Safety over EtherCAT®

Implementation Guide

Document: ETG.5101 G (R) V1.2.0

Nomenclature:	
ETG-Number	ETG.5101
Type	G (Guideline)
State	R (Release)
Version	1.2.0

Created by:	ETG
Contact:	info@ethercat.org
Date:	04.03.2012

EtherCAT® Technology Group

LEGAL NOTICE

Trademarks and Patents

EtherCAT® and Safety over EtherCAT® are registered trademarks and patented technologies, licensed by Beckhoff Automation GmbH, Germany. Other designations used in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

Disclaimer

The documentation has been prepared with care. The technology described is, however, constantly under development. For that reason the documentation is not in every case checked for consistency with performance data, standards or other characteristics. In the event that it contains technical or editorial errors, we retain the right to make alterations at any time and without warning. No claims for the modification of products that have already been supplied may be made on the basis of the data, diagrams and descriptions in this documentation.

Copyright

DOCUMENT HISTORY

Version	Comment
1.1.0	First Draft
1.1.1	FAQs update
1.2.0	ETG.9100 FSoE Policy, FSoE Conformance Test released

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

µC	Microcontroller
CoE	CAN application protocol over EtherCAT
COTS	commercially of the shelf
CTT	Conformance Test Tool
DPRAM	Dual-Ported RAM
ENI	EtherCAT Network Information (EtherCAT XML Master Configuration)
EoE	Ethernet over EtherCAT
ESC	EtherCAT Slave Controller
ESI	EtherCAT Slave Information (EtherCAT Device Description)
ESM	EtherCAT State Machine
ETG	EtherCAT Technology Group
FoE	File Access over EtherCAT
FSoE	FailSafe over EtherCAT
I/O	Input/Output
IEC	International Electrotechnical Commission
IRQ	Interrupt Request
MAC	Media Access Controller
MI	(PHY) Management Interface
MII	Media Independent Interface
NIC	Network Interface Card
ns	nanoseconds (10^{-9} seconds)
OD	Object Dictionary
PELV	Protected extra low voltage
PLC	Programmable Logic Controller
PDO	Process Data Object
SDO	Service Data Object
SELV	safety extra low voltage
SIL	Safety Integrity Level
SoE	Servo drive profile over EtherCAT
TUV	German Technical Inspection Agency (notified body)
TWG	Technical Working Group
WD	Watchdog
WKC	Working Counter
XML	eXtensible Markup Language

1 Scope

This document describes from a very practical point of view which topics have to be kept in mind for a successful usage and/or implementation of the Safety over EtherCAT Technology. It considers the following issues:

- What are the requirements for a machine builder, EtherCAT master manufacturer or Safety device manufacturer
- What kind of information and documentation is available
- How to start with an implementation
- Where can I get technical support
- Is a conformance test available?

The EtherCAT Technology Group will not assume any responsibility or liability if a manufacturer of a Safety over EtherCAT device is infringing safety standards or regulations.

All responsibilities for the proper application of Safety over EtherCAT Technology, i.e. the development, the creation and certification of safe products in whole or in part including the safety risk and hazard analysis and classification, remains with the device manufacturer.

2 Terms, Definitions and Word Usage

2.1 Terms and Definitions

The terms and definitions of ETG.1000 series [15] shall be fully valid, unless otherwise stated.

EtherCAT device
non safety-related device with EtherCAT interface

FailSafe over EtherCAT (FSoE)
Protocol for transferring safety data up to SIL3 between FSoE devices

protective extra-low-voltage (PELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

safety extra-low-voltage (SELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

FSoE Device
Device incorporating the Safety over EtherCAT Technology, can be implemented as FSoE Master or FSoE Slave device

2.2 Word usage: shall, should, may, can

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

3 Safety over EtherCAT technology

3.1 Overview

Safety over EtherCAT (FSoE) describes a protocol for transferring safety data up to SIL3 between FSoE devices. FSoE Frames are cyclically transferred via a subordinate fieldbus that is not included in the safety considerations, since the subordinated fieldbus can be regarded as a black channel. The FSoE Frames exchanged between two communication partners are regarded as process data by the subordinated fieldbus.

FSoE uses a unique master/slave relationship between the **FSoE Master** and a **FSoE Slave**; it is called FSoE Connection (Figure 1). In the FSoE Connection, each device only returns its own new message once a new message has been received from the partner device. The complete transfer path between FSoE Master and FSoE Slave is monitored by a separate watchdog timer on both devices, and in each FSoE Cycle.

The FSoE Master can handle more than one FSoE Connection to support several FSoE Slaves.

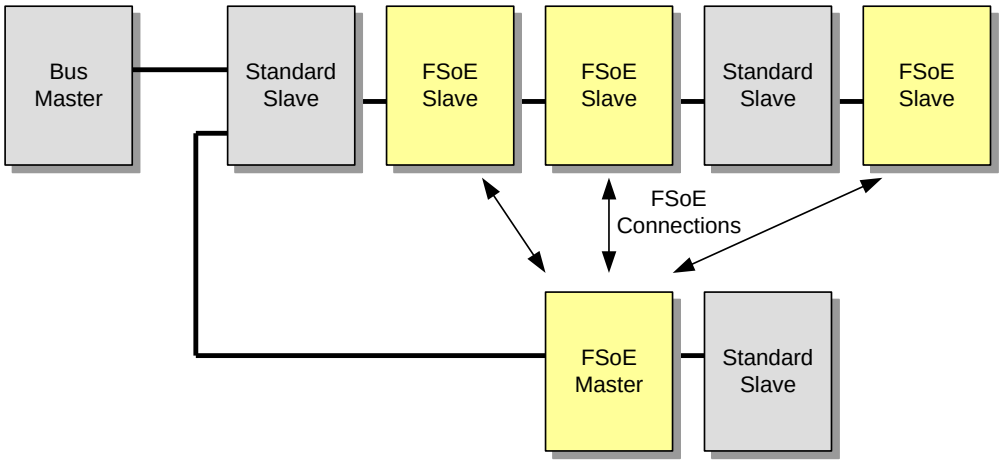

Figure 1: FSoE system architecture

The integrity of the safety data transfers is ensured as follows:

- session-number for detecting buffering of a complete startup sequence;
- sequence number for detecting interchange, repetition, insertion or loss of whole messages;
- unique connection identification for safely detecting misrouted messages via a unique address relationship;
- watchdog monitoring for safely detecting delays not allowed on the communication path
- cyclic redundancy checking for data integrity for detecting message corruption from source to sink.

State transitions are initiated by the FSoE Master and acknowledged by the FSoE Slave. The FSoE state machine also involves exchange and checking of parameter for the communication relation.

The FSoE state machine is a separate state machine and runs on top of the EtherCAT state machine (ESM).

Black channel approach

FSoE protocol is implemented using a black channel approach; there is no safety related dependency to the standard communication interface. The communication interface including controllers, ASICs, links, couplers, etc. remains standard.

The communication path is arbitrary; it can be a fieldbus system, Ethernet or similar paths, fibre optics, copper wires or even wireless transmission. There are no restrictions or requirements on bus coupler or other devices in the communication path.

3.2 Standards & References

Table 1 lists the relevant documents for the Safety over EtherCAT technology.

Table 1: Standards and References

Document	Description	Reference
[1] ETG.5100	**Safety over EtherCAT Specification** FSoE Protocol specification approved by TUV.	Available per email Send request to ETG (info@ethercat.org)
[2] IEC 61784-3	**IEC specification of FSoE protocol** IEC 61784-3: Industrial communication networks - Profiles – Part 3: Functional safety fieldbuses, Defines general requirements for functional safety fieldbuses. Functional Safety Communication Protocol FSCP 12/1 defines the Safety over EtherCAT Technology This part has the same content as ETG.5100.	www.iec.ch
[3] ETG.5120	**Safety over EtherCAT Specification Enhancements** This specification contains enhancements of the Safety over EtherCAT protocol. These enhancements are part of the Safety over EtherCAT specification and shall be taken into account for device implementation.	www.ethercat.org/ETG5120
[4] FSoE License	**Safety over EtherCAT License** Safety over EtherCAT is registered trademark and patented technology licensed by Beckhoff Automation GmbH. Beckhoff has assured that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. **The license is available free of charge.** Beckhoff offers a license agreement.	Send request to ETG (info@ethercat.org) Send request to Beckhoff (your local representative)
Safety over EtherCAT Conformance Test		
[5] ETG.9100	**Safety over EtherCAT Policy** Rules and Requirements for using and implementing Safety over EtherCAT technology. The objective of this specification is to maintain the integrity of both EtherCAT and Safety over EtherCAT (FSoE). All requirements defined in the ETG.9100 that are applicable for a device shall be fully met.	www.ethercat.org/ETG5100
[6] ETG.7100 series	**FSoE Conformance Test Specification** The ETG.7100 series consists of following parts:	www.ethercat.org → Downloads
[7] ETG.7100.1	**ETG.7100.1: General Requirements** defines the FSoE Test in which the conformance of the FSoE Device under Test with the FSoE Specification is tested	www.ethercat.org → Downloads
[8] ETG.7100.1a	**ETG.7100.1a: FSoE Conformance Test Tool Change Request Template** Change Requests to the FSoE Conformance Test procedure or the FSoE CTT shall use this template	www.ethercat.org → Downloads
[9] ETG.7100.2	**ETG.7100.2: FSoE Conformance Test Record** A set of test instructions for the performance of the FSoE Conformance Test and documentation of it at the same time	www.ethercat.org → Downloads
[10] ETG.7100.3	**ETG.7100.3: FSoE Test cases specification** Comprehensive test list for FSoE Master and FSoE Slaves (Excel Sheet) Approved by TUV	Comes with ET9402 FSoE Conformance Test Tool

Document	Description	Reference
[11] ET9402	**FSoE Conformance Test Tool for FSoE Slaves** • Automatic test tool for FSoE Slaves • Mandatory for approval of FSoE Slave devices. (The tool is offered by Beckhoff. Test cases are defined in ETG TWG Safety)	Send request to Beckhoff (your local representative)
Safety over EtherCAT Profile specifications		
[12] ETG.5001.4	**Modular Device Specification – Part 4: MDP Safety Modules Specification** standardized Module Profiles for FSoE digital I/O devices, FSoE Drives and FSoE Master devices	www.ethercat.org/ETG5001
[13] ETG.6100	**Safety over EtherCAT Drive Profile** Profile for adjustable speed electrical power drive systems that are suitable for use in safety-related application PDS(SR) with Safety over EtherCAT protocol	www.ethercat.org/ETG6100
Safety over EtherCAT Training		
[14] FSoE_Seminar.pdf	**Safety over EtherCAT Seminar presentation** • Basic of safety networks and international standards • Safety over EtherCAT technology • Technical implementation aspects • Safety Drive Profile • Benefits for the user	http://www.ethercat.org/download/safety_seminar/default.asp
Important Standard EtherCAT specifications, further standards**:** www.ethercat.org → Downloads		
[15] ETG.1000	**EtherCAT Specification** EtherCAT Data link layer and application layer specification	www.ethercat.org/ETG1000
[16] ETG.2000	**EtherCAT Slave Information (ESI) Schema and Specification** Describes the structure of the EtherCAT slave device description in XML format. FSoE related Parts are included.	www.ethercat.org/ETG2000
[17] ETG.2100	**EtherCAT Network Information (ENI) Schema and Specification** Describes the structure of the EtherCAT network information description in XML format. Parts for Copy Information (Slave-to-Slave communication) are included	www.ethercat.org → Downloads
[18] ETG.2200	**EtherCAT Slave Implementation Guide** describes from a very practical point of view which topics have to be kept in mind for a successful EtherCAT slave implementation	www.ethercat.org/ETG2200

4 Technology Users

According to different use cases different users of the FSoE technology can be distinguished:

- Machine builder
  builds a machine with COTS devices including FSoE devices
- EtherCAT master manufacturer
  vendor of non safety-related control systems (Master and/or IO devices).
  Integration of COTS FSoE Devices in the control architecture is required.
- FSoE device manufacturer
  vendor of safety-related devices with FSoE interface

4.1 Machine builders

A machine builder or system designer who uses devices with the Safety over EtherCAT Technology has the responsibility to perform a safety risk and hazard analysis and classification for his machine and to ensure a continuous safety-chain.

All devices connected to a safety communication system shall fulfill SELV/PELV requirements, which are specified in the relevant IEC standards, such as IEC 60204-1.

The resulting safety-function response time must fit to the application.

4.2 Standard EtherCAT master manufacturer

A vendor of a non safety-related control system (e.g. standard PLC) with an EtherCAT interface (EtherCAT master) can support the usage of FSoE devices within the EtherCAT network. The master acts like a bus master; the FSoE Master is integrated in an FSoE Device that is an EtherCAT slave.

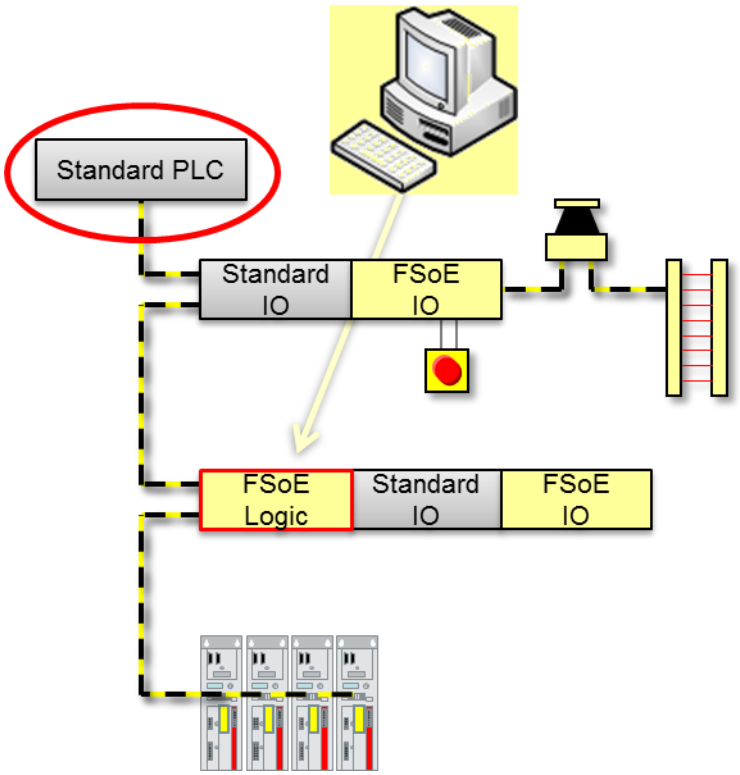

Figure 2: Decentralized Safety Logic approach with Standard PLC

Requirements for the EtherCAT master:

- Support Slave-to-Slave communication
  copy the Safety Frames from the FSoE Master to the FSoE Slaves and vice versa.
  The copy information is part of the ENI [17] file.

- The EtherCAT master should support an interface for the configuration tool of the FSoE Logic device.

4.3 FSoE Device Manufacturer

The device manufacturer has to implement the Safety over EtherCAT Protocol and the safety application according to the related safety standards. It is mandatory that the implementation is approved by a notified body.

The Safety over EtherCAT Policy ETG.9100 [5] defines rules and requirements for using and implementing the Safety over EtherCAT Technology.

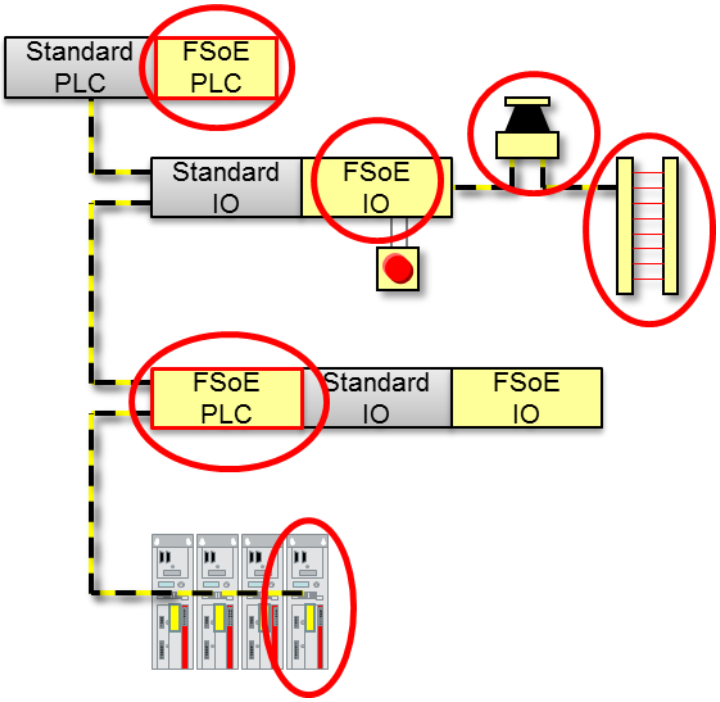

Figure 3: Devices with FSoE interface

The implementation of FSoE devices requires an FSoE license [4], offered by Beckhoff.

See clause 5 for implementation details.

5 Safety over EtherCAT implementation aspects

5.1 FSoE device structure

The ETG.5100 Safety over EtherCAT specification [1] comprises a protocol specification for a safety-related data transfer up to SIL 3. It does not define a particular hardware architecture or software design.

The report of the protocol approval demands an implementation that fulfills the following requirements:

- complete fulfillment of IEC 61508 and IEC 61784-3
- complete fulfillment of the FSoE Protocol Specification (ETG.5100)
- implementation must fulfill the requirements of the claimed safety level and corresponding product specific requirements.

The ETG.9100 FSoE Policy [5] defines further rules and requirements for using and implementing the Safety over EtherCAT Technology. All requirements defined in the ETG.9100 that are applicable for a device shall be fully met.

5.2 Hardware architecture

According to the black channel approach the communication hardware in a device can remain single channel, i.e. the standard EtherCAT Slave Controller (ESC) for the EtherCAT interface can be used.

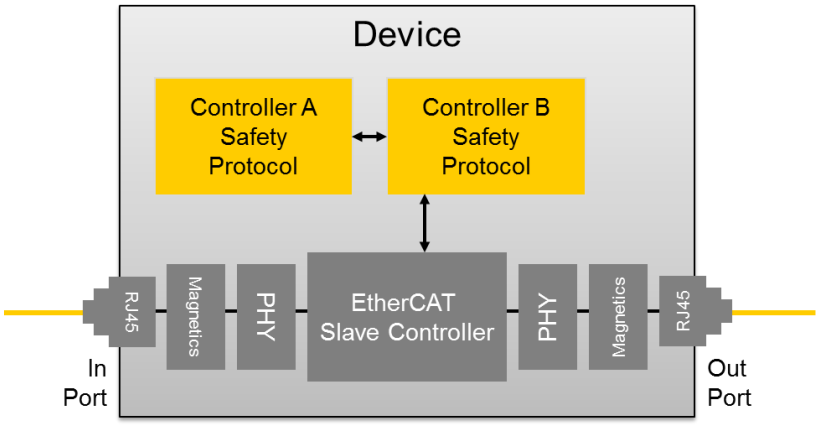

Figure 4: Hardware architecture

EtherCAT or any other communication interface like an internal backbone can be used.

For the processing of the FSoE protocol usually redundant microcontroller architecture is needed. Each microcontroller calculates the Safety over EtherCAT protocol; the results are cross-checked.

5.3 Software architecture

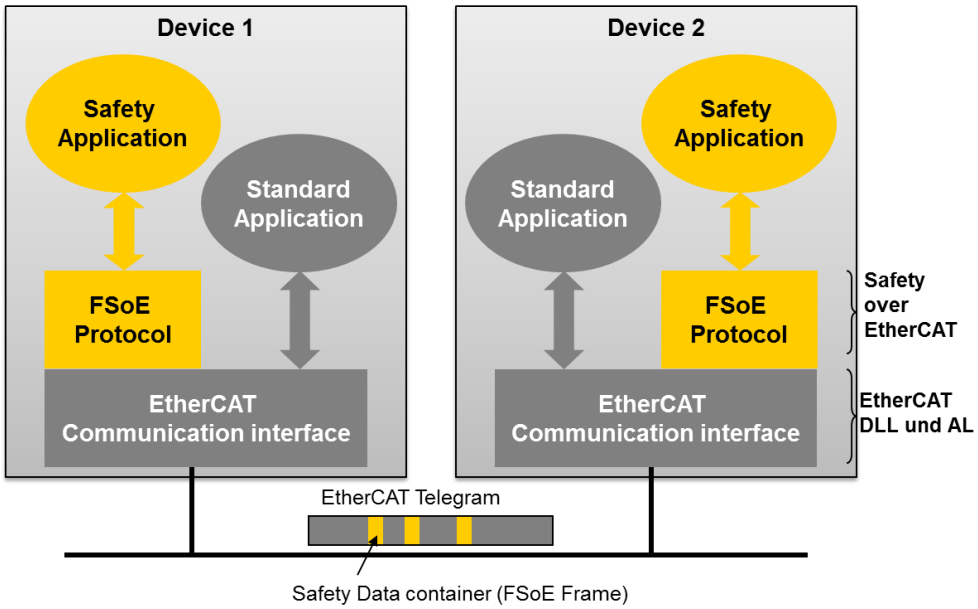

Figure 5: Software architecture

The FSoE protocol is processed upon the application layer of the communication interface.

For a safety-related software environment several self-test functions (e.g. memory tests, controller tests and peripheral tests) must be performed to detect dangerous errors. These requirements are outside the scope of the FSoE protocol – see IEC 61508 or appropriate product specific standards.

5.4 Safety Manual

Implementers shall supply a safety manual, but meeting the following points at a minimum:

- The safety manual shall inform the users of constraints for calculation of system characteristics.
- The safety manual shall inform the users of their responsibilities of proper parameterization of the device.

In addition to the requirements of this clause the safety manual shall follow all requirements in the FSoE Policy and IEC 61508.

6 Device approval

For the device approval the procedure and requirements described in the Safety over EtherCAT Policy [5] and in the FSoE Conformance Test specification ETG.7100 [6] shall be fulfilled.

ETG.9100 FSoE Policy [5] defines the overall assessment and approval procedure of FSoE Devices according to Figure 6.

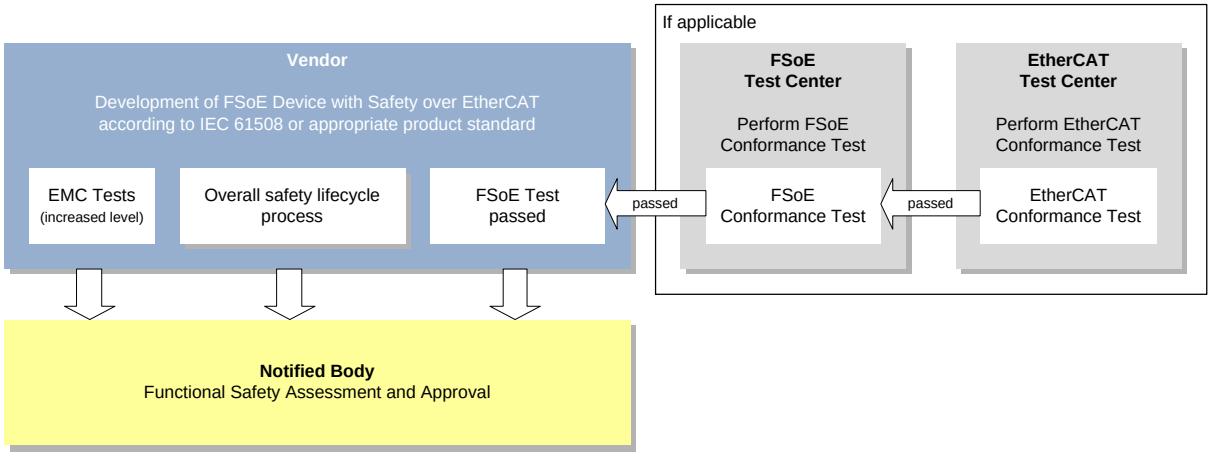

Figure 6: FSoE Device assessment and approval

6.1 FSoE Conformance Test

The FSoE Conformance Test is defined in ETG.7100 series [6].

For the approval of a conformant implementation of the FSoE protocol the FSoE test case specification ETG.7100.3 [10] is available. The TUV has approved the test cases.

Test cases for an FSoE Slave have been implemented based on the EtherCAT Conformance Test Tool. The implementation is approved by TUV, too.

The test cases for an FSoE Master have not yet been implemented within the Conformance Test Tool. The implementation of test cases for an FSoE Master specific development must be done manually or according to the developments' test environment.

Table 2 shows different possible test executions, which can be used depending on the device type.

Table 2: Depending on the device Type different test executions are possible

	FSoE Master	**FSoE Slave**	
EtherCAT Master	ETG.7100.3 Master tests incorporated in vendors' test environment	ETG.7100.3 Slave tests incorporated in vendors' test environment	
EtherCAT Slave	ETG.7100.3 Master tests incorporated in vendors' test environment	**FSoE CTT for FSoE Slave devices**	
Non-EtherCAT device	ETG.7100.3 Master tests incorporated in vendors' test environment	ETG.7100.3 Slave tests incorporated in vendors' test environment	

7 Implementation Support

7.1 Workshop and Training

Table 3: Workshop and Training

Description	Reference
EtherCAT technology basics for developers TR8110 One day training class handles: • EtherCAT Basics • Slave Structure • Physical Layer • Device Model • Data Link Layer • Distributed Clocks (DC) • Application Layer • Slave Information Interface (EEPROM) • Device Profiles • EtherCAT Slave Information (ES) file • Tools (Configuration Tool, Monitor, …) • EtherCAT Master • Standard & References	www.ethercat.org → Events
Safety over EtherCAT seminar Decision makers, product managers as well as engineers who are involved in their companies' safety product strategy are invited to this seminar. A comprehensive overview about up-to-date requirements for safety machine architectures with the focus on safety communication with the Safety over EtherCAT protocol is given. Usually each 6 month, one day before the ETG Technical Committee Meeting.	www.ethercat.org → Events
1 Day implementation Workshop Introduction to the FSoE technology, 1 day seminar	Send request to ETG (info@ethercat.org)

7.2 Technical Support

Technical support throughout the development process is provided by the EtherCAT Technology Group predominantly by the headquarters in Germany, but also by the various ETG offices worldwide (depending on local capacity). If you need direct contact, please address your specific question to ETG (info@ethercat.org).

7.3 Step by Step Implementation for an FSoE Device Manufacturer

The following approach of implementing FSoE for an existing EtherCAT slave device might look like:

- Get an overview of the Safety over EtherCAT Technology
  www.ethercat.org/safety
- Attend the Safety over EtherCAT Seminar
  (for dates see www.ethercat.org → Events)
- Download all relevant documentation (see Table 1)
- In addition take care at least of the following Safety standards:
  - IEC 61508 and IEC 61784-3
- Get a free of charge Safety over EtherCAT license (send email to info@ethercat.org)
- Use FSoE Conformance Test cases for the Conformance Test and FSoE CTT for FSoE Slave devices to test your device with the latest FSoE features implemented.

- System test, interoperability test (e.g. at an EtherCAT Plug Fest)
- FSoE Slave devices shall be tested in a FSoE Test Center
- Approve your integration by a notified body (see 6)

8 Frequently asked questions

1. Do I need a redundant EtherCAT Interface within my Safety over EtherCAT device?
No.
The Safety over EtherCAT protocol is implemented using a black channel approach; there is no safety related dependency to the standard communication interface. The communication interface such as controllers, ASICs, links, couplers, etc. remains unmodified.

2. Do I need redundant controller architecture for my Safety over EtherCAT device?
Usually yes.
Usually means, that common solutions use two Microcontrollers. In fact this is not demanded by the Safety over EtherCAT Specification. A protocol implementation must fulfill following requirements:

- complete fulfilment of IEC 61508 and IEC 61784-3
- complete fulfilment of the FSoE Protocol Specification
- complete fulfilment of the claimed safety level and corresponding product specific requirements.

3. Can I use Safety over EtherCAT via other communication systems than EtherCAT?
Yes.
Since the beginning in 2005 Safety over EtherCAT was open and independent of the underlying bus system. The communication path is arbitrary; it can be EtherCAT, a fieldbus system, Ethernet or similar paths, fibre optics, copper wires or even wireless transmission. There are no restrictions or requirements on bus coupler or other devices in the communication path.

4. Is there a certified Safety over EtherCAT stack available?
Yes,
within the ETG there are service providers available offering per-certified FSoE protocol stacks and safety development services.
ETG does not offer such kind of stack, because the Safety over EtherCAT specification is quite lean and the protocol state machine is well defined. The experience shows that an implementation can be done in very short time – often shorter than to adapt a certified stack that is not changeable in existing software architectures.

5. Is a Safety over EtherCAT conformance test available?
Yes.
For Safety over EtherCAT devices a Safety over EtherCAT test case specification exists and is approved by TUV. For Safety over EtherCAT Slaves those test cases are available for the EtherCAT Conformance Test Tool (CTT) so that an automated test can be performed. In general the automated test of a master stack is much more complex due to the flexible master configuration. Therefore the available test case specification can be integrated in the vendors test environment for the Master approval.
The Safety over EtherCAT Policy ETG.9100 includes the overall Test procedure for a device approval.

6. Do I need an approval by a notified body (e.g. TUV, BGIA) for my Safety over EtherCAT device?
Yes.
The development of a device using the Safety over EtherCAT technology shall be assessed. The device approval includes a passed EMC report, the Safety over EtherCAT conformance approval and the overall safety lifecycle process approval according to IEC 61508 or appropriate product standards. The assessment shall be done by a notified body.

7. Do I need to perform an official test at an FSoE Test Center for my device release?
Yes, for FSoE Slave devices.
For EtherCAT slave devices the FSoE device approval shall further include a passed test in an official EtherCAT Test Center. Precondition for the FSoE Conformance Test is a valid EtherCAT Conformance Certificate for the FSoE Device.
All tests performed by the FSoE Test Center are available for preparation in-house.

8. Why do I need a license to use the Safety over EtherCAT protocol within my device?
Safety over EtherCAT is a technology that is used by many device manufacturers. For such a technology the most important issue is compatibility! This ensures the safety integrity according to the approved Safety over EtherCAT specification but also – and this is of same importance – interoperability in the field. With the license the device manufacturer gets the right to implement the technology – but he has to do this compatible to the specification. This rule is part of the license agreement.
Machine builders and control system providers who use off-the-shelf Safety over EtherCAT devices do not need a license.

9. How can I get and use the Safety over EtherCAT logo?
The Safety over EtherCAT logo can be obtained by the ETG Headquarters. The Safety over EtherCAT logo shall only be used in accordance with the EtherCAT marking rules as published by the ETG.

10. I'm an EtherCAT master vendor. How can I support Safety over EtherCAT devices?
If you just want to support off-the-shelf Safety over EtherCAT devices in the EtherCAT segment you do not need any safety-related implementation in the master. Safety over EtherCAT Masters with an EtherCAT slave interface are available and can be used as safety logic devices.
Only slave-to-slave communication must be supported by the EtherCAT Master to route the safety frames from the Safety over EtherCAT Master to the Safety over EtherCAT Slaves and vice versa.

11. I'm a machine builder. Do I need a license to use Safety over EtherCAT devices?
No.
You can use off-the-shelf Safety over EtherCAT devices in the machine without a license.
You have to take care of the resulting Safety Integrity Level (SIL) or Performance Level (PL). Relevant standards (IEC 62061, ISO 13849) or product standards as well as compliance to other relevant standards, like national and international legal requirements (e.g. Directive of machinery, OSHA, UL etc.) must be fulfilled, of course.