STÖBER

Safety module SX6

PILZ
THE SPIRIT OF SAFETY

Operating Manual-1006446-EN-03-STÖBER ID 443337.03




This document is the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

1 Overview

The safety module SX6 expands the drive controllers in the SC6, SI6 and SB6 series by adding drive-integrated safety functions in accordance with EN 61800-5-2.

When we refer to drive controllers below, we mean the SC6, SI6 and SB6 series.

The safety module SX6 contains the following safety-related functions:

- Stop functions
- Safe motion functions
- Safe monitoring functions
- Safe brake functions

In addition to the safety module itself, the following components are involved in the drive controllers' safety functions:

- Non-safety-related motor encoders
- Non-safety-related mechanical brakes

1.1 Structure

The safety module has a two-channel structure with internal diagnostic tests, thus no external safety system is required. The non-safety-related properties and functions of the drive controller do not affect the functional safety of the safety module.

1.2 Safety functions

The safety module SX6 contains the following safety functions:

Safe stop functions in accordance with EN 61800-5-2

- Safe Torque Off (STO)
- Safe stop 1 (SS1)
- Safe stop 2 (SS2)

Safe motion functions in accordance with EN 61800-5-2

- Safe Direction (SDI)
- Safely limited increment (SLI)
- Safely Limited Speed (SLS)
- Safe Operating Stop (SOS)
- Safe Speed Range (SSR)

Safe monitoring functions

- Safely Monitored Direction (SDI-M)
- Safely monitored increment (SLI-M)
- Safely Monitored Speed (SLS-M)
- Safely monitored operation stop (SOS-M)
- Safely Monitored Speed Range (SSR-M)

Safe brake functions

- Safe brake control (SBC)
- Safe brake test (SBT)

Other functions

- Safe Restart Lock (SRL)
- Safe Status Output (SSO)

Error reaction functions

When a limit value violation or an internal error is detected, the safety module SX6 triggers an error reaction function. This switches off the motor and safely interrupts torque/force generation.

- Safe stop 1 (SS1)
- Safe Torque Off (STO)

1.3 Device features

The product has the following features:

- 2 safe, dual-pole hardware outputs for control of quiescent current-activated mechanical brakes (Application of the SBC and SBT safe brake functions [📖 56]).
- EtherCAT FSoE interface for safe communication with an FSoE MainInstance with
  - 1 Byte control word per axis (ETG 6100.2 Safety Drive Profile)
  - 1 Byte status word per axis (ETG 6100.2 Safety Drive Profile)
  - 4 Byte control word (freely configurable in the user program)
  - 4 Byte status word (freely configurable in the user program)
  - 8-pin DIP switch for FSoE addressing

  The safety functions can be assigned to the freely available inputs and outputs (EtherCAT FSoE status/control bits) in the safety module's configuration tool.
- Option to monitor the drive controller's encoder supply voltage

LEDs for the safety module SX6

- Status (STAT)
- System status (STO/FS)

LEDs for FSoE status

- Status of FSoE

1.4 Terminal overview, drive controller

1.4.1 Connection overview, using SC6A162 as an example

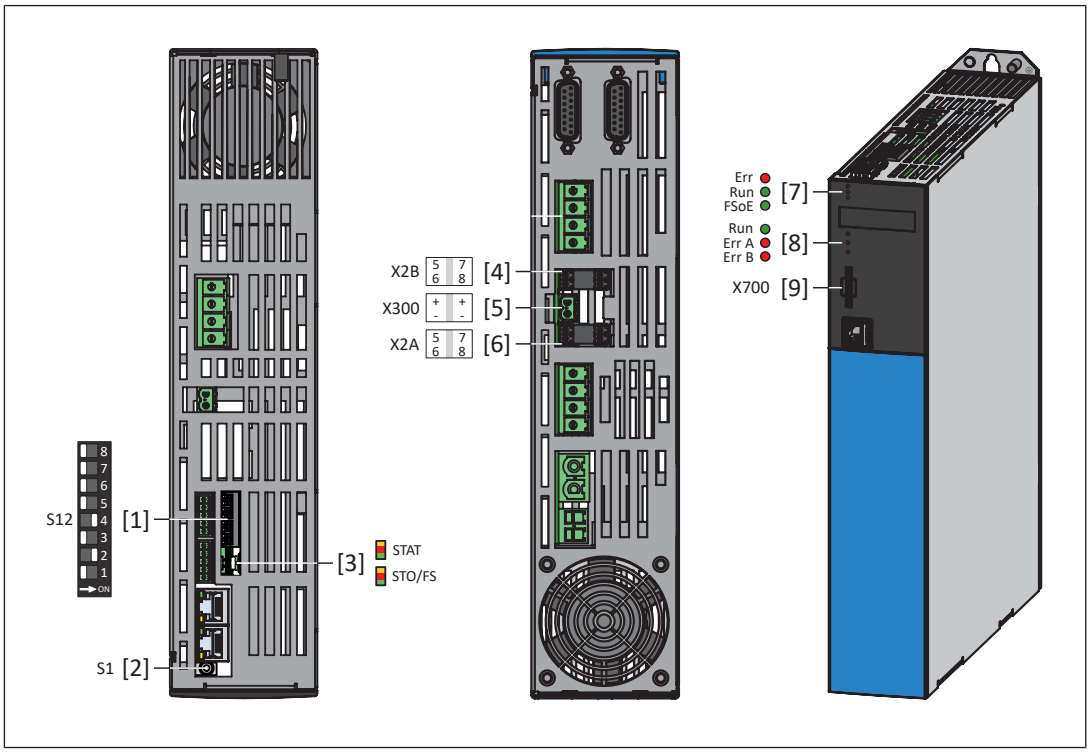


Fig.: Connection overview, using SC6A162 as an example

Legend

	Top of device		Bottom of device		Front of device
[1]	S12: DIP switch for FSoE address	[4]	X2B: Brake B (pin 5/6) and temperature sensor B (pin 7/8)	[7]	3 diagnostic LEDs Communication and safety technology
[2]	S1 operator key	[5]	X300: Supply 24 V_{DC} brake	[8]	3 diagnostic LEDs Drive controller
[3]	2 diagnostic LEDs on the safety module to display the status of the operating states	[6]	X2A: Brake A (pin 5/6) and temperature sensor A (pin 7/8)	[9]	X700: SD slot

1.4.2 Connection overview, using SB6 as an example

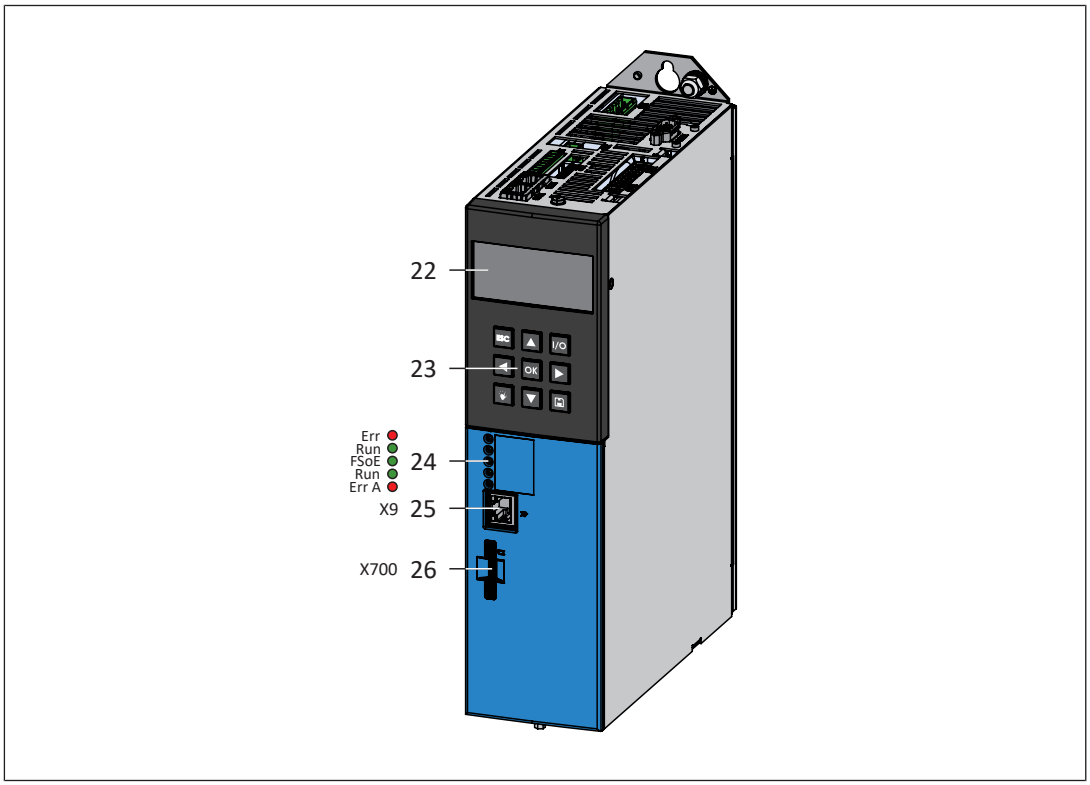


Fig.: Connection overview, using SB6 as an example, with the option OP6 (Display), device front

Legend

22	Display
23	Keys (left/right, for recommissioning after device exchange)
24	5 diagnostic LEDs
25	X9: Ethernet service interface
26	X700: SD slot

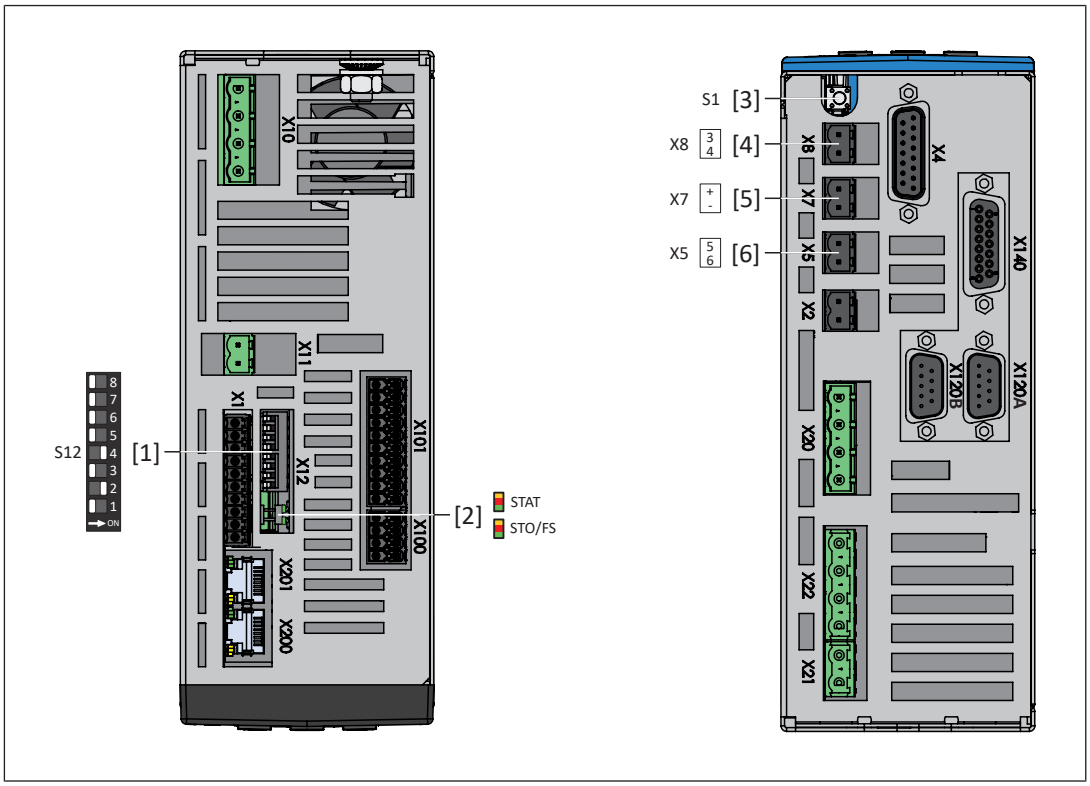


Fig.: Connection overview, using SB6 as an example, top and bottom of the device

Legend

	Top of device		Bottom of device
[1]	S12: DIP switch for FSoE address	[3]	S1 operator key
[2]	2 diagnostic LEDs on the safety module to display the status of the operating states	[4]	X8: Brake
		[5]	X7: Supply 24 V_{DC} brakes
		[6]	X5: Brake

2 Introduction

The safety module and its integration into the drive controller are the result of close co-operation between Pilz GmbH & Co. KG and STÖBER Antriebstechnik GmbH + Co. KG.

2.1 Consulting, service, address

Our website provides you with detailed information and a range of services related to our products:
https://www.stoeber.de/services

For additional or personalised information, contact our system support:
https://www.stoeber.de/services/technologieberatung/

Tel. +49 7231 582-3060
systemsupport@stoeber.de

Call our 24-hour service hotline:

Tel. +49 7231 582-3000

Our address is:

STÖBER ANTRIEBSTECHNIK GmbH + Co. KG
Kieselbronner Straße 12
75177 Pforzheim, Germany

2.2 Terminology

EtherCAT® and Safety over EtherCAT® are registered trademarks and patented technology, licensed by Beckhoff Automation GmbH, Germany.

EtherCAT designations	Abbreviations for the EtherCAT designations
Safety over EtherCAT	FSoE
MainDevice	MDevice
SubordinateDevice	SubDevice
MainInstance	MInstance
SubordinateInstance	SubInstance

2.3 Validity of documentation

This documentation is valid for the safety module SX6. It is valid until new documentation is published.

STÖBER provides the latest document versions to download from its website: https://www.stoeber.de/downloads/

2.4 Retaining the documentation

This documentation is intended for instruction and should be retained for future reference.

Please hand over this documentation when selling or passing on the product to a third party.

2.5 Disclaimer

This document was compiled in accordance with the standards and regulations current at the time of publication, and in accordance with the state of the art.

Pilz and STÖBER cannot be held liable for any damage resulting from non-adherence to the documentation or inappropriate use of the product. This particularly applies to damage caused by individual technical modifications to the project or its use and operation by non-qualified staff.

2.6 Further information

This operating manual explains the function and operation of the safety module SX6 and provides guidelines on how to connect the product.

You should also consider the following:

- The configuration of the safety module SX6 is also described in the online help for the **P**ASmotion **S**afety **C**onfigurator (PSC). This configuration tool is called "PSC" in the text below.

The documentation listed in the following table provides additional relevant information about the drive controllers. You will find current document versions at:

https://www.stoeber.de/downloads/

Device	Documentation	Contents	ID No.
Multi-axis drive system with SI6 and PS6	Manual	System structure, technical data, storage, installation, connection, commissioning, operation, service, diagnostics	442728
Drive controller SC6	Manual	System structure, technical data, storage, installation, connection, commissioning, operation, service, diagnostics	442790
Drive controller SB6	Manual	System structure, technical data, storage, installation, connection, commissioning, operation, service, diagnostics	443340
Communication EtherCAT – SC6, SI6	Manual	Electrical installation, data transfer, commissioning, diagnostics, further information	443025

You will need to be conversant with the information in these documents in order to fully understand this operating manual.

2.7 Definition of symbols

Information that is particularly important is identified as follows:

DANGER!

This warning must be heeded! It warns of a hazardous situation that poses an immediate threat of serious injury and death and indicates preventive measures that can be taken.

WARNING!

This warning must be heeded! It warns of a hazardous situation that could lead to serious injury and death and indicates preventive measures that can be taken.

CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.

NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken. It also highlights areas within the text that are of particular importance.

INFORMATION

This gives advice on applications and provides information on special features.

3 Safety

3.1 Intended use

The drive controller with installed safety module SX6 is a safety component in accordance with the Machinery Directive 2006/42/EC Annex IV and is intended for use in safety-related applications.

The following requirements have been met:

- the requirements of EN 61800-5-2 to SIL 3
- the requirements of EN 62061 to SIL 3
- the requirements of EN ISO 13849-1 to PL e (Category 4)

Intended use includes compliance with the

- operating manual for the drive controller
- online help for the PSC configuration tool.
- EMC-compliant assembly and wiring.

The following is deemed improper use

- any component, technical or electrical modification to the drive controller.
- use of the drive controller for applications other than those described in this operating manual.
- use of the drive controller contrary to the documented technical details (see Technical details [179]).

The safety module SX6 may only be used in combination with the following drive controllers:

Series	Type
SI6	SI6A061
	SI6A062
	SI6A161
	SI6A162
	SI6A261
	SI6A262
	SI6A361
SC6	SC6A062
	SC6A162
	SC6A261
SB6	SB6A06
	SB6A16
	SB6A26

3.1.1 Permitted motor types

The following motor types are approved for use with the safety module:

- Rotary synchronous motors
- Linear synchronous motors

INFORMATION

Operation of the following is not permitted:

- Synchronous motors without a motor encoder (sensorless operation)
- Asynchronous motors

3.1.2 Approved motor encoders

The motor encoder is connected to an input on the drive controller. The following motor encoders are approved for use with the safety module:

Approved motor encoders	**Drive controller interface**	
Absolute encoder	**SC6/SI6**	**SB6**
EnDat 3	X4	X4
EnDat 2.2	X4	X4, X140
EnDat 2.1 digital	X4	X4, X140
EnDat 2.1 Sin/Cos	---	X140
HIPERFACE DSL	X4	X4
SSI	X4	X4, X120
Resolver	X4	X140
Incremental encoder	**SC6/SI6**	**SB6**
HTL	X101	X4, X1
TTL	X4	X4, X120
Sin/Cos	---	X140

NOTICE

Please note the following when using the potential motor encoders:

- Problems can occur with wake & shake if encoder monitoring is active when enabled.
- When used with a commutation encoder, the incremental encoder is the deciding factor.
- Encoder with serial data transmission must provide a new value every 200 µs.
- The internal encoder resolution must be a min. 4096 incr./revolution.
- Digital incremental encoders require a resolution of min. 1024 incr./revolution.

3.1.3 Permitted brakes

Only standby current-operated mechanical brakes may be used.

The following brakes are not approved for use with the safety module:

- Magnetic powder brakes
- Eddy current brakes

Important values from the data sheet of the standby current-operated mechanical brake

For the configuration of the brake test, the following values from the data sheet of the standby current-operated mechanical brake can be relevant:

- Permitted switching frequency
- Brake engagement time

You find further information on this in chapter Brake test (SBT).

3.1.4 Third-party manufacturer licence information

The product contains open source software, whose terms of use could further limit the product's application area. It is essential that you observe the third-party manufacturer licence information.

Further information is available in the document "Third-party manufacturer licence information SX6" (document number 1006997) at www.pilz.com.

3.2 Safety regulations

3.2.1 Safety assessment

Before using a device, a safety assessment in accordance with the Machinery Directive is required.

The product as an individual component fulfils the functional safety requirements in accordance with EN ISO 13849 and EN IEC 62061. However, this does not guarantee the functional safety of the overall plant/machine. To achieve the relevant safety level of the overall plant/machine's required safety functions, each safety function needs to be considered separately.

The user is responsible for the safety of the project created in the PSC configuration tool. Pay special attention when configuring the project and observe local standards and regulations (see also Safety checks [📖 163]).

3.2.2 Use of qualified personnel

The products may only be assembled, installed, programmed, commissioned, operated, decommissioned and maintained by persons who are competent to do so.

A competent person is a qualified and knowledgeable person who, because of their training, experience and current professional activity, has the specialist knowledge required. In order to inspect, assess and handle products, devices, systems, plant and machinery, this person must be familiar with the state of the art and the applicable national, European and international laws, directives and standards.

It is the company's responsibility only to employ personnel who

- Are familiar with the basic regulations concerning health and safety / accident prevention,
- Have read and understood the information provided in the section entitled Safety
- Have a good knowledge of the generic and specialist standards applicable to the specific application.

3.2.3 Warranty and liability

All claims to warranty and liability will be rendered invalid if

- The product was used contrary to the purpose for which it is intended,
- Damage can be attributed to not having followed the guidelines in the manual,
- Operating personnel are not suitably qualified,
- Any type of modification has been made (e.g. exchanging components on the PCB boards, soldering work etc.).

3.2.4 Disposal

- In safety-related applications, please comply with the mission time T_M stated in the safety-related characteristic data.
- When decommissioning, please comply with local regulations regarding the disposal of electronic devices (e.g. Electrical and Electronic Equipment Act).

3.3 Error types, error detection and error reaction

The safety module SX6 has various error detection functions, whereby a detected error always leads to a defined error reaction.

The error types are described under Error definition [📖 26].

Error detection and error reaction are described in the subsections under Function description [📖 22].

3.4 Data backup and data security

Various data security mechanisms are used on the safety module SX6. A distinction is made between technical measures and organisational measures.

Technical measures

Technical measures contribute towards data security with regard to errors and faults. They automatically come into effect as soon as data is exposed to external influences (e.g. errors due to electromagnetic interference). Technical measures include, for example

- Redundancy when recording and processing safe signals
- Backup procedure when downloading a project
- Noise immunity

Organisational measures

Organisational measures contribute towards data security with regard to accidental or intentional data manipulation. The user is primarily responsible for applying appropriate organisational measures.

Organisational measures can mainly be covered with the term "Security". We recommend that you develop a comprehensive strategy with regard to security measures. All criteria that concern the integrity, availability, confidentiality, liability, operational safety and authenticity of data fall under the term "security" (see also the ISO 2700x series of standards).

Security measures include, for example:

- Authentication
- Password management
- Logical and functional division of the office and automation environment on Ethernet-based networks, through firewalls for example
- Mechanical interlock on unused Ethernet interfaces on the control systems

Data security measures on the configurable safety module SX6

The safety module SX6 has the following technical and organisational data security measures:

- Assignment of various access permissions for a configuration in the PSC configuration tool
  Each project must be assigned 2 passwords. The passwords are used to define access permissions to a different function range (see online help for PSC).
- Detection of different configurations
  A check sum (= "CRC safety configuration") is included when a configuration is downloaded. Different configurations can be detected based on this information.

- Detection of a deviating check sum in the remanent device memory and in the remanent memory of the safety module on restart.
- Detection of an invalid configuration when restarting a safety module
- Detection of faulty or incompatible configurations when restarting the safety module

Further information is available under Security [📖 21]

4 Security

To secure plants, systems, machines and networks against cyberthreats it is necessary to implement (and continuously maintain) an overall industrial security concept that is state of the art.
Perform a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care. If necessary, seek advice from Pilz Customer Support.

- The product is not protected from physical manipulation or from reading of memory contents during physical access. Use appropriate measures to ensure that there is no physical access by unauthorised persons. You should also use security seals so that you can detect any manipulation of the product or interfaces. Installation inside a lockable control cabinet is recommended as a minimum measure.
- The configuration computer that accesses the product has to be protected from attacks by a firewall or other suitable measures. We recommend that a virus scanner is used on this configuration computer and updated regularly.
- If necessary, protect the configuration computer and the product from unauthorised use by assigning passwords and taking further measures if required. We also recommend that the user logged on to this configuration computer does not have administrator rights.
- Only assign strong passwords and handle the passwords carefully. Be guided by generally accepted guidelines such as NIST 800-63b for example.
- Assign different permissions for the various user groups (e.g. diagnostics - configuration).

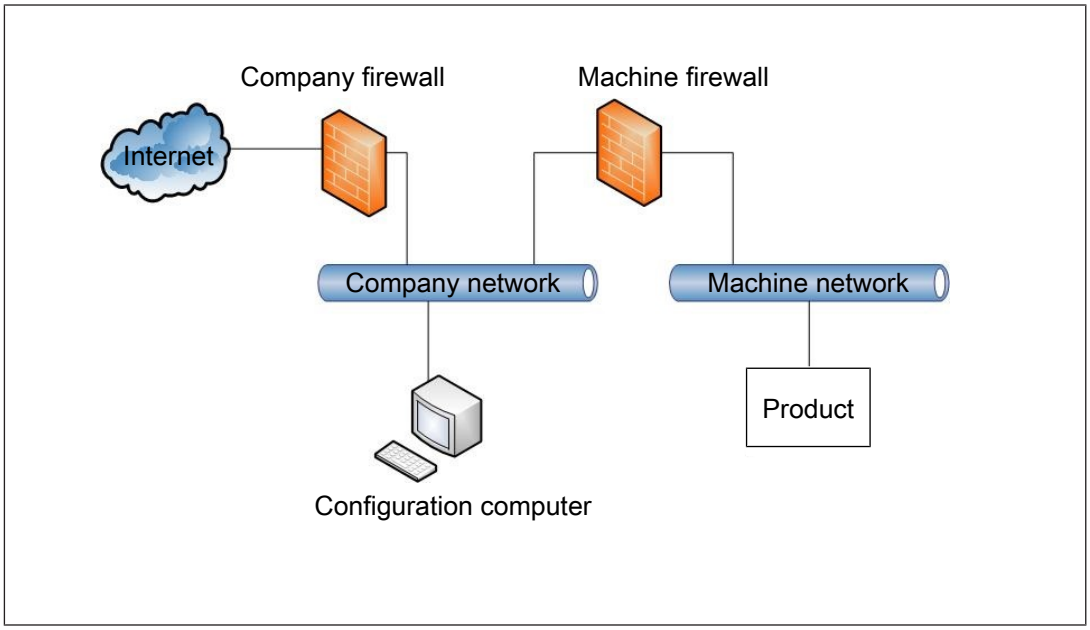


Fig.: Example network topology

5 Function description

5.1 Overview

The safety module SX6 is incorporated into the drive controller. Assembly and inspection take place before delivery. It is not possible for customers to retrofit the safety module. In the information below, the combination of drive controller and integrated safety module is called a safe drive controller.

A **safe drive system** consists of

- a safe drive controller.
- a motor with motor encoder.
- quiescent current-activated mechanical brakes (standard or safety components, optional).
- a safety controller.
- a configuration tool (PSC).

INFORMATION

The safety configurator PSC forms part of the STÖBER DriveControlSuite from Version V6.6-A.

Example: Overview of safe drive system with one axis (single axis operation)

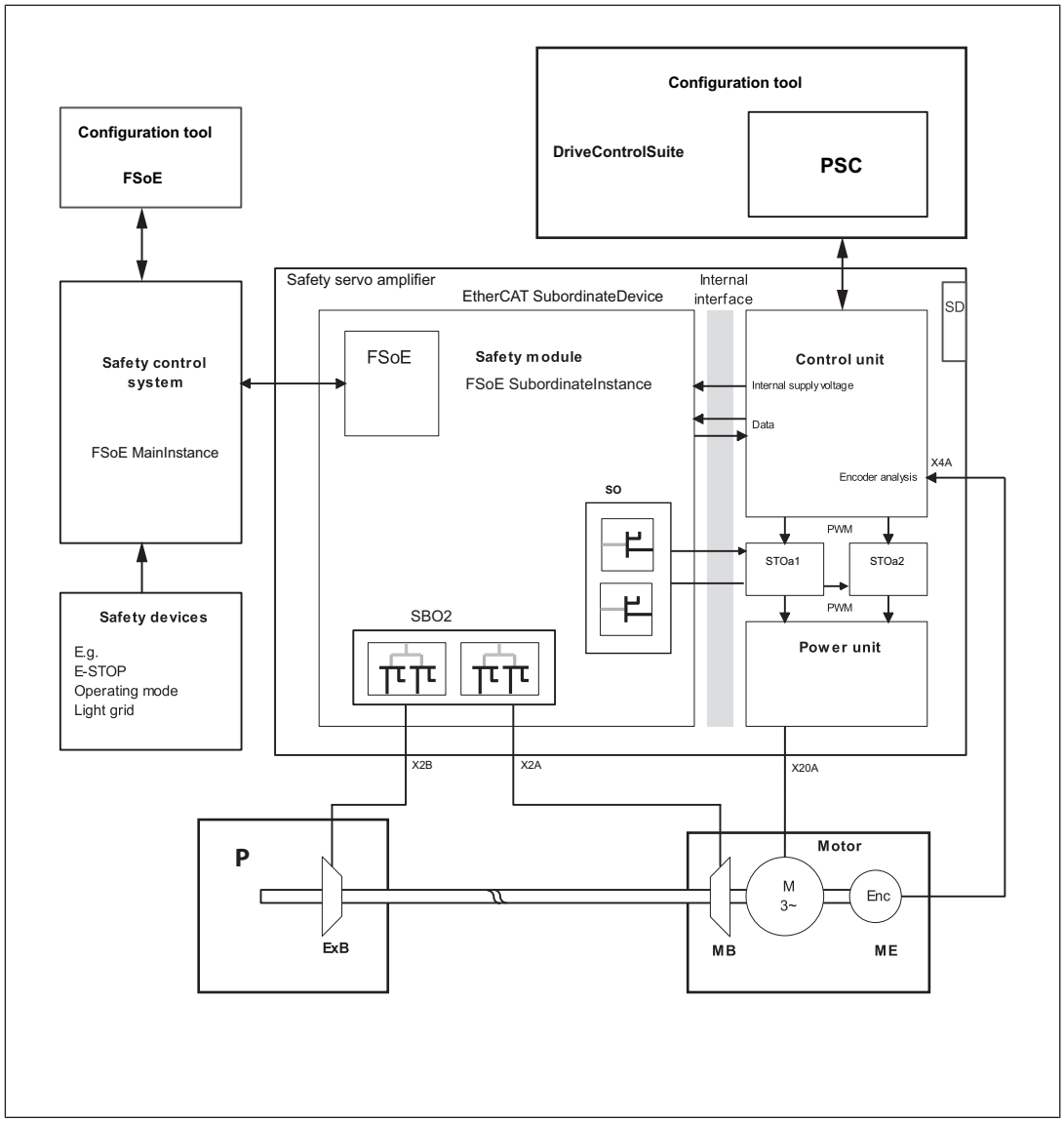


Fig.: Safe drive system with one axis (in this case with drive controller SI6/SC6 by way of example)

Legend

FSoE	**F**ail**S**afe **o**ver **E**therCAT (protocol for transferring safety-related data via EtherCAT)
SD	Card slot for SD card in the drive controller
SO	Safe output for STO control
STO_{a1}	Safe shutdown path STO_{a1}
STO_{a2}	Safe shutdown path STO_{a2}
SBO2	Safe 2-pole brake output
MB	Motor brake
P	Driven device
ME	Motor encoder
PWM	Pulse width modulation

ExB External brake

Example: Overview of safe drive system with two axes (dual axis operation)

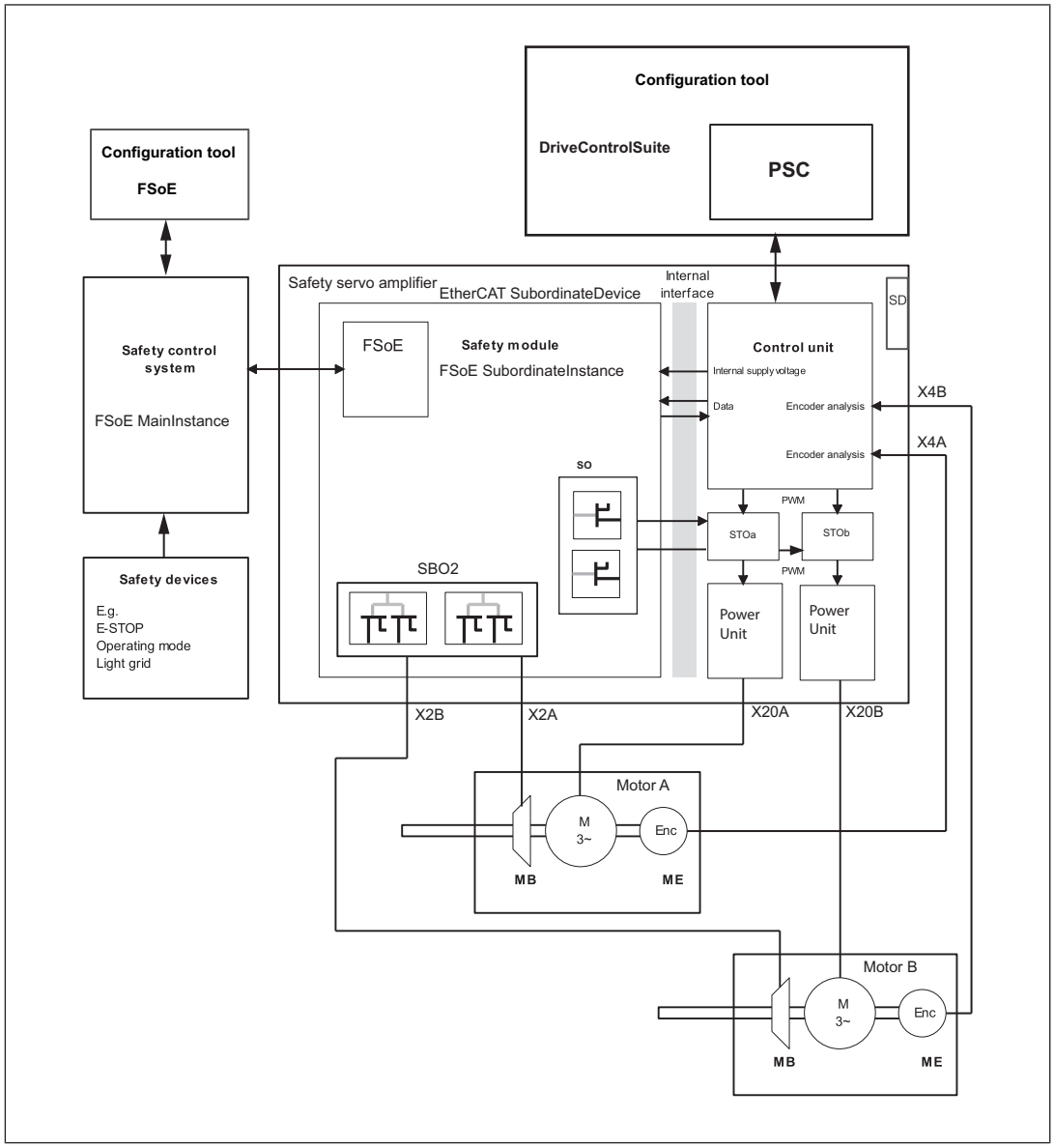


Fig.: Safe drive system with two axes (in this case with drive controller SI6/SC6 by way of example)

Legend

FSoE	**F**ail**S**afe **o**ver **E**therCAT (protocol for transferring safety-related data via EtherCAT)
SD	Card slot for SD card in the drive controller
SO	Safe output for STO control
STO_a	Safe shutdown path STO_a
STO_b	Safe shutdown path STO_b
SBO2	Safe 2-pole brake output
MB	Motor brake

ME	Motor encoder
PWM	Pulse width modulation

The safety module SX6 (depending on the configuration)

- performs a plausibility check on the connected motor encoder and uses that to generate safe speed and position values.
- compares the current speed or the current position with limit values and triggers an error reaction on the assigned drive axis when a limit value is violated.
- signals the status of safety functions to the safety controller.
- activates controlled shutdown of the assigned drive axis by the drive controller with safety functions SS1 and SS2 (optional).
- activates the integrated safe pulse block on request or in the event of an error on the assigned drive axis.
- has an option for safe triggering of up to two quiescent current-activated, mechanical brakes.
- detects faults in the mechanical brakes by means of a brake test (optional).

The safe drive controller

- interrupts the torque/power generation by the motor when the pulse block is activated.
- brakes the motor to standstill with safety functions SS1 and SS2 (optional).
- transfers configuration data from the configuration tool to the safety module.
- saves the device configuration in the drive controller’s remanent memory.

The safety controller

- evaluates signals from safety devices, such as:
  - E-STOP pushbuttons
  - Safety gates
  - Light barriers
  - Two-hand pushbuttons
- activates the safety functions in the safety module (optional).
- processes safe feedback outputs on the safety module (optional).

The PSC configuration tool

- configures and parametrises the safety module.
- ensures safe uploading and downloading of the configuration file.
- displays the status of the inputs/outputs in the online display.
- displays the error stack.

5.2 General definitions

5.2.1 Resolution of position values

The internal resolution of the safety module is always 4096 increments per revolution, irrespective of the specific application and resolution of the motor encoder (optional, user-defined planned units are converted accordingly).

WARNING!

Functional restriction of the safety function due to the use of user-defined units!

The use of user-defined units for position values can lead to a loss of accuracy due to conversion and rounding errors.

5.2.2 Determination of the rotation/movement direction

Determination of the motor's direction of rotation/movement (relative to the motor shaft when looking towards the motor flange):

- left, negative, counter-clockwise (CCW)
- right, positive, clockwise (CW)

5.2.3 Error definition

The following errors may occur in the safety module:

- Definition of **global error**
  A global error is an error that affects the whole safety module (with all defined drive axes). This includes the error types "internal error" and "FATAL error".
  Global errors have no axis reference.
- Definition of **axis-specific error**
  An axis-specific error is an error that only occurs on a drive axis, such as a limit value violation or a plausibility error on the motor encoder, for example. Axis-specific errors always have an axis reference.
- Definition of **internal error**
  An internal error is an error that occurred in the system. The safety module triggers the safety function "Safe stop 1 (SS1)" for all configured drive axes.
- Definition of **FATAL** error
  A fatal error cannot be reset. If a fatal error occurs, the safety module triggers the safety function "Safe torque off (STO)" for all configured drive axes.

5.2.4 General terminology

The following terms are used in the safety module:

- Definition of "**Motion-monitoring safety function**"

  Motion-monitoring safety functions are functions that safely monitor motor movement. These include: SOS, SOS-M, SLS, SLS-M, SSR, SSR-M, SDI, SDI-M, SLI, SLI-M, SBT, SS2 and SS1 (only with active brake ramp monitoring).

  These do not include: SSO, SBC, SRL and SS1, if brake ramp monitoring is not configured.

5.2.5 Naming of inputs and outputs on the safety functions

The input and output data for safe fieldbus communication is called safe control and status information.

In the configuration tool PSC, the activation input ACT is linked to a safe control bit. The feedback output ACK is linked to a safe status bit.

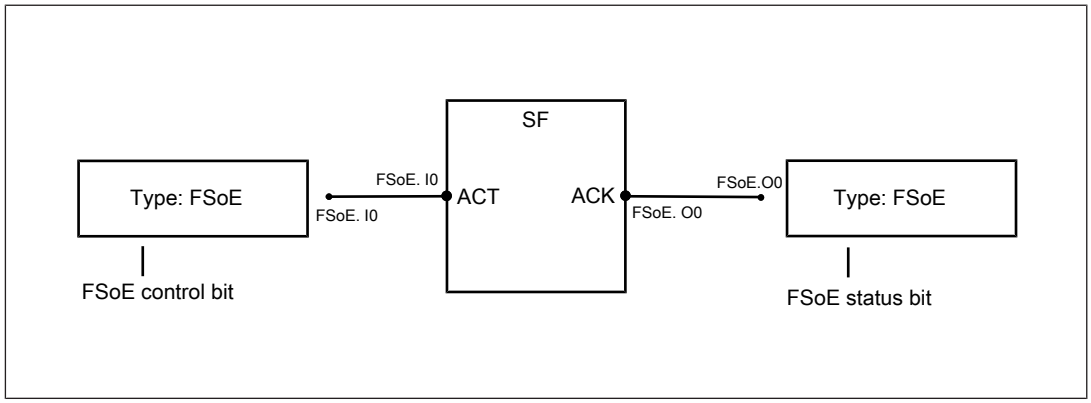


Fig.: Naming of inputs and outputs

Legend

SF	Safety function
ACT	Activation input
ACK	Feedback output (alternative designations: SRA, SDA, SSA, SBC…)

5.3 Activation and feedback from safety functions

The safety functions on the safety module SX6 are activated or deactivated by evaluating the signal levels at the safe inputs. These inputs operate in accordance with the quiescent current principle. The safety controller activates the safety functions via a 0-signal (exception: the safety function SBT is activated via a 1-signal).

The states/status of the safety functions on the safety module SX6 can be reported to the safety controller via outputs.

EtherCAT FSoE

To ensure safe connection between the safety controller and the safety module via the communication system EtherCAT FSoE, the following feature applies:

- Safe transfer is ensured by the communication system FSoE

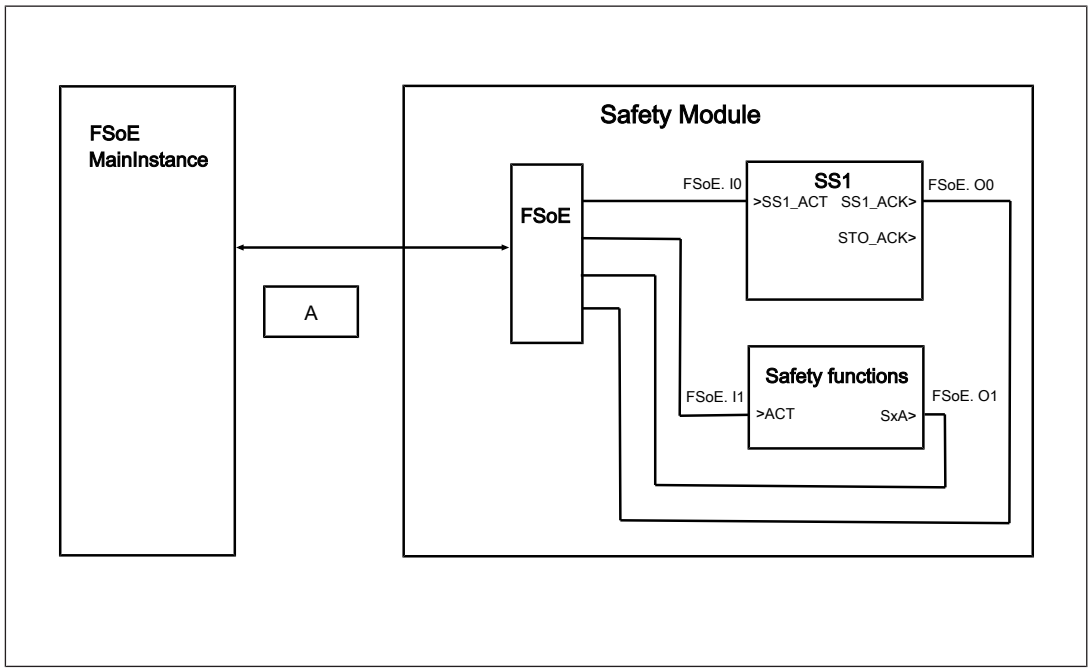


Fig.: Activation and feedback of a safety function via FSoE

Legend

A	Fault detection via the communication system FSoE

5.4 FSoE inputs/outputs

The safety module has

- Safe FSoE inputs, which can be assigned to the safety functions' activation inputs.
- Safe FSoE outputs, which can be assigned to the safety functions' feedback outputs.

FSoE inputs/outputs are assigned to the safety functions in the configuration tool.

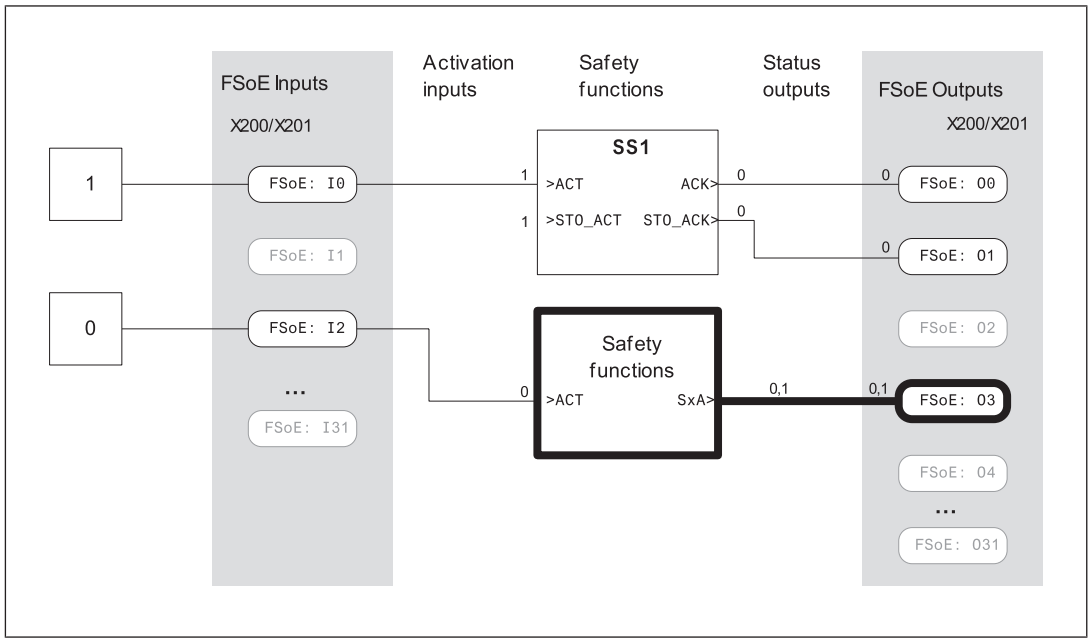


Fig.: Example assignment of FSoE inputs/outputs

Legend

Line width light	Deactivated safety function
Line width bold	Activated safety function

5.4.1 FSoE inputs

Assignment of FSoE inputs

If an FSoE input is assigned to an activation input of a safety function, this is read in and evaluated cyclically during operation.

Signals at the FSoE input

0-signal at the input: Safety function is activated

1-signal at the input: Safety function is deactivated

5.4.2 FSoE outputs

Assignment of the FSoE outputs

If an FSoE output is assigned to a feedback output on a safety function, it is updated cyclically during operation.

0-signal at the FSoE output:

- Activated safety function reports a limit value violation or a hazardous state.
- Safety function is not active.

1-signal at the FSoE output:

- Activated safety function reports the safe state.

A deactivated safety function always supplies a 0-signal at the assigned output.

NOTICE

Device state STO

In the device states STO and STARTUP, a 0-signal is output at all feedback outputs of the configured safety functions.

Exceptions:

- Feedback outputs STO_ACK and SS1_ACK of the safety function SS1 report the active state STO with a 1-signal.
- Feedback output SBT_SBA of the safety function SBT remains set throughout the inspection period.
- Safe status output READY of the safety function SSO signals readiness for operation via a 1-signal.

Feedback via shared output

When assigning FSoE outputs, there is the option of assigning multiple feedback outputs from safety functions to one FSoE output. As soon as a feedback output from an active safety function (i.e. safety function is activated and the on-delay has elapsed) issues a 0-value as the status, the FSoE output is set to 0.

NOTICE

Deactivated safety functions are disregarded by the shared output.

Even if a deactivated safety function has a 0-value, the shared output can still issue a 1-signal.
Only activated safety functions contribute to the result.

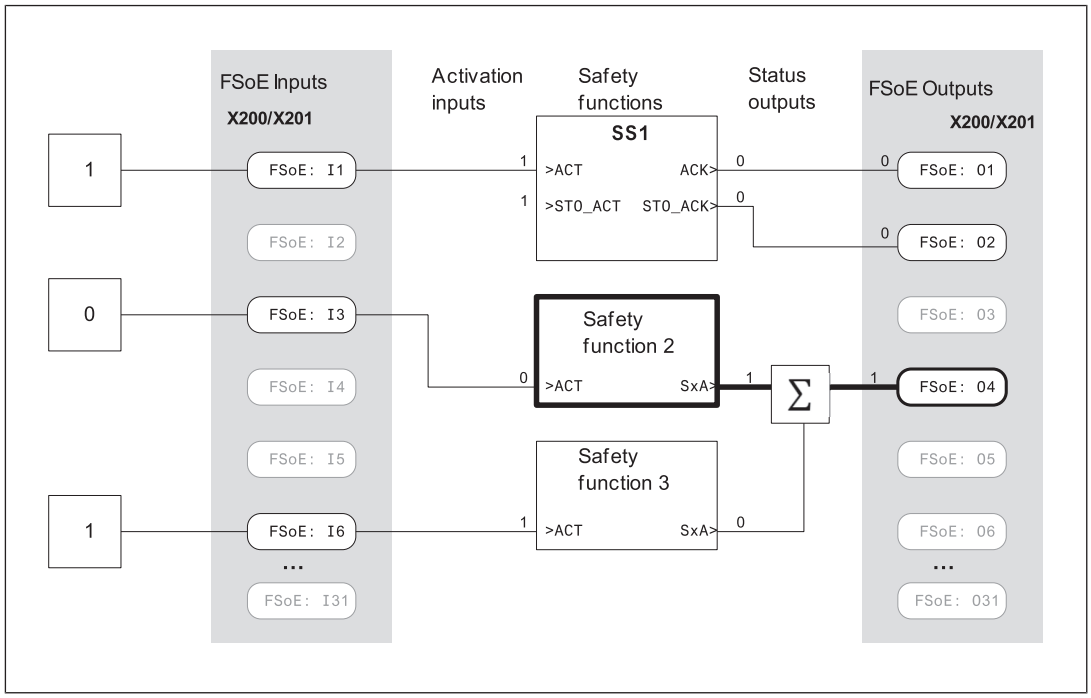


Fig.: Example, shared output emits 1-signal

Legend

Safety function 2	Safety function 2 **activated**, no limit value violation (1-signal)
Safety function 3	Safety function 3 **not activated** (0-signal)

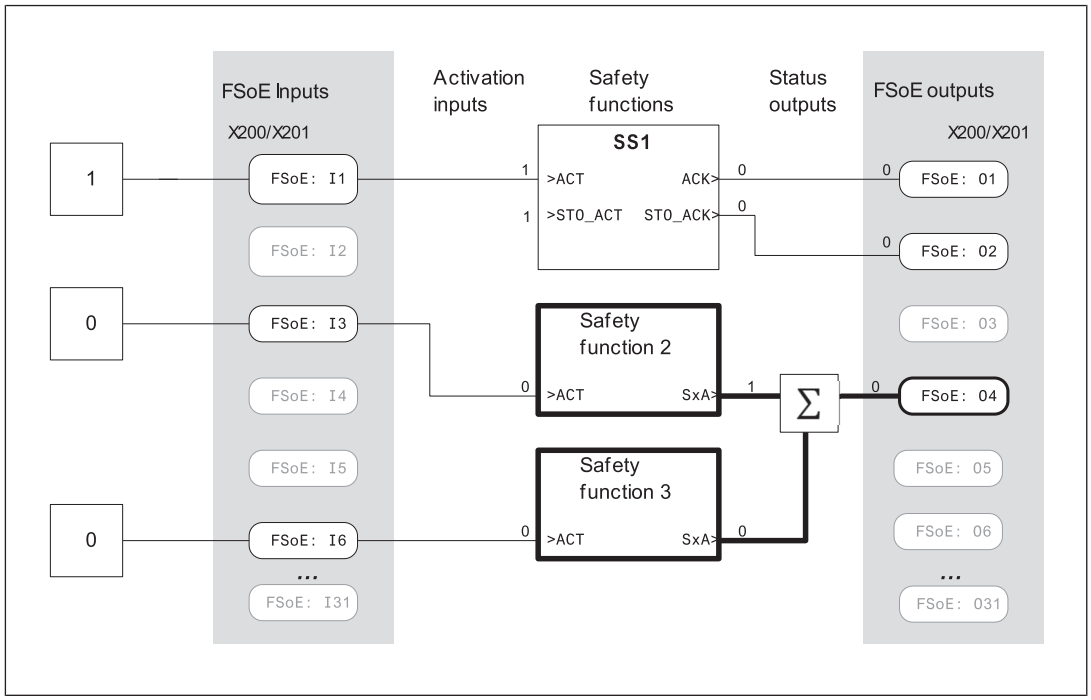


Fig.: Example, shared output emits 0-signal

Legend

Safety function 2	Safety function 2 **activated, no limit value violation (1-signal)**
Safety function 3	Safety function 3 **activated, limit value violation (0-signal)**

Shared output in conjunction with outputs from safety functions on different drive axes

If outputs from safety functions that are assigned to different drive axes are assigned to a common FSoE output, you must note the following:

If the safety function SS1 is activated on an axis (e.g. as the result of a limit value violation), then the shared output no longer takes into account the output on the safety function that is assigned to this axis.

Explanation: When the safety function SS1 is activated, the assigned drive axis is shut down and all safety functions on the affected axis are deactivated.

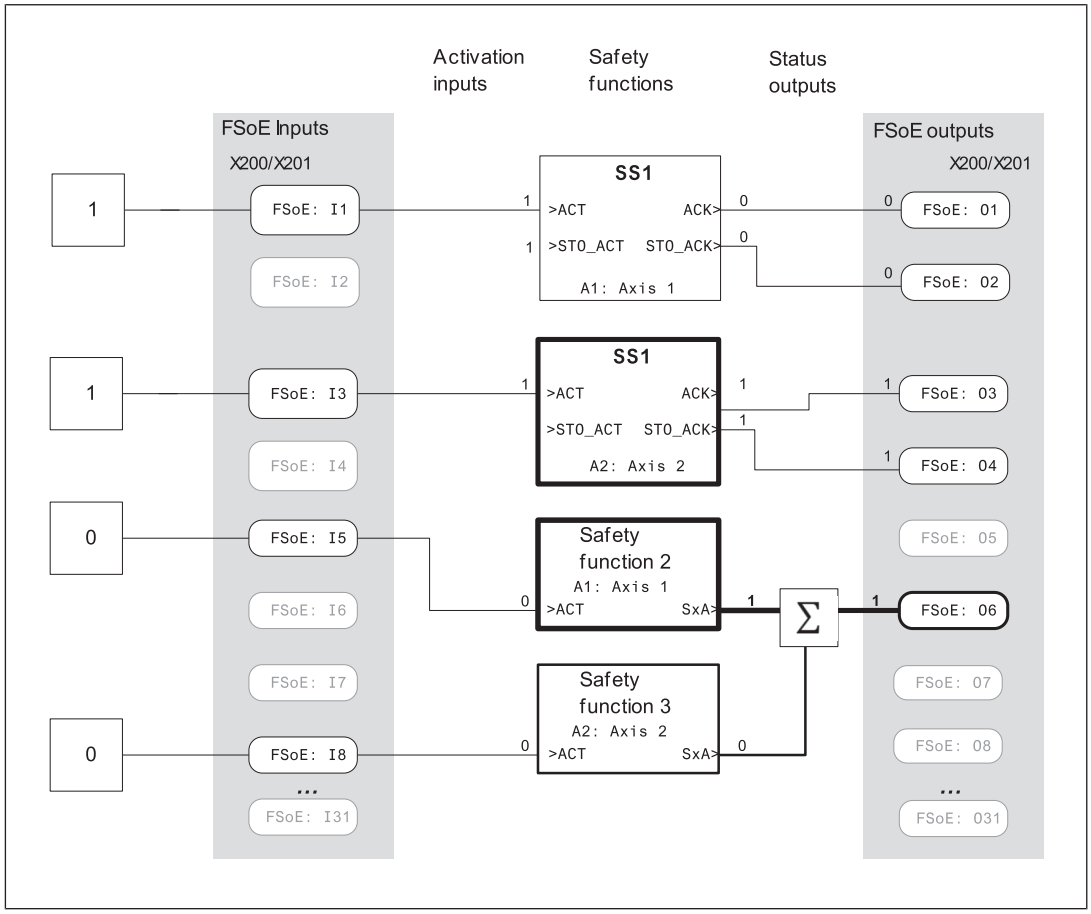


Fig.: Shared output emits a 1-signal (example, shared output with safety functions on different drive axes)

Legend

SS1 Axis 1	SS1 axis 1 **not activated** (0-signal)
SS1 Axis 2	SS1 axis 2 **activated, limit value violation (1-signal)**
SF 2 Axis 1	Safety function 2, axis 1 **activated, no limit value violation (1-signal)**
SF 3 Axis 2	Safety function 3, axis 2 **not activated** (0-signal)

5.5 Safe 2-pole hardware outputs

Safe 2-pole brake outputs

The safety module has two safe 2-pole hardware outputs to control quiescent current-activated, mechanical brakes. The outputs can be assigned to the safety function SBC (2-pole).

The hardware outputs are assigned in the configuration tool.

0-signal (0 V) at the output

- Output is high impedance.
- No current to the load.
- A connected quiescent current-activated brake is engaged, causing the braking torque/ mechanical braking force to be applied to the axis.

1-signal (+24 V) at the output

- Output is low impedance.
- Current is supplied to the load.
- A connected quiescent current-activated brake is released, causing the braking torque/ mechanical braking force to be removed from the axis.

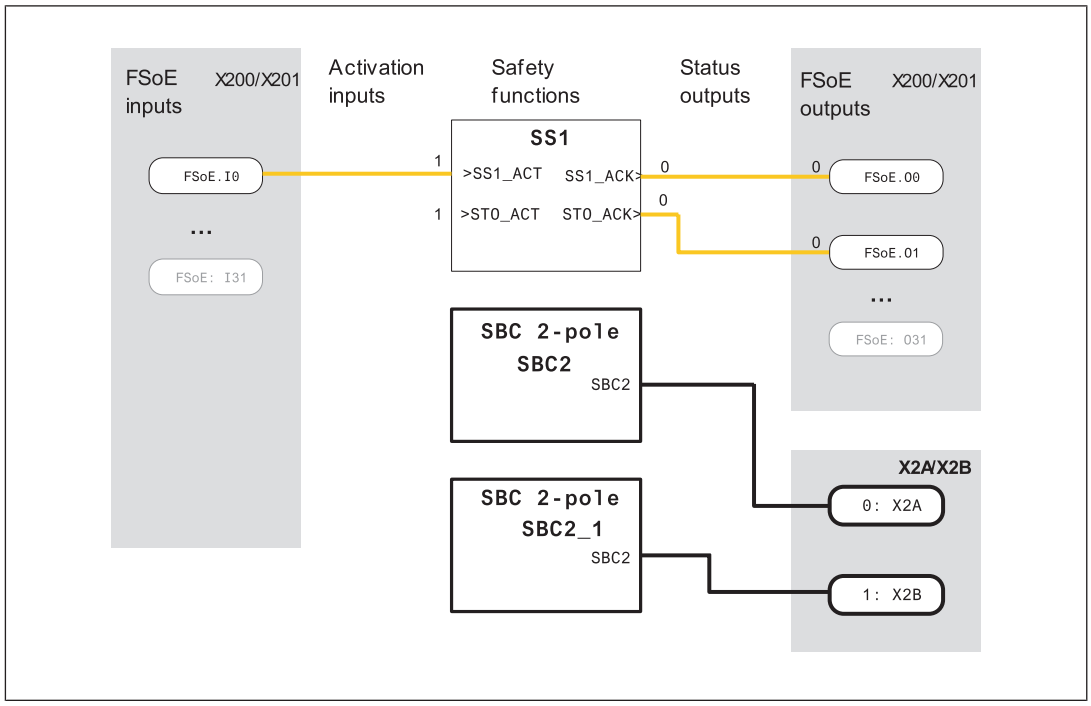


Fig.: Example assignment of SBC 2-pole, using drive controller SC6 as an example

Legend

SBC 2-pole	Safety function SBC for 2-pole brake outputs
X2A/X2B (by way of example)	Safe 2-pole hardware output to control a quiescent current-activated, mechanical brake
Yellow line	Safe fieldbus connection

Supply voltage

- The 2-pole brake outputs are supplied via the 24 V_{DC} infeed at connector X300.

General

- The maximum capacity at a hardware output is limited (see Classification according to ZVEI, CB24I [📖 184], safe dual-pole SC outputs). Connecting a higher capacity may lead to an error.
- Operation with electronic contactors has not been tested and may lead to errors. You must comply with the specification of the safety module's hardware outputs.
- Testing the 2-pole hardware output can detect an open circuit.
- The output cannot be used as a 1-pole output.

Output test

- Hardware outputs that are switched on are checked via regular off-tests.
  - Test pulses for outputs that are switched on, see Technische Daten [📖 179]
  - Outputs that are switched on are switched off for the duration of the test pulse.
  - The load must not switch off because of the test.
- Hardware outputs that are switched off are checked via regular on-tests.
  - Test pulses for outputs that are switched off, see Technical details [📖 179]
  - Outputs that are switched off are switched on for the duration of the test pulse.
  - The load must not switch on because of the test.

Open circuit detection

- The module will detect an open circuit at the hardware outputs.
- The result of open circuit detection is signalled by an error reaction.
- Loads over 3 kOhm may mistakenly be detected as an open circuit.

5.6 FailSafe over EtherCAT interface (FSoE)

The FailSafe over EtherCAT interface, also referred to as FSoE below, is used for safe data exchange between one FSoE MainInstance control system and one or more drive controllers with integrated FSoE SubInstance safety module via EtherCAT.

The safe input and output data that is transferred via FSoE is selected and configured for each safety module in the configuration tool PSC.

5.6.1 FSoE network

The FSoE protocol is standardised internationally in the standard IEC 61784-3 and signifies a safe communication system used to transfer safe process data between FSoE devices. FSoE is an open technology, supported by the **E**therCAT **T**echnology **G**roup (ETG).

A prerequisite for safe data communication via an FSoE network is a functioning EtherCAT network. Essentially this consists of an EtherCAT MainDevice [1] and one or more EtherCAT SubDevices [5], [6]. For safe data exchange via an FSoE network, an FSoE MainInstance control system [2] and one or more FSoE SubInstance devices [7], [8] are also required.

The EtherCAT and FSoE subscribers are connected in a linear topology. That means that all the subscribers are connected in series, without branches. The subscriber sequence in the configuration has no influence on communication.

In this example, the drive controller acts as EtherCAT SubDevice [5], [6] and the integrated safety module SX6 acts as FSoE SubInstance [7], [8].

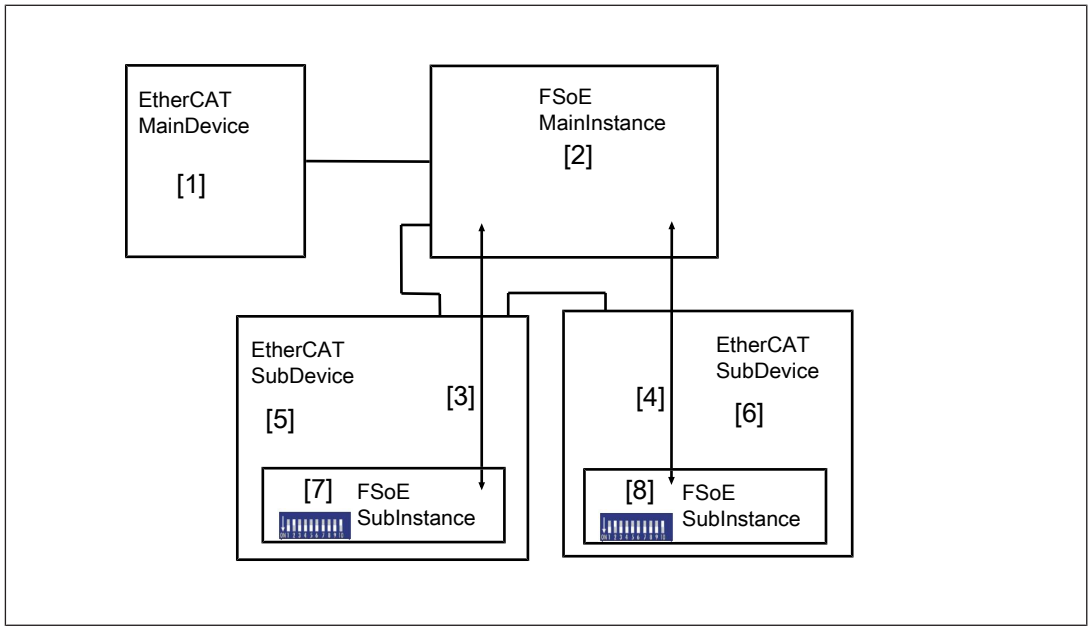


Fig.: Example, FSoE network

Legend

[1] Logic controller, motion controller (EtherCAT MainDevice)

[2] Safety controller (FSoE MainInstance)

[3] Logic connection between FSoE MainInstance and FSoE SubInstance
FSoE Connection with FSoE Connection-ID 1

[4] Logic connection between FSoE MainInstance and FSoE SubInstance
FSoE Connection with FSoE Connection-ID 2

[5] Drive controller A

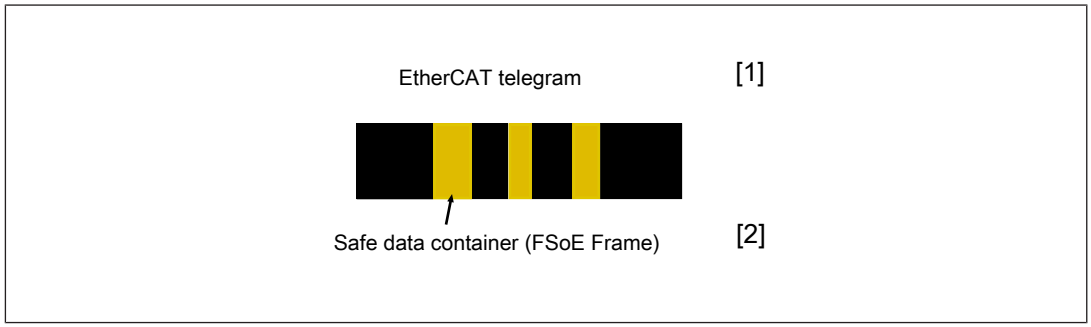
[6] Drive controller B

[7] Safety module with DIP switch in drive controller A
with unique system-wide **FSoE address**

[8] Safety module with DIP switch in drive controller B
with unique system-wide **FSoE address**

Within the standard EtherCAT telegram [1], FSoE telegrams are transported between two subscribers in a safe data container (FSoE Frame) [2]. In the drive controller, the FSoE telegrams are forwarded to the safety module and evaluated safely.

EtherCAT is regarded as "black channel" and contains both standard and safety-related data.



Legend

[1] EtherCAT telegram contains safety-related and standard data

[2] FSoE Frame contains safety-related data

5.6.2 FSoE connection

The FSoE MainInstance control system establishes a logical point-to-point connection with the respective FSoE SubInstance device.

In this connection, the FSoE MainInstance sends a request telegram to the respective FSoE SubInstance. The FSoE MainInstance initiates communication and simultaneously starts a watchdog with a configured **watchdog time**. The FSoE SubInstance acknowledges the data received at the FSoE MainInstance and also starts a watchdog for runtime monitoring. The FSoE MainInstance receives and processes the acknowledgment of the FSoE SubInstance and stops the watchdog. If the data has been processed in full, the FSoE MainInstance creates a new data packet. The complete transfer of the protocol data (request and response) represents one **FSoE cycle**. Data transfer on both devices is monitored by a watchdog.

FSoE Connection-ID

The FSoE Connection-ID is a unique identifier within the network, which defines the point-to-point connection between FSoE MainInstance and the respective FSoE SubInstance.

5.6.3 FSoE configuration

The FSoE network is configured using the configuration tool of the FSoE MainInstance control system. The communication parameters for the FSoE network are stored in the FSoE MainInstance. At power-on, the FSoE SubInstance safety module receives all the necessary configuration parameters for the FSoE communication from the FSoE MainInstance.

The FSoE configuration for a SX6 FSoE SubInstance safety module comprises the following parameters as a minimum:

- FSoE SubInstance address
- FSoE watchdog time

5.6.3.1 FSoE SubInstance address

The FSoE SubInstance address is set using the 8-pin DIP switch on the safety module/ drive controller. As a result, FSoE addresses from 1 to 254 are available. Address 0 and address 255 are not permitted. Each FSoE address may only occur once within a network.

INFORMATION

The FSoE address is read in while booting. The drive controller must be re-started in order to adopt a new address.

The FSoE address is entered via DIP switch

The DIP switch for entering the address is located on the top of the drive controller. The address results from the values of the DIP switches that are set to ON. The graphic below illustrates the safety module and DIP switches with the values 2 and 8; the corresponding FSoE address is 10.

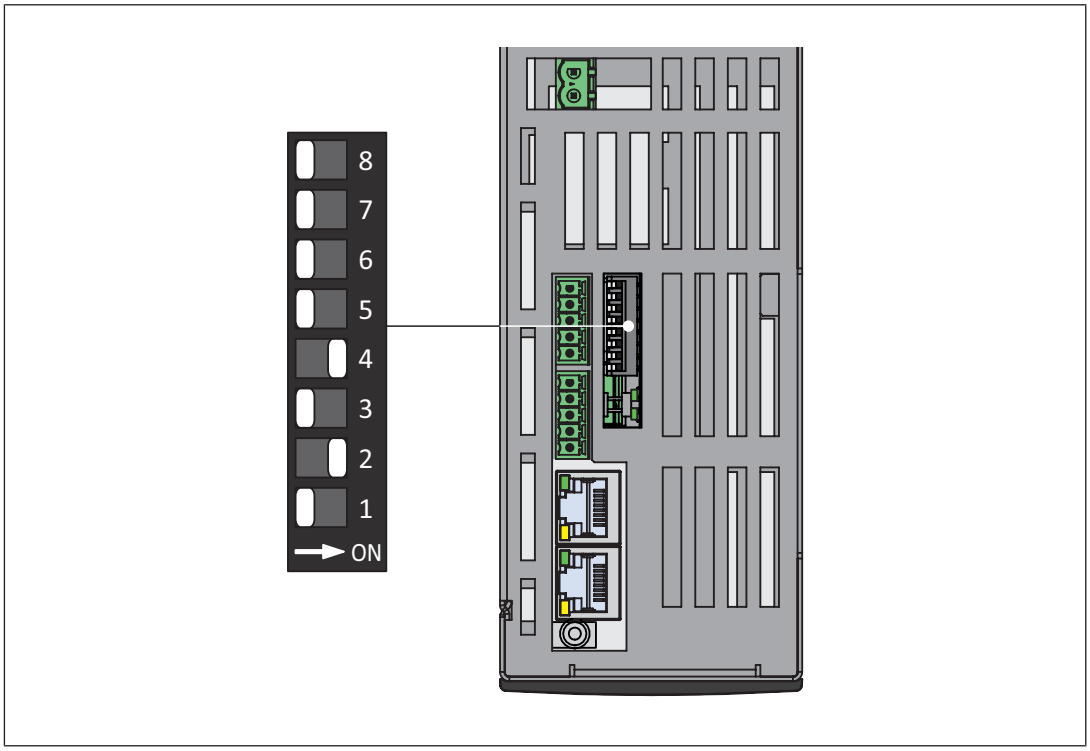


Fig.: Safety module/drive controller DIP switch

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

5.6.3.2 FSoE watchdog time

In order to identify any potential errors, communication between FSoE MainInstance and FSoE SubInstance is monitored by an FSoE watchdog. As soon as an FSoE telegram has been sent, both the FSoE MainInstance and FSoE SubInstance start a watchdog. If FSoE MainInstance or FSoE SubInstance do not receive a corresponding response telegram before the watchdog time has elapsed, the FSoE connection goes to the RESET state and the respective device switches to a safe state. The watchdog time is taken into account when calculating the maximum reaction time in the event of an error.

The FSoE watchdog time is the tolerated downtime of FSoE telegrams used to monitor FSoE communication in the EtherCAT network. It is set for each FSoE connection in the "Safety communication parameter" of the FSoE MainInstance.

The FSoE watchdog time can be set to a value between 10 ms and 10000 ms. In the case of values outside of the permitted value range, a global error is triggered in the safety module SX6, see Error definition [📖 26].

5.6.4 FSoE data exchange

The FSoE SubInstance safety module can exchange safety-related data with an FSoE MainInstance device. Communication can begin when all the subscribers needed in the FSoE network are configured and are in the FSoE state "Data" (process data is being exchanged cyclically).

Communication is ended as soon as an FSoE subscriber triggers an FSoE reset, thereby ending participation in FSoE communication.

- Data is exchanged cyclically.
- At the start of a cycle, the safety module reads the input data from the FSoE MainInstance.
- After a cycle of the safety module has ended, the output data is transferred to the FSoE MainInstance.

Safe FSoE inputs and outputs

32 safe FSoE inputs and 32 safe FSoE outputs can be configured for each safety module. The assignment of inputs and outputs to the safety functions is defined in the configuration tool PSC.

The following control and status information from the ETG.6100.2 Safety Drive Profile is also supported:

- Control Byte 1:
  - Bit 0: STO
- Status Byte 1:
  - Bit 0: STO

INFORMATION

The controlled stop (SS1) should be preferred over the uncontrolled stop (STO).
For simpler diagnostics in the event of an error, we recommend you use the STO function of the safety function SS1.
In this case, the STO control bit in the Safe Drive Profile Control Byte must be set constantly at 1. Both SS1 and a direct STO request can be selected at the safety function SS1.

5.6.5 FSoE communication

The section below shows communication between subscribers in the EtherCAT/FSoE network.

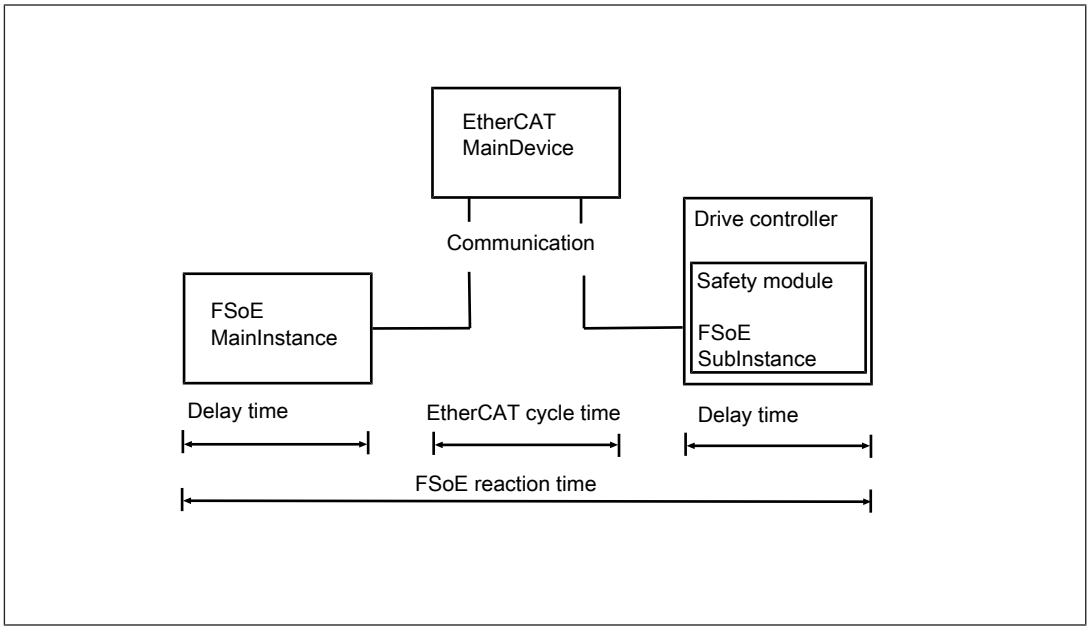


Fig.: FSoE reaction time

5.6.5.1 Reaction time of the EtherCAT FSoE connection

The EtherCAT FSoE reaction time corresponds to the transmission time of a data telegram from the FSoE MainInstance to the FSoE SubInstance and comprises the delay times of the components involved, including communication. The following times must be included in the calculation:

- EtherCAT cycle time
- Delay time FSoE MainInstance
- Delay time FSoE SubInstance
- FSoE watchdog time (for calculating the maximum reaction time in the event of an error)

Reaction time between an FSoE MainInstance and an FSoE SubInstance safety module in **error-free** normal operation (worst case).

Calculation of the FSoE reaction time in normal operation [*]	
T_{bus_react} =	2 x cycle time FSoE MainInstance +
	6 x cycle time EtherCAT communication +
	2 x cycle time FSoE SubInstance safety module
[*] The result is the min. FSoE watchdog time, see Calculation of the minimum watchdog time [📖 42]	

Maximum reaction time between an FSoE MainInstance and an FSoE SubInstance safety module in the **event of an error**.

Calculation of the maximum FSoE reaction time in the event of an error	
T_{bus_max} =	1 x FSoE watchdog time +
	3 x cycle time FSoE SubInstance safety module

5.6.5.2 Calculation of the minimum FSoE watchdog time

Calculation of the minimum FSoE watchdog time
$T_{watchdog} > T_{bus\_react}$

INFORMATION

The minimum FSoE watchdog time corresponds to the reaction time between FSoE MainInstance and SX6 FSoE SubInstance safety module in the system's normal, error-free operation.
For error-free FSoE communication, the value set for the watchdog time should be a little larger than the FSoE reaction time in normal operation.
The added reserve should generally be a min. 10%.

5.7 Motor encoder fault detection

The different aspects of motor encoder error detection are shown here.

5.7.1 Plausibility with internal system variables

Errors in the connected encoders must be safely detected in order to generate safe speed and position values. The safety module checks the plausibility of the position values of the connected motor encoder with internal system variables.

Sensor technology	Supported motor type		Supported safety functions	
	Rotary synchronous motor	Linear synchronous motor	SS1, SS2	SOS, SLS, SSR, SDI, SLI, SBC, SBT
Motor encoder and internal system variables	X	X	X	X

INFORMATION

Plausibility checks of the motor encoder with internal system variables are possible up to a power element output frequency of maximum 700 Hz.

Forced dynamisation of encoder

In order to detect errors in the connected encoders, even after prolonged standstill of the drive axis, the axis must be moved within 8 hours when the safety function is active, as follows:

- At least one turn of the motor for rotary synchronous motors
- At least a distance of 3/2 * pole pair width, for linear synchronous motors

5.7.2 Distance to fault detection

Errors in a connected motor encoder can only be detected by a plausibility test using internal system parameters once a minimum distance has been covered. This must be considered in the safety evaluation, for example the determination of the overrun distances.

Sensor technology	Fault detection per motor type	
	Rotary synchronous motor	Linear synchronous motor
Motor encoder and internal system variables	At the latest after one mechanical motor turn	At the latest after a travelled distance of 3/2 * pole pair width

5.7.3 Maximum achievable safety integrity

Error detection via internal system variables achieves the following maximum values for safety integrity for all safety functions:

Sensor technology	Maximum achievable safety integrity	
	Rotary synchronous motor	Linear synchronous motor
Motor encoder and internal system variables	SIL 3 in accordance with EN 62061 PL e (category 4) in accordance with EN ISO 13849-1	

The safety-related characteristic data of the safe drive system depends on the failure rates of the encoder used.

Various encoders with their failure rates are already considered under Technical details [📖 179]/Safety-related characteristic data.

5.8 Reaction times

Type C standards for machinery specify minimum distances between a safeguard and the hazardous area either directly or refer to the international standard ISO 13855.

The overrun of the dangerous movement by the total system must be determined to specify the minimum distances. This is made up of several times.

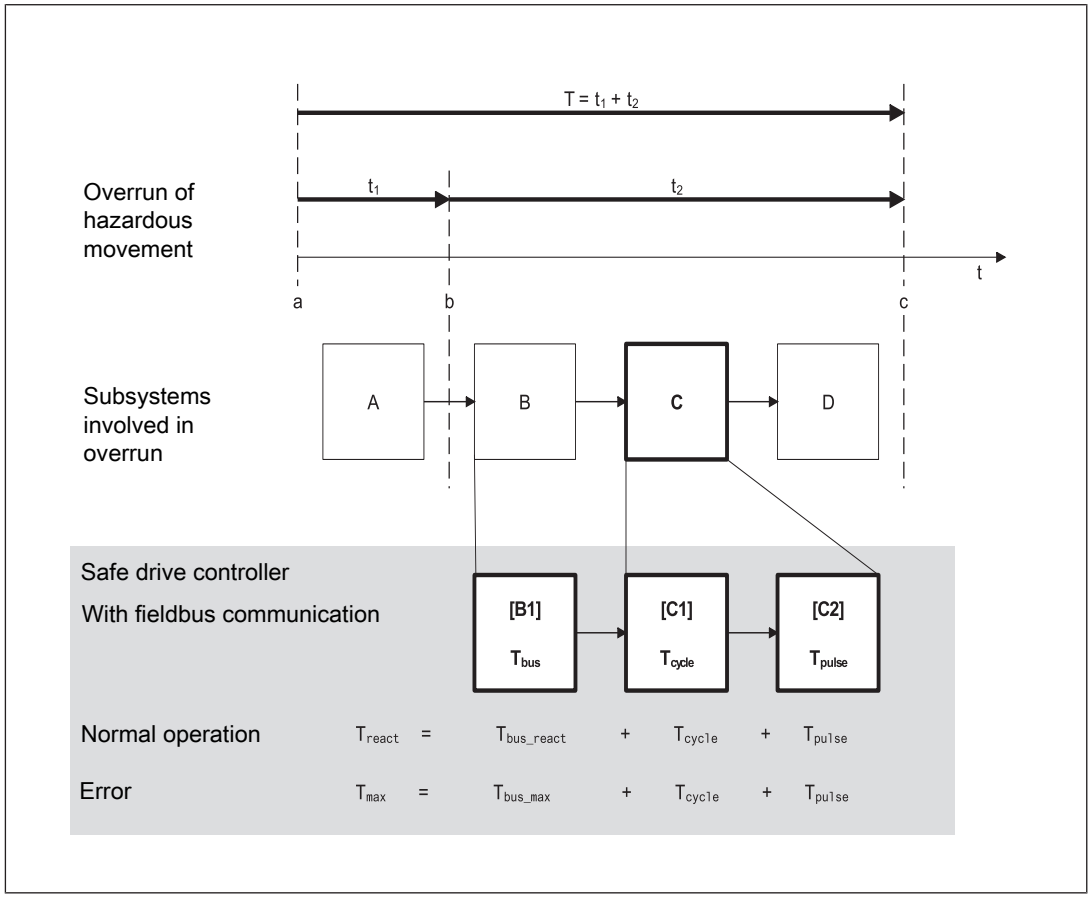


Fig.: Reaction times

Legend

T	Overall system stopping performance
t_1	Response time of the safeguard
t_2	Stopping time
a	Triggering of the safeguard
b	OFF signal is generated
c	Safe state of machine
A	Sensor/safeguard
B	Higher-level safety controller
C	Safe drive controller
D	Mechanics
[B1]	Reaction time of the fieldbus communication

[C1]	Cycle time of the safety module
[C2]	On-delay of the safe pulse block
T_{react}	Reaction time in normal operation
T_{max}	Reaction time in the case of an error

This documentation specifies the following times for subsystem B – Safety controller with fieldbus communication:

Time	Description	Section
T_{bus_react}	Reaction time of the fieldbus communication in normal operation	FSoE communication
T_{bus_max}	Maximum reaction time of the fieldbus communication in the event of an error	FSoE communication

This documentation specifies the following times for subsystem C – Safe drive controller:

Time	Description	Section
T_{cycle}	Cycle time of the safety module processor system	Technical details
T_{pulse}	On-delay of the safe pulse block	Technical details

Reaction time in normal operation T_{react}

This time includes

- Reaction time of the fieldbus communication in normal operation.
- The cycle time of the safety module processor system.
- The on-delay of the safe pulse block.

Maximum reaction time in the case of an error T_{max}

This time includes

- Maximum reaction time of the fieldbus communication in the event of an error.
- The cycle time of the safety module processor system.
- The on-delay of the safe pulse block.

Cycle time of the processor system T_{cycle}

This time includes

- Reading the inputs and the position values.
- Executing the safety functions.
- Detection of limit value violations.
- Setting the outputs.
- Activating the safety function SS1 in the event of an error.

NOTICE

For the mechanical system (subsystem D), the time it takes for the machine to reach a safe state must be determined.
The times for the stop functions (SS1, SS2) are application-specific and are not included in the stated times.

5.8.1 Reaction time for detecting that a limit value has been exceeded

The reaction time for detecting that a limit value has been exceeded is the time it takes during an active motion-monitoring safety function for the safe drive controller to detect that the permitted limit value has been violated and shut down the affected drive axis.

This time includes

- The cycle time of the safety module processor system (T_{cycle}).
- The on-delay of the safe pulse block (T_{pulse}).

A limit value violation is only detected reliably if the drive remains in the prohibited zone for longer than the cycle time of the processor system T_{cycle}.

Maximum reaction time for detecting that a limit value has been exceeded

Calculating the maximum reaction time when a limit value is exceeded	
T_{react} =	2 x cycle time of the processor system (T_{cycle}) +
	1 x on-delay of the safe pulse block (T_{pulse})

WARNING!

A violation of the prohibited zone is not detected in the case of special applications

If a configured danger zone is only violated for a very short time or a narrow, blocked zone is traversed at high speed, in some circumstances the safety module may not detect the violation of the prohibited zone due to the specified cycle time of the processor.

– Check that the safety function performs correctly if such conditions are really relevant (brief violation of danger zone, rapid passage through the blocked zone).
– Please also refer to the section entitled Safety checks [📖 163].

5.8.2 Reaction time for error detection on the motor encoder

One important aspect of the intended use of the safety module with the permitted motor types (see Permitted motor types [16]) is that, to detect plausibility between the encoder and internal system variables, the path lengths stated for the different motor types must be taken into account. The time taken to activate the safe stop function SS1 and the deceleration of the moving masses should also be accounted for in an error reaction.

The reaction time for detecting an error on the motor encoder is the result of the time for the required path length plus the time for activating the safety function and the deceleration. This must be taken into account when calculating the minimum distances and overrun on the plant/machine's hazardous movements.

NOTICE

An error on the motor encoder can lead to a commutation error on the drive controller (see Commutation error in the drive controller).

5.8.3 Commutation error in the drive controller

Faulty commutation in the drive controller can lead to uncontrolled movement of the motor. Controlled deceleration using the safe stop function SS1 is no longer possible in this case. The following measures can be taken to reduce the related increase in the plant/machine's overrun:

- Configuration of a shortest possible E-STOP brake ramp time
- Activation and configuration of brake ramp monitoring in the safe stop function SS1

5.9 Safe restart of the machine

A safe standstill during human intervention in danger zone is one of the most important requirements for the operation of machinery in accordance with the Machinery Directive.

The EN ISO 14118 standard provides an overview of various measures to avoid unexpected start-up.

If the machine

- is standing still, resetting the stop command may not trigger a restart, but merely enable it.
- is standing still following a power failure, the spontaneous restart of a machine when the power supply is reinstated must be prevented if such a restart could pose a risk.
- is standing still, the effect on machine sensors may not trigger any hazardous movements.

To prevent unexpected start-up, the safety module provides the following safety functions:

- Safe torque off (STO)
- Safe stop 1 (SS1)
- Safe stop 2 (SS2)
- Safe operating stop (SOS)
- Safe restart lock (SRL)

NOTICE

The start-up behaviour of the safety module following a fault or a stop is described under Resetting (RESET) the safety module and must be taken into account when designing the safe restart of the machine.

5.10 Resetting (RESET) the safety module

In the axis state STO (see Operating states [📖 165]),

- the safety function STO is activated. (The motor is switched to torque-free/force-free, the drive controller cannot enable the output stage.)
- There is a 1-signal at the feedback output STO_ACK.

To exit the operating state (device state or axis state) STO (see under Operating states [📖 165]), the safety module must be reset (RESET).

The safety module can be RESET in a variety of ways:

- **Safety-related**, by a higher-level safety controller
  - – Via the inputs SS1_ACT or STO_ACT of safety function SS1
  - – Via the ACT input of the safety function SRL (safe restart lock)
- **Non-safety-related**, by the drive controller
  - – Via the "ACK" command

The transition of the operating states (device state or axis state) from STO → STARTUP → RUN/FSRUN on the safety module is called a RESTART (see Operating states [📖 165]). When switching from STARTUP to RUN/FSRUN, the safety function STO is deactivated (the drive controller can enable the output stage) and the motor can execute a movement.

The RESET behaviour of the safety module can be adapted to the requirements of the application through configuration:

RESET trigger	RESET behaviour	Description
Inputs SS1_ACT/STO_ACT	0: NOP	No operation No RESTART occurs.
	1: RESTART	Acknowledge error The RESTART is triggered.
ACK command from drive controller	0: NOP	No operation No RESTART occurs.
	1: ACK ERR	Acknowledge error No RESTART occurs.
	2: RESTART	Acknowledge error A RESTART is triggered.

RESET trigger	RESET behaviour	Description
Safety function SRL	0: NOP	No operation No RESTART occurs.
	1: ACK ERR	Acknowledge error No RESTART occurs.
	2: RESTART	Acknowledge error A RESTART is triggered.

NOTICE

A RESTART of the safety module can only occur if there is a 1-signal at inputs SS1_ACT and STO_ACT (optional).

Safety-related RESET by the inputs SS1_ACT or STO_ACT

Resetting of the safety module is triggered by switching from 0-signal to 1-signal at one of the two inputs.

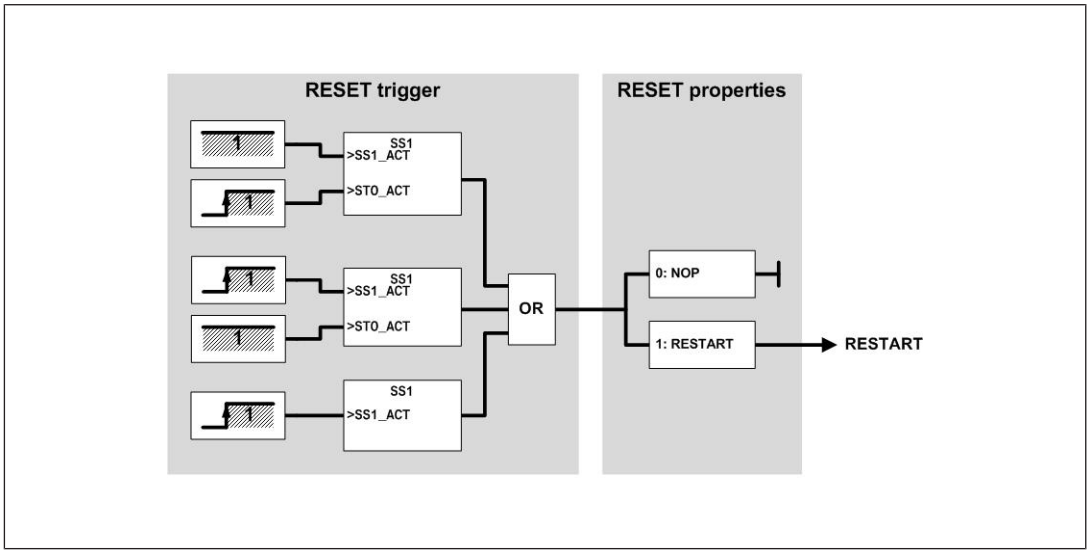


Fig.: RESET by the inputs SS1_ACT or STO_ACT

Legend

NOP	No operation
RESTART	A RESTART is triggered

Configuration of the RESET behaviour in the configuration tool

Field: RESET trigger SS1: inputs SS1_ACT/STO_ACT			
Input field	**Valid entry**	**Unit**	**Description**
RESET behaviour	0: NOP	--	No operation No RESTART occurs.
	1: RESTART	--	A RESTART is triggered.

INFORMATION

A combination with the safety function SRL (safe restart interlock) is possible (see above). In this case, the RESTART only occurs if there is a 1-signal at the input of the safety function SRL (a RESTART is enabled).

NOTICE

If the safety module is in the operating state (device state or axis state) STO, without a stop function having been activated (e.g. because of an internal error), there is a 1-signal at the inputs. To trigger resetting of the safety module, the higher-level controller needs to perform the following steps:

- Bring the plant/machine to a safe state
- Create a positive edge at one of the inputs of safety function SS1

Non-safety-related RESET by the drive controller's ACK command

The drive controller's ACK command can be used as follows:

- It performs no operation in the safety module (0: NOP).
- It acknowledges the safety module's error stack (1: ACK ERR).
- It acknowledges the error stack and triggers a RESTART of the safety module (2: RESTART).

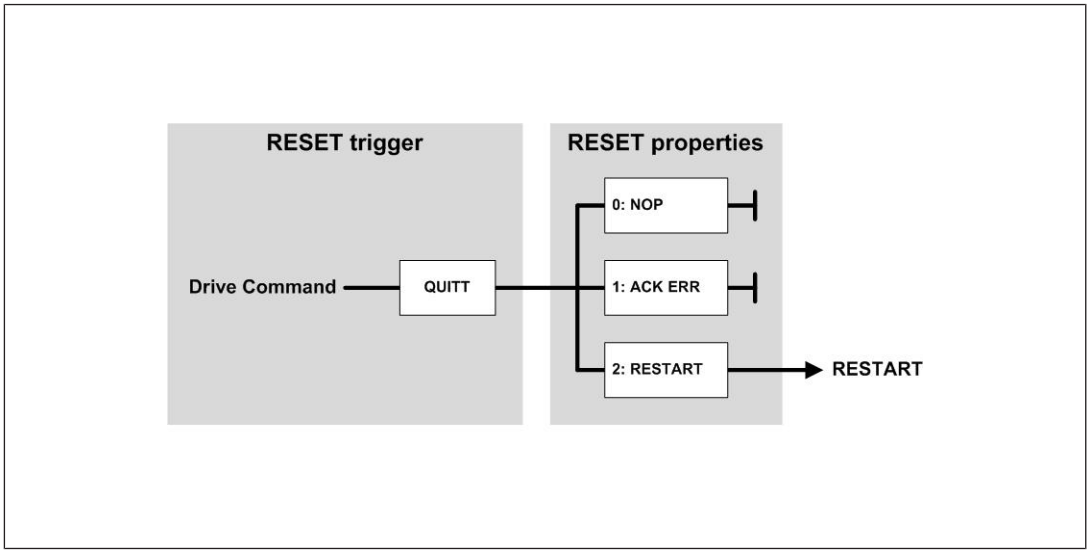


Fig.: RESET by the drive controller's ACK command

Legend

NOP	No operation
ACK ERR	Acknowledge errors
RESTART	A RESTART is triggered

Configuration of the RESET behaviour in the configuration tool

Field: RESET trigger: ACK command from drive controller			
Input field	**Valid entry**	**Unit**	**Description**
RESET behaviour	0: NOP	--	No operation No RESTART occurs.
	1: ACK ERR	--	Acknowledge error No RESTART occurs.
	2: RESTART	--	Acknowledge error A RESTART is triggered.

DANGER!

Potentially fatal injuries as a result of unexpected start-up of the motor

If the non-safety-related ACK command of the drive controller is used to RESTART the safety module, the drive controller could be enabled unintentionally, causing the motor to start up unexpectedly.
Use the ACK command of the drive controller in combination with the safety function Safe Restart Interlock (SRL) or use the inputs SS1_ACT/STO_ACT of safety function SS1. Both combinations enable a safety-related RESET of the safety module.

INFORMATION

For example, the ACK command can be triggered by the drive controller as follows:

- By pressing the ESC button on the drive controller operating panel.
- By setting the control bit A180, bit 1 (source binary signals device control: A61 must be set to "Parameter").
- By setting the control bit A181, bit 1 (source binary signals device control: S31 must be set to "Parameter")

  Further acknowledgement options are available to the drive controller, based on the specific application. These are stated in the drive controller manual.

Safety-related RESET by the safety function SRL

The safety function SRL can be used as follows:

- As safety-related enable for a RESTART (0: NOP, 1: ACK ERR). The RESTART is triggered by the alternative RESTART options for inputs SS1_ACT/STO_ACT or by the ACK command of the drive controller.
- Triggering the RESTART of the safety module (2: RESTART).

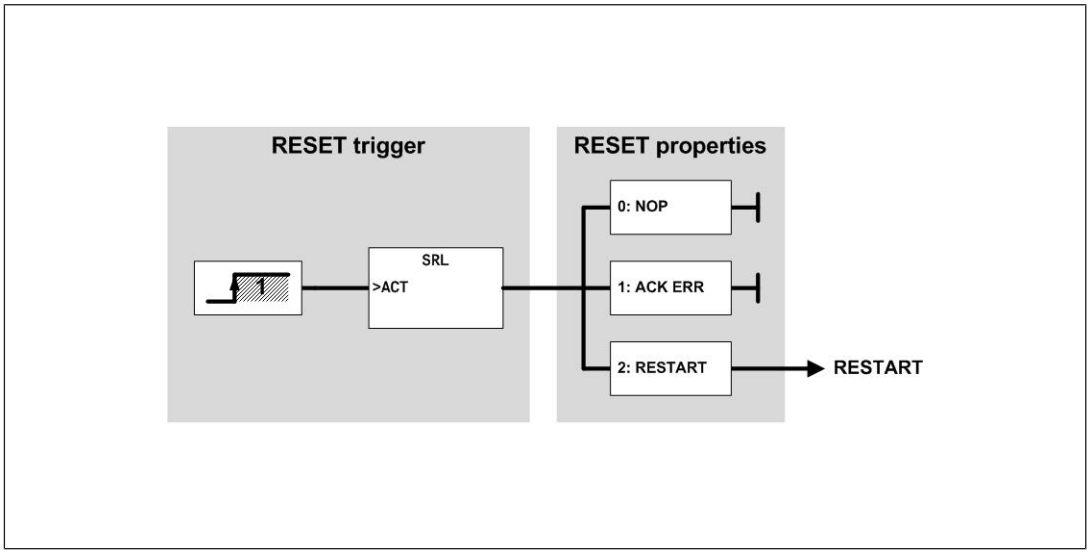


Fig.: RESET by the safety function SRL

Legend

NOP	No operation
ACK ERR	Acknowledge errors
RESTART	A RESTART is triggered.

Configuration of the RESET behaviour in the configuration tool

Field: RESET trigger: Safety function SRL			
Input field	**Valid entry**	**Unit**	**Description**
RESET behaviour	0: NOP	--	No operation No RESTART occurs.
	1: ACK ERR	--	Acknowledge error No RESTART occurs.
	2: RESTART	--	Acknowledge error A RESTART is triggered.

The safety function SRL is described in detail under Safe Restart Lock (SRL)

A combination with the ACK command of the drive controller is possible (see above). In this case, the RESTART only occurs if there is a 1-signal at the input of the safety function SRL (a RESTART is enabled).

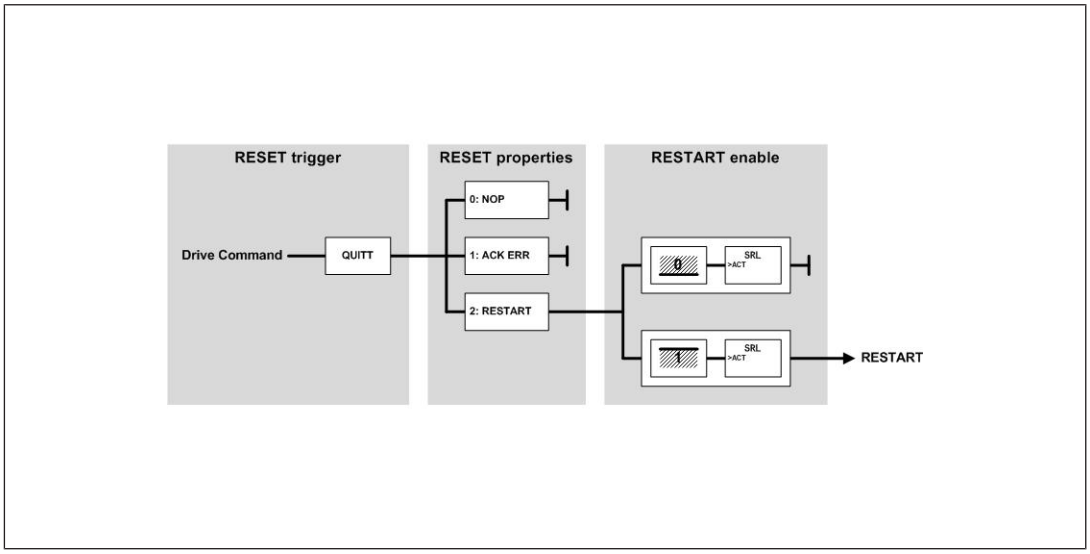


Fig.: RESET by the ACK command of the drive controller and enable via the safety function SRL

Legend

NOP	No operation
ACK ERR	Acknowledge errors
RESTART	A RESTART is triggered.

5.11 Application of the SBC and SBT safe brake functions

The safety module enables the control and testing of quiescent current-activated mechanical brakes. Mechanical brakes may be required to reduce the risk in environments where "load suspension" is used.

Mechanical brakes are particularly used with vertical traversing movements that could endanger operators and third parties. Such movements may pose risks both during operation and when the system is switched off, due to the force of gravity.

If a load has been stopped but is to be suspended in its current position, a brake is usually used. In the safety module, the "load suspension" safety function can be implemented using the safety functions SBC and SBT.

In addition to safe "load suspension", the safety functions SBC and SBT can also contribute to risk reduction in other applications with mechanical brakes, such as when "load stopping".

NOTICE

Please note that the brake must be suitable for "load stopping".

5.11.1 Definition of the "load suspension" safety function

The "load suspension" safety function is a technical measure to prevent unintended movements.

Gravity-loaded axes must be kept in position:

- During normal operation
- During interrupted operation

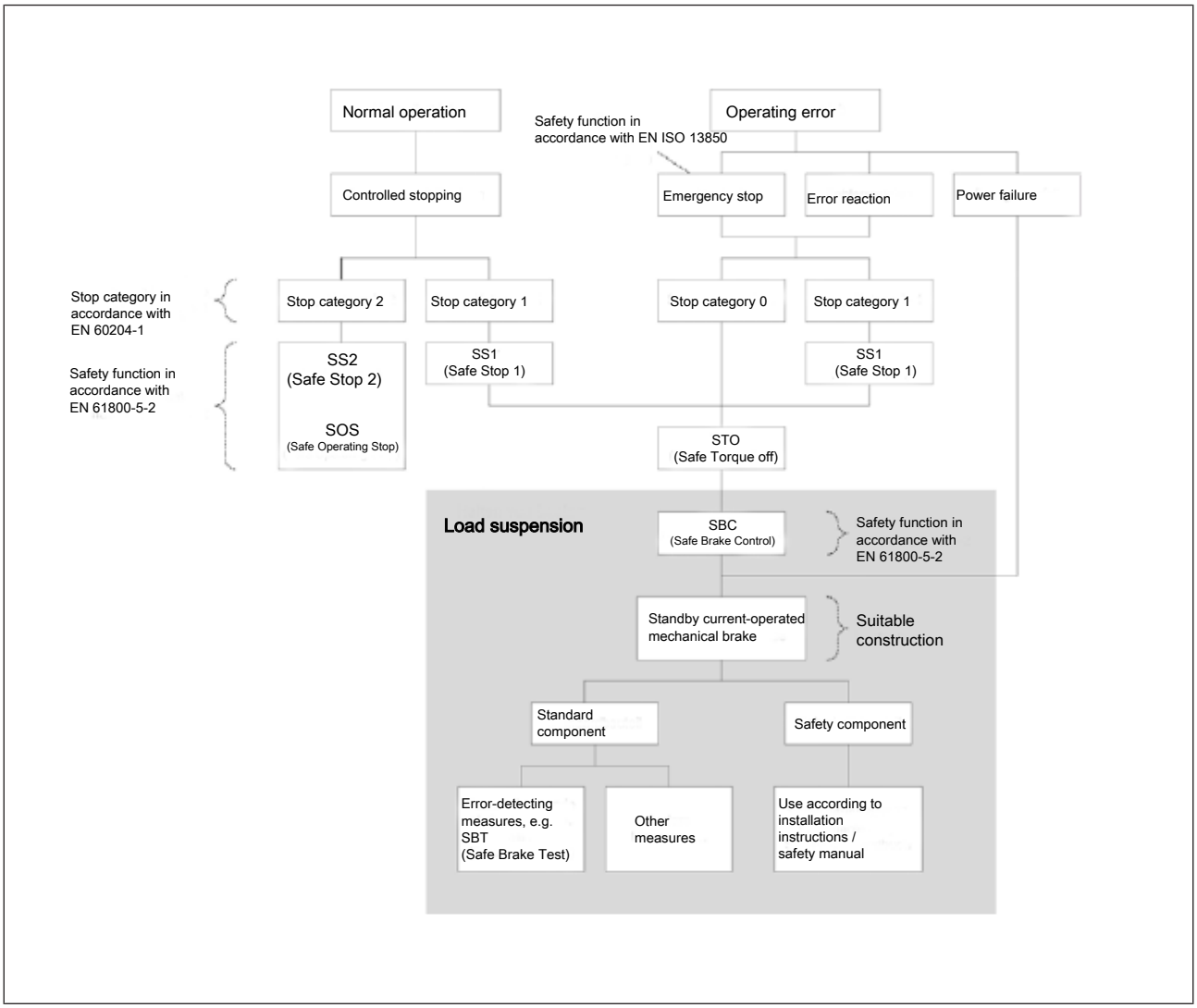


Fig.: Overview of "load suspension" during normal and interrupted operation

5.11.2 Standby current-operated, mechanical brakes

5.11.2.1 Safety components

Mechanical brakes provided by the manufacturer for safe suspension or stopping are deemed to be safety components in terms of the Machinery Directive, provided that they are sold separately.

The manufacturer provides the following documents together with the brake:

– A statement of conformity

– Installation instructions

– A safety manual for intended use in safety-related applications

5.11.2.2 Standard components

Brakes are frequently used as standard components in safety functions.

In this case the user must perform safety-related monitoring in accordance with EN ISO 13849-1 and provide proof that the brakes meet the following requirements:

– All requirements of the PL r related to the "Load suspension" safety function

Other essential measures are as follows:

– Appropriate design of the brake

– Error detection measures, such as a brake test

5.11.2.3 Motor brakes

Motor brakes (motor-integrated brakes) cannot be sold separately. This means that they cannot be sold independently from the motor. They can therefore not be categorised as a safety component in accordance with the Machinery Directive 2006/42/EC.

5.11.3 Options of "Load suspension" implementation

The safety module offers the option

- To activate quiescent current-activated, mechanical brakes.
- To activate an external safe device to activate brakes.

The safety module provides functions and interfaces that permit the user to implement "load suspension" in various ways.

The implementation concept is determined by:

- The specifications for mechanical brakes
  (depending on the load to be suspended, mounting location, etc.)
- The required performance level (PL r)
- The required category
- The test options

The following requirements can be derived from the specified mechanical brakes:

- Activation of the brakes
  (voltages, currents, performance drop, emergency shutdown, etc.)
- Fault detection measures

5.11.3.1 Safety module has direct control of quiescent current-activated mechanical brakes

For activation, the brakes are connected to the 2-pole hardware outputs of the safety module.

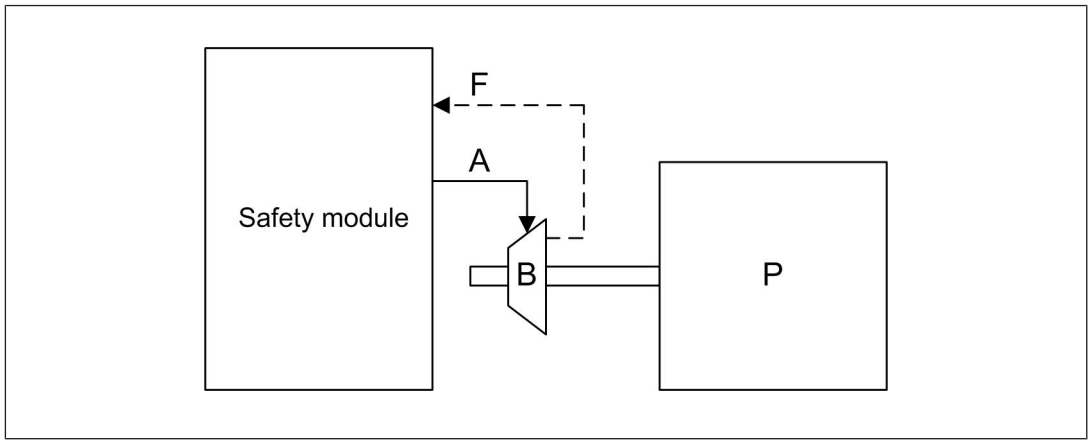


Fig.: Activation of quiescent current-activated, mechanical brakes

Legend

F	Optional feedback
A	Control
B	Quiescent current-activated, mechanical brake
P	Driven system (for example a gravity-loaded axis)

5.11.3.2 Triggering an external safe system

If an external safe system is used, this is activated via the safety function SBC 1-pole.

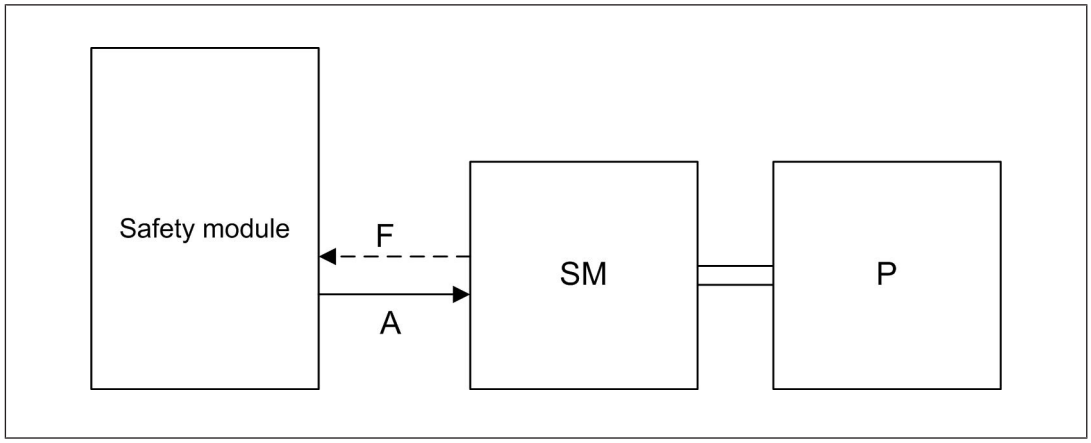


Fig.: Activation of an external safe device

Legend

F	Optional feedback
A	Trigger signal
SM	Safe device to stop and suspend loads
P	Driven system (for example a gravity-loaded axis)

5.11.4 Examples

General information about the examples:

The safety integrity tables indicate the maximum achievable categories in accordance with EN ISO 13849-1.

No performance levels can be indicated, as the failure rates and the mechanical requirements differ from application to application.

The following requirements apply to all "Load suspension" examples:

- To detect a hazardous movement (e.g. sagging of the load to be suspended), it is essential that a safe motion function (e.g. SLS, SOS, etc.) must be active. In the event of an error, this triggers and activates the safety function STO.
- To ensure that a brake is engaged if the STO safety function is activated, thus stopping the hazardous movement, at least one safety function SBC must be configured (see Safe Brake Control (SBC)).
- An error analysis must be carried out for the mechanical brake used.
- An error analysis must be carried out for the driven system.

INFORMATION

The following examples of options for implementing "Load suspension" illustrate methods of control with a drive axis.

5.11.4.1 "Load suspension" with a motor brake and an external system

Triggering a standby current-activated, mechanical motor brake and an external safe system. In this example, the safety function SOS (safe operating stop) should be used as the active safety function.

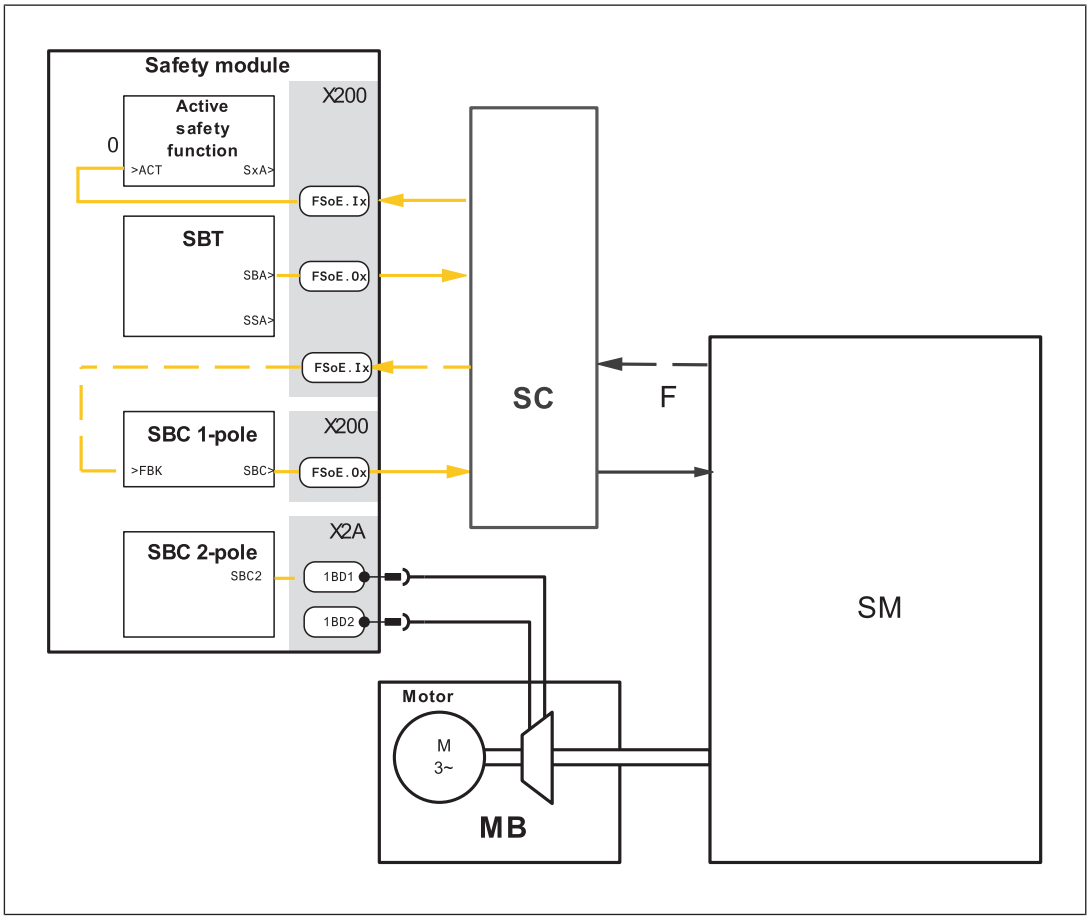


Fig.: "Load suspension" with a motor brake and an external safe system

Legend

SC	Safety controller (FSoE MainInstance)
F	Optional release monitoring
- - -	Dotted line, optional
SM	Safe device for "load suspension"
MB	Quiescent current-activated, mechanical motor brake
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	**4**
Active stop function or safety function for motion monitoring	Essential
SBC (safe brake control)	Essential
Feedback SBC release monitoring	Optional
SBT (safe brake test)	Essential
Categorisation of the motor brake as a well-tried component (Cat. 1)	Not required

Max. category in accordance with EN ISO 13849-1	4
Categorisation of the motor brake as a safety component	Optional

- The safety module only generates trigger signals for activation of the "Load suspension" safety function for the external system.
- If necessary, feedback signals from the system can be evaluated by the safety module.
- The external system should be regarded as a separate, safety-related subsystem (SRP/CS in accordance with EN ISO 13849-1).
- A separate error evaluation must be carried out for the components included in the safe system (e.g. brake, power control, driven system, etc.).
- Brakes must meet the basic requirements of the application (momentum, temperature, environment, vibration, etc.).
- Brakes must be employed in accordance with the intended use as prescribed by the manufacturer.

5.11.4.2 "Load suspension" with an external brake (standard component)

Triggering of a quiescent current-activated, mechanical brake by the 2-pole SBC+/- output (X2A) with or without release monitoring (feedback).

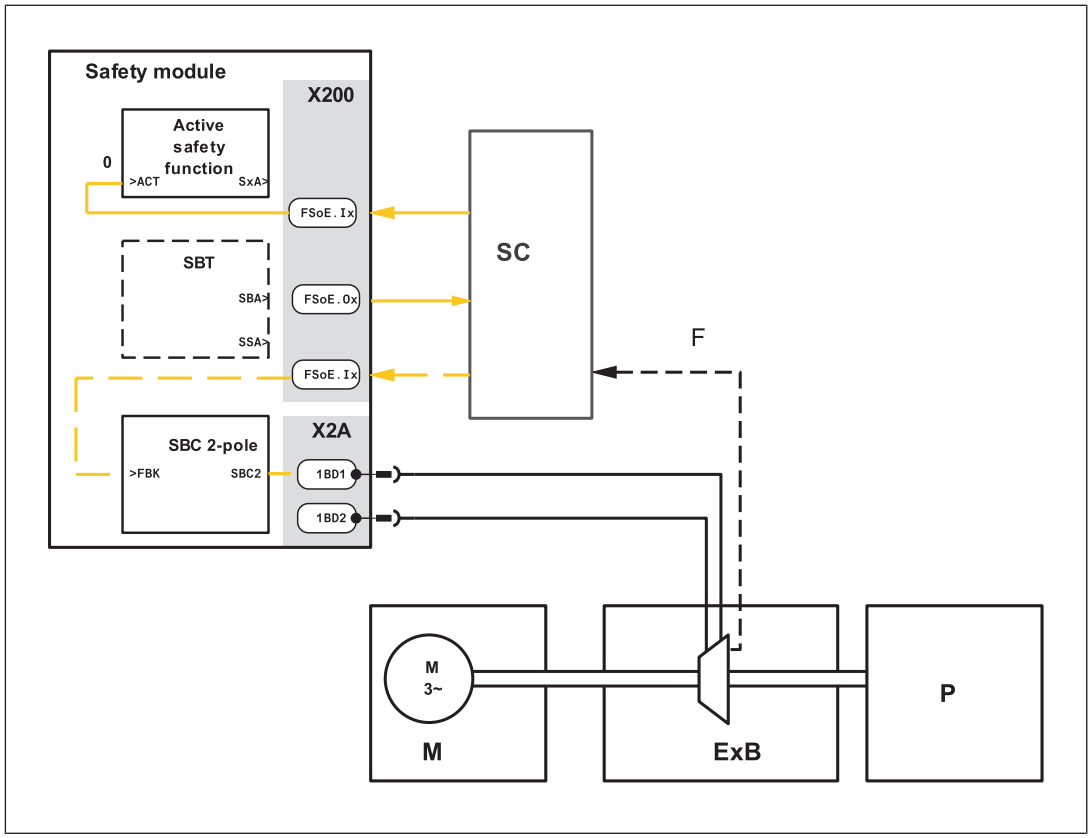


Fig.: "Load suspension" with an external brake (standard component)

Legend

SC	Safety controller (FSoE MainInstance)
M	Motor
F	Optional release monitoring (feedback)
- - -	Dotted line, optional
ExB	External, quiescent current-operated, mechanical brake
P	Driven system (for example a gravity-loaded axis)
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	1	2
Active stop function or safety function for motion monitoring	Essential	Essential
SBC (safe brake control)	Essential	Essential
Feedback SBC release monitoring	Optional	Optional
SBT (safe brake test)	Not required	Essential

Max. category in accordance with EN ISO 13849-1	1	2
Categorisation of the brake as a well-tried component (Cat. 1)	Essential	Not required
Categorisation of the brake as a safety component	Not required	Not required

The following notes apply:

- A mechanical brake must be used to achieve Category 1 in accordance with EN ISO 13849-1. This must be categorised as a well-tried component.
- If necessary, release monitoring of the brake can be evaluated by the safety function SBC.
- If Category 2 in accordance with EN ISO 13849-1 is to be achieved, the safety function SBT must be configured in the safety module and the brake must be tested at regular intervals.

5.11.4.3 "Load suspension" with a motor brake (standard component)

Control of an acquiescent current-activated mechanical motor brake through the 2-pole SBC+/- output (X2A).

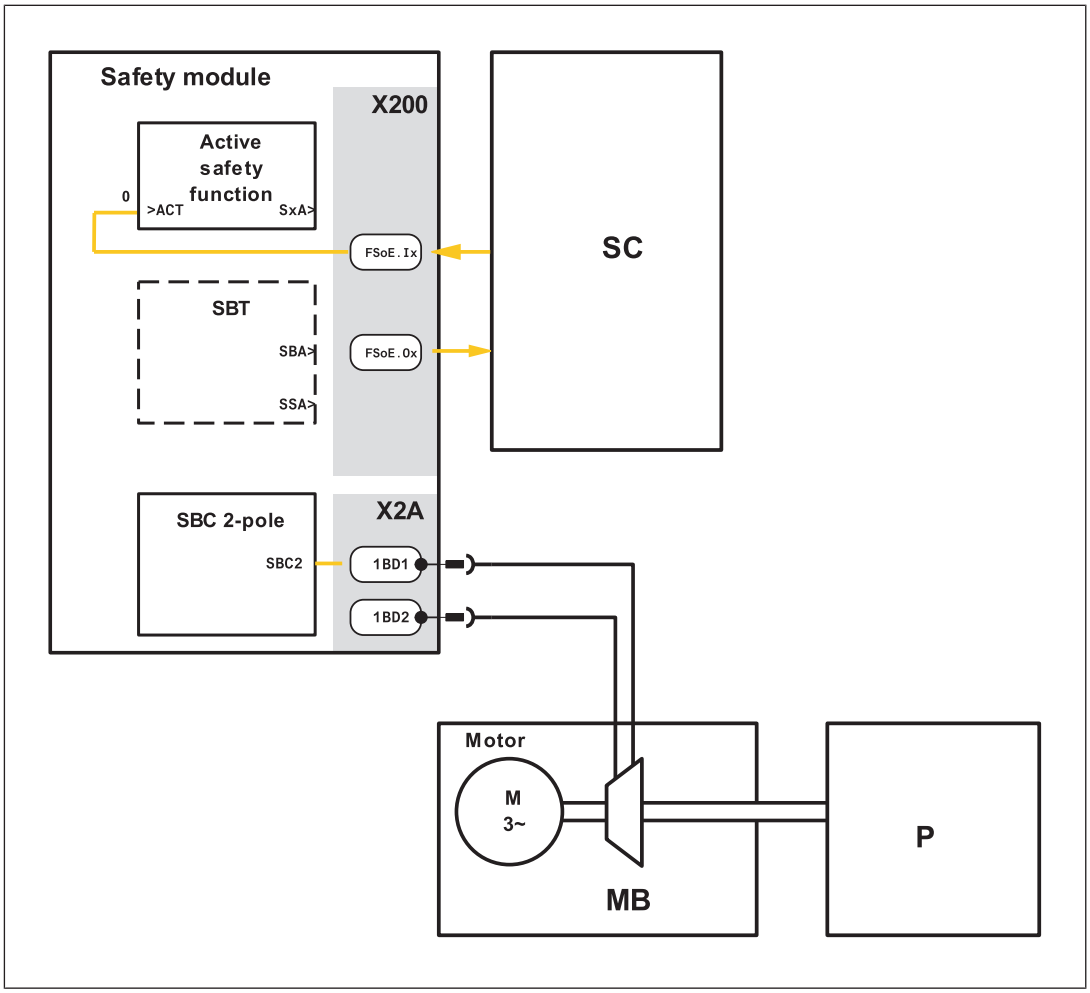


Fig.: "Load suspension" with a motor brake

Legend

SC	Safety controller (FSoE MainInstance)
MB	Quiescent current-activated, mechanical motor brake
P	Driven system (for example a gravity-loaded axis)
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	1	2
Active stop function or safety function for motion monitoring	Essential	Essential
SBC (safe brake control)	Essential	Essential
Feedback SBC release monitoring	Not required	Not required
SBT (safe brake test)	Not required	Essential

Max. category in accordance with EN ISO 13849-1	1	2
Categorisation of the brake as a well-tried component (Cat. 1)	Essential	Not required
Categorisation of the brake as a safety component	Not required	Not required

The following notes apply:

- A mechanical brake must be used to achieve Category 1 in accordance with EN ISO 13849-1. This must be categorised as a well-tried component.
- If Category 2 in accordance with EN ISO 13849-1 is to be achieved, the safety function SBT must be configured in the safety module and the brake must be tested.

5.11.4.4 "Load suspension" with an external safety brake (safety component)

Triggering of an external, quiescent current-activated, mechanical safety brake by the 2-pole SBC+/- output (X2A).

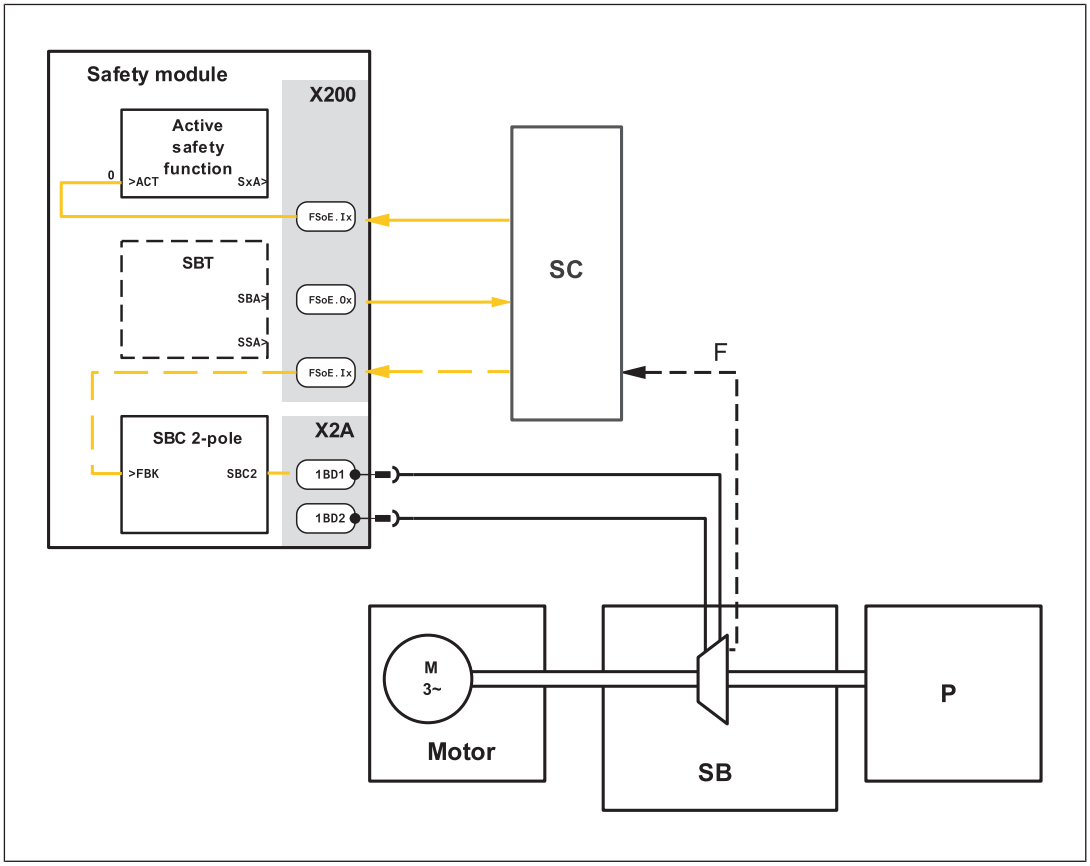


Fig.: "Load suspension" with an external safety brake (safety component)

Legend

SC	Safety controller (FSoE MainInstance)
F	Optional release monitoring
SB	External, quiescent current-operated, mechanical safety brake
- - -	Dotted line, optional
P	Driven system (for example a gravity-loaded axis)
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	4
Active stop function or safety function for motion monitoring	Essential
SBC (Safe Brake Control)	Essential
SBC ventilation monitoring feedback	optionally
SBT (Safe Brake Test)	optionally
Categorisation of the brake as a proven component (Cat. 1)	Not required

Max. category in accordance with EN ISO 13849-1	4
Categorisation of the brake as a safety component	Essential

The following notes apply:

- If a mechanical brake categorised as a safety component is used, a maximum of Category 4 in accordance with EN ISO 13849-1 can be achieved.
- The brake requirements in accordance with the installation instructions/ safety manual must be taken into account.
- Depending on the requirement, the safety function SBT and release monitoring may be used as an option.

5.11.4.5 "Load suspension" by triggering an external system

Triggering of an external safe device for load suspension and optional evaluation of feedback signals.

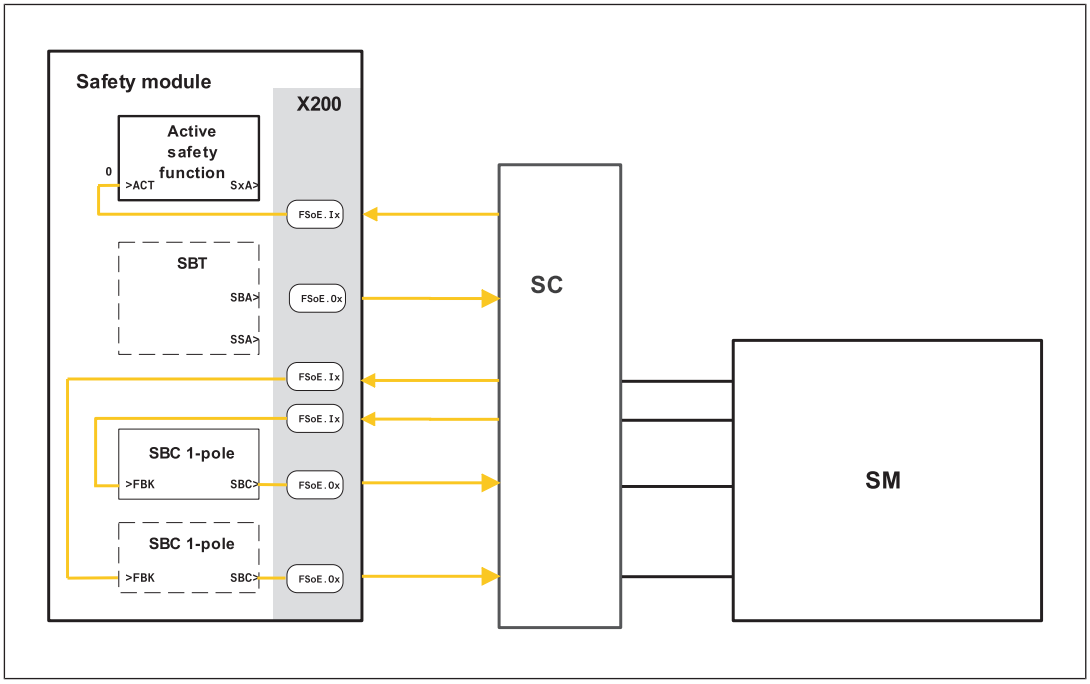


Fig.: "Load suspension" by triggering an external system

Legend

SC	Safety controller (FSoE MainInstance)
SM	Safe system for load suspension
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	4
Active stop function or safety function for motion monitoring	Essential
SBC (Safe Brake Control)	Essential
SBC ventilation monitoring feedback	optional
SBT (Safe Brake Test)	optional
Categorisation of the brake as a proven component (Cat. 1)	optional
Categorisation of the brake as a safety component	optional

The following notes apply:

- The safety module only generates trigger signals for activation of the "Load suspension" safety function.
- If necessary, feedback signals from the system can be evaluated by the safety module.
- Error monitoring of brakes, control and the driven system must be covered by the external system.

- The external system should be regarded as a separate, safety-related subsystem (SRP/CS in accordance with EN ISO 13849-1).
- The achievable category depends on the characteristics of the safe, external brake controls.

5.11.4.6 "Load suspension" with two brakes

Triggering a standby current-activated, mechanical motor brake and an external standby current-activated brake.

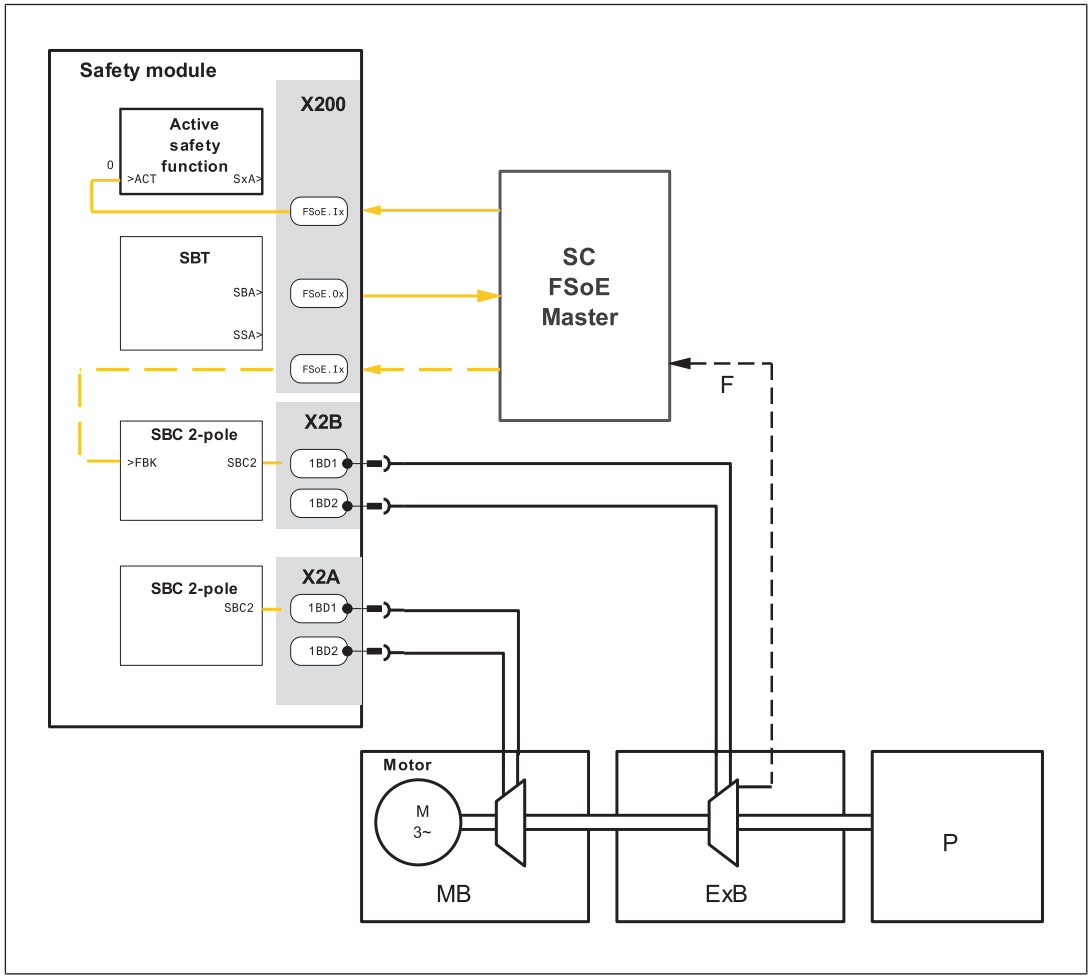


Fig.: "Load suspension" with two brakes

Legend

SC	Safety controller (FSoE MainInstance)
F	Optional release monitoring
- - -	Dotted line, optional
MB	Quiescent current-activated, mechanical motor brake
ExB	External, quiescent current-operated, mechanical brake
P	Driven system (for example a gravity-loaded axis)
Yellow line	Safe fieldbus connection

Max. category in accordance with EN ISO 13849-1	4
Active stop function or safety function for motion monitoring	Essential
SBC (Safe Brake Control)	Essential
SBC ventilation monitoring feedback	optionally
SBT (Safe Brake Test)	Essential
Categorisation of the brakes as a proven component (Cat. 1)	Not required
Categorisation of the brakes as a safety component	Not required

The following notes apply:

- When using two brakes in combination with the SBT safety function, a "Load suspension" up to Category 4 in accordance with EN ISO 13849-1 can be achieved.
- Brakes must meet the basic requirements of the application (momentum, temperature, environment, vibration, etc.).
- Brakes must be employed in accordance with the intended use as prescribed by the manufacturer.

5.11.5 Procedure when determining the safety integrity

The "Load suspension" safety function consists of several safety-related components. These components differ from application to application.

This operating manual contains the following information and help functions:

- Typical examples for implementation using a maximum achievable category
- Description of the safety functions of the safety module
- Safety characteristic values of the safety module
- Description of test functions for error detection

In addition, the following values must be determined for the mechanical brakes:

- $MTTF_D$ values
- Diagnostic coverage (DC)
  The safety module provides the following error detection functions:
  - Safe brake test (SBT)
  - Evaluation of feedback signals by the safety function SBC

5.12 Safety functions

Safety functions maintain a safe condition on a plant or prevent hazardous conditions arising on a plant.

Safety functions for electrical drives are defined in EN 61800-5-2.

Configuration of safety functions in the configuration tool

A maximum of 20 safety functions can be configured in the configuration tool, using function blocks. In addition, a safe stop 1 (SS1) safety function must be configured for each drive axis.

The safety function SS1 cannot be deactivated in the configurator.

The following function blocks for safety functions can only be used **once per drive axis**:

- Safe stop 1 (SS1) - a fixed component of the safety configuration -
- Safe brake test (SBT)

The following function blocks for safety functions can only be used **once per device**:

- Safe restart lock (SRL)
- Safe status output (SSO)

The possible combinations of the SBC safety function are described in the following section Combination options for SBC 1-pole and SBC 2-pole [📖 128].

The other function blocks for the safety functions can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of safety functions

- The safety functions are activated via the inputs on the FSoE interface.
- These inputs operate in accordance with the quiescent current principle. The safety controller activates the safety functions via a 0-signal (exception: the safety function SBT is activated via a 1-signal).

Feedback from the safety functions

- Message via outputs on the FSoE interface
  - 1-signal: if monitoring has been activated and is within the parametrised limit values
  - 0-signal: if monitoring has been deactivated or is outside the parametrised limit values

Simultaneous activation of safety functions

- All safety functions can be active at the same time. However, safety function SS1 has priority over all other safety functions on the affected drive axis.
- If SS1 is activated, the drive is stopped in accordance with its configuration.
- No other safety functions on the affected drive axis are processed or called up during this time.

Reaction to limit value violations on a drive axis

- When the parametrised limit values are exceeded, the SS1 safety function assigned to the drive axis is triggered with the emergency stop brake ramp and the feedback outputs on the safety functions are switched to a 0-signal.

- When parametrised limit values are exceeded during monitoring functions, only the feedback output of the safety function assigned to this drive axis is switched to a 0-signal. The drive axis remains in the axis state FSRUN.

Reaction to errors on the safety module

- In the event of internal errors on the safety module, the safety function SS1 is triggered with the emergency stop brake ramp on all drive axes.
- In the event of a serious (FATAL) error, an internal memory or data error for example, the safety function STO is activated directly on all drive axes. Torque or force generation in the motors is prevented. The safety module can only be restarted once it has been switched off and on again and can only continue to be operated if the error is not permanent.

For further information see Operating states SX6 [📖 165].

5.12.1 Permanent monitoring (optional)

Permanent monitoring means the motion and monitoring functions are permanently activated. When permanent monitoring of a safety function is configured, this is active after the safety module has booted (run-up). The safety module then automatically switches to the device and axis state FSRUN (safe operation). Activation or deactivation during runtime is not possible.

- The safety function is monitored without an activation signal, permanently without an on-delay.
- No activation is required.

INFORMATION

Permanent monitoring in conjunction with the control mode "wake and shake"

If the drive controller is operated in "wake and shake" control mode, the "permanent monitoring" option is not recommended.
During the commutation finding process using "wake and shake", the plausibility check of the motor encoder can be triggered if a safety function is permanently active.

Permanent monitoring can be configured for the following safety functions

Motion functions

- Safe Direction (SDI)
- Safely Limited Speed (SLS)
- Safe Speed Range (SSR)

Monitoring functions

- Safely Monitored Direction (SDI-M)
- Safely Monitored Speed (SLS-M)
- Safely Monitored Speed Range (SSR-M)

Configuration of permanent monitoring in the configuration tool

Field: Monitoring type			
Input field	**Valid entry**	**Unit**	**Description**
Monitoring type	Activation via input (default)	--	Activation via input
	Permanent	--	Activates permanent monitoring

INFORMATION

Hysteresis (optional)

If **"Permanent" monitoring type** has been selected in the configurator of a monitoring function, then it is mandatory to select the **"Hysteresis" monitoring behaviour** (see Hysteresis for monitoring functions).

The SET/RESET function (default) is then not possible.

5.12.2 Safe torque off, STO

The safety function STO prevents torque or force generation in the motor.

It is implemented for each drive axis via a safe shutdown path.

To prevent the motor running down in an uncontrolled manner, in normal operation the safety function STO is activated via the safety function SS1. The safety function STO forms part of the safety function SS1 and is also configured via this function. Through this connection, the safety function STO is permanently assigned to a drive axis (see Safe stop 1 (SS1) [81]).

- The safety function STO corresponds to the definition in accordance with EN 61800-5-2.
- The safety function STO corresponds to a category 0 stop (uncontrolled stop) in accordance with EN 60204-1.
- An emergency stop in accordance with EN ISO 13850 can be implemented with the safety function STO.
- The safety function STO can be used to remove power to prevent an unexpected start-up in accordance with ISO 14118.
- A safety stop in accordance with EN ISO 10218-1 can be implemented with the safety function STO.

STO shutdown paths

Two dual-channel STO shutdown paths are available in the safety module for safety-related applications (see Overview [22]).

When used as a dual axis controller, the safety function STO controls both STO shutdown paths separately.

Activation of the safety function STO

The safety function STO is activated on the assigned drive axis:

- In normal operation, through activation at the optional activation input STO_ACT of the safety function SS1, see Safe stop 1 (SS1) [81].
- In normal operation, when safety function SS1 is activated, once standstill has been detected or the monitoring time has elapsed.
- In the event of an error, as an error reaction of brake ramp monitoring on the safety function SS1.

When safety function STO is activated on an axis, the assigned drive axis switches to the axis state STO (see Axis state [169]).

The safety function STO is activated on all configured drive axes

- In the event of an error, as an error reaction when a global error occurs (see Error definition [26])
- In the event of an error, as an error reaction when a fatal error occurs

When the safety function STO has been activated on all axes, the safety module switches to the device state STO, see Device state [166].

Interaction with safe brake control (SBC)

If any external forces influence the motor axis (e.g. suspended loads), additional measures (e.g. quiescent current-activated brakes) are required. This is to avoid hazards when the safety function STO is active, see Application of the SBC and SBT safe brake functions [56]. The safety function SBC must be configured in the configuration tool for this purpose. If the safety function STO has been activated, the output is set to a 0-signal (brake is engaged). If the safety function STO is cancelled again, the output on the safety function SBC is activated in accordance with its configuration (configuration: connection to brake control signal from the drive controller active or inactive). When the release is enabled, the output is set to a 1-signal (brake is released).

NOTICE

For interaction between the safety function STO and the safe brake control SBC, the same axis assignment must be configured for safety functions SS1 and SBC.

For further information on the safety function SBC, see Safe Brake Control (SBC) [122].

Activation inputs and feedback outputs of the STO safety function

The activation inputs and feedback outputs of the STO safety function form part of the SS1 safety function and are described in the chapter Safe stop 1 (SS1) [81].

NOTICE

Device state STO

In the device states STO and STARTUP, a 0-signal is output at all feedback outputs of the configured safety functions.

Exceptions:

- Feedback outputs STO_ACK and SS1_ACK of the safety function SS1 report the active state STO with a 1-signal.
- Feedback output SBT_SBA of the safety function SBT remains set throughout the inspection period.
- Safe status output READY of the safety function SSO signals readiness for operation via a 1-signal.

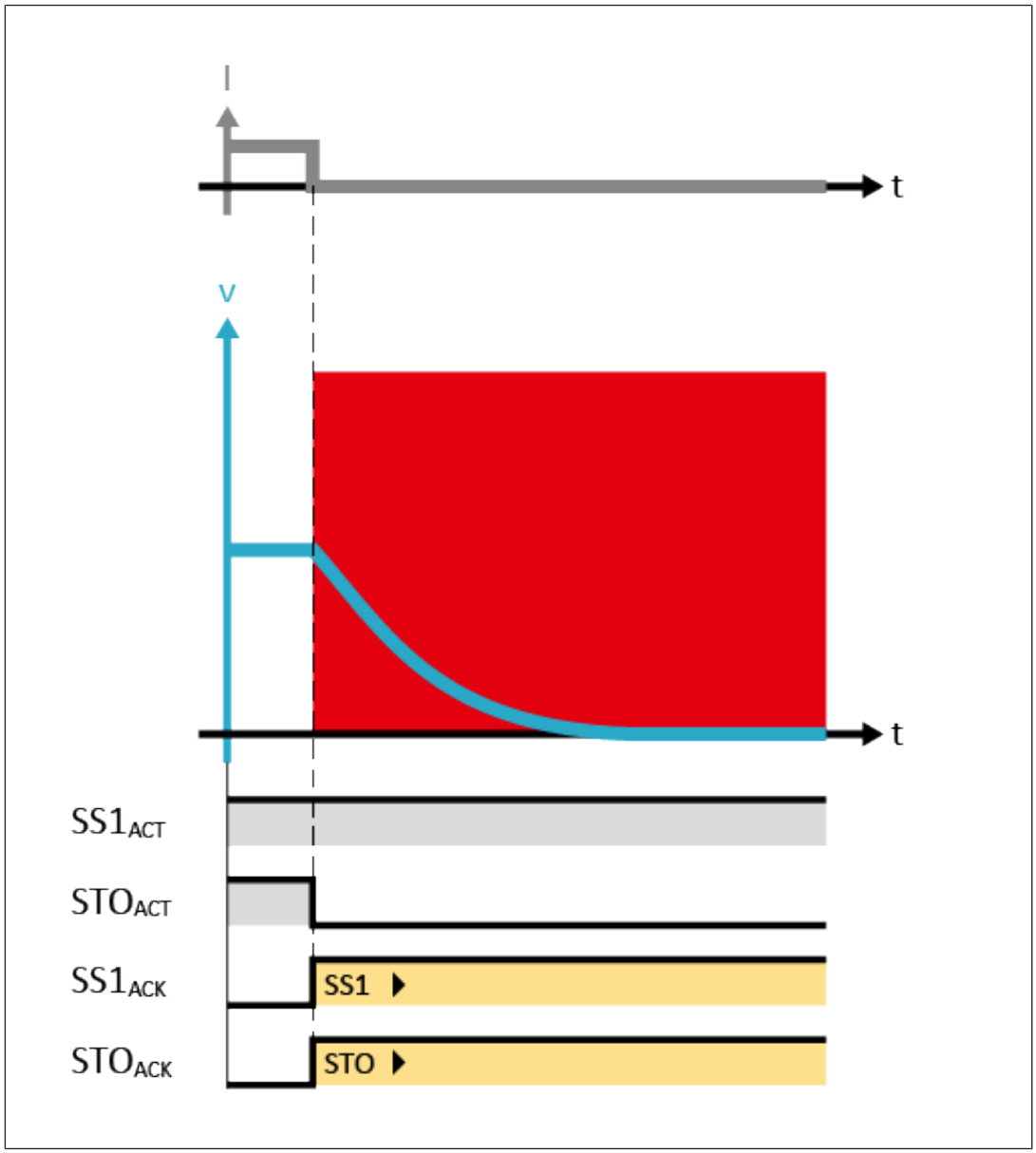


Fig.: Safety function STO

Legend

I	Current, torque/force generation
v	Speed
t	Time
$SS1_{ACT}$	Input for activation of the SS1 safety function
STO_{ACT}	Input for activation of the safety function STO Activation input STO_ACT (optional)
$SS1_{ACK}$	Output for feedback from safety function SS1
STO_{ACK}	Output for feedback from safety function STO

5.12.3 Safe stop 1 (SS1)

The safety function SS1 enables a controlled stop of the motor. The safety function STO is then performed and the motor is switched to torque-free/force-free.

- The safety function SS1 corresponds to the definition in accordance with EN 61800-5-2.
- The safety function SS1 corresponds to a category 1 stop, a controlled stop in accordance with EN 60204-1.
- The safety function SS1 is relevant for calculation of overrun in accordance with EN ISO 13855.
- A safety stop in accordance with EN ISO 10218-1 can be realised with the safety function SS1.

The safety function SS1 is permanently assigned to a drive axis. It must always be included in a configuration once per drive axis. It cannot be used multiple times per axis.

As an option, the assigned drive axis can be RESET via the inputs of the safety function SS1 (see "Resetting (RESET) the safety module").

Activation of safety function SS1

The safety function SS1 can be activated in a variety of ways:

- In normal operation, through activation at the activation input SS1_ACT
- In the event of an error, as a reaction when a limit value is violated by other safety functions
- In the event of an error, as a reaction to an internal error in the safety module

Stop motor in normal operation and in the event of an error

Both in normal operation and in the event of an error, the control of the braking ramp to stop the motor is either

- Drive-activated - by the drive controller, or
- Controller-activated – by a higher-level controller.

INFORMATION

If an error occurs due to brake ramp monitoring in "controller-activated" mode, control of the brake ramp is always "drive-activated".

Assignment of the drive axis to safety function SS1

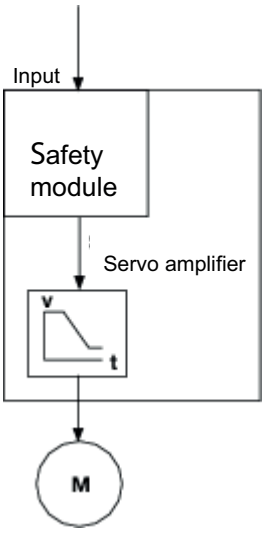
The safety function SS1 is permanently assigned to a drive axis.

Fixed configuration of the safety function SS1 in the configuration tool

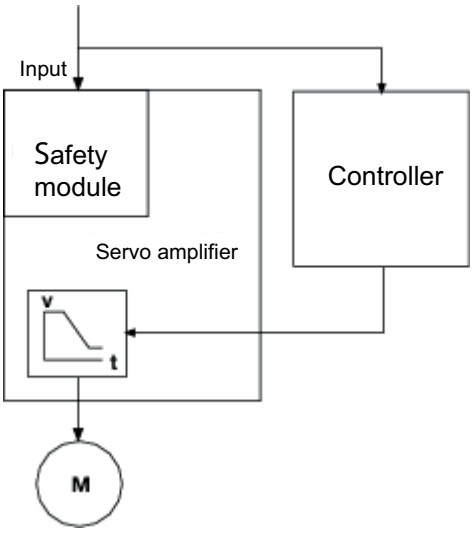
Field: Axis SS1			
Field	**Defined assignment**	**Unit**	**Description**
Axis	A1: Axis 1	--	Assignment to axis A
	or		
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SS1 in the configuration tool

Field: Braking ramp specification		
Input field	**Options**	**Description**
Specification Brake ramp	Controller	Control of the brake ramp controller-activated (external)
	Drive controller (Default)	Control of the brake ramp drive-activated (internal)



Drive-activated brake ramp



Controller-activated brake ramp

Drive-activated brake ramp

The safety module

- Transmits the brake ramp (normal operation or in event of error) to the Drive controller.
- Starts the braking process in the Drive controller.
- Monitors the braking process (optional).

Setpoints for a higher-level controller are ignored by the Drive controller while the safety function SS1 is active

NOTICE

Drive-activated brake ramp

With a drive-activated stop, axes lose their connection if the axes form an axis system via the controller.

Compensation movements of the motor may occur upon restarting.

Controller-activated brake ramp

The safety module

- provides the signal for starting the braking process of a higher-level controller via the fieldbus connection of the Drive controller.
- Monitors the braking process (optional).

Information on drive controller/control system fieldbus communication

See chapter Field bus communication [📖 178].

E-STOP brake ramp

If an error occurs, when a limit value is violated for example, the motor brakes in accordance with the E-STOP brake ramp.

Brake ramp monitoring

The safety function SS1 offers the option of identifying a hazardous movement at an early point by monitoring the brake ramp. By means of a target/actual comparison of the motor position curve during the braking process, an error reaction is initiated if a configurable "Deceleration window" is exceeded.

In the event of an error, the following options are available:

- For a drive-activated brake ramp, the safety function STO is triggered directly.
- For a controller-activated brake ramp, either the safety function STO or the E-STOP brake ramp (drive-activated) can be triggered directly.

Configuration of the safety function SS1 in the configuration tool

Field: Brake ramp monitoring (drive)			
Input field	**Valid entry**	**Unit**	**Description**
Brake ramp monitoring	Activate/deactivate (Default: deactivated)	---	Activation of brake ramp monitoring
Deceleration window Dec_win	0 … 2147483647 (Default: 0)	User-defined [Default: Increments]	Deceleration window based on the position of the brake ramp (Deceleration window)
Brake ramp	0 … 2147483647 (Default: 50000000)	User-defined [Default: Increments/s^2]	Brake ramp for normal operation
E-STOP brake ramp	0 … 2147483647 (Default: 50000000)	User-defined [Default: Increments/s^2]	E-STOP brake ramp

Configuration of the safety function SS1 in the configuration tool

Field: Brake ramp monitoring (controller)			
Input field	**Valid entry**	**Unit**	**Description**
Error reaction	STO direct	---	For controller-activated brake ramp, direct triggering of the safety function STO
	E-STOP	---	For controller-activated brake ramp, triggering of the E-STOP brake ramp (drive-activated)

INFORMATION

When braking ramp monitoring is activated, the valid input range of the braking ramp is reduced to 2 … 2147483647.

INFORMATION

The braking period depends on the speed of the motor when braking is started.

Activate STO

(see Safe torque off, STO)

The safety function STO can be activated in a variety of ways, on the assigned drive axis:

- After a configured maximum time has elapsed in normal operation
- After a configured E-STOP brake ramp time has elapsed in the event of an error
- After a configurable speed limit has been undercut (optional)
- Directly via the activation input STO_ACT (see Activation and feedback from safety functions [28])
- Directly via the FSoE Control Byte1, Bit 0 (see FSoE data exchange [40])

INFORMATION

The STO is activated at the very latest after the maximum time has elapsed, on the assigned drive axis.

Configuration of the safety function SS1 in the configuration tool

Field: Brake ramp times			
Input field	**Valid entry**	**Unit**	**Description**
E-STOP brake ramp time	0 … 120000 (Default: 50)	[ms]	Brake ramp time for E-STOP after an error leading to shutdown with STO.
Maximum time t_max	0 … 120000 (Default: 100)	[ms]	Maximum time for normal operation between activation of SS1 and shutdown with STO.

NOTICE

Please note that maximum times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

Automatic STO

Using the option "Automatic STO", the safety function STO can be activated before the configured maximum time has elapsed as follows:

- The motor speed must fall below a configured speed limit value.
- At a speed limit value of 0, the software controller enable is evaluated.
  This means that if the controller enable is withdrawn, the safety function STO is activated.

This option is active in both normal operation and in the event of an error.

Configuration of the safety function SS1 in the configuration tool

Field: Automatic STO			
Input field	**Valid entry**	**Unit**	**Description**
Speed limit value	Activate/deactivate (Default: deactivated)	--	Activation of the automatic STO.
Speed limit value v_lim	0 … 16777215 (Default: 340)	User-defined [Default: Increments/s]	If the speed falls below the speed limit value, the safety function STO is triggered.

Activation and feedback

For activation and feedback of the safety function SS1, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

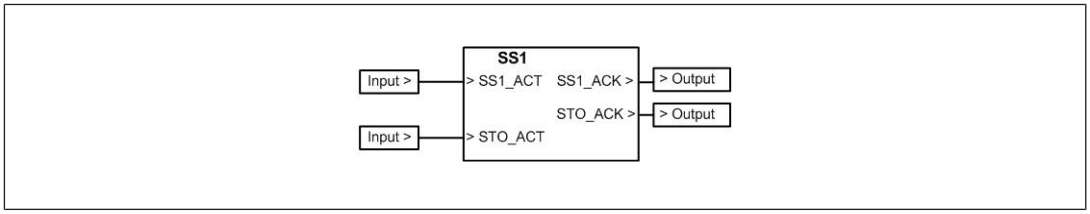


Fig.: Safety function SS1

Legend

SS1_ACT	The safety function SS1 is activated or deactivated via the activation input SS1_ACT. (0-signal activated, 1-signal deactivated)
STO_ACT	The safety function STO is activated or deactivated via the activation input STO_ACT. (0-signal activated, 1-signal deactivated)
SS1_ACK	The feedback output SS1_ACK reports whether the safety function SS1 is activated or deactivated. (1-signal activated, 0-signal deactivated)
STO_ACK	The feedback output STO_ACK reports whether the safety function STO is activated or deactivated. (1-signal activated, 0-signal deactivated)

Activation input STO_ACT (optional)

- The safety function STO is activated directly via the activation input STO_ACT (0-signal activated, 1-signal deactivated)

The activation input STO_ACT may be necessary for the following reasons:

- Direct triggering of the safety function STO by a higher-level controller.

Configuration of the safety function SS1 in the configuration tool

Field: Additional inputs/outputs			
Input field	**Valid entry**	**Unit**	**Description**
STO ACT	Activate/deactivate (default: deactivated)	--	Use of activation input for STO

NOTICE

The safety function SS1 is a fixed component of the safety configuration.
When the safety function SS1 is activated (drive-activated), one axis loses its connection to other axes in an axis system.
The safety function SS1 is available just once per drive axis in each safety configuration.

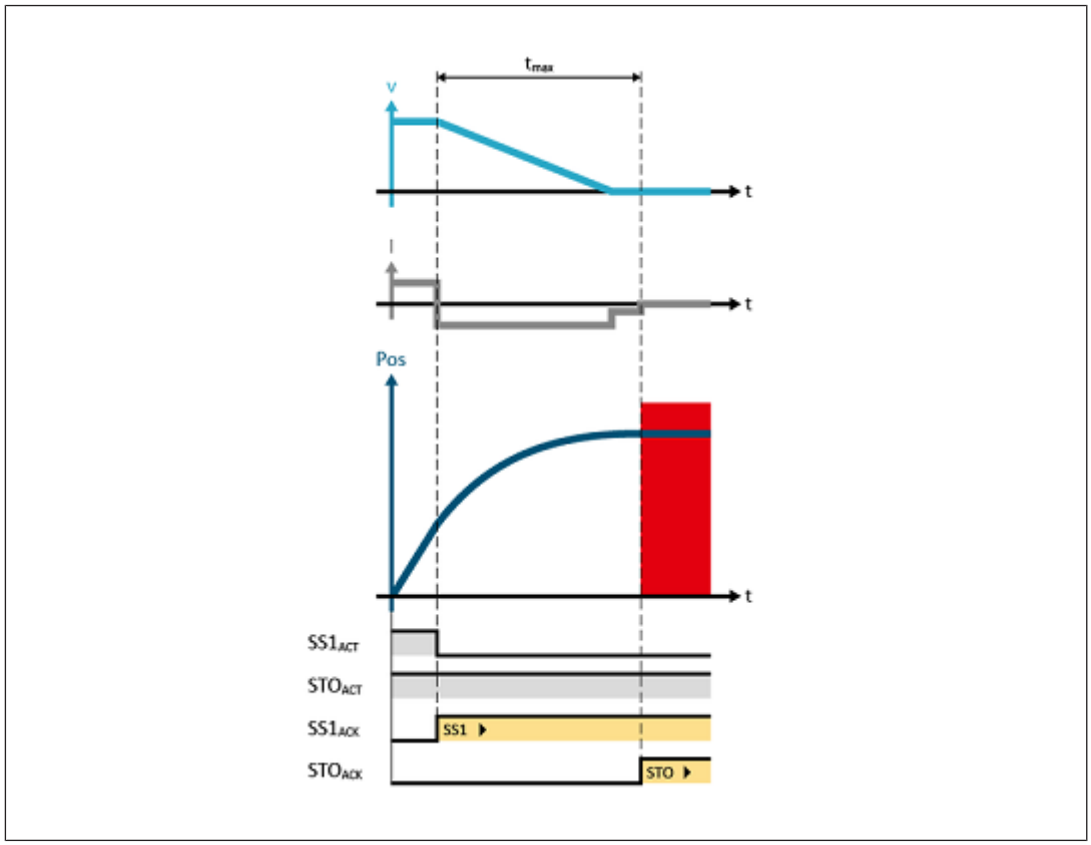


Fig.: Safety function SS1

Legend

t_{max}	Maximum time of the brake ramp
v	Speed
t	Time
I	Current
Pos	Position
$SS1_{ACT}$	Input for safety function SS1
STO_{ACT}	Input for safety function STO
$SS1_{ACK}$	Output for feedback from safety function SS1
STO_{ACK}	Output for feedback from safety function STO

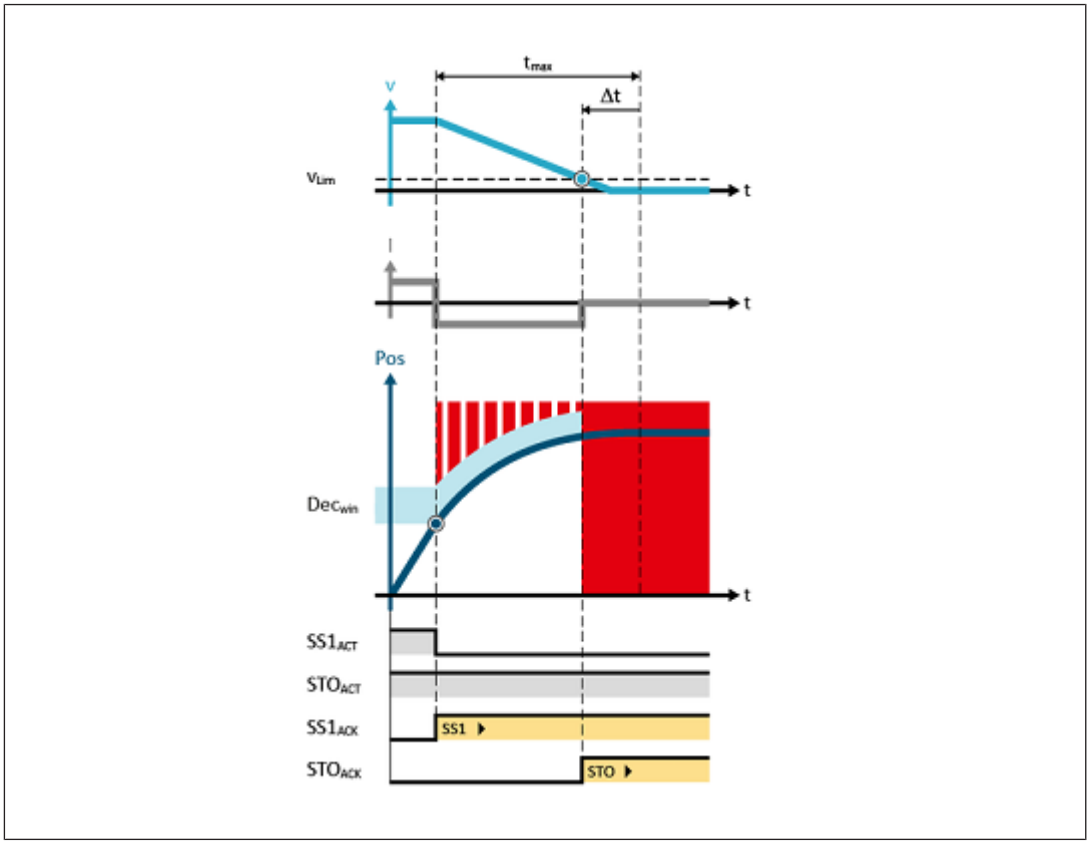


Fig.: Safety function SS1 and brake ramp monitoring

Legend

t_{max}	Maximum time of the brake ramp
v	Speed
t	Time
Δt	Variable time, resulting from the entry of v_{lim}
V_{lim}	Speed limit value
I	Current
Pos	Position
Dec_{win}	Deceleration window
$SS1_{ACT}$	Input for safety function SS1
STO_{ACT}	Input for safety function STO
$SS1_{ACK}$	Output for feedback from safety function SS1
STO_{ACK}	Output for feedback from safety function STO

5.12.4 Safe Stop 2 (SS2)

The safety function SS2 enables a controlled stop of the motor. The motor is then monitored for a safe standstill (SOS).

- The safety function SS2 corresponds to the definition in accordance with EN 61800-5-2.
- The safety function SS2 corresponds to a category 2 stop, a controlled stop in accordance with EN 60204-1.
- The safety function SS2 is relevant for calculation of overrun in accordance with EN ISO 13855.
- A safety stop in accordance with EN ISO 10218-1 can be realised with the safety function SS2.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

NOTICE

Avoid activating several safety functions SS2 with differently configured brake ramps simultaneously on one axis. In this case it is not clearly defined which SS2 brake ramp is executed.

Activation of safety function SS2

The safety function SS2 can be activated in the following way:

- Though activation at the activation input ACT.

Stop motor

Control of the brake ramp to stop the motor is either:

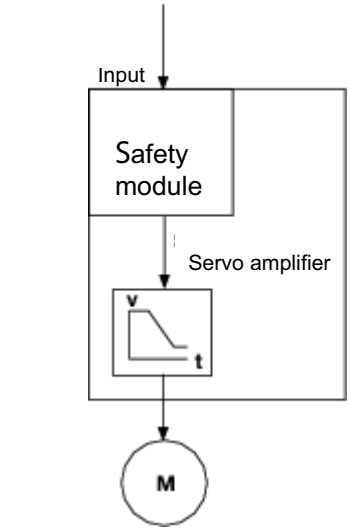
- Drive-activated - by Drive controller, or
- Controller-activated – by a higher-level controller.

Configuration of the safety function SS2 in the configuration tool

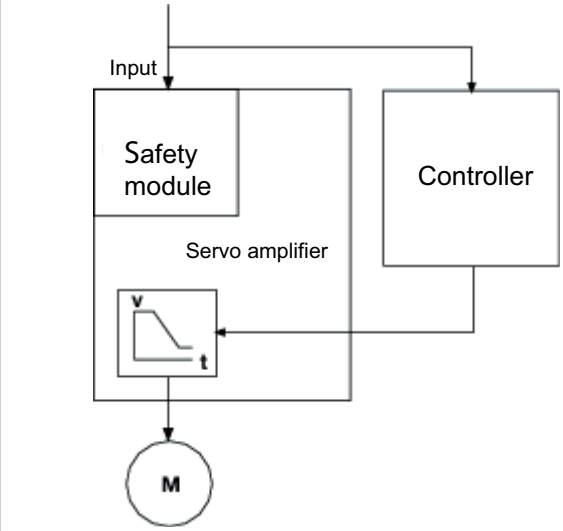
Field: Axis			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SS2 in the configuration tool

Field: Brake ramp specification		
Input field	**Options**	**Description**
Specification Brake ramp	Controller	Control of the brake ramp controller-activated (external)
	Drive controller (default)	Control of the brake ramp drive-activated (internal)



Drive-activated brake ramp



Controller-activated brake ramp

Drive-activated brake ramp

The safety module

- Transmits the brake ramp (normal operation) to the Drive controller.
- Starts the braking process in the Drive controller.
- Monitors the braking process (optional).

Setpoints for a higher-level controller are ignored by the Drive controller while the safety function SS2 is active

NOTICE

Drive-activated brake ramp

With a drive-activated stop, axes lose their connection if the axes form an axis system via the controller.

Compensation movements of the motor may occur upon restarting.

Controller-activated brake ramp

The safety module

- provides the signal for starting the braking process of a higher-level controller via the fieldbus connection of the Drive controller.
- monitors the braking process (optional).

Information on drive controller/control system fieldbus communication

See chapter Field bus communication.

Brake ramp in event of an error

The safety function SS1 is activated in the event of an error, when a limit value is violated for example.

Brake ramp monitoring

The safety function SS2 offers the option of identifying a hazardous movement at an early stage by monitoring the brake ramp. By means of a target/actual comparison of the motor position curve during the braking process, an error reaction is triggered if a configurable "Deceleration window" is exceeded.

Configuration of the safety function SS2 in the configuration tool

Field: Brake ramp monitoring			
Input field	**Valid entry**	**Unit**	**Description**
Brake ramp monitoring	Activate/deactivate (Default: deactivated)	--	Activation of brake ramp monitoring
Deceleration window Dec_win	0 … 2147483647 (Default: 0)	User-defined [Default: Increments]	Deceleration window based on the position of the brake ramp (Deceleration window)
Brake ramp	0 … 2147483647 (Default: 10000000)	User-defined [Default: Increments/s^2]	Brake ramp for normal operation
Maximum time t_max	0 … 120000 (Default: 100)	[ms]	Maximum time for normal operation between activation of SS2 and monitored standstill with SOS.

INFORMATION

When braking ramp monitoring is activated, the valid input range of the braking ramp is reduced to 2 … 2147483647.

INFORMATION

The braking period depends on the speed of the motor when braking is started.

NOTICE

Please note that maximum times that are not a multiple of the processor system's cycle time (see Technical details [📖 179]) will not elapse until the following system cycle.

Activate SOS

The safety function SOS can be activated in a variety of ways:

- After the configured maximum time has elapsed
- If a set speed limit has been undercut (optional)

INFORMATION

The SOS is activated at the very latest after the configured maximum time has elapsed.

Monitoring with safety function SOS

- The actual position of the motor is continuously compared with the set standstill position window. The feedback output SSA becomes active when monitoring is started (see diagram). If it is seen to be exceeded, an error reaction is triggered.

Configuration of the safety function SS2 in the configuration tool

Field: Standstill position window			
Input field	**Valid entry**	**Unit**	**Description**
Tolerance (Tol)	0 … 2147483647 (Default: 100)	USER-DEFINED [Default: Increments]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Automatic SOS (optional)

With automatic SOS, the safety function SOS is activated before the configured maximum time has elapsed. For this to occur, the motor speed must fall below a configurable speed limit value.

Configuration of the safety function SS2 in the configuration tool

Field: Automatic SOS			
Input field	**Valid entry**	**Unit**	**Description**
Speed limit value	Activate/deactivate (Default: deactivated)	--	Activation of automatic SOS.
Speed limit value v_lim	0 … 16777215 (Default: 340)	User-defined [Default: Increments/s]	If the speed falls below the speed limit value, the safety function SOS is triggered.

Error reaction with activated SOS

If a limit value violation is identified during standstill monitoring, the safety function SS1 is triggered as a reaction.

Activation and feedback

For activation and feedback of the safety function SS2, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

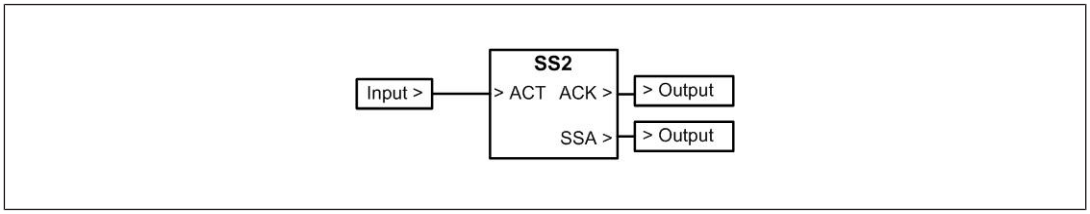


Fig.: Safety function SS2

Legend

ACT	The safety function SS2 is activated or deactivated via the activation input ACT. (0 signal activated, 1 signal deactivated)
ACK	The feedback output ACK reports whether the safety function SS2 is activated or deactivated. (1 signal activated, 0 signal deactivated)
SSA	Safe Standstill Acknowledge The feedback output SSA reports whether the motor is at a standstill (1 signal), or whether there is a limit value violation (0 signal). If the safety function SS2 is not activated, the feedback output likewise reports a 0 signal.

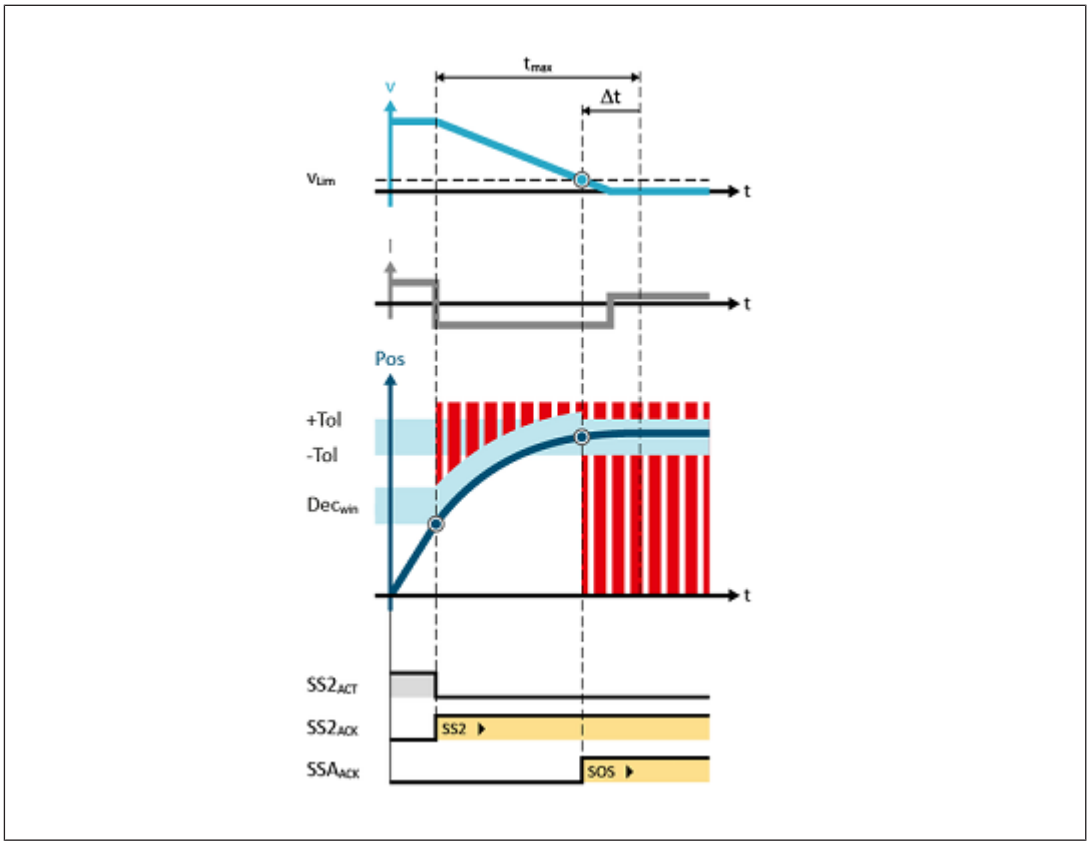


Fig.: Safety function SS2 with brake ramp monitoring

Legend

t_{max}	Maximum time of the brake ramp
v	Speed
Δt	Variable time, resulting from the entry of v_{lim}

V_{lim}	Speed limit value
I	Current
Pos	Position
+/-Tol	Standstill tolerance window +/-
Dec_{win}	Deceleration window
$SS2_{ACT}$	Input for safety function SS2
$SS2_{ACK}$	Output for feedback from safety function SS2
SSA_{ACK}	Safe standstill acknowledge Output for feedback from limit value monitoring

5.12.5 Safe Direction (SDI) and Safely Monitored Direction (SDI-M)

INFORMATION

The **monitoring function SDI-M "safely monitored direction"** can be selected as a variant of the normative safety function SDI "safe direction".
The monitoring function SDI-M corresponds to the normative safety function SDI, with the exception of the error reaction.
When parametrised limit values are exceeded:

- No SS1 is activated on the assigned drive axis
- A 0-signal is issued at the output SDA (safe direction acknowledge)

For further information see Hysteresis for monitoring functions [📖 150]

The safety function SDI monitors whether the motor's motion complies with a defined direction. To monitor the positive and negative direction, the SDI function must be used twice.

- The safety function SDI corresponds to the definition in accordance with EN 61800-5-2.
- Safe axial and spatial boundaries in accordance with EN ISO 10218-1 can be realised with the safety function SDI.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of safety function SDI

The safety function SDI can be activated in the following way:

- Activation via input
- Permanent, see Permanent monitoring (optional)
  - The direction of movement is monitored without an activation signal, permanently, without an SDI on-delay.
  - No activation is required.

Start of monitoring

- After SDI on-delay has elapsed

Configuration of the safety function SDI in the configuration tool

Field: Axis			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SDI in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 20)	[ms]	Time between activation of the safety function SDI and the point at which monitoring begins

NOTICE

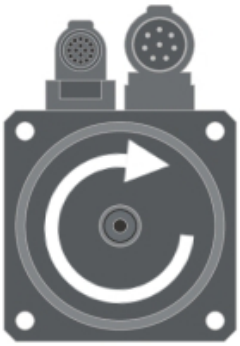
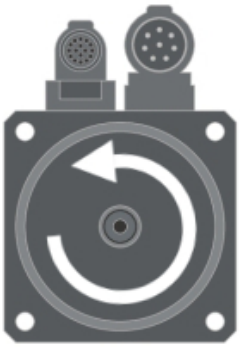
Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [📖 179]) will not elapse until the following system cycle.

Monitoring

- The motor's direction of movement is continuously compared with the parametrised, permitted direction (positive or negative).
- An application-specific position window prevents a limit value violation caused by minimal movements around the standstill position.
- The position window is drawn behind the actual position provided the motor is turning in the permitted direction.
- If there is a movement in the non-permitted direction that exceeds the distance set in the position window, the error reaction is triggered.
- The feedback output SDA is active (see diagram).

Configuration of the safety function SDI in the configuration tool

Field: Permitted direction of movement			
Input field	**Valid entry**	**Unit**	**Description**
Safely monitored direction	Negative (default)	--	Determination of permitted direction
	Positive	--	

Information clockwise/anti-clockwise	
	**Clockwise** ⇨ positive direction The shaft rotates clockwise looking at the drive end.
	**Anti-clockwise** ⇨ negative direction The shaft rotates anti-clockwise looking at the drive end.

Configuration of the safety function SDI in the configuration tool

Field: Standstill position window			
Input field	**Valid entry**	**Unit**	**Description**
Position window Standstill Tol_win	0 … 2147483647 (Default: 100)	User-defined [Default: increments]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

SDI error reaction

- If the limit value is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SDA feedback output.

SDI-M error reaction

- A 0 signal is issued at the feedback output SDA if the limit value is exceeded.

Activation and feedback

For activation and feedback of the safety function SDI, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

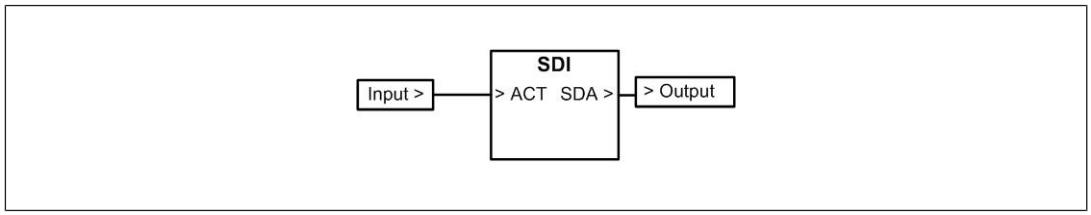


Fig.: Function block SDI

Legend

ACT	The safety function SDI is activated or deactivated via the activation input ACT. (0 signal activated, 1 signal deactivated)
SDA	Safe Direction Acknowledge The feedback output SDA reports whether the motor is within its permitted limit values (1 signal), or whether there is a limit value violation (0 signal). If the safety function is not activated, the feedback output likewise reports a 0 signal.

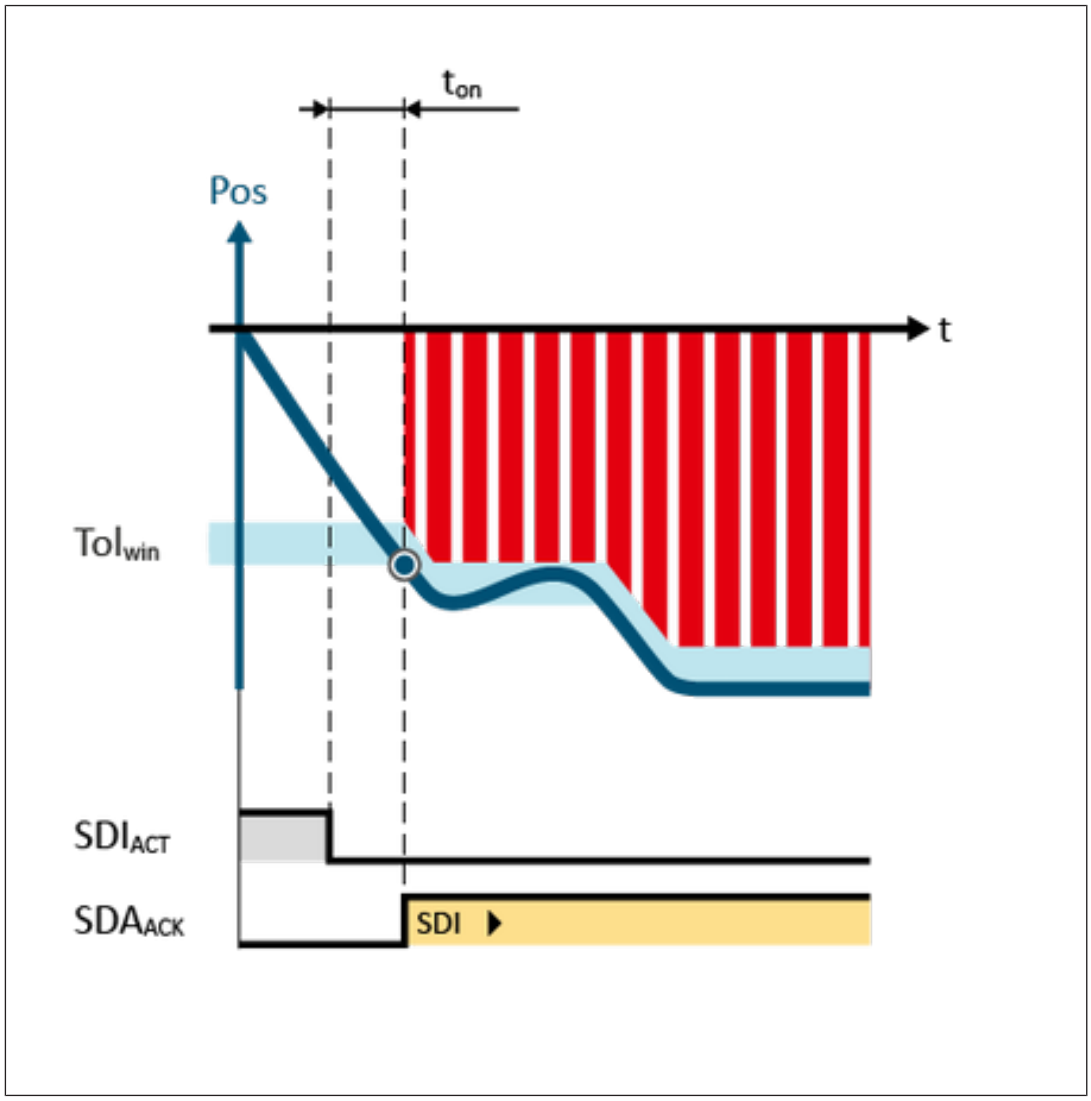


Fig.: Safety function SDI, permitted direction of movement negative

Legend

t_{on}	On-delay
Pos	Position
Tol_{win}	Standstill position window
SDI_{ACT}	Input for safety function SDI
SDA_{ACK}	Safe direction acknowledge
	Output for feedback from safety function SDI

Hysteresis for monitoring functions

A hysteresis can be configured with monitoring functions, as an option; see Hysteresis for monitoring functions [📖 150].

5.12.6 Safely Limited Increment (SLI) and Safely Monitored Increment (SLI-M)

INFORMATION

The **monitoring function SLI-M "safely monitored increment"** can be selected as a variant of the normative safety function SLI "safely limited increment".
The monitoring function SLI-M corresponds to the normative safety function SLI, except for the error reaction.
When parametrised limit values are exceeded:

- No SS1 is activated on the assigned drive axis
- A 0-signal is issued at the output SRA (safe range acknowledge)

For further information see Hysteresis for monitoring functions [📖 150]

The safety function SLI monitors whether the motor's motion complies with a defined increment. After activation, the motor may only move within the permitted parameterised position range.

- The safety function SLI corresponds to the definition in accordance with EN 61800-5-2.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of safety function SLI

The safety function SLI can be activated in the following way:

- Though activation at the activation input ACT

Start of monitoring

- After SLI on-delay has elapsed

Configuration of the safety function SLI in the configuration tool

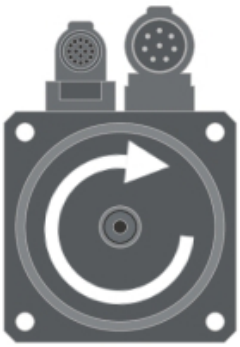
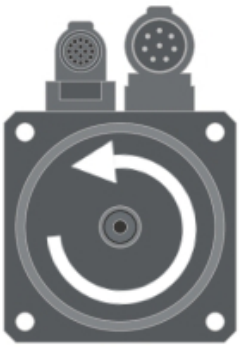
Field: Axis			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SLI in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 20)	[ms]	Time between activation of the safety function SLI and the point at which monitoring begins

NOTICE

Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

Information clockwise/anti-clockwise	
	**Clockwise** ⇨ positive direction The shaft rotates clockwise looking at the drive end.
	**Anti-clockwise** ⇨ negative direction The shaft rotates anti-clockwise looking at the drive end.

Monitoring

- The position when monitoring starts is considered the reference position.

- The current motor position is continuously compared with the parametrised position limit values.
  If it is seen to be exceeded, an error reaction is triggered.
- The feedback output SRA is active (see diagram).

Configuration of the safety function SLI in the configuration tool

Field: Position limit values			
Input field	**Valid entry**	**Unit**	**Description**
Max. position Pos_max	0 …… 2147483647 (Default: 0)	User-defined [Default: Increments]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.
Min. position Pos_min	0 … 2147483647 (Default: 0)	User-defined [Default: Increments]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Error reaction SLI

- If a limit value is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SRA feedback output.

Error reaction SLI-M

- A 0-signal is issued at the feedback output SRA if a limit value is exceeded.

Activation and feedback

For activation and feedback of the safety function SLI, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

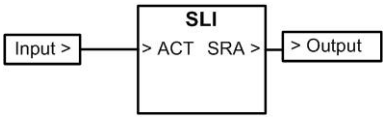


Fig.: Function block SLI

Legend

ACT	The safety function SLI is activated or deactivated via the activation input ACT (0-signal activated, 1-signal deactivated).
SRA	Safe range acknowledge The feedback output SRA reports whether the motor is within its permitted limit values (1-signal), or whether there is a limit value violation (0-signal). If the safety function is not activated, the feedback output likewise reports a 0-signal.

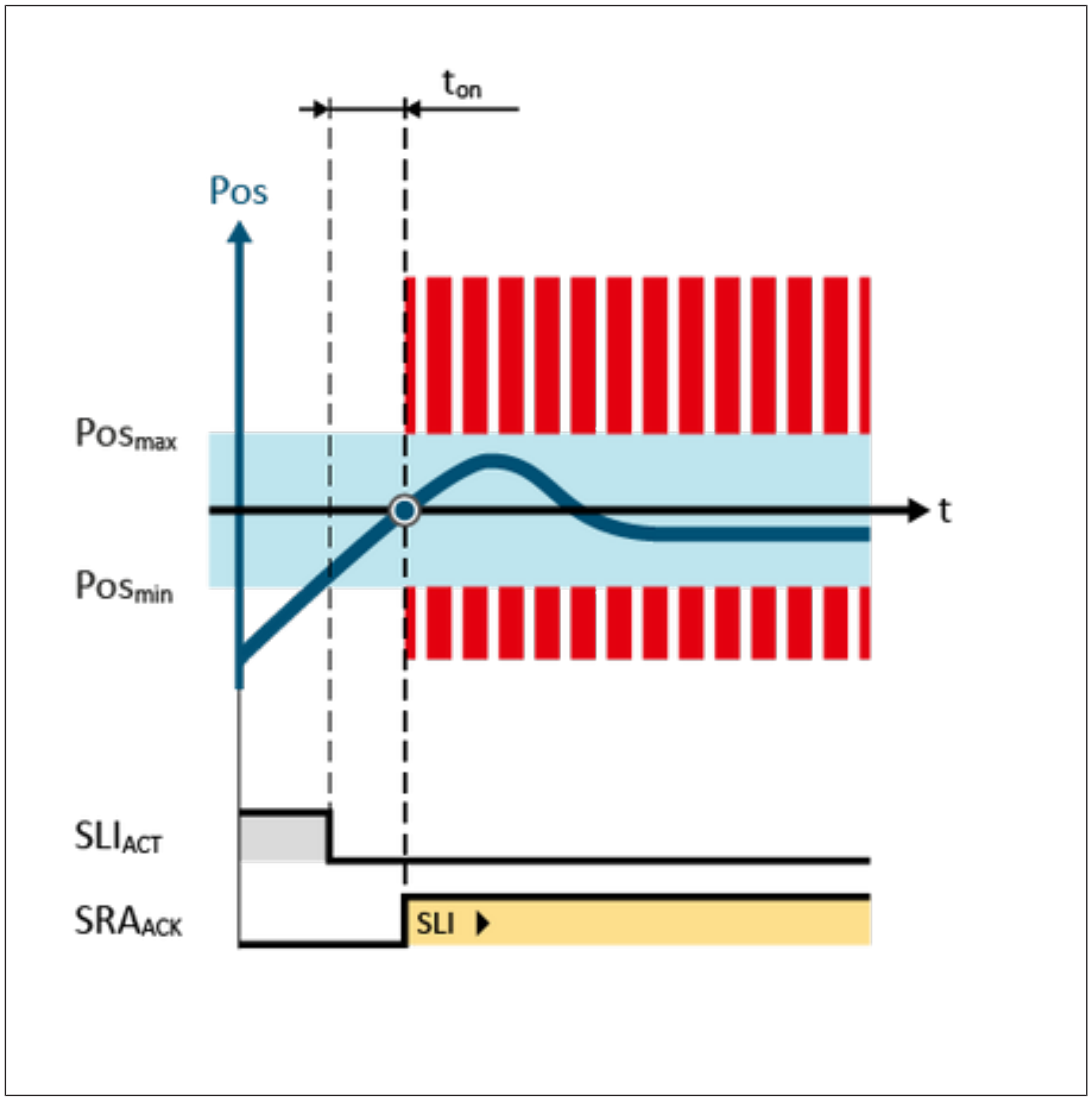


Fig.: Safety function SLI

Legend

t_{on}	On-delay
Pos	Position
Pos_{max}	Maximum position limit value
Pos_{min}	Minimum position limit value
SLI_{ACT}	Input for safety function SLI
SRA_{ACK}	Safe range acknowledge
	Output for feedback from safety function SLI

Hysteresis for monitoring functions

A hysteresis can be configured with monitoring functions, as an option; see Hysteresis for monitoring functions [📖 150].

5.12.7 Safely Limited Speed (SLS) and Safely Monitored Speed (SLS-M)

INFORMATION

The **monitoring function SLS-M "Safely monitored speed"** can be selected as a variant of the normative safety function SLS "Safely limited speed". The monitoring function SLS-M corresponds to the normative safety function SLS, except for the error reaction.
When parametrised limit values are exceeded:

- No SS1 is activated on the assigned drive axis
- A 0-signal is issued at the output SRA (safe range acknowledge)

For further information see Hysteresis for monitoring functions [📖 150]

The SLS safety function prevents the motor from exceeding the specified speed limit.

- The safety function SLS corresponds to the definition in accordance with EN 61800-5-2.
- The safety function SLS makes it possible to realise a safety-rated reduced speed and a safety-rated monitored speed in accordance with EN ISO 10218-1.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of safety function SLS

The safety function SLS can be activated in the following way:

- Activation via input
- Permanent, see Permanent monitoring (optional)
  - The speed is monitored without an activation signal, permanently, without an SLS on-delay.
  - No activation is required.

Start of monitoring

- After SLS on-delay has elapsed

Configuration of the safety function SLS in the configuration tool

Field: Axis SLS			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SLS in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 20)	[ms]	Time between activation of the safety function SLS and the point at which monitoring begins.

NOTICE

Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

Monitoring

- The actual speed of the motor is continuously compared with the set speed limit value.
- If it is seen to be exceeded, an error reaction is triggered.
- The feedback output is active (see diagram).

Configuration of the safety function SLS in the configuration tool

Field: Speed limit value			
Input field	**Valid entry**	**Unit**	**Description**
Speed limit value v_lim	0 … 16777215 (Default: 100000)	User-defined [Default: increments/s]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Error reaction SLS

- If the limit value is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SRA feedback output.

Error reaction SLS-M

- A 0-signal is issued at the feedback output SRA if the limit value is exceeded.

Activation and feedback

For activation and feedback of the safety function SLS, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

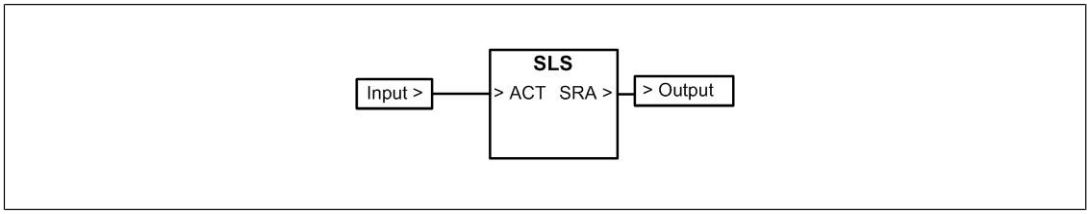


Fig.: Function block SLS

Legend

ACT	The safety function SLS is activated or deactivated via the activation input ACT (0-signal activated, 1-signal deactivated).
SRA	Safe range acknowledge The feedback output SRA reports whether the motor is within its permitted limit values (1-signal), or whether there is a limit value violation (0-signal). If the safety function is not activated, the feedback output likewise reports a 0-signal.

Parametrise the tolerance range (optional)

A tolerance range may also be set for the limit values used to monitor the speed. This tolerance range modifies the set limit values. As a result, one-off or periodic overshoots that exceed the limit values can be tolerated.

The following values can be parametrised for the tolerance range

- Tolerance window, which takes into account the amplitude of the overshoots.
- Tolerance time, which takes into account the width of the overshoots.
- Tolerance period, which takes into account the oscillation period.

Activation of the tolerance range

- If the speed limit value is exceeded, the tolerance range becomes active (see diagram "Safety function SLS with activated tolerance range").

Tolerance range error reaction

- If the tolerance range is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SRA feedback output.

Configuration of tolerance range in the configuration tool (optional)

Field: Tolerance monitoring			
Input field	**Valid entry**	**Unit**	**Description**
Tolerance	Activate/deactivate (Default: deactivated)	--	Activates the tolerance range
Tolerance window Tol_win	1 … 25 (Default: 1)	[%]	Permitted amplitude of the overshoots
Tolerance time t1	1 … 120000 (Default: 100)	[ms]	Permitted width of the overshoots
Tolerance period t2	2 … 120000 (Default: 1000)	[ms]	Permitted period of oscillation

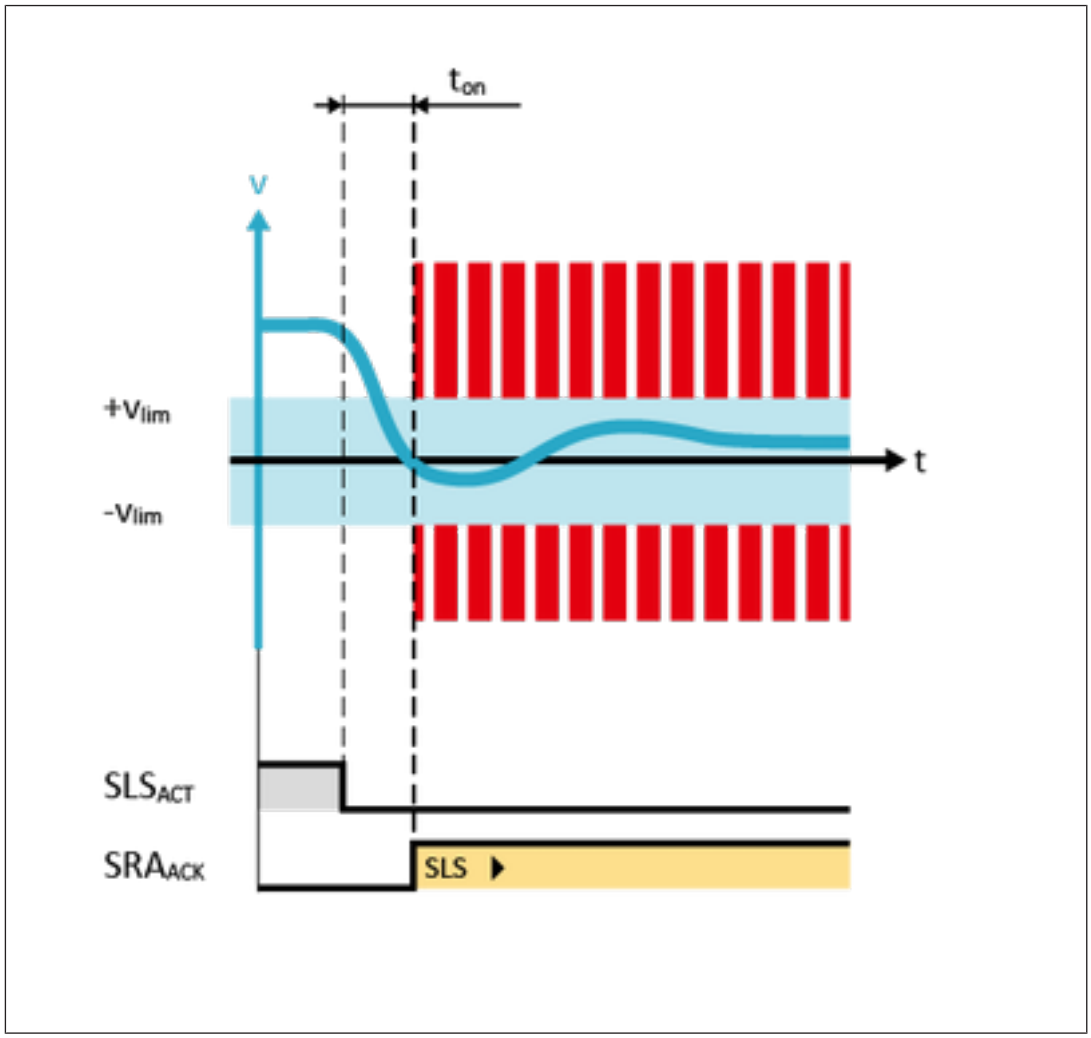


Fig.: Safety function SLS without tolerance range activated

Legend

t_{on}	On-delay
v	Speed
$+/-v_{lim}$	Speed limit value +/-
SLS_{ACT}	Input for safety function SLS
SRA_{ACK}	Safe range acknowledge
	Output for feedback from safety function SLS

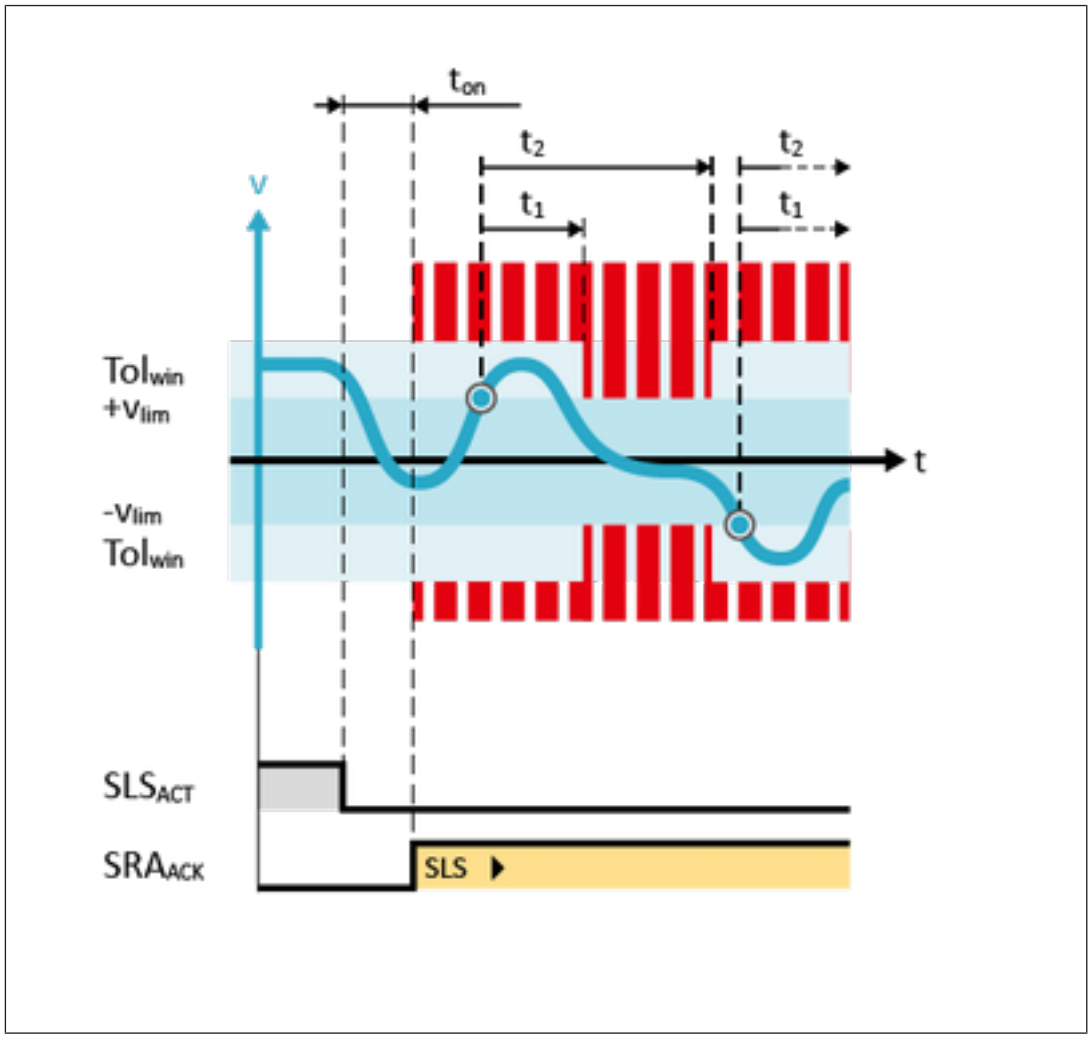


Fig.: Safety function SLS with tolerance range activated

Legend

ton	On-delay
t_2	Tolerance period
v	Speed limit value
t_1	Tolerance time
Tol_{win}	Tolerance window
$+/-v_{lim}$	Speed limit value +/-
SLS_{ACT}	Input for safety function SLS
SRA_{ACK}	Safe range acknowledge
	Output for feedback from safety function SLS

Hysteresis for monitoring functions

A hysteresis can be configured with monitoring functions, as an option; see Hysteresis for monitoring functions [📖 150].

5.12.8 Safe Operating Stop (SOS) and Safely Monitored Operating Stop (SOS-M)

INFORMATION

The **monitoring function SOS-M "safely monitored operating stop"** can be selected as a variant to the normative safety function SOS "safe operating stop".
The monitoring function SOS-M corresponds to the normative safety function SOS, except for the error reaction.
When parametrised limit values are exceeded:

- No SS1 is activated on the assigned drive axis
- A 0-signal is issued at the SSA (safe standstill acknowledge) output

For further information see Hysteresis for monitoring functions [📖 150]

The safety function SOS monitors whether the motor's motion complies with the standstill position.

- The safety function SOS corresponds to the definition in accordance with EN 61800-5-2.
- A safety-rated monitored stop in accordance with EN ISO 10218-1 can be realised with the safety function SOS.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of safety function SOS

The safety function SOS can be activated in the following way:

- Though activation at the activation input ACT

Start of monitoring

- After SOS on-delay has elapsed
- If a set speed limit has been undercut (optional)

Configuration of the safety function SOS in the configuration tool

Field: Axis SOS			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SOS in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 100)	[ms]	Time between activation of the safety function SOS and the point at which monitoring begins

NOTICE

Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

Monitoring

- The position when monitoring starts is considered the reference position.
- The actual position of the motor is continuously compared with the set standstill position window. If it is seen to be exceeded, an error reaction is triggered.
- The feedback output is active (see diagram).

Configuration of the safety function SOS in the configuration tool

Field: Standstill position window			
Input field	**Valid entry**	**Unit**	**Description**
Tolerance (Tol) Tol_win	0 … 2147483647 (Default: 100)	USER-DEFINED [Default: Increments]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Error reaction SOS

- If a limit value is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0 signal is issued at the SSA feedback output.

Error reaction SOS-M

- A 0 signal is issued at the feedback output SSA if a limit value is exceeded.

Automatic SOS (optional)

With automatic SOS, the safety function SOS is activated before the on-delay has elapsed. For this to occur, the motor speed must fall below a configurable standstill limit value.

INFORMATION

The standstill threshold is to be understood as a limit value because an ideal standstill (speed = 0) is frequently not achieved in real systems.

Configuration of the safety function SOS in the configuration tool

Field: Automatic SOS			
Input field	**Valid entry**	**Unit**	**Description**
Speed limit value	Activate/deactivate (Default: deactivated)	--	Activation of automatic monitoring.
Speed limit value v_lim	0 … 16777215 (Default: 340)	User-defined [Default: Increments/s]	If the speed falls below the speed limit value, monitoring is started.

Activation and feedback

For activation and feedback of the safety function SOS, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

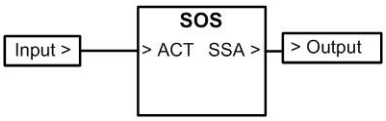


Fig.: Function block SOS

Legend

ACT	The safety function SOS is activated or deactivated via the activation input ACT (0-signal activated, 1-signal deactivated).
SSA	Safe standstill acknowledge The feedback output SSA reports whether the motor is within its permitted limit values (1-signal), or whether there is a limit value violation (0-signal). If the safety function is not activated, the feedback output likewise reports a 0-signal.

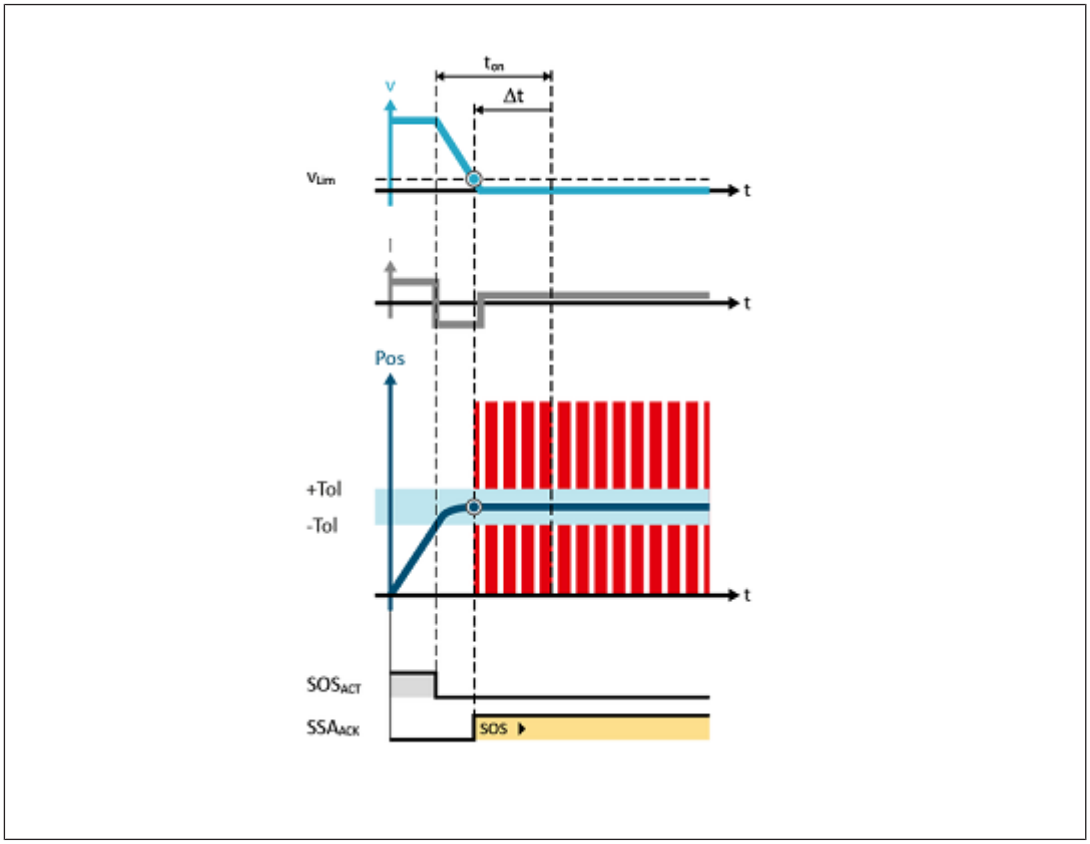


Fig.: Safety function SOS

Legend

ton	On-delay
v	Speed
t	Time
Δt	Variable time, resulting from the entry of v_{lim}
v_{lim}	Speed limit value
I	Current
Pos	Position
+/-Tol_{win}	Standstill tolerance window +/-
SOS_{ACT}	Input for safety function SOS
SSA_{ACK}	Safe standstill acknowledge
	Output for feedback from limit value monitoring

Hysteresis for monitoring functions

A hysteresis can be configured with monitoring functions, as an option; see Hysteresis for monitoring functions [📖 150].

5.12.9 Safe Speed Range (SSR) and Safely Monitored Speed Range (SSR-M)

INFORMATION

The **monitoring function SSR-M "safely monitored speed range"** can be selected as a variant of the normative safety function SSR "safe speed range".
The monitoring function SSR-M corresponds to the normative safety function SSR, except for the error reaction.
When parametrised limit values are exceeded:

- No SS1 is activated on the assigned drive axis
- A 0-signal is issued at the output SRA (safe range acknowledge)

For further information see Hysteresis for monitoring functions [📖 150]

The SSR safety function prevents the motor from exceeding the specified maximum and minimum permitted speed range.

- The safety function SSR corresponds to the definition in accordance with EN 61800-5-2.
- The safety function SSR makes it possible to realise a safety-rated reduced speed and a safety-rated monitored speed in accordance with EN ISO 10218-1.

The safety function can be used as many times as desired (limited only by the maximum number of safety functions).

Activation of the safety function SSR

The safety function SSR can be activated in the following way:

- Though activation at the activation input ACT
- Permanent monitoring (optional)
  - The speed range is monitored without an activation signal, permanently, without an SSR on-delay.
  - No activation is required.

Start of monitoring

- After SSR on-delay has elapsed.

Configuration of the safety function SSR in the configuration tool

Field: Axis SSR			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

Configuration of the safety function SSR in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 20)	[ms]	Time between activation of the safety function SSR and the point at which monitoring begins

NOTICE

Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

Monitoring

- The actual speed of the motor is continuously compared with the maximum and minimum set speed limit value.
- If one of the two limit values is seen to be exceeded, an error reaction is triggered.
- The feedback output SRA is active (see diagram).

Configuration of the safety function SSR in the configuration tool

Field: Speed limit values			
Input field	**Valid entry**	**Unit**	**Description**
Maximum speed limit value v_max	-16777216… 16777215 (Default: 100000)	User-defined [Default: Increments/s]	If the limit value is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.
Minimum speed limit value v_min	-16777216 … 16777215 (Default: -100000)	User-defined [Default: Increments/s]	If the limit value is undercut, the safety function SS1 (E-STOP brake ramp) is activated.

Error reaction SSR

- If a limit value is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SRA feedback output.

Error reaction SSR-M

- A 0-signal is issued at the feedback output SRA if a limit value is exceeded.

Activation and feedback

For activation and feedback of the safety function SSR, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

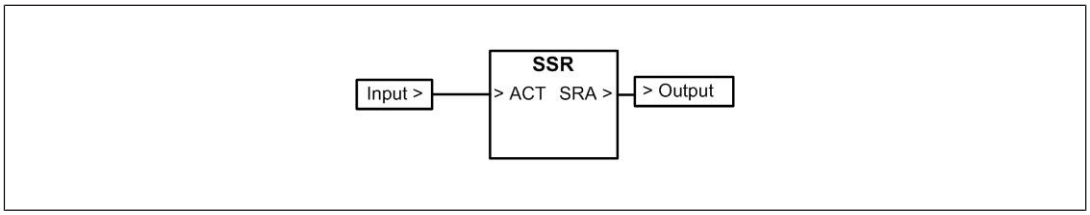


Fig.: Function block SSR

Legend

ACT	The safety function SSR is activated or deactivated via the activation input ACT. (0 signal activated, 1 signal deactivated)
SRA	Safe Range Acknowledge The feedback output SRA reports whether the motor is within its permitted limit values (1 signal), or whether there is a limit value violation (0 signal). If the safety function is not activated, the feedback output likewise reports a 0 signal.

Parametrise the tolerance range (optional)

A tolerance range may also be set for the limit values used to monitor the speed. This tolerance range modifies the set limit values. As a result, one-off or periodic overshoots that exceed the limit values can be tolerated.

The following values can be parametrised for the tolerance range

- Tolerance window, which takes into account the amplitude of the overshoots.
- Tolerance time, which takes into account the width of the overshoots.
- Tolerance period, which takes into account the oscillation period.

Activation of the tolerance range

- If the speed limit value is exceeded, the tolerance range becomes active (see illustration "Safety function SSR with activated tolerance range").

Tolerance range error reaction

- If the tolerance range is exceeded, the safety function SS1 is triggered on the assigned drive axis.
- A 0-signal is issued at the SRA feedback output.

Configuration of tolerance range in the configuration tool (optional)

Field: Tolerance monitoring			
Input field	**Valid entry**	**Unit**	**Description**
Tolerance	Activate/deactivate (Default: deactivated)	--	Activates the tolerance range
Tolerance window Tol_win	1 … 25 (Default: 1)	[%]	Permitted amplitude of the overshoots
Tolerance time t1	1 … 120000 (Default: 100)	[ms]	Permitted width of the overshoots
Tolerance period t2	2 … 120000 (Default: 1000)	[ms]	Permitted period of oscillation

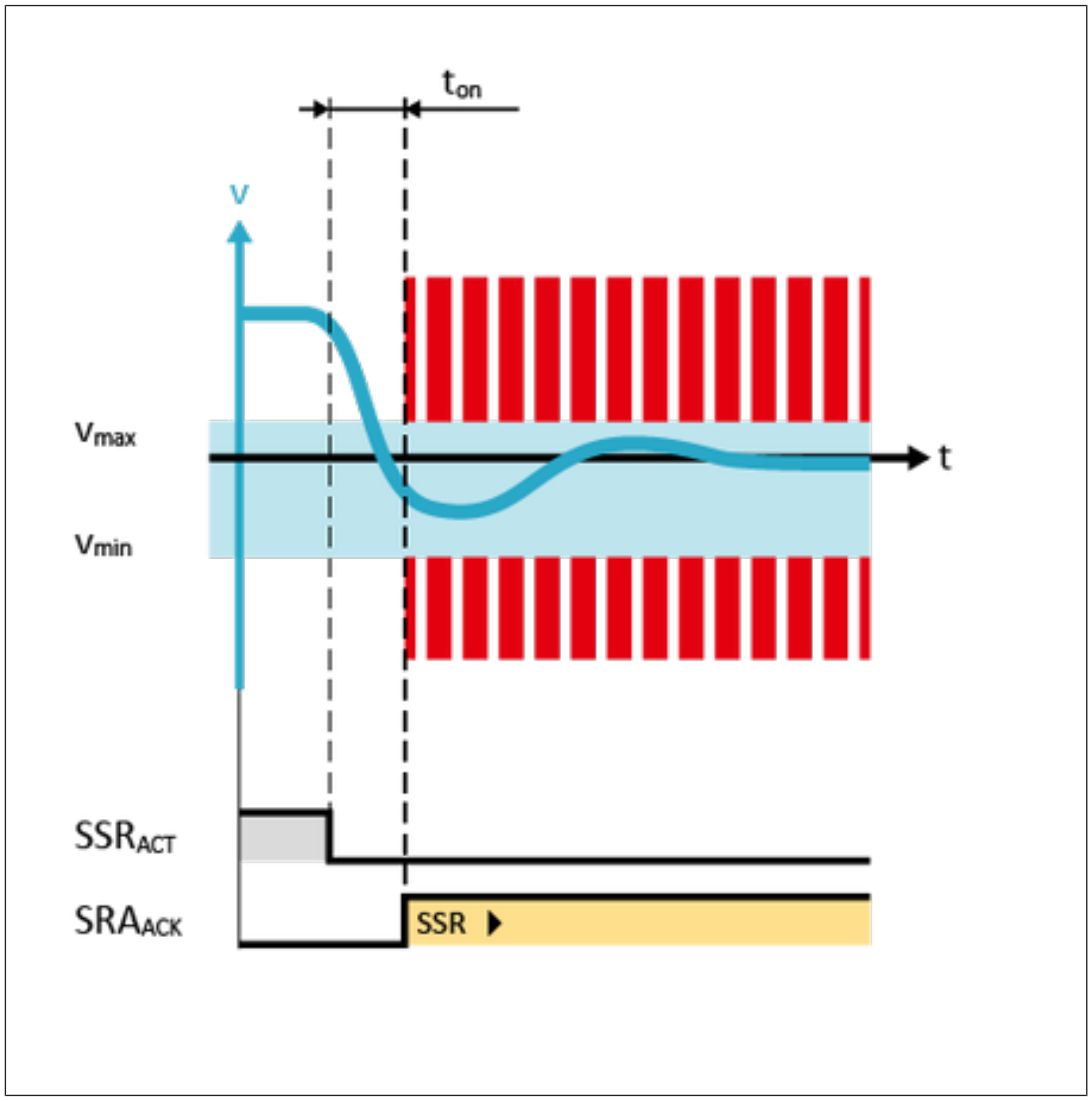


Fig.: Safety function SSR without tolerance range activated

Legend

t_{on}	On-delay
v	Speed
v_{max}	Maximum speed limit value
v_{min}	Minimum speed limit value
SSR_{ACT}	Input for safety function SSR
SRA_{ACK}	Safe range acknowledge
	Output for feedback from safety function SSR

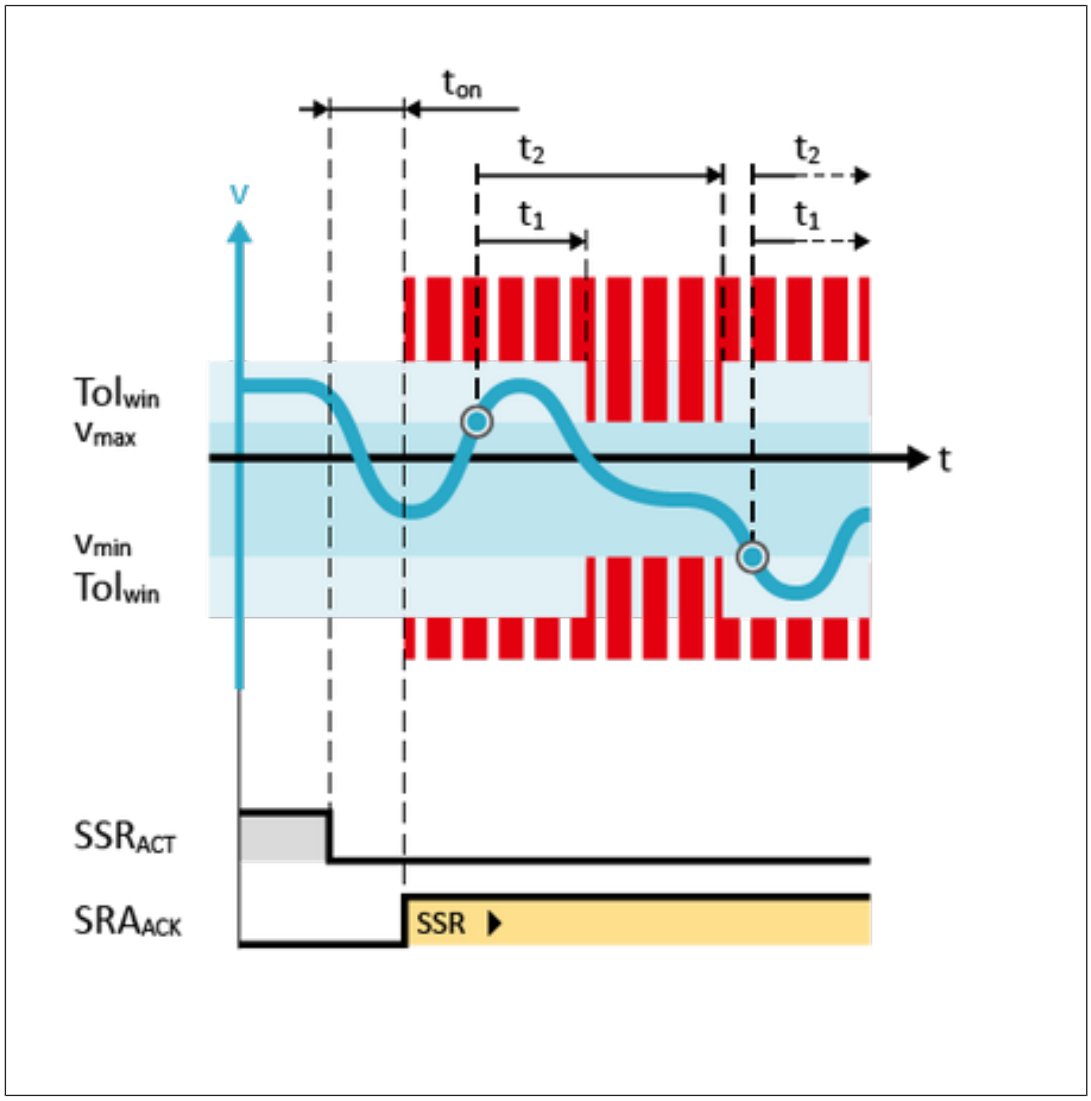


Fig.: Safety function SSR with tolerance range activated

Legend

t_{on}	On-delay
t_2	Tolerance period
t_1	Tolerance time
Tol_{win}	Tolerance window
v_{max}	Maximum speed limit value
v_{min}	Minimum speed limit value
SSR_{ACT}	Input for safety function SSR
SRA_{ACK}	Safe range acknowledge
	Output for feedback from safety function SSR

Hysteresis for monitoring functions

A hysteresis can be configured with monitoring functions, as an option; see Hysteresis for monitoring functions [📖 150].

5.12.10 Safe Brake Control (SBC)

The safety function SBC supplies a safe output signal to control a

- quiescent current-activated mechanical brake or
- safe device to control a brake, such as the Pilz PNOZ s50 for example.

The safety function can be used especially if additional measures to control external influences (e.g. suspended loads falling) are required in the application.

- The safety function SBC corresponds to the definition in accordance with EN 61800-5-2.
- "Holding of loads" can be realised with the safety function SBC.

See under Application of the safe brake functions SBC and SBT [📖 56]

Activating the safety function SBC

The safety function SBC is activated as soon as the safety function STO is active. Direct activation via a safe input is not necessary.

Control of the assigned output

With the safety function SBC activated, a 0 signal is issued at the assigned output. A connected quiescent current-activated brake is engaged, causing the mechanical braking force to be applied to the axis.

If the safety function SBC is deactivated, the state of the output depends on the parameters set for the SBC function.

Assignment of the drive axis to the safety function SBC

The safety function SBC (single-pole brake output SBC 1-pole or dual-pole brake output SBC 2-pole) must be permanently assigned to a drive axis.

Configuration of the safety function SBC (1-pole and 2-pole) in the configuration tool

Field: Axis SBC (SBC 1-pole/SBC 2-pole)			
Input field	**Valid entry**	**Unit**	**Description**
Axis	A1: Axis 1 (Default: A1)	--	Assignment to axis A
	A2: Axis 2	--	Assignment to axis B

INFORMATION

The following applies for SBC function blocks (SBC 1-pole/SBC 2-pole):
When the safety function STO is triggered, all SBC function blocks with the same axis reference as the STO safety function are shut down.
This is independent of the brake control signal from the drive controller.

Connection of drive controller brake control

The safety module offers the option to assign the non-safety-related brake control signal from the drive controller to the safe brake output of an SBC function. As a result, the functional brake control of the drive controller can be combined with the safe brake control via the safety function SBC.

By activating the connection, a quiescent current-activated braking device can be used simultaneously for the following:

- Non-safety-related functions of the drive controller
- Safety functions of the safety module SX6

Configuration of the safety function SBC (1-pole and 2-pole) in the configuration tool

Field: Connection of brake to drive controller			
Input field	**Valid entry**	**Unit**	**Description**
Connection of brake to drive controller	0: No connection (Default: 0)	--	Connection deactivated
	2: Connection brake 1	--	Connection of brake control signal 1 from the drive controller to the safety module
	3: Connection brake 2	--	Connection of brake control signal 2 from the drive controller to the safety module

When the connection is inactive, the safe brake output behaves as follows:

- The safety module is in the axis status STO
  - The safety module issues a 0-signal at the brake output.
  - The brake is engaged, or the braking device allows the engagement of the brake.
  - Control by the drive controller is not possible.
- The safety module is in the axis state RUN or FSRUN
  - The safety module issues a 1-signal at the brake output.
  - The brake is released, or the braking device allows the brake to be released.
  - Control by the drive controller is not possible.

With the connection activated, the safe brake output behaves as follows

- The safety module is in the axis status STO
  - The safety module issues a 0-signal at the brake output.
  - The brake is engaged, or the braking device allows the engagement of the brake.

– Control by the drive controller is not possible.

▸ The safety module is in the axis state RUN or FSRUN

– The brake output is controlled in a non-safety-related way by the drive controller.

NOTICE

In the **axis state RUN**, active safety functions must safeguard against hazardous or unpermitted movements of the drive. If the axis status STO is activated by the safety function SS1 when an error has been detected, the brake is engaged safely via the safety function SBC, independently of the brake control signal from the drive controller.

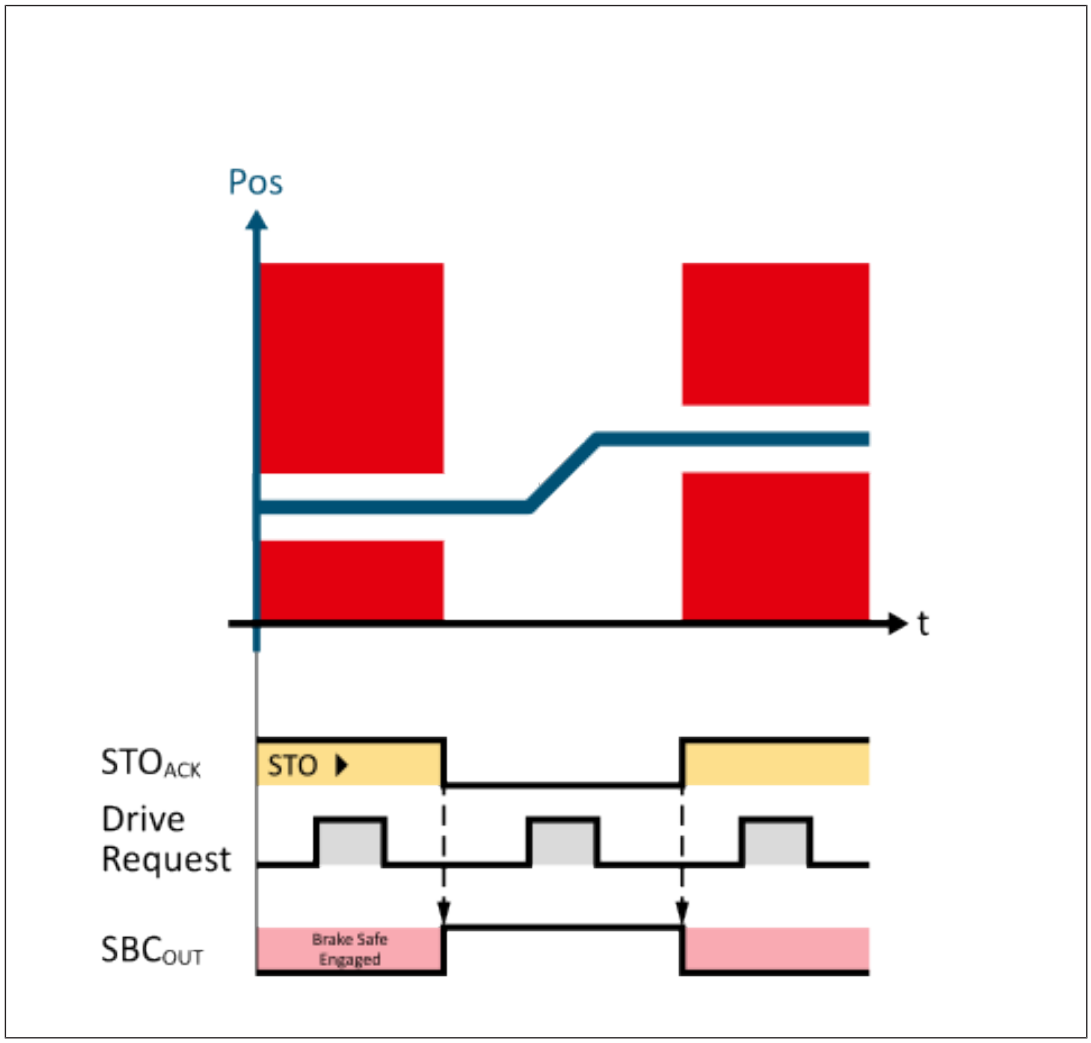


Fig.: Safety function SBC connection deactivated

Legend

Pos	Position
STO_{ACK}	Output for feedback from safety function STO
Drive request	Brake control signal from drive controller
SBC_{out}	Brake control output

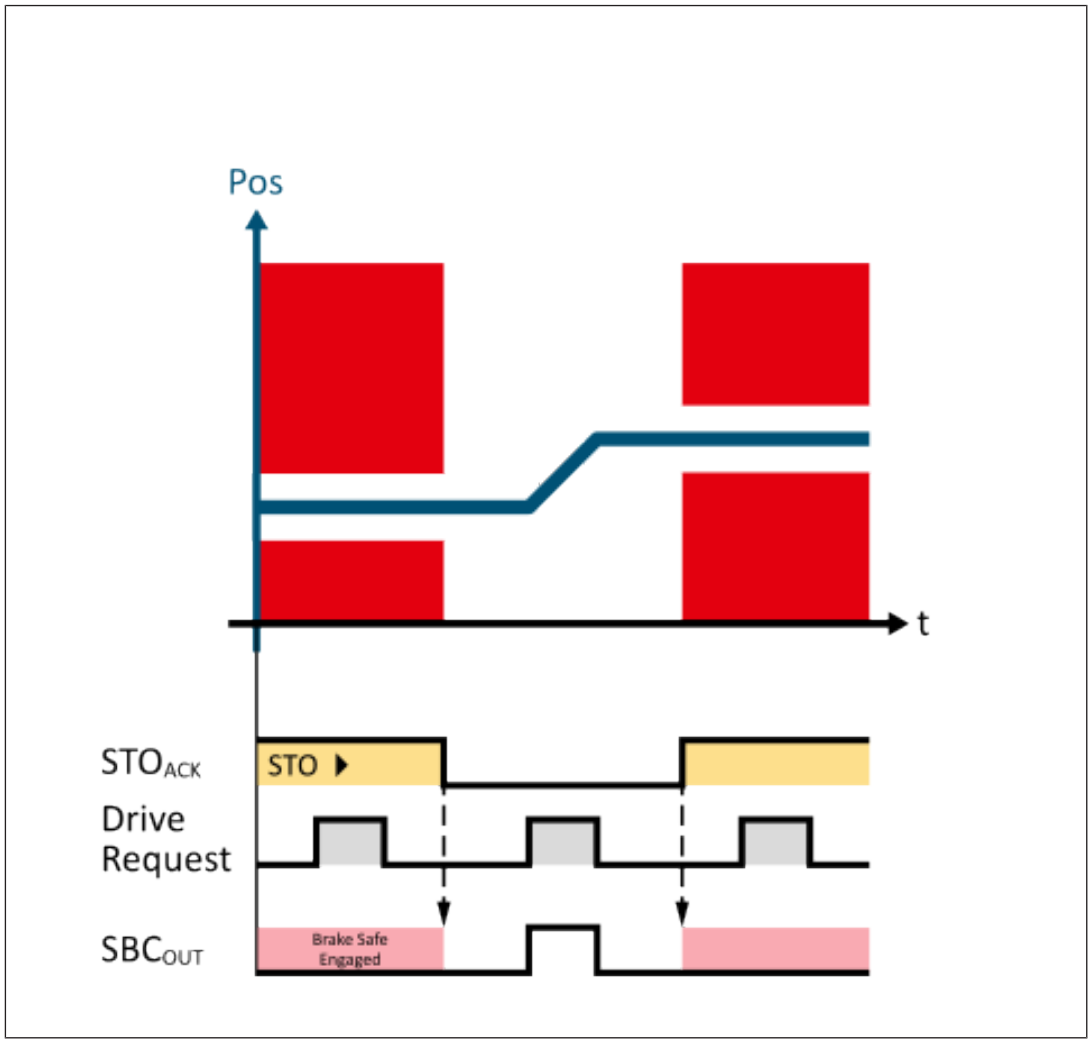


Fig.: Safety function SBC connection activated

Legend

Pos	Position
STO_{ACK}	Output for feedback from safety function STO
Drive request	Brake control signal from drive controller
SBC_{out}	Brake control output

Use of a feedback input (optional)

The safety function SBC offers scope for evaluating a feedback signal from the activated braking device.

If the feedback signal is not detected correctly at the input, the safety function SS1 is triggered on the assigned drive axis.

You can choose between the following inputs as feedback input:

- Safe FSoE fieldbus input on the safety module
- Standard input on the drive controller

Configuration of the reset input in the configuration tool

Field: Brake feedback			
Input field	**Valid entry**	**Unit**	**Description**
Activate feedback via input	0: Feedback off (Default: 0)	--	Feedback deactivated
	1: FSoE (safe)	--	Feedback via a safe FSoE fieldbus input on the safety module
	2: Brake 1 (drive controller input, source: F106)	--	Feedback via drive controller
	3: Brake 2 (drive controller input, source: F107)	--	Feedback via drive controller

The parameters for the behaviour of the feedback signal can be set in the configuration tool.

NO – Normally open

When the braking device is released, a 1-signal is expected as the feedback signal.

When the braking device is engaged, a 0-signal is expected as the feedback signal.

NC – Normally closed

When the braking device is released, a 0-signal is expected as the feedback signal.

When the braking device is engaged, a 1-signal is expected as the feedback signal.

The maximum on-delay for feedback when the signal changes to a 1-signal (ON) and the maximum off-delay to a 0-signal (OFF) can be set in the configuration tool.

NOTICE

Please note that on-delay/off-delay times that are not a multiple of the processor system's cycle time (see Technical details [📖 179]) will not elapse until the following system cycle.

Configuration of the safety function SBC in the configuration tool

Field: Brake feedback			
Input field	**Valid entry**	**Unit**	**Description**
On-delay Ton	0 …120000 (Default: 20)	[ms]	Maximum on-delay when signal changes to a 1-signal
Off-delay Toff	0 …120000 (Default: 20)	[ms]	Maximum off-delay when signal changes to a 0-signal
Type	1: normally open (NO)	--	Selection of feedback type
	2: Normally closed (NC) (Default: 2)		

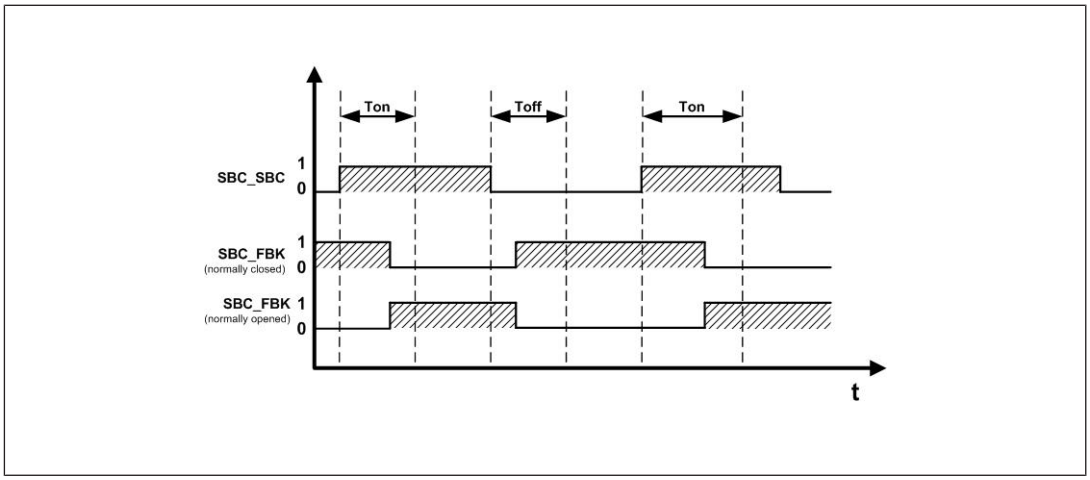


Fig.: Safety function SBC, feedback

Legend

Ton	On-delay ON Feedback when signal changes to a 1-signal
Toff	Off-delay OFF Feedback when signal changes to a 0-signal
SBC_SBC	Brake control output
SBC_FBK (normally closed)	Feedback input (feedback FBK) (normally closed, N/C)
SBC_FBK (normally opened)	Feedback input (feedback FBK) (normally open, N/O)

5.12.10.1 Combination options for SBC 1-pole and SBC 2-pole

There is a choice of the following function blocks in the configuration tool:

- SBC 1-pole
- SBC 2-pole

INFORMATION

The function blocks SBC 1-pole and SBC 2-pole can each be used a maximum of twice in the configuration tool.
Also, only two SBC function blocks can be used per drive axis.
Possible application of the SBC function blocks per drive axis:
SBC 1-pole + SBC 1-pole
SBC 2-pole + SBC 1-pole
SBC 2-pole + SBC 2-pole

The various combinations are described under
Application of the safe brake functions SBC and SBT [📖 56]

5.12.10.2 SBC with 1-pole output for controlling an external safe device

The safety function SBC 1-pole is intended for indirect control of the brake or to control an external safe braking device.

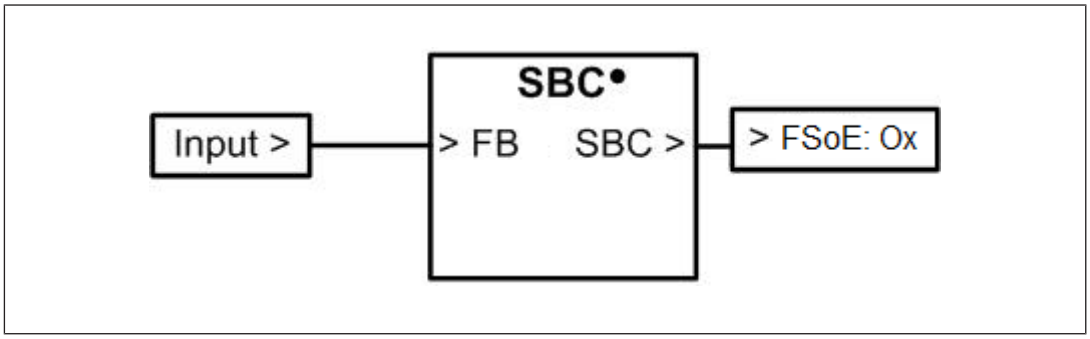


Fig.: Function block SBC 1-pole

The safety function SBC 1-pole can be assigned to any FSoE output.

5.12.10.3 SBC with 2-pole output for direct and indirect control of a brake

The safety function SBC 2-pole is intended for direct control of quiescent current-activated, mechanical brakes.

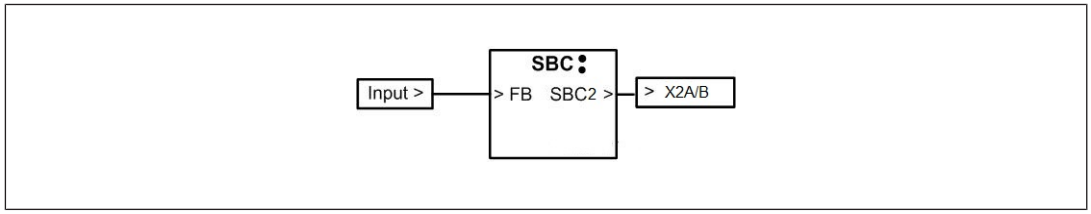


Fig.: Function block SBC 2-pole, using SC6 drive controller as an example

The safety function SBC 2-pole must be assigned to a 2-pole SBC output on the drive controller (see "Direct control of quiescent current-actuated, mechanical brakes by the safety module").

5.12.11 Safe Brake Test (SBT)

The proper functioning of quiescent current-actuated brakes can be tested with the safety function SBT.

The safety function SBT corresponds to a cyclical test of the braking device.

The safety function can only be used once per drive axis and has a fixed assignment to the drive axis.

The safe brake test (SBT), in conjunction with safe brake control (SBC), meets the requirements of EN ISO 16090-1 for safeguarding gravity-loaded axes.

INFORMATION

When configuring the brake test, make sure that the permitted switching frequency of the connected brakes is not exceeded (see data sheet for the quiescent current-actuated, mechanical brake).

Up to four test steps can be configured in the test sequence. In each test step, a check is carried out to determine whether the configured brake can generate the necessary holding torque for the assigned drive axis over the defined period. During the test, standstill of the motor is monitored from a safety-related perspective.

The following components are involved in executing the safety function SBT:

- The drive controller with integrated safety module
- A motor connected to the drive controller (see Permitted motor types [📖 16]) with motor encoder (see Permitted motor encoders [📖 16])
- One or more quiescent current-actuated brakes/braking devices

"Holding of loads" can be tested with the safety function SBT. The safety function "Holding of loads" can be implemented in conjunction with the safety function SBC.

For further information on application of the safety function SBT see Application of the safe brake functions SBC and SBT [📖 56].

CAUTION!

Risk of injury

A hazardous status may occur if there is a faulty brake or braking device.

– Carry out the brake test in an appropriate position and ensure that nobody remains in the danger zone during the brake test.

INFORMATION

It is possible to run the brake test for two brakes on an axis without applying power to the motor on the corresponding drive axis (gravity test).

The brake test can only be performed if the drive axis assigned to the SBT function is in the axis state RUN and no STOP function is active on this axis.

Encoder test

At the start of the brake test, the encoder on the assigned drive axis is first tested with the brake(s) open. In this case, the motor rotates at approx. 60 1/min for maximum 45° in a positive direction of rotation. If the direction of rotation lock in the drive controller is active for the positive direction of rotation, the motor will travel in the negative direction. In this phase, the safety module's standstill monitoring is not yet active.

Inspection period and tolerance time

The safety function SBT must be activated cyclically, within an inspection period.

INFORMATION

The inspection period should be measured in accordance with EN ISO 16090-1 (e.g. 8 h – once per shift).

The inspection period

- can be set in the configuration tool.
- is monitored in a safety-related manner.
- is restarted once the safety function SBT has been executed without errors.

If there is no activation of the safety function SBT within the inspection period

- the tolerance time is started.
- a 0 signal is issued at the feedback output SBA.

The tolerance time

- can be set in the configuration tool.
- is monitored in a safety-related manner.
- is reset by RESTART on the assigned drive axis, after a brake test error and when the tolerance time has elapsed.

If there is equally no activation of the safety function SBT within the tolerance time

- the motor on the assigned drive axis is shut down with the safety function SS1.
- the assigned drive axis on the motor switches to the axis state FAULT via the safety module.

If the device state RUN is achieved after the safety module has run up, the inspection period is treated as elapsed and the safety function SBT must be activated within the tolerance time.

Configuration of the safety function SBT in the configuration tool

Field: Brake test check			
Input field	**Valid entry**	**Unit**	**Description**
Inspection period	0 … 10000 (Default: 480)	[min]	Time after which the safety function SBT must be executed.
Tolerance time	1 … 100 (Default: 10)	[%]	Tolerance time of inspection period

Activation of the safety function SBT

The safety function SBT can be activated in the following way:

- By external activation at the activation input SBT_ACT
- By internal activation via the drive controller

Configuration of the safety function SBT in the configuration tool

Field: Brake test start		
Input field	**Options**	**Description**
Brake test start	Input SBT_ACT (Default)	Activation of the safety function SBT via input SBT_ACT
	Drive controller	Activation of the safety function SBT via drive controller

Start of test sequence

With external activation on the safety module's activation input

- the test sequence begins after the SBT on-delay has elapsed.
- the feedback output SSA actively signals that the axis position is being monitored for standstill.

With internal activation via the drive controller

- The test sequence starts without an on-delay.
- the feedback output SSA actively signals that the axis position is being monitored for standstill.

INFORMATION

Please note that on-delay times that are not a multiple of the processor system's cycle time (see Technical details [179]) will not elapse until the following system cycle.

The configuration of the safety function SBT in the configuration tool

Field: On-delay			
Input field	**Valid entry**	**Unit**	**Description**
On-delay t_on	0 … 120000 (Default: 20)	[ms]	Time between activation of the safety function SBT and the point at which monitoring begins

The on-delay is only effective when the brake test is started via SBT_ACT.

Test sequence procedure

Up to four test steps can be defined in the configuration tool for the test sequence. These are performed in succession.

The entire test sequence is monitored via a total time t_max (timeout) that can be set in the configuration tool, and must be completed before this time period has elapsed. If that is not the case, safety function SS1 is activated on the assigned drive axis and the safety module switches to the axis state FAULT. The brake test is considered to have been failed.

INFORMATION

Determine the total time manually

The total time depends on the set times for the total test sequences and must be determined manually.

Field: Total time (t_max)			
Input field	**Valid entry**	**Unit**	**Description**
Total time t_max	0 … 2147483647 (Default: 30000)	[ms]	If the brake test is not completed within the total time, an error reaction is triggered.

INFORMATION

The total duration of the brake test (parameter total time t_max) can be extended by the configured brake release time and/or waiting time, if the test step requires additional brake switching. This should be taken into account when configuring the total time for the brake test.

During the entire test sequence, the assigned drive axis is monitored for standstill in a safety-related manner. The permitted tolerance window for standstill monitoring can be set in the configuration tool.

Field: Tolerance window (Tol)			
Input field	**Valid entry**	**Unit**	**Description**
Tolerance window Tol	0 … 2147483647 (Default: 50)	User-defined [Default: Increments]	Tolerance window of the safety function SBT during the test sequence.

If there is movement away from the standstill position (SOS is triggered), the safety function STO is activated on the assigned drive axis and the axis is brought to a safe state.

Aborting the test sequence

The test sequence can be aborted by the following safety functions:

- Activation of safety function STO
- Activation of safety function SS1
- Activation of safety function SS2
- Deactivation of safety function SBT

After aborting

- the safety function STO is activated on the assigned drive axis.
- the brake test is considered to have been failed.

Test steps

For all test steps

Once a test step has ended, the next test step begins after the waiting period t_wait has elapsed and, if the brake is changed, after the release time t_lift has elapsed.

If the brake test fails one of the test steps, the entire brake test is aborted and the safety function STO is activated on the assigned drive axis.

Field: Steps			
Input field	**Valid input/ Permanently set**	**Unit**	**Description**
Waiting time (t_wait)	100 … 120000 (Default: 2000)	[ms]	Waiting time after each test step

INFORMATION

The configured waiting time between two test steps (waiting time parameter t_{wait}) must as a minimum correspond to the longest engagement time of the connected brakes.
When a waiting time is configured in this way, it should avoid the situation where one brake is still closing while the other brake is already beginning to open. This can prevent a suspended load from slipping.

Additional configuration options for all test steps

Field: Test current tolerance			
Input field	**Valid entry**	**Unit**	**Description**
Test current tolerance	0 … 1000 (Default: 200)	[mA]	Tolerance window for test current

NOTICE

Please note that configuring a tolerance value greater than or equal to the test current may render current monitoring ineffective. Ensure that the "Tolerance value test current" is set correctly and sensibly (maximum 90% of the amount of the lowest configured test current).

Field: Current rise time			
Input field	**Valid entry**	**Unit**	**Description**
Current rise time (t_ramp)	0 … 2147483647 (Default: 1500)	[ms]	Defines the length of time until maximum power.

Field: Brake release time			
Input field	**Valid entry**	**Unit**	**Description**
Brake release time (t_lift)	0 … 10000 (Default: 200)	[ms]	Defines the waiting time needed to completely release a brake, before power is activated.

Test step

Each of the four test steps can be activated individually in the configuration tool.

In the test step,

- in the case of two brakes, the brake that is not to be tested is released.
- the brake or braking device to be tested on the assigned drive axis is activated, so that a braking force is applied.
- the torque/force-generating test current for the connected motor is determined (with a current ramp that is adjustable in the configuration tool).
- the duration of energisation is monitored (adjustable in the configuration tool).
- motor standstill is monitored on the assigned drive axis in a safety-related manner.
- the amplitude of the motor current on the assigned drive axis is monitored for compliance with the tolerance window that can be set in the configuration tool.

Configuration of the safety function SBT in the configuration tool

Feld: Step 1 … 4			
Input field	**Valid entry**	**Unit**	**Description**
Test current	-100000 … 100000 (Default: 0)	[mA]	Max. current value that must be achieved
Duration	0 … 120000 (Default: 1000)	[ms]	Duration of energisation
Brake	**0** – Brake	--	Cannot be set
	1 – SBC-NameX* the same axis assignment as the SBT function	--	Specification of brake for testing
	2 - SBC-NameY* the same axis assignment as the SBT function	--	Specification of brake for testing
*SBC-NameX, SBC-NameY The designations/names of the brakes are specified in the configuration tool of the safety function SBC			

The brake/braking device of the completed test step is released as soon as the braking force of the brake/braking device for the next test step is applied. This overlap prevents a suspended load from dropping.

Throughout the entire test step, the motor may only move within the configured tolerance window.

INFORMATION

Annex G of EN ISO 16090-1 recommends the following for gravity-loaded axes:

- a minimum test duration of 1 s
- for applications with one brake, a test with 1.3 times the weight load
- for applications with two brakes, a test with 1.0 time the weight load

If the safety module detects an error via one of the monitoring functions

- the safety function STO is activated on the assigned drive axis.
- the affected drive axis switches to the axis state FAULT.

Calculation of test current

The test current corresponds to the force-forming component of the motor current.

For rotary motors, the test torque is calculated using the following formula:

- Test current x torque constant

For linear motors, the test force is calculated using the following formula:

- Test current x force constant

Forces or torques already acting on the axis must be considered in the measurement, e.g. suspended loads.

Test sequence completed successfully

If all test steps have been performed without errors, the test sequence has been completed successfully.

Then

- the test period is started afresh.
- a 1 signal is issued at the feedback output SBA.

INFORMATION

Error messages that can occur due to an incorrectly designed configuration of the safety function SBT can be read via the diagnostics (e.g. error stack in the safety configurator "PSC").

Activation and feedback

For activation and feedback of the safety function SBT, the following activation and feedback signals from the function can be routed to safe inputs and outputs.

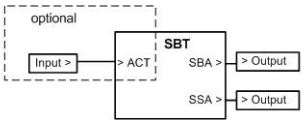


Fig.: Function block SBT

Legend

ACT	The safety function SBT is activated or deactivated via the activation input ACT (1-signal activated, 0-signal deactivated).
SBA	Safe Brake Acknowledge The feedback output reports that the last brake test was completed successfully and the inspection period has not yet elapsed (1-signal) or that the brake test is in progress (0-signal) or that the inspection period has expired (0-signal).
SSA	Safe standstill acknowledge The feedback output reports that standstill monitoring is active and the motor is at a standstill (1 signal) or that the motor has moved during the brake test in progress (0 signal).
Optional	As an option, the safety function SBT can be activated via the drive controller (can be selected in the configuration tool).

INFORMATION

The only safety function activated is the SBT safety function with positive edge.

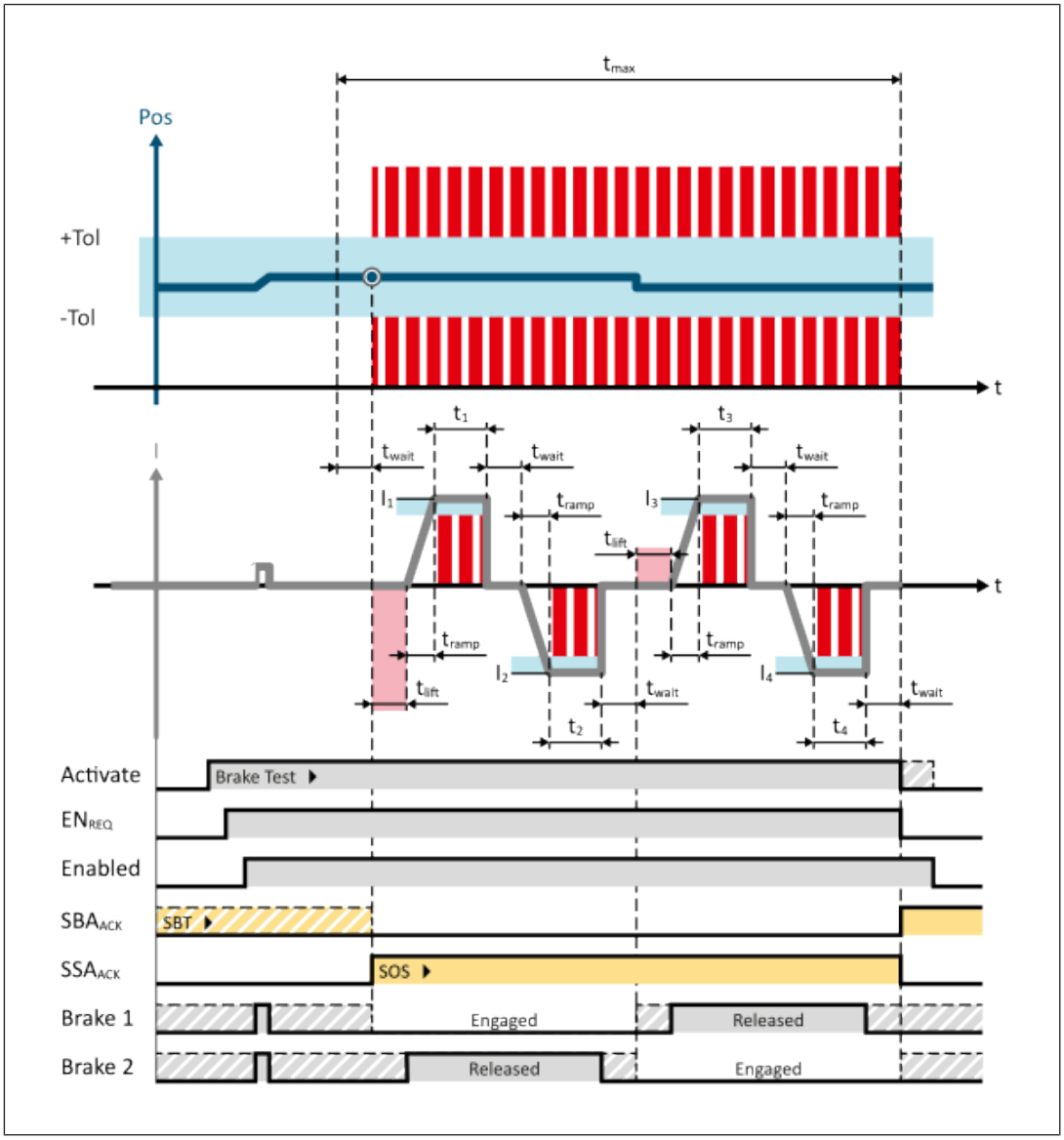


Fig.: Safety function SBT with control via drive controller

Legend

t_{max}	Total time
t_{on}	On-delay
Pos	Position
+/-Tol	Tolerance window +/-
t_{lift}	Brake release time
t_{ramp}	Current rise time
t_1	Brake test duration test step 1
t_2	Brake test duration test step 2
t_3	Brake test duration test step 3
t_4	Brake test duration test step 4
t_{wait}	Waiting time

I_1	Test current test step 1
I_2	Test current test step 2
I_3	Test current test step 3
I_4	Test current test step 4
SBT_{ACT}	Input for safety function SBT
SBA_{ACK}	Safe brake acknowledge Output for feedback from safety function SBT
SSA_{ACK}	Safe standstill acknowledge Output for feedback from standstill monitoring

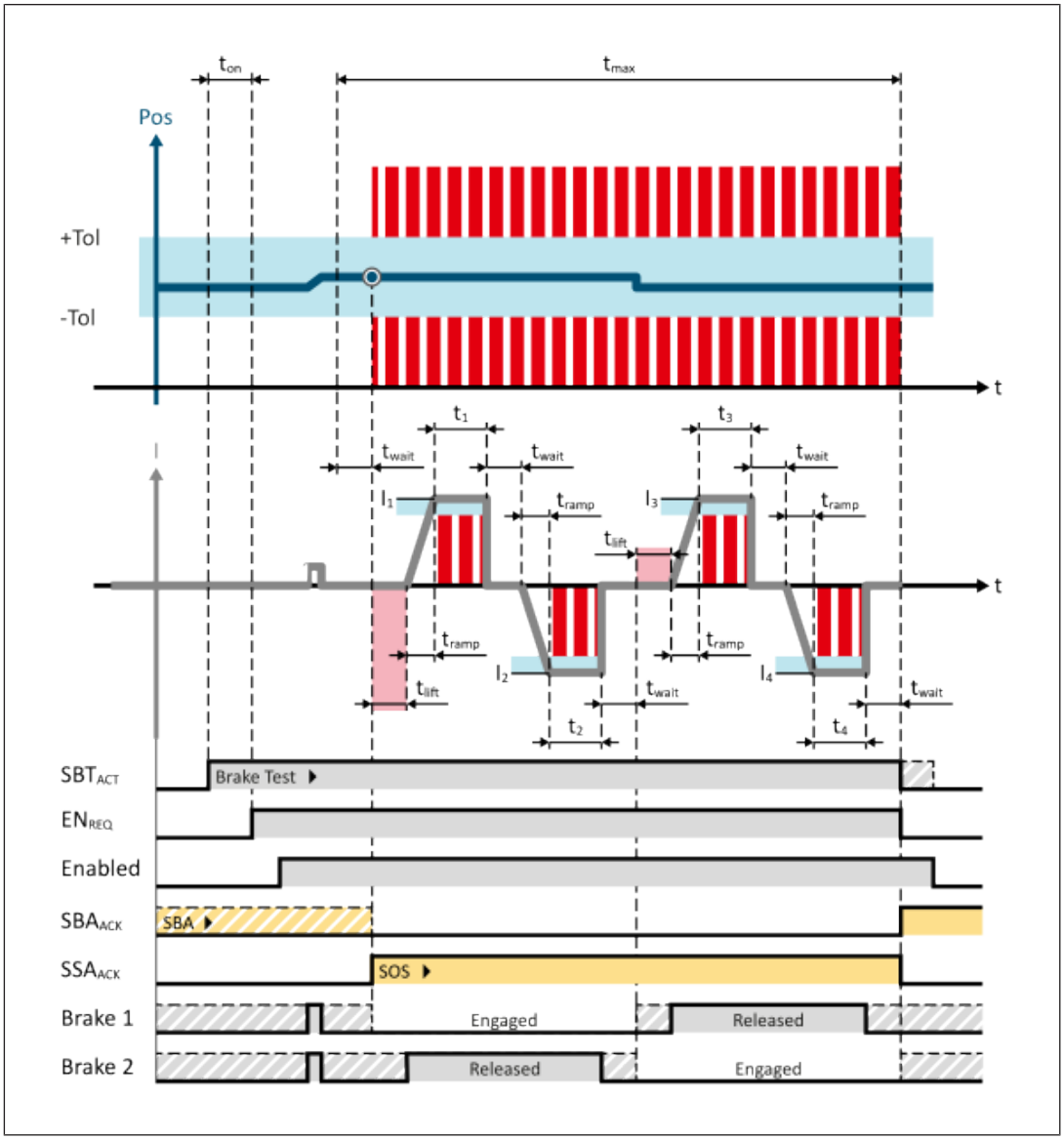


Fig.: Safety function SBT with control via "input (SBT_ACT)"

Legend

t_{max}	Total time
t_{on}	On-delay
Pos	Position

+/-Tol	Tolerance window +/-
t_{lift}	Brake release time
t_{ramp}	Current rise time
t_1	Brake test duration test step 1
t_2	Brake test duration test step 2
t_3	Brake test duration test step 3
t_4	Brake test duration test step 4
t_{wait}	Waiting time
I_1	Test current test step 1
I_2	Test current test step 2
I_3	Test current test step 3
I_4	Test current test step 4
SBT_{ACT}	Input for safety function SBT
SBA_{ACK}	Safe brake acknowledge Output for feedback from safety function SBT
SSA_{ACK}	Safe standstill acknowledge Output for feedback from standstill monitoring

5.12.12 Safe Restart Lock (SRL)

The safety function SRL prevents the safety module from leaving the device state STO and the axis state STO via a reset. An unexpected or unintended start-up of the drive axis or axes is therefore impossible.

- The safety function SRL can be used to prevent an unexpected start-up in accordance with ISO 14118.

The safety function can only be used once in the configuration.

Activation of the safety function SRL

The safety function SRL can be activated in the following way:

- Though activation at the activation input ACT

The following activation signals for the function can be connected to a safe input for activation of the safety function SRL:

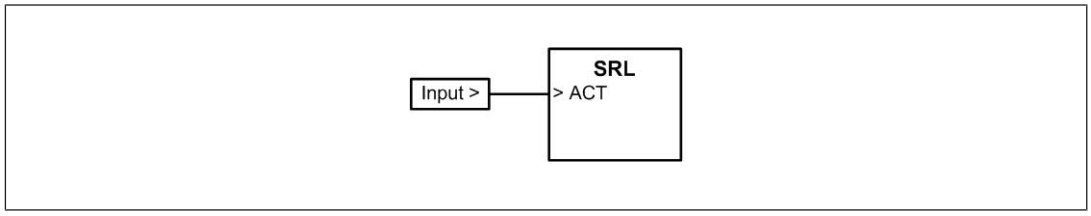


Fig.: Function block SRL

Legend

ACT	The safety function SRL is activated or deactivated via the activation input ACT (0-signal activated, 1-signal deactivated).

0-signal (activated)

The RESET is blocked and cannot be triggered.

Additional information on the RESET behaviour is provided under:
Safe restart of the machine [📖 49]
RESET of the safety module

Switching from 0-signal to 1-signal

Various actions can be configured in the configuration tool.

The following can be performed when switching from 0-signal to 1-signal:

- RESTART of safety module is triggered, errors are acknowledged or
- Only errors are acknowledged or
- No operation takes place.

1-signal (deactivated)

A RESET is possible (as an option, depending on other RESET settings).

Configuration of the safety function SRL in the configuration tool

Field: RESET trigger			
Input field	**Valid entry**	**Unit**	**Description**
RESET behaviour	0: NOP (Default: 0)	--	No operation No RESTART occurs.
	1: ACK ERR	--	Acknowledge error No RESTART occurs.
	2: RESTART	--	Acknowledge error A RESTART is triggered.

INFORMATION

A RESET of the drive axis or axes (switching to the axis state RUN) can only take place if the activation input SS1_ACT and the activation input STO_ACT (if configured) and the STO bit in the FSoE control word (FSoE Control Byte 1, Bit 0) have a 1-signal.

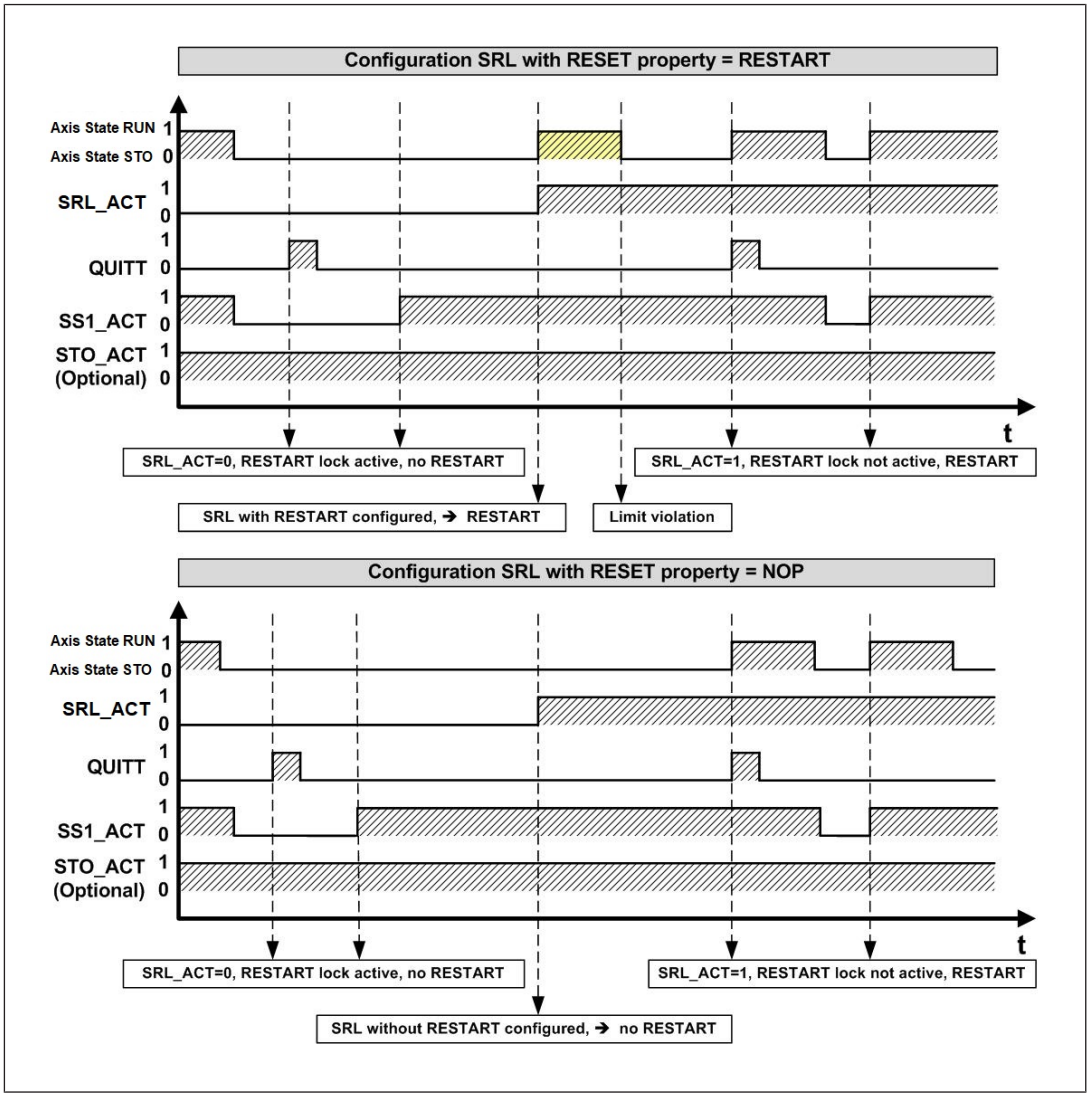


Fig.: Safety function SRL, RESET

Legend

Axis state RUN	The axis state is RUN (see Operating states [📖 165]).
Axis state STO	The axis state is STO (see Operating states [📖 165]).
SRL_ACT	Input for safety function SRL
ACK	The ACK command was performed via the drive controller.
SS1_ACT	Input for safety function SS1
Optionally STO_ACT	Optional input for safety function STO

5.12.12.1 Effects of RESET with safety function "Safe restart lock (SRL)"

- The RESET affects all axes that are in the STO state (see Operating states SX6 [📖 165]).
- In the event of a RESET, all errors (global and axis-specific) are reset.

5.12.12.2 Effects of run-up and configuration refresh with safety function "Safe restart lock (SRL)"

Effects of run-up (RUNUP) with safety function "Safe restart lock (SRL)"

- In the event of a run-up with configured SRL safety function, the behaviour of the safety module depends on the state of the activation input SRL_ACT:
  - SRL_ACT = 0: Run-up ends in STO (restart lock active)
  - SRL_ACT = 1: Run-up ends in RUN (restart lock inactive)

Effects of configuration refresh with safety function "Safe restart lock (SRL)"

- In the event of configuration refresh with configured SRL function, the behaviour of the safety module depends on the state of the activation input SRL_ACT:
  - SRL_ACT = 0: RESTART ends in STO (restart lock active)
  - SRL_ACT = 1: RESTART ends in RUN (restart lock inactive)

Deactivation SRL

When the SRL safety function is activated via a safe fieldbus input, the function cannot be deactivated until safe bus communication has started up successfully and cyclical data exchange (exchange of process data) between the subscribers is active.

5.12.13 Safe Status Output (SSO)

The safety function "safe status output" (SSO) reports the current device status of the safety module. The three outputs READY, FSRUN and $\overline{\text{FAULT}}$ (no error) are available.

The safety function can only be used once in the configuration.

The safety function SSO does not require explicit activation.

READY output

1-signal

- The safety module is operational.

0-signal

- In the following cases the safety module is not operational:
  - No supply voltage
  - Safety module is in RUNUP, see Operating states [165]
  - Safety module is in STARTUP, see Operating states [165]
  - Fatal error

FSRUN output

1-signal

- The safety module is in the device state FSRUN (see Operating states [165]).
  - A motion-monitoring safety function is activated (see "General terminology [27] ").
  - Standstill monitoring during the brake test SBT is active ("encoder test" and "on-delay" phase is already complete).

0-signal

- The safety module is not in the device state FSRUN (see Operating states [165]).
  - No motion-monitoring safety function is activated (see "General terminology [27]").
  - Standstill monitoring during the brake test SBT is not active.

Output $\overline{\text{FAULT}}$ (no error)

1-signal

- The safety module has no error.

0-signal

- The safety module has an error.
- The safety module is in the device state STO-FAULT.
- The safety module is in the device state STO-FATAL.

Feedback

The following feedback signals from the function can be connected to safe outputs for feedback from the safety function SSO:

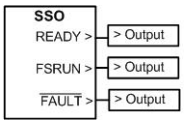


Fig.: Function block SSO

Legend

READY	The READY output reports whether the safety module is operational.
FSRUN	The FSRUN output reports whether a safety function is active. (The safety functions SSO, SBC or SRL are excluded)
$\overline{\text{FAULT}}$ (no error)	The $\overline{\text{FAULT}}$ output reports whether the safety module has an error (global or axis-specific).

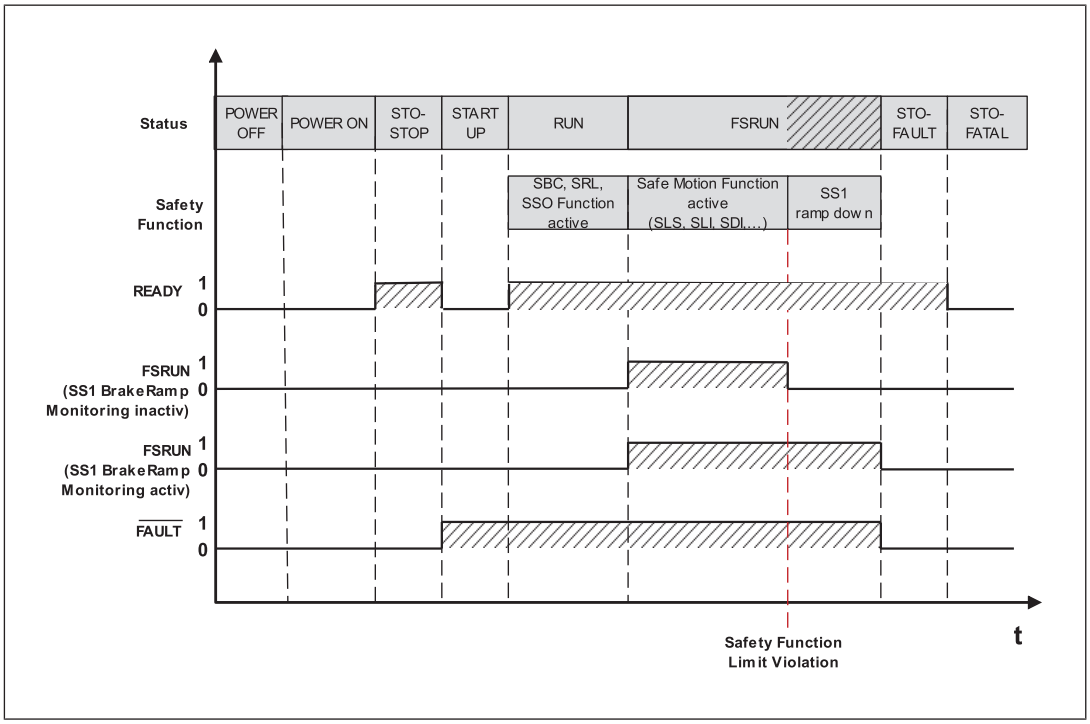


Fig.: Safety function SSO

Legend

Status	Device status of the safety module
Safety function	Safety functions
READY	Output for feedback on whether the safety module is ready for operation.

FSRUN (SS1 brake ramp monitoring inactive)	Output for feedback on whether a motion-monitoring safety function is active. (The safety functions SSO, SBC or SRL are excluded, brake ramp monitoring is not activated on the safety function SS1)
FSRUN (SS1 brake ramp monitoring active)	Output for feedback on whether a safety function is active. (The safety functions SSO, SBC or SRL are excluded, brake ramp monitoring is activated on the safety function SS1)
$\overline{\text{FAULT}}$	Output for feedback on whether the safety module has an error.
Safety function Limit violation	Limit value exceeded by a motion-monitoring safety function

5.12.14 Hysteresis for monitoring functions

A **hysteresis window** can also be defined for the monitoring limit values.

This makes it possible to avoid toggling the feedback signal in the limit value range.

A hysteresis window can be defined for the following monitoring functions:

- SDI-M (safely monitored direction)
- SLI-M (safely monitored increment)
- SLS-M (safely monitored speed)
- SOS-M (safely monitored operating stop)
- SSR-M (safely monitored speed range)

INFORMATION

Hysteresis (optional)

If the **"Permanent" monitoring type** has been selected in the configurator for a monitoring function (see Permanent monitoring (optional) [76]), it is mandatory to select the **"Hysteresis" monitoring behaviour**.

Monitoring behaviour

If it is identified that a limit value has been exceeded, the output for the safety function in question is reset (0 signal).

Renewed setting of the feedback output (1 signal) must be performed via one of the two functions:

- Set/reset function (default)
- Hysteresis (optional)

Set/reset function (default)

- The output remains permanently reset (0-signal) even if exceeding of the limit value no longer applies.
- The output remains reset (0-signal) until the safety function has been activated again at the input after an activation edge, the on-delay has elapsed, and the limit value violation no longer applies.

Hysteresis (optional)

- Defines a range around the specified limit value within which the feedback output does not change.
- After a limit value has been exceeded, the feedback output is only reset when the actual value leaves the configured hysteresis range.

Configuration of a monitoring function with hysteresis in the configuration tool

Field: Monitoring behaviour			
Input field	**Valid entry**	**Unit**	**Description**
Monitoring behaviour	Set/Reset (Default)	--	The set/reset function is active.
	Hysteresis	---	Automatic control of the feedback output based on the hysteresis window.
Hysteresis window hyst_win	0 ... 100 (Default: 10)	[%]	Range around the specified limit value within which the feedback output does not change.

Behaviour of hysteresis, depending on monitoring function

Safety function	Valid entry	Description
SDI-M	-	The tolerance window configured in the input field "Standstill position window (Tol_win)" is used as the hysteresis window. After a limit value has been exceeded, if the current position moves in the correct direction by more than the configured tolerance window, the feedback output is set again.
SLI-M	0 … 100 %	0 … 100 % of the permitted position range, in other words the sum of the input value "Position max (Pos_{max})" and "Position min (Pos_{min})" is used as the hysteresis window.
SLS-M	0 … 100 %	0 … 100 % of the limit value configured in the input field "Limit value speed (v_{lim})" is used as the hysteresis window.
SOS-M	0 … 100 %	0 … 100 % of the limit value configured in the input field "Position window standstill (Tolerance (Tol))" is used as the hysteresis window.
SSR-M	0 … 100 %	0 … 100 % of the permitted speed range, in other words the difference between the input value "Maximum speed limit value (v_{max})" and "Minimum speed limit value (v_{min})" is used as the hysteresis window.

The monitoring function SLS-M (safely monitored speed) serves as an example of the behaviour with hysteresis and set/reset.

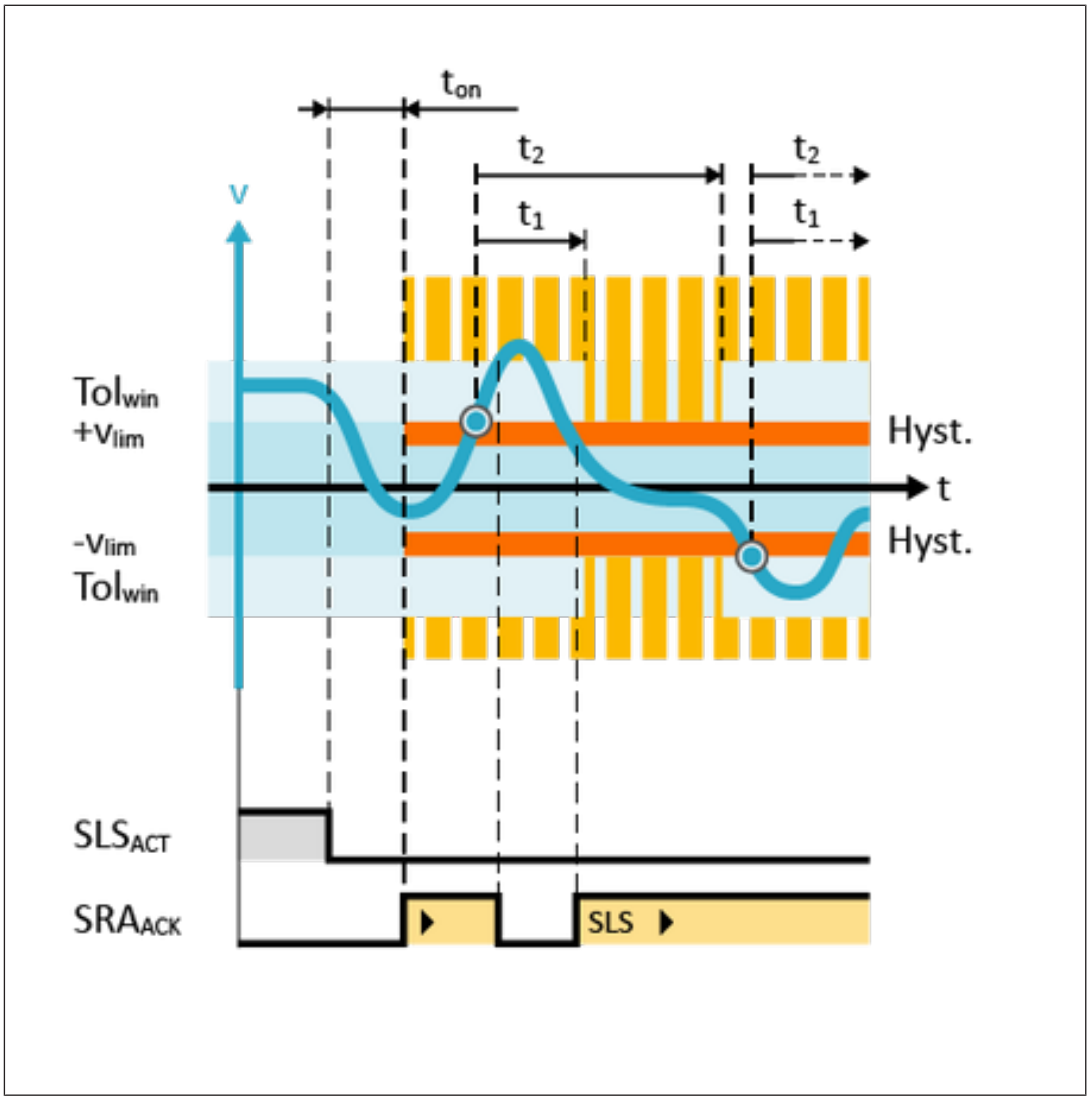


Fig.: Safety function SLS-M, with hysteresis monitoring behaviour

Legend

t_{on}	On-delay
t_2	Tolerance period
t_1	Tolerance time
Tol_{win}	Tolerance window
$+/-v_{lim}$	Speed limit value +/-
Hyst.	Hysteresis window
SLS_{ACT}	Activation input for safety function SLS-M
SRA_{ACK}	Safe range acknowledge Output for feedback from the safety function SLS-M

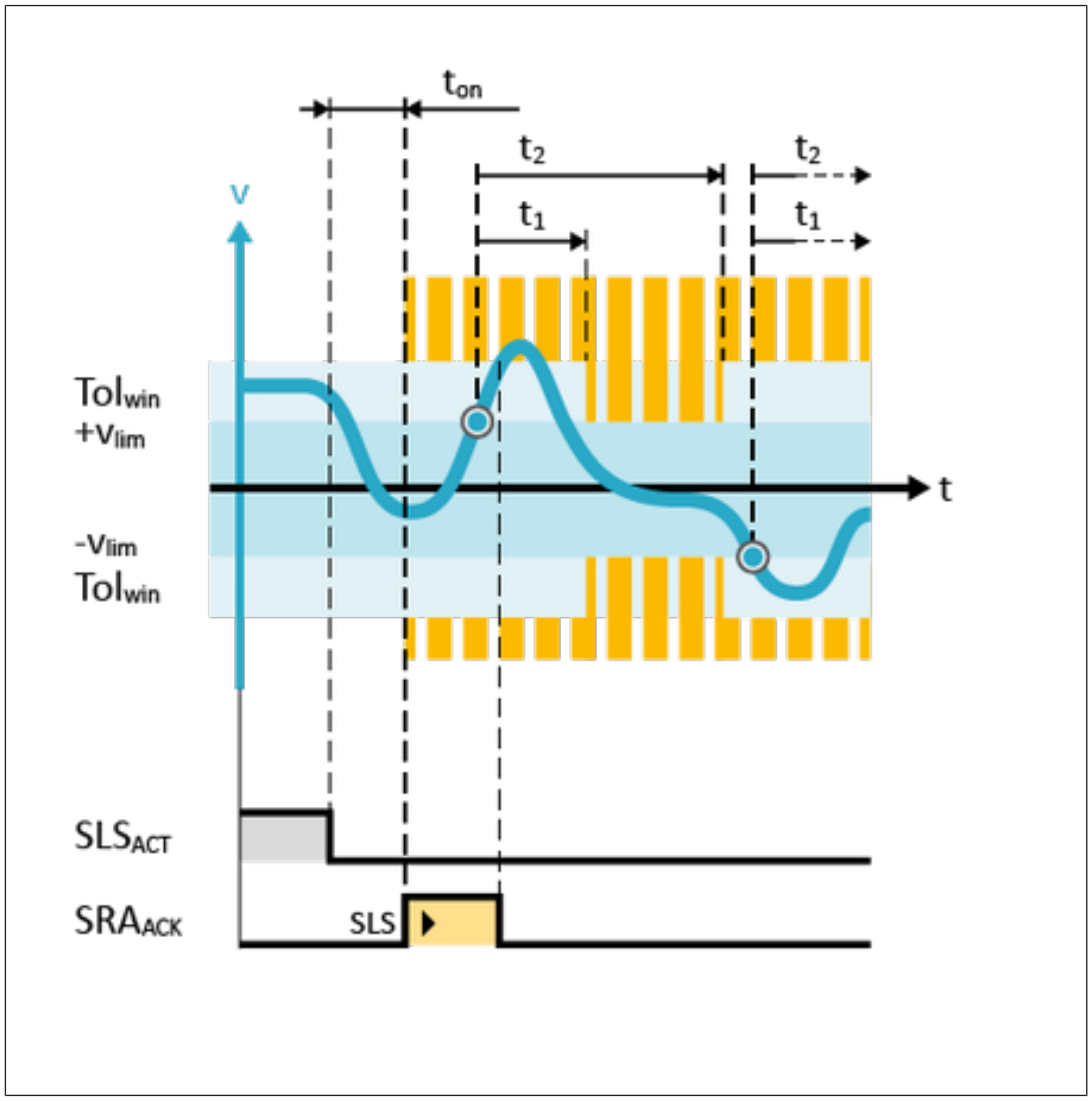


Fig.: Safety function SLS-M, with set/reset monitoring behaviour

Legend

t_{on}	On-delay
t_2	Tolerance period
t_1	Tolerance time
Tol_{win}	Tolerance window
$+/-v_{lim}$	Speed limit value +/-
SLS_{ACT}	Activation input for safety function SLS-M
SRA_{ACK}	Safe range acknowledge Output for feedback from the safety function SLS-M

5.13 Configuration

INFORMATION

The safety module is delivered unconfigured.
Before operation is possible, a configuration must be created and transferred to the safety module.

The safety functions that the safety module is to perform are defined in the safety configurator (PSC):

- Configuration of the safety functions required for safe motion sequences.
- Setting parameters for
  - Limit values
  - Brake ramps for the safety functions
  - Monitoring motion sequences
- The inputs and outputs of the safety functions are assigned to the user interface.

There are various ways of transferring the configuration.

Transfer of the configuration to the safety module

- Online from the configurator to the safety module (download)
- Transfer of the configuration from the drive controller's SD memory card to the safety module.

Transfer of the configuration from the safety module to the configuration tool

- Online, from the safety module to the configurator (upload)
- Offline, from a DriveControlSuite project to the configurator

In online mode it is possible to

- Display the safety module's operating states
- Display messages from the safety module (error stack)
- Download configuration from the PC to the safety module
- Upload configuration from the safety module to the PC
- The configuration is saved in the drive controller's remanent memory

The following security mechanisms are integrated

- Safe addressing of the safety module (identification of the safety module from the serial number)
- The feasibility of the configuration is checked during download and upload.
- Access to projects is password protected

- The configuration during download and upload is password protected
- Unique check sum(s) for the project

A PDF file can be created to **document** the project and all its settings (Report).

INFORMATION

Further information on the configuration and parameter settings for the safety functions is available in the safety module Configurator's online help.

6 Connection

INFORMATION

Information on how the brake outputs are connected can be found in the relevant manuals for the drive controller.

6.1 EtherCAT

The drive controllers have the two RJ45 sockets X200 and X201. The corresponding pin assignment and colour coding meet the standard EIA/TIA-T568B.

As an input, X200 is to be connected to the cable coming from the EtherCAT-MainDevice or the output of an upstream EtherCAT subscriber. As an output, X201 is to be connected to any subsequent EtherCAT subscribers.

INFORMATION

Further information on how to connect the EtherCAT subscribers can be found in the relevant manuals for the drive controller.

The maximum cable length between two EtherCAT/FSoE devices is 100 m.

The cable must conform to quality level CAT 5e as a minimum.

The following cables are suitable:

- Ethernet patch cable
- Crossover cable

7 Commissioning

7.1 Safety guidelines

When commissioning/recommissioning, please note the following:

- Secure the site in accordance with the regulations (barrier, warning signs etc.). The system may only be commissioned/recommissioned by qualified personnel.
- Please refer to the information and specifications stated in the operating manual of the relevant programmable control system.
- During commissioning/recommissioning, make sure that no personal injury and/or material damage can occur, even if the plant/machine moves unintentionally.
- When commissioning the safety module, please read the safety guidelines for the Drive controller.

WARNING!

Risk of electrocution!

- Never wire the electrical connections on Drive controller while voltage is applied.
- Switch off the mains voltages when working on the device installation!
- Make sure that the control cabinet is made safe, e.g. through an access lock or warning signs.
- Do not switch on the voltages until the system is commissioned!

WARNING!

Risk to life from the automatic start-up of the motor!

The motor can start moving immediately after configuration of the safety module if the Autostart option (parameter A34) has been set in the drive configuration:

- Appropriate measures should be taken so that the start of the machine does not create a hazardous situation.
  - after the safety module has booted
  - when recommissioning after a fault

INFORMATION

The safety function safe restart lock (SRL) can be used to prevent an unexpected automatic start-up of the motor, for example.

7.2 Initial commissioning

Requirements for commissioning

- The drive controller is ready for commissioning (see operating manual for the drive controller).
- The safety module must be included in the commissioning software for the drive controller.
- The serial number of the safety module is known. It can be read as follows via parameter S54 of the drive controller:
  - By calling up the parameter list in the commissioning software DriveControlSuite.

INFORMATION

During commissioning, the serial number must be confirmed in the safety configuration.

1. Connect safety module to the FSoE network

INFORMATION

Please note the guidelines given under Connection [📖 156].

- Connect the drive controller with integrated SX6 safety module to the EtherCAT/FSoE network.

INFORMATION

Do not switch on the supply voltage at this point.

2. Connect the configuration PC to the drive controller

- Connect the PC to the drive controller.

3. Switch on supply voltage

- Switch on all the supply voltages for the drive controller and the safety module.

You will know when the drive controller and safety module are ready for operation by the LEDs on the drive controller. A description of the status output of the safety module can be found under Display elements [📖 172].

⇨ The system starts up and boots (RUNUP).

Further information can be found under Operating states SX6 [📖 165].

The safety module switches to the state STO_FAULT.

INFORMATION

The safety module is provided by the factory without a safety configuration, thus the system stops booting when it has reached the fault state (STO_FAULT) during commissioning.

4. Start DriveControlSuite and configure safety module

- Start the commissioning software DriveControlSuite.
- Plan and configure your drive system.
  (More detailed information can be found in the commissioning manual for the drive controller.)

5. Configure safety module via PSC

INFORMATION

You will find additional useful recommendations and function descriptions for the safety functions in the online help of the configurator.

- In the project tree, highlight the drive controller with the safety module that is to be configured.
- Click on "  Safety configuration"
  - ⇨ The configuration tool PSC opens.
  - ⇨ In the configuration tool's Project Manager, select the safety module you wish to configure.
- The following basic settings for offline operation are mandatory:
  - – Define passwords
  - – Configure motor
  - – Configure the safety function SS1 Safe stop 1
  - – Assign inputs and outputs
- Additional configuration is optional.
  - – Define units
    (The units are independent of the drive controller's axis model.)

6. Download safety configuration

Prerequisites for downloading the safety configuration

- The corresponding safety configuration has been selected in the PSC.
- The safety configuration has been created and saved in offline mode.
- You have read the serial number for the safety module contained in parameter S54 via the parameter list for the DriveControlSuite.
- Establish a write online connection to the drive controller in the DriveControlSuite.
  - ⇨ Once the connection to the drive controller has been established, the safety configurations are compared. In the case of an initial commissioning, there can be no configuration present as yet, so PSC defines various safety configurations.
- Select ***Next***.
- Confirm the correct serial number for the safety module.
- Select ***Next.***
- Select ***Download.***
  - ⇨ The "Download completed successfully" window (green circle with tick) opens.
- Select ***Done.***

Further information on the download can be found in the safety module's online help.

7. Save configuration on the safe drive controller

- Save the configuration in the DriveControlSuite using the "Save values" assistant.
  - ⇨ The configuration is saved in the drive controller's remanent memory.

You have successfully transferred the configuration from the safety module to the drive controller and saved it.

8. Safety checks

Please refer to the section entitled Safety checks [📖 163].

7.3 Restarting after device replacement

The drive controller with safety module has been replaced with a new device.

The configuration stored on the SD card is to be installed on the new device.

INFORMATION

Precise information on recommissioning after a device has been exchanged can be found in the operating manual for the drive controller.

The most important steps for recommissioning are:

Insert the SD card into the new drive controller and switch on the drive controller

- Insert the SD card with the saved configuration into the drive controller.

- Switch on the 24 VDC supply voltage on the drive controller.

A deliberate action is required to intentionally transfer the safety configuration from the inserted SD card to the safety module. This action must be performed on the device during recommissioning. The procedure varies depending on the type of drive controller used.

Drive controller SC6/SI6

- If the "red double flash" pattern is displayed on the Err A LED (see Connection overview, using SC6A as an example [📖 8]), press the operator key S1 for 2 seconds. The purpose of "pressing for 2 seconds" is to intentionally transfer the safety configuration from the SD card and save it in the safety module. Please note that this transfer and the saving of the safety configuration on the safety module is a deliberate action.

NOTICE

Deliberate action!

By pressing the operator key S1 (see Connection overview, using SC6A as an example [📖 8]) for at least 2 seconds, you confirm the correct mapping of the safety configuration to the safety module.

Drive controller SB6

- If the red LED flashes twice, activation of the safety configuration begins. Press the operator key S1 within 30 seconds (see Connection overview, using SB6 as an example [📖 9]) and keep it pressed until the green LED flashes twice. Please note that this transfer and the saving of the safety configuration on the safety module is a deliberate action.

NOTICE

Deliberate action!

By pressing the operator key S1 (see Connection overview, using SB6 as an example [📖 9]) until the green LED flashes twice, you confirm the correct mapping of the safety configuration to the safety module.

Drive controller SB6 with the option OP6 (Display)

- If SAFETY ACTIVATION appears on the display, press the left and right arrow keys (see Connection overview, using SB6 as an example [📖 9]) for two seconds to activate the safety configuration. Please note that this transfer and the saving of the safety configuration on the safety module is a deliberate action.

NOTICE

Deliberate action!

By pressing the left and right arrow keys simultaneously (see Connection overview, using SB6 as an example [📖 9]) for at least 2 seconds, you confirm the correct mapping of the safety configuration to the safety module.

7.4 Safety checks

The safety module is a safety component in accordance with Annex V of the Machinery Directive. It guarantees functional safety against hardware and firmware errors, for example. However, it does not guarantee the safety of the overall process, nor of the configuration.

The machine manufacturer must check and verify the functionality of the employed safety functions.

- The safety function may only be checked by qualified personnel.

The safety function must be checked

- After initial commissioning
- After changing the configuration of the safety functions
- After exchanging the safety module or drive controller (e.g. when changing the motor type, motor encoder type or brake selection)

A full check comprises

- Proper execution of the safety functions used on the safety module
- Proper execution of the overall safety function (e.g. combination and integration of safety functions)
- Inspection of the parameters
- Examination of the overruns and safety distances of the plant/machine

NOTICE

When commissioning the plant/machine, loss of the motor encoder signal and the motor acceleration that may result should be simulated. This demonstrates that the calculated overrun and the resulting minimum distance of the plant/machine are adequate.

Basis for testing

- The requirements of the safety functions on the safety module, resulting from the risk analysis of the machine or process
- The description of the safety module and its safety functions in accordance with this operating manual
- All safety-related parameters and values of the employed safety functions

The result of the test must be documented in a test report. This report must contain the following:

- A description of the application, including a diagram
- A description of the safety-related components (including software versions) used by the application
- A list of the employed safety functions
- The results of all tests related to these safety functions
- A list of all safety-related parameters and their values
- Check sums, test dates and confirmation by the test staff

Safety tests conducted on equivalent applications may be carried out as an individual type test of the equivalent application, provided that it can be ensured that the safety functions are configured as intended for all devices. The CRC safety configuration can also be used here (see PSC tool: Information about the safety module).

INFORMATION

If any of the parameters for the safety functions have been changed, the check must be repeated and this must be recorded in the test report.

8 Safety module operation

Prerequisites for operating the safety module are:

- The safety module contains the configuration data
- FSoE communication is running

During operation

- Signal levels and edge changes at the safety function inputs are monitored.
- Safety functions are performed in accordance with the configuration.
- The switching capability of the hardware outputs is monitored.
- Self tests are carried out on the safety module constantly.

8.1 Operating states SX6

The safety module is always in a clearly defined operating state. This is based on the multi-axis device state and the axis states.

INFORMATION

Behaviour of the axis states in the STARTUP device state:
The safety module self-test is performed in the STARTUP device state during run-up (RUNUP) and restart (RESTART). During this time, the axis state of a drive axis remains in the STO state and only changes to the RUN axis state when the RUN device state is also achieved, following a successful self-test.

8.1.1 Device state

The device state is derived from the axis states (see Axis state [169]).

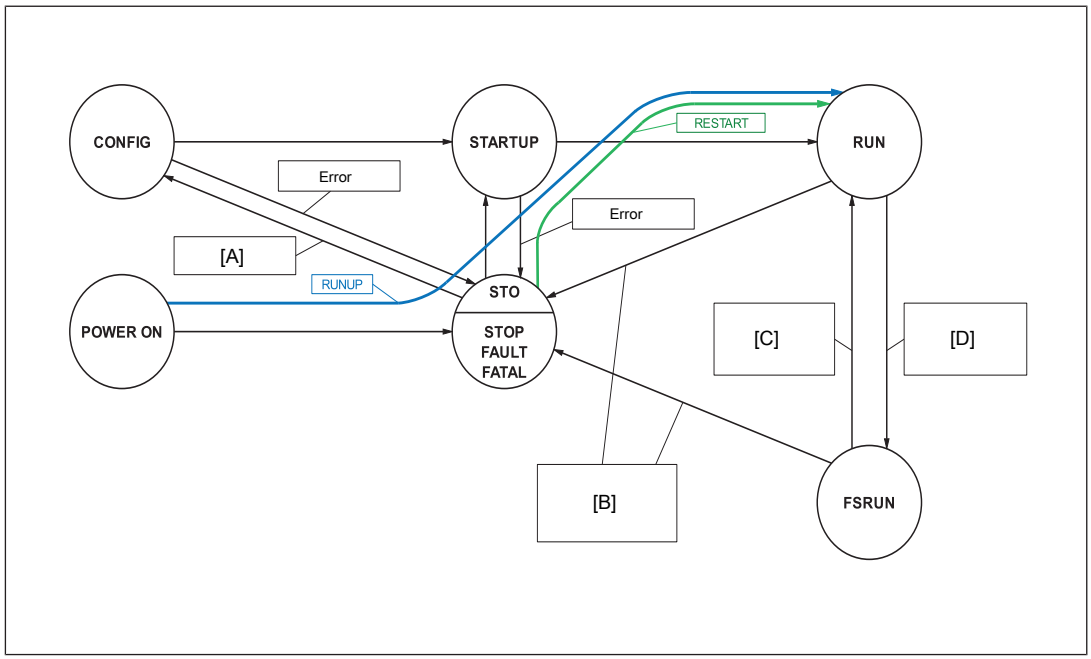


Fig.: Device state

Legend

[A] Configurator requirement

[B] Transition to STO when

- All axes are in the state STO
- When a fatal error occurs (see Error definition [26])

[C] No motion-monitoring safety function (SF) active

[D] At least one motion-monitoring safety function (SF) active

CONFIG	Transfer of the configuration to the safety module. The motor on all configured drive axes is switched to torque/force-free in the CONFIG operating state (STO is active). Transition to device state STARTUP: configuration downloaded without error Transition to device state STO: incorrect configuration data
POWER ON	Supply voltage is present on the device Transition to device state STO: once supply voltage is applied
STARTUP	Self-test of safety module is performed. Transition to device state STO: after error Transition to device state RUN: no error present

STO	**If all the configured drive axes are in the axis state STO, the device state will also be in STO.**
	The motor on all configured drive axes is switched to torque/force-free. Depending on the cause, the following (sub-)states are active:
	STOP – Stop Motor on all configured drive axes switched to torque/force-free through: ▸ Activation input SS1_ACT or ▸ Activation input STO_ACT (optional)
	FAULT – Error Motor on all configured drive axes switched to torque-free/force-free via the safety function SS1, as the result of an error reaction: ▸ Limit value violation ▸ Internal error through self-test
	FATAL – Fatal error Motor on all configured drive axes switched to torque-free/force-free via the safety function STO, as the result of an error reaction: ▸ Safety-critical error that requires shutdown of the entire device ▸ Internal software error
	Transition to device state CONFIG: after configuration request Transition to device state STARTUP: with RUNUP or RESTART
RUN (Normal operation)	**If at least one axis is in the axis state RUN and no axis is in FSRUN, the device state will also be in RUN.**
	Safety module in operation: no motion-monitoring safety function is activated Transition to device state STO: ▸ After a fatal error (FATAL) ▸ All drive axes in STO Transition to device state FSRUN: a motion-monitoring safety function on a configured drive axis is activated
FSRUN (Safe operation)	**If at least one axis is in the axis state FSRUN, the device state will also be in FSRUN.**
	Safe operation: at least one motion-monitoring safety function on a configured drive axis is activated Transition to device state STO: ▸ After a fatal error (FATAL) ▸ All drive axes in the axis state STO Transition to device state RUN: no motion-monitoring safety function is active

RESET	Action that triggers the RESTART (see Safe restart of the machine [📖 49]) (see Resetting (RESET) the safety module) (see Effects of RESET with safety function "Safe restart lock (SRL)" [📖 145])
RUNUP	Run-up (see Effects of run-up and configuration refresh with safety function "Safe restart lock (SRL)" [📖 146]
RESTART	Restart

INFORMATION

Motion-monitoring safety function

Motion-monitoring safety functions are all safety functions with the exception of SSO, SBC, SRL and SS1, if brake ramp monitoring is not configured.

8.1.2 Axis state

The axis state is derived from the states and transitions of the axis state machine.

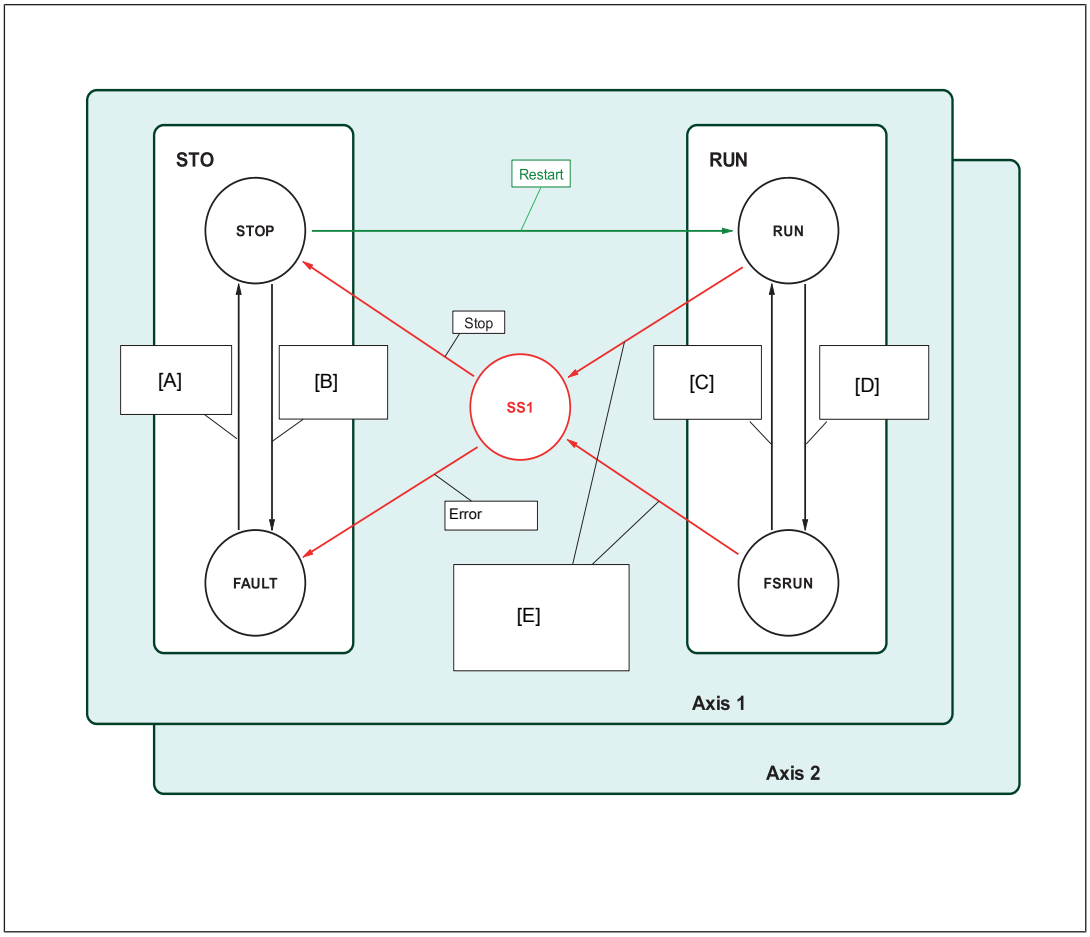


Fig.: Axis state

Legend

[A]	No error active	
[B]	Error active	
[C]	No motion-monitoring safety function (SF) active	
[D]	At least one motion-monitoring safety function (SF) active	
[E]	Activation of safety function SS1 with	
	Request via SS1_ACT/STO_ACT	STOP
	Request from a new configuration	STOP
	An error has occurred (global, axis-specific) See Error definition [📖 26]	FAULT

STO	The motor on the (assigned) drive axe is switched to torque/force-free. Transition to axis state RUN: RESTART requested Depending on the cause, the following (sub-)states are active:
	STOP Motor of the (assigned) drive axe is switched to torque/force-free due to: ▸ Activation input SS1_ACT or ▸ Activation input STO_ACT (optional) Transition to axis state FAULT: after error
	FAULT Motor on (assigned) drive axis switched to torque-free/force-free via the safety function SS1, as the result of an error reaction: ▸ Limit value violation ▸ Internal error through self-test (global error) Transition to axis state STOP: after error acknowledgement
RUN (Normal operation)	Safety module in operation: no motion-monitoring safety function is activated Transition to FSRUN state: a motion-monitoring safety function on the (assigned) drive axis is activated Transition to axis state SS1: after SS1 requested
FSRUN (Safe operation)	Safe operation: at least one motion-monitoring safety function on the (assigned) drive axis is activated Transition to axis state SS1: after SS1 requested Transition to axis state RUN: no motion-monitoring safety function on the (assigned) drive axis is active
RESTART	Restart
SS1	SS1 is executed on the (assigned) drive axis

INFORMATION

Motion-monitoring safety function

Motion-monitoring safety functions are all safety functions with the exception of SSO, SBC, SRL and SS1, if brake ramp monitoring is not configured.

8.2 RUNUP (booting)

After switching on, the safety module passes through the following device states:

POWER ON → STO → STARTUP → RUN

Once switched on (POWER ON), the system enters the STO safe state. The booting process continues automatically to the STARTUP state. During the STARTUP, the safety module carries out a self-test. Once this has been completed, the system automatically enters the RUN state.

During the runup, the system passes through the aforementioned states without user action.

8.3 RESTART

The safety module passes through the following states during the restart:

STO → STARTUP → RUN

INFORMATION

The safety module SX6 provides various optional configuration options for the restart.

The RESTART function can be optionally configured via the safety functions Safe Restart Lock (SRL) and Safe Stop 1.

Further information on the RESET can be found under
Safe restart of the machine [📖 49]
Resetting (RESET) the safety module [📖 50].
Safe restart interlock (SRL)

Restart in the event of STO-STOP

Perform a restart as follows:

- Switch the input SS1_ACT to 1-signal (positive edge)
  - ⇨ The safety module passes through the states STARTUP → RUN → FSRUN (depending on the configuration)

Restart in the event of STO-FAULT

Rectify the fault, noting the following:

- The error messages in the error stack

Perform a restart as follows:

- Switch the input SS1_ACT to 1-signal (positive edge)

or

- Execute the "QUITT" command on the drive controller, see under Resetting (RESET) the safety module [📖 50]

⇨ The safety module passes through the states STARTUP → RUN → FSRUN (depending on the configuration)

8.4 Display elements

The following LEDs, relevant for the safety module, are available on the drive controller:

- On the top of the drive controller
  - "STAT" LED and "STO/FS" LED to display the status of the safety module
- On the front of the drive controller
  - "FSoE" LED to display the status of the FSoE communication

8.4.1 Safety module LEDs

Two safety module LEDs to display the status of the operating states are visible on the top of the drive controller.

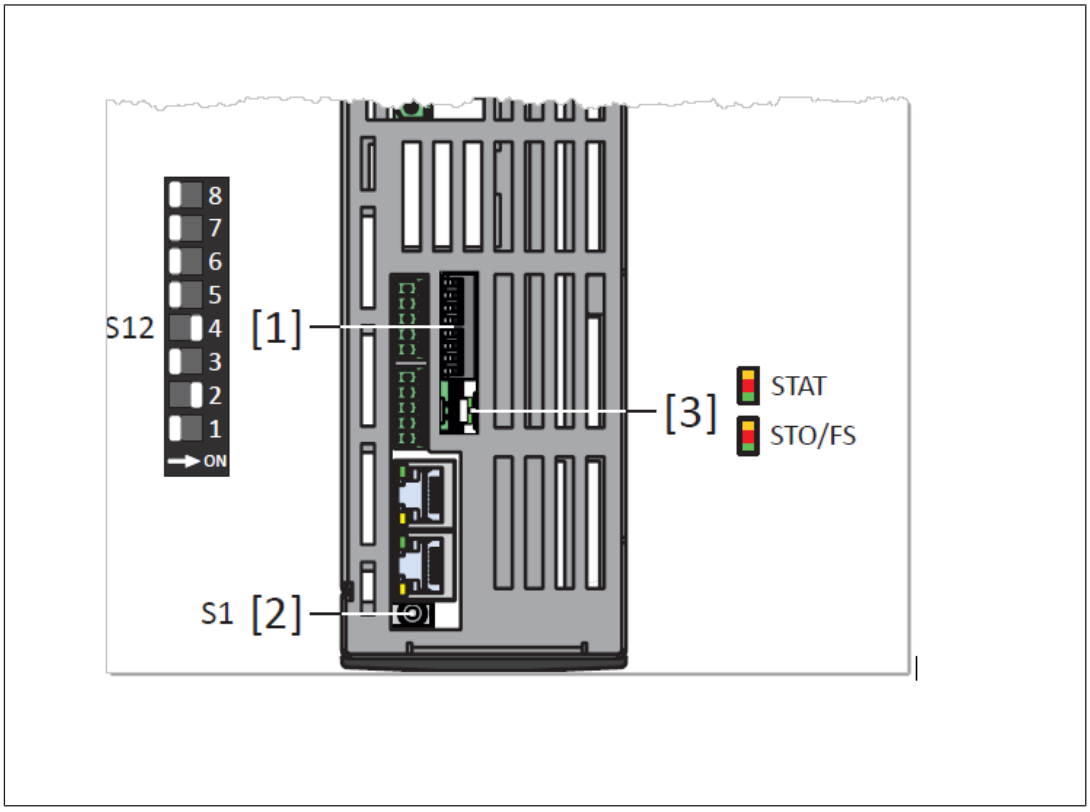


Fig.: Top of the drive controller SC6A, safety module LEDs by way of example

Legend

[1]	DIP switch for FSoE address
[2]	S1 operator key
[3]	**Safety module LEDs:**
	STAT
	STO/FS

Meaning of the "STAT" and "STO/FS" LEDs

LED			Device status/meaning
Name	Colour	Status	
STAT		 Off	Supply voltage is not present
	Green	 On	RUN (normal operation) STO-STOP FSRUN (safe operation)
	Green	 Flashes	RUN (start-up)
STAT	Red	 On	STO-FATAL
	Red	 Flashes	STO-FAULT
STAT	Yellow	 Flashes	CONFIG
STO/FS		 Off	Supply voltage is not present RUN (normal operation)
	Green	 On	FSRUN
STO/FS	Red	 On	RUN (start-up) CONFIG STO FAULT FATAL

Legend

 LED on

LED flashes

LED off

8.4.2 FSoE status indicator LED

The "FSoE" LED to display the status of FSoE communication is visible on the front of the drive controller. It provides information about the status of FSoE communication.

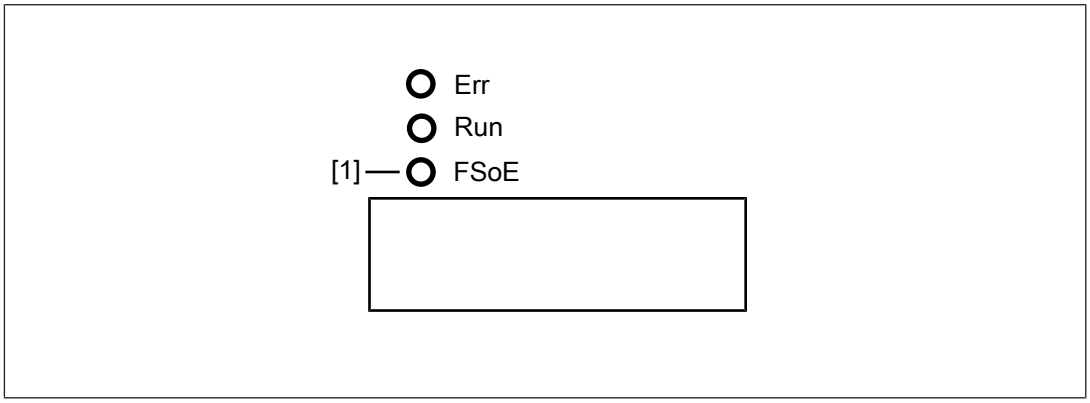


Fig.: Light emitting diodes on the front, drive controller SC6 by way of example

Legend

[1] Light emitting diode for FSoE status

Meaning of "FSoE" LED

LED FSoE	Colour	Meaning	Further information
	--	No communication	Status of communication is unknown or in initialisation state, invalid configuration
	Green	Establishment of FSoE communication Transfer of FSoE parameters	FSoE communication is established, FSoE parameters are transferred
(4 Hz)	Green	FSoE connection active FSoE connection in RESET state	FSoE SubInstance is ready for communication, but FSoE connection is still in RESET state
(2 Hz)	Green	Communication is active Process image empty	Communication with FSoE MainInstance is active, but no process data has been transferred yet
	Green	Communication is active	Communication with FSoE MainInstance is active and process data is being received/sent

Legend


LED on


LED flashes (2 Hz)


LED flashes (4 Hz)


LED flashes quickly


LED off

8.5 Messages

Information about safety module messages can be found in the manual of the respective drive controller.

The following options are available for detailed diagnostics and fault detection:

- LEDs on the top of the drive controller provide information about the operating states of the safety module, see Display elements [📖 172].
- Outputs on the safety module display the states of the safety functions (e.g. feedback output STO_ACK from the safety function SS1).
- Errors and messages are entered in the safety module's error stack.
- The following are displayed in the Configurator PSC in online mode:
  - Status messages for the safety module
  - Error messages for the safety module (error stack)

8.6 Diagnostic tests

- The safety module has a two-channel structure with internal diagnostic tests, thus no external safety system is required.
- The test functions for the safe, 2-pole hardware outputs are described under Safe 2-pole hardware outputs [📖 34].
- Forced dynamisation is mandatory for the encoder, see Motor encoder fault detection [📖 42]

9 Change, maintenance, decommissioning

9.1 Change

It may be necessary to change a process/machine because:

- A safety requirement has changed
- A systematic error has occurred
- There are new operational or production requirements
- The process cycle/machine has changed

Before changing a safe process/safe machine, a preparatory analysis must be carried out. The following effects must be analysed:

- How the changes will affect the safety of the process/machine
- How the changes will affect the safety functions of the safety module

The change requirements can be combined in a catalogue of

requirements. This should include:

- Detected hazards
- Desired changes
- Reason for the changes

The change should only be carried out by persons with the necessary knowledge and experience (competent persons).

INFORMATION

- Note the information about assembly/disassembly in the operating manual for the Drive controller.
- Following a change, if the safety analysis has shown that safety functions need to be validated and tested, the change itself must be tested, as must the course of the entire process. This must be taken into account for recommissioning.
- Please note the requirements for recommissioning after a change.

NOTICE

The check sums can be used to establish whether safety-related changes have been made and therefore whether safety functions need to be validated and tested. However, a comparison may only be used as an additional aid. Under no circumstances can it replace a prior safety analysis for the changes.

9.2 Maintenance

No maintenance work is necessary on a safety module SX6. Please return any faulty drive controllers with integrated safety module to Stöber.

9.3 Decommissioning

Note the mission time t_M stated in the safety-related characteristic data of the safety module.

Note the information about assembly/disassembly in the operating manual for the drive controller.

When decommissioning, please comply with local regulations regarding the disposal of electronic devices (e.g. Electrical and Electronic Equipment Act).

10 Field bus communication

Further information about the fieldbus connection can be found in the corresponding manual, see Further information [📖 13].

11 Technical details

Where standards are undated, the 2024-03 valid editions apply.

General	
Application range	**Failsafe**
Semiconductor outputs	
Galvanic isolation	**Yes**
Semiconductor outputs, 2-pole	
Number of dual-pole semiconductor outputs	**2**
Max. current at ambient temperature > 45 °C	**2,5 A**
Typ. output current at "1" signal and rated voltage of semiconductor output	**2,5 A**
Max. switching frequency	**0,5 Hz**
Residual current at "0" signal	**0,5 mA**
Short circuit-proof	**Yes**
Times	
Cycle time, processor system	**5 ms**
Delay time, pulse disabler	**1 ms**
Environmental data	
Climatic suitability	**EN 60068-2-1, EN 60068-2-14, EN 60068-2-2, EN 60068-2-78**
Ambient temperature	
in accordance with the standard	**EN 60068-2-1, EN 60068-2-14, EN 60068-2-2**
Temperature range	**0 - 55 °C**
Storage temperature	
in accordance with the standard	**EN 60068-2-1/-2**
Temperature range	**-40 - 70 °C**
Max. change	**20 K/h**
Climatic suitability	
in accordance with the standard	**EN 60068-2-78**
Humidity	**85 % r. h.**
Condensation during operation	**Not permitted**
Max. operating height above SL	**2000 m**
EMC	**EN 61800-3**
Vibration	
in accordance with the standard	**EN 60068-2-6**
Frequency	**10 - 57 Hz**
Amplitude	**0,075 mm**
Shock stress	
in accordance with the standard	**EN 60068-2-27**
Number of shocks	**3**
Acceleration	**50 m/s²**
Duration	**30 ms**

Environmental data	
Airgap creepage	
in accordance with the standard	**EN 61800-5-1**
Overvoltage category	**II**
Pollution degree	**2**
Mechanical data	
Dimensions	
Height	**15 mm**
Width	**76 mm**
Depth	**104 mm**
Weight	**35 g**

11.1 Safety characteristic data

The safety module carries out drive-related safety functions, as described in the EN 61800-5-2 standard, for example.

These safety functions generally only form part of an overall safety function that may consist of various subsystems.

The figure shows subsystems involved in the overall safety function as an example.

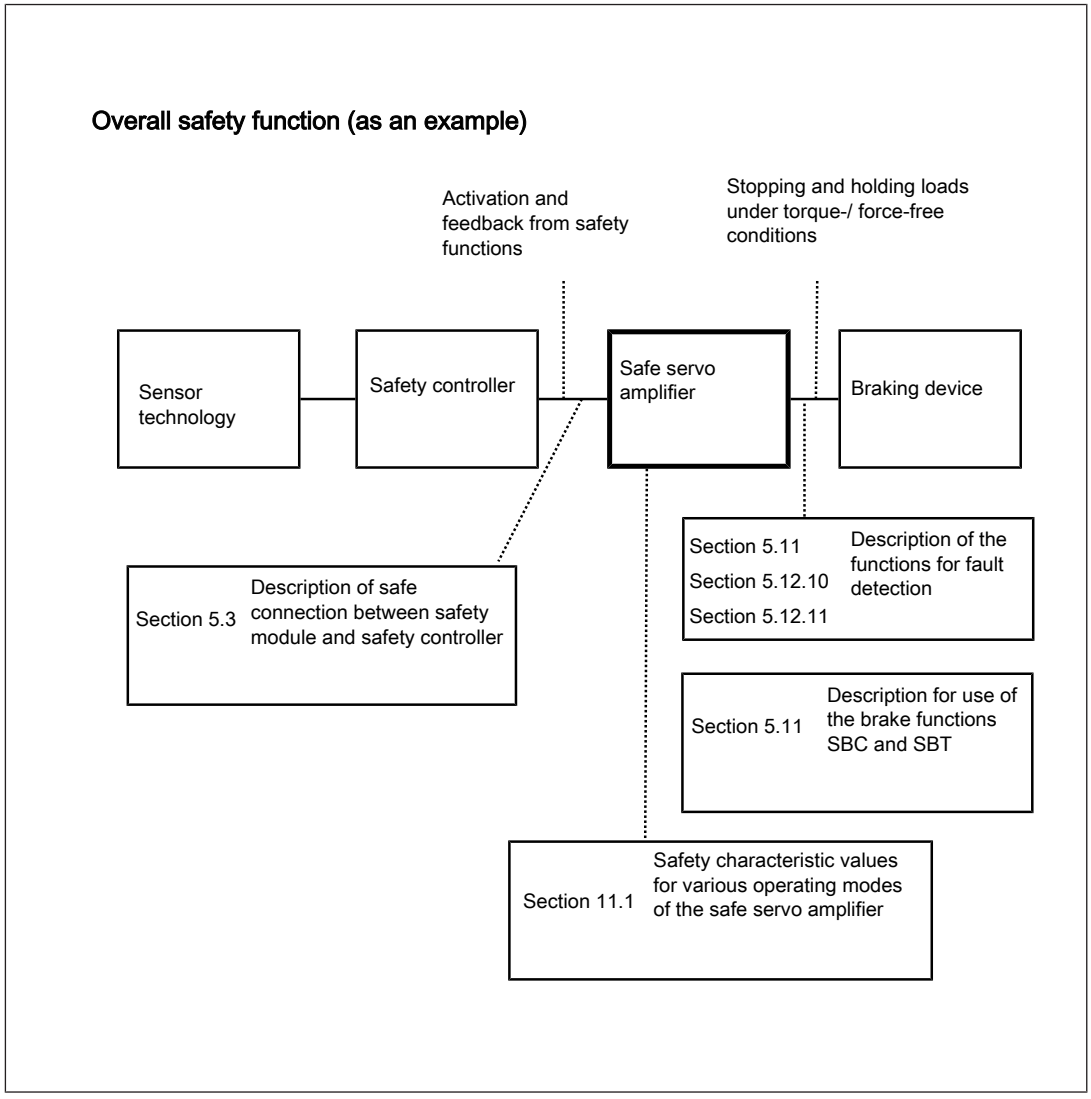


Fig.: Overall safety function and safety-related subsystems

A "safe drive controller" is a structural and functional unit consisting of

- a drive controller with integrated safety module SX6.

To determine the safety integrity of the overall safety function, this operating manual for the **safe drive controller** subsystem

- Describes the safety functions.
- Provides the safety characteristic values for various operating modes.

- Describes the test functions for error detection on other subsystems.

Operating modes

Various configurations of the **safe drive controller** subsystem are represented via the operating modes.

They differ in

- The MTTF values of the sensor technology for safe position detection.

A set of safety-related characteristic data is assigned to a combination of a safety function and an operating mode.

The operating modes differ with regard to the MTTF values of the sensor technology used for position detection

Safe speed and position values are processed for the safe motion/monitoring functions of the safety module. Fault detection takes place by cross-comparing two diverse sensors.

The following combination of sensors for safe position detection can be used:

- Motor encoder and internal system variables

See also under Motor encoder fault detection [📖 42]

To simplify the calculation, sensor combinations with assumed failure rates are included in the safety-related characteristic data. The following differences arise in the operating modes:

- Operating mode **Encoder MTTF ≧ 10a**
  - Motor encoder with MTTF ≧ 10 years and internal system variables
  - In accordance with EN ISO 13849-1, an $MTTF_D$ of ten years can be assumed for a component if no manufacturer data is available.
  - The mission time of the motor encoder must be T_M = 20 years.
- Operating mode **Encoder MTTF ≧ 57a**
  - Motor encoder with MTTF ≧ 57 years and internal system variables
  - The MTTF value of the encoder employed must be reviewed.
  - The mission time of the motor encoder must be T_M = 20 years.

Assuming that all faults are dangerous, $MTTF_D$ = MTTF can be set. The characteristic data MTTF is a property of the sensor, which can only be stated by the manufacturer.

Overview of operating modes and safety-related characteristic data

Operating mode	Description	Safety integrity Restrictions
Encoder MTTF ≧ 10a	▸ Position sensors possible in this operating mode – Motor encoder with MTTF ≧ 10 years and internal system variables ▸ Safety functions that can be used in this operating mode – Stop functions: STO, SS1, SS2 – Motion functions: SLS, SSR, SOS, SDI, SLI – Monitoring functions: SLS-M, SSR-M, SOS-M, SDI-M, SLI-M – Brake management: SBC – Other safety functions: SRL, SSO ▸ External interfaces that can be used in this safety function operating mode: – FailSafe over EtherCAT interface (FSoE) – 2 x safe output, 2-pole	SIL 2, PL d (Cat. 3) Limitation imposed by the failure rate of the encoder system
Encoder MTTF ≧ 57a	▸ Position sensors possible in this operating mode – Motor encoder with MTTF ≧ 57 years and internal system variables ▸ Safety functions that can be used in this operating mode – Stop functions: STO, SS1, SS2 – Motion functions: SLS, SSR, SOS, SDI, SLI – Monitoring functions: SLS-M, SSR-M, SOS-M, SDI-M, SLI-M – Brake management: SBC – Other safety functions: SRL, SSO ▸ External interfaces that can be used in this safety function operating mode: – FailSafe over EtherCAT interface (FSoE) – 2 x safe output, 2-pole	SIL 3, PL e (Cat. 4)

NOTICE

You must comply with the safety characteristic data in order to achieve the required safety level for your plant/machine.

Operating mode	EN ISO 13849-1 PL	EN ISO 13849-1 Category	EN IEC 62061 SIL CL/max. SIL	EN IEC 62061 61508 PFH [1/h]	EN/IEC 61511 61508 SIL	EN/IEC 61511 61508 PFD	EN ISO 13849-1 T_M [year]
FSoE, encoder MTTF ≥ 10a	**PL d**	**Cat. 3**	**SIL 2**	**3,84E-09**	**SIL 2**	**2,44E-04**	**20**
FSoE, encoder MTTF ≥ 57a	**PL e**	**Cat. 4**	**SIL 3**	**3,23E-09**	**SIL 3**	**1,95E-04**	**20**

All the units used within a safety function must be considered when calculating the safety characteristic data.

INFORMATION

A safety function's SIL/PL values are **not** identical to the SIL/PL values of the products used and may differ from these.

11.2 Classification according to ZVEI, CB24I

The following tables describe the classes and specific values of the product interface and the classes of interfaces compatible with it. The classification is described in the ZVEI position paper "Classification of Binary 24 V Interfaces - Functional Safety aspects covered by dynamic testing".

Safe 2-pole SC outputs

Source			Drain			
Safety module	D2		Brake	D2		

Parameter source	Min.	Typ.	Max.
Test pulse duration	150 µs	-	350 µs
Test pulse interval	600 ms	-	
Leakage current in OFF state	-	-	0,5 mA
Nominal current in ON state	-	-	2,5 A
Capacitive load	-	-	0,1 µF

Safe Brake Control (SBC)

Safety function in accordance with EN 61800-5-2: "The SBC function supplies a safe output signal or signals to drive a quiescent current-activated mechanical brake or brakes."

Safe Brake Test (SBT)

Supplementary safety function: The safety function SBT tests the proper functioning of a closed-current brake.

Safe Direction (SDI)

Safety function in accordance with EN 61800-5-2: "The SDI function prevents the motor shaft from moving in an unintended direction."

Safe Operating Stop (SOS)

Safety function in accordance with EN 61800-5-2: "The SOS function prevents the motor from deviating from the stop position by more than a defined amount. The PDS(SR) (electrical power drive system) supplies power to the motor that enables it to withstand the engagement of external forces."

Safe Restart Lock (SRL)

This supplementary safety function prevents uncontrolled start-up following a fault / interruption.

Safe Speed Range (SSR)

Safety function in accordance with EN 61800-5-2: "The SSR function holds the motor speed within defined limit values."

Safe Status Output (SSO)

Supplementary safety function: This is used for diagnostic purposes and provides the safe outputs with status information.

Safe Stop 1 (SS1)

Safety function in accordance with EN 61800-5-2: "The PDS(SR) performs one of these functions: a) Either initiates and controls the length of the motor delay within defined limits and initiates the STO function (see 4.2.2.2) if the motor speed falls below a defined limit value, or b) Initiates and monitors the length of the motor delay within defined limits and initiates the STO function if the motor speed drops below a defined limit value, or c) Initiates the motor delay and then initiates the STO function after an application-specific time delay."

Safe Stop 2 (SS2)

Safety function in accordance with EN 61800-5-2: "The PDS(SR) performs one of these functions: a) Either initiates and controls the length of the motor delay within defined limits and initiates the SOS function if the motor speed falls below a defined limit value, or b) Initiates and monitors the length of the motor delay within defined limits and initiates the SOS function if the motor speed drops below a defined limit value, or c) Initiates the motor delay and then initiates the SOS function after an application-specific time delay."

Safe Torque Off (STO)

Stop function in accordance with EN 61800-5-2: "No power that can cause a rotation (or in the case of a linear motor, a movement) is supplied to the motor. The PDS(SR) (electrical power drive system) does not supply any power to the motor that can generate torque (or in the case of a linear motor, force)."

Safely Limited Increment (SLI)

Safety function in accordance with EN 61800-5-2: "The SLI function prevents the motor shaft from exceeding the specified limit of position increment."

Safely Limited Position (SLP)

Safety function in accordance with EN 61800-5-2: "The SLP function prevents the motor shaft from exceeding the specified position limit(s)."

Safely Limited Speed (SLS)

Safety function in accordance with EN 61800-5-2: "The SLS function prevents the motor from exceeding the specified speed limit."

Safely Monitored Direction (SDI-M)

Supplementary safety function: The monitoring function SDI-M is based on the normative safety function SDI. Exceeding the parameterised limit values is reported but does not trigger any error reaction function.

Safely Monitored Position (SLP-M)

Supplementary safety function: The monitoring function SLP-M is based on the normative safety function SLP. Exceeding the parameterised limit values is reported but does not trigger any error reaction function.

Safely Monitored Speed (SLS-M)

Supplementary safety function: The monitoring function SLS-M is based on the normative safety function SLS. Exceeding the parameterised limit values is reported but does not trigger any error reaction function.

Safely Monitored Speed Range (SSR-M)

Supplementary safety function: The monitoring function SSR-M is based on the normative safety function SSR. Exceeding the parameterised limit values is reported but does not trigger any error reaction function.

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

24 h Service Hotline +49 7231 582-3000