Overview
Safety over EtherCAT

EtherCAT Technology Group
Safety over EtherCAT

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

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

Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based

Design objective
Applicable standards

IEC 61784-3
Functional safety communication profiles

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

IEC 61784-5
Installation guide (profile-specific)

IEC 61918
Installation guide (common part)

IEC 61784-4
Security

IEC 62443
Security (common)

IEC 61800-5-2
Safety functions for Drives

IEC 61326-3-1
EMI and Functional safety

USA: NFPA 79 (2006)

IEC 60204-1
Safety of electrical equipment

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

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

Electrical

IEC 61496
Safety t. e.g. Light curtains

IEC 61131-X
Safety for PLC

IEC 61905

Safety communication as part of a safety system

Requirements

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

Conformance

Applications

- Probability of failure for the safety system:
  - \( PFH_{\text{Safety function}} = PFH_{\text{Sensor}} + PFH_{\text{Logic}} + PFH_{\text{Actor}} + 2 \times PFH_{\text{Bus}} < 10^{-8} \ldots 10^{-7} /h \) 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:
  - \( PFH_{\text{Bus}} < 10^{-9} /h \) for SIL 3

- More than 100,000 years communication without an undetected Error!
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 within the EtherCAT Technology Group (ETG).

• The protocol is approved by an independent Notified Body (TUV Sued Rail GmbH).
1-channel communication system
Model A according to IEC 61784-3 Annex A
Safety over EtherCAT | Software Architecture

- 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
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.

**SafeOutputs in FSoE Master Frames**
**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 Master**

**SafeOutputs in FSoE Master Frames**

---

**SafeInputs in FSoE Slave Frames**

---

**FSoE Slaves**

---
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.
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.
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.
FSoE | Unique Address

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.

Requirements

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

Conformance

Applications

© EtherCAT Technology Group
Requirements
Safety over EtherCAT
- Architecture
- Definitions
- State Machine
- Frame Structure
- Summary
Conformance
Applications

FSoE State Machine per Connection

- 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
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.
<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.
Safety over EtherCAT | Features

- 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
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**
Safety over EtherCAT | Conformance Test

• 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
Certification Process | Proposal

**Requirements**

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

**Conformance**

Device Development with Safety over EtherCAT (FSoE) according to IEC 61508 or relevant Product Norm

**Applications**

- EMC Tests (Increased Levels)
  - EMC-Lab
- FSoE Conformance Test
  - EtherCAT Test Center
- IEC 61508 Approval
  - Notified Body

Device Certification

- Notified Body
FSoE Conformance Test | FSoE Slave

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

**Conformance**

**Applications**

- Equipment under Test (EuT)
- FSoE Slave
- EtherCAT Slave

- EtherCAT Master
- Test Logic
- Test Report
- XML
- FSoE Slave Information File (ESI)
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

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
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
Ostendstr. 196
90482 Nuremberg, Germany
g.beckmann@ethercat.org