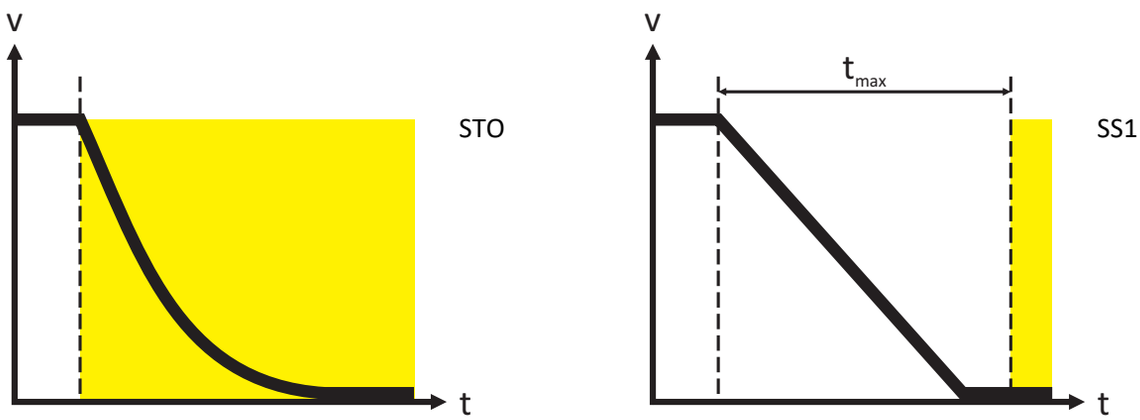
Safety over EtherCAT®



SY6 safety module
Manual

en-US
03/2020
ID 442744.03

STÖBER

Table of contents

03/2020 | ID 442744.03

03/2020 | ID 442744.03

03/2020 | ID 442744.03

1 Foreword

The SY6 safety module adds the **Safe Torque Off (STO)** and **Safe Stop 1 (SS1)** safety functions, both described as standard in DIN EN 61800-5-2, to STOBER drive controllers of the SC6 or SI6 series.

STO prevents an electrical rotating magnetic field, needed for the operation of synchronous or asynchronous motors, from being generated in a drive controller immediately once the safety function has been activated. In the case of SS1-t, the switch-off happens after a configurable amount of time.

For a combination consisting of a drive controller and SY6 safety module, the STO and SS1 safety functions are actuated via EtherCAT (FSoE).

SY6 is a fast and wear-free fully electronic solution. The safety module is designed so that regular system tests that interrupt operation are eliminated. In practical terms, this means increased availability of machines and systems. The often complex planning and documentation of function tests are also eliminated.

Drive controllers with an integrated safety module can be used in systems with high safety requirements up to SIL 3, PL e, category 4. Compliance with standard requirements has been certified by an independent testing institute as part of type-examination.

Drive controllers of the SC6 and SI6 series successfully passed the EtherCAT as well as Fail Safe over EtherCAT (FSoE) Conformance Test. There, the communication interface was tested to ensure the reliability and function of the lower-level communication regardless of vendor.

03/2020 | ID 442744.03

2 User information

This documentation provides all information on the intended use of the drive controller in combination with the SY6 safety module.

2.1 Storage and transfer

As this documentation contains important information for handling the product safely and efficiently, it must be stored in the immediate vicinity of the product until product disposal and be accessible to qualified personnel at all times.

Also pass on this documentation if the product is transferred or sold to a third party.

2.2 Described product

This documentation is binding for:

Drive controllers of the SC6 or SI6 series in combination with the SY6 safety module and DriveControlSuite (DS6) software in V 6.4-E or later and associated firmware in V 6.4-E or later.

2.3 Timeliness

Check whether this document is the latest version of the documentation. We make the latest document versions for our products available for download on our website:
http://www.stoeber.de/en/downloads/.

2.4 Original language

The original language of this documentation is German; all other language versions are derived from the original language.

2.5 Limitation of liability

This documentation was created taking into account the applicable standards and regulations as well as the current state of technology.

STOBER shall assume no responsibility for damage resulting from failure to comply with the documentation or from use that deviates from the intended use of the product. This is especially true for damage caused by individual technical modifications to the product or projecting and operation of the product by unqualified personnel.

03/2020 | ID 442744.03

2.6 Formatting conventions

Orientation guides in the form of signal words, symbols and special text markups are used to emphasize specific information so that you are able identify it in this documentation quickly.

2.6.1 Use of symbols

Safety instructions are identified with the following symbols. They indicate special risks when handling the product and are accompanied by relevant signal words that express the extent of the risk. Furthermore, useful tips and recommendations for efficient, error-free operation are specially highlighted.

ATTENTION!

Notice

This indicates that damage to property may occur

- if the stated precautionary measures are not taken.

⚠ CAUTION!

Caution

This word with a warning triangle indicates that minor personal injury may occur

- if the stated precautionary measures are not taken.

⚠ WARNING!

Warning

This word with a warning triangle means there may be a considerable risk of fatal injury

- if the stated precautionary measures are not taken.

⚠ DANGER!

Danger

This word with a warning triangle indicates that there is a considerable risk of fatal injury

- if the stated precautionary measures are not taken.

Information

Information indicates important information about the product or serves to emphasize a section in the documentation that deserves special attention from the reader.

2.6.2 Markup of text elements

Certain elements of the continuous text are distinguished as follows.

Important information	Words or expressions with a special meaning
Interpolated position mode	Optional: File or product name or other name
Detailed information	Internal cross-reference
http://www.samplelink.com	External cross-reference

Software and other displays

The following formatting is used to identify the various information content of elements referenced by the software interface or a drive controller display, as well as any user entries.

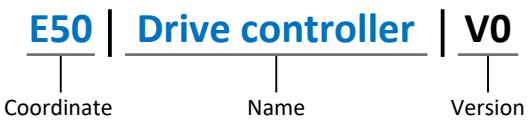
Main menu Settings	Window names, dialog box names, page names or buttons, combined proper nouns, functions referenced by the interface
Select `Referencing method A`	Predefined entry
Save your `<own IP address>`	User-defined entry
EVENT 52: COMMUNICATION	Displays (status, messages, warnings, faults) for status information referenced by the interface

Keyboard shortcuts and command sequences or paths are represented as follows.

[CTRL], [CTRL] + [S]	Key, shortcut
Table > Insert table	Navigation to menus/submenus (path specification)

Interpretation of parameter identification

Parameter identification consists of the following elements, where short forms are also possible, i.e. only specifying a coordinate or the combination of coordinate and name.



2.6.3 Mathematics and formulas

The following signs are used to represent mathematical relationships and formulas.

-	Subtraction
+	Addition
×	Multiplication
÷	Division
| |	Amount

03/2020 | ID 442744.03

2.7 Trademarks

The following names used in connection with the device, its optional equipment and its accessories are trademarks or registered trademarks of other companies:

EtherCAT®, Safety over EtherCAT®, TwinCAT®	EtherCAT®, Safety over EtherCAT® and TwinCAT® are registered trademarks of patented technologies licensed by Beckhoff Automation GmbH, Verl, Germany.

All other trademarks not listed here are the property of their respective owners.

Products that are registered as trademarks are not specially indicated in this documentation. Existing property rights (patents, trademarks, protection of utility models) are to be observed.

3 General safety instructions

There are risks associated with the product described in this documentation that can be prevented by complying with the described warning and safety instructions as well as the included technical rules and regulations.

3.1 Standards

The following standards are relevant to the product specified in this documentation:

- DIN EN ISO 13849-1:2016
- DIN EN ISO 13849-2:2013
- DIN EN 61800-5-2:2017-11
- DIN EN 61508-x:2011
- DIN EN 60204-1:2007
- DIN EN 62061:2016
- IEC 61784-3:2010

Subsequent references to the standards do not specify the respective year in order to improve readability.

3.2 Qualified personnel

In order to be able to perform the tasks described in this documentation, the persons instructed to perform them must have the appropriate professional qualification and be able to assess the risks and residual hazards when handling the products. For this reason, all work on the products as well as their operation and disposal may be performed only by professionally qualified personnel.

Qualified personal are persons who have acquired authorization to perform these tasks either through training to become a specialist and/or instruction by specialists.

Furthermore, valid regulations, legal requirements, applicable basic rules, this documentation and the safety instructions included in it must be carefully read, understood and observed.

03/2020 | ID 442744.03

3.3 Intended use

The SY6 safety module can be combined with STOBER drive controllers of the SC6 or SI6 series.

If a drive controller with the integrated SY6 safety module is used in a safety-related application, the safety module must be activated by a safety relay or a safety controller.

⚠ DANGER!

Electrical voltage! Risk of fatal injury due to electric shock!

An active STO safety function only means that generation of the rotating magnetic field at the motor has been interrupted. The motor may still be energized with dangerous high voltages.

- Make sure that persons cannot come into contact with conductive parts.
- If the supply voltage must be switched off, observe the requirements of DIN EN 60204-1.

Improper use

The safety module may not be operated outside of the drive controller or operated not in compliance with the applicable technical specifications.

Information

An emergency off in accordance with DIN EN 60204-1 is not possible with the SY6 safety module!
Observe this standard regarding the difference between **emergency off** and **emergency stop** in conjunction with **Safe Torque Off**.

Modification

As the user, you may not make any technical or electrical modifications to the SY6 safety module. Any removal of the module from the drive controller as well as any attempt at repair or replacement is prohibited.

Maintenance

The safety module does not require maintenance.

Product life span

A drive controller with integrated safety module must be taken out of operation 20 years after the production date. The production date of a drive controller is found on the accompanying nameplate.

3.4 Decommissioning

In safety-oriented applications, note the mission time T_M = 20 years in the safety-relevant key performance indicators.

4 Safety module SY6

The SY6 safety module adds the STO (Safe Torque Off) and SS1 (Safe Stop 1) safety functions to the drive controller. The module prevents the formation of a rotating magnetic field in the power unit of the drive controller and, in the event of an error or by external request, switches the drive controller to the STO state immediately or after a time delay (SS1-t).

Features

- Possible safety functions:
  - Safe Torque Off – STO in accordance with DIN EN 61800-5-2
  - Stop category 0 in accordance with DIN EN 60204-1
  - Safe Stop 1 (time-delayed) – SS1-t in accordance with DIN EN 61800-5-2
  - Stop category 1 in accordance with DIN EN 60204-1
- Activation of the safety functions using Safety over EtherCAT (FSoE)
- STO switch-off time: < 50 ms
- Wear-free

Certifications in accordance with DIN EN 61800-5-2 and DIN EN ISO 13849-1

- Safety Integrity Level (SIL) 3
- Performance Level (PL) e
- Category 4

5 System design and function

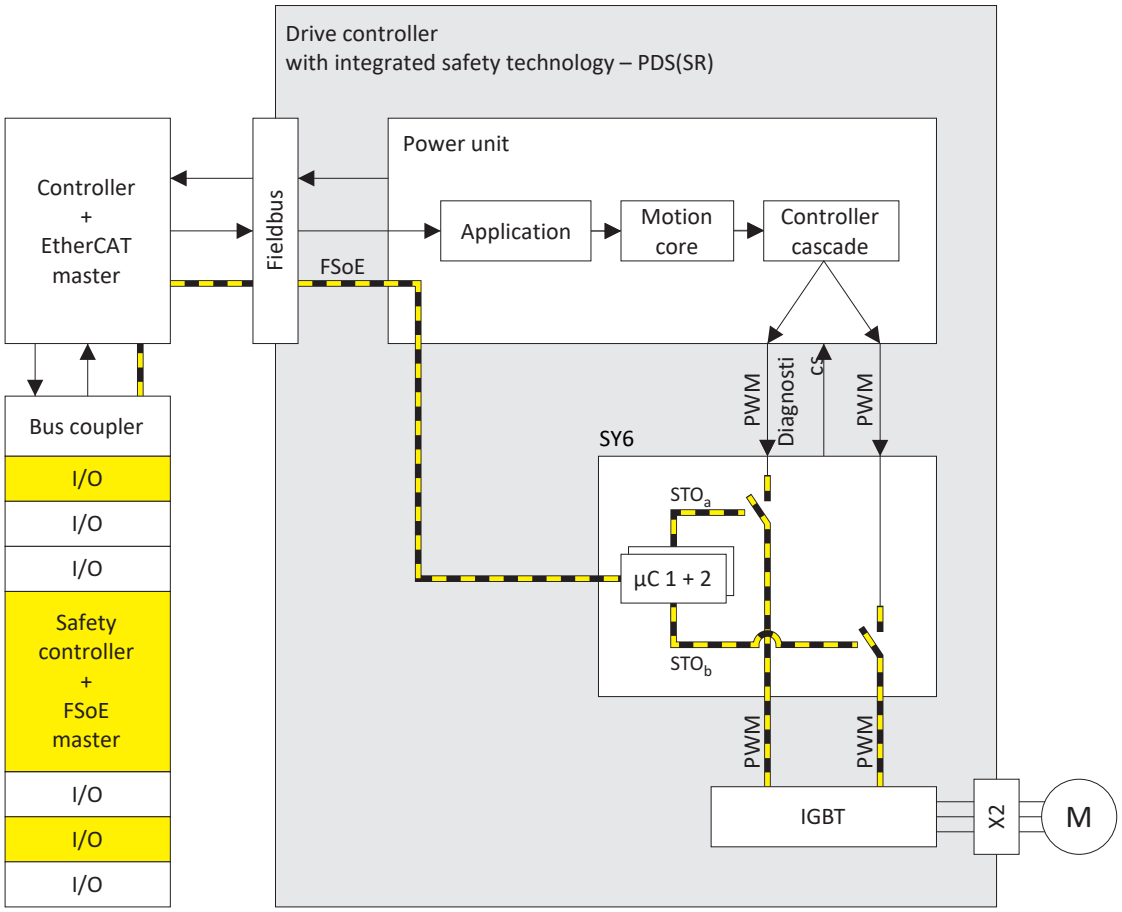


Fig. 1: Components of the FSoE-based safety concept

System components

Central components of the FSoE-based safety concept are:

- Drive controller with integrated SY6 safety module
  ... for implementing the STO and SS1-t safety functions
- Controller (PLC) with integrated EtherCAT master
  -... for organizing all network communication
- Bus coupler (EtherCAT coupler)
  ... as a connector between the controller and safety controller; the bus coupler passes messages from the safety controller to the EtherCAT master
- Safety controller (S-PLC) with integrated FSoE master
  ... for FSoE communication and logic gate links between FSoE nodes; the safety controller includes certified safety function modules that can be configured to the specific application using suitable automation software
- Safety terminals with digital failsafe inputs and outputs
  ... for the connection of 24 V_{DC} safety sensors such as emergency stop or position switches, light barriers, pressure mats etc.
- FSoE protocol
  ... for the transmission of safety-related data
- EtherCAT
  ... as the underlying fieldbus system

Function

The control unit of the drive controller generates pulse patterns (PWM) to produce a rotating magnetic field at the IGBT module in the power unit. This rotating magnetic field is necessary for operating synchronous and asynchronous motors.

If the safety function is not active, the SY6 safety module allows for the generation of a rotating magnetic field in the power unit; the connected motor can create a rotating magnetic field. If the safety function is active, SY6 disables the generation of the rotating magnetic field in the power unit and the drive controller cannot generate any torque in the connected motor.

The SY6 safety module implements an FSoE slave. It exchanges control and status information with the FSoE master via the EtherCAT master in accordance with the black channel principle. The slave extracts the safety-related data, checks it for plausibility and enables or disables the two safety channels in the power unit.

The STO and SS1-t safety functions relate to the device and are not axis-specific. On double-axis controllers, both axes are brought to a safe state at the same time.
An activated SS1 cannot be interrupted.

⚠ WARNING!

Increased overrun distance! Residual motion!

The safety module cannot prevent a failure of the functional part of the drive controller (e.g. during a controlled stop) while the SS1-t safety function is executed. Therefore, SS1-t cannot be used if this failure could cause a dangerous situation in the end application. Observe this during project configuration.

In the event of an error in the power unit of the drive controller, static energization of the motor is possible despite active STO. In this case, the motor shaft can move by an angle of up to 360° ÷ (p × 2).

03/2020 | ID 442744.03

6 Technical data

The transport, storage and operating conditions of the safety module can be found in the technical data of the drive controller (see the chapter Detailed information [▶ 48]).

The following table contains the variables relevant to safety technology for the SY6 module.

SIL CL	3
SIL	3
PL	e
Category	4
PFHD	5×10^{-9} [1/h]
Mission time	20 years
STO switch-off time	< 50 ms
SS1 delay time	10 – 655350 ms (± 1%)

Tab. 1: SY6 – Safety-related variables

7 What you should know before commissioning

The following chapters provide a quick introduction to the structure of the program interface and accompanying window designations as well as relevant information about generally saving your project configuration.

7.1 Program interfaces

The following chapters include an overview of the program interfaces for the described software components.

7.1.1 DS6: Structure of the program interface

The DriveControlSuite commissioning software (DS6) offers a graphic interface that you can use to project, parameterize and start up your axis model quickly and efficiently.

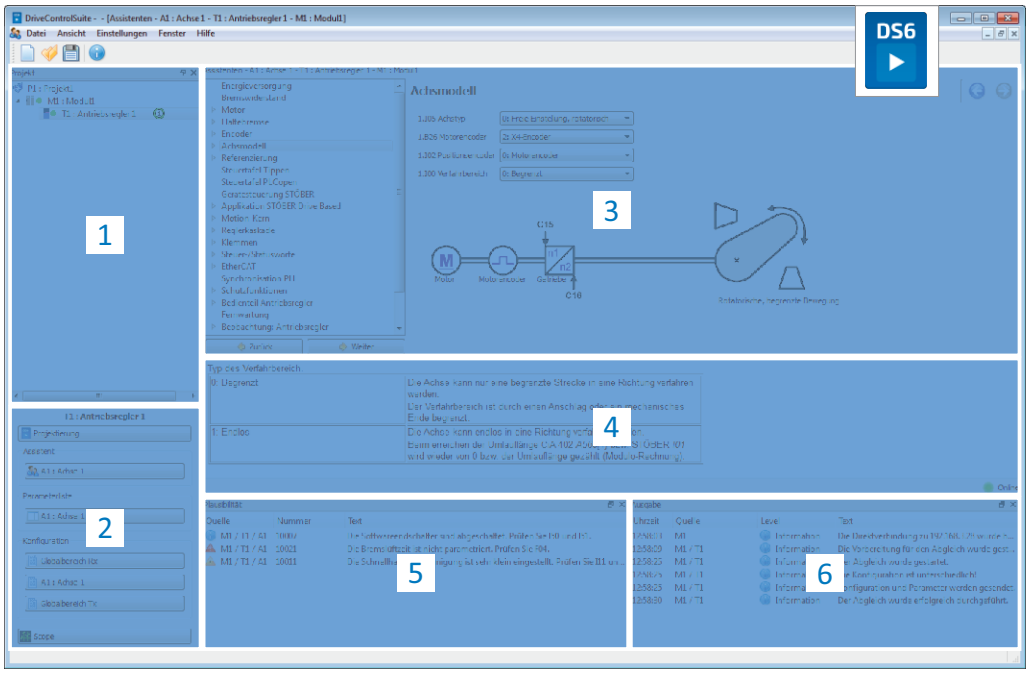


Fig. 2: DS6: Program interface

1 Project tree
2 Project menu
3 Workspace
4 Parameter description
5 Parameter check
6 Messages

7.1.2 TwinCAT 3: Structure of the program interface

In TwinCAT 3, you operate your EtherCAT system using TwinCAT XAE. The following graphic shows the interface elements relevant to this documentation.

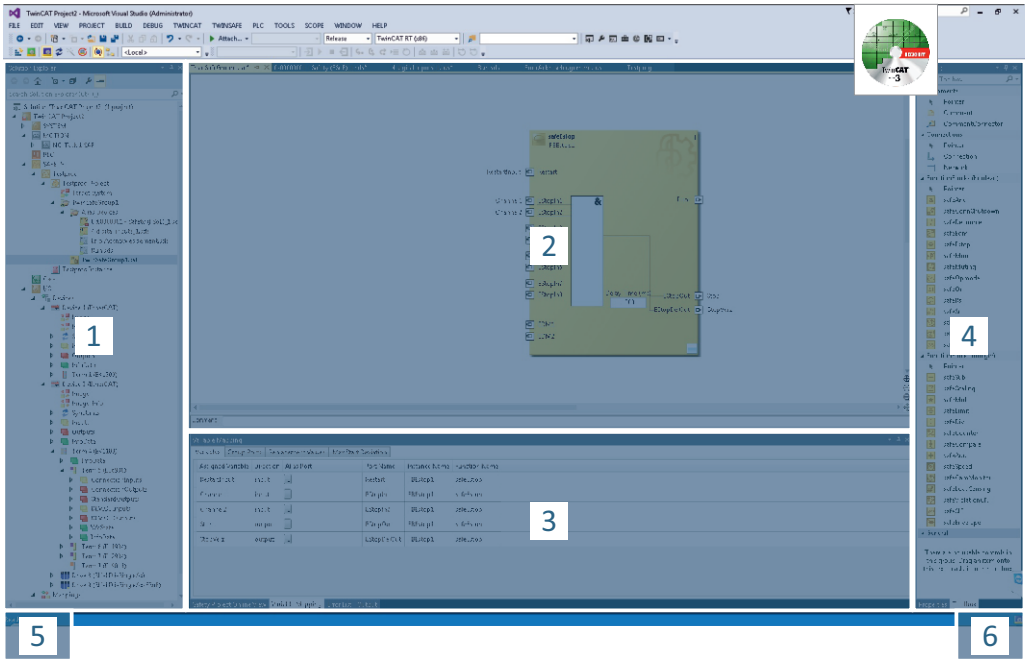


Fig. 3: TwinCAT 3 (TwinCAT XAE) – program interface

1 Solution explorer
2 Main window
3 Message view
4 Toolbox
5 Event display
6 Status display (configuration, run, connection setup/timeout mode)

7.2 Power-loss protected storage

All project configurations, parameterizations and related changes to parameter values are in effect after transmission to the drive controller, but are not yet stored in non-volatile memory.

You save the data using the Save values function in parameter A00 (Project menu > Wizards area > Projected axis > Save values wizard).

Only then is the data stored with power-loss protection.

8 Commissioning

The following chapters cover commissioning your drive controller and SY6 safety module using the STOBER DriveControlSuite software and the TwinSAFE configurator of TwinCAT 3 from Beckhoff Automation GmbH & Co. KG.

We put forward the following system environment as an example so that you can follow the individual commissioning steps exactly:

- Beckhoff CX2030 – CPU base module (controller, EtherCAT master)
- Beckhoff TwinSAFE EL6900 logic terminal (safety controller, FSoE master)
- Beckhoff EK1100 bus coupler (EtherCAT bus coupler)
- Beckhoff TwinSAFE 4-channel EL1904 digital input terminal (digital terminal with 4 failsafe inputs)
- Beckhoff TwinCAT 3 automation software: TwinCAT System Manager (TwinSAFE configurator), TwinCAT XAE
- STOBER drive controller of the SC6 or SI6 series with integrated SY6 safety module
- STOBER DriveControlSuite commissioning software in version 6.4-D or later

Information

The ability to commission the drive controller and SY6 safety module in combination with the STOBER MC6 motion controller and STOBER AutomationControlSuite (AS6) development environment is in the pipeline.

Commissioning is divided into the following steps:

1. SY6 safety module
   Enter a valid FSoE address.
2. Observe the time setting recommendations for the following configuration.
3. DriveControlSuite
   Configure all drive controllers including safety modules, device control systems, process data for fieldbus communication and the axes of your drive system in DriveControlSuite. Generate an ESI file then transmit your project configuration to the drive controller of the system network.
4. TwinCAT
   Make the generated ESI file available to TwinCAT 3. Next, map your entire hardware environment and configure it. Then activate your system and check the TwinSAFE communication of the connected device.

8.1 SY6: Assigning the FSoE address

In order to be able to identify the SY6 safety module in the FSoE network, you must assign it a unique address in the FSoE network. The address is based on values from the DIP switches that are switched to ON (for detailed information, see the chapter SY6: Assigning the FSoE address [▶ 44]).

Information

Note that the drive controller must be switched off before you enter the FSoE address using the DIP switches. The drive controller has to be restarted to apply the address.

8.2 Recommended time settings

In order to ensure that the power unit is not switched off and the axis movement is continues to be controlled by the drive controller in case of a quick stop with subsequent STO (stop category 1 in accordance with DIN EN 60204-1 or Safe Stop 1 (SS1) in accordance with DIN EN 61800 5 2) or in case of an interruption of the communication during controlled braking, the delay time that occurs during a quick stop (quick stop time) is taken into account when parameterizing the SS1 delay time and FSoE watchdog time.

Quick stop time

The quick stop time is a result of the application-specific quick stop deceleration and maximum velocity. In applications in accordance with CiA 402, parameterize the quick stop deceleration in A578 Quick stop deceleration. Parameterize the maximum velocity in I10 Maximal speed.

SS1 delay time

Set a larger value for T_SS1 in the FSoE master than for the resulting quick stop time. The reserve should generally be 10% and should not fall below 50 ms. You can check the SS1 delay time in S593 SS1 time until STO.

FSoE watchdog time

Set a larger value for the watchdog time in the FSoE master than for the resulting quick stop time plus PDO timeout (A258 EtherCAT PDO-Timeout). The reserve should generally be 10% and should not fall below 100 ms. You can check the watchdog time in S27 FSoE watchdog time. In TwinCAT 3, a global watchdog time of 100 ms is set by default. More information on the watchdog time can be found in the chapter FSoE watchdog time [▶ 45].

8.3 DS6: Configuring the drive controller

Project and configure all drive controllers for your drive system using DriveControlSuite.

8.3.1 Initiating the project

In order to be able to configure all drive controllers and axes of your drive system using DriveControlSuite, you must record them as part of a project.

8.3.1.1 Projecting the drive controller and axis

Creating a new project

1. Start DriveControlSuite.
2. Click Create new project.

⇨ The project configuration window opens and the Drive controller button is active.

Projecting the drive controller

1. Properties tab:
   Establish the relationship between your circuit diagram and the drive controller to be projected in DriveControlSuite.
   Reference: Specify the reference code (equipment code) of the drive controller.
   Designation: Give the drive controller a unique name.
   Version: Version your project configuration.
   Description: If necessary, specify additional supporting information, such as the change history of the project configuration.
2. Drive controller tab:
   Select the series and device type of the drive controller.
3. Option modules tab:
   Safety module: Select the SY6 module.
4. Device controller tab:
   Device controller: Select the device controller that defines the underlying activation signals for the drive controller.
   Process data Rx, Process data Tx: Select EtherCAT Rx and EtherCAT Tx for transmitting the EtherCAT process data.

03/2020 | ID 442744.03

Projecting the axis

1. Click on Axis 1.
2. Properties tab:
   Establish the connection between your circuit diagram and the axis to be projected in DriveControlSuite.
   Reference: Specify the reference code (equipment code) of the axis.
   Designation: Give the axis a unique name.
   Version: Version your project configuration.
   Description: If necessary, specify additional supporting information, such as the change history of the project configuration.
3. Application tab:
   Select the desired controller-based application.
   If you are working with hardware and software products from Beckhoff, we recommend CiA 402 (incremental version).
4. Motor tab:
   Select the type of motor operated using this axis. If you are working with motors from third-party suppliers, enter the accompanying motor data at a later time.
5. Repeat steps 2 – 4 for the 2nd axis (only for double-axis controllers).
6. Confirm with OK.

8.3.2 Parameterizing general EtherCAT settings

✓ You have projected the SY6 safety module and the device control with the EtherCAT Rx and EtherCAT Tx process data as part of drive controller and axis project configuration.

1. Highlight the relevant drive controller in the project tree and click on the first projected axis in the project menu > Wizard area.
2. Select the EtherCAT wizard.
3. A213 Fieldbus scaling:
   Leave the default setting at 1: Native (values are passed unchanged).
4. A258 EtherCAT PDO-Timeout:
   In order to be able to detect a communication failure, monitor the arrival of cyclical process data by defining a PDO timeout.
   Permitted value range: 0 – 65535 ms.
   Please note:
   0 and 65535 = Monitoring is inactive
   1 to 65531 = Monitoring is active
   65532 = Monitoring is active but the loss of an individual data packet is ignored
   65533 = Monitoring is active but the loss of 3 data packets in a row is ignored

8.3.3 Configuring PDO transmission

PDO channels are able to transmit control and status information in real time as well as actual and set values from an EtherCAT master to EtherCAT slaves and vice versa.

PDO communication allows for several PDO channels to be operated simultaneously per transmission and sending direction. The channels for axes A and B each include a PDO with a defined sequence of up to 24 parameters to be transmitted. These are free to be configured in any way. One channel is reserved for FSoE communication and is parameterized automatically.

In order to guarantee error-free communication between the controller and drive controller, STOBER offers an application-dependent pre-assignment of the channels which can be changed at any time.

8.3.3.1 Adapting RxPDO

✓ You have configured the global EtherCAT settings.

1. Highlight the relevant drive controller in the project tree and click on the first projected axis in the project menu > Wizard area.
2. Select the EtherCAT wizard > Received process data RxPDO.
3. Check the default settings and/or configure the process data according to your requirements.
   A225[0] – A225[23], A226[0] – A226[23]:
   Parameters whose values are received by the drive controller from the controller. The position of the parameters provides information about the associated receiving sequence.

8.3.3.2 Adapting TxPDO

✓ You have configured the global EtherCAT settings.

1. Highlight the relevant drive controller in the project tree and click on the first projected axis in the project menu > Wizard area.
2. Select the EtherCAT wizard > Transmitted process data TxPDO.
3. Check the default settings and/or configure the process data according to your requirements.
   A233[0] – A233[23], A234[0] – A234[23]:
   Parameters whose values the respective drive controller sends to the controller. The position of the parameters provides information about the associated transmission sequence.

03/2020 | ID 442744.03

8.3.4 Transmitting and saving the configuration

In order to transmit and save the configuration to one or more drive controllers, your PC must be located in the same network with the respective devices.

Transmitting the configuration

✓ The drive controllers are ready for operation.

1. In the project tree, highlight the module under which you have recorded your drive controller and click Assignment and live firmware update in the project menu.
   ⇨ The Add connection window opens. All drive controllers found via IPv4 limited broadcast are displayed.
2. Direct connection tab > IP address column:
   Activate the IP address in question or activate all listed using the context menu. Confirm your selection with OK.
   ⇨ The Assignment and live firmware update window opens. All drive controllers connected through the previously selected IP addresses are displayed.
3. Select the drive controller to which you would like to transfer the configuration. Change the selection of transmission type from Read to Send.
4. Change the selection Create new drive controller:
   Select the configuration that you would like to transfer to the drive controller.
5. Repeat steps 3 and 4 for all other drive controllers to which you would like to transfer your configuration.
6. Online tab:
   Click on Establish online connections.

⇨ The configurations are transferred to the drive controllers.

Information

During the search, all drive controllers within the broadcast domain are found via IPv4 limited broadcast.

Prerequisites for finding a drive controller in the network:

- Network supports IPv4 limited broadcast
- All drive controllers are in the same subnet (broadcast domain)

Saving the configuration

✓ You have successfully transferred the configuration.

1. Assignment and live firmware update window:
   Click on Save values (A00) ....
   ⇨ The Save values (A00) window opens.
2. Click on Start action.
   ⇨ The configuration is saved.
3. Close the Save values (A00) window.
4. Assignment and live firmware update window:
   Click on Restart (A09) ....
   ⇨ The Restart (A09) window opens.
5. Click on Start action.
6. Confirm the safety instruction with OK.
   ⇨ The Restart (A09) window closes.
   ⇨ The fieldbus communication and connection to DriveControlSuite are interrupted.
   ⇨ The drive controllers restart.

8.3.5 Creating and saving ESI files

The functions and properties of the STOBER drive controllers are described in the form of various objects and collected in an ESI file.
In order to map and configure one or more drive controllers in the network, generate an ESI for your configured application and make it available to TwinCAT System Manager in the directory specified below.

Information

Be aware that TwinCAT can only read in one ESI file per drive controller series.
A new ESI file must be generated and made available to TwinCAT after each change to the configuration.

✓ You have configured the PDO transmission.

1. Highlight the relevant drive controller in the project tree and click on the first projected axis in the project menu > Wizard area.
2. Select the EtherCAT wizard.
3. Click on Create ESI.
   ⇨ The Write ESI file dialog box opens.
4. Save the XML file in the directory C:\TwinCAT\IO\EtherCAT (default installation).

⇨ TwinCAT reads in the file when the program is restarted.

8.4 TwinCAT 3: Putting the EtherCAT system into operation

TwinCAT 3 offers the option of mapping your hardware environment using TwinCAT XAE.
Parameterize all necessary bus parameters in the software automatically via hardware scan. Next, configure a customized safety program that manages the STO and SS1 safety request signals.
Predefined function blocks that connect you to the desired inputs and outputs are available for this purpose. The configuration of a safety program is described below using the example of a safeEstop (Emergency Stop) function block.
You will transmit the finished safety program to the FSoE master as the last step.

Be aware that it must be possible to obtain unique identification of all FSoE system devices in the EtherCAT network by means of a customized FSoE address (adjustment via DIP switches). Enter the FSoE addresses before installing and networking the individual devices and terminals.

Information

Always perform the steps included in the following chapters in the specified order!

Some parameters of the DriveControlSuite are interdependent and do not become accessible to you until you have first configured certain settings. Follow the steps in the specified sequence so that you can finish the parameterization completely.

03/2020 | ID 442744.03

8.4.1 Activating the EtherCAT master

✓ You have already projected all drive controllers of your system using DriveControlSuite and transmitted the project configuration to the individual drive controllers. The EtherCAT master is connected to the network, all safety components have an FSoE address and are energized, and the infrastructure is ready for operation. You have saved the generated ESI file in the specified directory. The ESI files for Beckhoff devices are already stored in the TwinCAT system.

1. Start TwinCAT XAE.
   ⇨ The stored ESI file is read in upon program start and the main window of TwinCAT System Manager opens. Start page tab is active.
2. Select File > New > Project.
   ⇨ The New Project dialog box opens.
3. Select Installed > Templates > TwinCAT Projects > TwinCAT XAE Project (XML format).
4. Name, Location, Solution name:
   Label the project and enter a save location and an internal project name.
5. Close the dialog box.
6. If the runtime package (EtherCAT master) and TwinCAT XAE have been installed on the same PC, they are connected to each other automatically. Continue to step 12.
7. If the runtime package (EtherCAT master) and TwinCAT System Manager have been installed on different computers, you must connect them to each other.
   Click on the <Local> list field in the TwinCAT XAE toolbar and select Choose Target System.
   ⇨ The Choose Target System dialog box opens.
8. Click on Search (Ethernet).
   ⇨ The Add Route dialog box opens.
9. Click on Broadcast Search.
   ⇨ All available control systems are listed.
10. Highlight the desired controller, activate the IP Address option and confirm with Add Route.
    ⇨ The Logon Information dialog box opens.
11. Enter the following information for a new device (TwinCAT standard access) and confirm with OK:
    User name: `Administrator`
    Password: `1`
12. Close the dialog box.
13. Choose Target System dialog box:
    Highlight the previously selected EtherCAT master and confirm with OK.
    ⇨ The EtherCAT master is saved as the target system.
14. In order to be able to configure the EtherCAT system online, you must activate Config mode for the TwinCAT XAE software.
    Select the menu TWINCAT > Restart TwinCAT (Config mode).
    ⇨ The Restart TwinCAT System in Config Mode dialog box opens.
15. Confirm with OK.

⇨ The EtherCAT master is saved as the target system, TwinCAT XAE is in Config mode.

8.4.2 Scanning the hardware environment

If all system components are connected to the EtherCAT network and the network is energized, it is possible to scan for connected devices automatically. In this scenario, TwinCAT XAE searches for connected devices and terminals and integrates them into the existing project in accordance with their configuration entries in the accompanying ESI files.

If the actual EtherCAT infrastructure is not available, i.e. you are configuring in offline mode, you must map and project all connected devices manually in TwinCAT XAE. You can get more detailed information on this in the online help tool of the TwinCAT XAE software.

✓ You have activated Config mode.

1. In the solution explorer, navigate to I/O > Devices > Context menu Scan.
   ⇨ TwinCAT XAE scans the EtherCAT system for the EtherCAT master.
   The ... new I/O devices found dialog box opens.
2. Activate the EtherCAT master in question and confirm with OK.
   ⇨ The EtherCAT master is created in the solution explorer under I/O > Devices as a device (EtherCAT).
   The Scan for boxes? dialog box opens.
3. Confirm with Yes.
   ⇨ TwinCAT XAE scans the EtherCAT system for the EtherCAT slaves.
   The EtherCAT drive(s) added dialog box opens.
4. Append linked axis to:
   If a NC or CNC function is required, activate the desired option and confirm with OK.
   ⇨ The bus coupler EtherCAT slaves (EK1100 terminal) along with the FSoE master (EL6900 terminal), secure inputs (EL1904 terminals) and the drive controller are created in the solution explorer.
   The Activate Free Run dialog box opens.
5. In order to shift the system components during configuration into free run mode and thereby enable verification of the signal exchange, confirm with Yes.

⇨ EtherCAT master and slaves are created in TwinCAT XAE.

8.4.3 Configuring the TwinCAT SAFETY project

A TwinCAT SAFETY project consists of a TwinSAFE group with alias devices, i.e. the hardware components of your system and the actual SAFETY element along with accompanying function blocks that represent safety-related logic. The function blocks contain parameters that must be adapted according to the application.

The first step is to create a SAFETY project along with alias devices and then configure the function block safeEstop, for example.

8.4.3.1 Creating the TwinCAT SAFETY project

1. In the solution explorer, navigate to SAFETY > Context menu Add New Item.
   ⇨ The Add New Item dialog box opens.
2. Highlight the entry TwinCAT Default Safety Project.
3. Name:
   Label the SAFETY project and confirm with Add.
   ⇨ The TwinCAT Safety Project Wizard dialog box opens.
4. Internal Project Name:
   If necessary, enter an internal project name and confirm with OK.
   ⇨ The SAFETY project with the name you provided, a target system and a TwinSAFE group are created in the solution explorer. The TwinSAFE group already includes a folder for the alias devices to be created; the alias device ErrorAcknowledgement.sds is available as a reset input by default.
5. In order to define the FSoE master as the target system, select the newly created SAFETY project in the solution explorer and double click on Target System.
6. Main window > Physical Device:
   Click on the appropriate icon.
   ⇨ The Choose physical terminal for mapping dialog box opens.
7. Terminal:
   Highlight the EL6900 FSoE master and confirm with OK.
8. Main window > Hardware Address:
   The FSoE address of the FSoE master has been read into TwinCAT XAE automatically.
9. In order to save the project, select the menu FILE > Safe Selected Items.

⇨ The SAFETY project is created and the FSoE master is configured as the associated target system.

8.4.3.2 Creating alias devices

The hardware required for the SAFETY project is incorporated into the TwinSAFE group as the respective alias device.

1. In the solution explorer, navigate to your SAFETY project > TwinSafeGroup1 > Alias Devices > Context menu Add > New Item.
   ⇨ The Add New Item dialog box opens.
2. Create an alias device as an input for the start of the TwinSAFE group.
   Select Installed > Standard > 1 Digital Input (Standard).
3. Name:
   Label the alias device with RUN and confirm with Add.
4. In the solution explorer, reselect the folder Alias devices > Context menu Add > New item.
5. Create an alias device for the secure inputs (terminal EL1904).
   Select Safety > EtherCAT > Beckhoff Automation GmbH > 4 digital inputs.
6. Name:
   If necessary, label the device and confirm with Add.
7. In the solution explorer, reselect the folder Alias devices > Context menu Add > New item.
8. Create an alias device for the drive controller with the integrated SY6 safety module.
   Select Safety > EtherCAT > STOEBER ANTRIEBSTECHNIK GmbH & Co. KG > 0xB1EC5956 - Safety (FSoE).
9. Name:
   If necessary, label the device and confirm with Add.

⇨ The named hardware components are created as alias devices for the TwinSAFE group in the solution explorer.

8.4.3.3 Assigning alias devices and entering FSoE addresses

Assign the created alias devices to the individual hardware components of your system and enter the accompanying FSoE addresses.

1. In the solution explorer, navigate to your SAFETY project > TwinSafeGroup1 > Alias Devices and double click on ErrorAcknowledgement.sds.
2. Main window > Full name:
   Click on the appropriate icon.
   ⇨ The Attach Variable Standard in Var 1 (output) dialog box opens.
3. Show Variables:
   In order to display all devices, activate the option Used and unused.
4. Show Variables:
   In order to display the standard inputs, uncheck the checkbox Exclude other devices.
5. Select the desired standard input for the reset of the TwinSAFE group and confirm with OK.
6. In the solution explorer, select the folder Alias Devices and double click on RUN.sds.
7. Main window > Full name:
   Click on the appropriate icon.
   ⇨ The Attach Variable Standard in Var 1 (output) dialog box opens.
8. Select the desired standard input for starting the TwinSAFE group and confirm with OK.
   ⇨ The hardware standard inputs for resetting and starting the TwinSAFE group are linked with the accompanying alias devices.
9. In the solution explorer, select the folder Alias Devices and double click on 4 digital inputs_1.sds.

10. Main window > Linking tab > Physical Device:
    Click on the accompanying icon.
    ⇨ The Choose physical channel dialog box opens.
11. Select the first module of the EL1904 terminal and confirm with OK.
    ⇨ Terminal EL1904 is linked with the corresponding alias device.
12. Linking tab > FSoE address:
    The FSoE address of the EL1904 terminal has been read into the TwinCAT XAE Dip Switch field during the hardware scan automatically. In order to apply the address, click on the accompanying icon.
    ⇨ The address is taken from the Dip switch field and input into the FSoE address field.
13. In the solution explorer, select the folder Alias Devices and double click on 0xB1EC5956 – Safety(FSoE).sds.
14. Main window > Linking tab > Physical Device:
    Click on the accompanying icon.
    ⇨ The Choose physical channel dialog box opens.
15. Select the first module of the drive controller with the integrated SY6 safety module and confirm with OK.
    ⇨ The drive controller is linked with the corresponding alias device.
16. Linking tab > FSoE address:
    The FSoE address of the safety module has been read into the TwinCAT XAE Dip switch field during the hardware scan automatically. In order to apply the address, click on the accompanying icon.
    ⇨ The address is taken from the Dip switch field and input into the FSoE address field.
17. In order to configure the SS1 delay time after which the STO function is triggered automatically, select in the main window > Safety Parameters tab > T_SS1 parameter.
18. T_SS1:
    Double click on the entry.
    ⇨ The Set Value dialog window opens.
19. Dec.:
    Parameterize the parameters for the desired SS1 delay time and confirm with OK.
    ⇨ Be aware that the value configured here is multiplied by a factor of 10 within the system (example: T_SS1 = 100, equals 1000 ms).
    T_SS1 is displayed in parameter S593 SS1 time until STO of DriveControlSuite.

⇨ The hardware components are linked with the corresponding alias devices and the FSoE addresses are entered.

8.4.3.4 Configuring the function block

Using the safeEstop function block, configure an emergency stop button that is connected to the secure input terminal EL1904 via two NC contacts.

8.4.3.4.1 Creating a function block and assigning signal sources

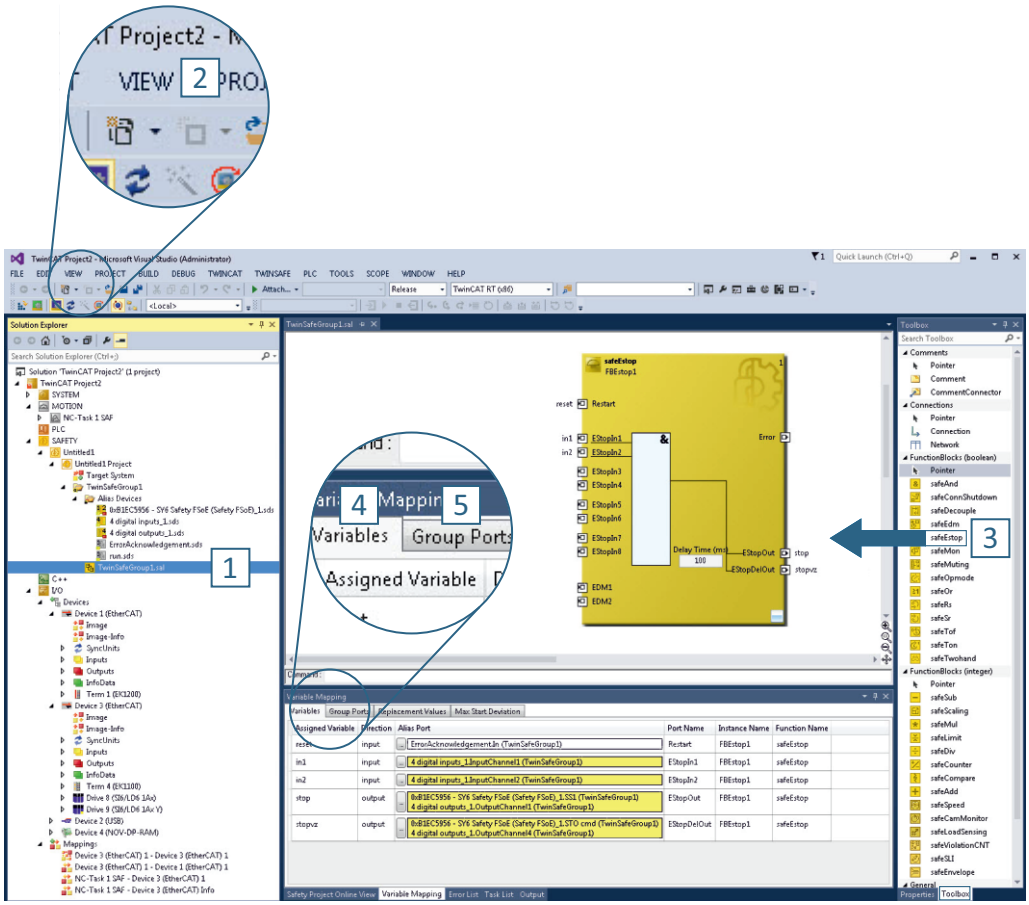


Fig. 4: TwinCAT 3 – Configuring safeEstop function block and assigning signal sources

1. In the solution explorer, navigate to your SAFETY project > TwinSafeGroup1 and double click on TwinSafeGroup1.sal (1).
2. VIEW menu (2):
   Open the Toolbox view.
3. Toolbox > Function blocks (boolean) (3):
   Drag and drop the safeEstop function block into the main window > TwinSafeGroup1.sal tab.
4. Click to the left of the icon for Restart.
5. Label the variable with `RestartInput`.
6. Click to the left of the icons for both EStopIn1 and EStopIn2.
7. Label the variables with `Channel1` and `Channel2`.
8. Click to the right of the icons for both EStopOut and EStopDelOut.
9. Label the variables with `Stop` and `StopVerz`.

10. Delay time (ms):
    Enter the SS1 delay time configured in T_SS1 .
    Be aware that the value in this entry field is NOT multiplied by a factor of 10 within the system.
    ⇨ All necessary variables for configuring the safeEstop function block have been created.
11. In the message view, switch to the Variable Mapping tab > Variables subtab (4).
    ⇨ The previously defined variables for the function block are listed in the Assigned Variable column.
12. RestartInput variable > Alias Port column:
    Click on the accompanying button.
    ⇨ The Map to dialog box opens.
13. Usage:
    Activate the Used and unused option.
14. Assign the ErrorAcknowledgement alias device to the variable and confirm with OK.
15. Variables subtab > Variables Channel1 and Channel2 > Alias port column:
    Click on the accompanying buttons.
    ⇨ The Map to dialog box opens.
16. Assign the alias device 4 digital inputs > Channel1 > InputChannel1 to the variable Channel1 and 4 digital inputs > Channel2 > InputChannel2 to the variable Channel2 and confirm with OK.
17. Variables subtab > Variables Stop and StopVerz > Alias Port column:
    Click on the accompanying buttons.
    ⇨ The Map to dialog box opens.
18. Assign the alias device 0xB1EC5956 - Safety (FSoE) > Channel > SS1 to the variable Stop and the alias device 0xB1EC5956 - Safety (FSoE) > Channel > STO to variable StopVerz, confirm with OK.
    ⇨ All configured variables for the safeEstop function block have been linked to the associated alias devices.
19. Switch to the Group Ports subtab (5).
20. Variables ErrAck and Run/Stop > Alias Port column:
    Click on the accompanying buttons.
    ⇨ The Map to dialog box opens.
21. Usage:
    Activate the Used and unused option.
22. Assign the alias devices ErrorAcknowledgement and RUN of the TwinSAFE group to the variables, respectively, and confirm with OK

⇨ The configured function block is available for download to the FSoE master.

8.4.3.4.2 Transmitting the function block

Validate the configured function block and transmit this to the FSoE master.

1. In the solution explorer, navigate to your SAFETY project > TwinSafeGroup1 and double click on TwinSafeGroup1.sal.
2. Select the menu TWINSAFE > Verify Complete Safety Project.
3. If validation was successful, the status VERIFICATION PROCESS SUCCEEDED is displayed in the left area of the footer of the TwinCAT XAE interface.
4. Select the menu TWINSAFE > Download Safety Project.
   ⇨ The Check if the addresses configured on hardware terminals [...] dialog box opens.
5. Confirm the prompt with Yes.
   ⇨ The Download Project Data > Steps: Login dialog box opens.
   The download to the FSoE master is password-protected.
6. Login area:
   Enter the following information for a new device (TwinCAT standard access) and confirm with Next:
   Username: `Administrator`
   Serial Number: `Serial number of the FSoE master`
   Password: `TwinSAFE`
   ⇨ The Download Project Data > Steps: Download dialog box opens.
7. Begin the download by clicking on Next.
   ⇨ The Download Project Data > Steps: Final Verification dialog box opens.
8. Final Verification area > I have manually verified the data shown [...] confirmation prompt:
   Check the configured data, confirm the confirmation prompt by checking the accompanying checkbox and click on Next.
   ⇨ The Download Project Data > Steps: Activation dialog box opens.
9. Activation area > Password:
   Enter the `TwinSAFE` password again and confirm with Finish.
   ⇨ The function block is transmitted to the FSoE master.
10. Restart the TwinCAT system:
    Select the menu Actions > Set/Reset TwinCAT to Config Mode.
    ⇨ The Restart TwinCAT System in Config Mode dialog box opens.
11. Confirm with OK.

8.4.4 Checking the function of the TwinSAFE group

Check that the TwinSAFE group functions correctly.

1. In the solution explorer, navigate to your SAFETY project > TwinSafeGroup1 and double click on TwinSafeGroup1.sal.
2. Select the menu TWINSAFE > Show Online Data.
   ⇨ The FSoE master (terminal EL6900) is stopped, the safeEstop function block is deactivated, the accompanying status is set to red.
3. Start the TwinSAFE group via `RUN = true`.
4. Unlock the emergency stop button and press the reset button.

⇨ The function block is not active and the TwinSAFE group works correctly.

9 Diagnostics

In the event of fault, the various diagnostic options described below are available.

9.1 LED display

STOBER drive controllers feature diagnostic LEDs that visualize the state of fieldbus communication and the states of the physical connection.

9.1.1 EtherCAT state

There are 2 LEDs on the front of the drive controller that provide information about the connection between EtherCAT master and slave and about the state of the data exchange. This information can also be read out in parameter A255 EtherCAT Device State. If the drive controller includes the SY6 safety module, the STO and SS1 safety functions are activated via EtherCAT FSoE. In this case, an additional LED on the front of the device provides information about the FSoE state.

Fig. 5: LEDs for the EtherCAT state

1 Red: Error

2 Green: Run

Red LED	Conduct	Error	Description
	Off	No Error	No error
	Flashing	Invalid Configuration	Invalid configuration
	Single flash	Unsolicited State Change	The EtherCAT slave changed operating states by itself
	2x flashing	Application Watchdog Timeout	The EtherCAT slave did not receive new PDO data during the configured watchdog timeout

Tab. 2: Meaning of the red LED (error)

Green LED	Conduct	Operating state	Description
	Off	Init	No communication between the EtherCAT master and slave; the configuration starts, saved values are loaded
	Flashing	Pre-operational	No PDO communication; the EtherCAT master and slave exchange application-specific parameters via SDOs
	1x flash	Safe-operational	The EtherCAT slave sends the current actual values to the EtherCAT master, ignores its set values and refers to internal default values
	On	Operational	Normal operation: The EtherCAT master and slave exchange set and actual values

Tab. 3: Meaning of the green LED (Run)

9.1.2 FSoE state

If the drive controller includes the SY6 safety module, the STO and SS1 safety functions are activated via EtherCAT FSoE. In this case, an LED on the front of the device provides information about the state of FSoE communication. This information can also be read out in parameter S20 FSoE status indicator.

Fig. 6: LED for the FSoE state

1 Green: FSoE

Green LED	Conduct	Description
	Off	Initialization
	Flashing	Ready for parameterization
	On	Normal operation
	Single blink	Failsafe command from FSoE master received
	Rapid blinking	Undefined connection error
	Rapid blinking with 1x flash	Error in the safety-related communication settings
	Rapid blinking with 2x flash	Error in the safety-related application settings
	Rapid blinking with 3x flash	Incorrect FSoE address
	Rapid blinking with 4x flash	Prohibited command received
	Rapid blinking with 5x flash	Watchdog error
	Rapid blinking with 6x flash	CRC error

Tab. 4: Meaning of the green LED (FSoE status indicator in accordance with IEC 61784-3)

9.1.3 EtherCAT network connection

The LEDs LA $_{EC}$IN and LA $_{EC}$OUT at X200 and X201 on the top of the device indicate the state of the EtherCAT network connection.

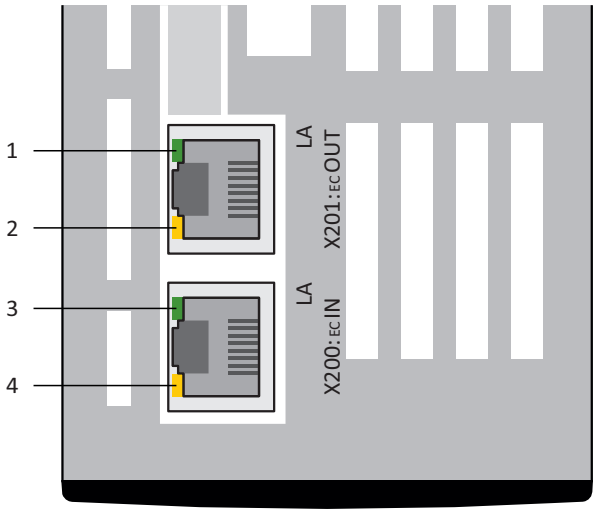


Fig. 7: LEDs for the state of the EtherCAT network connection

1 Green: LA $_{EC}$OUT at X201
2 Yellow: No function
3 Green: LA $_{EC}$IN at X200
4 Yellow: No function

Green LED	Behavior	Description
	Off	No network connection
	Flashing	Active data exchange with other EtherCAT nodes
	On	Network connection exists

Tab. 5: Meaning of the green LEDs (LA)

9.2 Parameters

The following diagnostic parameters are available in the safety technology with drive controllers of the SC6 or SI6 series and SY6 safety module.

9.2.1 E54 | Information safety module | V0

Signifying data of the safety module.

- [0]: Type
- [1]: Hardware version
- [2]: Production number
- [3] – [5]: Reserved
- [6]: Diagnostic code

9.2.2 E67 | STO state | V1

STO state of the safety module:

- [0]: STO was triggered by input signal $STO_a = 0$ or $STO_b = 0$
  - 0: Inactive = not triggered
  - 1: Active = triggered
- [1]: STO was triggered by input signal $STO_a = 0$
  - 0: Inactive = not triggered
  - 1: Active = triggered
- [2]: STO was triggered by input signal $STO_b = 0$
  - 0: Inactive = not triggered
  - 1: Active = triggered

03/2020 | ID 442744.03

9.2.3 S20 | FSoE status indicator | V0

State of the transmission of safety-related data via FSoE.

Corresponds to the FSoE status indicator in accordance with IEC 61784-3.

Standard

- 0 hex = Initialization
  Possible in the FSoE state Pre-Reset
- 1 hex = Ready for parameterization by the FSoE master
  Possible in the FSoE states Reset, Session, Connection, Parameter
- 2 hex = normal operation
  Possible in the FSoE state Process Data
- 3 hex = Failsafe command received by the FSoE master
  Possible in the FSoE state Failsafe Data

Error

- 4 hex = Undefined connection error
  Possible in all FSoE states
- 5 hex = Error in the safety-related communication settings
  Possible in the FSoE state Parameter
- 6 hex = Error in the safety-related application settings
  Possible in the FSoE state Parameter
- 7 hex = Incorrect FSoE address
  Possible in the FSoE state Connection
- 8 hex = Prohibited command received via FSoE communication interface
  Possible in all FSoE states
- 9 hex = Data transmission timeout (watchdog)
  Possible in all FSoE states
- A hex = Inconsistent data transmission (CRC checksum)
  Possible in all FSoE states

9.2.4 S21 | FSoE slave address | V0

Drive controller address (FSoE slave) in the EtherCAT network (prerequisite: FSoE master is active; source: DIP switch).

Address changes are applied when the drive controller is restarted.

9.2.5 S25 | Diagnostic code SY6 | V0

Status byte with diagnostic code of the safety module.

- Bit 0: Internal OSSD channel error
- Bit 1: Reserved
- Bit 2: FSoE communication error
- Bit 3: Reserved
- Bit 4: Overtemperature
- Bit 5: Reserved
- Bit 6: SS1 time
  0 = not running; 1 = running
- Bit 7: STO state
  1 = in safe state

If not otherwise specified: 0 = inactive; 1 = active.

9.2.6 S27 | FSoE watchdog time | V0

Tolerated failure time of FSoE frames for monitoring FSoE communication in the EtherCAT network (use: triggering internal STO; source: FSoE master).

The FSoE monitoring does not depend on PDO monitoring and is specified by the FSoE master (PDO monitoring: A258).

9.2.7 S130 | Run time | V0

Operating time of the safety module.

9.2.8 S544 | Safety controlword | V0

Control byte for FSoE.

Corresponds to the Safety controlword communication object in accordance with ETG.6100.1; object 6620 hex.

- [0]: First byte
  Corresponds to the 1st byte communication object in accordance with ETG.6100.1; subindex 1 hex
  - Bit 0: STO
    0 = Activate STO; 1 = Do not activate STO
  - Bit 1: SS1
    0 = Activate SS1; 1 = Do not activate SS1
  - Bit 2 – 7: Reserved
- [1]: Second byte: Reserved
  Corresponds to the 1st byte communication object in accordance with ETG.6100.1; subindex 2 hex

Enabling the power unit requires that bit 0 and bit 1 are set to 1.

9.2.9 S545 | Safety statusword | V0

Status byte for FSoE.

Corresponds to the Safety statusword communication object in accordance with ETG.6100.1; object 6621 hex.

- [0]: First byte
  Corresponds to the 1st byte communication object in accordance with ETG.6100.1; subindex 1 hex
  - Bit 0: STO
    1 = STO active
  - Bit 1 – 7: Reserved
- [1]: Second byte: Reserved
  Corresponds to the 1st byte communication object in accordance with ETG.6100.1; subindex 2 hex

9.2.10 S593 | SS1 time until STO | V0

SS1 delay time, i.e. the duration between the activation of a time-based SS1 by S544 Safety controlword, bit 1, and the internal triggering of the STO function (unit: 10 ms; source: FSOE master).

Corresponds to the SS1 time until STO communication object in accordance with ETG.6100.1; object 6651 hex.

A change to the SS1 delay time in the FSoE master takes effect and becomes visible in parameter S593 the next time the FSoE master is restarted.

03/2020 | ID 442744.03

9.3 Events

The drive controller has a self-monitoring system that uses test rules to protect the drive system from damage. Violating the test rules triggers a corresponding event. There is no possible way for you as the user to intervene in some events, such as the Short/ground event. In others, you can influence the effects and responses.

Possible effects include:

- Message: Information that can be evaluated by the controller
- Warning: Information that can be evaluated by the controller and becomes a fault after a defined time span has elapsed without the cause being resolved
- Fault: Immediate drive controller response; the power unit is disabled and axis movement is no longer controlled by the drive controller or the axis is brought to a standstill by a quick stop or emergency braking

ATTENTION!

Damage to property due to interruption of a quick stop or emergency braking

If, when executing a quick stop or emergency braking, another fault occurs or a safety function is activated, the quick stop or emergency braking is interrupted. In this case, the machine can be damaged by the uncontrolled axis movement.

Events, their causes and suitable measures are listed below. If the cause of the error is corrected, you can usually acknowledge the error immediately. If the drive controller has to be restarted instead, a corresponding note can be found in the measures.

9.3.1 Event 50: Safety module

The drive controller is interrupted:

- The power unit is disabled and axis movement is no longer controlled by the drive controller
- The brakes are no longer controlled by the drive controller and engage in the event of an inactive release override (F06)

Cause		Check and action
2: Wrong safety module	The projected E53 safety module does not match the E54[0] detected by the system	Check the project configuration and drive controller and correct the project configuration or exchange the drive controller if necessary; fault cannot be acknowledged
3: Internal error	Defective safety module	Exchange drive controller; fault cannot be acknowledged
16: Remove enable!	STO request with active power unit	Only request STO with inactive power unit
		Request Enable-off without quick stop at the same time as the STO request (Drive Based A44)

Tab. 6: Event 50 – Causes and actions

9.3.2 Event 70: Parameter consistency

The drive controller is interrupted:

- The power unit is disabled and axis movement is no longer controlled by the drive controller
- The brakes are no longer controlled by the drive controller and engage in the event of an inactive release override (F06)

Cause		Check and action
15: FSoE watchdog time	Ratio of FSoE watchdog time to EtherCAT PDO timeout too small	Check the FSoE watchdog time in the FSoE master and EtherCAT PDO timeout in the drive controller; if necessary, increase the watchdog time or reduce the PDO timeout (guide value: FSoE watchdog time = EtherCAT PDO timeout + 100 ms; S27, A258)

Tab. 7: Event 70 – Causes and actions

9.4 Parameter from the FSoE master

When establishing a connection, the SY6 safety module expects the following process data units (PDU) in the specified order in the FSoE state parameter from the FSoE master. Process data units are the data packets exchanged between the FSoE master and FSoE slave:

PDU	Byte	Value	Description
PDU 1	SafeData[0]	0x02	2 bytes, length of the communication parameters
	SafeData[1]	0x00	
PDU 2	SafeData[0]	T_WD Low Byte	FSoE watchdog time in ms; Value range: 12 to 65534 ms
	SafeData[1]	T_WD High Byte	
PDU 3	SafeData[0]	0x06	6 bytes, length of the application parameters
	SafeData[1]	0x00	
PDU 4	SafeData[0]	0x01	SY6 identification number; Value = 1 (permanently set!)
	SafeData[1]	0x00	
PDU 5	SafeData[0]	0x00	
	SafeData[1]	0x00	
PDU 6	SafeData[0]	T_SS1 Low Byte	Delay time in s; Value range: 0 to 655.35 s; Resolution: 1 LSB = 10 ms
	SafeData[1]	T_SS1 High Byte	

Tab. 8: Process data units in the FSoE state Parameter

10 More information on FSoE, safety functions and SY6?

This chapter summarizes the important terms, relationships and measures regarding FSoE, the STO and SS1 safety functions and the SY6 safety module.

10.1 FSoE: Fail Safe over EtherCAT

The safety protocol known as **Safety over EtherCAT** (FSoE = Fail Safe over EtherCAT) exists in parallel with the real-time Ethernet system **EtherCAT** for transmitting safety-related messages between FSoE devices in a network. The protocol is TÜV-certified and internationally standardized in accordance with the IEC 61784-3 standard. The design of FSoE is based on the black channel principle.

Secure communication

During each FSoE cycle, a FSoE master sends safety-related data to a FSoE slave and simultaneously starts a watchdog timer. The FSoE slave acknowledges the received data before sending it back to the master and also begins runtime monitoring via a watchdog timer. The master receives and processes the confirmation from the slave and stops the watchdog timer. If the data has been fully processed, the FSoE master generates a new data package.

Unique FSoE addressing

It must be possible to identify each FSoE slave using a unique FSoE address.

The address is assigned to the device using a DIP switch. A valid address is within the address range 1 – 255 (8 bit, 0 address may not be assigned).

10.2 Safety functions

The SY6 safety module supports the Safe Torque Off (STO) and Safe Stop 1 (SS1-t) safety functions. The safety controller must activate the STO as well as the SS1 output of the drive controller if the drive axis is to be moved. If only one of the outputs is configured, the drive controller remains in a safe state (STO active).

The safety functions relate to the device and are not axis-specific. This means that for multi-axis controllers, only the entire drive controller can be set to a safe state, not individual axes.

10.2.1 Safe Torque Off – STO

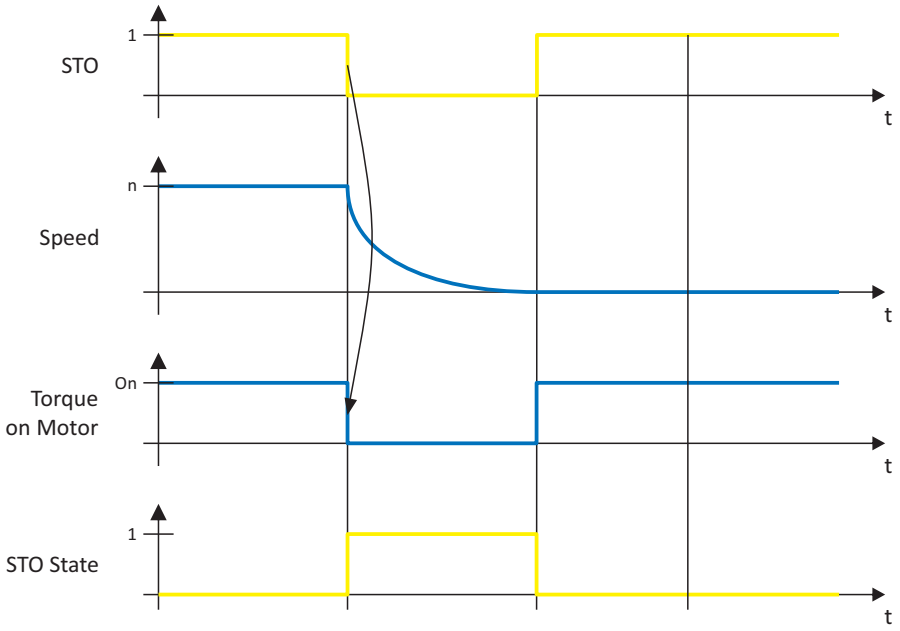


Fig. 8: STO function principle in accordance with ETG.6100.2

STO corresponds to stop category 0 in accordance with EN 60204.

STO is the most fundamental drive-integrated safety function. STO prevents energy that generates torque from acting on the connected motor and prevents unintentional start-up. The goal is to safely eliminate material damage and injuries to persons caused by a rotating, unintentionally activated motor.

The use of STO is always suitable if the motor comes to a standstill on its own in a sufficiently short time period due to load torque or friction or in an environment in which motor coasting does not have safety-related implications.

03/2020 | ID 442744.03

10.2.2 Safe Stop 1 – SS1-t

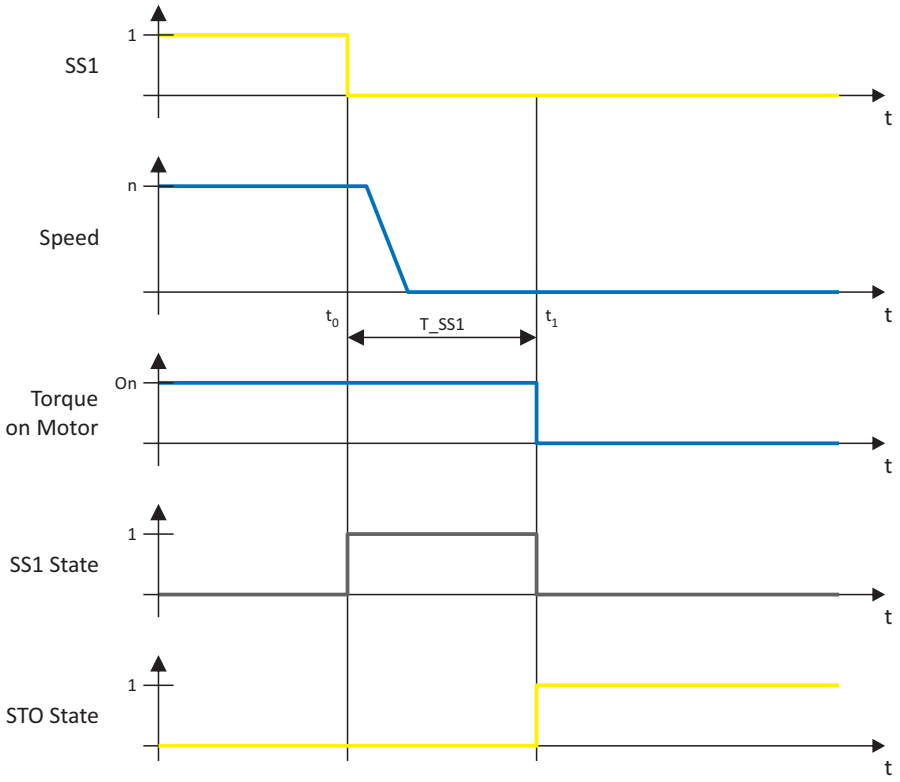


Fig. 9: SS1-t function principle in accordance with ETG.6100.2

t_0	SS1 activation
t_1	STO activation
T_SS1	SS1 delay time

SS1 corresponds to stop category 1 in accordance with IEC 60204-1.

In the case of SS1-t, the switch-off happens after a configurable amount of time.

The SS1-t safety function enables controlled stopping of a motor and switches it to a torque-free state after the parameterized SS1 delay time has passed, i.e. the STO safety function is activated. STO is triggered after a time delay, regardless of whether the motor has already reached a standstill.

Information

Be aware that the drive controller continues to follow the set values of the controller during the SS1 delay time, which enables controlled stopping in multi-axis applications.

The SS1 delay time T_SS1 is a safety-related parameter configured in the automation software and transmitted to the FSoE master. Upon initialization of the FSoE protocol, the value of this parameter is transferred from the safety controller to the drive controller and displayed in DriveControlSuite via parameter S593 SS1 time until STO.

10.3 SY6: Assigning the FSoE address

In order to be able to identify the safety module in the FSoE network, you must assign it an FSoE address from the address range 1 – 255 manually using a DIP switch. An address of 0 is invalid, i.e. the value is ignored if an address of 0 is assigned and the SY6 remains in the STO state.

Information

Note that the drive controller must be switched off before you enter the FSoE address using the DIP switches. The drive controller has to be restarted to apply the address.

FSoE address input using a DIP switch

The DIP switch for entering the address is located on the top of the drive controller. The address is based on the values from the DIP switches that are switched ON. The following graphic shows the safety module along with the DIP switches with the values 2 and 8; the associated FSoE address is 10.

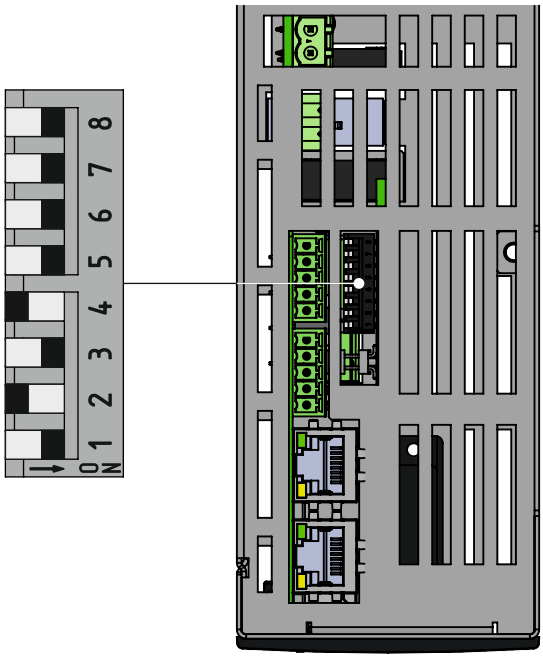


Fig. 10: SY6 – DIP switches

Switch number	1	2	3	4	5	6	7	8
Value – FSoE address	1	2	4	8	16	32	64	128

Tab. 9: DIP switches and FSoE addresses

Checking the FSoE address in SY6

You can verify the FSoE address you have entered for the safety module using the parameter S21 FSoE slave address of DriveControlSuite.

10.4 Safety system time

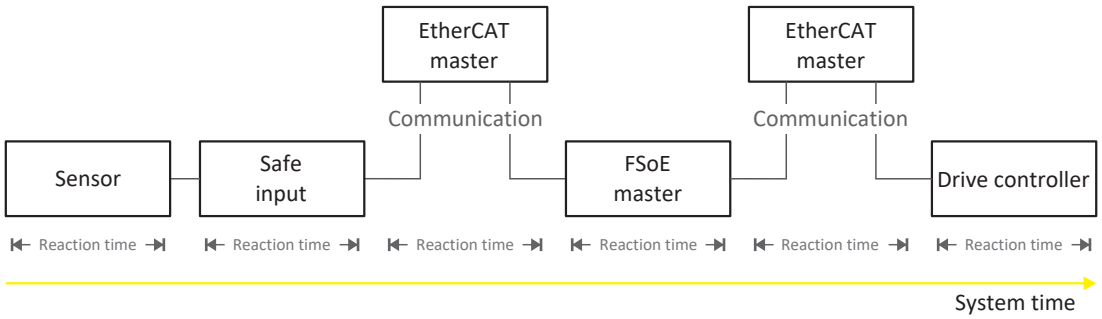


Fig. 11: Reaction times and safety system time

STO system time is understood as the time span from the request for safe switch-off (STO) at a sensor until the actual safe switch-off at the EtherCAT connection of the drive controller.

The system time depends on the response times of the individual system components and the communication and transmission times in the EtherCAT group.

The accompanying processes are:

- Sensor:
  Providing the STO request signal
- Safety terminal (safe input):
  Detecting the STO request signal
- EtherCAT master:
  Transmitting the state of the safe input to the FSoE master
- FSoE master:
  Evaluating the STO request signal
- EtherCAT master:
  Transmitting the STO request signal to the drive controller
- Drive controller:
  Activating and switching off STO (STO switch-off time); this process is divided into the following:
  - EtherCAT processing time in the control unit
  - Transfer time of the data packet to the SY6 safety module
  - SY6: Duration for evaluating the data packet
  - Switch-off time of the power unit

10.5 FSoE watchdog time

In order to detect possible faults, the communication between FSoE master and slave is monitored by a FSoE watchdog. Once a FSoE frame has been sent, the master as well as slave start a watchdog. If the master or slave receive no corresponding response message before the watchdog time runs out, the respective device switches into a safe state. The watchdog time is taken into account when calculating the worst case response time.

The watchdog time is parameterized individually for each slave in the FSoE master.

In TwinCAT 3, a global watchdog time of 100 ms is set by default. If you would like to change this default time, switch to the properties of the respective alias devices of a TwinSAFE group for TwinCAT 3.

11 Appendix

11.1 Supported communication objects

11.1.1 ETG.6100.3 Safety over EtherCAT Drive Profile: 6600 hex – 67FF hex

The following table includes the supported communication objects of the standardized ETG.6100.3 Safety over EtherCAT Drive Profile and their mapping to the corresponding STOBER-specific parameters.

Index	Subindex	TxPDO	RxPDO	Name	Comment
6600 hex	0 hex	—	—	Time unit	Unit: 10 ms
6620 hex				Safety controlword	Array
6620 hex	0 hex	—	—	Highest subindex supported	Number of array elements: 2
6620 hex	1 hex	—	—	Safety controlword, 1st byte	S544[0]
6620 hex	2 hex	—	—	Safety controlword, 2nd byte	S544[1]; no function
6621 hex				Safety statusword	Array
6621 hex	0 hex	—	—	Highest subindex supported	Number of array elements: 2
6621 hex	1 hex	—	—	Safety statusword, 1st byte	S545[0]
6621 hex	2 hex	—	—	Safety statusword, 2nd byte	S545[1]; no function
6640 hex	0 hex	—	—	STO command supported	Function is supported = 1
6641 hex	0 hex	—	—	STO restart acknowledge	STO restart without acknowledge = 0
6650 hex	0 hex	—	—	SS1 command supported	Function is supported = 1
6651 hex	0 hex	—	—	SS1 time to STO	S593, unit defined in object 6600 hex

Tab. 10: ETG.6100.3 communication objects: 6600 hex – 67FF hex

11.1.2 ETG.5001.4 Safety over EtherCAT: E000 hex – EFFF hex

The following table includes the supported communication objects of the standardized ETG.5001.4 Safety over EtherCAT profile.

Index	Subindex	TxPDO	RxPDO	Name	Comment
E901 hex				FSoE connection communication parameter	Structure
E901 hex	0 hex	—	—	Highest subindex supported	Number of structure elements: 8
E901 hex	1 hex	—	—	Version	
E901 hex	2 hex	—	—	FSoE slave address	
E901 hex	3 hex	—	—	Connection ID	
E901 hex	4 hex	—	✓	Watchdog time	
E901 hex	5 hex	—	—	Reserved	
E901 hex	6 hex	—	—	Connection type	
E901 hex	7 hex	—	—	ComParameterLength	
E901 hex	8 hex	—	—	ApplParameterLength	
F980 hex	0 hex	—	—	FSoE slave address	

Tab. 11: ETG.5001.4 communication objects: E000 hex – EFFF hex

11.2 Detailed information

The documentation listed in the following table offers additional information relevant to the drive controller.

Current document versions can be found at http://www.stoeber.de/en/downloads/.

Device/Software	Documentation	Contents	ID
SC6 drive controller	Manual	System design, technical data, project configuration, storage, installation, connection, commissioning, operation, service, diagnostics	442790
SC6 drive controller	Commissioning instructions	System design, technical data, storage, installation, connection, commissioning	442793
Multi-axis drive system with SI6 and PS6	Manual	System design, technical data, project configuration, storage, installation, connection, commissioning, operation, service, diagnostics	442728
Multi-axis drive system with SI6 and PS6	Commissioning instructions	System design, technical data, storage, installation, connection, commissioning	442731
EtherCAT communication – SC6, SI6	Manual	Installation, electrical installation, data transfer, commissioning, detailed information	443025

Additional information and sources that form the basis of this documentation or are referenced by the documentation:

Beckhoff Automation GmbH & Co. KG (publisher): *EtherCAT System Documentation*. Version 5.1. Verl, 2016.

A basic version of the TwinCAT 3 automation software is available for free at https://www.beckhoff.de/default.asp?download/tc3-downloads.htm.

EtherCAT Technology Group (ETG), 2012. *ETG.1300 : EtherCAT Indicator and Labeling*. ETG.1300 S (R) V1.1.0. Specification. 2012-01-27.

EtherCAT Technology Group (ETG), 2016. *ETG.5001: Modular Device Profile, Part 4: Safety Modules Specification*. ETG.5001.4 S (D) V0.2.1. Specification. 2016-08-05.

EtherCAT Technology Group (ETG), 2016. *ETG.6100: Safety Drive Profile, Part 1: Overview, Scope*. ETG.6100.1 S (R) V1.2.0. Specification. 2016-02-08.

EtherCAT Technology Group (ETG), 2016. *ETG.6100: Safety Drive Profile, Part 2: Generic Safety Drive Profile for adjustable speed electrical power drive systems that are suitable for use in safety-related applications PDS(SR)*. ETG.6100.2 S (R) V1.2.0. Specification. 2016-02-08.

EtherCAT Technology Group (ETG), 2016. *ETG.6100: Safety Drive Profile Part 3: Mapping to Safety-over-EtherCAT*. ETG.6100.3 S (WD) V1.2.0. Specification. 2016-02-08.

11.3 Abbreviations

Abbreviation	Meaning
µC	Microcontroller
CRC	Cyclic Redundancy Check
EMC	Electromagnetic Compatibility
ESI	EtherCAT Slave Information
ETG	EtherCAT Technology Group
EtherCAT	Ethernet for Control Automation Technology
FSoE	Fail Safe over EtherCAT
IGBT	Insulated Gate Bipolar Transistor
I/O	Input/Output
PDO	Process Data Objects
PDS(SR)	Power Drive System(Safety Related)
PDU	Process data units
PL	Performance Level
PWM	Pulse Width Modulation
RxPDO	Receive PDO
SIL	Safety Integrity Level
SIL CL	Safety Integrity Level Claim Limit
PLC	Programmable Logic Controller
SRECS	Safety-Related Electrical Control System
SRP/CS	Safety-Related Part of a Control System
SS1	Safe Stop 1
SS1-t	Safe Stop 1-time
STO	Safe Torque Off
TwinCAT	The Windows Control and Automation Technology
TxPDO	Transmit PDO

12 Contact

12.1 Consultation, service and address

We would be happy to help you!

We offer a wealth of information and services to go with our products on our website:
http://www.stoeber.de/en/service

For additional or personalized information, contact our consultation and support service:
http://www.stoeber.de/en/support

Do you need our first-level support?:
Phone +49 7231 582-3060
applications@stoeber.de

Do you need a replacement device?:
Phone +49 7231 582-1128
replace@stoeber.de

Call our 24-hour service hotline:
Phone +49 7231 582-3000

Our address:
STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Strasse 12
75177 Pforzheim, Germany

12.2 Your opinion is important to us

We created this documentation to the best of our knowledge with the goal of helping you build and expand your expertise productively and efficiently with our products.

Your suggestions, opinions, wishes and constructive criticism help us to ensure and further develop the quality of our documentation.
If you want to contact us for a specific reason, we would be happy to receive an e-mail from you at:
documentation@stoeber.de

Thank you for your interest.
Your STOBER editorial team

03/2020 | ID 442744.03

12.3 Close to customers around the world

We offer you committed, expert advise and support in over 40 countries worldwide:

STOBER AUSTRIA www.stoeber.at Phone +43 7613 7600-0 sales@stoeber.at	**STOBER SOUTH EAST ASIA** www.stober.sg sales@stober.sg
STOBER CHINA www.stoeber.cn Phone +86 512 5320 8850 sales@stoeber.cn	**STOBER SWITZERLAND** www.stoeber.ch Phone +41 56 496 96 50 sales@stoeber.ch
STOBER FRANCE www.stober.fr Phone +33 4 78.98.91.80 sales@stober.fr	**STOBER TAIWAN** www.stober.tw Phone +886 4 2358 6089 sales@stober.tw
STOBER ITALY www.stober.it Phone +39 02 93909570 sales@stober.it	**STOBER TURKEY** www.stober.com Phone +90 212 338 8014 sales-turkey@stober.com
STOBER JAPAN www.stober.co.jp Phone +81 3 5395 678 8 sales@stober.co.jp	**STOBER UNITED KINGDOM** www.stober.co.uk Phone +44 1543 458 858 sales@stober.co.uk
STOBER USA www.stober.com Phone +1 606 759 5090 sales@stober.com	

03/2020 | ID 442744.03

Glossary

Black channel principle

Technology that allows secure data to be transmitted over unsecure network or bus lines. Safety components can transmit safety-related data regardless of hardware using a secure protocol that tunnels through the underlying network channel. Possible transmission errors are noted in the standards IEC 61784-3 and IEC 61508.

Broadcast domain

Logical grouping of network devices within a local network that reaches all nodes via broadcast.

Category

In accordance with DIN EN ISO 13849-1: Classification of safety-related parts of a controller regarding their resistance to faults and their subsequent behavior in the event of a fault. A category is attained through the structure and the arrangement of parts, their fault detection and/or their reliability. Possible category designations, i.e. classifications, are B, 1, 2, 3, 4.

ESI file

Device description file for EtherCAT slaves. In accordance with ETG.2000: XML file that contains all relevant data for an EtherCAT node in the EtherCAT system, such as the identity of the manufacturer, the product code, the version or the production number. The EtherCAT master requires this file to configure the EtherCAT system.

Fail Safe over EtherCAT (FSoE)

Protocol for transferring safety-related data via EtherCAT using a FSoE master and an indefinite number of FSoE slaves (i.e. devices that have a Safety over EtherCAT interface). The protocol enables the realization of functional safety via EtherCAT. FSoE and its implementation are TÜV-certified and comply with the SIL 3 requirements in accordance with IEC 61508.

FSoE address

Each FSoE slave has an address that provides unique identification for it in the FSoE network. The address is generally configured on the device itself, for example, using a DIP switch. In a FSoE system, a maximum of 65,534 (16-bit, 0 address is prohibited) nodes can be differentiated by their addresses.

Insulated Gate Bipolar Transistor (IGBT)

Bipolar transistor with insulated gate electrode. Four-layer semiconductor component that is controlled using a gate and combines the advantages of bipolar and field-effect transistor. An IGBT is primarily used in power electronics.

IPv4 limited broadcast

Type of broadcast in a network with IPv4 (Internet Protocol version 4). The IP address 255.255.255.255 is entered as the destination. The content of the broadcast is not redirected by a router, which limits it to the local network.

Mission time (TM)

In accordance with DIN EN 61800-5-2: Determined cumulative length of operation of the PDS(SR) during its overall service life.

03/2020 | ID 442744.03

PDO

Communication objects in a CANopen or EtherCAT network that transmit data such as set and actual values, control commands or status information based on events or objectives, in cycles or in real time on request. PDOs are generally exchanged over the process data channel with high priority. Depending on the view of the respective node, a distinction is made between receive PDOs (RxPDO) and transmit PDOs (TxPDO).

Performance Level (PL)

In accordance with DIN EN 13849-1: Measure for the reliability of a safety function or a component. The Performance Level is measured on a scale of a – e (lowest – highest PL). The higher the PL, the safer and more reliable the function in question is. The PL can be assigned to a specific SIL. A reversed inference from a SIL to a PL is not possible.

Probability of a dangerous failure per hour (PFHD)

In accordance with DIN EN 61508/DIN EN 62061: Average probability of a dangerous device failure per hour. Together with PFH, one of the most important bases for calculating the safety function reliability of devices, the SIL.

Safe Stop 1 (SS1)

In accordance with DIN EN 61800-5-2: Procedure for stopping a PDS(SR). With the SS1 safety function, the PDS(SR) performs one of the following functions: a) Triggering and controlling the motor delay variable within defined limits and triggering the STO function if the motor speed falls below a specified limit value (SS1-d), or b) triggering and monitoring the motor delay variable within defined limits and triggering the STO function if the motor speed falls below a specified limit value (SS1-r), or c) triggering the motor delay and triggering the STO function after an application-specific delay (SS1-t). In this case, SS1(-t) corresponds to the time-controlled stop in accordance with IEC 60204-1, stop category 1(-t).

Safe Torque Off (STO)

In accordance with DIN EN 61800-5-2: Procedure for stopping a PDS(SR). The STO safety function prevents the motor from being supplied with any energy that could cause rotation (or motion in a linear motor). The PDS(SR) does not supply the motor with any energy that could generate torque (or force in a linear motor). STO is the most fundamental drive-integrated safety function. It corresponds to an uncontrolled stop in accordance with DIN EN 60204-1, stop category 0.

Safety Integrity Level (SIL)

In accordance with DIN EN 61800-5-2: Probability of a safety function failure. SIL is divided into levels 1 – 4 (lowest – highest level). SIL precisely assesses systems or subsystems based on the reliability of their safety functions. The higher the SIL, the safer and more reliable the function in question is.

Safety Integrity Level Claim Limit (SIL CL)

Maximum SIL that can be claimed, based on the structural limitations and systematized safety integrity of a SRECS subsystem. A SIL CL is determined by the hardware fault tolerance (HFT) and the safe failure fraction (SFF) of the subsystems.

STO switch-off time

Time span starting from the activation of the safety function until the power unit of the drive controller is safely switched off.

Worst case response time

Maximum time span required in order to switch off the actuator in the event of an error.

List of figures

03/2020 | ID 442744.03

List of tables

03/2020 | ID 442744.03

442744.03

03/2020

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Str. 12
75177 Pforzheim
Germany
Tel. +49 7231 582-0
mail@stoeber.de
www.stober.com

24 h Service Hotline
+49 7231 582-3000

STÖBER

www.stober.com