ST6 safety module
Manual

STÖBER

Table of contents

1   Foreword

The ST6 safety module adds the **Safe Torque Off (STO)** safety function (described as standard in DIN EN 61800-5-2) to STOBER drive controllers of the SD6 series.

STO prevents an electrical rotating magnetic field, needed for the operation of synchronous or asynchronous motors, from being generated in a drive controller. Additional safety functions can be built upon the STO function with the suitable external wiring, such as Safe Stop 1 (SS1-t).

Different interfaces are available for activating STO in a drive controller, including the terminal-based ST6 safety module.

ST6 is a fast and wear-free fully electronic solution. In addition, 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 is ensured by an external testing institute as part of type testing.

2 User information

This documentation provides all information on the intended use of the drive controller in combination with the ST6 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 SD6 series in combination with the ST6 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.

No warranty or liability claims for damage shall result 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 the project configuration and operation of the product by unqualified personnel.

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   Display of safety instructions

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!

Attention

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 Distinction 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

2.6.3 Mathematics and formulas

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

-	Subtraction
+	Addition
×	Multiplication
÷	Division
| |	Amount

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:

- EN ISO 13849-1:2015

- EN ISO 13849-2:2012

- EN 61800-5-2:2007

- EN 61508-x:2010

- EN 60204-1:2018

- EN 62061:2005

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

3.2   EU declaration of conformity

We, STÖBER Antriebstechnik GmbH + Co. KG, declare that the products described in this document correspond the requirements of the guidelines of the European Parliament and of the Council.

Representatives: Stephan Scholze, STÖBER Antriebstechnik GmbH + Co. KG, Kieselbronner Str. 12, 75177 Pforzheim, Germany.

Complete product-specific EU declaration of conformity can be found at http://www.stoeber.de/en/downloads/ or you can obtain it from our service department.

3.3   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 personnel are persons who have acquired the authorization to perform these activities 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.

3.4   Intended use

The ST6 safety module can be combined with STOBER drive controllers of the SD6 series. The module must be wired compliant for EMC.

If a drive controller with the integrated ST6 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 EN 60204-1.

When installing drive controllers in machines, commissioning (i.e. commencing intended operation) may not be performed until it has been determined that the machine is in compliance with local laws and directives. For example, in the European region, the following applies:

- Machinery Directive 2006/42/EC
- Low Voltage Directive 2014/35/EU
- EMC Directive 2014/30/EU

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 EN 60204-1 is not possible with the ST6 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 ST6 safety module.

Maintenance

The safety module is maintenance-free.
Take appropriate measures to detect or prevent possible errors in the connecting wiring (see the chapter Monitoring the connection wiring).

3.5   Decommissioning

In safety-oriented applications, note the mission time T_M = 20 years in the safety-relevant key performance indicators. A drive controller with integrated safety module must be taken out of operation 20 years after the production date. The production date of the drive controller is found on the accompanying nameplate.

4 Safety module ST6

The ST6 safety module adds the STO (Safe Torque Off) safety function to the drive controller . In the event of an error or by external request, STO prevents the formation of a rotating magnetic field in the power unit of the drive controller.

Additional safety functions can be built upon the STO function with suitable external wiring, such as SS1-t (Safe Stop 1).

Features

- Two one-pole digital inputs for activating the safety functions:
  - Safe Torque Off – STO in accordance with EN 61800-5-2
  - Stop category 0 in accordance with EN 60204-1
- STO switch-off time < 10 ms
- Free of wear

Maximum safety figures in accordance with EN 61800-5-2 and EN ISO 13849-1

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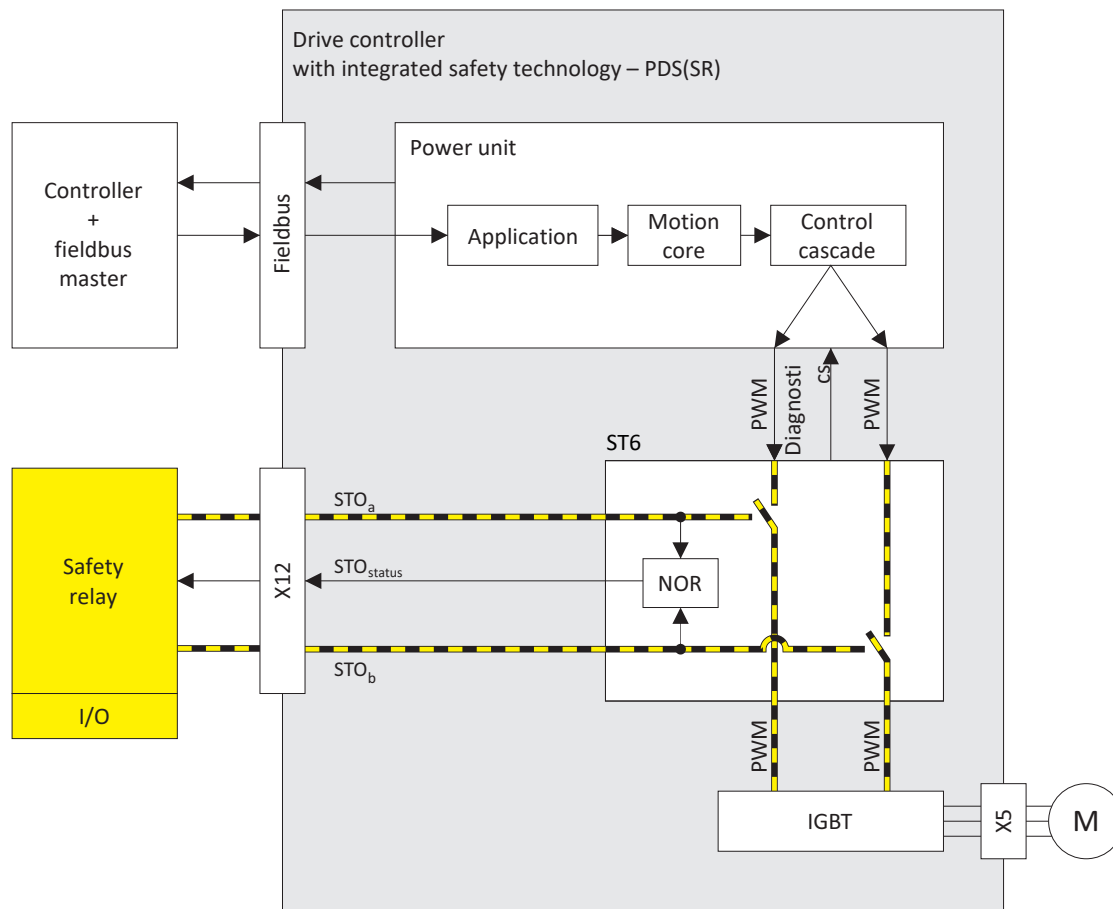- Category 4

5   System design and function

Fig. 1: Drive controller and safety module (PDS(SR) – System design

Function

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

If the STO safety function is not active, the ST6 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, ST6 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 immediate switch-off, e.g. after an emergency stop, corresponds to the STO safety function in accordance with EN 61800-5-2. In EN 60204-1, this type of switch-off is defined as stop category 0.

A time-delayed switch-off, e.g. after an emergency stop, corresponds to the SS1-t safety function in accordance with EN 61800-5-2. In EN 60204-1, this type of switch-off is defined as stop category 1.

> ⚠ **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 $360° \div (p \times 2)$.

ST6 – Design

The ST6 safety module is designed with two channels. Both safety channels are independent of one another. To deactivate the safety functions, they must be activated at the corresponding STO_a (safety channel 1) and STO_b (safety channel 2) inputs at the same time. This is done either directly via floating contacts with 24 V_{DC} or alternately via 24 V_{DC} semiconductor outputs with layered testing.
Using both the STO_a and STO_b inputs, rotating magnetic field generation in the drive controller is enabled or disabled.

The safety module is developed according to the fail-safe principle. The failure of a component or a module activates the STO function.

Monitoring the connection wiring

Status signals are provided for checking the status of the connecting wiring and the function of the safety channels:

- Signal STO_{status} (via terminal X12)
  STO_{status} is the result of a NOR gate of the two STO_a and STO_b inputs, meaning that the STO_{status} output is always 1 (high level) if the STO_a input equals 0 (low level) and the STO_b input equals 0 (low level). The signal is output on the X12 terminal of the drive controller.

- Parameter E67
  Parameter E67 is an array parameter that visualizes the state of both safety channels in detail.

Information

If both STO inputs are controlled via outputs with test pulses, e.g. interface type C or D, the check of the connecting wiring is taken over by the signal-generating controller. Potential faults are detected directly, eliminating the need to evaluate the STO status signals.

More detailed information can be found in the chapter Monitoring the connection wiring [▶ 30].

6 Technical data

The transport, storage and operating conditions of the safety module correspond to those of the drive controller. The technical data is part of the drive controller manual (see the chapter Further information [▶ 46]).

6.1 Key safety-related figures

The table includes the key figures for the ST6 module that are relevant for the safety technology.

Safety figure	Value
SIL CL in accordance with EN 62061	3
SIL in accordance with EN 61508	3
PL in accordance with EN ISO 13849	e
Category in accordance with EN ISO 13849	4
PFH	5×10^{-9} [1/h]
Mission time (T_M)	20 years

Tab. 1: ST6 – Key safety-related figures

6.2 System times

The following diagram visualizes the temporal relationships in the event of STO activation and execution; the associated values for the drive controller in combination with the ST6 safety module are found in the subsequent table.
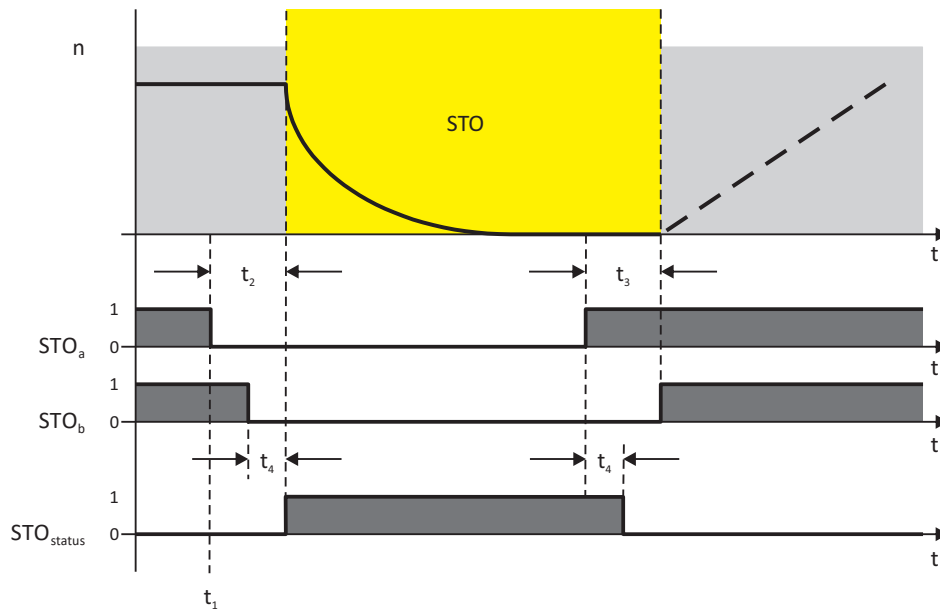
Fig. 2: STO – Temporal relationships (detailed representation)

t_1	STO triggering
t_2	Maximum reaction time
t_3	Maximum time difference
t_4	Maximum response time

Be aware that the reaction times of the individual part systems must be taken into account to calculate an application-specific total reaction time (see the chapter SRP/CS: Processing a typical safety function [▶ 29]).

System time	Value
Maximum reaction time	10 ms
Maximum time difference	500 ms
Maximum response time	15 ms

Tab. 2: STO – System times

6.3   Interface classification

According to the 24 V_{DC} interface classification from ZVEI, the ST6 safety module can be used as a data sink (sink) for interface types C and D and activated by data sources (sources) of the same interface types.

The values contained in the tables apply for the ST6 used as a data sink for interface types C and D. [1]

	Min.	Typ.	Max.
Class		2	
Test pulse duration t_i	—	—	600 µs
Test pulse interval T_i	10 ms	—	—
Input resistance R_1	1000 Ω	—	—
Input capacitance C_1	—	—	100 nF
Input inductance L_1	—	—	5 µH

Tab. 3: ST6 – Specific figures for the interface type C

	Min.	Typ.	Max.
Class		2	
Test pulse duration t_i	—	—	600 µs
Test pulse interval T_i	10 ms	—	—
Input resistance R_1	500 Ω	—	—
Input current I_{1on} in ON state	2 × 10 mA	2 × 14 mA	2 × 15 mA
Input current I_{1off} in OFF state	—	—	3 mA
Input capacitance C_1	—	—	100 nF
Input inductance L_1	—	—	5 µH

Tab. 4: ST6 – Specific figures for the interface type D

---

[1] See ZVEI, p. 16 and p. 19ff.

7   Connection

The ST6 safety module is connected via the X12 terminal of the drive controller.

More detailed information on errors in the connection wiring, their connection and an STO function test can be found in the chapter Monitoring the connection wiring [▶ 30].

7.1   Connection compliant with EMC

For an EMC-compliant connection, observe the corresponding recommendations in the drive controller manual (see the chapter Further information [▶ 46]).

7.2   X12 terminal
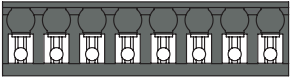
Information

Incompatibility of the safe inputs and outputs
The test pulses of the outputs will be distorted due to the input capacitance. The safety relay or the safety controller will go to a fault state. When selecting the safe outputs, consider the input capacitance and the input current of the inputs of terminal X12.

Specification	Electrical data
STO_a	$U_{1max} = 30\ V_{DC}$ (PELV)
STO_b	High level = $15 - 30\ V_{DC}$ Low level = $0 - 8\ V_{DC}$ $I_{1max} = 100$ mA $I_{1N} = 10 - 15$ mA per channel $C_{1max} = 100$ nF
STO_{status}	$U_2 = U_1 - (200\ m\Omega * I_1)$
STO_{status} supply	$U_1 = +24\ V_{DC}$, +20%/25% $I_{1max} = 100$ mA
GND	—

Tab. 5: X12 electrical data

Terminal	Pin	Designation	Function
1|2|3|4|5|6|7|8	1	STO_a	Input of safety channel 1
	2		
	3	STO_b	Input of safety channel 2
	4		
	5	0 V GND	Reference potential for STO_a and STO_b, internally bridged with terminal 7
	6	STO_{status}	Feedback signal of safety channels 1 and 2 for diagnostic purposes
	7	0 V GND	Reference potential for STO_a and STO_b, internally bridged with terminal 5
	8	$U_{1status}$	STO supply $_{status}$; recommended fuse protection: max. 3.15 AT[2]

Tab. 6: X12 connection description

Connecting wiring

Feature	Line type	Value
Contact spacing	—	3.81 mm
Nominal current at ϑ_{amb} = 40 °C	—	CE/UL/CSA: 16 A/10 A/11 A
Max. conductor cross-section	Flexible without end sleeve	1.5 mm²
	Flexible with end sleeve without plastic collar	1.0 mm²
	Flexible with end sleeve with plastic collar	1.0 mm²
	2 conductors, flexible, with double end sleeve with plastic collar	—
	AWG according to UL/CSA	16
Min. conductor cross-section	Flexible without end sleeve	0.14 mm²
	Flexible with end sleeve without plastic collar	0.25 mm²
	Flexible with end sleeve with plastic collar	0.25 mm²
	2 conductors, flexible, with double end sleeve with plastic collar	—
	AWG according to UL/CSA	26
Insulation stripping length	—	10 mm
Tightening torque	—	—

Tab. 7: BCF 3.81 180 SN BK specification

Cable requirements

Feature	All sizes
Max. cable length	30 m

Tab. 8: Cable length [m]

---

[2] For UL-compliance, use of a 3.15 A fuse (time delay) is required. The fuse must be certified for DC voltage in accordance with UL 248.

X12 wiring

The two-channel design of the ST6 with shared potential reference supports various options for connection. These depend upon whether ST6 is used via contacts or as a data sink for interface type C or D from the ZVEI interface classification.

Subsequent graphics visualize the activation options using corresponding switch contacts. Activation via the semiconductor outputs with test pulses is also permitted.

Fig. 3: X12 wiring – ST6 as data sink for interface type C

Both STO_a and STO_b inputs are connected by two discrete channels; the GND reference potential is permanently wired.

In the event of circuits with contacts, errors in the connection wiring can be detected only in some cases. Short circuits to GND from STO_a and STO_b are identified with the aid of upstream fuse protection; they remain undetected with $24\ V_{DC}$. Possible short circuits and cross circuits can be determined only by line or output tests.

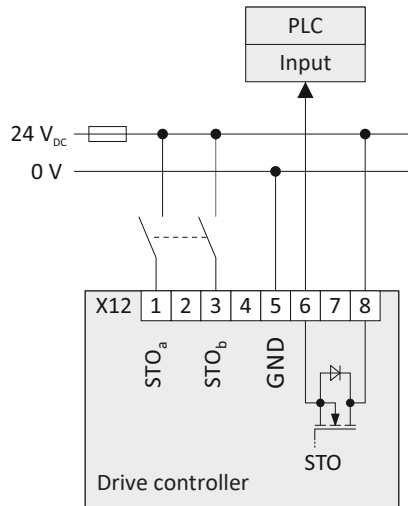Redundant wiring in accordance with interface type C detects short circuits and cross circuits in the connection wiring.
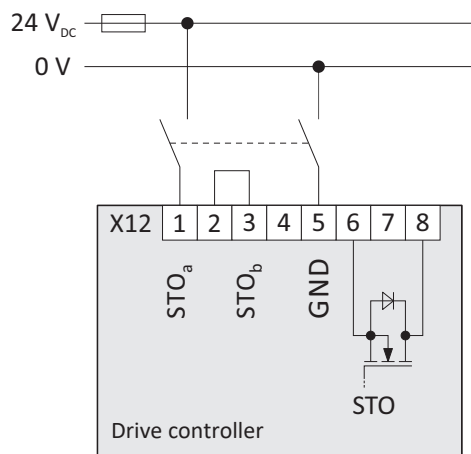
Fig. 4: X12 wiring – ST6 as data sink for interface type D

Both STO$_a$ and STO$_b$ inputs are connected together; the GND reference potential serves as a second independent switch-off channel.

In the event of activation with contacts, errors in the connection wiring can be detected only in some cases. Possible short circuits and cross circuits can be determined only by line or output tests.

Wiring in accordance with interface type D detects short circuits and cross circuits in the connection wiring.

Information

In the case of wiring according to interface type D, the status output at X12 cannot be used. Alternatively, the status information is available via parameter E67.

7.3   Parallel connection

It is possible to activate STO on multiple drive controllers simultaneously using the output of a safety relay. A parallel connection of up to 32 drive controllers is possible depending on the required safety figure.

⚠ **WARNING!**

Property damage and injury to persons due to loss of safety function!

In parallel connection, possible wiring or activation errors can lead to the loss of safety function for all drive controllers.

- ▪ Take appropriate measures to detect or exclude wiring faults (see the chapter Monitoring the connection wiring [▶ 30]).

- ▪ Be aware that the STO$_{status}$ outputs cannot be connected in series for a shared evaluation.

8 Commissioning

This chapter describes how to commission the ST6 safety module and activate or deactivate the STO safety function.

Information

The safety module is a permanently integrated component in the drive controller where any design, technical and electrical modifications are prohibited!

Detailed information on commissioning the drive controller can be found in the drive controller manual (see the chapter Further information [▶ 46]).

8.1 Putting the safety module and drive controller into operation

Proceed as follows to put a drive controller with integrated ST6 safety module into operation.

1. Check whether the planned safety technology is sufficient for the safety requirements of your entire system.

2. Wire the safety-related X12 terminal in accordance with the data contained in the chapter X12 terminal.

3. Connect and start up the drive controller. Detailed information on this process and all relevant safety instructions associated with this can be found in the drive controller manual.

4. Start by performing an STO function test. Proceed as described in the chapter Monitoring the connection wiring [▶ 30], along with all related subsections. Document your test results.

Information

Be aware that the listed steps must also be performed and documented every time before putting the drive controller and integrated ST6 safety module back into operation after a replacement!

8.2 Activating STO

In order to activate the STO safety function, the activation signals of the STO_a and STO_b inputs must be switched off or interrupted. The power unit of the drive controller cannot generate a rotating magnetic field after reaction time t_2 and the motor is free of torque (also see the chapter System times).

Before the drive controller can be enabled again, both the STO_a and STO_b inputs must be deactivated for at least 100 ms.

⚠ **DANGER!**

Risk of fatal injury due to gravity-loaded vertical axes or motor coasting!

The drive controller in the motor cannot generate torque when the STO safety function is active. Consequently, vertical axes subject to gravitational forces may fall. If the motor is moving when STO is activated, it will coast uncontrolled.

▪   Secure gravity-loaded vertical axes by braking or taking similar actions.

▪   Make sure that the motor coasting does not create any hazards.

8.3   Deactivating STO

In order to deactivate the STO safety function, the STO_a and STO_b inputs must be actuated simultaneously within 500 ms with 24 V_{DC}.

If the safety function is deactivated, the drive controller power unit on the motor can generate the necessary torque for active motion.

8.4   Recommissioning after device replacement

Information

Send defective drive controllers to STOBER Service with a description of the fault for fault analysis.

When recommissioning, carry out a new validation by performing an STO function test.

9 STO as a safety subfunction within other safety functions

The STO safety subfunction is a component of multiple safety functions in machines and systems. With suitable external wiring, further safety functions can be implemented from the STO safety subfunction.

9.1 SS1-t based on STO

The SS1-t safety function in accordance with EN 61800-5-2 corresponds to stop category 1 in accordance with EN 60204-1. Both are based on STO.

The following diagram visualizes the sequences over time during activation of a drive controller in order to implement the SS1-t safety function.
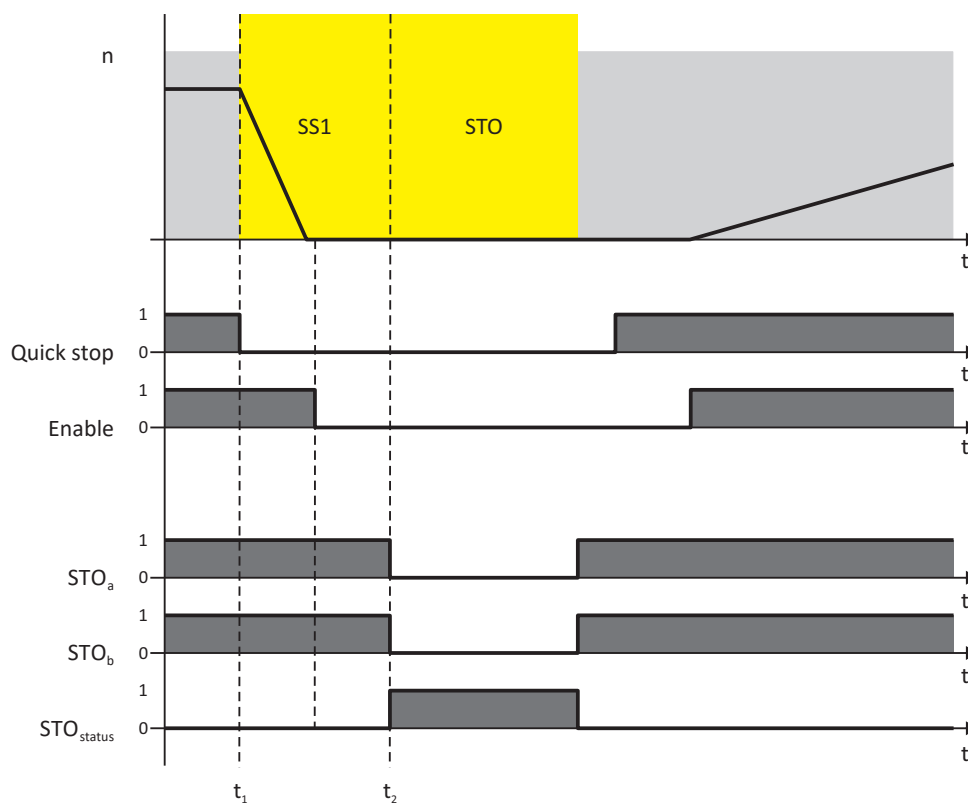
Fig. 5: ST6 and SS1-t – Sequence over time

| t_1 | SS1 triggering |
| t_2 | STO triggering |

The SS1-t safety function consists of 2 parts:

- Part 1: Controlled stop

- Part 2: Safe shutdown of the drive controller (STO)

A safety relay activates a controlled stop in the drive controller at time t_1, such as by using the **quick stop** function. After the projected time SS1-t in the safety relay has passed, STO is activated at time t_2. This process corresponds to a **time-controlled SS1-t** defined in EN 61800-5-2.

10 Diagnostics

10.1 Meaning of parameters

You can adapt the function of the drive controller to your individual application using parameters. In addition, parameters visualize the current actual values (actual velocity, actual torque, etc.) and trigger general actions like Save values, Test phase, etc.

Interpretation of parameter identification

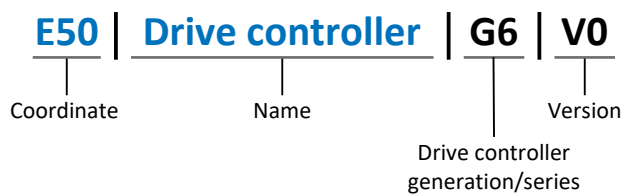Parameter identification consists of the following elements, where short forms are also possible, i.e. only specifying a coordinate or the combination of coordinate and name.

```
E50 │ Drive controller │ G6 │ V0

Coordinate        Name                      Version

                            Drive controller
                            generation/series
```

10.1.1 Parameter groups

Parameters are assigned to individual groups by topic. The 6th generation of STOBER drive controllers differentiates between the following parameter groups.

Group	Topic
A	Drive controllers, communication, cycle times
B	Motor
C	Machine, velocity, torque/force, comparators
D	Set value
E	Display
F	Terminals, analog and digital inputs and outputs, brake
G	Technology – Part 1 (application-dependent)
H	Encoders
I	Motion (all motion settings)
J	Motion blocks
K	Control panel
L	Technology – Part 2 (application-dependent)
M	Profiles (application-dependent)
N	Additional functions (application-dependent; extended cam control unit)
P	Customer-specific parameters (programming)
Q	Customer-specific parameters, instance-dependent (programming)
R	Production data for the drive controller, motor, brakes, motor adapter, gear unit and geared motor
S	Safety (safety technology)
T	Scope
U	Protection functions
Z	Fault counter

Tab. 9: Parameter groups

10.1.2   Parameter types and data types

In addition to topic-based sorting in individual groups, all parameters belong to a certain data type and parameter type. The data type of a parameter is displayed in the parameter list, properties table. The connections between parameter types, data types and their value range can be found in the following table.

Type	Style	Length	Value range (decimal)
INT8	Integer or selection	1 byte (signed)	-128 – 127
INT16	Integer	2 bytes (1 word, signed)	-32768 – 32767
INT32	Integer or position	4 bytes (1 double word, signed)	-2147483648 – 2147483647
BOOL	Binary number	1 bit (internal: LSB in 1 byte)	0, 1
BYTE	Binary number	1 byte (unsigned)	0 – 255
WORD	Binary number	2 bytes (1 word, unsigned)	0 – 65535
DWORD	Binary number or parameter address	4 bytes (1 double word, unsigned)	0 – 4294967295
REAL32 (single type according to IEE754)	Floating-point number	4 bytes (1 double word, signed)	$-3.40282 \times 10^{38} – 3.40282 \times 10^{38}$
STR8	Text	8 characters	—
STR16	Text	16 characters	—
STR80	Text	80 characters	—

Tab. 10: Parameters: Data types, styles, possible values

Parameter types: Use

- Integer, floating-point number
  For general computing processes
  Example: Set and actual values

- Selection
  Numeric value to which a direct meaning is assigned
  Example: Sources for signals or set values

- Binary number
  Bit-oriented parameter information that is collected in binary
  Example: Control and status words

- Position
  Integer combined with associated units and decimal places
  Example: Actual and set values of positions

- Velocity, acceleration, deceleration, jerk
  Floating-point number combined with the associated units and decimal places
  Example: Actual and set values for velocity, acceleration, deceleration, jerk

- Parameter address
  Corresponds to the storage location of another parameter
  Example: Indirect read sources for analog and digital outputs and for fieldbus mapping

- Text
  Outputs or messages

10.1.3 Parameter types

The following types of parameters are differentiated.

Parameter type	Description	Example
Simple parameters	Consist of one group and one line with a defined value.	A21 Brake resistor R: Value = 100 ohms
Array parameters	Consist of a group, a line and multiple sequential (listed) elements, which have the same properties but different values.	A10 Access level ▪ A10[0] access level: Value = Access level via operating unit ▪ A10[2] access level: Value = Access level via CANopen and EtherCAT ▪ A10[4] access level: Value = Access level via PROFINET
Structure parameters	Consist of a group, a line and multiple sequential (listed) elements, which can have different properties and different values.	A00 Save values ▪ A00[0] Start: Value = Start action ▪ A00[1] Progress: Value = Display action progress ▪ A00[2] Result: Value = Display action result

Tab. 11: Parameter types

10.1.4 Parameter structure

Every parameter has specific coordinates with the following pattern.
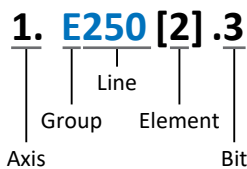
▪ Axis

The axis to which a parameter is assigned in the case of multiple axes (optional).

▪ Group

The thematic group to which a parameter belongs.

▪ Line

Distinguishes the parameters within a parameter group.

▪ Element

Elements of an array or structure parameter (optional).

▪ Bit

Selection of an individual bit for complete data addressing (optional).

10.1.5   Parameter visibility

The visibility of a parameter depends on the access level defined in the software, the dependency of other parameters, the selected application and the version of the associated firmware.

Access level

The access options for the individual software parameters are ranked hierarchically and divided into individual levels. This means that parameters can be hidden for a specific purpose and, relatedly, their configuration options can be locked starting from a specific level. The following levels are present:

- Level 0
  Elementary parameters

- Level 1
  Important parameters of an application

- Level 2
  Important parameters for service with extensive diagnostic options

- Level 3
  All parameters needed for commissioning and optimizing an application

Parameter A10 Access level controls general access to parameters:

- Over the SD6 drive controller display (A10[0])

- Over CANopen or EtherCAT (A10[2])

- Over PROFINET (A10[3])

Hiding functions

Hiding functions are used to hide parameters with regard to their logical relationships to other option modules or parameters.

For example, a drive controller can evaluate an encoder using terminal X120, provided that terminal module XI6 has been installed. The accompanying evaluation is activated using parameter H120. However, this parameter is visible only if terminal module XI6 was initially selected during the drive project configuration.

Applications

Applications generally differ in terms of functions and their activation. For this reason, different parameters are available with each application.

Firmware

A newer version of the firmware may introduce new parameters. Parameters that have been configured for files of an older firmware function may not be visible in newer versions. In such cases, the respective parameter description includes a corresponding note.

10.2   Parameters

The following display parameters are significant for safety technology in combination with the ST6 safety module.

10.2.1   E53 | Required safety module | G6 | V3

Configured safety module.

10.2.2   E54 | Information safety module | G6 | V0

Signifying data of the safety module.

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

10.2.3   E67 | STO active | G6 | V0

STO state of the safety module:

- [0]: STO requested by safety channel 1 or safety channel 2
  Source: logical OR operation of E67[1] and E67[2], including a deactivation delay of 32 ms
  - 0: Inactive = not requested
  - 1: Active = requested

- [1]: STO requested by safety channel 1
  Source ST6, SR6: terminal X12.1/.2, signal STO_a = 0; source SE6, SY6, SU6: safety module-internal
  - 0: Inactive = not requested
  - 1: Active = requested

- [2]: STO requested by safety channel 2
  Source ST6, SR6: terminal X12.3/.4, signal STO_b = 0; source SE6, SY6, SU6: safety module-internal
  - 0: Inactive = not requested
  - 1: Active = requested

10.3   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, a fault occurs or STO is active, 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.

Information

To make it easier for control programmers to set up the human-machine interface (HMI), a list of events and their causes can be found in the STOBER download center at http://www.stoeber.de/en/downloads/.

10.3.1   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 behavior of the brakes depends on the configuration of the safety module and an optional release override (F06)

Cause		Check and action
1: Inconsistent request (single channel)	Connection error	Check the connection and correct it if necessary; error cannot be acknowledged until both STO channels have been requested for at least 100 ms
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

Tab. 12: Event 50 – Causes and actions

11 More on safety technology and ST6?

The following chapters outline the important terms, relationships and measures regarding the ST6 safety module and safety technology.

11.1 SRP/CS: Processing a typical safety function

If a machine or system poses hazards that cannot be eliminated through design measures, suitable protective devices and safety functions must be defined and implemented in order to reduce the risk potential.

The safety functions and associated requirements necessary for the Safety Integrity Level and Performance Level (SIL, PL) depend on the respective application and possible dangers. For electrical power drive systems with adjustable speed, the safety functions are defined in EN 61800-5-2.

The execution of safety functions is generally handled by safety-related parts of control systems (SRP/CS).

A typical safety function is a combination of the safety-related parts of a controller (SRP/CS) and the following components:

- Input (SRP/CS$_a$)
- Logic (SRP/CS$_b$)
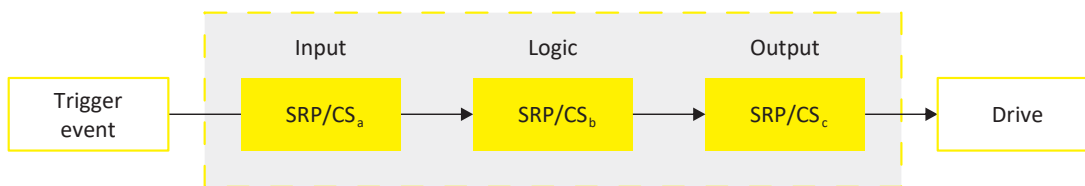- Output (SRP/CS$_c$)
- Connections, e.g. electrical or optical

Fig. 6: SRP/CS components for processing a typical safety function

Input	Sensor, e.g. limit switch
Logic	Safety controller or safety relay
Output	Actuator, e.g. drive controller including safety module
Trigger event	Opening a separating protective device or pressing a button by hand
Drive	Motor or cylinder

Explanation

A sensor acts as an input component to detect a situation that triggers the safety function. The logic component processes the measured signals and then the actuator acts as an output component to safely trigger the dangerous motion.
The drive controller in combination with the integrated ST6 safety module is part of the SRP/CS actuator.

Whether a safety controller or a safety relay is used as a logic component of a SRP/CS depends on its complexity as well as on the required SIL and PL.

11.2   Monitoring the connection wiring

The ST6 safety module does not require any maintenance; however, it cannot detect external wiring errors.

⚠ **WARNING!**

Loss of safety function and unexpected drive motion due to wiring errors!

The ST6 safety module does not detect any errors in the connecting wiring of X12!
To identify or eliminate these errors and prevent a possible error in the wiring or actuation of the safety function from causing a loss of safety, take one of the following actions.

- Continuous monitoring of the connecting wiring by a safety relay

- Fault exclusion for lines and connections in accordance with EN ISO 13849, or

- Monitoring of the connecting wiring by checking the plausibility of the actuation signals from STO_a and STO_b against the STO status signals (by means of STO function test).

11.2.1   Monitoring by a safety relay

If the STO_a and STO_b inputs are activated by monitored outputs, the accompanying safety relay inspects the wiring and the switching capability of the outputs using test pulses.

In the event of an error, always switch the device off using the other STO input and then correct the error.

11.2.2   Fault exclusion for lines and connections in accordance with EN ISO 13849

Errors in the connecting wiring of modules and components can lead to a loss of safety functions. Possible measures for excluding faults and information on fault exclusion are provided in table D.4 of the standard EN ISO 13849-2.

Observed errors	Fault exclusion	Remarks
Short circuit between any two conductors	Short circuits between conductors that are either: - Permanently installed and protected from external damage, e.g. by cable duct or armored conduit - In different sheathed cables - Inside an electrical installation space (see note) - Individually protected by a ground connection	The lines as well as the installation space must correspond to the respective requirements (see IEC 60204-1)
Short circuit between any conductor and an unprotected conductive part, the ground or a grounding conductor connection	Short circuits between conductors and any unprotected conductive part inside an installation space (see note)	
Interruption of a conductor	No	–

Tab. 13: EN ISO 13849, table D.4 – Errors and measures for excluding faults – lines/cables

11.2.3   Monitoring by means of plausibility check of the signals

The state of the connecting wiring and the function of the safety channels can be verified with a plausibility check.

In order to check the plausibility of the activation signals of both the STO_a and STO_b inputs against the STO status signals, perform an STO function test before each deactivation of the STO function.

Deviating test cycles may be necessary depending on the respective application area, the intended use of the safety relay or machine-specific and system-specific requirements.

In the event of an error, always switch the device off using the other STO input and then correct the error.

11.2.3.1   STO function test

An STO function test requires that both STO_a and STO_b signals be switched in alternation and checked for plausibility with the resulting STO status signals. In the event of a fault, the safety function must be activated at both STO inputs. The drive controller must no longer be enabled.

STO_{status} is made available directly on terminal X12 of the drive controller for monitoring purposes. If you are working with a fieldbus system, you can access detailed status information by transmitting parameter E67 STO status, array E67[0] – E67[2]. They can be used as an alternative to STO_{status} for the plausibility check.

In applications with increased safety requirements such as SIL 3 or PL e, a safety controller must check the connecting wiring. In applications with reduced safety requirements up to SIL 2, PL d, a standard controller can perform the STO function test. More information on the use of a standard controller can be found in the IFA Report 2/2016 *Sicherheitsbezogene Anwendungssoftware von Maschinen – die Matrixmethode des IFA* (Safety-related application software for machinery – The IFA matrix method); see the chapter 9.5 *Einsatz von Standardkomponenten für fehlerbeherrschende Maßnahmen*.

Information

During the STO function test, the drive controller switches to the **switch-on lockout** operating state.

Switch sequences and test results

The following graphic shows the switch sequences of STO_a and STO_b as well as the expected results. All test results deviating from this must be considered errors. If this is the case, check the wiring, correct any potential errors and repeat the STO function test. If errors reappear, take advantage of our services and contact STOBER Support.

Information

Be aware that the test pulses may last a maximum of 500 ms. Starting at 500 ms, the drive controller rates the pulses as an inconsistent request and switches to the **fault** operating state.
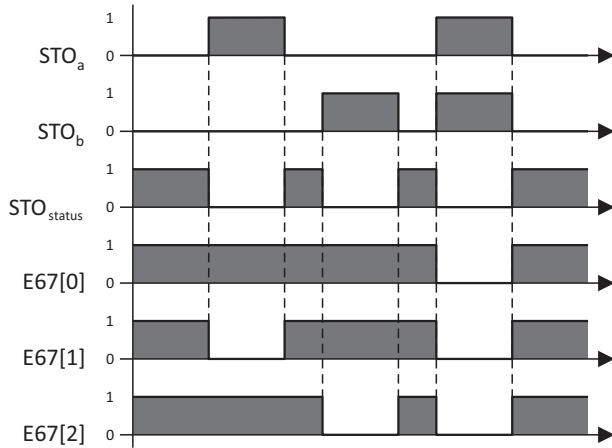
Fig. 7: Function test – Switch sequences

STO$_a$, STO$_b$	Inputs of both safety channels
STO$_{status}$	STO status signal at terminal X12
E67[0]	At least one safety channel requests STO activation (STO$_a$ = 0 V or STO$_b$ = 0 V)
E67[1]	STO$_a$ requests STO activation (STO$_a$= 0 V)
E67[2]	STO$_b$ requests STO activation (STO$_b$= 0 V)

STO function test for drive controller parallel connection

Be aware that the STO$_{status}$ outputs cannot be connected in series for diagnostics.

> **Information**
>
> In order to ensure correct wiring of the drive controller parallel connection, you must check the STO$_{status}$ signal of each drive controller separately.

11.3   Calculation of suitable protective measures – Examples

In order to be able to assess and calculate the suitable protective measures necessary for a system, the accompanying safety-related parts on machine control systems must meet the specified requirements.

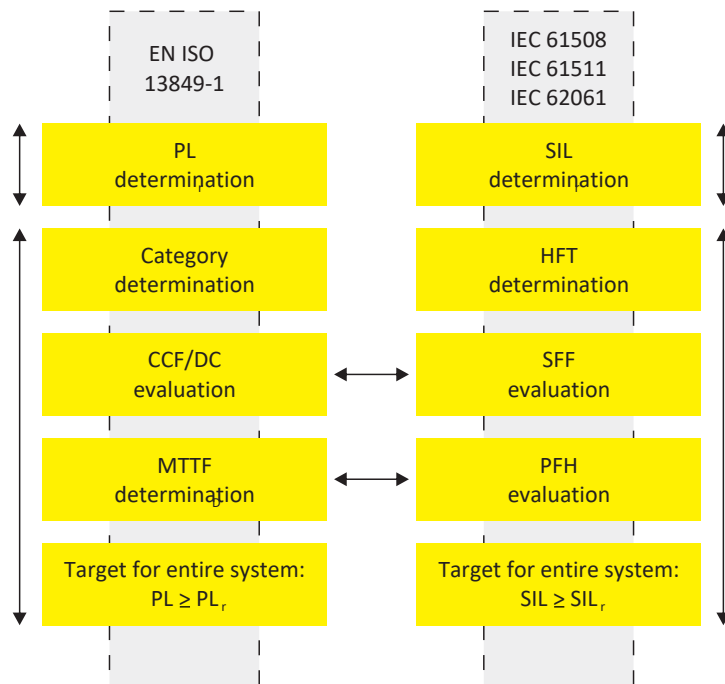| EN ISO 13849-1	IEC 61508 / IEC 61511 / IEC 62061
PL determination	SIL determination
Category determination	HFT determination
CCF/DC evaluation ↔	SFF evaluation
MTTF determination ↔	PFH evaluation
Target for entire system: $PL \geq PL_r$	Target for entire system: $SIL \geq SIL_r$

Fig. 8: Determining and assessing protective measures

In order to determine the necessary PL for a system, we recommend abiding by a fixed workflow.
Before making the actual calculations, all safety-related components whose failure may interfere with the activation of the safety functions should be recorded in a schematic diagram.

A block diagram that divides the entire system into individual subsystems can be derived from the schematic diagram. For each subsystem, the safety-related figures are either taken from the accompanying manufacturer information or specified sources. If you need to calculate the figures yourself, the openly available software SISTEMA[3] provides reliable assistance.

The following chapters show the implementation of the STO and SS1-t safety functions based on example schematic and block diagrams as well as the accompanying calculation of required safety figures for the individual systems and finally for the entire system.

---

[3] Software provided free of charge by the German Social Accident Insurance (DGUV) for assessing safety-related machine control systems and for the standard-compliant calculation of safety figures.

11.3.1 STO – Creating schematic and block diagrams

In order to be able to calculate the protective measures suited for a system, start by generating a schematic diagram of your system with all relevant components. Safety-related block diagrams can then be derived from this schematic diagram.

11.3.1.1 Generating a schematic diagram

The following graphic shows uses the implementation of the STO safety function in conjunction with a movable, separating safety device with position switch as an example. The safety function is triggered by opening the safety door.

The schematic diagram includes the wiring of the position switch, the connection of the STO_a and STO_b inputs, a safety relay and a controller. Moreover, it illustrates the interaction between the sensor technology and logic.[4]
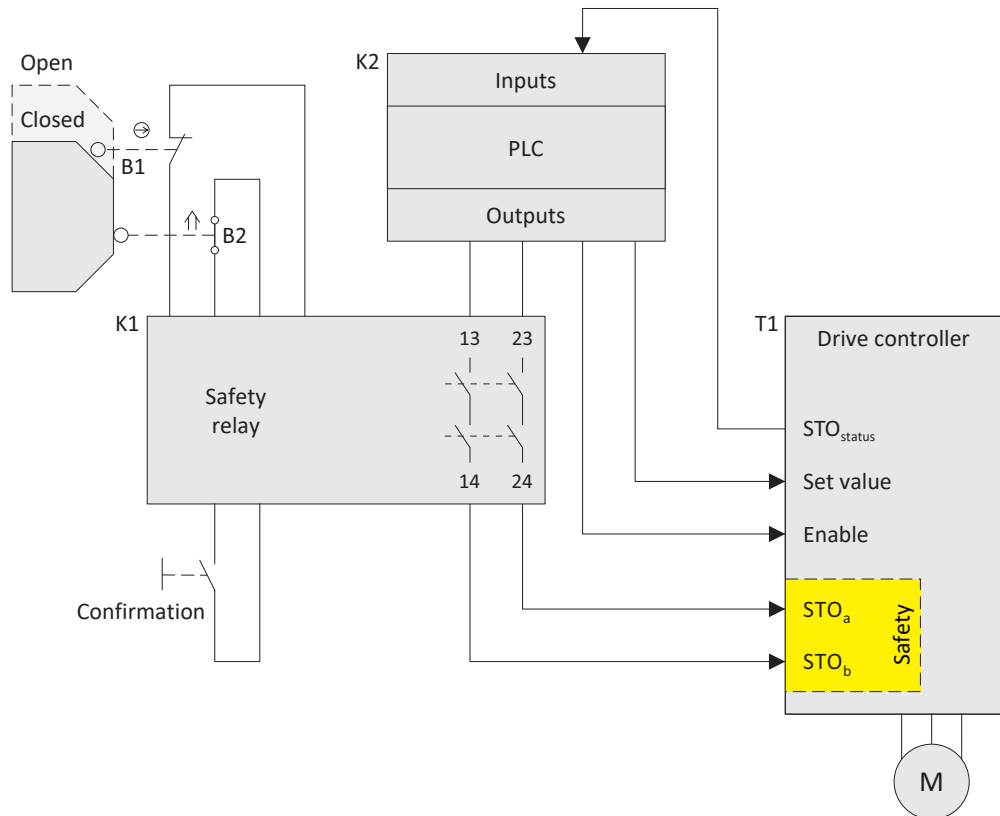
Fig. 9: STO – Schematic diagram

B1, B2	Position switches
K1	Safety relay
K2	Controller
T1	Drive controller with integrated ST6 safety module

---
[4] Schematic diagram and accompanying explanation are based on an IFA report, 07 / 2013, p. 64ff.

Explanation

The drive function is controlled by the PLC K2. It transmits target values to drive controller T1, switches both STO_a and STO_b inputs and can start and stop the drive using an enable signal. The PLC is not involved in the safety function.

The danger point is protected by a movable, isolating safety door. The two position switches B1 and B2 detect when the protective device is opened, which is then also analyzed by the safety relay K1. K1 switches off the STO inputs in drive controller T1, independent of the PLC. This safely prevents the generation of a rotating magnetic field in the drive.

The safety relay K1 detects any potential errors in the position switches by using a plausibility comparison. K1 is equipped with the appropriate self-monitoring functions that open the enable paths when errors are detected.

A malfunction of the ST6 safety module triggers the STO safety function and prevents the drive from restarting in the event of an error.

Faulty STO connection wiring of K1, K2 and T1 can, if needed, be detected by the PLC K2 through a plausibility comparison. In this case, the drive controller T1 transmits a corresponding STO status message to the PLC K2. This becomes part of the safety circuit.

11.3.1.2   Creating block diagrams

Block diagrams focus on the connections between design and logic for the components of the accompanying schematic diagram.
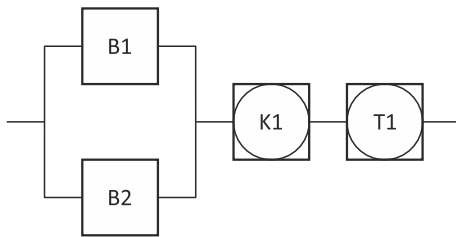

Fig. 10: Safety-related block diagram

B1, B2	Position switches
K1	Safety relay (encapsulated subsystem)
T1	Drive controller with integrated ST6 safety module (encapsulated subsystem)

Each component of a safety function is part of a specific permanent structure. This is referred to as the category in EN ISO 13849-1. The categories form the basis for the calculation of the resulting safety figures, e.g. in the SISTEMA software. In this process, a subsystem represents either a group of category blocks or a safety component with manufacturer information on PL, category, PFH, etc. (= encapsulated subsystem).
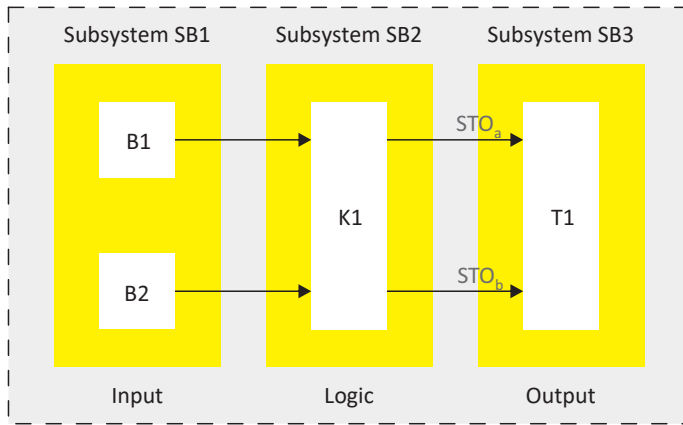
Fig. 11: Safety-related block diagram with subsystems

SB1 – SB3	(Encapsulated) subsystems 1 – 3
B1, B2	Position switches
K1	Safety relay
T1	Drive controller with integrated ST6 safety module

The protective device with the position switches forms subsystem 1, the safety relay forms subsystem 2, the drive controller along with integrated ST6 safety module is represented by subsystem 3.

Design features

Fundamental, established safety principles such as the requirements for the controller structure of category B are observed; protective wiring systems (e.g. contact fuse protection, grounding for the control circuit) are provided.

Cross circuits and short circuits in electrical connection lines are to be taken into account during planning according to EN ISO 13849-2, Table D.4. Errors that arise must be detected and brought to a safe state. Alternatively, the lines can be routed in such a way as to exclude any possible short circuits or cross circuits.

The starting mechanism must be properly designed and installed for the electromechanical position switches B1 and B2. Actuation elements and position switches are to be protected from changes in position. Only rigid mechanical parts may be used (no spring elements). The position switch B1 is an established component in accordance with EN ISO 13849-2, Table D.3 with a positively driven contact in accordance with EN 60947-5-1, Appendix K.

The safety relay fulfills the requirements of category 4 and PL e.

T1 indicates a drive controller with integrated STO safety function. The requirements of category 4 and PL e are met.

11.3.2   SS1 – Creating schematic and block diagrams

In order to be able to calculate the protective measures suited for a system, start by generating a schematic diagram of your system with all relevant components. Safety-related block diagrams can then be derived from this schematic diagram.

11.3.2.1   Generating a schematic diagram

The following graphic shows uses the implementation of the SS1-t safety function in conjunction with a movable, isolating protective device with position switches as an example. The safety function is triggered by opening the safety door.

The schematic diagram contains the wiring of the position switches, the connection of STO_a and STO_b inputs, a safety relay with switch-off delay contacts and a controller. Moreover, it illustrates the interaction between the sensor technology and logic.
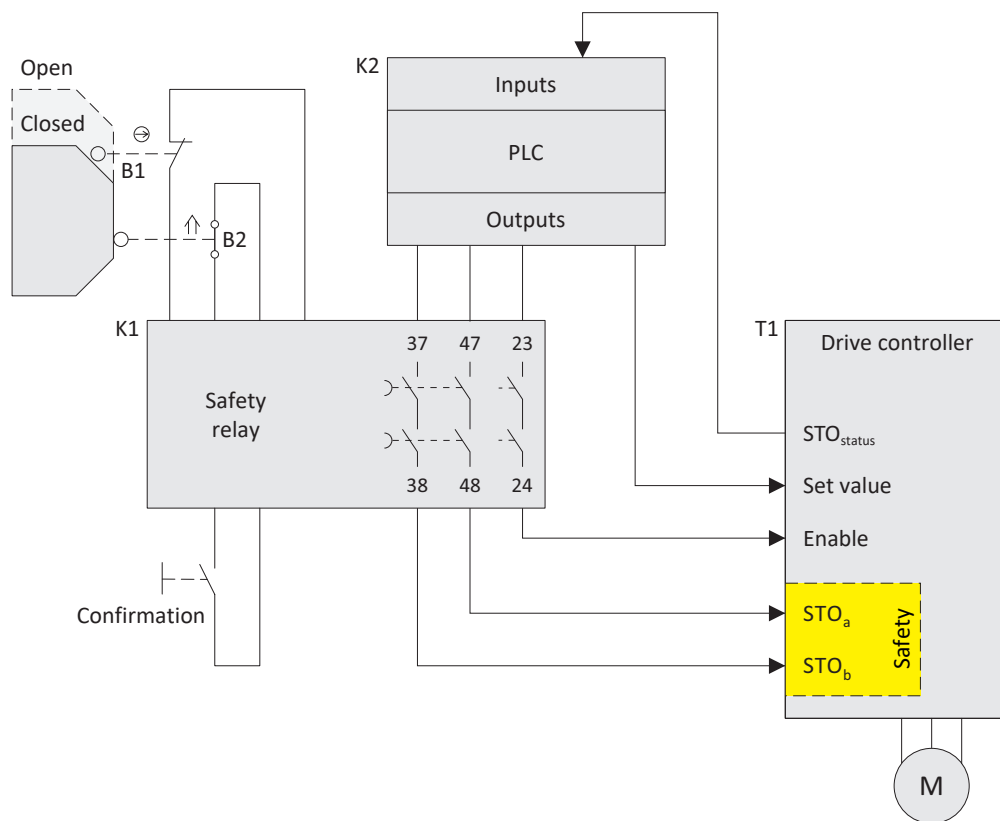
Fig. 12: SS1 – Schematic diagram

B1, B2	Position switches
K1	Safety relay
K2	Controller
T1	Drive controller with integrated ST6 safety module

Explanation

The drive function is controlled by the PLC K2. It transmits target values to drive controller T1, switches both STO_a and STO_b inputs and can start and stop the drive using an enable signal. The PLC is not involved in the safety function.

The danger point is protected by a movable, isolating safety door. The two position switches B1 and B2 detect when the protective device is opened, which is then also analyzed by the safety relay K1.

The STO inputs are switched off after a defined delay time has passed, independent of the PLC, via the switch-off delayed enable paths of the safety relay K1. Either the drive controller or PLC can be brought to a stop safely during this delayed STO switch-off of the drive. If the drive controller triggers the stopping, as in this example, there is the option of activating and parameterizing the function **quick stop during enable-off**.

The safety relay K1 detects any potential errors in the position switches by using a plausibility comparison. K1 is equipped with the suitable self-monitoring functions that open the enable paths in the event that errors are detected.

A malfunction of the ST6 safety module triggers the STO safety function and prevents the drive from restarting in the event of an error.

Faulty STO connection wiring of K1, K2 and T1 can, if needed, be detected by the PLC K2 through a plausibility comparison. In this case, the drive controller T1 transmits a corresponding STO status message to the PLC K2. This becomes part of the safety circuit.

11.3.2.2   Creating block diagrams

Block diagrams focus on the connections between design and logic for the components of the accompanying schematic diagram.
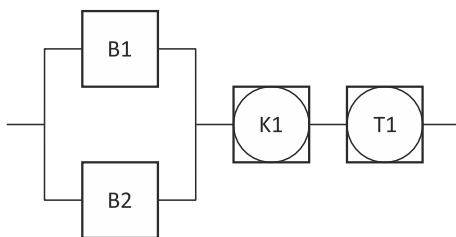

Fig. 13: Safety-related block diagram

B1, B2	Position switches
K1	Safety relay (encapsulated subsystem)
T1	Drive controller with integrated ST6 safety module (encapsulated subsystem)

Each component of a safety function is part of a specific permanent structure. This is referred to as the category in EN ISO 13849-1. The categories form the basis for the calculation of the resulting safety figures, e.g. in the SISTEMA software. In this process, a subsystem represents either a group of category blocks or a safety component with manufacturer information on PL, category, PFH, etc. (= encapsulated subsystem).
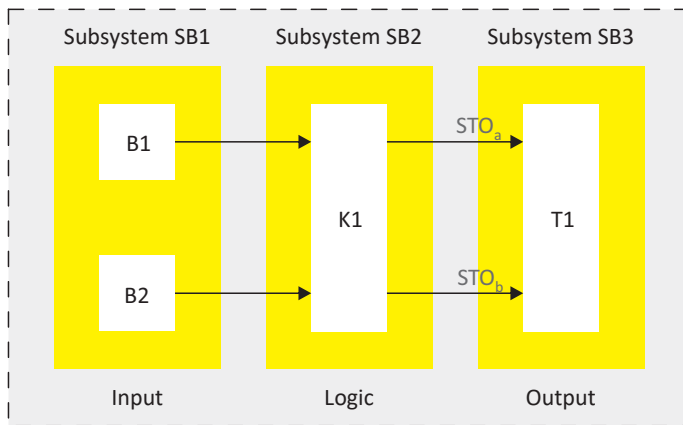
Fig. 14: Safety-related block diagram with subsystems

SB1 – SB3	(Encapsulated) subsystems 1 – 3
B1, B2	Position switches
K1	Safety relay
T1	Drive controller with integrated ST6 safety module

The protective device with the position switches forms subsystem 1, the safety relay forms subsystem 2, the drive controller along with integrated ST6 safety module is represented by subsystem 3.

Design features

Fundamental, established safety principles such as the requirements for the controller structure of category B are observed; protective wiring systems (e.g. contact fuse protection, grounding for the control circuit) are provided.

Cross circuits and short circuits in electrical connection lines are to be taken into account during planning according to EN ISO 13849-2, Table D.4. Errors that arise must be detected and brought to a safe state. Alternatively, the lines can be routed in such a way as to exclude any possible short circuits or cross circuits.

The starting mechanism must be properly designed and installed for the electromechanical position switches B1 and B2. Actuation elements and position switches are to be protected from changes in position. Only rigid mechanical parts may be used (no spring elements). The position switch B1 is an established component in accordance with EN ISO 13849-2, Table D.3 with a positively driven contact in accordance with EN 60947-5-1, Appendix K.

The safety relay fulfills the requirements of category 4 and PL e.

T1 indicates a drive controller with integrated STO safety function. The requirements of category 4 and PL e are met.

11.3.3 Determining the safety figures

In order to determine the safety figures for the entire system, the key figures of the individual subsystems must be investigated, calculated and evaluated. As the subsystems in both examples (STO and SS1) are nearly identical, the following chapter applies to STO as well as SS1.

11.3.3.1 Subsystem SB1

Subsystem SB1 contains both position switches B1 and B2. The mechanical switches of type PSEN me4 from Pilz GmbH und Co. KG serve as a specific example in this case.

Average Diagnostic Coverage – DC_{avg}

- DC_{avg} of subsystem SB1: 99%

- B1 and B2 are monitored for plausibility, cross circuits and short circuits using the safety relay K1.

Source: DIN EN ISO 13849-1, Appendix E, Table E.1

Failure resulting from common cause – CCF

The following measures are taken in order to fulfill the requirements for the prevention of errors from a common cause. For each measure category, a specific number of points are allotted. The maximum value for CCF is 100 points. At 65 points, all CCF requirements are considered to be fulfilled.

- Separation of the wiring: 15 points in category "Isolation/Separation"

- Use of NC and NO contacts: 20 points in category "Diversity"

- Protection from overvoltage and use of tried-and-tested components: 20 points in category "Design/Application/Experience"

- FMEA of the wiring example: 5 points in category "Assessment/Analysis"

- Position switches are set in accordance with the manufacturer specification: 10 points in category "Setting"

- -> CCF of subsystem SB1: 70 total points

Source: DIN EN ISO 13849-1, appendix F, table F.1

Nominal life span – B_{10D}

For the position switch with positive opening B1, fault exclusion for the electrical contact is possible. For the electrical NO contact of B2, the B_{10D} value is taken from 2000000 cycles. This is also true for the mechanical part of B1 and B2.

- $B1_{(NC)}$
  Elimination of dangerous component errors possible for the electrical contact
  B_{10D} (mechanical): 2,000,000 cycles

- $B2_{(NO)}$
  B_{10D} (mechanical): 2,000,000 cycles

- $B2_{(NO)}$
  B_{10D} (electrical): 2,000,000 cycles

Source: Pilz GmbH und Co. KG

Information

If the manufacturer does not provide any figure, figures can be taken from table C.1 in Annex C of DIN EN ISO 13849-1.

Switching frequency – n$_{op}$

With 365 working days per year, 16 working hours per day and a cycle time of 5 minutes, this amounts to a respective switching cycle of n$_{op}$ = 70080 cycles/year for B1 and B2.

Source: DIN EN ISO 13849-1, Appendix C, Table C.1, calculation: SISTEMA

Mean time to dangerous failure – MTTF$_D$

- B1
  MTTF$_D$: 285 years

- B2
  MTTF$_D$: 143 years

Calculation: SISTEMA

Probability of a dangerous failure – PFH$_D$

B1 and B2
PFH$_D$: 2.47×10^{-8}

Calculation: SISTEMA

11.3.3.2   Subsystem SB2

Subsystem SB2 is an encapsulated subsystem, i.e. a safety component where the PL, PFH and category are already specified by the manufacturer.

Subsystem SB2 includes the safety relay K1. The type PNOZ S5 device from Pilz GmbH und Co. KG serves as a specific example here.

Performance Level – PL, category

- PL = e

- Category = 4

Source: Pilz GmbH und Co. KG

Probability of a dangerous failure – PFH$_D$

- Undelayed contacts (STO)
  PFH$_D$ = 2.31×10^{-9} [1/h]

- Switch-off delaying contacts (SS1)
  PFH$_D$ = 2.34×10^{-9} [1/h]

Source: Pilz GmbH und Co. KG

04/2021 | ID 442478.02

11.3.3.3 Subsystem SB3

Subsystem SB3 is also an encapsulated subsystem for which the safety-related data is designated by the manufacturer.

Subsystem SB3 includes the drive controller T1 of the SD6 series, including the ST6 safety module.

Performance Level – PL and category

- PL = e
- Category = 4

Source: STÖBER Antriebstechnik GmbH + Co. KG

Probability of a dangerous failure – PFH$_D$

$PFH_D = 5 \times 10^{-9}$ [1/h]

Source: STÖBER Antriebstechnik GmbH + Co. KG

11.3.3.4 Wiring the subsystems

Safety relay K1 is configured and wired so that it monitors position switches B1 and B2 and their wiring for plausibility, cross circuits and short circuits. Due to the installation of these components inside an electrical installation space, exclusion of faults in accordance with EN ISO 13849-2, Appendix D, Table D 5.2 is assumed for the wiring between safety relay K1 and drive controller T1.

11.3.3.5 Safety figures for the entire system

The following table includes safety figures for individual subsystems and the resulting probability of a total failure.

Subsystem	Value source	Probability of a dangerous failure [1/h]
SB1 – Input	SISTEMA calculation	$PFH_D = 2.47 \times 10^{-8}$
SB2 – Logic	Manufacturer information	$PFH_D = 2.31 \times 10^{-9}$ (STO) $PFH_D = 2.34 \times 10^{-9}$ (SS1)
SB3 – Output	Manufacturer information	$PFH_D = 5.0 \times 10^{-9}$
Entire system	SISTEMA calculation	$PFH_D = 3.2 \times 10^{-8}$

Tab. 14: PFH$_D$ – Subsystems and entire system

The determination and calculation of the dangerous failure probability per hour for the example systems with the STO and SS1 safety functions result in a value of 3.2×10^{-8} [1/h], which corresponds to the respective system PL e and a SIL 3 in a high, continuous operating mode (see following table).

Performance Level	Probability of a dangerous failure [1/h]	Safety Integrity Level
a	$\geq 10^{-5}$ to $< 10^{-4}$	No corresponding level
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Tab. 15: PL, PFH_D, SIL – Entire system

In addition to the requirements for the probability of failure, structural requirements must be taken into account when determining the Performance Level.

The SB1 – SB3 subsystems fulfill the minimum requirements of category 4 systems regarding controller structures:

- DC_{avg}: High

- CCF: Requirement fulfilled

- $MTTF_D$: High

11.4 ST6 in accordance with interface classification (ZVEI)

The German Electrical and Electronic Manufacturer's Association (ZVEI) published a policy document in 2016 (see the chapter Further information [▶ 46]) that addresses the classification of binary 24 V_{DC} interfaces in the field of functional safety.

The policy document defines technical terms, works out the characteristic features of the individual interface types with dynamic test pulses and describes manufacturer-specific product information and technical data for the interface types in question.

Based on the classification presented in this policy document, the ST6 safety module can be used as a data sink (sink) for interface types C and D and activated using information sources (sources) of the same interface types.
Data sinks and sources of interface types C and D are divided into classes according to the time behavior of the test pulses, where a higher class indicates shorter test pulses. When combining data sinks and sources, it is important to ensure that a selected source at least belongs to the same class as the selected data sink.
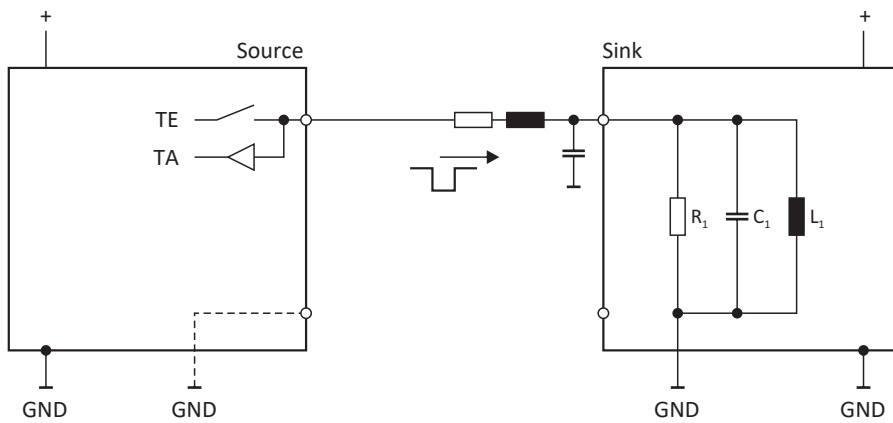
Interface type C

Fig. 15: Interface classification – Interface type C

TE	Test pulse generation
TA	Test pulse assessment
GND	Reference potential
R_1	Input resistance
C_1	Input capacitance
L_1	Input inductance

Interface type C[5] is often used as an OSSD output, such as for safety outputs for light barriers and proximity switches (with defined behavior under fault conditions in accordance with EN 60947-5-3). The corresponding devices act as a source for checking the function of their outputs using test pulses; the corresponding data sink, e.g. ST6 safety module, is not allowed to react to these test pulses by definition.
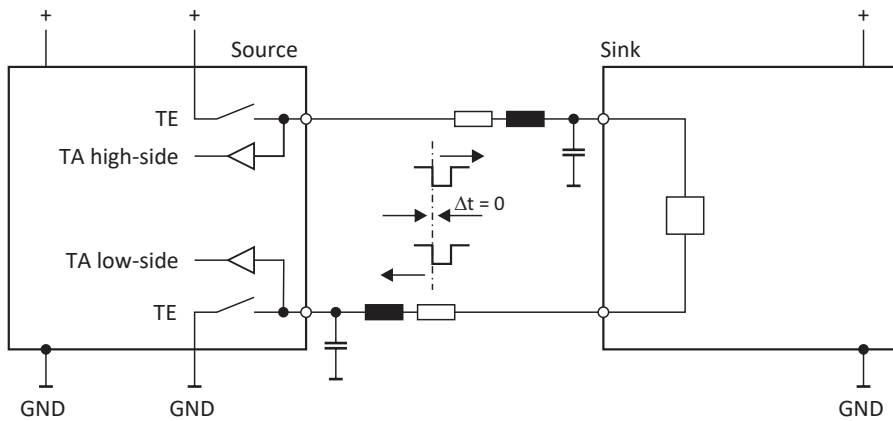
Interface type D

Fig. 16: Interface classification – Interface type D

TE	Test pulse generation
TA	Test pulse assessment
TA high-side	Test pulse assessment high-side switch
TA low-side	Test pulse assessment low-side switch
GND	Reference potential
Δt_i	Interval

---

[5] See ZVEI, p. 13ff.

Interface type D[6] is intended either for safely switching actuators (contactors, motors, valves) or for fully de-energizing electrical/electronic modules and devices of their operating voltage. The difference from the pure pulse-switching output of interface type C is primarily the circuitry and the testing of the return circuit.

Possible return circuit errors such as short circuits can be detected against 0 V. This connection type prevents voltage carryover through a shared floating 0 V connection point.

There is also the option of a two-channel switch-off over two lines. An individual short circuit on one of the conductors consequently does not lead to improper switching of the actuator. For this, the source transmits test pulses to the data sink, which are in turn evaluated by the source. The test pulses are neither distorted nor delayed by the data sink.

The data sink, e.g. an ST6 safety module, can contain inductive, capacitive and ohmic portions. The source is typically a safety controller or a safety relay with a bipolar output.

[6] See ZVEI, p. 17ff.

12 Appendix

12.1 Further 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
SD6 drive controller	Manual	System design, technical data, project configuration, storage, installation, connection, commissioning, operation, service, diagnostics	

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

Deutsche Gesetzliche Unfallversicherung, 2013. *Sichere Antriebssteuerungen mit Frequenzumrichtern* (Safety drive controls with frequency converters) [online]. *IFA Report 7 / 2013*.
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Accessed on 2016-08-01]. Available at

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), 2010. *Das SISTEMA-Kochbuch 1. Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA* (The SISTEMA Cookbook 1. From the circuit diagram to the Performance Level – Quantification of safety functions with SISTEMA) [online]. *Version 1.0 (DE) / 2010*.
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Accessed on 2016-08-01]. Available at

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA). *SISTEMA 1.1.9* [Software]. *Bewertung von sicherheitsbezogenen Maschinensteuerungen nach DIN EN ISO 13849.* (A Tool for the Easy Application of the Control Standard EN ISO 13849-1)
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Accessed on 2016-08-01]. Available at

Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI). *Klassifizierung binärer 24-V-Schnittstellen mit Testung im Bereich der Funktionalen Sicherheit* (Classification of binary 24 V interfaces with testing in functional safety) [online]. Edition 2.0, *November 2016*.
Frankfurt am Main: ZVEI – Zentralverband Elektrotechnik- und Elektroindustrie e. V. (Fachverband Automation) (German Electrical and Electronic Manufacturer's Association, professional association: Automotive)
[Accessed on 2016-11-17]. Available at

12.2 Formula symbols

Symbol	Unit	Explanation
B_{10D}	–	Number of cycles until 10% of components have failed dangerously
C_1	F	Input capacitance
C_{1max}	F	Maximum input capacitance
DC	%	Diagnostic coverage
DC_{avg}	%	Average diagnostic coverage
Δt	s	Timespan
I_{max}	A	Maximum current
I_{1max}	A	Maximum input current
I_{1off}	A	Input current in OFF state
I_{1on}	A	Input current in ON state
L_1	H	Input inductance
MTTF	Year, a	Average time before failure
$MTTF_D$	Year, a	Average time before dangerous failure
n_{op}	1/a	Average number of annual actuations (switching frequency)
p	–	Number of pole pairs
PFH_D	1/h	Average probability of a dangerous failure per hour
R_1	Ω	Input resistance
T_i	ms	Test pulse interval
t_i	µs	Test pulse duration
T_M	Year, a	Mission time
U_1	V	Input voltage
U_{1max}	V	Maximum input voltage
U_2	V	Output voltage

12.3   Abbreviations

Abbreviation	Meaning
AWG	American Wire Gauge
CCF	Common Cause Failure
EMC	Electromagnetic Compatibility
FMEA	Failure Modes and Effects Analysis
HFT	Hardware Fault Tolerance
OSSD	Output Signal Switching Device
PDS(SR)	Power Drive System(Safety Related)
PELV	Protective Extra Low Voltage
PFH, PFH_D	Probability of a (dangerous) Failure per Hour
PL	Performance Level
PWM	Pulse Width Modulation
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIL CL	Safety Integrity Level Claim Limit
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
TA	Test Pulse Assessment
TE	Test Pulse Generation
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie (en: German Electrical and Electronic Manufacturers' Association)

13 Contact

13.1 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 system support?:
Phone +49 7231 582-3060
systemsupport@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

13.2 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

13.3   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 +90 216 510 2290 sales-turkey@stober.com
STOBER JAPAN www.stober.co.jp Phone +81 3 5875 7583 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	

Glossary

Average Diagnostic Coverage (DC_{avg})

In accordance with DIN EN ISO 13849-1: Average diagnostic coverage. Measure for the effectiveness of diagnostics, which can be determined as a ratio of the failure rate of detected dangerous failures and the failure rate of all dangerous failures. It can apply to the entire system or parts of a safety-related system.

B_{10D} value

In accordance with DIN EN ISO 13849-1: Number of cycles until 10% of the components have failed dangerously (for pneumatic and electromechanical components).

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.

Class

In accordance with the German Electrical and Electronic Manufacturers' Association: Amount of data sources and sinks with compatible technical data in terms of test pulses within an interface type.

Common cause failure (CCF)

Failure due to a common cause. In accordance with DIN EN 61800-5-2: Failure that is the result of one or multiple events that cause simultaneous failures of two or more isolated channels in a multi-channel system and lead to safety function failure.

Data sink (sink)

In accordance with the German Electrical and Electronic Manufacturers' Association (ZVEI): Receiver of information from a data source. A data sink features an input that is connected to the output of the source. A data sink can fulfill the requirements of various interface types at the same time. The term "data sink" refers to the evaluation of information, not to the evaluation of the associated test pulses.

Data source (source)

In accordance with the German Electrical and Electronic Manufacturers' Association (ZVEI): Sender of information to the data sink. The source features an output that is connected to the input of the sink. A source can fulfill the requirements of various interface types at the same time. The term "data source" refers to the generation of information, not to the generation of the associated test pulses.

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.

Interface type

In accordance with the German electrical and Electronic Manufacturers' Association (ZVEI): Standardized interface between senders ("data sources") and receivers ("data sinks") of signals with specifications about generation by evaluating the associated test pulses.

Mean time to dangerous failure (MTTF$_D$)

In accordance with DIN EN ISO 13849-1: Expected value for the average time before dangerous failure of systems or modules. Statistical value that is determined through trials and empirical values. Does not claim a guaranteed life span or guaranteed failure-free time.

Mission time (T$_M$)

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

NOR gate

NOT-OR gate. Gates are binary signal states (0 or 1) of variables connected together by a function. All gate variants can be realized with the negation NOT and the operators AND and OR. A NOR gate reverses the result of an OR link, i.e. the output variable only has the signal 1 if all input variables supply a 0 signal.

OSSD output

Output with integrated test pulses. During operation, the associated devices use short test pulses to check the function of this output type.

Performance Level (PL)

In accordance with DIN EN ISO 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.

Power Drive System(Safety Related) (PDS(SR))

In accordance with DIN EN 61800-5-2: Electrical power drive system with integrated safety function and adjustable speed that is suited for use in safety-related applications.

Probability of a dangerous failure per hour (PFH$_D$)

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.

Probability of a failure per hour (PFH)

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

Safety Related Part of a Control System (SRP/CS)

In accordance with DIN EN ISO 13849-1: Safety-related part of a controller that reacts to safety-related input signals and generates safety-related output signals.

STO reaction time

Time between activation of the STO safety function (edge from 1 to 0) and disabling of the pulse pattern on the power unit.

STO response time

Time between activation or deactivation of the STO safety function and feedback in the STO status signals.

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.

Switching frequency (n_{op})

In accordance with DIN EN ISO 13849-1: Average number of annual actuations.

Test pulse

In accordance with the German Electrical and Electronic Manufacturers' Association: Temporary change of a signal voltage level for checking whether the output or device functions properly or for checking the transmission path.

Test pulse assessment (TA)

In accordance with the German Electrical and Electronic Manufacturers' Association: Part of the circuit that assesses the test pulse needed for diagnostic testing.

Test pulse generation (TE)

In accordance with the German Electrical and Electronic Manufacturers' Association: Part of the circuit that generates the test pulse needed for diagnostic testing.

List of figures

List of tables

STÖBER

www.stober.com