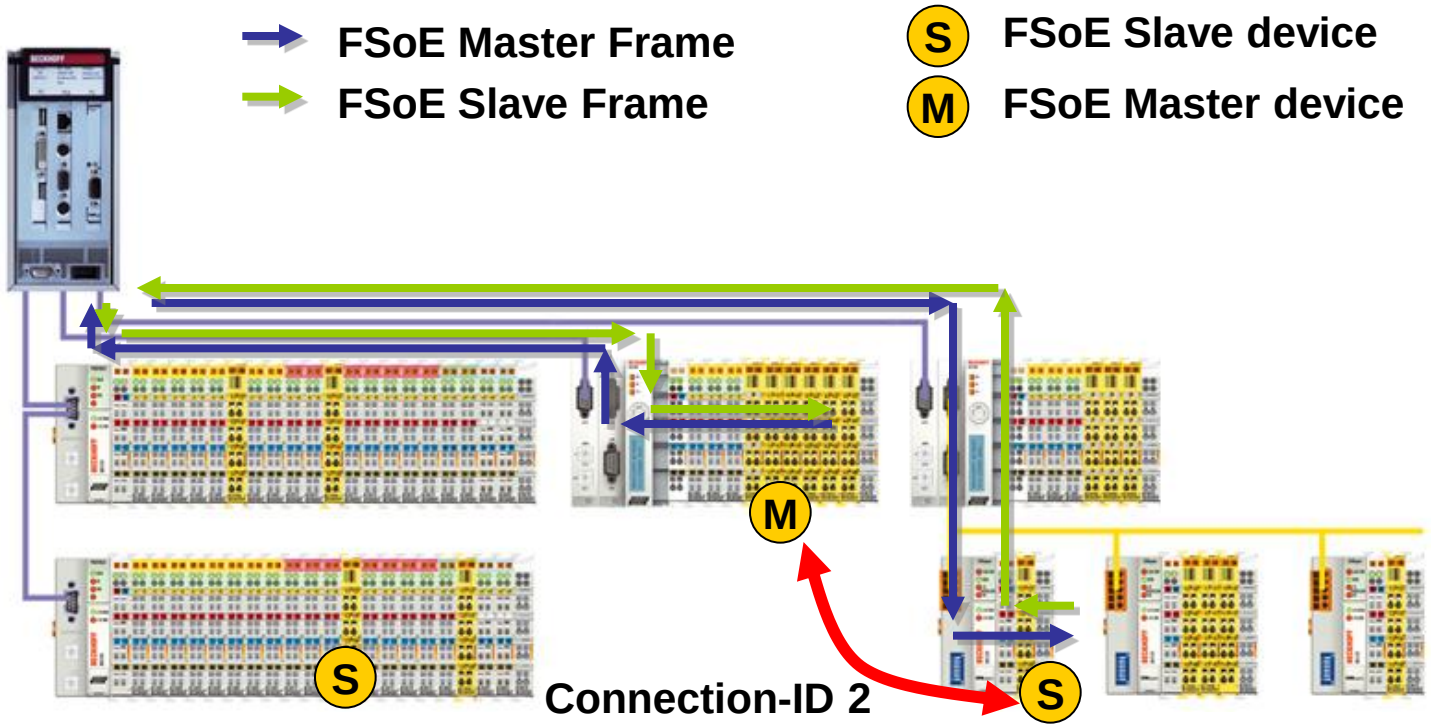
- Gemischtes Netzwerk für Standard- und Sicherheitsfunktionen
- Standard-Netzwerk mit einer dezentralen Sicherheitsinsel
- Separate Netzwerke für Standard- und Sicherheitsfunktionen

Sicherheitstechnik in der modernen Automation



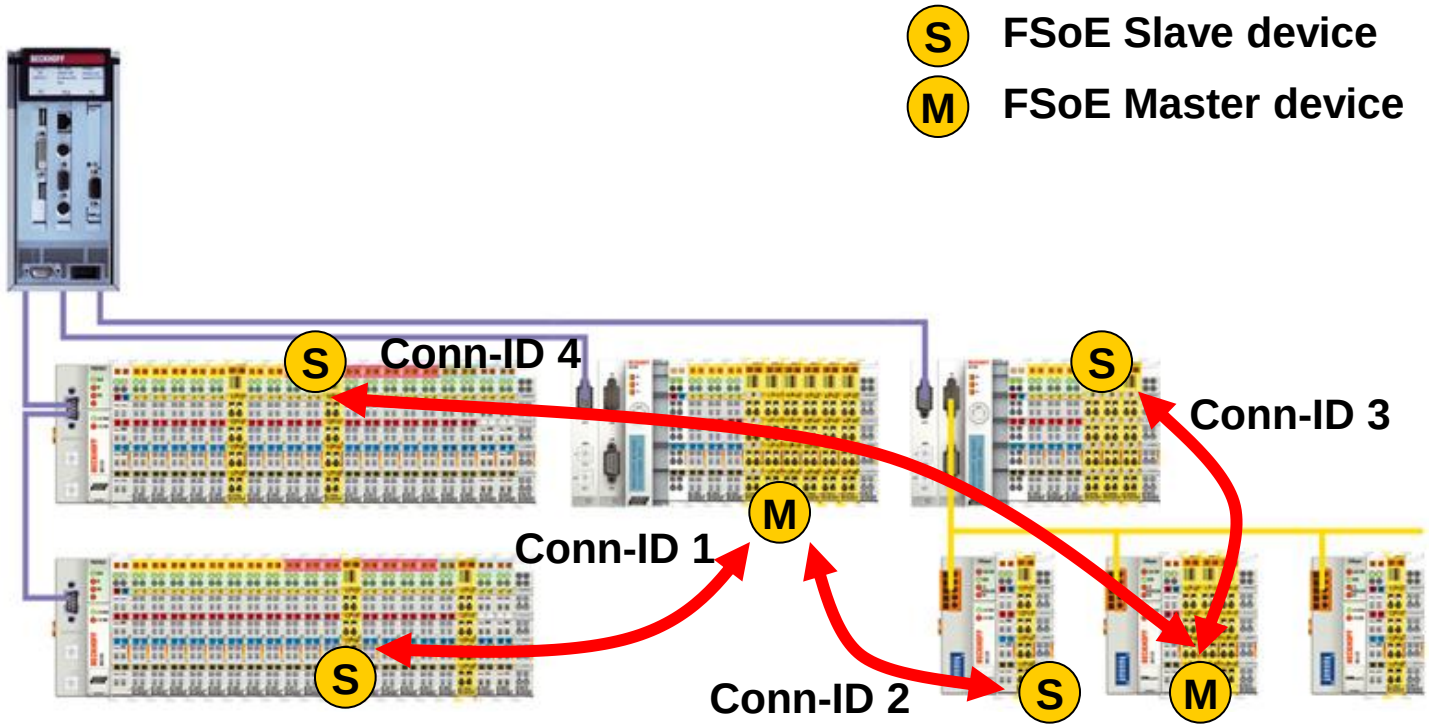
- Konfigurierte Master-Slave Connections
- Kommunikation wird über Standard-SPS geroutet

Sicherheitstechnik in der modernen Automation



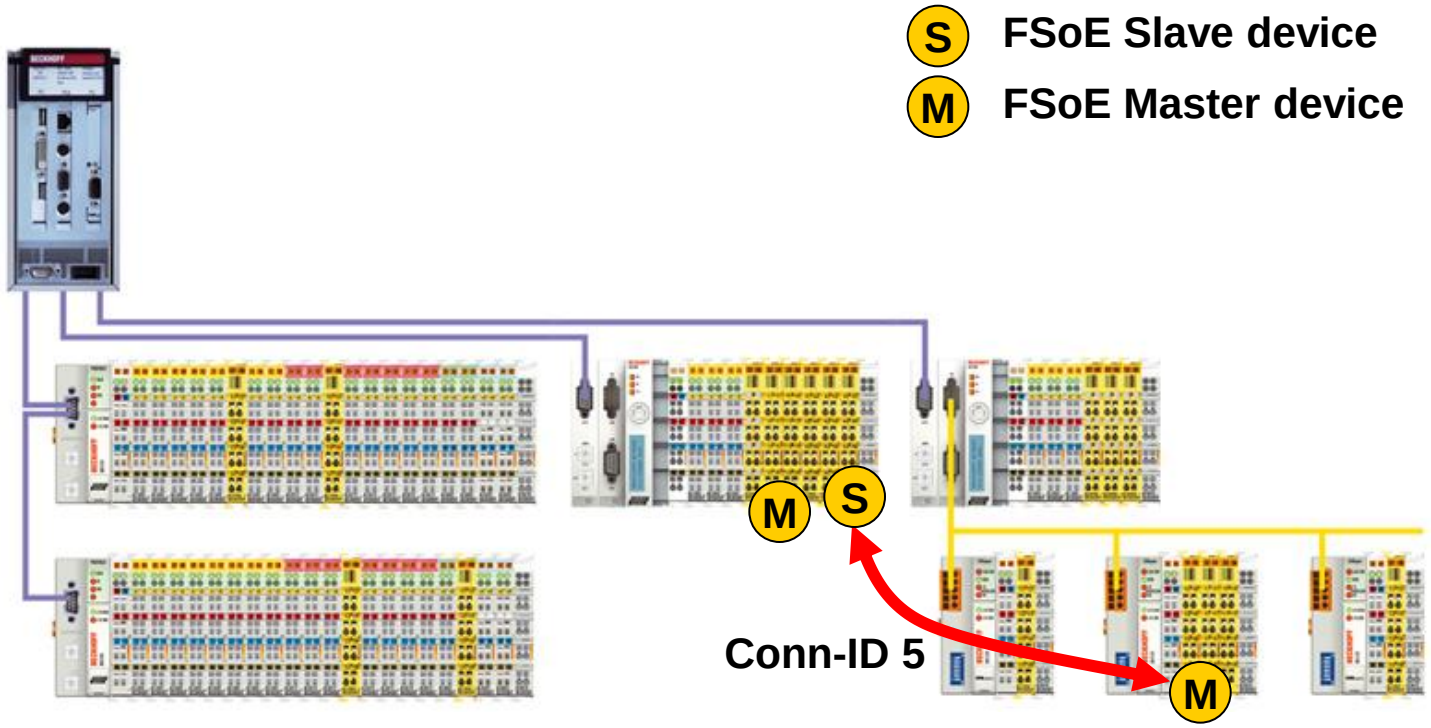
- Konfigurierte Master-Slave Connections
- Kommunikation wird über Standard-SPS geroutet

Sicherheitstechnik in der modernen Automation



- Mehrere Safety-Master in einem Netzwerk
- Sicherheitsgruppen mit Gruppenabschaltung möglich

Sicherheitstechnik in der modernen Automation



- "Master-Master" Kommunikation möglich, über Master & Slave Implementierung im Gerät
- Eindeutige Conn-ID
- Nutzung bei Anlagenverkettung

Applikation | Reifenprüfstände Fa. Seichter

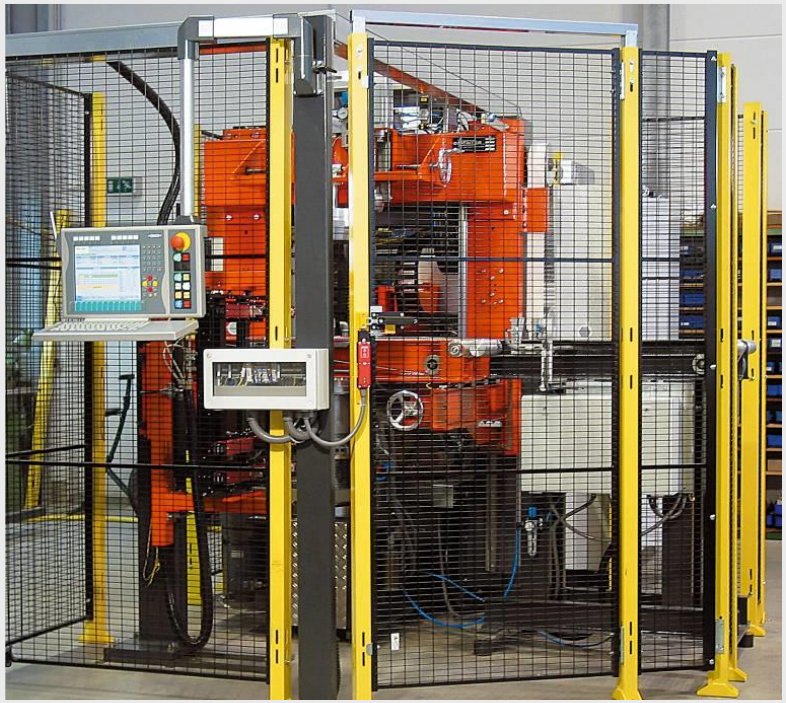
Anforderungen

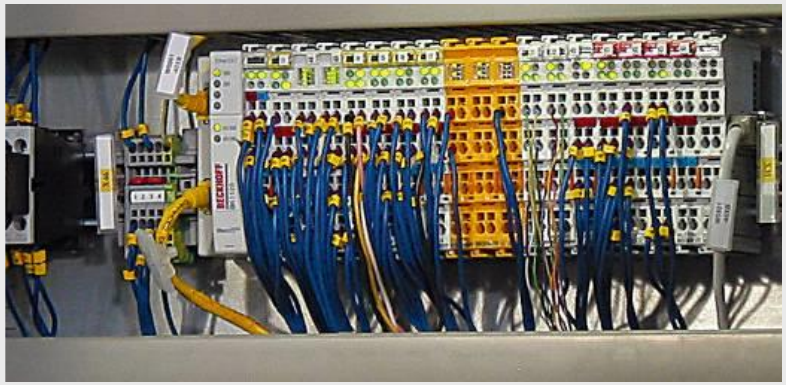
Safety over EtherCAT

- Architektur
- Definitionen
- State-Machine
- Telegrammstruktur
- Zusammenfassung

Konformität

Anwendungen



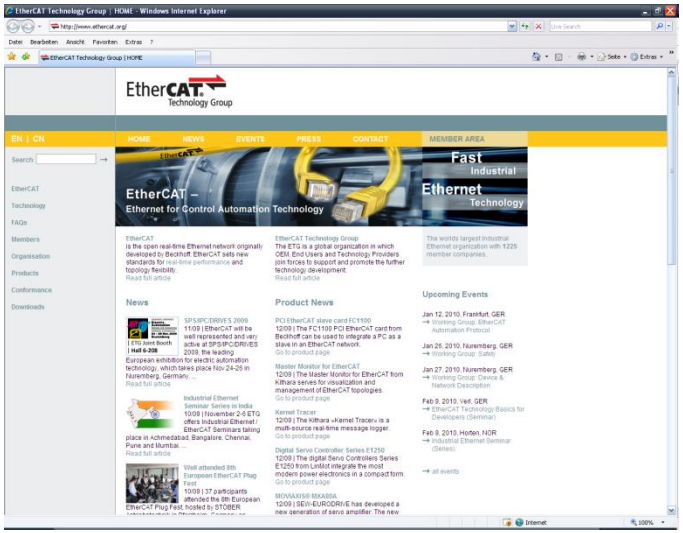


Applikation | Reifenprüfstände Fa. Seichter

- Kundenvorteile:
- Einbindung der Sicherheitsfunktionen in das TwinSAFE-System
  - Not-Aus
  - Schutztürüberwachung
- Kleiner Schaltkasten direkt an der Maschine
- Optimales Zusammenspiel zwischen Standard-Automatisierungstechnik und Sicherheitstechnik
  - Reduzierung der Engineering- und Hardwarekosten
  - Vereinfachte Verdrahtung
  - Erweiterungen einfach zu integrieren
- Durchgängige Verwendung einer einzigen Software
  - Ein Editor zur Projektierung der Standard- und der Sicherheitsfunktionen

Safety over EtherCAT

www.ethercat.org



EtherCAT Technology Group
Dr. Guido Beckmann
Ostendstr. 196
90482 Nürnberg
g.beckmann@ethercat.org