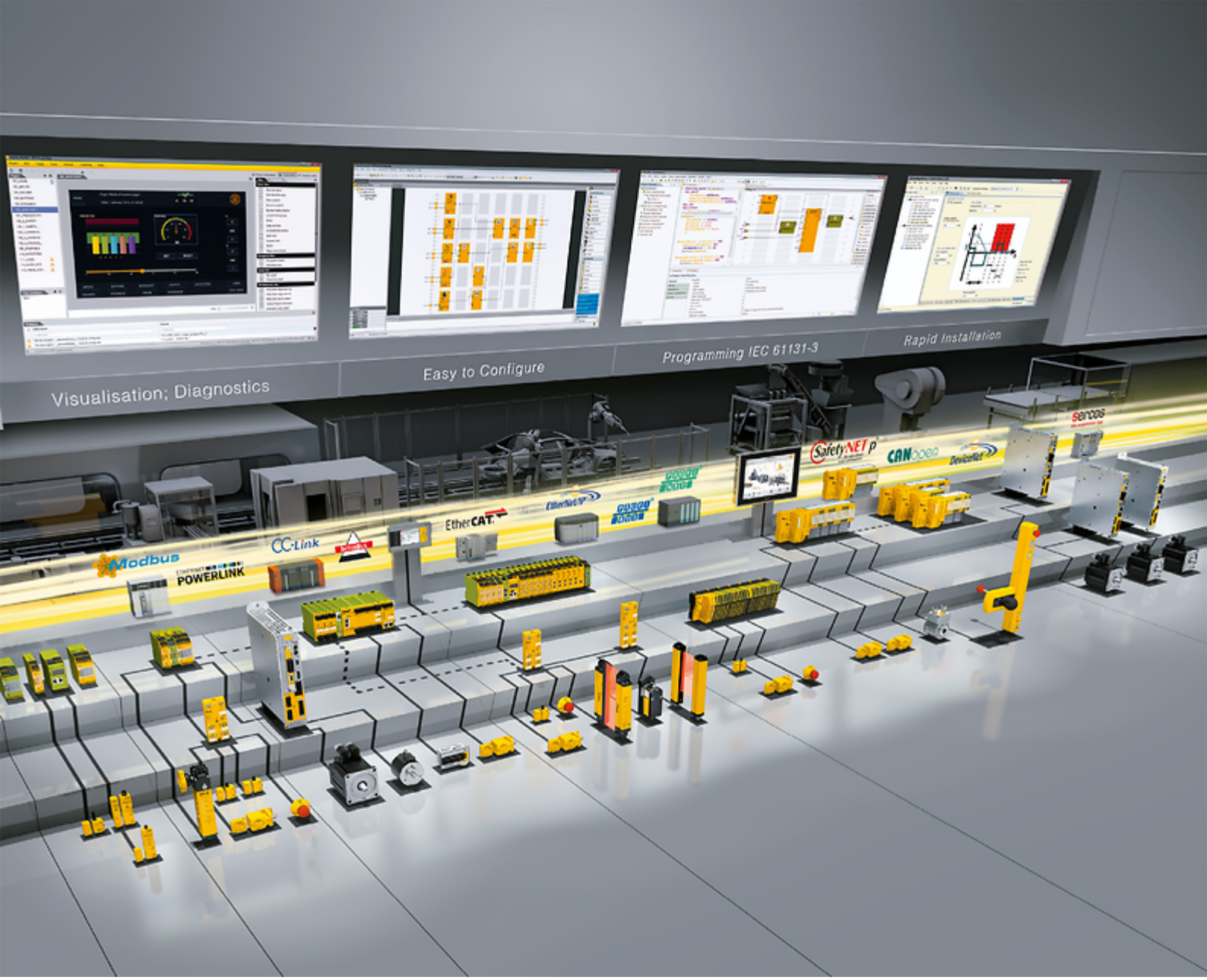


Safety module
PMCprotego S3.SN 8DI 6DO EI BR

PILZ
THE SPIRIT OF SAFETY

PMCprotego - Safe Motion

Operating Manual-1004379-EN-02

1 Introduction

1.1 Validity of documentation

The documentation is valid for the safety module PMCprotego S3.SN 8DI 6DO EI BR, hereafter called PMCprotego S3. It is valid until new documentation is published.

This operating manual explains the product's function and operation, describes the installation and provides guidelines on how to connect the PMCprotego S3.

Please refer to the following documents from the Motion Control range:

- The configuration of the safety module is described in the online help for the Configurator PASmotion.
- The servo amplifier PMCprotego D is described in the PMCprotego D operating manual.
- Details of how to set the parameters for the servo amplifier are described in the help for the commissioning software PASmotion.
- Optional: When using the safe communication system SafetyNET p RTFL
  - Operating manual PNOZ m EF SafetyNET
  - System description PNOZmulti

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

1.2 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.

1.3 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.

1.4 Third-party manufacturer licence information

This product includes Open Source software with various licences.

Further information is available in the document "Licence information PMCprotego S3.SN 8DI 6DO EI BR" (document number 1005866) at www.pilz.com.

2 Overview

The safety module PMCprotego S3 expands the Servo amplifier PMCprotego D by adding drive-integrated safety functions in accordance with EN 61800-5-2.

The safety module PMCprotego S3 is suitable for Servo amplifier from the product range PMCprotego D.

The following safety-related functions form part of the safety module PMCprotego S3:

- 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 safety functions of Servo amplifier:

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

2.1 Structure

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

2.2 Safety functions

The following safety functions form part of the safety module PMCprotego S3:

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

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

Safe movement function 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)
- Safely Limited Position (SLP)

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)
- Safely Monitored Position (SLP-M)

Safe brake functions

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

Other functions

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

Reaction functions

When a limit value violation or an internal error is detected, the safety module PMCprotego S3 triggers a reaction function. This switches off the motor and safely interrupts torque/ force generation.

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

2.3 Features

- 8 safe, single-pole hardware inputs, which can be freely assigned for the activation of safety functions.
- 6 safe, single-pole hardware outputs, which can be freely assigned the status of safety functions.
- 1 encoder interface for connection of an additional external TTL or SSI encoder. The encoder can be connected using a mini-IO.
- 2 safe, dual-pole hardware outputs for control of standby current-operated mechanical brakes.
- SafetyNET p RTFL interface (IN/OUT) with 32 inputs and 32 outputs for safe communication with a control system PNOZmulti 2 in a network with up to 16 subscribers. The safety module PMCprotego S3 can exchange data with max. 3 SafetyNET p subscribers.

The safety functions are allocated to the inputs and outputs (hardware or SafetyNET p) in the configuration tool of the safety module.

LED indicators for

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

2.4 Front view

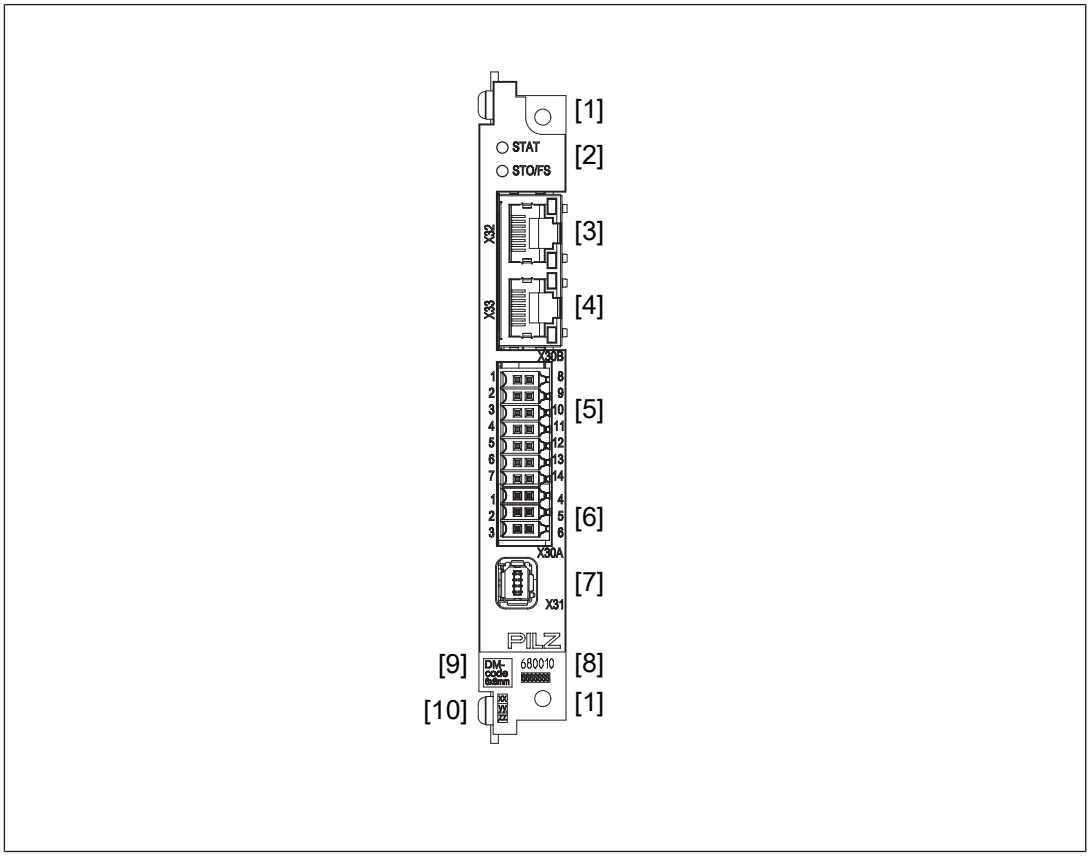


Fig.: Front view PMCprotego S3

Legend

[1] Mounting hole (screws are enclosed)

[2] LEDs to display operating states

[3] (X32) Communication: SafetyNET p RTFL (IN)

[4] (X33) Communication: SafetyNET p RTFL (OUT)

[5] (X30B) 8 hardware inputs, 6 single-pole hardware outputs

[6] (X30A) brake output 1 (SBC1+/-), brake output 2 (SBC2+/-), supply voltage for safety module, brake outputs and external encoders

[7] (X31) connection external encoder

[8] Order number

Serial number

[9] 2D code

[10] HW version (XX)

FW version (YY.ZZ)

3 Safety

3.1 Intended use

The Servo amplifier PMCprotego D with installed safety module PMCprotego S3 is a safety component in accordance with Machinery Directive 2006/42/EC Appendix IV and intended for use in safety-related applications.

The following conditions have been met:

- the EN 61800-5-2 requirements for drive-integrated safety functions
- the requirements of EN 62061 to SIL CL3
- the requirements of EN ISO 13849-1 to PL e (Category 4)

Intended use includes compliance with the

- operating manual Servo amplifier PMCprotego D.
- the online help function for the PASmotion configuration tool.
- EMC-compliant assembly and wiring.

The following is deemed improper use

- any structural, technical or electrical modification of Servo amplifier.
- use of Servo amplifier for applications other than those described in this operating manual.
- Use of the Servo amplifier contrary to the documented technical details (see "Technical Details" [📖 200]).

The safety module PMCprotego S3 may only be used in combination with the following servo amplifiers:

- PMCprotego D.01 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.03 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.06 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.12 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.24 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.48 from Version 1.6, Firmware ≥ 6.24
- PMCprotego D.72 from Version 1.6, Firmware ≥ 6.24

3.1.1 Permitted motor types

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

- Rotary synchronous motors
- Linear synchronous motors
- Asynchronous motors

INFORMATION

The operation of synchronous motors without a motor encoder (sensorless operation) is not permitted.

Please note the following fault detection guidelines:

When the drive is operated with a motor encoder (standard motor encoder on the servo amplifier), a fault on the encoder system is detected by the safety module as follows:

- **Rotary synchronous motors**

  Detected within one mechanical revolution of the motor.

- **Linear synchronous motors**

  Detected within the distance travelled, in accordance with the following formula:

  Distance = (Number of poles /2) · Pole pair pitch

  Commands in the servo amplifier:

  – Number of poles: MPOLES

  – Pole pair pitch: MPITCH

3.1.2 Approved motor encoders

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

Motor encoder	Encoder type (parameter FBTYPE) in the servo amplifier's commissioning software	Connection to the servo amplifier
Resolver	0	X2
Hiperface (Stegmann)	2	X1
EnDat (Heidenhain)	4	X1
SinCos 5 V with W&S	7	X1
SinCos 12 V with W&S	8	X1
RS422 24V	12	X3
ROD 5 V with Hall	15	X1
ROD 24V with W&S	16	X3
ROD 5V with W&S	17	X1
BiSS encoder 5 V - digital	20	X1

Motor encoder	Encoder type (parameter FBTYPE) in the servo amplifier's commissioning software	Connection to the servo amplifier
BiSS encoder 12 V - digital	22	X1
SSI	25	X1
SSI - Linear encoder	26	X1
ROD 5V	27	X1
EnDat 2.2 with 5 V	32	X1
BiSS-C encoder 5 V - digital	33	X1
EnDat 2.2 with 12 V	34	X1
Hiperface DSL (performance and feedback in a cable)	35	X1
SFD 3 (performance and feedback in a cable)	36	X1
BiSS-C encoder 12 V - digital	37	X1

3.1.3 Approved external encoders

NOTICE

To guarantee the diversity and to prevent common cause failures (CCF) the external encoder must not be from the same manufacturer as the motor encoder (take care with badged products!).

Approved external encoders
SSI
TTL

Connection to the safety module PMCprotego S3 is via X31.

For further information about wiring, see External encoder [📖 165].

For further information about the use of external encoders, see Motor encoder fault detection [📖 45].

3.1.4 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 [📖 136] (SBT).

3.2 Safety regulations

3.2.1 Additional documents that apply

Please read and also take note of:

- The configuration of the safety module PMCprotego S3
  - In the Online help of PASmotion
  - in the PNOZmulti Configurator Online help (optional)
- The operating manuals
  - PNOZmulti 2, base unit PNOZmulti m B0, PNOZmulti m B1 (optional)
  - PNOZmulti m EF SafetyNET (optional)
- The operating manual of the servo amplifier PMCprotego D
- The "Safety module PMCprotego S3 - Diagnostics" document

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

Further information, software packages and operation manuals available on the Internet at www.pilz.com

3.2.2 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 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 PASmotion configuration tool. Pay special attention when configuring the project and observe local standards and regulations (see also Safety checks [📖 184]).

3.2.3 Use of qualified personnel

The products may only be assembled, installed, programmed, commissioned, operated, maintained and decommissioned 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. To be able to inspect, assess and operate devices, systems and machines, the person has to be informed of 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.

3.2.4 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.).

3.2.5 Disposal

- In safety-related applications, please comply with the mission time T_M 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 PMCprotego S3 has various functions for error detection, with a detected error always resulting in a defined error reaction.

The error types are described in chapter Operating states [📖 187].

Error detection and error reaction are described in the sub-chapters of chapter Function description [📖 21].

3.4 Data backup and data security

Various data security mechanisms are used for the safety module PMCprotego S3. 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 for the configurable safety module PMCprotego S3

The safety module PMCprotego S3 has the following technical and organisational data security measures:

- Assignment of various access permissions for a configuration in the PASmotion 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 PASmotion).
- Detection of different configuration
  A check sum (= "check sum safe") is included when a configuration is downloaded. Different configurations can be detected based on this information.
- Detection of a deviating check sum on the SD memory card of the servo amplifier and in the flash memory when restarting a safety module
- Detection of an invalid configuration when restarting a safety module
- Detection of faulty or incompatible configurations when restarting the safety module

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. We therefore recommend that you install the product in a lockable control cabinet.
- 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.
- Assign only safe passwords. When assigning passwords, please note:
  - The password should have at least 8 characters.
  - The password should contain upper and lower case characters, as well as special characters and numbers.
  - If possible, the password should not be available in dictionaries.
  - The password should not be made up of standard variants and repetitions or keyboard patterns (so not: 1234abcd).
  - Use a password manager for optimum management of complex passwords.
  - Language-independent characters are not available in every keyboard language.
  - Make sure you regularly change the passwords of the user accounts on the system and/or ask the users to change their passwords themselves.
  - Make the users aware of the responsible use of their access data.
- Assign different permissions for the various user groups (e.g. diagnostics - configuration).

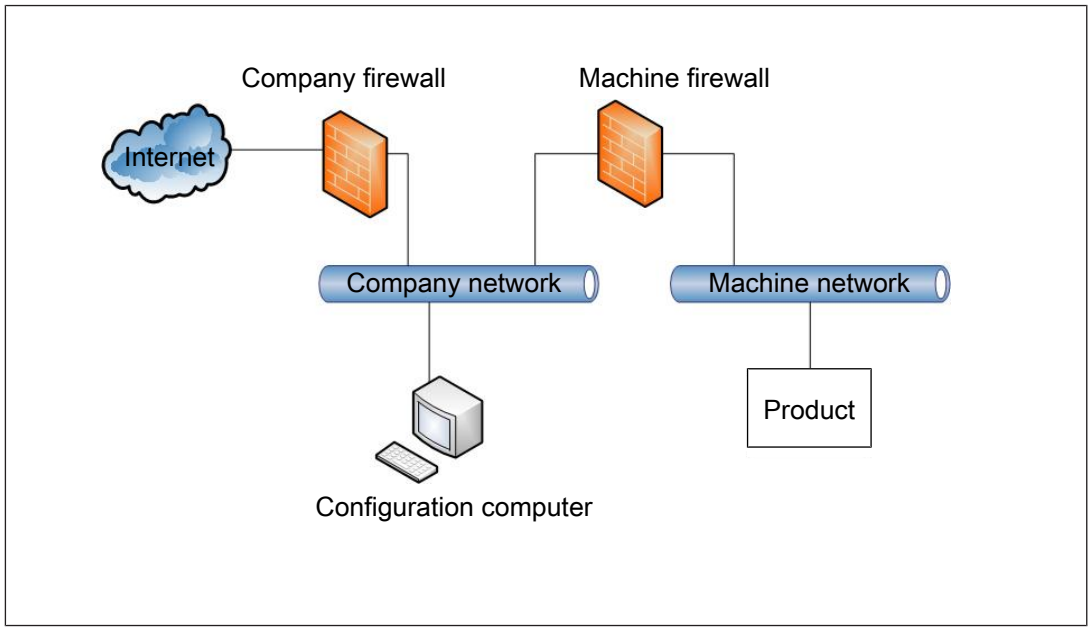


Fig.: Example network topology

5 Function description

5.1 Overview

The safety module PMCprotego S3 is installed in the Servo amplifier PMCprotego D. The combination of Servo amplifier with an integrated safety module is referred to as a safe Servo amplifier hereafter.

A **safe drive system** consists of:

- a safe Servo amplifier.
- a motor with motor encoder.
- an external encoder (optional).
- standby current-activated mechanical brakes (standard or safety components, optional).
- a programmable safety system.
- a configuration tool (PASmotion).

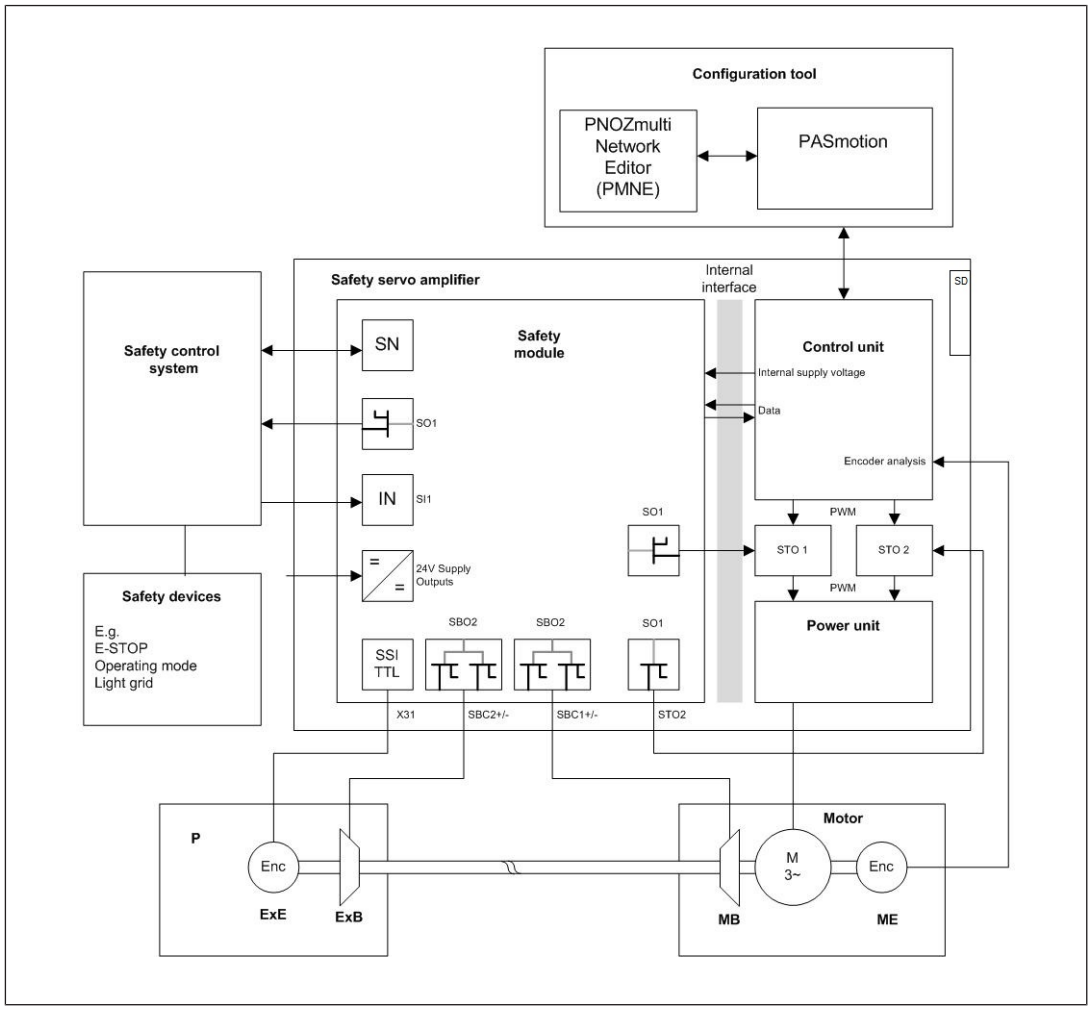


Fig.: Safe drive system

Legend

SN	SafetyNET p RTFL
SD	Card slot for SD card in the servo amplifier
SO1	Safe 2-pole STO controls
SI1	Safe 1-pole input
SBO2	Safe 2-pole brake output
STO1	Safe pulse lock 1
STO2	Safe pulse lock 2
PWM	Pulse width modulation
P	Driven installation
ExE	External encoder
ExB	External brake
MB	Motor brake
ME	Motor encoder
(PMNE)	PNOZmulti Network Editor, configuration tool for SafetyNET p RTFL (optional)

PASmotion	Configuration tool for servo amplifier and safety module

The safety module PMCprotego S3 (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 the limit values and triggers a response function when a limit value was violated.
- signals the status of safety functions to the programmable safety system.
- activates controlled shut-down by the Servo amplifier (optional) for the SS1 and SS2 safety functions.
- activates the integrated safe pulse lock on request or in the event of an error.
- has an option for safe triggering of up to two standby current-activated, mechanical brakes.
- detects faults in the mechanical brakes by means of a brake test.
- has a connection for an optional, external encoder.
- detects faults (cross-wire fault, short circuits) in the wiring of the output signals and initiates an error reaction.

The safe servo amplifier

- interrupts the torque/power generation by the motor when the pulse lock is activated.
- brings the motor to a standstill when the SS1 or SS2 safety function is activated.
- transfers the configuration data from the configuration tool to the safety module.
- stores configuration data on a removable data medium (SD memory card).
- reads the error memory of the safety module and provides detailed status information.

The programmable safety system

- evaluates signals from safety devices, such as:
  - Emergency stop pushbuttons
  - Safety gates
  - Light barriers
  - Two-hand pushbuttons
- activates the safety functions via inputs on the safety module (optional).
- processes safe feedback outputs of the safety module (optional).
- detects faults (cross-wire fault, short circuits) in the wiring to the safety module and initiates an error reaction (optional).

The PASmotion configuration tool

- configures and parametrises the safety module.
- ensures safe uploading and downloading of the configuration file.
- displays the status of the inputs/outputs (hardware or SafetyNET p) in the online display.
- displays the error stack.
- saves the configuration to an SD card.

The configuration tool PNOZmulti Network Editor

- configures the SafetyNET p RTFL network.
- defines the Bit mapping of the network subscribers.
- sends the network configuration to the configuration tool PASmotion.

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!

Potential loss of safety function due to 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 rotation/movement direction of the motor (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

- Definition of internal error
  An internal error is an error that occurred in the system and could not be removed by the user.
- Fault definition: STOP, FAULT, FATAL and "movement monitoring safety function"
  see Operating states [📖 187]

5.2.4 Naming of inputs and outputs

Hardware inputs and hardware outputs are digital inputs and outputs that can be connected via terminals.

In the Technical details chapter, the hardware outputs are also named semiconductor outputs.

SafetyNET p inputs and SafetyNET p outputs are part of the safe communication system SafetyNET p RTFL. The states of the inputs and outputs are transferred as Bits.

In the configuration tool PASmotion the activation input ACT is linked to a hardware input (IO) or a SafetyNET p input (SNp). The feedback output ACK is linked to a hardware output (IO) or a SafetyNET p output (SNp).

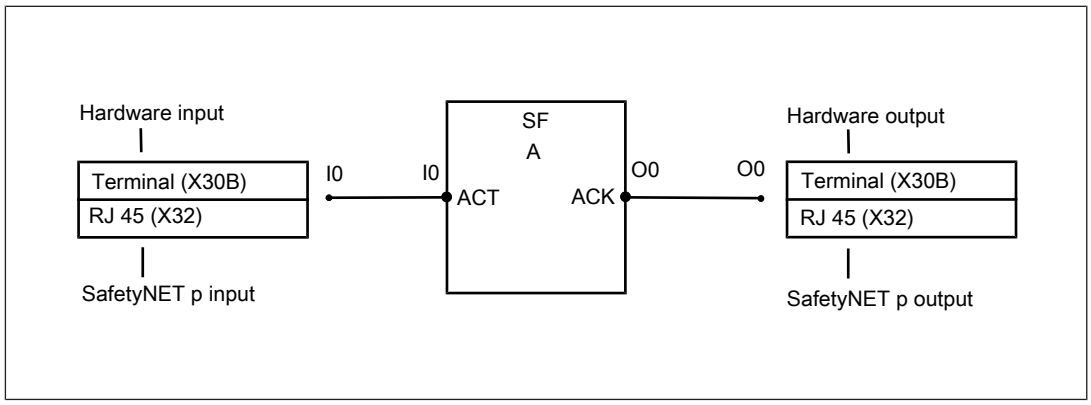


Fig.: Naming of inputs and outputs

Legend

SF	Safety function
ACT	Activation input
ACK	Feedback output

5.3 Activation and feedback on safety functions

The safety functions of the safety module PMCprotego S3 are activated or deactivated by evaluating the signal levels on the safe inputs. These inputs operate in accordance with the standby current principle. The programmable safety system activates the safety functions via a 0 signal.

The states/status of the safety functions of the safety module PMCprotego S3 can be reported via outputs to the programmable safety system.

5.3.1 Activation of the safety functions via hardware inputs

The safe hardware inputs of the safety module detect NO errors in the wiring.

One of the following measures must be applied to ensure safe connection between the programmable safety system and the safety module:

- Error detection by tested control signals and shutdown in the event of an error by a second shutdown route.
- Error elimination for short circuit between any of two conductors according to EN ISO 13849-2, Table D.4.
- Error detection through feedback of status signals of the safety module and shutdown in the event of an error by a second shutdown route.

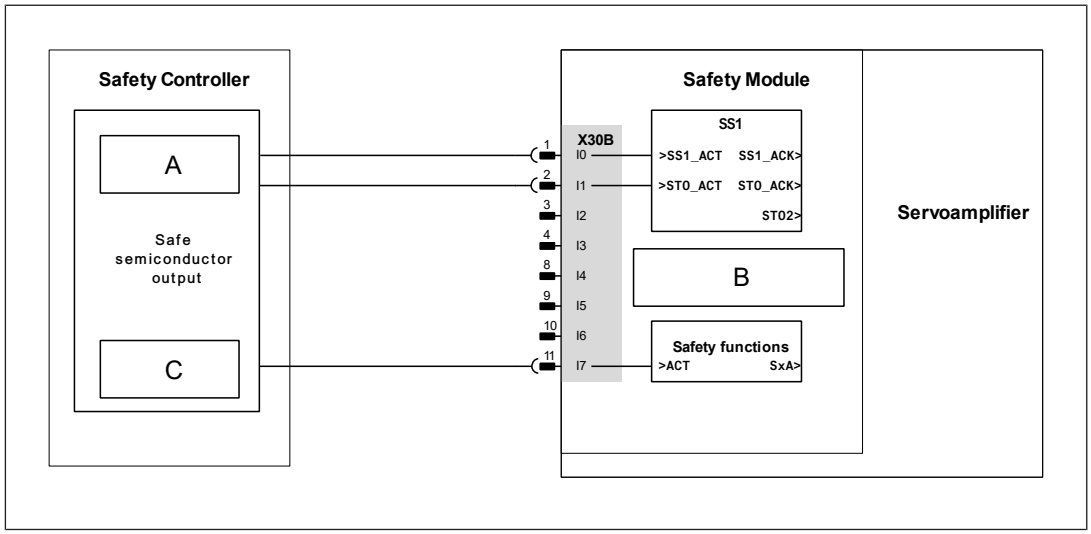


Fig.: Activation of a safety function with fault detection by testing

Legend

A Error detection by tested control signals (OSSD) and shutdown in the event of an error by the STO_ACT second shutdown route.

B The safe hardware inputs of the safety module detect NO errors in the wiring.

C Error detection with tested output signal switching device (OSSD) and shutdown by the SS1 function in the event of an error.

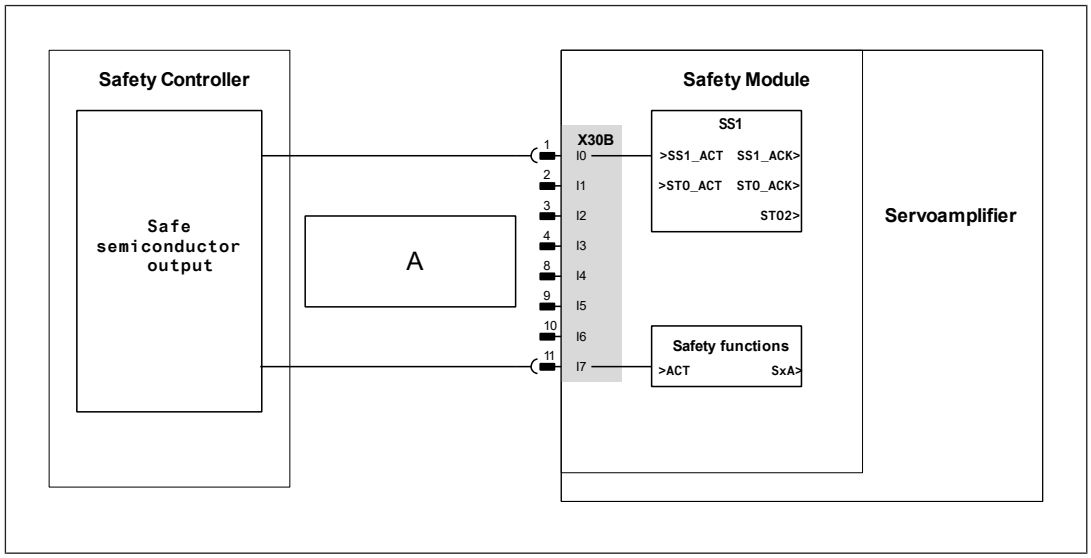


Fig.: Activation of a safety function with fault exclusion

Legend

A Error elimination for short circuit between any of two conductors according to EN ISO 13849-2, Table D.4.

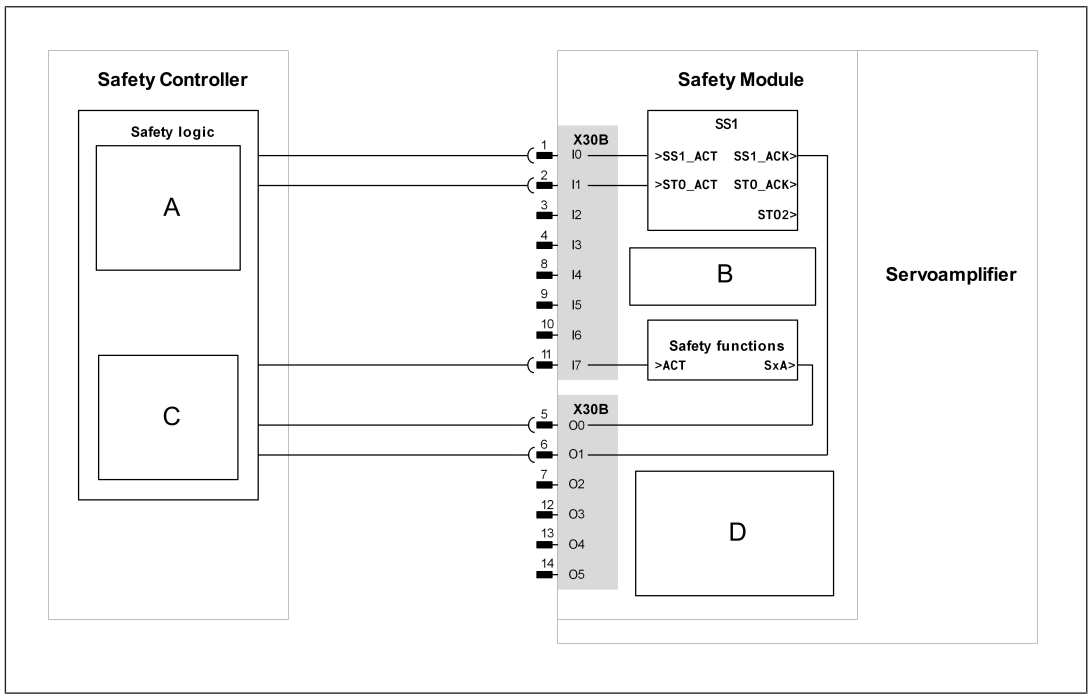


Fig.: Activation of a safety function with fault detection by feedback

Legend

A Error detection by evaluating the SS1_ACK signal in the higher-level controller and shutdown by a second, STO_ACT shutdown route in the event of an error.

B The safe hardware inputs of the safety module detect NO errors in the wiring.

C Error detection by evaluating the SxA signal of the activated safety function in the higher-level controller. Shutdown by the SS1 function in the event of an error.

D The safe hardware outputs of the safety module detect errors in the wiring. The SS1 safety function is activated and the motor is shut down when an error is detected.

5.3.2 Feedback of the safety functions via hardware inputs

The states/status of the safety functions of the safety module PMCprotego S3 can be reported via safe hardware outputs to the programmable safety system.

- 1 signal at the exit of the safety function means:
  - the safety module reports a safe state (depending on the respective safety function).
- 0 signal at the exit of the safety function means:
  - the safety function is not active, or
  - the allocated safety function has detected a dangerous state or
  - the output has not been assigned to a safety function.

Fault detection in wiring

Detecting the safe hardware outputs of the safety module:

- Short circuits to 24 V_{DC}
- Short circuits to 0 V
- Shorts across contacts

The motor is safely shut down by the SS1 safety function when an error is detected.

- a 1 signal is issued at the SS1_ACK output.
- A 1 signal is put on the STO_ACK output when the motor has been safely switched to a torque-/power-free state, see Safe stop 1 (SS1) [📖 84].

Fault prevention and fault detection during overvoltage

CAUTION!

Loss of safety

Overvoltage > 40 V in the connection between safety module and programmable safety system can lead to loss of safety. Feeding overvoltage in the programmable safety system to the 1-pole hardware outputs of the safety module may cause switched-off hardware outputs to provide a 1 signal.

- Use a power supply with overvoltage protection for the output voltage for the programmable safety system.
- Limit the output voltage to a max. of 40 V.

Measures for fault detection and triggering of fault reactions:

- The safety module detects overvoltage and triggers the SS1 safety function as an error reaction. The safety module changes to the STO operating status.
- The defective programmable safety system must recognise the error and switch to a safe condition.

Additionally required error detection when coupling a safety module with several programmable safety systems:

When the safe hardware outputs of the safety module are distributed over several, independent programmable safety systems,

- the STO-ACK output must be evaluated for each programmable safety system.
- a plausibility check of the STO_ACK signal with the respective feedback signals must be performed for each programmable safety system.

An error due to overvoltage is given when the Acknowledge output (SxA) and the STO_ACK output provide a 1 signal at the same time.

One of the following measures must be applied to ensure safe connection between the programmable safety system and the safety module:

- Error elimination for short circuit between any of two conductors according to EN ISO 13849-2, Table D.4.
- Evaluation of a second, additional feedback signal (STO_ACK) by the programmable safety system.

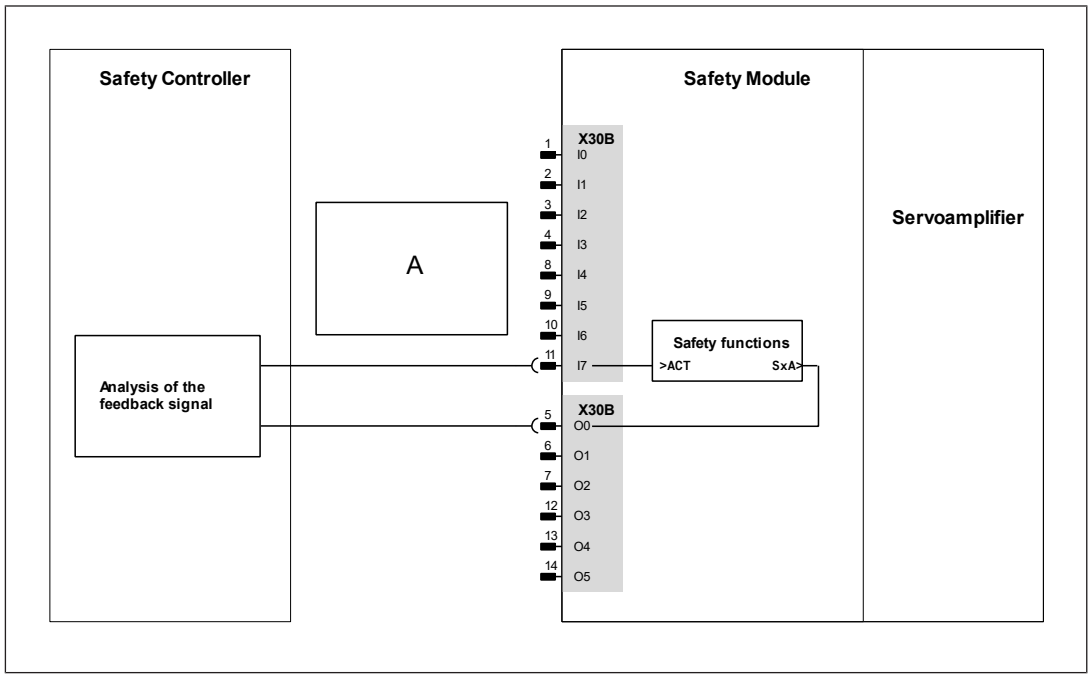


Fig.: Feedback on safety functions with fault exclusion

Legend

A Error elimination for short circuit between any of two conductors according to EN ISO 13849-2, Table D.4

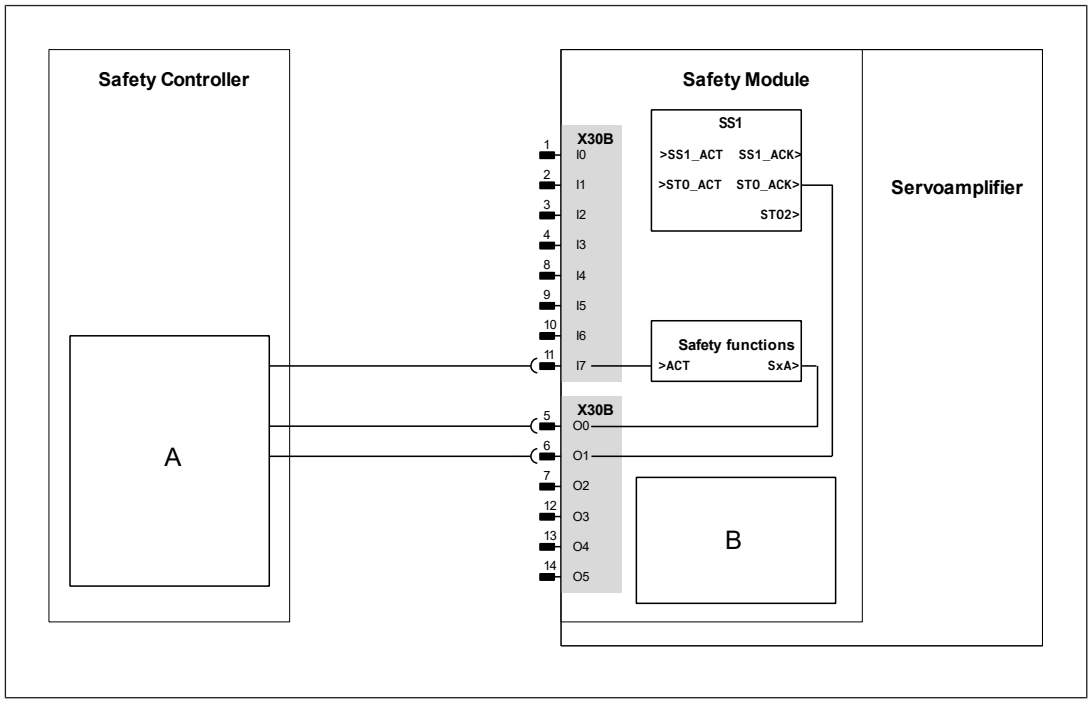


Fig.: Feedback from safety functions with evaluation of a second, additional feedback signal

Legend

A Evaluation of the feedback signal SxA of the safety function.

Error detection by the safe hardware outputs of the safety module shuts down the motor by activating the SS1 function and activates the STO. This is detected by the safety controller by evaluation of the STO_ACK signal.

B The safe hardware outputs of the safety module detect errors in the wiring.

The SS1 safety function is activated and the motor is shut down when an error is detected.

5.3.3 Activation and feedback of safety functions via SafetyNET p

To ensure safe connection between the safety controller and the safety module via the communication system SafetyNET p RTFL, the following feature applies:

- Safe transfer is ensured by the communication system SafetyNET p RTFL

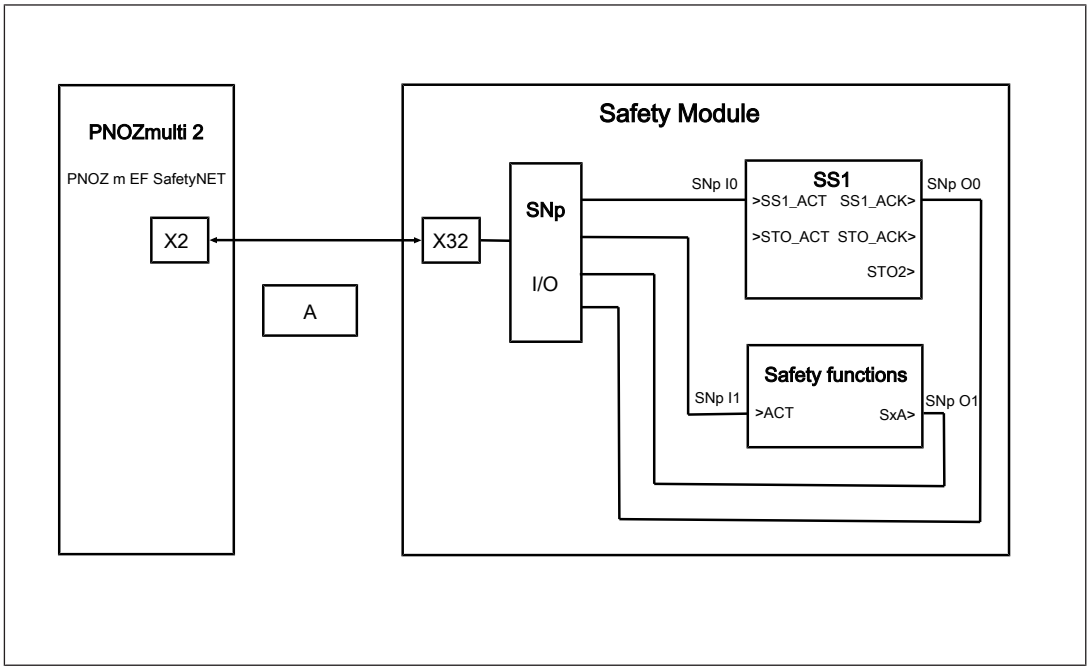


Fig.: Activation and feedback of a safety function via SafetyNET p

Legend

A	Error detection using the communication system SafetyNET p RTFL and switching-off using the safety function SS1 of the safety module

5.4 Hardware inputs/outputs

The safety module has

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

Hardware inputs and outputs are assigned to the safety functions in the configuration tool.

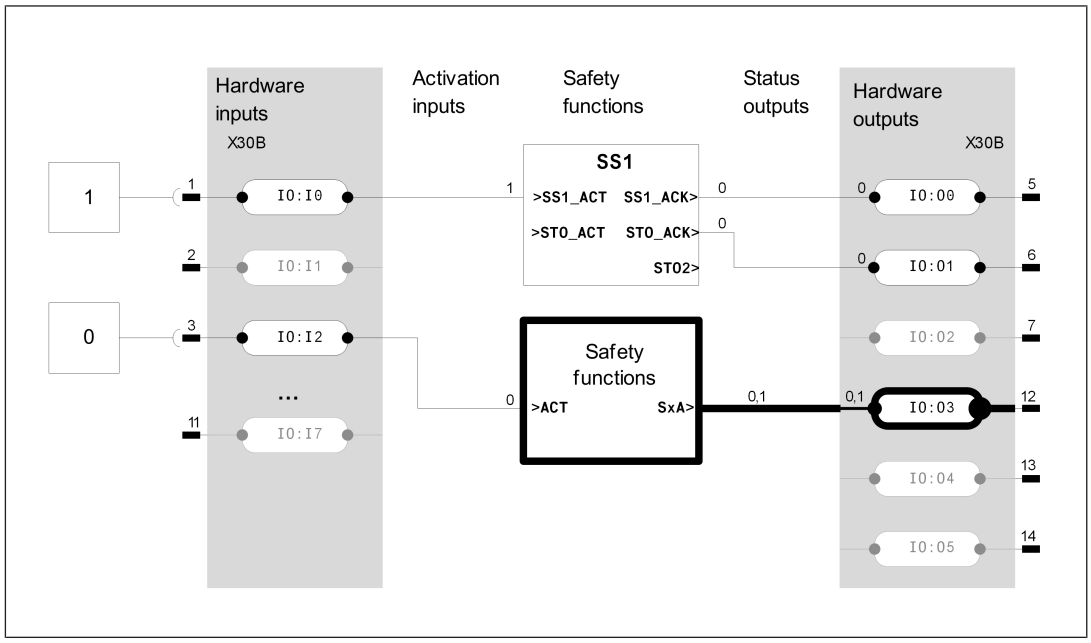


Fig.: Assignment hardware inputs/outputs

Legend

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

5.4.1 Hardware inputs

Assignment of the hardware inputs

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

Signals at the hardware input

0 signal at the input: Safety function is activated

1 signal at the input: Safety function is deactivated

Properties of the safe hardware inputs

The hardware inputs of the safety module can be controlled from the following outputs of a higher-level controller:

- Semiconductor outputs
- Contact-based outputs

The hardware inputs of the safety module correspond to

- The C-type interface from the ZVEI position paper "Classification of Binary 24 V Interfaces - Functional Safety aspects covered by dynamic testing" (see Technical details [200]).
- A type 1 input in accordance with IEC 61131-2.

With the hardware input active (1 signal), the correct function of the internal input circuitry is checked during every cycle ($T_{CYCLE,}$ see Reaction times [48]). This is done by test pulsing.

Signal detection at the hardware inputs

- A signal (0 signal or 1 signal) is always ignored if it is present for less than the minimum processing time.
- A signal is always detected and transmitted to the process image (PI) if it is present for longer than the maximum processing time (see diagram).

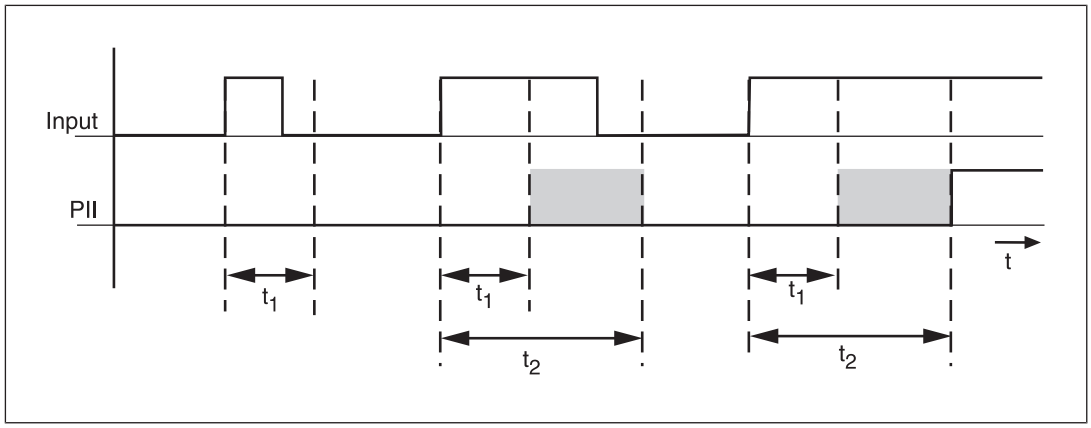


Fig.: Timing diagram for signal detection

Legend

Input	Signal at the input
t_1	Minimum processing time = filter time (adjustable) (see Technical details [200])
t_2	Maximum processing time = filter time (adjustable) + 1 cycle (see Technical details [200])
PII	Status of the process image of inputs (PII) (PII – Process Image Input)
Grey shaded area	Status of process image (PII) undefined

Input filter (pulse suppression)

The hardware inputs can be fitted with software input filters. The characteristic of the input filter corresponds to a 1st-order low pass.

Switch-off pulses, greater than the selected filter time, are identified reliably.

Configuration of the input filter time in the configuration tool:

From the ***Window*** menu bar select the button ***I/O settings***.

Physical address	Filter time	Filter time	Unit	Description
IO: I0 … IO: Ix	Activate/deactivate	1 …10	[ms]	The filter time can be activated/deactivated and the time specified for each hardware input. (default: activated, 1 ms)

5.4.2 Hardware outputs

5.4.2.1 Safe 1-pole hardware outputs

Mapping of the 1-pole hardware outputs

If a hardware output is assigned to a feedback output of a safety function, this is updated cyclically during operation.

0 signal (0 V) at hardware output:

- Output is high impedance.
- No current to the load.
- Activated safety function reports a limit value violation or a hazardous status.
- Safety function is not active.

1 signal (+24 V_{DC}) at hardware output:

- Output is low impedance.
- Current is supplied to the load.
- Activated safety function reports the safe status.

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

NOTICE

STO operating status

In the STO operating status, a 0 signal is output at all feedback outputs of the configured safety functions.
Exceptions:
Feedback output STO_ACK of the safety function SS1 reports the active status STO with a 1 signal.
Feedback output SBT_SBA of the safety function SBT remains set throughout the inspection period.

Shared output

When assigning hardware outputs there is the option of assigning multiple feedback outputs of safety functions to one hardware output. As soon as a feedback output of an activated safety function issues a 0 value as the status, the hardware output is set to 0.

NOTICE

Deactivated safety functions are disregarded by the shared output.

Despite a 0 value of a deactivated safety function, the shared output can issue a 1 signal.
Only activated safety functions contribute to the result.

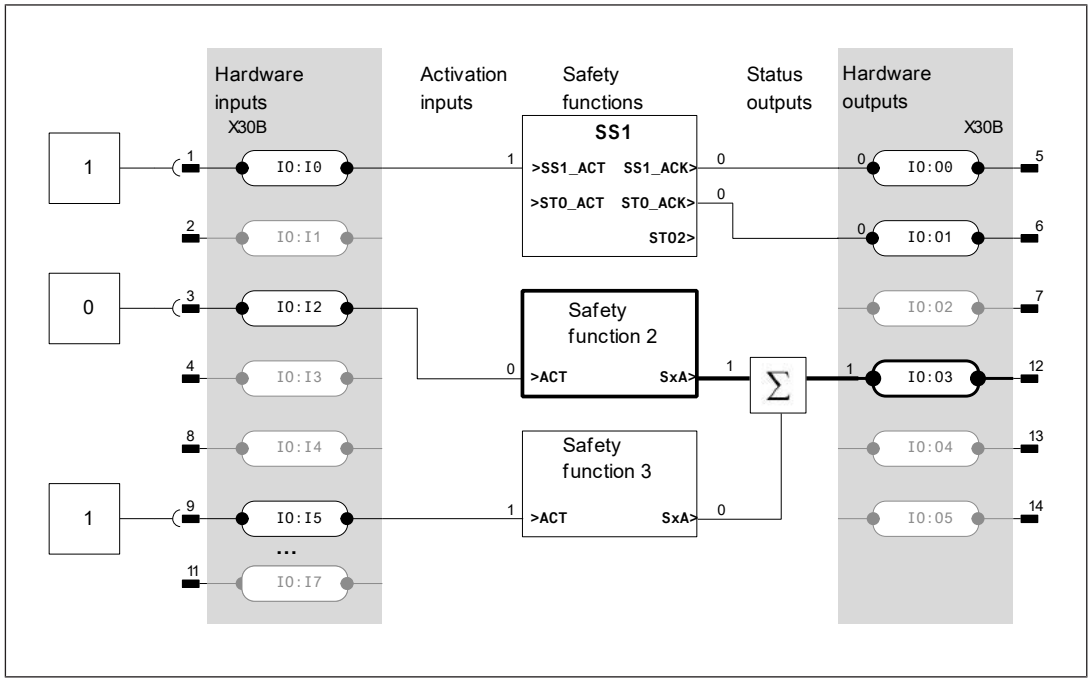


Fig.: Example for shared output 01

Legend

Safety function 2	Safety function 2 **activated**
Safety function 3	Safety function 3 **not activated**

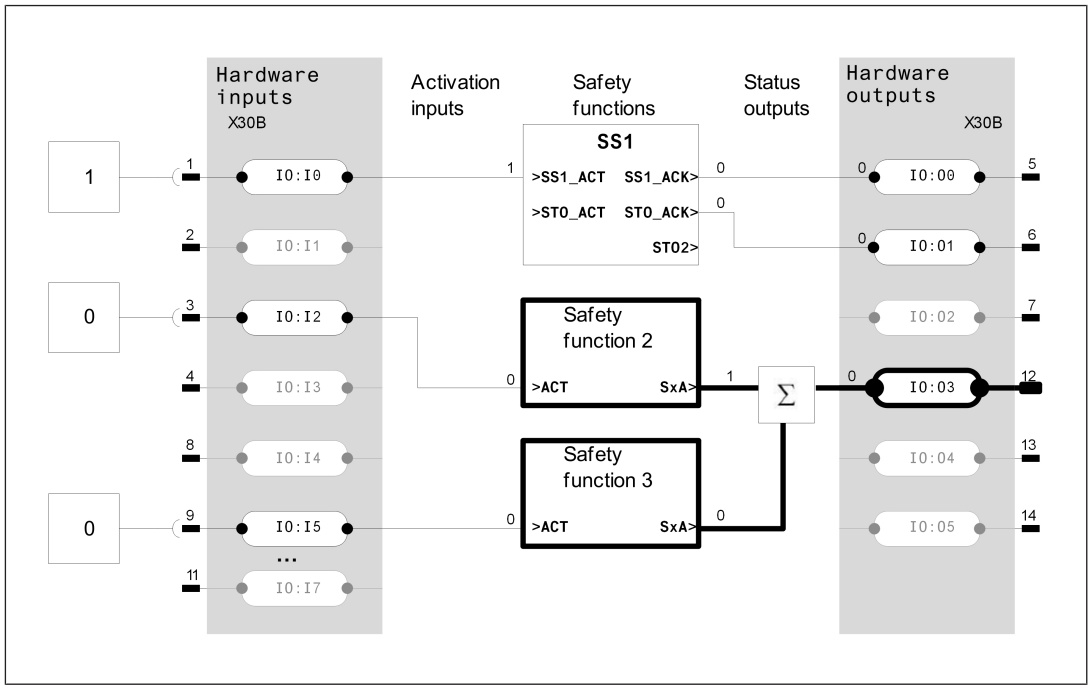


Fig.: Example for shared output 02

Legend

Safety function 2	Safety function 2 **activated**
Safety function 3	Safety function 3 **activated**

Supply voltage

- The 1-pole hardware outputs are supplied via the 24 V_{DC} infeed at X30A (pin 3 and pin 6).

General

- The maximum capacity at a hardware output is limited (see Classification according to ZVEI, CB24I [206], safe single-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. Observe without fail the specification of the hardware outputs of the safety module PMCprotego S3.

Output test

- Hardware outputs that are switched on are checked via regular off tests.
  - Test pulses for outputs that are switched on: see Technical details [200]
  - 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 [200]
  - 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.

WARNING!

Risk of injury due to the load switching on unintentionally

– When wiring a hardware output with capacitance please note the pulse duration and repetition time of the on test.

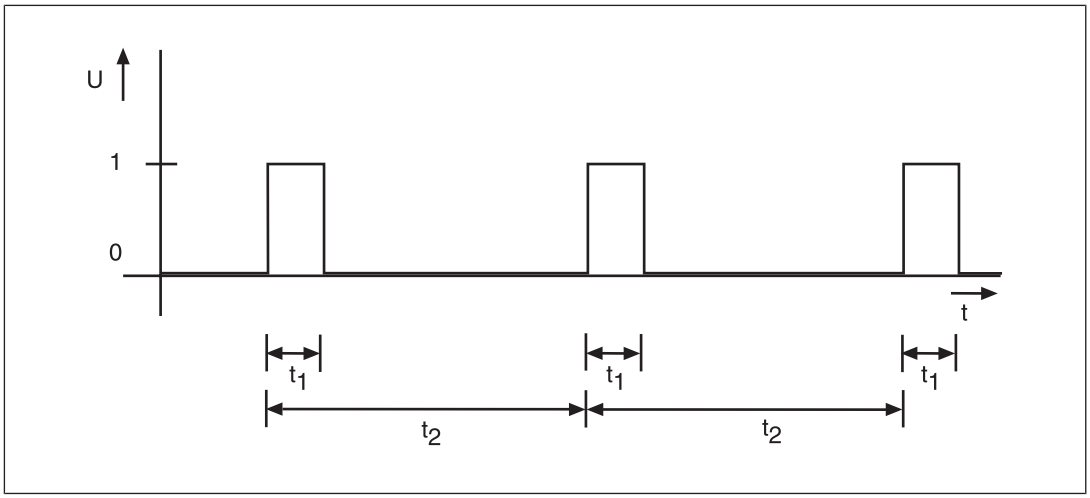


Fig.: Timing diagram

Legend

1	1 signal (high)
t_1	Pulse duration of the on/off test (see Technical details [📖 200])
t_2	Repetition time, normal time between two on/off tests (see Technical details [📖 200])
0	0 signal (low)

Configuring on and off tests

NOTICE

For applications in accordance with PL e (Category 4) and SIL 3, the on and off tests must be switched on (activated).

If a plant is particularly sensitive to test pulses, they may be switched off for individual hardware outputs.

The test must be replaced by other measures, depending on the safety requirement:

▸ When on test pulses are switched off

– The correct switch state is always checked. It is no longer checked whether a switched-off hardware output can still be switched on.

– The output's ability to switch will not be detected until the next time the hardware output is switched on.
– There are no longer any switch-on pulses in the output signal.

▸ When off test pulses are switched off:
– The correct switch state is always checked. It is no longer checked whether a switched-on hardware output can be switched off.
– The output's ability to switch will not be detected until the next time the hardware output is switched off.
– The supply voltage test for the hardware outputs cannot be switched off. Switch-off pulses are therefore still present in the output signal.

Configuration of the off tests in the configuration tool:

From the ***Window*** menu bar select the button ***I/O settings***.

Physical address	On test	Off test	Description
IO: O0 … IO: Ox	Activated/deactivated (default: activated)	Activated/deactivated (default: activated)	It is determined via the selection field whether the on/off test is switched on or off.

Testing for shorts

A test is regularly carried out to check for shorts between the hardware outputs.

For applications in accordance with PL e (category 4) and SIL 3, detection of shorts across contacts must be assured by the on/off test.

5.4.2.2 Safe 2-pole hardware outputs

Mapping of the 2-pole hardware outputs

If the 2-pole brake output SBC+/SBC- is mapped to the safety function SBC, the latter is set into operation cyclically.

0 signal (0 V) at the hardware output (SBC+/SBC-):

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

1 signal (+24 V) at the hardware output (SBC+/SBC-):

▸ Output is low impedance.
▸ Current is supplied to the load.

- A connected closed-current brake is vented, causing the braking torque/mechanical braking force to be removed from the axis.

The safety module has two safe two-pole hardware outputs to control spring-applied, mechanical brakes. Both outputs can only be mapped to the safety function SBC.

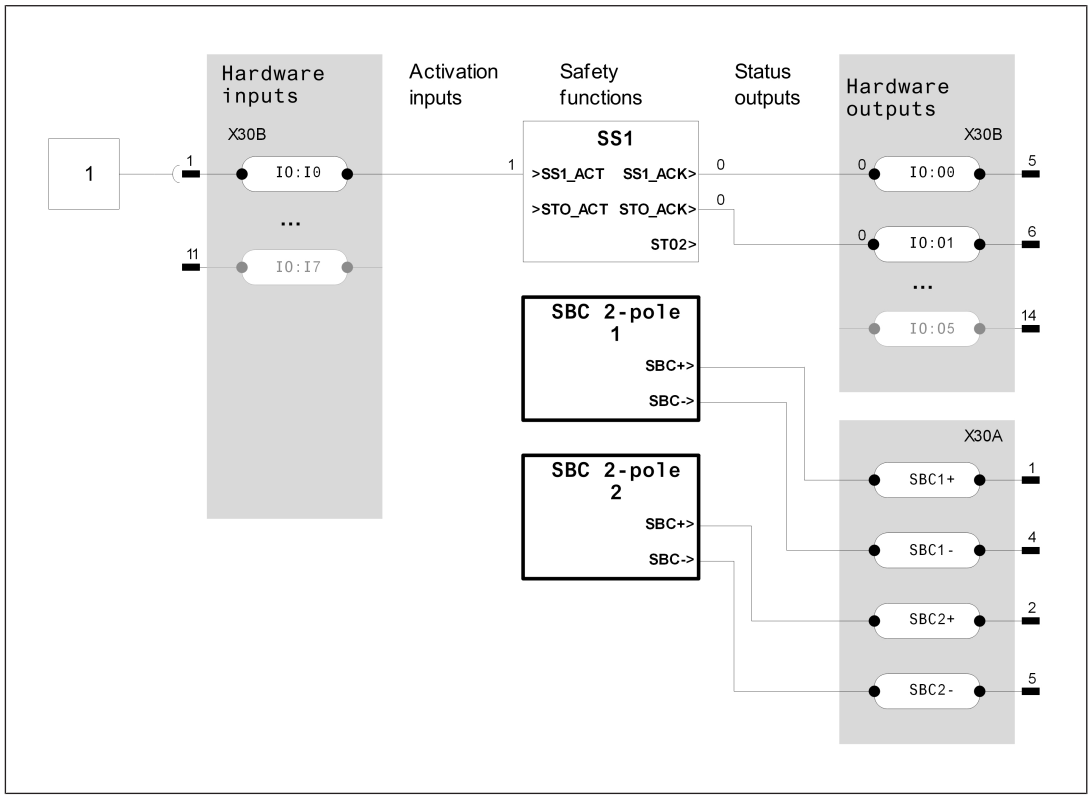


Fig.: IO SBC mapping

Legend

SBC 2-pole	Safe 2-pole hardware output to control a spring-applied, mechanical brake

Supply voltage

- The 2-pole brake outputs are supplied via the 24 V infeed at X30A (pin 3 and pin 6).

General

- The maximum capacity at a hardware output is limited (see Classification according to ZVEI, CB24I [📖 206], 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. Observe without fail the specification of the hardware outputs of the safety module PMCprotego S3.
- 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 Technical details [📖 200]
  - 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 [📖 200]
  - 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 between the hardware outputs SBC+ and SBC-.
- The result of open circuit detection is signalled by an error reaction.
- Loads over 3 kOhm may mistakenly be detected as an open circuit.

5.5 SafetyNET p RTFL interface

The SafetyNET p RTFL interface, described below also as SafetyNET p, is used for safe data exchange between one or more control systems PNOZmulti 2 and one or more safety modules PMCprotego S3 via a safe bus system.

INFORMATION

In the SafetyNET p RTFL network, at least one safe small control system PNOZmulti 2 must be connected to the expansion module PNOZmulti m EF SafetyNET from Version, HW: 01.01. 02, FW: 01.01. The PNOZmulti projects involved in SafetyNET p communication must be created using a PNOZmulti Configurator ≧ 10.11.0.
The PASmotion projects involved in SafetyNET p communication (PMCprotego D and PMCprotego S3) must be created using a PASmotion Configurator ≥ 1.4.0.
Further information and operating manuals are available on the Internet at www.pilz.com.

The safe input and output data transferred via SafetyNET is selected and configured for each safety module PMCprotego S3 in the configuration tool PASmotion. Inputs and outputs are mapped to the SafetyNET p subscribers in the configuration tool PNOZmulti Network Editor.

A further description of the configuration can be found in the online help for the PNOZmulti Network Editor.

SafetyNET p network:

Up to 16 subscribers can be connected via SafetyNET p and so can communicate with each other. The SafetyNET p subscribers are connected in a linear topology. That means that all the subscribers are connected in series, without branches. The subscriber sequence has no influence on communication.

Data exchange:

The safety module PMCprotego S3 can exchange data with a maximum of three other SafetyNET p subscribers. Communication can start when all the configured SafetyNET p subscribers are available.

Communication ends as soon as a SafetyNET p subscriber ends its participation (is in a stop state).

- Data is exchanged cyclically.
- At the start of a cycle, the safety module PMCprotego S3 reads the input data from the SafetyNET p network.
- After a cycle of the safety module PMCprotego S3 has ended, the output data is transferred to the SafetyNET p network.
- Within the next cycle, the output data are transferred to all the participating modules.

Maximum processing time of the SafetyNET p inputs

A signal (0 signal or 1 signal) is only safely detected and transferred to the process image (PII) when it is available for longer that the cycle time of the processor system (see Technical details [📖 200]).

Maximum processing time = 1 x Tcycle (cycle time of the safety module's processor system)

Safe fieldbus inputs and outputs:

32 safe fieldbus outputs and 32 safe fieldbus inputs can be defined for each safety module. The mapping of the inputs and outputs to the communicating systems is defined in the configuration tool PNOZmulti Network Editor.

PNOZmulti Configurator and PNOZmulti Editor

To be able to create network projects you will also need the PNOZmulti Configurator and the PNOZmulti Network Editor.

Install PNOZmulti Configurator and PNOZmulti Editor

Link to the PNOZmulti Configurator software (www.pilz.com Download Software PNOZmulti Configurator).

The PNOZmulti Network Editor is part of the PNOZmulti Configurator.

Prerequisites

The PASmotion Project Manger contains a project with the following devices:

- Servo amplifier PMCprotego D
- Safety module PMCprotego S3

Application example

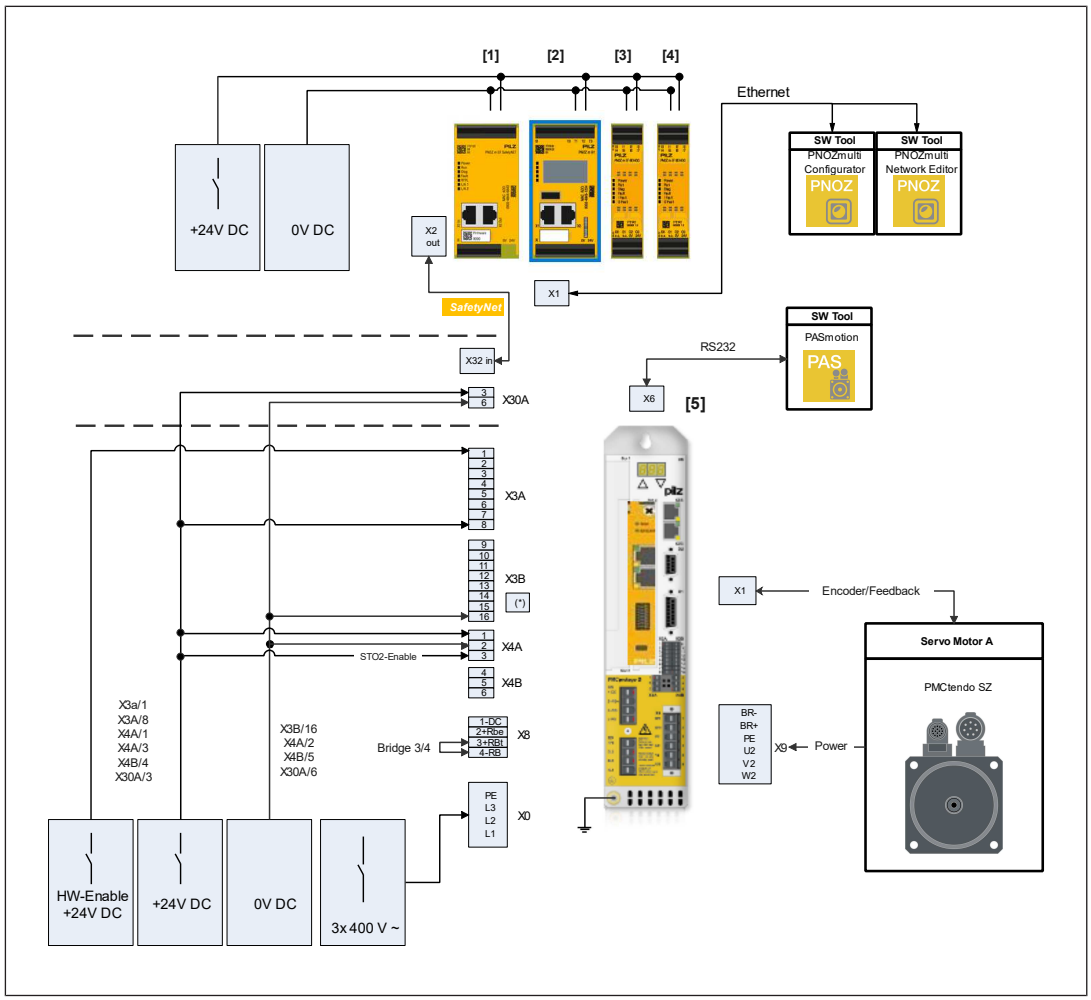


Fig.: Application example PMCprotego S3 with SafetyNET p RTFL interface

Legend

[1] PNOZ m EF SafetyNET

[2] Base unit PNOZ m B1

[3] Input/output module PNOZ m EF 8DI4DO (optional)

[4] Input/output module PNOZ m EF 8DI4DO (optional)

[5] PMCprotego D with safety module PMCprotego S3

INFORMATION

(*)
PMCprotego D, connection X3B, Pin 14 and 15: The BTB (ready for operation) relay must be included in the E-STOP (further information see operating manual PMCprotego D).

5.6 Motor encoder fault detection

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

5.6.1 Options

Errors in the connected encoders must be safely detected in order to generate safe speed and position values. The safety module offers different options for performing plausibility tests for the connected motor encoder.
An additional, external encoder is used in some applications. The second encoder can be used to detect additional errors in the mechanical transmission path between the motor and the driven device.

Sensor technology	Supported motor type			Supported safety functions		
	Rotary synchronous motor	Linear synchronous motor	Asynchron-ous motor	SS1, SS2	SOS, SLS, SSR, SDI, SLI, SBC, SBT	SLP
Motor encoder and internal system vari-ables	X	X	--	X	X	--
Motor encoder and external incremental encoder (TTL)	X	X	X	X	X	--
Motor encoder and external absolute encoder (SSI)	X	X	X	X	X	X

INFORMATION

Two different encoders are required for the plausibility check when asyn-chronous motors are used.

NOTICE

To guarantee the diversity and to prevent common cause failures (CCF) the external encoder must not be from the same manufacturer as the motor en-coder (take care with badged products!).

Forced dynamisation of encoder

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

- At least one turn of the motor for rotary synchronous motors/asynchronous motors
- At least a distance of (number of poles/2) * pole pair width for linear synchronous motors

5.6.2 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. A maximum permitted deviation of the position values of the two encoders can be parametrised in the configuration tool when two encoders are used.

Sensor technology	Fault detection per motor type		
	Rotary synchronous motor	Linear synchronous motor	Asynchronous motor
Motor encoder and internal system variables	At the latest after one mechanical motor turn	At the latest after a movement distance of (number of poles/2) * pole pair width	--
Motor encoder and external incremental encoder (TTL)	The maximum deviation between the two encoder positions can be parametrised, at the latest after one mechanical motor turn	The maximum deviation between the two encoder positions can be parametrised, at the latest after a movement distance of (number of poles/2) * pole pair width	The maximum deviation between the two encoder positions can be parametrised, at the latest after one mechanical motor turn
Motor encoder and external absolute encoder (SSI)			

5.6.3 Maximum achievable safety integrity

The different options for error detection can achieve the following maximum values for safety integrity for all safety functions:

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

The safety engineering characteristics of the safe drive system depend on the failure rates of the encoders used.

The chapter Technical details [📖 200]/safety-related characteristic data already considers various encoders with their failure rates.

5.7 Reaction times

Type-C standards for machines specify minimum distances between a protective device and the hazardous area either directly or by referring to the ISO 13855 international standard.

The overrun of the dangerous movement by the total system must be determined to specify the minimum distances.

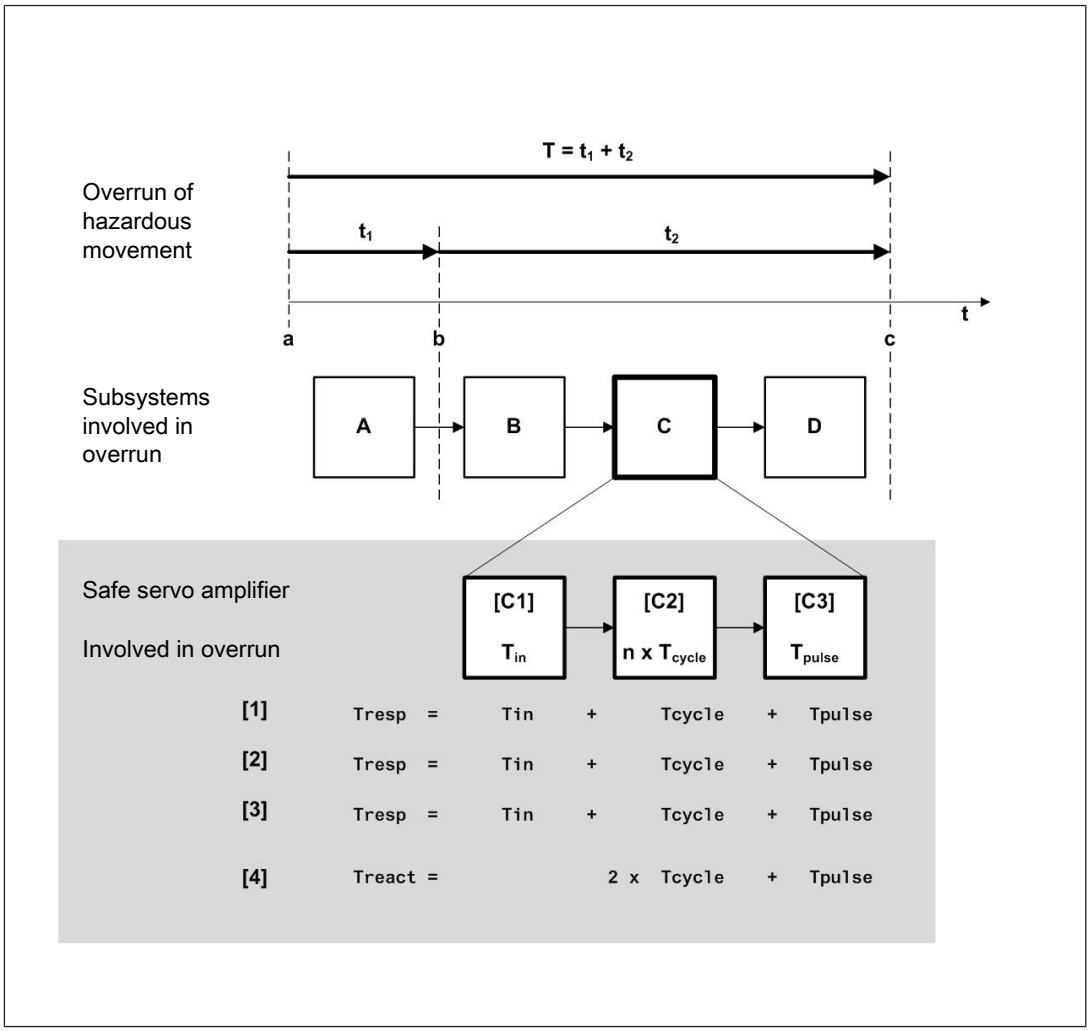


Fig.: Reaction times

Legend

T	Overall system stopping performance
t_1	Response time of a protective device
t_2	Stopping time
a	Triggering the protective equipment
b	OFF signal is generated
c	Safe state of machine
A	Sensor/protective device

B	Higher-level programmable safety system
C	Safe servo amplifier
D	Mechanics
[C1]	Input delay
[C2]	Processor system of the safety module
[C3]	Delay time for safe pulse lock
[1]	Response time for stop function (stop category 0) via the STO_ACT input
[2]	Response time for stop function (stop category 0) via the SS1_ACT input
[3]	Response time from the activation of movement monitoring to the error reaction of SS1 (delay time 0)
[4]	Reaction time from movement monitoring (already active) to the error reaction of SS1 (delay time 0)

The overrun of the dangerous movement of a machine includes several times.

This documentation specifies the following times for Subsystem C – Safe Servo amplifier:

Time	Description	Section
Tin	Maximum processing time of the input	Hardware inputs
		SafetyNET p RTFL interface
Tcycle	Cycle time of the safety module processor system	Technical details
Tpulse	Delay time for safe pulse lock	Technical details
Treact	Maximum error reaction time	Reaction times
Tresp	Maximum response time	Reaction times

Treact maximum error reaction time

This time includes

- the cycle time of the safety module processor system.
- the delay time for safe pulse lock.

The error reaction function includes the STO safety function (SS1 with delay time 0).

Tresp maximum response time

This time includes

- maximum processing time of the input.
- the cycle time of the safety module processor system.
- the delay time for safe pulse lock.

Tcycle cycle time of the processor system

This time includes

- reading the inputs and the position values.
- executing the safety functions.
- detection of limit value violations.
- setting the outputs.
- triggering the STO safety function in the event of an error.
- triggering the SS1 safety function in the event of an error.

INFORMATION

To determine the overrun time of the overall system, the reaction times of all the system's components must be considered. Please note also the relevant documentation of the components involved.

detecting the violation of a limit value

A limit value violation is only reliably detected if the drive remains in the prohibited area for longer than the cycle time of the Tcycle processor system.

WARNING!

A violation of the blocked area is not detected for special applications

If a configured danger zone is only very briefly violated or a narrow, blocked area is traversed at high speed (e.g. while the SLP or SLP-M safety functions are active), such a violation may not be detected by the safety module, due to the specified cycle time of the processor.

- Test the due performance of the safety function if such conditions are really relevant (brief violation of danger zone, rapidly passing through the blocked area).
- Please refer to the chapter Safety checks [📖 184].

NOTICE

For the mechanical system (subsystem D), the time until the machine has reached a safe condition must be determined.
The times for the stop functions (SS1, SS2) are application-specific and do not form part of the specified times.

INFORMATION

Input filter time

The input filter times for the hardware inputs I0 … I7 can be adjusted in the configurator, in the safety functions editor, under "I/O Settings". A value range between 1 ms and 10 ms is available for the filter time. A filter time of 1 ms is the standard setting.

5.8 Safe restart of the machine

A safe standstill during human intervention in hazardous areas is one of the most important requirements for the operation of machinery according to 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 Operating Stop (SOS)
- Safe Restart Lock (SRL)

NOTICE

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

5.9 Resetting (RESET) the safety module

In the operating state STO (see Operating states [📖 187])

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

To exit the STO operating state (see section entitled Operating states [📖 187]), the safety module needs to 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 servo amplifier
  - – Via the "CLRFAULT" command

The transition in operating states from STO → STARTUP → RUN/FSRUN for the safety module is described as RESTART (see Operating states [📖 187]). When switching from STARTUP to RUN/FSRUN, the safety function STO is deactivated (the servo amplifier can enable the output stage) and the motor can execute a movement.

The RESET behaviour of the safety module PMCprotego S3 can be set to reflect the requirements of the application by configuring:

RESET trigger	RESET behaviour	Description
Inputs SS1_ACT/STO_ACT	0: NOP	No action No RESTART occurs.
	1: RESTART	Acknowledge error The RESTART is triggered.
CLRFAULT command from the servo amplifier	0: NOP	No action 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 action 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 PMCprotego S3 is triggered by switching from 0 signal to 1 signal at one of the two inputs.

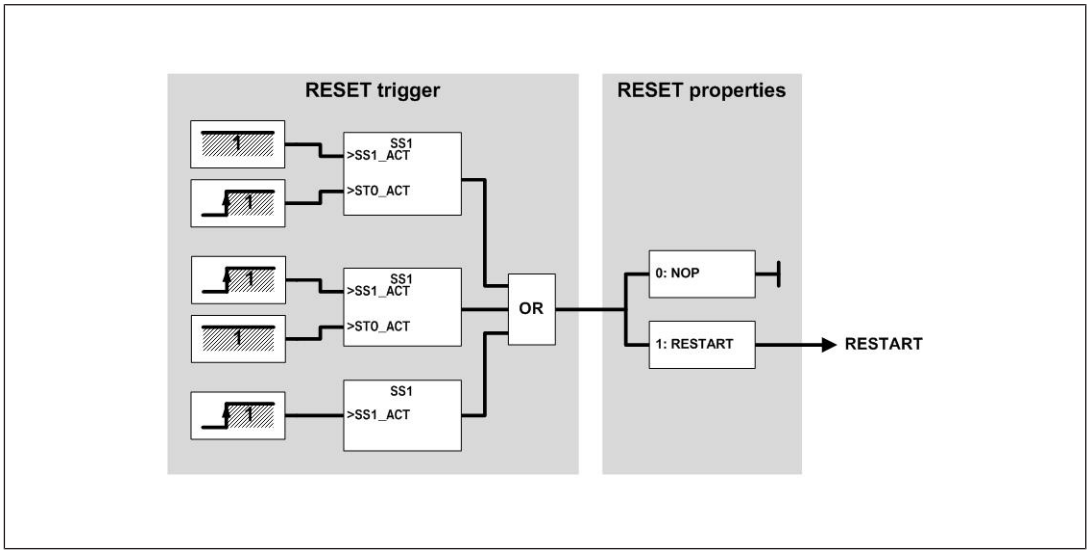


Fig.: RESET by the inputs SS1_ACT or STO_ACT

Legend

NOP	No operation
RESTART	A RESTART is triggered

Configuration of the RESET behaviour in the configuration tool

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

INFORMATION

A combination with the safety function SRL (Safe Restart Lock) is possible (see above). The RESTART then 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 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:

- Evaluate the STO_ACK signal to identify the operating state STO
- Bring the machine/system to a safe state
- Create a positive edge at one of the inputs of safety function SS1

Non-safety-related RESET by the servo amplifier's CLRFAULT command

The servo amplifier's CLRFAULT command can be used as follows:

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

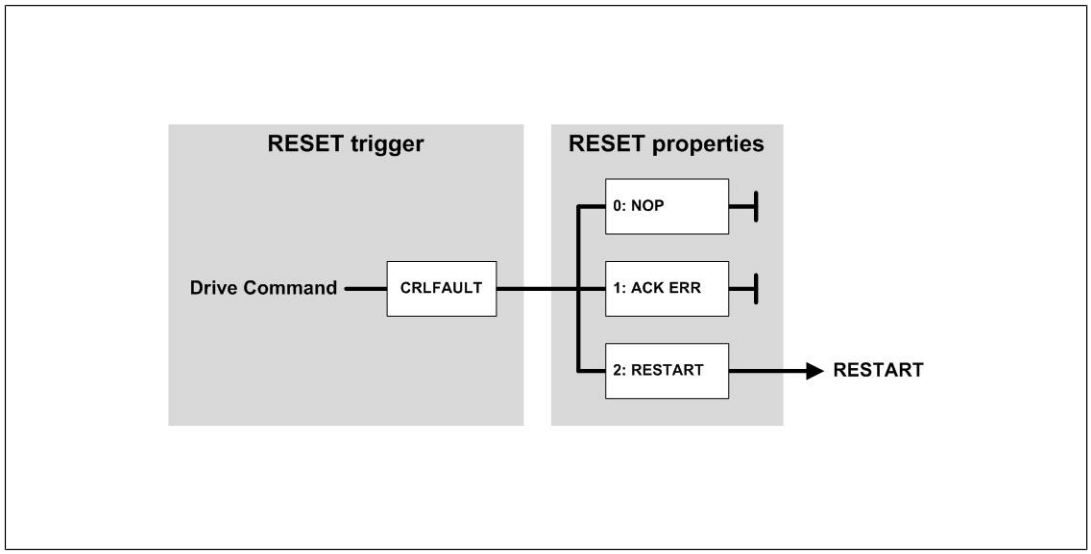


Fig.: RESET by the servo amplifier's CLRFAULT command

Configuration of the RESET behaviour in the configuration tool

Field: RESET trigger: CLRFAULT command from the servo amplifier			
Input field	**Valid entry**	**Unit**	**Description**
RESET behaviour	0: NOP	--	No action 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 exclusively the non-safety-related CLRFAULT command of the servo amplifier is used to RESTART the safety module, the servo amplifier could be enabled unintentionally, causing the motor to start up unexpectedly.
Use the CLRFAULT command of the servo amplifier 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.

Safety-related RESET by the safety function SRL

The safety function SRL can be used as follows:

- As a 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 CLRFAULT command of the servo amplifier.
- Triggering the RESTART of the safety module (2: RESTART).

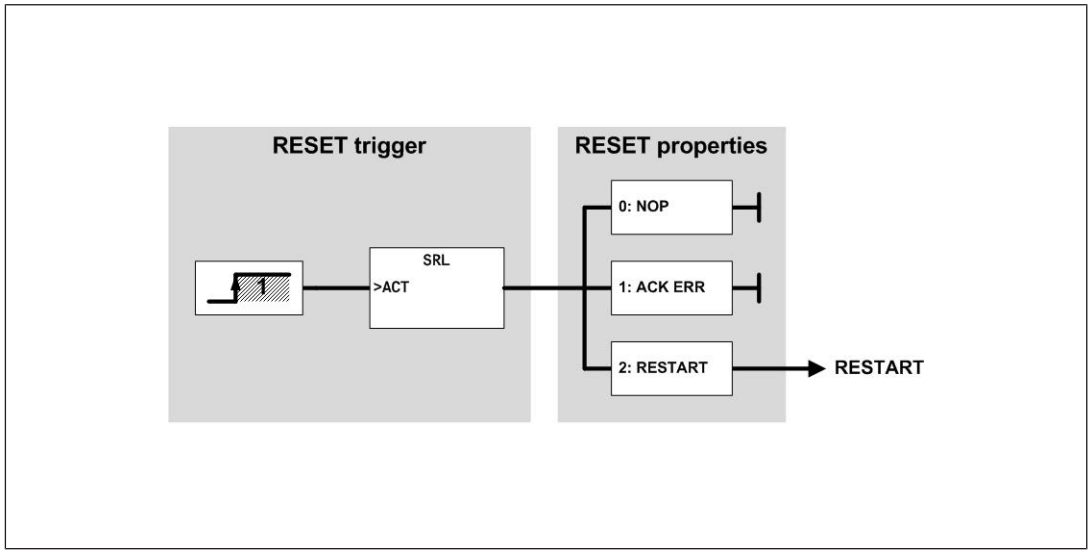


Fig.: RESET by the safety function SRL

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 action 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 in the following chapter Safe Restart Lock (SRL) [📖 145]

A combination with the CLRFAULT command of the servo amplifier is possible (see above). The RESTART then only occurs if there is a 1 signal at the input of the safety function SRL (a RESTART is enabled).

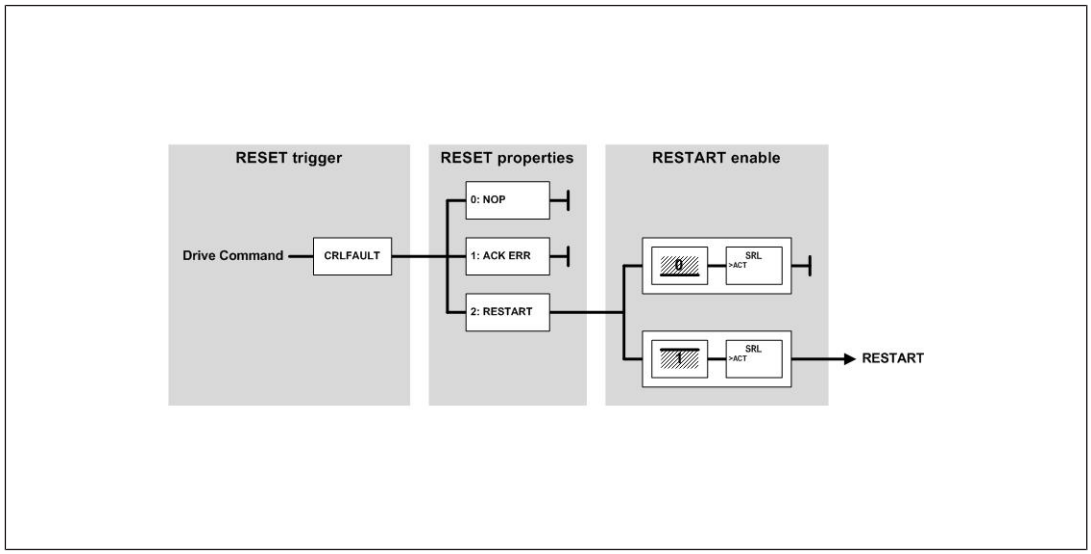


Fig.: RESET by the CLRFAULT command of the servo amplifier and enabling by the safety function SRL

Legend

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

5.10 Application of the SBC and SBT safe brake functions

The safety module PMCprotego S3 makes it possible to trigger and test standby current-activated mechanical brakes. Mechanical brakes may be required for various safety functions to reduce the risk in environments in which "load suspension" is common.

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. The "load suspension" safety function is one of the most important among the many different applications. In the safety module PMCprotego S3, the "load suspension" safety function can be implemented by using the SBC and SBT safety functions.

In addition to safe suspension, the SBC and SBT safety functions can also reduce the risk of other applications that make use of mechanical brakes, such as when stopping high mass inertias.

5.10.1 Definition of the "load suspension" safety function

The "load suspension" safety function is a technical measure to prevent unintended sagging of loads.

Gravity-loaded axes must be kept in position:

– During normal operation

– During interrupted operation

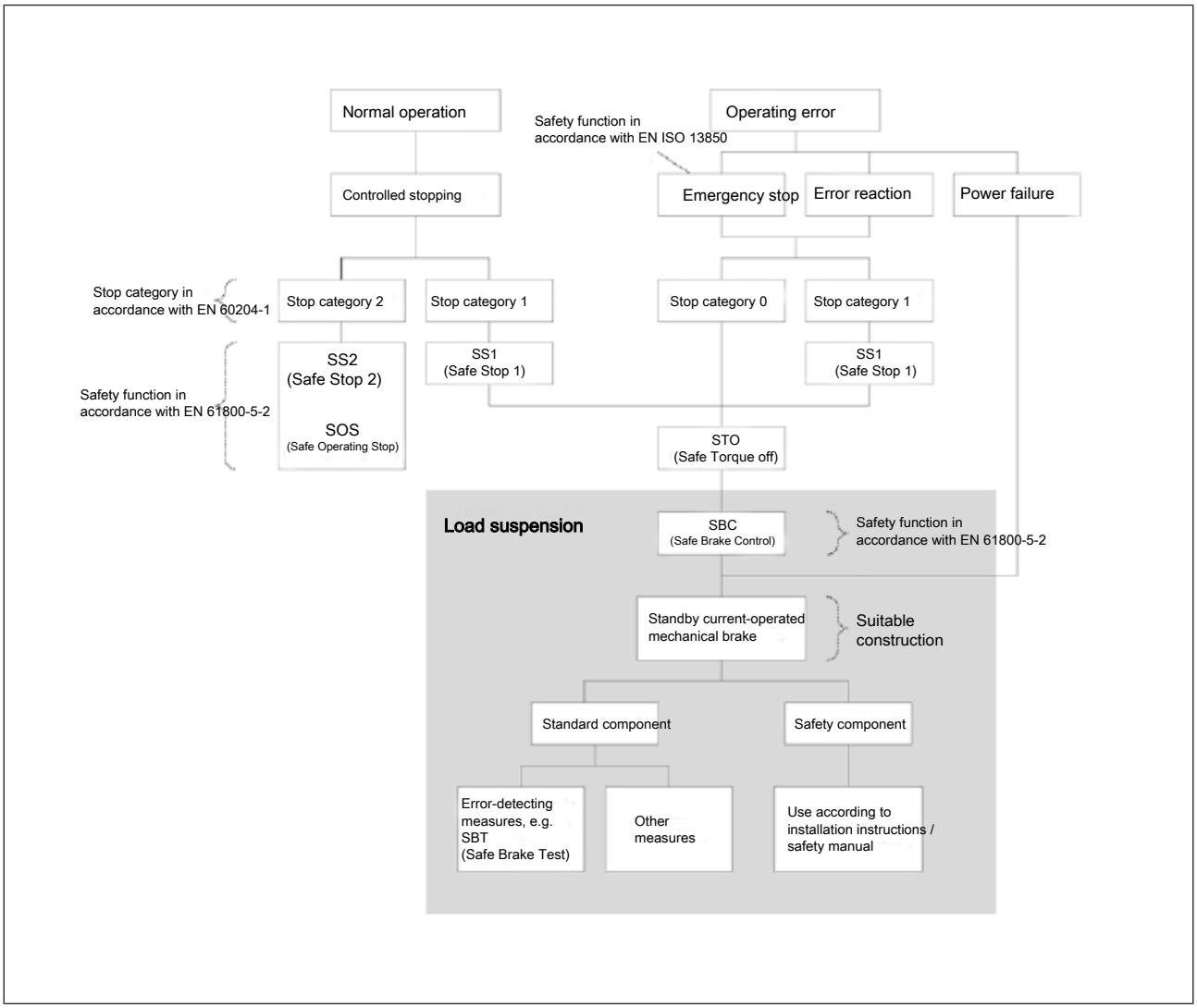


Fig.: Overview of "load suspension" during normal and interrupted operation

5.10.2 Standby current-operated, mechanical brakes

5.10.2.1 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

5.10.2.2 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

5.10.2.3 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.

5.10.3 Options of "Load suspension" implementation

The safety module PMCprotego S3 offers the option

– of triggering standby current-activated, mechanical brakes.

– of triggering an external safe system for load suspension.

The safety module PMCprotego S3 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:

– Brake triggering
(voltages, currents, performance drop, emergency shutdown, etc.)

– Measures for error detection

5.10.3.1 Performance trigger of standby current-activated mechanical brakes by the safety module

During performance triggering, the brakes are connected to the 2-pole hardware outputs of the safety module.

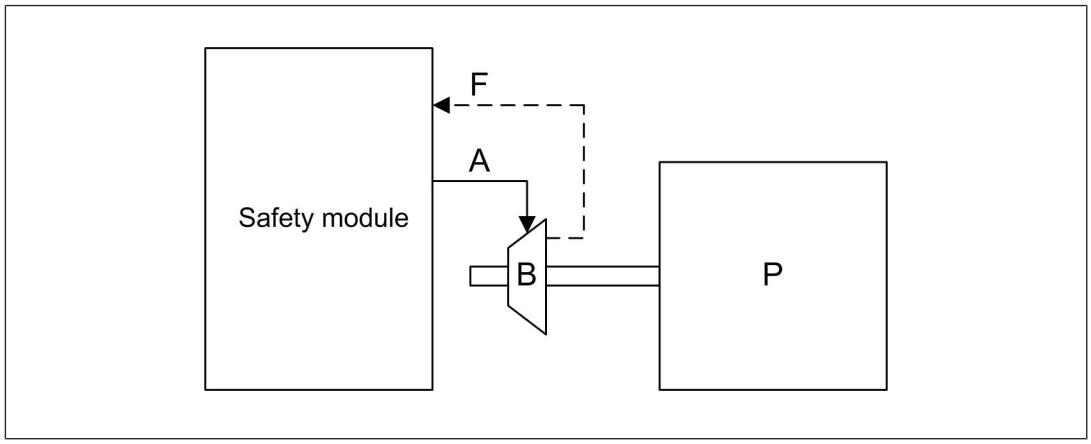


Fig.: Performance trigger for standby current-operated, mechanical brakes

Legend

F	Optional feedback
A	Performance trigger
B	Standby current-operated, mechanical brake
P	Driven system (for example a gravity-loaded axis)

5.10.3.2 Triggering an external safe system

If an external safe system is used, this is triggered via the 1-pole safe hardware outputs of the safety module. These outputs must be allocated to the SBC safety function.

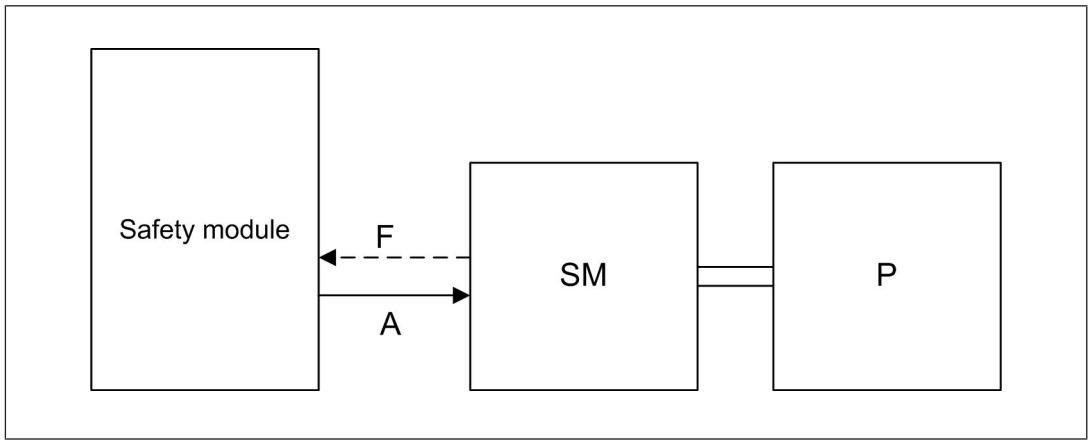


Fig.: Triggering an external safe system

Legend

F	Optional feedback
A	Trigger signal
SM	Safe system for shutdown and load suspension
P	Driven system (for example a gravity-loaded axis)

5.10.4 Examples

General information about the examples:

The safety integrity tables indicate the maximum achievable categories according to 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 save movement function (e.g. SLS, SOS, etc.) should be active. In the event of an error, this will trigger an error reaction function and activate the STO safety function.
- To ensure that a brake is activated if the STO safety function is active, thus stopping the hazardous movement, at least one SBC safety function must be configured (see Safe Brake Control (SBC) [130]).
- An error analysis must be carried out for the mechanical brake used.
  This must be performed for each application.
- An error analysis must be carried out for the driven system.
  This must be performed for each application.

Configuration servo amplifier/safety module with the software PASmotion

We assume for the following examples that the listed braking devices (motor brake, external brake and/or external safe system) are linked only to the safe semiconductor outputs of the safety module. The control is performed safely via the SBC function blocks (SBC 1-pole/SBC 2-pole). No brake is connected on the standard brake output BR+/- of the servo amplifier. During configuration the following settings result from this, which must be noted:

In the PASmotion software, when configuring the safety function, you can select in the settings of the function blocks SBC (1-pole/2-pole):

The parameter ***Connection*** can be activated or deactivated (default: Deactivated), seeSafe Brake Control (SBC) [130] "Connection of servo amplifier brake control".

If the ***Connection*** parameter is activated the following settings have to be made in the configurator:

- In the parameter navigation of the servo amplifier, select the ***Motor*** parameter, and in the ***Brake*** field select ***Type*** 4: With (no monitoring of the brake error).
- In the parameter navigation of the safety module, select the ***Motor*** parameter and in the ***Brake*** field select ***Type*** 4: Brake error (brake without monitoring).

INFORMATION

For motors/motor encoder types with an electronic type label it is necessary to also save the parameters in the memory of the electronic type label when the brake type is changed. To do this, enter the ASCII command "HSAVE" in the terminal.

Further information on the configuration of the servo amplifier/safety module is available from the Online help of the software PASmotion.

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

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

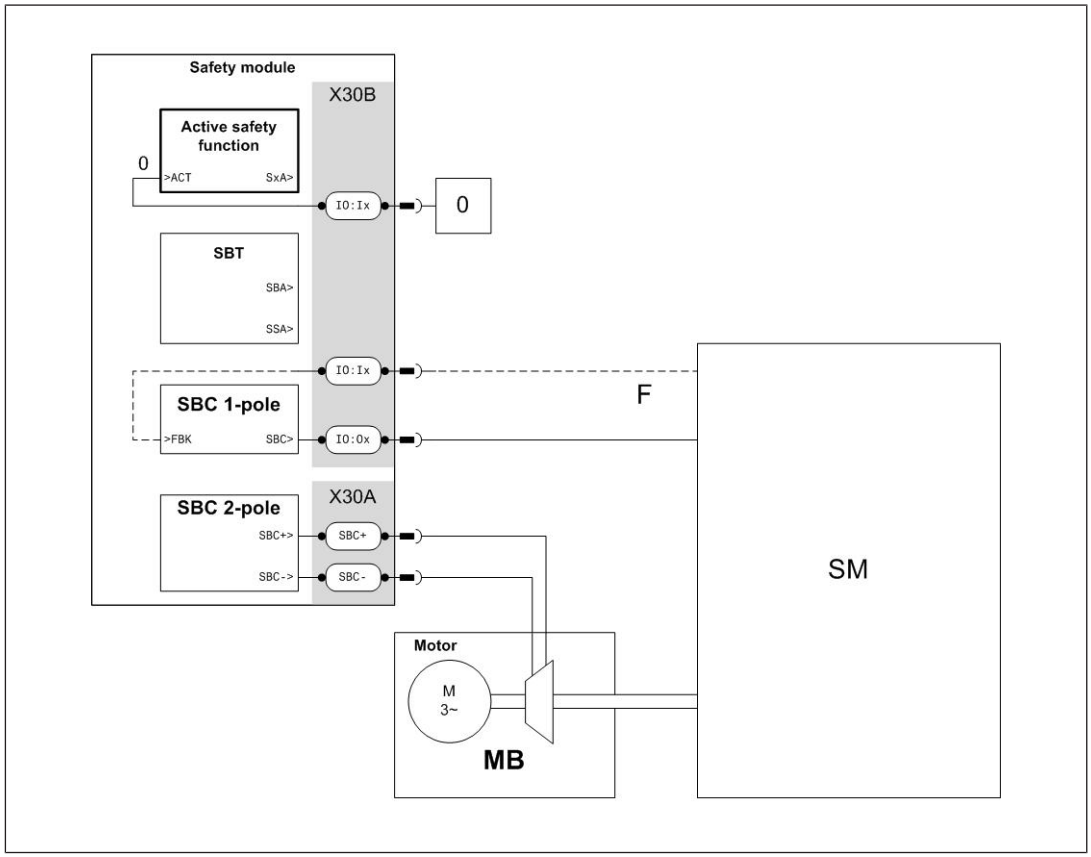


Fig.: "Load suspension" with a motor brake and an external safe system

Legend

F	Optional ventilation monitoring
SM	Safe system for load suspension
MB	Standby current-operated mechanical motor brake

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 brake as a proven component (Cat. 1)	Not required
Categorisation of the brake as a safety component	optionally

The following notes apply:

- The safety module PMCprotego S3 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 PMCprotego S3.
- The external system should be regarded as a separate, safety-related subsystem (SRP/CS according to EN ISO 13849-1).
- A separate error evaluation must be carried out for the components included in the safe system (e.g. brake, performance trigger, driven system, etc.)
- Please take note of the chapter on Feedback of the safety functions via hardware inputs [📖 29] to prevent and detect errors due to overvoltage.
- 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.

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

Triggering of a standby current-operated, mechanical brake by a 2-pole SBC+/- output (X30A) with or without ventilation monitoring (feedback).

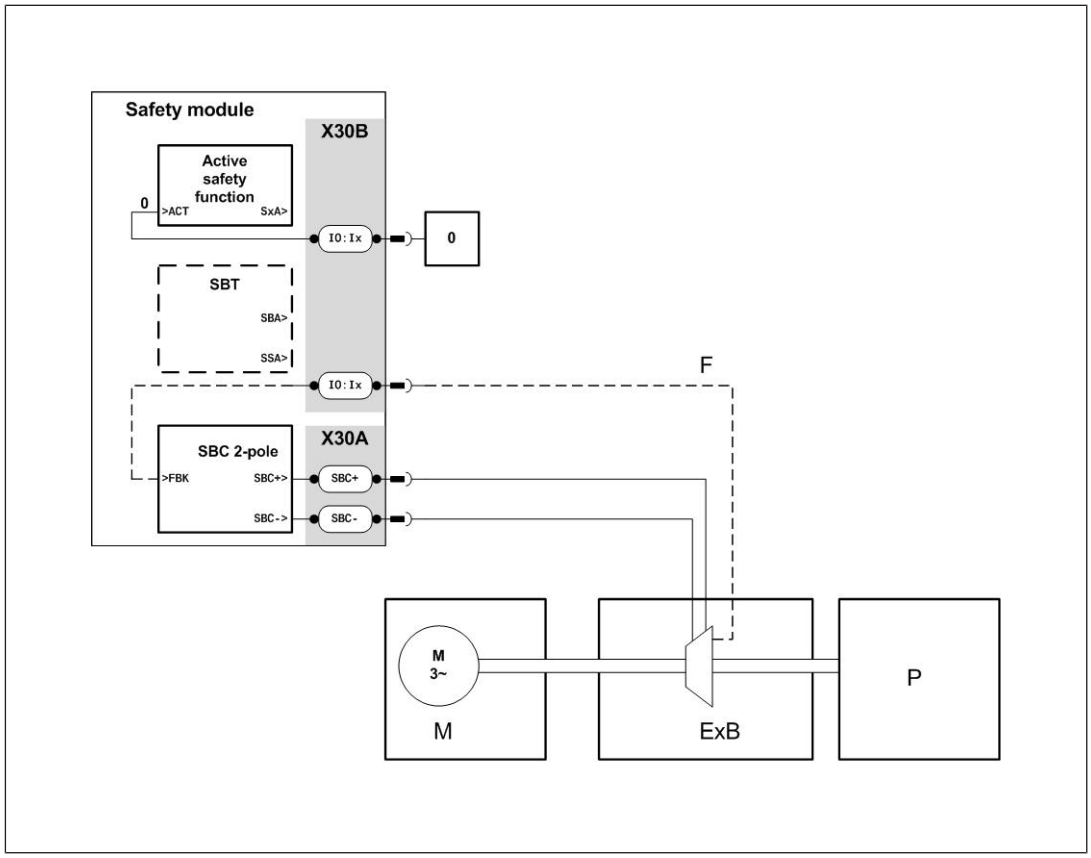


Fig.: "Load suspension" with an external brake (standard component)

Legend

M	Motor
F	Optional ventilation monitoring (feedback)
- - -	Dotted line, optional
ExB	External, standby current-operated, mechanical brake
P	Driven system (for example a gravity-loaded axis)

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
SBC ventilation monitoring feedback	optional	optional
SBT (Safe Brake Test) Test interval according to EN ISO 13849-1 (requirement rate ≤ 1/100 of test rate or testing takes place immediately when required by the safety function)	Not required	Essential

Max. category in accordance with EN ISO 13849-1	1	2
Categorisation of the brake as a proven 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 according to EN ISO 13849-1. This must be categorised as a proven component.
- If necessary, ventilation monitoring of the brake can be evaluated by the SBC safety function.
- If Category 2 according to EN ISO 13849-1 is to be achieved, the SBT safety function in the safety module PMCprotego S3 must be configured and the brake must be tested.

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

Triggering of a standby current-operated, mechanical motor brake by a 2-pole SBC+/- output (X30A).

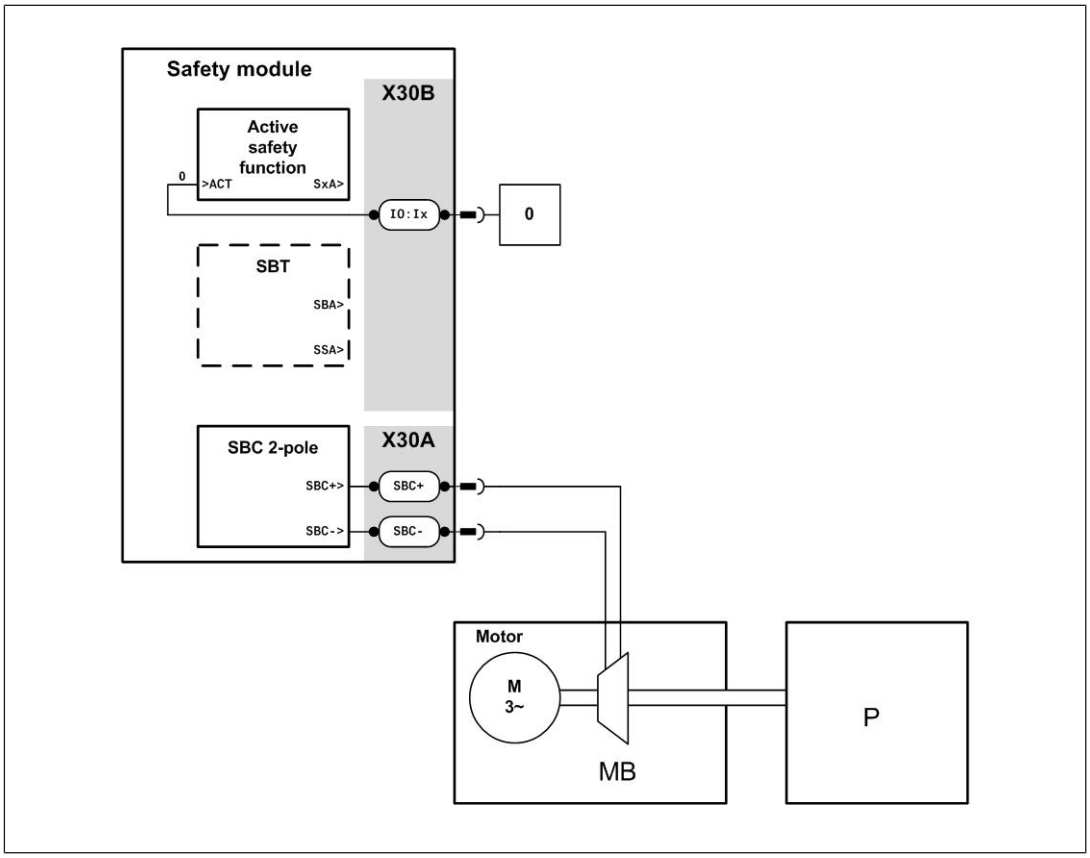


Fig.: "Load suspension" with a motor brake

Legend

MB	Standby current-operated mechanical motor brake
P	Driven system (for example a gravity-loaded axis)

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
SBC ventilation monitoring feedback	Not required	Not required
SBT (Safe Brake Test) Test interval according to EN ISO 13849-1 (requirement rate ≤ 1/100 of test rate or testing takes place immediately when required by the safety function)	Not required	Essential
Categorisation of the brake as a proven 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 according to EN ISO 13849-1. This must be categorised as a proven component.
- If Category 2 according to EN ISO 13849-1 is to be achieved, the SBT safety function in the safety module PMCprotego S3 must be configured and the brake must be tested.

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

Triggering of an external, standby current-operated, mechanical safety brake by a 2-pole SBC+/- output (X30A).

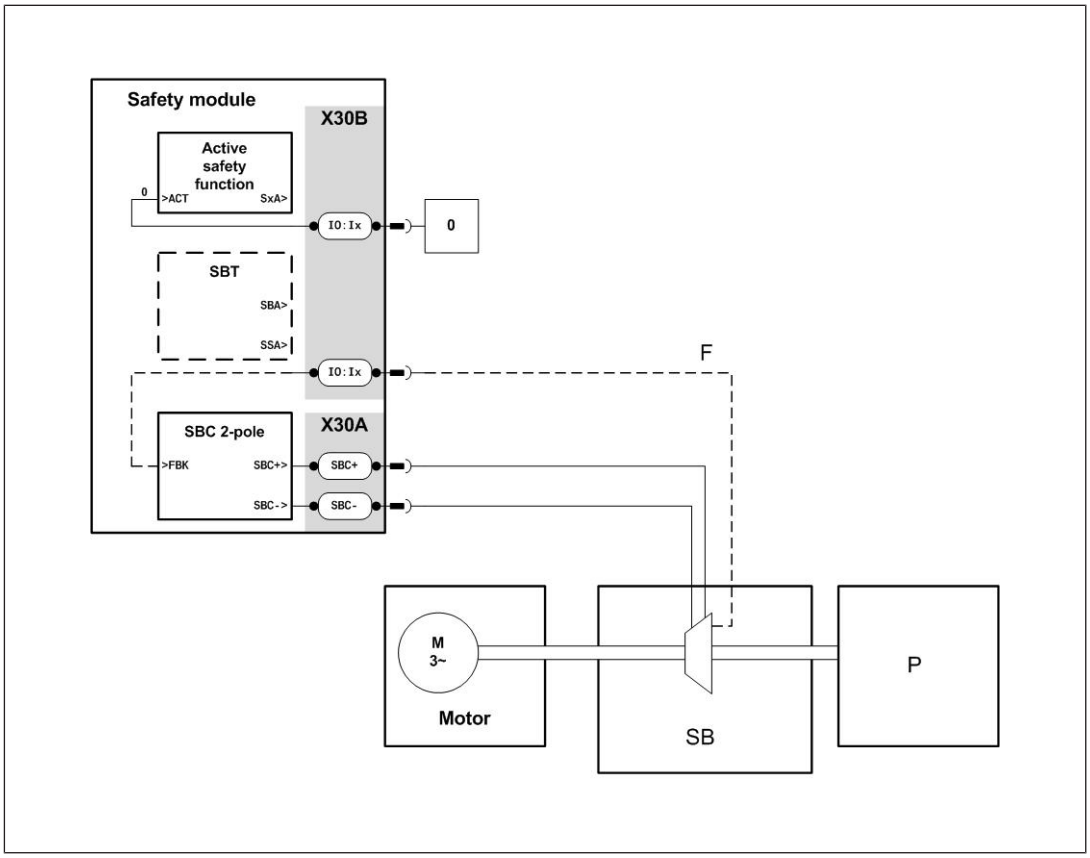


Fig.: "Load suspension" with an external safety brake (safety component)

Legend

F	Optional ventilation monitoring (feedback)
- - -	Dotted line, optional
SB	External, standby current-operated, mechanical safety brake
P	Driven system (for example a gravity-loaded axis)

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
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 according to 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 requirements, the SBT safety function and the ventilation monitoring system may be used.

5.10.4.5 "Load suspension" by triggering an external system

Triggering an external safe system for load suspension, using safe 1-pole hardware outputs and optional evaluation of feedback signals.

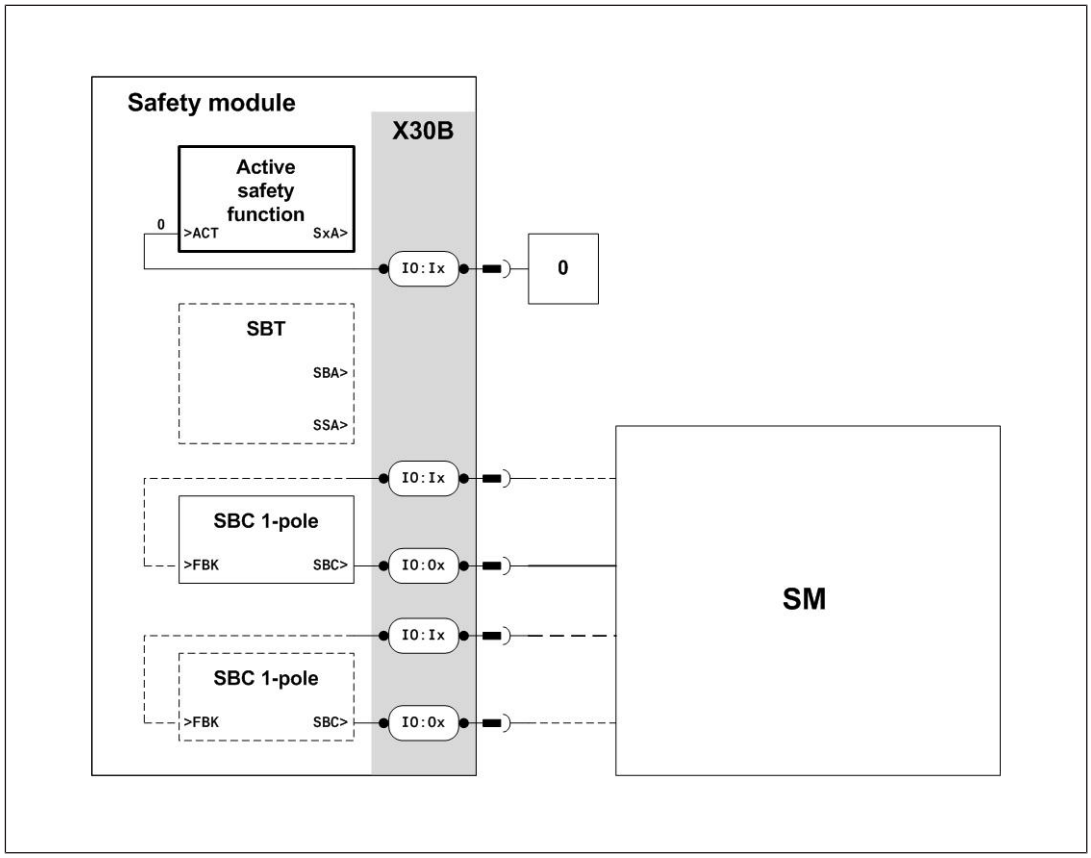


Fig.: Safe system for load suspension

Legend

SM Safe system for load suspension

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 PMCprotego S3 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 PMCprotego S3.

- Error monitoring of brakes, performance trigger 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 according to EN ISO 13849-1).
- The achievable category depends on the characteristics of the safe, external brake controls.
- Please take note of the chapter on Feedback of the safety functions via hardware inputs [29] to prevent and detect errors due to overvoltage.

Apply the measures in Chapter Application of the SBC and SBT safe brake functions [59].

5.10.4.6 "Load suspension" with two brakes

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

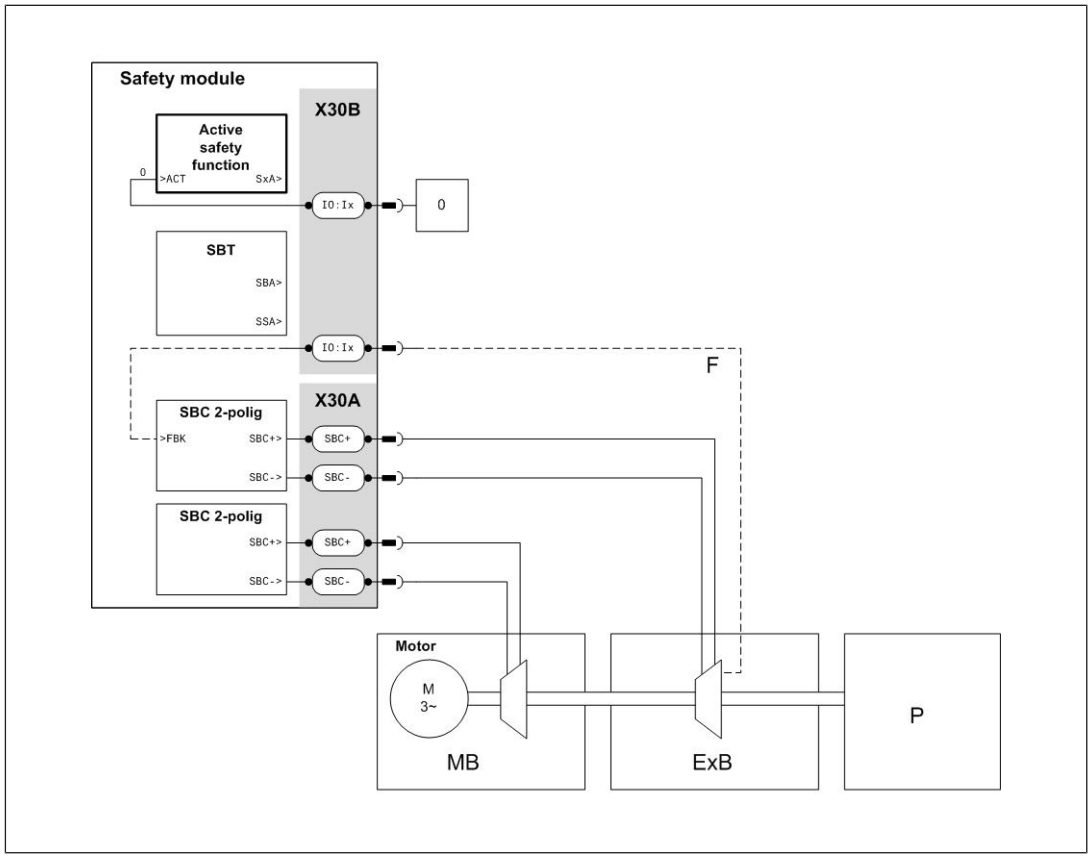


Fig.: "Load suspension" with two brakes

Legend

F	Optional ventilation monitoring
MB	Standby current-operated mechanical motor brake
ExB	External, standby current-operated, mechanical brake
P	Driven system (for example a gravity-loaded axis)

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.

5.10.5 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 PMCprotego S3
- Safety characteristics of the safety module PMCprotego S3
- 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 SBC safety function

5.11 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 10 safety functions can be configured in the configuration tool, using function blocks. In addition, the safety function Safe Stop1 (SS1) must always be configured.

The safety function SS1 cannot be deactivated in the configurator. The input of the safety function SS1 of the safety module must always be connected to an input of the safety module (hardware or SafetyNET input).

All safety functions must be configured individually.

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

- Safe Stop 1 (SS1), a fixed component of the safety configuration
- Safe Restart Lock (SRL)
- Safe Status Output (SSO)
- Safe Brake Test (SBT)

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).

External activation of safety functions

- The safety functions are activated with the 1-pole safe hardware inputs of the safety module PMCprotego S3, see Activation of the safety functions via hardware inputs [📖 27].
- The safety functions are activated via the inputs of the SafetyNET p RTFL interface.
- These inputs operate in accordance with the standby current principle. The programmable safety system activates the safety functions via a 0 signal.

Feedback from the safety functions

- Message via 1-pole semiconductor outputs, or via outputs of the SafetyNET p RTFL interface
  - 1 signal: If monitoring has been activated and within the parametrised limit values
  - 0 signal: If monitoring has been deactivated and 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.
- If SS1 is activated, the drive is stopped in accordance with its configuration.
- No other safety functions are processed or called up during this time.

Reaction to limit value violations and errors

- When the parametrised limit values are exceeded (FAULT), the SS1 safety function is triggered with the aid of the emergency stop deceleration ramp and the feedback output of the safety function is switched to the 0 signal.

- When parametrised limit values are exceeded for monitoring functions (FAULT), only the feedback output of the safety function is switched to the 0 signal.
- In the event of an internal fault (FAULT) of the safety module PMCprotego S3, the SS1 safety function is triggered with the emergency stop deceleration ramp.
- In the event of a serious fault (FATAL), for example an internal memory or data fault, the STO safety function is directly activated. The torque or force generation in the motor 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 fault is not permanent.

For further information see Operating states [📖 187].

Configuration of safety functions in the configuration tool

A maximum of 10 safety functions can be configured in the configuration tool, using function blocks. In addition, the safety function Safe Stop1 (SS1) must always be configured.

The safety function SS1 cannot be deactivated in the configurator. The input of the safety function SS1 of the safety module must always be connected to an input of the safety module (hardware or SafetyNET input).

All safety functions must be configured individually.

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

- Safe Stop 1 (SS1), a fixed component of the safety configuration
- Safe Restart Lock (SRL)
- Safe Status Output (SSO)
- Safe Brake Test (SBT)

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).

5.11.1 Permanent monitoring (optional)

Permanent monitoring means the motion and monitoring functions are permanently activated. With permanent monitoring of a safety function configured, this is active after run-up of the safety module. The safety module then automatically switches to the FSRUN state. Activation or deactivation at runtime is not possible.

- The safety function is monitored without an activation signal and permanently without a delay time.
- No external wiring is necessary.

Parameter monitoring can be configured for the following safety functions

Motion functions

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

Monitoring functions

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

Configuration of permanent monitoring in the configuration tool

Field: Permanent monitoring			
Input field	**Valid entry**	**Unit**	**Description**
Permanent monitoring	Activate/deactivate (default: deactivated)	--	Activates permanent monitoring

INFORMATION

Permanent monitoring for the safety function SLP

The situation may arise where the drive can no longer be moved back into the valid range in a controlled manner when it has left the valid position range. The safety module cannot be reset while the axis is in the invalid range.

Possible remedy:
The axis is returned mechanically (manually) to the valid range if this is technically feasible.
Alternatively permanent monitoring of the safety function must be dispensed with and activation can be performed via an input. In this case the safety function can be deactivated and the axis moved back into the permitted range.

INFORMATION

Hysteresis (optional)

If the **permanent monitoring option** has been selected in the configurator of a monitoring function, it is mandatory to select the hysteresis option (see Hysteresis for monitoring functions).

The Set/Reset function (default) is then not possible.

5.11.2 Safe torque off, STO

The STO safety function prevents torque or force generation in the motor. It is redundantly designed via two safe shutdown paths in the safety module PMCprotego S3. To prevent the motor running down in an uncontrolled manner, in normal operation the safety function STO is activated via the SS1 safety function. The STO safety function forms part of the SS1 safety function and is also configured via this function.

- The STO safety function corresponds to the definition in accordance with EN 61800-5-2.
- The STO safety function 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 realised with the STO safety function.
- The STO safety function can be used to prevent an unexpected start-up in accordance with ISO 14118 after the power supply has been switched off.
- A safety stop in accordance with EN ISO 10218-1 can be realised with the STO safety function.

INFORMATION

To achieve SIL3/PLe:
Wire the output STO2 of the safety module with the terminal STO2-ENABLE of the servo amplifier (see Single-pole hardware outputs [📖 163]).

Activation of the STO safety function

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

- During normal operation, by external activation at the optional activation input STO_ACT of the SS1 safety function, see Safe stop 1 (SS1) [📖 84].
- During normal operation, with the SS1 safety function activated, once a machine stop has been detected or the monitoring time has run out.
- In the event of an error, as an error reaction of the deceleration ramp monitoring of the SS1 safety function.
- When the STO safety function has been activated, the safety module switches to the STO operating state, see Operating states [📖 187].

Interaction with safe brake control (SBC)

If any external forces influence the motor axis (e.g. suspended loads), additional measures (e.g. a standby current brake) are required. This is to avoid hazards when the STO safety function is active, see Application of the SBC and SBT safe brake functions [📖 59]. The SBC safety function in the configuration tool must be configured for this purpose. If the STO safety function has been activated, the output is set to a 0-signal (brake activation). If the STO safety function is switched off, the hardware output of the SBC safety function is triggered, in accordance with its configuration (configuration: linking to the brake trigger signal of the Servo amplifier active or not). For ventilation purposes, the hardware output is set to the 1-signal (brake is ventilated).

For further information about the SBC safety function, see Safe Brake Control (SBC) [📖 130].

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) [84].

NOTICE

STO operating status

In the STO operating status, a 0 signal is output at all feedback outputs of the configured safety functions.
Exceptions:
Feedback output STO_ACK of the safety function SS1 reports the active status STO with a 1 signal.
Feedback output SBT_SBA of the safety function SBT remains set throughout the inspection period.

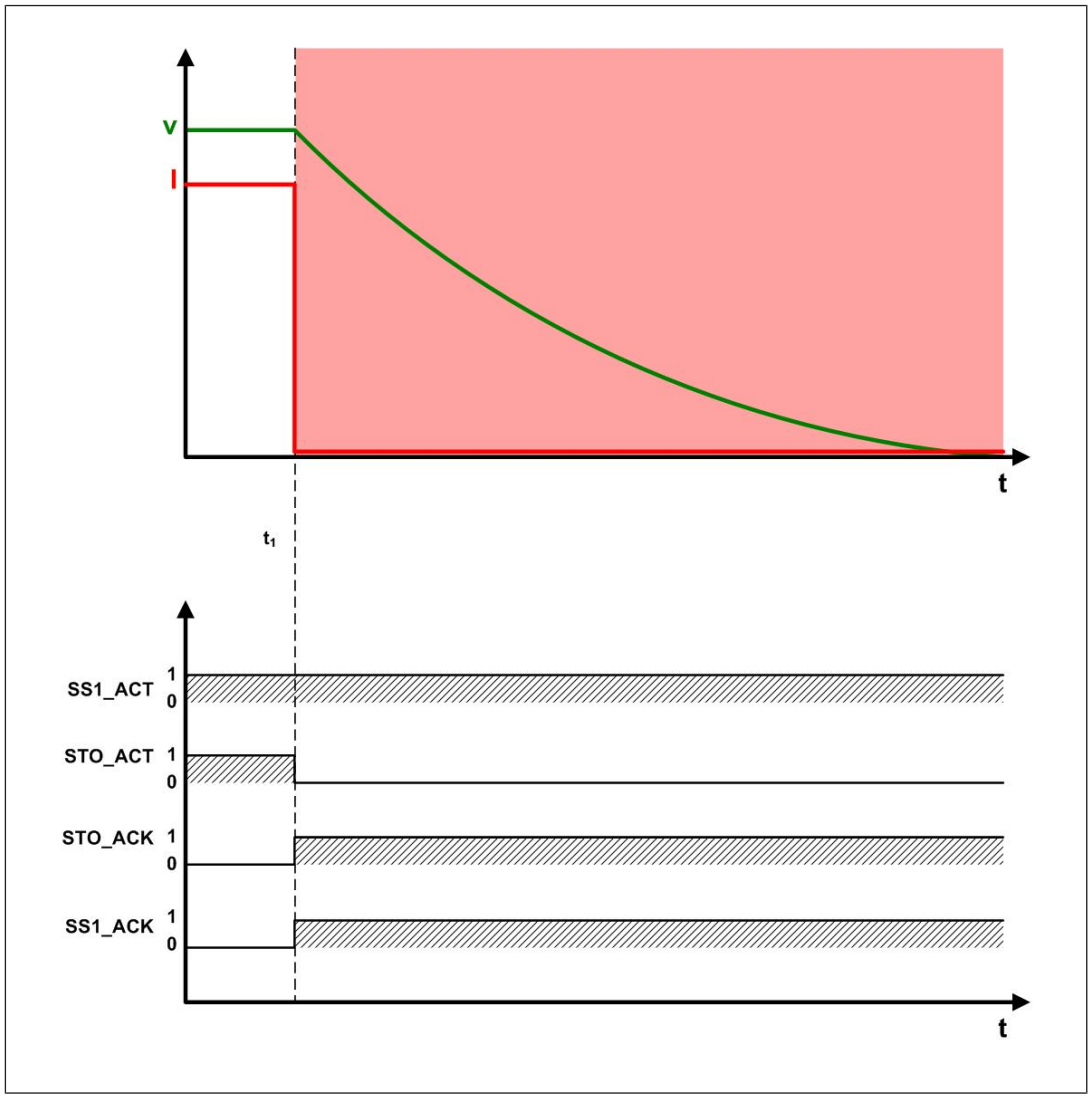


Fig.: Safety function STO

Legend

v	Speed
I	Current, torque/force generation
t_1	Activation of the safety function STO
SS1_ACT	Input for activation of the SS1 safety function
STO_ACT	Input for activation of the STO safety function. Activation input STO_ACT (optional) Input required as a second shutdown path to achieve SIL3/PLe.
STO_ACK	Output for feedback from safety function STO
SS1_ACK	Output for feedback from safety function SS1

5.11.3 Safe stop 1 (SS1)

The safety function SS1 triggers braking of the motor to a standstill. 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 must always be contained in a configuration. It cannot be used multiple times.

A RESET of the safety module can be carried out via the inputs of the safety function SS1 (see Resetting (RESET) the safety module [📖 53]).

Activating safety function SS1

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

- Normally by external activation at the activation input SS1_ACT.
- In the event of an error as a reaction upon limit value violation by other safety functions.
- In the event of an error as a reaction to an internal error in the safety module.

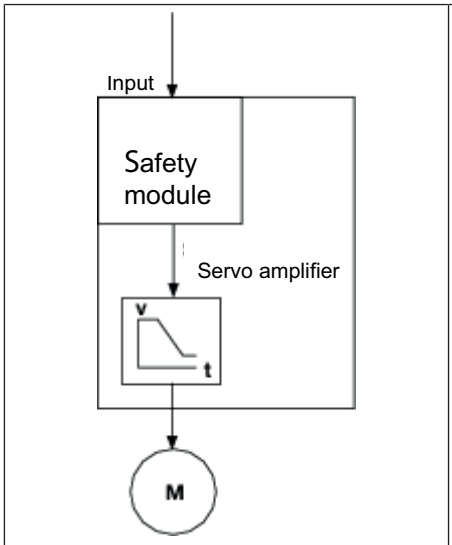
Motor shutdown in normal operation and in the event of an error

Controlling the brake ramp to shut down the motor, both in normal operation and in the event of an error, is performed either

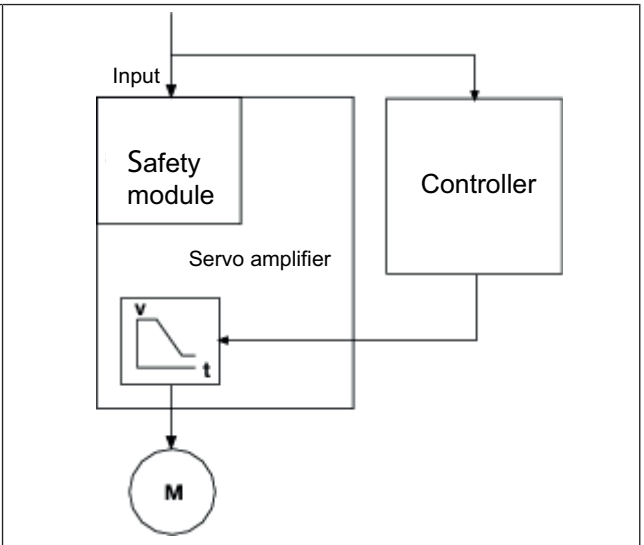
- drive-activated – by the Servo amplifier, or
- controller-activated – by a higher-level control system

Configuration of the safety function SS1 in the configuration tool

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



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 Servo amplifier.
- starts the braking process in the Servo amplifier.
- monitors the braking process.

Setpoints for a higher-level control system are ignored by the Servo amplifier while the safety function SS1 is active.

NOTICE

Drive-activated brake ramp

During drive-activated shutdown, axes lose their synchrony if the axes form a synchronous axis system via the control system.

Compensation movements of the motor may occur in the control system upon restarting.

Controller-activated brake ramp

The safety module

- provides the brake ramp (normal operation or in the event of an error) for a higher-level control system via the fieldbus connection of Servo amplifier.
- provides the signal for starting the braking process of a higher-level control system via the fieldbus connection of Servo amplifier.
- monitors the braking process.

Information on servo amplifier/control system fieldbus communication

See Chapter Field bus communication [📖 197].

Brake ramp for normal operation

Normally the motor brakes according to the brake ramp that can be set in the configuration tool.

Brake ramp in event of an error

In the event of an error the motor brakes according to the E-STOP brake ramp that can be set in the configuration tool.

Configuration of the safety function SS1 in the configuration tool

Field: Brake ramp			
Input field	**Valid entry**	**Unit**	**Description**
Brake ramp (a_{dec})	0 … 2147483647 (default: 50000000)	User-defined [default: increments/s²]	Brake ramp gradient for normal operation
E-STOP brake ramp ($a_{emergencyDec}$)	0 … 2147483647 (default: 50000000)	User-defined [default: increments/s²]	E-STOP brake ramp gradient

INFORMATION

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

INFORMATION

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

Activate STO

(see Safe torque off, STO [📖 81])

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

- After a configured delay time has elapsed in normal operation
- After a configured delay 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)

INFORMATION

The STO is activated at the very latest after the delay time has elapsed.
The safety margins in the application must be based on the safe delay time.

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SS1 in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
STO delay time (t_{del})	0 … 120000 (default: 100)	[ms]	Delay time for normal operation between activation of SS1 and shutdown with STO.
E-STOP delay time ($t_{emergencyDel}$)	0 … 120000 (default: 50)	[ms]	Delay time for E-STOP after an error leading to shutdown with STO.

Automatic STO

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

- The motor speed must fall below a configured standstill limit value.
- At a standstill limit value of 0, the software controller enable must be evaluated.
  In other words 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**
Automatic STO	Activate/deactivate (default: deactivated)	--	Activating the automatic STO.
Limit value standstill (v_{lim})	0 … 16777215 (default: 340)	User-defined [default: increments/s]	If the standstill limit value is undercut, the safety function STO is triggered.

Monitoring of brake ramp

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 position error is exceeded.

In the event of an error there are the following options

- 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: Monitoring of brake ramp			
Input field	**Valid entry**	**Unit**	**Description**
Monitor brake ramp	Activate/deactivate (default: deactivated)	--	Activating brake ramp monitoring
Position error (pos_{err})	0 … 2147483647 (default: 0)	User-defined [default: increments]	Maximum permitted position error
Error reaction	STO	--	For controller-activated brake ramp, direct triggering of the safety function STO
	E-STOP brake ramp	--	For controller-activated brake ramp, triggering of the E-STOP brake ramp (drive-activated)

Activation and feedback

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

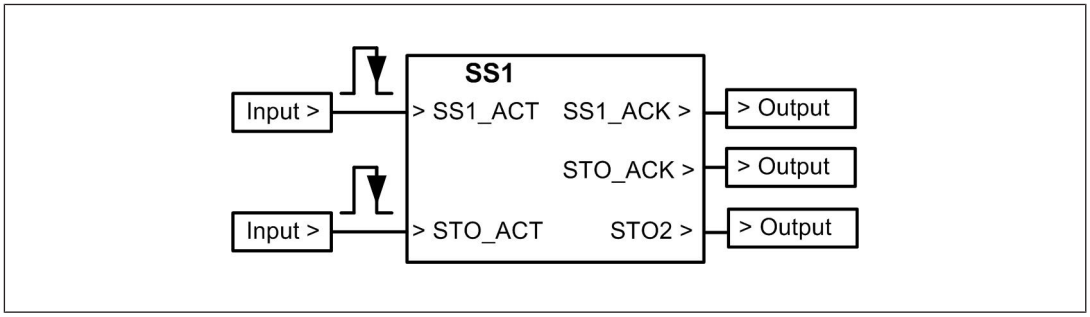


Fig.: Safety function SS1

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)
STO2	The triggering signal for the second shutdown route is output via the control output STO2. (0 signal STO activated, 1 signal STO deactivated)

Activation input STO_ACT (optional)

- The safety function STO is activated or deactivated 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.
- Second shutdown path for the higher-level controller if no error exclusion for activation can be applied.

Configuration of the safety function SS1 in the configuration tool

Input field	Valid entry	Unit	Description
I/O activation	Activate STO input	--	Use of activation input for STO

Control output STO2 (optional)

If a second shutdown path is required for the safety function STO, it can be configured in safety function SS1.

- To achieve SIL3/PLe, the control output STO2 must be mapped to a hardware output on the safety module and be wired to the input STO2 ENABLE on the servo amplifier.
- The triggering signal for the second shutdown route is output via the control output STO2. (0 signal STO activated, output stage disabled), (1 signal STO deactivated, output stage can be enabled)

Configuration of the safety function SS1 in the configuration tool

Input field	Valid entry	Unit	Description
I/O activation	Activate STO2 output	--	Use of a second STO shutdown path

NOTICE

The safety function SS1 is a fixed component of the safety configuration.
When the safety function SS1 is activated, one axis loses its synchrony with other axes in a synchronous axis system.
Safety function SS1 is present precisely once in every safety configuration.

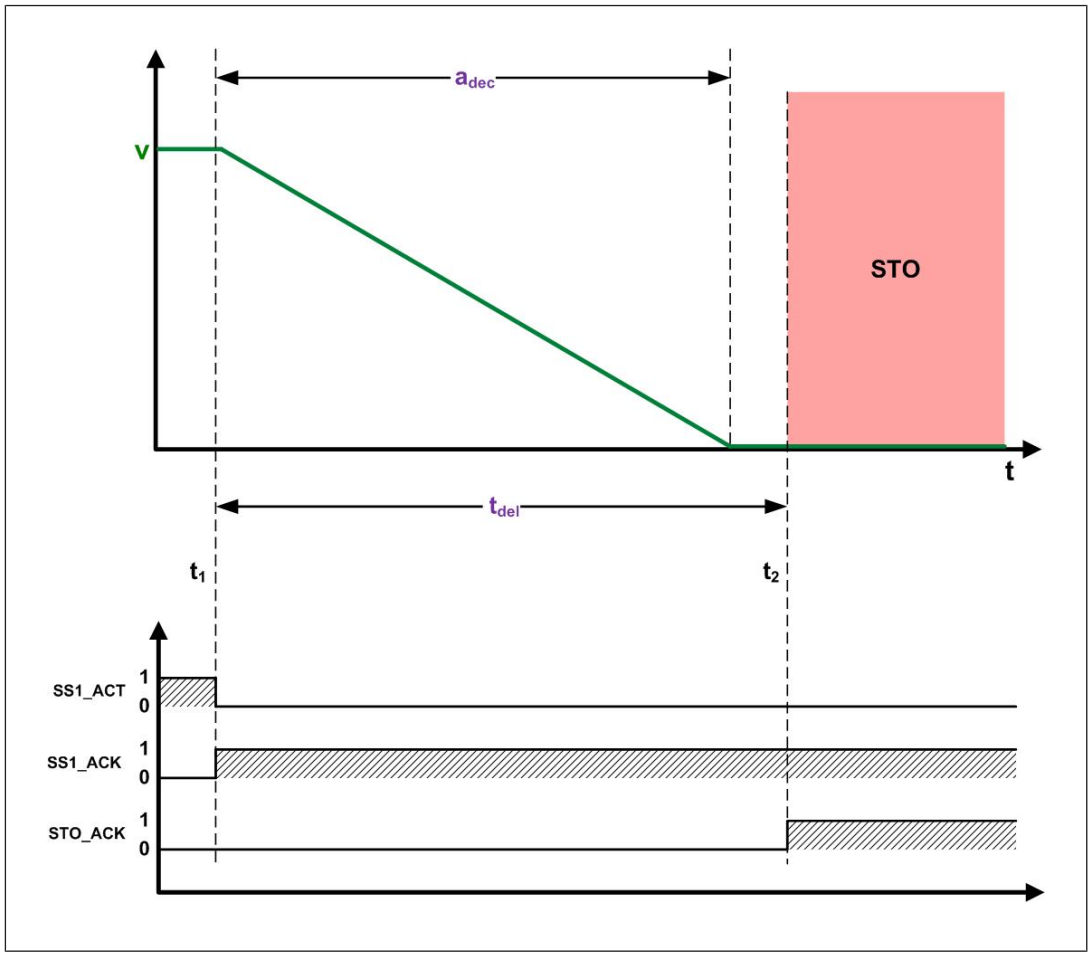


Fig.: Timing diagram: SS1 with STO once the STO delay time has elapsed

Legend

a_{dec}	Brake ramp
v	Speed
t_{del}	STO delay time
t_1	Activation of the safety function SS1
t_2	Activation of the safety function STO
SS1_ACT	Input for safety function SS1
SS1_ACK	Output for feedback from safety function SS1
STO_ACK	Output for feedback from safety function STO

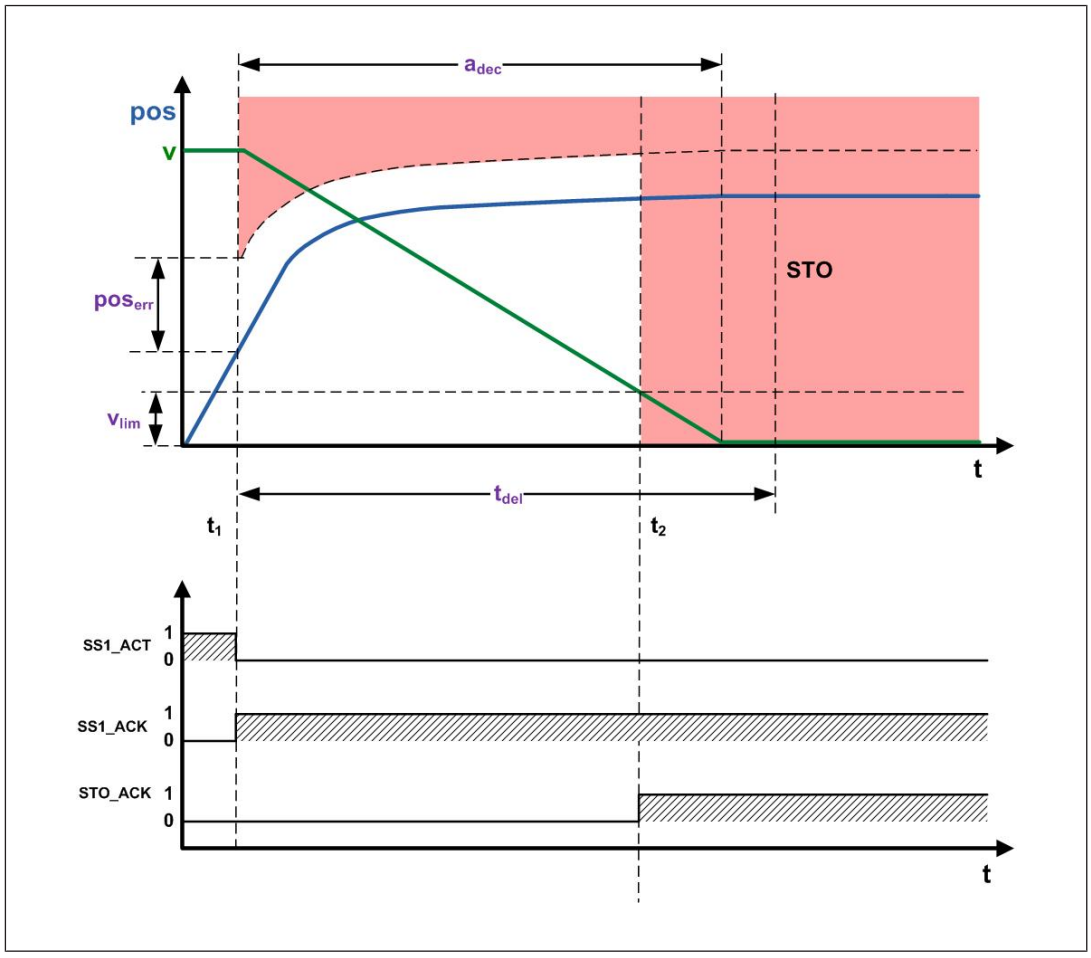


Fig.: Timing diagram: SS1 with automatic STO if standstill detected and brake ramp monitored

Legend

a_{dec}	Brake ramp
pos	Position
v	Speed
t_{del}	STO delay time
pos_{err}	Position error
v_{lim}	Standstill limit value
t_1	Activation of the safety function SS1
t_2	Activation of the safety function STO
SS1_ACT	Input for safety function SS1
SS1_ACK	Output for feedback from safety function SS1
STO_ACK	Output for feedback from safety function STO

5.11.4 Safe Stop 2 (SS2)

The safety function SS2 triggers braking of the motor to a standstill. 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 SS2 safety functions with differently configured brake ramps simultaneously. In this case it is not clearly defined what SS2 brake ramp is executed.

Activation of safety function SS2

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

- By external activation at the activation input ACT.

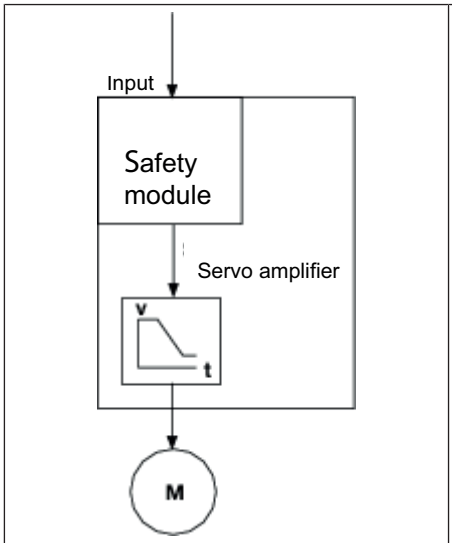
Motor shutdown

Controlling the brake ramp to shut down the motor is performed either:

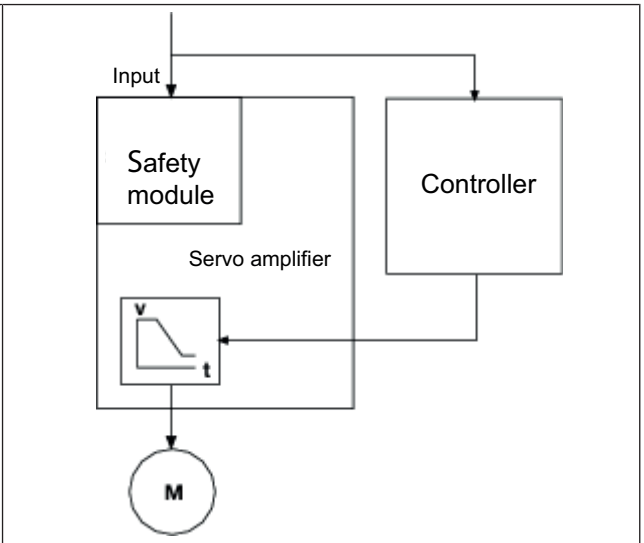
- drive-activated – by the Servo amplifier, or
- controller-activated – by a higher-level control system

Configuration of the safety function SS2 in the configuration tool

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



Drive-activated brake ramp



Controller-activated brake ramp

Drive-activated brake ramp

The safety module

- transmits the brake ramp (normal operation) to the Servo amplifier.
- starts the braking process in the Servo amplifier.
- monitors the braking process.

Setpoints for a higher-level control system are ignored by the Servo amplifier while the safety function SS2 is active.

NOTICE

Drive-activated brake ramp

During drive-activated shutdown, axes lose their synchrony if the axes form a synchronous axis system via the control system.

Compensation movements of the motor may occur in the control system upon restarting.

Controller-activated brake ramp

The safety module

- provides the brake ramp (normal operation or in the event of an error) for a higher-level control system via the fieldbus connection of Servo amplifier.
- provides the signal for starting the braking process of a higher-level control system via the fieldbus connection of Servo amplifier.
- monitors the braking process.

However the brake ramp can in addition be adjusted in the control system itself.

Information on servo amplifier/control system fieldbus communication

See Chapter Field bus communication [📖 197].

Braking ramp for normal operation

Normally the motor brakes in accordance with the braking ramp that can be set in the configuration tool.

Configuration of the safety function SS2 in the configuration tool

Field: Braking ramp			
Input field	**Valid entry**	**Unit**	**Description**
Braking ramp (a_{dec})	0 … 2147483647 (default: 10000000)	User-defined [default: increments/s²]	Braking ramp gradient for normal operation

INFORMATION

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

Braking ramp monitoring

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

Configuration of the safety function SS2 in the configuration tool

Field: Braking ramp monitoring			
Input field	**Valid entry**	**Unit**	**Description**
Monitor braking ramp	Activate/deactivate (default: deactivated)	--	Activating braking ramp monitoring
Position error (pos_{err})	0 … 2147483647 (default: 0)	User-defined [default: increments]	Maximum permitted position error

INFORMATION

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

Activate SOS

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

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

INFORMATION

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

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SS2 in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
SOS delay time (t_{del})	0 … 120000 (default: 100)	[ms]	Delay time between activation of SS2 and monitored standstill with SOS.

Monitoring

- 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.

Configuration of the safety function SS2 in the configuration tool

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

Automatic SOS (optional)

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

Configuration of the safety function SS2 in the configuration tool

Field: Automatic SOS			
Input field	**Valid entry**	**Unit**	**Description**
Automatic SOS	Activate/deactivate (default: deactivated)	--	Activating the automatic SOS.
Limit value standstill (v_{lim})	0 … 16777215 (default: 340)	User-defined [default: increments/s]	If the standstill limit value is undercut, 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:

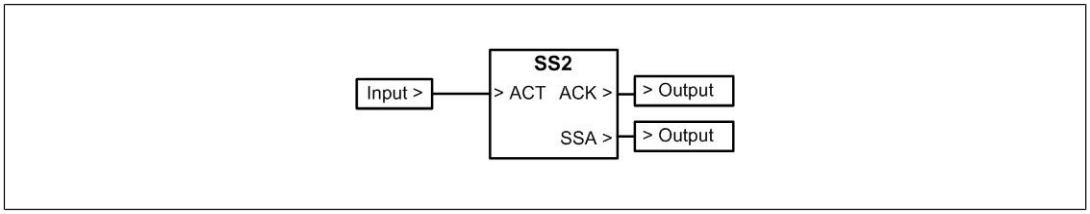


Fig.: Safety function SS2

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.

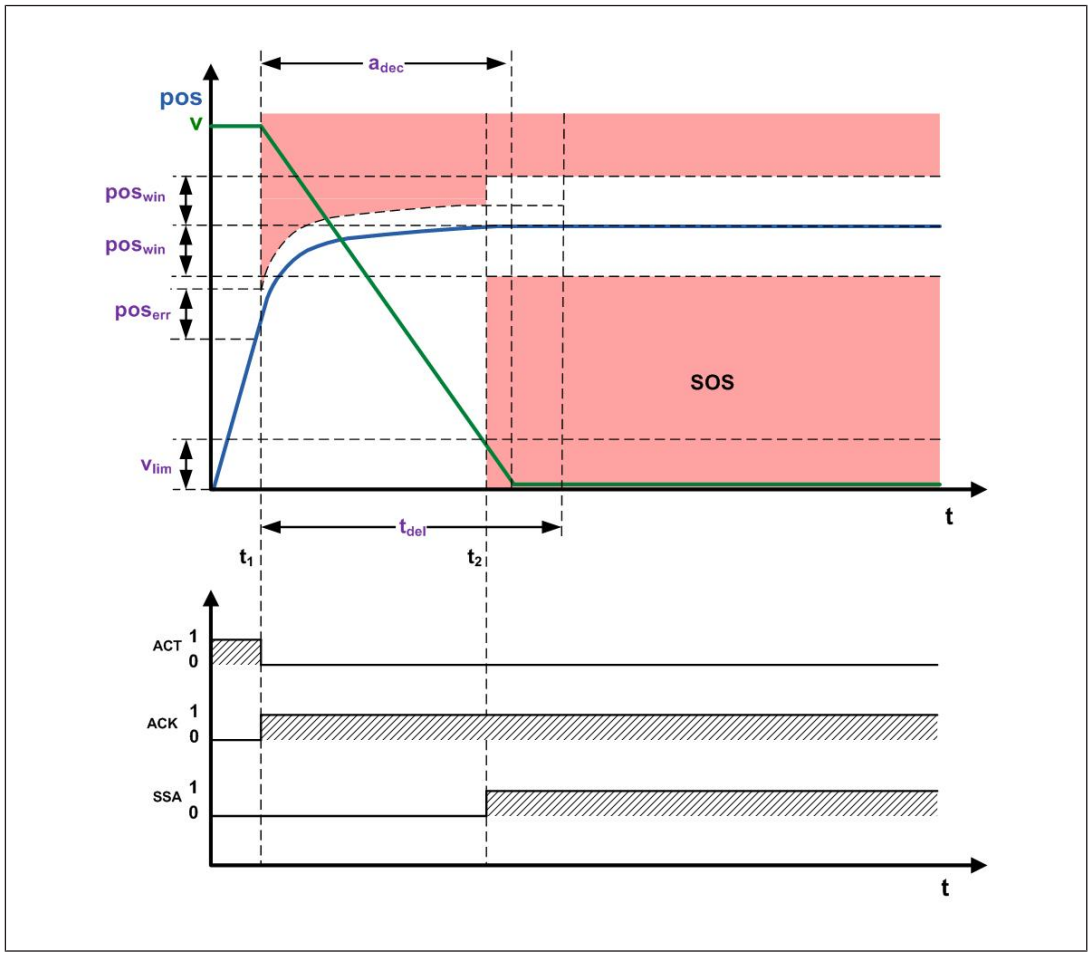


Fig.: Safety function SS2

Legend

a_{dec}	Brake ramp
pos	Position
v	Speed
pos_{win}	Standstill position window
pos_{err}	Position error
v_{lim}	Standstill limit value
t_{del}	SOS delay time
t_1	Activation of safety function SS2
t_2	Activation of safety function SOS
ACT	Input for safety function SS2
ACK	Output for feedback from safety function SS2
SSA	Safe Standstill Acknowledge Output for feedback from limit value monitoring

5.11.5 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 except for the error reaction.
When parameterised limit values are exceeded:

- no SS1 is triggered

- a 0 signal is issued at the SDA (Safe Direction Acknowledge) output

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:

- By external activation at the activation input ACT
- Permanent monitoring (optional) [79]
  - The direction is monitored without an activation signal and permanently, without an SDI delay time.
  - No external wiring is necessary.

Start of monitoring

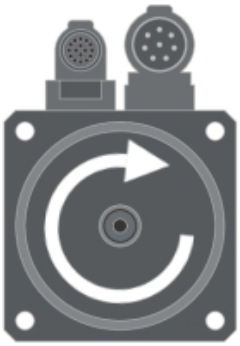
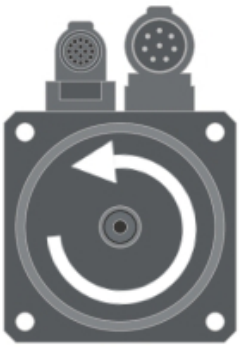
- Once the SDI delay time has elapsed, monitoring of the direction starts.
- Once the SDI delay time has elapsed, the feedback output SDA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SDI in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SDI and the point at which monitoring begins

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 motor's direction of rotation is continuously compared with the parameterised, permitted direction (positive or negative).
- A user-specific position window prevents 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 impermissible direction that exceeds the distance set in the position window, the SS1 function is triggered.

Configuration of the safety function SDI in the configuration tool

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

Field: Standstill position			
Input field	**Valid entry**	**Unit**	**Description**
Standstill position window (pos_{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, safety function SS1 is triggered.
- 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:

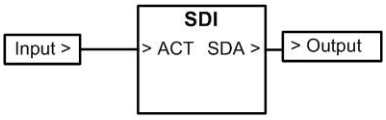


Fig.: Function block SDI

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.

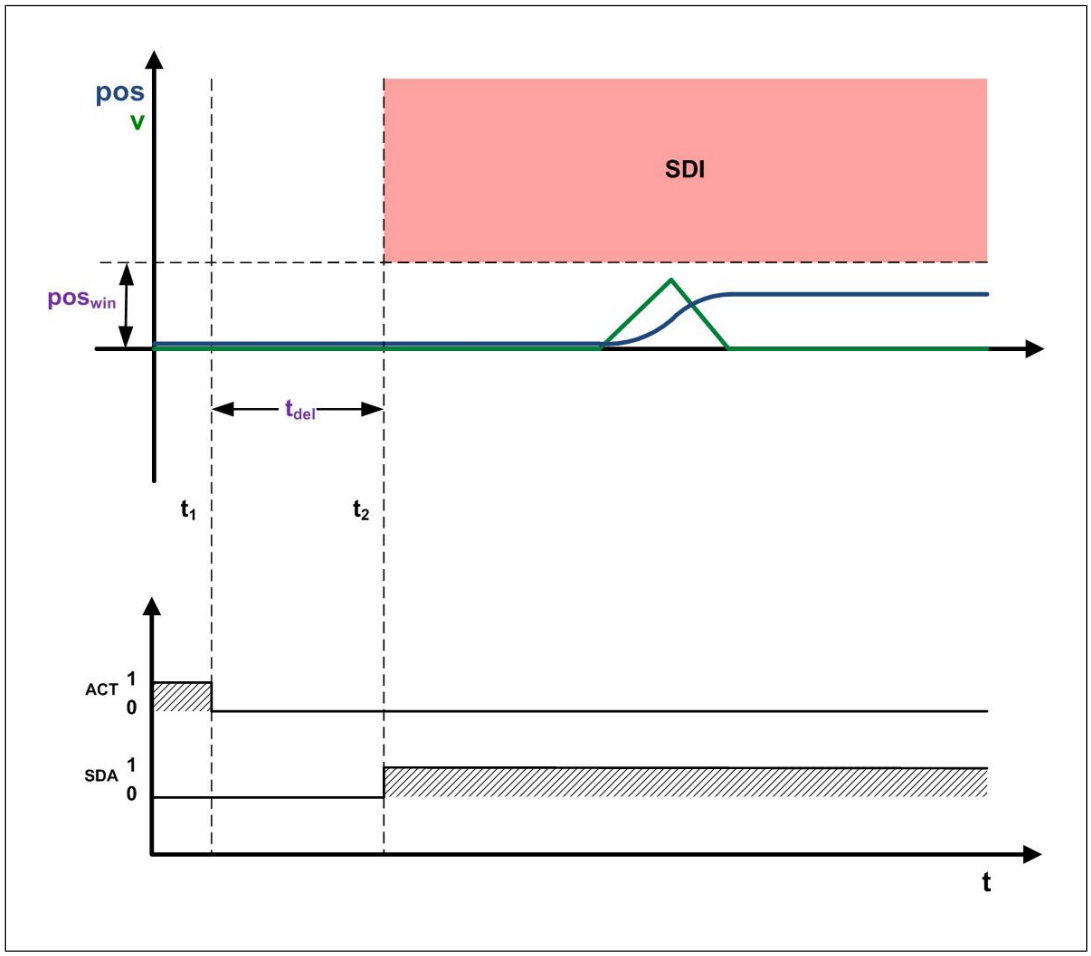


Fig.: Safety function SDI

Legend

pos	Position
v	Speed
pos_{win}	Standstill position window
t_{del}	Delay time
t_1	Activation of the safety function SDI
t_2	Start of monitoring
ACT	Input for safety function SDI
SDA	Safe Direction Acknowledge
	Output for feedback from safety function SDI

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.6 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 Monitored Increment".
The monitoring function SLI-M corresponds to the normative safety function SLI except for the error reaction.
When parameterised limit values are exceeded:

- no SS1 is triggered
- a 0 signal is issued at the SRA (Safe Range Acknowledge) output

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:

- By external activation at the activation input ACT

Start of monitoring

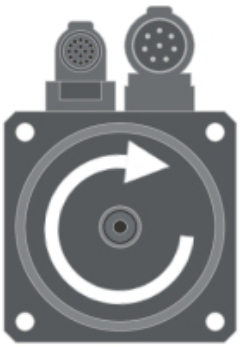
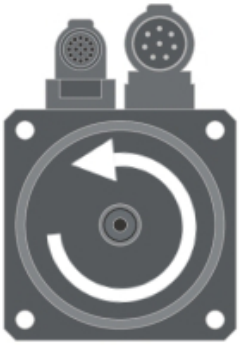
- Once the SLI delay time has elapsed, the defined increment is monitored.
- The position after the SLI delay time has elapsed is taken as the start position.
- Once the SLI delay time has elapsed, the feedback output SRA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [📖 200]) will not elapse until the following system cycle.

Configuration of the safety function SLI in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SLI and the point at which monitoring begins

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 present position of the motor is continuously compared with the set position limit values.
  If it is seen to be exceeded, an error reaction is triggered.

Configuration of the safety function SLI in the configuration tool

Field: Increment limit values			
Input field	**Valid entry**	**Unit**	**Description**
Upper limit value Position ($pos_{upperLimit}$)	0 …… 2147483647 (default: 0)	User-defined [default: increments]	If the limit value is exceeded, the safety function SS1 (E-STOP braking ramp) is activated.
Lower limit value Position ($pos_{lowerLimit}$)	0 … 2147483647 (default: 0)	User-defined [default: increments]	If the limit value is exceeded, the safety function SS1 (E-STOP braking ramp) is activated.

Error reaction SLI

- If a limit value is exceeded, safety function SS1 is activated.
- 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:

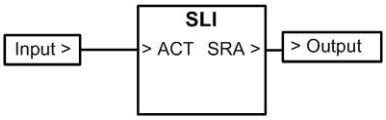


Fig.: Function block SLI

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.

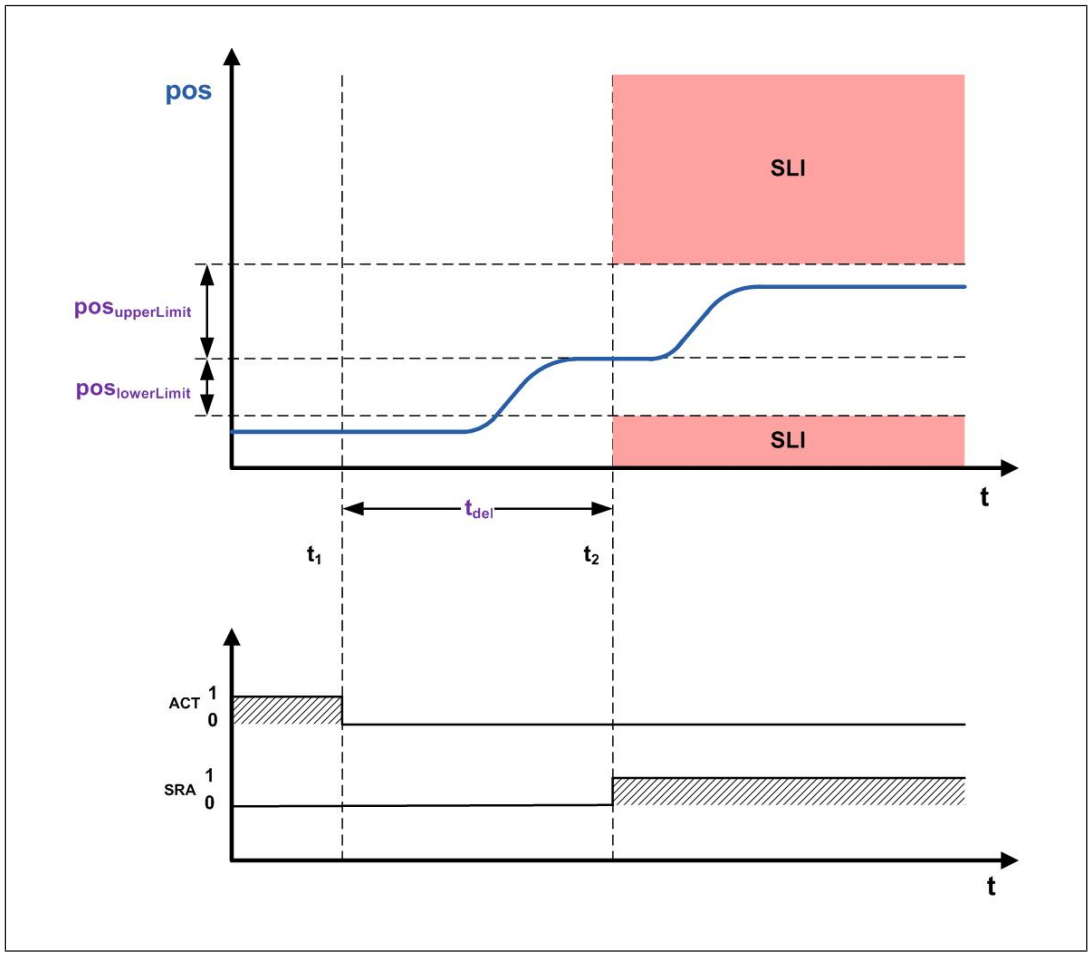


Fig.: Safety function SLI

Legend

pos	Position
$pos_{upperLimit}$	Upper limit value position
$pos_{lowerLimit}$	Lower limit value position
t_{del}	Delay time
t_1	Activation of the safety function SLI
t_2	Monitoring start
ACT	Input for safety function SLI
SRA	Safe Range Acknowledge
	Output for feedback from safety function SLI

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.7 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 parameterised limit values are exceeded:

- no SS1 is triggered

- a 0 signal is issued at the SRA (Safe Range Acknowledge) output

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:

- By external activation at the activation input ACT
- Permanent monitoring (optional) [79]
  - The speed is monitored without an activation signal and permanently, without an SLS delay time.
  - No external wiring is necessary.

Start of monitoring

- Once the SLS delay time has elapsed, the speed is monitored.
- Once the SLS delay time has elapsed, the feedback output SRA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SLS in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SLS and the point at which monitoring begins.

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.

Configuration of the safety function SLS in the configuration tool

Field: Speed limit value			
Input field	**Valid entry**	**Unit**	**Description**
Limit value speed (v_{lim})	0 … 16777215 (default: 100000)	User-defined [default: increments/s]	If the limit value is exceeded, the safety function SS1 (E-STOP braking ramp) is activated.

Error reaction SLS

- If the limit value is exceeded, safety function SS1 is triggered.
- 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:

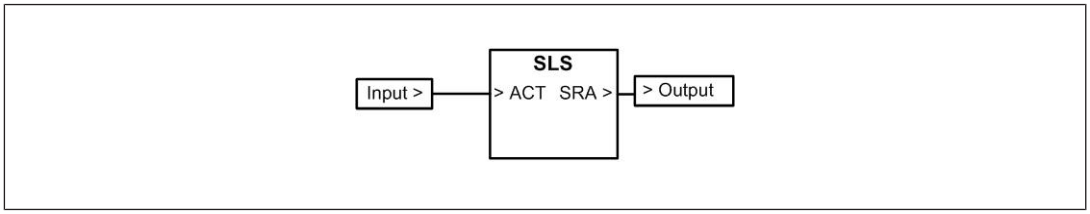


Fig.: Function block SLS

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.

Parameterising 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 parameterised 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.

Activating the tolerance range

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

Reaction

- If the first tolerance range is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Configuration of tolerance range in the configuration tool (optional)

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

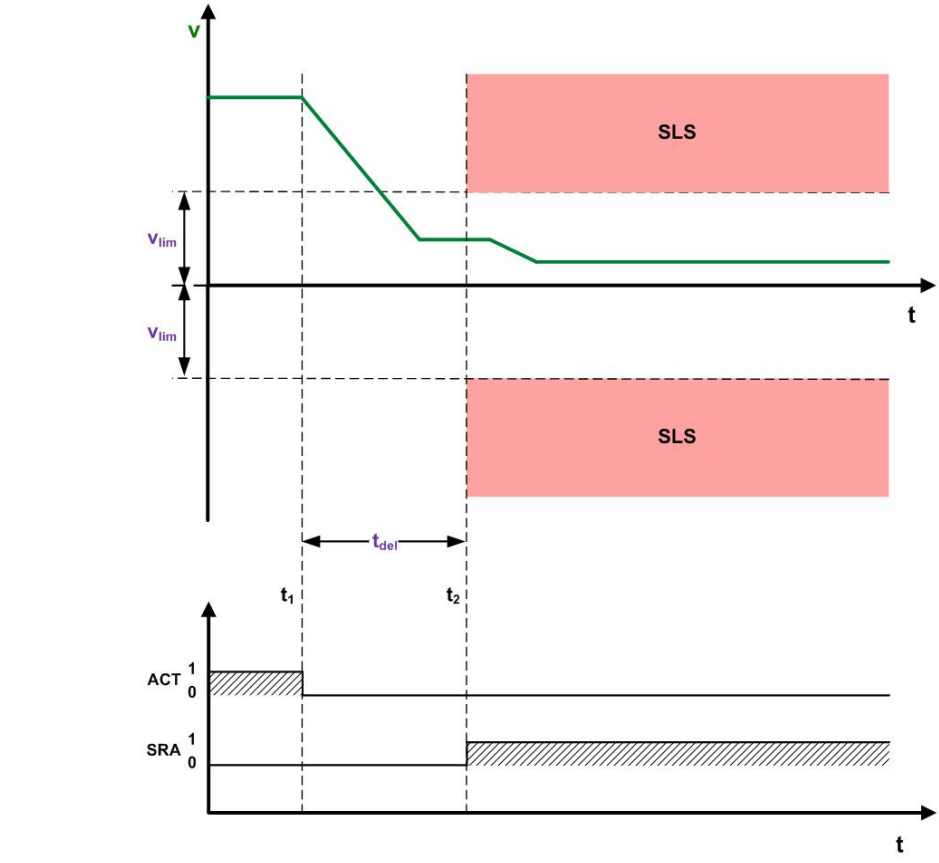


Fig.: Safety function SLS without tolerance range activated

Legend

v	Speed
v_{lim}	Speed limit value
t_{del}	Delay time
t_1	Activation of the safety function SLS

t_2	Monitoring start
ACT	Input for safety function SLS
SRA	Safe Range Acknowledge
	Output for feedback from safety function SLS

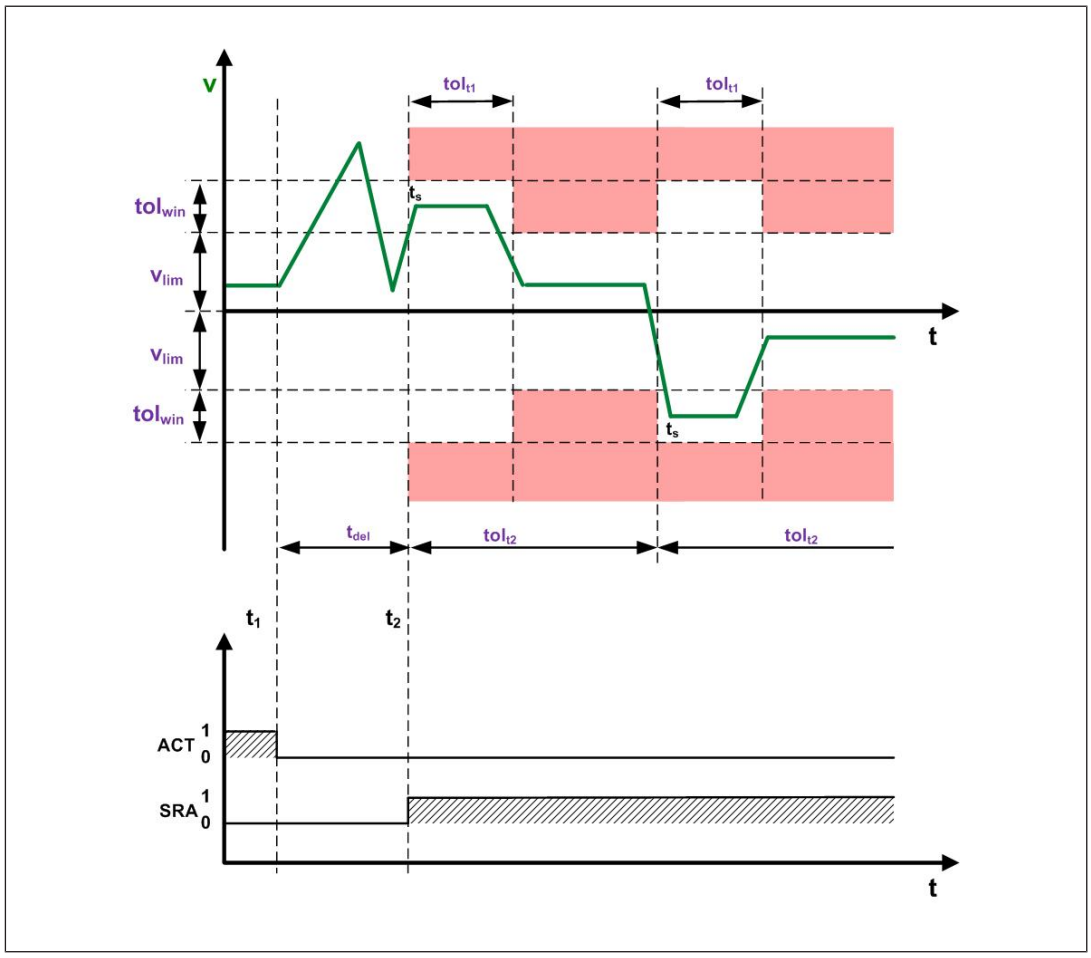


Fig.: Safety function SLS with tolerance window activated

Legend

v	Speed
tol_{win}	Tolerance window
v_{lim}	Speed limit value
t_1	Activation of the safety function SLS
t_2	Monitoring start
t_s	Speed V exceeds limit value and lies in the activated tolerance range. (tolerance window, tolerance time, tolerance period)
t_{del}	Delay time
tol_{t1}	Tolerance time
tol_{t2}	Tolerance period
ACT	Input for safety function SLS

SRA	Safe Range Acknowledge Output for feedback from safety function SLS

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.8 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 of 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 parameterised limit values are exceeded:

- no SS1 is triggered
- a 0 signal is issued at the SSA (Safe Standstill Acknowledge) output

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:

- By external activation at the activation input ACT

Start of monitoring

- Once the SOS delay time has elapsed, the motor position is monitored. It may not leave the set position window.
- The position after the SOS delay time has elapsed is taken as the start position for monitoring.
- Once the SOS delay time has elapsed, the feedback output SSA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SOS in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 100)	[ms]	Time between activation of the safety function SOS and the point at which monitoring begins

Monitoring

- 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.

Configuration of the safety function SOS in the configuration tool

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

Error reaction SOS

- If a limit value is exceeded, safety function SS1 is activated.
- 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)

For the automatic SOS, the safety function SOS is activated before the delay time 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**
Automatic standstill monitoring	Activate/deactivate (default: deactivated)	--	Activating the automatic SOS.
Limit value standstill (v_{lim})	0 … 16777215 (default: 340)	User-defined [default: increments/s]	If the standstill limit value is undercut, the safety function SOS is triggered.

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:

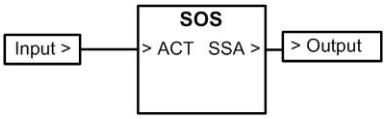


Fig.: Function block SOS

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.

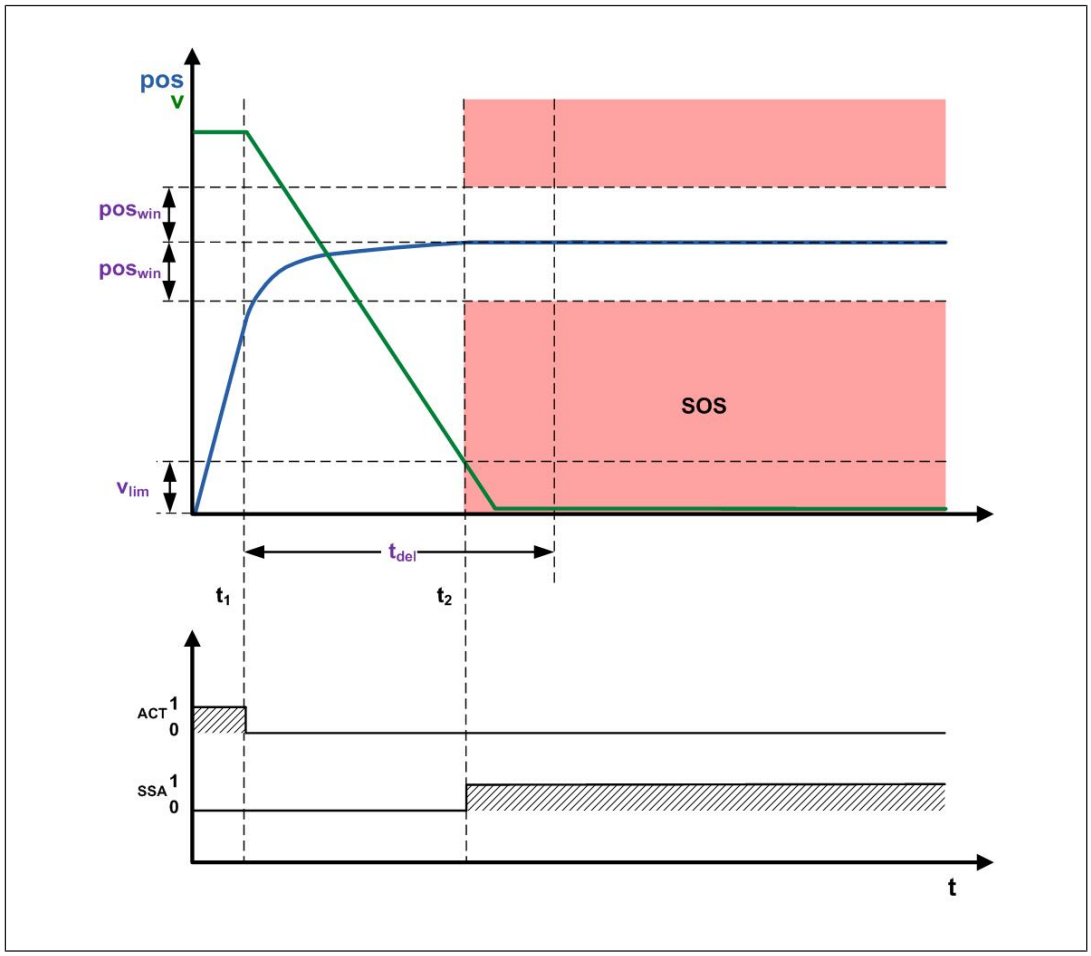


Fig.: Safety function SOS

Legend

pos	Position
v	Speed
pos_{win}	Standstill position window
v_{lim}	Standstill limit value
t_{del}	Delay time
t_1	Activation of safety function SOS
t_2	Monitoring start when automatic standstill monitoring is configured
ACT	Input for safety function SOS
SSA	Safe Standstill Acknowledge
	Output for feedback from limit value monitoring

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.9 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 parameterised limit values are exceeded:

- no SS1 is triggered

- a 0 signal is issued at the SRA (Safe Range Acknowledge) output

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:

- By external activation at the activation input ACT
- Permanent monitoring (optional) [79]
  - The speed range is monitored without an activation signal and permanently, without an SSR delay time.
  - No external wiring is necessary.

Start of monitoring

- Once the SSR delay time has elapsed, the speed is monitored.
- Once the SSR delay time has elapsed, the feedback output SRA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SSR in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SSR and the point at which monitoring begins

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.

Configuration of the safety function SSR in the configuration tool

Field: Speed limit value			
Input field	**Valid entry**	**Unit**	**Description**
Upper limit value speed ($v_{upperLimit}$)	-16777216… 16777215 (default: 100000)	User-defined [default: increments/s]	If the limit value is exceeded, the safety function SS1 (E-STOP braking ramp) is activated.
Lower limit value speed ($v_{lowerLimit}$)	-16777216 … 16777215 (default: -100000)	User-defined [default: increments/s]	If the limit value is undercut, the safety function SS1 (E-STOP braking ramp) is activated.

Error reaction SSR

- If a limit value is exceeded, safety function SS1 is activated.
- 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:

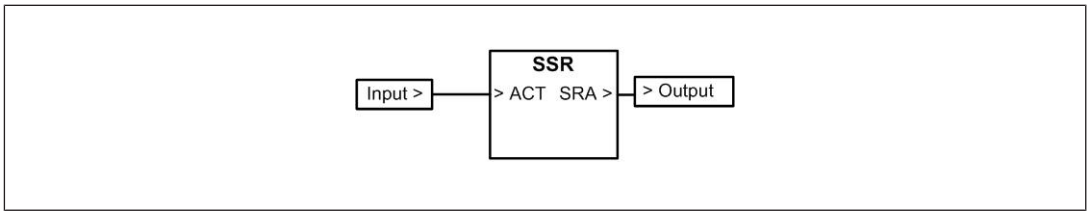


Fig.: Function block SSR

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.

Parameterising 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 parameterised 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.

Activating the tolerance range

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

Reaction

- If the first tolerance range is exceeded, the safety function SS1 (E-STOP brake ramp) is activated.

Configuration of tolerance range in the configuration tool (optional)

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

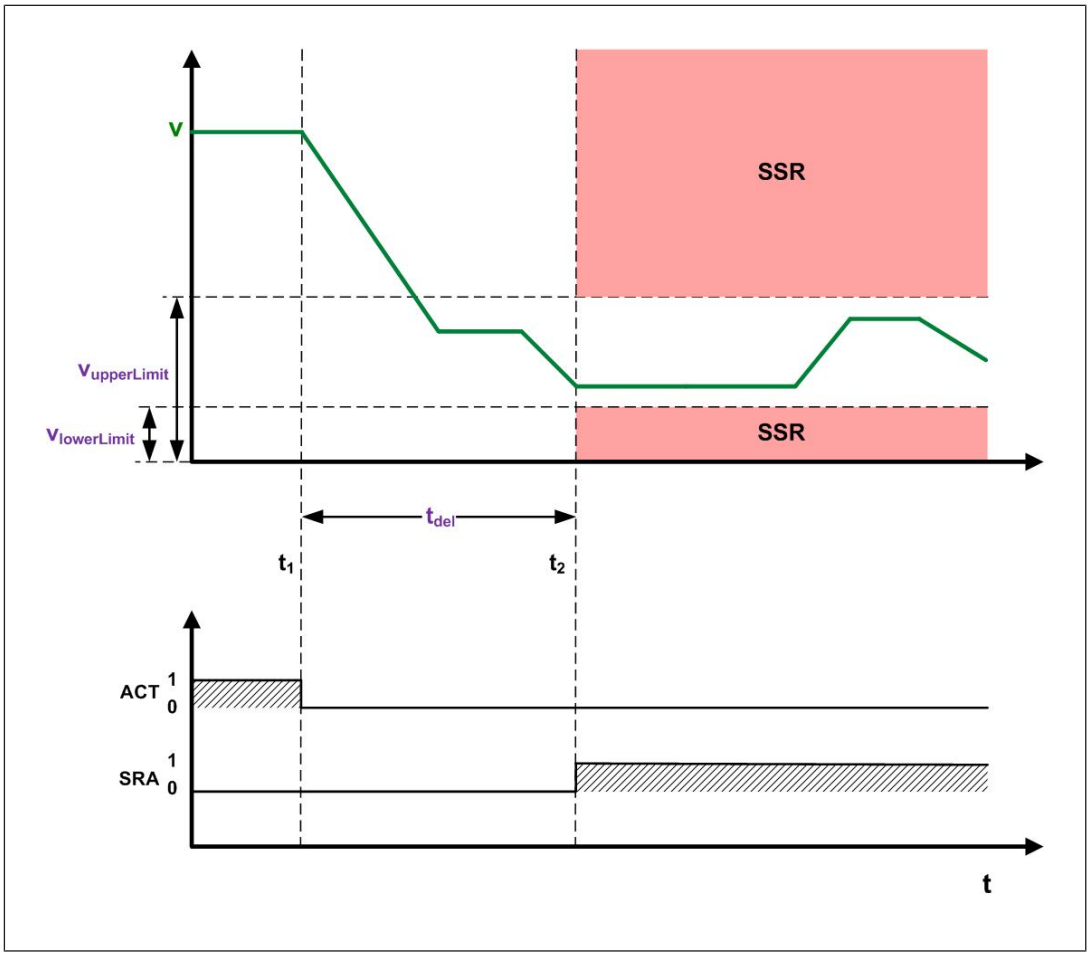


Fig.: Safety function SSR without tolerance range activated

Legend

v	Speed
$v_{upperLimit}$	Upper limit value speed
$v_{lowerLimit}$	Lower limit value speed

t_{del}	Delay time
t_1	Activation of the safety function SSR
t_2	Monitoring start
ACT	Input for safety function SSR
SRA	Safe Range Acknowledge
	Output for feedback from safety function SSR

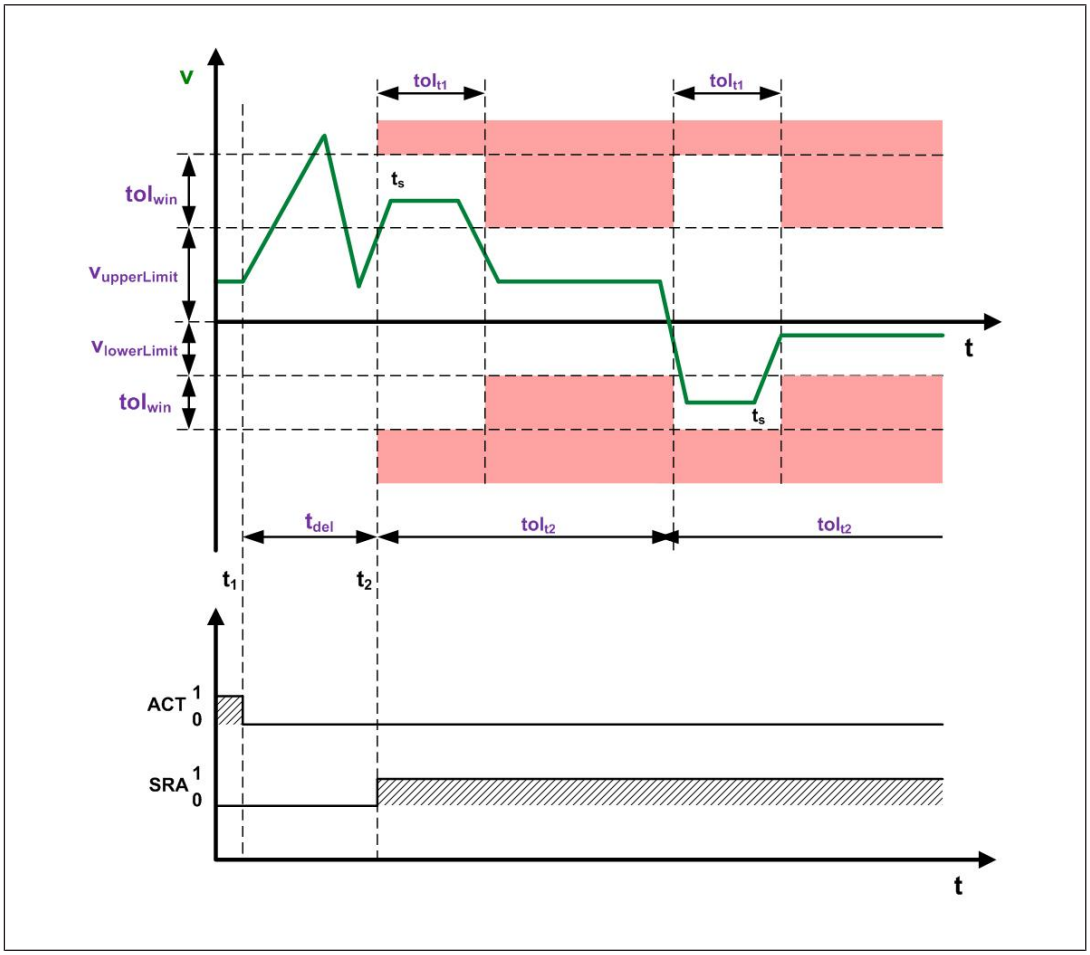


Fig.: Safety function SSR with tolerance range activated

Legend

v	Speed
tol_{win}	Tolerance window
$v_{upperLimit}$	Upper limit value speed
$v_{lowerLimit}$	Lower limit value speed
t_1	Activation of the safety function SSR
t_2	Monitoring start
t_s	Speed v exceeds limit value and activates tolerance range. (tolerance window, tolerance time, tolerance period)
tol_{t1}	Tolerance Time [ms]
tol_{t2}	Tolerance Period [ms]

ACT	Input for safety function SLS
SRA	Safe Range Acknowledge Output for feedback from safety function SSR

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.10 Safely Limited Position (SLP) and Safely Monitored Position (SLP-M)

INFORMATION

The **monitoring function SLP-M "Safely Monitored Position"** can be selected as a variant of the normative safety function SLP "Safely Limited Position".
The monitoring function SLP-M corresponds to the normative safety function SLP except for the error reaction.
When parameterised limit values are exceeded:

- no SS1 is triggered
- a 0 signal is issued at the SRA (Safe Range Acknowledge) output

The safety function SLP monitors whether the motor's motion complies with a defined lower and upper absolute position.

- The safety function SLP 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 SLP.

INFORMATION

For the safety function SLP, an additional external absolute encoder must be connected to the interface X31 of the safety module. The current position of the external encoder is verified using the absolute position of the motor encoder. The external encoder is configured in the safety module's configuration tool.

If an external encoder is used with a different (reduced) resolution range compared to the internal motor encoder resolution, the resulting overall resolution of the system may be restricted.
Equally, a reduced overall resolution range may arise if a gear ratio exists between the drive and output ends or as a result of the mechanical transmission path itself.

WARNING!

Potential loss of safety function due to overflow of the signals in the motor encoder or in the external absolute-value encoder!

Depending on the application, serious injury or death may result.
The position range of the motor encoder and external absolute-value encoder may not overflow when monitoring the absolute position.

Appropriate measures should be used to ensure that the signals are adapted to the mechanical travel.

Activation of safety function SLP

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

- By external activation at the activation input ACT
- Permanent monitoring (optional) [79]
  - The position is monitored without an activation signal and permanently, without an SLP delay time.
  - No external wiring is necessary.

INFORMATION

When you use the safety function SLP with permanent monitoring (optional), make sure that the axis can be reset to the permitted range after the limit value is exceeded.

Start of monitoring

- Once the SLP delay time has elapsed, the absolute position is monitored.
- Once the SLP delay time has elapsed, the feedback output SRA becomes active (see diagram).

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SLP in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SLP and the point at which monitoring begins

Monitoring

- The actual position of the motor is continuously compared with the set absolute position limit values (lower and upper).
  If it is seen to be exceeded, an error reaction is triggered.
- The absolute position of the motor encoder is verified using the position values of the external absolute encoder. The external encoder is configured with the safety module's configuration tool.
- The permitted position range is within the set limit values.

- With inverted monitoring, the permitted position range is outside the set limit values (optional).

Configuration of the safety function SLP in the configuration tool

Field: Position limit values			
Input field	**Valid entry**	**Unit**	**Description**
Upper limit value position ($v_{upperLimit}$)	-8388608 … 8388607 (default: 0)	User-defined [default: increments]	If the limit value is exceeded, the safety function SS1 (E-STOP braking ramp) is activated.
Lower limit value position ($pos_{lowerLimit}$)	-8388608 … 8388607 (default: 0)	User-defined [default: increments]	If the limit value is undercut, the safety function SS1 (E-STOP braking ramp) is activated.

Error reaction SLP

- If a limit value is exceeded, safety function SS1 is activated.
- A 0 signal is issued at the SRA feedback output.

Error reaction SLP-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 SLP, the following activation and feedback signals of the function can be routed to safe inputs and outputs:

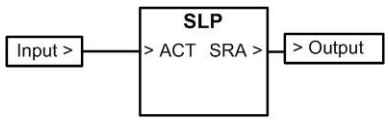


Fig.: Function block SLP

Legend

ACT	The safety function SLP 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.

SLP inverted (optional)

With inverted monitoring, the permitted position range is outside the set limit values.

Configuration of the safety function SLP inverted in the configuration tool

Field: Position range inverted			
Input field	**Valid entry**	**Unit**	**Description**
Safe range	Activate/deactivate (default: deactivated)	--	Activated position range inverted

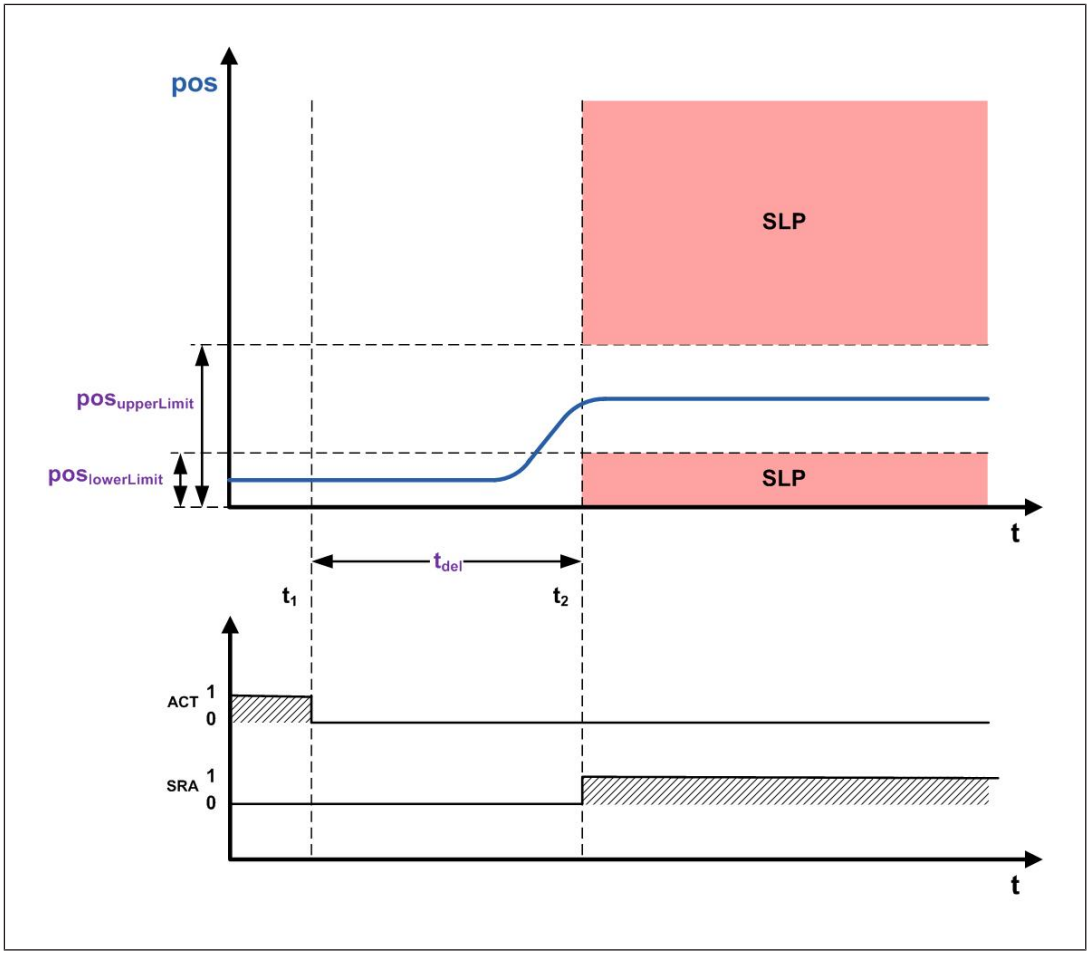


Fig.: Safety function SLP (not inverted)

Legend

pos	Position
$pos_{upperLimit}$	Upper limit value position
$pos_{lowerLimit}$	Lower limit value position
t_{del}	Delay time

t_1	Activation of the safety function SLP
t_2	Monitoring start
ACT	Input for safety function SLP
SRA	Safe Range Acknowledge
	Output for feedback from safety function SLP

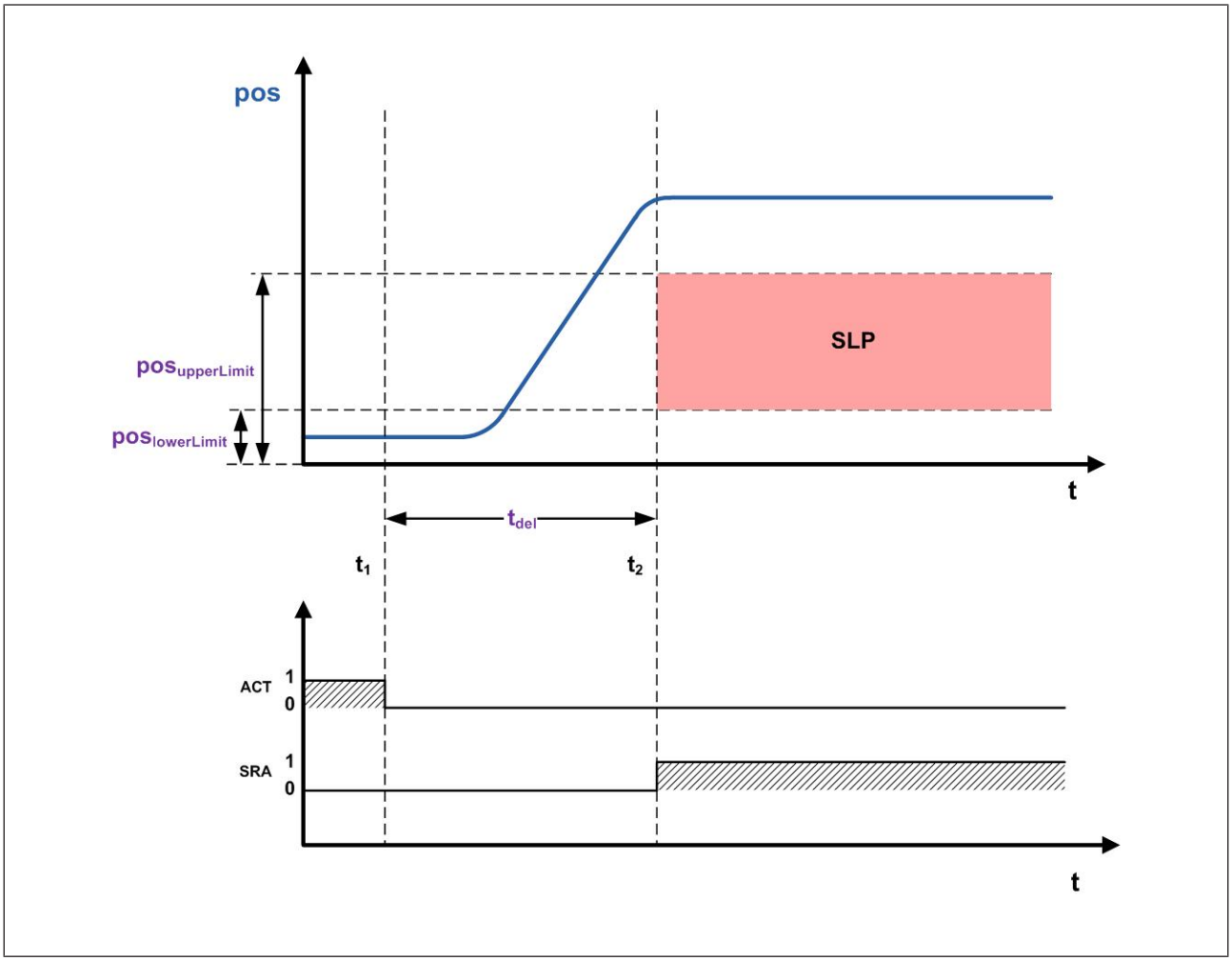


Fig.: Safety function SLP (inverted)

Legend

pos	Position
$pos_{upperLimit}$	Upper limit value position
$pos_{lowerLimit}$	Lower limit value position
t_{del}	Delay time
t_1	Activation of the safety function SLP
t_2	Monitoring start
ACT	Input for safety function SLP
SRA	Safe Range Acknowledge
	Output for feedback from safety function SLP

Hysteresis for monitoring functions

A hysteresis can be configured optionally for the monitoring functions, see Hysteresis for monitoring functions.

5.11.11 Safe Brake Control (SBC)

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

- closed-current mechanical brake or
- a safe device to control a brake (e.g. PWM switchgear PNOZ s50 for safe brake control).

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 chapter Application of the SBC and SBT safe brake functions [📖 59]

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 closed-current brake is applied, causing the mechanical braking force to be applied to the axis.

With the safety function SBC deactivated, a 1 signal is issued at the assigned output. A connected closed-current brake is released, causing the mechanical braking force to be removed from the axis

Servo amplifier brake control connection

The safety module provides the opportunity to assign the non-safety-related brake control signal from the servo amplifier PMCprotego D to the safe brake output of an SBC function. This allows the functional brake control on the servo amplifier to be combined with safe brake control through the safety function SBC.

By activating the connection, a spring-applied braking device can be used simultaneously for the following:

- Non-safety-related functions of the servo amplifier PMCprotego D
- Safety functions of the safety module PMCprotego S3

Configuration of the safety function SBC in the configuration tool

Field: Connection			
Input field	**Valid entry**	**Unit**	**Description**
Connection	Activate/deactivate (default: deactivated)	--	Activating the connection between the servo amplifier's brake control signal and the safety module

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

- The safety module is in the operating state STO
  - The safety module issues a 0 signal at the brake output.
  - The brake is applied, or the braking device prompts the brake application.
  - Control through the servo amplifier is not possible.
- The safety module is in the operating state FSRUN
  - The control of the brake output by the servo amplifier is non-safety-related.

NOTICE

In the **operating state RUN**, active safety functions must safeguard against hazardous or unpermitted movements of the drive. If the operating state STO is activated by the safety function SS1 when an error has been identified, the brake is applied safely via the safety function SBC, irrespective of the brake control signal from the servo amplifier.

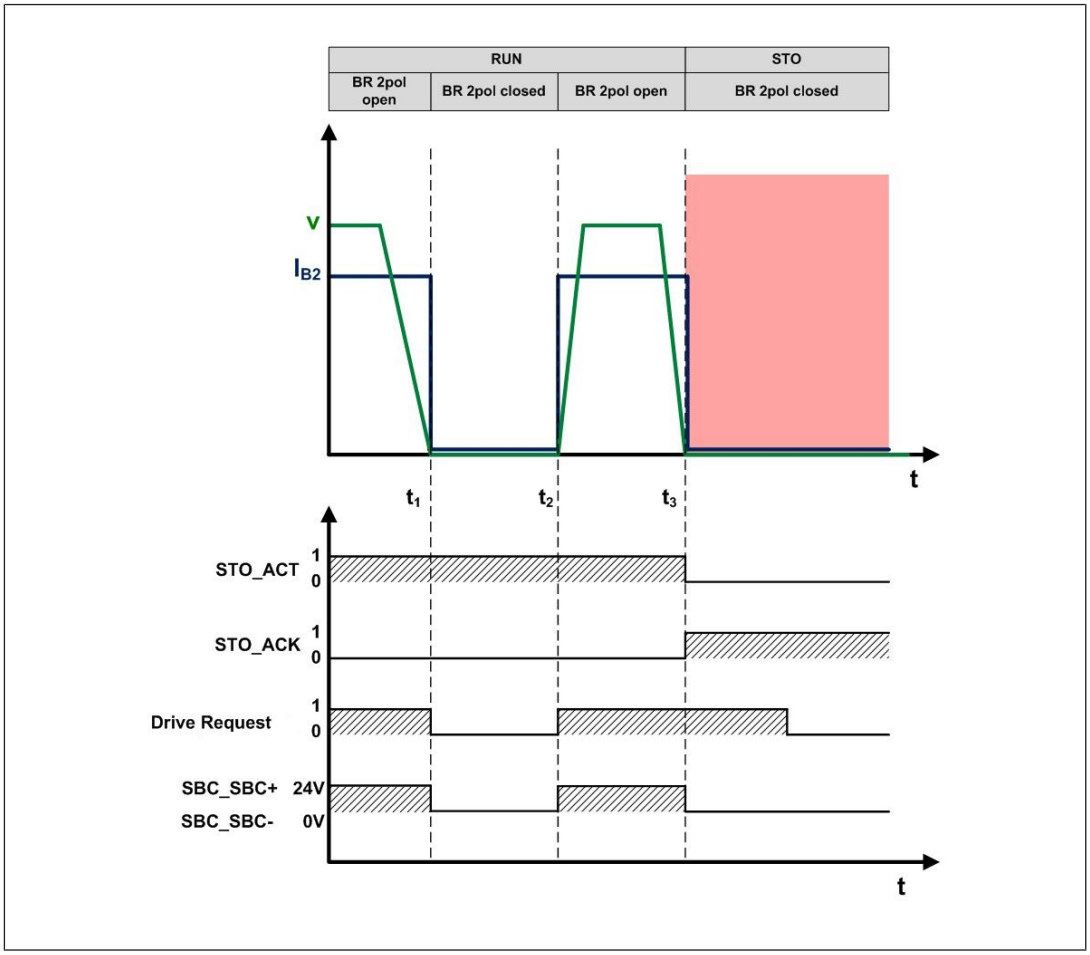


Fig.: Flow chart safety function SBC with connection activated

Legend

v	Speed
I_{B2}	Current, brake 2-pole
t_1	A non-safety-related 0 signal is issued at the brake output SBC+/SBC-.
t_2	A non-safety-related 1 signal is issued at the brake output SBC+/SBC-.
t_3	The safety functions STO and SBC are activated; a safety-related 0 signal is issued at the brake output SBC+/SBC-.
STO_ACT	Input for safety function STO
STO_ACK	Output for feedback from safety function STO
Drive request	Brake control signal from the servo amplifier
SBC+ / SBC-	Brake control output

Use of a feedback input (optional)

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

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

NO – normally open

With the braking device released a 1 signal is expected as the feedback signal.

With the braking device applied a 0 signal is expected as the feedback signal.

NC – normally closed

With the braking device released a 0 signal is expected as the feedback signal.

With the braking device applied a 1 signal is expected as the feedback signal.

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

NOTICE

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [200]) will not elapse until the following system cycle.

Configuration of the safety function SBC in the configuration tool

Field: Feedback control			
Input field	**Valid entry**	**Unit**	**Description**
Feedback input	Activate/deactivate (default: deactivated)	--	Activation of the feedback input
Type	1: Normally open (NO)	--	Contact type selection
	2: Normally closed (NC) (Default: 2)		
Delay time ON (Ton)	0 …120000 (default: 20)	[ms]	Maximum delay time when changing signal to 1 signal
Delay time OFF (Toff)	0 …120000 (default: 20)	[ms]	Maximum delay time when changing signal to 0 signal

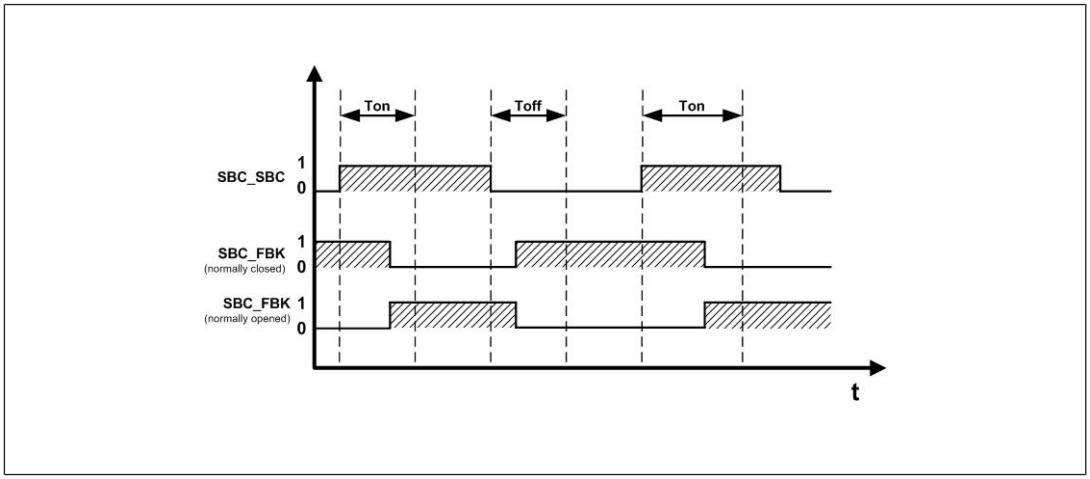


Fig.: Safety function SBC, feedback

Legend

Ton	Delay time ON Feedback when changing signal to 1 signal
Toff	Delay time OFF Feedback when changing signal to 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)

5.11.11.1 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

A maximum of two SBC function blocks can be used in the configuration tool.
Possible use of the SBC function blocks:
SBC 1-pole + SBC 1-pole
SBC 2-pole + SBC 1-pole
SBC 2-pole + SBC 2-pole

The various combinations are described in the following chapter
Application of the SBC and SBT safe brake functions [📖 59]

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

The safety function SBC 1-pole is envisaged for controlling an external safe braking device. This is connected to the assigned 1-pole safe output.

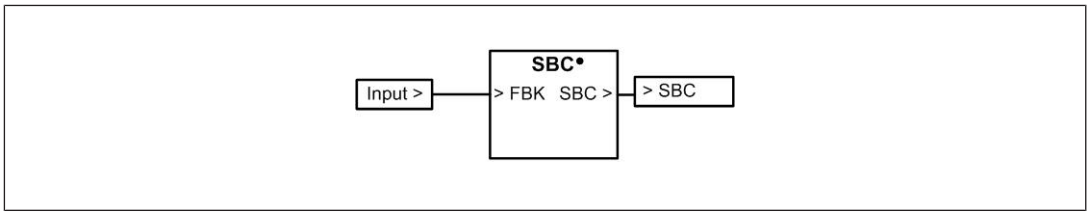


Fig.: Function block SBC 1-pole

The safety function SBC 1-pole can be assigned to any 1-pole output (O0 … Ox).

5.11.11.3 SBC with 2-pole output for direct power control of a brake

The safety function SBC 2-pole is envisaged for direct power control of closed-current, mechanical brakes. The brake is connected directly to the terminals of a 2-pole output SBC +/-.

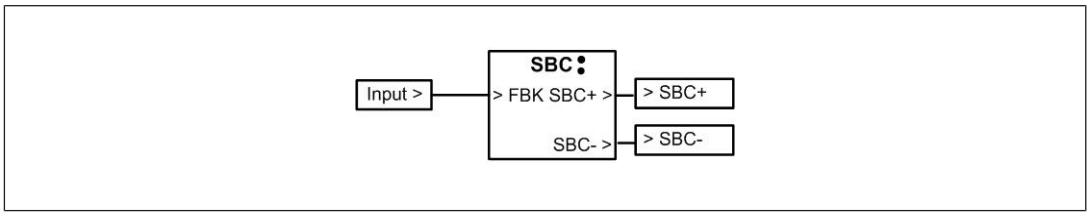


Fig.: Function block SBC 2-pole

The safety function SBC 2-pole is assigned to a 2-pole, digital output SBC+/SBC- (see Performance trigger of standby current-activated mechanical brakes by the safety module [📖 61]).

5.11.12 Safe Brake Test (SBT)

The proper functioning of a spring-applied brake 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.

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 spring-applied 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 brake can generate the necessary holding torque for the drive axle over a 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:

- Servo amplifier PMCprotego D
- A motor connected to Servo amplifier (see Permitted motor types [📖 14]) with motor encoder (see Approved motor encoders [📖 14])
- One or more spring-applied brakes/braking devices
- Safety module PMCprotego S3

"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 SBC and SBT safe brake functions [📖 59].

CAUTION!

Risk of injury

A hazardous status may occur if there is a faulty brake or braking device.
Ensure that no persons remain in the danger zone during the brake test.

INFORMATION

It is possible to run the brake test without applying power to the motor (gravity test). The safety module monitors that no power is flowing.
In this way it is possible to implement cyclical testing of spring-applied, mechanical brakes in accordance with EN ISO 16090-1.

Inspection period and tolerance time

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

The inspection period

- should be limited to a maximum of 8 h.
- can be set in the configuration tool.
- is monitored in a safety-related way.
- 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 way.

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

- the motor is shut down with the safety function SS1.
- the safety module switches to the FAULT state.

If the RUN state is achieved after the safety mode 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: Time Settings			
Input field	**Valid entry**	**Unit**	**Description**
Period	X … 10000 (default: 480)	[min]	Time after which the safety function SBT must be executed. Max. 8 h
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 ACT
- By internal activation via Servo amplifier

Configuration of the safety function SBT in the configuration tool

Field: Activation			
Input field	**Valid entry**	**Unit**	**Description**
Drive Activated	Activate/deactivate (default: deactivated)	--	Activation of the safety function SBT is by the parameters for Servo amplifier .

Start of test sequence

With external activation on the safety module's activation input

- Once the SBT delay time has elapsed, the test sequence starts.
- Once the SBT delay time has elapsed, the feedback output SSA becomes active.
- The SBT delay time is adjustable in the configuration tool.

With internal activation via the servo amplifier

- The test sequence starts without a delay time.
- The feedback output SSA is active.

INFORMATION

Please note that delay times that are not a multiple of the processor system's cycle time (see Technical details [📖 200]) will not elapse until the following system cycle.

The configuration of the safety function SBT in the configuration tool

Field: Delay time			
Input field	**Valid entry**	**Unit**	**Description**
Delay time (t_{del})	0 … 120000 (default: 20)	[ms]	Time between activation of the safety function SBT and the point at which monitoring begins

Test sequence procedure

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

The entire test sequence is monitored via a total time t_{Σ} (timeout) that is adjustable 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 and the safety module switches to the FAULT state. 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: Maximum total time			
Input field	**Valid entry**	**Unit**	**Description**
Total time (t_{Σ})	0 … 2147483647 (default: 120000)	[ms]	If the brake test is not performed within the total time, an error reaction is triggered.

INFORMATION

The total duration of the brake test (parameter total time t_{Σ}) 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 total test sequence, standstill of the drive is monitored from a safety-related perspective. The permitted position window for standstill monitoring can be set in the configuration tool.

Field: Position window			
Input field	**Valid entry**	**Unit**	**Description**
Standstill position window (pos_{win})	0 … 2147483647 (default: 50)	User-defined [default: increments]	Position window of the safety function SOS (SOS is active throughout the entire brake test).

Aborting of the test sequence

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

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

After aborting

- the safety function STO is activated.

▶ 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 a waiting period that can be set (in the configuration tool).

Field: Steps			
Input field	**Valid input/ Permanently set**	**Unit**	**Description**
Waiting time (t_{wait})	0 … 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.
Refer to the brake's data sheet for details of the brake application time.

Additional configuration options for all test steps

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

Field: Current ramp			
Input field	**Valid entry**	**Unit**	**Description**
Current 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	0 … 10000 (default: 100)	[ms]	Defines the waiting time needed to completely release a brake, before power is activated. Mechanical movements are required in order to release a brake.

Test step

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

In the test step,

- 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).
- The brake or braking device to be tested is controlled so that a braking force is applied.
- Motor standstill is monitored from a safety-related perspective.
- The amplitude of motor current is monitored for compliance with the tolerance window that is adjustable in the configuration tool.

Configuration of the safety function SBT in the configuration tool

Field: 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: 500)	[ms]	Duration of energisation
Brake	**0** – brake servo amplifier BR+/BR-*	--	Specification of brake for testing
	1 – SBC nameX*	--	Specification of brake for testing
	2 - SBC nameY*	--	Specification of brake for testing
*Brake servo amplifier BR+/BR- When the motor brake on the standard brake output BR+/BR- of the servo amplifier (connector X9) is operated, the duration of the energisation phase, (injection of the test current) must be expanded by the brake release time of the motor brake.			
*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 brake 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.

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

- the safety function SS1 is activated.
- the safety module switches to the FAULT state.

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 a badly designed configuration of the safety function SBT are available in the diagnostic document “Safety module PMCprotego S3 – Diagnostics”.

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.

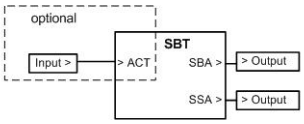


Fig.: Function blocks SBT

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 test period has not yet elapsed (1 signal) or that the brake test is in progress (0 signal) or that the test period has elapsed (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 Servo amplifier (selectable in the configuration tool).

INFORMATION

The safety function SBT is activated with a positive edge.
The safety function SBT is the only safety function that has direct influence on the drive axle by applying power to the motor. All other safety functions monitor the drive axle controlled by the Servo amplifier.

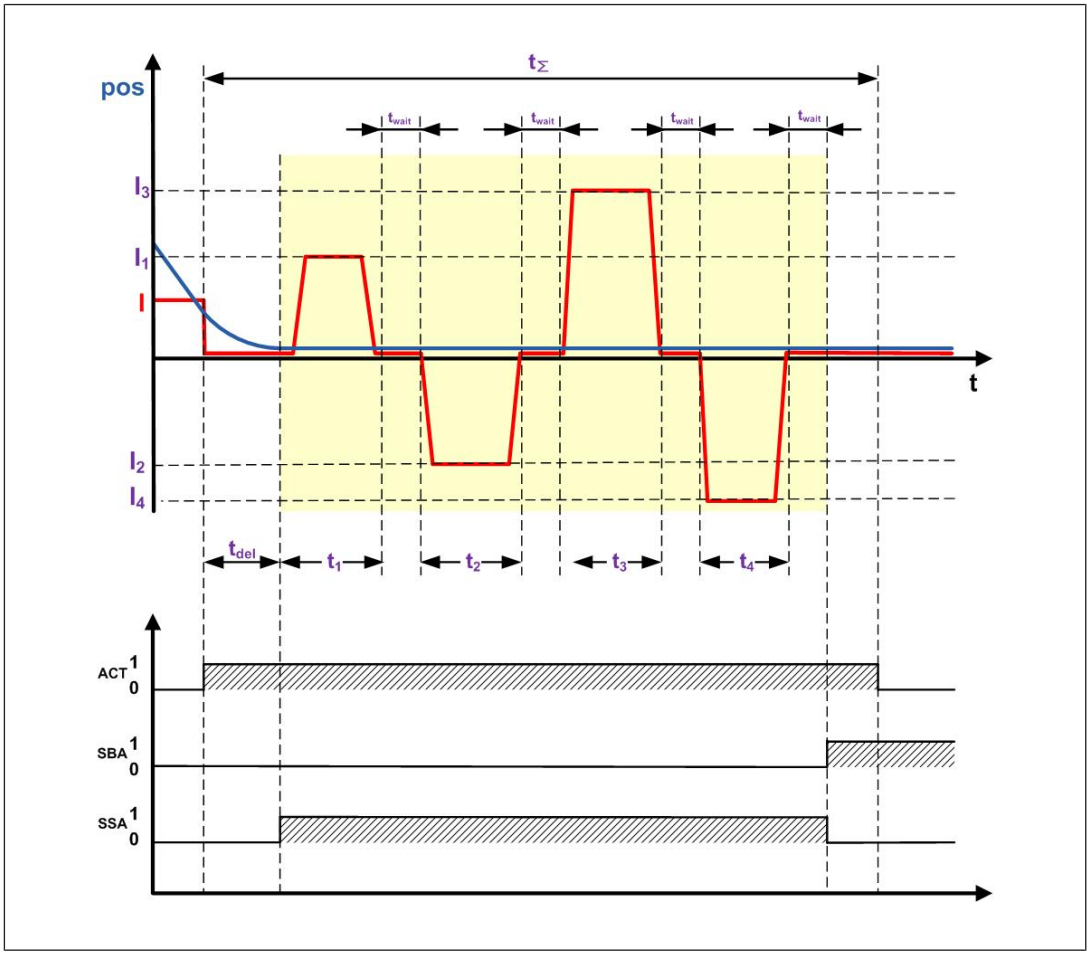


Fig.: Safety function SBT

Legend

pos	Position
t_Σ	Total time
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
t_{del}	Delay 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
ACT	Input for safety function SBT
SBA	Safe Brake Acknowledge Output for feedback from safety function SBT
SSA	Safe Standstill Acknowledge Output for feedback from standstill monitoring

5.11.13 Safe Restart Lock (SRL)

The safety function SRL prevents the safety module from leaving the operating status STO by a reset. An unexpected or unintended motor start-up is thus not possible.

- 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.

Activation of the safety function SRL

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

- By external 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:

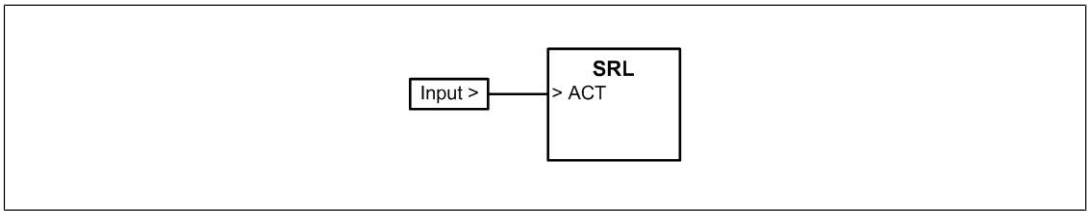


Fig.: Function block SRL

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.

Supplementary information on the RESET behaviour is provided in the following sections:
Safe restart of the machine [52]
Resetting (RESET) the safety module [53]

Switching from 0 signal to 1 signal

Various actions can be configured in the configuration tool.

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

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

1 signal (deactivated)

A RESET is possible (optionally 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 action No RESTART occurs.
	1: ACK ERR	--	Acknowledge error No RESTART occurs.
	2: RESTART	--	Acknowledge error The RESTART is triggered.

INFORMATION

A RESET of the safety module (switching to the operating status RUN) can only take place if the activation input SS1_ACT (and STO_ACT, if configured) has a 1 signal.

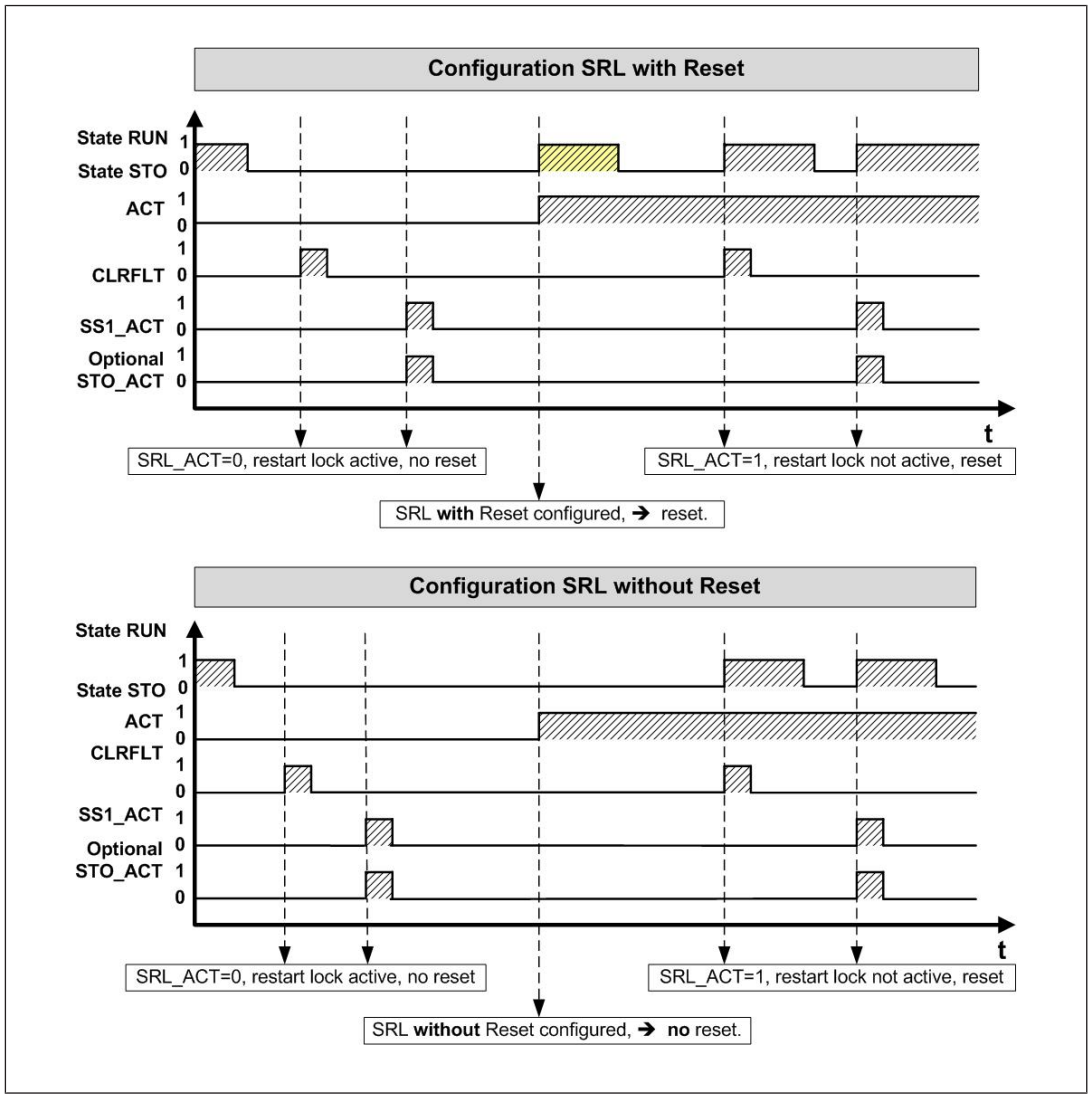


Fig.: Safety function SRL, RESET

Legend

State RUN	State RUN
State STO	State STO
ACT	Input for safety function SRL
CLRFLT	The CLRFLT command was performed via the servo amplifier
SS1_ACT	Input for safety function SS1
Optionally STO_ACT	Input for safety function STO

5.11.14 Safe Status Output (SSO)

The safety function "Safe Status Output" (SSO) reports the current 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.

The safety function SSO does not require explicit activation.

Output READY

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 [📖 187]
  - Safety module is in STARTUP, see Operating states [📖 187]
  - Fatal error

Output FSRUN

1 signal

- A motion-monitoring safety function is active
  (in other words excluding SSO, SBC, SRL or the safety function SS1 if braking ramp monitoring is not configured).
- Standstill monitoring during the brake test SBT is active (“delay time” phase is already complete).
- The safety module is in the operating state FSRUN (see Operating states [📖 187])

0 signal

- No motion-monitoring safety function is active
  (in other words, SSO, SBC, SRL or the safety function SS1 may be active if braking ramp monitoring is not configured).
- Standstill monitoring during the brake test SBT is not active (for example, during the “delay time” phase).
- The safety module is not in the operating state FSRUN (see Operating states [📖 187])

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

1 signal

- The safety module has no error.

0 signal

- The safety module has an error.

Feedback

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

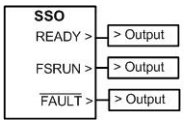


Fig.: Function block SSO

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.

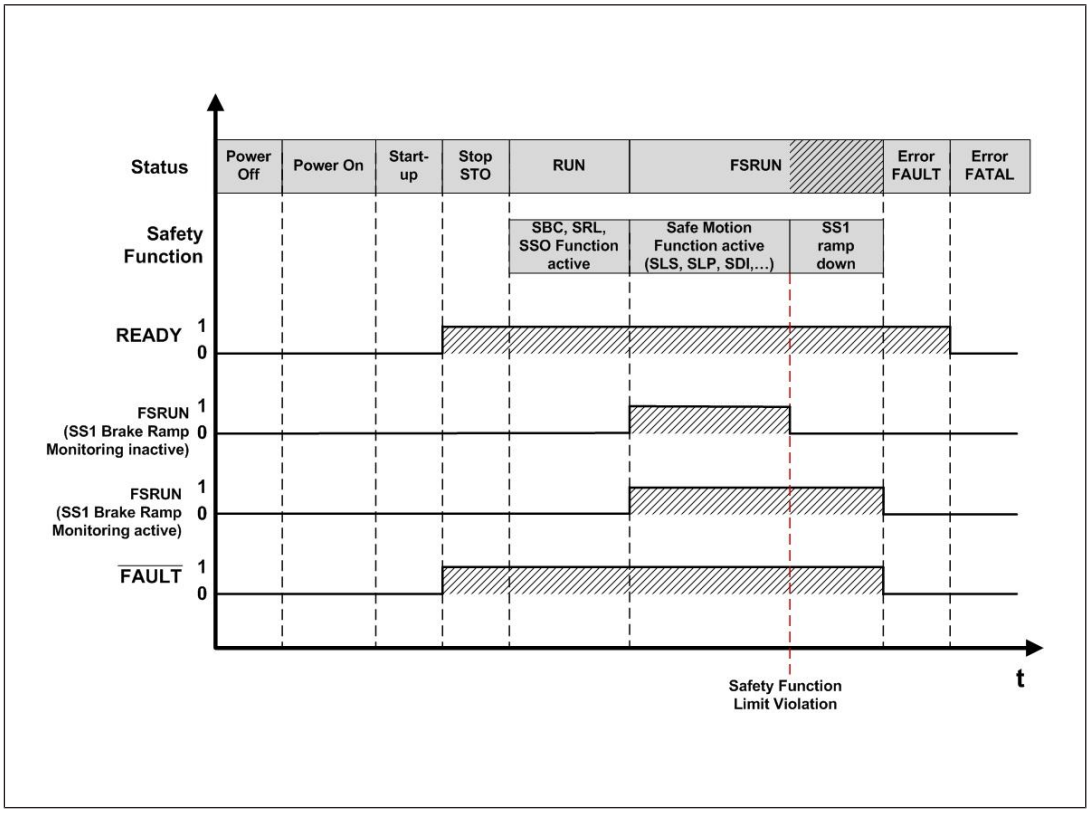


Fig.: Safety function SSO

Legend

Status	Status of safety module
Safety Function	Safety functions
READY	Output for feedback on whether the safety module is operational.

FSRUN (SS1 brake ramp monitoring inactive)	Output for feedback on whether a safety function is active. (The safety functions SSO, SBC or SRL are excluded, the safety function SS1 with non-activated brake ramp monitoring)
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, the safety function SS1 with activated brake ramp monitoring)
$\overline{\text{FAULT}}$	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 Operating mode of the servo amplifier

Activation of safety functions SS1 and SS2 has repercussions on the servo amplifier's operating mode:

SS1 when OPMODE = 0 ... 8

- The drive-activated safety function "safe stop 1" (SS1) behaves the same in all of the servo amplifier's operating modes, as ultimately the movement is not continued. The safety module must be reset to resume operation.
- The status of the safety module (SS1 activated) is transmitted to the servo amplifier. As a result, the information is available to a higher-level control system (status word).
- The transfer of setpoint values from external servo amplifier interfaces (bus system or analogue input) is disabled.
- The servo amplifier applies speed-controlled braking with the preset braking ramp until standstill is achieved, and disables the servo amplifier's power element.
- When the set delay time has elapsed, the safety module activates the safety function STO. The servo amplifier cannot be restarted.

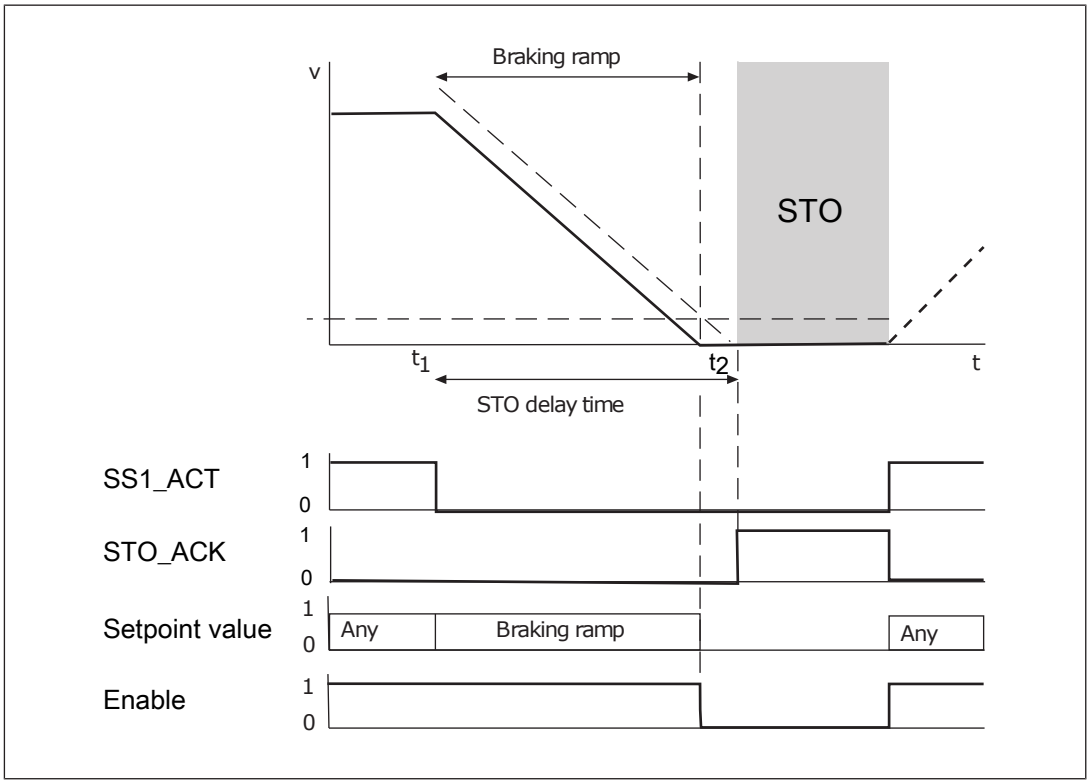


Fig.: Behaviour servo amplifier for the safety function SS1

Legend

SS1_ACT	Input for activation of the SS1 safety function
STO_ACK	Output for feedback from safety function STO
Setpoint	Specification of setpoint values
Activate	Servo amplifier's readiness for operation

SS2 when OPMODE = 0 ... 8

- With the drive-activated safety function "safe stop 2" (SS2), the movement is ultimately continued.
- The status of the safety module (SS2 activated) is transmitted to the servo amplifier. As a result, the information is available to a higher-level control system (status word).
- The transfer of setpoint values from external servo amplifier interfaces (bus system or analogue input) is disabled.
- The servo amplifier applies speed-controlled braking with the preset braking ramp until standstill is achieved.

  This status is maintained for as long as safety function SS2 is active.
- If safety function SS2 is deactivated, the status word is updated.
- The servo amplifier automatically switches to the OPMODE that was originally set.
- The transfer of setpoint values from external servo amplifier interfaces (bus system or analogue input) is once again permitted.
- When OPMODE = 8, the existing motion block can be continued via the "CONTINUE" command.

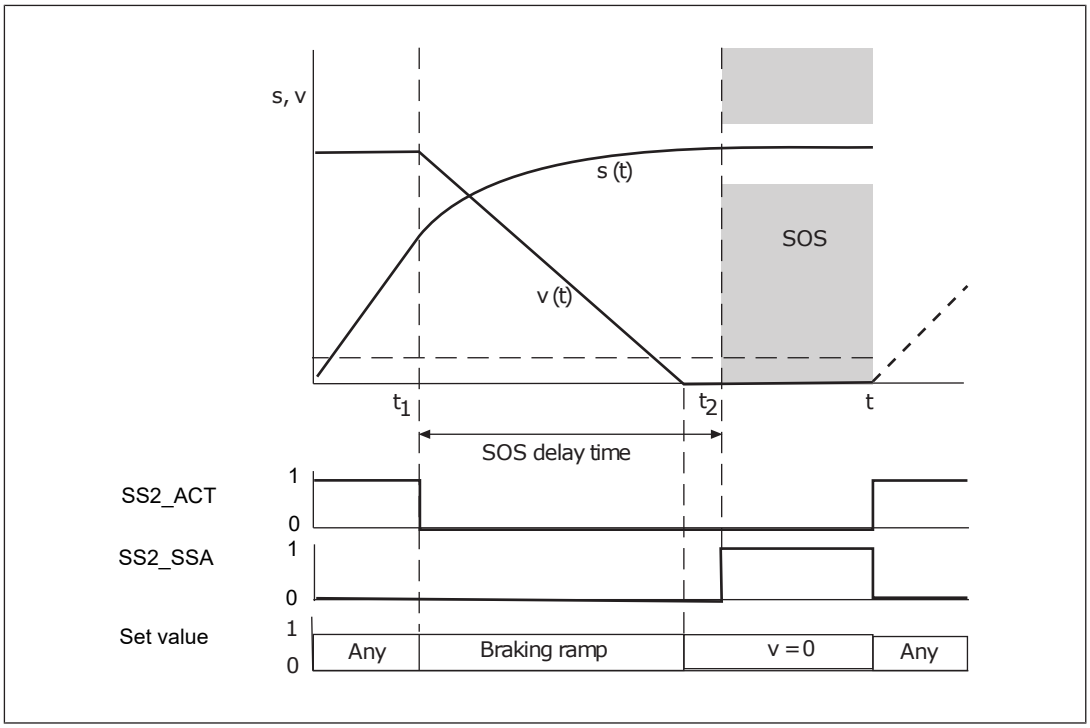


Fig.: Behaviour servo amplifier for the safety function SS2

Legend

SS2_ACT	Input for activation of the safety function SS2
SS2_SSA	Output for feedback from safety function SOS
Setpoint	Specification of setpoint values

INFORMATION

Further information on the commands of the servo amplifier can be found in the servo amplifier's online help.
Please also refer to the operating instructions for the servo amplifier.

5.13 Configuration

Safety module configuration

INFORMATION

The safety module is delivered without a configuration.
Before operation is possible, a configuration must be created and the safety configuration must be transferred to the safety module.

The safety functions to be carried out by the safety module are defined in the configurator (PASmotion):

- Configuration of the safety functions required for safe motion sequences. In the event of an error, the safety functions switch off the power element of Servo amplifier.
- Setting the parameters
  - for limit values
  - for braking ramps for the safety functions
  - for monitoring motion sequences
- The inputs and outputs are mapped to the safety functions.
- Selection and configuration of the safe, inputs/outputs, which are transferred via the SafetyNET p RTFL interface. The inputs and outputs are mapped to the SafetyNET p RTFL subscribers in the configuration tool PNOZmulti Network Editor (optional).

Transfer of the configuration to the safety module:

- Online from the configurator to the safety module (download)
  - In single-axis systems or in networked systems without PMCprimo the configuration is made via the RS232 interface of the servo amplifier (point-to-point connection).
  - For networked systems with PMCprimo via the RS 232 or Ethernet interface on the higher-level control system. The control system PMCprimo passes the configuration to the respective safety module.
- Transfer of the configuration from the SD memory card of the servo amplifier to the safety module

Transfer of the configuration from the safety module:

- Online from the safety module to the configurator (upload)
- The configuration is saved on the servo amplifier's SD memory card
- The plausibility of the configuration is checked as it is uploaded.

In online mode it is possible to

- Display of the safety module’s operating states

- Display messages of the safety module (error stack)
- Download configuration to the safety module
- Upload configuration from the safety module to the PC
- The configuration is saved on the servo amplifier's SD memory card

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
- Project has unique checksum

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 Installation

6.1 General requirements

Please also refer to the operating manual for the servo amplifier.

CAUTION!

Damage due to electrostatic discharge!

Electrostatic discharge can damage components. Ensure against discharge before touching the safety module, e.g. by touching an earthed, conductive surface or by wearing an earthed armband.

6.2 Dimensions

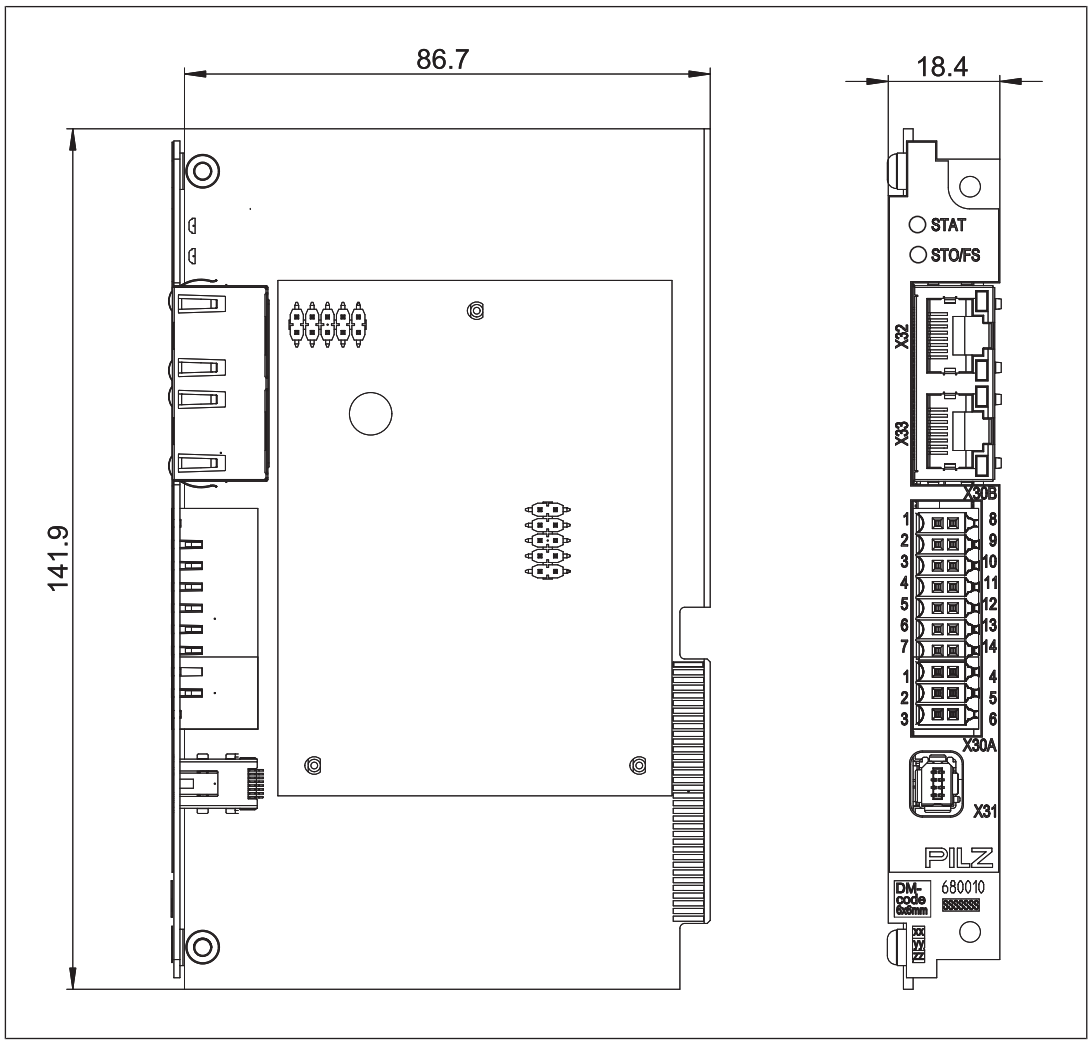


Fig.: Dimensions, stated in mm

6.3 Installation of the safety module

The expansion card is installed in slot 3 of the servo amplifier. When installing, please note the guidelines given under "Installation" in the operating manual of the servo amplifier.

1. Remove the film.

2. Break the middle link

3. Break the top link and lever out the cover plate

4. Use suitable pliers, pull out the blank in the safety module plug

5. Plug in the safety module and tighten the enclosed screws

7 Wiring

7.1 General wiring guidelines

Hardware inputs

Note the wiring considerations described in the following chapter.
Activation of the safety functions via hardware inputs [📖 27]

Hardware outputs

Note the wiring considerations described in the following chapter.
Feedback of the safety functions via hardware inputs [📖 29]

Cable material

- Use copper wiring.
- Max. cable lengths
  - – Supply voltage: Max. 30 m
  - – Hardware inputs and outputs: Max. 30 m
  - – 2-pole hardware outputs max. 30 m

Conductor cross-sections:

X30A, X30B				
Connection type DIN 46228/4	**Maximum conductor cross-section [mm²]**	**AWG**	**Ferrule length [mm]**	**Stripping length [mm]**
Flexible with crimp connector with plastic sleeve	0.75	18	12	14
Flexible with crimp connector with plastic sleeve	0.5	20	10	12

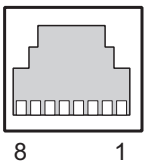
INFORMATION

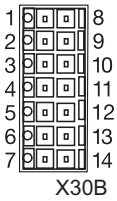
When the motor brake is not connected to the standard brake output BR+/- of the servo amplifier, but to the SBC outputs of the safety module, the following should be noted:
The connection cable of the motor brake must be extended using a terminal or a crimp connector.

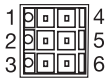
Please note:

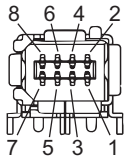
- To prevent EMC interferences (particularly common-mode interferences) the measures described in EN 60204-1 must be executed. This includes the separate routing of cables of the control circuits (input, start and feedback loop) from other cables for energy transmission or the shielding of cables, for example.

7.2 Connector pin assignment

X32, X33	Pin	Description
	1	RJ45 See SafetyNET p RTFL [📖 168]
	2	
	3	
	4	
	5	
	6	
	7	
	8	

X30B	Pin	Designation	Description
	1	I0	Safe hardware input
	2	I1	Safe hardware input
	3	I2	Safe hardware input
	4	I3	Safe hardware input
	5	O0	Safe hardware output
	6	O1	Safe hardware output
	7	O2	Safe hardware output
	8	I4	Safe hardware input
	9	I5	Safe hardware input
	10	I6	Safe hardware input
	11	I7	Safe hardware input
	12	O3	Safe hardware output
	13	O4	Safe hardware output
	14	O5	Safe hardware output

X30A	Pin	Designation	Description
 X30A	1	SBC1+	Output to control external brake1 +
	2	SBC2+	Output to control external brake 2 +
	3	24 V DC	Supply voltage for Safety module (24 V DC) and external encoder
	4	SBC1-	Output to control external brake 1 -
	5	SBC2-	Output to control external brake 2 -
	6	0 V	Reference potential for safety module (0 V) and external encoder (0 V)

Connector X31	Pin	Description
	1	External encoder [165]
	2	
	3	
	4	
	5	
	6	
	7	
	8	

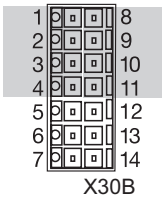
7.3 Shielding

The signal lines of the encoder must be shielded because of the noise immunity:

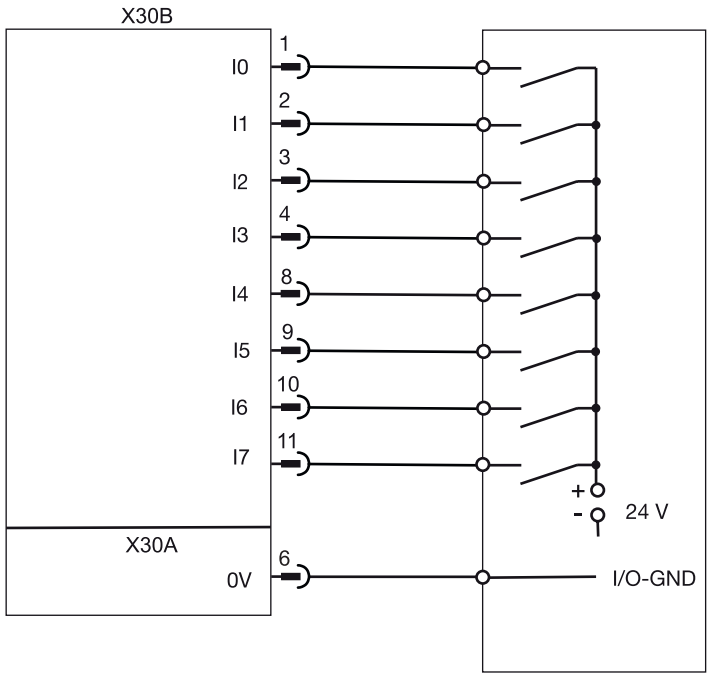
- All shielded cables are to be attached at both ends to the shield terminals provided or should be connected to the connector housing.
- Use cables with braided shield, with a minimum cover area of 80 %.
- Any interruptions to the shielding e.g. at terminals, should be at low impedance over a wide area.
- All connectors or sockets should be fastened with screws to ensure ample, conductive contact between the braided shield and the front plate.

The shield of the encoder's signal lines is connected to the connector housing.

7.4 Hardware inputs

Pin X30B	Pin	Designation	Description
	1	I0	Safe hardware input
	2	I1	Safe hardware input
	3	I2	Safe hardware input
	4	I3	Safe hardware input
	8	I4	Safe hardware input
	9	I5	Safe hardware input
	10	I6	Safe hardware input
	11	I7	Safe hardware input

Connector pin assignment

Input circuit	Hardware input
	Max. cable length: 30 m 24 V DC Referenced to earth: 0 V Supply X30A, Pin 6

Connection

7.5 Hardware outputs

7.5.1 Supply voltage

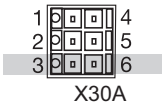
The hardware outputs need a 24 VDC supply.

- When selecting the power supply, take note of the requirements in chapter Technical details.

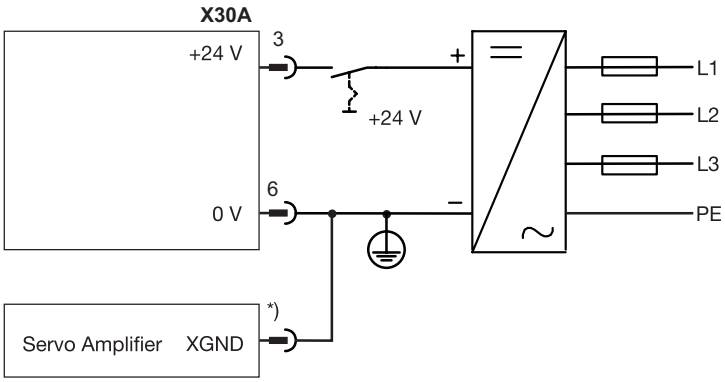
WARNING!

Risk of electrocution!

Safe electrical isolation must be ensured for the external power supply that generates the supply voltage.

Pin X30A	Pin	Designation	Description
	3	24 V Supply	Supply voltage for hardware outputs (24 V) and external encoders
	6	0 V Supply	Supply voltage for hardware outputs (0 V) and external encoders

Connector pin assignment

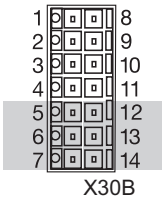
Supply voltage	
	Max. cable length: 30 m 24 V connection isolated from external power supply, e.g. with isolating transformer Noise suppression filter integrated within the safety module ***) Please note the following**: Connect X30A, Pin 6 to XGND on the servo amplifier

Connection

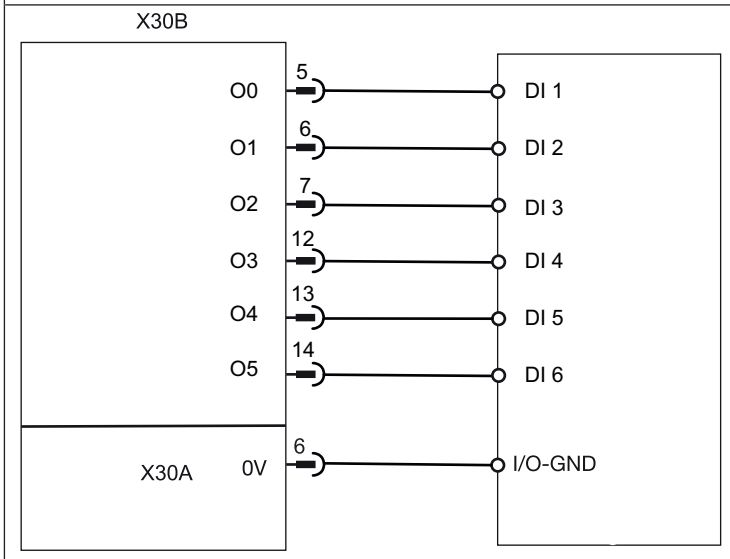
*) XGND:

- PMCprotego D.01 … D.24:
  X4A, Pin 2
- PMCprotego D.48/D.72:
  X4, Pin 3

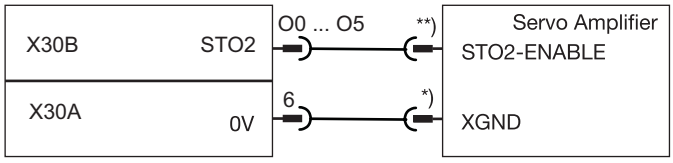
7.5.2 Single-pole hardware outputs

Pin X30B	Pin	Designation	Description
	5	O0	Safe hardware output
	6	O1	Safe hardware output
	7	O2	Safe hardware output
	12	O3	Safe hardware output
	13	O4	Safe hardware output
	14	O5	Safe hardware output

Connector pin assignment

Output circuit	Hardware output
	Max. cable length: 30 m 24 V DC Referenced to earth: 0V Supply X30A Pin 6

Connection

Output circuit	Hardware output
	24 V DC Referenced to earth: 0V Supply

Connection

*) XGND:

- PMCprotego D.01 … D.24:
  X4A, Pin 2
- PMCprotego D.48/D.72:

X4, Pin 3

**) STO2-ENABLE:

- PMCprotego D.01 … D.24:
  X4A, Pin 3
- PMCprotego D.48/D.72:
  X4, Pin 5

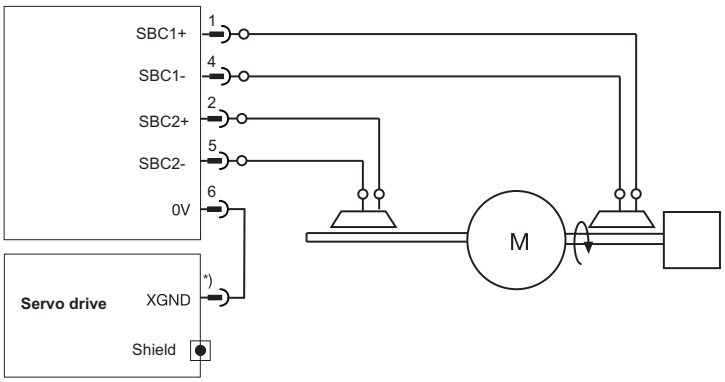
INFORMATION

If the "STO2" output is not used, 24 VDC must be applied to the "STO2-ENABLE" input on the servo amplifier.

7.5.3 Dual-pole hardware outputs

Pin X30A	Pin	Designation	Description
 X30A	1	SBC1+	Hardware output: Control external brake 1 +
	2	SBC2+	Hardware output: Control external brake 2 +
	4	SBC1-	Hardware output: Control external brake 1 -
	5	SBC2-	Hardware output: Control external brake 2 -

Connector pin assignment

External mechanical brake	Hardware output
	Max. cable length: 30 m Brake's supply voltage: 24 V DC, tolerance 0 … 15% *) **It is essential to note:** Connect X30A, Pin 6 to XGND on the servo amplifier

Connection

*) XGND:

- PMCprotego D.01 … D.24:
  X4A, Pin 2
- PMCprotego D.48/D.72:
  X4, Pin 3

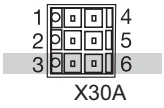
7.6 External encoder

7.6.1 Supply voltage

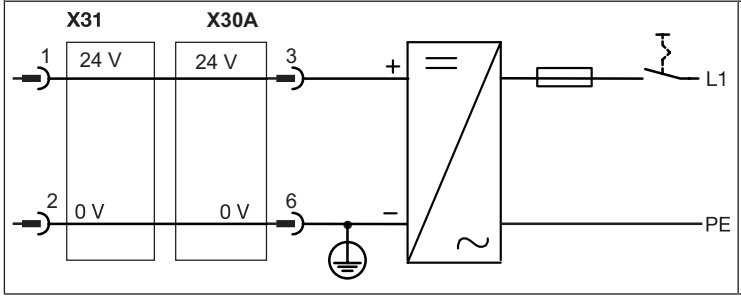
WARNING!

Risk of electrocution!

Safe electrical isolation must be ensured for the external power supply that generates the supply voltage.

Pin X30A	Pin	Designation	Description
	3	24 V Supply	Supply voltage for external encoder
	6	0 V Supply	Reference potential for external encoder (0 V)

Connector pin assignment

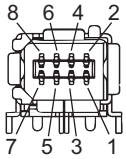
Supply voltage	
	Max. cable length: 30 m X31/1 is internally linked to X30A/3 and X31/2 is linked to X30A/6

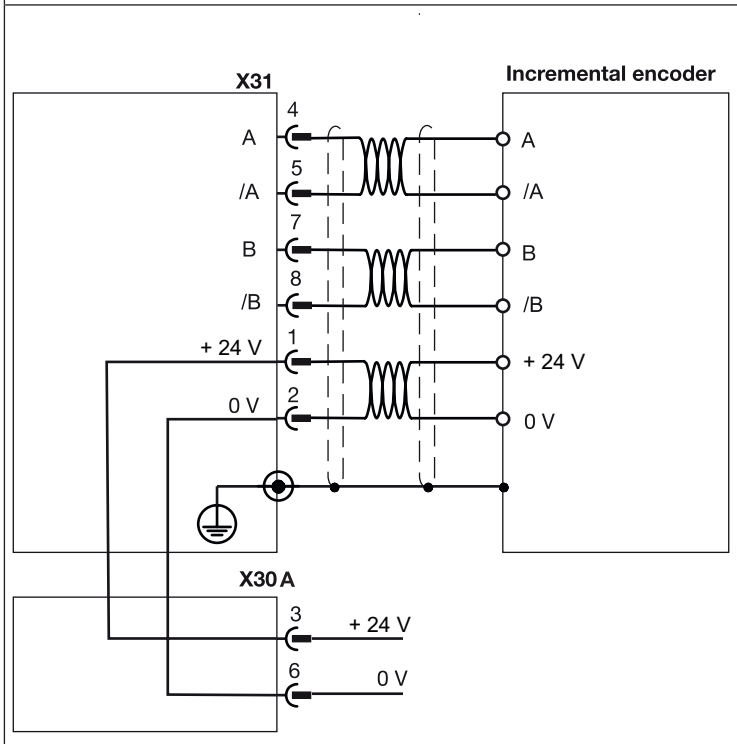
Connection

INFORMATION

When using the safety module with the servo amplifier PMCprotego D.72: Position a foldable ferrite (Würth, No. 7427111) in front of terminals X30/3, 6 above cables + 24 V and 0 V.

7.6.2 Incremental encoder with TTL signal

Connector X31	Pin	Designation	Description
	1	+ 24 V	Supply voltage
	2	0 V	Supply voltage 0 V
	3	n. c.	--
	4	A	Channel A
	5	/A	Channel A inverted
	6	n. c.	--
	7	B	Channel B
	8	/B	Channel B inverted
	n. c.: Not connected		

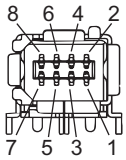
Input circuit	Incremental encoder
	Twisted pair, shielded Shield connection in the housing

Connection

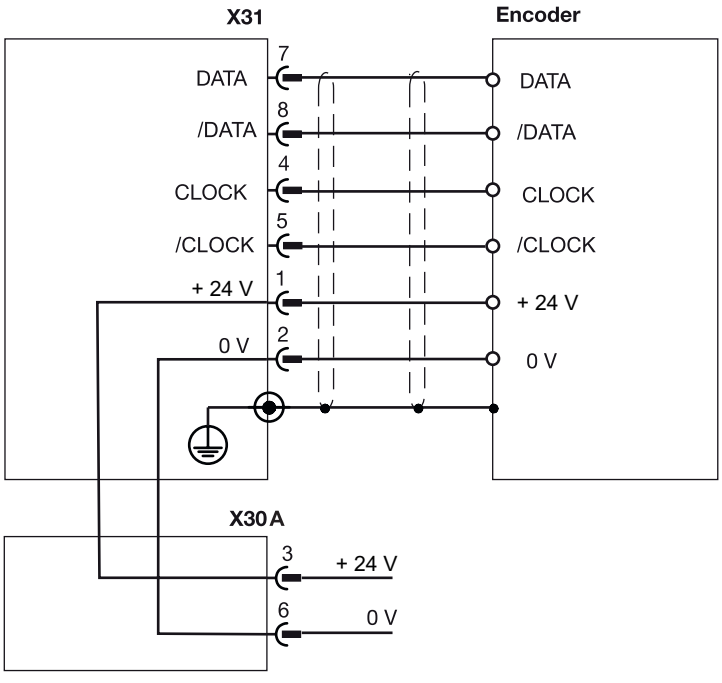
If the cable length is > 50 m, please speak to our Customer Support.

7.6.3 Absolute encoder with SSI interface

If the cable length is > 50 m, please speak to our Customer Support.

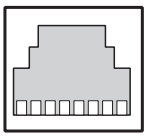
Connector X31	Pin	Designation	Description
	1	+ 24 V	Supply voltage
	2	0 V	Supply voltage 0V
	3	n c.	---
	4	CLOCK	Pulse signal
	5	/CLOCK	Pulse signal inverted
	6	n. c.	---
	7	DATA	Data
	8	/DATA	Data inverted
	n c.: Not connected		

Connector pin assignment

Input circuit	Incremental encoder
	Shielded Shield connection in the housing

Connection

7.7 SafetyNET p RTFL

Socket X32, X33	Pin	Designation	Description
	1	TX+	Transmit +
	2	TX-	Transmit -
	3	RX+	Receive +
	4	n. c.	
	5	n. c.	
	6	RX-	Receive -
	7	n. c.	
	8	n. c.	
	n. c. = not connected		

Recommended cable:

- Min. category CAT5 in accordance with EN 50173
- Maximum cable length: 100 m
- Crossover cables cannot be used

8 Commissioning

8.1 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 Servo amplifier.

DANGER!

Risk of electrocution!

Never wire the electrical connections for the Servo amplifier while the system is live.

Switch off the mains voltages and 24 V supply!

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 option for software enable when booting is set in the PASmotion commissioning software:

- 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 Safe Restart Lock (SRL) safety function can be used to prevent unexpected automatic start-up of the motor.

8.2 Initial commissioning

Requirements for commissioning

- The servo amplifier is ready for commissioning (see operating manual for the servo amplifier).
- The commissioning software PASmotion is available for the configuration of the servo amplifier PMCprotego D and the safety module PMCprotego S3.
- The serial number of the safety module is known. It can be read on the safety module, see Front view [📖 12].

INFORMATION

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

Possible connections with a safety controller

Connection is made via the I/O version

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

Hardware inputs and outputs are mapped to the safety functions in the configuration tool PASmotion.

Connection via the SafetyNET p version

The SafetyNET p RTFL interface is used for safe data exchange between one or more control systems PNOZmulti 2 and one or more safety modules PMCprotego S3 via a safe bus system.

The SafetyNET inputs and outputs are mapped via the commissioning software tools PASmotion, PNOZmulti Configurator and PNOZmulti Network Editor.

The connection is made via a combination of I/O and SafetyNET p

Activation and feedback of the safety functions can occur via SafetNET p and via hardware inputs/outputs.

The SafetyNET inputs and outputs are mapped via the commissioning software tools PASmotion, PNOZmulti Configurator and PNOZmulti Network Editor.
Hardware inputs and outputs are mapped to the safety functions in the configuration tool PASmotion.

8.2.1 Connection is made via the I/O version

1. Wire the safety module

INFORMATION

Please note the guidelines given under "Wiring".

- Connect the reference potential for the hardware outputs/external encoders (X30A/6) and the supply voltage for the hardware outputs/external encoders (X30A/3).

INFORMATION

Do not switch on the supply voltage at this point.

Wire the hardware inputs and outputs that are to be configured.

- Note that the SS1_ACT input for the SS1 safety function must always be connected. (Connection of the STO_ACT input is optional).

2. Connect the configuration PC to the servo amplifier

- Connect the PC to the servo amplifier.

3. Switch on the supply voltage

- Switch on all the supply voltages for the servo amplifier and the safety module.

You will know when the servo amplifier and the safety module by the LEDs of the servo amplifier, see Display elements [193]. A description of the status output of the safety module is provided in the following chapter Safety module operation [186].

⇨ The system starts up and boots (RUNUP).

Further information is provided in Chapter Operating states [187].

The safety module switches to the STO_FAULT state.

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 PASmotion

- Start the commissioning software PASmotion.

- Perform the relevant settings on the servo amplifier and create a project. (Detailed information can be found in the PASmotion online help.)

5. Configure the safety module via PASmotion

INFORMATION

You will find additional useful recommendations and function descriptions in the online help.

- The following basic settings are obligatory to configure the safety module in the offline mode:
  - Define passwords
  - Defining units (optional)
    The units are independent of the servo amplifier's axis model.
  - External encoder (optional)
  - Configure motor
  - Configure safety function SS1 (Safe stop 1)
  - Map hardware inputs/outputs
- Additional configuration is optional.

6. Download the safety configuration

Prerequisites for downloading the safety configuration

- The corresponding safety configuration was selected in PASmotion.
- The safety configuration has been created and saved in offline mode.
- You have the serial number of the safety module ready.

- Switch on the servo amplifier PMCprotego D and establish an online connection to it.
  - ⇨ Once the connection to the servo amplifier has been established, the safety configurations are compared. As there is no configuration as yet during commissioning, PASmotion defines various safety configurations.
- Run the download. Further information on the download can be found in the safety module's online help.

7. Save configuration on the servo amplifier's SD card

The function is described in the following chapter Download configuration to SD card [📖 182].

8. Safety tests

Please note the following chapter Safety checks [📖 184].

8.2.2 Connection is performed via SafetyNET pa or via the combination SafetyNET p and I/O version

1. Wire the safety module

INFORMATION

Please note the guidelines given under "Wiring".

- Connect the reference potential for the hardware outputs/external encoders (X30A/6) and the supply voltage for the hardware outputs/external encoders (X30A/3).
- Connect the cable for the SafetNET p connection (PNOZ m EF SafetyNET (X2 out) --- subscriber PMCprotego S3 (X32 in)).

NOTICE

Recommended SafetyNET p cable:
Min. category CAT5, no crossover cable
Max. cable length: 100 m

INFORMATION

Do not switch on the supply voltage at this point.

Wire the hardware inputs and outputs that are to be configured.

- Note that the SS1_ACT input for the SS1 safety function must always be connected. (Connection of the STO_ACT input is optional).

2. Connect the configuration PC to the servo amplifier/PNOZmulti

- Connect the PC to the servo amplifier/PNOZmulti.

3. Switch on the supply voltage

- Switch on all the supply voltages for the servo amplifier and the safety module.

You will know when the servo amplifier and the safety module by the LEDs of the servo amplifier, see Display elements [📖 193]. A description of the status output of the safety module is provided in the following chapter Safety module operation [📖 186].

⇨ The system starts up and boots (RUNUP).

Further information is provided in Chapter Operating states [📖 187].

The safety module switches to the STO_FAULT state.

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.

INFORMATION

The two following points **4.** (Using the commissioning software to create "Project A") and **5.** (Use the PNOZmulti Configurator to create “Project B") can be in any order.

4. Use the commissioning software to create "Project A”

- Start the commissioning software PASmotion.
- Perform the relevant settings on the servo amplifier and create a project. (Detailed information can be found in the PASmotion online help.)

Configuring the safety module via PASmotion

INFORMATION

You will find additional useful recommendations and function descriptions in the PASmotion online help.

- The following basic settings are obligatory to configure the safety module in the offline mode:
  - Define passwords
  - Defining units (optional)
    The units are independent of the servo amplifier’s axis model.
  - External encoder (optional)
  - Configure motor
  - Configure the safety function (SS1 Safe stop 1)
  - Map inputs and outputs/map SafetyNET p connections
- Additional configuration is optional.

- Save the PASmotion "Project A" on the PC's hard drive.

5. Use the PNOZmulti Configurator to create "Project B"

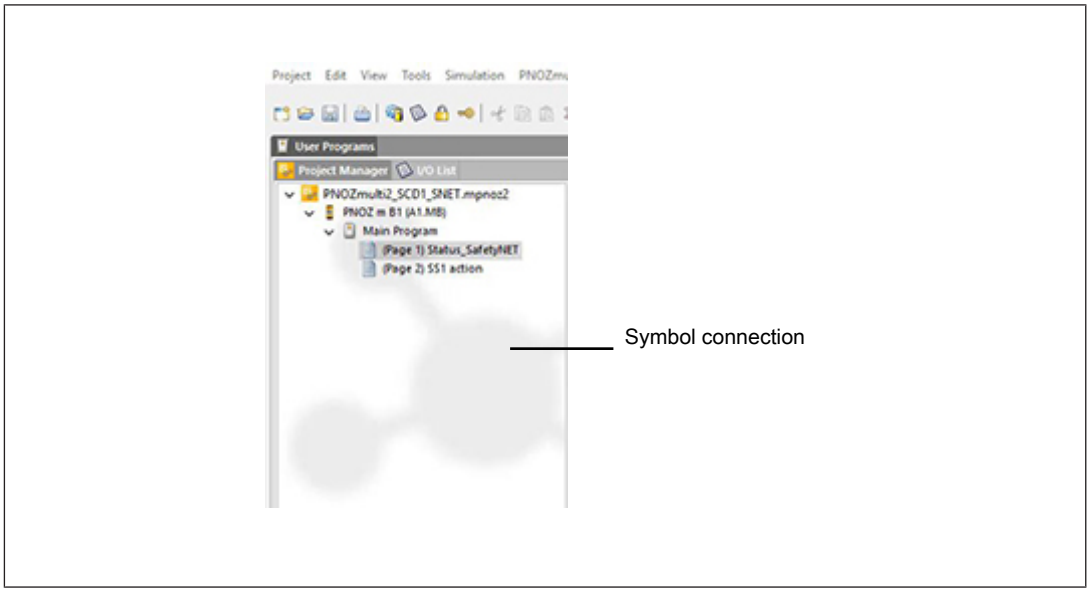
- Start the PNOZmulti Configurator.
  (Further information on PNOZmulti Configurator can be found in the relevant Online help.)
- Configure a project and save it as "Project B" on the hard drive of the PC.

6. Create the SafetyNET p mapping in the network project in the PNOZmulti Network Editor

- Start the PNOZmulti Network Editor in the PNOZmulti Configurator/in PASmotion.
  (Further information on PNOZmulti Network Editor can be found in the PNOZmulti Configurator Online help.)
- Create a network project.
- In the network project, open the "Project B" subproject (as data source/data sink) and the "Project A" subproject (as data source/data sink) in the PNOZmulti Network Editor.
- Create the I/O mapping.
- You don't need to save the PNOZmulti Network Editor. Each change is saved automatically.

7. Start "Project B" in the PNOZmulti Network Editor and perform download

The following symbol shows that there is a network project:



- Switch to online operation and start the download.

8. Start "Project A" in the PNOZmulti Network Editor and perform download

The "symbol connection" shows that there is a network project, see 7.

- Switch to online operation and start the download.

9. The SafetyNET p connection is established with the corresponding mapping

The LEDs show when it is ready for operation, see Display elements [📖 193].

(Connected and everything runs error-free: LED STAT: green, LED STO: green)

10. Save configuration on the servo amplifier's SD card

The function is described in the following chapter Download configuration to SD card [📖 182].

11. Safety tests

Please note the following chapter Safety checks [📖 184].

8.3 Recommissioning

8.3.1 Recommissioning at a restart

The timing diagram below illustrates the signal sequence of the servo amplifier and safety module at a restart. The safety module has already been configured (see "Initial commissioning")

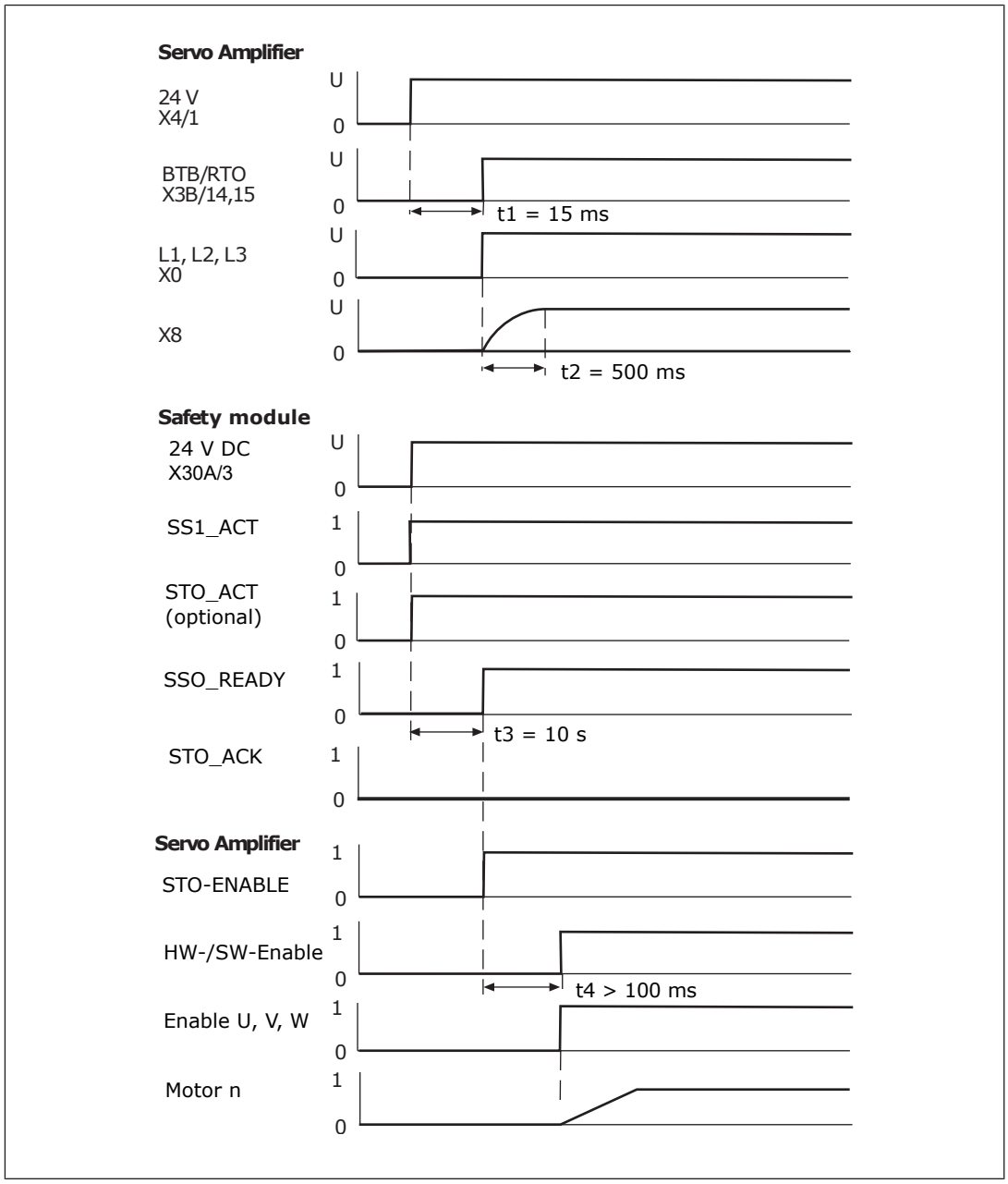


Fig.: Timing diagram restart

Legend

Servo amplifier	
24 V DC	Supply voltage
BTB/RTO	Relay contact for operational readiness, servo amplifier
L1, L2, L3	Mains voltage
X8	Intermediate circuit
STO-ENABLE	Start interlock
HW/SW Enable	Hardware and software enable
Enable U, V, W	Motor connection
Motor n	Motor speed

t1	Servo amplifier's run-up time
t2	Charging time intermediate circuit capacitance
t4	Processing time until servo amplifier is enabled
Safety module	
24 V DC	Supply voltage
SS1_ACT	SS1 activated
STO_ACT	Input for activating STO (optional)
SSO_READY	Operational readiness
STO_ACK	Status: STO activated
t2	Run-up time of the safety module

8.3.2 Recommissioning after error

This section describes the recommissioning process after an error has occurred.

Rectify the error, noting:

- The error messages in the error stack
- The LED display.

Perform a reset as follows:

- Switching the inputs SS1_ACT or STO_ACT (optional) of safety function SS1
- Switching the input SRL_ACT of safety function SRL

  or

- Run the command "CLRFAULT", see Resetting (RESET) the safety module [📖 53]

8.3.2.1 Switch the inputs SS1_ACT or STO_ACT (optional)

1. Switch the input SS1_ACT or STO_ACT (optional) to 0 V

- The safety module performs the safety function SS1 (Safe Stop 1) and switches to a "STO" condition. The STO/FS LED lights up red.

2. Switch the input SS1_ACT and STO_ACT (optional) to 24 V.

- The safety module switches to a "STARTUP" condition. The device and the safe pulse disabler are tested. The STAT LED flashes green.
- The safety module changes to the RUN operating status. The STAT LED lights up green.

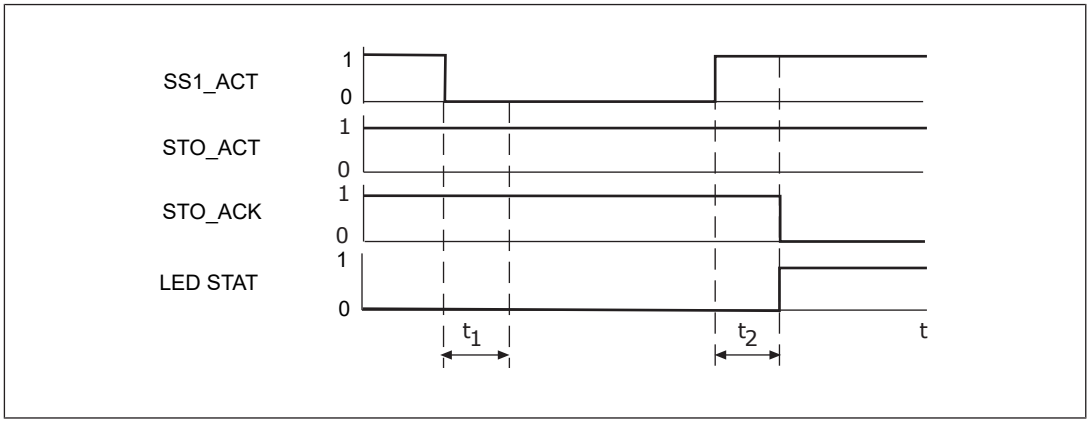


Fig.: Timing diagram recommissioning after error

Legend

t_1	At least 2 ms, time, while SS1_ACT or STO_ACT (optional) must have a 0 signal
t_2	Approx. 2 s, safety module's run-up time
SS1_ACT	Input for safety function SS1
STO_ACT	Input for function STO (optional)
STO_ACK	Output for feedback from safety function STO
LED STAT	System is ready, in RUN state

8.3.2.2 Command "CLRFAULT"

The safety module can be restarted using the command "CLRFAULT" [192] via the serial interface or fieldbus interface on the servo amplifier.

8.3.3 Exchange safety module

When swapping the safety module, please note the following:

- If the firmware version has changed, configured functions and stated parameters may no longer be supported or may have been modified. Adapt the configuration in the Configurator PASmotion.
- You will need to download the configuration to the safety module again. Please note down the serial number of the new safety module.
- We recommend that you swap the whole unit (servo amplifier with safety module). Please contact Pilz.

NOTICE

Damage due to electrostatic discharge!

Electrostatic discharge can damage components. Ensure against discharge before touching the product, e.g. by touching an earthed, conductive surface or by wearing an earthed armband.

After swapping the safety module, following a defect for example, you will need to download the configuration data to the safety module again.

You can download the configuration data to the safety module as follows:

- ① From the configurator to the servo amplifier's communications interface (RS 232 or Ethernet) to the safety module.
- ④ From an SD card in the servo amplifier to the safety module.

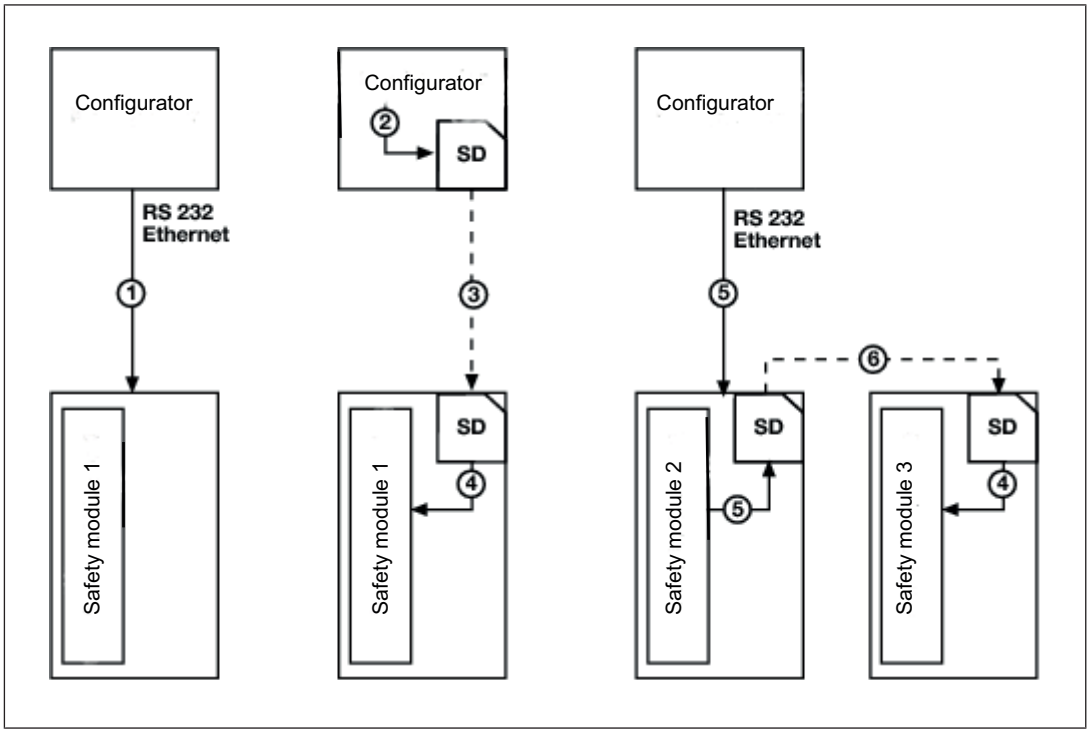


Fig.: Download configuration

Legend:

①	Downloading a configuration from the configurator directly to safety module 1
②	Downloading a configuration via an SD card, which is written by the PC
③	Inserting an SD card into the card slot of the servo amplifier for safety module 1
④	Downloading a configuration from an SD card in the servo amplifier to the safety module
⑤	Downloading a configuration via an SD card, which is written by the servo amplifier (safety module 2)
⑥	Inserting an SD card from the servo amplifier for safety module 2 into the card slot of the servo amplifier for safety module 3

8.3.3.1 Download configuration from configurator to safety module

① The configuration data on the safety module can be downloaded directly from the configurator to the safety module in the servo amplifier.

Prerequisite:

- Connection is established between the PC and servo amplifier (RS 232 or Ethernet).

Procedure:

- Select *Online Mode -> Download Project* in the safety module's configurator.

INFORMATION

Further information is available in the configurator's online help.

8.3.3.2 Download configuration from SD card to safety module

Before carrying out the steps described in this section, please note the following safety guidelines:

CAUTION!

Make absolutely sure that the SD card with the safety module configuration is inserted into the card slot of the correct servo amplifier. If not, invalid parameter settings (e.g. limit values) may lead to unexpected movements and hazardous situations for either people or equipment.

When the configuration is downloaded from the SD card, the servo amplifier does not check the safety module configuration, nor does it check that the configuration is assigned correctly to a specific safety module.

After swapping the safety module, check that the safety functions are activated correctly.

④ The safety module's configuration data can be downloaded to the safety module from an SD card inserted in the servo amplifier, without using the configurator.

During this process, the firmware for the servo amplifier is also reloaded.

Prerequisite:

▸ The SD card (③ or ⑥) must contain the following files:

- default.sm3: Configuration file of the safety module
- default.bin or default.s19: Firmware for the servo amplifier
- default.par: Parameter file for the servo amplifier

Procedure:

1. **Switch off the 24 V supply to the servo amplifier.**
2. **Insert the SD card into the card slot of the servo amplifier.**
3. **Keep both operator keys  on the servo amplifier pressed down.**
4. **Switch on the 24 V supply of the servo amplifier.**
5. **Release the keys when "-" appears on the display.**
6. **Press both operator keys  again and then release.**
   - The firmware update for the servo amplifier is started.
   - The file default.bin or default.s19 is loaded.
   - Display: Counts from 0 to 100, stops at 100 and then counts from 100 to 0.

– The servo amplifier is restarted. The parameter file default.par is loaded.
– The safety module will restart: The LED "STAT" flashes yellow.

7. **Wait until "dis"** (= **d**rive **i**ntegrated **s**afety) **appears on the display.**
   ⇨ Note: You must then press the left-hand operator key on the servo amplifier within 60 seconds (see step 8).
8. **Press the left-hand operator key**  **for al lest 2 seconds.**

NOTICE

Deliberate action!
By operating the operator key for at least 2 seconds you confirm the correct mapping of the safety configuration to the safety module.

– The configuration file default.sm3 starts downloading to the safety module. Display: "…".
– Once the configuration file has been downloaded, the safety module starts up. The safety module is in "STARTUP" condition ("STO/FS" LED flashes).
– If the download has been successful, the safety module switches to "RUN" condition (LED "STO/FS" is lit).

8.3.3.3 Download configuration to SD card

② ⑤ You can download the configuration data to the safety module via an SD card. The configuration data must first be saved to the SD card.

There are two options for downloading a configuration to an SD card:

1. Option ②: Downloading a configuration via an SD card, which is written by the PC.

   Prerequisite:

   ⇨ Connection to the SD card in the PC

   Procedure:

   – In the configurator in the Project Manager, select the safety module and right-click -> Export as safety module configuration (*.sm3) file.
     This function is active only when the safety configuration in PASmotion is up-to-date.
   – Remove the SD card from the card slot of the PC and insert the SD card into the card slot of the servo amplifier ③ (further with section "Download configuration from SD card to safety module").
2. Option ⑤: Downloading a configuration via an SD card, which is written by the servo amplifier.

   Prerequisite

   – Connection is established between the PC and servo amplifier (RS 232 or Ethernet).
   – An SD card must be inserted in the servo amplifier.

Procedure:

– Select *Online Mode -> Servo Amplifier Configuration -> SD Card* in the safety module's configurator
– Remove the SD card from the servo amplifier and insert it into the card slot of the servo amplifier to be configured ⑥ (further with section "Download configuration from SD card to safety module").

8.4 Safety checks

The safety module PMCprotego S3 is a safety component under the Machinery Directive in accordance with Annex V. 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 the Servo amplifier
- After changing the configuration of the Servo amplifier (for example when changing the motor type, motor encoder type or brake selection)

A full check comprises

- proper execution of the employed safety functions of the safety module PMCprotego S3
- Proper execution of the overall safety function (e.g. combination and integration of safety functions)
- Inspection of the parameters

The basis for testing

- are the requirements for the safety functions of the safety module PMCprotego S3 resulting from the risk analysis of the machine or process
- is the description of the safety module PMCprotego S3 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.

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.

Brake test

Depending on the application, the regular checks may include a test of the internal (motor brake) and external brake(s).

INFORMATION

Refer to Safe Brake Test (SBT) [📖 136] for the function of the safe brake test.

9 Safety module operation

Prerequisites for normal operation are:

- Commissioning is complete
- The safety module contains the configuration data
- The safety functions have been tested
- The "STAT" LED lights up green

During operation

- the signal level and edge change are monitored at the safe inputs of the safety module.
- the safety functions are performed in accordance with the configuration.
- the switchability of the hardware outputs is monitored.
- permanent hardware self-tests are carried out.

9.1 Operating states

The safety module is always in a clearly defined operating status.

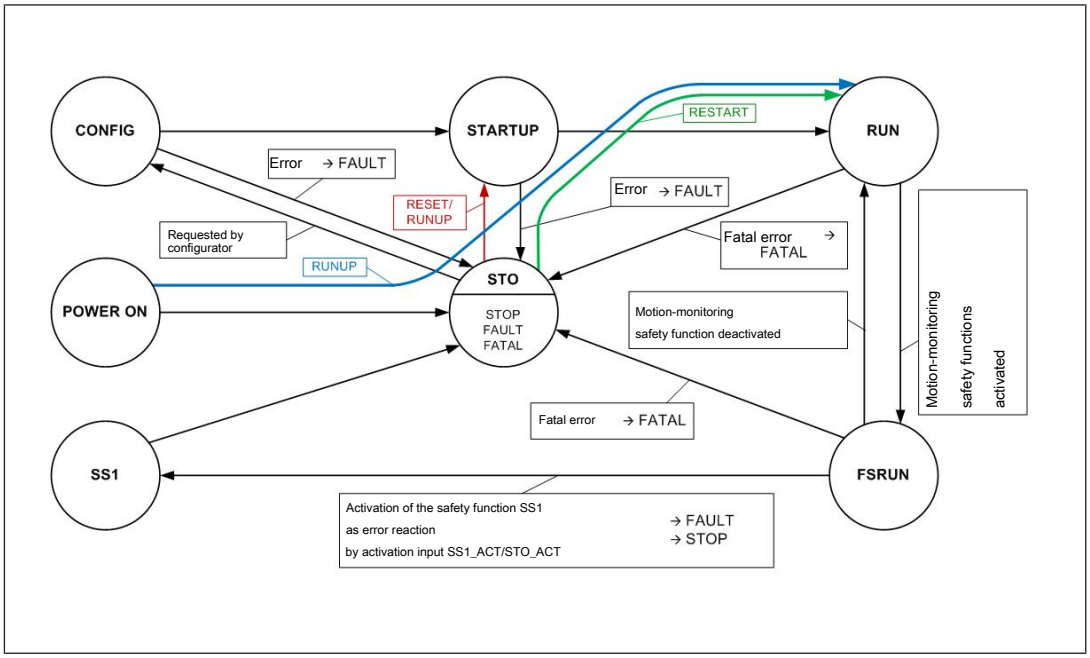


Fig.: Operating statuses

CONFIG	Transfer of the configuration to the safety module. The motor is switched to torque/force-free in the CONFIG operating status (STO is active). Transition to STARTUP state: configuration downloaded without error Transition to STO state: incorrect configuration data
POWER ON	The supply voltage is present. Transition to STO state: after applying supply voltage
SS1	SS1 is performed: ▸ As error reaction function (FAULT) ▸ By the activation input SS1_ACT (STOP) ▸ By internal request – e.g. demand from "Download configuration" tool Transition to STO state: ▸ After FATAL ▸ When exceeding brake ramp (optional) ▸ After STO delay time has elapsed
STARTUP	Self-test of safety module is performed. Transition to STO state: after FAULT Transition to RUN state: No fault present

STO	The motor is switched to torque-free/force-free. Depending on the cause, the following (sub-)statuses are active:
	STOP – Stop Switching motor to torque-free/force-free by: ▸ Activation input SS1_ACT or ▸ Activation input STO_ACT (optional)
	FAULT – Error Switching motor to torque-free/force-free via the safety function SS1, as a result of an error reaction: ▸ Limit value violation ▸ Internal error from self-test
	FATAL – Fatal error Switching motor to torque-free/force-free via the safety function STO, as a result of an error reaction: ▸ Safety-critical error that requires shutdown of the entire module ▸ Unrecoverable internal software error ▸ Errors that are neither revealed by a self-test nor constitute a limit value violation
RUN	Safety module in operation: no motion-monitoring safety function is activated Transition to STO state: After FATAL Transition to FSRUN state: a motion-monitoring safety function is activated
FSRUN	Safe operation: at least one motion-monitoring safety function is activated Transition to STO state: After FATAL Transition to SS1 state: After STOP or after FAULT Transition to RUN state: motion-monitoring safety function is deactivated
RESET	Action that triggers the RESTART (see Safe restart of the machine [📖 52]) (see Resetting (RESET) the safety module [📖 53])
RUNUP	Run-up
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.

9.2 RUNUP (booting)

The safety module passes through the following states during the runup:

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.

9.3 RESTART

The safety module passes through the following states during the restart:

STO → STARTUP → RUN

INFORMATION

Note the optional configuration options for restarting

The RESTART function can be optionally configured via the safety functions Safe Restart Lock (SRL) and Safe Stop 1 (SS1).
(See Safe Restart Lock (SRL) [145])
(See Safe stop 1 (SS1) [84])
Further information about a RESET can be found in chapters:
Safe restart of the machine [52]
Resetting (RESET) the safety module [53]

STO after STOP

Perform a restart as follows:

- Switch the input SS1_ACT to 24 V
  - ⇨ The safety module passes through the states STARTUP → RUN → FSRUN (depending on the configuration)

STO after 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 24 V

or

- Perform the "CLRFAULT" command, see chapter entitled "CLRFAULT" command

⇨ The safety module passes through the states STARTUP → RUN → FSRUN (depending on the configuration)

9.4 Command "CLRFAULT"

The safety module can be reset using the "CLRFAULT" command via the serial interface or fieldbus interface on the servo amplifier.

Prerequisites for using the "CLRFAULT" command

- The safety module is in "STO" state. The STO/FS LED lights up red.
- The two inputs SS1_ACT and STO_ACT have "1" signal (24 V).

Alternatively, this function can also be assigned to a digital input on the servo amplifier. Two commands are available:

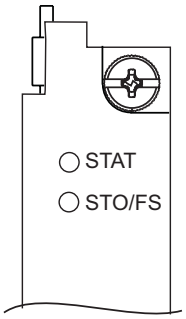
- The command IN1MODE=1, (servo amplifier error reset), activates the function on digital input DIGITAL-IN1 of the servo amplifier.
- The commands INxMODE=30 or INxMODE=33 (run any command string) activate the function on one of the digital inputs on the servo amplifier (e.g. IN4MODE=30 on input DIGITAL-IN4).

INFORMATION

Further information on the command can be found in the servo amplifier's online help.

9.5 Display elements

The safety module has LEDs to display the status of the operating states.



LED			Meaning
Designation	Colour	Status	
STAT		● Off	Supply voltage is not present
	Green	☼ On	RUN (normal operation) STO FSRUN (safe operation)
	Green	◐ Flashes	RUN (start-up)
STAT	Red	☼ On	FATAL
	Red	◐ Flashes	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
STAT	Green-yellow	Flashes	SafetyNET p connection not active (connection setup, interference, for example)

Legend

 LED on

 LED flashes

 LED flashes briefly

 LED off

9.6 Messages

Any errors of the safety module are indicated on the servo amplifier display with message "F31".

The following options are available for detailed diagnostics and fault detection:

- LEDs on the front of the safety module provide information on the operating statuses see Display elements [📖 193].
- Outputs on the safety module display the states of the safety functions (e.g. STO Acknowledge).
- Errors and messages are entered in the safety module's error stack.
- The following are displayed in online mode in the Configurator PASmotion:
  - Safety module status messages and error messages (error stack)
  - States of safety module inputs and outputs

9.7 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 hardware inputs and outputs are described in the chapter Hardware inputs/outputs [📖 33].
- The encoder is subject to forced dynamisation, see Motor encoder fault detection [📖 45].

10 Change, maintenance, decommissioning

10.1 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 Servo amplifier.
- 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.

10.2 Maintenance

No maintenance work is necessary on a PMCprotego S3 safety module. Please return the safety module to Pilz.

10.3 Decommissioning

Note the mission time T_M stated in the safety-related characteristic data of the PMCprotego S3 safety module.

Note the information about assembly/disassembly in this operating manual.

When decommissioning, please comply with local regulations regarding the disposal of electronic devices (e.g. Electrical and Electronic Equipment Act).

11 Field bus communication

Servo amplifier/control system field bus communication

The CANopen Service Data Objects (SDOs) for the safety module are described in the following documents:

- PMCprotego_D_DD5_CANopen_Prog_Manual_1002905-XX-XX.pdf.
- PMCprotego_D_DD5_EtherCAT_Prog_Manual_1002906-XX-XX.pdf

The parameter numbers (PNUs) for the safety module are described in the following documents:

- PMCprotego_D_DD5_PROFIBUS_Prog_Manual_1002907-XX-XX.pdf
- PMCprotego_D_DD5_PROFINET_Prog_Manual_1003784-XX-XX.pdf

PROFIBUS PROFINET	CANopen EtherCAT	Length	Unit	Description	
--	0x4454 Sub 0	DWORD	--	Serial number of safety module	
PNU 1712 Index 33	0x4401 Sub 0	DWORD	--	Status of safety module	
PNU 1713 Index 33	0x44F2 Sub 0	DWORD	--	Signals for starting the deceleration ramp. Bit 26=1 STO active Bit 28=0 SS1 active Bit 27=0 SS2 active Bit 31=0 SS1 fault active	Signal for start of normal operation deceleration ramp. Signal for start of emergency stop deceleration ramp.
PNU 1862 Index 33	0x4424 Sub 0	DWORD	[Incr/s^2]	Increase in current deceleration ramp requested by safety module. (4096 increments are one rotation)	
PNU 1714 Index 33	0x4402 Sub 0	DWORD		Error register	
PNU 1863 Index 33	0x3927 Sub 1	DWORD		Fieldbus inputs 0 … 31	
--	0x44F0 Sub 1	WORD		Fieldbus inputs 0 … 15	
--	0x44F0 Sub 2	WORD		Fieldbus inputs 16 … 31	
PNU 1864 Index 33	0x3928 Sub 1	DWORD		Fieldbus outputs 0 … 31 (only read back)	
--	0x44F1 Sub 1	WORD		Fieldbus outputs 0 … 15 (only read back)	
--	0x44F1 Sub 2	WORD		Fieldbus outputs 16 … 31 (only read back)	

12 Technical details

General	
Certifications	**CE, TÜV, UKCA**
Application range	**Failsafe**
Absolute encoder input	
Number of counter inputs	**1**
Type of counter inputs	**SSI encoder**
Supply voltage for absolute encoder	**24 V DC**
Output signal (clock)	**Differential signal (RS-422/TTL)**
Max. number of bits on the counter input	**12 - 28 Bit**
Transmission rate	**300 kHz**
Coding of the input signal	**Binary, Gray**
Signal at the data input	**Differential signal (RS-422/TTL)**
Incremental encoder input	
Number of inputs	**1**
Supply voltage for incremental encoders	**24,0 V**
Signal level at "1"	**>= 2,5 V**
Signal level at "0"	**<= 0,5 V**
Phase position for the differential signals A, /A and B,/B	**90° ±30°**
Maximum cutoff frequency	**0,5 MHz**
Inputs	
Number	**8**
Signal level at "0"	**-3 - +5 V DC**
Signal level at "1"	**15 - 30 V DC**
Input current range	**3,5 - 10,8 mA**
Pulse suppression	**1 - 10 ms**
Semiconductor outputs	
Number of positive-switching single-pole semiconductor outputs	**6**
External supply voltage	**24 V**
Voltage tolerance	**-15 %/+20 %**
Typ. output current at "1" signal and rated voltage of semiconductor output	**0,5 A**
Residual current at "0" signal	**0,02 mA**
Monitoring threshold of semiconductor output	**9 V**
Max. duration of on time during self test	**200 µs**
Max. duration of off time during self test	**200 µs**
Repetition time of the on/off test	**1,5 s**
Galvanic isolation	**yes**
Short circuit-proof	**yes**
Semiconductor outputs, 2-pole	
Number of dual-pole semiconductor outputs	**2**

Semiconductor outputs, 2-pole	
Typ. output current at "1" signal and rated voltage of semiconductor output	**2 A**
Max. switching frequency	**1 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**
Ambient temperature	
In accordance with the standard	**EN 60721-3-3**
Class	**3K3**
Temperature range	**0 - 40 °C**
Storage temperature	
In accordance with the standard	**EN 60721-3-1**
Temperature range	**-25 - 70 °C**
Max. change	**20 K/h**
Storage temperature class	**1K4**
Climatic suitability	
In accordance with the standard	**EN 60721-3-3**
Humidity	**85 % r.h.**
Relative humidity class	**3K3**
Condensation during operation	**Not permitted**
Max. operating height above sea level	**2000 m**
EMC	**EN 61800-3**
Vibration	
In accordance with the standard	**EN 60721-3-2**
Class	**2M1**
Airgap creepage	
In accordance with the standard	**EN 61800-5-1**
Overvoltage category	**II**
Pollution degree	**2**
Protection type	
In accordance with the standard	**EN 60529**
Housing	**IP20**
Terminals	**IP20**
Mounting area (e.g. control cabinet)	**IP54**
Mechanical data	
Mounting position	**vertical**
Dimensions	
Height	**141,9 mm**
Width	**86,7 mm**
Depth	**18,4 mm**
Weight	**124 g**

Where standards are undated, the 2021-03 latest editions shall apply.

12.1 Safety characteristic data

The safety module carries out drive-related safety functions, as described in the EN 61800-5-2 standards, 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.

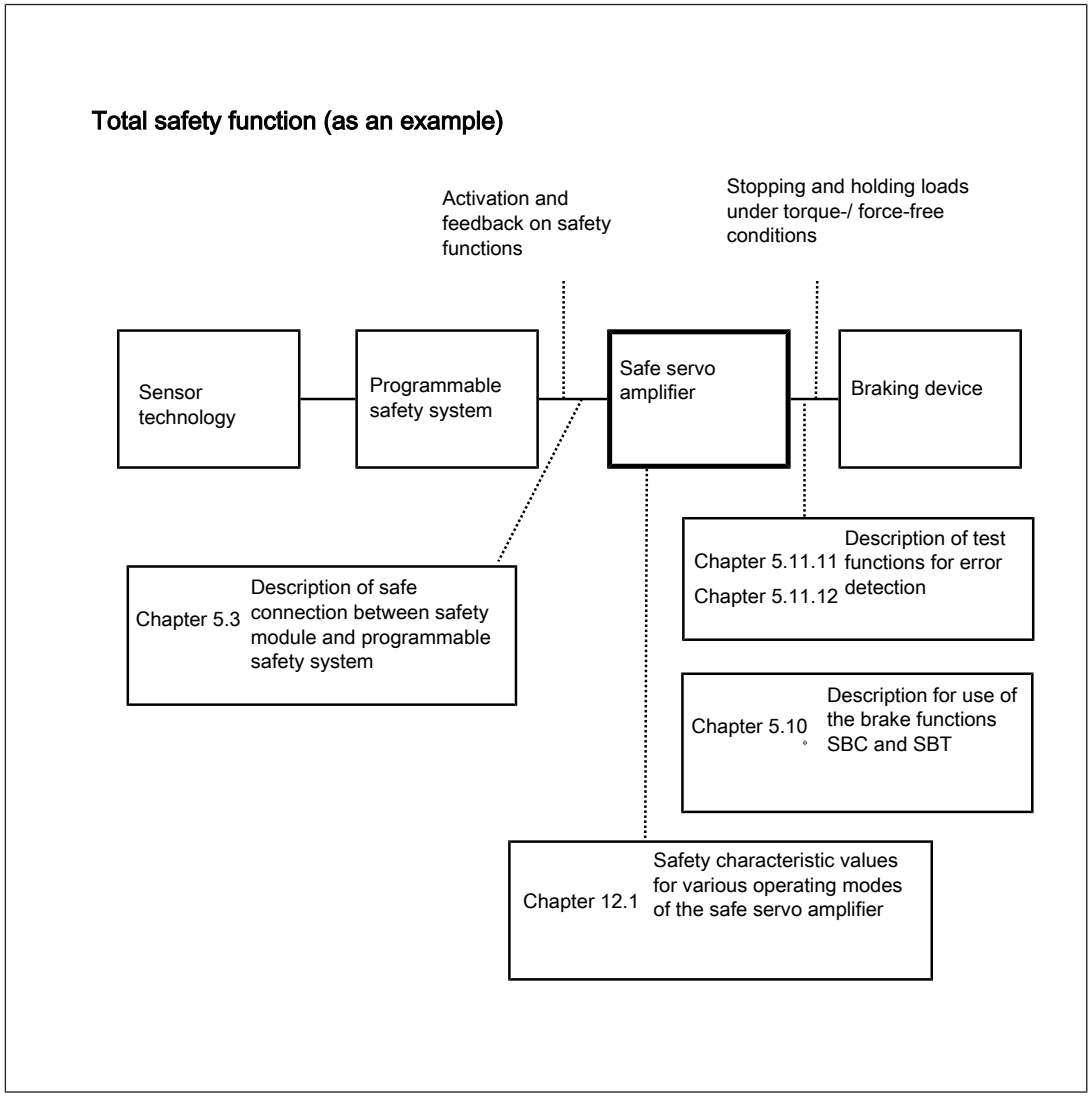


Fig.: Overall safety function and safety-related subsystems

A "safe servo amplifier" is a structural and functional unit consisting of

- a servo amplifier PMCprotego D with installed safety module PMCprotego S3

To determine the safety integrity of the overall safety function, this subsystem operating manual for the safe **servo amplifier**

- describes the safety functions.
- provides the safety characteristic data for various operating modes.
- describes the test functions for fault detection of other subsystems.

Operating modes

The operating modes are divided into various subsystem configurations for **safe servo amplifier**.

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. Error detection takes place by cross-comparing 2 different sensors.

The following combinations of safe position detection sensors can be used:

- Motor encoder and internal system variables
- Motor encoder and external encoder

Also see chapter Motor encoder fault detection [📖 45]

To simplify the calculation, sensor combinations with assumed failure rates are included in the safety-related characteristic data. The following differences in operating modes result:

- Operating mode **Encoder MTTF ≧ 10a**
  - Motor encoder with MTTF ≧ 10 years and internal system variables
  - Motor encoder with MTTF ≧ 10 years and external encoder with MTTF ≧ 10 years
  - According to EN ISO 13849-1, an $MTTF_D$ of ten years can be assumed for a component if no manufacturer data are available.
  - The service life 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
  - Motor encoder with MTTF ≧ 57 years and external encoder with MTTF ≧ 57 years
  - The MTTF value of the encoder employed must be reviewed.
  - The service life of the motor encoder must be T_M = 20 years.

Assuming that all errors 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 Limitations
DIO SNp, Encoder MTTF ≧ 10a	▸ Position sensors possible in this operating mode – Motor encoder with MTTF ≧ 10 years and internal system variables – Motor encoder and external encoder with MTTF ≧ 10 years ▸ Safety functions that can be used in this operating mode – Stop functions: STO, SS1, SS2 – Motion functions: SLS, SSR, SOS, SDI, SLI, SLP – Monitoring functions: SLS-M, SSR-M, SOS-M, SDI-M, SLI-M, SLP-M – Brake management: SBC, SBT – Other safety functions: SRL, SSO ▸ External interfaces that can be used in this safety function operating mode: – 2 x safe input, 1-pole – 2 x safe output, 1-pole – 1 x safe output, 2-pole – SafetyNET p RTFL interface	SIL 2, PL d (Cat. 3) Limitation imposed by the failure rate of the encoder system

Operating mode	Description	Safety integrity Limitations
DIO SNp, Encoder MTTF ≧ 57a	▸ Position sensors possible in this operating mode – Motor encoder with MTTF ≧ 57 years and internal system variables – Motor encoder and external encoder with MTTF ≧ 57 years ▸ Safety functions that can be used in this operating mode – Stop functions: STO, SS1, SS2 – Motion functions: SLS, SSR, SOS, SDI, SLI, SLP – Monitoring functions: SLS-M, SSR-M, SOS-M, SDI-M, SLI-M, SLP-M – Brake management: SBC, SBT – Other safety functions: SRL, SSO ▸ External interfaces that can be used in this safety function operating mode: – 2 x safe input, 1-pole – 2 x safe output, 1-pole – 1 x safe output, 2-pole – SafetyNET p RTFL interface	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: 2015 PL	EN ISO 13849-1: 2015 Category	EN 62061 SIL CL	EN 62061 PFH_D [1/h]	IEC 61511 SIL	IEC 61511 PFD	EN ISO 13849-1: 2015 T_M [year]
DIO SNp, Encoder MTTF ≥ 10a	**PL d**	**Cat. 3**	**SIL CL 2**	**2,61E-09**	**SIL 2**	**1,45E-04**	**20**
DIO SNp, Encoder MTTF ≥ 57a	**PL e**	**Cat. 4**	**SIL CL 3**	**2,00E-09**	**SIL 3**	**9,55E-05**	**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 units that are used and may be different. We recommend that you use the PAScal software tool to calculate the safety function's SIL/PL values.

12.2 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".

Inputs

Source			Drain			
Safety control system	C0		Safety module	C0		

Drain parameters	Min.	Typ.	Max.
Test impulse duration	-	-	10 ms
Test impulse interval	40 ms	-	
Input resistance	2,2 kOhm	-	
Capacitive load	-	-	68 nF

Safe 1-pole HL outputs

Source			Drain			
Safety module	C2		Safety control system	C2		

Source parameters	Min.	Typ.	Max.
Test impulse duration	-	-	200 µs
Rated current	-	-	0,5 A
Capacitive load	-	-	0,5 µF

Safe dual-pole SC outputs

Source			Drain			
Safety module	D2		Brake	D2		

Source parameters	Min.	Typ.	Max.
Test impulse duration	150 µs	-	350 µs
Test impulse interval	600 ms	-	
Leakage current in OFF-state	-	-	0,5 mA
Nominal current in ON-state	-	-	2 A
Capacitive load	-	-	0,5 µF

13 EC declaration of conformity

This product/these products meet the requirements of the directive 2006/42/EC for machinery of the European Parliament and of the Council. The complete EC Declaration of Conformity is available on the Internet at www.pilz.com/downloads.
Authorised representative: Norbert Fröhlich, Pilz GmbH & Co. KG, Felix-Wankel-Str. 2, 73760 Ostfildern, Germany

14 UKCA-Declaration of Conformity

This product(s) complies with following UK legislation: Supply of Machinery (Safety) Regulation 2008.
The complete UKCA Declaration of Conformity is available on the Internet at www.pilz.com/support/downloads.

Representative: Pilz Automation Technology, Pilz House, Little Colliers Field, Corby, Northamptonshire, NN18 8TJ United Kingdom, eMail: mail@pilz.co.uk

15 Order reference

Product type	Features	Order no.
PMCprotego S3.SN 8DI 6DO EI BR	Safety module	680010

Accessories SafetyNET

Product type	Features	Order no.
SafetyNETp Connector RJ45	SafetyNETp connector	380401
SafetyNET Cable	SafetyNET p cable (4-pin) Cable for assembling	380000
SafetyNET Cable 'SN CAB RJ45sRJ45s'	SafetyNET p cable (4-pin) Assembled in various lengths: 0.5 m 1 m 2 m 5 m 10 m	 380001 380003 380005 380007 380009
Stripping tool	Stripping tool for SafetyNETp cable	380070

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 an external 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 (see 4.2.3.1) 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.

SafetyNET p RTFL (Real Time Frame Line)

The safe bus system is used for communication for applications with high real-time requirements.

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 21 60880878-216
Japan
+81 45 471-2281
South Korea
+82 31 778 3300

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-0
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Turkey
+90 216 5775552
United Kingdom
+44 1536 462203

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

BRANDS OF THE CENTURY PILZ 2019 GERMAN STANDARDS

Quality Management ISO 9001:2015 REG. NO. 2462
Environmental Management ISO 14001 REG. NO. 2462
Energy Management ISO 50001 REG. NO. 2462

1004379-EN-02, 2021-09 Printed in Germany

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY