Overview
Safety over EtherCAT
EtherCAT Technology Group
Safety over EtherCAT

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

Requirements

Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

Material feeding Mutig
Two-Hand control
Protection of workspace e.g. with Laser scanner
Emergency stop
Operator Diagnosis
Safely-limited Position / Speed
Door guarding with Interlocking
Safety guard

Setup / Maintenance

© EtherCAT Technology Group
June 2014

Safety-over-EtherCAT
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 Standards for Safetybus Systems

- 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
IEC 61784-3

Requirements

Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

Product Standards

IEC 61496
Safety f. e.g. Light curtains

IEC 61131-X
Safety for PLC

IEC 61800-5-2
Safety functions for Drives

IEC 61784-4
Security

IEC 62443
Security (common)

IEC 61784-5
Installation guide (profile-specific)

IEC 61918
Installation guide (common part)

IEC 61784-3
Functional safety communication profiles

IEC 61158 / 61784-1/2
Fieldbus for use in industrial control systems

IEC 61326-3-1
EMI and Functional safety

IEC 61508
Functional safety (basic standard)

ISO 12100-1 & ISO 14121
Safety of machinery – Principles for design and risk assessment

IEC 60204-1
Safety of electrical equipment

USA: NFPA 79 (2005)

IEC 62061
Functional safety for machinery (SRECS) (including EMI for industrial environment)

ISO 13849-1, -2
Safety-related parts of machinery (SRPCS) Non-electrical

SIL based

Electrical

PL based

Design objective

Applicable standards

Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
IEC 61784-3 – Black channel approach

Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications

Safety Communication Layer

Application Layer (opt.)
Data Link Layer
Physical Layer

Safety logical connection

Black channel

Gateway
Application Layer (opt.)
Data Link Layer
Physical Layer

Fieldbus, Backplane

Repeater, Switch

Fieldbus

Fieldbus

© EtherCAT Technology Group
June 2014
Safety function decomposition

- Probability of failure for the safety function, acc. to IEC 61508:
  \[ PFH_{\text{SafetyFunction}} < 10^{-8} \ldots 10^{-7}/h \text{ for SIL 3} \]

- 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:
  \[ PFH_{\text{LogicalConnection}} < 10^{-9}/h \text{ for SIL3} \]

- More than 100.000 years communication without an undetected Error!

\[ PFH_{\text{SafetyFunction}} = PFH_{\text{Sensor}} + PFH_{\text{Logic}} + PFH_{\text{Actor}} + PFH_{\text{LogicalConnection}} \]
Safety over EtherCAT

- **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
  - Supported by EtherCAT Technology Group (ETG)
  - Part of IEC 61784-3 international standard

- The protocol is approved by an independent Notified Body (TUV Sued Rail GmbH).

© EtherCAT Technology Group
FSoE – Typical Hardware Architecture

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

![Diagram of FSoE architecture](image)

**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.
Safety over EtherCAT | System Example

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

![System Diagram]

- Safety Inputs
- Safety Sensors
- Safety Outputs
- Standard PLC
- Safety Logic
- Safety Drives
- Safety Sensors
- Safety Outputs
- Safety Logic
- Safety Drives
FSoE | Master / Slave Connection

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.

FSoE | Master / Slave Connection

FSoE Master

SafeOutputs in FSoE Master Frames

FSoE Master

FSoE Master Frame

SafeOutputs
FSoE | Master / Slave Connection

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.

FSoE Slaves

SafelInputs in FSoE Slave Frames

SafeOutputs in FSoE Master Frames

FSoE Master

FSoE | Master / Slave Connection

© EtherCAT Technology Group

June 2014

Safety-over-EtherCAT

16
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 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.
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.
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.
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.
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.
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
**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 over EtherCAT | Safety Measures

<table>
<thead>
<tr>
<th>Error</th>
<th>Measure</th>
<th>Sequence Number</th>
<th>Watchdog</th>
<th>Connection ID</th>
<th>CRC Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintended repetition</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Loss</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Insertion</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Incorrect sequence</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Corruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Unacceptable delay</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masquerade</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Repeating memory errors in Switches</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Incorrect forwarding between segments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
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, fieldbus systems or backbones is possible, even wireless!
Safety over EtherCAT | Features

- The protocol is developed according to IEC 61508 Safety Integrity Level SIL 3
  - Residual Error Probability $R_p < 10^{-9}$/h
  - No restriction to the underlying communication layer

- 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 | 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.

• **Safe Device Parameter can be downloaded from the Master to the Slave at Boot-Up of a FSoE Connection**
  - Watchdog time
  - Device specific safety-related Parameter for Slave application
Safety over EtherCAT – Open Solution

- FSoE is disclosed within the ETG.5100 and part of IEC 61784-3 Functional Safety Fieldbuses

- 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

(Vendors that ship or have announced Safety over EtherCAT devices as of 03/2014. Not all products shipping yet.)
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

Vendor

Device development with Safety over EtherCAT
(according IEC 61508 or appropriate product norm)

- EMC Tests (increased immunity)
- Overall safety lifecycle process
- FSoE Test passed

EMC Test Lab

If applicable

FSOE Test Center

Perform FSoE Conformance Test

EtherCAT Test Center

Perform EtherCAT Conformance Test

Notified Body

Functional Safety Assessment and Approval

Passed

Passed
FSoE Conformance Test Tool | FSoE Slave

Requirements
Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance
Applications

FSoE Test cases (XML)

EtherCAT Slave Information ESI (XML-File)

EtherCAT Conformance Test Tool (CTT)

EtherCAT

EtherCAT Master

Device under Test EtherCAT Slave FSoE Slave

FSoE Test Results
Safety engineering in modern automation

- Mixed network for standard and safety functions
- Standard network with a decentralized safety island
- Separate networks for standard and safety functions
Safety engineering in modern automation

- Configured Master-Slave Connections
- Communication routed via Standard-PLC
Safety engineering in modern automation

- Configured Master-Slave Connections
- Communication routed via Standard-PLC
Safety engineering in modern automation

- Multi Master networks
- Safety groups with group failsafe possible.
Safety engineering in modern automation

- "Master-Master" Communication possible with Master & Slave implementation in the Master device
- Unique Conn-ID
- Used for plant concatenation
Application | Tire and wheel testing machine

Requirements
Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary

Conformance

Applications
Application | Tire and wheel testing machine

- 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
Safety over EtherCAT

www.ethercat.org

EtherCAT Technology Group
Dr. Guido Beckmann
Ostendstr. 196
90482 Nuremberg, Germany
g.beckmann@ethercat.org