

Übersicht der Technologie Safety over EtherCAT

EtherCAT Technology Group

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

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

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- **BGIA Prüfgrundsatz GS-ET-26**
 - Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten
 - Prüfgrundsatz der BGIA zur Bewertung von sicheren Bussystemen
- **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

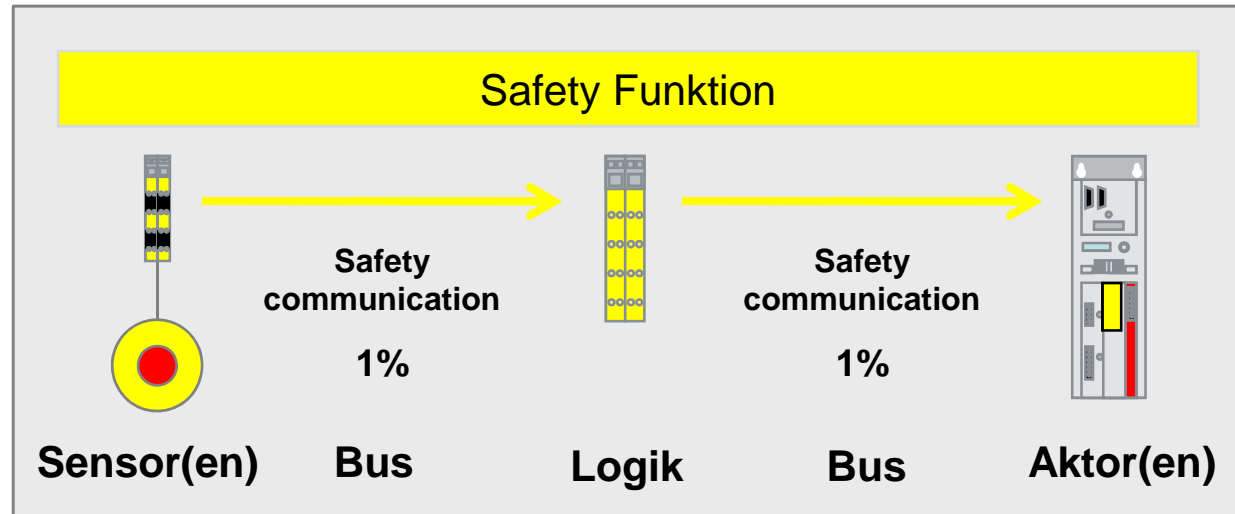
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



- Restfehlerrate der Sicherheitsfunktion im gesamten System:
 - $PFH_{\text{Safetyfunktion}} = PFH_{\text{Sensor}} + PFH_{\text{Logik}} + PFH_{\text{Aktor}} + 2x PFH_{\text{Bus}}$
 $< 10^{-8} \dots 10^{-7} / \text{h}$ bei SIL 3 (IEC 61508)
- In der IEC 61784-3 wird gefordert, dass auf den Kommunikationskanal nur 1% aller Fehler entfallen.
 Das entspricht einer zulässigen Restfehlerrate von:
 - $PFH_{\text{Bus}} < 10^{-9} / \text{h}$ für SIL 3
- Mehr als 100.000 Jahre Datentransport ohne unerkannten Fehler!

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- **Safety over EtherCAT (FSoE)** bezeichnet einen sicheren Kommunikationslayer, mit dem sichere Prozessdaten zwischen Safety over EtherCAT Geräten übertragen werden können.
- FSoE ist innerhalb der EtherCAT Technology Group (ETG) offen gelegt.
- Einhaltung des Safety-Integrity-Level SIL3 ist vom TÜV Süd Rail GmbH bestätigt

Safety over
EtherCAT[®]

Anforderungen

Safety over EtherCAT

- Architektur

- Definitionen

- State-Machine

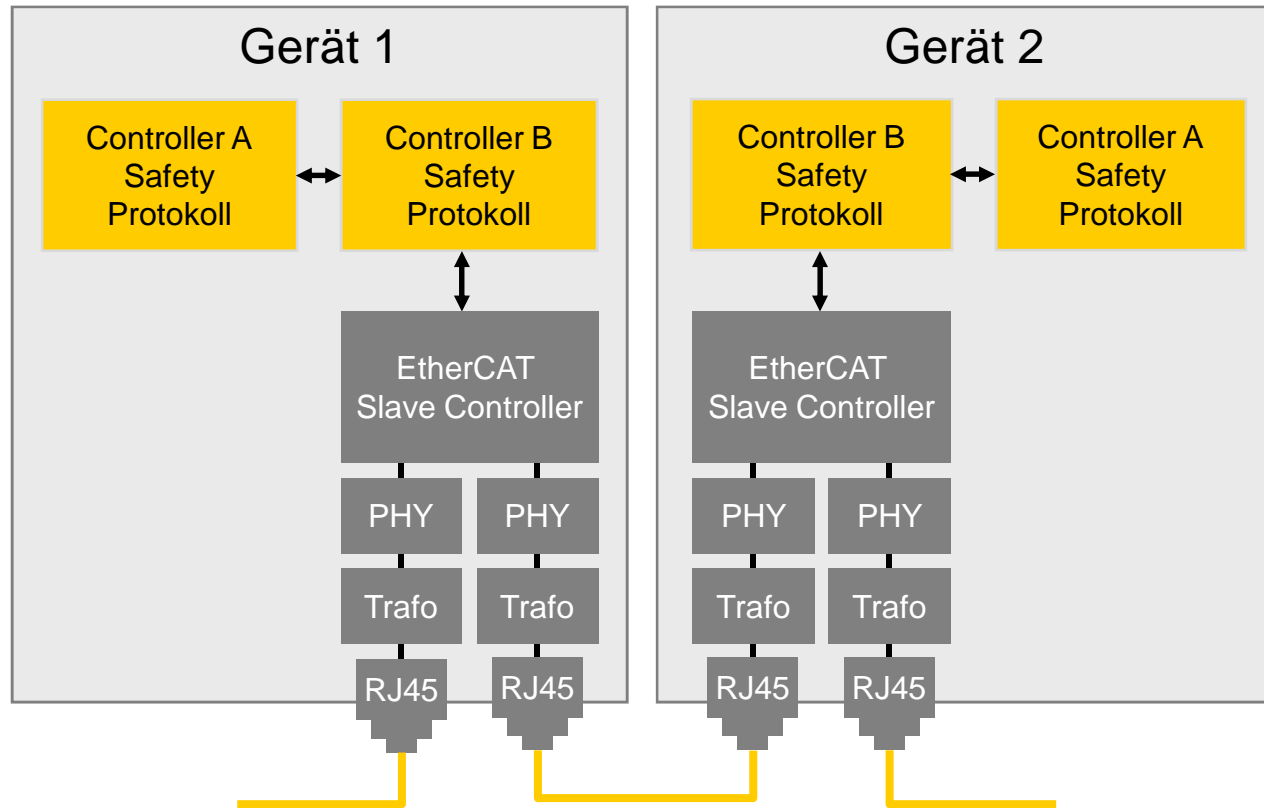
- Telegrammstruktur

- Zusammenfassung

Conformance

Anwendungen

- Einkanaliges Kommunikations-System
z.B. entsprechend Modell A der IEC 61784-3 Annex A



Anforderungen

Safety over EtherCAT

- Architektur

- Definitionen

- State-Machine

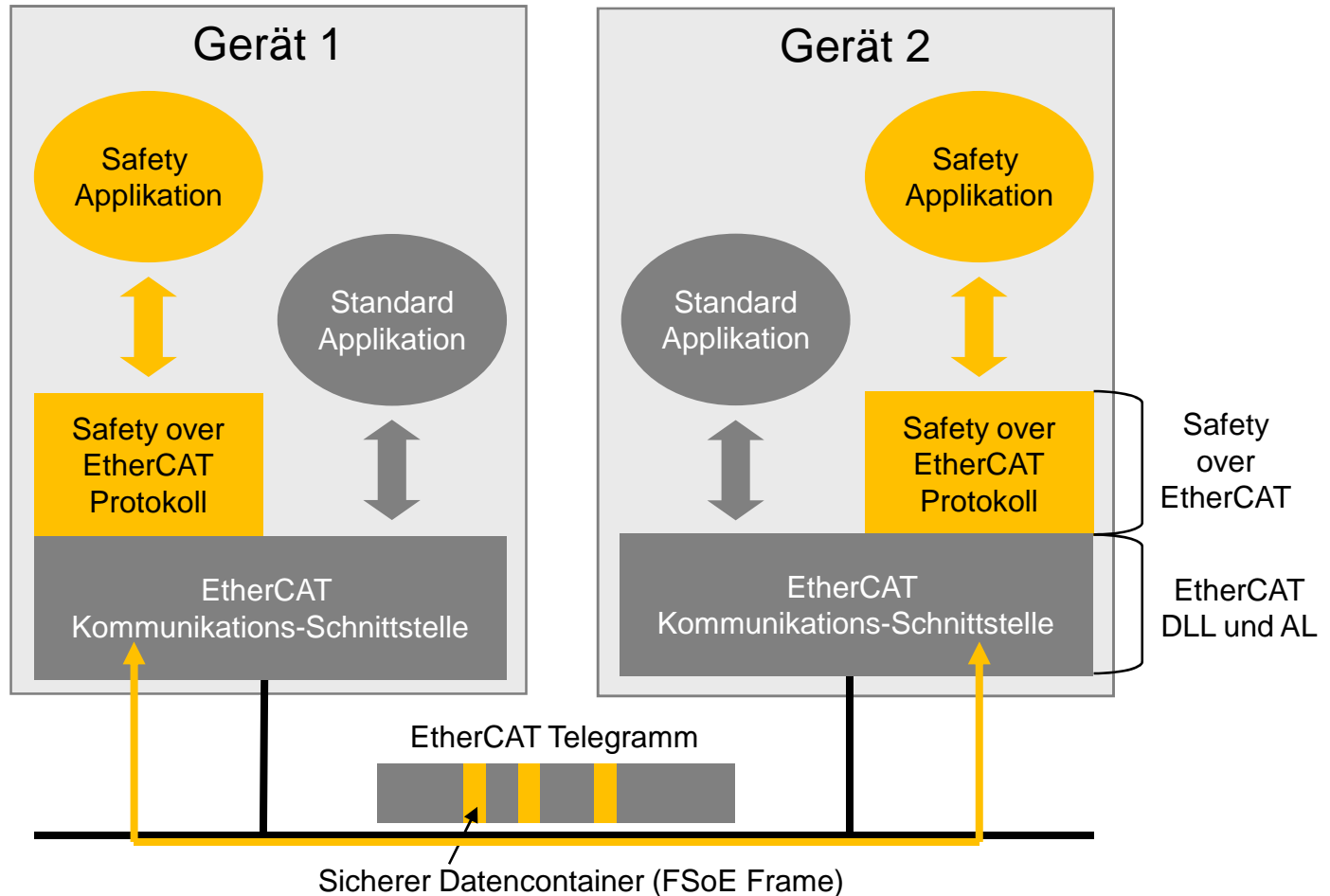
- Telegrammstruktur

- Zusammenfassung

Conformance

Anwendungen

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



Anforderungen

Safety over EtherCAT

- Architektur

- Definitionen

- State-Machine

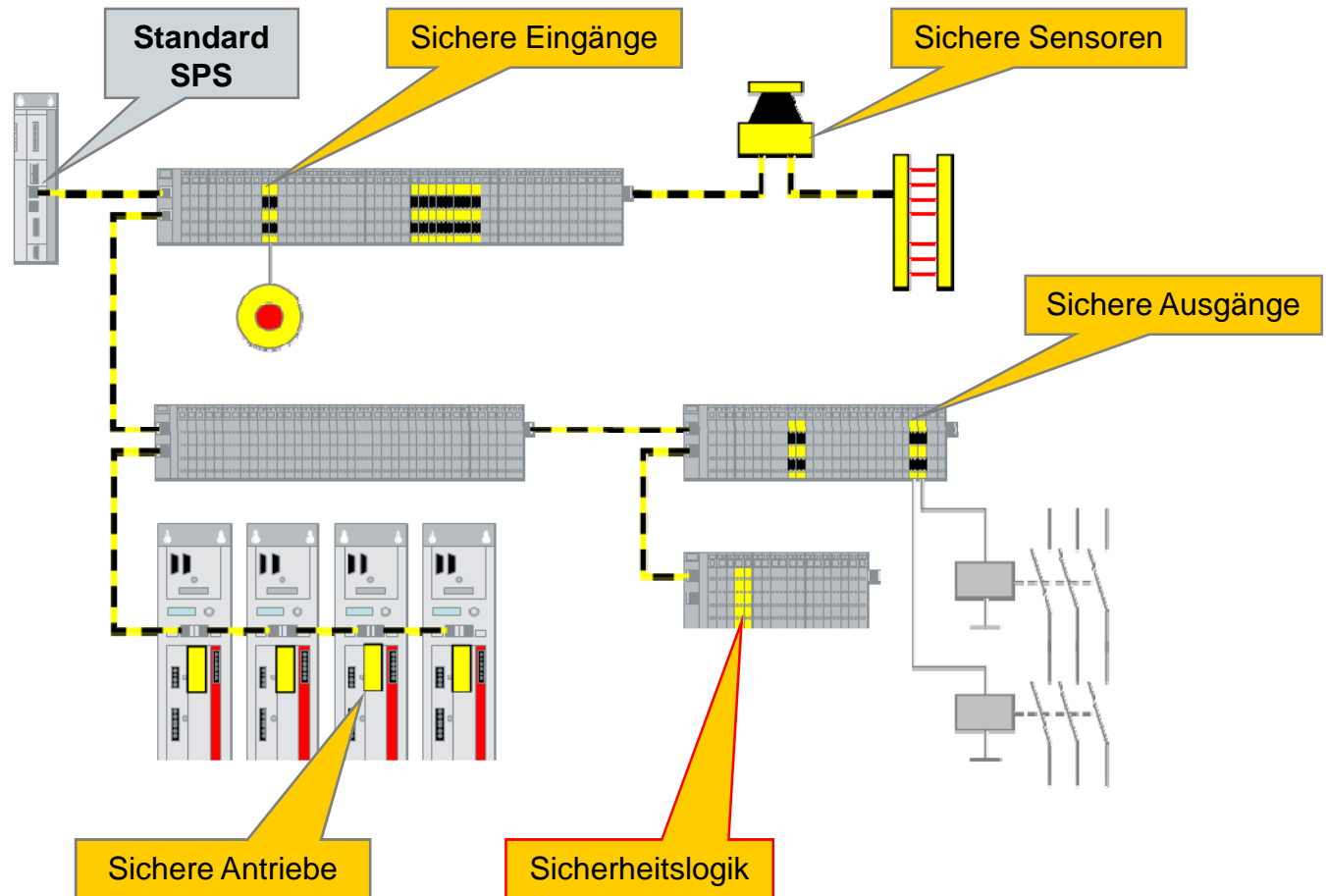
- Telegrammstruktur

- Zusammenfassung

Conformance

Anwendungen

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



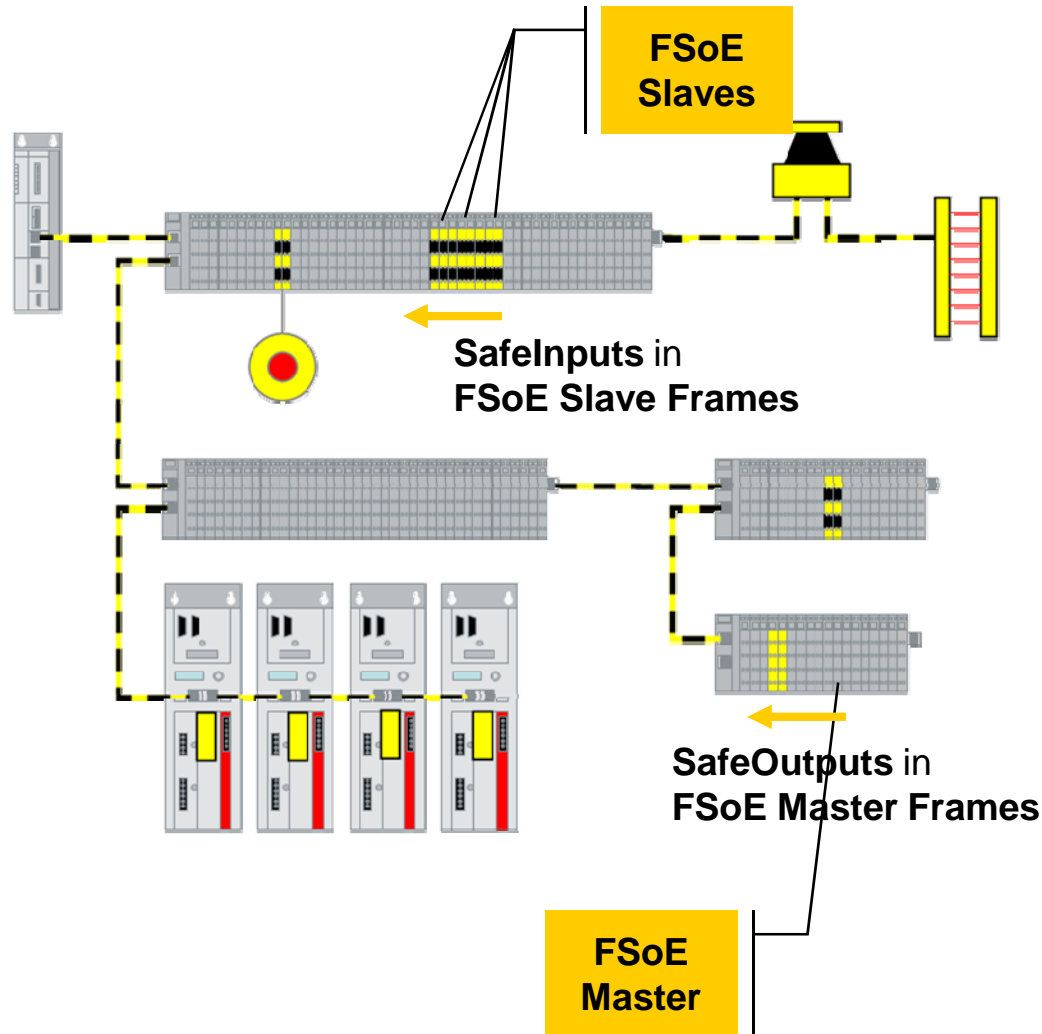
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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.

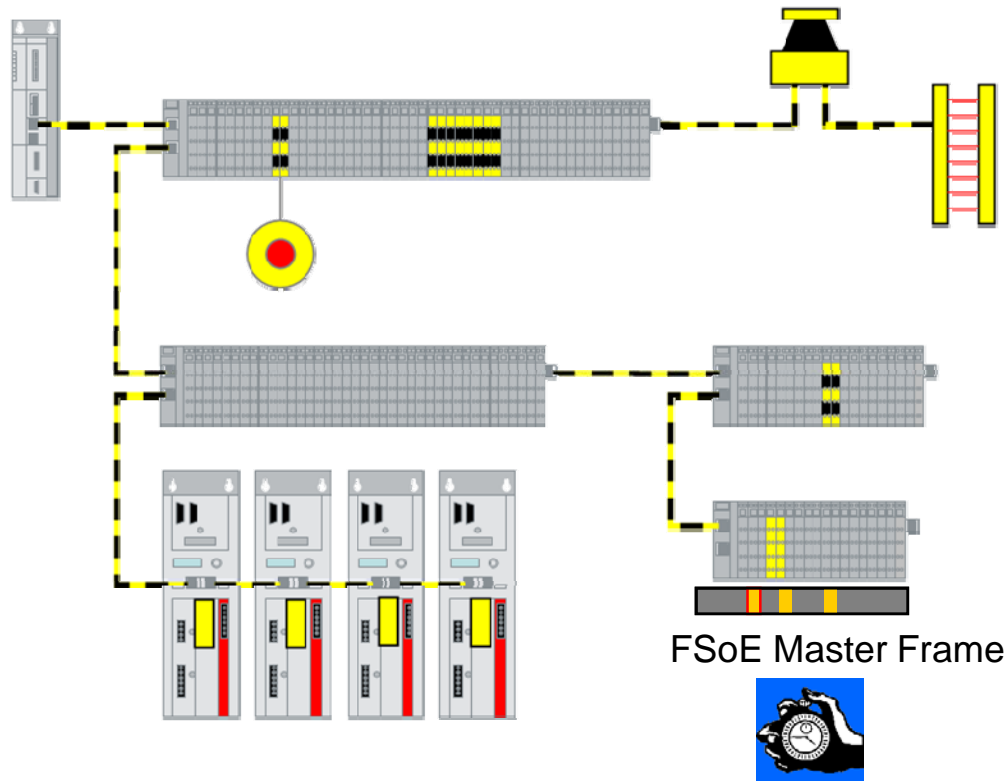
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

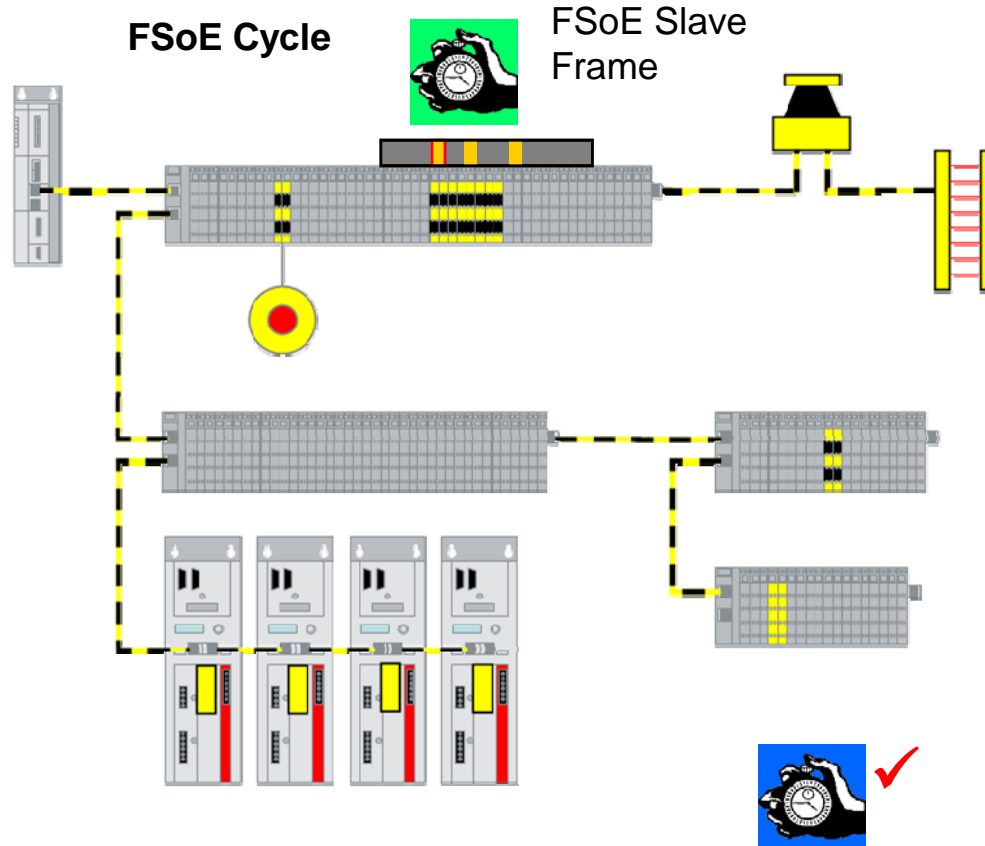
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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.

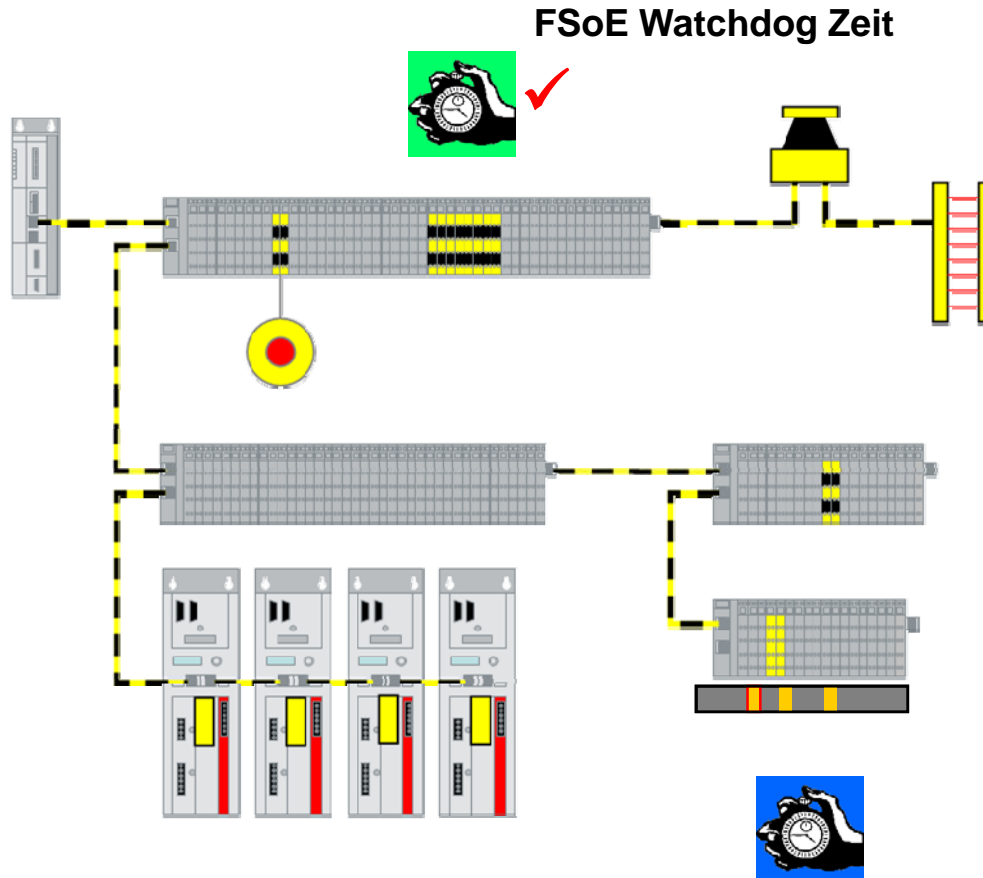
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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.

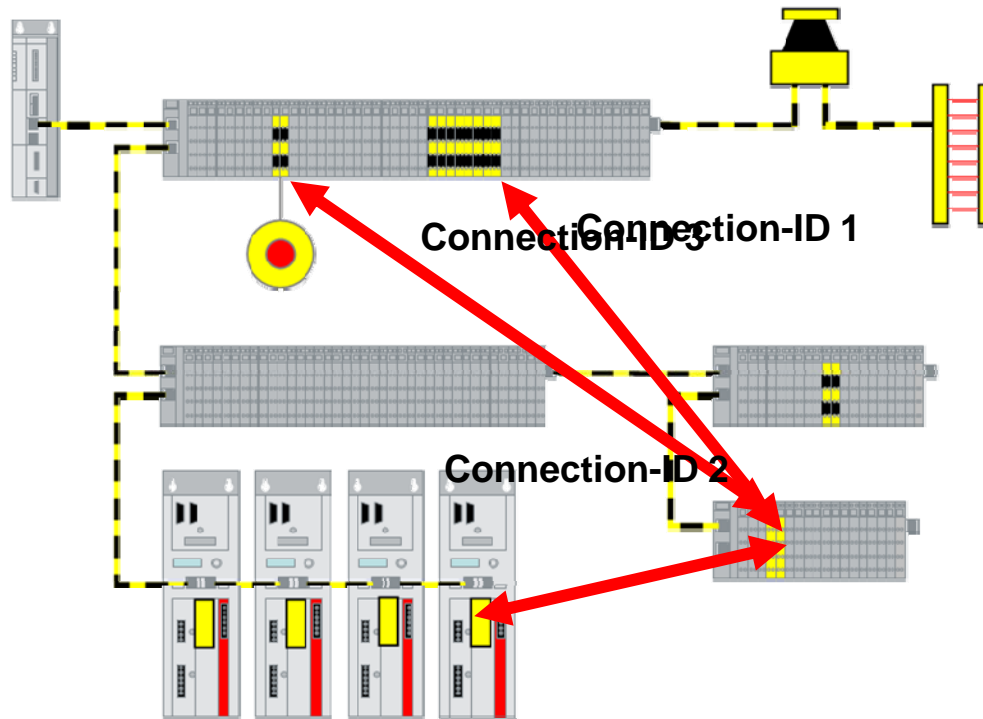
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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.

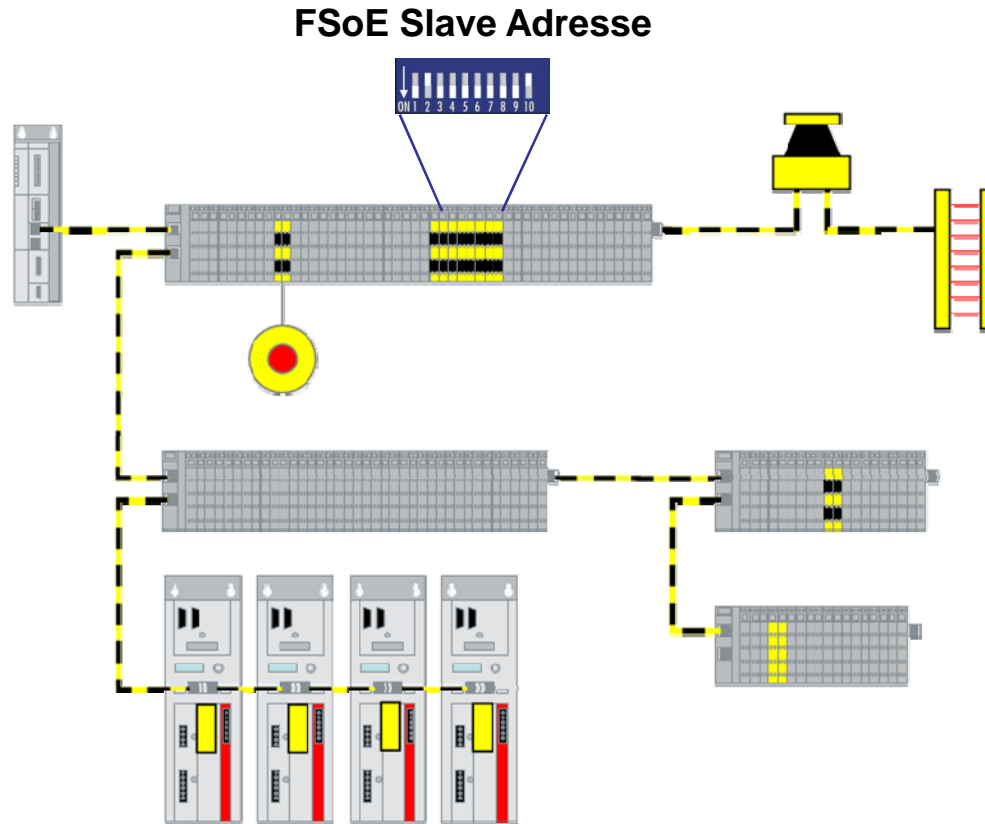
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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.

Anforderungen

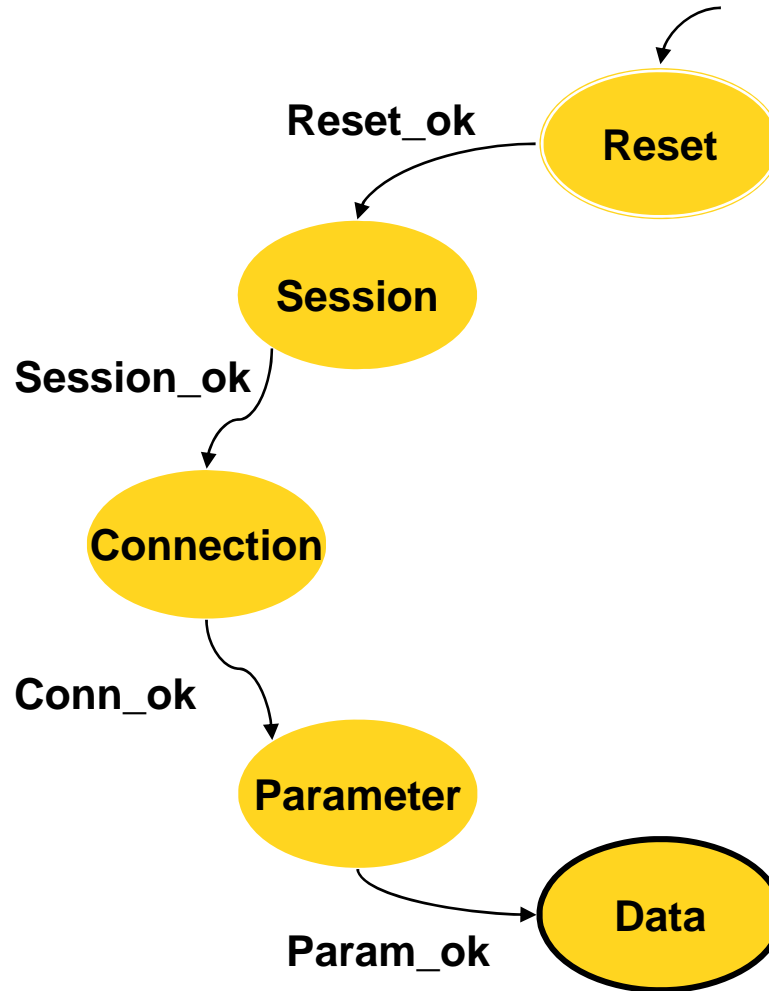
Safety over EtherCAT

- Architektur
- Definitionen
- State-Machine

- Telegrammstruktur
- Zusammenfassung

Conformance

Anwendungen



- 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.

Anforderungen

Safety over EtherCAT

- Architektur

- Definitionen

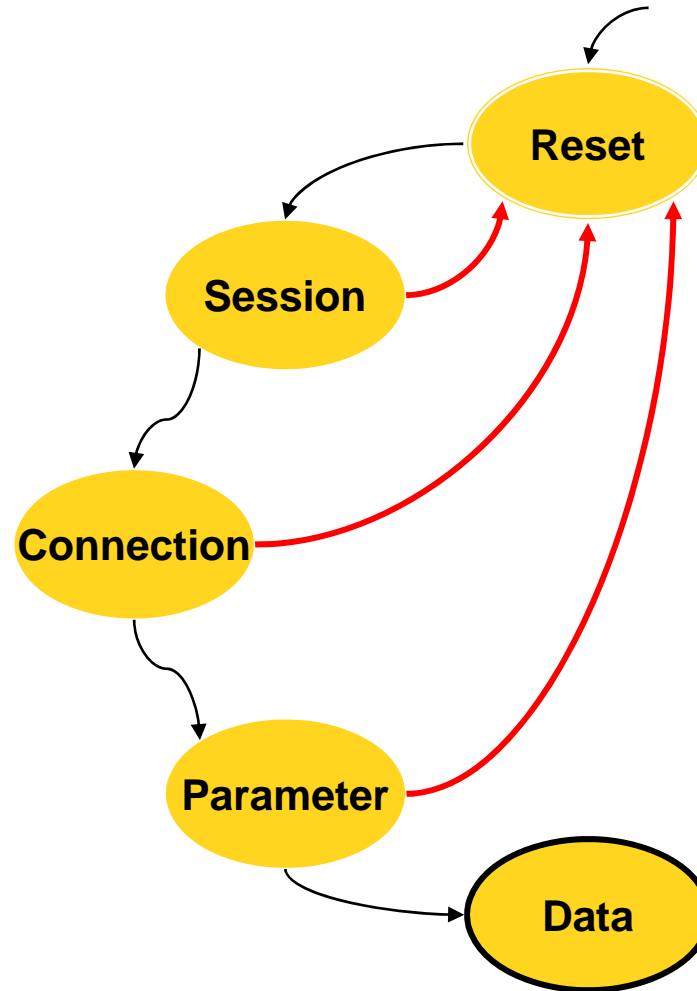
- State-Machine

- Telegrammstruktur

- Zusammenfassung

Conformance

Anwendungen



- 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

Anforderungen

Safety over EtherCAT

- Architektur
- Definitionen
- State-Machine

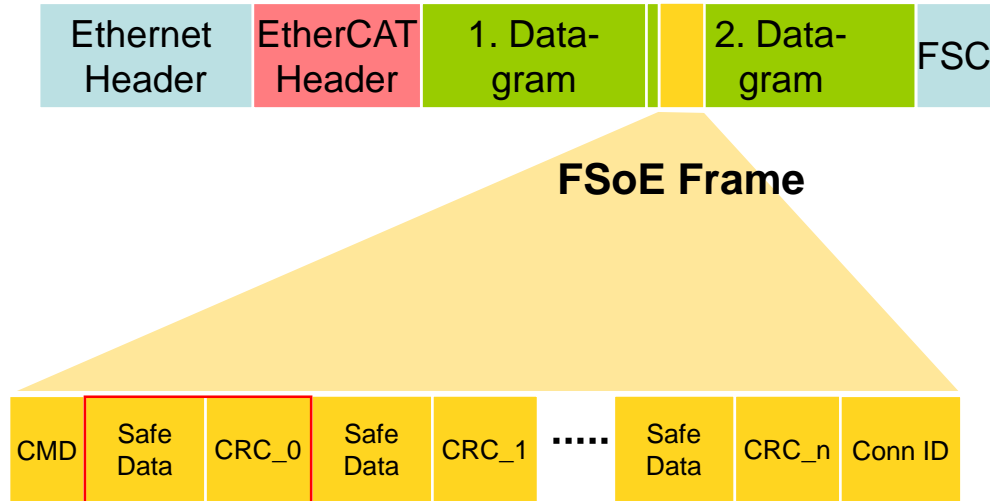
- Telegrammstruktur

- Zusammenfassung

Conformance

Anwendungen

- Ethernet Frame



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

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

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

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- Die FSoE Spezifikation enthält keine Einschränkungen bezüglich:
 - Kommunikationsmedium
 - Übertragungsrate
 - Länge der sicheren Prozessdaten
- Routing via unsichere Gateways, Feldbusse oder Backbones ist möglich.



Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- Restfehlerrate $R_{(p)} < 10^{-9}/h$
- Das Protokoll ist entwickelt nach IEC 61508
 - Geeignet für den Einsatz in Geräten bis SIL 3
- 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 eingereicht für die IEC 61784-3 Functional safety fieldbuses
 - Veröffentlichung 2010

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- 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.

Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- Protokolltest für Safety-Geräte
 - Verbindung über die EtherCAT-Schnittstelle
 - Black Box Test
- Tests verfügbar für Gerätehersteller
 - Tests kann während des Entwicklungsprozesses genutzt werden
 - Keine zusätzliche Hardware erforderlich
- Unabhängiges Testlabor zur Bestätigung der Konformität

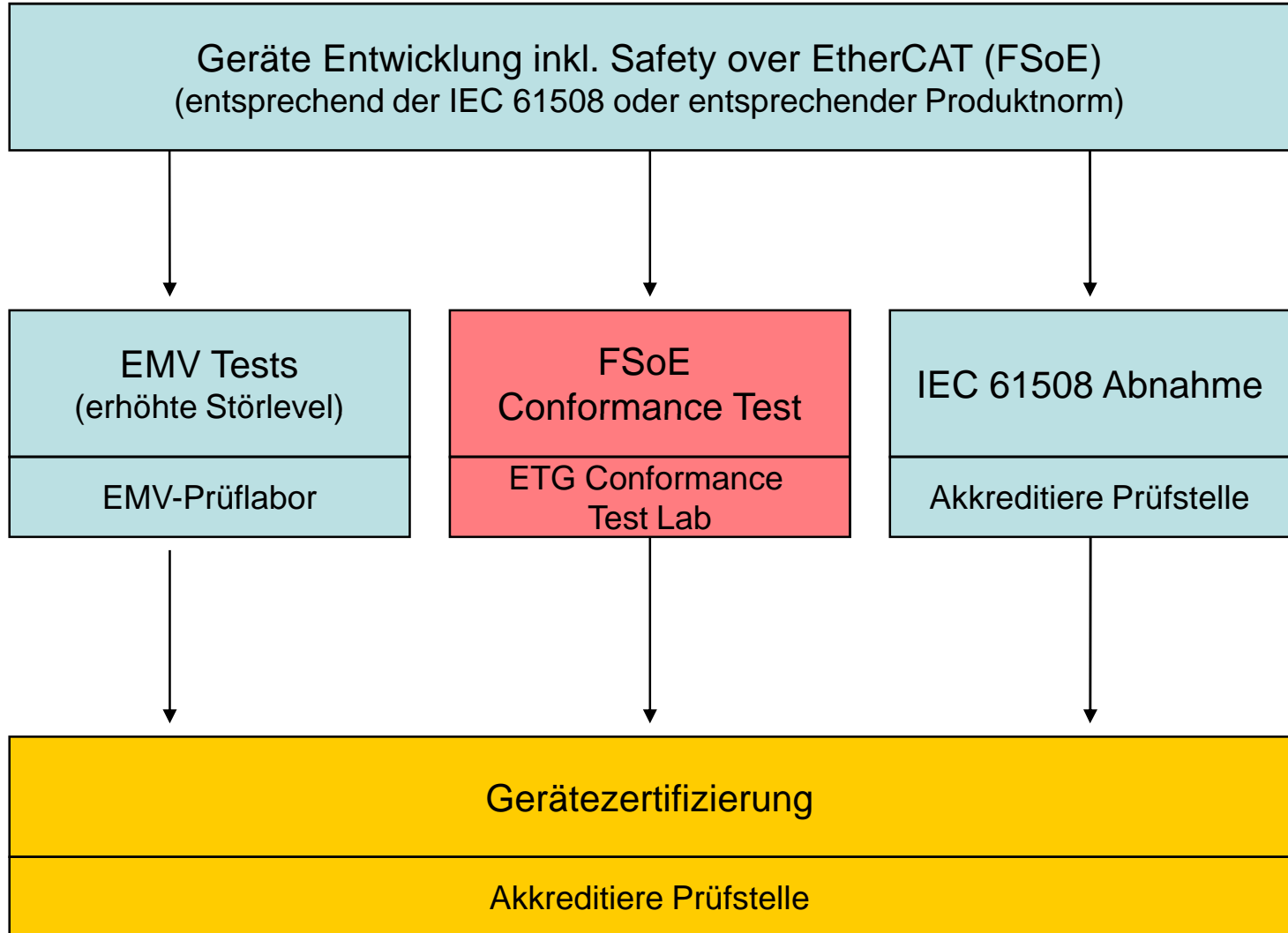
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



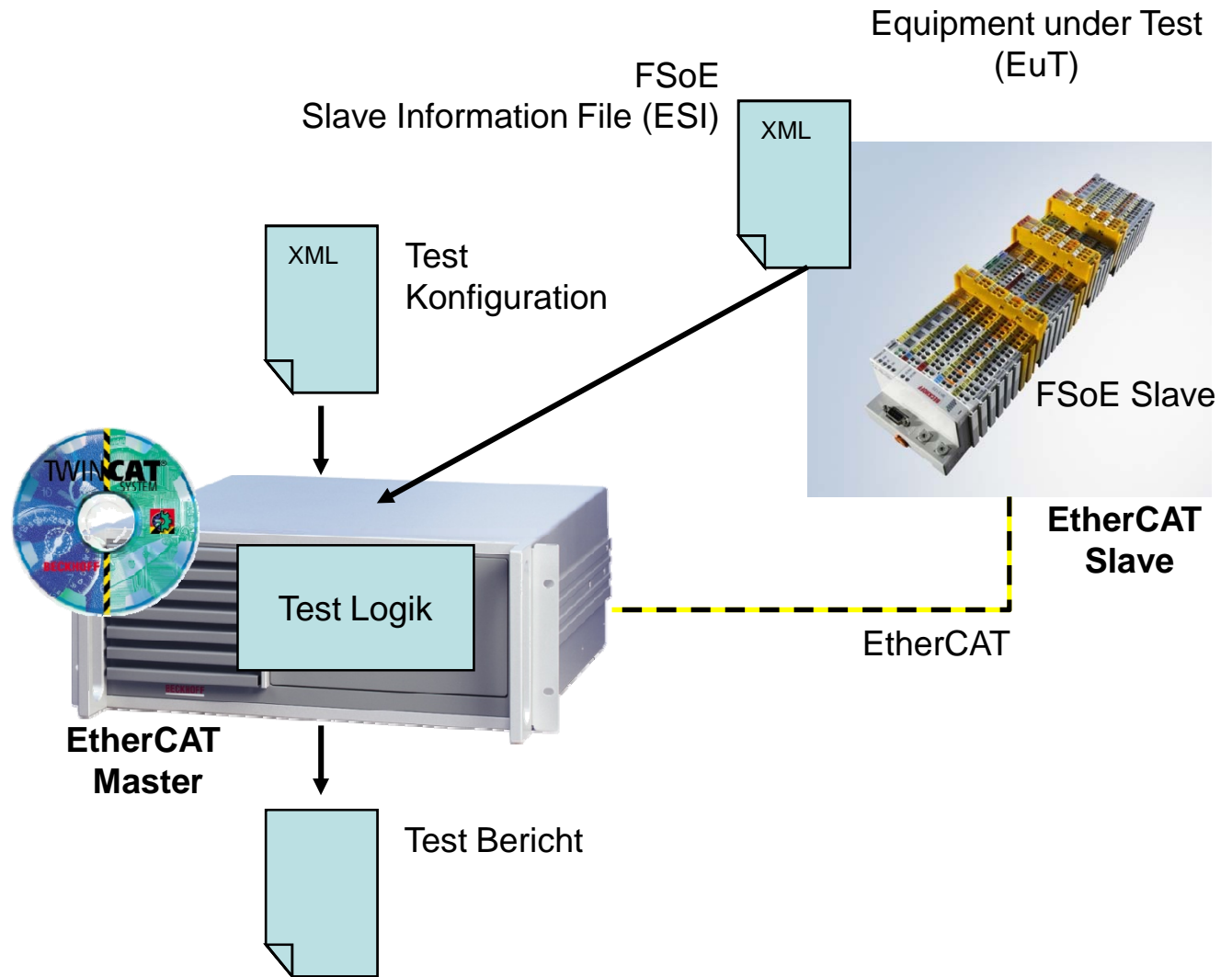
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



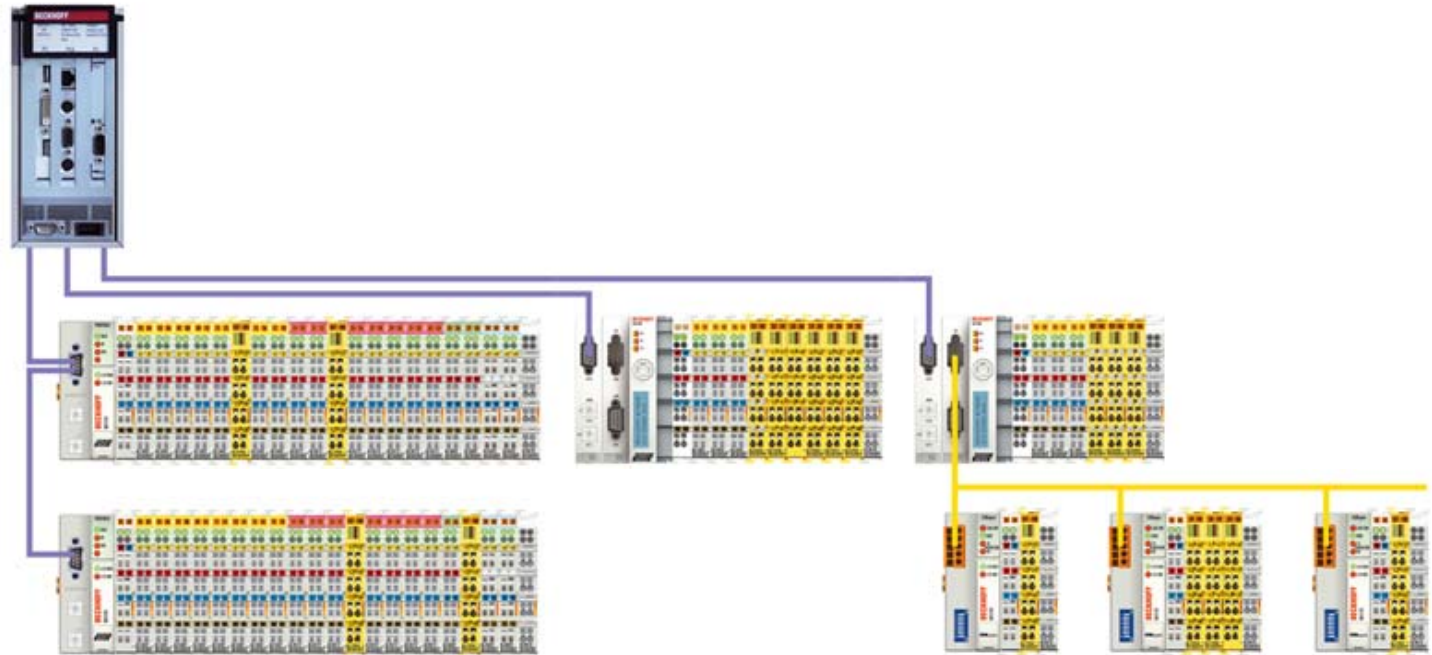
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

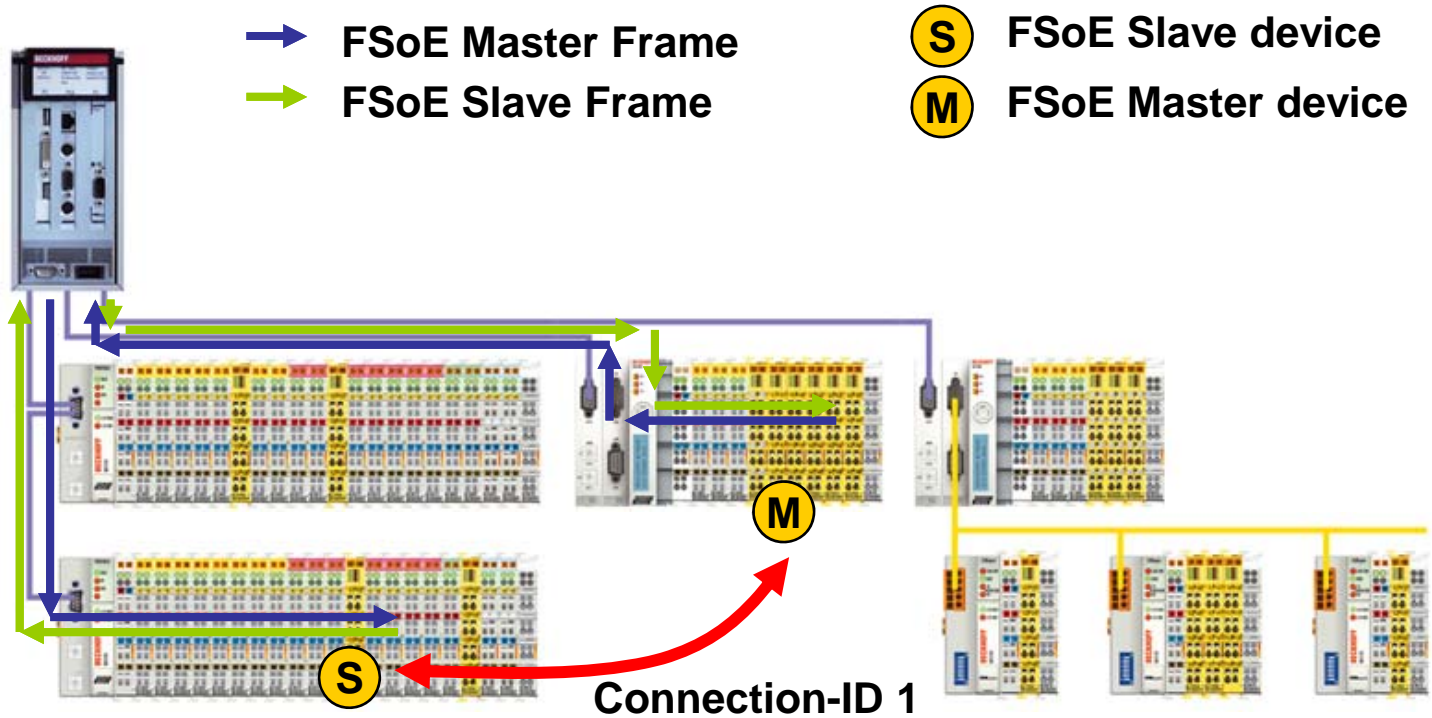
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

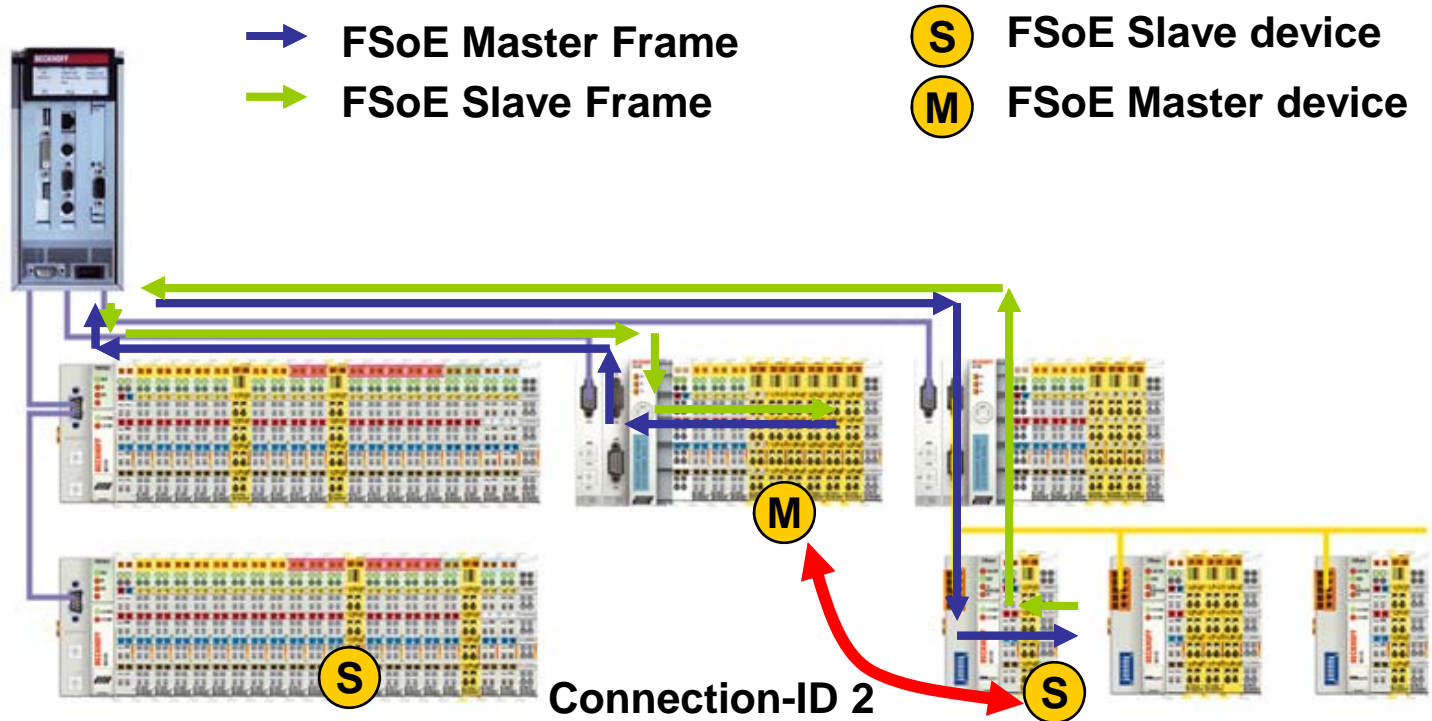
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

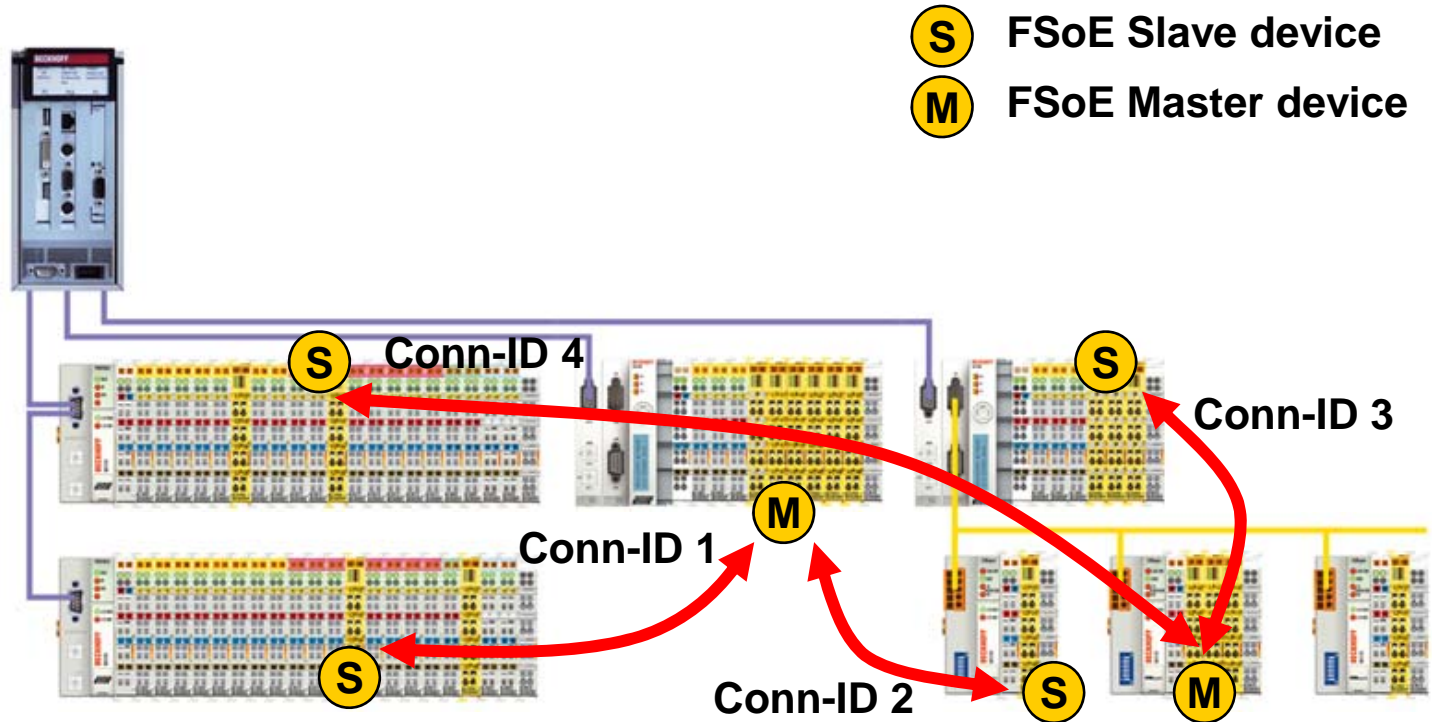
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

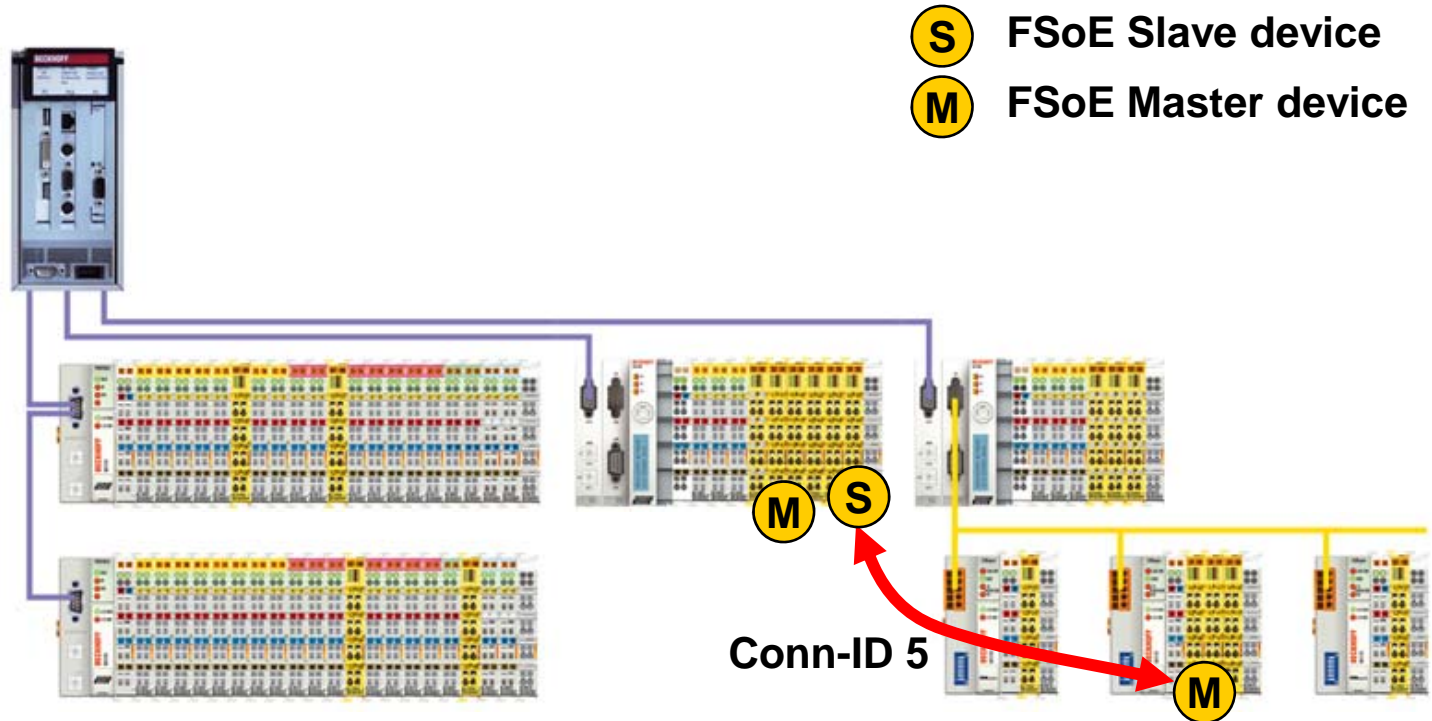
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



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

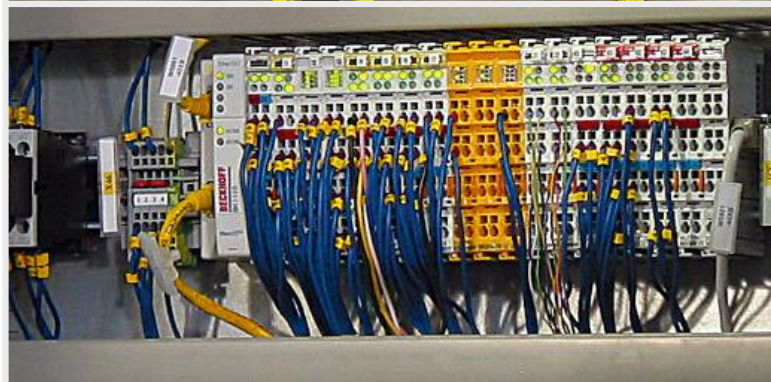
Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen



Anforderungen

Safety over EtherCAT

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

Conformance

Anwendungen

- 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

Anforderungen

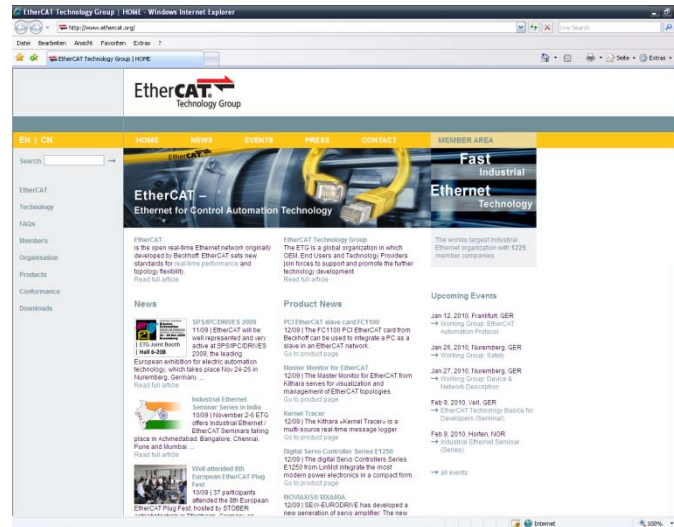
Safety over EtherCAT

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

Conformance

Anwendungen

www.ethercat.org



EtherCAT Technology Group

Dr. Guido Beckmann

Ostendstr. 196

90482 Nürnberg

g.beckmann@ethercat.org