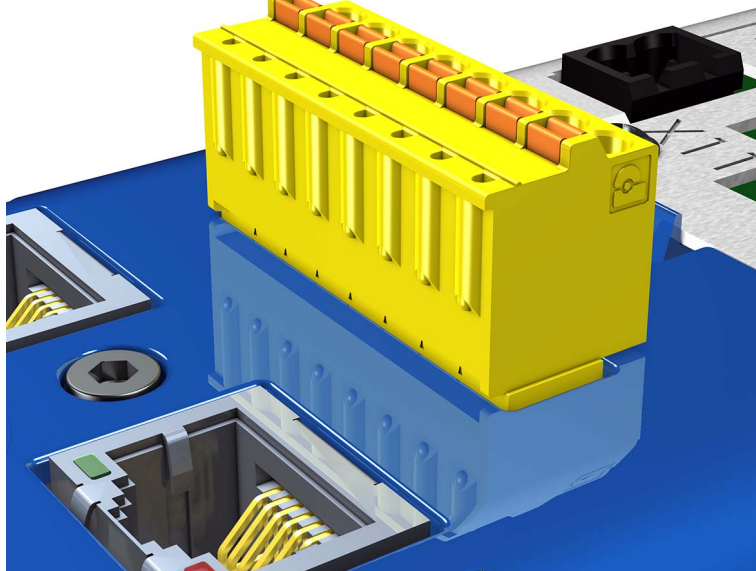




# STÖBER

## ST6

### Manual



## Table of contents

1	General Information . . . . .	3	4.5	Device features . . . . .	12
1.1	About this manual . . . . .	3	5	Connection . . . . .	13
1.2	Further documentation . . . . .	4	5.1	Requirements . . . . .	13
1.3	Further support . . . . .	4	5.2	Wiring . . . . .	13
2	Notes on safety . . . . .	5	5.3	EMC connection . . . . .	13
2.1	Operation in accordance with its intended use . . . . .	5	5.4	Terminal description X12 . . . . .	13
2.2	Component part of the product . . . . .	5	5.5	Cascading . . . . .	14
2.3	Risk assessment . . . . .	5	6	Commissioning and maintenance . . . . .	15
2.4	Qualified personnel . . . . .	6	7	Diagnosis . . . . .	16
2.5	Working on the machine . . . . .	6	7.1	Parameters . . . . .	16
2.6	Modification and repair . . . . .	6	7.2	Events . . . . .	17
2.7	Disposal . . . . .	6	7.2.1	50:Safety function . . . . .	17
2.8	Presentation of notes on safety . . . . .	7	8	Appendix . . . . .	18
3	How it functions . . . . .	8	8.1	Wiring check . . . . .	18
4	Technical data . . . . .	10	8.2	SS1 . . . . .	19
4.1	Safety figures . . . . .	10	8.3	Sample application . . . . .	19
4.2	Electrical data . . . . .	10	8.3.1	Calculations of the failure probability . . . . .	20
4.3	System times . . . . .	11	8.3.2	Result . . . . .	22
4.4	Ambient conditions . . . . .	11	9	Glossary . . . . .	24

## 1 General Information

The ST6 safety card is an extension of the SD6 drive controller. This manual contains technical data of the ST6 safety card, and explains its operation and the connection of the ST6 safety card to the SD6 drive controller. The ST6 safety card is used to realize the STO safety function and thus prevents the generation of a rotary field in the power output stage of the SD6 drive controller. For an external requirement or in the event of error, the ST6 switches the drive controller to the STO state.

The control board in the drive controller generates the pulse patterns required by the power unit to produce the rotary field. The pulse patterns in the SD6 are transferred from the control board to the power unit via the ST6 safety card.

If the safety function is active, a reliable pulse inhibit prevents the pulse pattern from being transferred to the power unit. The power unit is unable to generate a rotary field and the motor is torque-free.

If the safety function is active, pulse patterns are directed to the power unit and the motor can be operated.

This is equivalent to the safety function *Safe torque off* (STO) in accordance with DIN EN 61800-5-2:2007. This type of shutdown is designated as *Stop category 0* in DIN EN 60204-1:2006.

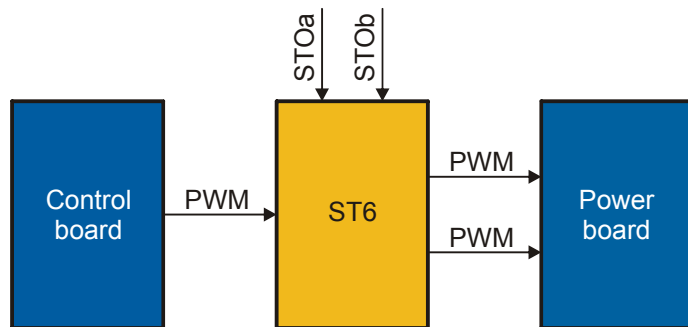


Fig. 1-1 Complete system of SD6 drive controller with ST6

In the following safety block diagram SD6 and ST6 correspond to the actuator and form the basis for a restart inhibit.

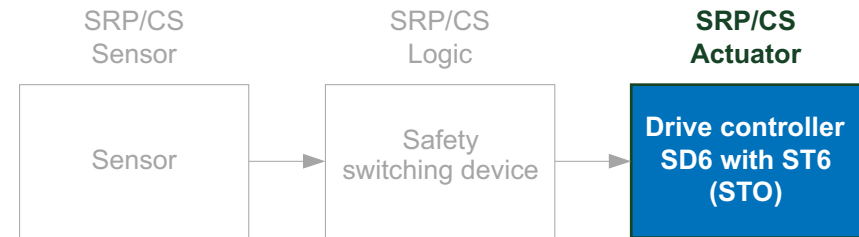


Fig. 1-2 Safety block diagram

### 1.1 About this manual

This manual explains the operation of the safety card, contains associated technical data and describes its connection to external safety devices.

#### Original version

The original version of this manual is in German.

#### This documentation applies to the following devices:

- Drive controller SD6 with DriveControlSuite 6.0-A or higher

#### What is new?

Index	Date	Changes
00	06/2014	First edition
01	08/2015	<ul style="list-style-type: none"> <li>• Size 3 adopted</li> <li>• Terminal voltage corrected</li> <li>• Device cascading (status output) corrected</li> <li>• Standards detailed</li> </ul>

## 1.2 Further documentation

The documentation listed in the following table provides relevant information on the SD6 drive controller. You can find the latest document versions at [www.stoeber.de](http://www.stoeber.de) (Services).

Device/Software	Documentation	Contents	ID
SD6 drive controllers	Manual	System environment, technical data, commissioning, communication, diagnosis	442426
SD6 drive controllers	Commissioning instructions	Technical data, installation, commissioning, function test	442537

## 1.3 Further support

If you have technical questions that are not answered by this document, please contact:

- Phone: +49 7231 582-3060
- E-mail: [applications@stoeber.de](mailto:applications@stoeber.de)

## 2 Notes on safety

### 2.1 Operation in accordance with its intended use

If the STO safety function is used in a safety-relevant application, it must be activated by a higher-level safety switching device or a safety controller.

The ST6 safety card may be used for the sizes 0 – 3 of the SD6 drive controller.

Unintended use includes:

- any structural, technical or electrical change to the ST6,
- use of the ST6 outside of areas that are described in these operating instructions,
- use outside of the technical specifications.



#### Information

Designated use of the ST6 safety card does not include the realization of the *Emergency Off* function (no voltage present after activation) or the operation outside of a SD6.



#### WARNING!

#### Danger of personal injury and material damage due to voltage present!

Hazardous voltages may be present at the output of the drive controller for an active STO.

- ▶ The difference between *Emergency Off* and *Safe Torque Off* (emergency stop) is described in the DIN EN 60204-1:2006 standard.

If the STO safety function of the drive controller is not used, the  $STO_a$  and  $STO_b$  signals must be connected to  $24 V_{DC}$  so that the drive controller can be put into operation.

### 2.2 Component part of the product

The technical documentation is a component part of a product.

- Since the technical documentation contains important information, always keep it handy in the vicinity of the device until the machine is disposed of.
- If the product is sold, disposed of, or rented out, always include the technical documentation with the product.

### 2.3 Risk assessment

Before the manufacturer may bring a machine onto the market, he must conduct a risk assessment according to Machine Directive 06/42/EC. As a result, the risks associated with the use of the machine are determined. The risk assessment is a multi-stage and iterative process. On no account can sufficient insight into the Machine Directive be given as part of this documentation. For this reason, seek detailed information about the norms and legal position. When installing the drive controller in machines, commissioning is forbidden until it has been determined that the machine meets the requirements of EC Directive 06/42/EC.

## 2.4 Qualified personnel

There are residual risks associated with the devices. For this reason, only qualified personnel who are aware of possible dangers may carry out work on the devices as well as operate and dispose of them.

Qualified personnel are persons who have acquired the required specialist knowledge as a result of their professional training, their vocational experience and their recent professional activity to check, assess and operate devices, systems, machines and plants according to the generally applicable standards and guidelines of safety engineering.

In addition the valid regulations, legal requirements, basic rules and this technical documentation, particularly the safety information included in it, must be carefully

- read,
- understood and
- observed.

## 2.5 Working on the machine

Apply the 5 safety rules in the order stated before performing any work on the machine:

1. Disconnect.  
Also ensure that the auxiliary circuits are disconnected.
2. Protect against being turned on again.
3. Check that voltage is not present.
4. Ground and short circuit.
5. Cover or block off adjacent live parts.



### Information

Note that the discharge time of the DC link capacitors is up to 5 minutes. You can only determine the absence of voltage after this time period.

## 2.6 Modification and repair

The housing of the drive controller may not be opened. You must not convert or repair the ST6 safety card. Observe the documentation of the drive controller (for manuals, see 1.2 Further documentation).

## 2.7 Disposal

Please observe the current national and regional regulations! Dispose of the individual parts separately depending on the quality and currently applicable regulations, e.g. as

- Electronic waste (circuit boards)
- Plastic
- Sheet metal
- Copper
- Aluminum
- Battery

## 2.8 Presentation of notes on safety

### NOTICE

#### Notice

means that property damage may occur

- ▶ if the stated precautionary measures are not taken.
- 

### CAUTION!

#### Caution

with warning triangle means that minor injury may occur

- ▶ if the stated precautionary measures are not taken.
- 

### WARNING!

#### Warning

means that there may be a serious danger of death

- ▶ if the stated precautionary measures are not taken.
- 

### DANGER!

#### Danger

means that serious danger of death exists

- ▶ if the stated precautionary measures are not taken.
- 



#### Information

refers to important information about the product or serves to emphasize a section in the documentation to which the reader should pay special attention.

### 3 How it functions

The safety card has a two channel design. Both channels are independent of each other and must be controlled synchronously by two control signals with 24 V<sub>DC</sub> (maximum time difference 500 ms; the event 50 with cause 1 is triggered if exceeded, see 7.2.1). Note that a safety switching device must supply these signals.

#### WARNING!

##### Danger of electric shock!

If the STO safety function is active, only the rotary field generation at the motor is interrupted. Dangerous high voltages may still be applied to the motor.

- ▶ Make sure that live parts can not be touched.
- ▶ If the supply voltage must be switched off, observe the requirements for an Emergency Stop according to DIN EN 60204-1:2006.



#### Information

No cyclic function test is necessary for the ST6 safety card. Note that you may have to cyclically test the wiring depending on your wiring concept. Note also section 5.1 Requirements.

To activate the STO safety function, the *STO<sub>a</sub>* and *STO<sub>b</sub>* control signals must be switched off or interrupted. The rotary field generation of the motor is safely interrupted after the response time  $t_2$  has elapsed (see ) and the motor cannot generate any torque.

#### WARNING!

##### Personal injury or property damage due to gravity-loaded axes or the motor coasting down.

If the STO safety function is active, the motor cannot generate any torque. As a result, gravity-loaded axes can drop. If the motor moves when STO is activated, it coasts down in an uncontrolled manner.

- ▶ Secure the gravity-loaded axes using brakes or other suitable measures.
- ▶ Make sure that no risks can arise due to the motor coasting down.

To deactivate the STO safety function, the *STO<sub>a</sub>* and *STO<sub>b</sub>* control signals must be controlled simultaneously with 24 V<sub>DC</sub>. If the STO safety function is deactivated, the motor can move.

The *STO<sub>Status</sub>* output signal is available for the diagnosis of the connection wiring. The output signal is derived from a NOR operation of the *STO<sub>a</sub>* and *STO<sub>b</sub>* control signals:

<i>STO<sub>a</sub></i>	<i>STO<sub>b</sub></i>	<i>STO<sub>Status</sub></i>
0	0	1
1	0	0
0	1	0
1	1	0



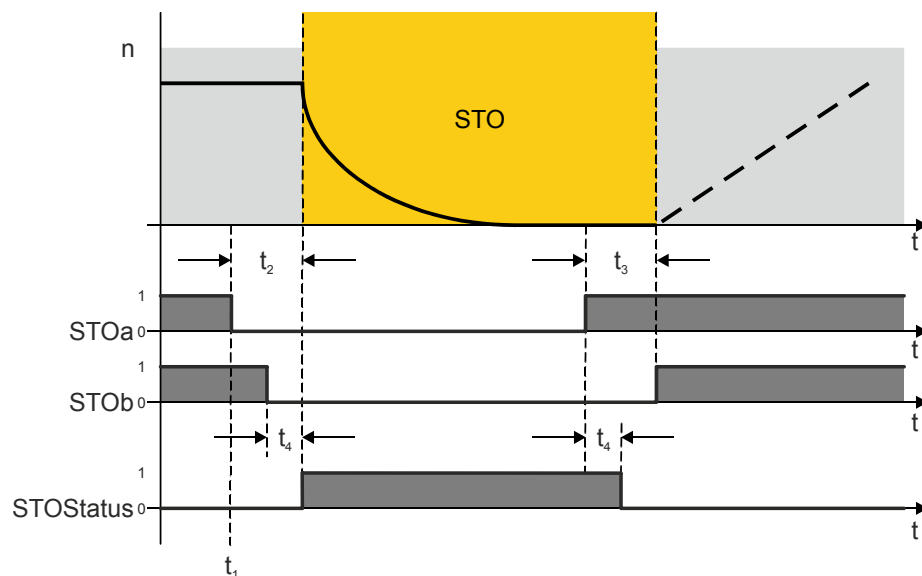


Fig. 3-1 Function diagram

- $t_1$  Trigger safety function
- $t_2$  Max. response time
- $t_3$  Max. time difference
- $t_4$  Max. response time

The values of the times  $t_2$  to  $t_4$  can be found in section 4.3 System times.

Before the drive controller can be enabled again, both switch-off channels must be deactivated (for at least 500 ms).

Note that the idealized switching sequence without the times  $t_1$  to  $t_4$  is used in the following documentation to illustrate more clearly.

If an error occurs on the ST6 safety card, the STO safety function is activated.



#### Information

Depending on the functionality of the higher-level safety switching device, you can realize additional safety functions based on the STO safety function. Also note section 8.2 SS1.

## 4 Technical data

### 4.1 Safety figures

Safety figures for SD6 with ST6 (STO) for two channel requirement

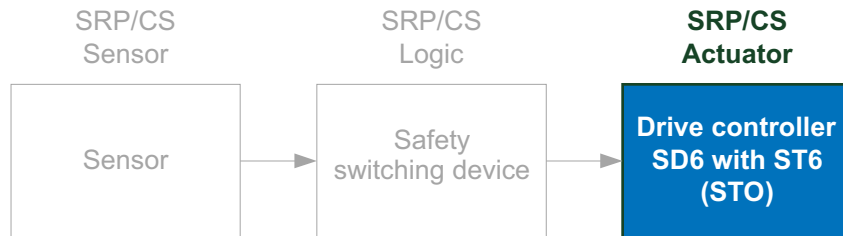


Fig. 4-1 Safety figures – SD6 and ST6

Safety figures	Value
SIL CL according to DIN EN 62061:2005	SIL CL 3
SIL according to DIN EN 61508:2010	SIL 3
PFH [1/h]	$5 \times 10^{-9}$
Service life $t_M$ [year]	20 years
PL according to DIN EN ISO 13849-1:2008	PLe (Cat. 4)

### 4.2 Electrical data

Electrical data

Pin	Designation/function	Data
1	STO <sub>a</sub> (bridged internally)	$U_{1max} = 30 V_{DC}$ (PELV) High level = 15–30 V Low level = 0–8 V
2		
3	STO <sub>b</sub> (bridged internally)	$I_{1max} = 100 \text{ mA}$ (< 30 mA at 24 V) $I_{Max \text{ terminal}} = 4 \text{ A}$ $C_1 = 100 \text{ nF}$
4		
5	GND for STO <sub>a</sub> and STO <sub>b</sub> (bridged internally with terminal 7)	—
6	STO <sub>status</sub>	$U_2 = U_1 - (200 \text{ m}\Omega \cdot I_1)$
7	GND for STO <sub>a</sub> and STO <sub>b</sub> (bridged internally with terminal 5)	—
8	Power supply of STO <sub>status</sub>	$U_1 = 18\text{--}28.8 V_{DC}$ $I_{1max} = 100 \text{ mA}$

$C_1$	F	Input capacity
$I_1$	A	Input current
$I_{1max}$	A	Maximum input current
$U_1$	V	Input voltage
$U_{1max}$	V	Maximum input voltage

### 4.3 System times

#### System times for SD6 with ST6 (STO) for two channel requirement



Fig. 4-2 System times – SD6 and ST6

Note that you must determine the complete response time from the response times of the individual part systems for your application.

System time	Value
Max. response time ( $t_2$ , s. 3 How it functions): time between activation of the STO safety function (edge change from 1 to 0) until the pulse pattern is disabled at the power unit.	10 ms
Max. time difference ( $t_3$ , s. 3 How it functions): Between activation of the $STO_a$ and $STO_b$	500 ms
Max. response time ( $t_4$ , s. 3 How it functions): time between activation of the STO safety function (edge change from 1 to 0) until acknowledgment by an edge change of the $STO_{Status}$ signal.	15 ms
Filter time constant: Max. OSSD test pulse length	600 $\mu$ s

### 4.4 Ambient conditions

The data of the drive controller applies (an excerpt follows). Refer to the manual of the drive controller for detailed information, see section 1.2 Further documentation.

<b>Ambient operating temperature</b>	0 °C to 45 °C with nominal data; for derating see 1.2 Further documentation
<b>Storage/transport temperature</b>	-20 °C to +70 °C; Maximum change: 20 K/h
<b>Relative humidity</b>	Relative humidity 85 %, non-condensing
<b>Installation altitude</b>	Up to 1000 m above sea level without restrictions; For derating see 1.2 Further documentation
<b>Contamination level</b>	Contamination level 2 as per EN 50178:1998
<b>Ventilated</b>	Installed fan
<b>Vibration (operation)</b>	5 Hz $\leq$ f $\leq$ 9 Hz: 0.35 mm 9 Hz $\leq$ f $\leq$ 200 Hz: 1 m/s <sup>2</sup>
<b>Vibration (transport)</b>	5 Hz $\leq$ f $\leq$ 9 Hz: 3.5 mm 9 Hz $\leq$ f $\leq$ 200 Hz: 10 m/s <sup>2</sup> 200 Hz $\leq$ f $\leq$ 500 Hz: 15 m/s <sup>2</sup>

## 4.5 Device features

The data of the drive controller applies (an excerpt follows). Refer to the manual of the drive controller for detailed information, see section 1.2 Further documentation.

### Device features

<b>Protection class of the device</b>	IP20
<b>Protection class of the control cabinet</b>	At least IP54
<b>Radio interference suppression</b>	EN 61800-3:2012, interference emission class C3
<b>Overvoltage category</b>	III according to EN 61800-5-1:2008

## 5 Connection

### 5.1 Requirements

#### WARNING!

##### Unexpected movements of the drive!

The ST6 safety card can not determine errors in the external wiring.

Take one of the following measures so that an error in the wiring and the control of the safety function does not lead to a loss of safety:

- ▶ Fault elimination for the wiring according to DIN EN 13849-2:2013
- ▶ Fault detection by tested control signals (OSSD) and switch-off for errors through the second switch-off path
- ▶ Fault detection by the evaluation of the *STOStatus* signal in the higher-level controller and switch-off for errors through the second switch-off path (see section 8.1 Wiring check)

### 5.2 Wiring

Observe the regulations applicable for your machine or system when installing the electrical equipment, e.g. DIN IEC 60364 or DIN EN 50110:2014.

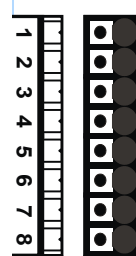
### 5.3 EMC connection

The maximum permitted line length is 30 m. Furthermore observe the specifications in the documentation of the drive controller for an EMC-compliant connection, see section 1.2 Further documentation.

### 5.4 Terminal description X12

#### Terminal description X12

Pin	Designation/function
1	STO <sub>a</sub> (bridged internally)
2	
3	STO <sub>b</sub> (bridged internally)
4	
5	GND for STO <sub>a</sub> and STO <sub>b</sub> (bridged internally with terminal 7)
6	STO <sub>Status</sub>
7	GND for STO <sub>a</sub> and STO <sub>b</sub> (bridged internally with terminal 5)
8	Supply of STO <sub>Status</sub>



#### Cable requirements

Feature	Line type	Unit	Min	Max
Cross-section	Fine wire line without cable end sleeve	mm <sup>2</sup>	0.14	1
	Fine wire line with cable end sleeve without plastic collar	mm <sup>2</sup>	0.2	1
	Fine wire line with cable end sleeve and plastic collar	mm <sup>2</sup>	0.2	1
	According to AWG	AWG	26	18
Length	—	m	—	30
Insulation stripping length	—	mm	—	9

### Principal circuit diagram

SD6

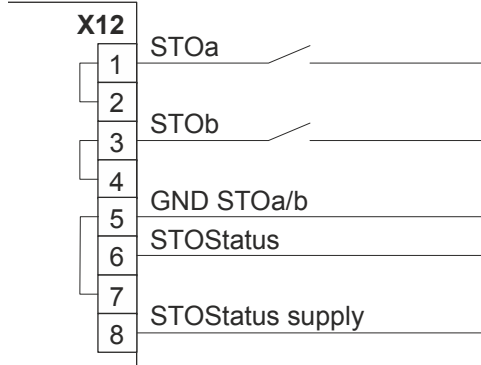


Fig. 5-1X12 – Principal circuit diagram

## 5.5 Cascading

At the output of a safety switching device, the STO safety function can be activated simultaneously at several drive controllers. The cascading of a maximum 32 devices is possible depending on the required safety figures.

### **WARNING!**

#### **Personal injury or property damage due to the loss of the safety function!**

For a cascade, an error in the wiring or control can lead to the loss of safety of the complete cascade.

- ▶ For a cascade, always apply one of the measures listed in section 5.1.
- ▶ Cascading of the status output is not possible.

## 6 Commissioning and maintenance

Test the STO safety function before initial commissioning and each subsequent commissioning of the drive controller, e.g. after conversions. Check the following:

- Does the projected function meet the safety requirements for the machine?
- Does the safety function operate without errors? Test it by means of a manual function test, for example. The function test is described in section 8.1 Wiring check.

Document the test when commissioning in a comprehensible manner.

The SD6 drive controller and the ST6 safety card are maintenance-free. However if an error occurs, send the drive controller together with the ST6 and an associated fault description to

STÖBER ANTRIEBSTECHNIK GmbH & Co. KG  
Kieselbronner Straße 12  
75177 Pforzheim

## 7 Diagnosis

### 7.1 Parameters

<b>E53</b>	<b>required SafetyModule</b>	version 0
------------	------------------------------	-----------

SafetyModule projected in DriveControlSuite, for example ST6A.

<b>E54</b>	<b>safety module information</b>	version 0
------------	----------------------------------	-----------

Information about the detected lower safety module:

- Element 0: Type
- Element 1: HW version
- Element 2: Serial number



## 7.2 Events

### 7.2.1 50:Safety function

Triggering	Level	Response	Counter
The drive controller has determined inconsistencies when monitoring the safety module. Note that the test is set up functionally and not in terms of safety.	Fault	The power board is switched off and the drive becomes torque-free/force-free. If the air override is inactive, a possibly existing brake will be controlled to close.	Z50

Cause	Description	Measure	Confirmable
1:inconsistent request (single channel)	STO was requested for more than 500 ms on one channel only.	<ul style="list-style-type: none"> <li>• Check the wiring.</li> <li>• Please contact our Service department.</li> </ul>	Yes
2:SafetyModul incorrect	The expected safety module ( <i>E53</i> ) does not match the safety module that was detected ( <i>E54[0]</i> ).	<ul style="list-style-type: none"> <li>• Project the installed safety module in the drive controller.</li> <li>• Use a drive controller with the projected safety module.</li> </ul>	No

## 8 Appendix

### 8.1 Wiring check

The STO function test detects errors in the connection wiring. The test is necessary if no other method can be applied according to section 5.1 Requirements.

During the test, the  $STO_a$  and  $STO_b$  channels must be alternately switched and checked for plausibility with the resulting  $STO_{Status}$  information. An event deviating from the expectation corresponds to an error. In case of error, the safety function must be activated at both STO channels. The drive controller may not be enabled.



#### Information

During the function test, the drive controller changes to the *switch-on disable* device state. Refer to the manual of the drive controller for further information about this device state and the device state machine, see 1.2 Further documentation.

The  $STO_{Status}$  is directly made available at the interface X12.

Alternatively you can also query the detailed status information via the fieldbus by sending the parameters  $E67[0]$  to  $E67[2]$ .



#### WARNING!

**Personal injury or property damage due to the loss of the safety function!**

The  $STO_{Status}$  outputs of the drive controller cannot be cascaded.

- To test the cabling for cascaded drive controllers, the  $STO_{Status}$  information of each individual drive controller must be checked.

A functional controller can perform the STO system test for applications up to SIL2/PLd. The test of a higher-level safety controller must be performed for SIL3/PLe applications.

The following graphic shows the switching sequence of the  $STO_a$  and  $STO_b$  channels as well as the expected responses for the STO function test.

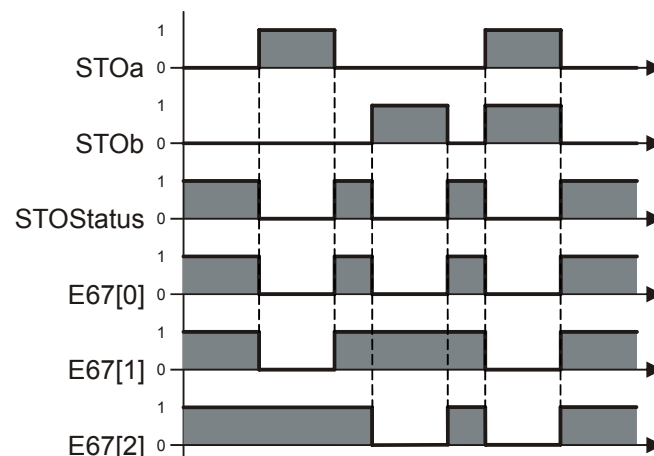


Fig. 8-1 Switching sequence of the channels

If you do not receive the desired result, check the wiring and eliminate any errors present. If a repeated function test fails, contact our Service Department (for contact details, see 1.3 Further support).

## 8.2 SS1

The SS1 safety function (Safe stop 1) according to DIN EN 61800-5-2:2007 corresponds to stop category 1 according to DIN EN 60204-1:2006. Both are based on the STO safety function.



### Information

The SS1 safety function can only be implemented in conjunction with an external safety controller or an external safety switching device.

After activation of the safety function at the time  $t_1$  an attempt is first made to stop the drive in a controlled manner before the drive is safely switched without torque at the time  $t_2$  by requesting the STO safety function.

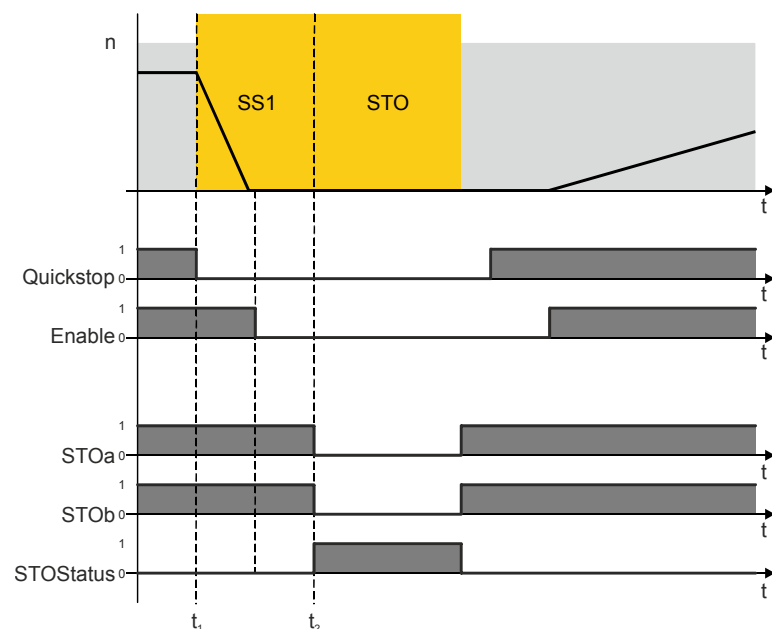


Fig. 8-2 Function diagram SS1

## 8.3 Sample application

This example (Fig. 8-3 Principal circuit diagram) shows the realization of the STO safety function in conjunction with a moving and separating safety device and a safety switching device from Pilz GmbH & Co. KG of type PNOZsigma S5.

The safety function is triggered by the safety door opening. This is recorded and monitored via the position switch (B1/B2) of the safety switching device (K1).

Both switch-off paths (T1a, T1b) are controlled in the drive controller (T1) via the enable contacts of K1. If a suitable safety switching device is used, you can also realize the safety function SS1 (Safe Stop 1). K1 must have enable contacts with a time delay for this.

The 1st switch-off path in the SD6 (T1a) is controlled via the STOb input of the drive controller. The pulse pattern transfer between the control board and power board is interrupted in the drive controller by switching the signal at this input to low level.

The 2nd switch-off path in the SD6 (T1a) is controlled via the STOb input of the drive controller. The pulse pattern transfer between the control board and power board is disabled redundantly to the T1A in the drive controller by switching the signal at this input to low level.

If you realize the STO safety function, both switch-off paths must be switched immediately after the request for low level.

If you realize the SS1 safety function, a stop ramp must be parameterized in the SD6 to be able to initially stop the drive in a controlled manner. Afterwards both switch-off paths must be switched to low level so that the transfer of the pulse pattern is disabled.

In this example the enable of the drive controller is directly switched off after opening the safety door. If this is parameterized accordingly in A44, switching off the enable in the drive controller triggers a quick stop before the STO switch-off channels are switched off with a time delay. Overall this behavior corresponds to a SS1.

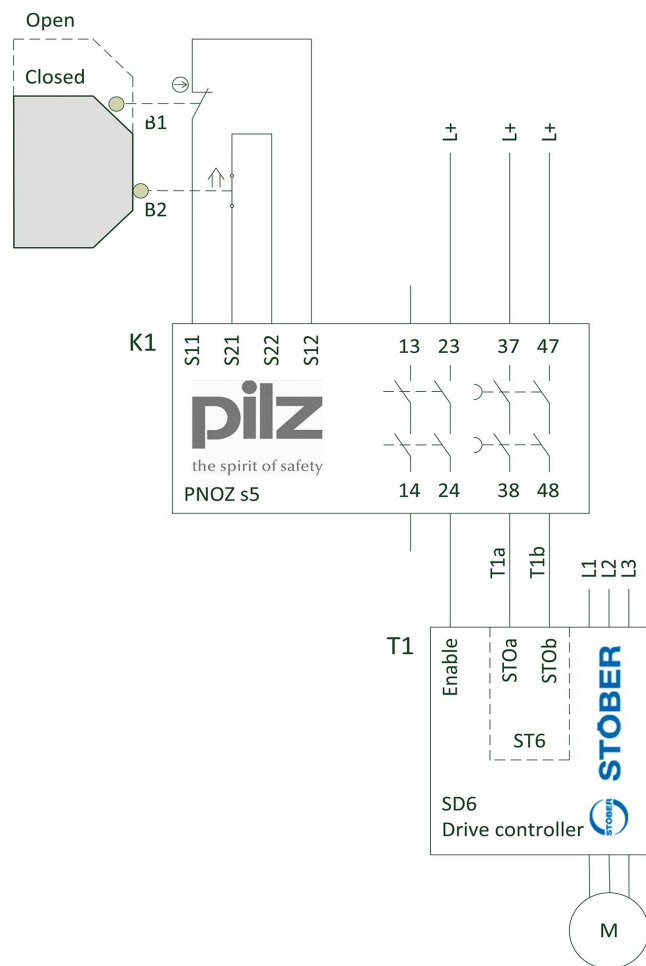


Fig. 8-3 Principal circuit diagram

### 8.3.1 Calculations of the failure probability

The safety figures are calculated according to DIN EN ISO 13849-1:2008. The calculation is based on the following safety-related block diagram that is derived from the principal circuit diagram.

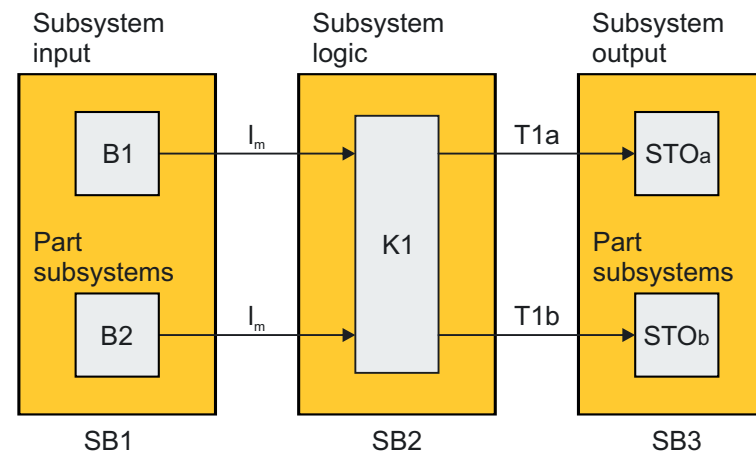


Fig. 8-4 Calculation of the safety figures



#### Information

Version 1.1.4 of the SISTEMA software is used for the norm-compliant calculation of the resulting safety figures. The SISTEMA software assistant for the assessment of safety-related machine controllers can be obtained for free from the "Institute for Occupational Safety" (IFA) of the "German Social Accident Insurance" (DGUV) ([www.dguv.de/ifa](http://www.dguv.de/ifa)).

The principal circuit diagram can be divided into three subsystems. Here, the safety device with the position switches (B1/B2) forms the SB1 subsystem, the safety switching device (K1) forms the SB2 subsystem and switch-off paths in the drive controller (T1a/T1b) are combined in the SB3 subsystem.

### 8.3.1.1 SB1 subsystem

The failure probability (PFH) for the SB1 subsystem is calculated in the following. In addition the average diagnostic coverage ( $DC_{avg}$ ) is determined and the exclusion of common cause failure (CCF) documented.

#### MTTF<sub>d</sub>

Normally the manufacturer gives the B10d safety figures as the basis for the calculation of the safety data for mechanical components such as the position switches used.

Pilz GmbH & Co.KG gives a B10d value of 2,000,000 operating cycles for the mechanical position safety switch of type PSEN me4.

If no figures are available from the manufacturer, you can take the figures of table C.1 in Appendix C of DIN EN ISO 13849-1:2008 as typical component values.

An exclusion of faults for the electrical contact is possible for the B1 position switch with positive opening operation. The B10d value of 2,000,000 cycles is assumed for the electrical NO contact of B2. This also applies for the mechanical part of B1 and B2.

For 365 workdays, 16 work hours/day and a cycle time of 5 minutes,  $n_{Op} = 70,080$  cycles/year for these components. This results in the following MTTF figures for the SB1 subsystem:

- MTTF<sub>d</sub> for position switch B1 = 285 years
- MTTF<sub>d</sub> for position switch B2 = 143 years

Both values are shortened to 100 years (MTTF classification = *high*) for further calculations.

#### DC<sub>avg</sub>

In the example the K1 safety switching device is configured and wired so that both position switches are monitored for plausibility, cross-connections and short-circuits. According to table E.1 in Appendix E of DIN EN ISO 13849-1:2008, an average total diagnostics coverage ( $DC_{avg}$ ) of 99% is assumed for the SB1 subsystem.

#### CCF

Depending on the safety structure, you must take and document measures to prevent common cause failure. For our example, choose the following measures to meet the requirement to prevent common cause failure:

- 15 points Isolation/Separation: isolation of the wiring
- 20 points diversity: use of NC and NO contacts
- 20 points draft/application/experience: protects against overvoltage and use of proven components
- 05 points assessment/analysis: FMEA of the wiring example
- 10 points environment: the position switches are applied according to the specification of the manufacturer.

This results in 70 of 100 possible points. The requirements are considered to be met with a score of at least 65. The general conditions and possible measures to prevent common cause failure can be found in DIN EN ISO 13849-1:2008 Table 10 and Appendix F, Table F.1.

### 8.3.1.2 SB2 subsystem

The K1 safety switching device in the SB2 subsystem is a finished product that meets the requirements of category 4 and PL e. The failure probability is specified by the manufacturer as

- $PFH = 2.31 \times 10^{-9}$  [1/h] for contacts without delay
- $PFH = 2.34 \times 10^{-9}$  [1/h] for contacts with switch-off delay

### 8.3.1.3 SB3 subsystem

The T1 drive controller in the SB3 subsystem is a finished product that meets the requirements of category 4 and PL e. The failure probability is specified by the manufacturer as:

- $PFH = 5.0 \times 10^{-9}$  [1/h]

### 8.3.1.4 Connection

In the example, the K1 safety switching device is configured and wired so that both position switches and their wiring are monitored for plausibility, cross-sections and short-circuits.

For the wiring between safety switching device and drive controller, fault exclusion according to DIN EN ISO 13849 2:2013 Table D.5.2 takes place. The fault exclusion in our example takes place based on the assembly of components K1 and T1 within an electrical installation space.

## 8.3.2 Result

The following table contains the calculated values for the failure probability of the individual subsystems and the resulting overall failure probability.

Subsystem	Calculation	Failure probability
SB1 - Input	SISTEMA	$PFH_d = 2.47 \times 10^{-8}$ [1/h]
SB2 - Logic	Manufacturer's specifications	$PFH_d = 2.34 \times 10^{-9}$ [1/h]
SB3 - Output	Manufacturer's specifications	$PFH_d = 5.0 \times 10^{-9}$ [1/h]
Total	SISTEMA	$PFH_d = 3.2 \times 10^{-8}$ [1/h]

For the complete STO and SS1 safety function as it is described in the application example, a failure probability of  $PFH_d = 3.2 \times 10^{-8}$  [1/h] is determined. This corresponds to the requirements for PLe or SIL3.

Performance Level	Hazardous failure/hour – Average probability ( $PFH_d$ )
a	$10^{-5} \leq PFH_d < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_d < 10^{-5}$
c	$10^{-6} \leq PFH_d < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_d < 10^{-6}$
e	$10^{-8} \leq PFH_d < 10^{-7}$

In addition to the requirements for the failure probability, structural requirements must be considered for the determination of the Performance Level.

The subsystems listed in the example meet the minimum requirements for category 4 systems.

- MTTFd = high
- DCavg = high
- CCF = requirement is met

Details about the requirements of the different categories and the determination of the safety figures for mixed subsystems can be found in Chapter 6 of DIN EN ISO 13849-1:2008.

The relationship between PL and SIL is described in table 4 of DIN EN ISO 13849-1:2008. PLe corresponds to a SIL3 in a high/continual operation mode according to this table.

## 9 Glossary

### **B10d**

Specifies the mean number of switch cycles when 10 % of the components involved have dangerously failed.

### **CCF – Common Cause Failures**

Failures due to common causes

Influencing factors that affect several systems simultaneously, e.g. failure of different components due to an individual event, whereby these failures are not based on a mutual cause.

### **DC<sub>avg</sub> – average Diagnostic Coverage**

Average diagnostic coverage

Specifies the average probability of revealing errors by a test.

### **MTTF, MTTF<sub>d</sub> – Mean Time To (dangerous) Failure**

Mean time to (dangerous) failure, also mean service life

Statistical parameter that is determined by trial and empirical values. Does not specify a guaranteed service life or guaranteed fault-free time.

### **PFH, PFH<sub>d</sub> – Probability of a (dangerous) Failure per Hour**

Probability of (dangerous) failure per hour

### **PL – Performance Level**

Performance level

Characteristic value (according to EN ISO 13849) for the reliability with which a controller fulfills a safety function.

### **SIL – Safety Integrity Level**

Integrity level – Safety

Safety Integrity Level according to EN62061 or EN61508.

### **SRP/CS – Safety Related Part of a Central System**

Safety-related part of a controller

Part of a controller that responds to safety-related input signals and safety-related output signals.





## STÖBER subsidiaries

### Technical offices

for advice and marketing in Germany

### Global presence

for advice and marketing in about 25 countries

### Service network Germany

### Service network international

#### USA

STÖBER DRIVES INC.  
1781 Downing Drive  
41056 Maysville  
Fon +1 606 759 5090  
sales@stober.com  
www.stober.com

#### Austria

STÖBER ANTRIEBSTECHNIK  
GmbH  
Hauptstraße 41a  
4663 Laakirchen  
Fon +43 7613 7600-0  
sales@stoeber.at  
www.stoeber.at

#### United Kingdom

STÖBER DRIVES LTD.  
Centrix House  
Upper Keys Business Village  
Keys Park Road, Hednesford  
Cannock | Staffordshire WS12 2HA  
Fon +44 1543 458 858  
sales@stober.co.uk  
www.stober.co.uk

#### Turkey

STÖBER Turkey  
Istanbul  
Fon +90 212 338 8014  
sales-turkey@stober.com  
www.stober.com

#### Switzerland

STÖBER SCHWEIZ AG  
Ruggölzli 2  
5453 Remetschwil  
Fon +41 56 496 96 50  
sales@stoeber.ch  
www.stoeber.ch

#### France

STÖBER S.a.r.l.  
131, Chemin du Bac à Traille  
Les Portes du Rhône  
69300 Caluire-et-Cuire  
Fon +33 4 78.98.91.80  
sales@stober.fr  
www.stober.fr

#### China

STÖBER China  
German Centre Beijing Unit 2010,  
Landmark Tower 2 8 North  
Dongsanhuan Road  
Chaoyang District BEIJING 10004  
Fon +86 10 6590 7391  
sales@stoeber.cn  
www.stoeber.cn

#### Taiwan

STÖBER Branch Office Taiwan  
Taipei City  
Fon +886 2 2216 3428  
sales@stober.tw  
www.stober.tw

#### Italy

STÖBER TRASMISSIONI S. r. l.  
Via Italo Calvino, 7 Palazzina D  
20017 Rho (MI)  
Fon +39 02 93909570  
sales@stober.it  
www.stober.it

#### South East Asia

STÖBER Singapore Pte. Ltd.  
50 Tagore Lane, #05-06,  
Entrepreneur Centre  
787494 Singapore  
Fon +65 65112912  
sales@stober.sg  
www.stober.sg

#### Japan

STÖBER JAPAN K. K.  
Elips Building 4F, 6 chome 15-8,  
Hon-komagome, Bunkyo-ku  
113-0021 Tokyo  
Fon +81 3 5395 6788  
sales@stober.co.jp  
www.stober.co.jp



# STÖBER

WE KEEP THINGS MOVING



## STÖBER ANTRIEBSTECHNIK GmbH & Co. KG

Technische Änderungen vorbehalten  
Errors and changes excepted  
ID 442478.01  
12/2015



4 4 2 4 7 8 . 0 1

Kieselbronner Str. 12  
75177 PFORZHEIM  
GERMANY  
Fon +49 7231 582-0  
mail@stoeber.de  
www.stoeber.com

24 h Service Hotline +49 7231 5823000