Operation Manual

Language	**English**
	Translation
Document No.	5.11016.04
Part No.	00440935
Date	13.11.2019

be in motion be in motion

BAUMÜLLER

BM5-O-SAF-002/3

Safety Module for b maXX 5000

CE

E	5.11016.04

Read the Operating Instructions before beginning!

Ostendstr. 80 - 90
90482 Nürnberg
Germany

Tel. +49 9 11 54 32 - 0
Fax: +49 9 11 54 32 - 1 30

E-Mail: mail@baumueller.de
Internet: www.baumueller.de

Table of Contents

1

DOCUMENT HISTORY

Revision level	State	Modifications
5.11016.01	25.03.2013	Initial document
5.11016.02	05.10.2015	Chapter C.5: Pin-no. in figures added Chapter 21: Accessories added Fig. 17 changed Chapter 15.4.2 text added
5.11016.03	19.11.2018	Software extension BM5-O-SAF-002-xxx-002-#01-yyy-zzz Chapter 7.1 text changed (in Abs. 4) Chapter 7.5 warning notices changed and text added Chapter 7.5.1 and chapter 7.5.2 new Chapter 7.7.2 new para. 2 new: Chapter 7.8 software extension SAF-002/3 module Chapter 7.9 (vorher chapter 7.8) type code extended Chapter 10.1 and chapter 10.2 para. 2 deleted Chapter 10.3.1 figure and note new Chapter 10.4 para. 2 new, figure changed and note new Chapter 10.4.1 and chapter 10.4.2 new Chapter 10.5 Abs. 2 new and figure changed Chapter 10.5.1 new Chapter 10.6 note 2 new and figure changed Chapter 10.6.1 new Chapter.7 figure changed Chapter 10.7.1 new Chapter 10.8 figure new Chapter 10.8.1 new Chapter 10.9 figure new, 3 notes, text new and figure new Chapter 10.9.1 new Chapter 10.10 figure changed, text (para. 5-7) new Chapter 10.10.1 new Chapter.11 figure new Chapter 10.11.1 and chapter 10.11.2 new Chapter 10.12 figure new Chapter 10.12.1 new Chapter 10.13 text changed (in para. 4) and figure new Chapter 10.13.1 new Chapter 10.14 figure new Chapter 10.14.1 new Chapter 10.15 new Chapter.11.3 note new continue →

		Chapter.12.3 note under figure new Chapter 12.6 status word "S_StatusWord1" bits 5-7 new and 2 notes after table new Chapter 19.5 operating states added (encoder fail) and text before error list inserted Chapter 19.5 error list extended (row „SS1 time general“ and error 31. 77, 78, 109-113) and additional information at error 48 extended (error no. 6, 192-194, 196) Chapter C.2.5 reaction times extended
5.11016.04	13.11.2019	Chapter 7.5.1 cross reference added, parameter 19.8.deleted Chapter 7.5.2 cross reference added Chapter 7.8 Software status extended Chapter 10.4.1 cross reference added Chapter 10.5.1 cross reference added Chapter 10.6.1 cross reference added Chapter 10.7.1 cross reference added Chapter 10.8.1 cross reference added Chapter 10.9.1 cross reference added Chapter 10.10.1 cross reference added Chapter 10.11.1 cross reference added Chapter 10.12.1 cross reference added Chapter 10.13.1 cross reference added Chapter 10.14.1 cross reference added

2

GENERAL

2.1 Information on the Operation Manual

This operation manual provides important information for the use of the Safety Module. Respect of the safety guidelines and instructions in this operation manual are prerequisites for the safe work.

Furthermore, the local accident prevention legislation and general safety regulations applying to the Safety Module's field of application must also complied with.

Read the operation manual completely, in particular the chapter on safety instructions, before beginning any work on the Safety Module. The operation manual is a component of the product and must be kept accessible in the immediate vicinity of the Safety Module at all times.

2.2 Legend

Warning notices

Warning notices are marked by symbols in this operation manual. The notices are introduced by signal words which express the extent of the hazard.

Comply with the notices under all circumstances and act with caution in order to avoid accidents, personal injury and property damage.

DANGER!

....notifies of an imminent dangerous situation which will lead to death or serious injuries if not avoided.

WARNING!

....notifies of a potentially dangerous situation which can lead to death or serious injuries if not avoided.

CAUTION!

....notifies of a potentially dangerous situation which can lead to minor or slight injuries if not avoided.

NOTICE!

....notifies of a potentially dangerous situation which can lead to property damage if not avoided.

Recommendations

NOTE!

....draws attention to useful tips and recommendations as well as information for efficient and trouble-free operation.

2.3 Limitation of liability

All statements and instructions in this operation manual have been compiled in compliance with the applicable standards and legislation while taking the current level of technology and our long-term experience and findings into account.

The manufacturer assumes no liability for damages resulting from:

- failure to observe the operation manual
- application for purposes other than those intended
- use by untrained personnel

The actual scope of materials delivered can vary from the explanations and illustrations described here in the event of custom designs, the use of additional ordering options or due to the most recent changes in technology.

The user assumes the responsibility of conducting maintenance and commissioning in accordance with the safety regulations of the applicable standards and all other relevant national or regional legislation relating to conductor dimensioning and protection, grounding, circuit breakers, overvoltage protection, etc.

The person who conducted the assembly or installation shall be accountable for damages occurring during assembly or connection.

2.4 Preliminary information

NOTICE!

The following shall apply if the document you are reading is designated as preliminary information:
This version pertains to preliminary technical information which the user of the described Safety Modules and functions should receive ahead of time, in order to be able to adjust to potential changes and/or functional expansions.
This information is to be seen as preliminary, since it has not yet been subjected to the Baumüller internal review process. In particular, this information is still subject to changes, meaning that this preliminary information cannot be construed as legally binding. Baumüller assumes no liability for damages resulting from this potentially incorrect or incomplete version.
Should you detect or suspect content-related and/or serious formal errors in this preliminary information, please contact the contact person at Baumüller assigned to you and inform us of your findings and comments, so that they can be taken into account and potentially incorporated during the transition from the preliminary information to the final (reviewed by Baumüller) information.

2.5 Copyright

Treat the operation manual as confidential. It is intended exclusively for those working with the Safety Module. It is not permissible to transfer the operation manual to third parties without the written approval of the manufacturer.

NOTE!

The content-related statements, texts, diagrams, images and other illustrations are copyright protected and subject to industrial property rights. Any improper use is liable to prosecution.

2.6 Further applicable documents from other manufacturers

Components from other manufacturers are built into the Safety Module. Hazard evaluations for these bought-in parts have been conducted by the applicable manufacturers. The conformity of the designs with the applicable European and national legislation has been declared by the respective component manufacturers.

2.7 Replacement parts

WARNING!

Improper or defective replacement parts can lead to damage, malfunctions or total failure as well as jeopardize safety.

Therefore:

- Only use original replacement parts from the manufacturer

Procure replacement parts from authorized dealers or directly at the manufacturer.

2.8 Disposal

If no return or disposal agreement has been made, dismantled components can be taken for recycling after proper disassembly.

See also ▹Disposal◃ on page 155.

2.9 Warranty and liability

The warranty and liability terms are to be found in a separate document in the sales data.

The operation of the Safety Modules described here in accordance with the specified methods/procedures/requirements is permissible. Everything else, even the operation of Safety Modules in installation positions not depicted here, for instance, is not permissible and must be clarified with the factor on a case-by-case basis. The warranty will be rendered null and void if the Safety Modules are operated differently than described here.

2.10 Customer service

Our customer service is available for technical support.

Information on the competent contact person can be found at any time via telephone, fax, E-mail or over the Internet.

2.11 Terms used

A list of the abbreviations used can be found in ▹Appendix A - Abbreviations◃ from page 157 onward.

2.12 Certification

The Safety Module (BM5-O-SAF-002/-003) from Baumüller Nürnberg GmbH has been developed in accordance with the standards specified in ▹chapter 2.12.1◃ and certified by TÜV Rheinland.

EC Type Examination Certificate Number:	**01/205/5261.01/18**
Test report no.:	968/M 264.06/18, dated 2018-09-07
Notified body:	0035

The declaration of conformity, see Appendix ▹Appendix D - Declaration of conformity on page 175.

2.12.1 Approvals, directives and standards

Safety engineering standards and directives	**Area of application**	**Approvals**
IEC 61508, Parts 1-7	Functional safety of safety-related electric, electronic and programmable electronic systems	up to SIL 3
DIN EN ISO 13849-1	Safety-related components of control units	up to performance level e
IEC 62061	Functional safety of safety-related electric, electronic and programmable electronic systems Fulfillment of increased stability requirements in accordance with EN 61326-3-1	
Additional standards	**Area of application**	
IEC 61800-3	Adjustable speed electrical power drive systems - Part 3: EMC requirements	
IEC 61800-5-1	Adjustable speed electrical power drive systems - Part 5-1: Safety requirements - Electrical, thermal and energy	
IEC 61800-5-2	Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional	
EN 61131-2	Programmable controllers - Part 2: Equipment requirements and tests	
IEC 60204	Electrical equipment of machines	

3

USE OF THIS MANUAL

This safety manual contains information on the intended use of the Baumüller Safety Module.

Knowledge of the regulations and proper technical implementation of the safety instructions in this manual by qualified personnel are prerequisites for the safe installation, commissioning and safety during the operation and maintenance of the Baumüller Safety Module. Unqualified interference with the Safety Modules during shutdown or use of the safety functions or failure to comply with the instructions of this manual can lead to serious personal injury, property damage or environmental harm, for which Baumüller assumes no liability.

Baumüller safety components and systems are developed, manufactured and tested in compliance with the applicable safety standards. They may only be used under the specified environmental conditions and only in connection with approved external Safety Modules.

The operation manual contains safety instructions, descriptions of the interfaces and information on the phases of the product's life cycle:

- Planning
- Installation/Assembly
- Commissioning
- Validation
- Operation
- Modification/Retrofitting
- Troubleshooting
- Maintenance/Repair
- Disassembly

4

SAFETY

This chapter provides an overview of all important safety aspects for the optimum protection of the personnel as well as for safe and trouble-free operation at the machine or installation on site. The observance of this is an important precondition for the safe an trouble-free operation

4.1 Contents of the operation manual

All persons assigned to work on or with the Safety Module must have read and understood that operation manual before beginning work with the Safety Module. This also applies if the person concerned has already worked with such a Safety Module or a similar Safety Module or has been trained by the manufacturer.

4.2 Alterations and rebuilding of the Safety Module

In order to avoid hazards and ensure optimum performance, neither alterations, additions nor rebuilding work may be conducted on the Safety Module unless explicitly authorized by the manufacturer.

4.3 Intended use

The Safety Module is exclusively designed and constructed for the intended purpose of use described here.

You are using the Safety Module according to the terms, as soon as you regard all notes and information in this operation manual.

WARNING!

Danger due to use other than intended!

Any use of the Safety Module different from and/or exceeding beyond the scope of the intended use can lead to dangerous situations.

Therefore:

- Only use the Safety Module as intended.
- Only use the Safety Module in combination with compatible controllers (see ▹Compatibility list◃ on page 31).
- Follow all specifications of this operation manual.
- Ensure that exclusively qualified personnel work on or with the Safety Module.
- Take care in project planning to see that the Safety Module is always used within its specifications.
- Ensure that the power supply meets the required specifications.
- Only operate the Safety Module if it is in technically faultless condition.
- Only use the Safety Module with certificated components or in combination with components approved by Baumüller Nürnberg GmbH.

4.4 Operator responsibility

The Safety Module is implemented in an industrial zone. The operator of the Safety Module is thus subject to the legal work safety obligations.

In addition to the work safety instructions in this operation manual, the safety, accident prevention and environmental protection regulations applicable to the area of application of this Safety Module must also be complied with. In doing so, the following applies in particular:

- The operator must inform himself of the applicable work safety regulations and additionally ascertain hazards arise through the special work conditions at the place of use of the Safety Module in a risk analysis.
  The operator must implement these in the form of operation instruction for the total operation of the machine /application in dependence of the accordant risk assessment.
- This operation manual must be kept in the immediate vicinity of the Safety Module and be accessible to persons working on and with the Safety Module at all times.
- The statements of the operation manual are to be followed completely and absolutely!
- The Safety Module may only be operated in technically faultless condition and must be safe for operation.

4.5 Protective category

When installed in the controller, the Safety Module complies with the protective category IP20.

4.6 Personnel training

WARNING!

Risk of injury if operated by insufficiently qualified persons!

Improper handling can lead to severe personal injury and property damage.

Therefore:

- Only allow certain activities to be conducted by persons specified in the respective chapters of this operation manual.

The following qualifications for various areas of operation are specified in the operation manual:

- **Operating personnel**
  The drive system may only be operated by persons who have been trained, instructed and authorized to do so.
  Troubleshooting, repairs, cleaning, maintenance and exchange may only be conducted by trained or instructed personnel. These persons must be familiar with the operation manual and act according to it.
  Commissioning and instruction may only be conducted by qualified personnel.
- **Qualified personnel**
  Electrical engineers and specialist electricians of the customer or a third party who are authorized by Baumüller Nürnberg GmbH, trained and certified in the installation and

commissioning of Baumüller drive systems and commissioning, grounding and designating electrical systems and Safety Modules in accordance with the safety engineering standards.
Qualified personnel is educated or trained in the maintenance and use of suitable safety equipment in accordance with the respective local safety engineering standards.

4.7 Personnel protective equipment

Wearing the appropriate personal protective equipment when working is required in order to minimize hazards to the health.

- Always wear the respective protective equipment required for the respective task when working.
- Observe signs on personal safety in the work area!

Protective work clothes

consists of close-fitting workwear of low tear strength, without loose sleeves or projecting parts. Intended mainly to protect the wearer from moving machine parts.

Do not wear any rings and necklaces.

Protective helmet

for protection from falling and flying parts.

Safety shoes

for protection from heavy falling objects.

Safety gloves

to protect hands from friction, abrasions, puncture, prick wounds or deeper injuries as well as from contact with hot objects.

To be worn during special work

Protective glasses

to protect the eyes from flying parts and spraying liquids.

4.8 Special dangers

The residual risks arising as a result of the hazard analysis will be specified in the following section.

Observe the safety instructions described here and the warning notices in the following chapters in order to reduce health hazards and avoid dangerous situations.

Electrical current

DANGER!

Live-threatening danger from electrical current!

There is a live-threatening danger at contact with live parts. The damage of the insulation or of a single part can be live-threatening.

Therefore:

- Switch off the voltage supply immediately if there is a damage of the insulation.
- Only qualified personnel may work at the electrical installation.
- De-energize the machine for all work with reference to the discharge times (e.g. the controller DC-link) and protect against switching it on again.
- Observe the valid product safety standards when dealing with high-voltage equipment.

Moving parts

WARNING!

Danger of injury due to moving parts!

Rotating and/or linear moving parts can cause severe injuries.

Therefore:

- Do not interfere with moving parts during operation.
- Do not open covers during operation.
- The mechanical residual energy depends on the application. Powered parts will also keep rotating/moving for a certain time after the power supply has been shut off. Make sure to provide suitable safety equipment.

4.9 Electric safety

The Safety Module is designed for contamination level 2 in accordance with DIN EN 61800-5-1. This means that only non-conductive contamination may appear during operating time.

This is achieved by installing the controller with the Safety Module into a protected mounting location (at least IP 54, e.g. the mounting in a control cabinet). Short-term conductivity from condensation is only permissible if the module is not in operation.

WARNING!

Risk of injury from conductive contaminants!

No conductive contaminants may appear during operating time.

Therefore:

- Before installing and commissioning the system, check if the contamination degree 2 is not exceeded (do this also by optical inspections, if it is necessary).

4.9.1 Notice on power supply

WARNING!

Risk of injury from electric current!

Only safety devices which have a safe disconnection to the 230 volt mains may be connected to the Safety Module.

The power supply unit for generating the 24 Volt supply must meet the requirements for PELV in accordance with EN 60204-1.

4.10 Safety equipment

WARNING!

Live-threatening danger from inoperable safety equipment!

Safety equipment provides a maximum of safety during operation. Even if the safety equipment may make work processes more complicated, they may not be put out of operation under any circumstances. Safety is only ensured if the safety equipment is intact.

Therefore:

- Before starting to work, check the installed safety equipment. Make sure that the safety equipment is without damages and was not manipulated.

4.11 Conduct in the event of danger and accidents

Preventive measures

- Always be prepared for accidents or fire!
- Keep first aid equipment (first-aid box, blankets, etc.) and fire extinguishers on hand!
- Instruct personnel in accident reporting, first aid and rescue equipment.

In case of emergency: Act properly

- Put the Safety Module out of operation immediately:
  - Always immediately EMERCENCY-OFF at electrical hazards like short-circuits, smoke, fire, lightning.
  - At mechanical hazards, if necessary EMERCENCY-STOP until the machine stops. Additionally, EMERCENCY-OFF.
- Keep people out of the danger zone.
- Introduce first aid measures.
- Inform the supervisors at the site.
- Notify a doctor and/or fire department.
- Clear access routes for rescue vehicles.

4.12 Signs

The following symbols and notification signs are found in the work area. They relate to their immediate installation environment.

WARNING!

Injury hazard due to illegible symbols!

In the course of time, stickers and symbols on the Safety Module can become dirty or otherwise illegible.

Therefore:

- Keep all safety, warning and operation signs on the Safety Module in easily legible condition at all times.

Electric current

Only qualified personnel may work in work spaces with this marking.

Unauthorized persons may not touch work equipment bearing this marking.

5

FUNCTIONAL SAFETY

This chapter describes parameters in relation to functional safety. In accordance with IEC 61508, safety means first of all, that a system is free of unwarranted risks. Functional safety is the part of the overall safety, which ensures that a safety system's response to its input conditions is free of errors. Internal safety-related device errors must be detected and brought into a safe condition in the process.

5.1 Safety-related parameters for an operation of 20 years

The following table lists the safety-related parameters of the Safety Module for an operation of 20 years with an average environmental temperature of 70°C.

Safety-related parameters of local I/O terminals and decentralized components can be found in the applicable documentation. The values in the following table relate exclusively to the Safety Module.

In the identification values indicated below, the calculation to the following safe in-/outputs is always contained.

- CHAIN_IN
- CHAIN_OUT
- Output brake to the controller
- Output pulse inhibit to the controller
- Cycle output / cycle outputs

Minimum configuration:

Values are valid for the additional parameterization of:

1 x safe input / 1 x safe output

(additionally also e. g.:

- DIG1_IN_1
- DIG1_OUT_1

)

Maximum configuration

Values are valid for the additional parameterization:

8 x safe input / 2 x safe output

(additionally also:

- DIG1_IN_1
- DIG2_IN_1
- DIG3_IN_1
- DIG1_IN_2
- DIG2_IN_2
- DIG3_IN_2
- STO_IN_1
- STO_IN_2
- DIG_OUT_1(A+B)
- DIG_OUT_2(A+B)

)

The specified values are valid for an environmental temperature of 70°C at the components.

Parameters in accordance with IEC 61508	
Safety Module configuration	**PFH** (Probability of dangerous Failure per Hour)
Single axis minimum configuration	PFH = 1,29 * 10^{-9} /h
Single axis maximum configuration	PFH = 1,95 *10^{-9} /h
Double axis minimum configuration	PFH = 2,10 * 10^{-9} /h
Double axis maximum configuration	PFH = 3,16 * 10^{-9} /h
Safety Module configuration	**PFD_{Av} (T=20 years)** (Probability of dangerous Failure on Demand)
Single axis minimum configuration	PFD_{avg} = 1,11 * 10^{-4}
Single axis maximum configuration	PFD_{avg} = 1,68 * 10^{-4}
Double axis minimum configuration	PFD_{avg} = 1,82 *10^{-4}
Double axis maximum configuration	PFD_{avg} = 2,72 * 10^{-4}

Parameters in accordance with IEC 61508	
Safety Module configuration	Safe Failure Fraction = fraction of failures which lead to a safe status.
Single axis minimum configuration	SFF according to SIL 3
Single axis maximum configuration	SFF according to SIL 3
Double axis minimum configuration	SFF according to SIL 3
Double axis maximum configuration	SFF according to SIL 3

Parameters in accordance with DIN EN ISO 13849-1		
Safety Module configuration	**$MTTF_D$** (Mean Time To Failure dangerous)	**Classification**
Single axis minimum configuration	$MTTF_D$ = 185 years	HIGH
Single axis maximum configuration	$MTTF_D$ = 124 years	HIGH
Double axis minimum configuration	$MTTF_D$ = 127 years	HIGH
Double axis maximum configuration	$MTTF_D$ = 70 years	HIGH
Safety Module configuration	**DC_{avg}** Diagnostic Coverage	**Classification**
All configurations	DC_{avg} = 97%	HIGH[a]

a. This values lies within the permissible tolerance of 5% according to EN ISO 13849-1 for the classification HIGH.

The SAF modules can be used in applications as far as Cat 4/PL e according to EN ISO 13849-1 and SIL3 according to EN 62061 / IEC 61508.

No proof test is necessary during the expected service life of the Safety Module of up to 20 years.

CAUTION!

If the user calculates his safety application for the specified values with 20 years, the Safety Module must be decommissioned after 20 years. This is the maximum service life of the device. The Safety Module must be decommissioned after this time. The Safety Module must be properly disposed of. It is forbidden to perform a proof test.

NOTICE!

The proper condition of the controller's fan must be checked before commissioning the Safety Module. The maintenance and cleaning of the fan must be made at least once a year.

6

PACKAGING AND SHIPPING

Before shipping, we package every Baumüller device in such a manner that damaging occurring during transport is very unlikely.

6.1 Shipping

Modules are packaged at the factory according to the order.

- Avoid heavy shaking and concussions during shipping.
- Avoid static discharges on the electronic components of the module.
- Only remove the module from the protective packaging immediately before assembly.

6.2 Unpacking

Upon receiving the still-packaged module:

- Check to see if any shipping damages can be found!

If so:

- Immediately file a complaint to the supplier. Confirm the complaint in writing and immediately contact the representative of Baumüller Nürnberg GmbH who is assigned to assist you.

CAUTION!

Danger due to electrostatic discharge!

The Safety Module (specifically its electronic components) can be damaged or totally destroyed if exposed to electrostatic discharges by being touched by hand.

Therefore:

- Follow the rules and instructions on handling components sensitive to electrostatic discharge when handling the Safety Module.

If no damage from shipping can be found:

- Open the packaging of the device.
- Check the items included in the delivery against the bill of delivery.

The items included in the delivery are:

- **Safety Module for b maXX 5000**, BM5-O-SAF-002 or BM5-O-SAF-003
- This operation manual including certificate of conformity / declaration of manufacturer.

- If any shipping damages can be found or any items are missing from the delivery, file a complaint to the Baumüller representative assigned to you.

6.3 Disposing of the packaging

The packaging consists of cardboard and plastic.

- Follow local regulations on disposal if you dispose of the packaging.

6.4 To be observed when shipping

The module has been packaged at the factory for the initial shipping. If you subsequently need to ship the module again, observe the following:

- Use the original packaging

or

- Use suitable packaging for the components groups which are sensitive to electrostatic discharge.

Make sure that the shipping conditions (see ▹Appendix C - Technical data◃ from page 163 onward) are consistently fulfilled throughout the entire shipping process.

7

DESCRIPTION OF THE SAFETY MODULE

This chapter describes the Safety Module, the meaning of the display- and operating elements and explains the type key on the module.

7.1 General information

The Safety Module monitors the drive's motion. It monitors the valid data of the drive's motion detection subject to the required safety functions. The drive functions and the drive control are executed in the controller. The drive functions are continued only then, if the Safety Module conforms with the motions, which are executed.

The safety functions (see ▷page 55◁), which are supported by the module, can be activated via the integrated digital module inputs as well as via the safe data telegrams.

The Safety Module has two independent and safe pulse inhibits for two drive axes on the output side. These are enabled either by a safety function or by a safety-relevant error. This puts the drive into the status STO (Safe Torque Off) (refer to the description of the interface of the safe pulse inhibit in chapter ▷STO-Inputs◁ from page 94.

Precondition at STO is a brake, which can be connected optionally. For this, the brake supply voltage is led internal via the Safety Module and the controller to the connection for the brake, which is there. Now the accordant brake supply can be switched off safely via a safe power output in the Safety Module.

The parameterization tool ProSafePara is used for the parameterization and the configuration of the Safety Module or the inputs and outputs. A detailed description of this tool is to be found in the corresponding online-help and in the application manual.

7.2 Compatibility list

The Safety Module can be operated in combination with b maXX 5000-type controllers, which have been released by Baumüller GmbH only.

Thereby, the safety level, which was defined in the type code of the controller, must accord to the safety level of the Safety Module at minimum.

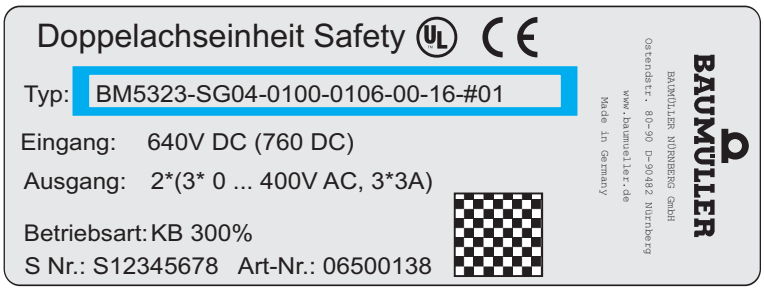


Figure 1: Example of a type plate of b maXX BM 5000

7.3 Safety notes

WARNING!

- Operate the Safety Module in combination with controllers, which where released by Baumüller Nürnberg GmbH only (see ▹Compatibility list◃ on page 31).
- The Safety Module may be operated with safety-relevant equipment, as e.g. safe I/O-terminals, EMERCENCY-STOP devices as per DIN EN ISO 13850 or with safety sensors as per EN 61496 only.
- At a total failure of one of the internal drives or of a control element, a short excitation of the drive (IGBT) (also in status STO) may occur. The angular movement thus traveled is dependent of the inductor's position and of the motor's pole pair number. It can reach a maximum of 180°/pole pair number.

DANGER!

Danger due to moving parts!

An immediate driver stage supply is caused by the input supply due to a connected safety element (emergency-stop device, safety-light grid). A fail of the controller can cause an unexpected start-up. Avoid an unexpected start-up during commissioning, by providing for external safety components.

Therefore:

- Remain at a safe distance from the moving machine parts / installation parts or from the moving machine / installation.

7.4 Operating mode

The module SAF-002 and SAF-003 have an identical hardware. They differ in the number of available safety functions. The allocation of the safety functions referring to the module types is shown in chapter ▹Safety Functions◃ on page 55. The module supports the monitoring of two independent drive axes.

There are two hardware types depending on the module: Daisy-Chain and with separated GNDs (see ▹Connector Assignment Interface X1◃ from page 89).

The functional principle of the modules SAF-002 and SAF-003 is shown in ▹Figure 2◃ on page 33. Monitoring- and safety function can be enabled directly via the wired safety components at the Safety Module as well as via connected safety components via a safety-oriented field bus.

The field bus communication always is made via the basic device. The Safety Modules have two power outputs, which can be used to activate safety-related brakes. In order to operate functional accesses of the controller on the brake, the safe brake supply is led from the Safety Module over the controller.

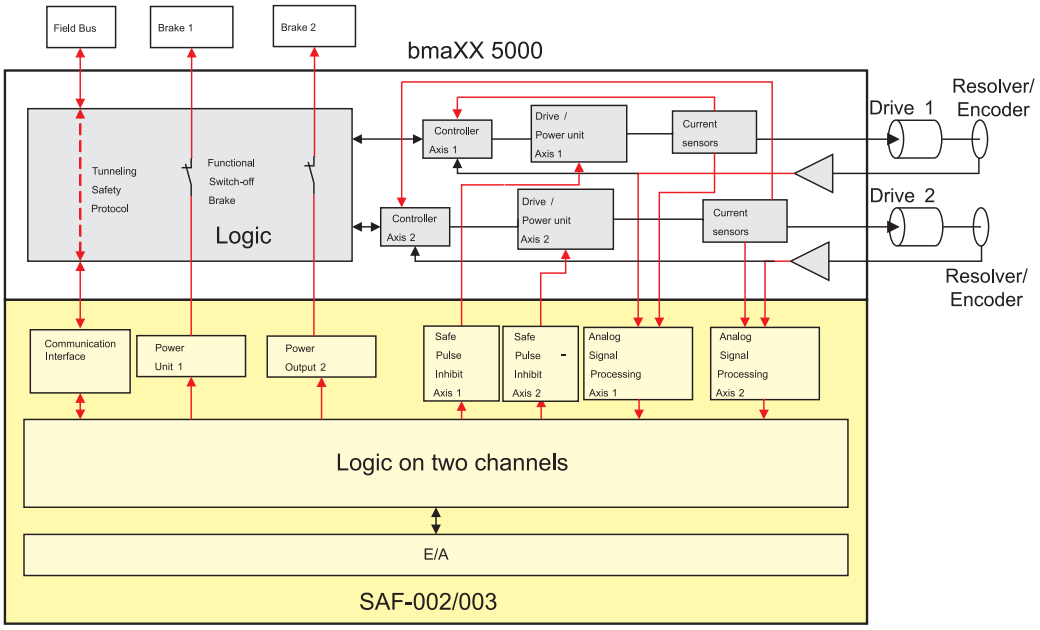


Figure 2: Operating mode

The encoder signals of the used rotary encoders from the controller's signal paths are decoupled and are provided for the parallel evaluation to the Safety Module for the motion detection of the input end.

The requirement for the rotary encoder is described in chapter ▹Requirements for the use of rotary encoders for the safety-related monitoring◃ on page 34.

If a required safety function is enabled, e.g. by a fault of the monitored limit in the Safety Module, a switch-off of the driver supply is enabled via the interfaces of the safe pulse inhibit. This is required for the control of the semiconductors, which are in the output stage. The drive now is in the status Safe Torque Off.

WARNING!

There are safety notes and risks referring to the safety function STO in chapter ▹Safety notes for the Function STO (Safe Torque Off)◃ on page 58, which must be considered.

7.5 Requirements for the use of rotary encoders for the safety-related monitoring

The following encoder types can be used for the safety-oriented monitoring with the Safety Module:

WARNING!

Only encoders, which have a certificate of an EC-type test or which have been released by Baumüller may be used for the safety-related monitoring.

The following requirements must be complied with.

- According to the applicable standards in the field of functional safety, encoders have a tested analog sine-/cosine-interface.
- The safety integrity level or the performance level of the encoder must be in accordance to a risk reduction of the supported safety functions at minimum.
- Encoders must have the possibility of a safe shaft connection between encoder shaft and motor shaft according to EN 61800-5-2, table D.16.
- Encoders must have the possibility of a safe connection between encoder cabinet and motor chassis according to EN61800-5-2, table D.16.
- The safety-relevant parameters must be common to the encoders:
  - Category
  - $MTTF_D$ per channel (Mean Time to Failure dangerous)
  - DC average (Diagnostic Coverage)
  - PL (Performance-Level)
  - PFH (Probability of Failure per Hour)
  - HFT (Hardware fault tolerance)
  - PFD (Probability of Failure on Demand)
  - SIL (Safety Integrity Level)
- Encoders should have internal diagnostic functions. The diagnostic functions take place independently without the excitation by the Safety Module.
- If present, the encoder-internal diagnostic functions switch the encoder outputs into a safe status, if errors occur.
- The maximum lifetime of the encoder must be considered. The encoder must be replaced upon completion of its lifetime.
- Encoders must apply to the appropriate EMC-directives and to the statutory environmental requirements for safety-related components.

DANGER!

The nonobservance of data sheet specifications and the exceeding of specified encoder data may result in the loss of the safety function. Integration guides and the encoder's specification must be strictly adhered to.

DANGER!

The encoder must be checked if it is applicable to be used for all monitoring functions.

DANGER!

The monitored controlled standstill (SOS) without dynamic sampling is permitted for a 12-hours period at the maximum.

If the SAF-002/-003 does not detect a movement at the encoder within the diagnosis test interval of 12 hours it automatically changes into the safe STO status (Safe Torque Off) and generates an accordant error message (error 108).

The SAF-002/-003 module must be switched off and on again. This means that the entire drive is switched off and on again or the voltage supply of the drive is interrupted for a short time:

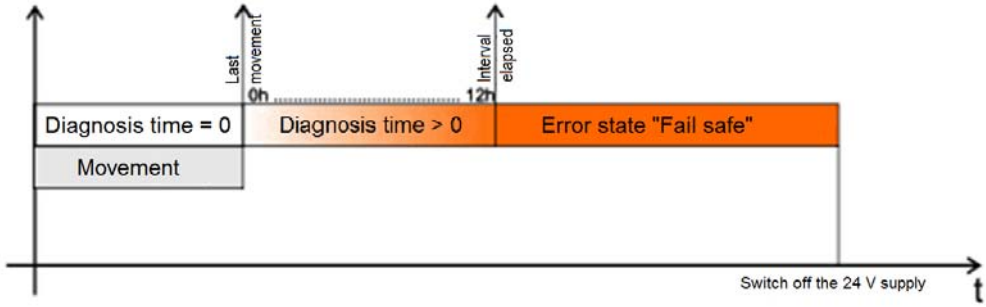


Figure 3: Encoder monitoring
Diagnosis time of 12 h expired -> Fail safe -> Switch off voltage supply

Instead of that, in the module version "Software extension" (refer to ▹Identification of the Safety Module - Type Key◃ from page 47 for the definition) the "Encoder Fail" is reported after 12 hours, which can be acknowledged by the user as long as it is not a permanent issue (refer to chapter ▹Acknowledgment encoder fail status◃ on page 40).

This way the switch-off of the module is avoided.

7.5.1 Standstill monitoring of the encoder at the SAF-002/-003 module in the "Software Extension" version

The encoder monitoring in the SAF-002/3 module in the "Software Extension" (see ▹chapter 7.8◃) differentiates between the following cases:

- Used encoder type (resolver or SINCOS-based encoders, such as the HIPERFACE®)
- Used motor type (synchronous or asynchronous motor)

Encoder type „resolver“

When using a resolver the encoder monitoring is made by an installed automatic test function in which the synchronization of the resolver signal is varied with the carrier frequency and the deviation of the signal amplitude resulting from this, is controlled. This way an encoder fail can be recognized quick and safe.

Encoder type „SINCOS“

The SINCOS encoder differs between the synchronous and the asynchronous motor type

The SAF module evaluates the controller parameter P107.038 whether the set motor type of the controller is synchronous or asynchronous. The SAF module selects the model of the standstill monitoring depending on the motor type:

„SINCOS“ with the synchronous motor

The electrical generated field of the controller corresponds with the mechanical angle when using the synchronous motor because of the rigid coupling from the field to the mechanics.

The voltage values at the encoder input of the SAF module do not change anymore. The electrical angle "Phi electrical" is read and evaluated by the SAF module in order to check the plausibility if the controller recognizes a standstill, as well: If the electrical angle changes and a change of the mechanical angle was recognized at the rotary encoder within 3 seconds, then the SAF module changes in the safe status and reports an encoder error.

NOTE!

When using the "SINCOS with synchronous motor" a plausibility of the encoder value during standstill is carried out at the SAF module input by the additional evaluation of the measured electrical angle "Phi electrical" of the controller.

Due to this, an undetected fail of the standstill monitoring, because of an incorrect encoder recognition is reliably avoided even if it goes beyond the 12 hours.

When using the "Resolver" as well as the "SINCOS with synchronous motor" consequently an encoder fail automatically is recognized. The module returns in the safe state and switches off the drive.

„SINCOS“ with an asynchronous motor

When using the SINCOS with asynchronous motor encoder type an automated encoder monitoring is not possible because of the physical features of the motor, as the electrical angle can even still change during standstill.

Here the check is made in the standard version by means of the diagnostic time. If and as long as there is no movement the diagnostic time starts running. If a movement is recognized at the encoder input the diagnostic time is set to "0" and immediately starts to operate again.

If an encoder-based safety function is activated and if the diagnostic time has extended the diagnostic testing interval of 12 hours, then the "Encoder fail" changes immediately into the safe status "Encoder Fail":

Figure 4: Encoder monitoring at the SINCOS encoder with asynchronous motor
Diagnosis time of 12 h expired -> the safety function is requested once more

Even if during an actively encoder-based safety functions the diagnostic interval is exceeded because there is no movement, the module changes into the safe status "Encoder Fail".

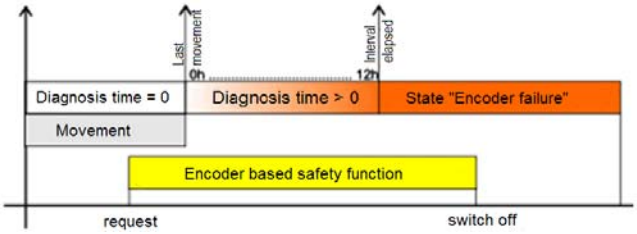


Figure 5: Encoder monitoring of the SINCOS encoder with asynchronous motor
Expiration diagnostic time during the encoder-based safety function -> Encoder fail

The "Encoder Fail" status can be exited by deactivating all of the safety functions of the module and after acknowledging the error message in the controller a movement can be generated at the encoder. With this movement the diagnostic time is set to "0" again and the module is ready for use, again.

Then the encoder-based safety functions of the module can be activated, again:

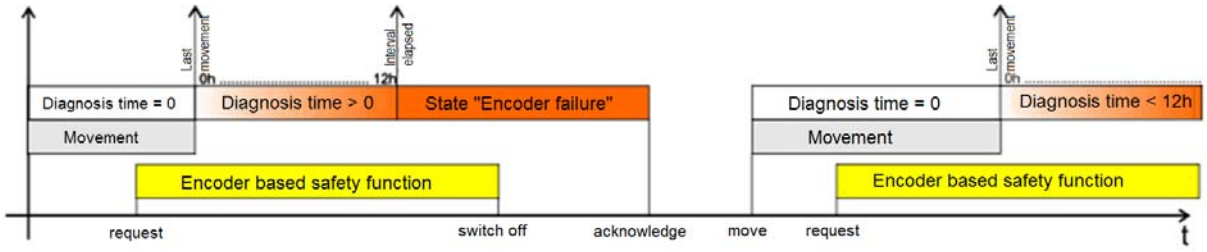


Figure 6: Encoder monitoring of the SINCOS encoder with asynchronous motor
Error acknowledgment -> Movement -> The safety function is requested once more.

If there is no movement or if the movement was not recognized by the module then it immediately changes into the status "Encoder Fail":

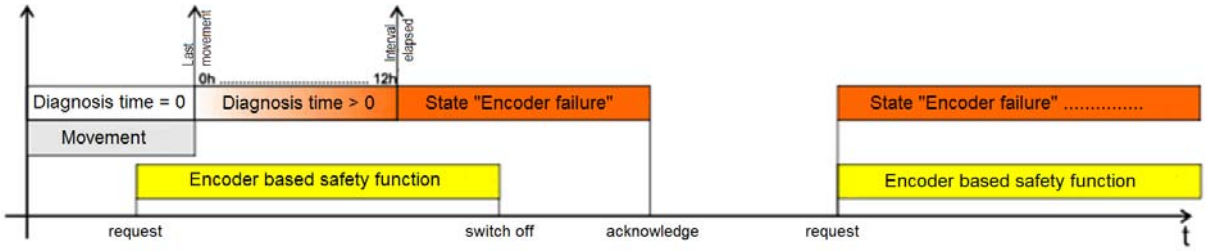


Figure 7: Encoder monitoring of the SINCOS encoder with asynchronous motor
Error acknowledgment has expired -> No movement -> Encoder fail during demand

The monitoring of the encoder in the "Software Extension" is evaluated, only if there is actually a safety function with the speed or the position information activated or is demanded. However, the diagnostic time is running Independently of this, as long as no movement is detected or the automatic encoder monitoring is reset (such as of the encoder type "Resolver"):

In case of the encoder monitoring of the SINCOS encoder with the asynchronous motor after expiration of the diagnostic time a movement must be carried out before the encoder-based safety function is activated:

Figure 8: Encoder monitoring of the SINCOS encoder with asynchronous motor
Expiration of diagnostic time -> Movement -> Demand

DANGER!

In order that the SAF-002/3 module can carry out the limit value calculations and the encoder monitoring properly, at first for each axis the parameters of the controller for the motor management and the parameters of the drive "Encoder Type", "Encoder PPR Count" and the "Motor Type" must be set correctly.

Parameter setting in the controller:

- P107.038 (motor flag), P106.001 (encoder type), P137.001 (PPR count).

The settings are made axis-specific in the controller.

Regarding axis 1:

- "Start page\Axis1\Configuration\Motor\Motor in general\Motor type"
- "Start page\Axis1\Configuration\Encoder 1\PPR count"

("Encoder type" is automatically determined)

Regarding axis 2:

- "Start page\Axis2\Configuration\Motor\Motor in general\Motor type"
- "Start page\Axis2\Configuration\Encoder 2\PPR Count"

("Encoder type" is automatically determined)

Setting of the parameters in ProSafePara:

- Axis 1: P207.004 (motor type), P207.006 (encoder type), P207.005 (encoder PPR count)
- Axis 2: P207.012 (motor type), P207.014 (encoder type), P207.013 (encoder PPR count)

The settings are carried out in the group "Parameter of the drive"

NOTE!

During the activated "Parameter check" (ProSafePara parameter P207.002="On" of axis 1 and P207.010="On" for axis 2) the set SAF module parameters "Motor Type", "Encoder Type" and "Encoder PPR count" are automatically checked with the actually set values of the controller (controller parameter P107.038, P106.001 and P137.001) during the set-up of the SAF module.

In exceptional cases the "Encoder PPR count" can differ from the encoder value, if for example an electronic or mechanic gear is used , so that the increments per revolution of the encoder and the motor differ. In this case the parameter check can knowingly be deactivated by the user.

This does not have negative effects on the SIL value or the PLd/e - estimation and accords to the previous operating principles in the software version "Standard" (refer to ▹Identification of the Safety Module - Type Key◃ on page 47).

When creating a new project in ProSafePara from v1.1.0.0 onward the parameter check is activated per default. In the previous ProSafePara version 1.0.0.20 the parameter check automatically is switched off.

DANGER!

The operating mode ("With encoder" / "Without encoder") can be activated axis-specific in the controller by ProDrive in the menu. The following must be selected when using "Modus motor operating mode" (P019.052):

- „Start page\Axis1\Configuration\Motor\Motor-In general\Motor-Type" or
- „Start page\Axis2\Configuration\Motor\Motor-In general\Motor-Type"

If the controller is operated in the "Open Loop" (encoderless) mode, then encoder-dependent safety functions may not be parameterized!

7.5.2 Acknowledgment encoder fail status

In the Module version "Software extension" (see ▹chapter 7.8◃) the encoder fail status can be acknowledged by the controller again. In order to do this, the following must be complied with:

- Deactivate all of the safety functions.
- Acknowledge the message "Encoder fail" in the controller.
- Generate a movement at the drive, so that the module can reset the internal diagnostic time leading to the encoder fail.
- If position-dependent safety functions were defined homing must be executed once more.

Optionally to the controller, the message "Encoder fail" can be acknowledged by the S1 key of the SAF module. The key must be pressed approximately 500 ms. The green LED H2 lights up if the key is pressed.

NOTE!

The encoder fail status can be acknowledged, if prior to this all of the safety functions were deactivated. After this, a movement of the drive must be carried out, so that the module detects a movement of the encoder and can reset the internal diagnostic time.

When using the safety function SLP or SCA homing must be carried out once more as a safe absolute position is required.

DANGER!

Before the deactivation of safety functions it must be considered that all persons keep the distance from the danger range of the machine or installation or that all persons on-site were informed about the planned deactivation of the safety functions and of the following movement.

Only until afterwards the safety functions may be deactivated and the drive or the machine may be used!

DANGER!

The Safety Module always evaluates the sin/cos-tracks and not the digital absolute track, since this is not safe.

A safe absolute position is required for the safety functions SLP and SCA. Therefore, the safe position must be referenced with each new switch-on!

7.6 The Structure of the Safety Module

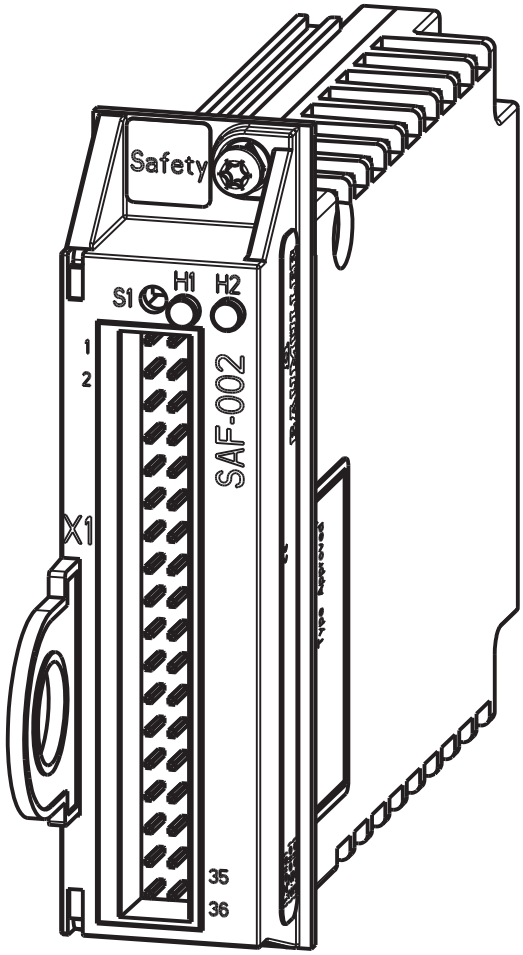


Figure 9: Safety Module SAF-002

7.7 Processing and Display Elements

7.7.1 LEDs for the Display of Operating States

For the display of the operating status the Safety Module has two LEDs on the front side (LED H1 - red, LED H2 - green).

- LED H1 (red) - Display of errors or incompatibility to the controller.
- LED H2 (green) - Display of an error-free operation.

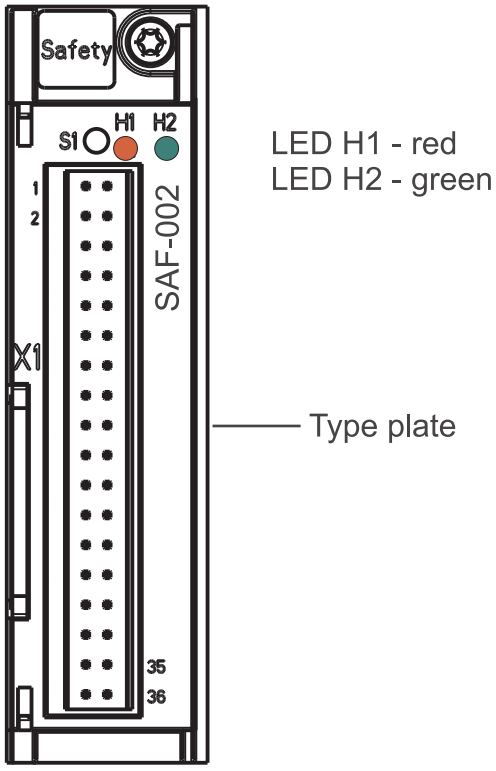


Figure 10: LEDs Safety Module

In the following table the possible display combinations of the status-LEDs and its meaning are listed:

LEDs		
H1 (red)	**H2 (green)**	**Meaning**
Off	Off	No supply voltage
Off	On	Error-free operation.

LEDs		
Off	Flashing (50 ms on / 50 ms off)	The configuration file was not loaded, Standard configuration active (see ▹Standard Configuration◃ from page 113)
Flashing	Off	Device error or unpermitted module change (commissioning not possible, see ▹Troubleshooting and Error Correction◃ from page 137).
On	Off	Firmware- or parameter data of Safety Module are not coinciding with the controller's data. Parameter data of the controller must be copied to the Safety Module by pressing the button. The green LED flashes when the button is pushed.

7.7.2 Button for verification reasons

The verification of the data import of the controller's standard parameter data in the Safety Module's parameter storage is made with the button on the front side of the Safety Module, also see chapter ▹Replacement of the module◃ from page 127).

The S1 button can also be used to acknowledge the message "Encoder fail" (refer to ▹Acknowledgment encoder fail status◃ on page 40).

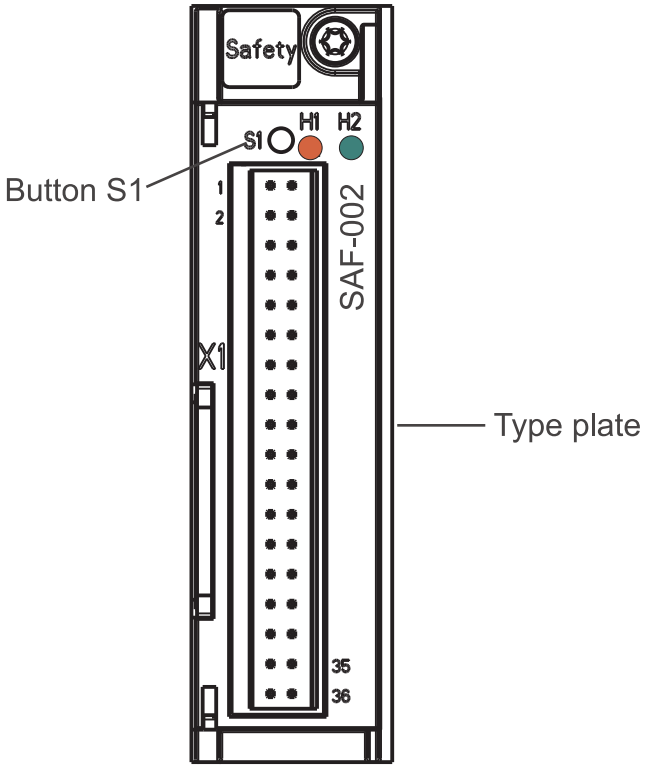


Figure 11: Button S1 Safety Module

7.8 Software Extension SAF-002/-003 Module

Due to field experiences with the SAF-module 002/-003 over a longer period the behavior was improved by a software extension.

In this way the following benefits can be achieved compared to the previous versions:

- Interference suppression of the encoder signals by electronic filters
  Interferences can be coupled into the encoder signals due to the IGBT switching procedures of the controller, causing that the SAF-002/-003 module switches off even before the set SLS speed limits are reached.

  ➲ Measure:
  The number of the encoder sensing is increased within 2ms from 1 up to now to 7 and on the basis of these a moving weighted averaging is implemented. Interferences are filtered, this way.

- "Encoder error" response after an inactivity of 12 hours.
  The module changes into the "Encoder Error" status after inactivity of 12 hours.
  The module must be switched off and then on again.

  ➲ Measure:
  At the asynchronous motor an encoder fail is reported only, if an encoder-based safety function was activated and no motion of the encoder was detected the last 12 hours.
  If an encoder failure has occurred the user can confirm it without interrupting the supply voltage with the module. In order to do this the user must deactivate all of the safety functions which confirm errors and reset the diagnostic time on the module back to "0" by a generated movement at the encoder, again. Then, the encoder-based safety function can be activated again.
  Homing must be carried out again, if the safety functions SLP or SCA are used, because a safe absolute positioning is required.

- Saving the gray data set on the SAF module
  Saving is possible if the module is in the basic state, only. The changing into the basic state is possible by using the configuration tool ProSafePara or if the module has detected an error (such as if there is no encoder connected).

  ➲ Measure:
  The change in the basic state can now be initiated by the controller, as well so that the parameter file can be transferred from the controller to the module and be stored there.
  The module returns into the active monitoring state after it was stored.

- Safety function SS1
  When activating this safety function the configured SS1-time elapses before the SAF module switches the drive into STO.
  This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

  ➲ Measure:
  In the parameterization referring to "SS1" in ProSafePara the new parameter "Signalize SS1 start to the controller " was added. If this parameter is "On" while the safety function SS1 is activated, then a message to the controller is carried out at the same time so that the drive can shut down at a brake ramp. In specific cases a higher-level control is not required.
  In order to achieve an efficient solution the brake ramp in the controller must be set in such a way that the drive comes to a standstill before the SS1-time in the SAF module

has elapsed and activates the module "STO".
The essential controller settings for this purpose are described in the current parameter manual b maXX BM5000 ("SS1 Stop" and "SS1 Stop Time").

- Programming a "General SS1 Time" for specific error types
  Basically, all error types carry out "STO" immediately and cause the drive to coast down and not being braked actively.

➲ Measure:
The user can now define an error reaction time for each axis in ProSafePara that are not assumed to be critical to the system (P207.003 "SS1-Time General Axis 1" and P207.011 "SS1-Time General Axis 2"), before "STO" is carried out.
This allows a higher-level control or alternatively the controller can bring down the drive precisely by a brake ramp. After the "SS1 Time General" has elapsed the drive is switched to STO by the module.

Example: Pulling the EtherCAT cable during a FSoE communication.
In order to achieve an efficient solution the braking ramp on the control or in the controller must be set in such a way that the drive comes to a standstill before the SS1 time in the SAF module elapses and activates the module "STO".
The related error reaction must be parameterized in the controller (refer to "Parameterization of the error reaction" and SS1 Stop Time" on ▹page 60◃).
The error types which support the SS1 error reaction were marked in the error list from ▹page 140◃ as "SS1 General".

- Function-specific SS1 times
  There are no configuration options for specific error procedures within the safety function such as the reaction behavior of a limit value noncompliance or the switching via FSoE to a data set which was not configured.

➲ Measure:
For most of the safety functions independent SS1 times can be defined, that are activated during specific error procedures within this safety function. This can include the following (-> listed in the descriptions referring to the specific safety functions):

- A limit value violation has occurred (such as the exceeding of the incremental dimension in "SLI").
- An encoder is not connected (such as in "SLS").
- Switchover to a data set via FSoE which is not configured.
- Exceeding the standstill time (no motion at the encoder within the last 12 hours at "SOS").

This allows a higher-level PLC to bring down the drive precisely by a brake ramp before "STO" is activated.

If an error occurs at the same moment a message is reported to the controller so that it can shut down the drive at the brake ramp. In specific cases a higher-level control is not necessary.

In order to achieve an efficient solution the brake ramp in the controller must be set in such a way that the drive comes to a standstill before the SS1-time in the SAF module has elapsed and the activates the module "STO".

- Automatic parameter check of the motor type, encoder type and the encoder increments

  During parameterization of the module via ProSafePara the user must already be aware of the motor and encoder type and of what number of increments are used. However, often unplanned delays or short-term changes occur previously to the commissioning. It often turns out to be, that the latest system test does not comply with the previously parameterized values of the system in the controller.

- Measure:
  When creating a new project in ProSafePara from v1.1.0.0 a parameter check is activated per default. When switching the system on the set SAF module parameters "Motor Type", "Encoder Type" and "EncoderPPR Count" are compared with the values that were set in the controller.

  If the values differ an error is generated.

  The parameter check can be deactivated by the user in ProSafePara project (such as at the "Open Loop" without encoder if the "STO" function is used, only).

  In the earlier ProSafePara version 1.0.0.20 the parameter check automatically is switched off.

The printed type key shows the SAF-002/3 module type (definition refer to chapter 7.8). The described software extension is coded directly in the type key and receives another part number than the "Standard" software version:

BM5 - O- SAF - 00x - xxx - **002** - #01	(SAF-002/3-module version "Software Extension")

Which software status was exactly installed can be read via the controller parameters P200.002 in ProDrive ("Firmware Version Module").

The Software Extension is supported from software status 004
(BM5 - O- SAF - 002 - xxx - **002** - #01 - yyy - **004**).

In order to profit from the benefits the ProSafePara version from V1.1.0.3 onward must be used to parameterize and in the controller the firmware from version V1.10 onward must be installed. The required settings in the controller are described in the parameter manual b maXX BM5000 ("SS1 Stop" and "SS2 Stop Time").

7.9 Identification of the Safety Module - Type Key

The type plate of the Safety Module with the accordant type key is on the right side of the module (see following example):

Figure 12: Type plate example Safety Module

NOTE!

The production year can be seen in the 3rd and the 4th digit. Example: Serial number „S311045208“ equates to the production year 2011.

NOTE!

This type key is valid for the Safety Module only. Other modules have their own type key.

BM5 - O- SAF - 002 - xxx - xxx - #01	Device generation (BM5 = BM5000), in which the module can be used
BM5 - O - SAF - 002 - xxx - xxx - #01	Option module
BM5 - O - SAF - 002 - xxx - xxx - #01	Safety Module
BM5 - O - SAF - 00x- xxx - xxx - #01	Type of the Safety Module 002 = Safety Module with 7 safety functions 003 = Safety Module with 12 safety functions
BM5 - O - SAF - 100- xxx - xxx - #00	Type of the Safety Module 100 = Reset module
BM5 - O - SAF - 002 - xxx - xxx - #01	Hardware type of the Safety Module 000 = Daisy Chain 001 = Separated grounds for operation with SO4000
BM5 - O - SAF - 002 - xxx - xxx - #01	Software type of the Safety Module 000 = Standard type 002 = Software extension
BM5 - O - SAF - 002 - xxx - xxx - #01	Safety level Identification for the compatibility between the module and the controller

As shown in ▹Figure 12◃ on page 47 after the safety level #01 two additional digits are printed on the type plate:

BM5 - O- SAF - 002 - xxx - xxx - #01 - **yyy** - zzz…….Hardware status

BM5 - O- SAF - 002 - xxx - xxx - #01 - yyy - **zzz**…….Software status

The hardware and the software status can be read with the controller operating tool "ProDrive":

The hardware status "yyy" is referred to as "**Hardware Version Module**" (P200.003) in ProDrive.

The software status "zzz" is referred to as "**Firmware Version Module**" (P200.002).

These states can be read either in ProDrive by the parameter list or in the navigation tree by the page "Diagnosis/SAF Module"

8

DESCRIPTION OF THE RESET-MODULE

This chapter describes the SAF-100 (Reset-Module) with its function and explains the type code on the module.

8.1 General

In order to operate the axis unit of the series b maXX 5000 the slot A of the device must be equipped with a module (also see 5.09021, instruction handbook b maXX 5000). In case the device was previously equipped with a higher safety level, the parameter storage of the controller must be reset before with the Reset Module (BM5-O-SAF-100) or with a reset command (see ▷Resetting of the safety level by the controller◁ on page 53).

8.2 Compatibility list

The Reset-Module (BM5-O-SAF-100) can only be used in the combination with controllers of the type b maXX 5000, which where released by Baumüller Nürnberg GmbH.

8.3 Operating mode of the Reset-Module (BM5-O-SAF-100)

In order to reset the module ID of the controller the slot A of the device must be equipped with a Reset-Module. After switching on the voltage supply of the controller the ID of the previously equipped modules is deleted.

After 15 seconds the voltage supply can be switched off and the slot A can be equipped with the requested Safety Module.

An operation of the controller with the Reset-Module is not possible, because the module does not provide supply for the controller's drivers.

8.4 Structure of the Reset-Module (BM5-O-SAF-100)

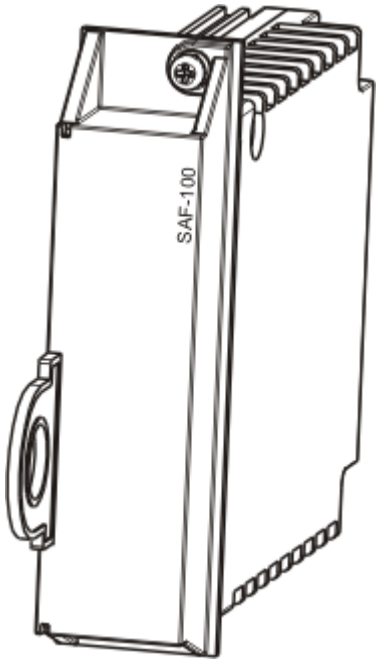


Figure 13: SAF-100 Reset-Module

8.5 Identification of the Reset-Module (BM5-O-SAF-100)

The type plate of the SAF module with its corresponding type code is found on the right side of the module (see the example below).

Figure 14: Example type code BM-O-SAF-100 Reset-Module

NOTICE!

- The exchange of the module must only be performed by authorized and qualified personnel.
- Prior to the exchange of the module, ensure that the Safety Module and the controller are compatible.

For a list of the controllers compatible with the Safety Module refer to the chapter ▷Compatibility list◁ on page 31.

NOTE!

The third and fourth digit of the serial number provide information on the year of production. Example: Serial number „S310045208“ corresponds to production year 2010.

8.6 Mode of operation module replacement

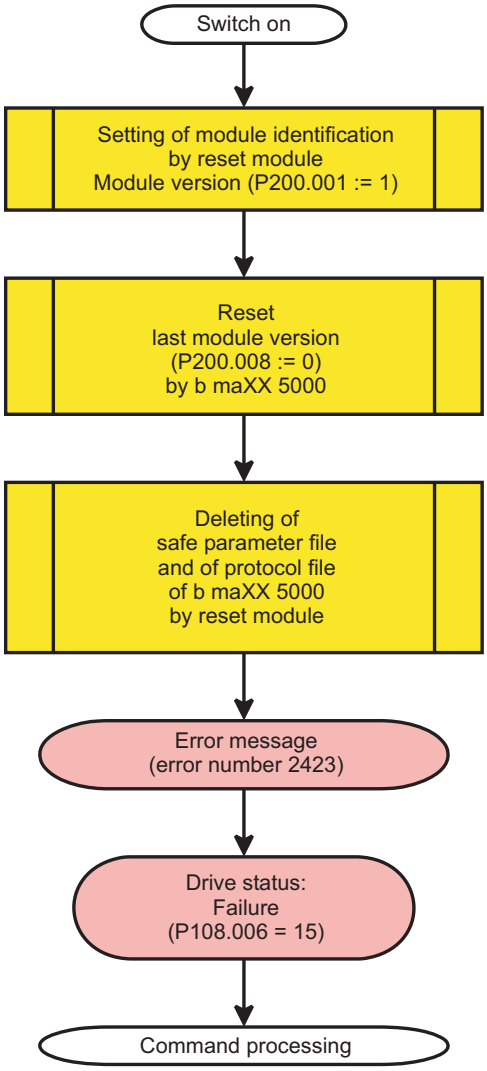


Figure 15: Mode of operation module replacement BM5-O-SAF-100

8.6 Mode of operation module replacement

9

RESETTING OF THE SAFETY LEVEL BY THE CONTROLLER

9.1 General

For the operation of an axis unit of the series b maXX 5000, the slot A of the device must be equipped with a module (also see 5.09021, Instruction handbook b maXX 5000). In case the device was already equipped with a module of a higher safety level, the safety level of the controller can be reset without a reset module with a controller command also.

9.2 Operation of mode of the reset command

The safety level of the controller is reset to the value zero by the command. The parameter files remain in the controller.

The following mode of operation for resetting must be followed:

1 Writing of the value 4096 into parameter 139.023.0.0 (system command)

2 On the 7-segment-display a four-digit code is displayed after the prefix „C“

3 This code must be written in parameter 200.020.0.0 (reset code).

4 After 15 seconds the voltage supply can be switched off and slot A can be equipped with the required module.

9.2 Operation of mode of the reset command

10

SAFETY FUNCTIONS

This chapter describes the supported safety functions of the Safety Modules BM5-O-SAF-002 and BM5-O-SAF-003.

10.1 Safety Functions of the Module BM5-O-SAF-002

The Safety Module BM5-O-SAF-002 supports the safety functions shown in the following table.

Safety Functions	Description see Chapter
Safe Torque Off (STO)	▹Safe Torque Off (STO)◃ from page 57
Safe Stop 1 (SS1)	▹Safe Stop 1 (SS1)◃ from page 59
Safe Stop 2 (SS2)	▹Safe Stop 2 (SS2)◃ from page 63
Safe Operating Stop (SOS)	▹Safe Operating Stop (SOS)◃ from page 65
Safely Limited Speed (SLS)	▹Safely Limited Speed (SLS)◃ from page 68
Safe Direction (SDI)	▹Safe Direction (SDI)◃ from page 70
Safe Brake Control (SBC)	▹Safe Brake Control (SBC)◃ from page 72

10.2 Safety Functions of the Module BM5-O-SAF-003

The Safety Module BM5-O-SAF-003 supports the safety functions shown in the following table.

Safety Function	Description see Chapter
Safe Torque Off (STO)	▹Safe Torque Off (STO)◃ from page 57
Safe Stop 1 (SS1)	▹Safe Stop 1 (SS1)◃ from page 59
Safe Stop 2 (SS2)	▹Safe Stop 2 (SS2)◃ from page 63
Safe Operating Stop (SOS)	▹Safe Operating Stop (SOS)◃ from page 65
Safely Limited Speed (SLS)	▹Safely Limited Speed (SLS)◃ from page 68
Safe Direction (SDI)	▹Safe Direction (SDI)◃ from page 70
Safe Brake Control (SBC)	▹Safe Brake Control (SBC)◃ from page 72
Safely Limited Position (SLP)	▹Safely Limited Position (SLP)◃ from page 75
Safely Limited Increment (SLI)	▹Safely Limited Increment (SLI)◃ from page 78
Safely Limited Acceleration (SLA)	▹Safely Limited Acceleration (SLA)◃ from page 81
Safe Speed Monitor (SSM)	▹Safe Speed Monitor (SSM)◃ from page 83
Safe Cam (SCA)	▹Safe Cam (SCA)◃ from page 85

10.3 Safe Torque Off (STO)

NOTE!

The Safety Modules SAF-002 and SAF-003 support the safety function STO.

10.3.1 Description

The safety function "Safe Torque Off (STO)" (as per EN 61800-5-2) is used for the safe switch-off of the drive at the safe pulse inhibit. In case of an error or at request the Safety Module assures, that the controller's voltage supply is switched off safe in the driver stage and that the pulse inhibit is therefore activated. The generation of a rotating field for motor control is prevented thereby. This switch-off function does not disconnect the energy supply from the motor.

Safe torque off (STO):

- The control of the power output stage is safely interrupted at the safety function. The motor's rotating field is safely interrupted. The drive coasts uncontrolled until it stops at activation of this safety function.
- The safety function complies with the stop category 0 as per EN 60204-1.

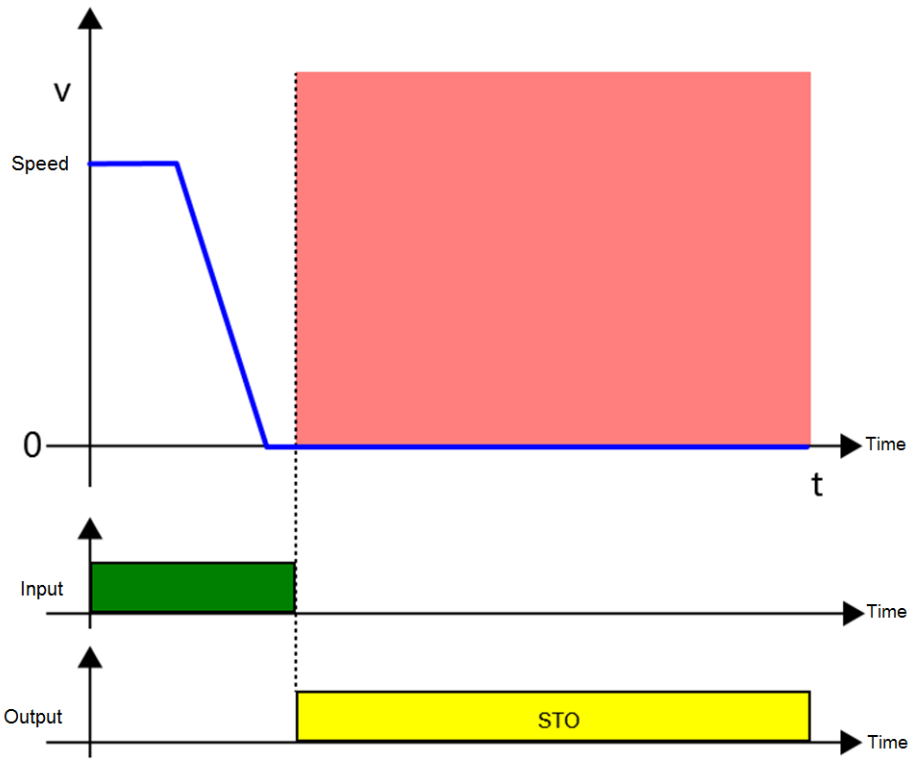


Figure 16: Safety function STO

NOTE!

If STO is activated, then a motor holding brake attached to the motor is activated, as well.

10.3.2 Safety notes for the Function STO (Safe Torque Off)

WARNING!

- In the status STO the drive is not disconnected from the energy supply.
- If drives have a permanent torque, as e.g. at suspended loads, then the safety function is not sufficient.
- The function STO is also active at error detection as well as at the fail of voltage supply. This can cause safety limits in dependence of the application. Therefore, in this case, additional actions must be made, as e.g. installing an appropriate holding brake.

DANGER!

Danger due to moving parts!

An immediate driver stage supply is caused by the input supply due to a connected safety element (emergency-stop device, safety-light grid). A fail of the controller can cause an unexpected start-up. Avoid an unexpected start-up during commissioning, by providing for external safety components.

Therefore:

- Remain at a safe distance from the moving machine parts / installation parts or from the moving machine / installation.

10.4 Safe Stop 1 (SS1)

NOTE!

The safety function SS1 is supported by the Safety Modules SAF-002 and SAF-003.

After activating the safety function „Safe Stop 1 (SS1)“ the drive is braked to an operating stop by the drive control. After elapse of the parameterized delay time (SS1-time) the drive is set to the state STO (Safe Torque Off). Thereby the braking ramp is not monitored.

- The safety function corresponds to the stop category 1 in accordance with EN 60204-1

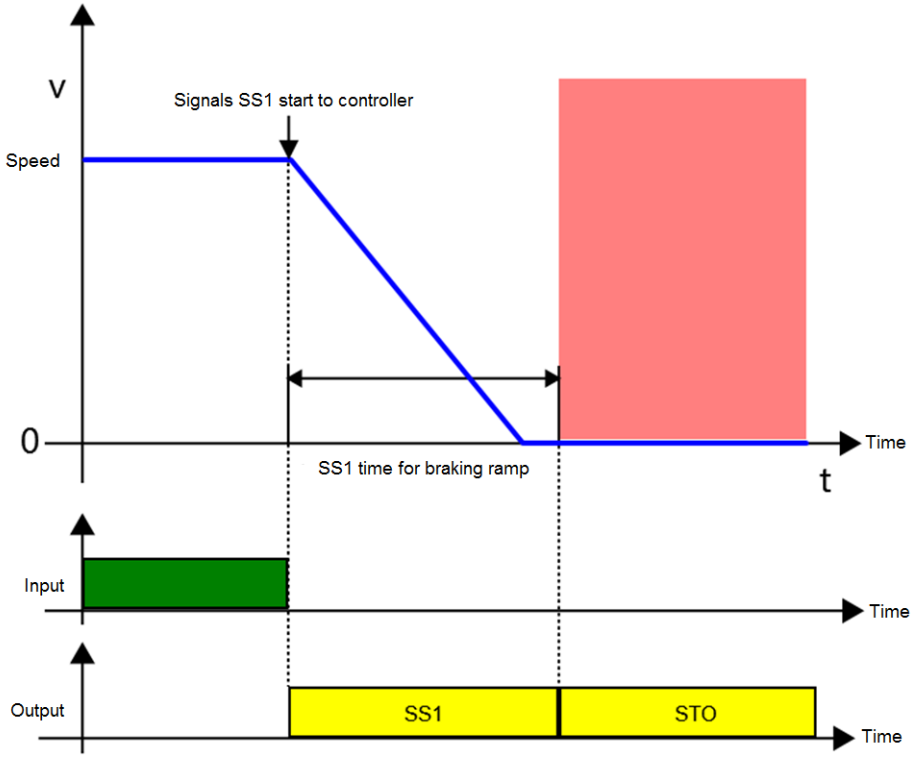


Figure 17: Safety function SS1 without monitoring the braking ramp

NOTE!

If STO is activated then the motor holding brake attached to the drive is activated.

10.4.1 Signalize SS1-start to the controller

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 due to the parameterization of P211.009 it is possible to report the activation start of the SS1 function to the controller (refer to ▹Figure 17◃ on page 59: "Signalize SS1-start to the controller"):

From FW 1.10 onwards the controller can be parameterized in such a way that it detects this signal from the SAF module and the drive can now be driven precisely and independently down a steep brake ramp. Thereby, in certain cases no higher level controller is required.

By the immediate active braking to the standstill of the drive it is avoided that the drive coasts to a stop.

In order to achieve an efficient solution the brake ramp of the controller must be set so that the drive comes to a standstill before the SS1-time in the SAF-module is processed and the "STO module is activated. The required setting of the controller are described in the current parameter manual b maXX BM5000 ("SS1 stop", SS1 stop time" and error reaction).

In ProSafePara the following parameters have to be set:

Setting SS1-time in the SAF module:

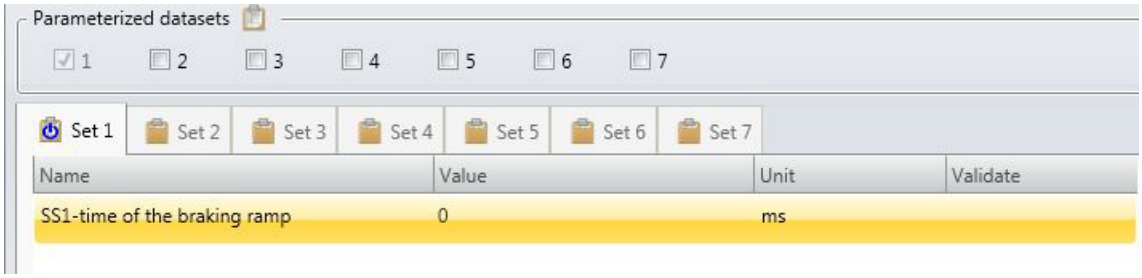


Figure 18: Example: Axis 1 setting SS1 time

The ProSafePara parameter P211.009 of the accordant axis must be set to "On" so that a signalization to the controller can be carried out:

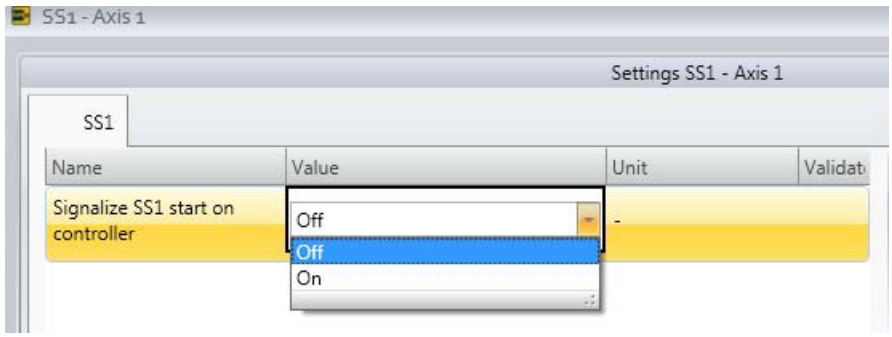


Figure 19: Example: Axis 1 activation of the signaling

The following setting of the controller must be carried out:

Parameterization of the error reaction (error 1066 "SS1 stop forced by SAF module"):

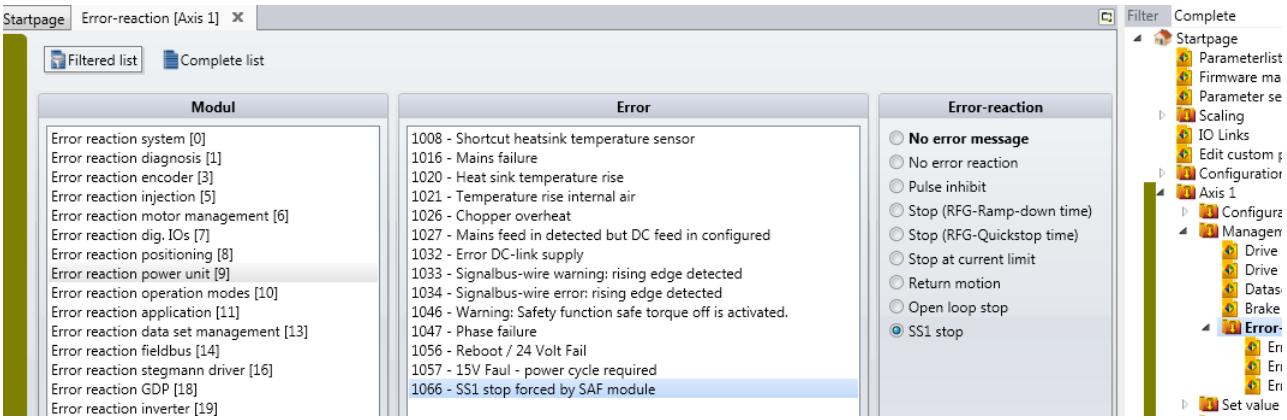


Figure 20: Parameterization of the error reaction

Besides the error reaction "SS1 stop" also another available error reaction can be parameterized (such as "Stop at the current limit")

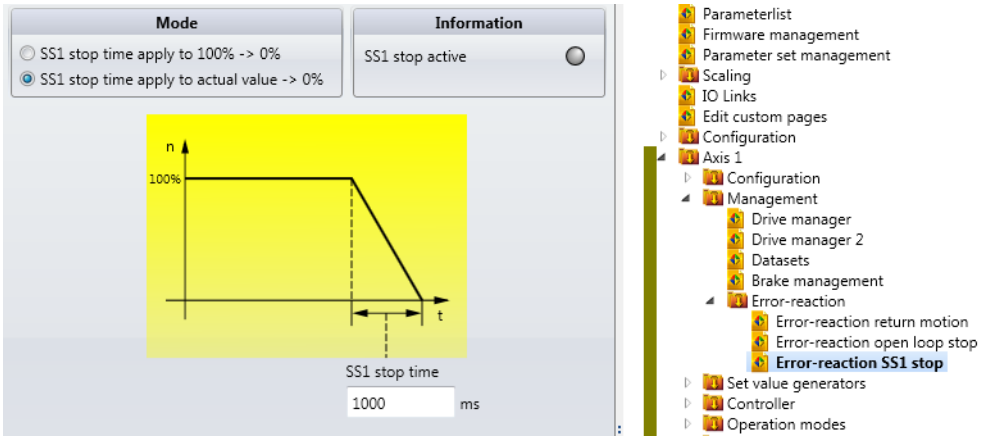


Figure 21: SS1 stop time (P110.029 in controller) in the "Error reaction SS1" setting

After the completion of the error reaction the drive changes to the fault state and inhibits the pulses.

It must be considered that the SS1 stop time in the controller (in the example 3000 ms) is lower than the set SS1 time on the SAF module (in the example above 4500 ms).

After the parameterized delay time in the SAF module expired (P211.030 "SS1 time of the brake ramp") the drive changes in the STO state (Safe Torque Off). Thereby, the brake ramp is not monitored. The pulses are inhibited safely even if the drive was not braked down, yet.

DANGER!

After completion of the error reaction "SS1 stop" the drive passes into the failure status and inhibits the pulses. The user can parameterize if an available brake is applied.

As the delay time in the SAF module is greater than in the controller the SAF module switches accordantly later into STO and this way the brake is safely applied.

A time gap can result of this in which the pulses of the controller have been inhibited in the failure status already and the brake has not been applied yet safely.

10.4.2 Error reaction for the safety function „SS1“

The following individual error can occur at the function "SS1":

- The switchover to a data set which is not applied.

During the occurrence of the individual error STO immediately becomes effective.

10.5 Safe Stop 2 (SS2)

NOTE!

The safety function SS2 is supported by the Safety Modules SAF-002 and SAF-003.

After activating the safety function „Safe Stop 2 (SS2)“ the drive is braked to an operating stop by the drive control. After the pre-parameterized delay time (SS2-time) the drive is set to the state SOS (Safe Operating Stop). Thereby the braking ramp is not monitored.

- The safety function complies with the stop category 2 as per EN 60204-1.

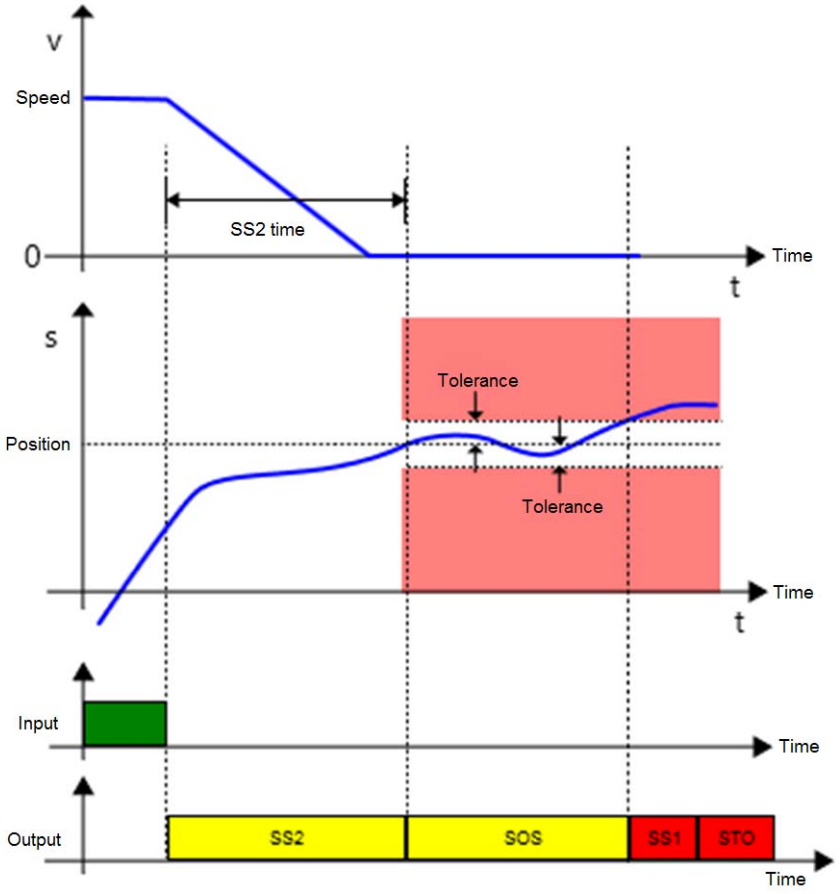


Figure 22: Safety function SS2 without monitoring of the brake ramp
During noncompliance with the following function "SOS" after a parameterizable "SS1" time " "STO" was initiated.

10.5.1 Error reaction with function-specific SS1 time for the safety function "SS2" and its following function "SOS"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 for every safety function a function-specific SS1-time can be parameterized:

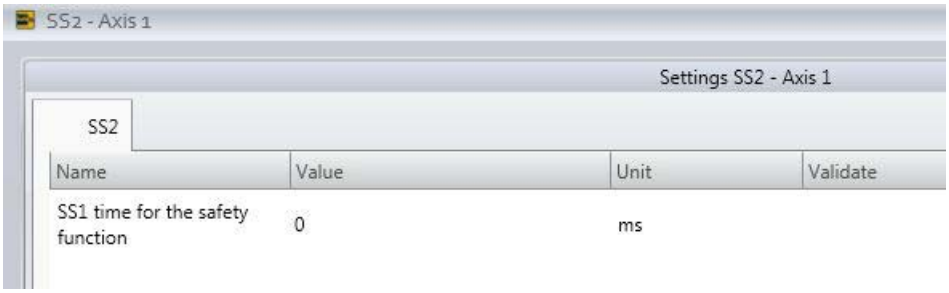


Figure 23: P212.005: SS1 time for the safety function „SS2“

This setting also applies to the following function SOS (an individual error can also occur during the following function SOS).

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

During the "SS2" function and its following function "SOS" the following individual errors can occur:

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Exceeding the tolerance window

If a value in P212.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

An accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting of "SS2 stop time" in ▹chapter 10.4.1◃).

Example:

During the process of the following function "SOS" the individual error exceeds the tolerance window. In ▹Figure 22◃ on page 63 this case is shown. The time "SS1" thereby accords to the parameterized time set in P212.005 before "STO" is operated.

10.6 Safe Operating Stop (SOS)

NOTE!

The safety function SOS is supported by the Safety Modules SAF-002 and SAF-003.

The safety function „Safe Operating Stop (SOS)“ monitors the reached operating stop position of the drive and avoids the leaving of the operating stop position.

The drive’s operating stop is monitored via a parameterized tolerance window (position window).

NOTE!

The ProSafePara parameter ""+/- tolerance for standstill (s_Zero_SOS)" was limited from ProSafePara V1.1.0.0 to a value of 1073676287 to avoid the exceeding of the number range by differential generation and in dependence of the encoder triggering which theoretically is possible (prior limit value: 4294967295).

This new limit applies to the tolerance inputs of "s_Zero_SOS" in all of the "SOS following functions.

The setting of greater values of earlier ProSafePara versions can lead to availability issues (immediate STO status after activation).

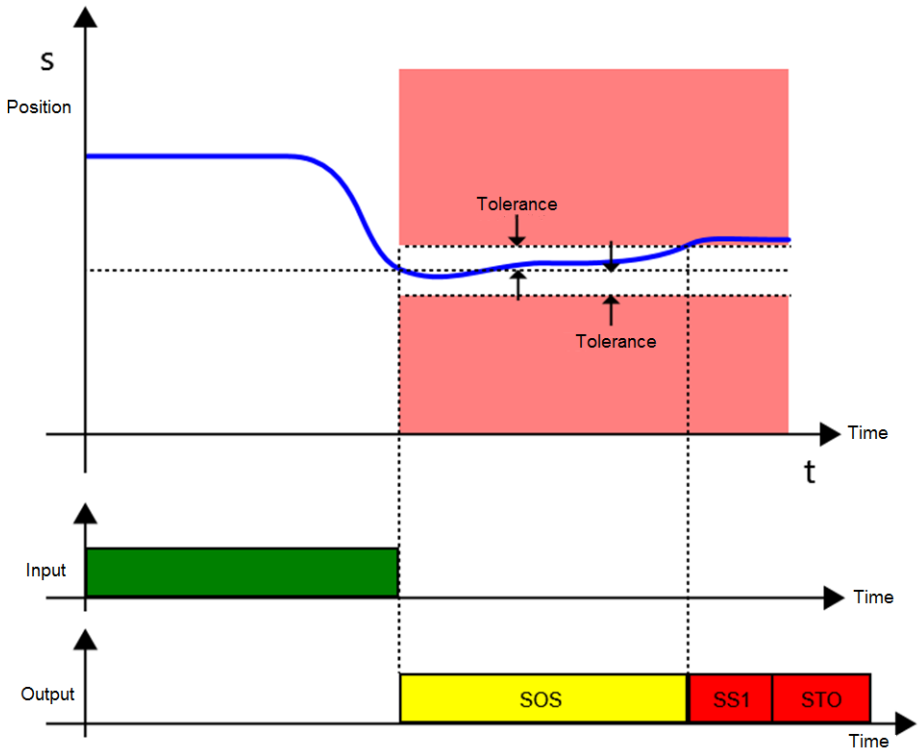


Figure 24: Safety function SOS
During noncompliance with "SOS" after a parameterizable "SS1" time "STO" is initiated

WARNING!

If a drive is operated in the operating mode SOS and if an external torque is existent, which is able to display a danger in case of an error (STO), then the drive must be equipped with a mechanical brake.

Observe chapter ▹Safety notes for the Function STO (Safe Torque Off)◃ on page 58.

10.6.1 Error reaction with function-specific SS1 time for the safety function "SOS"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and the SAF module configuration software ProSafePara a function-specific SS1 time can be parameterized from version V1.1.0.0 onward for every safety function:

Figure 25: P213.005: SS1 time for the safety function „SOS“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

The following individual errors can occur during the function "SOS":

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Exceeding the tolerance window

If a value in P213.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby, the drive error 1066 "SS1 stop forced by SAF module" is initiated.

In the controller an accordant error reaction is parameterized (refer to "Parameterization of the error reaction " and setting of the "SS1 stop time" in ▹chapter 10.4.1◃).

Example:

During the process of the function "SOS" the individual error exceeds the tolerance window. In ▹Figure 24◃ on page 66 this case is shown. Thereby, the "SS1" time accords to the parameterized time set in P213.005 before "STO" is operated.

10.7 Safely Limited Speed (SLS)

NOTE!

The safety function SLS is supported by the Safety Modules SAF-002 and SAF-003.

The safety function "Safely Limited Speed (SLS)" monitors the compliance of a limited drive speed after lapse of parameterizable delay time Δt (Delta t).

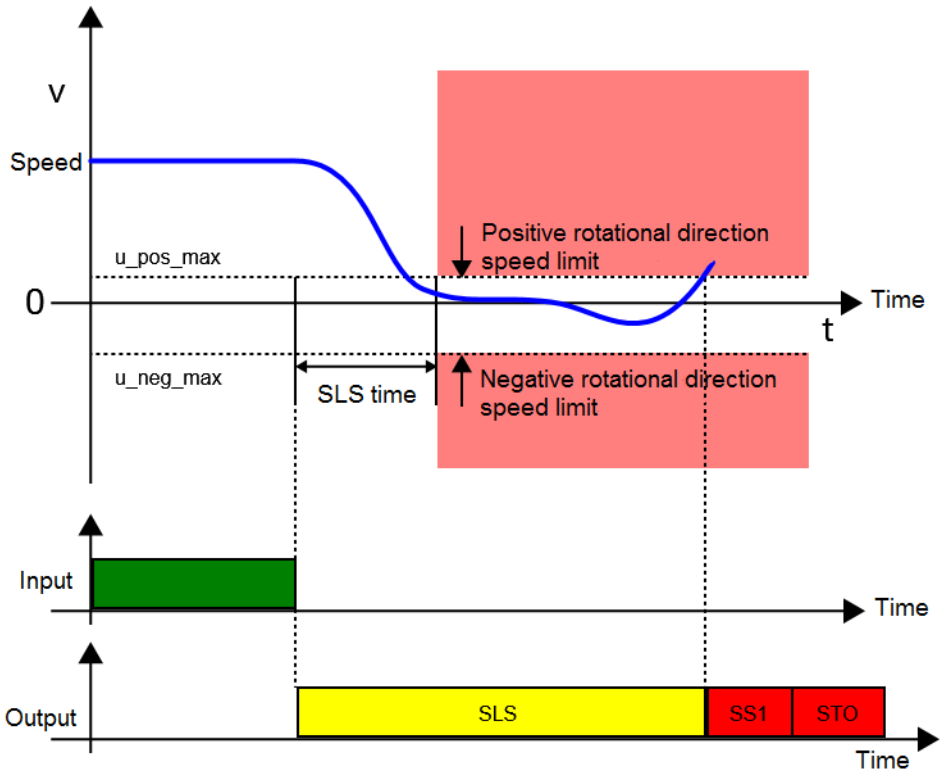


Figure 26: Safety function SLS
During noncompliance of "SLS" after a parameterizable "SS1" time "STO" is initiated

10.7.1 Error reaction with a function-specific SS1 time for the safety function "SLS"

When using the software extension SAF.002/3 (see ▹chapter 7.8◃) and of the SAF module configuration software ProSafePara from version V1.1.0.0 for every safety function a function-specific SS1 time can be parameterized:

Figure 27: P214.005: SS1 time for the safety function „SLS“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

During the "SLS" function the following individual errors can occur:

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Exceeding the speed limits

If a value was parameterized in P214.005 that is greater than zero, then not immediately a STO is carried out if an individual error occurs but the parameterized time at first is processed for this function. An automated signalization to the controller is initiated during the occurrence of the error. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

The accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting of "SS2 stop time" in ▹chapter 10.4.1◃).

Example:

During the process of the function "SLS" the individual error "Exceeding the speed limits" occurs. In ▹Figure 26◃ on page 68 this case is shown. Thereby, the time period "SS1" accords to the time parameterized in P214.005 before "STO" is carried out.

10.8 Safe Direction (SDI)

NOTE!

The safety function SDI is supported by the Safety Modules SAF-002 and SAF-003.

The safety function „Safe Direction (SDI)“ assures drive movement of the principal drive mode in one defined rotational direction only.

If there is no compliance with the rotational direction then the function STO (Safe Torque Off) is triggered.

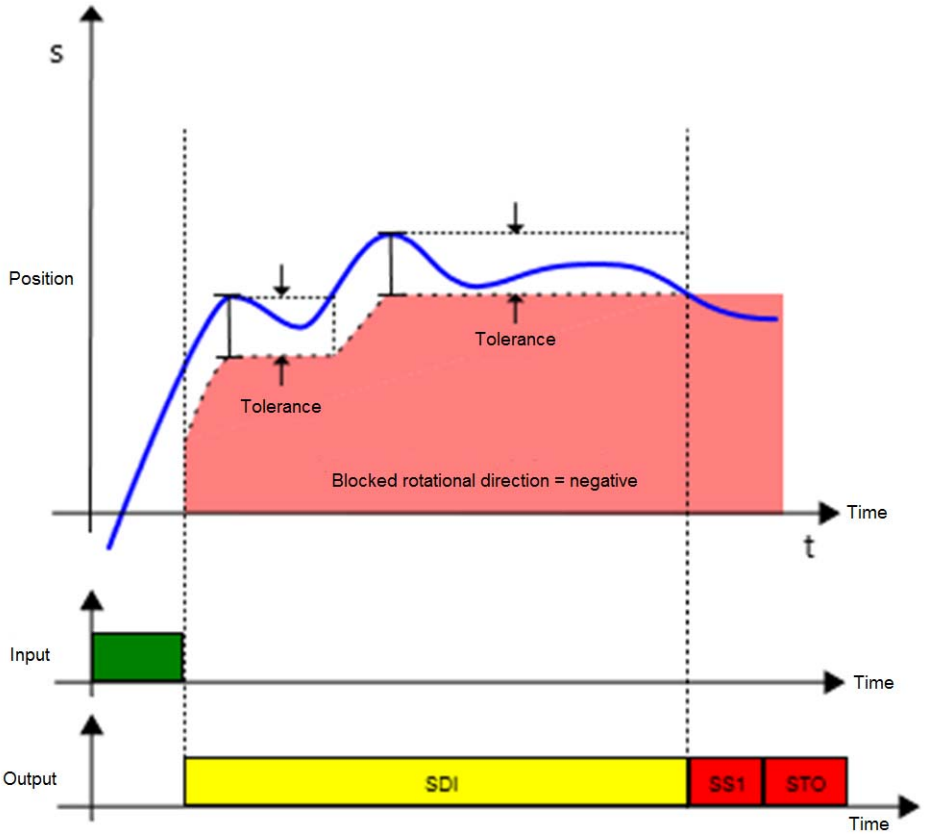


Figure 28: Safety function SDI
During noncompliance of "SDI" after a parameterizable "SS1" time "STO" is initiated

10.8.1 Error reaction with function-specific SS1 time for the safety function "SDI"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

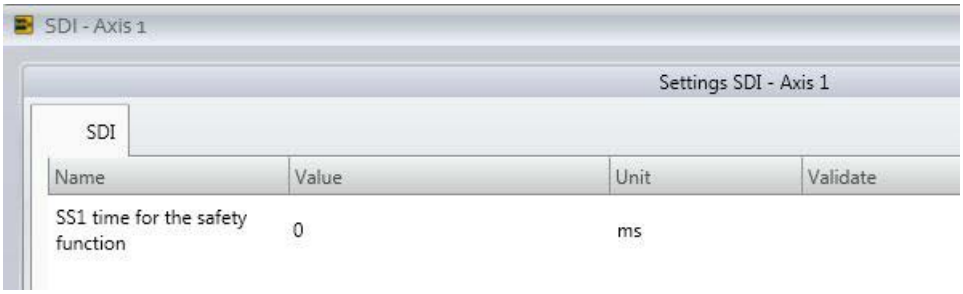


Figure 29: P219.005: SS1 time for the safety function „SDI“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

During the function "SDI" the following individual errors can occur:

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Incorrect rotational direction

If a value in P213.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

An accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting of "SS1 stop time" in ▹chapter 10.4.1◃).

Example:

During the processing of the function "SDI" the individual error "Incorrect rotational direction" occurs. In ▹Figure 28◃ on page 70 this is shown. Thereby, the period of time "SS1" accords to the time parameterized in P219.005 before "STO" is carried out.

10.9 Safe Brake Control (SBC)

NOTE!

The safety function SBC is supported by the Safety Modules SAF-002 and SAF-003.

The safety function "Safe Brake Control (SBC)" forces the application of the brake. This is executed by switching off the brake supply to the drive axis safely via the internal power output in the Safety Module.

At an input, which has closed input contacts and which was configured for the safety function SBC, the brake's application can be requested still by the controller's standard part (inputs on +24V = brake opened). This request is not safety-related.

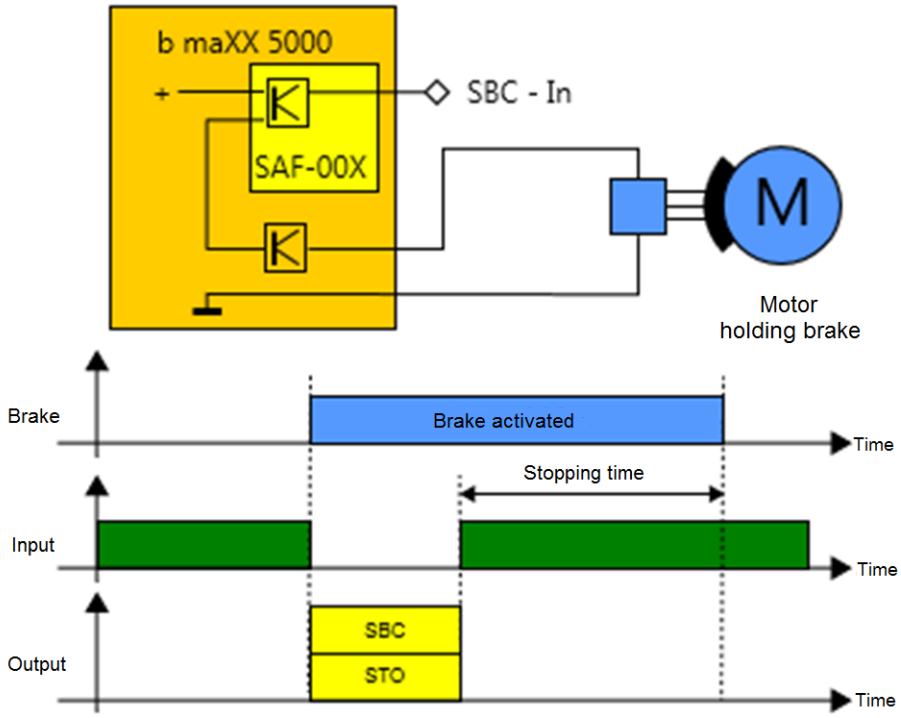


Figure 30: Safety function SDI

NOTE!

The delay time determines how long the motor holding brake remains closed after STO.

NOTE!

The safe brake (SBC) is not available at the BM5500.

NOTE!

The online test to check the brake voltage is carried out, only, if the function SBC is parameterized and STO is not active (the brake is supposed to be supplied).

The SBC function is parameterized if the inputs are linked to this.

When the brake is released by the SAF module can be checked by the user at the output status:

- In the drive by the controller parameter P201.003 (DWORD) "Status outputs (physical I/O)": Bit 4 brake axis 1 status and bit 12 axis 2 brake (refer to the following figure).
- By FSoE: Bit 7 in the FSoE status word 2 (refer to ▹chapter 12.7◃ "Coding of S_StatusWord" for axis 1 and axis 2)

In both cases a bit value shows "0" that a motor holding brake which is connected to the drive is -- independently of the status of the drive -- free of voltage and therefore activated by the SAF module.

If the bit shows the value "1" the release of the brake is dependent of the drive manager in the controller and the operating status of the drive.

The status of the physical outputs of the SAF module can be checked by the user by an installed SAF module diagnosis (=controller P201.003):

Figure 31: SAF module brake axis 1 released (green), brake axis 2 inhibited (gray)

WARNING!

According to the closed current principle, only brakes, which, are in a currentless state, may be applied. Energy always must be added, in order to open the brake.

NOTE!

Brakes, which do not apply due to an used test pulse, may be used only (see Appendix ▹C.2.4 Technical data power outputs on page 164).

10.9.1 Error reaction with a function-specific SS1 time for the safety function "SBC"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

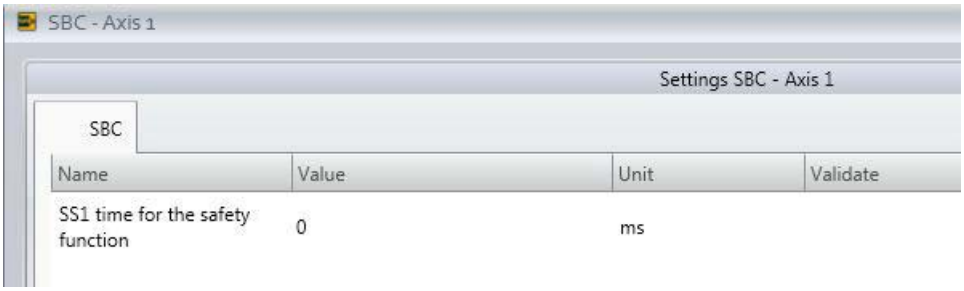


Figure 32: P220.005: SS1 time for the safety function „SBC“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

The following individual error can occur at the function "SBC":

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Homing was not carried out
- Exceeding the tolerance window

If a value in P220.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

The related error reaction must be parameterized in the controller (refer to "Parameterization of the error reaction" and SS1 Stop Time" in ▹chapter 10.4.1◃).

10.10 Safely Limited Position (SLP)

NOTE!

The safety function SLP is supported by the Safety Module SAF-003.

The safety function „Safely Limited Position (SLP)“ assures, that the parameterized absolute position limits are not exceeded by the principal drive mode. After activating the function the compliance with the parameterized position limits are monitored.

The drive’s maximum limited moving range is defined with the parameters „Position limit 1“ and „Position limit 2“.

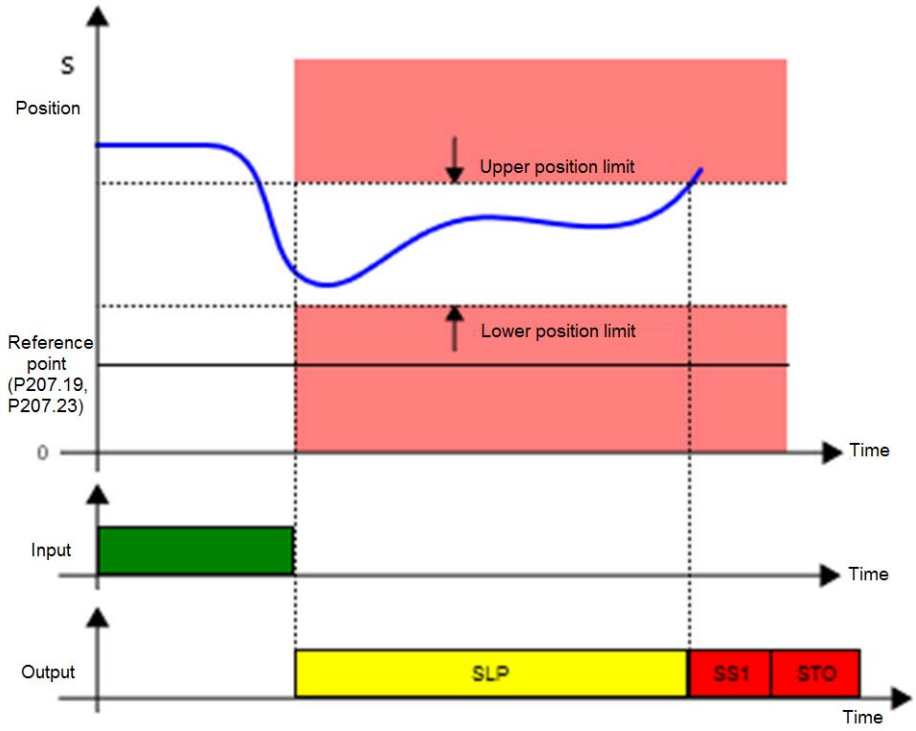


Figure 33: Safety function SLP
During noncompliance with "SLP" after a parameterizable "SS1" time "STO" is initiated

The Safety Module must know the safe absolute position in order to execute the safety function SLP. Upon first request of the safety function homing must be executed. The Safety Module requests an execution of homing at the controller via the communication interface (SPI) .

The reaching of the homing position via a control cable is signaled from the Safety Module to the controller.

The sensing of the homing position is made e.g. via a position switch, which occupies a safe Safety Module input on two channels. Additionally, an enabling interface input to the controller can be parameterized and processed.

The absolute value of the homing position, which is stored in the parameterization, is accepted as an absolute position during the sensing of the position switch by the input of the Safety Module. The position limits are monitored with the encoder increments on two channels. It must be considered, that a maximum speed and, if necessary, the encoder's rotational direction must be defined for the sensing of the absolute position.

During homing the specified absolute positioning value in P207.019 for axis 1 (or P207.022 for axis 2) is taken over as homing position. This is the positioning value 0, as long as nothing else was defined by the user.

The benefit is that the user can approach the home position anywhere on the route and can take over the default value.

Furthermore, the user can carry out a fine adjustment of the accessed home position because it can happen that the zero point is moved by a few increments (due to the different installations of the home switch regarding the mechanics). By the setting of a low offset this deviation can be compensated directly.

NOTICE!

- The principal drive mode must be within the parameterized limits at request of the safety function SLP.
- System parameters as e.g. the mechanic hysteresis of the position switch or the mechanic traction at sensing of all safe positions must be considered.

CAUTION!

The specification of the position limits at SLP takes place absolutely. This is in contrast to the safety function SOS with its relative parameter limits to the present standstill position.

Therefore the safe reference position after a switch-off of the drive must be determined again!

10.10.1 Error reaction with function-specific SS1 time for the safety function "SLP"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version v1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

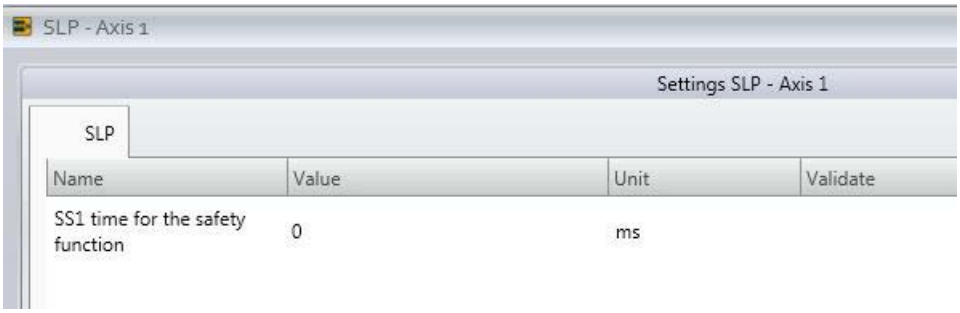


Figure 34: P215.005: SS1 time for the safety function „SLP“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

The following individual error can occur at the function "SLP":

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Homing was not carried out
- Exceeding the tolerance window

If a value in P215.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby, the drive error 1066 "SS1 stop forced by SAF module" is initiated.

The related error reaction must be parameterized in the controller (refer to "Parameterization of the error reaction" and SS1 Stop Time" in ▹chapter 10.4.1◃).

Example:

During the process of the function "SLP" the individual error "Exceeding the position range" occurs. In ▹Figure 33◃ on page 75 this case is shown. Thereby, the time period "SS1" accords to the time parameterized in P215.005 before "STO" is carried out.

10.11 Safely Limited Increment (SLI)

NOTE!

The safety function SLI is supported by the Safety Module SAF-003.

The safety function „Safely Limited Increment (SLI)“ avoids that the principal drive mode exceeds the defined limit of an incremental position mode.

The activation of an input of the Safety Module, which was configured with SLI causes the stop of the drive and going into the function SOS.

By pressing a button, which is placed at an input of the Safety Module, triggers a safely limited increment. This triggering via the button is made edge-controlled. That means, that the button must be pressed once per limited increment.

The operation of the button during execution of a limited increment is not accepted by the Safety Module.

The drive must have been on SOS for a defined time, before a request for a safely limited increment can be made.

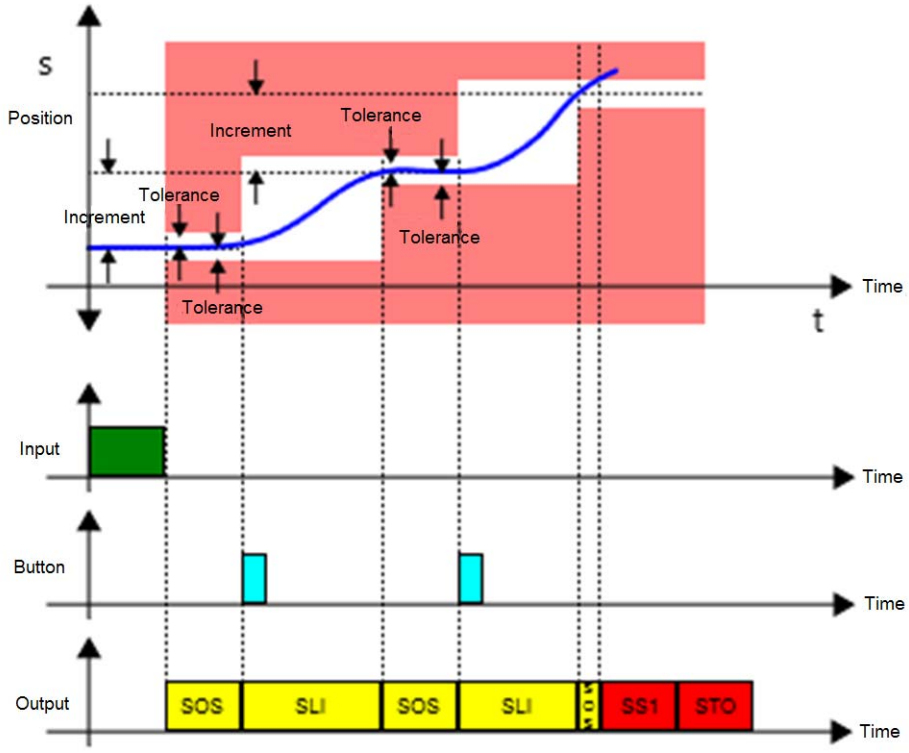


Figure 35: Safety function SLI
During noncompliance with "SOS" after a parameterizable "SS1" time "STO" is initiated.

10.11.1 Error reaction with function specific SS1 time for the Safety function "SLI" and the following function "SOS"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

Figure 36: P216.005: SS1 time for the safety function „SLI“

This setting option applies to the following function SOS (an individual error can occur during the following function SOS).

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

The following individual error can occur at the function "SLI" and the "following function SOS":

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Exceeding the tolerance window

If a value in P216.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby, the drive error 1066 "SS1 stop forced by SAF module" is initiated.

The related error reaction must be parameterized in the controller (refer to "Parameterization of the error reaction" and SS1 Stop Time" in ▹chapter 10.4.1◃).

Example:

During the process of the function "SOS" the individual error "Exceeding the position range" occurs. In ▹Figure 35◃ on page 78 this case is shown. Thereby, the time period "SS1" accords to the time parameterized in P216.005 before "STO" is carried out.

10.11.2 Operating principle of SLI and description of the transition SLI ->STO

After the safety function SLI was activated the current position is saved as SOS home position in the safety module. After expiration of the SOS hold time an incremental jog can be released by a switch. The drive can freely move within the released incremental jog. If the switch is operated again during the activated incremental jog then the safety module

ignores this. If the drive reaches the top incremental jog position it changes into the SOS status (the dashed line in the figure on top). After the expiration of the parameterized SOS hold time the next incremental jog can be activated by the switch again.

The safe input of the switch, the minimum SOS hold time, the incremental jog as well as the permitted maximum tolerance deviation for the SOS standstill in both directions can be parameterized in ProSafePara:

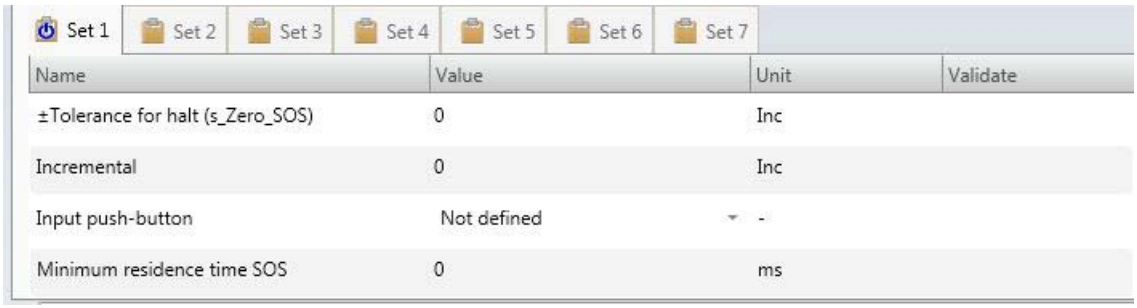


Figure 37: Example parameterization of the safety function "SLI" with switch input at "DIG3_IN_1"

It must be considered that the switch is debounced during the release of the next incremental jog. This can be reached by the parameterization in ProSafePara of accordant high filter times at the safe input of the switch:

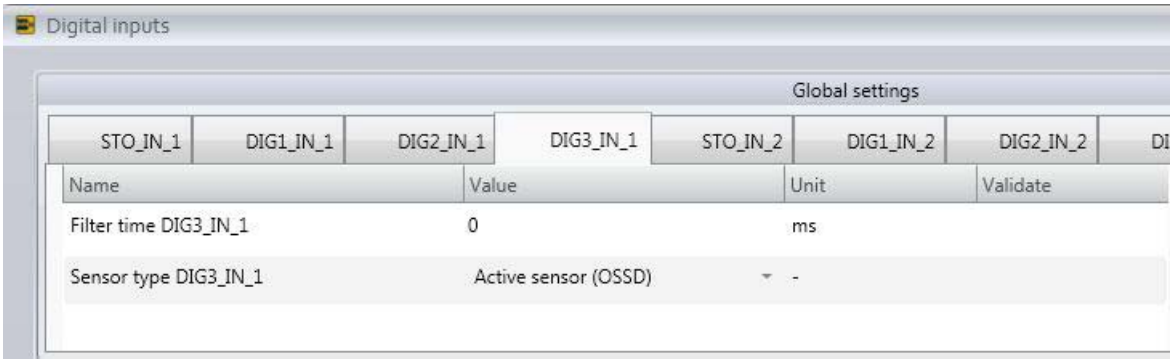


Figure 38: SLI digital inputs

If it shall be avoided that the next incremental jog is released by a short pressing on the switch, then the filter time must be increased accordantly to the demands of the entire machine.

If the input switch is supposed to be released by a safe signal automatic the filter time is not required. However, it must be considered that the signal lasts at least 2 ms so that the increasing signal edge of the module can be detected.

Here, a minimum time of approximately 20 ms is recommended.

For checking purposes the SLI function and the associated SOS following function can be parameterized as outputs. This way the SLI->SOS or SOS->SLI-transitions are monitored or can be visually displayed by lights.

10.12 Safely Limited Acceleration (SLA)

NOTE!

The safety function SLA is supported by the Safety Module SAF-003.

The safety function „Safely Limited Acceleration (SLA)“ monitors the compliance of a limited and parameterized acceleration.

The function STO (Safe Torque Off) is triggered when exceeding the parameterized acceleration.

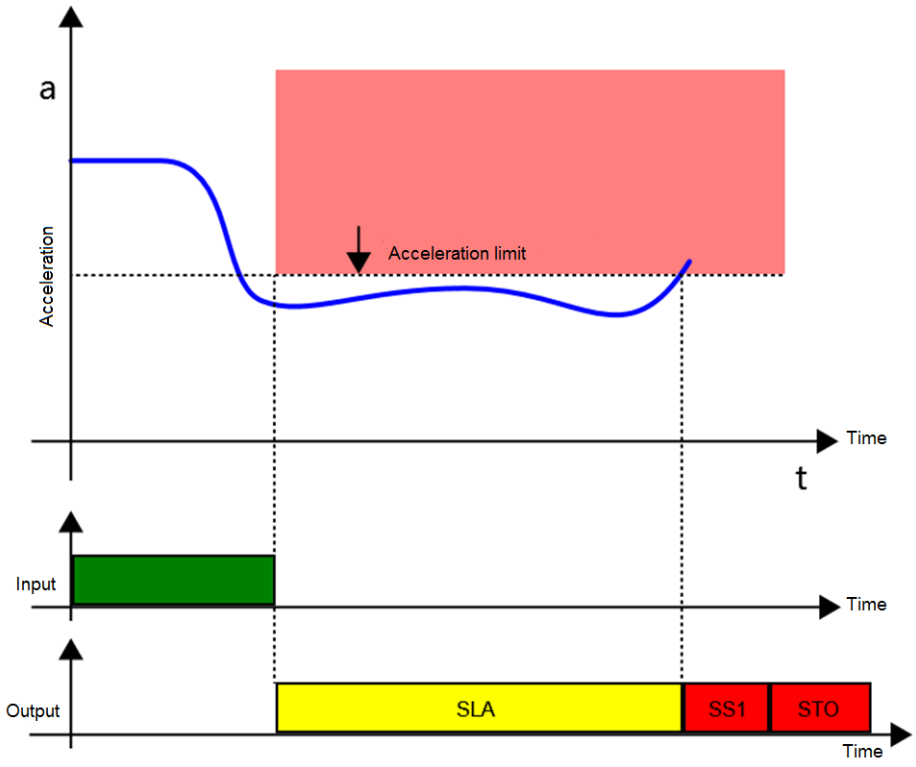


Figure 39: Safety function SLA
During noncompliance with "SLA" after a parameterizable "SS1" time "STO" is initiated.

10.12.1 Error reaction with function-specific SS1 time for the safety function "SLA"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

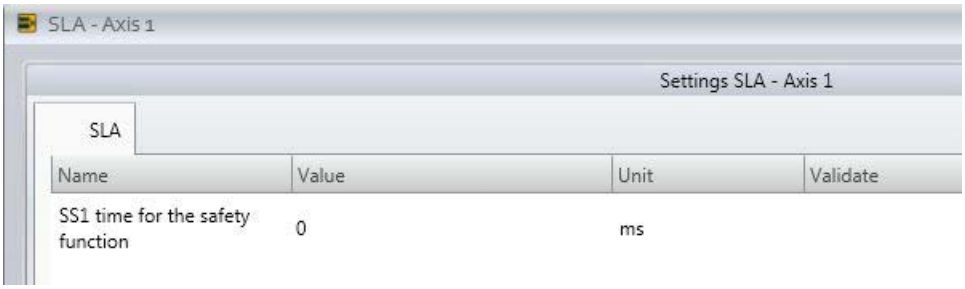


Figure 40: P218.005: SS1 time for the safety function „SLA“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

During the function "SLA the following individual errors can occur:

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Exceeding the acceleration

If a value in P218.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

The accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting "SS1 hold time" in ▹chapter 10.4.1◃).

Example:

During the process of the function "SLA" the individual error "Acceleration exceeded " occurs. In ▹Figure 39◃ on page 81 this case is shown. Thereby, the time period "SS1" accords to the time parameterized in P218.005 before "STO" is carried out.

10.13 Safe Speed Monitor (SSM)

NOTE!

The safety function SSM is supported by the Safety Module SAF-003.

The safety function "Safe Speed Monitor (SSM)" supplies a safety output signal, as long as the speed does not leave a v = 0 symmetric tolerance band.

If the value of the parameterized speed limit is exceeded in positive or negative direction with regard to a parameterizable hysteresis then the safe output signal is switched off:

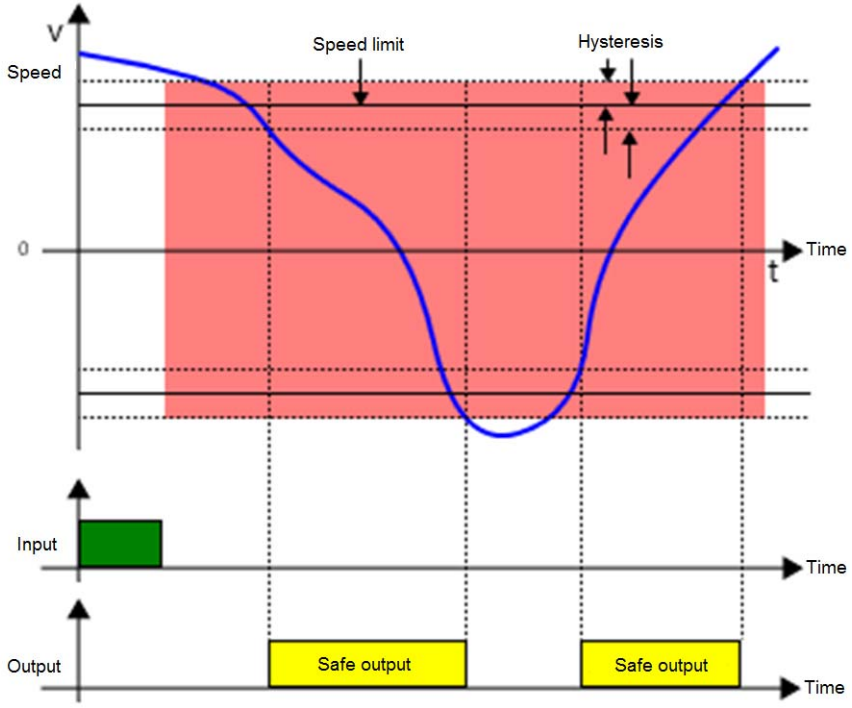


Figure 41: Safety function SSM

NOTE!

The safety function SSM operates the safe output, which is assigned to the safety function. It has no effects on the safe pulse inhibit.

10.13.1 Error reaction with function-specific SS1 time for the safety function "SSM"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

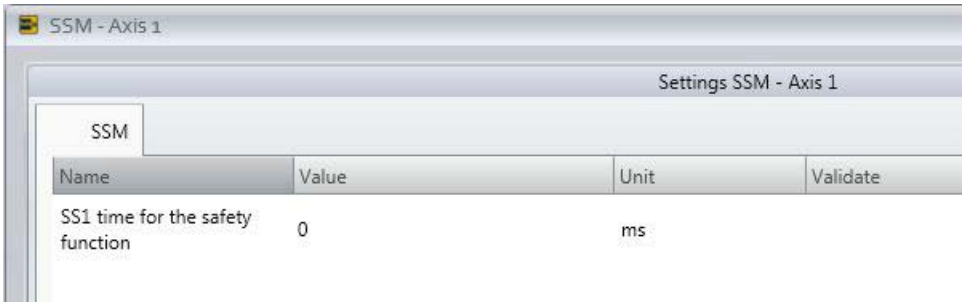


Figure 42: P221.005: SS1 time for the safety function „SSM“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

The following individual errors can occur at the function "SSM":

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended

If a value in P221.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

An accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting "SS1 stop time" in ▹chapter 10.4.1◃).

10.14 Safe Cam (SCA)

NOTE!

The safety function SCA is supported by the Safety Module SAF-003.

The safety function "Safe Cam (SCA)" provides a safe output signal, if the position of the cam is in a defined range around an absolute position (defined by "Position limit 1", "Position limit 2"). Before that homing must be executed.

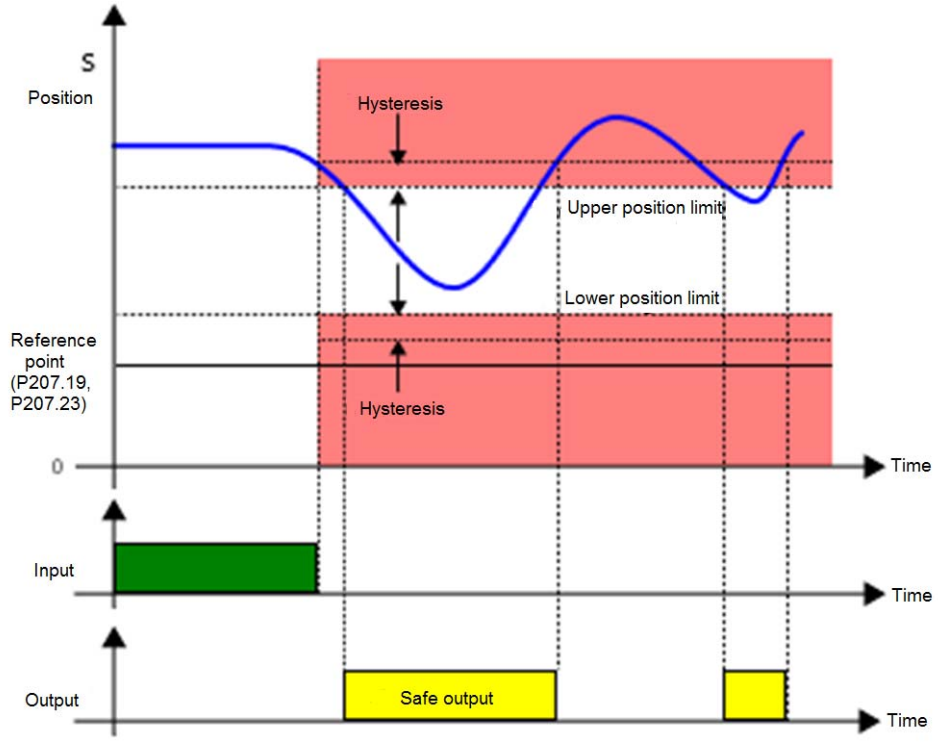


Figure 43: Safety function SCA
With regard to the homing point P 207.019 for axis 1 and P 207.022 for axis 2 refer to explanations in "SLP

NOTE!

The safety function SCA operates the safe output, which is assigned to the safety function. It has no effects on the safe pulse inhibit.

10.14.1 Error reaction with function-specific SS1 time for the safety function "SCA"

With the software extension SAF-002/3 (see ▹chapter 7.8◃) and with the SAF module configuration software ProSafePara from version V1.1.0.0 onwards for every safety function a function-specific SS1 time can be parameterized:

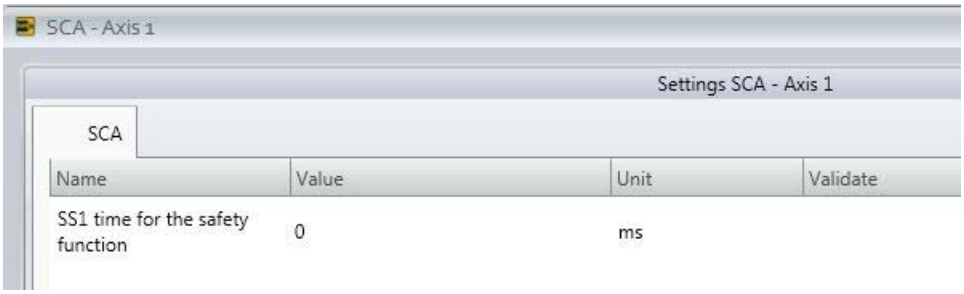


Figure 44: P222.005: SS1 time for the safety function „SCA“

This time always acts as a delay if an individual error occurs.

This is supposed to allow the drive to drive down a brake ramp before the STO is activated.

With the function "SCA" the following individual errors can occur:

- Switchover to a data set which was not set
- There is no encoder connected
- Encoder standstill time extended
- Homing was not carried out

If a value in P222.005 is parameterized greater than zero, STO is not immediately carried out if an individual error occurs, but at first the parameterized time of this function is processed. An automatic signalization to the controller is connected if the error occurs. Thereby the drive error 1066 "SS1 stop forced by SAF module" is initiated.

An accordant error reaction can be parameterized in the controller (refer to "Parameterization of the error reaction" and setting "SS1 stop time" in ▹chapter 10.4.1◃).

CAUTION!

After switching off the drive, the safe homing position because of the absolute position limits must be determined again, because of the absolute position limits!

10.15 Tolerance for the limit values of the safety functions

Due to the used encoder type and of the adapted measuring method thereon in the SAF module for the calculation of the position and the consequential derived quantities, such as speed, must be considered with regard to the system tolerances.

The most important characteristics of the encoder type SINCOS are the pulses per revolution. The higher the PPR count the more precise is the evaluation of positioning and speed.

The measuring of the position of the SINCOS is made in the SAF module by a four-quadrant counter. Thereby the following tolerances apply:

- Based on positioning:
  ± Standardized number of increments per revolution (65536) / 4 / Encoder PPR count
- Based on speed:
  ± Standardized number of increments per revolution (65536) per ms / 8 / Encoder PPR count

An example of a position-based function SOS:

The user sets a "Standstill tolerance"-limit value of 1000 increments for SOS in ProSafePara. The used SINCOS encoder to the axis has a PPR count of 1024.

For the above mentioned formula a deviation of 16 increments to the bottom and to the top of the limit value (65536/4/1024 = 16) must be taken into account.

With the setting of 1000 increments a switch-off can be made by a noncompliance of a limit at 984 increments or alternatively after 1016 increments.

Example of a speed-based function SLS:

The user sets "maximum speed positive rotational direction" for SLS of a limit value of 1000 Inc/ms. The used SINCOS encoder at the axis has a PPR count of 1024.

For the above mentioned formula a deviation of 8 Inc/ms to the bottom and to the top of the limit value (65536 Inc/ ms/8/1024 = 8) must be taken into account.

With the setting of 1000 Inc/ms a switch-off can be made by a noncompliance of a limit at 992 Inc/ms or alternatively after 1008 Inc/ms.

At the resolver encoder type the position in the unit circle from the demodulated sine and cosine signals as well as the speed (derived from this) are calculated by an arctan calculation the position in the unit circle. The following tolerances result from this:

Positioning-based:

± 6 ‰ of the standardized number of increment per revolution (65536) = ± 393 increments.

Speed-based:

± 3 ‰ of the standardized number of increments per revolution (65536) per ms = ± 197 Inc/ms

Example: SOS limit value 1000 Inc, limit value noncompliance between 607 Inc and 1393 Inc

Example: SLS limit value 1000 Inc/ms, limit value noncompliance between 803 Inc/ms and 1197 Inc/ms

NOTE!

Due to the arctan calculation at the resolver the deviations during the calculation of the standardized increments are very great compared to the SINCOS encoder. This is why, SINCOS encoders including a preferably large encoder PPR count, are recommended.

11

INTERFACES

This chapter describes the interfaces of the Safety Modules and the technical data of the inputs and the outputs.

11.1 Connector Assignment Interface X1

The Safety Module SAF-002 and SAF-003 is available in two different hardware versions (see ▷Identification of the Safety Module - Type Key◁ from page 47):

- Standard configuration "Daisy Chain"
  The standard configuration shows a common reference potential for all inputs, which is determined by the terminals GND group1 and GND group 2. The signal names of the terminals, the meaning and the physical assignment in its standard configuration are listed in the tables in ▷Chapter 11.1.1◁
- Optional configuration "Separate Grounds" (e.g. for operation with SO4000)
  For each input on two channels an own ground terminal is implemented in an optional configuration. This configuration is necessary in connection with the output terminals, which must be connected isolated. At this configuration the daisy-chain is not implemented and is therefore not available.
  The signal names of the terminals, the meaning and the physical assignment in the optional configuration are listed in the tables in ▷Chapter 11.1.2◁

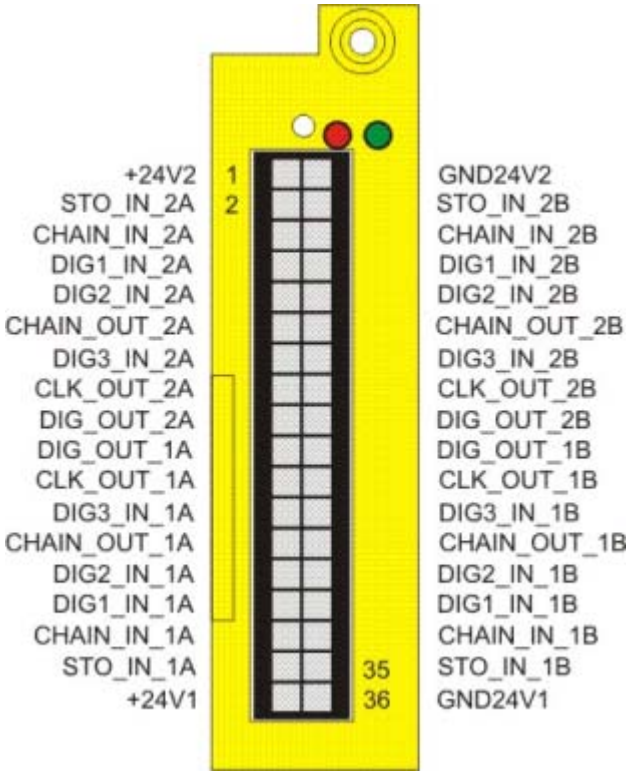


Figure 45: Representation SAF-module-pin assignment (option Daisy Chain)

11.1.1 Standard Terminal Configuration BM5-O-SAF-002-000-000

Standard configuration: signal names and meaning

Terminal no.	Assignment	Signal name
1	+24V2	+24V group2
2	STO_IN_2A	STO input A group2
3	CHAIN_IN_2A	Daisy-Chain input A group2
4	DIG1_IN_2A	input 1 A group2
5	DIG2_IN_2A	input 2 A group2
6	CHAIN_OUT_2A	Daisy-Chain output A group2
7	DIG3_IN_2A	input 3 A group2
8	CLK_OUT_2A	cycle output A group2
9	DIG_OUT_2A	output A group2
10	DIG_OUT_1A	output A group1
11	CLK_OUT_1A	cycle output A group1
12	DIG3_IN_1A	input 3 A group1
13	CHAIN_OUT_1A	Daisy-Chain output A group1
14	DIG2_IN_1A	input 2 A group1

Terminal no.	Assignment	Signal name
15	DIG1_IN_1A	input 1 A group1
16	CHAIN_IN_1A	Daisy-Chain input A group1
17	STO_IN_1A	STO-input A group1
18	+24V1	+24V group1
19	GND24V2	GND group2
20	STO_IN_2B	STO input B group2
21	CHAIN_IN_2B	Daisy-Chain input B group2
22	DIG1_IN_2B	input 1 B group2
23	DIG2_IN_2B	input 2 B group2
24	CHAIN_OUT_2B	Daisy-Chain output B group2
25	DIG3_IN_2B	input 3 B group2
26	CLK_OUT_2B	cycle output B group2
27	DIG_OUT_2B	output B group2
28	DIG_OUT_1B	output B group1
29	CLK_OUT_1B	cycle output B group1
30	DIG3_IN_1B	input 3 B group1
31	CHAIN_OUT_1B	Daisy-Chain output B group1
32	DIG2_IN_1B	input 2 B group1
33	DIG1_IN_1B	input 1 B group1
34	CHAIN_IN_1B	Daisy-Chain input B group1
35	STO_IN_1B	STO input B group1
36	GND24V1	GND group1

Standard configuration: physical assignment of the terminals

See pin assignment of Safety Module ▹C.4.1 Standard configuration „Daisy Chain“◃ on page 167.

11.1.2 Optional Terminal Configuration BM5-O-SAF-002-001-000

Optional configuration: signal names and meaning

Terminal no.	Assignment	Signal name
1	+24V2	+24V group2
2	STO_IN_2A	STO input A group2
3	GND_STO_IN_2	ground STO input group2
4	DIG1_IN_2A	input 1 A group2
5	DIG2_IN_2A	input 2 A group2

Terminal no.	Assignment	Signal name
6	GND_DIG2_IN_2	ground input 2 group2
7	DIG3_IN_2A	input 3 A group2
8	CLK_OUT_2A	cycle output A group2
9	DIG_OUT_2A	output A group2
10	DIG_OUT_1A	output A group1
11	CLK_OUT_1A	cycle output A group1
12	DIG3_IN_1A	input 3 A group1
13	GND_DIG2_IN_1	Ground input 2 group1
14	DIG2_IN_1A	input 2 A group1
15	DIG1_IN_1A	input 1 A group1
16	GND_STO_IN_1	Ground STO-input group1
17	STO_IN_1A	STO-input A group1
18	+24V1	+24V group1
19	GND24V2	GND group2
20	STO_IN_2B	STO-input B group2
21	GND_DIG1_IN_2	Ground input 1 group2
22	DIG1_IN_2B	input 1 B group2
23	DIG2_IN_2B	input 2 B group2
24	GND_DIG3_IN_2	Ground input 3 group2
25	DIG3_IN_2B	input 3 B group2
26	CLK_OUT_2B	cycle output B group2
27	DIG_OUT_2B	output B group2
28	DIG_OUT_1B	output B group1
29	CLK_OUT_1B	cycle output B group1
30	DIG3_IN_1B	input 3 B group1
31	GND_DIG3_IN_1	Ground input 3 group1
32	DIG2_IN_1B	input 2 B group1
33	DIG1_IN_1B	input 1 B group1
34	GND_DIG1_IN_1	Ground input 1 group1
35	STO_IN_1B	STO-input B group1
36	GND24V1	GND group1

Optional configuration: physical terminal assignment

See pin assignment of Safety Module ▹C.4.2 Optional configuration „Separate Grounds“ for operation with SO4000◃ on page 168.

11.2 Survey of Interfaces

The connection of all inputs and outputs is made via the external connector on the Safety Module. This is a S2L_36-connector (36 poles).

The following figure shows the internal and the external interfaces of the Safety Module SAF-002 and SAF-003. The internal interfaces are connected to the controller's electronic.

They provide a safe access on the drive in case of request and the decoupling of a safety-relevant signal of the controller in case of a demand mode and the decoupling of safety-relevant controller signals, as e.g. encoder signals.

A description of external interfaces are in chapter ▹External Interfaces◃ from page 93.

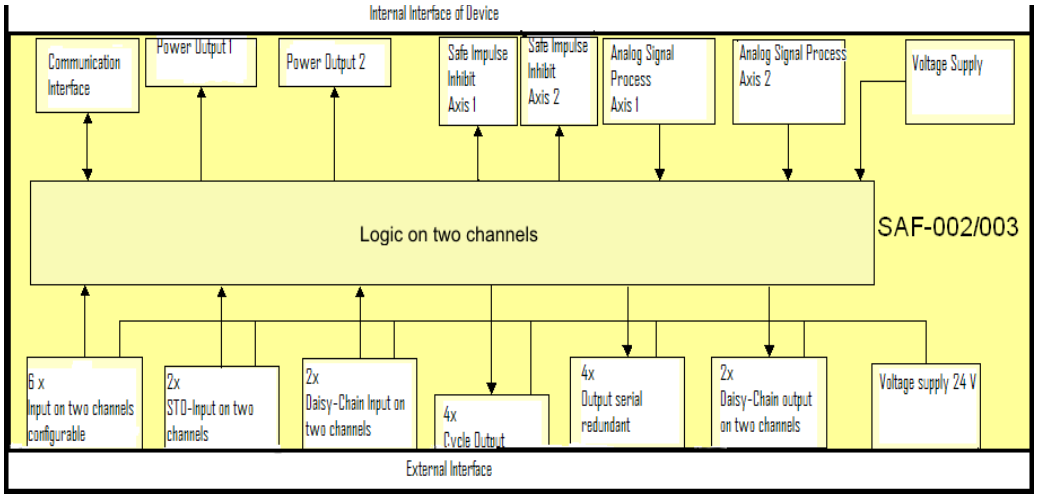


Figure 46: Interfaces SAF-002/-003

The different signal connection are described in the following.

11.3 External Interfaces

NOTE!

The physical inputs at the SAF module work on the closed current principle. That means that a missing voltage at a safe input is always connected to the safety function linked with this input.

A missing voltage at the safe input therefore is indicated as a "Low active input", as the safety function is activated by this.

For instance, if the connecting cable attached to the SAF module was intentionally or unintentionally removed or was torn off because a forklift truck drove over the cable, the safety connected to the SAF module must be activated.

11.3.1 Safe Inputs

The Safety Module has 6 parameterizable inputs on two channels, which can be assigned with the safety functions, which are described in chapter ▹Safety Functions◃ from page 55. The safe inputs of both axis can be used for this axis, if only one axis is operated.

The parameterization of the safe inputs is made with the parameterization tool ProSafePara.

Features

- LOW-active
- Logic isolation.
- For the operation of sensors with OSSD-outputs according to EN 61496.
  OSSD-outputs possess test pulses. This way the inputs of the Safety Modules can be parameterized in such a way, that they are not enabled by these pulses.

Crossfault detection / Short-circuit detection

- For the detection of external input-sided short-circuits between two inputs and for the detection of short-circuits of the inputs against electrical power supplies, external clock signals are supplied with current via the cycle outputs of the Safety Module when using electro-mechanical safety switches (e.g. emergency stop) (see chapter ▹Cycle Outputs◃ from page 97).
- Detection of internal errors of the parts and of internal crossfaults due to diagnostics functions.

NOTE!

The inputs comply with the specification type 3 according to EN 61131-2.

Technical Data see ▹C.2 Technical Data safe inputs, STO-Inputs and Daisy-Chain-Inputs◃ from page 163 onward.

11.3.2 STO-Inputs

The Safety Module has 2 STO-inputs on two channels for the activation of the safe pulse inhibit.

When activating the safe pulse inhibit the generation of a rotating field for the motor control is interrupted. With this the drive is put into the status STO (Safe Torque Off). The energy supply to the motor is not affected by this switch-off operation.

Features

- LOW-active
- Logic isolation

NOTE!

The inputs comply with the specification type 3 according to EN 61131-2.

Technical Data see ▹C.2 Technical Data safe inputs, STO-Inputs and Daisy-Chain-Inputs◃ from page 163 onward.

11.3.3 Daisy-Chain Cascading

The Safety Module has 2 Daisy-chain cables on two channels.

The Daisy-chain-inputs and -outputs on two channels enable the module-independent linking of safety functions. This is, e.g. necessary, if several or all drive axes of an application must have the status STO (Safe Torque Off) or if a safe reduced speed is necessary for all axes.

The fast STO-reaction saves time in contrast to a field bus solution.

Daisy-chain-inputs and -outputs can be parameterized with parameter tools. For example, the safety function, which shall be enabled on the corresponding Safety Module, in order to activate the Daisy-chain-input, can be set.

An open chain as well as a closed ring structure existing of several drive axes, can be made with the Daisy-chain-inputs and -outputs. The Daisy-chain consists of two control cables, which are wired as shown in ▹Figure 47◃ on page 95.

Daisy-Chain Example - Open Chain

An open chain is shown in the following figure. The safe inputs of the module axis 1 are configured in such a way, that they enable . the safety functions STO (Safe Torque Off) and SS1 (Safe Stop 19). Both safety functions are transmitted to the module axis 2, if an accordant parameterization of Daisy-chain-output of module axis 1 was made. The Daisy-chain-input of module axis 2 is configured, so that the function SS1 is operating. The configuration of the Daisy-chain-output of module axis 2 makes sure that the safety function SS1 is transmitted to axis 3. The Daisy-chain input of module axis 3 activates the function SS2 (Safe Stop 2).

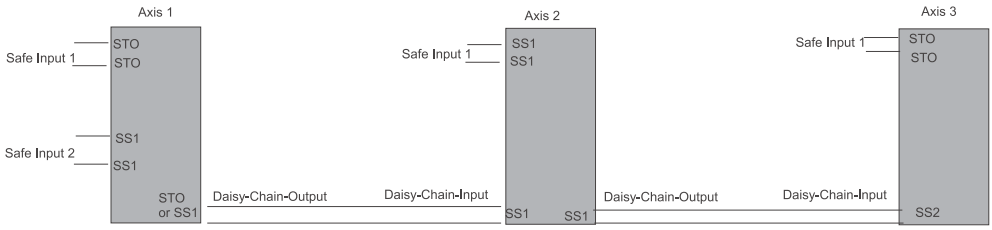


Figure 47: Daisy-chain cascading - Example of an open chain

11.3.3.1 Daisy-Chain-Inputs

The Safety Module has two safe Daisy-chain-inputs on two channels.

Each Daisy-chain-input on two channels can be assigned to a safety function or the Daisy-chain-input of the Safety Modules can be activated/deactivated with the

parameterization tools. In order to implement an open chain (without feedback) consisting of several Safety Modules (as shown in ▹Figure 47◃ on page 95), the Daisy-chain-input of the first module must be deactivated (referred to as master).

Features

- The inputs are isolated, in order to avoid potential shifts.

NOTE!

The inputs comply with the specification type 3 according to EN 61131-2.

Technical Data see ▹C.2 Technical Data safe inputs, STO-Inputs and Daisy-Chain-Inputs◃ on page 163.

11.3.3.2 Daisy-Chain-Outputs

The Safety Module has two safe Daisy-chain-outputs on two channels. The Daisy-chain-output provides that the activated safety functions on the Safety Module are safely transmitted to the following modules.

The configuration of the Daisy-chain-output is made with the parameterization tools ProSafePara. It specifies on which active safety function on the Safety Module the Daisy-chain-output is activated (output is on 0 V-potential). With an OR- function these different safety functions can be assigned to, at the same time.

Technical Data see ▹C.2.1 Technical data Daisy-Chain-Outputs◃ on page 164.

11.3.4 Safe Outputs

The Safety Module has 4 safe, parameterizable OSSD-outputs, which can randomly be assigned to both axes.

All safe outputs of both groups for this axis can be used, if one axis is operated only.

The safe outputs can be assigned to the safe drive function with the parameterization tools. That way, for example, a safe guard lock can be implemented through a safe output, which is triggered only if the machine has come to a standstill.

NOTE!

The polarity of the switching behavior of the safe outputs is parameterizable. If output „High-Active“, referring to the closed-circuit principle, is used (= setting in ProSafePara "Not inverted"), it must be considered a monitoring function, only. If the output is „Low-Active“ (= default setting in ProSafePara „inverted“), the safety chain, according to the closed-circuit principle can be generated.

Application case for such a safety chain is a STO-function, which is connected in series via several drives. They are controlled centrally via the control of the first drive in the chain.

Other application cases depend on the accordant application.

The closed-circuit principle implies that the safety function is always activated / enabled, if the voltage at the assigned safe input is "Low".This can occur, if a connected cable at the safe input is pulled off.

Crossfault detection / Short-circuit detection

A crossfault detection to other outputs or to the operating supply voltage potentials for the cables is assured by diagnostic functions and the construction of the hardware.

So that the crossfault detection does not generate wrong error messages, the capacitive load of the safe input, which is connected to the output may be 15 nF, at maximum.

Technical Data see ▹C.2.2 Technical data safe outputs◃ on page 164.

11.3.5 Cycle Outputs

The Safety Module has 4 cycle outputs, makes sure that there is a crossfault detection in the external wiring of the safety devices.

Features

- Current-limited and short-circuit proof
- At use of electro-mechanical switches or sensors, the clock signals provide detection of short-circuits of the connection cables and of the periphery devices to other cables or of any other potentials in the system

WARNING!

Cycle output A group 1 and cycle output A group 2 have an identical phase position. A trouble shooting takes place only between the cycle outputs A and B. Between these signals there is a phase shift of 90°.

Technical Data see ▹C.2.3 Technical data cycle outputs◃ on page 164.

11.4 Power Outputs

The Safety Module has 2 safe OSSD power outputs, which are suitable for the supply of brakes.

These outputs enable a safe interrupt of the supply voltage and therewith the safe switching off of the brakes.

The assignment of the brake outputs is fixed. They cannot be configured. At STO the brakes are controlled in principle. In the programming tool ProSafePara a switch-on delay and a switch-off delay can be configured for the brakes.

The brakes are connected at the basic unit (see Instruction handbook of the basic unit 5.09021). Both connecting cables of the brake must be routed through a ferrite ring. This ferrite ring is available as accessory (article no. 00453308).

NOTE!

The cables for brake control at the controller must be installed safely (see NOTES in ▹General safety regulations on page 119 and ▹Requirements on the connection cable on page 123

Features

- Protection against transient overvoltages.
- Tested by pulses
- Overcurrent-fixed
- Internal serial redundant

Technical Data see ▹C.2.4 Technical data power outputs◃ on page 164.

12

SAFE FIELD BUS COMMUNICATION VIA FSOE

NOTE!

The ETG-profile for the safe drives is not supported. Instead a I/O-architecture is emulated.

12.1 General

The safety module BM5-O-SAF-002 or BM5-O-SAF-003 was designed for the operation at a double axis of the type b maXX 5000 (designation „DA“ in the type code), however it also can be operated at a single axis of the type b maXX 5000 (designation „EA“ in the type code). The configuration of one axis (axis 1) within a double axis is possible, also. The configuration of the SAF-module is made via the parameterizing tool ProSafePara.

If the operator configures only one axis in ProSafePara (axis 1), axis 2 remains in STO (missing pulse enable and supply voltage to the brake is interrupted).

Generally must be considered, that a b maXX 5000 device of the type double axis contains one EtherCAT-slave only, but each SAF-module can be operated with up to two FSoE-drive slaves. Therefore, the FSoE-master, e. g. safePLC of Baumüller, must be able to generate two FSoE-telegrams, which are separated from one another and can be send to the common EtherCAT-slave of a double axis.

The assignment of the FSoE-telegrams is executed via different FSoE-slave addresses.

Single axis / double axis must be set at the binary switch. This is checked when starting the Safety Module.

If a double axis is present, the FSoE-slave address of the first drive is set over the binary switch „Single-/double axis“ at the safety module. The following is automatically valid for the address of the second axis:

FSoE-address axis 2 = set FSoE-slave address + 1

See ▹Setting of the Safe Module Address◃ from page 112.

The Safety Module BM5-O-SAF-002 and BM5-O-SAF-003 have a FSoE-slave-protocol stack (FSoE = Functional Safety over EtherCAT).

The protocol stack supports the evaluation of two control- and three status words for each axis. The control words serve as selection of safety functions as well as selection of data sets (= selection of parameter sets per safety function). Via the status words the selected safety functions as well as the display of activated safety functions are reported back to the FSoE-master.

- *S_ControlWord0* 16 Bit Data direction FSoE-Master -> FSoE-Slave
- *S_ControlWord1* 16 Bit Data direction FSoE-Master -> FSoE-Slave
- *S_StatusWord0* 16 Bit Data direction FSoE-Slave -> FSoE-Master
- *S_StatusWord1* 16 Bit Data direction FSoE-Slave -> FSoE-Master
- *S_StatusWord2* 16 Bit Data direction FSoE-Slave -> FSoE-Master

Because of the system architecture the meaning of "S_StatusWord2" of axis 1 and axis 2 is different (see description in the following).

The following functions are implemented via the FSoE-protocol.

- Connection of the FSoE-slave axes at the FSoE master when starting FSoE-communication.
- Selection and deselection of parameterized safety function of the SAF-module.
- Request of status "Fail-Safe", which identifies the safety functions, which released the set error reaction.
- Switchover of a data set of a single safety function.
- Reading of inputs of the SAF-module of a higher-level control.
- Reading of SAF-module outputs of a higher-level control.

12.2 FSoE-Master Registration

After switching on the installation, the FSoE-master runs up its connected FSoE-slaves over the following FSoE-state-machine into the FSoE-state "Data":

Statuses of Safety over EtherCAT Master:

Status	Description
	The Safety over EtherCAT connection is reset (outputs are in the safe state)
Session	The Session ID is transmitted (outputs are in the safe state)
Connection	The Connection ID is transmitted (outputs are in the safe state)
Parameter	The parameters are transmitted (outputs are in the safe state)
Data	Processing data or Fail Safe data are transmitted (outputs are active only, if the command *ProcessData* is received)

In the FSoE-state *Parameter* safe application parameters are transmitted from the FSoE-master to a FSoE-slave. These are two safe parameters, which can be configured in the FSoE-master by the user:

1 FSoE-Timeout value for the communication FSoE-Master <-> FSoE-Slave.

2 Data set-version number (major/minor).
This version number is permanently stored in the SAF-module. If, however, a new SAF-firmware must be generated, which is incompatible with the versions used up to now, e.g. because of incompatible changes in ProSafePara, the major part of the version number in the new firmware of the SAF-module is incremented by one.
This assures, that the user must adjust the existing application program on the FSoE-master, if there are real incompatibilities of the SAF-firmware states among each other, only.

Structure of data set version number:

1st byte: Major byte of the version number
2nd byte: Minor byte of the version number

Example of a version of a valid version number:

1.0 (Major = 1; Minor = 0)

The adjustment of the version number between master and slave is an organizational measure, which is made by the user, in order to assure, that there are no incompatiblities between the versions of the configured application parameters, which were made over ProSafePara and the SAF-module. The rule is as follows:

Evaluation Major/Minor byte of the version number:

Major Byte	Minor Byte	Result
Slave == Master	Slave >= Master	OK
Slave == Master	Slave < Master	False
Slave < Master	-	False
Slave > Master	-	False

The SAF-module checks, if the received version number (major/minor) from the FSoE-master in the status *Parameter* is correct for each axis:

- Result==OK
  => The used versions are interoperable. The FSoE-state can change into the normal FSoE-operation mode "Data".
- Result==False
  => The FSoE-state machine aborts the run-up procedure, a "PARA_FAIL"-error message is returned to the FSoE-master.
  In this case, the user must check, if the used versions of ProSafePara, of the SAF-module as well as of the major/minor-version number, which were configured in the FSoE-master, are interoperable.

The version number "Major/Minor" is displayed in ProDrive in the parameter 200.7.0.0 with the name "Version of the data set".

12.3 Control word "S_ControlWord0": Activate and deactivate safety functions

In order to select a safety function over FSoE, a bit in a bit mask can be freely configured over FSoE. After download of the configuration over ProSafePara to the SAF-module, the safety function can be activated by the FSoE-master during operation by the setting of this bit in the bit mask "S_ControlWord0".

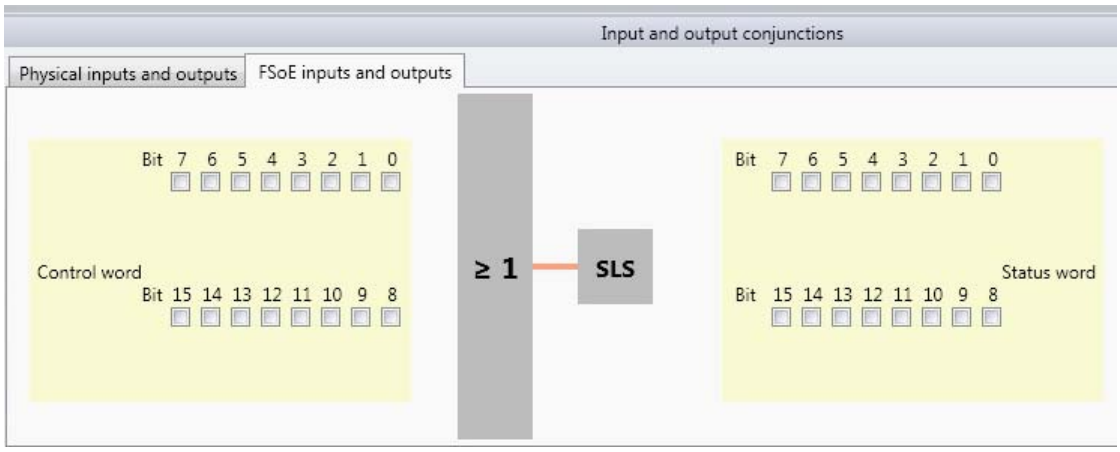


Figure 48: ProSafePara: free configuration of a bit

NOTE!

The user can parameterize every safety function individually in ProSafePara by the mask of the input/output connections if the safe function is activated via a physical input or FSoE input.

Thereby, is to be regarded that at the physical input the safe function with a low-active input value (0 volt) is activated, the activation via FSoE however must be made by a logic "1" (when the parameterized bit is set by the FSoE master).

A mixed operation with physical inputs at the SAF module and the FSoE inputs is accepted, as well:

The safe function is activated if either the connected physical input is activated (= on 0V, which means that the voltage is off) or if the connected FSoE input bit is set (to the SAFETRUE value).

Furthermore, several bits can be configured at the same time. The function is activated if one of the bits is activated.

Up to 16 different safety function can be configured with the available 16 bits in the bit mask. It is also possible to configure several safety function to the same bit in the bit bar. At selection of this bit by the FSoE-master, several safety functions are activated at once. This feature can be, for example used, to activate the safe functions SLI and SDI at one axis at the same time.

Several bits in the bit mask can be configured on a safety function, also. This safety function is activated, as soon as one of the bits, which were configured for this case, is set.

At operation of a SAF-module at a double axis the control word "S_ControlWord0" is available at each axis.

The bit-assignment of the control word is shown in an example for the safety functions STO/SS1/SS2/SOS and SLS in the following table for Axis 1. The assignment of the control word is fixed via the configuration in ProSafePara. An assignment change always must be adjusted in the profile of the FSoE-master.

With the setting of the configured bits in "S_ControlWord0", the FSoE-master can activate the safe function. In the example, "STO" (Bit 1) and "SLS" (Bit 8) are activated at the same time. ("S_ControlWord0" = 0x0102).

Example control word "*S_ControlWord0*" Axis 1: Simultaneous activation of safety functions "STO" and "SLS" (dependent on the parameterized ProSafePara-configuration).

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	**activated**
S_ControlWord0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	
STO Axis 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	**Yes**
SS1 Axis 1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**No**
SS2 Axis 1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**No**
SOS Axis 1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	**No**
SLS Axis 1	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	**Yes**
….																	

WARNING!

The assignment of the control word must be adapted to the configuration of the communication master (e.g. Safety PLC) before commissioning. Deviations will cause failures, which can lead to serious consequences or even to death.

A detailed description in order to configure the control word S_ControlWord0 is described in the manual „Parameterization Tool ProSafePara.

12.4 Control word "S_ControlWord1": Parameter switchover and acknowledge of activated safety function

A general requirement is the switchover of parameterized data sets of a safety function; at the same time another data set of this safety function is active (selected). The switchover of data sets of a safety function can be made over FSoE only.

This functionality is, for example, used at the safe function SLS, in order to switch over a momentarily monitored speed 1 without delay to another monitored speed 2, whereat the safety function is not deactivated. The switchover is immediately effective.

12.4 Control word "S_ControlWord1": Parameter switchover and acknowledge of activated safety function

In ProSafePara up to 7 different parameterized data sets can be configured as at one safety function.

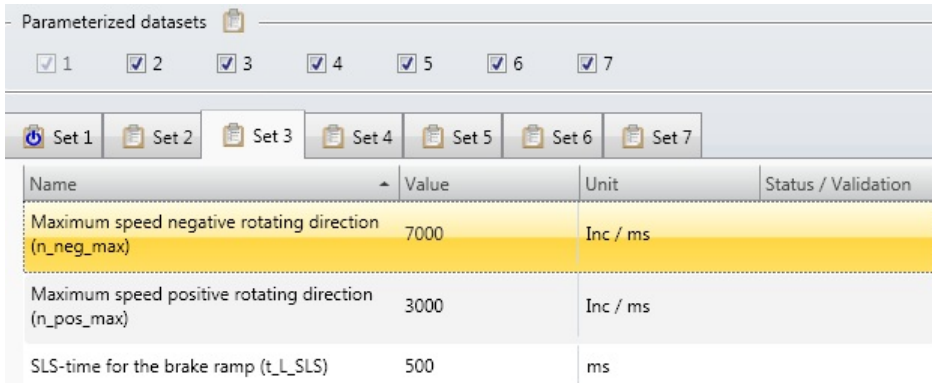


Figure 49: Switching over of parameterized data sets

The switching over of data sets is made specific according to the safety function. This means, that, for example, at the SLS-function the data set 3 is active and at the SDI-function of the data set 1 at the same time.

As long as a data set of a safe function is not switched over, the boot data set is active. The boot-data set accords to the data set with the index 1. This assignment to the index 1 can be re-configured to another index in ProSafePara.

At operation of the SAF-module at a double axis, the control word "S_ControlWord1" is available at each axis.

If a safety function is activated, the axis moves into the safe state. The controller generates an error message 1013 "Switch-off by safety functions".

The activation of a safety function is displayed to the FSoE-master via the status word "S_StatusWord1".

Due to a bit status change from "0" to "1" of bit 8 in the "S_ControlWord1", the FSoE-master can accept the enabled safety function again (see spreadsheet).

DANGER!

After acknowledge of an activated safety function, a starting of the drive can be made immediately!

Specification for S_ControlWord1:

- Bit 0 ... 4 → Selection of safety function, which is to be switched over.
- Bit 5 ... 7 → Index of the new data set (1 ... 7)
- Bit 8 → Acknowledge for activated safety function (change 0 → 1)
- Bit 9 ... 15 → reserved

Specification of *S_ControlWord1*:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit
											0	0	0	0	1	STO
											0	0	0	1	0	SS1
											0	0	0	1	1	SS2
											0	0	1	0	0	SOS
											0	0	1	0	1	SLS
											0	0	1	1	0	SDI
											0	0	1	1	1	SBC
											0	1	0	0	0	SLP
											0	1	0	0	1	SLI
											0	1	0	1	0	SLA
											0	1	0	1	1	SSM
											0	1	1	0	0	SCA
											0	1	1	0	1	SLT
								0	0	1						Data set 1
								0	1	0						Data set 2
								0	1	1						Data set 3
								1	0	0						Data set 4
								1	0	1						Data set 5
								1	1	0						Data set 6
								1	1	1						Data set 7
							0									Acknowledge bit to reset an activated safety function (rising edge $0 \rightarrow 1$)
0	0	0	0	0	0	0										reserved

12.5 Status word "S_StatusWord0": Display of the selected safety function

Over "S_ControlWord0" with the FSoE-master, the selection of the safety function, which was previously configured, is executed. In a FSoE-status bar in ProSafePara, one or several bits can be configured, which display a selected safety function. These are now mapped to the status word "S_StatusWord0" and can be accessed in the FSoE-master, in order to check the selection.

At the operation of the SAF-module at a double axis the status word "S_StatusWord0" is available at each axis.

Example: Display for "Safety function is selected" (bit coding dependent on the parameterized ProSafePara-configuration)

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	**activated**
S_StatusWord0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	
STO															**1**		**Yes**
SLS								**1**									**Yes**

12.6 Status word "S_StatusWord1": Display of activated safety function and of the last active parameter switchover

The status- and error messages are displayed in the S_StatusWord1. Which kind of active safety function was activated, due to an error reaction and was set to status "Fail Safe" (bit 0-4), is mainly related to this.

In order to check the parameter switchover, which was executed via the control word "S_ControlWord1" directly , the safety function, which was changed the last in the SAF-module, is displayed with index (bit 8-15).

At the operation of a SAF-module at a double axis the status word "S_StatusWord1" is available at each axis.

Specification for S_StatusWord1:

- Bit 0 ... 4 → „error reaction“
  Displays, at which safety function an error (such as a switchover to a parameter set, which was not parameterized) or noncompliance has occurred (such as a limit violation).
- Bit 5 ... 7 → „error cause“
  For a detailed description refer to error cause (effective from the module version "Software extension") with regard to the definition refer to ▹chapter 7.9◃
- Bit 8 ... 15 → Display of the last parameter switchover in the SAF-module

Coding of S_StatusWord1

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit
											0	0	0	0	0	No error
											0	0	0	0	1	STO
											0	0	0	1	0	SS1
											0	0	0	1	1	SS2
											0	0	1	0	0	SOS
											0	0	1	0	1	SLS
											0	0	1	1	0	SDI
											0	0	1	1	1	SBC
											0	1	0	0	0	SLP
											0	1	0	0	1	SLI
											0	1	0	1	0	SLA
											0	1	0	1	1	SSM
											0	1	1	0	0	SCA
											0	1	1	0	1	SLT
								0	0	0						No error
								0	0	1						Triggering caused by a limit violation
								0	1	0						Triggering caused by an incorrect parameter set
								0	1	1						Triggering caused by a missing absolute position
								1	0	0						Triggering caused by a missing rotary encoder
								1	0	1						Triggering caused by time-out of the rotary encoder
								1	1	0	0	0	0	0	0	No FSoE connection
X	X	X	X	X	X	X	X									Specification for *S_ControlWord1* Bit 0 – 7 [a]

[a] This is a copy of S_ControlWord1 bit 0 - 7. It acts as a feedback, if the setting is acting and when it started to act.

NOTE!

At the standard version of "STO" bit 0 is not set, as there is neither a noncompliance nor an error; bit 0 is set as an error reaction not before it is switched over to a STO parameter set, which is not applied.

NOTE!

Bit 0-4 in "S_StatusWord1" shows, at which safety function an error (such as a switchover to a parameter set, which was not defined) or a noncompliance (such as a limit violation) has occurred.

If several safety functions are triggered at the same time, the first safety function is displayed only, which is the one that initiated the error status.

Starting from the module version "software extension" (with regard to the definition refer to ▹chapter 7.9◃) an error code is transmitted in bit 5-7, describing the noncompliance more precisely.

12.7 Status word "S_StatusWord2": Reading of digital inputs and outputs for a quicker diagnosis

The statuses of the safe in- and outputs of the Safety Module can be read by a higher-level safety control via FSoE.

All safe inputs at the SAF-module can be configured with ProSafePara for the activation of safe functions on axis 1 and on axis 2.

However, if only one axis is configured in a single or double axis, there is no FSoE-telegram generated for axis 2 and no FSoE-slave-response of axis two takes place. The evaluation of *S_StatusWord2* of axis 2 in the FSoE-master is omitted.

Therefore, all relevant digital inputs were completely mapped into *S_StatusWord2* of axis 1.

The status word for axis 1 is structured as shown in the table below. For a quick diagnosis, in addition to the inputs, also the statuses of defined digital inputs and outputs at the SAF-module are contained.

The terminal markings match with those in ProSafePara, the pin assignments refer to the terminal representation (see ▹Figure 45◃ on page 90).

Coding of *S_StatusWord2* Axis 1

Bit	Terminal marking	Pin A/B	Meaning
Bit 0	STO_IN_1	17/35	STO-Input group/axis 1
Bit 1	DIG1_IN_1	15/33	Input 1 group/axis 1
Bit 2	DIG2_IN_1	14/32	Input 2 group/axis 1
Bit 3	DIG3_IN_1	12/30	Input 3 group/axis 1
Bit 4	CHAIN_IN_1	16/34	Daisy Chain Input group/axis 1
Bit 5	DIG_OUT_1A	10	Output group/axis 1 A
Bit 6	DIG_OUT_1B	28	Output group/axis 1 B
Bit 7	Brake axis 1	-	Internal output axis 1 to the controller
Bit 8	CHAIN_OUT_1	13/31	Daisy Chain output axis 1
Bit 9	STO_IN_2	2/20	STO-input group/axis 2
Bit 10	DIG1_IN_2	4/22	Input 1 group/axis 2

Bit	Terminal marking	Pin A/B	Meaning
Bit 11	DIG2_IN_2	5/23	Input 2 group/axis 2
Bit 12	DIG3_IN_2	7/25	Input 3 group/axis 2
Bit 13	CHAIN_IN_2	3/21	Daisy Chain input group/axis 2
Bit 14	DIG_OUT_2A	9	Output group/axis 2 A
Bit 15	DIG_OUT_2B	27	Output group/axis 2 B

S_StatusWord2 axis 2 of a double axis is available only, if the axis 2 in the SAF-module also was configured as a FSoE-axis and differs from *S_StatusWord2* axis 1.

Coding of *S_StatusWord2* axis 2 (is omitted, if the SAF-module is configured as a FSoE-single axis)

Bit	Terminal marking	Pin A/B	Meaning
Bit 0	STO_IN_2	2/20	STO-input group/axis 2
Bit 1	DIG1_IN_2	4/22	Input 1 group/axis 2
Bit 2	DIG2_IN_2	5/23	Input 2 group/axis 2
Bit 3	DIG3_IN_2	7/25	Input 3 group/axis 2
Bit 4	CHAIN_IN_2	3/21	Daisy Chain input group/axis 2
Bit 5	DIG_OUT_2A	9	Output group/axis 2 A
Bit 6	DIG_OUT_2B	27	Output group/axis 2 B
Bit 7	Brake axis 2	-	Internal output axis 2 to the controller
Bit 8	CHAIN_OUT_2	6/24	Daisy Chain output axis 2
Bit 9 - Bit 15			reserved

12.7 Status word "S_StatusWord2": Reading of digital inputs and outputs for a quicker diagnosis

13

PARAMETERIZATION AND CONFIGURATION

This chapter describes the parameterization and the configuration of the Safety Module.

A detailed description for programming the Safety Module is found in the Application manual or in the online-help for the parameterization tool ProSafePara.

NOTE!

Contact Baumüller Support, if you have questions referring to the product ProSafePara for the parameterization of safety functions and questions concerning validation of the parameter container, which was generated with ProSafePara.

NOTE!

If the operator configures one axis in ProSafePara only (axis 1), then axis 2 remains in STO (no pulse inhibit, supply voltage to the brake is interrupted).

13.1 Safe Module Address

The Safety Module is provided with a safe module address (slave address, which serves as a clear identification in the safe communication network. It is necessary to establish the communication for the configuration tool ProSafePara and also as a clear FSoE-slave address.

WARNING!

After change of a module address the total application must be checked by the user again.

13.2 Setting of the Safe Module Address

The setting of a safe slave-address (FSoE-address) is made via single binary switches at the cabinet of the Safety Module. The assignment and meaning of the binary switches is demonstrated in ▹Figure 50◃.

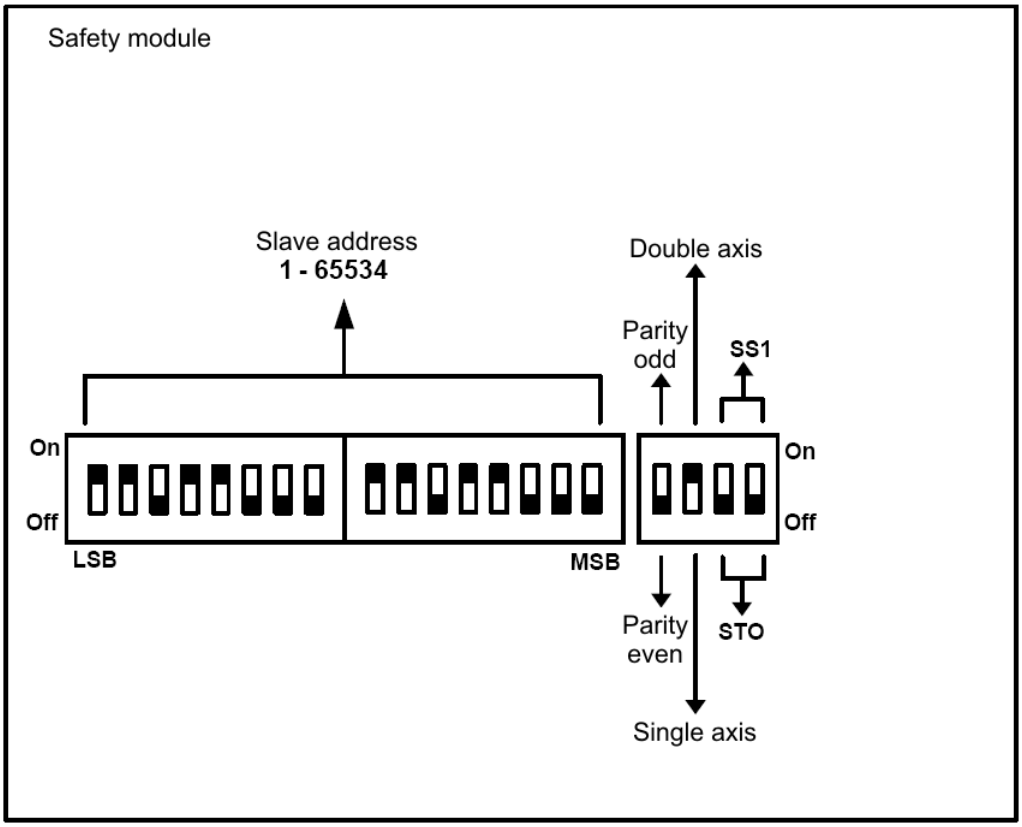


Figure 50: Setting of the slaves addresses and selection of „STO/SS1“ in the standard configuration

Setting possibilities of the binary switches:

- Slave address:

  16 binary switches are available, in order to set the slave address. The address range from 1 to 65534 is available for the user. The two slave addresses 0 (FSoE-master is fixed) and 65535 (provided as a error address; is ignored referring to FSoE addressing) are reserved and may not be set.
  Therefore, the address below (▹Figure 50◃) is the following:

  $2^0 + 2^1 + 2^3 + 2^4 + 2^8 + 2^9 + 2^{11} + 2^{12} = 1+2+8+16+256+512+2048+4096 = 6939$

- Parity (even/odd):

  In order to detect an incorrect binary switch positioning for the generation of the slave address a parity bit must be set using an additional binary switch.

  This parity bit must be set to "odd", in case the number of the set address switches is odd-numbered (= odd). If the parity bit was set incorrect, the address is automatically set to 65535 and an error message "Error at reading the DIP-switches" is generated. The axes remain in "STO".

- Single axis / double axis:

  The Safety Module can be used for single and for double axes. The determination on the Safety Module is executed via the binary switch "Single-/double axis".

  The safe addressing of a module at a single axis is executed via the set slave address. In case of a double axis the following is valid for the address of the second axis:

  Address Axis 2 = set Slave Address + 1

- STO/SS1:

  Provides information, if the drives at the controller in the standard configuration shall change in the safe status "STO" oder "SS1", when enabling the safety function. Information see ▹Chapter 13.3◃ .

13.3 Standard Configuration

In this operating mode a safety component can be operated at the STO-inputs, in order to enable the safety function "STO" oder "SS1" .

NOTE!

A module, which has not been configured has a standard configuration, also. Safety functions can be executed here.

If a Safety Module does not have a configuration file, because it was not loaded yet or because before an existing configuration tool ProSafePara was deleted, then the basic behavior of the Safety Module is determined via the two binary switches „STO/SS1“ and the STO-inputs, after it was started.

As the selected „STO/SS1“ - setting is valid for the total module, either „STO“ or „SS1“ can be operated. A mixed operation, where STO is executed on one axis and SS1 is executed on the other axis, is not implemented in the standard configuration.

The binary switch "STO/SS1" is redundant (double) to troubleshooting. The switch settings influence the function of the STO-inputs of the Safety Module similarity.

If both binary switches are set to "STO" ("off" = down-position, see ▹Figure 50◃), the module can activate the safe status STO after starting.

If both binary switches are on "SS1" ("on" = up-position), the module can activate the safe status SS1 after starting. The delay time SS1 is determined in the standard configuration to 500 ms per default, until STO will be effective.

The activation of the safety function is controlled by the status of the physical STO-inputs of the according axis (STO-input "STO_IN_1" (pin 17/35) for axis 1 and at a double axis additionally STO-input "STO_IN_2" (pin 2/20) for axis 2).

If the STO-input of an axis changes from High into the Low-status during operation or if the STO-input is not connected, which corresponds to the Low-status, the safe function, which was specified via the "STO/SS1"-setting is executed.

The cycle sensitivity of the STO-inputs is active at first. It is used for troubleshooting using safety switch devices with relay-outputs. Therefore, the Safety Module's cycle signals can be applied directly via safe switches to the STO-inputs:

Connection for axis 1: "CLK_OUT_1" -> Electronic switch -> "STO_IN_1" or

connection for axis 2: "CLK_OUT_2" -> Electronic switch -> STO_IN_2"

However, the cycle sensitivity can be switched off by a bridge, "CLK_OUT_1" -> DIG3_IN_1 (axis 1) and "CLK_OUT_2" -> DIG3_IN_2 (axis 2), which is wired from one cycle output on the input 3 of the respective group (DIG3_IN_1 for axis 1 and DIG3_IN_2 for axis 2) .

Now STO-inputs, which are linked with safe switches can be connected to +24V, directly. A cross connection identification is not possible in this case. Safety category 3 is valid!

In order to recognize, if the configuration data is on the Safety Module or if the standard configuration is active, two different flashing sequences were determined for the green LED of the controller's assembly group.

An active standard configuration is made clear by a flashing green LED H2, whereat the red LED H1 is off. The flashing pattern (50 ms on / 50 ms off) is displayed during the total operating time (see ▹LEDs for the Display of Operating States◃ on page 42).

NOTE!

Deleting of configuration data on the Safety Module is possible via the button "Delete parameterization" in the configuration tool ProSafePara.

14

PLANNING OF A SAFETY-ORIENTED CONTROL SYSTEM

The entire process of defining the safety system is carried out in the planning phase. In addition to risk assessment, the planning contains the detailed definition of all system components, the definition of the system parameters and the detailed installation and wiring of the components.

DANGER!

Conducting the planning thoroughly aids in avoiding failures. Failures in safety-oriented machines can lead to permanent injuries and death.

CAUTION!

The "Planning checklist" reproduced in the appendix must be used in the planning phase.

14.1 Risk assessment

The risk assessment establishes, which dangers a machine can present and which plant parts will have to be equipped with safety technology devices. The residual risk is reduced to a justifiable level by means of safety technology measures.

CAUTION!

As machine manufacturer, the applicable machine guidelines obligate you to conduct a risk assessment in order to establish the dangers associated with the machine and reduce the residual risk to a justifiable minimum.

CAUTION!

It is absolutely necessary to conduct the risk assessment during the planning phase and before conducting retrofitting work.

The risk assessment should be conducted according to the procedure described in the following.

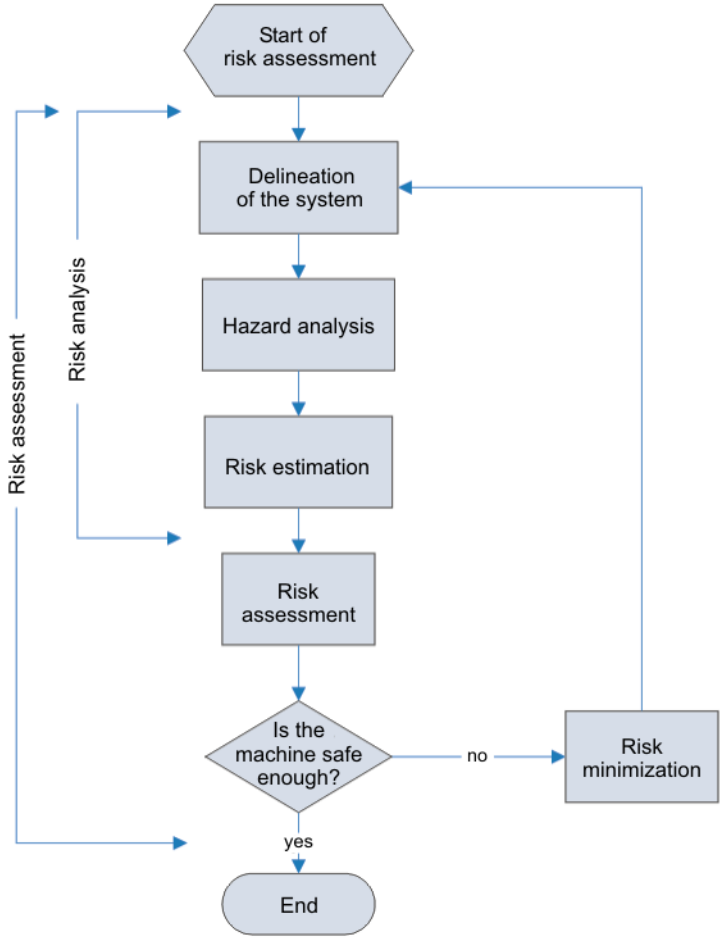


Figure 51: Risk assessment procedure in accordance with DIN EN ISO 12100-1 and EN ISO 14121

Delineation of the system:	Determination of the limits of the system's boundaries and the intended use
Hazard analysis:	Identification of hazards and the related hazardous situations
Risk estimation:	Estimation of the risks for each hazard identified
Risk assessment:	Assessment of the risks and establishment of risk reduction measures

The determination of the required safety class (SIL according to EN 62061 and performance level according to EN ISO 13849-1) is carried out in the scope of risk assessment for the installation/machine in accordance with EN ISO 12100-1 and EN ISO 14121.

14.2 Installation and wiring plan

An installation and wiring plan for the entire safety system is to be developed in the planning phase. It contains all system components and its wiring.

CAUTION!

The applicable standards and guidelines on laying electrical lines must be observed when developing the wiring plan.

14.3 Course of the planning phase

The system is planned according to the requirements of the installation or the machine. The components, which are available for the automation of the available components are described in the Automation Catalog of the company Baumüller Nürnberg GmbH. Here information on concepts, PLCs, field busses, motion control, technology blocks, HMIs, IPCs and I/Os is available.

Prior to commissioning of the Safety Module (SAF-002/-003), the following must be checked and guaranteed:

- Compatibility of the Safety Module (SAF-002/-003) with the controller (see chapter ▹Compatibility list◃ on page 31).
- Adequate supply of the controller by the connected power supply unit or safety components.

15

ASSEMBLY AND INSTALLATION

This chapter describes the mechanical assembly and the electrical installation of the Safety Module.

The assembly and installation process consists of the following steps:

1 Assemble the Safety Module.

2 Check the assembly and installation by means of the "Installation checklist" listed in Appendix ▹B.2◃ on page 161.

15.1 General safety regulations

CAUTION!

The "Installation checklist" reproduced in Appendix ▹B.2◃ on page 161 must be used during the assembly and installation phase.

- Make sure that the installation process is carried out entirely in accordance with the installation and wiring plan.
- Conduct a visual inspection and check all system components for visible damage.
- Check the system for wiring errors.
- Check the tightening torque and make sure that the electrical connection is not interrupted by insulation material.
- Check the tensile-load capacity of the electrical terminal and screw connections.
- Make sure that the installation and the cable routing are carried out in accordance with applicable standards and guidelines.
- Make sure that the system's environmental properties specified in Appendix ▹C.3.1◃ on page 166 are not exceeded.
- Make sure that the design of the system's type of protection is sufficient.
- Make sure that the safety system is not damaged by moving parts or work in the area surrounding the installed safety components.
- Make sure that the system components do not come into contact with aggressive substances (such as acids, bases, transmission oil).

➲ Follow the information in the chapter ▹Safety◃ from page 17 onward.

15.2 Requirements on the personnel conducting the work

DANGER!

Perilous danger from electrical current!

The device and surrounding area in the electrical cabinet can carry perilous voltages.

Therefore:

- The danger- and warning notes must be observed (see chapter ▹4.8◃ on page 21).
- Ensure, that only qualified personnel mounts and installs this module (see requirements in chapter ▹4.6◃ on page 19 "Personnel training").

15.3 Assembly instructions

The assembly of the controller is described in the operation manual for the controller.

DANGER!

Perilous danger from electrical current!

The device and surrounding area in the electrical cabinet can carry perilous voltages.

Therefore:

- The described danger- and warning notes must be observed (see chapter ▹4.8◃ on page 21.

The following tools are required:

- Torx screwdriver (size TX8) for fastening the Safety Module in the controller.

➲ Ensure that the suitable controller is available (see chapter ▹Compatibility list◃ on page 31).

Perform the assembly as follows:

1 Plug the Safety Module into the mounting opening of the frequency controller.

2 Secure the module with the torx screw against unintentional dropping.

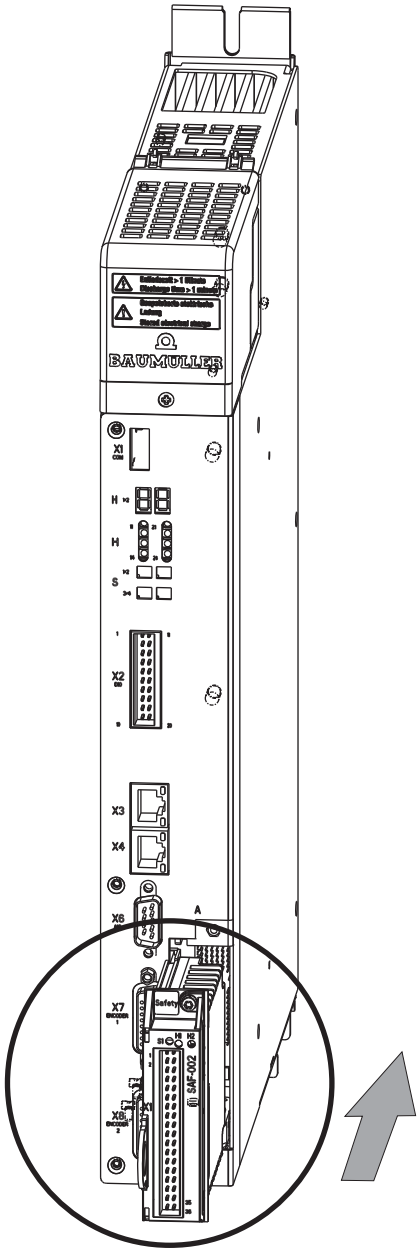


Figure 52: Assembly of Safety Module

15.4 Installation

Wire the Safety Module (SAF-002/-003) in accordance with the following connection diagram.

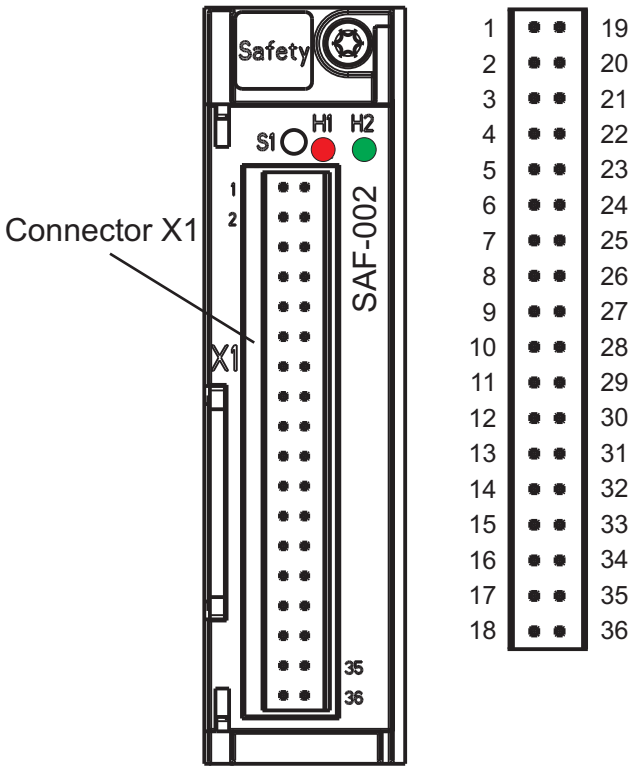


Figure 53: Connection diagram of the Safety Module

The pin assignment for the type with Daisy Chain and for the type with Grounds is in Appendix ▹C.4 Pin assignment of Safety Module connector X1◃ from page 167.

15.4.1 Requirements for the electrical connection

CAUTION!

Danger due to voltage!

The module can be damaged or destroyed, if the requirements for the electrical connection of the module are not met.

Therefore:

- Make sure that the connection values specified in technical data are met and that the connections are carried out in accordance with the specifications.
- Prevent a short circuit between inputs and outputs. A short circuit between inputs and outputs can destroy the Safety Module.

The standard EN 60 204-1 (Electrical Equipment of Machines) must be observed when installing and mounting cable connections.

Further notes:

- Make sure that the connection cable is routed in an EMC-compatible manner.
- Use appropriate cables with an appropriate cable cross section.
- Mark the cable connections, in order to protect against polarity reversals.
- Ensure, that the connection plugs cannot fall out.

15.4.2 Requirements on the connection cable

The connection cable must be selected in accordance with the EN 60204-1 standard.

The Safety Module is equipped with plugged connectors at delivery (2 pieces with 18 poles respectively, part number 00351525 per connector) for the connection of the conductors. These connectors must be plugged always in operation, even if a conductor is not connected.

Connectable conductors must observe to the following characteristics:

Terminal range, rated connection:	min. 0.08 mm², max.1 mm²
Conductor connection cross section AWG:	min. AWG 28, max. AWG 18
Single-wired/flexible:	min. H05(07) V-U 0.2 mm², max. H05(07) V-U 1 mm²
With wire end ferrule in accordance with DIN 46 228/1:	min. 0.13 mm², max. 0.34 mm²
With AEH with shroud DIN 46 228/4:	min. 0.13 mm², max. 0.34 mm²

Please take notice of chapter ▷11.4◁ on page 98 when connecting the brakes to the basic unit.

16

COMMISSIONING AND REPLACEMENT OF THE MODULE

This chapter describes the commissioning procedure of the Safety Module. The procedure of commissioning ensures that the Safety Module functions properly. In addition, the chapter describes how the module must be replaced.

NOTE!

The procedure of a correct commissioning is the prerequisite for an error-free operation.

Before beginning the commissioning procedure, make sure that the following prerequisites have been fulfilled:

1 The Safety Module is installed correctly.

2 Safety Module is connected to the safety component (e.g. safe sensors).

3 No individuals or parts are in the danger zone.

4 The controller is ready for use.

NOTICE!

The commissioning of the Safety Module is permitted only after the acclimation of the module.

The described climatic features in ▹Chapter C.3.1◃ must be observed.

Please take of ▹Troubleshooting and Error Correction◃ from page 137 onward for rectifying errors during the commissioning procedure.

16.1 General safety regulations

➲ Follow the chapter ▹Safety◃ from page 17 onward.

DANGER!

Danger of injury due to moving parts!

Machine parts/line parts or the entire machine/line can move during commissioning. The "Planning checklist" reproduced in Appendix ▹B.3 Commissioning and validation checklist◃ from page 162 onward must be used during commissioning.

Therefore:

- Maintain an adequate distance from moving machine parts/line parts or from the moving machine/line.
- Consider that the machine parts/line parts or machine/line can be set in motion via additional modules connected to the Safety Module.
- Activate the safety devices in any case prior to switching on the system.
- Make sure that the system is commissioned exclusively by qualified personnel.
- Make sure that there are no people in the danger zone during the initial commissioning. Always anticipate that a machine, system or safety device might react differently to what is inspected.
- If changes or expansions are conducted during the commissioning procedure, the effects on system reaction must be checked. To do this, it is necessary to execute the checklists for planning and installation procedure again.

16.2 Requirements on the personnel conducting the work

The commissioning work may only be conducted by professionally trained personnel, in particular personnel, who understands the safety regulations and follows them.

DANGER!

Danger from mechanical action!

The machine/line or parts of the machine or line can be started during the commissioning of the Safety Module.

Therefore:

- Maintain an adequate distance from moving machine parts/line parts or from the moving machine/line.
- The described danger- and warning notes in chapter ▹4.8◃ on page 21 must be observed.

16.3 Replacement of the module

NOTE!

The drive controller is inhibited automatically if the Safety Module is defective. The module or the entire controller unit must be replaced.

NOTICE!

- The replacement of the module may be performed by authorized and qualified personnel, only.
- No further changes in the system configuration may be made during the replacement of the module.
- Prior to the replacement of the module, ensure that the Safety Module and the controller are compatible.

  A list of the controllers, which are compatible with the Safety Module is in chapter ▹Compatibility list◃ on page 31.

Replacement procedure

After installation of the Safety Module (SAF-002/-003) into the controller and after switching on the controller, the following procedures must be performed in the controller and in the Safety Module (SAF-002/-003) (see ▹Figure 54◃ on page 128).

1 **Query of the controller ID and parameter data by the Safety Module**.

  The Safety Module contains a micro controller with communication interface. If the controller is switched on, the Safety Module initiates a request for the controller ID and the parameter data to the controller.

2 **Checking of data sets of controller and the Safety Module**.

  The saved data sets on the controller and on the Safety Module are compared.

  - Data sets of the Safety Module and of the controller are identical.
    In this case the Safety Module starts automatically and completes the procedure.
  - Data sets of the Safety Module and of the controller are not identical.
    The red LED on the Safety Module permanently is on. The copying of the data set on the controller into the parameter record of the Safety Module must be accepted by pressing the button on the Safety Module. The button must be pressed as follows: Long - short - short - long (long > 1000 ms, 500 ms > short > 1000 ms). The green LED flashes when the button is pushed.
    Then the user must execute a complete function test for the system.

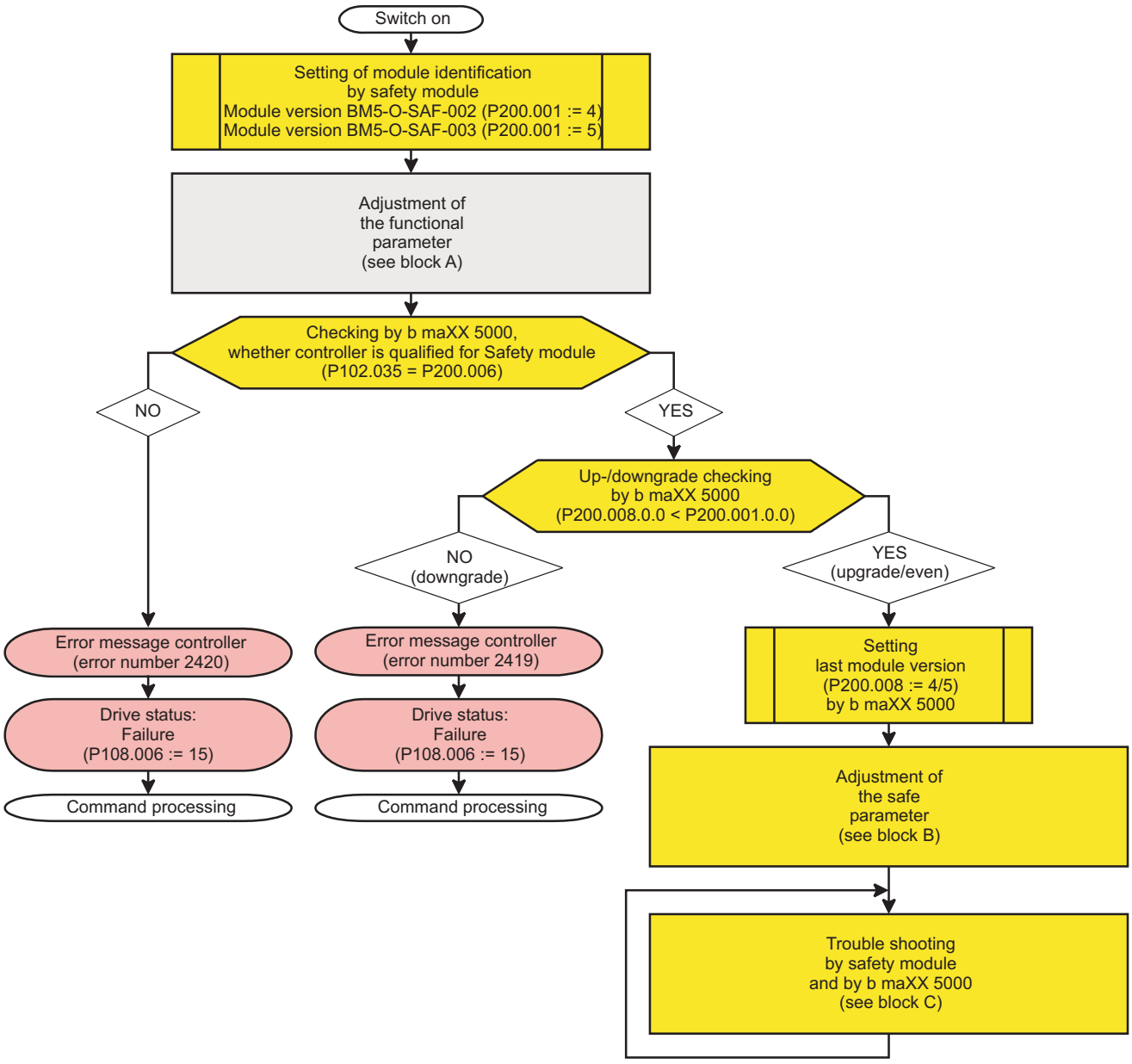


Figure 54: Process of the module change procedure

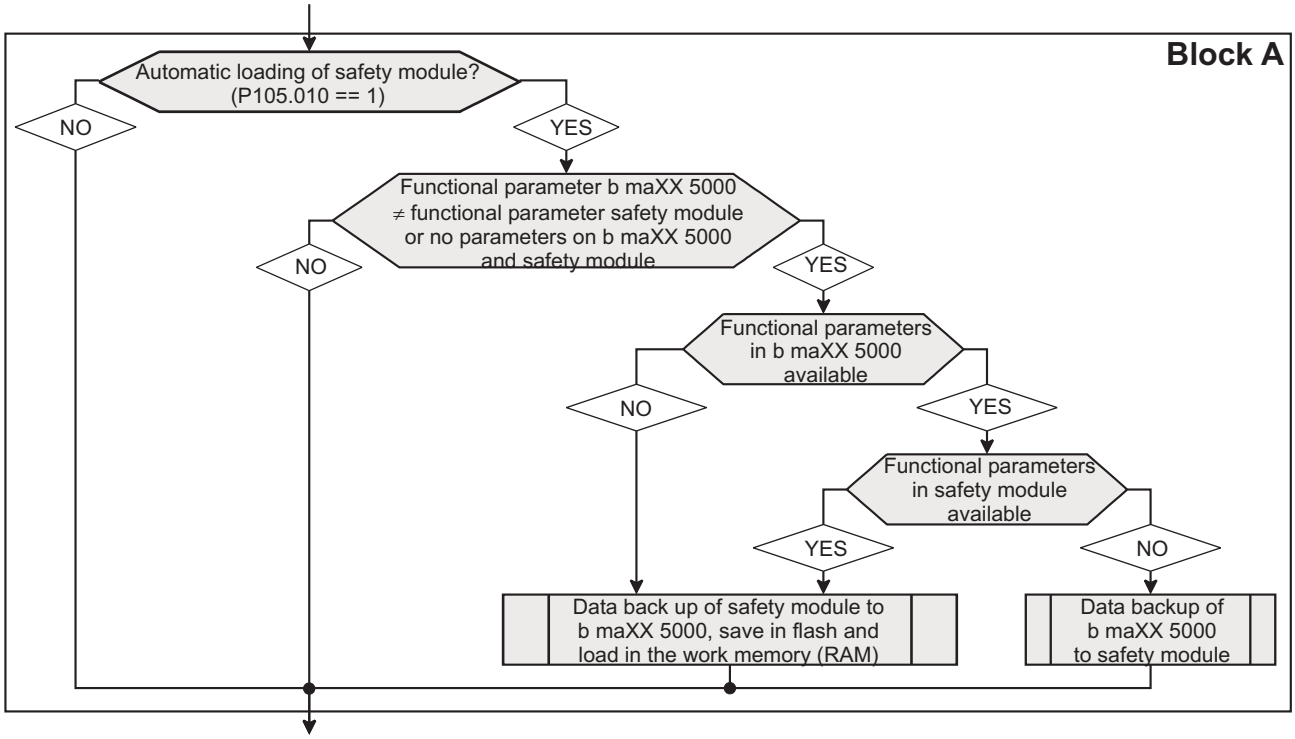


Figure 55: Process of the module change procedure block A

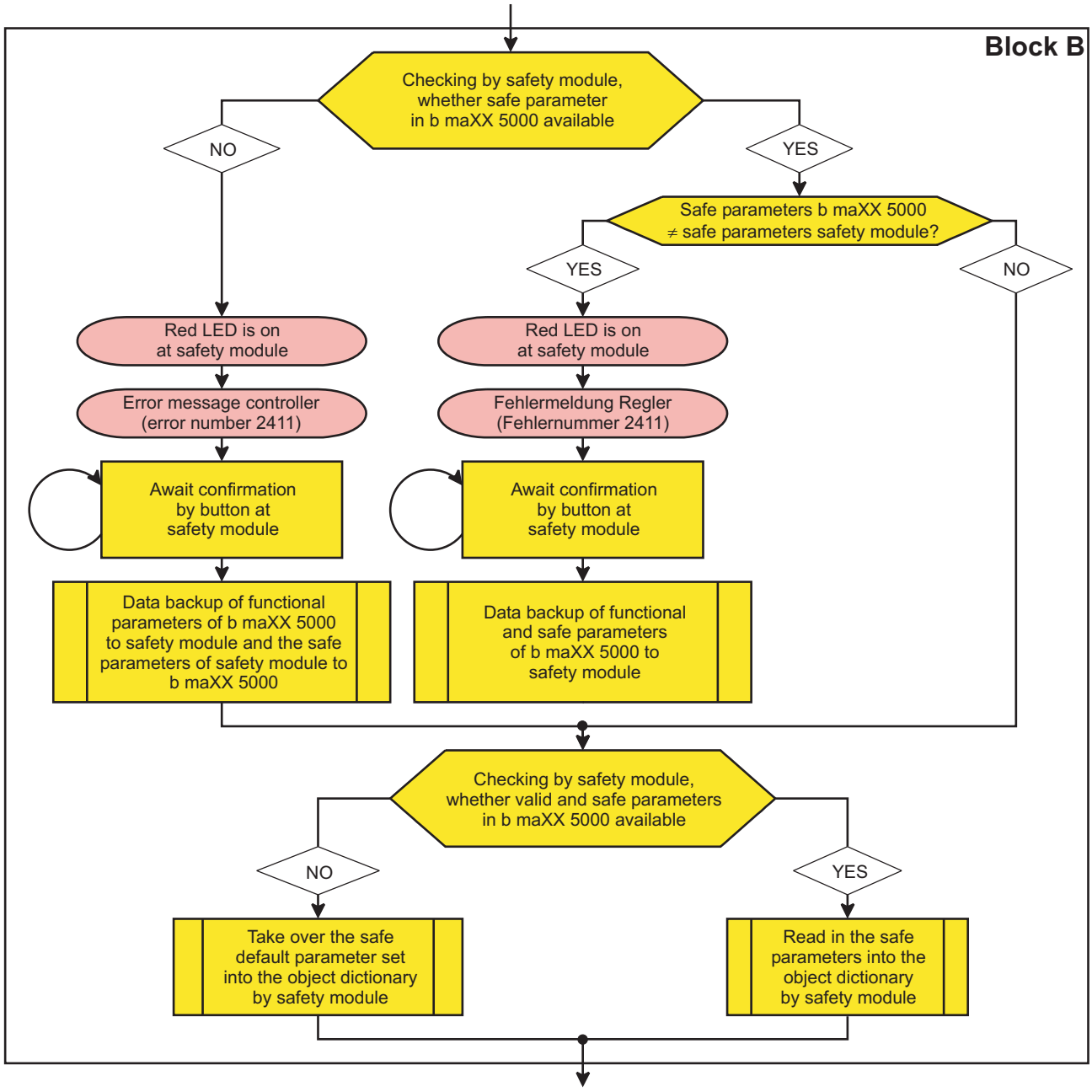


Figure 56: Process of the module change procedure block B

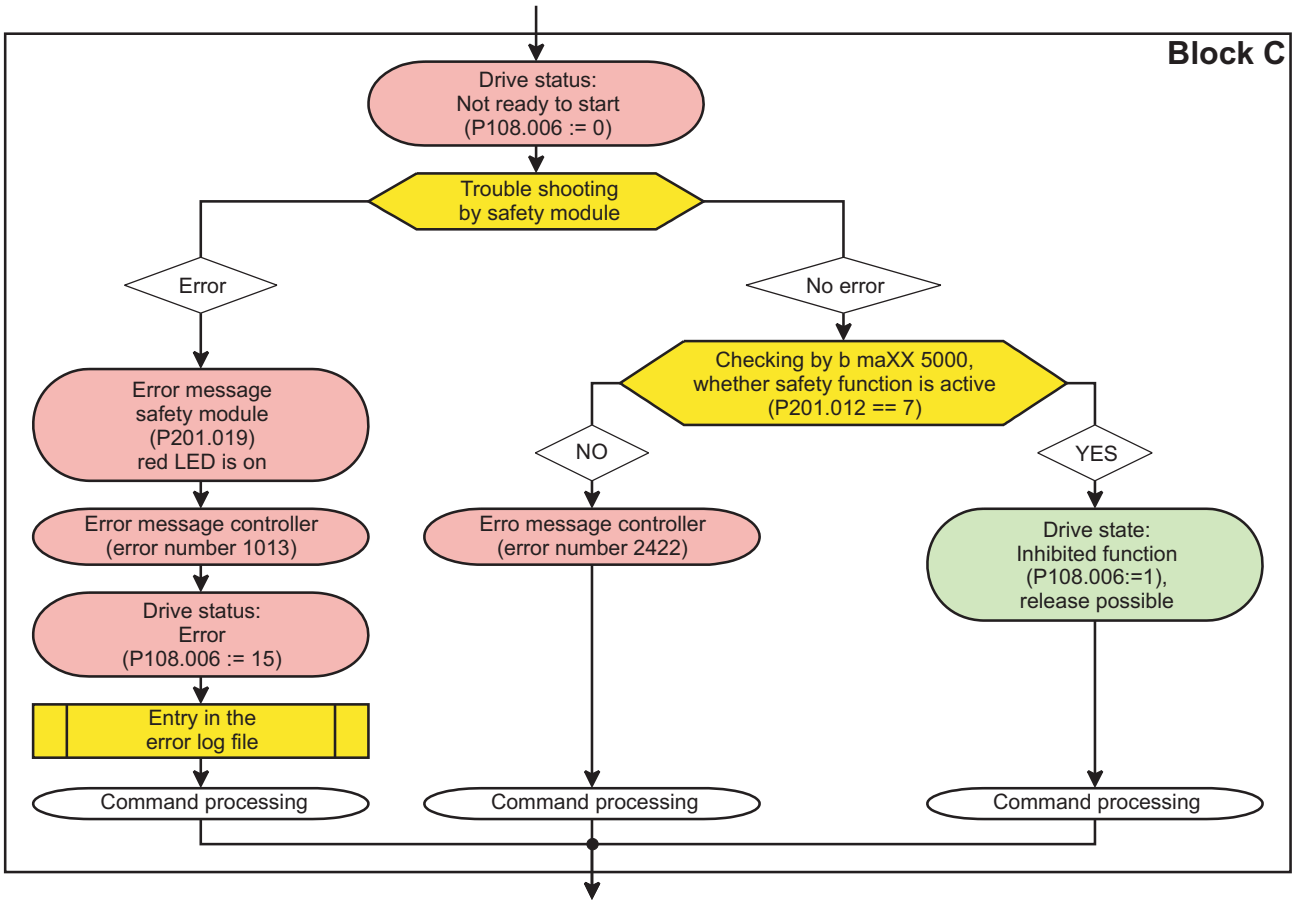


Figure 57: Process of the module change procedure block C

Error number	Short description
2411	No valid safety parameter file on SAF module
2419	Module change from SAF-003 to SAF-002
2420	No valid controller for SAF-module
2422	No FSoE communication active at SAF-002 or SAF-003
2423	Pulse inhibit because of SAF-100

NOTE!

- If the data sets on the Safety Module are **not identical** with the controller's data, a copy of the data set is made. Generally this copy is made from the controller in direction of the Safety Module.
- If a copy of the data set is necessary from the Safety Module to the controller, the controller's parameter record must be deleted with the reset-module before (see ▹Description of the Reset-Module◃ from page 49 onward).

NOTICE!

Once the module has been replaced, a complete function test for the system has to be conducted and documented accordingly.

NOTICE!

After the module was replaced, ensure an unexpected starting by using external safety components (for example emergency stop device).

NOTICE!

It is necessary to label defective components to indicate that they are defective. It is absolutely necessary to prevent defective components from being reused by taking measures in the scope of quality management on the user's side (see the chapter ▹Repair◃ from page 149 onward).

NOTE!

If the controller was equipped with a module of a higher safety level previously (SAF-002), and another module with a lower safety level shall be plugged (e.g. SAF-001), the parameter storage of the controller must be reset with the reset-module.

17

SYSTEM VALIDATION

All safety functions as well as the trouble-free functioning of the installed and parameterized system must be tested with the initial operation and after changes. The testing of the system must be documented.

WARNING!

Danger during commissioning!

The Safety Module may only be put into operation after being tested successfully by a technical expert.

Therefore:

- Conduct a complete function test. In doing so, check the correct allocation of the connected safety components.
- A checklist for the commissioning and validation of the system is reproduced in Appendix ▹B.3 Commissioning and validation checklist◃ from page 162 onward. Conduct the validation of the system in accordance with this checklist and document the procedure accordingly.
- Make sure that operating personnel has been instructed in the handling of the Safety Module.

17.1 Function test

The function test is a major part of the validation of the entire system. The function test is used to determine the trouble-free allocation of the network safety components and the programmed logic of the system.

Depending on the complexity of the logic circuit of the respective project, it is recommended to conduct the function tests in steps.

The following course of action is recommended when conducting the function tests:

1. Only connect the actuators and drives to the safe output terminals once no errors have been detected in the inspection of the logic circuit.
2. Conduct a complete function test with all sensors (initiators), switches, actuators and drives.

17.1 Function test

To conduct the function tests, trigger all safety functions sequentially and document the system's reaction. Check, whether the reaction corresponds with the expected behavior.

18

OPERATION

Instructions on the operation of the system components, which is connected to the used controller, can be found in the corresponding operation manuals and application manuals for these components.

DANGER!

It is not permitted to make any changes to the system configuration during the operation of the Safety Module.

Therefore:

- Before expanding the system and removing individual system components and making changes in the wiring, the Safety Module must, as a rule, be disconnected from the power source and put into safe condition by technical trained personnel.

19

TROUBLESHOOTING AND ERROR CORRECTION

This chapter describes the error indications of the Safety Module.

19.1 Safety regulations

Observe the applicable safety regulations, see ▹Safety◃ from page 17.

19.2 Requirements on the personnel conducting the work

Personnel working with the Safety Module must be instructed in the safety regulations and the operation of the module and be familiar with the proper operation of the system. The reaction to error indications and statuses in particular requires special knowledge, which the operator must have.

19.3 Error diagnosis

Fail-safe principle

The Safety Module is based on the fail-safe principle. This means that each error automatically causes the module to switch into the safe status STO (Safe Torque Off).

However, external errors, which are detected, cause a safe status STO. These errors can be caused by interferences of the FSoE-communication or from the diagnostic possibilities according to chapter ▹Detecting errors in the periphery◃ on page 138.

The red LED on the front panel of the Safety Module indicates the error status (see chapter ▹LEDs for the Display of Operating States◃ from page 42).

The parameters ▹201.12◃ and ▹201.23◃ of the controller are required for a general status diagnosis.

The parameters ▹201.19◃ and ▹201.20◃ of the controller are required for an error diagnosis.

The lists of the diagnosis- and error statuses are listed in ▹Operating states and error messages◃ from page 138.

WARNING!

Do not put a defective safety-oriented system back into operation as long as the cause of the error is unknown or an error has not been detected.

19.4 Detecting errors in the periphery

- The safe input and output have diagnostic functions in order to detect short circuits and crossfault on the input and output cables (see ▹External Interfaces◃ on page 93).
- Electronic sensors must have an own error detection regarding short circuits on the output.

CAUTION!

An elimination of errors for short-circuits on line must be made for safe outputs, which are used separately in order to safely switch-off an actuator. Measures must be taken in accordance with EN ISO 13849-2.

19.5 Operating states and error messages

Description of operating states in parameter ▹201.12◃ and the possible status- and error states in ▹201.13◃

▹201.12◃	Description	▹201.13◃	Description
1	Initialization	0	Request synchronization telegram
		1	Acknowledgment of synchronization telegram
		2	Request of Session ID for FSoE
		3	Acknowledgment of Session ID for FSoE
		4	Switch on LEDs
		5	Switch on waiting time
		6	Switch off waiting time
		7	Waiting for test manager and online test
		8	Waiting for initialization of the GDP protocol

▹201.12◃	Description	▹201.13◃	Description
2	Basic condition	0	Evaluation of controller identification
		1	Checking of CRC and version of the parameter container
		2	Reading of the parameter container in the object directory
		3	Reading of the Stand Alone configuration in the object directory
		4	Configuration of in- and outputs
		5	Entry in log file
		6	Configuration of encoder
		7	Setting of the starting values of the data sets
		8	Initialization of the real time GDP connection
		9	Waiting for encoder values
		10	Waiting for FSoE connection
		11	Waiting for GDP to complete transmission
		12	Waiting for the end of SS1 time for the safety function
		13	Parameter check: Comparison of Motor type/ Encoder type/Encoder PPR count of the drive and SAF module
3	Parameteri-zation	Bit 0	Saving the FU file on FU
		Bit 1	Saving of the parameter container on FU
		Bit 2	Deleting the FU file on FU
		Bit 3	Deleting the parameter container on FU
4	Reloading	-	Waiting for acknowledgment by button or download of a parameter container
5	Module change	-	-
6	Error	-	In the operating state “Error“ an accordant error code can be read over ProDrive in the parameter ▹201.19◃. There is additional information specifying an error code in the parameter ▹201.20◃. (see table: List of the error messages)

▹201.12◃	Description	▹201.13◃	Description
7	Safety function	Bit 0	STO due to limit exceeded at axis 1
		Bit 1	STO due to limit exceeded at axis 2
8	Encoder failure	--	At the asynchronous motor no movement was detected the last 12 hours at the encoder (occurs at SAF modules with software extension, only) This encoder fail status can be acknowledged by the user (refer to the chapter ▹Acknowledgment encoder fail status◃ on page 40)

Programming a "SS1-time general" for specifically error types:

At all of the error types STO is always carried out causing that the drive coasts down and is not actively braked.

Specific error types, that were not categorized as system-critical, the user can now globally define an error reaction time from the software extension SAF-002/3-module (refer to the description "SS1 time general" in chapter ▹Software Extension SAF-002/-003 Module◃ on page 44).

These error types are marked with "Yes" in the "SS1-time general" column in the following error list.

Operating state 6 "Error": List of error messages and the description (parameter ▹201.19◃ and, if required, more details in ▹201.20◃)

Error number	Description	SS1 time general
0	No error	
1	Nullpointer-access	no
2	Access to invalid parameter	no
3	Division by zero	
4	Error when writing in flash	yes
5	Error at reading the flash	yes
6	Error at deleting the flash	
7	CRC error in flash data	yes
8	Incorrect parameter value	no
9	No memory left in error file	
10	Writing an unknown parameter	yes
11	Reading an unknown parameter	yes
12	CRC error parameter file controller	yes
13	CRC error parameter file ProSafePara	
14	Error when reading or writing the serial number	yes
15	Error at data exchange with ProSafePara	yes
16	Error at switching over the mode with ProSafePara	yes
17	Incorrect session ID	yes
18	Invalid index for parameters	yes
19	Invalid subindex for parameters	yes

Error number	Description	SS1 time general
20	Invalid instance for parameters	yes
21	Invalid data set for parameters	yes
22	Invalid parameter access	yes
23	Run-time error for safe cycle	no
24	Invalid mode to delete the flash	no
25	Time exceeding when reading the analog values	no
26	Programming or deleting of flash is already activated	
27	Invalid encoder signal	no
28	Invalid encoder type	yes
29	Time exceeding when reading ProSafePara file	no
30	Time exceeding at cross monitoring	no
31	Invalid ProSafePara file	yes
32	Invalid telegram for cross communication	no
33	Invalid start character for cross communication	no
34	Invalid telegram type for cross communication	no
35	Invalid telegram length for cross communication	no
36	Telegram repetition at cross communication	no
37	CRC error cross communication	no
38	Interface for cross communication is already in use	
39	Time exceeding at cross communication	no
40	Online test wasn't synchronized	yes
41	Online test already active	
42	Error at online test	yes
48	No data exchange at FSE communication	
49	No new FSoE data from the master	
56	Incorrect identification for GDP real time telegram	yes
57	Incorrect command for GDP real time telegram	yes
58	Incorrect telegram length for GDP real time telegram	yes
59	Incorrect list parameter for GDP real time telegram	yes
60	Incorrect checksum for GDP real time telegram	yes
61	No GDP real time configuration was established	yes
62	Time exceeding for GDP real time telegram update	yes
72	Different number of axes at the DIP-switch and ProSafePara file	yes
73	Different number of axes at the DIP-switch and the controller	yes
74	Error when reading the DIP-switches	yes
75	No adequate controller for Safety Module	yes
76	Different versions of Safety Module and ProSafePara file	yes
77	Parameter check axis 1: Different values were detected in the drive and SAF module (Motor type/Encoder type/Encoder PPR count)	
78	Parameter check axis 2: Different values were detected in the drive and SAF module (Motor type/Encoder type/Encoder PPR count)	
80	Error when parameterizing the test manager	yes
81	Error when initializing the test manager	no
82	Error at RAM March C test	no
83	Error at RAM Galpat test	no

Error number	Description	SS1 time general
84	Underflow at stack usage	no
85	Overflow at stack usage	no
86	Error at CPU test	no
87	Error at firmware check	no
88	Error when switching off the interrupt	no
89	Unknown hardware error	no
90	Internal supply voltage 3.3V off-limits	no
91	External supply voltage 3.3V off-limits	no
92	Internal supply voltage 15V off-limits	no
93	External supply voltage 15V off-limits	no
94	Differences in detected current values	yes
95	Differences in detected temperatures	yes
96	Differences in detected positioning for axis 1	yes
97	Differences in detected positioning for axis 2	yes
98	Encoder signal axis 1 lower than limit value	yes
99	Encoder signal axis 1 higher than limit value	yes
100	Encoder signal axis 2 lower than limit value	yes
101	Encoder signal axis 2 higher than limit value	yes
102	Differences in the detected analog sine values for axis 1	yes
103	Differences in the detected analog cosine values for axis 1	yes
104	Differences in the detected analog sine values for axis 2	yes
105	Differences in the detected analog cosine values for axis 2	yes
106	Error when checking the DIP-switch	yes
107	Test manager is activated already	
108	Error at the hardware test	yes
109	No movement detected at the encoder for 12 hours (occurs at SAF modules with standardized software, only)	
110	Error at the comparison of motor angle (electr.) and encoder axis 1	
111	Error at the comparison of motor angle (electr.) and encoder axis 2	
112	Four-quadrants encoder counter value doesn't fit with the phase of the amplitude	
113	Standard configuration: invalid "STO/SS1" - combination of the binary switches	
128	Different serial number in ProSafePara telegram	
129	Different FSoE address in the ProSafePara telegram	
130	Incorrect checksum for ProSafePara telegram	
131	Unknown ProSafePara command	
132	Invalid mode for command processing	
133	Error at two-channel command processing	
134	Error when deleting the error file	
135	Error when loading and checking the ProSafePara file	
136	Error when loading an object	
137	Incorrect identification	

Additional information at error 42: Error at online test

Error number	Description
1	STO input 1 CPU 1 axis 1
2	Input 2 CPU 1 axis 1
3	Input 3 CPU 1 axis 1
4	Input 4 CPU 1 axis 1
5	Daisy Chain CPU 1 axis 1
6	STO input 1 CPU 1 axis 2
7	Input 2 CPU 1 axis 2
8	Input 3 CPU 1 axis 2
9	Input 4 CPU 1 axis 2
10	Daisy Chain CPU 1 axis 2
11	Enable output High Side CPU 1 axis 1 A
12	Enable output High Side CPU 1 axis 1 B
13	Output 1 and output 2 CPU 1 axis 1
14	Output brake CPU 1 axis 1 set
15	Output brake CPU 1 axis 1 read
16	Output Daisy Chain CPU 1 axis 1
17	Inputs with clock control CPU 1 axis 1
18	Enable output High Side CPU 1 axis 2 A
19	Enable output High Side CPU 1 axis 2 B
20	Output 1 and output 2 CPU 1 axis 2
21	Output brake CPU 1 axis 2 set
22	Output brake CPU 1 axis 2 read
23	Output Daisy Chain CPU 1 axis 2
24	Inputs with clock control CPU 1 axis 2
25	DIP-switch check 1
26	DIP-switch check 2
65	STO input 1 CPU 2 axis 1
66	Input 2 CPU 2 axis 1
67	Input 3 CPU 2 axis 1
68	Input 4 CPU 2 axis 1
69	Daisy Chain CPU 2 axis 1
70	STO input 1 CPU 2 axis 2
71	Input 2 CPU 2 axis 2
72	Input 3 CPU 2 axis 2
73	Input 4 CPU 2 axis 2
74	Daisy Chain CPU 2 axis 2
75	Enable output Low Side CPU 2 axis 1 A
76	Enable output Low Side CPU 2 axis 1 B
77	Output 1 CPU 2 axis 1
78	Output 2 CPU 2 axis 1
79	Output brake CPU 2 axis 1 set
80	Output brake CPU 2 axis 1 read
81	Output Daisy Chain CPU 2 axis 1
82	Inputs with clock control CPU 2 axis 1

Error number	Description
83	Enable output Low Side CPU 2 axis 2 A
84	Enable output Low Side CPU 2 axis 2 B
85	Output 1 CPU 2 axis 2
86	Output 2 CPU 2 axis 2
87	Output brake CPU 2 axis 2 set
88	Output brake CPU 2 axis 2 read
89	Output Daisy Chain CPU 2 axis 2
90	Inputs with clock control CPU 2 axis 2

Additional information at error 48: No data exchange at FSoE communication

Error number	Description
0	Reset with program or FSoE master
1	Invalid FSoE command
2	Unknown FSoE command
3	Invalid connection number
4	Checksum error
5	Watch Dog overflow
6	Invalid FSoE address requested by FSoE master
7	Invalid process data
128	Invalid FSoE parameter
129	Invalid user parameter
130	Invalid command sequence
192	Invalid FSoE address 65535 at DIP switch
193	Invalid session ID 0 received
194	CRC error
196	No new data from FSoE master (FailSafe)

20

MAINTENANCE

If you are complying with the mandatory environmental conditions, see ▹Appendix C - Technical data◃ from page 163 onward, then the Safety Module is maintenance-free.

A defective device cannot be repaired (see the accordant notes in ▹Repair◃ on page 149).

CAUTION!

The Safety Module does not require a proof-test within its service life of 20 years.

After this time it must be put out of operation and must be disposed of properly. It is forbidden to perform a proof-test (see ▹Safety-related parameters for an operation of 20 years◃ from page 25 onward).

21

ACCESSORIES

In this chapter, you will find a list of all the accessories that are available for Baumüller Nürnberg GmbH's safety module b maXX 5000..

If you have any queries about accessories or suggestions for improvements, Baumüller's Product Management will be pleased to hear from you.

21.1 List of all accessories

21.1.1 Supplement

Type	Article number
Supplement group 1	00443825
Supplement group 2	00443826

See examples for connecting the Safety Modules ▹C.5.5 BM5-O-SAF-00x-001-000 (separate grounds, with SO4000)◃ on page 173.

21.1.2 Ferrite ring

Type	Article number
Ferrite ring	00453508

21.1 List of all accessories

22

REPAIR

You cannot repair a defective Safety Module. Please contact Baumüller Nürnberg GmbH for a replacement.

NOTICE!

Defective components must be repaired by the manufacturer.

23

DISASSEMBLY, STORAGE

This chapter describes how to decommission and to store the Safety Module.

23.1 Safety regulations

➲ Follow the chapter ▹Safety◃ from page 17 onward.

CAUTION!

Damage through electrical destruction.

The component assembly can be destroyed by electricity if it is removed when the power is turned on.

Therefore:

- Make sure that the power to all electrical connections is shut off and secured to prevent from being turned back on.
- Using suitable measuring equipment, check to make sure that none of the connections are carrying live current before beginning work on the electrical connections.
- Only disassemble the connections and remove the connection once you are completely certain that the component assembly is not under power.

WARNING!

Danger of injury due to uncontrollable behavior of the machine/line.

The behavior of the machine/line can change as a result of removing the component assembly with the power source connected.

Therefore:

- Make sure that the power to all electrical connections is shut off and secured to prevent from being turned back on.
- Using suitable measuring equipment check, to make sure, that none of the connections are carrying live current before beginning work on the electrical connections.
- Only disassemble the connections and remove the connection once you are completely certain that the component assembly is not under power.
- Hanging loads could disconnect unexpectedly and fall, because STO is enabled during the removing of the assembly group.

23.2 Requirements on the personnel conducting the work

The personnel, who is assigned to carry out the disassembly must have the knowledge and training, which is necessary to perform this work properly. The personnel must be able to understand and use the safety instructions attached to the device and its components as well as the connections.

23.3 Disassembly

The personnel carrying out the disassembly must meet the requirements above.

Carry out the disassembly process in the following order:

1. Make sure that the power has been disconnected and cannot be turned back on accidentally.
2. Disassemble the Safety Module in the reverse order of the assembly (see chapter ▹Assembly and installation◃ from page 119 onward).
3. Document the disassembly (or replacement) of the Safety Module.
4. Document the disassembly (or replacement) of the controller, if applicable.
5. Document the disassembly (or replacement) of the additional system components, if applicable.

23.4 Storage conditions

Store the Safety Module in a adequate package with regard to the storage conditions specified in the ▹Technical data◃ from page 163 onward.

23.5 Recommissioning

If you want to put the Safety Module back into operation, observe the specifications under "Storage conditions". Then conduct the ▹Commissioning and replacement of the module◃ from page 125 onward again.

24

DISPOSAL

This chapter describes the proper and safe disposal of the Safety Module. For the most part, it can be classified as electronic scrap.

- Prerequisite: The disassembly procedure was carried out, see ▹Disassembly, storage◃ from page 151 onward.

24.1 Safety regulations

The disposal may only be conducted in compliance with the safety regulations. Observe special local regulations, if applicable. If you are not able to conduct the disposal, hire a suitable waste removal company to do so.

24.2 Requirements on the personnel conducting the work

The personnel you assign to carry out the disposal/disassembly must have the knowledge and training necessary to perform this work properly. The personnel must be able to understand and use the safety instructions attached to the controller and its components.

24.3 Disposal instructions

Prerequisites	Safety Module has already been disassembled properly All devices, which are necessary for the disassembly, are applicable and in a perfect working order.
Sheet steel	Parts of the module are made of galvanized sheet steel. Sheet steel must be put into the cycle of potential recyclables for ferrous metals.
Electronic scrap	Electronic scrap (circuit boards), which cannot be disassembled, must be disposed of as special waste. Observe the applicable regulations in doing so.
Plastic	The housing is made of plastic. Plastic must be put into the cycle of potential recyclables for plastics.

24.4 Recycling collection center/offices

Make sure that the disposal is carried out in compliance with your company's disposal guidelines as well as those of the competent recycling collection centers and offices. In the event of uncertainty, contact the industrial inspectorate, who is responsible for your company or the environmental agency.

APPENDIX A - ABBREVIATIONS

DC	Diagnostic Coverage
EMV	Electromagnetic compatibility (EMC)
EN	European Standard
ESD	Electrostatic sensitive device
EXT, ext	External
FSoE	Functional Safety over EtherCAT
I/O	Input/Output
ISO	International Organzation for Standardization
LED	Light emitting diode
$MTTF_d$	Mean Time To Failure dangerous
PFD	Probability of dangerous Failure on Demand
PFH	Probability of dangerous Failure per Hour
SAF	Safety module
SCA	Safe Cam
SBC	Safe Brake Control
SDI	Safe Direction
SFF	Safe Failure Fraction
SIL	Safety integrity level
SLA	Safely Limited Acceleration
SLI	Safely Limited Increment
SLP	Safely Limited Position
SLS	Safely Limited Speed
SLT	Safely Limited Torque
SOS	Safe Operating Stop
SS1	Safe Stop 1
SS2	Safe Stop 2
SSM	Safe Speed Monitor
STO	Safe Torque Off

APPENDIX B - CHECKLISTS

The use of checklists serves documentation purposes and guides in the implementation of a safety system. The checklists reproduced in this chapter serve to prevent errors and must be processed carefully for every project. It is also required to make copies of the printed checklists.

No claim is made that the checklists are complete. There may be additional requirements depending on the specific plant.

B.1 Planning checklist

Serial No.	Requirement	Fulfilled		Remarks
		Yes	No	
1	Planning			
1.1	Was a risk assessment carried out and were the required SIL and performance levels in accordance with DIN EN ISO 13849-1 or IEC 62061, determined?			
1.2	Are power supplies according to PELV specifications being used exclusively?			
1.3	Is the line routing carried out in accordance with the applicable standards and guidelines and are the fault exclusions considered?			
1.4	Is the electrical supply for the local I/O terminals and field bus components properly dimensioned?			
1.5	Do all safety-oriented system components meet the requirements of the established SIL (IEC 61508), performance levels (DIN EN ISO 13849-1) and safety category for this application?			

Serial No.	Requirement	Fulfilled		Remarks
		Yes	No	
1.6	Does the wiring of the safety components meet the requirements of the previously determined safety classification? (Example: Dual-channel wiring of an emergency stop for SIL 2 application)			
1.7	Do the components meet the environmental conditions prevailing in the application?			
1.8	Does the system fulfill the required type of protection?			
1.9	Is degree of pollution 2 complied with? If required, minimize contamination level by installation or encapsulation. Installation in IP54 according to EN 61800-5-2 D.2 and EN ISO 13849-2 D.5 is required.			
1.10	Has the maximum permissible reaction time of the safety functions been established by means of a risk analysis? (Reaction times of the safety module see ▹C.2.5 Technical data reaction times◃ on page 165)			
1.11	Is the maximum permissible reaction time reached? Has computational evidence been provided?			
1.12	Is the system protected from mechanical overloading?			
1.13	Is the system protected from corrosive substances?			
1.14	Are all specified electrical values of the in- and output terminals observed?			

Date	Name	Signature

B.2 Installation checklist

Serial no.	Requirement	Fulfilled		Remarks
		Yes	No	
2	Installation			
2.1	Has it been ensured that there are no short circuits from the wiring of the input and output terminals?			
2.2	Has it been ensured that the safety switch devices have not been bypassed as a result of wiring errors?			
2.3	Has a wiring inspection in accordance with the installation plan been conducted?			
2.4	Are all connection plugs labeled according to their allocation?			
2.5	Are the connection terminals loaded with the specified clamping torque?			
2.6	(Has it been ensured that the insulation of the lines is not causing any faulty contacts?) Is it ensured, that the insulation of the cables is not damaged?			
2.7	Has the reliability of all terminal connections been tested through mechanical tensile loading?			
2.8	Has a visual inspection of the installed components been conducted?			
2.10	Do the components meet the environmental conditions prevailing in the application?			
2.11	Does the system fulfill the required type of protection?			
2.12	Is degree of pollution 2 complied with?			
2.13	Is the system protected from corrosive substances?			

Date	Name	Signature

B.3 Commissioning and validation checklist

Serial no.	Requirement	Fulfilled		Remarks
		Yes	No	
3	Commissioning			
3.1	Has a complete function test been conducted and documented?			
3.2	Has the operating personnel been instructed in the handling of the module?			
3.3	Are encoders used exclusively which have been certified and/or released by Baumüller?			

Date	Name	Signature

B.4 Modification and retrofitting check list

Serial no.	Requirement	Fulfilled		Remarks
		Yes	No	
4	Modification and retrofitting			
4.1	Is the modification/retrofitting of the system compatible? Are all requirements, which are listed in the check lists on planning, installation and commissioning/validation of this Instruction Manual, fulfilled?			
4.2	Are the calculated reaction times still complied with after the modification/ retrofitting? Proof is required!			
4.3	Has a complete function test been conducted and documented?			

Date	Name	Signature

C

APPENDIX C - TECHNICAL DATA

This appendix contains the technical data for the Safety Module from Baumüller Nürnberg GmbH.

C.1 Connection values

External supply voltage +24 V group 1 / +24 V group 2	The 24 Volt voltage supply range is U_B = 24V -15%/+20%
Potential separation	Separated potentials for group 1 / group 2
Connection cables at connector X1 Safety Module	< 30 m

C.2 Technical Data safe inputs, STO-Inputs and Daisy-Chain-Inputs

Input-sided switch thresholds for voltage and current:

Voltage / Current	Switching Threshold
U high max	30 V
U high min	11 V
U low max	5 V
U low min	-3 V
I high max	15 mA
I high min	2 mA
I low max	15 mA
I low min	not defined

Test pulse length: 800 µs (active only, if in ProSafePara the sensor type „passive“ was parameterized).

C.2.1 Technical data Daisy-Chain-Outputs

Rated output voltage	24 V
Rated output current	50 mA
Proof voltage	60 V
Output type	protected output according to EN 61131-2

Test pulse length: 800 µs (always active)

C.2.2 Technical data safe outputs

Rated output voltage	24 V
Rated output current	500 mA
Required minimum current	50 mA
Proof voltage	60 V
Output type	protected output according to EN 61131-2.

Test pulse length: 800 µs (always active)

C.2.3 Technical data cycle outputs

Rated output voltage	24 V
Rated output current	50 mA
Output type	protected output according to EN 61131-2.

Test pulse length: 800 µs (active, if at least one input was parameterized as "Sensor type passive").

C.2.4 Technical data power outputs

Rated output voltage	24 V / 48 V (for details see Operating Manual b maXX 5000)
Rated output current	4 A
Proof voltage	60 V
Output type	protected output according to EN 61131-2.

Test pulse length: 2800 µs (always active)

C.2.5 Technical data reaction times

The reaction time of the safety module to trigger the IGBT power output element is 8.5 ms at the maximum via safe inputs.

In addition to the module reaction times the reaction times of the power module must also be regarded (refer to the NOTE in the following).

Module reaction time at a limit violation of a

- Safety function according to the position such as SOS, SLP, SCA: Max. 6 ms
- Safety function according to the speed such as SLS, SSM: Max. 8 ms
- Safety function according to the acceleration such as SLA: Max. 10 ms

DANGER!

In addition to the above specified maximum module reaction times of the SAF-002/3 module latency as well as discharge times in the controller and the power unit of the drive of 15.1 ms must be regarded, that can occur between the SAF module and the IGBT level.

Therefore, the total reaction time of the event (such as limit violation due to accelerated safety function) until to the switch-off of the IGBT level of the drive is 10 ms + 15.1 ms = 25.1 ms, at the maximum.

The maximum reaction time of the safety module to STO (Safe Torque Off), if triggering via safe inputs is 7 ms.

If triggering via FSoE, the total reaction time (up to STO) is determined by the FSoE master (times for signal acquisition / logic / FSoE telegram creation / transfer to EtherCAT master), transmission time of the FSoE telegram to the safety module and the reaction time of the safety module.

The safe limits are monitored at activated safety functions (e.g. SLS) directly in the safety module. The reaction time from a limit violation to the safety reaction of the safety module (max. 10 ms) is independent of the type of triggering selected by the user (safe inputs / FSoE).

C.3 Operational conditions

C.3.1 Climatic properties

Environmental conditions	0°C ... 55°C 95% relative humidity, no condensation
Storage conditions	-40°C ... 70°C 95% relative humidity, no condensation
Transport conditions	-40°C ... 70°C 95% relative humidity, no condensation
Installation height	Up to 2000 m above sea level

WARNING!

The operating conditions specified in the table above may not be exceeded at any time.

C.3.2 Mechanical properties

Dimensions (W x H x D)	24 mm x 89 mm x 136 mm
Weight	ca. 122 g
Assembly	In frequency controller of the type b maXX 5000 (see chapter ▹Compatibility list◃ on page 31)
Installation position	Vertical, parallel to the vertically installed frequency controller into which the module is inserted
Protection class	IP 20
Permissible degree of pollution	Pollution degree 2

C.3.3 EMC properties

EMC resistance / emission	In accordance with DIN EN 61800-3 / EN 62061 Annex E /

C.4 Pin assignment of Safety Module connector X1

C.4.1 Standard configuration „Daisy Chain“

- BM5-O-SAF-002-**000**-000
- BM5-O-SAF-003-**000**-000

Pin no.	**Assignment standard (with Daisy Chain)**	Pin no.	**Assignment standard (with Daisy Chain)**
1	+24V2	19	GND24V2
2	STO_IN_2A	20	STO_IN_2B
3	CHAIN_IN_2A	21	CHAIN_IN_2B
4	DIG1_IN_2A	22	DIG1_IN_2B
5	DIG2_IN_2A	23	DIG2_IN_2B
6	CHAIN_OUT_2A	24	CHAIN_OUT_2B
7	DIG3_IN_2A	25	DIG3_IN_2B
8	CLK_OUT_2A	26	CLK_OUT_2B
9	DIG_OUT_2A	27	DIG_OUT_2B
10	DIG_OUT_1A	28	DIG_OUT_1B
11	CLK_OUT_1A	29	CLK_OUT_1B
12	DIG3_IN_1A	30	DIG3_IN_1B
13	CHAIN_OUT_1A	31	CHAIN_OUT_1B
14	DIG2_IN_1A	32	DIG2_IN_1B
15	DIG1_IN_1A	33	DIG1_IN_1B
16	CHAIN_IN_1A	34	CHAIN_IN_1B
17	STO_IN_1A	35	STO_IN_1B
18	+24V1	36	GND24V1

C.4.2 Optional configuration „Separate Grounds“ for operation with SO4000

- BM5-O-SAF-002-**001**-000
- BM5-O-SAF-003-**001**-000

Pin no.	Assignment optional (separate Grounds)	Pin no.	Assignment optional (separate Grounds)
1	+24V2	19	GND24V2
2	STO_IN_2A	20	STO_IN_2B
3	GND_STO_IN_2	21	GND_DIG1_IN_2
4	DIG1_IN_2A	22	DIG1_IN_2B
5	DIG2_IN_2A	23	DIG2_IN_2B
6	GND_DIG2_IN_2	24	GND_DIG3_IN_2
7	DIG3_IN_2A	25	DIG3_IN_2B
8	CLK_OUT_2A	26	CLK_OUT_2B
9	DIG_OUT_2A	27	DIG_OUT_2B
10	DIG_OUT_1A	28	DIG_OUT_1B
11	CLK_OUT_1A	29	CLK_OUT_1B
12	DIG3_IN_1A	30	DIG3_IN_1B
13	GND_DIG2_IN_1	31	GND_DIG3_IN_1
14	DIG2_IN_1A	32	DIG2_IN_1B
15	DIG1_IN_1A	33	DIG1_IN_1B
16	GND_STO_IN_1	34	GND_DIG1_IN_1
17	STO_IN_1A	35	STO_IN_1B
18	+24V1	36	GND24V1

C.5 Examples for connecting the Safety Modules

C.5.1 BM5-O-SAF-00x-000-000 (Daisy Chain, passive input)

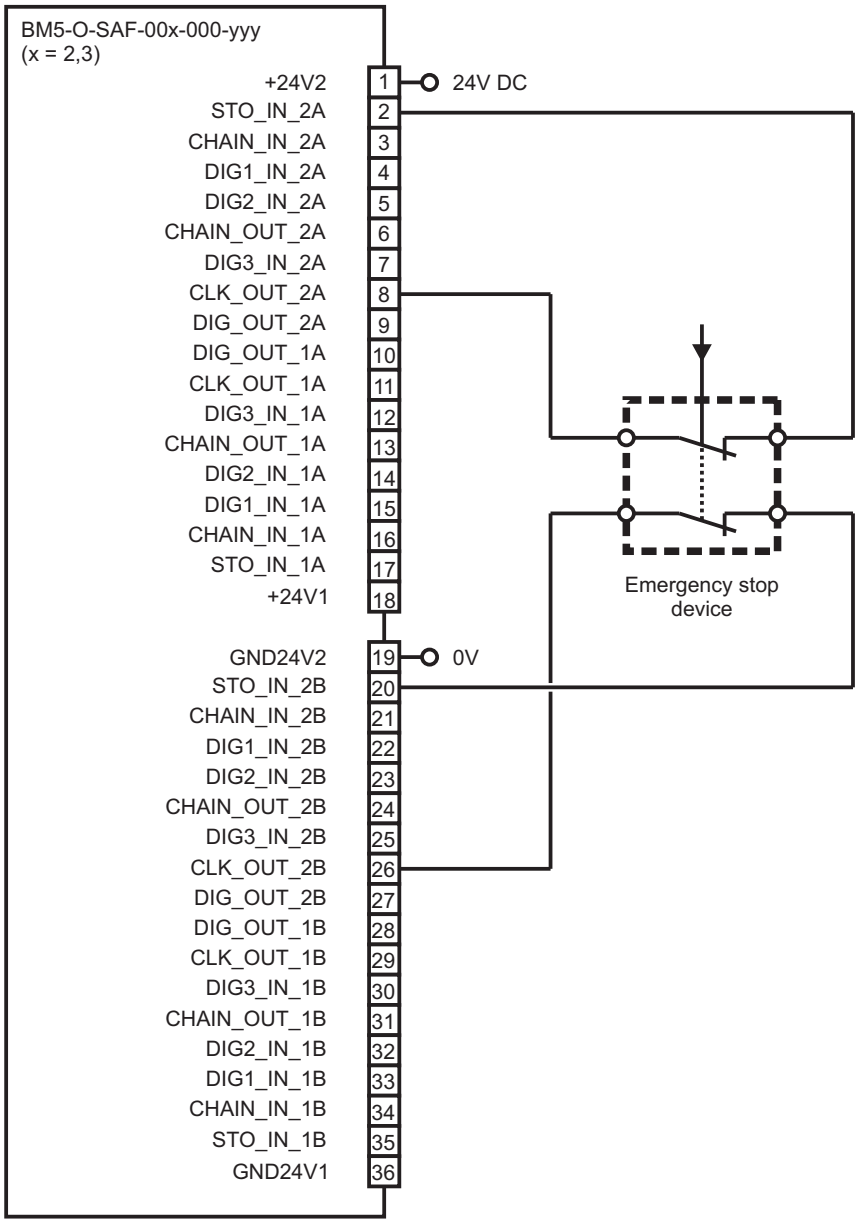


Figure 58: Connection diagram for passive input

C.5.2 BM5-O-SAF-00x-000-000 (Daisy Chain, active input)

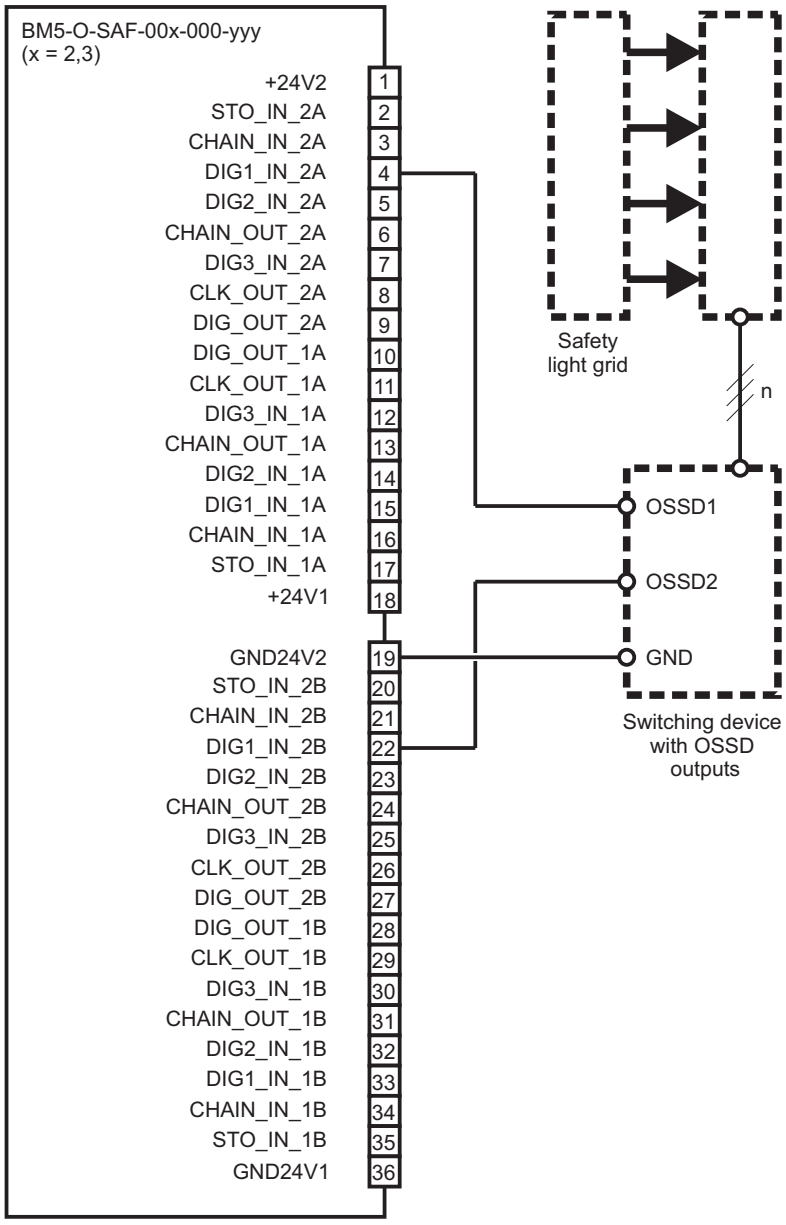


Figure 59: Connection diagram for active input

C.5.3 BM5-O-SAF-00x-001-000 (separate grounds, passive input)

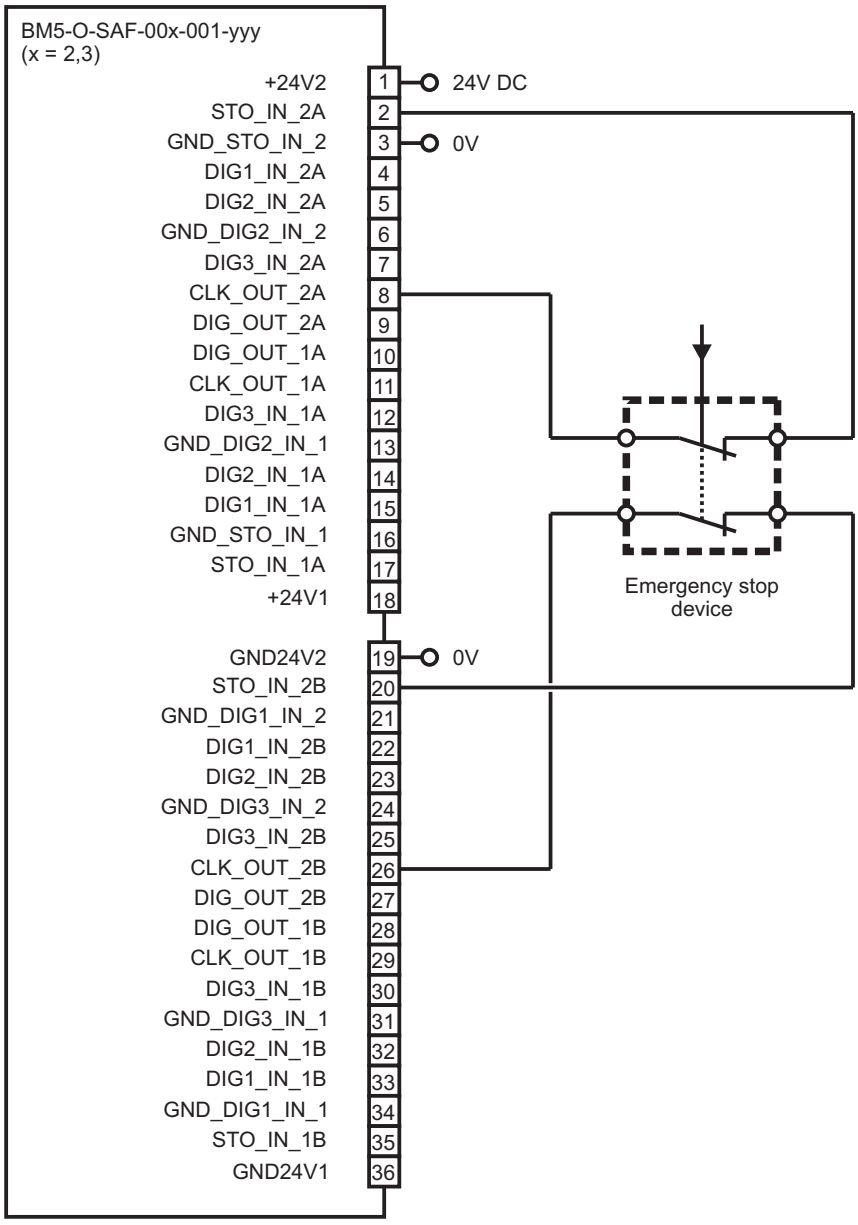


Figure 60: Connection diagram for the passive input

C.5.4 BM5-O-SAF-00x-001-000 (separate grounds, active input)

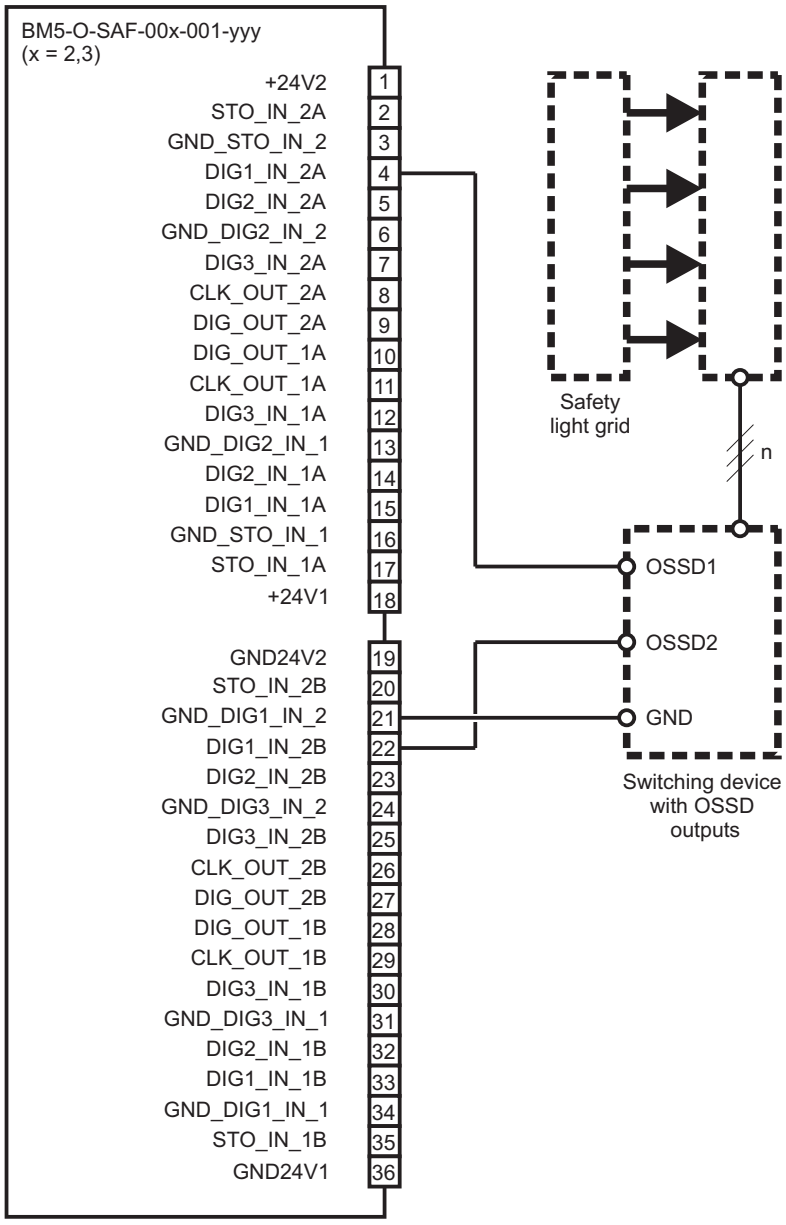


Figure 61: Connection diagram for the active input

C.5.5 BM5-O-SAF-00x-001-000 (separate grounds, with SO4000)

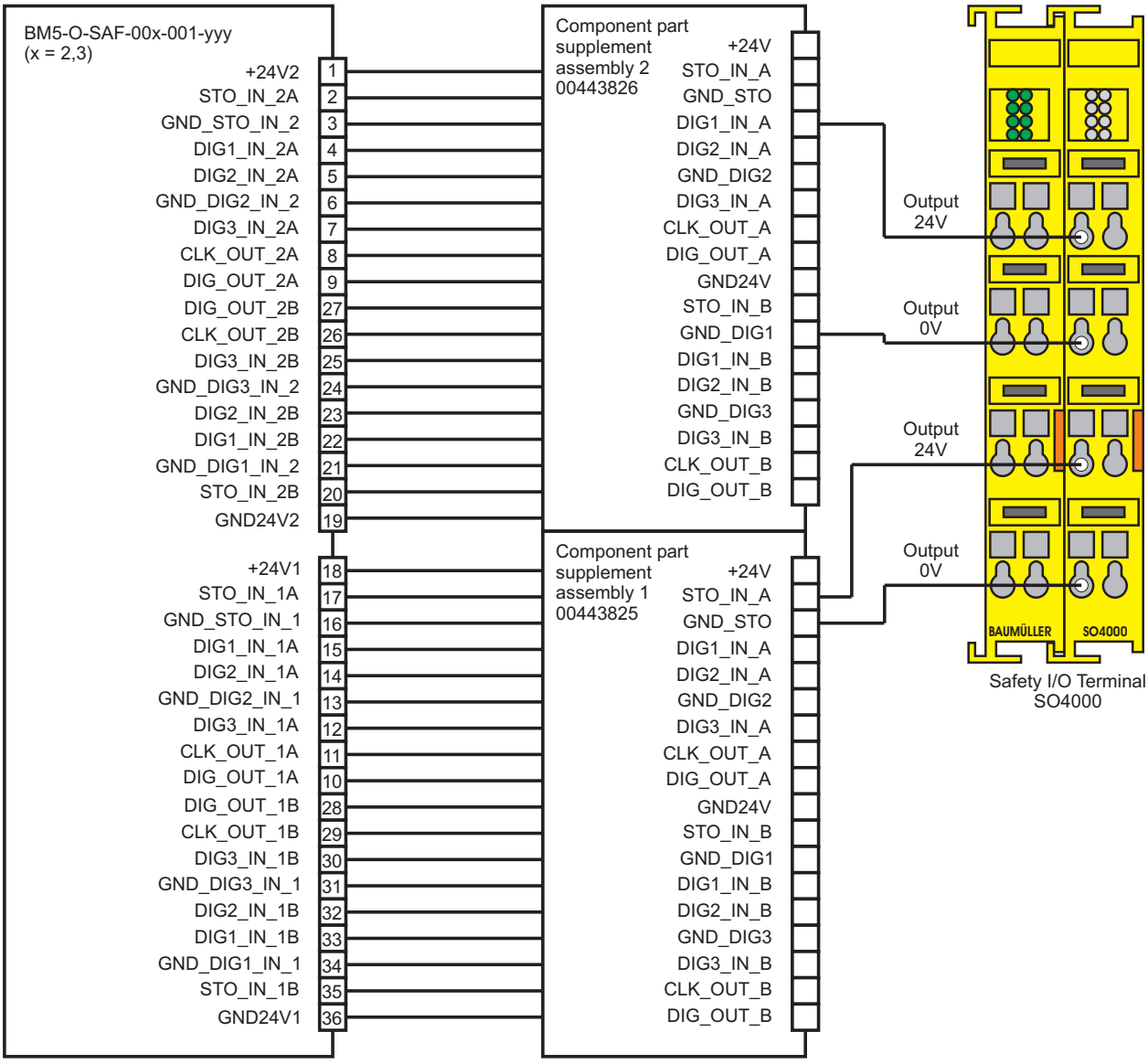


Figure 62: Connection diagram for safety I/O-terminal

C.5.6 Assignment optional supplement

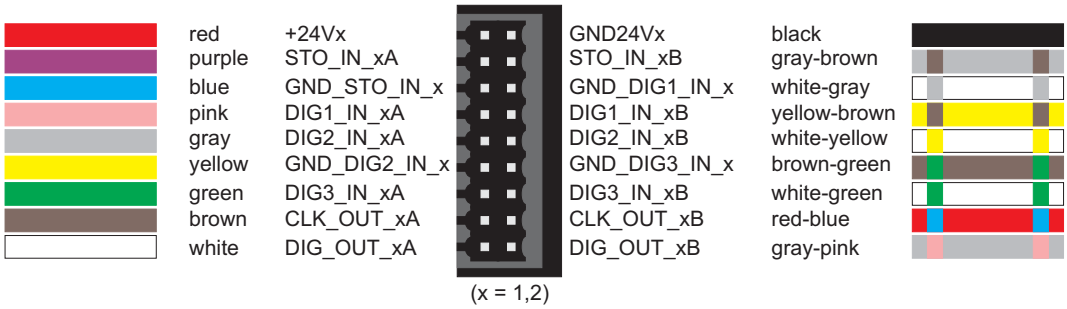
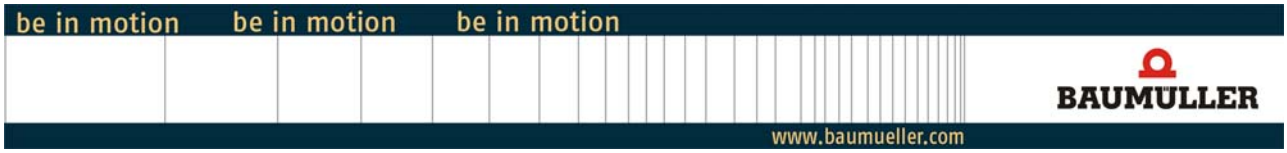


Figure 63: Pin assignment adapter for safety I/O terminal

D

APPENDIX D - DECLARATION OF CONFORMITY



EC - Declaration of Conformity

Doc.-No. **5.12065.01**
Date: **09/13/2018**

according to Machinery Directive 2006/42/EC

The Manufacturer: Baumüller Nürnberg GmbH
Ostendstraße 80-90
90482 Nürnberg, Germany

declares, that the products:

Designation: b maXX 5000 option module with safety functions
Type: BM5-O-SAF-002 and BM5-O-SAF-003
manufactured since: 10/02/2018

are developed, designed and manufactured in accordance with the Machinery Directive 2006/42/EC. These products comply with the requirements of the EMC Directive 2014/30/EU.

Applied harmonised standards:

Standard	Title
IEC 62061:2015 + Corr.1:2015	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
ISO 13849-1:2015	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design
IEC 61800-5-1:2016	Adjustable speed electrical power drive systems. Part 5-1: Safety requirements. Electrical, thermal and energy
IEC 61800-5-2:2016	Adjustable speed electrical power drive systems. Part 5-2: Safety requirements. Functional
IEC 60204-1:2016 (in extracts)	Safety of machinery. Electrical equipment of machines Part 1: General requirements
IEC 61800-3:2017	Adjustable speed electrical power drive systems. Part 3: EMC requirements and specific test methods
IEC 61508 Parts 1-7:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems

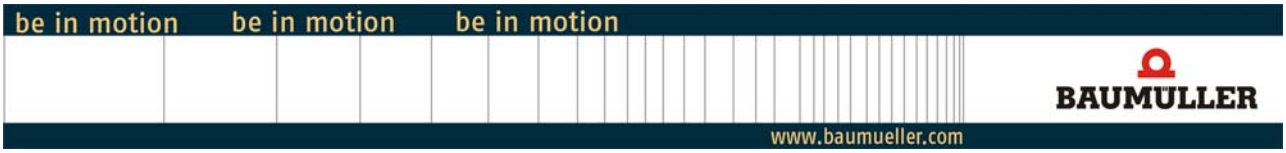
Authorised person to compile the technical files:
Name: Heinrich März, Baumüller Nürnberg GmbH
Adress: Ostendstraße 80-90, 90482 Nürnberg, Germany

Notified body executed the EC type-examination procedures according to Machinery Directive 2006/42/EC:
Name: TÜV Rheinland Industrie Service GmbH
Adress: Am Grauen Stein, 51105 Köln / Germany
Identification number: NB0035
Registration number: 01/205/5261.01/18

Attention should be paid to the safety instructions in the manual. This product is to be used in machinery and must not put into operation until the machinery, into with it is incorporated, has been declared to be in conformity with the Machinery Directive 2006/42/EC.

Nuremberg / 09/13/2018
Location / Date

Subject to change of this declaration of EC conformity without notice. Actual valid edition on request.



EC - Declaration of Conformity

Doc.-No. **5.12065.01**
Date: **09/13/2018**

according to EMC Directive 2014/30/EU

The Manufacturer: Baumüller Nürnberg GmbH
Ostendstraße 80-90
90482 Nürnberg, Germany

declares, that the products:

Designation: b maXX 5000 option module with safety functions
Type: BM5-O-SAF-002 and BM5-O-SAF-003

manufactured since: 10/02/2018

are developed, designed and manufactured in accordance with the EMC Directive 2014/30/EU.

Applied harmonised standards:

Standard	Title
IEC 61800-3:2017	Adjustable speed electrical power drive systems Part 3: EMC requirements and specific test methods

Attention should be paid to the safety instructions in the manual.

Nuremberg / 09/13/2018
Location / Date

Subject to change of this declaration of EC conformity without notice. Actual valid edition on request.

Index

be in motion

Baumüller Nürnberg GmbH Ostendstraße 80-90 90482 Nürnberg Tel: +49(0)911-5432-0 Fax: +49(0)911-5432-130 **www.baumueller.de**