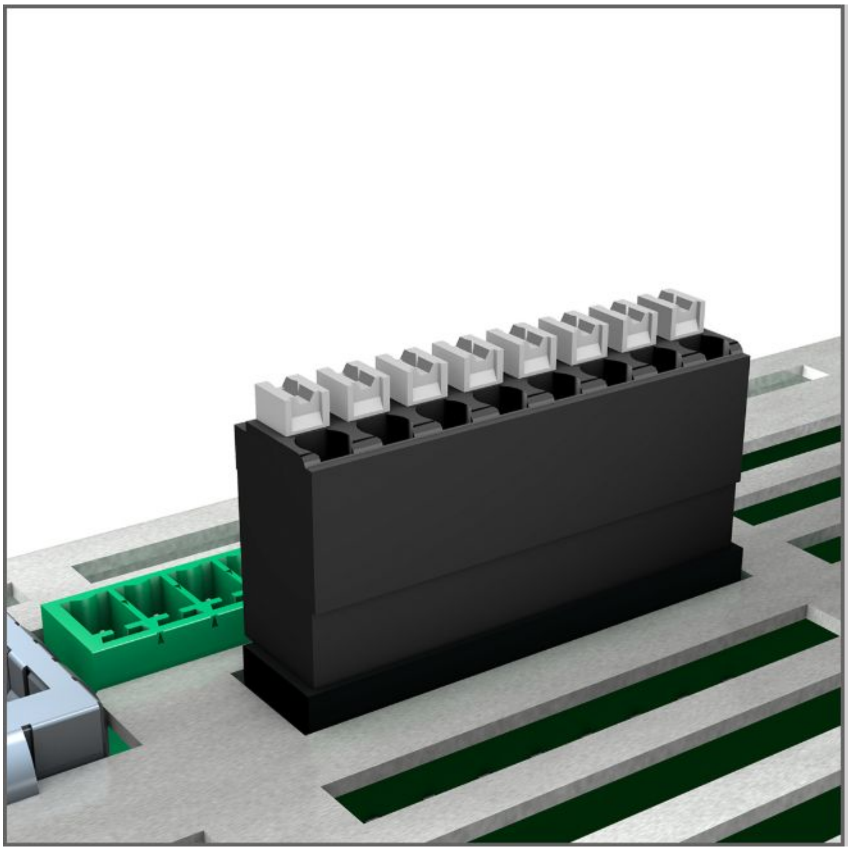
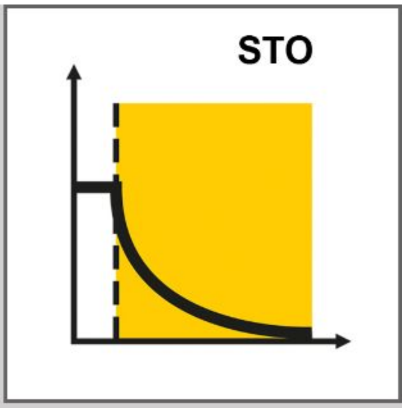
Safety module SR6
Manual





stober.com

en-US
03/2017
ID 442741.00

Table of contents

03/2017 | ID 442741.00

1 Foreword

The SR6 safety module adds the Safe Torque Off (STO) safety function (described in the DIN EN 61800-5-2 standard) to the SI6 series device types of the 6th generation of STOBER drive controllers.
STO prevents a 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 SR6 safety module.

SR6 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 demands up to SIL 3, PL e, category 4. Compliance with standard requirements is ensured by an external testing institute as part of a type examination.

2 User information

This documentation provides all information on the intended use of the SI6 drive controller in combination with the SR6 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 type

This documentation is binding for:

SI6 drive controller in combination with the SR6 safety module.

2.3 Timeliness

Check whether this document is the most up-to-date version of the documentation. We provide all document versions for our products for download on our website: http://www.stoeber.de/en/download.

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.

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 identify the extent of the risk. In addition useful tips and recommendations for efficient and faultless 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.

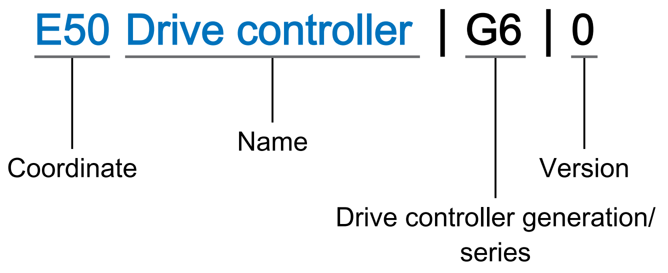
2.6.2 Markup of text elements

Certain elements of continuous text are distinguished as follows.

Quick DC-Link module	Words or expressions with a special meaning
Detailed information	Internal cross-reference
http://www.stoeber.de	External cross-reference

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.



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 European directives and standards are relevant to the product specified in this documentation:

- DIN EN ISO 13849-1:2016
- DIN EN ISO 13849-2:2013
- IEC 61800-5-2:2016 (basis for current revision of DIN EN 61800-5-2:2008)
- DIN EN 61508-x:2011
- DIN EN 60204-1:2007
- DIN EN 62061:2016

For reasons of improved readability, subsequent references to the standards do not specify the respective year.

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.

3.3 Intended use

The SR6 safety module can be combined with STOBER drive controllers from the SI6 series in sizes 0 – 3. The module must be installed and wired compliant for EMC.

If a drive controller with the integrated SR6 safety module is used in a safety-related application, the safety module must be activated by a safety relay or 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.

Unintended use

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

Information

An emergency off in accordance with DIN EN 60204-1 is not possible with the SR6 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 neither makes technical nor electrical modifications to the SR6 safety module. The safety module may not be removed from the drive controller, repaired or replaced.

Maintenance

The safety module is maintenance-free.
Take appropriate measures to detect or prevent possible errors in the connection wiring (see Monitoring the connection wiring [▶ 25]).

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.

4 Safety module SR6

The SR6 safety module adds the STO (Safe Torque Off) safety function to the SI6 drive controller . The module prevents the formation of a rotating magnetic field during 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.

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

SR6 – Features and certifications

- Two one-pin digital inputs for activating the safety functions:
  - Safe Torque Off – STO in accordance with DIN EN 61800-5-2
  - Stop category 0 in accordance with DIN EN 60204-1
- STO switch-off time < 20 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 setup and function

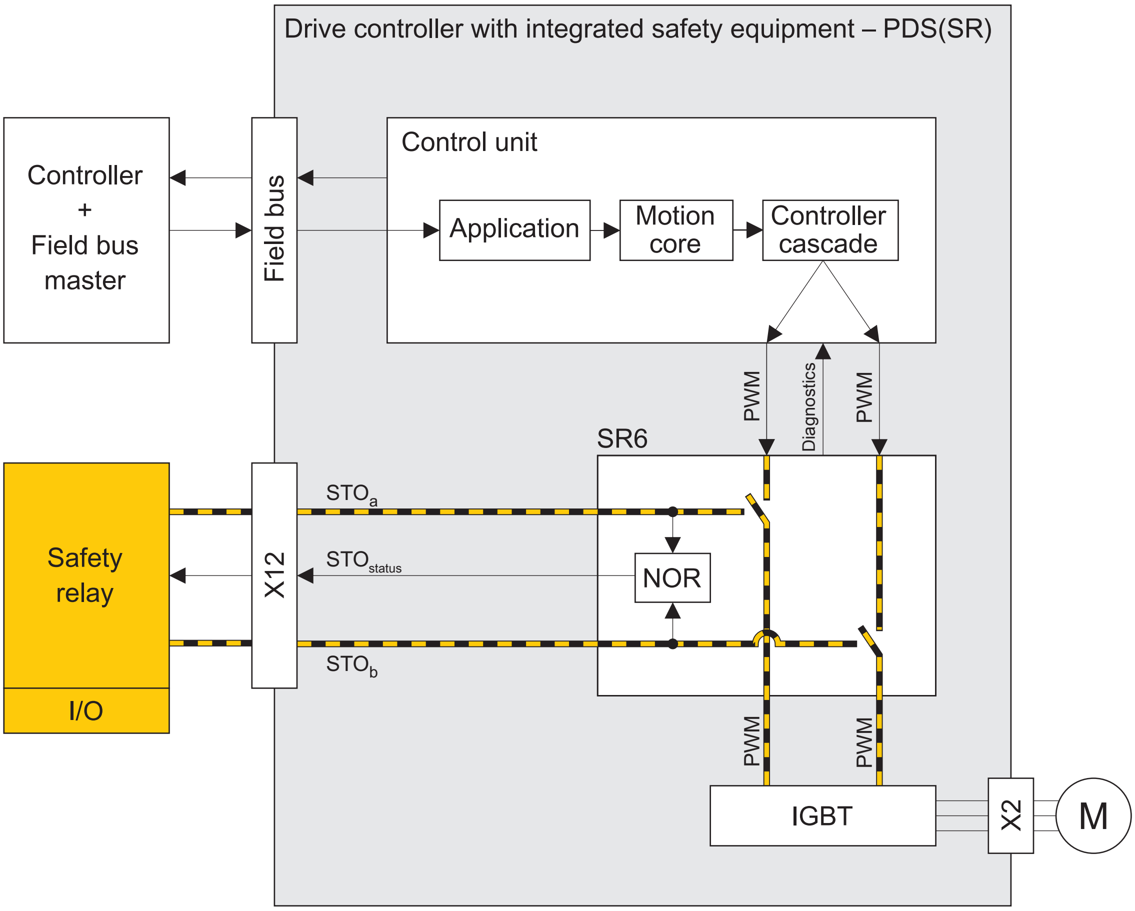


Fig. 1: Drive controller and safety module (PDS(SR)) – System setup

Function

The control unit of the drive controller generates a pulse pattern (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 SR6 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, SR6 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 corresponds to the STO safety function in accordance with DIN EN 61800-5-2. In DIN EN 60204-1, this type of switch-off is defined as stop category 0.

⚠ 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 shut-down) while the SS1-t safety function is triggered. This may result in an increased overrun distance.

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.

SR6 – Design

The SR6 module is designed with two channels. Both safety channels are independent of one another and must be activated at the corresponding STO_a (safety channel 1) and STO_b (safety channel 2) inputs at the same time, either directly via floating contacts with 24 V_{DC} or alternately via 24 V_{DC} semiconductor outputs with layered testing (such as OSSD outputs).
Using both the STO_a and STO_b inputs, rotating magnetic field generation in the drive controller is enabled or disabled.

Monitoring the connection wiring

STO status signals are provided for checking the status of the connection wiring and the function of the safety channels. These signals can be monitored and evaluated in two different ways:

- Using the STO_{status} signal
  STO_{status} is the result of a NOR link 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 SI6 terminal.
- Using parameter E67
  Parameter E67 is an array parameter that visualizes the state of both safety channels in detail.

Information

If both SR6 safety channels are controlled via OSSD outputs, their monitoring is taken over by the signal-generating controller. Potential faults are detected directly, eliminating the need to evaluate the STO status signals.

03/2017 | ID 442741.00

6 Technical data

The transport, storage and operating conditions of the safety module are found in the technical data of the respective drive controller (see Detailed information [▶ 44]).

6.1 Safety-related variables

The table includes the variables for the SR6 module relevant for safety equipment.

SIL CL	3
SIL	3
PL	e
Category	4
PFH	5×10^{-9} [1/h]
Length of use	20 years

Tab. 1: SR6 – Safety-related variables

6.2 System times

The following diagram visualizes the temporal relationships in the event of STO activation and performance; the associated values for the SI6 drive controller in combination with the SR6 safety module are found in the subsequent table.

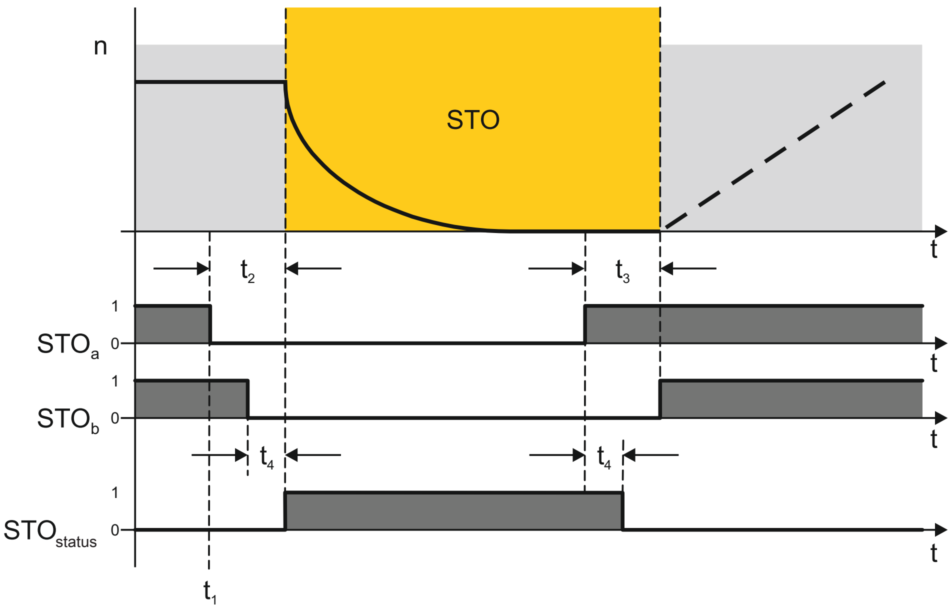


Fig. 2: STO – Temporal relationships (detailed representation)

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.

Maximum reaction time	20 ms
Maximum time difference	500 ms
Maximum response time	20 ms

Tab. 2: STO – System times

6.3 Interface classification

Due to the 24 V_{DC} interface classification from ZVEI, the SR6 safety module can be used as an 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 table apply for the SR6 used as a sink for interface types C and D[1].

	Min.	Typ.	Max.
Class		1	
Test pulse duration t_i	—	—	1000 µs
Test pulse interval T	10 ms	—	—
Input resistance R_1	300 Ω	—	—
Input capacitance C_1	—	—	1.5 nF
Input inductance L_1	—	—	10 µH

Tab. 3: SR6 – Specific figures for the interface type C

	Min.	Typ.	Max.
Class		1	
Test pulse duration t_i	—	—	1000 µs
Test pulse interval T	10 ms	—	—
Input resistance R_1	150 Ω	—	—
Input current I_{ON} in ON state	—	—	60 mA
Input current I_{OFF} in OFF state	—	—	1 mA
Input capacitance C_1	—	—	3 nF
Input inductance L_1	—	—	5 µH

Tab. 4: SR6 – Specific figures for interface type D

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

7 Connection

The SR6 safety module is connected over the X12 terminal of the respective drive controller. A device cascade is possible.

More detailed information on errors in the connection wiring, their connection and a STO function test can be found in Monitoring the connection wiring [▸ 25].

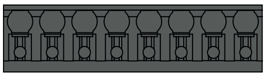
7.1 Connection compliant with EMC

The maximum cable length permitted is 30 m. Observe the associated recommendations in the documentation of the SI6 drive controller for an EMC-compliant connection (see Detailed information [▸ 44]).

7.2 X12 terminal

Specification	Electrical data
STO_a STO_b	U_{1max} = 30 V_{DC} (PELV) high level = 15 – 30 V_{DC} low level = 0 – 8 V_{DC} I_{1max} = 100 mA (typically < 30 mA for 24 V_{DC}) I_{max} = 4 A C_{1max} = 10 nF
STO_{status}	$U_2 = U_1 - (1.5\ \Omega * I_1)$
STO_{status} supply	U_1 = +24 V_{DC}, +20 % / -15 % 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	GND	Reference potential for STO_a and STO_b, internally bridged with terminal 7
	6	STO_{status}	Acknowledgment signal of safety channels 1 and 2 for diagnostic purposes
	7	GND	Reference potential for STO_a and STO_b, internally bridged with terminal 5
	8	STO_{status}	STO_{status} supply

Tab. 6: X12 connection description

Feature	Line type	Unit	Min.	Max.
Cross-section	Fine wire line without end sleeve	mm²	0.14	1.5
	Fine wire line with end sleeve without plastic collar	mm²	0.25	1
	Fine wire line with end sleeve and plastic collar	mm²	0.25	1
	According to AWG	AWG	26	18
Length	—	m	—	30
Insulation stripping length	—	mm	—	9

Tab. 7: Cable requirements

X12 wiring

The two-channel design of the SR6 with shared potential reference supports various options for connection. These depend upon whether SR6 is used via contacts or as a sink for interface type C or D from ZVEI interface classification.

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

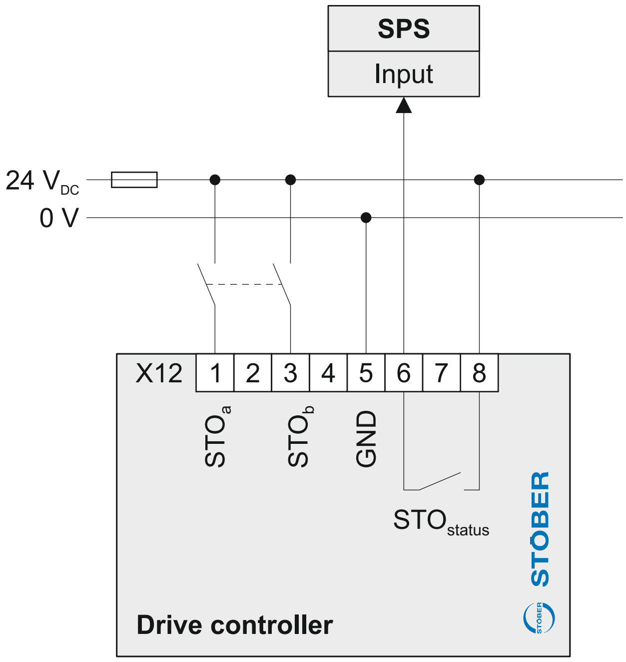


Fig. 3: X12 wiring – SR6 as sink for interface type C

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.

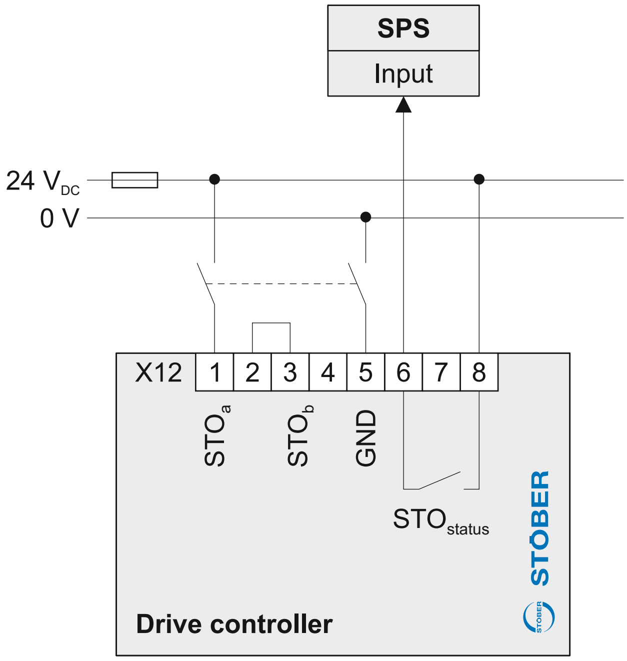


Fig. 4: Wiring for X12 – SR6 as sink for interface type D

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.

7.3 Cascading

It is possible to activate STO on multiple drive controllers simultaneously using the output of a safety relay. A chain, i.e. cascading multiple drive controllers, is possible depending on the required safety figure.

⚠ WARNING!

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

In a cascade, possible wiring or activation errors can lead to the loss of safety function for the entire cascade.

- Take appropriate measures to detect or eliminate wiring errors (see Chapter Monitoring the connection wiring [▸ 25]).
- Be aware that STO_{status} outputs cannot be cascaded.

8 Commissioning

This chapter describes how to commission the SR6 safety module and activate or deactivate the STO safety function.

Information

The SR6 safety module is a permanently integrated component in the drive controller where all design, technical and electrical modifications are prohibited!
Any removal of the safety module from the drive controller as well as any attempt at repair or replacement is prohibited. The drive controller and safety module do not require maintenance.

Detailed information for putting the SI6 drive controller into operation can be found in the accompanying start-up instructions (see Detailed information [▸ 44]).

8.1 Putting the safety module and drive controller into operation

Proceed as follows to put a drive controller with integrated SR6 safety module into operation.

1. Check whether the planned safety equipment is sufficient for the safety requirements of your entire system.
2. Wire the safety-related X12 terminal in accordance with the data contained in chapter X12 terminal [▸ 15] and eliminate any potential wiring errors (optional).
3. Connect and start up the drive controller. The accompanying start-up instructions contain detailed information on this process and associated safety notices relevant to all aspects (see Detailed information [▸ 44]).
4. Start by performing a STO function test. Proceed as described in chapter Monitoring the connection wiring [▸ 25], 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 SR6 safety module back into operation!

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 chapter System times [▶ 13]).

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

⚠ **WARNING!**

Property damage and injury to persons due to axes subject to gravitational force or motor coasting!

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

- Secure axes subject to gravitational forces through 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 activation signals of the STO_a and STO_b inputs must be activated with 24 V_{DC} within 500 ms.

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

9 SR6 and SS1

The SR6 safety module offers the option of implementing additional safety functions, such as SS1-t, if suitable external wiring is present. The SS1-t safety function in accordance with DIN EN 61800-5-2 corresponds to stop category 1 in accordance with DIN 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.

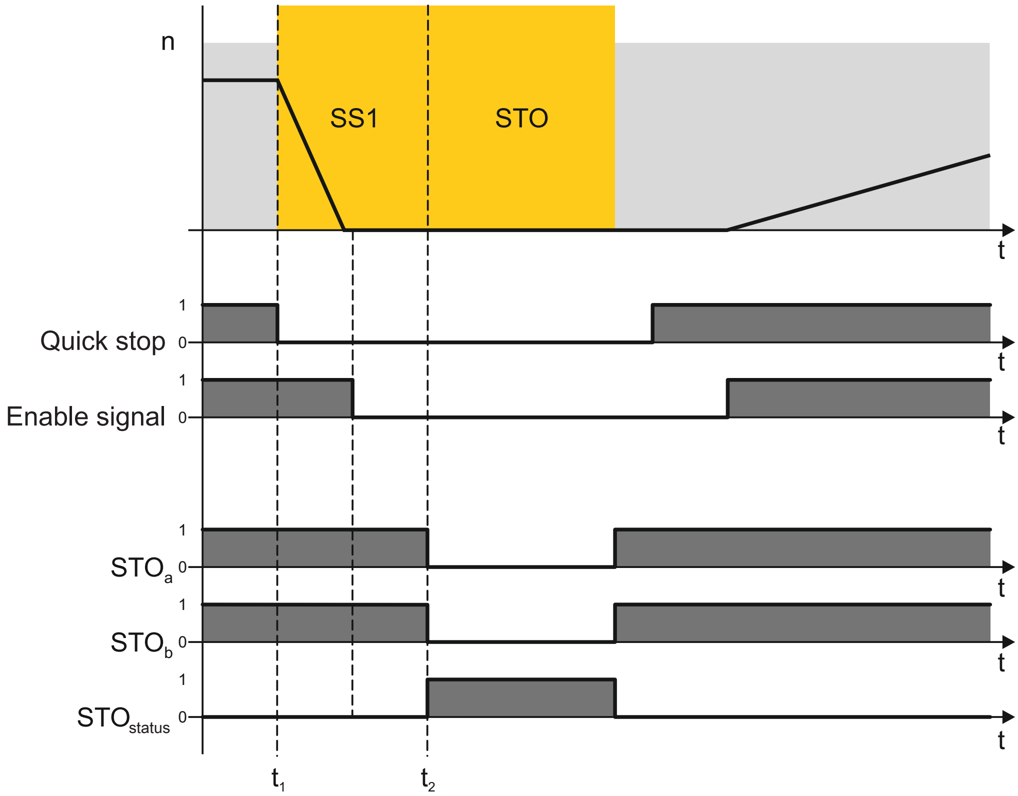


Fig. 5: SR6 and SS1-t – Sequence over time

t_1 SS1 triggering

t_2 STO triggering

After activation of the SS1-t safety function at time t_1, it attempts a controlled shutdown of the drive before it is safely switched to a torque-free state through the activation of STO at time t_2.

A safety relay activates a controlled shutdown in the drive controller at time t_1 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 DIN EN 61800-5-2.

10 Diagnostics

10.1 Parameters

The following display parameters are significant for safety equipment in combination with SI6 drive controller and SR6 safety module.

10.1.1 E53 Required safety module | G6 | 3

Projected safety module.

10.1.2 E54 Information safety module | G6 | 0

Signifying data of the safety module.

[0]: Type

[1]: Hardware version

[2]: Serial number

[3] – [5]: Reserved

[6]: Diagnostic code

10.1.3 E67 STO active | G6 | 0

STO state of the safety module:

[0]: 1 = STO triggered by input signal STO_a = 0 or STO_b = 0

[1]: 1 = STO triggered by input signal STO_a = 0

[2]: 1 = STO triggered by input signal STO_b = 0

- 0: Inactive
- 1: Active

10.2 Events

Possible events, the causes and suitable measures for which are listed below.

10.2.1 Event 50: Safety module

The drive controller is interrupted.

- The power unit is disabled, the drive controller no longer controls axis motion.
- The holding brakes are no longer controlled by the drive controller and engage in the event of an inactive purge override F06.

Causes and actions

Number	Cause	Check and action
1: Inconsistent request (single channel)	Connection error	Check the connection and correct if necessary, error can be confirmed only if STO was previously requested for at least 100 ms across two channels
2: Wrong safety module	The safety module projected in E53 does not match that detected in E54[0]	Check the projecting and drive controller and correct the projecting or exchange the drive controller if necessary; fault cannot be confirmed

Tab. 8: Event 50 – Causes and actions

11 More on safety equipment and SR6

The following chapters outline the important terms, relationships and measures regarding the SR6 safety module and safety equipment.

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 DIN EN 61800-5-2.

Implementation of safety functions is generally handled by safety-related parts of controllers (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

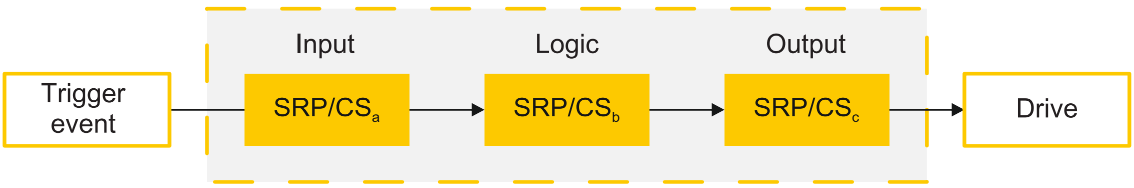


Fig. 6: SRP/CS components for processing a typical safety function

Input	Sensor or limit switch
Logic	Safety controller or safety relay
Output	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 an output component to safely trigger the dangerous motion.
The SI6 drive controller in combination with the integrated SR6 safety module are parts 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 SR6 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 SR6 safety module does not detect external wiring errors!
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 connection wiring by a safety relay
- Wiring error elimination in accordance with DIN EN 13849
- Monitoring of the connection 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 (e.g. OSSD outputs), the accompanying safety relay inspects the wiring and the switching capability of the outputs by use of 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 Error elimination for lines/connections in accordance with DIN EN 13849

Errors in the connection wiring of assemblies and components can lead to loss of safety functions. Possible measures for eliminating errors and notices for these measures are supplied in table D.4 of the standard DIN EN ISO 13849-2[2].

<table>
<tr><th>Observed errors</th><th>Error elimination</th><th>Remarks</th></tr>
<tr><td>Short circuit between any two conductors</td><td>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</td><td rowspan="2">The lines as well as the installation space must correspond to the respective requirements (see IEC 60204-1)</td></tr>
<tr><td>Short circuit between any conductor and an unprotected conductive part or the ground or a grounding conductor connection</td><td>Short circuits between conductors and any unprotected conductive part inside an installation space (see note)</td></tr>
<tr><td>Interruption of a conductor</td><td>No</td><td>–</td></tr>
</table>

Tab. 9: DIN EN 13849, table D.4 – Errors and measures for eliminating errors – lines/cables

[2] See DIN EN ISO 13849-2, p. 56.

11.2.3 Monitoring by means of plausibility check of the signals

The state of the connection wiring and the function of the safety channels can be checked using the STO status signals.

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

Shorter 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 fault, the safety function is activated at both STO inputs. The SI6 drive controller may no longer be enabled.

STO_{status} is made available directly on the SI6 terminal X12 for monitoring purposes. If you are working with a field bus system, you can access detailed status information by transmitting parameter E67 STO status, array E67[0] – E67[2]. This can be analyzed as an alternative to STO_{status}.

For applications with lower safety requirements, i.e. up to SIL 2, PL d, a standard control unit can perform the STO function test; for applications with increased safety requirements such as SIL 3, PL e, a safety controller must check the connection wiring.

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 STÖBER 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.

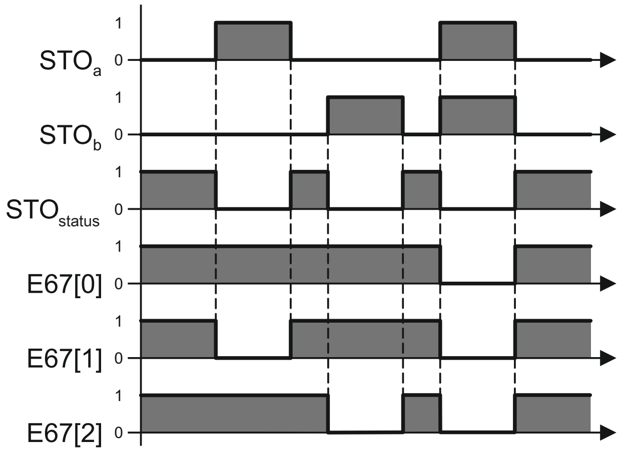


Fig. 7: Function test – switch sequences

STO_a, STO_b	Inputs of both SR6 safety channels
STO_{status}	STO status signal for diagnostic purposes
E67[0]	At least one SR6 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 a drive controller cascade

Be aware that STO_{status} outputs cannot be cascaded.

Information

In order to ensure correct wiring of a drive controller cascade, you must check the STO_{status} signal of each drive controller in the cascade 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.

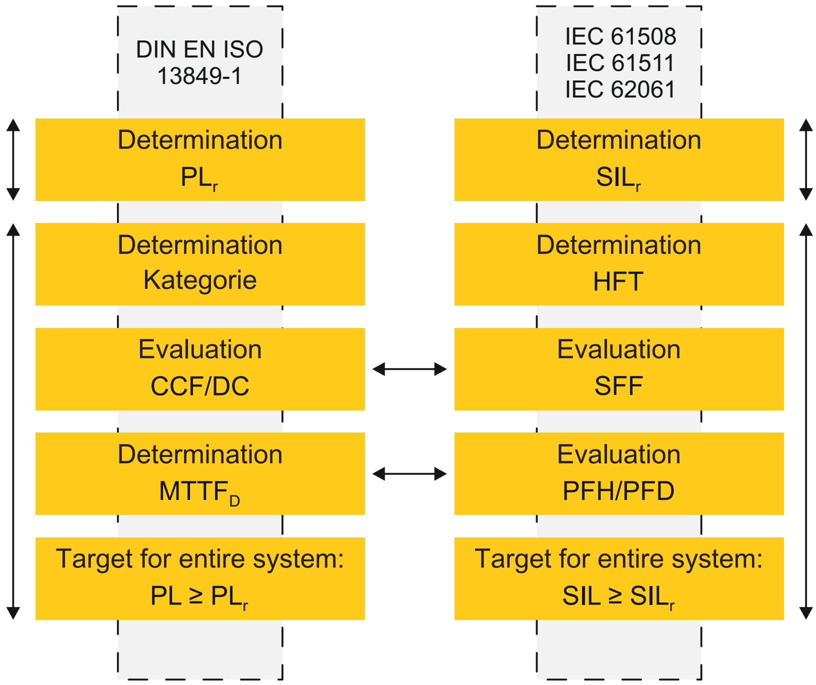


Fig. 8: Determining and assessing protective measures

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 a 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]

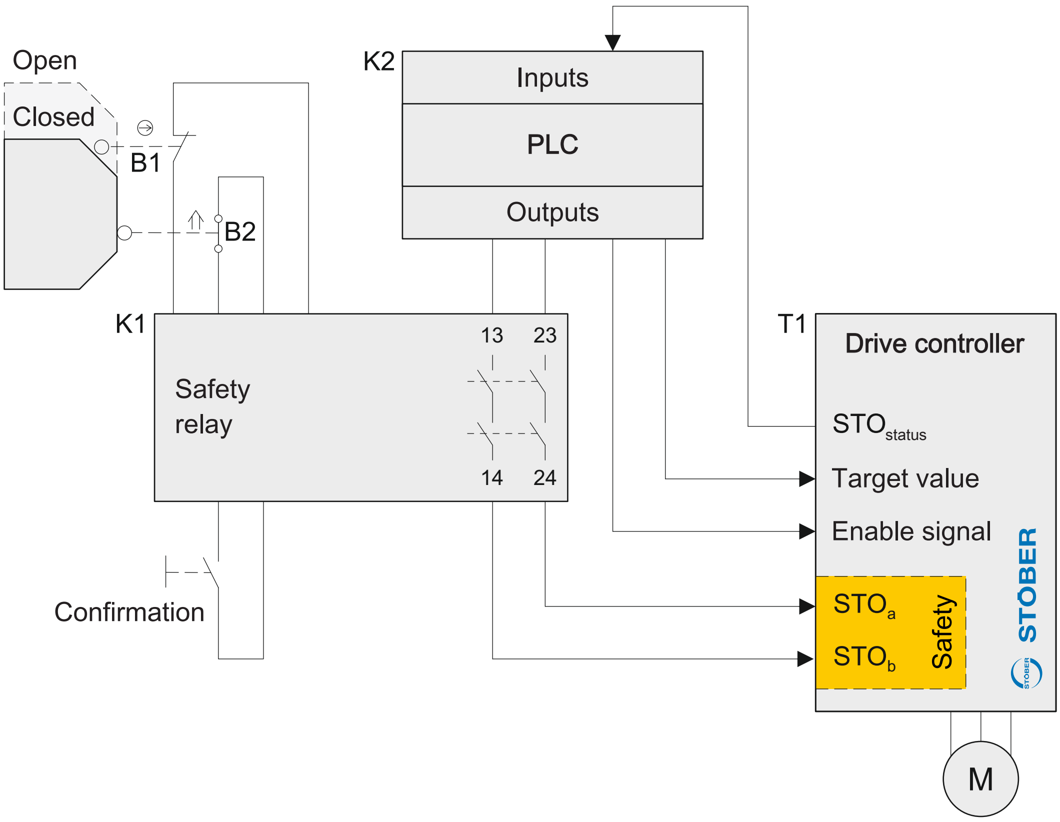


Fig. 9: STO – Schematic diagram

B1, B2	Position switches
K1	Safety relay
K2	Controller
T1	SI6 drive controller with integrated SR6 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 SR6 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.

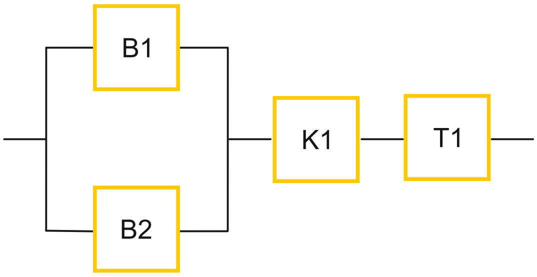


Fig. 10: Safety-related block diagram

B1, B2	Position switches
K1	Safety relay
T1	SI6 drive controller with integrated SR6 safety module

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 and is represented in the form of subsystems 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).

A safety-related block diagram of a safety function is therefore comprised of a chain of individual subsystems including categories.

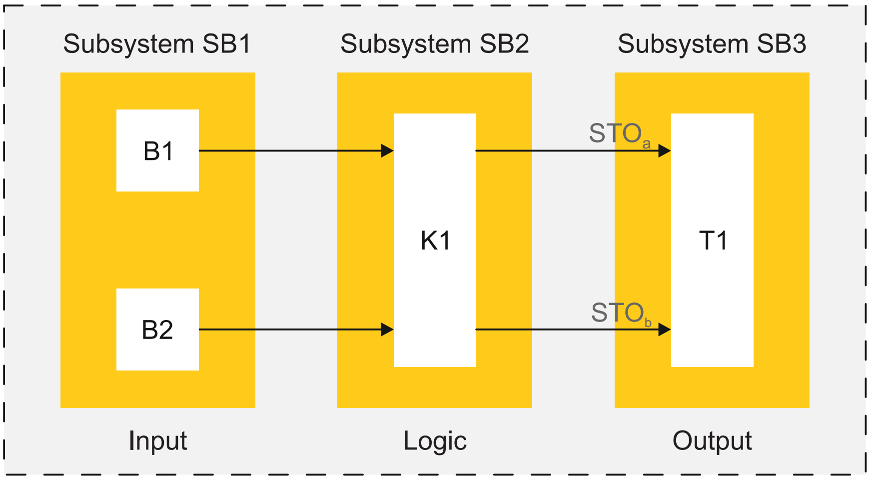


Fig. 11: Safety-related block diagram with subsystems

SB1 – SB3	(Encapsulated) subsystems 1 – 3
B1, B2	Position switches
K1	Safety relay
T1	SI6 drive controller with integrated SR6 safety module

03/2017 | ID 442741.00

The protective device with the position switches forms subsystem 1, the safety relay forms subsystem 2, the SI6 drive controller along with integrated SR6 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 DIN 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 eliminate 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 position changes. Only rigid mechanical parts may be used (no spring elements). The position switch B1 is an established component in accordance with DIN EN ISO 13849-2, Table D.3 with a positively driven contact in accordance with DIN 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.

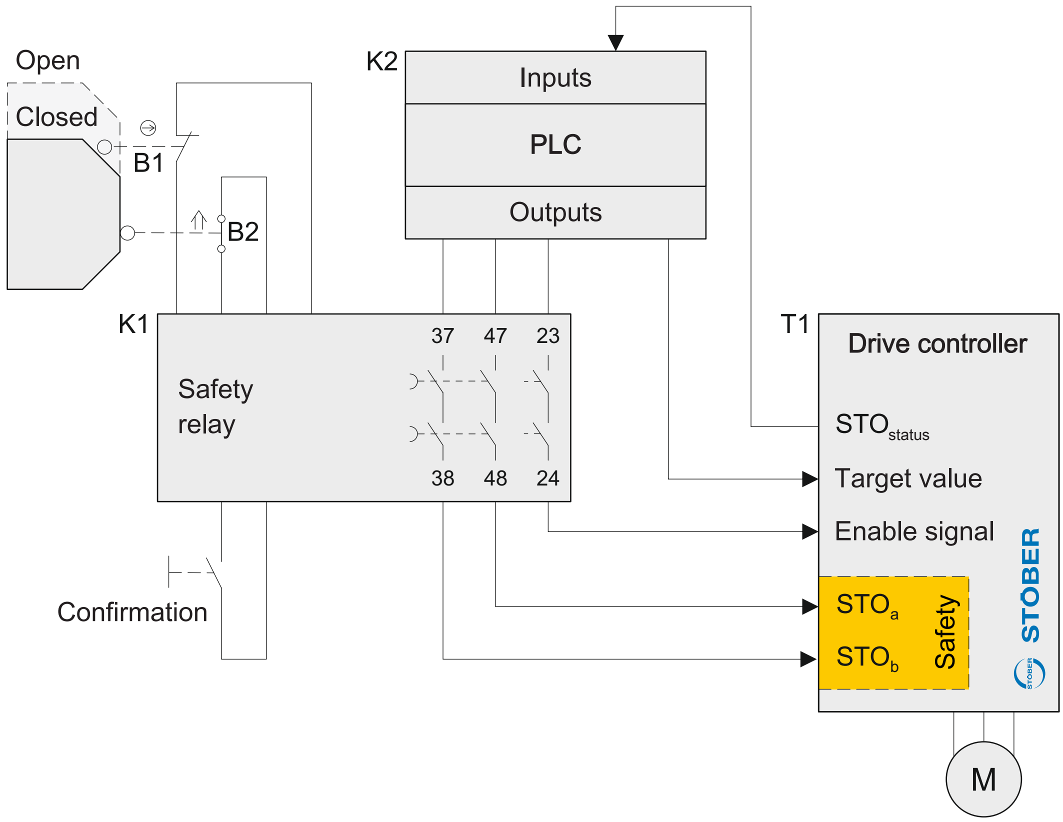


Fig. 12: SS1 – Schematic diagram

B1, B2	Position switches
K1	Safety relay
K2	Controller
T1	SI6 drive controller with integrated SR6 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 standstill safely during this delayed STO switch-off of the drive. If the drive controller triggers the standstill, 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 SR6 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.

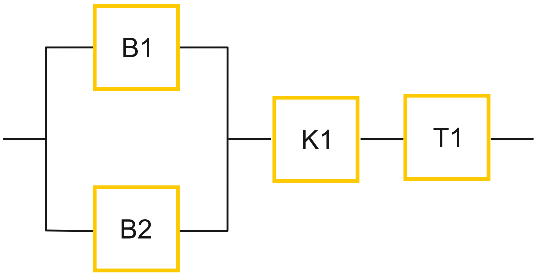


Fig. 13: Safety-related block diagram

B1, B2	Position switches
K1	Safety relay
T1	SI6 drive controller with integrated SR6 safety module

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 and is represented in the form of subsystems 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).

A safety-related block diagram of a safety function is therefore comprised of a chain of individual subsystems including categories.

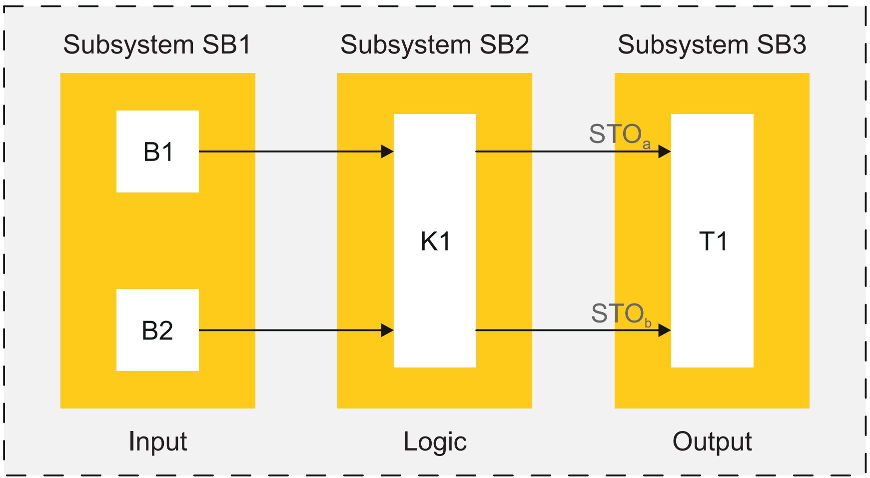


Fig. 14: Safety-related block diagram with subsystems

SB1 – SB3	(Encapsulated) subsystems 1 – 3
B1, B2	Position switches
K1	Safety relay
T1	SI6 drive controller with integrated SR6 safety module

The protective device with the position switches forms subsystem 1, the safety relay forms subsystem 2, the SI6 drive controller along with integrated SR6 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 DIN 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 eliminate 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 position changes. Only rigid mechanical parts may be used (no spring elements). The position switch B1 is an established component in accordance with DIN EN ISO 13849-2, Table D.3 with a positively driven contact in accordance with DIN 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 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}

- B1
  Elimination of dangerous component errors possible for the electrical contact
  B_{10D} (mechanics): 2000000 cycles
- B2
  B_{10D} (mechanics): 2000000 cycles

Source: Pilz GmbH und Co. KG

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 device type PNOZ S5 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)
  $PFH_D = 2.31 \times 10^{-9}$ [1/h]
- Switch-off delaying contacts (SS1)
  $PFH_D = 2.34 \times 10^{-9}$ [1/h]

Source: Pilz GmbH und Co. KG

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 T1 type SI6 drive controller including SR6 safety module from STÖBER ANTRIEBSTECHNIK GmbH & Co. KG.

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, elimination of errors in accordance with DIN 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	$PFH_D = 5.0 \times 10^{-8}$
Entire system	SISTEMA calculation	$PFH_D = 3.2 \times 10^{-9}$

Tab. 10: 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^{-9} [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. 11: 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 SR6 in accordance with interface classification (ZVEI)

The German Electrical and Electronic Manufacturer's Association (ZVEI) published a policy document in 2016 (see Detailed information [▶ 44]) 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 SR6 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.
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 sinks and sources, it is important to ensure that a selected source at least belongs to the same class as the selected sink.

Interface type C

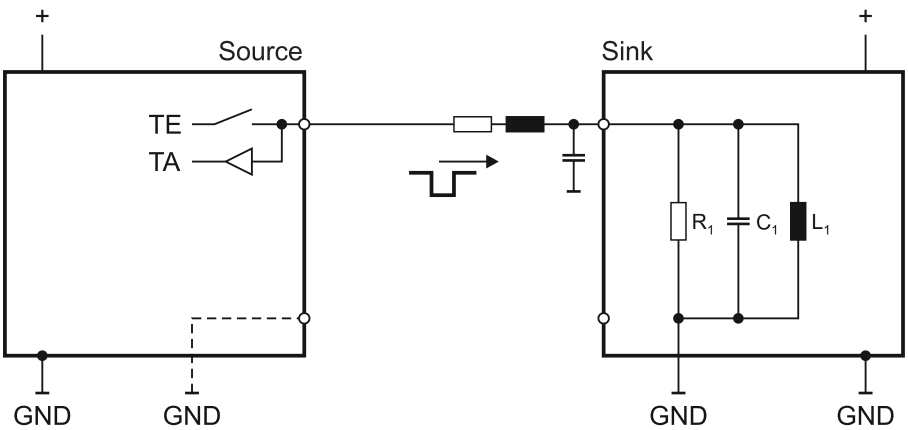


Fig. 15: Interface classification – Interface type C

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 curtains 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 sink, e.g. SR6 safety module, is not allowed to react to these test pulses by definition.

[5] See ZVEI, p. 13ff.

Interface type D

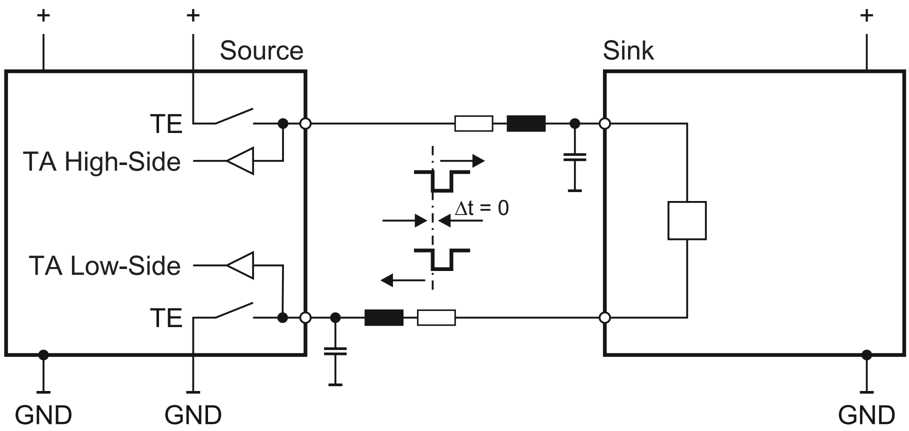


Fig. 16: Interface classification – Interface type D

TE	Test pulse generation
TA	Test pulse assessment
TA High-Side	Test pulse evaluation high-side switch
TA Low-Side	Test pulse evaluation low-side switch
GND	Reference potential
Δt_i	Timespan

Interface type D[6] is intended either for safely switching actuators (contactors, motors, valves) or for fully de-energizing electrical/electronic assemblies 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 sink, which are in turn evaluated by the source. The test pulses are neither distorted nor delayed by the sink.

The sink, e.g. SR6 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 Detailed information

The pieces of documentation listed in the following table offer additional relevant information for the SI6 drive controller. Current document versions can be found at http://www.stoeber.de/en/download.

Device/Software	Documentation	Contents	ID
Multi-axis drive system with SI6 and PS6	Manual	System setup, technical data, storage, installation, connection, start-up, operation, service, diagnostics	442728

Additional information and sources on which the documentation is based or which are cited 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
http://www.dguv.de/ifa/publikationen/reports-download/reports-2013/ifa-report-7-2013/index-2.jsp

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
http://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook1_end.pdf

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
http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/alle-sistema-versionen/index.jsp

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)
[Accessed on 2016-11-17]. Available at
http://www.zvei.org/Verband/Publikationen/Seiten/Klassifizierung-Binaerer-24-V-Schnittstellen.aspx

12.2 Formula symbols

Formula symbol	Unit	Explanation
B_{10D}	Cycles	Average number of cycles until 10% of components experience dangerous failure
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: RMS value of the maximum permitted line-to-line current with maximum torque M_{max} generated (tolerance ±5%).
I_{1max}	A	Maximum input current
I_{OFF}	A	Input current in OFF state
I_{ON}	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}	Cycles/a	Average number of annual actuations (switching frequency)
PFH_D	1/h	Average probability of a dangerous failure per hour
R_1	Ω	Input resistance
T	ms	Test pulse interval
t_i	µs	Test pulse duration
T_M	Year, a	Length of use
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
PFD	Probability of Failure per Hour
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 first-level support?:
Phone +49 7231 582-3060
applications@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.

You suggestions, opinions, wishes and constructive criticism help us to ensure and improve the quality of our documentation.
If you would like 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 Phone +65 65112912 sales@stober.sg
STOBER CHINA www.stoeber.cn Phone +86 10 6590 7391 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	

Glossary

Average Diagnostic Coverage (DC_{avg})

In accordance with DIN EN ISO 13849-1: Average diagnostic coverage. Value for reducing the probability of dangerous hardware failures through automatic diagnostic testing.
The average diagnostic coverage can apply to the entire system or part of a safety-related system.

B_{10D} value

In accordance with DIN EN ISO 13849-1: Number of cycles until 10% of components experience dangerous failure (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 against faults and their subsequent behavior in the event of 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 Manufacturer's 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 common cause. In accordance with DIN EN 61800-5-2: Failure that is the result of one or multiple events that cause 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 sink can fulfill the requirements of various interface types at the same time. The term sink relates to the evaluation of information, not to the evaluation of the accompanying 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 relates to the generation of information, not to the generation of the accompanying 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 a 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 determinations about the generation by evaluating the accompanying test pulses.

Length of use (T_M)

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

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 assemblies. Statistical values that are determined through trials and experiential values. Does not claim guaranteed life span or guaranteed failure-free time.

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.

Output Signal Switching Device (OSSD)

Output switching element that is part of a contact-free protective device (BWS). An OSSD switches to the off state if the SRP/CS sensor or the monitoring device triggers.

Performance Level (PL)

Dimension for the reliability of a safety function or a component according to DIN EN 13849-1. The performance level is rated on a scale of a – e (lowest – highest PL). The higher the PL, the safer and more reliable the function considered.

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: Probability of a dangerous device failure occurring per hour. Together with PFD, one of the most important foundations 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: Probability of device failure per hour. Together with PFD, PFH is one of the most important bases for calculating the reliability of the safety function of devices, the SIL.

Reaction time

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

Response time

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

Safe Stop 1 (SS1)

As per DIN EN 61800-5-2: procedure to stop a PDS(SR). For the safety function SS1, the PDS(SR) performs one of the following functions: a) Initiation and control of the size of the motor delay within defined limits and triggering the STO function when the motor speed drops below a defined limit value, or b) Initiation and monitoring of the size of the motor delay within defined limits and initiation of the STO function when the motor speed drops below a limit value, or c) initiation of the motor delay and initiation of the STO function after an application-specific time delay. SS1 corresponds to the controlled stop according to IEC 60204-1 stop category 1.

Safe Torque Off (STO)

Safety function that immediately interrupts the energy supply to the drive and stops the drive in an uncontrolled manner. It can no longer generate torque after shutdown. STO is the most basic drive-integrated safety function. It corresponds to stop category 0 according to IEC 60204-1.

Safety Integrity Level (SIL)

In accordance with DIN EN 61800-5-2: Probability of 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, related to the structural limitations and systematized safety integrity of a SRECS subsystem. A SIL CL is determined by the hardware fault tolerance (HFT) and the proportion of safe failures of the subsystems (SFF).

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 switch-off time

Timespan starting with the arrival of a FSoE telegram at the EtherCAT connection of the drive controller with the command to activate the safety function up to the safe switch-off of the power unit of the drive controller.

Switching frequency (n_{op})

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

Test pulse

In accordance with German Electrical and Electronic Manufacturer's Association: Temporary change of signal voltage level for checking the proper function of the output or device or for checking the transmission path.

Test pulse assessment (TA)

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

Time difference

Difference in time between a deactivation and reactivation of both the STO_a and STO_b signals. The drive controller can be enabled again once this time period has elapsed.

List of figures

List of tables

Technische Änderungen vorbehalten.
Errors and changes excepted.

ID 442741.00
03/2017

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