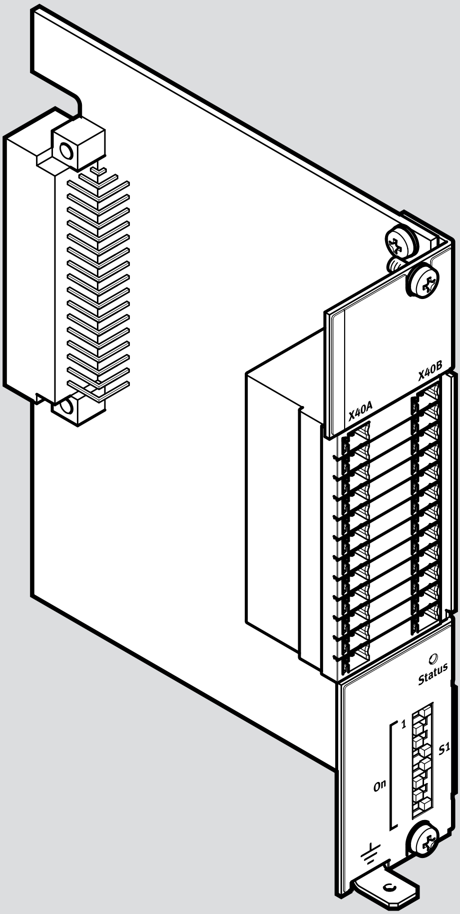
CAMC-G-S3
Safety module



FESTO

Manual | Advanced Safety, Safety function, STO, SS1, SS2, SOS, SBC, SLS, SSR, SSM

8219400

8219400
2024-07c
[8219402]

Original instructions

Table of contents

1 About this document

Notes regarding this documentation

This documentation is intended to ensure safe working in accordance with EN 61800-5-2 by using the safety module CAMC-G-S3 for the motor controllers CMMP-AS-...-M3 with the following safety functions:

– STO – Safe Torque Off
– SS1 – Safe Stop 1
– SS2 – Safe Stop 2
– SOS – Safe Operating Stop
– SLS – Safely Limited Speed
– SSR - Safe Speed Range
– SSM - Safe Speed Monitor
– SBC – Safe Brake Control

- In addition, always observe the general safety regulations for the motor controller CMMP-AS-...-M3.

ⓘ

The general safety regulations for the CMMP-AS-...-M3 can be found in the "Mounting and installation" hardware description, GDCP-CMMP-M3-HW-... ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M3.

Observe the information regarding safety and the requirements for product use in ➔ 2.2 Requirements for product use.

Product identification

ⓘ

This documentation refers to the following versions:

- Safety module CAMC-G-S3, from revision 03 (overall revision 1.4)
- Motor controller CMMP-AS-...-M3 with firmware from version 4.0.1501.2.1 and hardware version from 6.0 (CMMP-AS-C2-3A-M3, CMMP-AS-C5-3A-M3) or from 4.1 (CMMP-AS-C5-11A-P3-M3, CMMP-AS-C10-11A-P3-M3)
- FCT plug-in CMMP-AS from version 2.14.1.x with SafetyTool from version 1.0.5.x

These are the first available and/or supported versions. For newer versions or when replacing the safety module, check that the versions are compatible ➔ Documentation for the version in use.

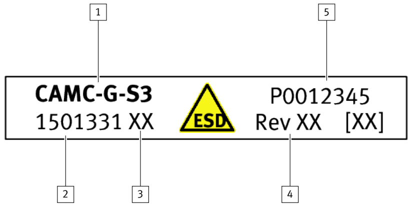


Fig. 1: Rating plate CAMC-G-S3 (example)

1	Order code (order reference)
2	Part number of the safety module CAMC-G-S3
3	Two-digit code for unique identification of the manufacturing period (enables traceability of the product)
4	Module revision (overall revision, i.e. combination of hardware and firmware status)
5	Serial number (enables traceability of the product)

Service

Contact the regional Festo contact if you have any technical problems.

Version of the specified standards

Version	
EN 61326-3-1:2008	EN ISO 13849-1:2015
EN 61800-3:2018	EN ISO 13849-2:2012
EN 61800-5-1:2007 + A1:2017	EN 62061:2005 + AC:2010 + A1:2013 + A2:2015
EN 61800-5-2:2017	IEC 61508-1/.../-7:2010

Tab. 1: Standards specified in the document

Documentation

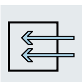
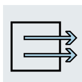
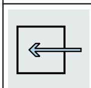
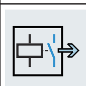
See the following documents for information on the motor controller:

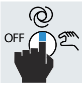
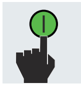
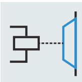
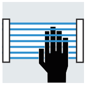
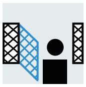
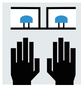
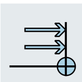
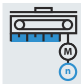
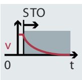
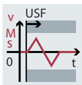
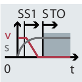
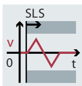
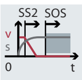
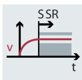
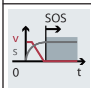
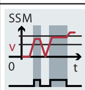
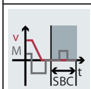
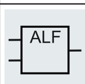
User documentation for the motor controller CMMP-AS-...-M3	
Name, type	Table of contents
Description of hardware, GDCP-CMMP-M3-HW-...	Mounting and installation of motor controller CMMP-AS-...**-M3** for all variants/performance classes (1-phase, 3-phase), pin assignments, error messages, maintenance.
Description of functions, GDCP-CMMP-M3-FW-...	Functional description (firmware) CMMP-AS-...**-M3**, notes for commissioning.
Description FHPP, GDCP-CMMP-M3/-M0-C-HP-...	Control and parameterisation of the motor controller via the Festo FHPP profile. Motor controller CMMP-AS-...**-M3** with the following fieldbuses: CANopen, PROFINET, PROFIBUS, EtherNet/IP, DeviceNet, EtherCAT. Motor controller CMMP-AS-...**-M0** with fieldbus CANopen.

User documentation for the motor controller CMMP-AS-...-M3	
Name, type	Table of contents
Description of CiA 402 (DS 402), GDCP-CMMP-M3/-M0-C-CO-...	Control and parameterisation of the motor controller via the device profile CiA 402 (DS402) motor controller CMMP-AS-...**-M3** with the following fieldbuses: CANopen and EtherCAT. Motor controller CMMP-AS-...**-M0** with fieldbus CANopen.
Description of CAM editor, P.BE-CMMP-CAM-SW-...	Cam disc functions (CAM) of the motor controller CMMP-AS-...**-M3**/**-M0**.
Description of safety module, GDCP-CAMC-G-S1-...	Functional safety engineering for the motor controller CMMP-AS-..**-M3** with the STO safety function.
Description of safety module, GDCP-CAMC-G-S3-...	Functional safety engineering for the motor controller CMMP-AS-...**-M3** with the STO, SS1, SS2, SOS, SLS, SSR, SSM, SBC safety functions.
Description of replacement and project conversion for GDCP-CMMP-M3-RP-...	Motor controller CMMP-AS-...**-M3** as replacement device for previous motor controller CMMP-AS. Changes to the electrical installation and description of project conversion.
Help for the FCT CMMP-AS plug-in	User interface and functions of the CMMP-AS plug-in for the Festo Configuration Tool. ➔ www.festo.com
SafetyTool Help	User interface and functions of the SafetyTool for parameterisation of the safety module CAMC-G-S3.

Tab. 2: Documentation for the motor controller CMMP-AS-...-M3

All available documents for the product ➔ www.festo.com/sp.

Symbols used for safety engineering	
Inputs and outputs	
 Input, two-channel	 Output, two-channel
 Input, single-channel	 Relay output

Symbols used for safety engineering			
Sensor types			
	Mode selector switch		Start button
	Holding brake		Exit safety function (restart)
	Light curtain		Door lock/protective hood
	Emergency stop switch		Enabling button
	Acknowledgement		Two-hand control unit
	Reliable reference switch		Position encoders
Safety functions			
	STO – Safe Torque Off		USF – Universal Safety Function
	SS1 – Safe Stop 1		SLS – Safely Limited Speed
	SS2 – Safe Stop 2		SSR - Safe Speed Range
	SOS – Safe Operating Stop		SSM - Safe Speed Monitor
	SBC – Safe Brake Control		ALF – Additional Logic Function, not a safety function

Tab. 3: Safety engineering symbols

2 Safety and requirements for product use

2.1 Safety

2.1.1 General safety instructions

– In addition, always observe the general safety regulations for the motor controller CMMP-AS-...-M3.

ⓘ

The general safety regulations for the CMMP-AS-...-M3 can be found in the hardware description, GDCP-CMMP-M3-HW-... ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M3.

NOTICE

Loss of the safety function.

The safety function may fail if you do not comply with the conditions required for the surroundings and connections.

- Comply with the specified ambient and connection conditions, in particular the input voltage tolerances ➔ 8.1 Technical data.

NOTICE

Incorrect handling may damage the safety module or motor controller.

- Switch off the power supply before mounting and installation work. Do not switch on the supply voltages until mounting and installation work is completely finished.
- Never unplug the safety module from or plug it into the motor controller when powered!
- Comply with the handling specifications for electrostatically sensitive components.

2.1.2 Intended use

The safety module CAMC-G-S3 is an extension of the motor controller CMMP-AS-...-M3 for implementation of the safety function:

– STO – Safe Torque Off
– SS1 – Safe Stop 1
– SS2 – Safe Stop 2
– SOS – Safe Operating Stop
– SLS – Safely Limited Speed
– SSR - Safe Speed Range
– SSM - Safe Speed Monitor
– SBC – Safe Brake Control

When suitable position sensors are used and with suitable control of the safety module, the requirements are fulfilled in accordance with EN 61800-5-2 up to and including SIL3 and in accordance with EN ISO 13849-1 up to and including category 4/PL e.

The achievable safety level depends on the other components used to implement a safety function, e.g. on the encoders used for position detection ➔ 2.1.4 Achievable safety level/safety function in accordance with EN ISO 13849-1/EN 61800-5-2.

The motor controller CMMP-AS-...-M3 with safety module CAMC-G-S3 is a product with safety-related functions and intended for installation in machines or automation systems and is to be used exclusively:

– in excellent technical condition
– in its original condition, without unauthorised modifications
– within the limits of the product defined by the technical data ➔ 8.1 Technical data
– in an industrial environment

The safety module CAMC-G-S3 can be operated in all motor controllers CMMP-AS-...-M3 that have the Ext3 slot for safety engineering. It cannot be plugged into one of the Ext1 or Ext2 slots for interfaces.

NOTICE

In the event of damage caused by unauthorised manipulation or use other than the intended use, the guarantee will be invalidated and the manufacturer will not be liable for damages.

2.1.3 Foreseeable misuse

The following are examples of foreseeable misuse and are not approved as intended use:
– use in a device other than the CMMP-AS-...-M3
– outdoor use
– use in non-industrial areas (residential areas)
– use outside the limits of the product defined in the technical data
– unauthorised modifications

NOTICE

- The STO function is not adequate as the sole safety function for drives subject to continuous torque (e.g. with suspended loads). Additional appropriate measures are required as a safeguard, e.g. a clamping unit.
- Safety devices must not be bypassed.
- Repairs to the safety module are prohibited! Professional replacement of the safety module is permissible.

ⓘ

The STO (Safe Torque Off) function does not provide protection against electric shock, only against dangerous movements! The drive is not disconnected from the power supply as required for electrical safety ➔ Hardware description, GDCP-CMMP-M3-HW-...

2.1.4 Achievable safety level/safety function in accordance with EN ISO 13849-1/EN 61800-5-2

The safety module fulfils the basic test requirements of:
– category 4, PL e in accordance with EN ISO 13849-1
– SIL CL 3 in accordance with EN 62061

The safety module can be used in applications up to Cat. 4 / PL e to EN ISO 13849-1 and to SIL 3 to EN 62061 / IEC 61508.
The achievable safety level depends on the other components used to implement a safety function.

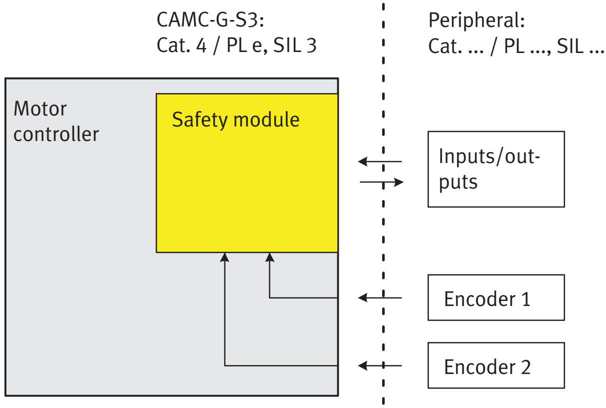


Fig. 2: Safety level CAMC-G-S3 and overall system

ⓘ

Take into account the approved combinations of position encoders along with the corresponding notes ➔ Tab. 11 Permissible combinations of position encoders.
Information on the characteristic safety values for the different safety functions that can be achieved with the corresponding peripherals ➔ 8.2 Safety reference data.

2.2 Requirements for product use

- Make the complete documentation available to the design engineer, installer and personnel responsible for commissioning the machine or system in which this product is used.
- Make sure that the specifications in the documentation are observed at all times. When so doing, also take into account the documentation for the other components and modules (e.g. motor controller, cables etc.).
- Take into account the legal regulations applicable for the location as well as:
  - Instructions and standards,
  - Regulations of testing organisations and insurers,
  - national specifications.
- The safety module fulfils the requirements of EN 61800-5-2. Additional instructions, standards and directives apply to the other safety devices used in the machine and their use, and must also be taken into account.
- For emergency stop applications, protection from automatic restart corresponding to the required category must be planned. This can be achieved, for example, with an external safety relay unit or suitable parameterisation of the safety module CAMC-G-S3 ➔ 3.7 Terminate safety functions.

2.2.1 Technical prerequisites

General information on correct and safe use of the product, which must be observed at all times:
- Comply with the connection and ambient conditions for the safety module (➔ 8.1 Technical data), motor controller and all connected components as specified in the technical data.

Only compliance with the limit values and/or load limits will enable operation of the product in accordance with the relevant safety directives.

- Observe the notes and warnings in this documentation.

2.2.2 Qualification of the specialist technicians (requirements for staff)

The device may only be set into operation by a qualified electrical technician who is familiar with:

- the installation and operation of electrical control systems,
- the applicable instructions for operating safety engineering systems,
- the applicable instructions for accident prevention and occupational safety and
- the documentation for the product.

2.2.3 Diagnostic coverage (DC)

Diagnostic coverage depends on the integration of the motor controller with safety module into the control loop system, the motors/position encoders used and the measures implemented for diagnostics.

If a malfunction is detected during the diagnostics, appropriate measures must be implemented to maintain the safety level.

NOTICE

The reaction of the safety module to detected faults can be parameterised accordingly, e.g. activation of the safety functions SS1 and SBC if there is a cross circuit of safe input signals.

NOTICE

Check whether detection of shorts across contacts of the input circuit and the connection wiring is required in your application.

If needed, use a safety relay unit with detection of shorts across contacts to control the safety module or use the safe outputs of the safety module to supply passive switching devices together with the corresponding monitoring functions for the safe inputs.

2.2.4 Range of application and approvals

The motor controller with integrated safety module is a safety device. For details of the safety-oriented standards and test values that the product complies with and fulfils, see ➔ 8.1 Technical data.

The product-relevant directives are listed in the declaration of conformity ➔ www.festo.com/sp.

Product conformity	
CE	in accordance with EU EMC Directive in accordance with EU Machinery Directive in accordance with EU RoHS Directive
UKCA	to UK EMC Regulations to UK Supply of Machinery Regulations to UK RoHS Regulations

Tab. 4: Product conformity

3 Product description of safety module CAMC-G-S3

3.1 Product overview

3.1.1 Purpose

As processes become increasingly automated, protecting people from potentially hazardous movements is becoming ever more relevant. Functional safety refers to measures required of electrical or electronic equipment to reduce or eliminate dangers due to malfunctions. In normal operation, protective devices prevent human access to hazard zones. In certain operating modes, e.g. during set-up, people need to have access to danger zones. In such situations, the operator must be protected by measures incorporated into the drive and control system.
The functional safety engineering integrated into the motor controller CMMP-AS-...-M3 by means of the safety module CAMC-G-S3 meets the requirements for optimised implementation of protective functions in the controller and drive. The complexity of planning and installation is reduced. The use of integrated functional safety engineering provides improved machine functionality and better availability compared to the levels achieved by conventional safety engineering.
The motor controllers of the CMMP-AS-...-M3 series can be fitted with plug-in modules for integrated functional safety engineering. The following modules are available:

Type	Description
CAMC-DS-M1	Switch module with DIL switches, no safety function.
CAMC-G-S1	Safety module with DIL switches and STO function.
CAMC-G-S3	Safety module with the STO, SS1, SS2, SOS, SBC, SLS, SSR, SSM functions and DIL switches.

Tab. 5: Overview of safety and switch modules for the CMMP-AS-...-M3

3.1.2 Performance characteristics

The safety module CAMC-G-S3 has the following performance characteristics:
- Achieving one or more of the safety functions:
  - STO – Safe Torque Off
  - SS1 – Safe Stop 1
  - SS2 – Safe Stop 2
  - SOS – Safe Operating Stop
  - SLS – Safely Limited Speed
  - SSR - Safe Speed Range
  - SSM - Safe Speed Monitor
  - SBC – Safe Brake Control
- two-channel and single-channel inputs to request the safety functions
- two-channel safe outputs to control additional safety elements and functions
- potential-free feedback contact for the operating status
- designed as a plug-in module that can be retrofitted by plugging it in from the outside.

The integrated safety functions in the motor controller enable:
- shortest reaction times by faster detection of potentially hazardous states
- comprehensive detection of hazards by fast, direct access to a wide range of signals and measured variables in the motor controller
- evaluation of a wide range of position sensors, e.g. resolver, SIN/COS encoder, Hiperface encoder, and the evaluation of position sensors with purely serial protocols (EnDat 2.2, BiSS, etc.)
- if necessary, fast, direct access to the setpoint values/controller of the servo drive. An axis can also be safety and precisely stopped or braked to a limited speed without action by the function controller/PLC.
- direct interaction between the sequence control in the motor controller and the safety module. For example, the clamping unit or holding brake, after a request for the SBC safety function and the subsequent restart, is only opened when the motor controller is again actively controlling the position. This prevents vertical axes from “dropping” and eliminates the need to program a sequence in the function controller.

3.1.3 Supported devices

The safety module CAMC-G-S3 can only be used in motor controllers of the type CMMP-AS-...-M3 with the corresponding hardware and firmware version ➔ 1 About this document.

ⓘ

The motor controllers CMMP-AS-...-M3 are supplied without a safety module or switch module in the Ext3 slot for safety modules:
- If a safety function is not required, the switch module CAMC-DS-M1 must be ordered and installed in the Ext3 slot.
- The safety module CAMC-G-S3 must be mounted in the Ext3 slot to achieve the safety function for safety-related motion monitoring and motion control described in this documentation.

3.1.4 Operating elements and connections

The safety module CAMC-G-S3 has the following control components, connections and display components:

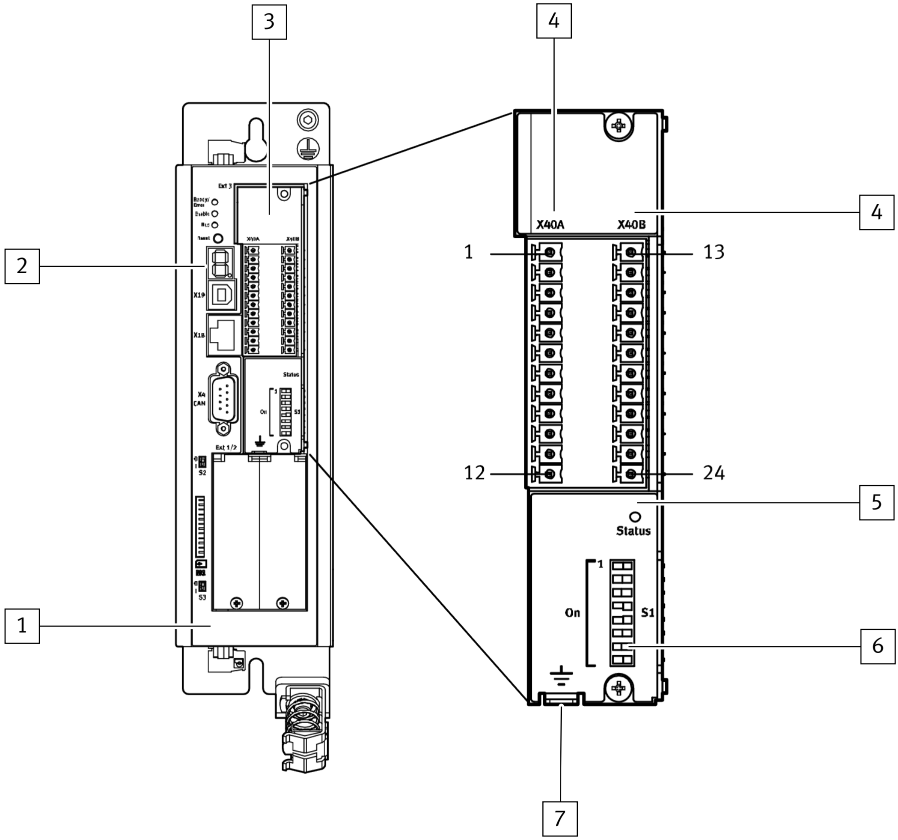


Fig. 3: Control section and connections CAMC-G-S3

1	Motor controller CMMP-AS-...-M3 with slot Ext3
2	7-segment display of the motor controller, for displaying the active safety function or error messages of the safety module
3	Safety module CAMC-G-S3
4	I/O interface [X40A] and [X40B] for controlling the safety functions
5	LED for display of the operating status (status of functional safety)
6	DIL switch (activation/configuration of fieldbus communication in the motor controller)
7	Functional earth connection (flat plug 6.3 mm)

3.1.5 Scope of delivery

Safety module CAMC-G-S3	
Safety module with mounting accessories (2 screws with split washer)	Module for safety functions STO, SS1, SS2, SOS, SLS, SSR, SSM, SBC
2 plugs for I/O interface [X40A], [X40B] (also available separately as an assortment of plugs NEKM-C-9)	PHOENIX CONTACT MiniCombicon MC1.5_12ST-3.81-BK
Instruction manual for the safety module	Brief overview of the function, assembly and installation of the safety module

Tab. 6: Scope of delivery

3.2 Function and application

3.2.1 System overview

The following figure shows a typical drive system with integrated functional safety engineering, comprising the following components:

- Motor controller CMMP-AS-...-M3
- Safety module CAMC-G-S3
- Synchronous servo motor, e.g. from the Festo EMMS-AS or EMME-AS series
- Linear axis with second measuring system, e.g. Festo EGC-...-M...
- Safe clamping unit

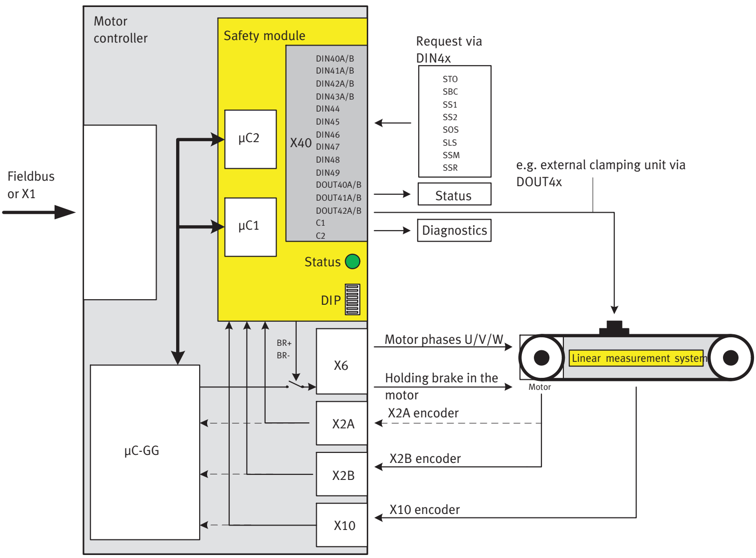


Fig. 4: Safety module functional principle

The drive control and the functional control of the movement axis are optionally controlled via:
- the motor controller CMMP-AS-...-M3 and the assigned control interface, e.g. [X1]
- a fieldbus

The safety module monitors the function of the motor controller servo drive. This function requires recording of the safety-relevant variables of the motion of the motor and monitoring them according to the selected safety functions.
Example: if the safety limits are violated by exceeding a maximum permissible speed, the safety module can safely switch off the driver power supply for the power semiconductor, thus preventing the power output stage from supplying the power required by the motor.

NOTICE

Technical failure or failure of the power supply will lead to a shutdown of the power output stage of the motor controller. Safety limitations could be the result, depending on the application.

The safety module monitors the safety of the axis as follows:
- In the CAMC-G-S3, two micro controllers operate in a redundant structure. During operation, they continuously compare all relevant input and output signals as well as the data of the position encoders.
- The safety functions in the CAMC-G-S3 are requested or activated via the digital safe inputs on the safety module, by other safety functions or as an error response. Logic operations can be used to set which digital inputs in which signal combination request a safety function.
- As soon as a safety function is active, safe monitoring of the status of the basic unit and axis takes place.
- The safety module detects the movement of the axis (position, speed) via the position encoder in the motor and, depending on the system structure, also via a second measuring system.
- The position sensors are connected to [X2A], [X2B] and [X10] on the basic unit for this purpose. The signals are forwarded internally to the safety module.

Important: the second measuring system on the axis may be essential, depending on the requested safety classification and the axis configuration.

- If the axis is in the safe state, the safety function reports the status SSR, “Safe State Reached”. If the safety conditions are violated, the safety function reports the status SCV “Safety Condition Violated”.
- The safe digital outputs report the safety status externally, e.g. to an external safety controller, to another CAMC-G-S3 or to digital inputs for supply of test pulses.
- The safety module uses an internal device path to control the brake control output at the motor connection [X6], thus enabling the safety function SBC in combination with an appropriately certified clamping unit.
- An external clamping unit can also be activated via a safe digital output and an external safe switching device.

ℹ

Important: to use the safety function SBC, a clamping unit with corresponding safety classification must be used. In principle, a risk assessment must be carried out for all types of holding brakes or clamping units without certification, and the suitability for the relevant safety-related application must be specified. Otherwise they must not be used. The holding brake in motors is not usually appropriately qualified and is thus not suitable.

- A potential-free signal contact is available for diagnostic purposes.
- The operating status of the safety module is displayed by a status LED and the 7-segment display of the basic unit.

Data is exchanged between the safety module and the basic unit via an internal communications interface.

- This means that the basic unit is always aware of the current operating status of the safety module, e.g. whether a safety function is requested and executed, or whether a violation of a safety condition is detected.
- This means that the operating status of the safety engineering can be reported to the function controller via the various fieldbus interfaces.
- The safety module can actively manipulate the controller of the basic unit without having to go through the function controller. For example, the drive can be decelerated actively to zero speed when safety function SS2 is requested

ℹ

Important: this function is primarily beneficial when individual axes are moved. However, if the axis is moved in an interpolating operating mode (e.g. CAN interpolated position mode), this function is not really useful.

Additional functions of the firmware in the safety module:
- safe switch-off of the motor controller in case of error, variable reaction to different errors.
- evaluation of the signals of the safe inputs, monitoring of the correct function of the hardware (test pulses).
- control of the safe outputs, monitoring the correct function of the hardware.
- safe monitoring of the correct function of the micro controllers: cyclical test of memory (RAM, flash) and CPU
- monitoring supply voltages
- cross-monitoring of the two micro controllers
- management of the parameter sets, implementation of a safe parameterisation secured with check sums and a password

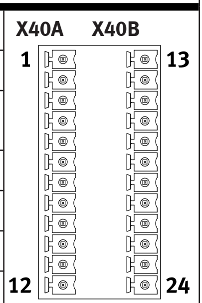
3.2.2 Circuitry of the safety module [X40]

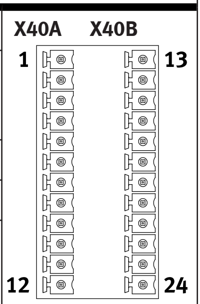
The safety module has a 24-pin interface [X40A/B] with the following connections for the circuitry of the safety functions:
- 4 digital two-channel sensor inputs with configurable allocation (SIL3 inputs),
- 6 digital single-channel inputs with configurable allocation (max. SIL2 inputs), e.g. as
  - 1 digital 3-pole mode selector switch
  - 1 input for error acknowledgement

  - 1 input for terminating the request of a safety function
  - 1 input for a feedback signal of an external clamping unit
- 3 digital two-channel outputs (SIL3) with configurable allocation, optionally useable as clock output
- 1 feedback contact (relay contact) for diagnostic purposes
- reference potential for all inputs and outputs
- a 24 V auxiliary power supply for connected sensors

The following table shows the connections sorted by functions (pin allocation according to pin number ➔ 4.2 Electrical installation).

Designation	Description (factory setting[1])	Pin, plug
Digital inputs		
DIN40A	Digital input 40, two-channel (factory setting: emergency stop switching device, STO and SBC request)	X40A.1
DIN40B		X40A.2
DIN41A	Digital input 41, two-channel	X40B.13
DIN41B		X40B.14
DIN42A	Digital input 42, two-channel	X40A.3
DIN42B		X40A.4
DIN43A	Digital input 43, two-channel	X40B.15
DIN43B		X40B.16
DIN44	Digital input 44 (factory setting: brake activation feedback)	X40A.7
DIN45	Digital inputs 45, 46, 47 (factory setting: mode selector switch)	X40A.8
DIN46		X40A.9
DIN47		X40A.10
DIN48	Digital input 48 (factory setting: error acknowledgement)	X40A.11
DIN49	Digital input 49 (factory setting: terminate safety function on rising edge)	X40A.12
Digital outputs and signal contact		
DOUT40A	Digital output 40, two-channel	X40A.5
DOUT40B		X40A.6
DOUT41A	Digital output 41, two-channel	X40B.17
DOUT41B		X40B.18
DOUT42A	Digital output 42, two-channel	X40B.19
DOUT42B		X40B.20



Designation	Description (factory setting[1])	Pin, plug	
C1)	Signal contact, relay contacts (factory setting: safe state reached, no safety condition violated) – Open: “safety functions not active” – Closed: “safety functions active”	X40B.21	
C2)		X40B.22	
Reference potential and auxiliary power supply			
GND24	0 V, reference potential for DINx/DOUTx/+24 V	X40B.23	
+24 V	24 V output, auxiliary power supply, e.g. for safety peripherals (24 V DC logic supply of the motor controller)	X40B.24	

1) Function when the device is delivered or after resetting to factory settings (advance parameterisation)

Tab. 7: Digital inputs and outputs, signal contact, reference potential and auxiliary power supply [X40]

3.2.3 Overview of the supported safety functions

The safety module supports the following safe stop/movement functions:

Function	Number	Comment	
STO	1	Uncontrolled stopping, safe restart interlock	
SS1	1	Controlled stopping with subsequent STO	
SS2	1	Controlled stopping with subsequent SOS	
SOS	1	Safe stop (with “fine rotational speed limit”[1])	
USF	4	"Universal Safety Function", combined safety functions. The following safety functions can be implemented with appropriate parameterisation in the “Safe Speed Function” (SSF) version:	
		SLS	Safely Limited Speed
		SSR	Safe Speed Range
		SSM	Safely Monitored Speed
SBC	1	Safe Brake Control	

1) A slow movement within the monitored position window can be permissible.

Tab. 8: Equipment of the safety module

Detailed information ➔ 3.5 Safety functions.

3.2.4 Functional diagram of the safety module

The functions of the safety module are explained using the following functional diagram:

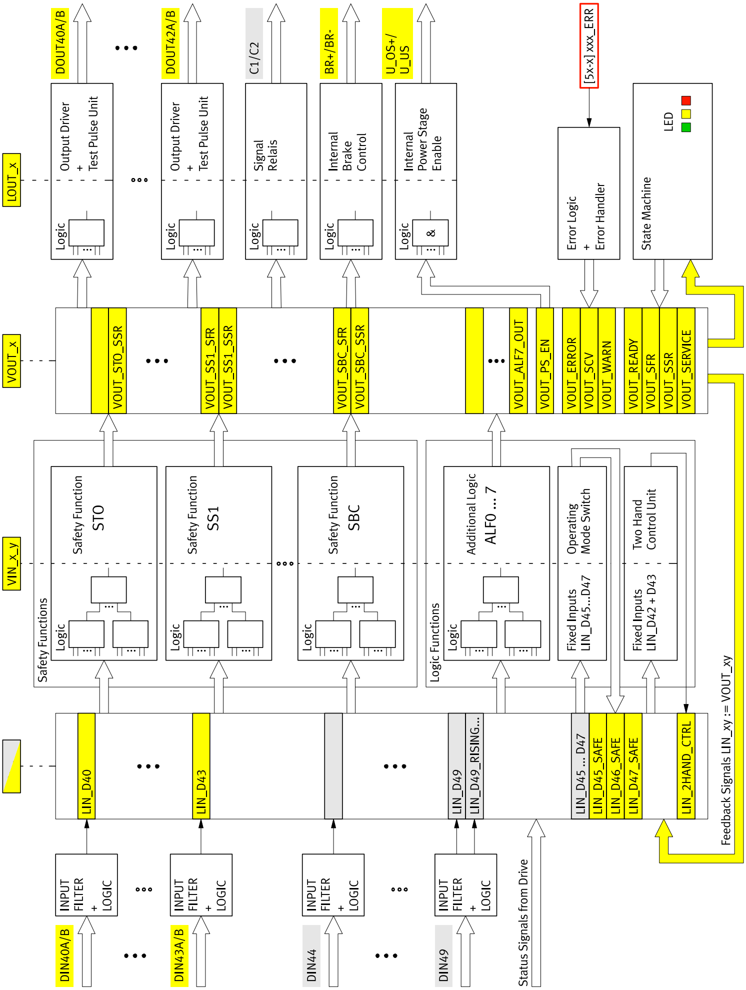


Fig. 5: Safety module functional diagram

Term/abbreviation	Explanation
DIN40A/B ... DIN43A/B	Two-channel digital inputs
DIN44 ... DIN49	Single-channel digital inputs
INPUT FILTER + LOGIC	Input filter and input logic
Status Signals from Drive	Status signals from drive
LIN_x	Logical inputs

Term/abbreviation	Explanation
VIN_x_y	Virtual inputs
Safety Functions	Safety functions
Logic	Logic, configurable for the safety functions using product terms
Safety Function STO, SS1, ...	Safety function STO, SS1, ...
Logic Functions	Logic functions
Additional Logic ALF...	Advanced logic functions ALF...
Fixed Inputs LIN_...	Permanently assigned logical inputs LIN_...
Operating Mode Switch	Mode selector switch
Two Hand Control Unit	Two-hand operator unit
VOUT_x	Virtual outputs
LOUT_x	Logical outputs
Output Driver + Test Pulse Unit	Output drive and test pulse generation
DOUT40A/B ... DOUT42A/B	Two-channel digital outputs
Signal relay	Signal contact
C1/C2	Pins C1/C2 of the signal contact
Internal Brake Control	Internal brake control
BR+/BR-	Pins BR+/BR- of the internal brake control
Internal Power Stage Enable	Internal power stage enable
U_OS+/U_OS-	Pins U_OS+/U_OS- of the internal power stage enable
Error Logic + Error Handler	Error logic and error handling
[5x-x] xxx_ERR	Internal error signal, error 5x-x
State Machine	State machine
Feedback Signals LIN_xy := VOUT_xy	Feedback of the signals LIN_xy := VOUT_xy

Tab. 9: Legend for safety module functional diagram

ⓘ

The digital inputs of the interface [X40] are shown on the far left in the functional diagram and the digital outputs on the far right. Between them is a structure with logic blocks and the safety functions. The following general rule applies in the functional diagram and in the other block diagrams:

- All safe signals are highlighted in yellow in the functional diagram and in the other block diagrams.
- Potentially unsafe signals have a grey background.

Input filters and logical inputs:

The digital input signals at [X40] are initially filtered in the “Input Filter + Logic” function block. The block also checks whether test pulses exist on the input signals and whether they are plausible. In the case of two-channel inputs, a test is carried out of whether the input level corresponds to the configured input type (equivalent/antivalent switching) and whether the signals switch at the same time.

The logic states of the input signals are mapped as a result of these checks. Input signals are identified in the block diagram with ‹LIN_x "Logic Inputs"›. Example: the LIN_D40 signal maps the logical switching status of the two-channel input DIN40.

List of logical inputs ➔ Tab. 185 Logical inputs, level assignment to the physical inputs.

Safety functions:

The safety functions have uniform characteristics. A configurable logic function defines which logical input signals (local inputs, LINs) are switched to the safety function:

- to request the safety function
- to terminate the request
- for the optional selection of additional control signals

The switching status of these signals can be read out and displayed. The internal control signals for the safety functions are designated as VIN_x_y “Virtual Inputs”.

Example: ‹VIN_SS1_RSF› designates the input for the request (Request Safety Function) of the safety function SS1.

List of virtual inputs ➔ Tab. 188 Virtual inputs.

A total of 32 product terms are available for configuring the switching conditions. The product terms are comparable with programmable logic modules (PLD) and can be flexibly distributed to the desired functions. The product terms are managed automatically using the SafetyTool (special software integrated into the FCT plug-in) and this process is thus scarcely visible to the user.

ⓘ

A maximum of 4 OR-linked product terms with a maximum of 7 inputs with or without inversion can be used for each control signal VIN_x_y and for the configuration of the VOUT_x outputs.

Virtual inputs, to which no product term has been assigned, have the logic state “0”.

The following example uses two of the 32 product terms to request the STO function:

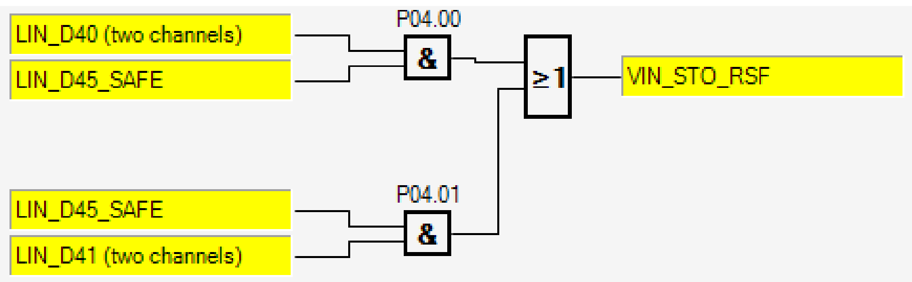


Fig. 6: Example of STO configuration

The safety function itself contains logic and sequence functions that can be parameterised. The safety function takes the current status of the drive (position, speed) into account and monitors the drive. Each safety function makes the following output signals available:
- the status signal that the safety function has been requested
- the status signal that the safe state has been reached
- an error message in the case of violation of the safety condition

Some safety functions also provide additional control signals for direct activation of functions in the servo drive. These status messages are shown as a group in the block diagram and are indicated by VOUT_x “Virtual Output Signals”.
List of virtual outputs ➔ Tab. 189 Virtual output signals.

Logic functions for the inputs:
Special logical control signals are required for some applications, and are made up of a combination of multiple input signals. The safety module supports these applications by making predefined logic functions available for:
- the mode selector switch
- the two-handed control device

The output signals of these logic blocks are mapped directly in LIN_x, as they also serve to control safety functions.
You can also configure customised additional logic blocks. “Additional Logic Functions” (ALF0 … ALF7) are available for this purpose. The output signals of the logic signals are available as “Virtual Output Signals” (VOUT_x).
List of virtual outputs ➔ Tab. 189 Virtual output signals.

Logical outputs and output drivers:
The safety module has configurable blocks with power drivers for:
- control of the digital outputs with generation of test pulses
- control of the relay output
- control of the basic unit.
  Examples:
  - control of the output for brake control
  - switch-off of the driver power supply for STO

A configurable logic function is used to define which VOUT signals are switched to the appropriate output driver as “Logic Output Signal” (LOUT).
The logic function consists of a product term with a maximum of seven inputs as well as input and output inversion.
List of logical outputs ➔ Tab. 190 Logical outputs, mapping the physical outputs.
The status of the logical output (one bit) is converted by the output driver to the physical output signals (frequently two signals, configurable as antivalent/equivalent/test pulses).

Feedback:
The safety module has an internal feedback path, as it is desirable in some applications to execute safety functions according to the status of another safety or logic function:
The most important VOUT signals are therefore guided back to logical inputs LIN and are available for logical operations.

List of logical inputs ➔ Tab. 185 Logical inputs, level assignment to the physical inputs.

State machine:
The operating status of the safety module is controlled using a finite state machine.
The operating status is displayed using a multi-coloured LED and is also mapped in VOUT.
Detailed description of the operating statuses ➔ 3.10 Operating status and status indicators.

Error management:
The error management controls how the safety module reacts when errors occur. The most important error response is to switch off the power output stage in the basic unit immediately (Safe Torque Off, STO) as well as to switch off all safe outputs.
Configuration of the error responses ➔ 3.8 Error management and error acknowledgement.

3.2.5 Overview of supported position encoders

Safe monitoring of speed, e.g. for SLS, and position, e.g. for SOS, requires corresponding sensors for position detection.
The motor controller CMMPAS... M3 supports many different rotary encoders via device interfaces X2A, X2B and X10. The signals of the position encoders are forwarded internally from the CMMP-AS-...-M3 to the safety module (➔ Fig. 4). Most rotary encoders can also be analysed directly by the safety module, as the signals are available to the safety module.
The rotary encoders detect the position and speed. The safety module supports the following rotary encoders:
- resolver via X2A
- SIN/COS incremental encoder via X2B
- SICK Hiperface rotary encoder via X2B (process data channel only)
- HEIDENHAIN EnDat encoder via X2B
- incremental encoder with digital A/B signals via X2B
- BiSS position sensors for linear motors via X2B
- Incremental encoder with digital A/B signals via X10

ⓘ

The safety functions supported by the safety module do not require knowledge of the absolute position. For this reason, safe evaluation of the absolute position of the encoders or safe homing is not intended.

Encoder evaluation
Each micro controller on the safety module can evaluate up to two position sensors.

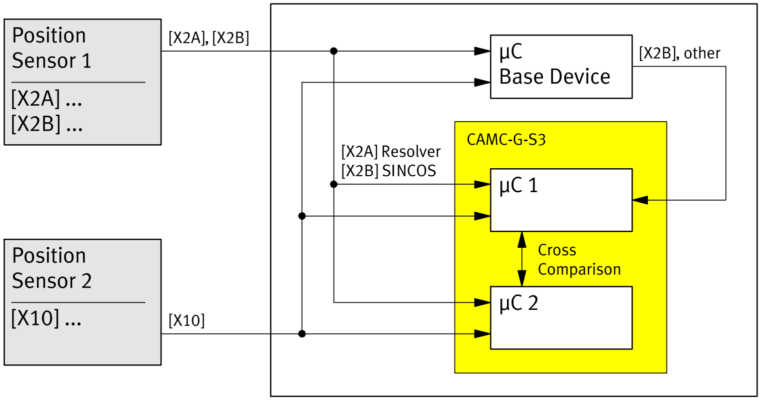


Fig. 7: Evaluation of the position sensors on the safety module

Term/abbreviation	Explanation
Position Sensor 1/2	Position encoder 1/2
µC Base Device	Micro controller basic unit
Cross Comparison	Cross-comparison

Tab. 10: Legend for evaluation of the position sensors on the safety module

- If two position sensors are used, each micro controller evaluates both sensors. Each micro controller compares the position and speed values of both sensors and triggers an error message if there are impermissible deviations.
- If only one position sensor with SIL classification is used, it is also evaluated by both micro controllers on the safety module.
- If a position sensor is used that can be analysed by the basic unit (µC GG) but is not directly supported by the safety module, the standardised angle information can be sent from the basic unit to the safety module. A safe system can be configured up (up to SIL2) in combination with a second position sensor that is evaluated directly by the safety module. The variant is marked in the table "Permissible combinations of position encoders" with "X2B other encoder" ➔ Tab. 11 Permissible combinations of position encoders.
- In all cases, there is a continuous cross-comparison of the position data between micro controller 1 and micro controller 2, with error triggering in the case of impermissible deviations.
- In each configuration, the two micro controllers 1 and 2 use various position and speed values to monitor the axis. Acceleration monitoring can also be configured for a plausibility check.

The manufacturers of SIL-certified rotary encoders publish instructions for the use of these rotary encoders in safety applications.
The CAMC-G-S3 takes the following manufacturer specifications into account when evaluating the encoder signals:

- Specification of the E/E/PES security requirements for the EnDat master dated 2009-10-19 (D533095 - 04 - G - 01) www.heidenhain.de (in preparation)
- Implementierungshandbuch/Implementation Manual HEIDENHAIN Safety dated 2010-12-21 (8014120/2010-12-21) www.sick.com
  Check these documents with reference to necessary measures for the attachment of the rotary encoders and required fault exclusions.

Permissible combinations of position encoders

The following table shows the permissible encoder combinations. Other combinations cannot be parameterised in the safety module.
Achievable safety characteristics for these combinations ➔ 8.2.3 Encoder systems.

First encoder	Second encoder	Note
[X2A] Resolver	[X2B] other encoder	–
[X2A] Resolver	[X10] incremental encoder	–
[X2A] Resolver	none	Note the information below!
[X2B] SIN/COS incremental encoder	none	Requires SIL classification of the encoder.
[X2B] SIN/COS incremental encoder	[X10] incremental encoder	Note the information below!
[X2B] Hiperface incremental encoder	[X10] incremental encoder	Note the information below!
[X2B] Hiperface incremental encoder	none	Requires SIL classification of the encoder.
[X2B] EnDat encoder	[X10] incremental encoder	Setting of encoder 1: "[X2B] other encoder". Note the information below!
[X2B] EnDat encoder	none	In preparation. Requires SIL classification of the encoder.
[X2B] other encoder	[X10] incremental encoder	–

Tab. 11: Permissible combinations of position encoders

NOTICE

- Evaluate whether the position encoders you selected are sufficiently accurate to fulfil the monitoring task, especially for the SOS safety function.
- Note the information on system accuracy ➔ 8.3 System precision and reaction time.

NOTICE

In applications with only one rotary encoder/position encoder it must have the SIL classification required in accordance with the risk assessment.
In most cases, the classification requires additional requirements or fault exclusions in the mechanical system.

- Check carefully that these requirements are fulfilled in your application and that the appropriate fault exclusions can be performed.
- In this regard, always observe the implementation information and the required fault exclusions required by the manufacturer of the position encoder.

NOTICE

In applications with a rotary/position encoder with analogue signal interface (resolver, SIN/COS, Hiperface, etc.):

- Take into account restrictions on diagnostic coverage as well as restrictions on the achievable accuracy of standstill and speed monitoring ➔ 8.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder) and ➔ 8.3.6 Effect of an angle error within the error limits of vector length monitoring on the speed signal.

NOTICE

When using two functional encoders without SIL classification

- Provide separate proof of suitability of the encoder combination for use in safe systems up to SIL3.
  Required proofs are e.g.
  Diversity of encoder systems with reference to CCF, MTTFd, ...
  Suitability of the encoders for the operating and ambient conditions for EMC ...

ⓘ

Recommendation: use sample solutions prepared by the manufacturer with defined combinations of axes, motors and encoders.

3.2.6 Data exchange and control of the motor controller

The safety module can manipulate the power output stage of the motor controller using digital control signals. The motor controller uses further digital control signals to indicate its operating status. In addition, the safety module is connected to the micro controller in the basic unit via an internal communication interface ➔ Fig. 4.

ⓘ

The safety module can control the motor controller (master control). :
- Switching off the power output stage
- Manipulation of the brake control
- Setpoint specification for control
- Error acknowledgement

The digital control signals are used as follows:
- a) Switching off the driver power supply in the motor controller:
  The power output stage of the motor controller can be switched off via two independent channels. One channel controls the power connected to the top switch and the other the power connected to the bottom switch. The channels are controlled with diversity by the safety module and are continuously monitored using test pulses during operation. They are controlled exclusively by the STO safety function ➔ 3.5.1 STO – Safe Torque Off.
- b) Manipulation of the brake control (connection [X6]):
  The brake control is switched off redundantly in the safety module using the appropriate control signals to the basic unit. The brake control is also monitored continuously during operation by test pulses. The safe brake output of the basic unit can thus also be used to control clamping units. They are controlled exclusively by the SBC safety function ➔ 3.5.2 SBC – Safe Brake Control.
  In contrast, a holding brake is only pressurised if the basic unit signals to the safety module via another control cable that it also wishes to enable the holding brake function. This logic operation allows a simple restart of the axis after SBC.

ⓘ

In the case of system errors in the safety module, dynamically activated hardware circuits ensure that the control cables for the driver supply and for brake control are switched off quickly and safely.

---

c) Triggering a quick stop in the basic unit:
The safety module can trigger a quick stop in the basic unit via an internal control cable. The reaction time of the basic unit is very short (< 2 ms).
If the signal is activated, the basic unit brakes to a speed of zero at the quick stop ramp in rotational speed control and positioning modes. After this, depending on the operating mode, the rotational speed is regulated to 0 rpm or the position to the current position.

ⓘ

The function is used to implement the safety function SS1 or SS2 type b) ➔ 3.5.3 SS1 – Safe Stop 1 and ➔ 3.5.4 SS2 – Safe Stop 2.

The internal communication interface between the safety module and the basic unit is used for the following tasks:
- setting up the outward communication connection between the safety module and the PC for parameterisation and diagnostics
- additional active manipulations by the safety module in the controller of the motor controller
- exchange of status messages and operating statuses

– provision of debug information for troubleshooting/analysis
– bi-directional transmission of secure data telegrams to external safety controllers (in preparation)

d) Interface for parameterisation:
The safety module is parameterised using the SafetyTool ➔ 3.2.7 Configuring the safety functions with the SafetyTool and ➔ 5.5 Safe parameterisation with the SafetyTool.
The SafetyTool is opened from the Festo Configuration Tool (FCT). Communication between the Safety-Tool and the safety module is optionally established via one of the interfaces of the motor controller (Ethernet [X18] or USB [X19]). The motor controller forwards the telegrams from and to the safety module without changing them.

e) Active limitation of the rotational speed/speed in the basic unit:
The safety module can use the internal communication connection to manipulate the drive control of the basic unit directly by actively limiting the speed setpoint in the basic unit. The basic unit is braked at the ramp parameterised in the safety module. The limiting is effective in the following operating modes of the basic unit:
– rotational speed/speed control
– positioning (set or direct operation)

ℹ

The function is used to implement the safety function SS1 or SS2 type a) ➔ 3.5.3 SS1 – Safe Stop 1 and ➔ 3.5.4 SS2 – Safe Stop 2. It can also be used in conjunction with safe speed functions, such as SLS, because the axis can be braked autonomously, even without manipulation by the controller.

If multiple safety functions that specify different speed limits are active simultaneously on the safety module, the minimum is formed from the limit values of all the safety functions and transmitted to the basic unit.
The rotational speed should not be actively limited in all interpolating operating modes in which the basic unit is run directly via the controller.

f) Status messages:
The operating status of the safety module and the status of the safety functions (e.g. Safety Function Requested (SFR), Safe State Reached (SSR)) are transmitted at regular intervals to the basic unit via the internal communication interface.
The basic unit can
– output and display this status via the digital outputs
– transmit this status to the higher-order controller via the currently active fieldbus interface
– output this status via the 7-segment display

ℹ

Description of the available status messages ➔ 3.10 Operating status and status indicators.
Status information available via communication protocols FHPP and CiA 402 ➔ 8.4 Status messages, diagnostics via fieldbus.

---

g) Error analysis/debugging:
The basic unit also receives the error status of the safety module via the communication interface and it has access to internal status variables, such as the measured safe speed or the monitoring limits for speed.
The basic unit uses the data:
- to display the operating status and any error messages on the 7-segment display
- to record all signals in non-volatile diagnostic memory for later diagnostics
- to analyse the status variables of the safety module via the oscilloscope function (trace). For example, recording the monitored speed limits and the current speed makes it possible to check why the safety module has detected a violation of a safety condition.

3.2.7 Configuring the safety functions with the SafetyTool

In contrast to a safety controller, the safety module is not freely programmable.
It has a defined function range, which can be activated and parameterised by the user. For flexible adaptation of the functions in the safety module for different applications, the actual safety functions and the outputs have a configurable logic section to specify the switching conditions.
The selection of the safety functions, the allocation of the I/Os and requesting the safety functions via inputs and other conditions are configured using the SafetyTool.
The SafetyTool is a software module for safe commissioning of the safety module and is started from the FCT plug-in CMMP-AS.
The parameterisation defines the following settings along with other items:
- The inputs to which a function is allocated are activated, e.g. a sensor type, example ➔ 5.6.7 Configuring digital inputs.
- The individual safety functions are activated and parameterised, e.g. by specifying limit speeds etc.
- The request for a safety function is parameterised as a logical link, e.g. via the request via an input, example ➔ 5.6.8 Selection and parameterisation of the safety functions.
- To signal an active safety function, the internal status can e.g. be linked to an output.
- The behaviour in case of error (the error response) can be configured.

ⓘ

Description of the procedure for parameterisation of the safety module with the SafetyTool ➔ 5.5 Safe parameterisation with the SafetyTool.

ⓘ

Important:
The SafetyTool supports automatic data migration from the basic unit.
Rotary encoders, gear unit, feed constants etc. are configured only once during commissioning of the basic unit. After commissioning the basic unit, the SafetyTool reads the data and sends it to the safety module, guided by dialogues.
- Fully parameterise the basic unit in the first step and functionally optimise the application.
- In the second step parameterise the safety engineering.

NOTICE

Safety functions in the commissioning phase.

Because measures to ensure the required functional safety are required during the commissioning phase of a system, note that:

- The safety module must be fully configured and the application must be fully validated before it can provide any protection.

ⓘ

The safety module is delivered “preconfigured” ex works ➔ 5.4 Basic principles for parameterisation of the safety module.

- The safety functions STO and SBC are requested via DIN40.
- The safety functions STO and SBC are terminated via DIN49 and a restart is enabled.
- Error acknowledgement takes place via DIN48.

The delivery status can also be recognised without FCT/SafetyTool by the green-red flashing LED of the safety module (if DIN40 has been connected and a safety function is not requested ➔ 3.10 Operating status and status indicators).

3.3 Data migration from the motor controller

For safe motion monitoring, the safety module must know what sensors are connected for position detection, their resolution, their mechanical design, the type of feed, gear unit etc. in use and the units in which the user wishes to parameterise the application. The SafetyTool provides support with menu-guided transfer of data from the basic unit, simplifying parameterisation and avoiding incorrect entries.

ⓘ

Recommendation for creating new projects:

- Use a safety module in the delivery status or reset the safety module to factory settings ➔ 5.4.2 Delivery status and ➔ 5.4.1 Factory setting
- First parameterise the basic unit with the FCT and, if possible, commission it.
- Then start the safe parameterisation with the SafetyTool and use the "Copy" buttons for automatic import of the configured data to the SafetyTool from the basic unit➔ 5.5.1 Program start and ➔ 5.6.2 Data migration and comparison.

NOTICE

Data migration from the basic unit is also required if you wish to use a safety module which has already been used in another application with a different mechanical design or if the safety module was reset manually to factory settings.

In this case too, the configuration of the basic unit is “leading”. The corresponding data for the display units, mechanical components and encoder configuration must be taken from the basic unit.

If previously configured safe motion functions exist in the safety module, then the limit values set in the safety module are transferred to the SafetyTool as setpoint values. They must be transmitted to the safety module again, so that the limit values remain unchanged.

Example:
An SLS function with a limit value of +/- 200 mm/s was originally configured in the safety module. It was operational on a toothed belt axis with a feed of 100 mm/rev.
The safety module is now used in another application, and the feed in this application is now 150 mm/rev.
After transfer of the changed feed, the SafetyTool now displays a discrepancy between the setpoint and actual value in the SLS function:
- Setpoint value: 200 mm/s
- Actual value: 300 mm/s

The setpoint value must therefore be written to the safety module again and validated.

3.3.1 Basic information

Basic information is used for conversion between display and device values and includes:
- the selected display units:
  - path (P06.3E and P06.41),
  - speed (P06.42 to P06.45),
  - acceleration (P06.46 to P06.49),
- a description of the mechanical ratio
  - gear ratio (numerator and denominator) between motor and output (P06.4A and P06.4B),
  - feed constant (numerator and denominator) for rotational -> translational conversion (P06.3F and P06.40).

Parameters for basic information:

NOTICE

These parameters must be transferred to the safety module and checked and validated. Only then can it be guaranteed that the safety module will perform calculations in the same units as the basic unit!

Basic information		
No.	Name	Description
P06.3E	Unit to be displayed for positions.	Unit to be displayed for positions. Selecting “UserDefined” in the SafetyTool means that a unit for position values is not displayed.
P06.3F	Numerator, feed constant of axis in position units	Numerator of the feed constant of the axis in position units per motor revolution (without gear ratios).
P06.40	Denominator, feed constant of axis in posi-tion units	Denominator of the feed constant of the axis in position units per motor revolution (without gear ratios).
P06.41	Number of decimal places displayed with positions.	Number of decimal places displayed with position values.

Basic information		
P06.42	Unit to be displayed for speeds.	Unit to be displayed for speeds. Selecting “UserDefined” means that a unit is not displayed. If the position is UserDefined, the speed must also be user-defined.
P06.43	Numerator, altered time base for speeds of the UserDefined type.	Numerator, altered time base for speeds of the “UserDefined” type.
P06.44	Denominator, altered time base for speeds of the UserDefined type.	Denominator, altered time base for speeds of the “UserDefined” type.
P06.45	Number of decimal places displayed with speeds.	Number of decimal places displayed with speeds.
P06.46	Unit to be displayed for accelerations.	Unit to be displayed for accelerations. Selecting “UserDefined” means that a unit is not displayed. If the position is “UserDefined”, the acceleration must also be user-defined.
P06.47	Numerator, altered time base for accelerations of the UserDefined type.	Numerator, altered time base for accelerations of the “UserDefined” type.
P06.48	Denominator, altered time base for accelerations of the UserDefined type.	Denominator, altered time base for accelerations of the “UserDefined” type.
P06.49	Number of decimal places displayed with accelerations.	Number of decimal places displayed with accelerations.
P06.4A	Numerator, total gear ratio between motor and axis.	Numerator, total gear ratio between motor and axis.
P06.4B	Denominator, total gear ratio between motor and axis.	Denominator, total gear ratio between motor and axis.

Tab. 12: Parameters for basic information

3.3.2 Configuration of the encoders

The selection and setting of the rotary encoders for measuring position, setting the angle/position counting direction, resolution of the position encoder and the setting of the gear ratios of the position encoders are also taken automatically from the configuration of the basic unit.

Important:
In many cases, only one position encoder on the motor is used for control in the basic unit. In many cases an additional position encoder is installed for functional safety, e.g. at the output.
Make sure that you have already configured the position encoders used in the basic unit via the FCT. Only then can data be migrated completely.

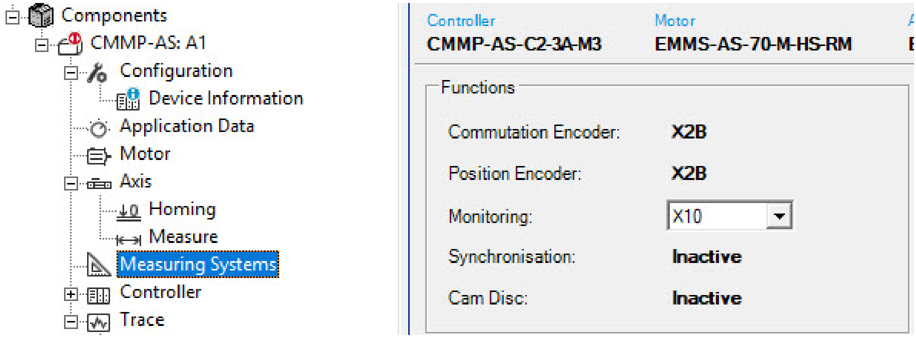


Fig. 8: Configuration example for 2 encoders

NOTICE

These parameters must be transferred to the safety module and checked and validated. Only then can it be guaranteed that the safety module will perform calculations in the same units as the basic unit!

The configuration of the position encoders is relatively complex, because the safety module supports many different encoder types and configurations. The configuration is divided into the following tabs in the SafetyTool:

- standard parameters (selection of the encoder interfaces and encoder types),
- parameters for position encoder at [X2B],
- parameters for position encoder at [X10],
- expert parameters for cross-comparison of position data,
- expert parameters for configuration of the safe rotational speed recording and standstill detection,
- expert parameters for signal monitoring of safe encoders with analogue signals (resolver, SIN/COS encoder).

Standard parameters

The encoder interface and the encoder type are selected here for use in the safety module as position encoder 1 and as position encoder 2. Gear units between motor and axis are mapped via the gear ratios. A reversal of the direction of rotation is taken into account using negative gear ratios.

Data migration/setting of the leading position encoder 1 (first encoder) is carried out:

- resolver [X2A],
- SIN/COS or Hiperface encoder [X2B],
- other encoders [X2B], e.g. EnDat, BiSS.

A gear ratio between encoder and motor for position encoder 1 can also be set.

Data is also migrated and set for position encoder 2 (second encoder):

- other encoder [X2B], e.g. SIN/COS, EnDat, BiSS,
- incremental encoder [X10],
- none (only if position encoder 1 is a certified position encoder).

A gear ratio can also be set between encoder and motor for position encoder 2.

Important: the SafetyTool will warn you of impermissible encoder combinations.

Input of parameters				
Send	ID	Name	Unit	Nominal value
	P06.00	Selection of leading position sensor 1		SINCOS / Hiperface (X2B) = [2]
	P06.0B	Gear ratio enumerator for position sen		1
	P06.0C	Gear ratio denumerator for position se		1
	P06.01	Selection of redundant position sensor		Other encoder (X2B) = [4]
	P06.0D	Gear ratio enumerator for position sen		1

Fig.9

Permissible encoder combinations and the corresponding safety classification ➔ 3.2.5 Overview of supported position encoders and ➔ Tab. 11 Permissible combinations of position encoders.

In the case of linear motors, FCT uses the position resolution of the measuring system and the pole pitch τ_p of the motor to calculate both a feed constant (basic information), a gear ratio and a resolution of the measuring system relative to $2\tau_p$.
This data is transferred to the SafetyTool. This means that automatic data migration is also guaranteed for linear motors.

NOTICE

Should a cross-comparison error between encoder 1 and 2 occur despite successful data migration.

- In this case, check the gear ratio of encoder 2, because it is only monitored by the safety module and is not integrated into the control in FCT.

3.3.3 Parameters for the position encoders

Parameters for position encoders at [X2A]

The connection [X2A] is intended for resolvers. The analogue amplitude-modulated track signals of the resolver in the CMMPAS... M3 are tapped behind the input differential amplifier, routed internally to the safety module and then securely evaluated by both micro controllers in two channels.
A parameterisation/data migration from the basic unit is not required.

Parameters for position encoders at [X2B]

The connection [X2B] is intended for encoders with analogue tracking signals:

– Incremental encoders with SIN/COS tracking signals
– Hiperface encoders with SIN/COS tracking signals

The tracking signals of the SIN/COS encoders and Hiperface encoders in the CMMPAS... M3 are tapped behind the input differential amplifier, routed internally to the safety module and then securely evaluated by both micro controllers in two channels. This is always the case if "SIN/COS encoder/ Hiperface (X2B) = [2]" was selected in the Standard parameters tab.

During data migration/parameterisation, the number of digital angular counting steps is set (corresponding to 4x division marks per motor revolution or, with linear motors, per $2T_p$).

NOTICE

When the axis is at standstill, SIN/COS encoders send static signals. If a second angle encoder is not used, Stuck-At errors (value not updated due the output signal remaining unchanged or changed too little) cannot be detected. For this reason, the axis must be moved regularly when safety functions are requested.
If a SIN/COS or Hiperface encoder is used as the sole encoder, then error 55-2 is triggered if a safety function is requested after 10 days at standstill.
If safety function SS2/SOS is requested continuously for longer than 10 days, this will trigger error 54-7.

NOTICE

In applications with only one rotary encoder or position encoder with analogue signal interface (resolver, SIN/COS, Hiperface etc.), the restrictions on diagnostic coverage as well as the restrictions on the achievable accuracy of standstill and speed monitoring must be taken into account
Additional information:
➔ 8.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder)
➔ 8.3.6 Effect of an angle error within the error limits of vector length monitoring on the speed signal

The connection [X2B] is also intended for encoders with digital interface:
- digital incremental encoders with A/B/N square wave signals,
- EnDat-2.1 and EnDat-2.2 encoders with digital interface,
- serial encoders with digital interface, e.g. BiSS.

These encoders are not analysed for safety in the basic unit CMMP-AS-...-M3. The safety module polls standardised digital angle information at regular intervals from the basic unit via the internal data interface. This is always the case if “Other encoder (X2B) = [4]” was selected in the Standard parameters tab.
The angular information of any encoder connected to X2B on the motor controller can be used as a channel of the two-channel safe angular detection.
It is possible to parameterise an error tolerance time if the safety module detects faulty data telegrams. The default value of 1 ms should not be changed without a significant reason, as the value acts as an additional filter on the reaction time of the safety module.

NOTICE

The use of encoders with purely digital data transfer in safety systems in only permissible in conjunction with a second encoder, e.g. at [X10].

ⓘ

It is not yet possible to use a safe EnDat encoder (in preparation). “Angle encoder 1 = EnDat” is formally parameterised if a safe EnDat encoder is used. Only one incremental encoder at [X10] can be additionally evaluated as angle encoder 2.

NOTICE

There is a jump in the actual position when saving during homing of drives with EnDat multiturn encoders that save the zero point offset in the encoder. This jump causes acceleration monitoring in the safety module to respond, leading to an error of the safety module.
This homing need only be carried out once during machine setup.

Parameters for position encoders at [X10]

The [X10] connection is intended for digital incremental encoders with A/B/N square wave signals. The position is detected using quadrature counter inputs of the micro controllers of the safety module. The incremental encoder [X10] is ideally used as the second position measurement system. This is always the case if “Incremental encoder (X10) = [5]” was selected in the Standard parameters tab.
During data migration/parameterisation, the number of digital angular counting steps is set (corresponding to 4x division marks per motor revolution or, with linear motors, per $2\tau_p$).

3.3.4 Parameters for encoder monitoring and rotational speed recording

The following diagram shows the structure of the encoder evaluation and monitoring:

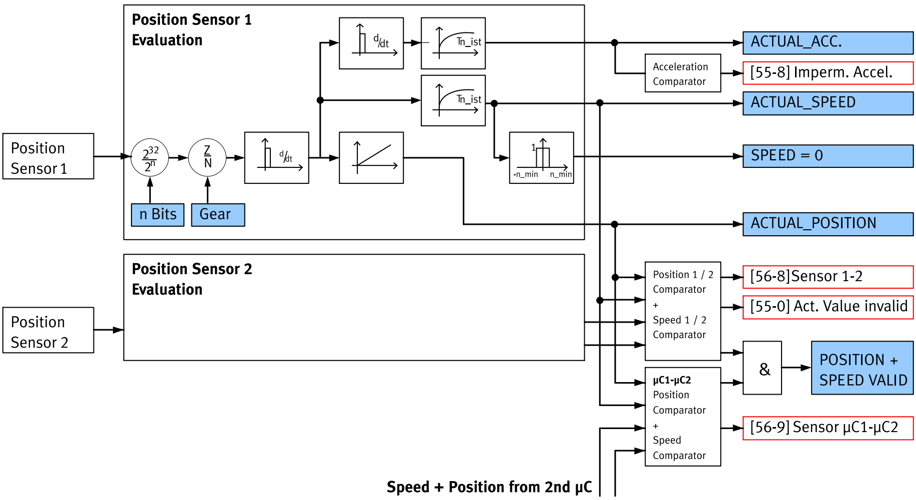


Fig. 10: Calculation of the speed and acceleration

Term/abbreviation	Explanation
Position Sensor 1/2	Evaluation of position encoder 1/2
Evaluation	Evaluation or analysis
Gear	Gear unit
Acceleration Comparator	Comparison of acceleration 1/2
Position 1/2 Comparator + Speed 1/2 Comparator	Comparison of position 1/2 and Comparison of speed 1/2

Term/abbreviation	Explanation
ACTUAL_ACC.	Internal signal: current acceleration
ACTUAL_SPEED	Internal signal: current speed
SPEED = 0	Internal signal: speed = 0
ACTUAL_POSITION	Internal signal: current position
POSITION + SPEED VALID	Internal signal: position and speed valid
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Tab. 13: Legend for calculation of the speed and acceleration

Description:

- The ‹Position Sensor Evaluation› block exists twice in each micro controller, separately for position encoder 1 and position encoder 2.
- The position information of encoder 1 and encoder 2 is first standardised to 2^{32}. Then a gear ratio is taken into account, which can also be used to map a counting direction reversal.
- Thus the block returns a standardised position and uses it to calculate the current speed and the acceleration.
- The data from position encoder 1 is used to monitor the status variables.
- The acceleration is monitored and checked for plausibility - this can be parameterised.
- Each micro controller continuously compares the position values and speed values of encoder 1 with those of encoder 2.
- The tolerances for this encoder comparison can be parameterised.
- In addition, each micro controller performs a cross-comparison to compare its own position and speed data with that of the other micro controller. Limit values can be parameterised for this purpose.
- The micro controller will generate various error messages if deviations or limit value violations are detected.

NOTICE

The factory settings of the parameters for encoder analysis are adapted to the resolution of the position encoders and to the evaluation electronics in the safety module.
What are referred to as "expert parameters" should only be changed in specific cases, because they influence the reaction time of the safety module when dangerous movements or errors are detected.

Expert parameters for configuration of the safe rotational speed recording and standstill detection

Both micro controllers use the recorded position data to calculate the safe speed and the acceleration. The following parameters are available for rotational speed recording and for standstill detection:

- Acceleration monitoring is used to check the plausibility of the position measurement. An acceleration has been parameterised that the motor certainly cannot reach due to its design. If the rotational speed ramp exceeds a limit defined by the maximum acceleration, error 55-8 is triggered ➔ 6.6 Diagnostic messages with information for fault clearance.
- The filter for the rotational speed/speed recording reduces the noise in the speed signal, particularly if encoders with analogue signals or a coarse resolution are used.
- The threshold value and the filter time for the standstill detection. The standstill detection is used, e.g. for the SOS safety function.

Expert parameters for cross-comparison of position data

This tab contains parameters for checking the plausibility of the position and speed data.

- The tolerance window and tolerance time for comparison of the position data of encoder 1/encoder 2 by the appropriate micro controller in the safety module.
- The tolerance window and tolerance time for comparison of the speed data of encoder 1/encoder 2 by the appropriate micro controller in the safety module.
- The tolerance window and tolerance time for the cross-comparison of the position data between micro controller 1 and micro controller 2 on the safety module.
- The tolerance window for the cross-comparison of the speed data between micro controller 1 and micro controller 2 on the safety module.

If the safety module detects a deviation in the position or speed data and/or their value exceeds the parameterised value continuously for the parameterisable time, then an error is triggered and the actual values are invalid.

Expert parameters for the signal monitoring of safe encoders with analogue signals

This tab contains parameters for monitoring the analogue encoder signals of SIN/COS encoders and resolvers.

- Amplitude and vector length monitoring for the resolver signals, as well as a tolerance time for monitoring.
- Parameterisable observer filter for the resolver evaluation.
- Amplitude and vector length monitoring for the SIN/COS and Hiperface encoder analysis, as well as a tolerance time for monitoring.

Influence of the parameters for the encoder configuration on the time response

The following configuration parameters for recording safe rotational speed influence the reaction time with which changes in the movement are detected.

Parameters for movement recording and error detection that influence the time response				
Parameter		min.	max.	Factory setting
P06.08	Filter time constant for recording rotational speed	0.4 ms	1000 ms	8.0 ms
P06.0A	Filter time for standstill detection	0.0 ms	1000 ms	10.0 ms
P06.04	Tolerance time for position difference 1 - 2	0.0 ms	1000 ms	10.0 ms
P06.06	Tolerance time for speed difference 1 - 2	0.0 ms	1000 ms	10.0 ms

Parameters for movement recording and error detection that influence the time response				
Parameter		min.	max.	Factory setting
P06.15	Resolver observer filter - filter time	0.0 ms	3 ms	1.0 ms
P06.13	Resolver signal monitoring tolerance time	0.0 ms	10 ms	1.0 ms
P06.1E	SIN/COS signal monitoring tolerance time	0.0 ms	10 ms	1.0 ms

Tab. 14: Parameters for error detection in the position sensors that influence the time response

ⓘ

If you do not change the factory settings, you can use the following for simplified reaction times:
Recording speed and position $T_I < 10$ ms
Detection of errors in position recording $T_F < 10$ ms

3.3.5 List of all parameters for encoder configuration

Encoder configuration		
No.	Name	Description
Standard parameters		
P06.00	Selection of the leading position encoder 1	Encoder 1 used for angles
P06.0B	Gear ratio numerator for position encoder 1	Gear ratio/pole pair number numerator
P06.0C	Gear ratio denominator for position encoder 1	Gear ratio/pole pair number denominator
P06.01	Selection of the redundant position encoder 2	Encoder 2 used for angles
P06.0D	Gear ratio numerator for position encoder 2	Gear ratio/pole pair number numerator
P06.0E	Gear ratio denominator for position encoder 2	Gear ratio/pole pair number denominator
X2B		
P06.19	Number of incr./rev. of the incremental encoder at X2B	Number of increments/revolution of the incremental encoder at X2B
Expert parameters		
P06.28	Tolerance time for faulty encoder communication	Tolerance time for faulty encoder communication
X10		

Encoder configuration		
No.	Name	Description
P06.18	Number of incr./rev. of the incremental encoder at X10	Number of increments/revolution of the incremental encoder at X10
Rotational speed recording		
Expert parameters		
P06.07	Maximum acceleration for encoder monitoring	Maximum acceleration that the drive never reaches ⇢ error limit for angle plausibility check
P06.08	Filter time constant for recording rotational speed	Filter time constant actual rotational speed value filter
P06.09	Speed threshold value for standstill detection	Max. rotational speed for standstill detection
P06.0A	Filter time for standstill detection	Time window for $n < n_{min}$ for standstill detection
Comparison encoder 1 - 2		
P06.03	Tolerance window for position offset encoder 1 - 2	Approved position offset between angle encoder 1 and 2
P06.04	Tolerance time for position difference	Maximum time for which the position difference may be outside the limit
P06.05	Tolerance window speed deviation encoder 1 - 2	Approved rotational speed offset between angle encoder 1 and 2
P06.06	Tolerance time for speed difference	Maximum time during which the rotational speed difference may be outside the limit
Expert parameters		
P1D.04	Tolerance window for position - cross-comparison µC1 - µC2	Approved angle offset between this processor and the partner
P1D.05	Tolerance time for position - cross-comparison µC1 - µC2	Maximum time during which the cross-comparison values may be outside the limit
P1D.06	Tolerance window for speed - cross-comparison µC1 - µC2	Approved rotational speed difference between this processor and the partner
Signal monitoring		
Expert parameters		
P06.11	Resolver signal amplitude - lower error limit	Min. input voltage sine or cosine signal

Encoder configuration		
No.	Name	Description
P06.12	Resolver signal amplitude - upper error limit	Max. input voltage sine or cosine signal
P06.0F	Resolver - vector length lower limit	Min. input voltage U = root($sin^2 + cos^2$)
P06.10	Resolver - vector length upper limit	Max. input voltage U = root($sin^2 + cos^2$)
P06.13	Resolver signal monitoring tolerance time	Maximum time during which a resolver signal may be outside the signal monitoring limits before an error is triggered.
P06.15	Resolver analysis filter time	Filter time for the observer filter
P06.1C	SIN/COS signal amplitude - lower error limit	Min. input voltage sine or cosine signal
P06.1D	SIN/COS signal amplitude - upper error limit	Max. input voltage sine or cosine signal
P06.1A	SIN/COS - vector length lower limit	Vector length root($sin^2 + cos^2$) min.
P06.1B	SIN/COS - vector length upper limit	Vector length root($sin^2 + cos^2$) max.
P06.1E	Tolerance time signal amplitude monitoring	Maximum time during which a signal may be outside the limit before an error is triggered.

Tab. 15: Encoder configuration

3.4 Digital inputs

3.4.1 Overview

The safety module has digital inputs and outputs for the connection of passive and active sensors. Safety functions are requested via two-channel safe inputs.

Term	**Meaning**
Discrepancy time	Maximum time during which the two channels of a safe input may be in antivalent states without the safety engineering triggering an error response.
Input filter time	Time during which the interfering pulses and test pulses, such as those from connected active sensors, are not detected.
Safety function in the OFF status	The function of the inputs can be freely configured over a wide range. During configuration, the user must ensure that the safe status is achieved on de-energised inputs (comply with quiescent current principle!).

Term	Meaning
Control function in ON status	The function of the inputs can be freely configured over a wide range. Control functions require active actuation/circuitry of the control input with 24 V in order to trigger the desired reaction (example: error acknowledgement, termination of a safety function, mode selection switch). The quiescent current principle would not be safe for this!
Equivalent input signals	A safe input consists of two control cables, which switch both HIGH and/or LOW simultaneously (equally switching inputs).
Antivalent input signals	A safe input consists of two control cables, which both switch HIGH or LOW against each another. At any time (with the exception of the discrepancy time) only one input is simultaneously HIGH or LOW (unequally switching inputs).

Tab. 16: Definition of terms used to describe the digital inputs

Passive sensors (two-channel)

Passive sensors are two-channel, contact-based switching elements. The connecting cables and the function of the sensors must be monitored.

The contacts can switch antivalently and equivalently (according to the standard for the appropriate switching element). Regardless of this, safety functions are triggered as soon as at least one channel is switched.

Examples of passive sensors:

- emergency stop switching devices (always equivalent)
- door contact switch (both antivalent and equivalent)
- enabling buttons (both antivalent and equivalent)
- two-handed control devices
- mode selector switch (1-of-n selection)

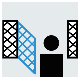
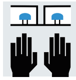
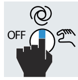
The following errors are detected by the safety module in the case of passive sensors:

- antivalent or equivalent input signals after the discrepancy time has elapsed, depending on the sensor type and parameterisation
- For supply via a safe output of the safety module:
  Cross circuits and shorts to +24 V and 0 V due to the absence of the test pulses.

ℹ

Passive sensors that trigger an emergency stop of the system (STO, SBC, SS1) must be designed as “positive opening” in accordance with EN 60204-1 and must be parameterised as equivalent inputs.

Sensor types

Function	Emergency stop switching device	Door contact switch	Enabling button	Two-hand operator unit	Mode selector switch
Symbol					
Input	DIN40A/B ... DIN43A/B	DIN40A/B ... DIN43A/B	DIN40A/B ... DIN43A/B	DIN40A/B ... DIN43A/B	DIN45, DIN46, DIN47
Output	DOUT40A/B ... DOUT42A/B (cycle A/B)				+24V[1]

1) Can also be supplied with test pulses from DOUT40 ... 42.

Tab. 17: Allocation of the sensors to the inputs and outputs (examples)

Emergency stop switching device

The emergency stop switching device is generally used to trigger the emergency stop; in most cases, the STO or SS1 safety function is activated.

Door contact switch

It is monitored to check, e.g. whether a safety door or light curtain is opened or penetrated.

Enabling button

The enabling button is generally used during setup.
Example: during setup, machine travel is allowed when the safety door is open with the SLS function as soon as the enabling button is actuated. In so doing, the enabling button temporarily cancels a safety function, which is temporarily replaced by another safety function. The function of the enabling button is implemented by corresponding parameterisation of the logic (request, terminate request) of the safety function.
The following logic functions are permanently allocated to specific inputs:

Two-handed control device (DIN42A/B and DIN43A/B)

The two-handed control unit is used in applications in which the operator must enable the movement with both hands as soon as the danger zone is clear. The two-handed control unit receives input from two safe input pairs. In this case also, a safety function, e.g. SS1, can be overwritten by another function, e.g. SLS. The function of the two-handed control unit (monitoring of the two inputs) is implemented in the safety module as a fixed logic function. The safety functions are switched over by corresponding parameterisation of the logic (request, terminate request) of the safety functions.

Mode selector switch (DIN45, DIN46, DIN47)

The switch for selecting the operating mode supports the following operating modes:

– normal operation/operating mode 1
– setup/operating mode 2
– special operation/operating mode 3

Note: the operating modes are named according to C standards for the corresponding machines. The function of the mode selector switch is implemented in the safety module as a fixed logic function. The safety functions are switched over by corresponding parameterisation of the logic (request, terminate request) of the safety functions.

Restart/termination of safety functions

“Restart” refers to the start-up of the drive after a previous stop. The safety module can initiate this stop, e.g. via the STO, SS1 or SS2 safety functions. Terminating the corresponding safety functions is a prerequisite for a restart. DIN49 is provided for terminating the safety functions, but any other input can also be parameterised accordingly.

Example:

- SS1 was requested via an emergency stop, SS2 via the door contact switch.
- Now the emergency stop is removed again and the door remains open.

⇒ When the "Terminate the safety function" input is actuated, the system stops with the active safety function SS2 and can start again immediately when the safety door is closed if the parameter "Automatic restart" was set for SS2.

Active sensors (two-channel)

Active sensors are units with two-channel semiconductor outputs (OSSD outputs).

Examples of active sensors:

- Light curtain
- Laser scanner
- Controllers

The safety module supports active sensors with equivalent/antivalent output signals as well as with/without test pulse outputs. Test pulses to monitor the outputs and cables are approved with the integrated safety engineering of the CMMP-AS-...-M3 series. Positive/negative-switching sensors switch the positive and negative cable or signal and earth cable of a sensor signal. The outputs must switch simultaneously. Regardless of this, safety functions are triggered as soon as at least one channel is switched.

These errors are detected by active sensors:

- antivalent or equivalent input signals after the discrepancy time has elapsed, depending on the sensor type and parameterisation

Passive and active sensors (single-channel)

Single-channel sensors are used for sequence control and for feedback and diagnostics.

Examples of passive sensors:

- feedback contact of an external clamping unit,
- button to acknowledge pending errors,
- button for terminating safety functions.

Combinations of single-channel sensors can also be used to control safety functions.

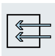
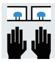
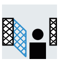
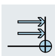
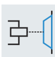
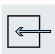
Example: mode selector switch (1-of-n selection)

These errors are detected by single-channel passive sensors:

- For supply via a safe output of the safety module:
  Cross circuits and shorts to +24 V and 0 V due to the absence of the test pulses

Approved sensor types

The following table shows an overview of the approved sensor types at the digital inputs.

Approved sensor type		**DIN ...**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**
			two-channel				single-channel					
1:	General two-channel input		X	X	X	X						
2:	Emergency stop switching device		X[1]	X	X	X						
3:	Enabling button		X	X	X	X						
4:	Two-handed control device[2]		X	X	X	X						
5:	Start button		X	X	X	X						
6:	Door lock		X	X	X	X						
7:	Reliable reference switch		X	X	X	X						
8:	Light curtain		X	X	X	X						
9:	Feedback brake control		X	X	X	X	X[1]	X	X	X		
10:	General single-channel input		X	X	X	X	X	X	X	X		
11:	Mode selector switch2)[2]		X	X	X	X		X[1]	X[1]	X[1]		

Approved sensor type		**DIN ...**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**
			two-channel				single-channel					
12:	Acknowledge error		X	X	X	X					X[1]	
13:	Terminating safety functions (restart possible)		X	X	X	X						X[1]

1) Factory setting
2) On activating the logic function in the SafetyTool, the corresponding inputs must be configured accordingly.

Tab. 18: Overview of approved sensor types at the digital inputs

3.4.2 Two-channel safe inputs DIN40 ... DIN43 [X40]

Use

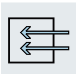


Fig. 11: Symbol, two-channel input

The digital inputs DIN40..DIN43 have two channels (DIN40A/B ... DIN43A/B). They serve the requirement of the safety functions up to Cat. 4/PL e or SIL3 and thus have a 1oo2 architecture.
To request safety functions, the allocated internal logical inputs are linked with the corresponding safety function.

Function

The following figure shows the block diagram of an input. The function is explained below for DIN40. The inputs DIN40 to DIN43 have an identical structure.

DIN40 ... DIN43

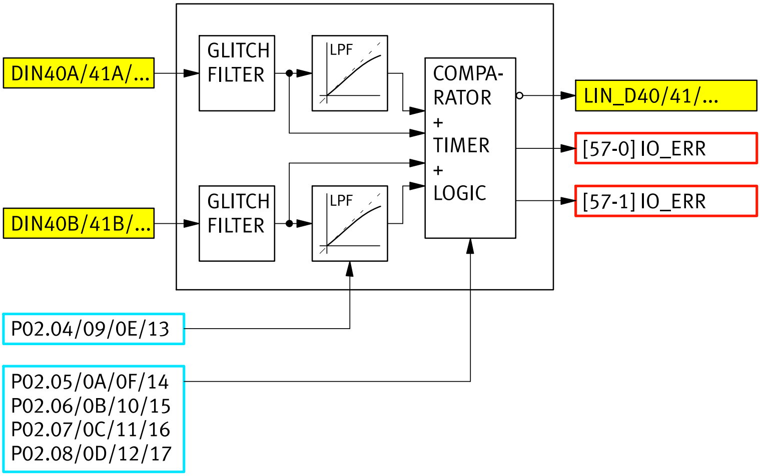


Fig. 12: Block diagram of the two-channel safe inputs

Term/abbreviation	Explanation
DIN40A/..., DIN40B/ ...	Two-channel digital inputs DIN40A/DIN40B ...
GLITCH FILTER	Filter for interference
LPF	Low-pass filter
COMPARATOR + TIMER + LOGIC	Comparator, timer and logic
LIN_x	Logical inputs ...
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Tab. 19: Legend for block diagram of the two-channel safe inputs

The signal levels at the inputs DIN40A and DIN40B are first dejammed in a preliminary EMC filter (glitch filter). The filter time constant is 500 µs and cannot be parameterised.
After this first filter, a second “LPF” low-pass filter, which can be parameterised using the parameter “Filter time constant” (P02.04/...), follows for each input signal, and is designed as a programmable monoflop.
The monoflop serves the following purposes:
- filtering out external test pulses, e.g. of an active sensor with OSSD outputs.
- filtering out the test pulses of DOUT4x in the case of passive sensors.
- filtering out contact bounces.

In a downstream logic operation with comparator, the two input signals A and B are used to form the logical control signal LIN_D40. The test pulses at the input are also analysed in this section. To request safety functions, the logical input is linked with the corresponding safety function (LIN_D40 = 1 means that the safety function has been requested). A sensor type can be selected using the parameter “Sensor type” (P02.24/...).

The inputs can be used in three different operating modes by using the “operating mode” parameter (P02.06/...):

- Operating mode = “unused” (P02.06/... = 0)
  The input is not used. The logical input signal LIN_D40 is continuously 0.
- Operating mode = “equivalent” (P02.06 = 1)
  The input is equivalent switching:
  - Inputs A and B of a channel must always have the same signal level.
  - The logical input signal LIN_D40 is inverse to the signal level at DIN40, as the following table shows.

  Note: the inversion of the logic state corresponds to the quiescent current principle. Use the inputs only according to the quiescent current principle. Request the safe status through 0 V at the input.
- Operating mode = “antivalent” (P02.06 = 2)
  The input is antivalent switching:
  - Inputs A and B must have opposite signal levels.
  - The logical input signal LIN_D40 is inverse to the signal level at DIN40A, as the following table shows.

  Note: passive sensors that trigger an emergency stop of the system (STO, SBC, SS1) must be designed as “positive opening” in accordance with EN 60204-1 and must be parameterised as equivalent inputs.

Input DIN40/ ... /43 equivalent	Standstill state	Safety function requested
DIN40A/.../43A	24 V	0 V
DIN40B/.../43B	24 V	0 V
Status LIN_D40/.../43	0	1

Tab. 20: Equivalent switching inputs

Input DIN40/.../43 antivalent	Standstill state	Safety function requested
DIN40A/.../43A	24 V	0 V
DIN40B/.../43B	0 V	24 V
Status LIN_D40/.../43	0	1

Tab. 21: Antivalent switching inputs

Error detection

The level of inputs A and B may deviate from the displayed statuses for a parameterisable time (“discrepancy time”, P02.05/...). If the deviation persists, error “[57-1] Digital inputs - Signal level error” (discrepancy error) is reported.
Inputs A and B can be monitored using test pulses. The test pulse source is selected with the parameter “Source for test pulse” (P02.07/...). If a test pulse is missing or the input logic detects a short circuit or cross circuit, error “[57-0] Self-test I/O (internal/external)” is generated.
In case of error, logical input LIN_D40 switches to 1 (Safety function requested).

NOTICE

A detected error is forwarded to the error management using the error signals shown in the block diagram. The reaction to the error can be set (warning only, STO, SS1, SS2, etc.). In this case, for further processing, the logical input LIN_D40 takes status 1.
The user must ensure that an error (error management) leads to the safe status for the overall system.

Timing diagrams

The following images show the associated timing diagrams of a two-channel input, for both equivalent and antivalent parameterisation.

Request Safety Function – Equivalent (P02.06 = 1)

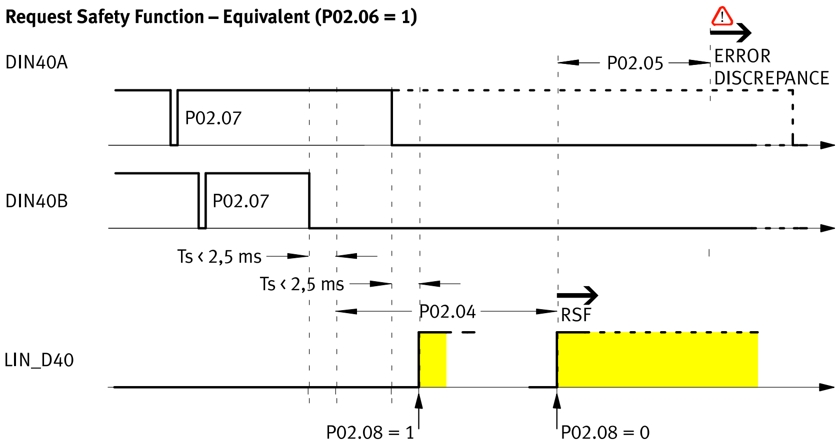


Fig. 13: Timing diagram of two-channel equivalent safe input – start request (DIN40)

Release Safety Function request – Equivalent (P02.06 = 1)

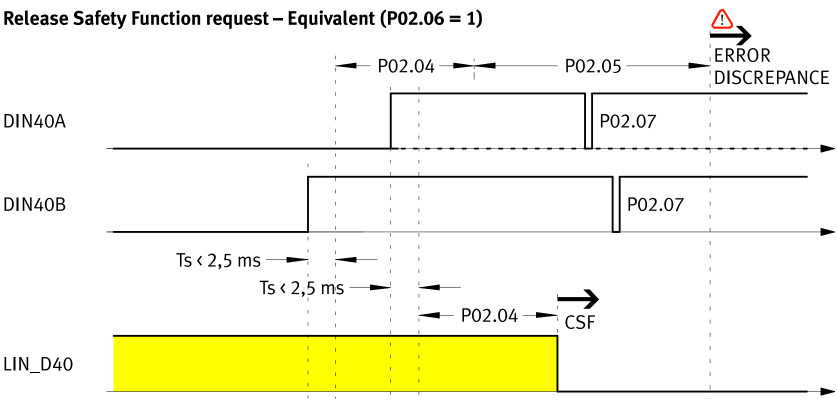


Fig. 14: Timing diagram of two-channel equivalent safe input – terminate request (DIN40)

Term/abbreviation	Explanation
RSF: Request Safety Function	Request safety function
CSF: Release Safety Function request	Terminate request of the safety function
Error Discrepance	Discrepancy error

Tab. 22: Legend for timing diagram of two-channel safe input equivalent

Request Safety Function – Antivalent (P02.06 = 2)

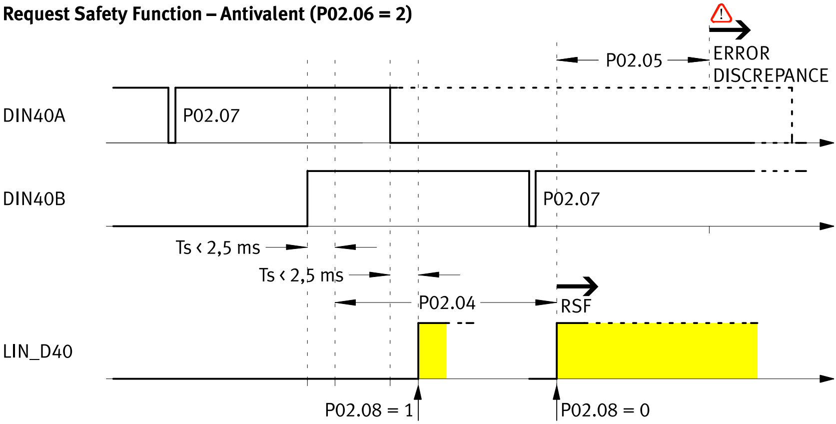


Fig. 15: Timing diagram of two-channel antivalent safe input – start request (DIN40)

Release Safety Function request – Antivalent (P02.06 = 2)

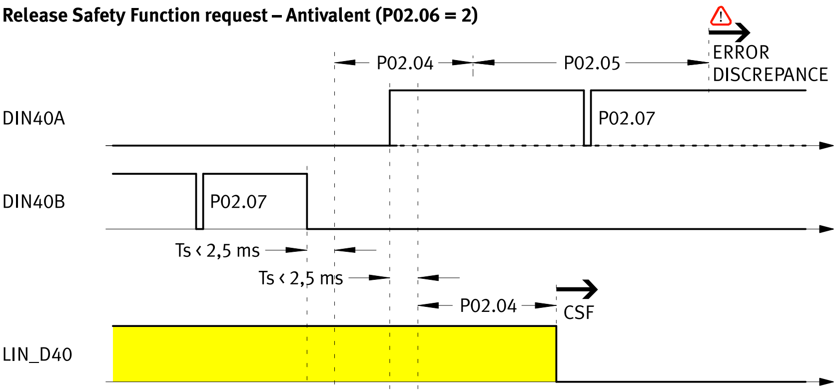


Fig. 16: Timing diagram of two-channel equivalent safe input – terminate request (DIN40)

Term/abbreviation	Explanation
RSF: Request Safety Function	Request safety function
CSF: Release Safety Function request	Terminate request of the safety function
Error Discrepance	Discrepancy error

Tab. 23: Legend for timing diagram of two-channel safe input equivalent

Rapid detection of a safety requirement can be activated using the “Quick detection request” parameter (P02.08/...). If both DIN40A and DIN40B inputs change level simultaneously, then the switching status is forwarded to the logical signal LIN_D40, bypassing the “LPF” filter. This means that very rapid detection of a safety function request is possible even with relatively long test pulses and thus large time constant of the filter.
After the request of a safety function via DIN40 ... DIN43, the following times elapse until the logical input LIN_D... and thus the safety function request is activated:

Time delays from the level change	Minimum	Maximum	Typical
Ts	0.5 ms	2.5 ms	1.5 ms
“Filter time constant” (P02.04/09/0E/13)	1.0 ms	1000.0 ms	3.0 ms
Reaction time for “Quick detection request” = 0 (P02.08/ P02.0D/P02.12/P02.17 = 0)	1.5 ms	12.5 ms	4.5 ms
Reaction time for “Quick detection request” = 1 (P02.08/ P02.0D/P02.12/P02.17 = 1)	0.5 ms	2.5 ms	1.5 ms

Tab. 24: Time delays DIN40 ... DIN43

Parameters for the two-channel digital inputs

Parameter no. for input ...				Name	Description
DIN40	DIN41	DIN42	DIN43		
P02.24	P02.25	P02.26	P02.27	Sensor type	Identifier of the sensor connected to DIN4x.
P02.06	P02.0B	P02.10	P02.15	Operating mode	Mode: 0 = unused, 1 = equivalent, 2 = antivalent
P02.05	P02.0A	P02.0F	P02.14	Discrepancy time	Discrepancy time.
P02.07	P02.0C	P02.11	P02.16	Source for test pulse	Selection of the output supplying the test pulses.
Expert parameters					

Parameter no. for input ...				Name	Description
DIN40	DIN41	DIN42	DIN43		
P02.04	P02.09	P02.0E	P02.13	Filter time constant	Filter time constant.
P02.08	P02.0D	P02.12	P02.17	Quick detection request	Use quick switch-off on low level at DIN4xA and DIN4xB.

Tab. 25: Parameters of two-channel digital inputs

Technical data for the control inputs in the specified operating range of logic voltages to EN 61131-1
➔ Tab. 143 Technical data: digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40].

3.4.3 Single-channel (partially safe) digital inputs DIN44 ... DIN49 [X40]

Use

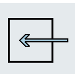


Fig. 17: Symbol, single-channel input

The digital inputs DIN44..DIN49 have one channel. They can be used to connect passive switches and active sensors.
Use the single-channel inputs as diagnostic inputs:
- for control functions that only require a single-channel input
- in combination with several inputs for requesting safety functions

If active two-wire sensors are used without self-diagnostics:
If the active two-wire sensor is not actuated, then not all the required tests are carried out by the safety module. For this reason, regular actuation is required for a function test. We recommend actuating every 8 hours or once per shift, but at least once every 24 hours ➔ Tab. 143 Technical data: digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40].

Only the two-channel inputs DIN40 ... DIN43 or suitable logical combinations of single-channel inputs may be used to request and deactivate safety functions.

Function
The following figure shows the block diagram of the single-channel inputs. The function is explained below for DIN44. The inputs DIN44 to DIN49 have an identical structure.

DIN44 ... DIN49

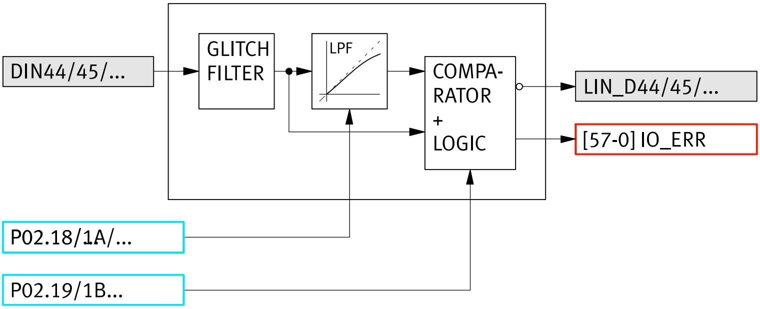


Fig. 18: Block diagram of the single-channel inputs

Term/abbreviation	Explanation
DIN40A/..., DIN40B/...	Two-channel digital inputs DIN40A/DIN40B ...
GLITCH FILTER	Filter for interference
LPF	Low-pass filter
COMPARATOR + LOGIC	Comparator and logic
LIN_x	Logical inputs ...
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Tab. 26: Legend for block diagram of the single-channel inputs

The signal levels at inputs DIN44 to DIN49 are first dejammed in a preliminary EMC filter, the “glitch filter”. The filter time constant is 500 µs and cannot be parameterised.
After this first filter, a second “LPF” filter, which can be parameterised using the parameter “Filter time constant” (P02.18), follows for each input signal, and is designed as a programmable monoflop. It is used for the following purposes:
- filtering out external test pulses, e.g. of an active sensor with OSSD outputs.
- filtering out the test pulses of DOUT4x in the case of passive sensors.
- filtering out contact bounces.

In a downstream logic operation with comparator the two input signals are used to form the logical control signal LIN_D44/.../49 (LIN_D44/.../49 = 1 equates to Control function requested). The test pulses at the input are also analysed in this section.
The sensor type can be selected using the parameter “Sensor type” (P02.28 ... P02.2D).

Input DIN44/ ... /49	Standstill state	Control function requested
DIN44 / ... / 49	0 V	24 V
Status LIN_D44 / ... /49	0	1

Tab. 27: Inputs, antivalent switching

The logic state directly represents the voltage level at the input - in contrast to the two-channel inputs DIN40...DIN43, which follow the quiescent current principle. The inputs are thus designed for control functions that require positive logic. Example: mode selector switch

If you use single-channel inputs or a combination thereof to request safety functions, the quiescent current principle must be observed:

- Use the inverted logic signal to request the safety function.

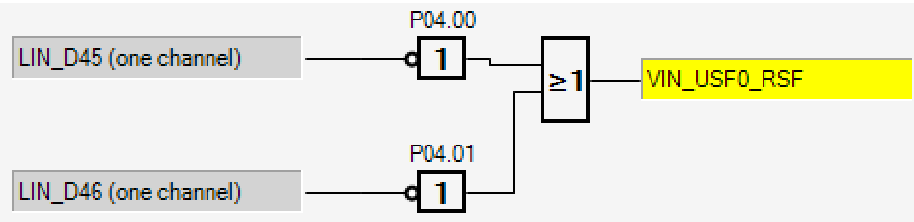


Fig. 19: Use of the inverted logic signal to request the safety function (example)

Error detection

The inputs can be monitored using test pulses. The test pulse source (DOUT40 to DOUT42) is selected with the parameter “Source for test pulse” (P02.19/...).

In the following cases, error “[57-0] Self-test I/O (internal/external)” is reported:

– A test pulse remains off.

– The input logic detects a short circuit or cross circuit.

In cases of error, the logical input LIN_D44 switches to 1 (Control function requested).

NOTICE

A detected error is forwarded to the error management using the error signals shown in the block diagram. The reaction to the error can be set (warning only, STO, SS1, SS2, etc.). In this case, for further processing, the logical input LIN_D44 takes status 1.

The user must ensure that an error (error management) leads to the safe status of the entire system.

Parameters for the single-channel digital inputs

Parameter no. for input ...						**Name**	**Description**
DIN44	DIN45	DIN46	DIN47	DIN48	DIN49		
P02.28	P02.29	P02.2A	P02.2B	P02.2C	P02.2D	Sensor type	Identifier of the sensor connected to DIN4x.
P02.19	P02.1B	P02.1D	P02.1F	P02.21	P02.23	Source for test pulse	Selection of the output supplying the test pulses.

Parameter no. for input ...						Name	Description
DIN44	DIN45	DIN46	DIN47	DIN48	DIN49		
Expert parameters							
P02.18	P02.1A	P02.1C	P02.1E	P02.20	P02.22	Filter time constant	Filter time constant

Tab. 28: Digital inputs

Timing diagram

The following figure shows the timing diagram of a single-channel input:

Digital Input DIN44

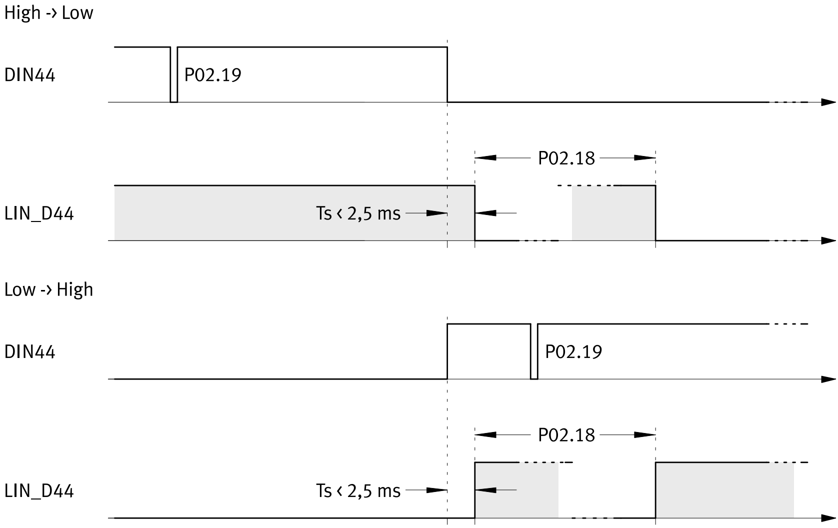


Fig. 20: Timing diagram of single-channel input (example DIN44)

After the request of a control function via DIN44 ... DIN49, the following times elapse until the logical input LIN_D... is switched to active:

Time delays from the level change	Minimum	Maximum	Typical
Ts	0.5 ms	2.5 ms	1.5 ms
Filter time constant (P02.18/1A/1C/1E/20/22)	1.0 ms	10.0 ms	3.0 ms
Reaction time	1.5 ms	12.5 ms	4.5 ms

Tab. 29: Time delays DIN44 ... DIN49

Technical data for the control inputs in the specified operating range of logic voltages to EN 61131-1
➔ Tab. 143 Technical data: digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40].

3.5 Safety functions

The safety functions have a two-part structure, which can be seen in all the functions:

Safety Function

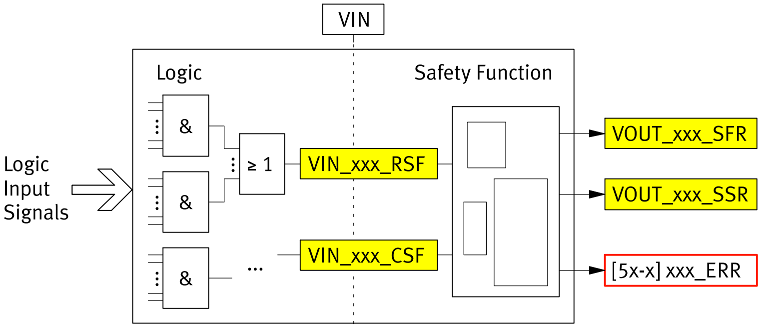


Fig. 21: Block diagram of the general structure of the safety functions

Term/abbreviation	Explanation
Logic Input Signals	Logical input signals
Logic	Logic, configurable for the safety functions using product terms
Safety Function	Safety function
VIN_xxx_RSF	Virtual input: request safety function xxx (Request Safety Function)
VIN_xxx_CSF	Virtual input: terminate safety function xxx request (Clear Safety Function request)
VOUT_xxx_SFR	Virtual output: safety function xxx requested (Safety Function requested)
VOUT_xxx_SSR	Virtual output: safety function xxx safe state reached (Safe State Reached)
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Tab. 30: Legend for the block diagram of the general structure of the safety functions

Logic section (left part)

A configurable logic function (AND or OR gate in disjunctive standard format) is used to define which input signals (LIN_x) are switched to the safety function for:

– requesting the safety function, VIN_xxx_RSF signal (Request Safety Function)
– terminating the request for the safety function, VIN_xxx_CSF signal (Clear Safety Function)
– selecting additional feedback signals (e.g. for SBC)

ⓘ

The input logic for the STO function may appear as follows in the “Request” tab in the SafetyTool, for example:

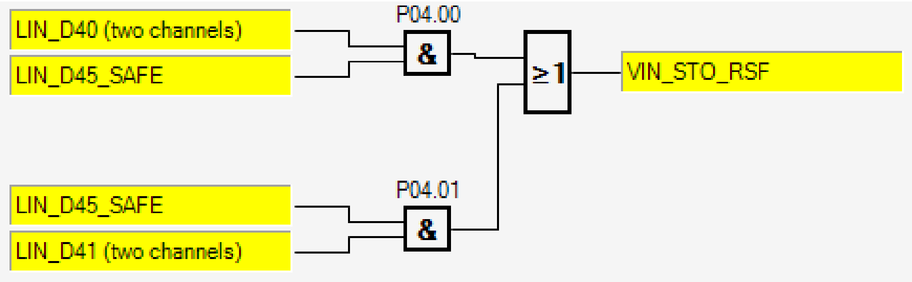


Fig.22

The STO function is requested via DIN40 if the mode selector switch DIN45 is active or via DIN41 if the mode selector switch DIN45 is not active. For every VIN... input there is an OR gate with four inputs and upstream AND gates with seven inputs. All signals can also be inverted.

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

Safety function (right part)

So long as the safety function is requested it safely monitors the status variables of the drive. It contains the required logic and sequence functions for this, and these can be parameterised.

The logic and sequence function are initialised on the rising edge of the request. For example, the start values for the braking ramps are calculated in this manner.

The safety function takes the current status of the drive (position, speed) into account and generates various status messages and control signals. The most important functions are described in brief below:

- A parameter is used to define whether the safety function should be terminated automatically after the request is cancelled.
- The stop functions have an additional control input to request the safety function. This input, ERR_xxx_RSF, is supplied directly from the error management, because the stop function can also be requested as error response by the error management.
- Some safety functions can also be requested directly from other safety functions. For example, STO is automatically activated at the end of the braking ramp of an SS1 function, but is also terminated with it as well.

Every safety function provides at least the following output signals

- the status message VOUT_xxx_SFR, safety function xxx requested,
- the status message VOUT_xxx_SSR, safe state xxx reached,
- at least one error message xxx_ERR if the safety condition is violated.

In addition, some safety functions provide additional control signals, e.g.

- for direct activation of the hardware, e.g. the driver supply or holding brake output for the safe brake control,
- for the request of downstream safety functions, e.g. STO_SBC_RSF.

These output signals can be transmitted to the function controller as a status message. They can be used to activate external safety relay units via safe outputs. For example, an external clamping unit can be controlled.

Safety functions for motion monitoring also use the safely detected speed (ACTUAL_SPEED) or the safely detected position (ACTUAL_POSITION) for monitoring. They control the approved speed in the functional section of the motor controller via a speed limit (SPEED_LIMIT).
The safety functions are configured using a series of parameters. The following can be set:
- speed ramps,
- monitoring limits for speed and position,
- time delays.

Additional configurable options are:
- the behaviour for terminating the safety function.
- the way in which the safety module manipulates operation of the basic unit:
  - it does not manipulate actively and only monitors.
  - it activates the quick stop in the basic unit and causes the basic unit to perform a quick stop while monitoring the braking operation.
  - it actively regulates the speed in the basic unit downwards and, at the same time, monitors compliance with the limit values.

EN 61800-5-2 defines the various safety functions for servo drives. It also defines three methods for monitoring braking. The above configuration enables the safety module to support all the methods listed in the standard.
The safety module supports the safe stop and movement functions described in the following sections.

3.5.1 STO – Safe Torque Off

Application

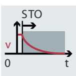


Fig. 23: STO symbol

The function implements the STO safety function in accordance with EN 61800-5-2 (stop category 0 from EN 60204-1).
Use the “Safe Torque Off” function (STO) whenever you have to safely disconnect the power supply to the motor in your particular application but there are no additional requests for targeted shutdown of the drive.

The STO function is activated by the factory setting (pre-parameterisation).
Because the function is used by other functions (request by SS1 or error response on violation of other requested safety functions), it cannot be deselected.

Function

The “Safe Torque Off” function switches off the driver power supply for the power semiconductor, thus preventing the power output stage from supplying the power required by the motor.
The power supply to the drive is safely disconnected when the STO “Safe Torque Off” safety function is active. The drive cannot generate torque and so cannot perform any dangerous movements. With suspended loads or other external forces, additional measures must be taken to ensure that the load does not drop (e.g. mechanical clamping units). The standstill position is not monitored in the STO “Safe Torque Off” state.
The machine must be stopped and locked in a safe manner. This especially applies to vertical axes without automatic locking mechanisms, clamping units or counterbalancing.

NOTICE

There is a danger that the drive will advance if there are multiple errors in the CMMP-AS-...-M3.
If the power stage of the motor controller fails during the STO state (simultaneous short circuit of 2 power semiconductors in different phases), this can result in a limited detent movement of the rotor. The rotation angle/travel corresponds to a pole pitch.
Examples:

- rotary axis, synchronous machine, 8-pole ➔ movement < 45° at the motor shaft.
- linear motor, pole pitch 20 mm ➔ movement < 20 mm at the moving part.

ⓘ

The STO (Safe Torque Off) function does not provide protection against electric shock, only against dangerous movements! The drive is not disconnected from the power supply as required for electrical safety ➔ Hardware description, GDCP-CMMP-M3-HW-...

The logic to request the STO safety function is shown in the following block diagram:

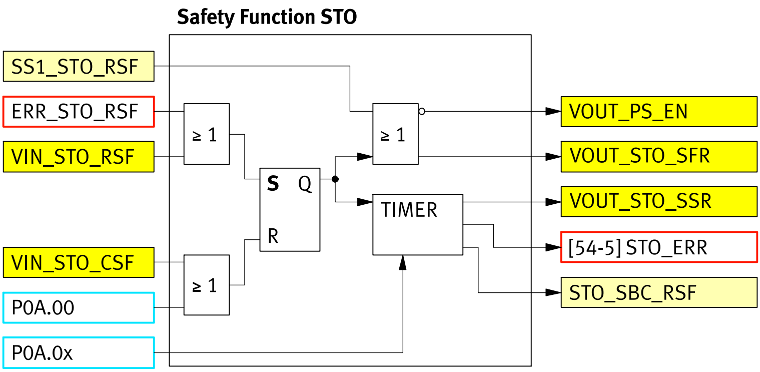


Fig. 24: STO block diagram

Term/abbreviation	Explanation
Safety Function STO	STO safety function
SS1_STO_RSF	Internal signal: STO request by SS1

Term/abbreviation	Explanation
ERR_STO_RSF	Internal signal: request STO by error response
VIN_STO_RSF	Virtual input: request STO
VIN_STO_CSF	Virtual input: terminate STO request
TIMER	Timer
VOUT_PS_EN	Virtual output: power stage enable approved
VOUT_STO_SFR	Virtual output: STO requested
VOUT_STO_SSR	Virtual output: safe state STO reached
[54-5] STO_ERR	Internal error signal: error 54-5
STO_SBC_RSF	Internal signal: request SBC by STO

Tab. 31: Legend for the STO block diagram

The safety function is requested as follows:
- by the user via any combination of input signals LIN_D... that lead to the VIN_STO_RSF signal
- as error response, controlled via the error management system, signal ERR_STO_RSF.
- via the safety function SS1, signal SS1_STO_RSF.

The request for the safety function STO is cancelled as follows:
- by the user via a combination of different inputs that lead to the VIN_STO_CSF signal
- by setting the parameter “Automatic restart allowed” (P0A.00).
  As a result, the safety function is automatically ended after the request is terminated.

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.
The safety function controls the switch-off of the driver supply via the VOUT_PS_EN signal. If necessary, the safety function SBC can also be requested automatically with the STO_SBC_RSF signal.
The safety function also generates the status messages:
- VOUT_STO_SFR, safety function STO requested.
- VOUT_STO_SSR, safe state STO reached.

Error detection

The power supply to the drive is disconnected safely and immediately when the safety function STO “Safe Torque Off” is active. This is ensured by a two-channel allocation of the cut-off circuit, which is checked continuously during operation. If one cut-off channel fails, an error message is generated. The drive is switched off by the remaining channel.
The error message [54-5] STO_ERR “Safety condition STO violated” is output in the event of an error in the STO function.

Sequence

The sequence of the STO safety function is shown in the following diagram:

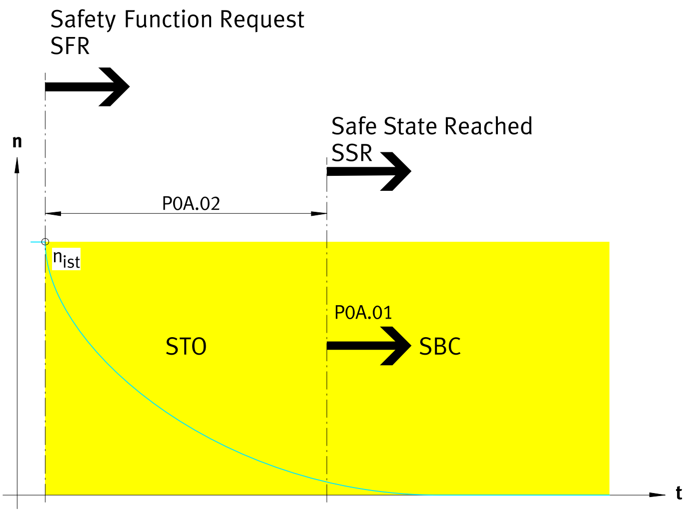


Fig. 25: STO flowchart

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
n_{act}	Actual speed

Tab. 32: Legend for STO flowchart

When the safety function STO is requested, the driver supply is switched off immediately and without any significant delay via two channels.
After a configurable delay time “Delay time to STO signal” (P0A.02), the internal status VOUT_STO_SSR “Safe state reached” becomes active.
After the request of the safety function STO, the following times elapse until the safety function is activated:

Time delays from VIN_STO_RSF	Minimum	Maximum	Typical
VOUT_STO_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_STO_SSR	2.0 ms + P0A.02	2.1 ms + P0A.02	2.0 ms + P0A.02
Reaction time until switch-off of driver supply for basic unit and power stage OFF	2.5 ms	4.5 ms	3.5 ms

Tab. 33: STO time delays

Parameters for STO

STO: Safe Torque Off		
No.	Name	Description
P0A.02	Time delay until "STO" signal	Time delay until the "Safe state reached" output becomes active.
P0A.00	Automatic restart permitted	If set: cancellation of the request (restart) with inactive request input
P0A.01	Automatic activation of SBC	If set: safe brake control is activated when the safe state is reached (after the delay time has expired).

Tab. 34: STO: Safe Torque Off

3.5.2 SBC – Safe Brake Control

Application

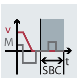


Fig. 26: SBC symbol

The function implements the safety function SBC in accordance with EN 61800-5-2. Use the "Safe Brake Control" (SBC) function to activate a clamping unit or holding brake in order to mechanically brake an axis in a controlled manner or to hold it securely.
The clamping unit or holding brake can optionally be controlled by:
- the safe brake output [X6] in the motor controller,
- a safe output of the safety module and an external brake switching device.

ⓘ

Important: to use the safety function SBC, a clamping unit or holding brake with appropriate safety classification must be used. A risk assessment must always be carried out for all types of clamping units without certification and the suitability for the relevant safety-related application must be determined. Otherwise they must not be used. The holding brake in motors is not usually appropriately qualified.

ⓘ

The SBC function is activated by the factory setting (pre-parameterisation).
The function cannot be deselected as long as it is used by other functions (request by STO, by other parameterisations or by error response when other requested safety functions are violated).

Function

The "Safe Brake Control" function immediately switches off the power for the connected clamping unit or holding brake. The clamping unit or holding brake is actuated and brakes the motor or the axis. Dangerous movements are mechanically braked. The braking time is dependent on how quickly the brake engages and how high the energy level is in the system.

NOTICE

If there are suspended loads, they usually drop if SBC is requested simultaneously with STO. This can be traced back to the mechanical inertia of the clamping unit or holding brake and is thus unavoidable.
The safety module also makes the safety function SS1 available in combination with SBC or the safety function SS2. Check whether these safety functions can or should be used in your application with SBC instead of STO.

Safe brake control can only be used with clamping units or holding brakes that are engaged in the de-energised state. The clamping unit or holding brake is then opened by supplying energy.
When using the brake output of the basic unit, ensure that the cables are routed so that they are protected. If the load capacity of the safe outputs of the safety module is sufficient, then detection of shorts across contacts with test pulses is possible.
The logic to request the SBC safety function is shown in the following block diagram:

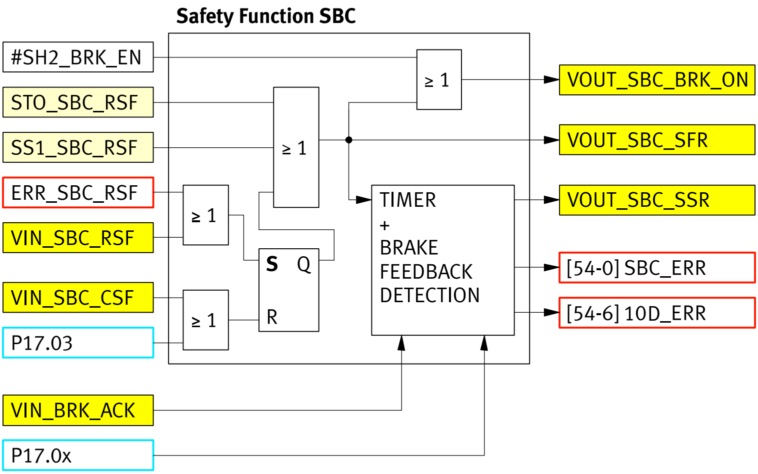


Fig. 27: Block diagram SBC

Term/abbreviation	Explanation
Safety Function SBC	Safety function SBC
#SH2_BRK_EN	The basic unit enables safe brake control
STO_SBC_RSF	Internal signal: request SBC by STO
SS1_SBC_RSF	Internal signal: request SBC by SS1
ERR_SBC_RSF	Internal signal: request SBC by error response
VIN_STO_RSF	Virtual input: request SBC
VIN_STO_CSF	Virtual input: terminate SBC request
VIN_BRK_ACK	Virtual input: evaluation of safe brake control feedback signal

Term/abbreviation	Explanation
TIMER + BRAKE FEEDBACK DETECTION	Timer and evaluation of safe brake control feedback
VOUT_SBC_BRK_ON	Virtual output: switch brake output
VOUT_SBC_SFR	Virtual output: SBC requested
VOUT_SBC_SSR	Virtual output: SBC safe state reached
[54-0] SBC_ERR	Internal error signal: error 54-0
[54-6] 10D_ERR	Internal error signal: error 54-6

Tab. 35: Legend for block diagram SBC

The SBC safety function is requested as follows:
- By the user via any combination of input signals LIN_D... that lead to the VIN_SBC_RSF signal.
- As error response, controlled via the error management system, signal ERR_SBC_RSF.
- Via the safety function STO, signal STO_SBC_RSF.
- Via the safety function SS1, signal SS1_SBC_RSF.

The request for the safety function SBC is cancelled as follows:
- By the user via a combination of different inputs that lead to the VIN_SBC_CSF signal.
- By setting parameter P17.03, the safety function is automatically ended after the request is cancelled.

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.
The safety function controls the switch-off of the safe brake control via the VOUT_SBC_BRK_ON signal. If the safety function is requested, VOUT_SBC_BRK_ON = 1. VOUT_SBC_BRK_ON is additionally linked internally with a control signal from the basic unit, which reflects the switching status of the brake control in the basic unit. Safe brake control is only energised if SBC is not requested and the basic unit enables the brake (#SH2_BRK_EN is Low).

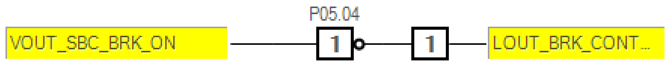
ⓘ

After a request of SBC and subsequent cancellation, the safe brake control is only energised when the basic unit enables the holding brake.
This ensures that Z-axes with a suspended load can be restarted without the load dropping.

The control signal VOUT_SBC_BRK_ON must either be switched to the internal brake activation of the motor controller (control signal LOUT_BRAKE_CTRL, ➔ 9.1.4 Logical outputs LOUT) or to a digital output for control of an external clamping unit (LOUT_D4x, ➔ 9.1.4 Logical outputs LOUT).

ⓘ

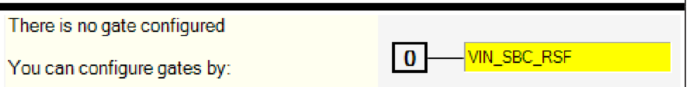
To use the brake control of the basic unit at [X6] in combination with SBC, configure the output “Internal brake” of the safety module:

Configure “Internal brake” output				
Requirement:				
Standard parameters:	P02.36	Operating mode		Equivalent = [1]
	P02.37	Test pulse length	ms	1,0

Tab. 36

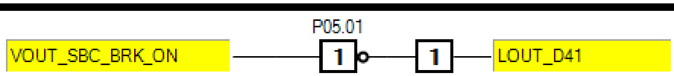
The brake control of the basic unit is now additionally monitored using test pulses.
The motor controller detects that safe brake control is switched off from the outside. It performs a quick stop if necessary and switches off the power stage. On the motor controller side, brake control can also be switched on continuously (use of the parameters from the holding brake control in the motor controller) so it is controlled exclusively via the safety module.

To use the brake control of the basic unit [X6] independently of SBC and to use SBC in combination with DOUT4x, configure the “Internal brake” output of the safety module to Continuous ON:

Configure “Internal brake” output to Continuous ON				
Requirement:				
Standard parameters:	P02.36	Operating mode		Static High = [2]
	P02.37	Test pulse length	ms	1,0

Tab. 37

In addition, configure an output, e.g. DOUT41, as an output of the control signal for the safe brake control:

Configure output DOUT41				
Requirement:				
Standard parameters:	P02.36	Operating mode		Equivalent = [1]
	P02.37	Test pulse length	ms	1,0

Tab. 38

If the SBC function controls an external clamping unit or holding brake via a digital output, the control signals for the internal safe brake control in the basic unit can be configured in such a way that SBC no longer has an effect on them. The brake output of the basic unit is then available for other functions (=› control signals FSM_BR+_EN and FSM_BR-_EN can be parameterised to high).

Information on parameterisation of the brake output can be found in the ➔ Description of functions for the CMMP-AS-...-M3, GDCP-CMMP-M3-FW-...
The control of a clamping unit with its increased power consumption (typically 8 A or more) requires an external circuitry via two intermediate contactors with forced feedback contacts. In this case, feedback must be wired separately. In this case, it is run to the safety module via a digital input, usually DIN44.
The SBC function also generates the status messages:

– VOUT_SBC_SFR, safety function SBC requested.
– VOUT_SBC_SSR, safe state SSBC reached (delay can be set with P17.01).

SBC output signals	Standstill state	Safety function requested/achieved
VOUT_SBC_BRK_ON	0	1
VOUT_SBC_SFR	0	1
VOUT_SBC_SSR	0	1 (delayed P17.01)

Tab. 39: SBC output signals

Error detection

The safety function can analyse an external feedback signal, thus checking that the clamping unit or holding brake has actually engaged. It is evaluated via the VIN_BRK_ACK input if this function is activated via parameter P17.02.
A time delay for feedback can be parameterised with parameter P17.00. The feedback signal is evaluated after the delay has expired. If there is no feedback, error message [54-0] SBC_ERR is generated.

NOTICE

If the brake output at [X6] is used, acknowledgement input VIN_BRK_ACK can be switched to the acknowledgement input of the basic unit (signal LIN_BRAKE_X6_FB). This signal maps the switching status of the safe brake output at the basic unit.
If there is a motor cable at brake output [X6] but a clamping unit or holding brake is not connected, then interference is possible in the open brake cable, leading to incorrect feedback (error [54-0]).

- In this case, deactivate the acknowledgement input.

NOTICE

If an external clamping unit is used, acknowledgement input VIN_BRK_ACK must be mapped to a safe digital input.
Only the status “Brake engaged” (level monitoring of VIN_BRK_ACR) is monitored. The feedback is not monitored if there is an "energised brake".

The SBC function also has integrated time monitoring:
The SBC function may be requested for a maximum of 10 days. The clamping unit or holding brake must therefore be switched (released) at least once within 10 days, because the circuit breakers can only be tested with test pulses when switched on.

The clamping unit or holding brake must then remain switched (released) for at least 20 s until all self-tests have been completed.
If the time limit is exceeded, error [54-6] 10D_ERR is generated.
The time restriction becomes invalid if the SBC function is used in connection with a safe output (DOUT40 ... DOUT42) or the holding brake is not used for safety purposes. The 10-day monitoring can then be deactivated using expert parameter P17.04.

NOTICE

When the safety module is delivered, the SBC function is always configured in conjunction with the output [X6], even if you do not wish to use the SBC function.
In the following application, an interference coupling into the open brake lines can cause the safety module to report error 57-0:

- The brake control cables are routed in the motor cable.
- A holding brake is not connected on the motor side.

In this case:

- Disconnect brake control cables at [X6]
- Connect brake control cables to [PE].

Sequence:
The sequence of the SBC safety function is shown in the following diagram:

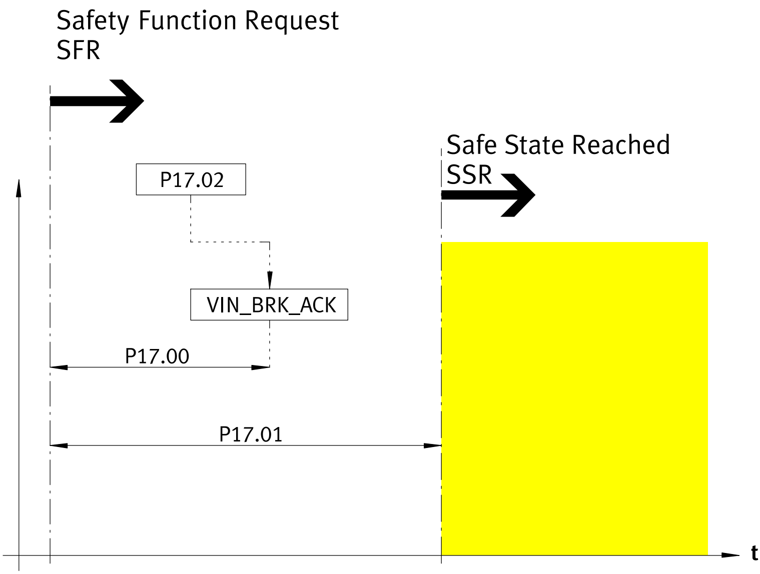


Fig. 28: SBC flowchart

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
VIN_BRK_ACK	Virtual input: evaluation of holding brake feedback signal

Tab. 40: Legend for SBC flow chart

If the SBC safety function is requested, the following times elapse for the switch-off of the clamping unit or holding brake (VOUT_SBC_BRK_ON) and the feedback signals from the safety function:

Time delays from VIN_SBC_RSF	Minimum	Maximum	Typical
VOUT_SBC_BRK_ON	2.0 ms	2.1 ms	2.0 ms
VOUT_SBC_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SBC_SSR	2.0 ms + P17.01	2.1ms + P17.01	2.0 ms + P17.01
Error reaction time for missing feed-back VIN_BRK_ACK	2.0 ms + P17.00	2.1 ms + P17.00	2.0 ms + P17.00

Tab. 41: SBC time delays

Parameters for SBC

SBC: Safe Brake Control		
No.	Name	Description
P17.00	Evaluation of brake feedback time delay	Time from the request of the safety function by which the feedback from the holding brake must be received.
P17.01	Time delay to “Brake engaged” signal	Time delay after request of the safety function until the “Safe state reached” output becomes active
P17.02	Evaluate holding brake feedback	If 1: evaluate feedback of the holding brake.
P17.03	Automatic restart permitted	If 1: cancellation of the request (restart) if an inactive request arrives

SBC: Safe Brake Control		
No.	Name	Description
Expert parameters		
P17.04	Deactivate cyclical test/10-day monitoring	Set to 0 if the holding brake output on the basic unit is used for SBC. Set to 1 if an external brake is controlled via DOUT4x for SBC If 1: the cyclical test of brake control and 10-day monitoring for actuation of the holding brake by the basic unit is deactivated. The safe brake output of the basic unit can be used as a “normal” DOUT with a high acceptable current load.

Tab. 42: SBC: Safe Brake Control

3.5.3 SS1 – Safe Stop 1

Application

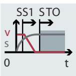


Fig. 29: SS1 symbol

The function implements the SS1 safety function according to EN 61800-5-2. Use the “Safe Stop 1” function (SS1) whenever you have to brake the motor and then safely disconnect the power supply to the motor in your particular application but there are no additional requests for targeted stopping of the drive (cf. stop category 1 in EN 60204-1).
The three characteristics described in the standard are supported:
a) Triggering and controlling the rate of motor deceleration within specified limits and triggering the STO function when the motor speed falls below a specified limit value.
➔ The drive is guided along a braking ramp until detection of standstill (P06.09), then the power stage is switched off.
b) Triggering and monitoring the rate of motor deceleration within specified limits and triggering the STO function when the motor speed falls below a specified limit value.
➔ The safety module activates a quick stop in the basic unit, the braking ramp is monitored, then the power stage is switched off.
c) Triggering the motor deceleration and after an application-specific time delay, triggering the STO function.
➔ The safety module returns a status message; the basic unit must be braked by the function controller; the power stage is switched off after a waiting time.

The SS1 function is activated by the factory setting (pre-parameterisation).
As long as the function is used by other functions (error response on violation of other requested safety functions), it cannot be deselected.

Function

When requesting the SS1 safety function, it checks that the drive is braked to standstill within a defined time using a defined braking ramp. After the defined time has elapsed, STO is triggered and the power output stage is switched off safely.

NOTICE

If there are suspended loads, they usually drop if STO is requested immediately after the braking ramp has elapsed.
For this reason, the SS1 can also trigger SBC, meaning that an existing clamping unit or holding brake engages, preventing an axis from dropping. SBC then triggers STO (linkage of the safety functions SS1 → SBC → STO).

The logic to request the SS1 safety function is shown in the following block diagram:

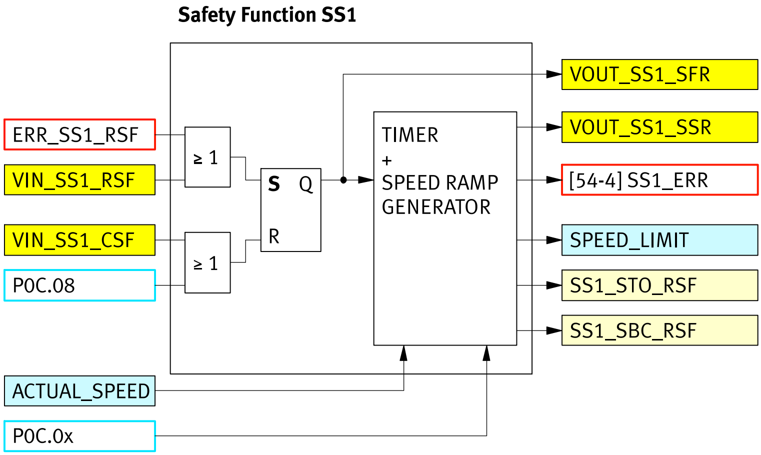


Fig. 30: Block diagram SS1

Term/abbreviation	Explanation
Safety Function SS1	Safety function SS1
ERR_SS1_RSF	Internal signal: request SS1 by error response
VIN_SS1_RSF	Virtual input: request SS1
VIN_SS1_CSF	Virtual input: terminate SS1 request
ACTUAL SPEED	Internal signal: current speed

Term/abbreviation	Explanation
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_SS1_SFR	Virtual output: SS1 requested
VOUT_SS1_SSR	Virtual output: SS1 safe state reached
[54-4] SS1_ERR	Internal error signal: error 54-4
SPEED_LIMIT	Internal signal: speed limit in basic unit
SS1_STO_RSF	Internal signal: STO request by SS1
SS1_SBC_RSF	Internal signal: request SBC by SS1

Tab. 43: Legend for SS1 block diagram

The SS1 safety function is requested as follows:
- By the user via any combination of input signals LIN_D... that lead to the VIN_SS1_RSF signal.
- As error response, controlled via the error management system, signal ERR_SS1_RSF.

The request of the safety function SS1 is cancelled as follows:
- By the user via a combination of different inputs that lead to the VIN_SS1_CSF signal.
- The safety function is automatically terminated after the request is cancelled by setting the parameter “Automatic restart allowed” (P0C.08).

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

The safety function controls the following safety functions directly:
- STO via the SS1_STO_SFR signal.
- SBC via the SS1_SBC_SFR signal.

When the request for the SS1 function is terminated, the safety functions that follow directly are also terminated automatically.

In addition, the SS1 function also supplies some control signals for activation of the basic unit:
- limits for speed in the basic unit, SPEED_LIMIT.
- a control signal to trigger the quick stop ramp in the basic unit (not shown in the block diagram).

The SS1 function also generates the status messages:
- VOUT_SS1_SFR, safety function SS1 requested
- VOUT_SS1_SSR, safe state SS1 reached

SS1 output signals	Standstill state	Safety function requested/achieved
VOUT_SS1_SFR	0	1
VOUT_SS1_SSR	0	1 (delayed via P0C.01 + P0C.0C + P0C.0B)

Tab. 44: SS1 output signals

Error detection

The safety function compares the current speed (ACTUAL_SPEED) with the calculated speed ramp at regular intervals. If the current speed is outside the permitted speed range for a parameterisable time "Allowable time for limit violation" (P0C.02), error [54-4] SS1_ERR is triggered.

With SS1, the status "Safety condition violated" is not cancelled if the drive is back in the permitted range after a temporary violation.

ⓘ

If the safety condition is violated, EN 61800-5-2 requires "STO" as an error response. However, in some applications, other error responses may be appropriate, e.g. "STO + SBC" ➔ 3.8.2 Parameterisation of the error response of the safety module.

Sequence

The sequence of the SS1 safety function is shown in the following diagram:

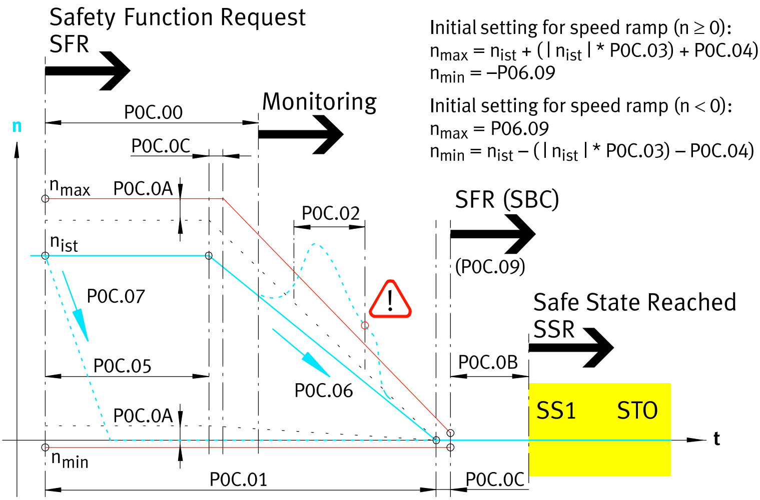


Fig. 31: SS1 flowchart

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
SFR (SBC)	SBC request
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed

Tab. 45: Legend for SS1 flowchart

ℹ

The flowchart and the following description apply for a positive speed n_{act}. This applies correspondingly for a negative speed, in which case n_{act} is delayed to zero by a negative speed.

After the request from SS1, the safety module starts a braking ramp to monitor the braking operation:
- A time delay is defined using “Time delay until monitoring starts” (P0C.00).
  Only after this time is compliance with the current speed limit values monitored.
- The duration of the braking ramp is specified by “Time for braking ramp” (P0C.01).
- If “Automatic activation SBC” (P0C.09) was activated, then the SBC safety function is triggered after the “Time for braking ramp” (P0C.01) has elapsed, otherwise STO is triggered.
- Only with SBC triggering (P0C.09 = 1):
  The mechanical delay time of the clamping unit or holding brake can be taken into account using “Delay after expiry of P0C.01 until STO is triggered” (P0C.0B). After the time P0C.01 + P0C.0B expires, STO is triggered and the VOUT_SS1_SSR message is set.
  The time P0C.0B must always elapse, even if P0C.01 = 0.
- The start value of the monitoring braking ramp, nmax, is calculated according to the equation in the diagram and can be parameterised via “Braking ramp - Start value factor” (P0C.03) and “Braking ramp - Start value offset” (P0C.04). The ramp ends at speed = 0.
  Tolerance is specified by the limit value “Speed threshold value for standstill detection” (P06.09).
- A time delay for the start of the braking ramp can be parameterised using “Braking ramp - time delay to start” (P0C.05).

ℹ

If the braking operation at SS1 is not to be controlled by the safety module but by the function controller, P0C.05 can be used to parameterise a delay to the ramp in order to compensate for the reaction time of the controller.

Active limiting of the speed in the basic unit is switched on with the parameter “Actively limit speed in the basic unit” (P0C.06):
- Current speed values are transmitted at regular intervals to the basic unit. The speed limits must have a safety gap to the monitoring limits. This gap is set with the parameter “Speed offset for limiting in the basic unit” (P0C.0A).
- At the end of the monitoring braking ramp the speed limit = 0.
- The basic unit actively limits the speed setpoint and, depending on the parameterisation, also the travel speed of running positioning operations.

The quick stop is activated in the basic unit with the “Activate quick stop ramp in the basic unit” parameter (P0C.07):
- When SS1 is requested, the quick stop ramp in the basic unit is activated automatically and the drive brakes to zero using the quick stop ramp.

NOTICE

To avoid a violation of the safety condition during braking via the quick stop ramp of the basic unit:
- Make sure that the ramp time parameterised via “Time for braking ramp” (P0C.01) is greater than the braking time of the basic unit at the quick stop ramp from maximum speed.

The SafetyTool will indicate a possible conflict during parameterisation.

After termination of the request of the SS1 function, the internal control signals for the quick stop and the speed limiting in the basic unit are reset.

Notes on parameterisation mode a), b) and c) in accordance with EN 61800-5-2

Mode	Parameterisation
Mode a)	Set “Actively limit speed in basic unit” (P0C.06). The safety module controls the braking ramp in the basic unit using the parameters set in the safety module for the ramp.
Mode b)	Set “Activate quick stop ramp in the basic unit” (P0C.07). The safety module initiates the basic unit braking with the quick stop ramp and also simultaneously monitors the braking ramp set in the safety module.
Mode c)	Do not parameterise braking ramp: The function controller must brake the axis, which requires the signal VOUT_SS1_SFR or the common message VOUT_SFR to be sent to the function controller ➔ Section B.1.5. Using “Time delay until monitoring starts” (P0C.00), set the desired time until the axis is at standstill and SS1 monitoring should actuate, and always ensure that this is at least 4 ms. A braking ramp is not monitored beforehand. Set “Time for braking ramp” (P0C.01), “Rotational speed ramp - time delay monitoring” (P0C.0C) and “Time delay after reaching n = 0 until STO is triggered” (P0C.0B) to the minimum value (2 ms each).

Tab. 46: Parameterisation mode a), b) and c) in accordance with EN 61800-5-2

The following times elapse after the request of the safety function SS1 until the safety function is activated and errors are detected:

Time delays from VIN_SS1_RSF	Minimum	Maximum	Typical
VOUT_SS1_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SS1_SSR	2.0 ms + P0C.01 + P0C.0B + P0C.0C	2.1 ms + P0C.01 + P0C.0B + P0C.0C	2.0 ms + P0C.01 + P0C.0B + P0C.0C
Detection of a violation of the safety condition after VOUT_SBC_SFR	2.0 ms + P0C.00 + P0C.02	2.1 ms + P0C.00 + P0C.02	2.0 ms + P0C.00 + P0C.02

Tab. 47: SS1 time delays

Parameterise P0C.00 so that it is smaller than the braking ramp to STO (P0C.01 + P0C.0B + P0C.0C). If the “Time delay until monitoring starts” (P0C.00) is parameterised greater than the total braking ramp to STO (P0C.01 + P0C.0B + P0C.0C), then STO and thus the signal SS1_SSR are also only reached after 2.1 ms + P0C.00.

Parameters for SS1

SS1: Safe Stop 1		
No.	Name	Description
P0C.00	Time delay until monitoring starts	Time from the safety function request during which rotational speed is not monitored
P0C.01	Time for braking ramp	Time from the safety function request, after which the rotational speed ramps are stopped and the safe status is reached.
P0C.02	Allowable time for limit value overrun	Time interval during which the actual rotational speed value may be outside the limits before the “Safety condition violated” status is reached.
P0C.06	Actively limit speed in basic unit	If set: control the rotational speed of the basic unit
P0C.07	Activate quick stop ramp in the basic unit	If set: when the safety function is requested, the quick stop command (control cable) is applied to the basic unit
P0C.08	Automatic restart permitted	If set: cancellation of the request (restart) with inactive request input
P0C.09	Automatic activation of SBC	If set: safe brake control is activated when standstill is reached or after the time delay has expired.
Expert parameters		
P0C.0C	Speed ramp - monitoring time delay	Time delay between the rotational speed ramp that is written to the basic unit and the start of monitoring by the safety module.
P0C.0B	Delay after expiry of P0C.01 until STO is triggered	Time after which STO is triggered at the end of the braking operation.
P0C.05	Braking ramp - time delay to start	Time delay after which the ramps start.

SS1: Safe Stop 1

No.	Name	Description
P0C.03	Braking ramp - start value factor	Factor for calculating the start value of the rotational speed ramps.
P0C.04	Braking ramp - start value offset	Offset for calculating the start value of the rotational speed ramps.
P0C.0A	Speed offset for the limitation in the basic unit	Offset for rotational speed limits to control the basic unit.

Tab. 48: SS1: Safe Stop 1

3.5.4 SS2 – Safe Stop 2

Application

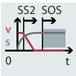


Fig. 32: SS2 symbol

The function implements the SS1 safety function according to EN 61800-5-2. Use the “Safe Stop 2” function (SS2) if you brake the motor in your application and must then ensure that the motor will not deviate from the holding position by more than a specified amount (cf. stop category 2 in EN 60204-1).
The three characteristics described in the standard are supported:
a) Triggering and controlling the rate of motor deceleration within specified limits and triggering the SOS function when the motor speed falls below a specified limit value.
➔ The drive is taken through a braking ramp until it is detected as at standstill (P06.09), after which a safe operating stop is executed.
b) Triggering and monitoring the rate of motor deceleration within specified limits and triggering the SOS function when the motor speed falls below a specified limit value.
➔ The safety module activates a quick stop in the basic unit, the braking ramp is monitored, after which a safe operating stop is executed.
c) Triggering the motor deceleration and after an application-specific time delay triggering the SOS function.
➔ The safety module returns a status signal, the basic unit must be braked by the function controller. After a waiting time, the safety function SOS is activated.

ℹ

The SS2 function can also be used as an error response when other requested safety functions are violated. This requires the function to be activated and parameterised.

Function

When requesting the SS2 safety function, it checks that the drive is braked to standstill within a defined time using a defined braking ramp. After the defined time has elapsed, SOS is triggered and thus a safe operating stop executed.

The logic to request the SS2 safety function is shown in the following block diagram:

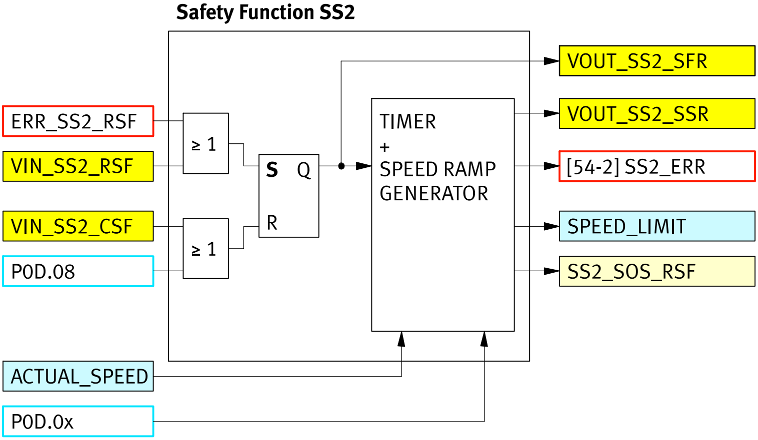


Fig. 33: Block diagram SS2

Term/abbreviation	Explanation
Safety Function SS2	Safety function SS2
ERR_SS2_RSF	Internal signal: request SS2 by error response
VIN_SS2_RSF	Virtual input: request SS2
VIN_SS2_CSF	Virtual input: terminate SS2 request
ACTUAL SPEED	Internal signal: current speed
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_SS2_SFR	Virtual output: SS2 requested
VOUT_SS2_SSR	Virtual output: SS2 safe state reached
[54-2] SS2_ERR	Internal error signal: error 54-2
SPEED_LIMIT	Internal signal: speed limit in basic unit
SS2_SOS_RSF	Internal signal: request SOS by SS2

Tab. 49: Legend for SS2 block diagram

The SS2 safety function is requested as follows:
- By the user via any combination of input signals LIN_D... that lead to the VIN_SS2_RSF signal.
- As error response, controlled via the error management system, signal ERR_SS2_RSF.

The request of the safety function SS2 is cancelled as follows:
- By the user via a combination of different inputs that lead to the VIN_SS2_CSF signal.
- The safety function is automatically terminated after the request is cancelled by setting the parameter “Automatic restart allowed” (P0D.08).

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.
The safety function controls the following safety functions directly:
– SOS via the signal SS2_SOS_RSF.
When the request for the SS2 function is terminated, the safety functions that follow directly are also terminated automatically.
In addition, the SS2 function also supplies some control signals for activation of the basic unit:
– limits for speed in the basic unit, SPEED_LIMIT.
– a control signal to trigger the quick stop ramp in the basic unit (not shown in the block diagram).
The SS2 function also generates the status messages:
– VOUT_SS2_SFR, safety function SS2 requested
– VOUT_SS2_SSR, safe state SS2 reached

SS2 output signals	Standstill state	Safety function requested/achieved
VOUT_SS2_SFR	0	1
VOUT_SS2_SSR	0	1 (delayed via P0D.01 + P0D.0A)

Tab. 50: SS2 output signals

Error detection
The safety function compares the current speed (ACTUAL_SPEED) with the calculated speed ramp at regular intervals. If the current speed is outside the permitted speed range for a parameterisable time "Allowable time for limit violation" (P0D.02), error [54-2] SS2_ERR is triggered.
With SS2, the status "Safety condition violated" is not cancelled if the drive is back in the permitted range after a temporary violation.
As soon as the drive has been braked to standstill, the safety function SOS is requested, which has its own error detection (position monitoring).

ℹ

If the safety condition is violated, EN 61800-5-2 requires "STO" as an error response. However, in some applications, other error responses may be appropriate, e.g. "STO + SBC" ➔ 3.8.2 Parameterisation of the error response of the safety module.

Sequence
The sequence of the SS2 safety function is shown in the following diagram:

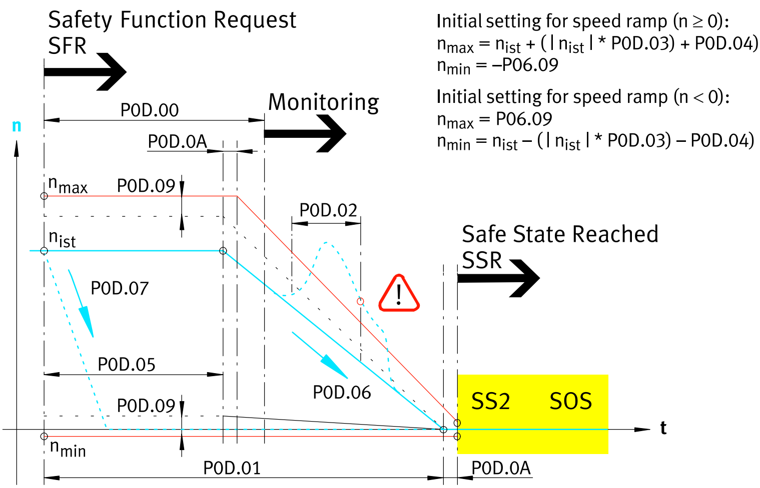


Fig. 34: SS2 flowchart

Term/abbreviation	**Explanation**
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed

Tab. 51: Legend for SS2 flowchart

The flowchart and the following description are applicable for a positive speed n_{act}. The chart mirrored on the time axis is applicable for a negative speed.

After the request from SS2, the safety module starts a braking ramp:

- A time delay is defined using “Time delay until monitoring starts” (P0D.00). Only after this time is compliance with the current speed limit values monitored.
- The duration of the braking ramp is specified by “Time for braking ramp” (P0D.01).
- The start value of the monitoring braking ramp, nmax, is calculated according to the equation in the diagram and can be parameterised via “Braking ramp - start value factor” (P0D.03) and “Braking ramp - start value offset” (P0D.04). The ramp ends at speed = 0 (tolerance is specified by the limit value for standstill detection “Speed threshold value for standstill detection” (P06.09)).
- A time delay for the start of the braking ramp can be parameterised with “Braking ramp - time delay to start” (P0D.05).

ⓘ

If the braking operation at SS2 is not to be controlled by the safety module but by the function controller, P0D.05 can be used to parameterise a delay to the ramp in order to compensate for the reaction time of the controller.

Active limiting of the speed in the basic unit is switched on with the parameter "Actively limit speed in the basic unit" (P0D.06):

- Current speed values are transmitted at regular intervals to the basic unit. The speed limits must have a safety gap to the monitoring limits. This gap is set with the parameter "Speed offset for limiting in the basic unit" (P0D.09).
- At the end of the monitoring braking ramp the speed limit = 0.
- The basic unit actively limits the speed setpoint and, depending on the parameterisation, also the travel speed of running positioning operations.

The quick stop is activated in the basic unit with the "Activate quick stop ramp in the basic unit" parameter (P0D.07):

- When SS2 is requested, the quick stop ramp in the basic unit is activated automatically and the drive brakes to zero using the quick stop ramp.

NOTICE

To avoid a violation of the safety condition during braking via the quick stop ramp of the basic unit:

- Make sure that the ramp time parameterised via P0D.01 is greater than the braking time of the basic unit at the quick stop ramp from maximum speed.

The SafetyTool will indicate a possible conflict during parameterisation.

After termination of the request of the SS2 function, the internal control signals for the quick stop and the speed limiting in the basic unit are reset.

Notes on parameterisation mode a), b) and c) in accordance with EN 61800-5-2

Mode	Parameterisation
Mode a)	Set “Actively limit speed in basic unit” (P0D.06). The safety module controls the braking ramp in the basic unit using the parameters set in the safety module for the ramp.
Mode b)	Set “Activate quick stop ramp in the basic unit” (P0D.07). The safety module initiates the basic unit braking with the quick stop ramp and simultaneously monitors the braking ramp set in the safety module.
Mode c)	Do not parameterise braking ramp: The function controller must brake the axis, which requires the signal VOUT_SS2_SFR or the common message VOUT_SFR to be sent to the function controller ➔ 9.1.5 Status words for the data exchange/diagnostics via fieldbus. Using “Time delay until monitoring starts” (P0D.00), set the desired time until the axis is at standstill and SS2 monitoring should actuate, and always ensure that this is at least 4 ms. A braking ramp is not monitored beforehand. Set “Time for braking ramp” (P0D.01), “Rotational speed ramp - time delay monitoring” (P0D.0A) to the minimum value (2 ms each).

Tab. 52: Parameterisation mode a), b) and c) in accordance with EN 61800-5-2

The following times elapse after the request of the safety function SS2 until the safety function is activated and errors are detected:

Time delays from VIN_SS2_RSF	Minimum	Maximum	Typical
VOUT_SS2_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SS2_SSR	2.0 ms + P0D.01 + P0D.0A	2.1 ms + P0D.01 + P0D.0A	2.0 ms + P0D.01 + P0D.0A
Detection of a violation of the safety condition after VOUT_SS2_SFR	2.0 ms + P0D.00 + P0D.02	2.0 ms + P0D.00 + P0D.02	2.0 ms + P0D.00 + P0D.02

Tab. 53: SS2 time delays

Parameterise P0D.00 less than the braking ramp to SOS (P0D.01 + P0D.0A).
If the “Time delay until monitoring starts” (P0D.00) is parameterised greater than the total braking ramp to SOS (P0D.01 + P0D.0A), SOS and thus the signal SS2_SSR are accordingly only reached after 2.1 ms + P0D.00.

Parameters for SS2

SS2: Safe Stop 2		
No.	Name	Description
P0D.00	Time delay until monitoring starts	Time from the safety function request during which rotational speed is not monitored. The monitoring limits of the SOS function are used for SS2.
P0D.01	Time for braking ramp	Time from the safety function request, after which the rotational speed ramps are stopped and the safe status is reached.
P0D.02	Allowable time for limit value overrun	Time interval during which the actual rotational speed value may be outside the limits before the "Safety condition violated" status is reached.
P0D.06	Actively limit speed in basic unit	If set: control the rotational speed of the basic unit
P0D.07	Activate quick stop ramp in the basic unit	If set: when the safety function is requested, the quick stop command (control cable) is applied to the basic unit
P0D.08	Automatic restart permitted	If set: cancellation of the request (restart) with inactive request input
Expert parameters		
P0D.0A	Speed ramp - monitoring time delay	Time delay between the start of the rotational speed ramp that is written to the basic unit and the start of monitoring by the safety module.
P0D.05	Braking ramp - time delay to start	Time delay after which the ramps start.
P0D.03	Braking ramp - start value factor	Factor for calculating the start value of the rotational speed ramps
P0D.04	Braking ramp - start value offset	Offset for calculating the start value of the rotational speed ramps
P0D.09	Speed offset for the limitation in the basic unit	Offset for rotational speed limits to control the basic unit.

Tab. 54: SS2: Safe Stop 2

3.5.5 SOS – Safe Operating Stop

Application

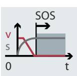


Fig. 35: SOS symbol

The function implements the SOS safety function in accordance with EN 61800-5-2. Use the "Safe Operating Stop" (SOS) function if your application requires the motor position or the axis position to be actively held and monitored safely.

ⓘ

The SOS function is also triggered by the SS2 function and can also be used as an error response (when other requested safety functions are violated). In this case, it is activated via the factory setting and cannot then be deselected.

Function

When requesting the SOS safety function, after a defined time the function monitors the control of the drive within a specified position tolerance. If necessary, a quick stop can be requested in the basic unit in advance in order to use it to brake the drive to standstill. Even if the SOS safety function has been requested, power will continue to be supplied to the motor to enable it to resist external forces. The speed is regulated to zero in the basic unit at this stage.

NOTICE

Because the signals of the position encoder may be static at standstill, e.g. with SIN/COS tracking signals, the SOS function cannot be continuously requested without limits. An axis movement is required at times.
If SOS is requested for › 10 days, error 54-7 is triggered.
This means that the maximum standstill time in the SOS function is limited to 10 days.

The logic to request the SOS safety function is shown in the following block diagram:

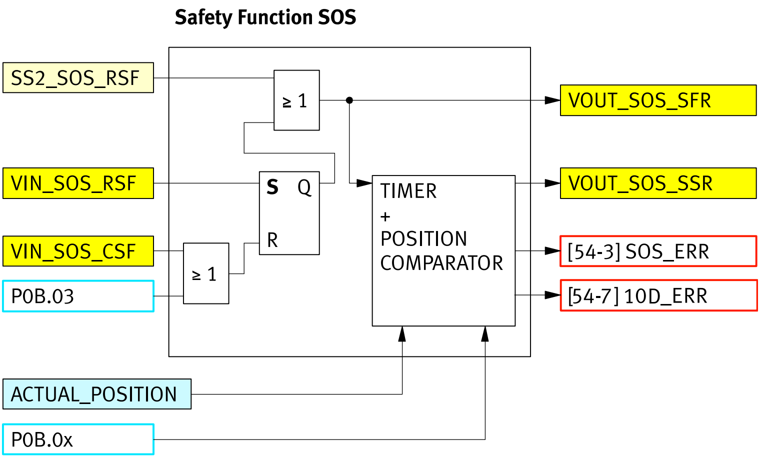


Fig. 36: SOS block diagram

Term/abbreviation	Explanation
Safety Function SOS	Safety function SOS
VIN_SOS_RSF	Virtual input: request SOS

Term/abbreviation	Explanation
VIN_SOS_CSF	Virtual input: terminate SOS request
ACTUAL POSITION	Internal signal: current position
TIMER + POSITION COMPARATOR	Timer and position comparator
VOUT_SOS_SFR	Virtual output: SOS requested
VOUT_SOS_SSR	Virtual output: safe state SOS reached
[54-3] SOS_ERR	Internal error signal: error 54-3
[54-7] 10D_ERR	Internal error signal: error 54-7

Tab. 55: Legend for SOS block diagram

The SOS safety function is requested as follows:

- By the user via any combination of input signals LIN_D... that lead to the VIN_SOS_RSF signal.
- Via the safety function SS2, signal SS2_SOS_RSF.

The request for the SOS safety function is cancelled as follows:

- By the user via a combination of different inputs that lead to the VIN_SOS_CSF signal.
- The safety function is automatically terminated after the request is cancelled by setting the parameter “Automatic restart allowed” (P0B.03).

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF signals is pending, the safety function cannot be terminated by an xxx_CSF signal.

Error detection

The safety condition is considered violated when the drive moves by more than the “Position monitoring tolerance window” distance (±P0B.01) after P0B.00 has elapsed, or if an axis movement is detected by the speed measuring device.

NOTICE

In applications with only one rotary encoder or position encoder with analogue signal interface (resolver, SIN/COS, Hiperface etc.), the restrictions on diagnostic coverage as well as the restrictions on the achievable accuracy of standstill and speed monitoring must be taken into account ➔ 8.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder) and ➔ 8.3.6 Effect of an angle error within the error limits of vector length monitoring on the speed signal.

The safety condition is also considered as violated if the actual position value has the “invalid” status while the safety function is requested (e.g. if a position encoder fails).

If the safety condition is violated, an error is triggered. The SOS function is implemented in accordance with EN 61800-5-2 if the error response is parameterised to STO.

The safety function can be executed independently of whether the axis is referenced or not.

Sequence

The sequence of the SOS safety function is shown in the following diagram:

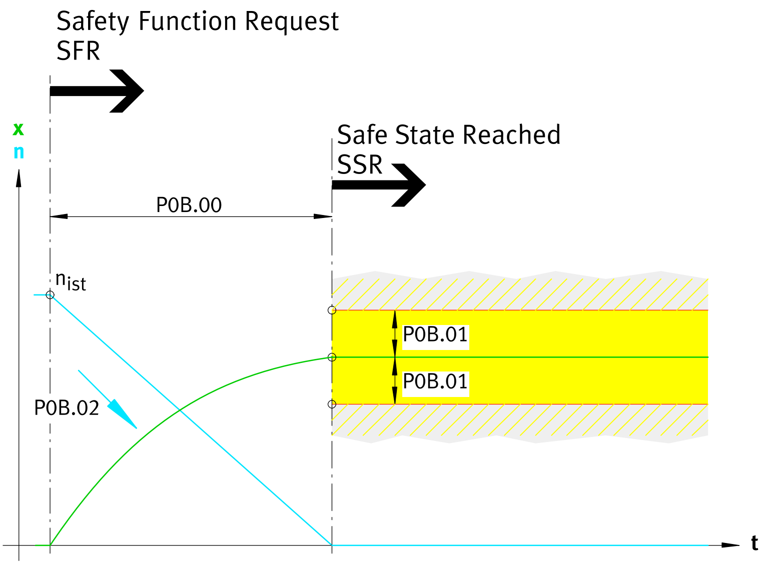


Fig. 37: SOS flowchart

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
n_{act}	Actual speed

Tab. 56: Legend for SOS flowchart

If parameterised appropriately with “Activate quick stop ramp in basic unit” (P0B.02), the motor controller is instructed to stop the drive via the “Quick stop” cable.
After the time “Time delay until monitoring starts” (P0B.00) has elapsed, the drive is monitored to check that it is at standstill. At this time, the “Safe state reached” output becomes active if the safety condition is not violated.
Position monitoring is not yet active during the P0B.00 time. After P0B.00 has elapsed, the current actual position is saved and is used as the setpoint value for the position to be monitored. The position is monitored by comparing the current position value with the saved value at regular intervals.
After the request of the SOS safety function, the following times elapse until the safety function is activated and errors are detected:

Time delays from VIN_SOS_RSF	Minimum	Maximum	Typical
VOUT_SOS_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SOS_SSR	2.0 ms + P0B.00	2.1 ms + P0B.00	2.0 ms + P0B.00
Detection of a violation of the safety condition[1] after P0B.00 within	0.0 ms	2.0 ms	2.1 ms

1) The safety condition is considered as violated if the monitoring window is exited +/- P0B.01 or if an axis movement is detected via standstill detection within the position window.

Tab. 57: SOS time delays

Parameters for SOS

SOS: Safe Operating Stop		
No.	Name	Description
P0B.00	Time delay until monitoring starts	Time delay after request of the function up to the start of monitoring
P0B.01	Tolerance window, position monitoring	Limit value for movement after standstill state is reached
P0B.03	Automatic restart permitted	If set: cancellation of the request (restart) with inactive request input
Expert parameters		
P0B.02	Activate quick stop ramp in the basic unit	Send brake command to basic unit (signal SS1) Yes/No

Tab. 58: SOS: Safe Operating Stop

3.5.6 Universal safety functions USF

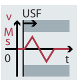


Fig. 38: USF symbol

The “Universal Safety Functions” (USF) serve to monitor the status variables (path, speed and force/torque) of the motor/axis.

Currently available:

– “Safe Speed Function” (SSF)

The USF function combines the following product terms:

– "Request", "Terminate request",
– the logical and virtual inputs and outputs (LIN_USFx..., VOUT_USFx...)
– the error management parameters

4 USF functions (USF0 ... USF3) are available.

3.5.7 Safe speed functions SSF

Application

The “Safe Speed Function” (SSF) can be parameterised as one of the following safety functions:

- SLS – Safely Limited Speed ➔ 3.5.8 SLS – Safely Limited Speed,
- SSR – Safe Speed Range ➔ 3.5.9 SSR - Safe Speed Range,
- SSM – Safe Speed Monitoring ➔ 3.5.10 SSM - Safe Speed Monitor.

The specific function is then defined by a specific parameterisation of the SSF, as shown in the following sections.

Every one of the 4 USF functions contains an SSF function for this (SSF0 ... SSF3). This means that up to 4 of the safety functions can be implemented and executed in parallel.

Function

The SSFs in the SLS/SSR/SSM versions monitor the speed of the drive using minimum and maximum limits. If the speed of the motor exceeds the limit value, then the “Safety condition violated” error is triggered.

The speed limits for monitoring are not specified statically. The SSF can calculate dynamic speed ramps and also monitor the drive to ensure that it is transferred to the desired safe speed range from any speed.

In addition, speed limiting of the motor controller can be controlled so the safety condition is not violated.

The logic to request the SSF0 safety function is shown in the following block diagram:

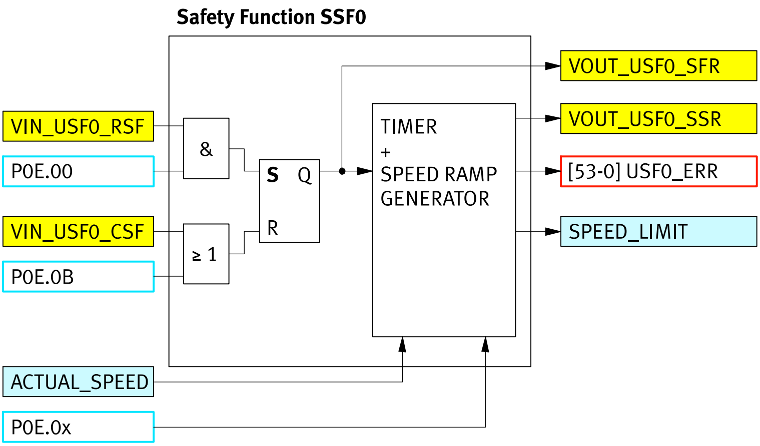


Fig. 39: SSF0 block diagram

Term/abbreviation	Explanation
Safety Function SFF0	Safety function SFF0
VIN_USF0_RSF	Virtual input: request USF0
VIN_USF0_CSF	Virtual input: terminate USF0 request
ACTUAL SPEED	Internal signal: current speed

Term/abbreviation	Explanation
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_USF0_SFR	Virtual output: USF0 requested
VOUT_USF0_SSR	Virtual output: USF0 safe state reached
[53-0] USF0_ERR	Internal error signal: error 53-0
SPEED_LIMIT	Internal signal: speed limit in basic unit

Tab. 59: Legend for block diagram SSF0

The SSF0 safety function is requested as follows:
- By the user via any combination of input signals LIN_D... that lead to the signal VIN_USF0_RSF, if the SSF function was activated using the parameter “Activate SSF” (P0E.00/...).

The request of the SSF0 safety function is cancelled as follows:
- By the user via a combination of different inputs that lead to the VIN_USF0_CSF signal.
- The safety function is automatically terminated after the request is cancelled by setting the parameter “Automatic restart allowed” (P0E.0B/...).

The SSF0 function provides the following control signals to control the basic unit:
- time-dependent limits for speed in the basic unit, SPEED_LIMIT.

The SSF0 function also generates the status messages
- VOUT_USF0_SFR, safety function USF0 requested.
- VOUT_USF0_SSR, safe state USF0 reached.

USF0 output signals	Standstill state	Safety function requested/achieved
VOUT_USF0_SFR	0	1
VOUT_USF0_SSR	0	1 (delayed, see time response)

Tab. 60: SSF0 status messages

Every request of the safety function has priority over termination of the request. This means: so long as one of the xxx_RSF signals is pending, the safety function cannot be terminated by an xxx_CSF signal.

Error detection

The safety condition is considered violated if the rotational speed is continuously outside the permitted range for the time “Allowable time for limit value violation” (P0E.03/...). The violation is considered as lifted when the rotational speed is continuously within the permitted range for the time “Allowable time for limit value violation” (P0E.03/...).

NOTICE

In applications with only one rotary encoder or position encoder with analogue signal interface (resolver, SIN/COS, Hiperface etc.), the restrictions on diagnostic coverage as well as the restrictions on the achievable accuracy of standstill and speed monitoring must be taken into account ➔ 8.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder) and ➔ 8.3.6 Effect of an angle error within the error limits of vector length monitoring on the speed signal.

If the safety condition is violated, an error is triggered, which results in an error response which can be parameterised.
The error “Safety condition violated” is also generated if a position encoder fails and thus reliable speed information is not available.

Sequence of the safety function (parameter ➔ Tab. 63 SSF: Safe Speed)

The sequence of the SSF0 safety function is shown in the following diagram:

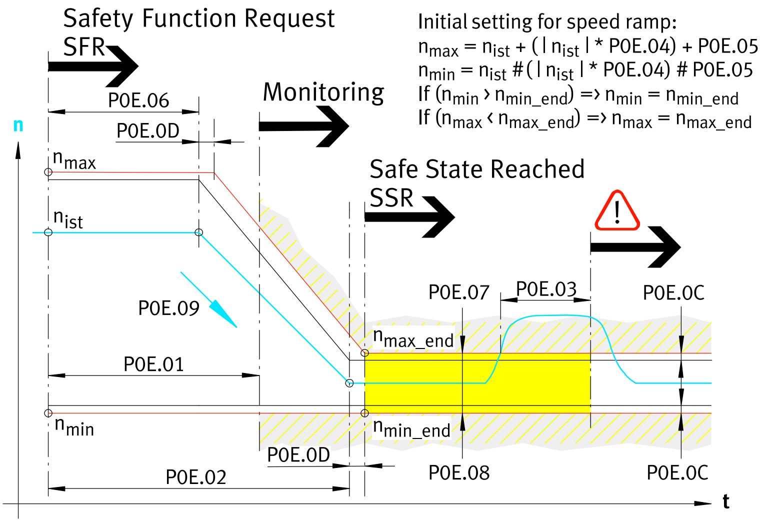


Fig. 40: SSF0 flowchart

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed

Tab. 61: Legend for SSF0 flowchart

The SSF0 safety function monitors the speed of the drive in the steady-state status. The permitted speed corridor is defined by the "Safe speed - upper limit“ (P0E.07/..., n_{max_end}) and "Safe speed - lower limit“ (P0E.08/..., n_{min_end}) parameters (➔ Fig. 40, right-hand section).
If the actual speed leaves the speed corridor, the “Safety condition violated” error is generated after an allowable time “Allowable time for limit violation” (P0E.03/...).

ℹ

The SSF safety functions are characterised as SLS, SSR or SSM, depending primarily on how the final speed is parameterised:

- "Safely Limited Speed" (SLS) ➔ 3.5.8 SLS – Safely Limited Speed,
- "Safe Speed Range" (SSR) ➔ 3.5.9 SSR - Safe Speed Range,
- "Safe Speed Monitoring" (SSM) ➔ 3.5.10 SSM - Safe Speed Monitor.

When the SSF0 safety function (VOUT_USF0_SFR) is requested, a calculation for a speed ramp is carried out for the drive to be transferred into the approved speed corridor, starting from the current speed:

- Calculation of the initial values nmax and nmin is based on the current speed nact as the starting value. A start window around the current speed is first calculated based on a gain parameter “Braking ramp - starting value factor” (P0E.04/...) and an offset parameter “Braking ramp - starting value offset” (P0E.05/...).
- The position of the start window is set relative to the desired speed corridor and the initial values are adapted as necessary to produce a trapezoidal, tapering speed corridor ➔ Fig. 40.
- The start time of the ramp can be specified using “Braking ramp - time delay to start” (P0E.06/..., minimum value: 6 ms) and the end time of the ramp via “Time for braking ramp” (P0E.02). After P0E.02 has elapsed, the stationary speed corridor has been reached and SSF0 sends the signal VOUT_USF0_SSR (if the actual speed is in the approved range!).
- The time from when the SSF0 function monitors the speed can be defined with “Time delay until monitoring starts” (P0E.01/...).

ℹ

A delay of the ramp via “Braking ramp - time delay to start” (P0E.06/...) is always preferable when the axis is braked by the function controller and is transferred to the monitored speed corridor. P0E.06 can be used to compensate the reaction time of the function controller.

The safety module can actively manipulate the controller of the basic unit, thus actively limiting the speed of the axis. The limit values are transferred to the basic unit at regular intervals:

- This function is activated by setting the parameter “Actively limit speed in basic unit” (P0E.09/...).
- There are additional parameters to ensure that the monitored limit values are complied with safely during active limiting of the speed in the basic unit:
  - The internal runtimes in the device for sending signals of the new limit values to the basic unit until the control in the basic device becomes active are compensated by the minimum value of “Braking ramp - time delay to start” (P0E.06, 6 ms).

– “Rotational speed ramp - monitoring time delay” (P0E.0D/...) can be used in order to add a delay of several additional milliseconds to a speed limit in the safety module used for monitoring. This gives the basic unit additional time, e.g. if a jerk-limited travel profile was selected in the basic unit and braking may only take place with jerk limiting.
– Finally, a speed offset can be parameterised using “Speed limit offset” (P0E.0C/...). The speed limits for the basic unit are then offset by P0E.0C/... within the speed corridor for monitoring, meaning that minor deviations in the actual speed do not lead to a response from the monitoring system.
– If the upper and lower speed limits for the basic unit overlap due to a very narrow corridor and the offset P0E.0C/..., then both limits are set to the average value between the monitored minimum and maximum rotational speed.

The description can be applied in a similar manner to the parameters for the SSF1, SSF2 and SSF3 functions.

ⓘ

Thus SSF0 permits adaptation to various applications.
The SSF0 parameters in the SafetyTool are divided into:

- standard parameters – these are the simple parameters that must be adapted individually to the application for every speed monitoring operation.
- expert parameters – these are parameters for optimisation of the function in conjunction with the control functions in the basic unit. These parameters are set appropriately at the factory.

You will only need the standard parameters for most applications!

The following times elapse after the request of the safety function SSF0 until the safety function is activated and errors are detected:

Time delays from VIN_USF0_RSF	**min.**	**max.**	**typical**
VOUT_USF0_SFR message	2.0 ms	2.1 ms	2.0 ms
VOUT_USF0_SSR message	8.0 ms + (P0E.02 + P0E.0D)	8.1 ms + (P0E.02 + P0E.0D)	8.0 ms + (P0E.02 + P0E.0D)
Start of monitoring of the safety condition according to VOUT_USF0_SFR	2.0 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))	2.1 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))	2.0 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))
Detection of a violation of the safety condition after P0E.01 or (P0E.06 + P0E.0D) within	P0E.03	P0E.03	P0E.03

Tab. 62: SSF0 time delays

Parameters for SSF

SSF: Safe Speed					
Parameter no. for ...				Name	Description
SSF0	SSF1	SSF2	SSF3		
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	If 1: request of the USF triggers request of the SSF
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until moni-toring starts	Time from the safety function request during which rotational speed is not monitored
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed upper limit	End value of the upper ramp at nmax_end
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed lower limit	End value of the lower ramp at nmin_end
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for braking ramp	Time from the safety function request, after which the ramps are stopped and the safe state is reached.
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Time interval during which the actual speed value may be outside the limits before the “Safety condition vio-lated” status is reached.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	If set: the speed limit is transferred to the basic unit and the speed is actively limited in the basic unit.
P0E.0B	P0E.1F	P0E.33	P0E.47	Automatic restart per-mitted	If 1: cancellation of the request (restart) if an inactive request arrives

SSF: Safe Speed					
Parameter no. for ...				Name	Description
SSF0	SSF1	SSF2	SSF3		
P0E.0D	P0E.21	P0E.35	P0E.49	Speed ramp - monitoring time delay	The ramp used to monitor the speed in the safety module is also delayed compared to the ramp applied to the basic unit.
P0E.06	P0E.1A	P0E.2E	P0E.42	Braking ramp - time delay to start	Time delay after which the monitoring ramp in the safety module starts.
P0E.04	P0E.18	P0E.2C	P0E.40	Braking ramp - start value factor	Factor for calculating the starting value of the ramps
P0E.05	P0E.19	P0E.2D	P0E.41	Braking ramp - start value offset	Offset for calculating the starting value of the ramps
P0E.0C	P0E.20	P0E.34	P0E.48	Speed limit offset	Offset for the speed limits for controlling the basic unit.
P0E.0A	P0E.1E	P0E.32	P0E.46	Activate quick stop ramp in the basic unit	If set: when the safety function is requested, the quick stop command (control cable) is applied to the basic unit

Tab. 63: SSF: Safe Speed

3.5.8 SLS – Safely Limited Speed

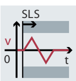


Fig. 41: SLS symbol

The function implements the SLS safety function in accordance with EN 61800-5-2. Use the “Safely Limited Speed” (SLS) function if you wish to prevent the motor from exceeding a specified speed limit in your application.
The function is characterised by a zero-symmetrical monitoring range for the speed. The limits can be set separately.
The drive can be braked to a permissible rotational speed along a braking ramp. The function can be

switched off. In the simplest case, monitoring starts after the time “Time delay until monitoring starts” (P0E.01/P0E.15/P0E.29/P0E.3D). The maximum rotational speed is specified using “Safe speed - upper limit” (P0E.07/P0E.1B/P0E.2F/P0E.43).
The following parameterisation means that the Safe Speed Function SSF corresponds to the SLS safety function, with immediate speed monitoring without slowdown ramp.

Parameterise SSF as SLS					
Parameter no. for ...				Name	Setting for safety function SLS
SSF0	SSF1	SSF2	SSF3		
SSF standard parameters					
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	= 1, activate
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until monitoring starts	2.0 ms
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed upper limit	Set positive speed limit for SLS.
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed lower limit	= -P0E.07/-P0E.1B /-P0E.27 /-P0E.43
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for braking ramp	6.2 ms, minimum value
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Default value: 10 ms, can be reduced for faster error detection.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	Can be set.
SSF expert parameters: no change to factory setting (important!)					
P0E.06	P0E.1A	P0E.2E	P0E.42	Braking ramp - time delay to start	= 6 ms (smallest settable value)
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: safety condition violated	Corresponds to the required error response of the application.

Tab. 64: Parameterise SSF as SLS

3.5.9 SSR - Safe Speed Range

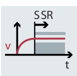


Fig. 42: SSR symbol

The function implements the SSR safety function in accordance with EN 61800-5-2. Use the “Safe Speed Range” (SSR) function if you wish to ensure that the motor speed remains within specified limit values in your application.
The following parameterisation means that the Safe Speed Function SSF corresponds to the SSR safety function (with immediate speed monitoring without braking ramp):

Parameterise SSF as SSR					
Parameter no. for ...				Name	Setting for safety function SSR
SSF0	SSF1	SSF2	SSF3		
SSF standard parameters					
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	= 1, activate
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until monitoring starts	2.0 ms
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed upper limit	Set upper speed limit for SSR.
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed lower limit	Set lower speed limit for SSR.
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for braking ramp	6.2 ms, minimum value
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Default value: 10 ms, can be reduced for faster error detection.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	Can be set.
SSF expert parameters: no change to factory setting (important!)					
P0E.06	P0E.1A	P0E.2E	P0E.42	Braking ramp - time delay to start	= 6 ms (smallest settable value)
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: safety condition violated	Corresponds to the required error response of the application.

Tab. 65: Parameterise SSF as SSR

3.5.10 SSM - Safe Speed Monitor

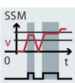


Fig. 43: SSM symbol

The function implements the SSM safety function in accordance with EN 61800-5-2.
Use the “Safe Speed Monitor” (SSM) function if you require a safe output signal in your application to display whether the motor rotational speed is within the specified limit values. Set a limit value to zero in order to implement the SSM function as described in EN 61800-5-2.
The parameterisation of the SSM corresponds to that for SSR. Only error management must be adapted:

Parameterise SSF as SSM					
Parameter no. for ...				Name	Setting for SSM safety function
SSF0	SSF1	SSF2	SSF3		
SSF standard parameters: see SSR, ➔ Tab. 65 Parameterise SSF as SSR					
SSF expert parameters: see SSR, ➔ Tab. 65 Parameterise SSF as SSR					
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: safety condition violated	Depending on the application: – none = [0], or – none, only diagnostic memory entry = [1] – warning + diagnostic memory entry = [2]

Tab. 66: Parameterise SSF as SSM

3.6 Logic functions

3.6.1 Mode selector switch

Use

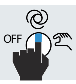


Fig. 44: Symbol for mode selector switch

Use the “Mode selector switch” logic function to switch between various operating modes/monitoring functions of the safety module.
Example:
- Normal operation of the system is possible in the normal operation switch position. A stop is initiated in the event of intervention in the system, e.g. via SS1.
- The SLS safety function is activated in the setup mode switch position. Intervention in the system should not result in SS1, since setup mode is permitted.

The DIN45, DIN46 and DIN47 inputs can be configured as inputs for mode selection. The “mode selector switch” provides three safe logical control signals, which can be used to switch between various safety functions:
- LIN_D45_SAFE
- LIN_D46_SAFE
- LIN_D47_SAFE

Function
The status of the three inputs DIN45, DIN46 and DIN47 is mapped directly to the safe logical signals LIN_D45_SAFE, LIN_D46_SAFE and LIN_D47_SAFE.
If the inputs DIN45 ... DIN47 are configured as mode selector switches, then exactly one input must be High. To achieve this, the logic function executes 1-of-n monitoring, with discrepancy time monitoring.

Logical inputs	**System start-up**[1)]	**Normal operation**	**Error status**
LIN_D45_SAFE	1	= LIN_D45	Last valid status
LIN_D46_SAFE	0	= LIN_D46	
LIN_D47_SAFE	0	= LIN_D47	

1) Status until a valid status is detected or status if safe evaluation of the mode selector switch is not active.

Tab. 67: Mode selector switch logical inputs

Operating mode switch

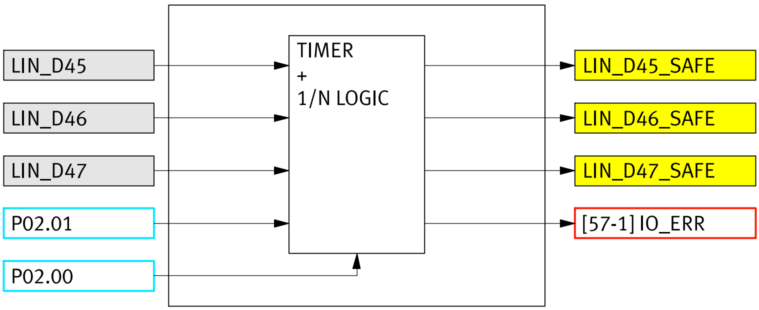


Fig. 45: Block diagram of the mode selector switch

Term/abbreviation	**Explanation**
LIN_ ...	Logical inputs
TIMER + 1/N LOGIC	Timer and 1-of-n logic
[57-1] IO_ERR	Internal error signal error 57-1

Tab. 68: Legend for block diagram of the mode selector switch

Error detection

If no input or more than one input is High for a parameterisable time in the mode selector switch function, an error is triggered and the input signals are marked as invalid.
If the inputs DIN45 ... DIN47 have a faulty status, the signals LIN_D45_SAFE, LIN_D46_SAFE and LIN_D47_SAFE retain the most recently detected error-free status.

Time delays from level change LIN_D...	Minimum	Maximum	Typical
LIN_D45/46/47_SAFE	2.0 ms	2.1 ms	2.0 ms
Error reaction time on violation of the 1-of-n condition	2.0 ms + P02.01	2.1 ms + P02.01	2.0 ms + P02.01

Tab. 69: Time response of the mode selector switch

Parameters of the mode selector switch

Mode selector switch		
No.	Name	Description
P02.00	Activation	DIN45..DIN47 are used as mode selector switches (1 of 3).
P02.01	Discrepancy time	Time in which more than one input simultaneously or no input can be High.

Tab. 70: Mode selector switch

3.6.2 Two-hand control unit

Use

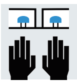


Fig. 46: Symbol for two-hand control device

The “Two-handed control unit” logic function is used in applications in which the operator must release the movement with both hands as soon as the danger zone is clear (e.g. press applications).

Use

The two-handed control unit sends the control signal LIN_2HAND_CTRL = LIN_DIN42 OR LIN_DIN43, with which safety functions can be switched via logical operations. It also monitors the simultaneous switching of the inputs (discrepancy time monitoring).
The two-handed control unit occupies the two inputs DIN42 and DIN43 (each with two channels A and B) and can only be activated if the connected sensor type "Two-handed control unit" was selected for the control inputs DIN42 and DIN43. In the operating mode “Two-handed control unit” the individual inputs DIN42 and DIN43 continue to have all the “standard” functions (equivalence/antivalence, test signals, cross-comparison with 2nd processor, etc.).

Function

The result of the logic operation of the two inputs is transferred to the separate logical input LIN_2HAND_CTRL. LIN_2HAND_CTRL represents an OR operation of LIN_D42 and LIN_D43. LIN_2HAND_CTRL only has the status “0” if both logical inputs have the status “0”.
LIN_2HAND_CTRL = LIN_DIN42 OR LIN_DIN43

Two-hand control unit

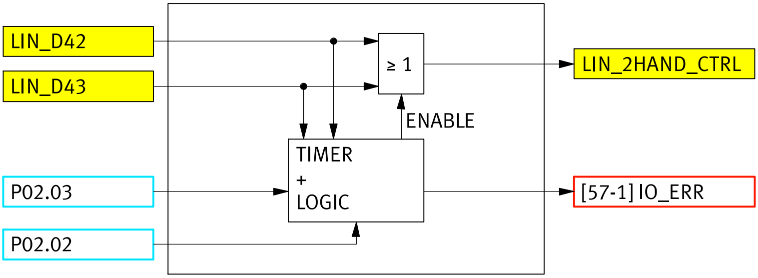


Fig. 47: Block diagram of the two-handed control unit

Term/abbreviation	Explanation
LIN_ ...	Logical inputs
TIMER + LOGIC	Timer and logic
ENABLE	Enable signal
[57-1] IO_ERR	Internal error signal error 57-1

Tab. 71: Legend for block diagram of the two-handed control unit

Error detection

The logic states of the DIN42 and DIN43 inputs must agree. If the logic states deviate from one another for longer than an adjustable discrepancy time, an error is generated.

i

The “Discrepancy time” parameter (P02.03) should usually be set longer than the discrepancy time for the monitoring of the DIN42, DIN43 inputs, because this bridges the time the operator needs to press or release both buttons of the two-handed control unit.

Time delays from level change LIN_D...	Minimum	Maximum	Typical
LIN_2HAND_CTRL	2.0 ms	2.1 ms	2.0 ms
Error reaction time on violation of the two-handed condition	2.0 ms + P02.03	2.1 ms + P02.03	2.0 ms + P02.03

Tab. 72: Time response of the two-handed control unit

Parameters of the two-handed control unit

Two-hand control unit		
No.	Name	Description
P02.02	Activation	DIN42 and DIN43 are used as a two-handed terminal
P02.03	Discrepancy time	Time in which the logic states of DIN42 and DIN43 may deviate from one another

Tab. 73: Two-hand control unit

3.6.3 Additional logic functions - ALF

Use

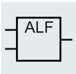


Fig. 48: Symbol for ALF

Use ALF to create more complex operations of logical input signals LIN_x or if, for reasons of clarity in the application, it makes sense to create a specific combination of LIN_x as an internal safe logic signal
The additional logic function can be used to link internal inputs and outputs logically. For example, this enables the implementation of special input combinations. ALF is used when more complex logical links are required and the input logic (OR gate with 4 upstream AND gates, each with 7 inputs) of a safety function is insufficient.

Function

Additional logic function

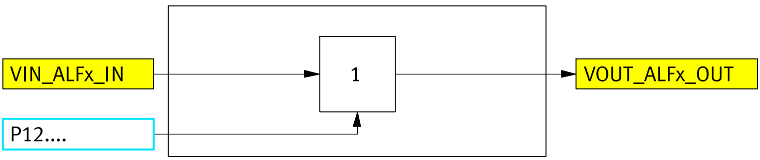


Fig. 49: Block diagram of additional logic functions

Term/abbreviation	Explanation
VIN_x_y	Virtual inputs
VOUT_x_y	Virtual outputs

Tab. 74: Legend for additional logic functions block diagram

Time delays from VIN_ALFx_IN	Minimum	Maximum	Typical
VOUT_ALFx_OUT	2.0 ms	2.1 ms	2.0 ms

Tab. 75: Time response of the additional logic functions

Parameters of the additional logic functions

Additional logic functions			
ALF...	No.	Name	Description
ALF0	P12.00	Transmission function	Selection of the functionality (fixed): Identity (OUT = IN) = [2] The output always has the logic state of the input with the "Identity" function.
ALF1	P12.03	Transmission function	
ALF2	P12.06	Transmission function	
ALF3	P12.09	Transmission function	
ALF4	P12.0C	Transmission function	
ALF5	P12.0F	Transmission function	
ALF6	P12.12	Transmission function	
ALF7	P12.15	Transmission function	

Tab. 76: Additional logic functions

3.7 Terminate safety functions

3.7.1 Function range

Function range

Fig. 50: Symbol for terminate safety function (restart)

One or more safety functions are terminated with the function so the drive can “restart”.
In combination with safe movement functions, such as SLS, “Restart” means that the drive is no longer monitored and can travel at full speed again.
The user can specify separately for each safety function which control signal is to terminate the safety function. The safety functions have the virtual input VIN_xxx_CSF (Clear Safety Function) for this purpose.
This must be defined for every safety function unless the safety function has been parameterised to “Automatic restart”. In this case, the safety function is terminated automatically as soon as the request for the safety function is withdrawn.
A safety function can only be terminated if the request for the safety function has previously been cancelled. A request of a safety function always has a higher priority than termination.

When the device is delivered, the single-channel input DIN49 is preset to the sensor type “Terminate safety function” and to the “STO” and “SBC” safety functions.
The signal LIN_D49_RISING_EDGE supplies for every rising edge (0 V -› 24 V) at DIN49 a short switching pulse for 2 ms with which the safety functions can be reset.

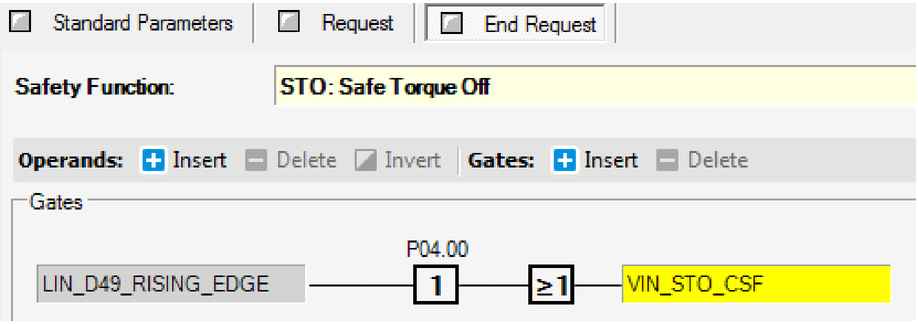


Fig. 51: Configuration of restart (example)

Time delays from LIN_D49_RISING_EDGE	Minimum	Maximum	Typical
VIN_xxx_CSF until termination of the safety function	0.0 ms	2.1 ms	2.0 ms

Tab. 77: Time response of safety function termination

NOTICE

Check whether a single-channel control input is permitted in your application for terminating the safety function and whether implementation is to be level-controlled or edge-controlled.
Use the following inputs:

- LIN_D49, if a level-controlled reset is permitted,
- LIN_D49_RISING_EDGE, if an edge-controlled reset is required,
- in all other cases, use one of the two-channel inputs LIN_D40 to LIN_D43.

NOTICE

Check whether the risk assessment for the machine includes additional requirements for control of the restart and for the diagnostics of the related control inputs, e.g. **a manual edge-controlled reset in cases where it is possible to walk behind protective devices**.

3.7.2 Examples and special notes on implementation

Termination of STO

The following figure shows the structure for the STO safety function ➔ Fig. 52. STO can be requested during operation via VIN_STO_RSF. Request of the STO safety function causes the driver supply in the motor controller to be switched off. To switch the drive back on after the STO request has been completed, the request must be terminated ➔ 3.7.1 Function range.

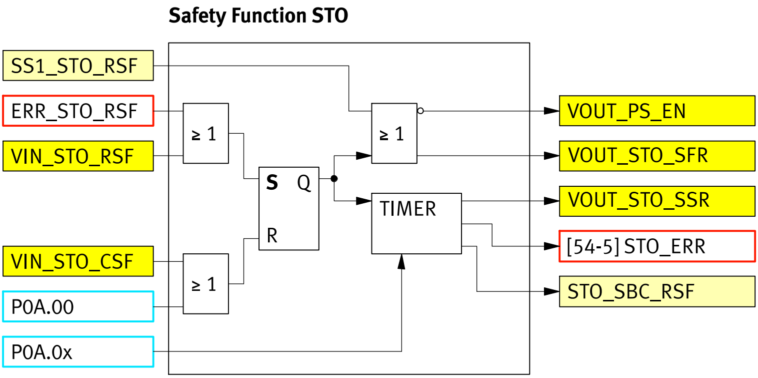


Fig. 52: Request of a safety function (example of STO)/restart

Terminate the safety function after error acknowledgement

The error management can also request the STO function as an error response (via ERR_STO_RSF signal). The request is fed into the STO function as shown in the figure above.

To enable STO to be terminated after an acknowledged error, a restart via VIN_STO_CSF is required, or the "Automatic restart allowed" (P0A.00) parameter must be set. This also applies in a similar manner for the SS1, SS2 and SBC safety functions, which can be configured as an error response.

Terminate STO after completion of SS1

The SS1 function requests STO at the end of its sequence via control input SS1_STO_RSF.

The STO request is automatically deactivated when the request for the SS1 function is no longer active ➔ Fig. 52. The request of the STO function does not need to be deactivated separately. This also applies when the SS1 function is requested in the event of an error; the error must be acknowledged and SS1 deactivated. STO does not need to be deactivated separately.

Terminate SBC after completion of STO/SS1

The logic for requesting and terminating the SBC function largely corresponds to that for requesting STO ➔ Fig. 27.

In addition to conventional logic, SBC can be controlled by direct control signals from STO (STO_SBC_RSF) and from SS1 (SS1_SBC_RSF). With the termination of STO or SS1, SBC is also automatically terminated.

ⓘ

It is thus possible to implement different conditions for terminating safety functions, although the same safety functions are used:

- Direct request of SBC, termination e.g. via LIN_D49_RISING_EDGE,
- Indirect request, e.g. via SS1, termination of SBC together with termination of SS1 as soon as its restart condition is fulfilled (e.g. LIN_D40).

Terminate SOS after completion of SS2

The combination of SS2 and SOS functions similarly to the combination of SS1 and STO described above.

3.8 Error management and error acknowledgement

3.8.1 Triggering errors and error classes

The safety module executes the required safety functions. It monitors itself, the inputs and outputs and position encoders 1 and 2. If a safety function is violated or an error is detected, the safety module switches to the error state.
The following error groups are defined in combination with the functional safety technology and the CAMC-G-S3 safety module:

– Errors triggered by the basic unit.
– Errors triggered by the safety module.

The errors are divided into different classes, which can be identified by the error number shown on the 7-segment display of the motor controller.
The number consists of a two-digit main index (range 51 ... 59) and a subindex (range 0 ... 9):

Error number											
Main index	Subindex										Error type/class
Basic device error											
51-x	9[1)]	8[1)]	7[1)]	6	5	4	3	2	1	0	Control signals from the safety module not OK, module type/identifier not OK
52-x	9[1)]	8[1)]	7[1)]	6[1)]	5[1)]	4[1)]	3	2	1	0	Error in control sequence with the safety module
Error of the safety module											
53-x	9[1)]	8[1)]	7[1)]	6[1)]	5[1)]	4[1)]	3	2	1	0	Violation of a safety function
54-x	9[1)]	8[1)]	7	6	5	4	3	2	1[1)]	0	Violation of a safety function
55-x	9[1)]	8[1)]	7	6	5	4	3	2	1	0	System error: actual value recording/position encoder not OK
56-x	9	8	7[1)]	6[1)]	5[1)]	4[1)]	3[1)]	2[1)]	1[1)]	0[1)]	System error: position recording/comparison not OK

Error number											
Main index	Subindex										Error type/class
57-x	9 1)	8 1)	7 1)	6	5	4	3	2	1	0	System error: inputs and outputs or internal test signals not OK
58-x	9 1)	8 1)	7 1)	6	5	4	3	2	1	0	System error: external/internal communication not OK
59-x	9	8	7	6	5	4	3	2	1	0	System error of the firmware/hardware error of the safety module

1) reserved for future extensions

Tab. 78: Bit field of the error numbers

You can find a full description of all the errors with possible causes and possible measures for avoiding them ➔ 6.6 Diagnostic messages with information for fault clearance.

Basic device error:
The basic unit monitors during operation communications with the safety module and the plausibility of the control signals from the safety module. After switch-on, the basic unit checks that the correct type of safety module has been mounted and whether a module has been replaced. If there are errors, it generates a corresponding error message with parameterisable error response (➔ Description of functions of CMMP-AS-...-M3, GDCP-CMMP-M3-FW-...).

Errors of the safety module:
The safety module executes the required safety functions. It monitors itself, the inputs and outputs and position encoders 1 and 2. If a safety function is violated or an error is detected, the safety module switches to the error state.
A distinction is made between the following errors in the safety module
- Errors when a safety condition is violated (53-x and 54-x)
  LED is continuous red
- System errors (55-x to 59-x)
  LED flashes red.

Additional information on the LED display ➔ 3.10.2 Status display on the safety module

Errors are generated by the various function blocks in the safety module.
For example, the SSF safety function generates an error signal if the drive moves outside the monitored speed range.
The error may be very short if the drive only leaves the permitted range for a brief interval. For this reason, both the basic unit and the safety module have an internal diagnostic memory.
Each error occurring during operation is first entered into the diagnostic memory and stored temporarily:

- The diagnostic memory of the basic unit can hold more than 200 entries. When this limit is reached, the oldest entries are overwritten.
- The diagnostic memory of the safety module holds 32 entries.
  It serves as an intermediate buffer before the errors are transferred to the basic unit and entered there into the permanent diagnostic memory.

ⓘ

The permanent diagnostic memory of the basic unit remains intact even if there is a power failure, meaning that an error history is always available. Events other than errors are also saved in the permanent diagnostic memory.
Detailed description ➔ 3.11 Permanent and temporary diagnostic memory in the motor controller.

The error number, consisting of the main index and the subindex, is also displayed on the 7-segment display of the motor controller. The most recently triggered error of the highest priority (error number) is displayed. Later errors with a lower priority are also saved in the diagnostic memory but are not output to the 7-segment display.
An error status remains pending until it is acknowledged.

Violation of safety conditions

The “Safety condition violated” signals of the various safety functions are combined into a common error message or a common warning message, depending on the parameterised error response.
For example, the signal relay can be controlled. The common messages themselves do not generate an error response.
The error response is specified separately for every safety function ➔ 5.6.12 Error management and ➔ 9.2 List of additional parameters. An error is triggered once on the first violation of the safety condition after the request of the safety function. A repeated violation of the safety condition will not generate a new error message until the error has been acknowledged.
The “Safety condition violated” output displays the current status. Example:

1. SLS is requested.
2. Speed outside the approved range } error message, output active.
3. Speed back in approved range } output becomes inactive.
4. Speed again outside the approved range } output active, no new error message.

Reaction to faulty status variables

As long as a safety function is not requested, the validity of the input variables (e.g. speed signal, signal of standstill detection, etc.) is neither monitored nor checked.
The validity of the input variables is monitored when a safety function is requested or implemented. If an error is detected, it generates the corresponding error message “Safety condition violated”.

ⓘ

The hidden expert parameter P09.00 can be used to set a mask to prevent individual safety functions from generating the VOUT_SSR and VOUT_SCV status.
The parameter can be applied to use safety functions for monitoring, e.g. "Safe Speed Monitor, SSM" and hide them from operating status messages.
Consult your regional Festo contact person if necessary.

3.8.2 Parameterisation of the error response of the safety module

The error response can be configured over a wide range for many errors of groups 53-x to 57-x. The selection is restricted or prevented completely for some critical errors. Every error triggers the error response assigned to it regardless of the time sequence in which they occurred. If multiple errors are pending simultaneously, multiple error responses are activated simultaneously.
If a safety condition is violated, the safety module must initiate a defined stop of the axis depending on the stop category requested (STO, SS1, SS2, possibly SBC).
The scope of the required error response to system errors depends on whether or not the safe function of the safety module can still be guaranteed.
The following error responses (starting with those of the highest priority) are available:
[8] Request for STO + SBC + set all digital outputs to "0"
[7] STO + SBC request
[6] STO request
[5] SS1 + SBC request
[4] SS1 request
[3] SS2 request
[2] Generation of a warning (motor controller display), no further response
[1] No response, entry in diagnostic memory only
[0] No response, no entry in diagnostic memory

NOTICE

If there are errors, in cases of doubt the drive must be de-energised as quickly as possible (STO), the clamping unit or holding brake must be engaged (SBC), and all the safe outputs must be switched off, corresponding to error response [8]. This status is the "Safe basic status" of the safety module.
- Power can no longer be supplied to the motor.
- A movement is braked by an external clamping unit with emergency braking properties.
- External downstream electronic systems are switched off/switched to safe status.

Check which error response is required in your safety application. In case of doubt, select the highest error response [8].

3.8.3 Logic for error acknowledgement

Fig. 53: Symbol for acknowledgement

The "Error acknowledgement" function described here resets errors which have occurred. This is the prerequisite for terminating active safety functions as a result of an error response.

Errors can be acknowledged by a rising edge of the VIN_ERR_QUIT control signal. The control signal must be connected to a digital input:
– Switch a control input to VIN_ERR_QUIT
– Actuate the input so the safety module exits the error status.
It is configured in the same manner as configuration of the request or the termination of a safety function.

In the delivery status and after a reset to factory settings, the input DIN48 is intended for the “Error acknowledgement” function. Errors are acknowledged with the rising edge (0 V -> 24 V).

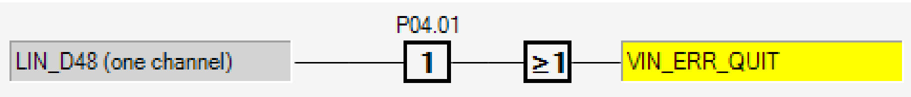


Fig. 54: Configuration of error acknowledgement

An error can only be acknowledged (deleted from the “temporary” diagnostic memory of the safety module) when the error condition no longer exists. Thus, during acknowledgement, the safety module systematically checks all the error conditions and deletes the entries of the errors which have been eliminated. The remaining errors remain intact. After an acknowledgement operation, the safety module writes an “Error acknowledgement” entry to the “permanent” memory of the basic unit. After the end of error acknowledgement, any errors that still exist are entered in the diagnostic memory again.
At the end of error acknowledgement in the safety module, the module sends an “Acknowledge error” command to the basic unit so pending errors in the basic unit can also be acknowledged.

The safety module has a master function for the acknowledgement of errors:
- Errors acknowledged in the safety module are also acknowledged in the basic unit.
- Error numbers generated by the safety module (53-x to 59-x) can only be acknowledged via the safety module.
- During error acknowledgement via the function controller or I/O, the basic unit can only acknowledge those error numbers that are also generated by the basic unit.

Errors of the safety module are only acknowledged by the appropriately configured control input.

Time delays LIN_D48 to ...	**Minimum**	**Maximum**	**Typical**
VIN_ERR_QUIT up to the deletion of the temporary diagnostic memory and change of the operating mode	4.0 ms	20 ms	10 ms
VIN_ERR_QUIT up to the deletion of the errors in the basic unit and ready status of the basic unit	20 ms	500 ms	100 ms

Tab. 79: Time response of error acknowledgement

NOTICE

When a safety condition is violated, the error can only be acknowledged when the status variables of the drive are once more in the approved range.

Example - violation of SOS:
After SOS has been requested, the axis is moved outside the tolerance range -> error [54-3] SOS violation is generated.
The error can only be acknowledged when:
- the axis has been moved back into the permitted range or (alternatively)
- the request of the SOS safety function was terminated.

The result of the SOS violation is that another safety function, in this example SS1, is executed as an error response.
The following sequence is required for a restart after an “SOS violation”:
1. Actuation "Terminate safety function"
   ➞ Terminates the SOS function, SS1 (from error response) continues to be executed
2. Error acknowledgement
   ➞ Clears the error “SOS violation”
3. Press "Terminate safety function" again
   ➞ Terminates the SS1 safety function ➞ axis/motor can be restarted

Errors of the following safety functions can also be acknowledged when the safety function is requested:
STO, SS1, SBC, USF/SSF in all three types SLS, SSR, SSM.

3.9 Digital outputs

3.9.1 Two-channel safe outputs DOUT40 ... DOUT42 [X40]

Use

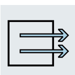


Fig. 55: Symbol, two-channel output

Use the two-channel safe outputs to:
- transmit safe status messages to external control devices.
- control safety relay units.
- When switched on permanently, they can be used as a source for test pulses.

Function
The safety module has three safe outputs DOUT40A/B, DOUT41A/B, DOUT42A/B. The outputs are largely freely configurable and can have various functions (safety function requested, safe state reached, errors, etc.) assigned to them. The operating status of the safety module or an individual safety function can therefore be transferred externally:
- to indicate the safety status to downstream drives,
- to request safety functions in downstream drives with safety module CAMC-G-S3,

– to report the safety status to an external safety controller or a function controller,
– to activate external safe actuators, e.g. a clamping unit, a valve exhaust, a door lock or similar.

Block diagram

DOUT40 ... DOUT42

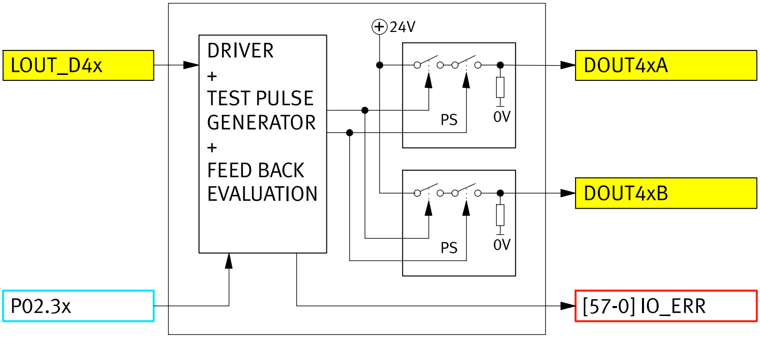


Fig. 56: Block diagram of the two-channel safe outputs

Term/abbreviation	Explanation
LOUT_x	Logical outputs
DRIVER + TEST PULSE GENERATOR + FEED BACK EVALUATION	Drivers, generation of test pulses and evaluation
DOUT4...A / DOUT4...B	Two-channel digital outputs
[57-0] IO_ERR	Internal error signal error 57-0

Tab. 80: Legend for block diagram of the two-channel safe outputs

The output is controlled by selecting one or more VOUT_x signals, which are applied to LOUT_D4x. Every safe digital output can be configured as follows (P03.30 for DOUT40):
– permanently OFF (DOUT40A/B = 0 V)
– permanently ON (DOUT40A/B = 24 V)
– equivalent switching
– antivalent switching
The test pulse length can be parameterised (P03.31 for DOUT40).

You can use the outputs to monitor passive sensors using test pulses. To do this, configure one of the outputs to “Permanently on” and use the outputs DOUT4x A/B to power the switching device ➔ 4.3 Sample circuits.

The following tables show the allocation of the logic signal LOUT_D4x to the output level for outputs switching equivalently and antivalently:

Output DOUT40/41/42 equivalent	Standstill state	Safe state requested
LOUT_D40/41/42	1	0
DOUT40A/41A/42A	24 V	0 V
DOUT40B/41B/42B	24 V	0 V

Tab. 81: Logic signals DOUT40/41/42 equivalent

Output DOUT40/41/42 antivalent	Standstill state	Safe state requested
LOUT_D40/41/42	1	0
DOUT40A/41A/42A	24 V	0 V
DOUT40B/41B/42B	0 V	24 V

Tab. 82: Logic signals DOUT40/41/42 antivalent

The safe outputs (including the clock output) should always follow the quiescent current principle, which means that the low level is the safe state.
The user must ensure this during configuration by inverting the control signal LOUT_D40 to ensure this principle is implemented.

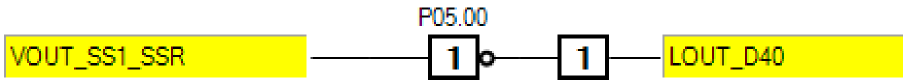


Fig. 57: Configuration of the safe outputs (example)

The user must ensure that a voltage-free output leads to a safe status for the overall system.
Every safe digital output can also be used as a clock output to feed passive sensors. In this case, it is configured as “permanently ON”.

Error detection

The output drivers have a two-channel, redundant structure. The output levels at DOUT4xA/B are continually read back by both micro controllers during operation. Both micro controllers output test pulses to the outputs, which alternately read back and evaluate the pulses from their respective counterpart.
These measures safely detect short circuits to 24 V, 0 V and cross circuits between any outputs. If there is an error, the output switches to the safe status (DOUT4xA/B switched off or 0 V). An error message [57-0] IO-ERR is generated.
If there are serious internal errors and, as a result, one or both micro controllers can no longer control the status of the outputs safely, then all the outputs are switched off jointly. Even in the case of antivalent outputs, both pins A/B are switched to Low.
Examples of such errors:

- operating voltage faulty
- position sensors faulty

– memory error, stack error
– program sequence monitoring indicates an error, internal communication error

Timing diagram

The diagram below shows an example of the time response when the output DOUT40 is switched off and on again. The test pulses for High are also shown. They are time-offset for all outputs.

Digital Output DOUT40A/B

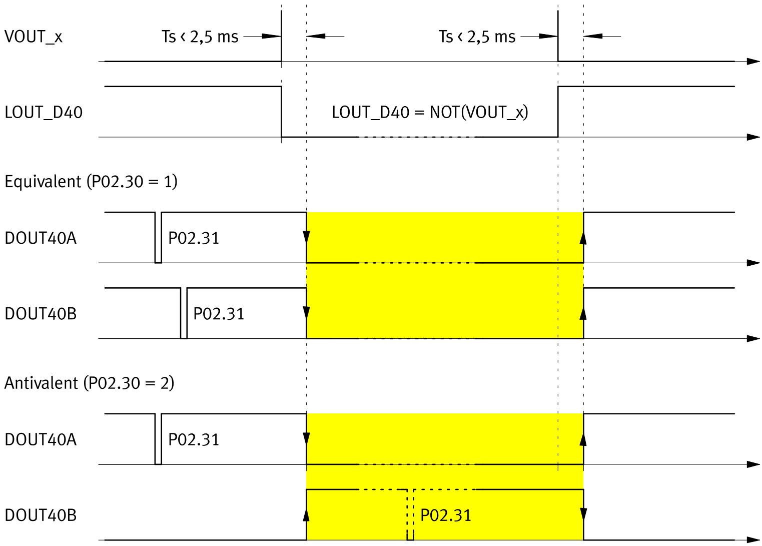


Fig. 58: Timing diagram of the two-channel safe outputs

Term/abbreviation	**Explanation**
VOUT_x	Virtual outputs
LOUT_x	Logical outputs
DOUT40A, DOUT40B	Two-channel digital outputs
Equivalent / Antivalent	Equivalent/antivalent

Tab. 83: Legend for timing diagram of the two-channel safe outputs

The following times elapse from the control of a safe output until the output pins are switched over:

Time delays from LOUT_D4x until level change at output	**Minimum**	**Maximum**	**Typical**
Time delay Ts	0.0 ms	2.5 ms	0.5 ms
Duration of the test pulses (P02.31, ...)	0.4 ms	10.0 ms	1.0 ms

Tab. 84: Time delays DOUT40 ... DOUT42

Parameters for the two-channel digital outputs

Parameter no. for output ...			Name	Description
DIN40	DIN41	DIN42		
P02.30	P02.32	P02.34	Operating mode	Mode: Off (0 V)/equivalent/anti-valent/ON (24 V)
P02.31	P02.33	P02.35	Test pulse length	Length of the test pulse

Tab. 85: Parameters of two-channel digital outputs

3.9.2 Internal brake control of the motor controller [X6]

Use

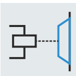


Fig. 59: Symbol for holding brake

The motor controller has integrated circuit breakers for safe brake control. Both the +24 V connection and the 0 V connection of the holding brake are switched by separate power transistors.
The holding brake is normally activated functionally by the motor controller. However, the circuit breakers can also be used in combination with the CAMC-G-S3 to control a clamping unit or holding brake via the SBC safety function.

ⓘ

The integrated brake control at output [X6] meets the requirements for PL d/Cat. 3 according to EN ISO 13849, or SIL 2 according to EN 61800-5-2.

Function

The safety module actively intervenes in the control of the high and low-side switches in the motor controller. The safety module is controlled by both micro controllers via the signals BR+_BASEUNIT and BR-_BASEUNIT. The Low status of the respective signal switches off the corresponding power transistor and the holding brake takes effect.

ⓘ

When the device is delivered, the internal brake control is already configured so that a request by the SBC safety function causes a switch-off of the signals BR+_BASEUNIT and BR-_BASEUNIT.
Observe the polarity of the control signal from the SBC function:
VOUT_SBC_BRK_ON = 1 means that the clamping unit or holding brake should engage.
For this reason, the control signal must be inverted:
LOUT_BRAKE_CTRL = NOT(VOUT_SBC_BRK_ON)

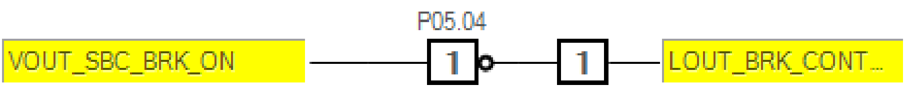


Fig. 60: Configuration of brake control (example)

Block diagram

Internal Brake

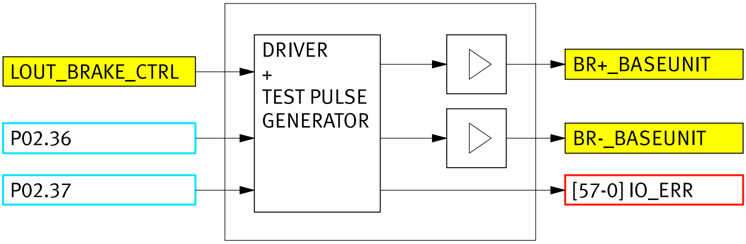


Fig. 61: Block diagram of the safe brake control in the basic unit

Term/abbreviation	Explanation
LOUT_BRAKE_CONTROL	Logical output brake control
DRIVER + TEST PULSE GENERATOR	Driver and generation of test pulses
BR+_BASEUNIT/BR-_BASEUNIT	Internal signals: brake control
[57-0] IO_ERR	Internal error signal error 57-0

Tab. 86: Legend for block diagram of the safe brake control in the basic unit

Output control signals BR+/BR-	Safe brake control not energised	Safe brake control energised
LOUT_BRAKE_CTRL	1	0
BR+_BASEUNIT	0	1
BR-_BASEUNIT	0	1

Tab. 87: Logic signals BR+_BASEUNIT/BR-_BASEUNIT

Error detection

Test pulses are used to test the function of the high-side and low-side switches during operation. The test pulse length can be parameterised (P02.37). When the safe brake control is energised, every circuit breaker in the basic unit is checked separately with test pulses. The pulse duration can be parameterised. An internal feedback signal is used to measure the voltage at the safe brake output of the safety module.

The following faults are recognised

- short from BR+ to 24 V.
- short from BR- to 0 V.

If there is a fault, error [57-0] IO_ERR is generated.

ⓘ

The integrated brake control at the output [X6] is suitable for clamping units or holding brakes with 24 V and max. 2 A current consumption ➔ Technical data of brake output in the hardware description GDCP-CMMP-AS-G3-HW-...
Alternatively, the clamping unit or holding brake can be controlled via a safe digital output (DOUT40 to DOUT42) and an external brake switching device.
Examples ➔ 4.3.5 Control of a clamping unit and ➔ 4.3.6 Control of a 2-channel clamping unit.

Timing diagram

The following diagram shows an example of the time response when the internal brake output [X6] is switched off and on again. The test pulses for the energised clamping unit or holding brake (pressurised) are also shown. They are time offset.

Internal brake

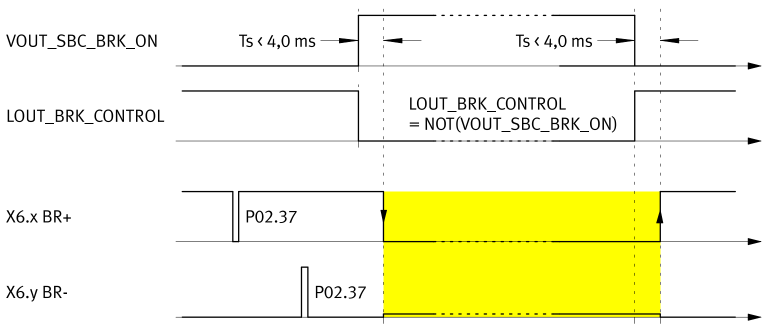


Fig. 62: Timing diagram of the integrated brake control in the basic unit

Term/abbreviation	Explanation
VOUT_SBC_BRK_ON	Virtual output, control of internal brake
LOUT_BRK_CONTROL	Logical output, control of internal brake
X6.x BR+ / X6.y BR-	Signals at the contacts of the brake output in the basic unit

Tab. 88: Legend for timing diagram of the integrated brake control in the basic unit

The following times elapse from control of the internal brake until the output pins at [X6] are switched over:

Time delays from LOUT_BRAKE_CTRL until level change of brake output [X6] of the basic unit	Minimum	Maximum	Typical
Time delay Ts	0.0 ms	4.0 ms	2.0 ms
Duration of the test pulses (P02.37)	0.4 ms	10.0 ms	1.0 ms

Tab. 89: Time delays, internal brake

Parameters for the internal safe brake control

Internal brake		
No.	Name	Description
P02.37	Test pulse length	Length of the test pulse

Tab. 90: Parameters of internal brake

3.9.3 Signal contact C1, C2 [X40]

Use

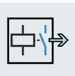


Fig. 63: Symbol for relay output

The potential-free signal contact is ideally used as a diagnostic output. It can be used to signal the operating status of the safety module to an external safety controller.

Function

The signal contact has one channel and may not be used as a part of a safety chain.
The contact does not have forced contacts for safety monitoring of the fault-free function. The potential-free signal contact can be configured in the same way as a safe output, although test pulses to test digital inputs cannot be output.
The contact is an N/O contact. The contact is open in the standstill/de-energised status and also during initialisation and Power off/on of the safety module.

Block diagram

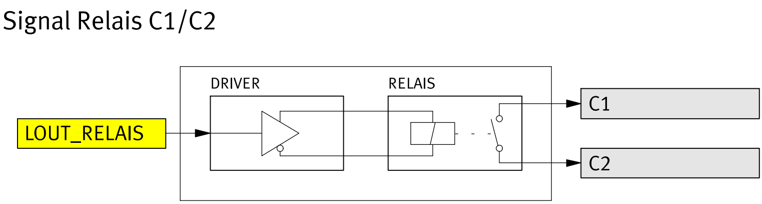


Fig. 64: Block diagram of the potential-free relay output

Term/abbreviation	**Explanation**
LOUT_RELAY	Logical output, feedback contact
DRIVER	Driver

Tab. 91: Legend for block diagram of the potential-free relay output

Signal contact output	Standstill state	Active
LOUT_RELAY	0	1
Contact C1/C2	open	closed

Tab. 92: Logic signals, signal contact

Error detection

The status of the switching contact is not monitored.

ⓘ

When the device is delivered, the signal contact is preconfigured as follows:
Contact closed when no error is pending and all requested safety functions return the safe status (common message VOUT_SSR "Safe State Reached").

Timing diagram

The following diagram shows an example of the time response when the signal contact is switched off and on again.

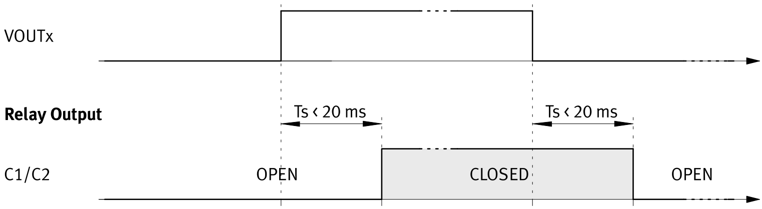


Fig. 65: Timing diagram of the potential-free signal contact

Signalling contact C1/C2

Term/abbreviation	Explanation
VOUTx	Virtual output
OPEN / CLOSED	(Relay contact) open/closed

Tab. 93: Legend for timing diagram of the potential-free signal contact

The following times elapse from control of the relay until the output pins are switched over:

Time delays from LOUT_RELAY until relay switches	Minimum	Maximum	Typical
Time delay Ts	0.0 ms	20.0 ms	6.0 ms

Tab. 94: Time delays, relay output

The signal contact is implemented as a miniature relay.

ⓘ

The service life and switching cycle resistance of the relay is primarily dependent on the level and type of the load on the relay contact.
Electrical data of the signal contact ➔ Tab. 145 Technical data: signal contact C1/C2 [X40].

3.9.4 +24 V auxiliary power supply [X40]

The auxiliary supply can be employed when using feedback contact C1/C2 or to supply external active sensors.
The safety module provides a 24 V DC voltage at interface X40 with a load capacity of max. 100 mA. The output for the 24 V is protected against overload and short circuits by a PTC.

ⓘ

Electrical data of the auxiliary power supply ➔ Tab. 146 Technical data: 24 V auxiliary supply [X40].

3.10 Operating status and status indicators

3.10.1 Statuses of the system/finite state machine

The following diagram shows the status transitions of the safety module on starting after Power ON.

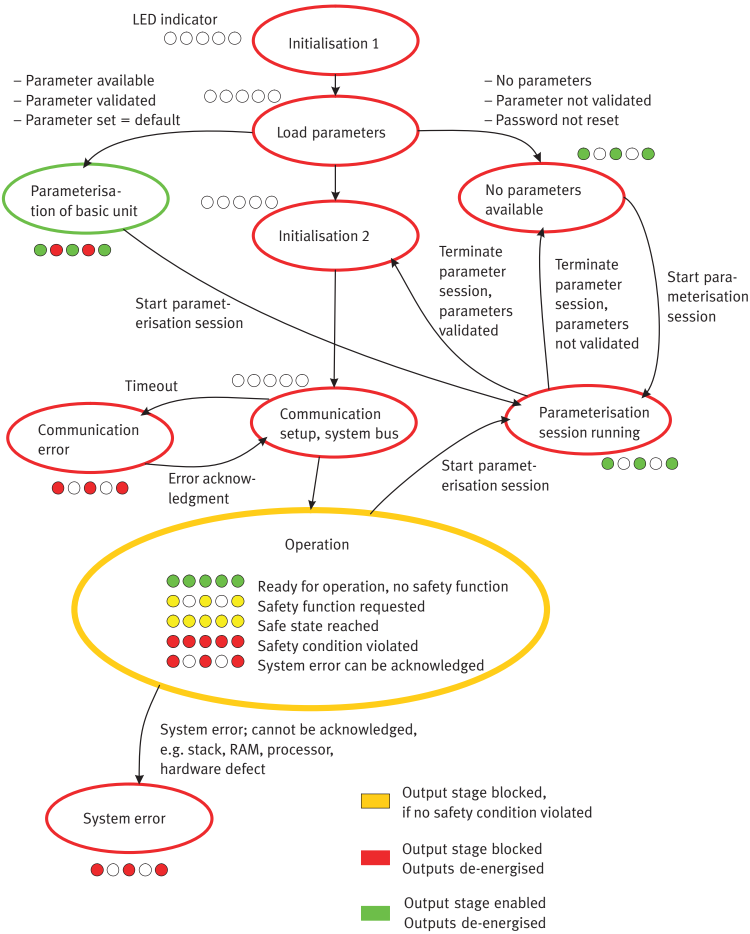


Fig. 66: Statuses of the “complete system”

Description of the statuses of the “complete system”

- In phase 1, Initialisation, basic system tests of the hardware and firmware are performed.
- Then the parameter set is loaded from the flash memory of the module and is checked:
  - The safety module checks whether there is a valid safe parameter set in the safety module. A valid safe parameter set exists when all the individual parameters have been validated and the whole parameter set has the identification “validated”.
  - It checks whether the safety module is in the delivery status. In the delivery status, all the individual parameters are validated but the whole parameter set has the identification “not validated”. In addition, the identifier “Delivery status” is set in the parameter set.

ⓘ

The basic unit can be commissioned and the motor run in the delivery status. The safety module is pre-configured with the safety functions STO and SBC, which can be requested via DIN40, thus offering minimum protection ➔ 5.4.2 Delivery status and ➔ 5.4.1 Factory setting.

- If not all the individual parameters have been validated or the whole parameter set has the identifier “not validated” and the system is not in delivery status, then the safety module switches to the “Service” status and waits for external parameterisation.

ⓘ

The motor and the basic unit cannot be commissioned in the “Service” status. The safety module has switched off all safe outputs and the device-internal control signals for enabling the power stage and the holding brake.

- When parameterisation is complete, a second initialisation takes place.
- It then establishes communication with the basic unit.
- If no errors have been found up to that point and the safety module has a valid, safe and fully validated parameter set, it switches to the “Operation” status in which safety functions can be requested and executed. In the “Operation” status all the modules work according to their specified functionality.
- If system errors are detected, e.g. a defective position encoder, then the safety module switches to the “System error” status, which can only be exited after elimination of the error and subsequent error acknowledgement or a restart of the system.

Status transitions of the safety module during "Operation" ➔ Fig. 67.

- The “Ready for operation” status remains valid so long as a safety function has not been requested.
- If at least one safety function is requested, the safety module switches to the status “Safety function requested”. Monitoring is already active but the safe status has not yet been reached, e.g. because a speed ramp is being shut down.
- The status “Safe state reached” is then set. Monitoring is active. The drive is in the safe state.
- The status “Safety condition violated” is set in case of error. It can only be exited via error acknowledgement.

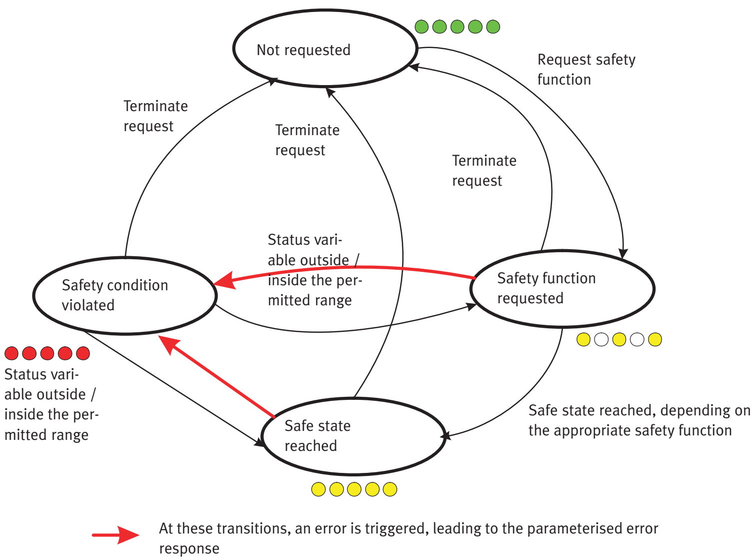


Fig. 67: Statuses of the “Operation” safety functions

The safety functions, for their part, have small-scale sequence controls and generate status and error messages (example: Safety function SS1 ➔ Fig. 30). Various common status messages are generated from the errors or operating statuses of the individual safety and logic functions.

The common messages are formally implemented as virtual outputs. They are fed back as corresponding logical inputs.
This means that outputs (e.g. signal relay) can be controlled according to the system status, and safety functions can be controlled according to the system status.
The common status messages are described below.

VOUT_READY: “Ready for operation, no safety function requested”

The “Ready for operation, no safety function requested” signal becomes “1” when no error message is pending whose reaction exceeds a warning and no safety function has been requested.

VOUT_SERVICE: “Service”, the safety module must be parameterised

The “Service” signal becomes “1” if the parameter set of the module is invalid, if a parameterisation session is running or if no parameter set is available. There is an identifier in the parameter set with which the safety module can detect whether this is the delivery status (= standard parameter set).

NOTICE

If the checksum of the parameter set is faulty, this is a serious internal error, which will lead to the “System error” status.

VOUT_SFR: “Safety Function Requested”
The “Safety function requested” signal becomes “1” when at least one safety function has been requested. It remains active until all requests have been reset.

VOUT_SSR: “Safe State Reached”
The “Safe state reached” signal becomes “1” if the “Safe state reached” output is active for **all** the requested safety functions and if at least one safety function has been requested.

VOUT_ERROR: “System Error”
The “System error” signal becomes “1” if there is at least one error pending whose reaction is parameterised higher than “Warning”. An exception to this is errors of the category “Safety condition violated”, which have their own common error message.
Note: this is the case if either an acknowledgeable error of a module is pending or if the entire system is in the “System Error” or “Communication Error” status.

VOUT_SCV: "Safety Condition Violated"
The “Safety condition violated” signal becomes“1” if at least one error of the category “Safety condition violated” is pending in the error management and if the error response of this error is prioritised higher than “Warning”.

VOUT_WARN: “Warning”
The “Warning” signal becomes “1” if there is at least one error pending whose reaction is parameterised as “Warning”. An exception to this is errors of the category “Safety condition violated”.

VOUT_PS_EN: “Power Stage Enable”/“Ready to switch on the power stage”
The signal “Ready to switch on the power stage” directly maps the status of the safe pulse inhibitor (STO safety function). It is “1” if the driver supply has been enabled by the safety module and “0” if the driver supply was switched off via the STO safety function.

3.10.2 Status display on the safety module

The safety module has an LED on the front to indicate the status of the safety function ➔ 6.4.1 LED indicators on the safety module.
The status LED displays the operating status of the safety module. The display is exclusively for diagnostics and must not be used in a safety-oriented way.
If several statuses are present at the same time and result in a display, the status with the highest priority is displayed. The priorities are shown in the following table.
The display is steady or flashes at approx. 3 Hz.

LED display	Status signal	Priority	Safety module status	Internal status
flashing red 	VOUT_ERROR = 1	7	“System Error”	The entire system is in the “System Error” or “Communication Error” status.
lit up red 	VOUT_SCV = 1 VOUT_SFR = 1	6	“Safety Condition Violated”, error response initiated	Violation of at least one of the currently required safety functions.

LED display	Status signal	Pri-ority	Safety module status	Internal status
lit up yellow	VOUT_SSR = 1 VOUT_SFR = 1	5	“Safe State Reached”	All requested safety functions are in the status “Safe State Reached”.
flashing yellow	VOUT_SFR = 1	4	“Safety Function Requested”	The signal is active as soon as at least one safety function is requested. It remains active until all requests have been reset.
flashing red/ green	VOUT_SERVICE = 1 VOUT_PS_EN = 1	3	“Delivery Status”	The delivery status can be distinguished from the “Service status” using VOUT_PS_EN.
flashing green	VOUT_SERVICE = 1 VOUT_PS_EN = 0	2	"Service Status"	No parameters present, parameters invalid or parameterisation session is running.
lit up green	VOUT_READY = 1 VOUT_PS_EN = 1	1	“Ready”	Operational, no safety function requested, no errors.
Off	VOUT_READY = 0 VOUT_PS_EN = 0	0	“Initialisation Running”	Initialisation 1: load parameter, Initialisation 2: establish communication.

Tab. 95: System statuses and messages

3.10.3 7-segment display of the motor controller

The 7-segment display of the motor controller shows additional information ➔ 6.4.2 7-segment display of the motor controller, e.g.:

- Display of the active safety function
- Display of error messages of the safety module with unique error numbers. Previously requested stop functions (STO, SS1, SS2, SOS) have a higher display priority than the other safety functions ➔ 6.6 Diagnostic messages with information for fault clearance.
- Display of an active parameterisation session.

3.11 Permanent and temporary diagnostic memory in the motor controller

The diagnostic messages are permanently saved in the permanent memory of the motor controller (secure in the event of a power failure). This memory consists of 2 segments, which are filled one after the other. If both segments are filled, the older segment is automatically deleted. This provides a quasi-ring memory for the permanently stored messages.
The motor controller manages a permanent diagnostic memory, which is stored in the non-volatile memory of the device and thus remains intact, even in the case of voltage failure/power-off. The permanent diagnostic memory is intended for non-volatile storage of errors and other events.

The permanent diagnostic memory consists of two blocks, which can be written to alternately. If one block is full, the other block is deleted. The architecture of the memory means that half of the saved entries are lost during a deletion operation.
The permanent diagnostic memory is used both by the safety module and by the motor controller. Entries of the motor controller use up the total available memory capacity. There is no memory reservation for the safety module.
Status and error messages are entered chronologically. The oldest entries are deleted when a block is full.
The following events with reference to the safety module are logged in the permanent diagnostic memory:

- starting a parameterisation session (also attempt to start)
- ending a parameterisation session
- changing/resetting the password
- backing up the parameter set in the safety module
- errors and warnings
- acknowledging errors
- request for a safety function (can be activated)

Logging of requests for safety functions is deactivated in the factory settings; this can be activated using parameter P20.4A.

An entry in the error list looks like this in the FCT:

No.	Fault no.	Fault description	Time stamp	Constant	Free parameter	Type
1	00-21	Log entry of the safety module	580:15:03	0x0000	Error acknowledged, source: 0x01, error-free	Error
2	00-8	Controller switched on	580:15:00	0x0000	0x0000	Error
3	00-12	Module replacement: current module	580:15:22	0x4830	CAMC-G-S3, S/N: 1212820487, HW rev.: 1.0, SW rev.: 1.0	Error
4	00-11	Module replacement: previous module	580:15:22	0x48FF	CAMC-DS-M1, S/N: 3781764777, HW rev.: 0.1, SW rev.: 0.1	Error
...	...	...	...	...	...	...

Tab. 96: Example of entries in the permanent diagnostic memory of the basic unit, with error messages of the safety module

An entry in the permanent diagnostic memory contains the following information:
- Sequence number
- Status or error number, comprising the main index and subindex, with brief description
- Diagnostic parameters in hexadecimal representation:
  1 x 16 bit constant
  1 x 32 bit free parameter (meaning dependent on the error)
- Time stamp, current system time of the operating hours counter in the motor controller

Error messages of the safety module may contain additional information, which is shown in a subsequent entry. For example, entry no. 2 contains the additional information for error entry no. 1.

Always document the full error information for support enquiries, in particular the diagnostic parameters and also subsequent entries.
The diagnostic parameters contain internal information, for example the program module and the conditions in which the error occurred. This information is intended for the manufacturer and may be of use for solving the problem.
You can read out the entire diagnostic memory of the device and export it to a CSV file. The file then contains the entire error history of the device and can be used for troubleshooting and support enquiries.

3.12 Time response

3.12.1 Sampling times

The safety module records all input and output variables at regular intervals. The variables are recorded at two fixed switching frequencies ➔ Tab. 97 Sampling times of the safety module.

Cycle	Sampling frequency	Cycle time	Function
TSample	typ. 8 kHz	typ. 125 µs	The cycle is internally synchronised to the control sampling cycle of the basic unit, range T_{Sample} = 100 µs - 200 µs – Recording all inputs and outputs – Evaluation of position encoders – Filter calculation – Generation of test pulses – Internal communication
TLogic	500 Hz	2 ms	Fixed sampling cycle for safety functions – Calculation of safety functions – Calculation of logic functions – Finite state machine, error management – Signal sequence LIN_x ➔ VOUT_x

Tab. 97: Sampling times of the safety module

ⓘ

The detection of the input signals is thus subject to a maximum jitter of $T_{Logic} + T_{Sample}$. Therefore, an input signal is recorded at best immediately or, at the latest, after 2.125 ms. The start of a safety function can also be affected by this jitter relative to the input signal. The jitter is taken into account in the specified reaction times of the individual function blocks.

3.12.2 Reaction time on request of a safety function

The reaction time of the safety module is made up of three components:

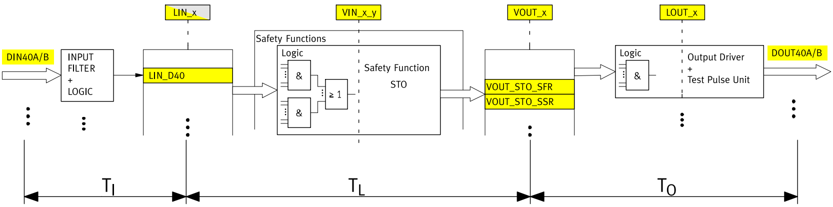


Fig. 68: Reaction times of the safety module (schematic diagram, excerpt from ➔ Fig. 5)

T_I: time from the signal change at the input to mapping of the input status in the logical input signal LIN_x. The time is dependent upon the settings of the input filters ➔ 3.4 Digital inputs.

T_L: time execution of the safety or logic function LIN_x to output of the status in VOUT_x. The time is dependent on the settings of the safety and logic functions, specified in ➔ 3.5 Safety functions and ➔ 3.6 Logic functions.

T_O: time for output of status information VOUT_x to the digital outputs. The time is dependent on the switching delay of the outputs ➔ 3.8 Error management and error acknowledgement.

ⓘ

If the output signals VOUT_x lead back to inputs LIN_x, note that there is an additional run-time of T_{Logic}.

Example: use of the extended logic functions to request a safety function via the LIN_ALFx_OUT signal.

➔ If possible, safety functions should be requested directly in order to minimise run-times.

The resulting reaction time up to the execution of the safety function is made up of:

$T_{res} = T_I + T_L$

Example: STO request via DIN40, quick request P02.08 set

Reaction times	**Minimum**	**Maximum**	**Typical**
Specification for T_I for DIN4x ➔ Tab. 24 Time delays DIN40 … DIN43			
Reaction time for “Quick detection request” = 1 (P02.08 / P02.0D / P02.12 / P02.17 = 1)	0.5 ms	2.5 ms	1.5 ms
Specification for T_L for STO ➔ Tab. 33 STO time delays			

Reaction times	**Minimum**	**Maximum**	**Typical**
Reaction time until switch-off of driver supply for basic unit and power stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**3.5 ms**	**7.0 ms**	**5.0 ms**

Tab. 98

The time until the status message that the safety function has been requested is calculated from

$T_{res} = T_I + T_L + T_O$

Example: SOS request via DIN40, P02.08 =0, P02.04 = 3 ms, P0B.00 = 2 ms

Reaction times	**Minimum**	**Maximum**	**Typical**
Specification for T_I for DIN4x ➔ Tab. 24 Time delays DIN40 ... DIN43			
Reaction time without “Quick detection request” and 3 ms filter time	3.5 ms	5.5 ms	4.5 ms
Specification for T_L for SOS ➔ Tab. 57 SOS time delays			
VOUT_SOS_SSR output with P0B.00 = 2 ms	4.0 ms	4.1 ms	4.0 ms
Specification for T_O via DOUT40 ➔ Tab. 84 Time delays DOUT40 ... DOUT42			
Time delay T_S	0.0 ms	2.5 ms	0.5 ms
Total:	**7.5 ms**	**12.1 ms**	**9.0 ms**

Tab. 99

3.12.3 Reaction time on violation of a safety function

The reaction time of the safety module when hazardous movements occur or if a position encoder fails is also made up of three components:

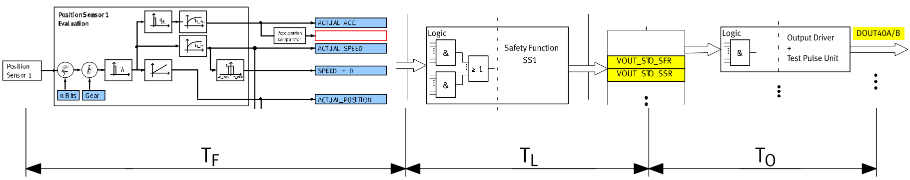


Fig. 69: Calculation of the speed and acceleration (schematic diagram, excerpts from ➔ Fig. 10 and ➔ Fig. 5)

T_F: time from occurrence of the hazardous movement up to mapping in the safety module (filter for speed signals), or time up to the detection of the defective position encoder ➔ Tab. 14 Parameters for error detection in the position sensors that influence the time response

T_L: time for execution of the safety or logic function of LIN_x, taking into account any allowable times up to the output of the error signal VOUT_xxx_SCV ➔ 3.5 Safety functions.

T_O: time for output of status information VOUT_x to the digital outputs. The time is dependent on the switching delay of the outputs ➔ 3.8 Error management and error acknowledgement.

Detection of a dangerous movement: the reaction time up to the internal detection of the violation is made up of:

$T_{res} = T_F + T_L$

Example: SSF0 safety function, indicated as SLS, allowable time P0E.03 = 4 ms encoder configuration with rotational speed filter P06.08 = 8 ms

Reaction times	Minimum	Maximum	Typical
Recording the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, T_L			
Reaction time with reference to the allowable time P0E.03	4.0 ms	6.0 ms	5.0 ms
Total:	**12.0 ms**	**14.1 ms**	**13.0 ms**

Tab. 100

Detection of a dangerous movement: the time up to safe output of the status messages indicating that the safety function has been violated is calculated as follows:

$T_{res} = T_F + T_L + T_O$

Reaction times	Minimum	Maximum	Typical
Recording the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, T_L			
Reaction time with reference to the allowable time P0E.03 = 4 ms	4.0 ms	6.0 ms	5.0 ms
Specification for T_O via DOUT40 ➔ Tab. 84 Time delays DOUT40 ... DOUT42			
Time delay Ts	0.0 ms	2.5 ms	0.5 ms
Total:	**12.0 ms**	**16.6 ms**	**13.5 ms**

Tab. 101

Detection of a dangerous movement: the time from the occurrence of a dangerous movement until the error response (here STO) and until the power stage is safely switched off is calculated as follows:

$T_{res} = T_F + T_{L, SSF0} + T_{L,STO}$

Example: as above, switch-off of the drive via STO error response

Reaction times	Minimum	Maximum	Typical
Recording the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, T_L			

Reaction times	Minimum	Maximum	Typical
Reaction time with reference to the allowable time P0E.03 = 4 ms	4.0 ms	6.0 ms	5.0 ms
Specification for T_L for STO ➔ Tab. 33 STO time delays			
Reaction time until switch-off of driver supply for basic unit and power stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**14.5 ms**	**18.6 ms**	**16.5 ms**

Tab. 102

Detecting a defective position encoder. The time from the occurrence of an error in the position encoder until the error response (here STO) and until the power stage is safely switched off is calculated as follows:

$T_{res} = T_F + T_{L,STO}$

Example: detection of encoder error, switch-off of the drive via STO error response

Reaction times	Minimum	Maximum	Typical
Detection of encoder error T_F			
Error detection in the encoder evaluation	10.0 ms	10.1 ms	10.0 ms
Specification for T_L for STO ➔ Tab. 33 STO time delays			
Reaction time until switch-off of driver supply for basic unit and power stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**12.5 ms**	**14.6 ms**	**13.5 ms**

Tab. 103

3.12.4 Other times for error detection and communication

See the following table for additional delay times/error reaction times:

Description	Time TF maximum
Safety function is requested, status variables not available ⇢ safety condition violated	2 ms
Input: Stuck-At error detected, no test pulse	< 16 s
Output: Stuck-At error detected, no test pulse	< 16 s
Two-channel inputs: equivalence/antivalence error at input (discrepancy time)	parameterisable, typically 100 ms (P02.05, P02.0A, P02.0F, P02.14)
Two-handed control unit: Time violation simultaneity (discrepancy time)	parameterisable, typically 500 ms (P02.03)
Mode selector switch: violation 1-of-n (discrepancy time)	parameterisable, typically 100 ms (P02.01)

Description	Time TF maximum
RAM error, flash error, stack error, CPU error, program run error	depending on error type 2 ms ... 8 h
Cross-comparison of data µC1/µC2 returns errors	< 16 s
Faulty operating voltage: time between occurrence of error and triggering of the reaction	≤ 2 ms
Digital angle encoders: communication error, error of four-cycle (EnDat packages incorrect or missing)	≤ 2 ms
Other angle encoder [X2B]: delay time for transferring the data from the basic unit	≤ 400 µs, typically 250 µs
Determination of the setpoint limits (safety functions control setpoint limits in the motor controller)	≤ 2 ms

Tab. 104: Other time delays/error reaction times

3.13 DIL switch

DIL switches are located on the front panel of the safety module. They do not have a safety function. The meaning of the individual switches depends on the interface used for fieldbus communication. The DIL switches can be used to activate/deactivate fieldbus communication and, for example, to set up a device address.

ℹ

You can find information on the DIL switch settings in the ➔ Mounting and installation description, GDCP-CMMP-M3-HW-...

4 Assembly and installation

4.1 Mounting/removal

The safety module CAMC-G-S1 is suitable exclusively for integration into the motor controller CMMPAS-...-M3. It cannot be operated outside the motor controller.

⚠ WARNING

Danger of electric shock if the safety module is not mounted.

Touching live parts causes severe injuries and may cause death.
Before touching live parts during maintenance, repair and cleaning work and when there have been long service interruptions:

- Switch off power to the electrical equipment at the main switch and lock the switch to prevent reactivation.
- After switch-off, wait at least 5 minutes for the equipment to discharge before accessing the controller.

NOTICE

Incorrect handling may damage the safety module or motor controller.

- Switch off the power supply before mounting and installation work. Do not switch on the supply voltages until mounting and installation work is completely finished.
- Never unplug the safety module from or plug it into the motor controller when powered!
- Observe the handling specifications for electrostatically sensitive devices. Do not touch the components and conductive tracks on the PCB or the pins on the terminal strip in the motor controller. Hold the safety module only by the front plate or the edge of the PCB.

Mounting the safety module

1. Slide the safety module into the guides.
2. Tighten screws. Use a tightening torque of 0.4 Nm ± 10%.
   Result: the front plate is in electrical contact with the housing.

Removing the safety module

1. Unscrew screws.
2. Release the safety module a few millimetres by gently levering the front panel or by pulling on the mating plug, and pull it out of the slot.

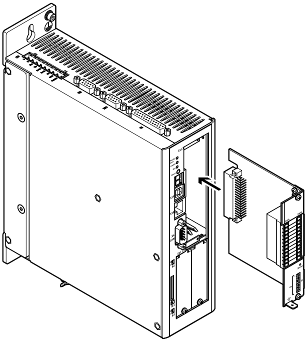


Fig. 70: Mounting/removal

4.2 Electrical installation

4.2.1 Safety instructions

⚠ WARNING

Danger due to failure of the safety function!

It can always be assumed that a loss of power will lead to the safe status (quiescent current principle) in mechanical equipment without the impact of external forces. This must be shown/confirmed by the danger and risk analysis of the application.

Absence of safety function can result in serious, irreversible injuries, e.g. due to unintentional movements of the connected actuator technology.

- Ensure that your application has a reliable power supply or use other appropriate measures.

The requirements of EN 60204-1 must be fulfilled for the installation. If this is not possible, e.g. fault exclusion can be achieved by using a safety relay unit with detection of shorts across contacts.

⚠ WARNING

Danger of electric shock from voltage sources without protective measures.

- Use only PELV circuits in accordance with EN 60204-1 (protective extra-low voltage, PELV) for the electrical logic power supply.
- Observe the general requirements in accordance with EN 60204-1 for PELV circuits.
- Use only voltage sources that ensure a reliable electric separation of operating voltage from other active circuits in accordance with EN 60204-1.

The use of PELV circuits ensures protection against electric shock (protection against direct and indirect contact) in accordance with EN 60204-1. The 24 V fixed power supply used in the system must be able to control the voltage interruption defined in EN 60204-1.

The cables are connected with two plugs. As a result, the cables can remain plugged into the plugs when replacing the safety module, for example.

ⓘ

Make sure that bridges or the like cannot be inserted parallel to the safety wiring. For example, use the maximum wire cross section of 1.5 mm² or appropriate wire end sleeves with insulating collars. Use twin wire end sleeves for looping cables between adjacent devices.

ESD protection

Damage may be caused to the device or to other system parts at unassigned plugs as a result of ESD (electrostatic discharge). Earth the system parts prior to installation and use appropriate ESD equipment (e.g. earthing straps etc.).

4.2.2 Functional earth

If you use a shielded connecting cable for [X40]:

Keep the unshielded part of the cable as short as possible (< 50 mm); use a short earthing strap with 6.3 mm flat plug for the shield connection.

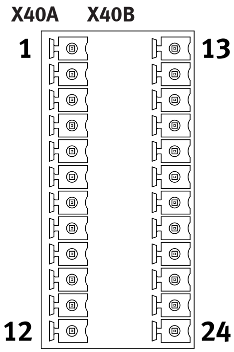
Connect the flat plug for the shield connection to the connection for functional earth provided in ➔ Fig. 3, connection [7].

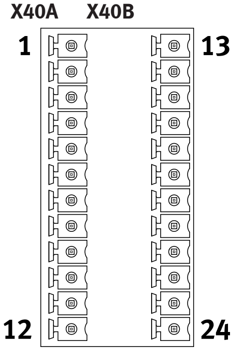
4.2.3 Connection [X40]

The safety module CAMC-G-S3 has a combined interface for control and feedback via the plug [X40] on the front panel.

– Version on the device: PHOENIX CONTACTMINICOMBICON MC 1.5/8-GF-3.81 BK
– Plug (included in the scope of delivery): PHOENIX CONTACT MINICOMBICON MC 1.5/8-STF-3.81 BK

The mating plug set, consisting of mating plugs for X40A and X40B, can also be ordered separately: assortment of plugs NEKM-C-9.

Plugs	Pin	Designation	Description (factory setting[1)])
	X40A plug connectors		
	1	DIN40A	Digital input 40, two-channel (Factory setting: emergency stop switching device, STO and SBC request)
	2	DIN40B	
	3	DIN42A	Digital input 42, two-channel
	4	DIN42B	
	5	DOUT40A	Digital output 40, two-channel
	6	DOUT40B	
	7	DIN44	Digital input 44 (Factory setting: brake feedback)
	8	DIN45	Digital inputs 45, 46, 47 (Factory setting: mode selector switch)
	9	DIN46	
	10	DIN47	
	11	DIN48	Digital input 48 (Factory setting: error acknowledgement).

Plugs	Pin	Designation	Description (factory setting[1])
	12	DIN49	Digital input 49 (Factory setting: terminate safety function on rising edge).
	X40B plug connector		
	13	DIN41A	Digital input 41, two-channel
	14	DIN41B	
	15	DIN43A	Digital input 43, two-channel
	16	DIN43B	
	17	DOUT41A	Digital output 41, two-channel
	18	DOUT41B	
	19	DOUT42A	Digital output 42, two-channel
	20	DOUT42B	
	21	C1)	Signal contact, relay contacts (Factory setting: safe state reached, no safety condition violated). – Open: “safety functions not active” – Closed: “safety functions active”
	22	C2)	
	23	GND24	0 V, reference potential for DINx/ DOUTx/+24 V
	24	+24 V	24 V output, auxiliary supply, e.g. for safety-related peripherals (24 V DC logic supply of the motor controller).

1) Function when the device is delivered or after resetting to factory settings (advance parameterisation)

Tab. 105: Pin allocation [X40]

To ensure the safety functions, the control ports are to be connected in two channels with parallel wiring. For an example, see ➔ Further information.

4.2.4 Minimum wiring for initial start-up [X40]

NOTICE

Loss of the safety function!

Absence of safety function can result in serious, irreversible injuries, e.g. due to unintentional movements of the connected actuator technology.

- Before initial commissioning, define what safety functions are required during the commissioning phase in order to guarantee the safety of the system during this phase as well prior to final delivery. At least one safe emergency stop function is generally required.

ⓘ

Commissioning in accordance with the EC Machinery Directive is the first intended use of the machine by the end customer. This is the commissioning performed by the manufacturer during mounting of the machine.

If, during the commissioning phase, safety-oriented circuitry is not (yet) required, then the switch module CAMC-DS-M1 can be used. The CAMC-G-S3 can then only be integrated into the motor controller after functional commissioning of the axes.
If, during the commissioning phase, only the STO and SBC safety functions are required (emergency stop), the initial commissioning of the motor controller CMMP-AS-...-M3 with the safety module CAMC-G-S3 should be performed with minimum wiring as shown in the sample circuit (➔ 4.3 Sample circuits) with one emergency stop switch ([2]).
Use a safety module in the “Delivery status” (it flashes red/green ■■■■■), ➔ Further information. The STO and SBC safety functions are already prepared in the delivery status.

NOTICE

Safety functions must never be bypassed:
- Carry out the minimum wiring for initial commissioning in such a way that it must be removed for the final safety circuitry.

ⓘ

You can find other sample circuits with a detailed description in the following sections.

4.3 Sample circuits

ⓘ

The following sample circuits all show a single-phase motor controller CMMP-AS-C...-3A-M3. The circuitry of [X9] must be adapted accordingly for three-phase motor controllers.
Only one input/switching device is shown in the examples. However, all four two-channel inputs can be used to request safety functions.

NOTICE

Some of the following sample circuits use passive sensors, such as emergency stop switches, which are monitored using external clock signals. The digital outputs of the safety module should be used as the source for the clock signals. This allows detection of the following errors:
- short circuits between input A and B, in the output circuit (DOUT4x) and in the input circuit (DIN4x).
- shorts of a cable to 0 V or +24 V.

Shorts between the input and output of the passive sensor are not detected or only detected on actuation (via discrepancy monitoring). For this reason, preventive measures are required in the system wiring to avoid this error (fault exclusion).

4.3.1 Safety request via devices with switch contacts

The safety function (e.g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request. The safety request is made over 2 channels via input device S1 and results in 2-channel switch-off of the power stage of the motor controller.

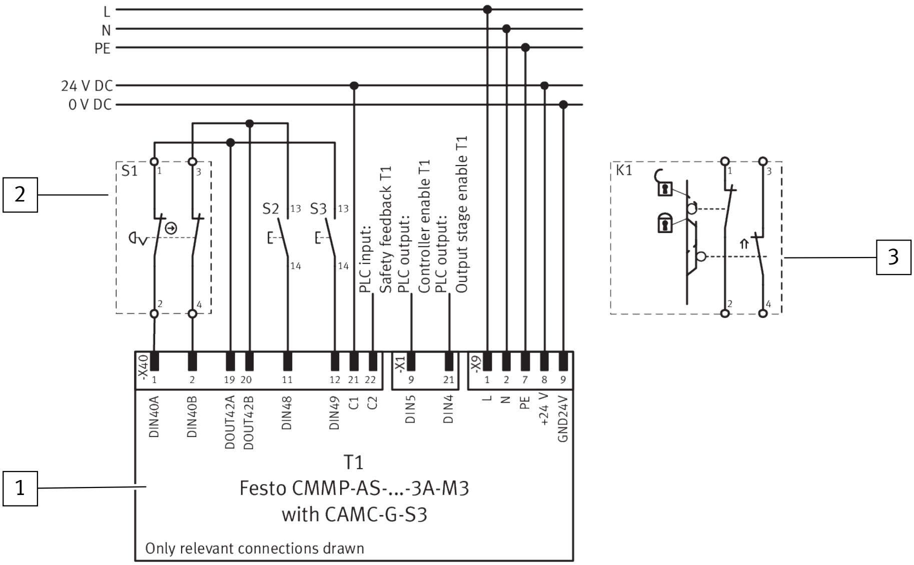


Fig. 71: Sample circuit with switch contacts

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device, e.g. emergency stop switch
3	S1: input device, e.g. safety door

Information on the sample circuit:

- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the switches S1, for the acknowledgement button S2 and for the start button S3.
- The safety functions are terminated by pressing the start button S3.
- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The feedback contact C1/C2 should be polled via the controller.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.2 Safety request via devices with semiconductor outputs

The safety function can be requested via various devices. Switch S1 can be a light curtain or a safety relay unit with semiconductor outputs. The safety request is sent over 2 channels via switch S1. If the safety function is active, then, in the example, this is output by the potential-free contact C1/C2.

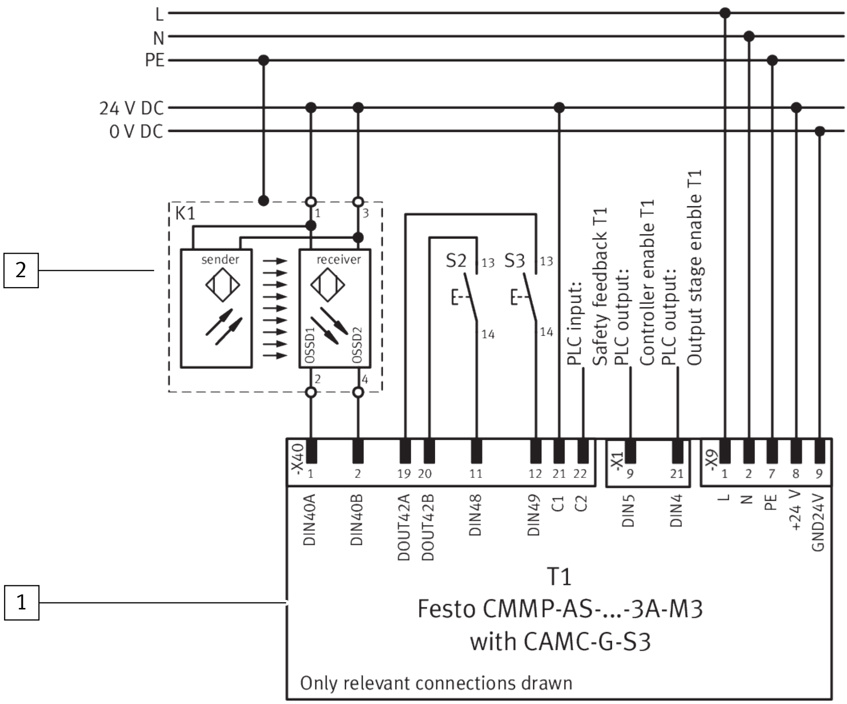


Fig. 72: Sample circuit, device with semiconductor outputs

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device, e.g. light curtain

Information on the sample circuit:

- The light curtain S1 detects shorts across contacts in the input circuit for the switches S1.
- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the start button S3 and the acknowledgement button S2.
- Errors are acknowledged by pressing the acknowledgement button S2, and the safety functions are terminated by pressing S3.
- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The feedback contact C1/C2 should be polled via the controller.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.3 Safety request via a safety relay unit

If more than four safety command devices (S1) are required or if a higher-order safety control is to be used, the motor controller (T1) can also be controlled via other safety command devices.

The safety function can be requested via various devices. The safety request is sent over 2 channels via switch S1 and is analysed by the safety relay unit S2 (safety relay, safety PLC). If the safety function is active, then, in the example, this is output by the potential-free contact C1/C2.

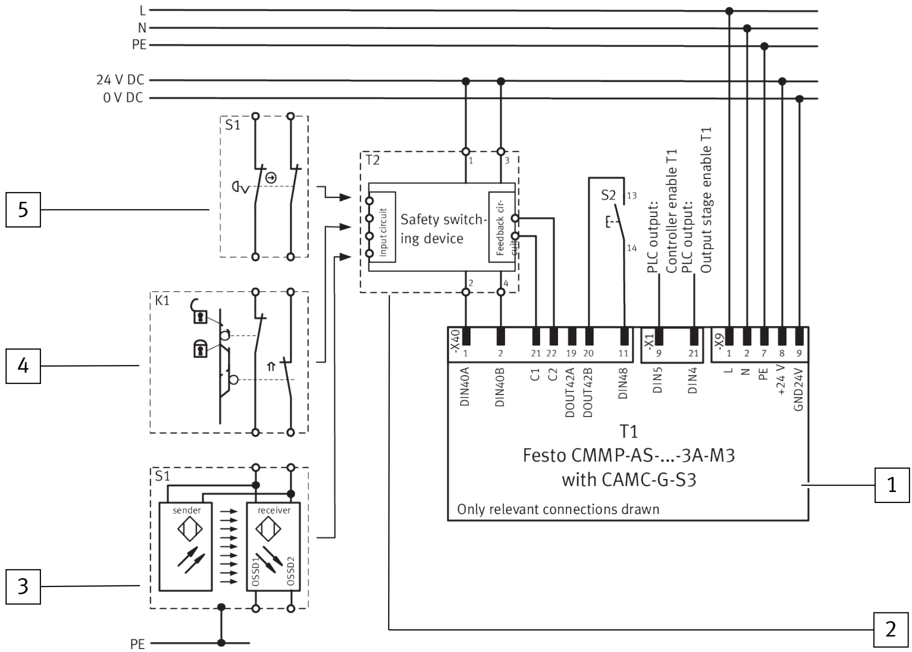


Fig. 73: Sample circuit with safety relay unit

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: safety relay unit
3	S1: light curtain
4	S1: safety door
5	S1: emergency stop switch

Information on the sample circuit:

- The safety relay unit T2 detects shorts across contacts in the input circuit for the switches S1. If a start button is required for the application, it is also connected to the safety relay unit T2. The safety module CAMC-G-S3 detects shorts across contacts for the acknowledgement button S2.
- The safety functions in the CAMC-G-S3 are parameterised to “automatic restart after cancellation of request” when an external safety relay unit is used.
- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The feedback contact C1/C2 is included in the feedback loop of the safety relay unit.

- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.4 Linking of several CMMP-AS-...-M3 with CAMC-G-S3

The safety function is triggered by an input device for the safety request for both motor controllers. The safety request is made over 2 channels via the input device S1 and results in 2-channel switch-off of the power stage of motor controllers T1 and T2. If the safe status has been reached in both motor controllers, it is output by the potential-free contact C1-C2 of motor controllers T1 and T2.

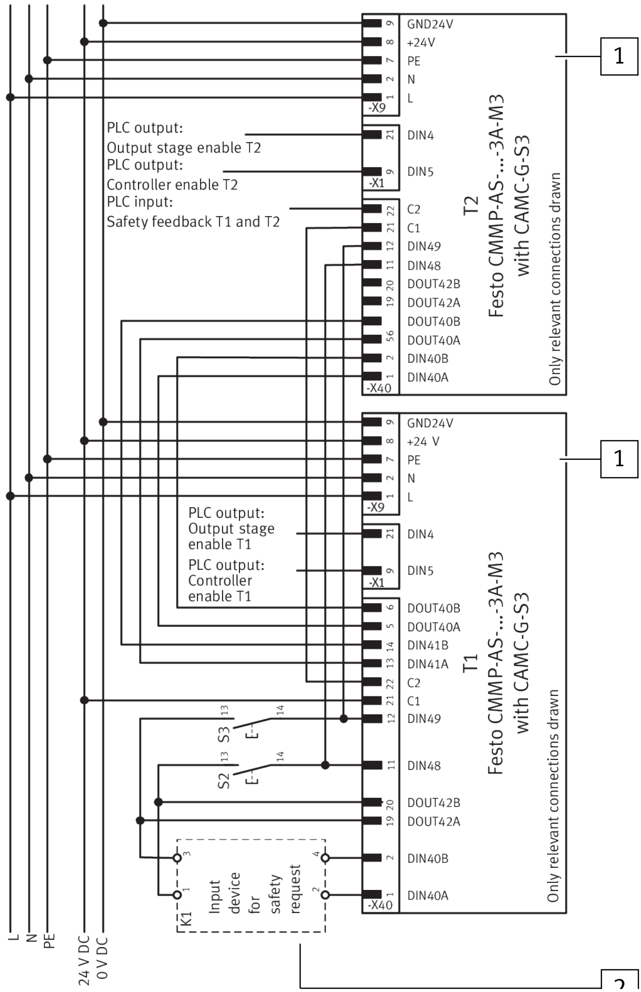


Fig. 74: Sample circuit for several CMMP-AS-...-M3 with CAMC-G-S3

1	T1/T2: motor controller with safety module (only relevant connections shown)
2	S1: input device for safety request

Information on the sample circuit:

- The CAMC-G-S3 in T1 detects shorts across contacts in the input circuit for the input devices for security requirement S1, for the acknowledgement button S2 and for the start button S3.
- The safety functions are terminated by pressing the start button S3.
- The motor controller T1 must forward the safety request to the motor controller T2 via DOUT40A/B, which then also responds to the safety request. – The motor controller T2 must send a safety request to the motor controller T1 as feedback.

- Feedback contacts C1, C2 of T1 and T2 are connected in series, and the signal should be polled via the controller. If a safety request has been issued, the controller should react appropriately (e.g. in the case of SLS the setpoint values should be reduced, while, in the case of SS1, the controller enable should be retracted).
- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.5 Control of a clamping unit

The safety function (e.g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request. The safety request is made over 2 channels via input device S1 and results in 2-channel switch-off of the power stage of the motor controller. The clamping unit is activated and monitored at the same time.

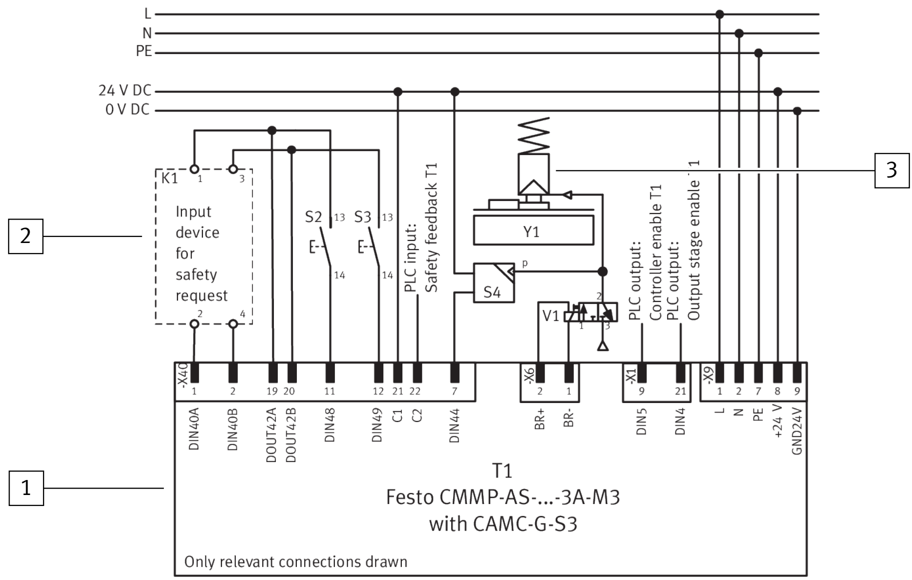


Fig. 75: Sample circuit, clamping unit

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device for safety request
3	V1/Y1: valve and clamping unit S4: pressure switch for monitoring control of the clamping unit

Information on the sample circuit:

- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the input devices for the safety request S1, for the acknowledgement button S2 and for the start button S3.
- The safety functions are terminated by pressing the start button S3.

– The feedback contact C1, C2 should be polled via the controller. If a security requirement has been made, the controller enable should be cancelled.
– If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
– The clamping unit is controlled via the BR+/BR- output of the motor controller (T1) and monitored via switch S4 of the safety module CAMC-G-S3. (Note: this uses active pressure switches; detection of shorts across contacts is not possible with DOUT42!). The indirect monitoring shown requires a regular function test of the clamping unit.
– Monitoring of the clamping unit checks only actuation and not whether the friction value of the clamping unit is high enough for it to be able to continue to function properly.
– The sample circuit has a monitored single-channel structure in the clamping unit, which is suitable up to category 2 with a function test of the clamping unit.
– Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.6 Control of a 2-channel clamping unit

The safety function (e.g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request. The safety request is made over 2 channels via input device S1 and results in 2-channel switch-off of the power stage of the motor controller. The clamping units are activated and monitored at the same time.

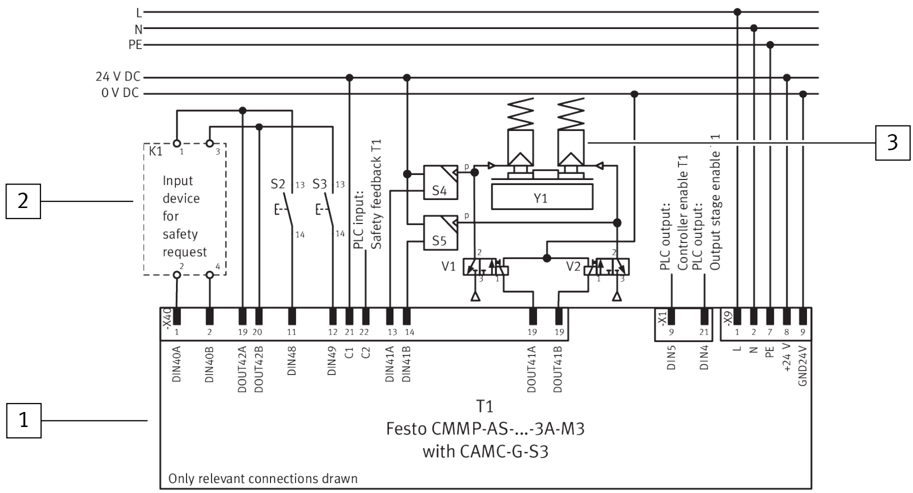


Fig. 76: 2-channel fixed sample circuit

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device for safety request
3	V1/V2/Y1: valves and two-channel clamping unit S4/S5: pressure switch to monitor the control of the clamping unit

Information on the sample circuit:

- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the input devices for the safety request S1, for the acknowledgement button S2 and for the start button S3.
- The safety functions are terminated by pressing the start button S3.
- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The clamping units are controlled via two-channel output DOUT41A/DOUT41B of the safety module.
- If the valves for the clamping units request more power than DOUT41 can supply, a suitable relay (with forced contacts and feedback) must be connected between them. Alternatively, check whether the BR+/BR- output of motor controller T1 can be used.
- Functioning of the clamping units is monitored by the safety module using pressure switches S4 and S5 (note: active pressure switches are used for this, detection of shorts across contacts is not possible with DOUT41!). The indirect monitoring shown requires a regular function test of the clamping unit.
- Monitoring of the clamping unit checks only actuation and not whether the friction value of the clamping unit is high enough for it to be able to continue to function properly.
- The sample circuit has a 2-channel structure in the clamping unit, which is suitable up to category 2 with a function test of the clamping unit.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

4.3.7 Connection of encoders for dynamic safety functions

Monitoring with encoders is implemented with push-in connectors [X2A], [X2B] and [X10]. Speed and standstill monitoring can be carried out, depending on the available incremental or absolute measured values.
In “Automatic” operating mode, the safety function (e.g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request.
The safety function “Safely Limited Speed (SLS)” is requested using the mode selector switch S6 in the “Manual” position.
The safety request is made over 2 channels via input device S1 and results in 2-channel switch-off of the power stage of the motor controller. If the power stage is switched off, it is output by the potential-free contact C1/C2 of the motor controller.

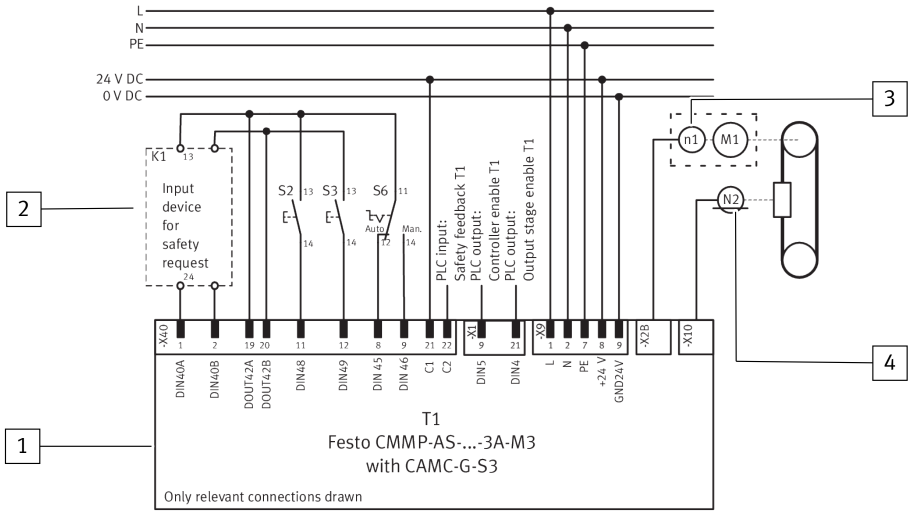


Fig. 77: Sample circuit of an encoder for dynamic safety functions

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device for safety request
3	n1: encoder in servo motor to X2B
4	n2: encoder to X10

Information on the sample circuit:

- The encoders must be suitable for safety-oriented applications.
- Encoders with purely incremental signals can be used to monitor speed safely (SLS, SSR, SS1, etc.). Such encoders can also be used for standstill-position monitoring with SS2 and SOS.
- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the input devices for the safety request S1, for the acknowledgement button S2, for the start button S3 and for the mode selector switch S6.
- The safety functions are terminated by pressing the start button S3.
- The feedback contact C1, C2 should be polled via the controller. If a security requirement has been made, the controller enable should be cancelled.

4.3.8 Control of a 2-channel valve control block with safety functions

The safety function (e.g. for the motor controller STO – Safe Torque Off or SS1 – Safe Stop 1; for the valve control block Safe Venting or Safe Reversing) is triggered by an input device which makes a safety request for the motor controller and the control block with safety function. The safety request is made over 2 channels via the input device S1 and results in a 2-channel switch-off of the power stage of the motor controller and the control block.

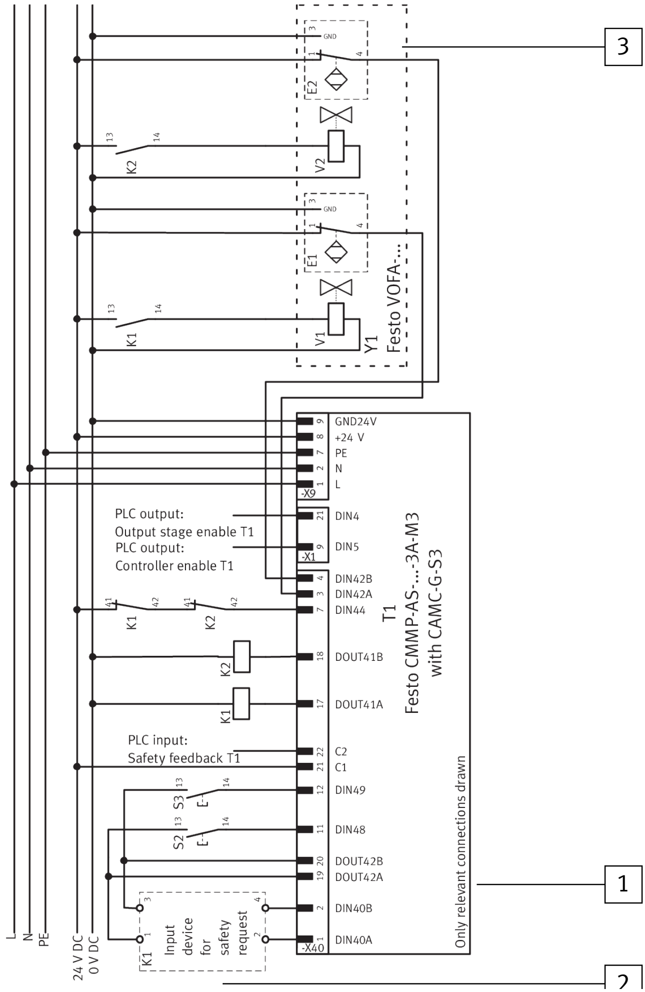


Fig. 78: Sample circuit of a 2-channel control block with safety functions

1	T1: motor controller with safety module (only relevant connections shown)
2	S1: input device for safety request
3	Y1: two-channel control block

Information on the sample circuit:

- The safety module CAMC-G-S3 detects shorts across contacts in the input circuit for the switches S1, for the acknowledgement button S2 and for the start button S3.
- The safety functions are terminated by pressing the start button S3.

- If the safety module CAMC-G-S3 detects a violation of a safety condition or an error is pending, e.g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement button S2.
- The inputs DIN42A/B must be configured to monitor the switching on and off of control block V1. Protective contacts 41/42 of contactors K1 and K2 cannot be connected in series, because this is not possible with the inductive proximity sensors in use.
- The feedback contact C1, C2 should be polled via the controller. If a security requirement has been made, the controller enable should be cancelled.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required depending on the scope of the application and the safety concept of the machine.

5 Commissioning

ⓘ

This chapter describes the commissioning of the safety module. You can find information on commissioning the motor controller here:

➔ Description of hardware “Mounting and installation” GDCP-CMMP-M3-HW-...

➔ Help for FCT plug-in CMMP-AS.

NOTICE

Commissioning in the sense of this document does not mean the first intended use by the end customer, but commissioning by the machine manufacturer when setting up the machine.

NOTICE

Loss of the safety function!

Lack of safety functions can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuator technology.

- Operate the safety module only:
  - if it is installed,
  - after the safety module has been completely parameterised,
  - if all protective measures, including the safety function, have been installed and the function tested.
- Validate the safety function to complete commissioning ➔ 5.8 Function test, validation.

ⓘ

Incorrect wiring, use of an incorrect safety module or external components that were not selected according to the category will result in failure of the safety function.

– Carry out a risk assessment for your application and select the circuitry and components accordingly.

– Observe the examples ➔ 4.3 Sample circuits.

5.1 Prior to commissioning

Carry out the following steps in preparation for commissioning:

1. Make sure that the safety module is correctly mounted ➔ 4.1 Mounting/removal.
2. Check the electrical installation (connecting cables, contact assignment, ➔ 4.2 Electrical installation). All PE conductors connected?

5.2 DIL switch setting

The safety module has DIL switches for activation and control of the bus configuration. The DIL switches have the identical function for all modules in the Ext3 slot and it depends on the bus interface used.

Set the DIL switches as described in the hardware description “Mounting and installation” GDCP-CMMP-M3-HW-... or the corresponding bus-specific documentation ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M3.

5.3 Notes on parameterisation with the FCT plug-in CMMP-AS

The motor controller must be completely parameterised using the FCT plug-in CMMP-AS prior to parameterisation of the safety module using the SafetyTool.
The following sections provide some information on what to look for when working with the safety module.

You can find additional information on commissioning with the FCT in the Help file of the CMMP-AS plug-in or, if necessary, in the description of the functions for the CMMP-AS-...-M3, GDCP-CMMP-M3-FW-...

5.3.1 Setting the configuration

Carry out the project engineering of the safety module in the FCT, described on the “Configuration” screen for the CMMP-AS plug-in, as follows:

– drive configuration not available: press “Create a new drive configuration” button.
– drive configuration available: press “Change” button.
– Then select the safety module used for the Ext3 option slot in the “Create drive configuration” or “Edit drive configuration” window.

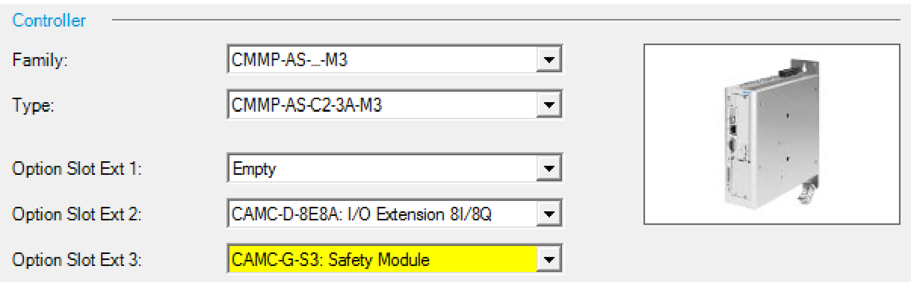


Fig. 79: FCT plug-in CMMP-AS: “Create/edit drive configuration”

As you continue to parameterise the motor controller, you must explicitly accept the safety module in online mode ➔ 5.3 Notes on parameterisation with the FCT plug-in CMMP-AS.

5.3.2 Setting the encoder configuration

Safe monitoring of speed, e.g. for SLS, and position, e.g. for SOS, requires corresponding sensors for position detection.

Information on the required encoders ➔ 3.2 Function and application. Note the permissible encoder combinations ➔ Tab. 11 Permissible combinations of position encoders.

Specify the first encoder by selecting the motor during drive configuration. Information is displayed on the “Motor” screen in the “Angle encoder” tab.
Select the interface of the second encoder on the “Measuring systems” screen, “General” tab under “Monitoring”.
You must then configure the encoder in the appropriate tab of the selected interface.

5.3.3 Specifying the units of measurement (optional)

The units of measurement in the FCT plug-in CMMP-AS are defined by the following settings:
- selection of the axis – linear or rotational units.
- optional: set the units of measurement (Menu [Component] [Units of measurement]) – metric/imperial units (mm/inches), decimal places.

5.3.4 Accepting the safety module

Functional safety requires that engineering changes can be traced. To guarantee this, the specifications for module type, serial number and revision are stored in the safety module. This data is read out in the motor controller and permanently saved when the module is accepted. This makes it possible to detect an engineering change in the components.
Information on the versions is displayed on the “Device information” screen in online mode.

“Device Information” screen	
Controller	
Controller type	Type of the motor controller (basic unit).
Hardware version	Hardware version of the motor controller.
Firmware version	Firmware version of the motor controller.
Serial number	Serial number of the motor controller.
Option slot Ext3	
Module type	Type of the module: : CAMC-G-S3: safety module.
Overall revision	Overall revision of the safety module, e.g. 1.0.
Serial number	Serial number of the safety module, e.g. 1212820487.

Tab. 106: “Controller” screen – information on the versions

Accept safety module

If an invalid change is detected, e.g. a module replacement, a non-acknowledgeable error is triggered. To be able to restart the application with the motor controller, the change must be “projected”. This means that the change is explicitly accepted or confirmed. With reference to the safety or switch modules, these traceable changes involve a module replacement.

ⓘ

The following rules apply to the module replacement:
- It is always possible to replace a switch module with another switch module.
- Replacing a CAMC-G-S1 module with another CAMC-G-S1 does not normally need confirmation. Exception: the version check in the basic unit shows that the modules are incompatible - error message 51-3 - meaning that the module change must be confirmed.
- When a module type is replaced with a different type – error message 51-2 – the module replacement must always be confirmed.
- When a CAMC-G-S3 module is replaced with a CAMC-G-S3 – error message 51-6 – the module replacement must also always be confirmed.

You have two options for confirming the module replacement:
- When activating online mode, the module change is detected and a confirmation dialogue is automatically displayed.
- If you have not confirmed the module change directly when activating online mode, you can open the confirmation dialogue at any time using the menu command [Component] [Online] [Confirm module change].

The "Confirm module change" dialogue displays the module type, overall revision (CAMC-G-S3) or revision and version (CAMC-G-S1, CAMC-DS-M1) and the serial numbers of the previous module and also of the currently installed module.
- Selecting “Yes” confirms the module change, the parameters are saved permanently in the basic unit and it is restarted.

5.3.5 Status indicator

Information on the status of the safety module is displayed in the project output section of the “Safety functions” tab in online mode.

Project output – online tab: "CAMC-G-S3: Safety module”			
Frame “CAMC-G-S3: status signals”			
	Display of the status of the safety module		Status[1)]
	Green	Power stage enable approval	VOUT_PS_EN = 1
	Red	Warning	VOUT_WARN = 1
	Red	Safety condition violated	VOUT_SCV = 1
	Red	Errors	VOUT_ERROR = 1
	Yellow	Safety function reached	VOUT_SSR = 1
	Yellow	Safe state requested	VOUT_SFR = 1
	Green	Service status	VOUT_SERVICE = 1
	Green	Ready for operation	VOUT_READY = 1
“CAMC-G-S3: Safety functions” frame			
	Safety functions STO SS1 SS2 SOS SBC USF0 USF1 USF2 USF3		Status[2)]

Project output – online tab: "CAMC-G-S3: Safety module”			
	Green	Normal operation	VOUT_xxx_SFR = 0
	Yellow	Safe state reached	VOUT_xxx_SFR = 1
“CAMC-G-S3: Digital I/O” frame			
	DINxx, DOUTxx, C1/C2 status (GND/+24V without function)		
	Green	Input= 1	
	Yellow	Output = 1 or relay closed	
	Grey	Input or output = 0 or relay open	

1) Status of the safety module
2) Status of the safety function

Tab. 107: Displays in the online tab "CAMC-G-S3: safety module“

Status of the safety module ➔ Further information.
Status of the safety function ➔ 3.5 Safety functions.

5.3.6 Display permanent diagnostic memory of the motor controller

To display or save the permanent diagnostic memory, activate the online “Diagnostics” tab in the FCT plug-in.
If there is an active online connection, you should then activate the “Permanent” tab. “Read” reads the number of entries of the permanent diagnostic memory specified under “Entries” and displays them in chronological order, newest first.
Selecting “All entries” reads the complete permanent diagnostic memory. This can take several minutes.
The content of the diagnostic memory is displayed in the form of a table:

Column	Explanation
No.	Sequence number of the entry.
Fault no.	Error, warning or event number ➔ 6.5.3 Diagnostic messages.
Fault description	Name of the entry, error text.
Time stamp	Time of the diagnostic event in the ‹hh›:‹mm›:‹ss› format (operating hour counter, duty cycle of the logic supply).
Constant	Additional information for Festo service personnel
Free parameter	Additional information for Festo service personnel
Type	Type of entry (error, warning, log entry).

Tab. 108: Display of the permanent diagnostic memory

The following table shows some entries as examples:

No.	Fault no.	Fault description	Time stamp	Constant	Free parameter	Type
1	00-21	Log entry of the safety module	580:15:03	0x0000	Error acknowledged, source: 0x01, error-free	Errors
2	00-8	Controller switched on	580:15:00	0x0000	0x0000	Errors
3	00-12	Module replacement: current module	580:15:22	0x4830	CAMC-G-S3, S/N: 1212820487, HW rev.: 1.0, SW rev.: 1.0	Errors
4	00-11	Module replacement: previous module	580:15:22	0x48FF	CAMC-DS-M1, S/N: 3781764777, HW rev.: 0.1, SW rev.: 0.1	Errors
...	...	...	...	...	...	...

Tab. 109: Example of entries in the diagnostic memory

ⓘ

Additional information on the entries in the diagnostic memory:

- Entries are made chronologically, meaning that the top entry is the most recent entry.
- Minor deviations with the time stamp are possible after Power OFF/ON, as the motor controller only saves the time stamp to non-volatile memory once every minute.

“Copy” and “Export” can be used to transfer the contents in csv format with ';' separators to the Windows clipboard or a file.
The value of the operating hours counter of the motor controller at the time of the log entry is displayed in the “Time stamp” column.

ⓘ

The current value of the operating hours counter of the motor controller is displayed above the list as the “Current system time”

5.4 Basic principles for parameterisation of the safety module

5.4.1 Factory setting

To simplify parameterisation, some functions are activated and standard values are preset in the delivery status or after the reset to factory settings.
The following table provides an overview of the most important settings.

Panel	Factory setting		Assignment
Digital inputs			
DIN40	Sensor type:	Emergency stop switching device	STO and SBC request

Panel	Factory setting		Assignment
DIN40	Operating mode	Equivalent	STO and SBC request
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN41	Sensor type:	Not defined	Not used
	Operating mode	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN42	Sensor type:	Not defined	Not used
	Operating mode	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN43	Sensor type:	Not defined	Not used
	Operating mode	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN44	Sensor type:	Brake feedback	Not used
	Source for test pulse:	None	
DIN45	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN46	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN47	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN48	Sensor type:	Error acknowledgement	Request for error acknowledgement
	Source for test pulse:	None	
DIN49	Sensor type:	Terminate safety function	Rising edge: terminate STO, SS1 and SBC
	Source for test pulse:	None	
Safety functions			
STO	Request:	DIN40	–
	Automatic restart:	no	
	Automatic activation of SBC:	Yes	

Panel	Factory setting		Assignment
STO	Terminate request:	DIN49, rising edge	–
SS1	Request:	no allocation	Not used
	Quick stop ramp:	Yes	
	Automatic restart:	no	
	Automatic activation of SBC:	no	
	Terminate request:	DIN49, rising edge	
SS2	not activated		–
SOS	not activated		–
USF...	not activated		–
SBC	Request:	DIN40	–
	Feedback, holding brake:	no	
	Automatic restart:	no	
	Deactivate 10 day cyclical test	no	
	Terminate request:	DIN49, rising edge	
Logic functions			
Mode selector switch	Not activated		–
Two-hand operator unit	Not activated		–
ALF...	Not activated		–
Logic error acknowledgement			
Logic error acknowl-edgement	Request:	DIN48	–
Digital outputs			
DOUT40	Request:	no allocation	–
	Operating mode	Equivalent	–
DOUT41	Request:	no allocation	–
	Operating mode	Equivalent	–
DOUT42	Request:	No allocation	–
	Operating mode	Permanently switched on	–

Panel	Factory setting		Assignment
Internal brake	Request:	SBC requested	–
	Operating mode	Equivalent	–
Signal contact C1/C2	Request:	Safe state reached and no safety condition violated	–
Error management			
Error management	Safety condition violated: various others	SBC + STO	Observe and check additional settings.
	Other serious errors:	SBC + STO + outputs = 0	

Tab. 110: Factory setting

5.4.2 Delivery status

The safety module is received from the factory in the so-called “delivery status”.
This is indicated by the green and red flashing LED as well as corresponding status messages → Further information.
Special features of the delivery status in comparison to the factory settings:

- The safety module is “validated as a whole” with the parameterisation of the factory setting and is thus functional. The motor controller can be commissioned, and the power stage and controller enable can be set.
- All error messages caused by differences in parameterisation of the basic unit and safety module are suppressed.
  Hence, you can perform basic commissioning of the motor controller independently of complex safety-engineering peripherals. For example, the safety module is parameterised to “Resolver” in the delivery status. If other encoders are used, the motor controller could not be commissioned without suppressing the error message from the safety module.

ℹ

The user cannot restore the delivery status. Only the factory settings can be restored.

5.4.3 FCT plug-in CMMP-AS and SafetyTool

Basic commissioning of the motor controller is performed with the corresponding CMMS-AS plug-in for the Festo Configuration Tool (FCT).
It contains the specification of the hardware configuration, such as the connected motor, the measuring systems, the axis and the modules and interfaces assembled in the optional slots.
The safety module is then parameterised with special software, the SafetyTool. The SafetyTool is opened from the FCT CMMP-AS plug-in.

NOTICE

Before starting the SafetyTool, you must load and back up the hardware configuration and any specified units of measurement to the motor controller → 5.3 Notes on parameterisation with the FCT plug-in CMMP-AS.
This is necessary for data migration to the SafetyTool.

5.5 Safe parameterisation with the SafetyTool

5.5.1 Program start

When the FCT CMMP-AS plug-in is active, start the SafetyTool with the “Start SafetyTool” button.

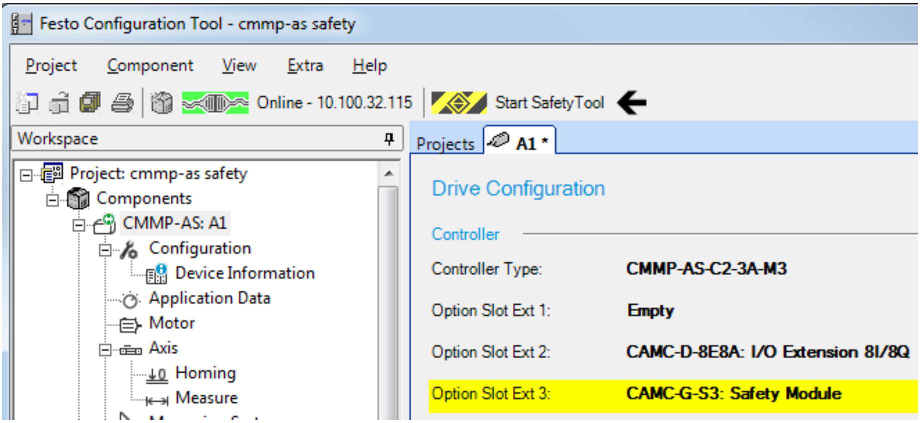


Fig. 80: Start SafetyTool

5.5.2 Selection of the session types - configuration wizard

In both session types (online/offline) the SafetyTool is an offline software tool as defined by EN 61508 for installation and commissioning (Phase 12). In addition, the SafetyTool provides support during validation (Phase 13), during which a corresponding record can be created using the parameterised functions of the safety module. It is not possible to change parameters during active operation. When an online parameterisation session is started, the safety module switches to the safe status (STO + SBC). In all cases there is a duty on the machine manufacturer or machine operator to validate the functions.

The SafetyTool supports 2 session types:

- **Online: work on the safety module.**
  The SafetyTool communicates with the target system (the safety module).
  You can observe the safety module and read the parameters, you can change specific parameters or transfer a complete safe parameter set.
  Before you change the parameters, the safety module switches to the “Safe basic status”. The parameters must be validated before the safety module leaves the “Safe basic status”. Changed parameters do not take effect immediately and do not become active until after full validation and restart.
- **Offline: work on local file.**The SafetyTool does not communicate with the target system (the safety module).
  However, you can create and save a preliminary parameterisation for the safety module.

ⓘ

If the SafetyTool does not permit an online session even though there is a communication connection to the device, the following message appears:

- A parameterisation session is already opened on the safety module!
  Only offline parameterisation sessions are possible.
  Alternative: terminate the other session.
  After the connection is interrupted: restart device.

When you start the program, the SafetyTool supports you by displaying the “Configuration Wizard for safe parameterisation”. Select the desired session variant.

Session type	Session variant	Description
Online ➔ 5.5 Safe parameterisation with the SafetyTool	Start new parameterisation	Opens a new project with the standard parameters from the safety module.
	Start new parameterisation with existing project[1)]	Opens a new project based on a locally saved project file.
	Display parameterisation	Displays the parameterisation in the safety module (read-only!).
	Change existing parameterisation	Loads the parameterisation in the safety module for editing.
	Transfer safe parameter set	Transfers a previously saved safe parameter set to the safety module.
Offline ➔ 5.5 Safe parameterisation with the SafetyTool	Create a new project	Opens a new project with the standard settings of the SafetyTool.
	Generate a new project from safe parameter set	Opens a new project based on a saved safe parameter set.
	Open existing project[1)]	Opens a locally saved project file.

1) Only possible if the axis type (linear/rotating) of the SafetyTool project file agrees with the current FCT project.

Tab. 111: Selection of session variants - configuration wizard

5.5.3 Online parameterisation

If the online connection to the motor controller is active in the FCT plug-in, the functions for online parameterisation are available in the SafetyTool.

ⓘ

Make sure that the data in the motor controller match the project data (“Download”) and have been backed up (“Backup”) before starting the SafetyTool. Otherwise the basic information after the basic unit is restarted may differ from the basic information that had been used.

The parameters and the parameter set can only be validated during online parameterisation. It is always necessary to state a user name and to enter a password for the online parameterisation functions:

ⓘ

The factory setting for the password is: **SAFETY**
Assign your own password for your project to protect the safety parameters from unintentional changes (Menu [Tools] [Change password] ➔ 5.7 Special functions of the SafetyTool.

When it is started, the SafetyTool compares its database with the data of the basic unit and with that of the safety module. Depending on the selected session variant, the parameters must be uploaded from the safety module for this.
The operation is indicated by a progress bar. The length of time may vary, depending on the session variant and the speed of the communication connection.

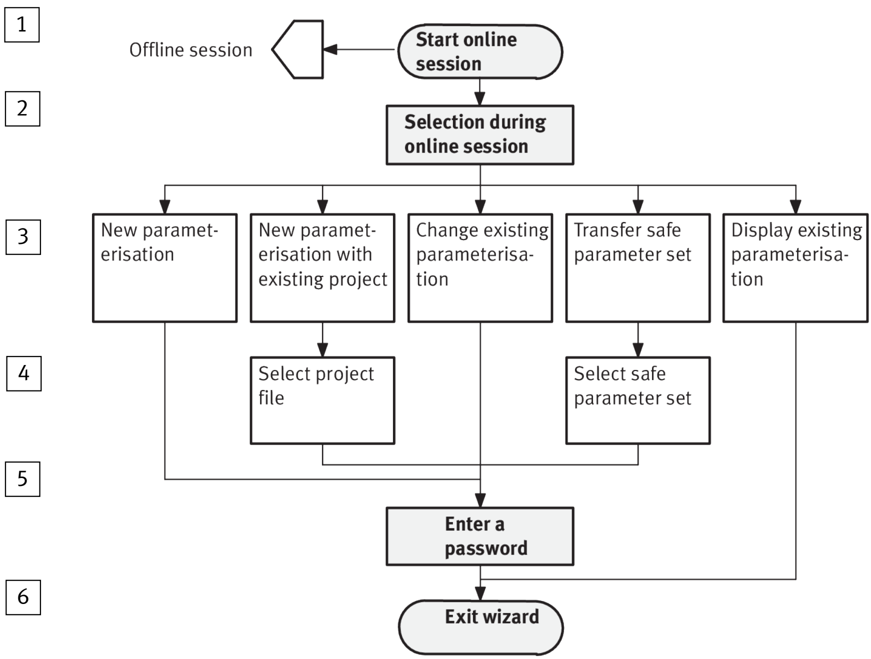


Fig. 81: Steps to selection of the online session variant

1	Start the wizard with the option of selecting offline mode
2	Selection of the online session variant
3	Note on the specific session variant
4	Selection of a project file/parameter set
5	Personal identification
6	Start/terminate wizard

A parameterisation session can also be started with the drive switched on. When the parameterisation session has been started, the drive is switched off by the safety module (no power stage enable).
All digital outputs are switched off during a running parameterisation session.

The SafetyTool is automatically terminated when the parameterisation session is closed. All parameters must have the status “validated” on termination. Otherwise all changes will be lost and the safety module starts with the most recently saved and validated parameter set.

5.5.4 Offline parameterisation

You can do this initially completely offline in preparation for parameterisation.
However, to commission the safety module correctly, you must validate the parameters online and transfer the validated parameters to the safety module.

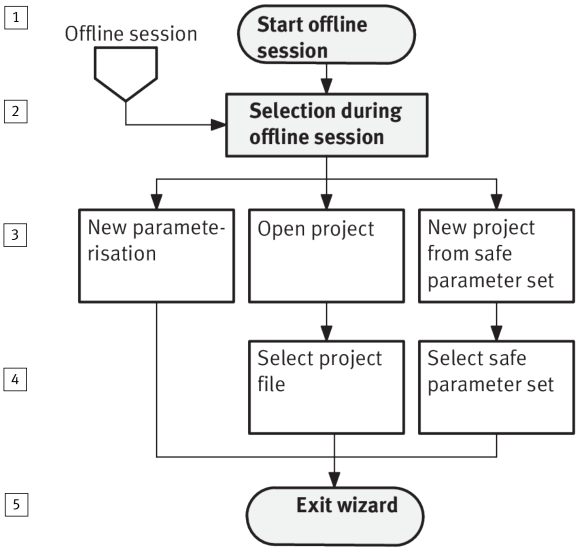


Fig. 82: Steps for selection of the offline session variant

1	Start the wizard in offline mode
2	Selection of the offline session variant
3	Note on the specific session variant
4	Selection of a project file/parameter set
5	Exit wizard.

5.5.5 Basic rules for parameterisation with the SafetyTool

Common properties of the parameterisation operations

Parameterisation always consists of the following steps:

1. Open a parameterisation session.
2. Change individual parameters.
3. Validate individual parameters or the entire parameter set (generation of a validation code).
4. Permanently save the parameter set in the safety module; entire parameter set is considered validated. After further parameter changes, steps 3 and 4 must be run again.
5. Close the parameterisation session, “activate” the parameter set.
6. Restart the safety module.

Opening a parameterisation session

When a parameterisation session is opened, the safety module goes into the safe basic state and the drive is switched off (power stage switched off, safe brake control not energised, DOUT4x switched off at the safety module).
The VOUT_SERVICE status is active during a parameterisation session.
Switch-on and switch-off of the drive is only possible after the parameterisation session is closed and only when the parameter set has been validated.
The opening of a parameterisation session is saved in the permanent diagnostic memory.
During the active parameterisation session, the message “FSPArA” is output on the 7-segment display of the motor controller (providing that no error is pending), ➔ 6.4 Diagnostics and fault clearance.
Pressing “Start identification” in the Start Wizard allows you to output the message “HELLO...”.
The message is there for the identification of the motor controller if multiple motor controllers are connected to the parameterisation PC.
Only one parameterisation session per safety module can be opened at one time.
If a parameterisation session is already opened, the safety module will reject further requests until the current parameterisation session is closed.
This prevents a safety module from being parameterised simultaneously via several PCs with the SafetyTool. The SafetyTool only allows parameters to be changed after a parameterisation session has been opened.

User ID and password

When a parameterisation session is opened, a user ID (user name) and a password must be entered.
The user ID and password both consist of ASCII characters (letters, numbers and umlauts, no special characters) and have a maximum length of 8 characters.
In delivery status or after a reset to the factory setting, the password is “SAFETY”.

ⓘ

The password should be changed immediately after commissioning.
The new password and the password of the factory setting should only be known to the “Person responsible for functional safety on the machine”.
The changed password is saved in the safety module and replaces the previously valid password; it applies for all users. The password is not saved in a parameter file. It cannot be read out of the safety module.

Data migration from the motor controller

To compare the relevant parameters in the safety module with those of the motor controller (basic unit), during an online session variant data is in all cases first migrated from the basic unit.

ⓘ

When you exit the SafetyTool, any data loaded from the FCT plug-in to the motor controller could be lost during a restart. To prevent this, always make sure that the data is backed up when you start the SafetyTool with an active online connection. This is polled by a dialogue.

When transferring data to the SafetyTool, in addition to the units of measurement, the parameters of the connected rotary encoders are also migrated and are mapped to the safety parameters for encoder 1 and encoder 2.

Principle of “sending and validating”

All parameters changed in the SafetyTool must be sent to the safety module, checked and validated. This applies to the data migrated from the motor controller (basic unit) as well as to the product terms for requesting safety functions or other mappings.

The sequence is identical on all parameter screens:

- Step 1: enable parameters for editing using the “Enable editing” button.
- Step 2: manipulate or change parameters. This step checks the value range.
- Step 3: transmit the changed parameters to the safety module using the “Send” button.
- Step 4: finally, the transmitted parameters must be validated.

The setpoint values (from the SafetyTool) and the actual values (from the safety module) are displayed for validation. Deviating values are marked by a symbol:

Symbol	Status
≠	The setpoint and actual value deviate from each another. This parameter must be compared.
≈	The setpoint and actual value deviate slightly from each another. Certain values, such as times, are rounded to a multiple of the basic unit in the safety module. This is why the setpoint and actual value may differ as a result of the rounding. Such a value can be validated!

Tab. 112: Display of deviation in setpoint and actual values

For validation after the check, tick the appropriate checkbox in the “Checked” column and validate the selected parameters with the “Validate” button. Only then are the parameters validly transferred to the safety module.

The “Valid” column displays whether the actual values of the parameters are valid, i.e. validated.

Symbol	Status
	Parameter is not yet validated.
	Parameter is validated.

Tab. 113: Display of the validity of the parameters

Plausibility check

The SafetyTool runs various plausibility checks during the parameterisation session.

This ranges from monitoring the range limits to logical testing of the rotational speed limits (upper rotational speed limit must not be less than the minimum rotational speed, lower limits must be less than upper limits, etc.). The plausibility check can also be run manually ➔ 5.7 Special functions of the SafetyTool.

Enabling and permanently saving in the device

After parameters have been changed, they must be saved permanently in the safety module. In addition, consistency of the parameter set is secured by a unique full validation code. The non-volatile saving and calculation of the validation code is implemented using the appropriate button on the “Finish” screen.

If a parameterisation session was active in the SafetyTool with write access, then a restart is carried out automatically when the SafetyTool is exited.

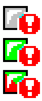
Save parameterised intermediate states (without full validation):
The function “Parameterisation/Save parameters permanently in the safety module” saves the parameters, although they are not “fully validated”. The safety module detects this status on restarting and switches to the safe basic status.

Standard and expert parameters
Some of the parameters are indicated as “Expert parameters” or are displayed in their own “Expert parameters” tab.

NOTICE

Expert parameters do not normally need to be changed. Changes may only be required if absolutely necessary.

Status of the parameter groups
Each screen in the SafetyTool contains a so-called parameter group. The status of this parameter group is displayed by the LED symbol in the navigation tree during an online session:

Symbol	Status
	The parameters are not yet validated (all stages of the parameters before validation).
	All the parameters of this screen are validated. These parameters are identical to the parameters in the device. Only when all the parameters on all the screens have been validated is full validation and permanent saving of the parameters in the safety module possible.
	At least one parameter deviates from the parameters in the device. The differences must be resolved.
	There is a faulty value in an entry or selection field. The error must be corrected.

Tab. 114: Display of the status of the parameter groups

5.5.6 Behaviour in case of invalid parameterisation

If there is not a valid parameter set in the safety module, the power stage of the motor controller is blocked and all digital outputs are voltage-free. The safety module must be parameterised again with the SafetyTool.

5.5.7 Parameter set version

When the revision of the safety module changes, that does not necessarily mean that a new version of the parameter set is needed (change in the firmware version or hardware version leads to a new full revision of the safety module).
The parameter set version monitors the compatibility between the SafetyTool and the safety module.

New parameter set in old firmware
Parameter sets generated with a firmware version that is more recent than that in the safety module are not accepted. An error message “Incompatible parameter set” is generated.

Old parameter set in new firmware
The parameters are loaded first. The version number of the parameter set is used to check how to proceed with the parameter set.
If the version of the parameter set is not compatible, then validation via the validation code is rejected.
If the version of the parameter set is compatible, for example, parameters that the set does not have are set to values which ensure that the safety module behaves in the same way as with an older revision.

ⓘ

The firmware can only be updated by the manufacturer.

5.6 Sequence of parameterisation with the SafetyTool (example)

This section describes a complete parameterisation sequence using an example. However, the basic steps can be applied to other applications. The following is required for the sequence:
- Basic commissioning of the motor controller has been implemented with the FCT plug-in and an online connection to the FCT is active.
- The safety module is in the delivery status or has the factory setting➔ 5.7 Special functions of the SafetyTool.

ⓘ

You can find a complete description of the interface and the functions of the SafetyTool in the SafetyTool help.
Information on some special functions ➔ 5.7 Special functions of the SafetyTool.

Sample application:
Machine with:
1. Emergency stop switch (DIN40), which, when actuated, should always trigger SS1 type b) and then SBC.
2. Light curtain (DIN41) as protection against manipulation in the machine. In normal operation, SS1 is also triggered, whilst, in Setup mode, SS2 is requested.
3. Enabling button (DIN42), for traversing the axis with SLS in setup mode.
4. Mode selector switch for normal operation and Setup mode (DIN45, DIN46).
5. Monitoring of switches with test pulses from DOUT42.
6. Acknowledge error (DIN48).
7. Terminating the safety function (DIN49) rising edge, SS1 is terminated via an external control signal.
8. The switch-over between SS2 and SLS takes place on automatic restart.

In the example the following parameterisation is carried out:
- **After switching on:**
  STO with automatic SBC activation is requested.
- **Normal operation:**

SS1 should be triggered with emergency stop actuation or entry into the light curtain with subsequent SBC, termination of the safety function only via DIN49.

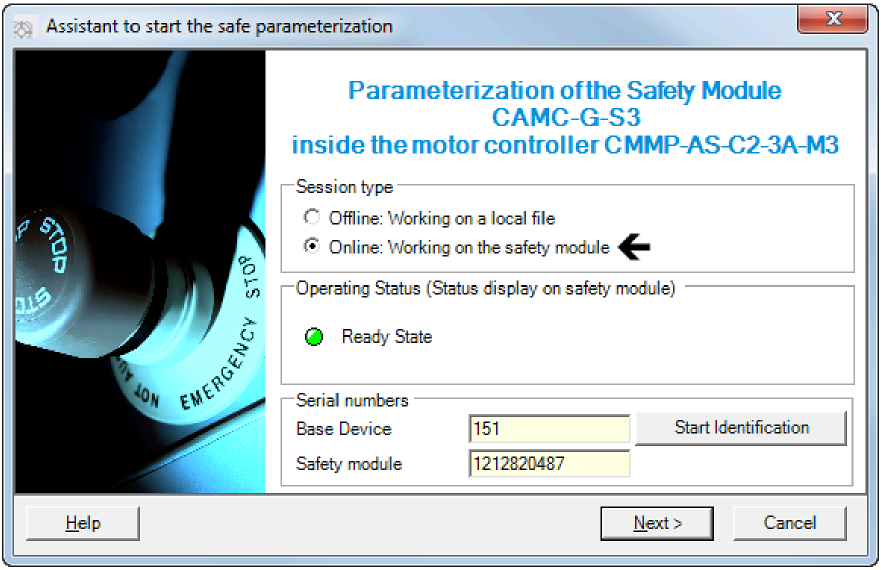
- **Setup mode:**
  - SLS is always requested when Setup mode is selected.
  - SLS can only be terminated if,
    a) the mode selector switch is reset to normal operation and
    b) the light barrier is no longer interrupted and
    c) restart is actuated.
  - SS2 is also triggered when the light curtain is interrupted.
  - Termination of SS2 only via DIN49 and when the light curtain has been exited, or via the enabling button DIN42.
  - When the enabling button is actuated there should be a switch from SS2 to SLS.

ℹ

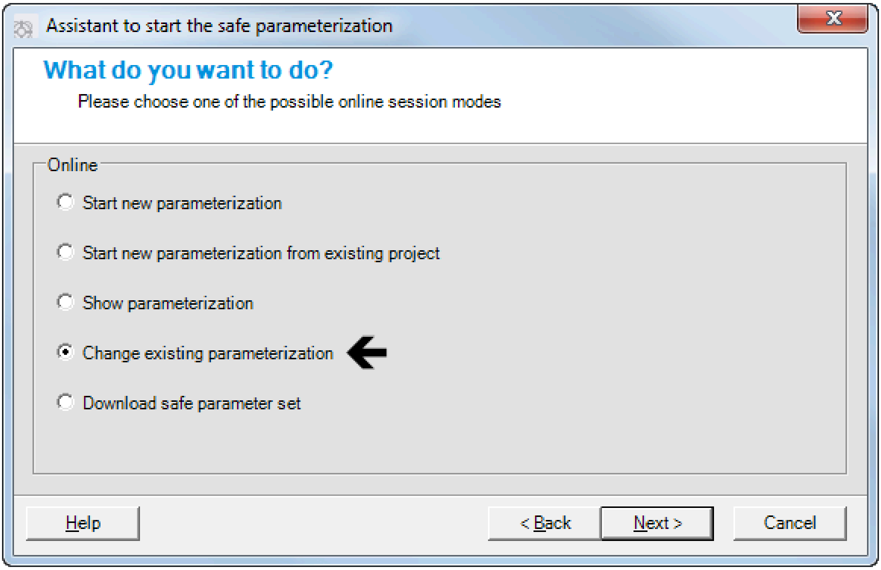
You must determine the circuitry and parameterisation required for your application as part of your risk assessment.

5.6.1 Selection of the session variant in the wizard

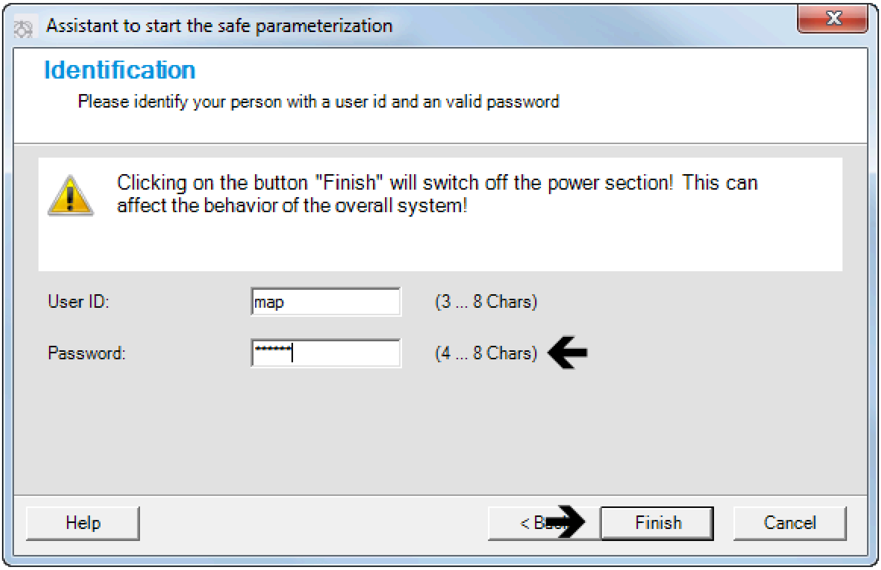
1. Start the SafetyTool with the “Start SafetyTool” button ➔ 5.5.1 Program start.
2. In the wizard for starting safe parameterisation select the session type “Online ...” and confirm with “Next”.



3. Select the session variant “Change existing parameterisation” and confirm with “Next”.
   After this, a note on the session variant is displayed which you should read and then confirm with “Next”.



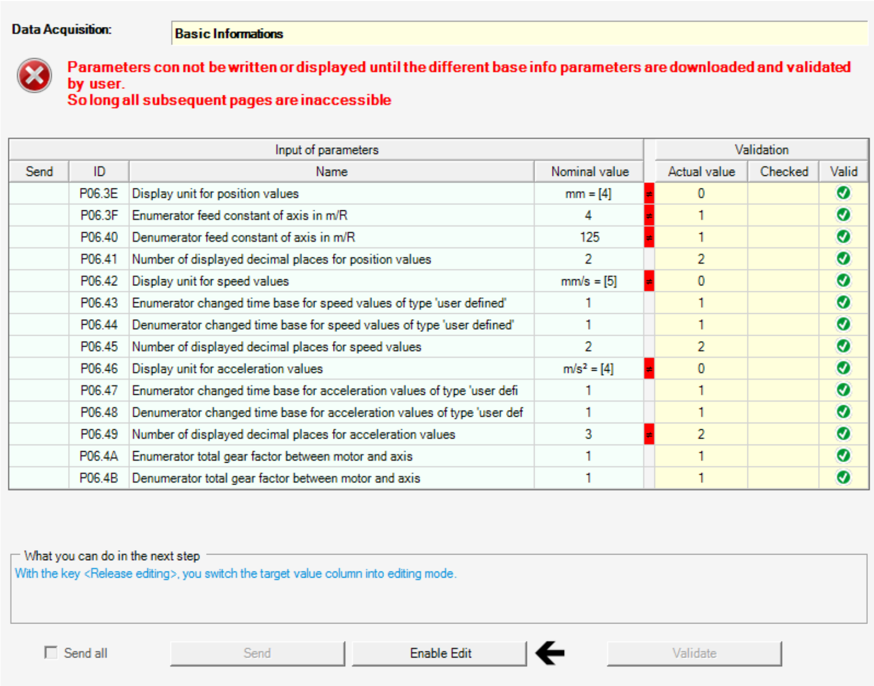
4. A user ID and password are required in order to write parameters. In delivery status or after a reset to the factory setting the password is “SAFETY”.
   Exit the wizard with “Finish”.



5.6.2 Data migration and comparison

1. The basic information of the factory setting usually deviates from the current basic unit parameterisation. This is shown in a dialogue, which you should confirm with “OK”. If this is not the case, you can continue with item 3.

2. The deviating values are displayed in red on the Basic information screen and must first be synchronised.



Input of parameters					Validation		
Send	ID	Name	Nominal value		Actual value	Checked	Valid
	P06.3E	Display unit for position values	mm = [4]		0		
	P06.3F	Enumerator feed constant of axis in m/R	4		1		
	P06.40	Denumerator feed constant of axis in m/R	125		1		
	P06.41	Number of displayed decimal places for position values	2		2		
	P06.42	Display unit for speed values	mm/s = [5]		0		
	P06.43	Enumerator changed time base for speed values of type 'user defined'	1		1		
	P06.44	Denumerator changed time base for speed values of type 'user defined'	1		1		
	P06.45	Number of displayed decimal places for speed values	2		2		
	P06.46	Display unit for acceleration values	m/s² = [4]		0		
	P06.47	Enumerator changed time base for acceleration values of type 'user defi	1		1		
	P06.48	Denumerator changed time base for acceleration values of type 'user def	1		1		
	P06.49	Number of displayed decimal places for acceleration values	3		2		
	P06.4A	Enumerator total gear factor between motor and axis	1		1		
	P06.4B	Denumerator total gear factor between motor and axis	1		1		

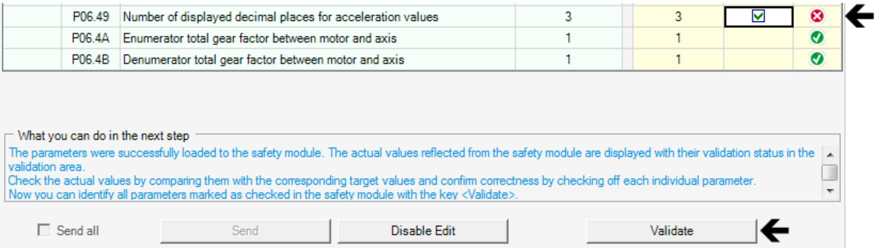
3. Click “Enabling editing” and tick the checkboxes of the deviating parameters under “Send”.

Input of parameters					Validation		
Send	ID	Name	Nominal value		Actual value	Checked	Valid
☑	P06.3E	Display unit for position values	mm = [4]		0		
☑	P06.3F	Enumerator feed constant of axis in m/R	4		1		

4. The “Send” button loads the selected parameters into the safety module.
5. This means that the parameters are initially no longer invalid. Check the parameters by comparing the values under “Setpoint” and “Actual value”. Confirm the check by ticking the checkbox under “Checked”. Then validate them with the “Validate” button.

Input of parameters				Validation		
Send	ID	Name	Nominal value	Actual value	Checked	Valid
	P06.3E	Display unit for position values	mm = [4]	4	☐	
	P06.3F	Enumerator feed constant of axis in m/R	4	4	☐	

6. If all the parameters of the basic information are identical, then the other parameters are loaded from the safety module and the “Data migration” screen is shown with the comparison of the data transmitted from the basic unit.



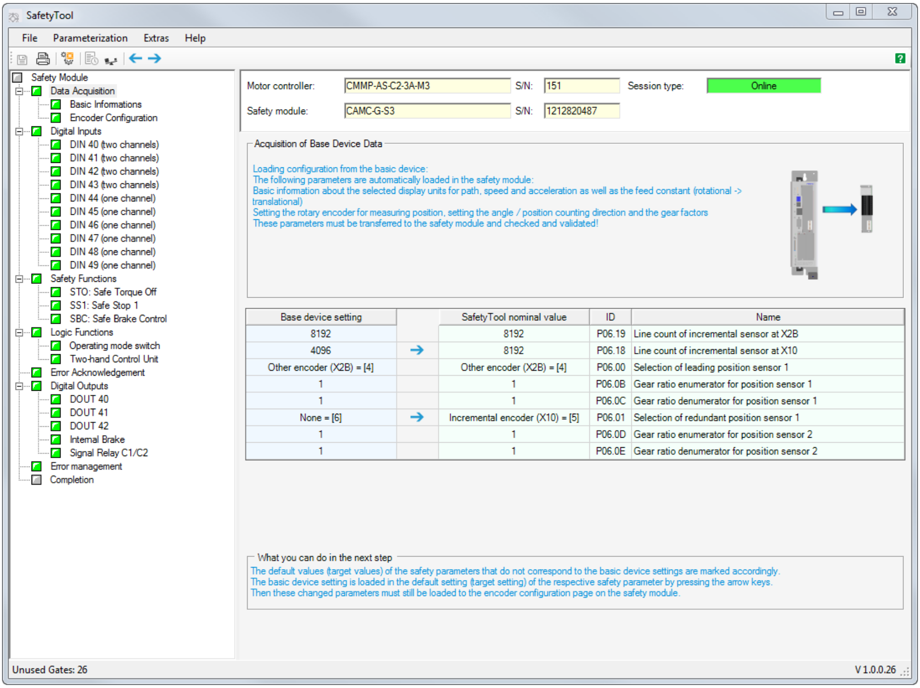


Fig.83

5.6.3 Starting parameterisation

The session variant “Change existing parameterisation” is now active and you can start the actual parameterisation.

- To do this, use the arrow buttons [1] to navigate through **all** the parameter screens and check or change the displayed parameters.

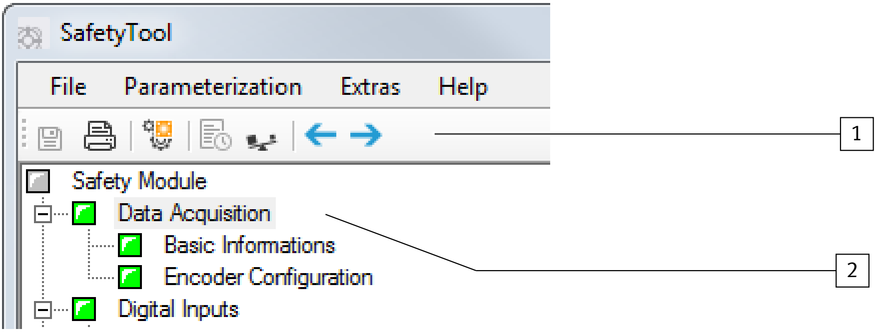


Fig. 84: Data migration

The appropriate parameter screen is displayed in the navigation tree [2], with which you can also switch directly to another screen, e.g. to subsequently review parameters.
We recommend checking or editing all screens in succession for commissioning.

5.6.4 Checking the data migration

The most important parameters of the encoder configuration are displayed on the first “Data migration” parameter screen.

Base device setting	↓	SafetyTool nominal value	ID	Name
8192		8192	P06.19	Line count of incremental sensor at X2B
4096	→	8192	P06.18	Line count of incremental sensor at X10
Other encoder (X2B) = [4]		Other encoder (X2B) = [4]	P06.00	Selection of leading position sensor 1
1		1	P06.0B	Gear ratio enumerator for position sensor 1
1		1	P06.0C	Gear ratio denumerator for position sensor 1
None = [6]	→	Incremental encoder (X10) = [5]	P06.01	Selection of redundant position sensor 1
1		1	P06.0D	Gear ratio enumerator for position sensor 2
1		1	P06.0E	Gear ratio denumerator for position sensor 2

Fig.85

Any deviations are shown by a blue arrow. Clicking the arrow migrates the basic unit setting as the parameter setpoint value. The parameter setpoint value must then be sent to the safety module on the appropriate encoder configuration screen and validated.

5.6.5 Basic information

If the basic information has already been edited (➔ 5.6 Sequence of parameterisation with the SafetyTool (example) the values on this screen should already be correct.

5.6.6 Encoder configuration

- Check or edit all parameters of the encoder configuration in succession.

If you have transferred the setpoint values, they are already entered in the appropriate parameter (➔ 5.6 Sequence of parameterisation with the SafetyTool (example)). They can then be transferred using “Enable editing”, “Send” and then checked and validated.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.18	Line count of incremental sensor at X10		4096	8192		✓

Fig.86

5.6.7 Configuring digital inputs

The allocation of all single-channel and two-channel inputs is displayed on the “Digital inputs” screen. However, every input is edited separately on the following screens.

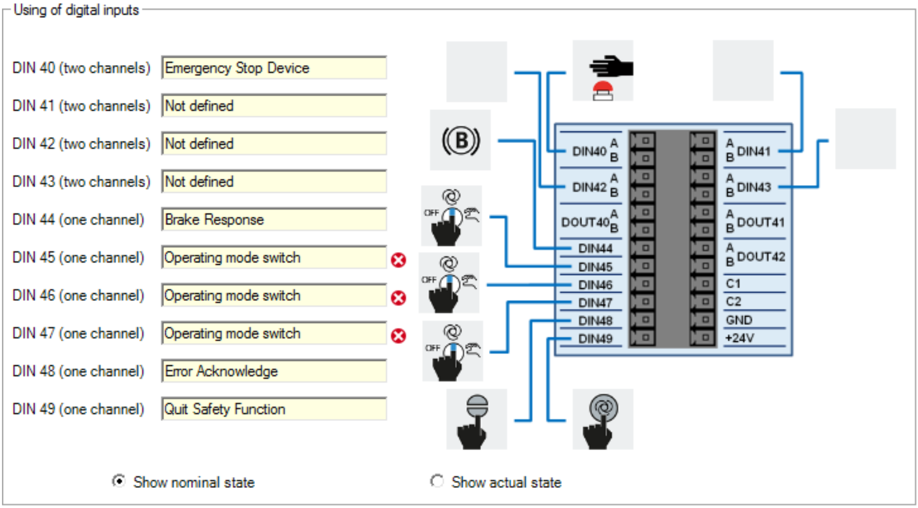


Fig.87

Inconsistencies are indicated by an error symbol. In the example, DIN45, DIN46 and DIN47 are parameterised as the sensor type “Mode selector switch”, but the “Activation” parameter of the mode selector switch is not active.
You should now edit the screens of the digital inputs one after another.

DIN40

- For the example, DOUT42A/B is set as the source of the test pulse.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
☐	P02.24	Sensor type		Emergency Stop Device = [2]	2		✓
☐	P02.06	Operating mode		Equivalent = [1]	1		✓
☐	P02.05	Discrepancy time	ms	100,0	100,0		✓
☑	P02.07	Test pulse source		DOUT42A/B = [3]	≠ 0		✓

Fig.88

DIN41

- For the example, “Light curtain” is set as the sensor type and DOUT42A/B as the source of the test pulse.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
☑	P02.25	Sensor type		Light Curtain = [8]	0		✓
☐	P02.0B	Operating mode		Equivalent = [1]	1		✓
☐	P02.0A	Discrepancy time	ms	100,0	100,0		✓
☑	P02.0C	Test pulse source		DOUT42A/B = [3]	0		✓

Fig.89

DIN42

- For the example, “Enabling button” is set as the sensor type and DOUT42A/B as the source of the test pulse.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
☑	P02.26	Sensor type		Enable Switch = [3]	0		✓
☐	P02.10	Operating mode		Equivalent = [1]	1		✓
☐	P02.0F	Discrepancy time	ms	100,0	100,0		✓
☑	P02.11	Test pulse source		DOUT42A/B = [3]	0		✓

Fig.90

DIN45 ... DIN47

- For the example, DOUT42B is set as the source of the test pulse for DIN45, DIN46 and DIN47.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
☐	P02.29	Sensor type		Operating mode switch = [11]	11		✓
☑	P02.1B	Test pulse source		DOUT42B = [10]	4		✓

Fig.91

DIN43 and DIN44, DIN48 and DIN49

No changes are required for the example because all settings correspond to the factory settings.

5.6.8 Selection and parameterisation of the safety functions

The active functions are displayed on the “Safety functions” screen.

- For the example, you should also activate SS2, SOS and USF0. You can parameterise the SLS safety function using USF. Sending and validation are not required to activate safety functions.

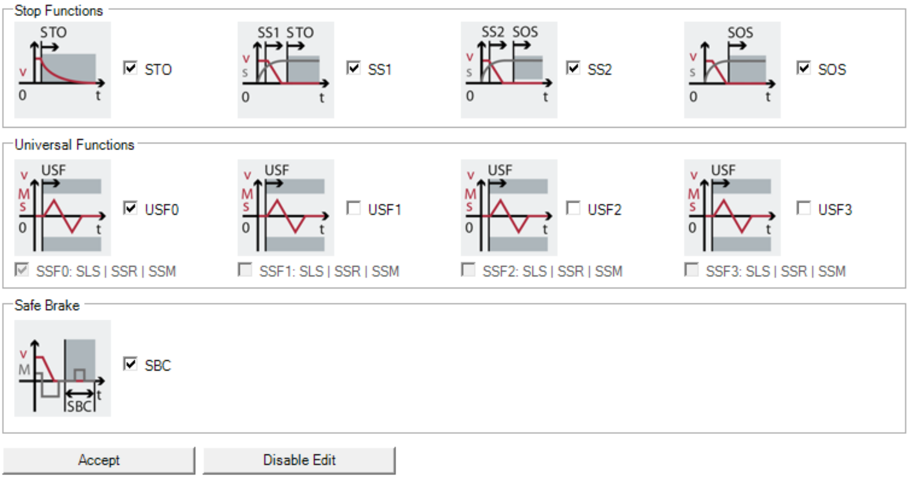
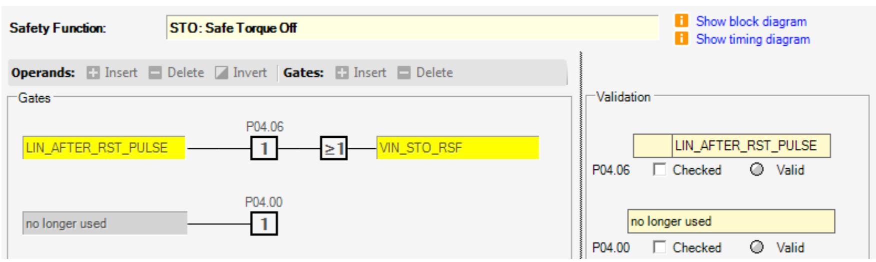


Fig.92

STO: Safe Torque Off

1. Check, and if necessary change the parameters of the STO safety function ➔ 3.5 Safety functions.
2. In the “Request” tab, delete the request in the factory setting via DIN40. After editing has been enabled, select the logical input LIN_D40 in the gate (highlighted in blue) and remove it using “Operands: Del.”.
   As the operand has now been deleted from the product term but the product term (here P04.00) is still assigned, it is still displayed at the bottom.
3. In the right-hand “Operands” frame, select LIN_AFTER_RST_PULSE and apply the entry with “Gate: Ins.”.



4. “Send” sends the change to the safety module. Then, under “Validation” (in the top right of the above figure), the new allocation and the deletion operation are displayed and can be checked and validated.

In the example, the setting in the “Terminate request” tab can be left as LIN_D49_RISING_EDGE.

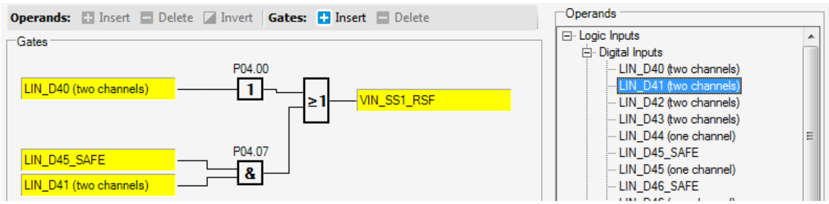
SS1: Safe Stop 1

1. Check the settings in the “Standard parameters” tab and adapt them to your application if necessary ➔ 3.5 Safety functions.

2. For the example, activate “Automatic activation SBC” (P0C.09).
   For the example, create the following logic in the “Request” tab:

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0C.00	Delay time for start of monitoring	ms	2,0	2,0		✓
	P0C.01	Brake ramp time	ms	300,0	300,0		✓
	P0C.02	Tolerance time for limit exceed	ms	10,0	10,0		✓
	P0C.06	Limit speed in base device		☐	0		✓
	P0C.07	Activate quick stop ramp in base device		☑	1		✓
	P0C.08	Automatic restart allowed		☐	0		✓
	P0C.09	Automatic activate SBC		☑	1		✓

3. For the example, create the following logic in the “Request” tab:



4. In the right frame “Operands”, select LIN_D40 and apply the entry with “Operands: Ins.”. Alternatively, you can drag the entry to the driver connection with the mouse (here product term P04.00).
5. Then select LIN_D45_SAFE and apply the entry with “Gate: Ins.”. Alternatively, you can drag the entry with the mouse onto the OR gate (≥ 1). This inserts a new gate with the input LIN_D45_SAFE (in the example, product term P04.07).
6. Now select the entry LIN_D45_SAFE just inserted under “Gate” to mark the second gate as the target for inserting further operands (here product term P04.07).
7. Then select the LIN_D41 entry in the right “Operands” frame and copy it with “Operands: Ins.”. Alternatively, you can drag the entry onto the driver connection with the mouse. As a result, the driver connection automatically changes to the AND operation.
8. After transmission, you must now validate 2 product terms using the OR operation.

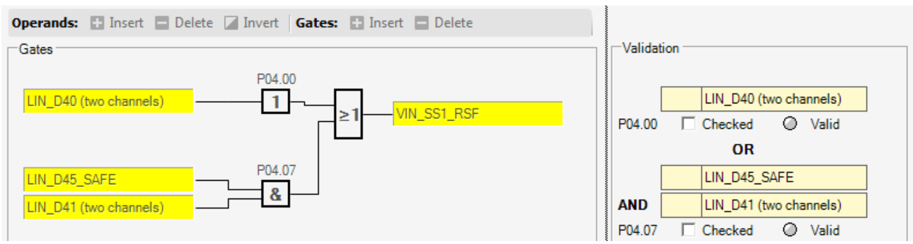
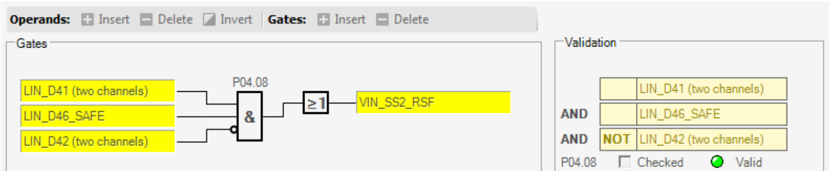


Fig.93

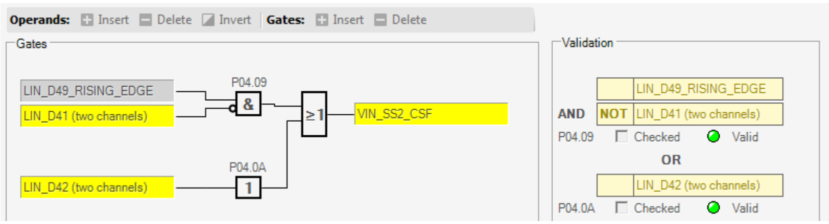
In the example, the setting in the “Terminate request” tab can be left as LIN_D49_RISING_EDGE.

SS2: Safe Stop 2

1. Check the settings in the "Standard parameters" tab and adapt them to your application if necessary ➔ 3.5 Safety functions.
   Create the following logic for the example in the "Request" tab:



2. In the right frame "Operands", select LIN_D41 and apply the entry with "Operands: Ins.". Alternatively, you can drag the entry to the driver connection with the mouse (here product term P04.08).
3. Repeat step 2 with the operands LIN_D46_SAFE and LIN_D42.
4. Invert LIN_D42 with "Operands: Invert". If you selected another element in the meantime, you may need to select LIN_D42 again in advance.
5. After transmission, you only need to validate one product term.
   For the example, create the following logic in the "Terminate request" tab:



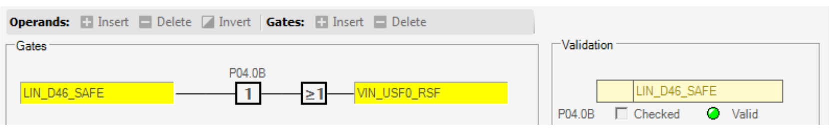
6. In the right frame "Operands", select LIN_D49_RISING_EDGE and apply the entry with "Operands: Ins.".
7. Repeat step 6. with LIN_D41.
8. Invert LIN_D41 with "Operands: Invert".
9. Then select LIN_D42 and add as an AND operation using "Gate: Ins.".
10. After transmission, you must now validate 2 product terms using the OR operation.

SOS: Safe Operating Stop

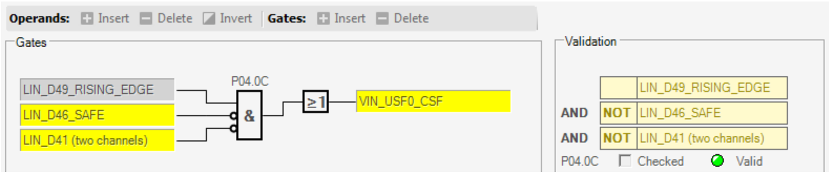
1. Parameterise the safety function SOS according to your application ➔ 3.5 Safety functions.
2. No logic is required to request SOS, as SOS is only used as an error response.
3. For "Terminate request", insert LIN_D49_RISING_EDGE (as for SS2).

USF0: universal function

1. To request USF0 in the example, add LIN_DIN46_SAFE.



2. For the example, create the following logic in the “Terminate request” tab:



The basic operating steps are described in the steps listed above.

SSF0: Safe Speed

- For the SLS safety function, parameterise the function SSF0 according to your application ➔ 3.5 Safety functions.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.00	Activate SSF		☑	1		✓
	P0E.01	Delay time for start of monitoring	ms	2,0	2,0		✓
	P0E.07	Safe speed - upper limit	mm/s	225,00	225,00		✓
	P0E.08	Safe speed - lower limit	mm/s	-225,00	-225,00		✓
	P0E.02	Brake ramp time	ms	300,0	300,0		✓
	P0E.03	Tolerance time for limit exceed	ms	10,0	10,0		✓
	P0E.09	Limit speed in base device		☑	1		✓
	P0E.0B	Automatic restart allowed		☐	0		✓

Fig.94

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.0D	Speed ramp - Delay time monitoring	ms	0,0	0,0		✓
	P0E.06	Brake ramp - start delay	ms	6,0	6,0		✓
	P0E.04	Brake ramp - starting value factor		0,10	0,10		✓
	P0E.05	Brake ramp - starting value offset	mm/s	75,00	75,00		✓
	P0E.0C	Offset speed limit	mm/s	75,00	75,00		✓
	P0E.0A	Activate quick stop ramp in base device		☐	0		✓

Fig.95

SBC: Safe Brake Control

1. Parameterise the safety function SBC according to your application ➔ 3.5 Safety functions.
2. In the example, delete the request by LIN_D40.
3. For “Terminate request”, leave LIN_D49_RISING_EDGE.
4. Depending on your application, logic for the brake feedback may be necessary in the “Feedback” tab.

5.6.9 Logic functions

The Additional Logic Functions ALFx are not used in the example and therefore do not need to be activated on the “Logic functions” screen.

Mode selector switch

- Activate the mode selector switch on the “Mode selector switch” screen.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P02.00	Activation		☑	1		✔
	P02.01	Discrepancy time	ms	500,0	500,0		✔

Fig.96

Two-hand control unit

The two-handed control unit is not used in this example.

5.6.10 Logic error acknowledgement

The logic error acknowledgement can be left in the factory setting in this example.

5.6.11 Digital outputs

DOUT40, DOUT41

Digital outputs DOUT40 and DOUT41 are not used in the example.

DOUT42

The parameterisation does not need to be changed for the example because DOUT42 is already parameterised as “Permanently switched on” in the factory setting.

Internal brake

In the example, the factory setting can be used for parameterisation of the internal brake.

Signal contact

In the example, the factory setting can be used for parameterisation of the signal contact. The relay is closed if all the requested safety functions are active and no safety condition has been violated.

5.6.12 Error management

You must select an adequate error response on the “Error management” screen for the violation of safety conditions and for errors, for example in the angle encoder analysis.
For the example, use the factory settings. If there is an error, STO or SS1 as well as SBC is usually triggered.

5.6.13 Finishing parameterisation

If the LEDs of the main node are “green”, the parameter set can be validated (full validation).
The validation code currently calculated by the safety module is read out and displayed in hexadecimal form in the “Validation code” display field.
The current status of parameterisation is displayed beneath the “Validation code” field.
To be able to complete parameterisation successfully, the parameters must be backed up in the device.

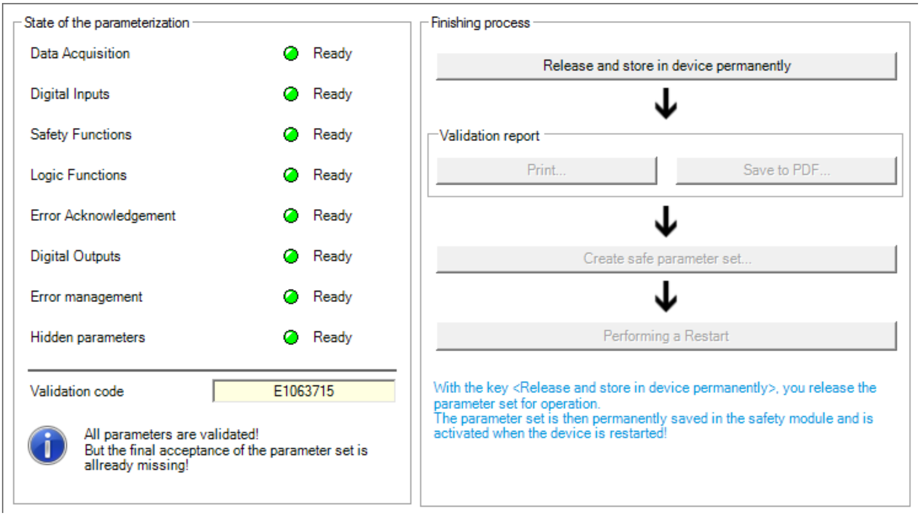
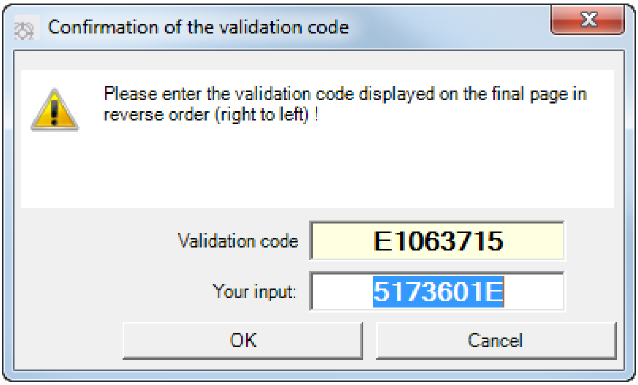


Fig.97

1. To do this, click “Enable and save permanently in the device” first.
2. As confirmation, the validation code must be entered **in reverse order** and confirmed with OK.



3. When the validation code has been entered correctly, the safety module saves the parameters permanently in the flash memory and the “Finish” screen is now also shown in green in the navigation tree.
4. To create the necessary validation report, you can now either output the summary to a printer using the “Print” option or generate a corresponding PDF document using “Save as PDF”.
5. You can send the validated parameter set to other safety modules that have the same parameters for subsequent use. For this, or to replace the safety module, use "Create safe parameter set" to save a file.

6. To finish parameterisation, click “Perform restart”. This restarts the motor controller and the safety module.

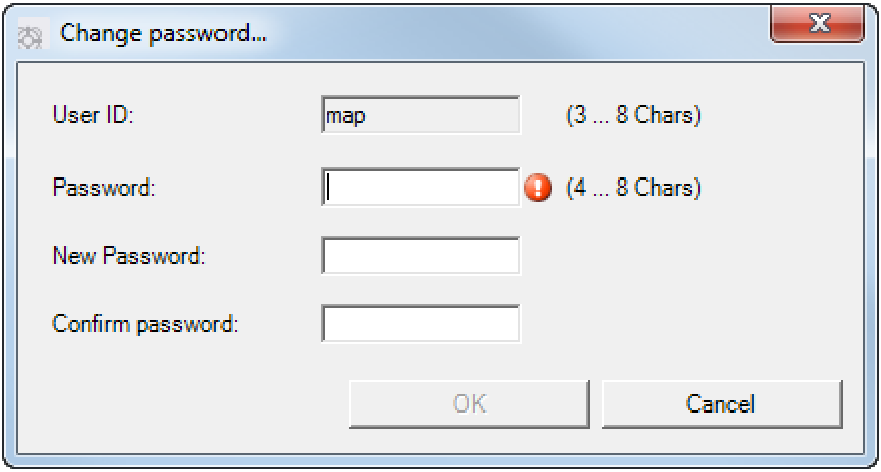
The parameterisation of the example is completed

5.7 Special functions of the SafetyTool

5.7.1 Change password

The password can be changed at any time while a parameterisation session is active.

1. Open the “Change password” dialogue with the menu command [Options] [Change password].
2. Enter the existing password under “Password”.



3. Enter the new password twice under “New password” and “Confirm password”.
4. Confirm with “OK”.

The new password is immediately active in the safety module.

5.7.2 Restore factory settings

Factory settings ➔ 5.4.1 Factory setting.

To reset the safety module to factory settings:

1. Start the SafetyTool ➔ 5.6 Sequence of parameterisation with the SafetyTool (example) with an active online connection.
2. Select the online session variant “Display parameterisation” (no password required).
3. Deviating basic information may then be displayed, which you confirm with OK.
4. The safety module is reset with the menu command [Options] [Restore factory settings]. For this purpose, the user name is queried (is logged in the permanent diagnostic memory).
5. The parameter set is then read again from the safety module. Any deviating basic information must be confirmed again.
6. Close the SafetyTool.

5.7.3 Plausibility check

The plausibility check can be performed at any time during a parameterisation session.

– Open the “Plausibility check” window with the menu command [Options] [Check parameters for plausibility].

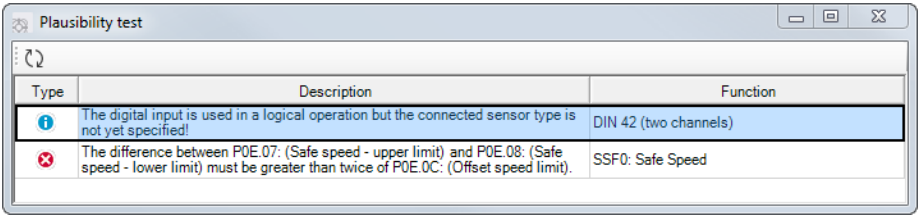


Fig.98

The points detected during the test are each marked with a symbol.

Symbol	**Meaning**
	Information: information only with no functional meaning.
	Warning: parameterisation works, but may not be complete.
	Error: incorrect parameterisation, the safety module will not function properly.

Tab. 115: Display of the plausibility check

5.7.4 Overview of parameters

The parameters can be displayed and edited in a separate window for quick access for experts.

– Open the “Parameter overview” window with the menu command [Options] [Parameter overview].

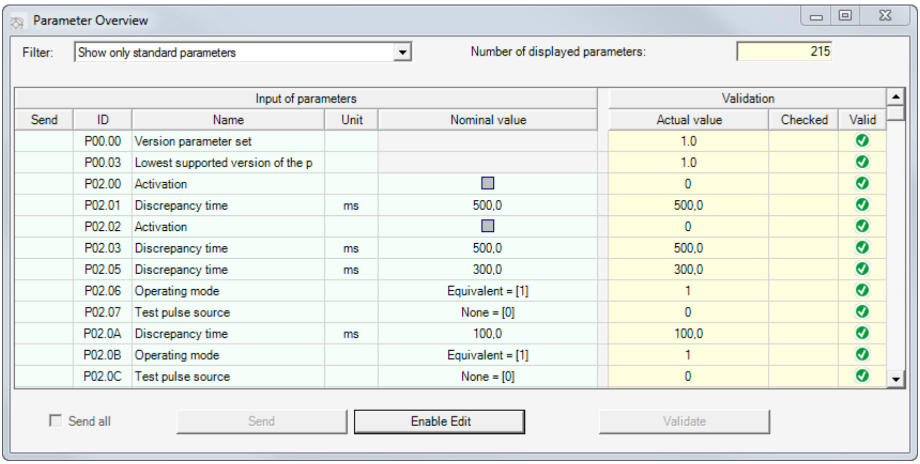


Fig.99

5.7.5 Diagnostics window

The [Options] [Diagnostics] submenu contains various commands for displaying a range of diagnostics windows. For more information see the SafetyTool help.

For example, the “Digital I/O (logic states)” window displays the logic state of the inputs and outputs:

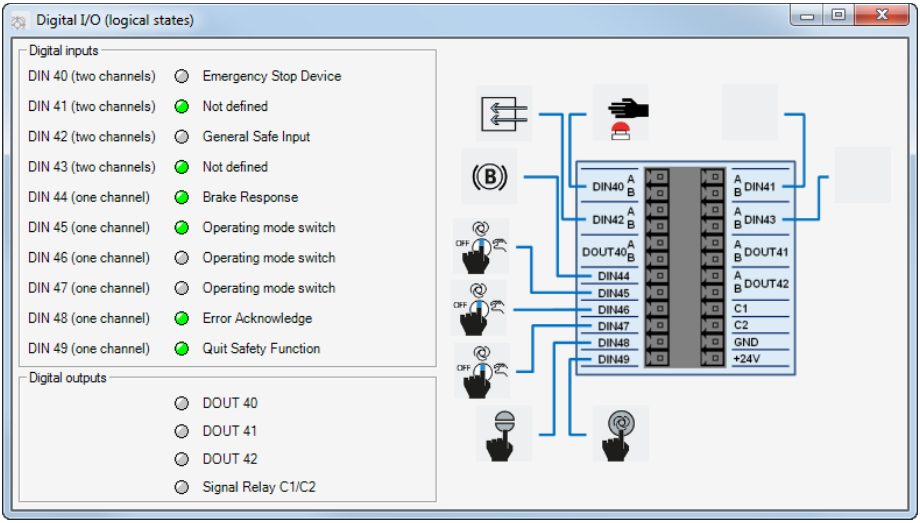


Fig. 100: Digital I/O – logic states

The “Error display” window displays the active errors. You can acknowledge them here with the “Acknowledge error!” button, if possible.

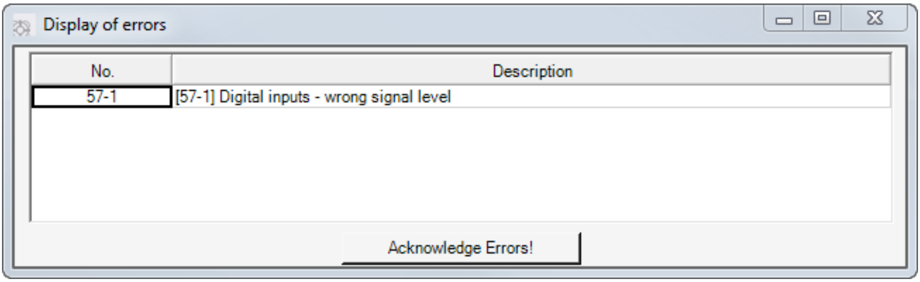


Fig. 101: Error display

Open the "Functional diagram" window with the menu command [Options] [Diagnostics] [Internal Signals]. The window shows an overview of the logical and virtual inputs as well as the virtual and logical outputs of the safety module.
Clicking on one of the blue text links opens another window in which the status of the signal group is displayed (in the example, the logical inputs depicted by the physical inputs).

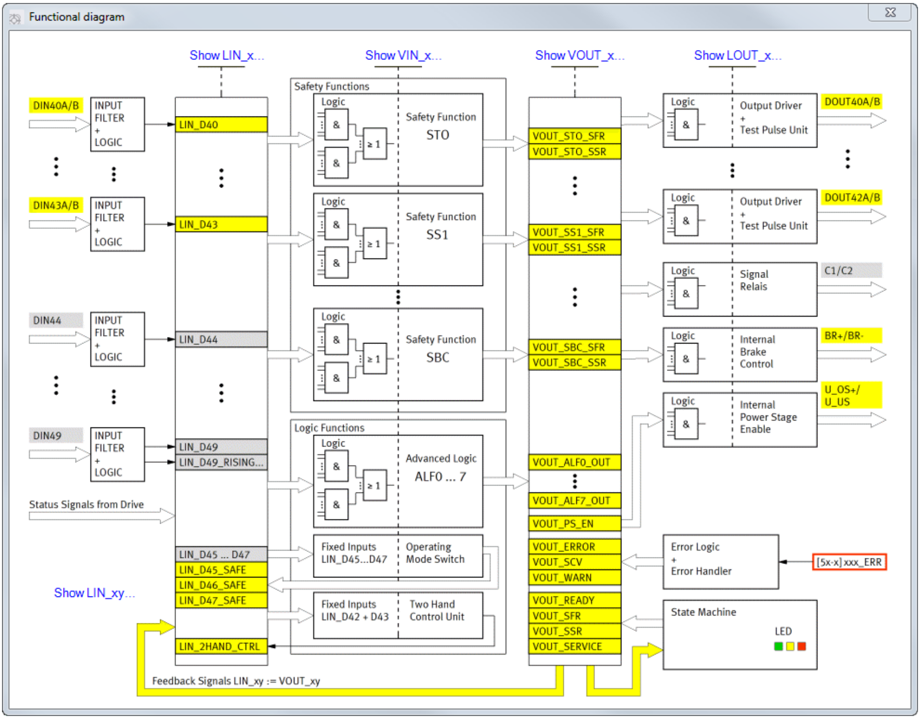


Fig. 102: Functional diagram

5.8 Function test, validation

NOTICE

The safety functions must be validated after installation and after every modification to the installation.

This validation must be documented by the person who commissions the device. To assist you with commissioning, we have put together some sample questions for risk reduction in the form of the check lists below.

ⓘ

The following check lists are no substitute for training in safety engineering.

The completeness of the check lists cannot be guaranteed.

No.	Questions	Relevant	Done
1.	Have all operating conditions and interventions been taken into account?	Yes ☐ No ☐	☐
2.	Has the 3-step method for risk reduction been applied, i.e.: 1. Inherently safe design, 2. Technical and any additional protective measures, 3. User information about the residual risk?	Yes ☐ No ☐	☐
3.	Have the hazards been eliminated or the hazard risks reduced as far as practically possible?	Yes ☐ No ☐	☐
4.	Can it be guaranteed that the implemented measures do not create new hazards?	Yes ☐ No ☐	☐
5.	Have the end users been given sufficient information and warning regarding the residual risks?	Yes ☐ No ☐	☐
6.	Can it be guaranteed that the implemented protective measures have not led to a deterioration in the working conditions of the operating personnel?	Yes ☐ No ☐	☐
7.	Are the implemented protective measures mutually compatible?	Yes ☐ No ☐	☐
8.	Has adequate consideration been given to the potential consequences of using a machine designed for commercial/industrial purposes in a non-commercial/non-industrial area?	Yes ☐ No ☐	☐
9.	Can it be guaranteed that the implemented measures will not severely impair the machine's ability to perform its function?	Yes ☐ No ☐	☐

Tab. 116: Questions for validation in accordance with EN 12100 (example)

No.	Questions	Relevant	Done
1.	Has a risk assessment been carried out?	Yes ☐ No ☐	☐
2.	Have a list of issues and a validation plan been drawn up?	Yes ☐ No ☐	☐
3.	Has the validation plan – including analysis and inspection – been worked through and has a validation report been created? The following must be inspected as a minimum as part of the validation:	Yes ☐ No ☐	☐
	a) Check the components: is the CMMP-AS-...-M3 used with the CAMC-G-S3? (check using the rating plates)	Yes ☐ No ☐	☐

No.	Questions	Relevant	Done
3.	b) Is the wiring correct (check using the circuit diagram)?	Yes □ No □	□
	– Have safety command devices, e.g. protective door switches, emergency stop switches etc. been wired to X40?	Yes □ No □	□
	– Are the safety command devices suitable for the requirements of the application and have they been wired accordingly?	Yes □ No □	□
	c) Check of parameterisation:	Yes □ No □	□
	– If the parameterisation of the safety module has been completed, are all parameters validated?	Yes □ No □	□
	– Has the parameter set been printed and added to the validation plan?	Yes □ No □	□
	d) Functional tests:	Yes □ No □	□
	– Actuation of the emergency stop of the system: Is the drive stopped?	Yes □ No □	□
	– Actuation of the emergency stop of the system: If only one of the DIN4xA or DIN4xB inputs allocated to the emergency stop is activated - is the allocated safety function executed immediately and the error “Discrepancy time violation” (display 57-1) generated in the CMMP-AS-M3 after the discrepancy time has elapsed?	Yes □ No □	□
	– Actuation of the other safety functions of the system - to be carried out separately for each safety function: If only one of the two-channel inputs DIN4xA/B allocated for the request of the safety function is activated - is the allocated safety function executed immediately and is the error “Discrepancy time violation” (display 57-1) generated in the CMMP-AS-...-M3 after the discrepancy time has elapsed?	Yes □ No □	□
	– When using safe outputs - to be carried out separately for each output: Do both outputs DOUT4xA/B switch off equivalently if the corresponding switching condition is present and is the subsequent safety relay unit in the safe state in the event of a fault (line break, short circuit etc.)?	Yes □ No □	□

No.	Questions	Relevant	Done
3.	– Only when using a safety relay unit with evaluation of the feedback contact C1/C2: Is the drive stopped at the latest with the next safety request in the event of a short circuit from C1 to C2?	Yes ☐ No ☐	☐
	– Is the restart prevented? That is, with activated emergency stop and active enable signals, does no movement take place in response to a start command without prior activation of the "Terminate safety function" input?	Yes ☐ No ☐	☐

Tab. 117: Questions for the validation in accordance with EN ISO 13849-2 (example)

6 Operation and use

6.1 Obligations of the operator

The functionality of the safety module CAMC-G-S3 is to be checked at appropriate intervals. It is the responsibility of the operator to choose the type and frequency of the checks within the specified time period. The manner in which the test is conducted must make it possible to verify that the safety device is functioning perfectly in interaction with all components. Proof test interval ➔ 8.1.1 Safety engineering.

⚠ WARNING

Danger due to failure of the safety function!

In the event of a power failure, the safety functions are not guaranteed (exception: safe torque off, STO; safe brake control, SBC).

Lack of the safety function can result in serious, irreversible injuries, e.g. due to unintentional movements of the connected actuator technology.

- Ensure that your application has a reliable power supply or use other appropriate measures.

6.2 Maintenance and care

The safety module is maintenance-free.

6.3 Protective functions

6.3.1 Supply - overvoltage and reverse polarity protection; voltage monitoring

The 24 V power supply comes from the basic unit. The permissible operating voltage range is monitored by the safety module. The power supply of the safety module is also specially protected against

– surges in accordance with EN 61326-3-1.
– increase in the 24 V supply in the event of a fault up to 60 V (PELV supply specification).

Reverse polarity protection is provided by the basic unit.

6.3.2 Internal electronics power supply

The internal operating voltages are generated from the 24 V supply.
The internal electronics supply voltages are of redundant design.
This means that the two micro controllers in the safety module are powered independently.
They alternately monitor all internal operating voltages.

6.3.3 Fail-safe power supply

The core of the control of the outputs is the so-called "fail-safe power supply". Each micro controller uses a dynamic signal to generate its own (internal) auxiliary power supply (U_FS1, U_FS2) to activate the different (safe) outputs for

– the power supply for driver activation, separate for top and bottom switches,
– brake control, separate for circuit breakers BR + and BR-,
– digital outputs DOUT40 - DOUT42, separate for pin A and pin B.

U_FS1 acts on the outputs that are controlled by micro controller2; conversely, U_FS2 acts on the outputs of micro controller1. This ensures that each micro controller can switch off the outputs of the other micro controller in the event of a fault.
If a micro controller fails (for whatever reason - hardware error, program crash etc.), the corresponding "Fail-safe" power supply fails and the outputs are switched off.

6.3.4 Protective functions for the digital outputs

The digital outputs are protected against:
- short circuit to 0 V and 24 V and PE
- any cross circuits to other outputs
- voltage surge to 60 V

Active outputs are monitored during operation by test pulses.
In the event of a fault the outputs are switched off, including all at the same time.

6.3.5 Protective functions for the digital inputs

The digital inputs are protected against:
- short circuit to 0 V and 24 V and PE
- any cross circuits to other outputs
- surge malfunctions
- voltage surge to 60 V

The inputs are monitored during operation by internal test pulses.
The connected passive sensors are monitored by external test pulses via DOUT4x.
In the case of multi-channel inputs, a plausibility check takes place for simultaneous switching with discrepancy time monitoring.

6.3.6 Protective functions for the brake activation

The outputs for brake activation are protected against:
- short circuit to 0 V and 24 V and PE
- any cross circuits to other outputs
- voltage surge to 60 V

The outputs are monitored during operation by test pulses. The outputs are switched off in the event of a fault.

6.3.7 Protective functions of the power supply for driver activation

The outputs for driver activation are protected against:
- short circuit to 0 V and 5 V, as well as external voltage up to 60 V
- cross circuits between the two power supplies
- voltage surge to 60 V

The outputs are monitored during operation by test pulses.
The outputs are switched off in the event of a fault.

6.3.8 Protective function for the connected position encoder

The function of the position encoder is continuously monitored during operation.
What is monitored depends on the type of encoder, e.g.:

- Monitoring of the analogue tracking signals, amplitudes and vector length monitoring for SIN/COS and Hiperface encoders and also resolvers
- Monitoring of communication for purely serial encoders
- Additional plausibility check of the position data using acceleration monitoring
- Comparison of the position and speed data of position encoder 1 with those of position encoder 2 in a cross-comparison between the micro controllers
- Timeout control in case of standstill and requested safety function for position encoders without forced dynamisation (10-day monitoring).

6.3.9 Internal protective function of the electronics on the safety module

The safety module has numerous other internal monitoring functions, which can be performed by the internal micro controllers for each other:
- Dynamisation of many internal analogue signals using test pulses
- Self-monitoring of the micro controllers during operation using memory tests, OP code tests, stack and program sequence monitoring
- Cross-comparison of correct program execution and synchronous program processing between micro controller 1 and micro controller 2
- Cross-comparison of all key operating statuses and key status variables between micro controller 1 and micro controller 2
- Monitoring of ambient conditions (temperature)
- Monitoring of the internal communication interfaces
- Monitoring of communication to outside
- Monitoring of the data integrity of the safe parameter sets
- Monitoring of the operating statuses and changeover
- Monitoring of the parameterisation session (session, password, master control etc.)
- Monitoring of the error status

6.3.10 Monitoring compliance with the requested safety functions

All the requested safety functions and logic functions are monitored permanently in the safety module. If a safety limit is violated, the corresponding error is triggered. Monitoring primarily comprises:
- Compliance with the set speed limits
- Compliance with the set position limits
- Standstill monitoring
- Compliance with the requested time conditions
- Monitoring feedback signals (existence, time response)
- 10-day monitoring (for Safe Operating Stop SOS and Safe Brake Control SBC)

6.4 Diagnostics and fault clearance

6.4.1 LED indicators on the safety module

The operating status is displayed on the two-colour status LED of the safety module ➔ Fig. 3, [5].
The following statuses are displayed:

LED display	Operating status	Status signal
flashing red	Safety module is in the status “Internal error”, error in the safety module.	VOUT_ERROR = 1
lit up red	Safety module is in the status “Safety condition violated”, error response started.	VOUT_SCV = 1 VOUT_SFR = 1
lit up yellow	Safety module is in the status “Safe state reached”.	VOUT_SSR = 1 VOUT_SFR = 1
flashing yellow	Safety module is in the status “Safety function requested, not yet reached”.	VOUT_SFR = 1
flashing red/green	Safety module is in the status “Delivery status - parameterisation of motor controller”. The drive is enabled, all the digital IOs are de-energised.	VOUT_SERVICE = 1 VOUT_PS_EN = 1
flashing green	– Safety module is in the status “Service” (basic status). – The parameter set of the safety module has not been validated. – There is no parameter set in the motor controller. – A parameterisation session was opened. – Parameter sets in the motor controller and in the safety module deviate.	VOUT_SERVICE = 1 VOUT_PS_EN = 0
lit up green	Safety module is in the status “Ready for operation, no safety function requested”. Safety module has been initialised without error and is ready for operation.	VOUT_READY = 1 VOUT_PS_EN = 1
off	Safety module has not been initialised/is not ready for operation.	VOUT_READY = 0 VOUT_PS_EN = 0

Tab. 118: LED display of the safety module

Complete description of the statuses ➔ 3.10.2 Status display on the safety module.

6.4.2 7-segment display of the motor controller

NOTICE

The 7-segment display of the motor controller is a purely diagnostic display. The display of safety-relevant data would require an upstream function test of the display - this is not intended.

Status signals of the motor controller are displayed on the 7-segment display of the motor controller. In addition, the safety module can output status and error messages via the 7-segment display, if the motor controller is not in an error state.

Display of strings

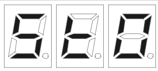
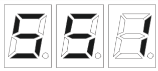
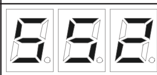
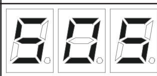
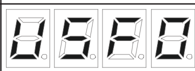
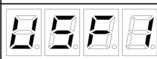
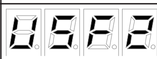
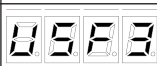
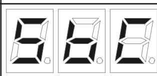
The individual characters are displayed in succession. The display goes blank briefly each time the character changes. The display is repeated at regular intervals. There is a break between the last character of the string and the first character of the repeat and the display goes dark briefly. Strings can also "flash rapidly" when displayed: every character flashes multiple times during the display time.

Display of errors

Only errors and warnings are displayed (an error has occurred whose response was not parameterised as "No response, entry in diagnostic memory only").
Errors of the safety module are displayed in the same way as the errors in the motor controller.

A safety function was requested

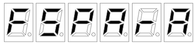
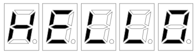
Functions that result in a stop of the drive (STO, SOS, SS1, SS2) are given preference, otherwise the most recently displayed safety function is displayed.
If a safety function has been requested but the safe status has not yet been reached, the name of the function flashes rapidly.
The requested safety functions are displayed as described in the following table.

Safety function	Display	
STO	S t O	
SS1	S S 1	
SS2	S S 2	
SOS	S O S	
USF0 (with SSF0: SLS, SSR, SSM)	U S F 0	
USF1 (with SSF1: SLS, SSR, SSM)	U S F 1	
USF2 (with SSF2: SLS, SSR, SSM)	U S F 2	
USF3 (with SSF3: SLS, SSR, SSM)	U S F 3	
SBC	S b C	

Tab. 119: Display of the safety functions

Other displays

The following table shows other displays connected with the safety module.

Function/status	Display	
Active parameterisation session The string is displayed at regular intervals while a parameterisation session is running.	F S P A r A	
Identify controller The string HELLO followed by the serial number[1)] of the basic unit is displayed cyclically as long as the “Identification” function is active (wave function).	H E L L O …	

1) The serial number of the basic unit is displayed in the FCT plug-in on the “Controller” page and in the SafetyTool. You will also find the serial number on a small sticker on the bottom of the device (between [X6] and [X2A]).

Tab. 120: Other displays

6.5 Error messages and error handling

6.5.1 Error numbers

Error numbers 51 to 59 are reserved for the safety module.
The table below contains an overview of the allocation.

No.	Description
51-x	Motor controller: hardware errors (safety module available, module replacement).
52-x	Motor controller: safety module errors (state machine, discrepancy time …) and motor controller errors if they affect the safety module.
53-x	Safety module: (errors of the safety module).
54-x	
55-x	
56-x	
57-x	
58-x	
59-x	

Tab. 121: Error messages generated by the motor controller and the safety module

6.5.2 Error acknowledgement

Errors 51-x and 52-x generated by the motor controller can be acknowledged via the motor controller
➔ see function description for the CMMP-AS-...-M3.
Errors 53-x to 59-x are generated by the safety module and can only be acknowledged via the safety module.
They are acknowledged by the parameterised control input on the safety module or in the SafetyTool (on the “Safety module” start page or in the “Error display” window – Menu [Options] [Diagnostics]

[Errors]). In so doing, all the errors, including errors of the basic unit, are acknowledged as far as possible. After a restart of the motor controller (reset button of the basic unit or switching the power supply off and on), the errors are also “acknowledged”, provided that the cause no longer exists.

ⓘ

Additional information on error acknowledgement in the safety module ➔ 3.8.3 Logic for error acknowledgement.

6.5.3 Diagnostic messages

If an error occurs, the safety module indicates this using a steady or flashing red LED. The motor controller CMMP-AS-...-M3 also displays a diagnostic message cyclically in the 7-segment display. An error message is a combination of E (for error), a main index and a subindex, e.g.: **E 0 1 0.**
Warnings have the same number as error messages. The difference is that a warning is displayed with a prefixed and suffixed hyphen, e.g. -. **1 7 0 -**

ⓘ

Section ➔ 6.6 Diagnostic messages with information for fault clearance lists the messages that are relevant for functional safety in combination with the safety module.
The complete list of error messages can be found in the hardware documentation GDCP-CMMP-M3-HW-... of the motor controller used.

The following table explains the entries in the tables in section ➔ 6.6 Diagnostic messages with information for fault clearance.

Column	**Meaning**
No.	Main index and subindex of the diagnostic message.
Code	The Code column includes the error code (Hex) via CiA 301.
Message	Message that is displayed in the FCT.
Cause	Possible causes for the message.

Column	Meaning
Measure	Action by the user.
Response	The Reaction column contains the error response (default setting, partially configurable): – PS off (switch off power stage), – MCStop (fast stop with maximum current), – QStop (fast stop with parameterised ramp), – Warn, – Ignore (No message, entry in diagnostic memory only), – NoLog (No message and no entry in diagnostic memory). The response to errors 53-x to 59-x is configured with the SafetyTool: – Request for SBC + STO + set all digital outputs to “0” [8] – SBC + STO request [7] – STO request [6] – SBC SS1 request [5] – SS1 request [4] – SS2 request [3] – Generation of a warning, no further response [2] – corresponds to “Warn” – No response, entry in diagnostic memory only [1] – corresponds to “Entry” – No response, no entry in diagnostic memory [0] – corresponds to “Ignore”

Tab. 122: Explanations of the table “Diagnostic messages of the CMMP-AS-...-M3”

If an error message cannot be acknowledged, the cause must first be remedied in accordance with the recommended measures. Then reset the motor controller, and check whether the cause of the error and thus the error message have been cleared.

6.6 Diagnostic messages with information for fault clearance

Error group 0		**Information**		
No.	Code	Message		Reaction
0-0	–	**Invalid error**		Ignore
		Cause	Information: an invalid error entry (corrupted) has been marked with this error number in the diagnostic memory. The system time entry is set to 0.	
		Action	–	
0-1	–	**Invalid error detected and corrected**		Ignore
		Cause	Information: an invalid error entry (corrupted) was detected in the diagnostic memory and corrected. The additional information contains the original error number. The system time entry includes the address of the corrupted error number.	

Error group 0		Information		
No.	Code	Message		Reaction
0-1	–	Action	–	
0-2	–	**Error cleared**		Ignore
		Cause	Information: active errors have been acknowledged.	
		Action	–	
0-4	–	**Serial number/type of equipment (module replacement)**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-7	–	**Subsequent entry**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-8	–	**Controller switched on**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-9	–	**Controller safety parameters changed**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-10	–	**Safety module: parameters changed**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-11	–	**Module replacement: previous module**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-12	–	**Module replacement: current module**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-13	–	**Safety module: error acknowledged**		Ignore
		Cause	Information: → diagnostic memory entry.	
		Action	–	
0-14	–	**Safety function requested**		Ignore
		Cause	Information: → diagnostic memory entry.	

Error group 0		Information		
No.	Code	Message		Reaction
0-14	–	Action	–	
0-15	–	**Safety module: parameterisation session started**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-16	–	**Safety module: parameterisation session closed**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-17	–	**Safety module: password changed**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-18	–	**Safety module: password reset**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-19	–	**Safety module: parameter set loaded**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-20	–	**Safety module: parameter set saved**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	
0-21	–	**Log entry of the safety module**		Ignore
		Cause	Information: ➔ diagnostic memory entry.	
		Action	–	

Tab. 123

Error group 51		Safety module/function		
No.	Code	Message		Reaction
51-0	8091h	**No/unknown safety module or driver supply defective**		PSoff
		Cause	Internal voltage error of the safety module or switch module.	
		Action	– Module presumably defective. If possible, replace with another module.	

Error group 51		Safety module/function		
No.	Code	Message		Reaction
51-0	8091h	Cause	No safety module detected or unknown module type.	
		Action	– Install safety or switch module appropriate for the firmware and hardware. – Load firmware appropriate for the safety or switch module, see order reference on the module.	
51-1	8092h	**Safety function: driver supply faulty**		PSoff
		Cause	Internal hardware error (voltage error) of the safety module or switch module.	
		Action	– Module presumably defective. If possible, replace with another module.	
		Cause	– Error in driver circuit section in the basic unit.	
		Action	– Basic unit presumably defective. If possible, replace with another basic unit.	
51-2	8093h	**Safety module: different module type**		PSoff
		Cause	Type or revision of the module does not match the project engineering.	
		Action	– Check whether correct module type and correct revision are being used. – With module replacement: module type not yet entered in project. Accept currently integrated safety or switch module.	
51-3	8094h	**Safety module: different module version**		PSoff
		Cause	Type or revision of the module is not supported.	
		Action	– Install safety or switch module appropriate for the firmware and hardware. – Load firmware appropriate for the module; see order reference on the module.	
		Cause	The module type is correct but the module revision is not supported by the basic unit.	
		Action	– Check module revision; if possible use module of same revision after replacement. Install suitable safety or switch module for the firmware and hardware. – If only a module with a more recent revision is available: load firmware that is appropriate for the basic unit; see order reference on the module.	

Error group 51		Safety module/function		
No.	Code	Message		Reaction
51-4	8095h	**Safety module: SSIO communication error**		PSoff
		Cause	Fault in internal communication connection between basic unit and safety module.	
		Action	– This error may occur if a CAMC-G-S3 was entered in the project for the basic unit but a different module type was plugged in. – Load firmware appropriate for the safety or switch module, see order reference on the module.	
51-5	8096h	**Safety module: brake control error**		PSoff
		Cause	Internal hardware error (brake actuation control signals) of the safety module or switch module.	
		Action	– Module presumably defective. If possible, replace with another module.	
		Cause	Error in brake driver circuit section in the basic unit.	
		Action	– Basic unit presumably defective. If possible, replace with another basic unit.	
51-6	8097h	**Safety module: different serial number**		PSoff
		Cause	Serial number of currently connected safety module is different from the saved serial number.	
		Action	Error only occurs after replacement of the CAMC-G-S3. – With module replacement: module type not yet entered in project. Migrate currently installed CAMC-G-S3 as accepted.	

Tab. 124

Error group 52		Safety function		
No.	Code	Message		Reaction
52-1	8099h	**CAMC-G-S1: safety function: STO discrepancy time exceeded**		PSoff
		Cause	– Control inputs STO-A and STO-B are not actuated simultaneously.	
		Action	– Check discrepancy time.	
		Cause	– Control inputs STO-A and STO-B are not wired in the same direction.	

Error group 52		Safety function		
No.	Code	Message		Reaction
52-1	8099h	Action	– Check discrepancy time.	
		Cause	Upper and lower switch supply not simultaneously activated (discrepancy time exceeded) – Error in control/external circuitry of safety module. – Error in the safety module.	
		Action	– Check circuitry of the safety module – are the STO-A and STO-B inputs switched off on two channels and simultaneously? – Replace safety module if a fault is suspected.	
52-2	809Ah	**Safety function: failure of driver supply with active PWM control**		PSoff
		Cause	This error message does not occur with devices supplied from the factory. It can occur when customer-specific device firmware is used.	
		Action	– The safe status was requested with power output stage enabled. Check integration into the safety-oriented interface.	
52-3	809Bh	**Safety module: overlapping rotational speed limits in the basic unit**		PSoff
		Cause	Basic unit reports error if the currently requested direction of movement is not possible because the safety module has blocked the setpoint value in this direction. Error may occur in connection with the SSFx safe speed functions if an asymmetrical speed window is used where one limit is set to zero. In this case, the error occurs if the basic unit travels in the blocked direction in the positioning operating mode.	
		Action	– Check application and modify if necessary.	

Tab. 125

Error group 53		Violation of safety conditions		
No.	Code	Message		Reaction
53-0	80A1h	**USF0: safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF0 in operation/when USF0/SSF0 requested.	

Error group 53		Violation of safety conditions		
No.	Code	Message		Reaction
53-0	80A1h	Action	Check when the violation of the safety condition occurs: a) during dynamic braking to safe rotational speed b) after the drive has reached the safe speed. – If a): critical check of braking ramp – record trace - can the drive follow the ramp? – Change parameters for the braking ramp or start time/delay times for monitoring. – If b): check how far the current speed is from the monitored limit speed; increase gap if necessary (parameter in safety module) or correct speed specified by controller.	
53-1	80A2h	**USF1: safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF1 in operation/when USF1/SSF1 requested.	
		Action	– see USF0, error 53-0.	
53-2	80A3h	**USF2: safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF2 in operation/when USF2/SSF2 requested.	
		Action	– see USF0, error 53-0.	
53-3	80A4h	**USF3: safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF3 in operation/when USF3/SSF3 requested.	
		Action	– see USF0, error 53-0.	

Tab. 126

Error group 54		Violation of safety conditions		
No.	Code	Message		Reaction
54-0	80AAh	**SBC: safety condition violated**		configurable
		Cause	– Brake should engage; feedback not received within the expected time.	

Error group 54		Violation of safety conditions		
No.	Code	Message		Reaction
54-0	80AAh	Action	– Check how the feedback signal is configured – was the correct input selected for the feedback signal? – Does the feedback signal have the correct polarity? – Check whether the feedback signal is actually switching. – Is the parameterised time delay for the evaluation of the feedback signal appropriate to the brake used (measure switching time if necessary).	
54-2	80ACh	**SS2: safety condition violated**		configurable
		Cause	– Actual speed outside permitted limits for too long.	
		Action	Check when the violation of the safety condition occurs: a) during dynamic braking to zero. b) after the drive has reached zero rotational speed. – If a): critical check of braking ramp – record trace - can the drive follow the ramp? Change parameters for the braking ramp or start time/delay times for monitoring. – If a): if the option “Trigger basic unit quick stop” is activated: critical check of the basic unit’s quick stop ramp. – If b): check whether the drive continues to oscillate after reaching the zero speed or remains at standstill and stable – increase monitoring allowable time if necessary. – If b): if the actual speed value is very noisy at rest. Check and if necessary adjust expert parameters for speed recording and detection of standstill.	
54-3	80ADh	**SOS: safety condition violated**		configurable
		Cause	– Angle encoder analysis reports “Motor running” (actual rotational speed exceeds limit). – Drive has rotated out of its position since reaching the safe state.	
		Action	– Check position tolerance for SOS monitoring and increase if necessary, if this is permissible. – If the actual speed value is very noisy when at rest: check and if necessary adjust expert parameters for speed recording and standstill detection.	
54-4	80AEh	**SS1: safety condition violated**		configurable
		Cause	– Actual speed outside permitted limits for too long.	

Error group 54		Violation of safety conditions		
No.	Code	Message		Reaction
54-4	80AEh	Action	Check when the violation of the safety condition occurs: a) during dynamic braking to zero. b) after the drive has reached zero rotational speed. – If a): critical check of braking ramp – record trace - can the drive follow the ramp? Change parameters for the braking ramp or start time/delay times for monitoring. – If a): if the option “Trigger basic unit quick stop” is activated: critical check of the basic unit’s quick stop ramp. – If b): check whether the drive continues to oscillate after reaching the zero speed or remains at standstill and stable – increase monitoring allowable time if necessary. – If b): if the actual speed value is very noisy when at rest: check and if necessary adjust expert parameters for speed recording and standstill detection.	
54-5	80AFh	**STO: safety condition violated**		configurable
		Cause	– Internal hardware error (voltage error) of the safety module.	
		Action	– Module presumably defective. If possible, replace with another module.	
		Cause	– Error in driver circuit section in the basic unit.	
		Action	– Basic unit presumably defective. If possible, replace with another basic unit.	
		Cause	– Feedback from the basic unit that the power stage has been switched off remains absent.	
		Action	– Check whether the error can be acknowledged and whether it occurs again upon a new STO request – if yes: basic unit is presumably faulty. If possible, replace with another basic unit.	
54-6	80B0h	**SBC: brake > 10 days without releasing**		configurable
		Cause	– Error occurs when SBC is requested and the brake has not been opened by the basic unit in the last 10 days.	
		Action	– If the brake is actuated via the brake driver in the basic unit [X6]: the brake must be energised at least once within 10 days before the SBC request, because the circuit breaker check can only be performed when the brake is switched on (energised). The brake must be energised for at least 20 s. – Only if brake control takes place via DOUT4x and an external brake controller: deactivate 10-day monitoring in the SBC parameters if the external brake controller allows this.	

Error group 54		**Violation of safety conditions**		
No.	Code	Message		Reaction
54-7	80B1h	**SOS: SOS requested > 10 days**		configurable
		Cause	– If SOS is requested for more than 10 days, the error is triggered.	
		Action	– Terminate SOS and move axis once during this time. The travel distance must be greater than one signal period of the measuring system.	

Tab. 127

Error group 55		**Measuring of actual value 1**		
No.	Code	Message		Reaction
55-0	80C1h	**Actual speed/position value not available or standstill for > 10 days**		configurable
		Cause	– Consecutive error if a position encoder fails. – Safety function SSF, SS1, SS2 or SOS requested and actual rotational speed value is not valid.	
		Action	– Check the function of the position encoder(s) (see following error).	
55-1	80C2h	**SINCOS encoder [X2B] - tracking signal errors**		configurable
		Cause	– Vector length $\sin^2+\cos^2$ outside the permitted range. – The amplitude of one of the two signals is outside the permissible range. – Offset between analogue and digital signal > 1 quadrant.	
		Action	Error may occur with SIN/COS and Hiperface encoders. – Check the position encoder. – Check the connection wiring (broken wire, short between two signals or signal/shielding). – Check the supply voltage for the position encoder. – Check the motor cable/shield support on motor and drive side – EMC malfunctions may trigger the error.	
55-2	80C3h	**SINCOS encoder [X2B] - standstill > 10 days**		configurable
		Cause	– Input signals of the SinCos encoder have not changed by a minimum value (at least one signal period) for 10 days with requested safety function.	
		Action	Terminate SS2 or SOS and move axis once during this time.	
55-3	80C4h	**Resolver [X2A] - signal error**		configurable

Error group 55		Measuring of actual value 1		
No.	Code	Message		Reaction
55-3	80C4h	Cause	– Vector length $\sin^2+\cos^2$ outside the permitted range. – The amplitude of one of the two signals is outside the permissible range. – Input signal is static (same values to right and left of maximum).	
		Action	– Check the resolver. – Check the connection wiring (broken wire, short between two signals or signal/shielding). – Check for failure of the exciter signal – Check the motor and encoder cable/shield support on motor and drive side. EMC malfunctions can trigger the error.	
55-4	–	**EnDat encoder [X2B] - sensor error**		configurable
		Cause	– Communication error between safety module and the ENDAT encoder. – Error message of the ENDAT encoder pending.	
		Action	– Check the ENDAT encoder. – Check the connection wiring (broken wire, short between two signals or signal/shielding). – Check the supply voltage for the ENDAT encoder – Check the motor cable/shield support for the motor and drive side – EMC malfunctions can trigger the error.	
55-5	–	**EnDat encoder [X2B] - incorrect sensor type**		configurable
		Cause	– Number of lines does not correspond to parameterisation. – Serial no. Does not correspond to parameterisation. – Encoder type does not correspond to parameterisation.	
		Action	– Check the parameterisation. – Use only approved encoders.	
55-6	80C5h	**Incremental encoder [X10] - signal error**		configurable
		Cause	– Faulty tracking signals from incremental encoder.	
		Action	– Check the connection wiring (broken wire, short between two signals or signal/shielding). – Check the motor cable/shield support on motor and drive side – EMC malfunctions may trigger the error.	
55-7	80C6h	**Other encoder [X2B] - faulty angle information**		configurable

Error group 55		Measuring of actual value 1		
No.	Code	Message		Reaction
55-7	80C6h	Cause	– “Angle faulty” message is sent from basic unit when status lasts for longer than the allowed time. – Encoder at X2B is evaluated by the basic unit, – Encoder is faulty.	
		Action	– Check the position encoder at X2B. – Check the connection wiring (broken wire, short between two signals or signal/shielding). – Check the supply voltage for the ENDAT encoder. – Check the motor cable/shield support on motor and drive side – EMC malfunctions may trigger the error.	
55-8	–	**Impermissible acceleration detected**		configurable
		Cause	– Error in connected position encoder. – EMC malfunctions affecting the position encoder. – Impermissibly high acceleration rates in the movement profiles. – Acceleration limit parameterised too low. – Angle jump after reference movement in the position data transmitted from the basic unit to the safety module.	
		Action	– Check the connected position encoder: if further error messages occur in conjunction with the encoders, then eliminate their cause first. – Check the motor and encoder cable/shield support on motor and drive side. EMC malfunctions can trigger the error. – Check the setpoint specifications/movement profiles of the controller: do they contain impermissibly high accelerations above the limit value for acceleration monitoring (P06.07)? – Check whether the limit value for acceleration monitoring was parameterised correctly - the limit value (P06.07) should be at least 30% ... 50% above the actual maximum acceleration. – In case of an angle jump in the position data transmitted from the basic unit - acknowledge error once.	

Tab. 128

Error group 56		Measuring of actual value 2		
No.	Code	Message		Reaction
56-8	80D1h	**Speed/angle difference encoder 1 - 2**		configurable
		Cause	– Rotational speed difference between encoders 1 and 2 of one µC outside the permissible range for longer than the allowed time. – Angle difference between encoders 1 and 2 of one µC outside the permissible range for longer than the allowed time.	
		Action	– Problem may occur if two position encoders are used in the system and they are not “rigidly coupled”. – Check for elasticity or looseness, improve mechanical system. – Adjust the expert parameters for the position comparison if this is acceptable from an application point of view.	
56-9	–	**Error cross-comparison encoder evaluation**		configurable
		Cause	Cross-comparison between µC1 and µC2 has detected an angle difference or rotational speed difference or difference in capture times for the position encoders.	
		Action	– Timing disrupted. If the error occurs against after a reset, the safety module is presumably faulty.	

Tab. 129

Error group 57		Input/output error		
No.	Code	Message		Reaction
57-0	80E1h	**Self test I/O error (internal/external)**		configurable
		Cause	– Error on the outputs DOUT40 … DOUT42 (detection via test pulses). – Internal error of digital inputs DIN40 ... DIN49 (via internal test signals). – Error at brake output at X6 (signalling, detected by test pulses). – Internal error of brake output (via internal test signals). – Internal error of digital outputs DOUT40 DOUT42 (via internal test signals).	

Error group 57		**Input/output error**		
No.	Code	Message		Reaction
57-0	80E1h	Action	– Check the connection wiring for the digital outputs DOUT40 ... DOUT42 (short circuit, cross circuit etc.). – Check the connection wiring for the brake (short circuit, cross circuit etc.). – Brake connection: the error may occur with relatively long motor cables if: 1. The brake output X6 was configured for the brake (this is the case with factory settings!) and 2. A motor without a holding brake is used and the brake connection lines in the motor cable are connected to X6. In this case: disconnect the brake connection lines at X6. – If there is no error in the connection wiring, there may be an internal error in the module (check by replacing the module).	
57-1	80E2h	**Digital inputs - signal level error**		configurable
		Cause	Exceeding/violation of discrepancy time with multi-channel inputs (DIN40 ... DIN43, two-handed control device, mode selector switch).	
		Action	– Check the external active and passive sensors – do they switch on two channels and simultaneously (within the parameterised discrepancy time). – Two-handed control device: check how the device is operated by the user – are both buttons pressed within the discrepancy time? Give training if necessary. – Check the set discrepancy times – are they sufficient?	
57-2	–	**Digital inputs - test pulse error**		configurable
		Cause	– One or more inputs (DIN40 ... DIN49) were configured for the evaluation of the test pulses of the outputs (DOUT40 ... DOUT42). The test pulses from DOUTx do not arrive at DIN4x.	
		Action	– Check the wiring (shorts after 0 V, 24 V, cross circuits). – Check the allocation – correct output selected/configured for test pulse?	
57-6	–	**Electronic temperature too high**		configurable

Error group 57		Input/output error		
No.	Code	Message		Reaction
57-6	–	Cause	– The safety module temperature monitoring has been triggered; the temperature of µC1 or µC2 was below -20° or above +75°C.	
		Action	– Check the operating conditions (ambient temperature, control cabinet temperature, installation situation in the control cabinet). – If the motor controller is experiencing high thermal load (high control cabinet temperature, high power consumption/output to motor, large number of occupied slots), a motor controller of the next higher output level should be used.	

Tab. 130

Error group 58		Error during communication/parameterisation		
No.	Code	Message		Reaction
58-0	80E9h	**Plausibility check parameters**		configurable
		Cause	The plausibility check in the safety module returned errors, e.g. an invalid angle encoder configuration; the error is triggered if a validation code is requested by the SafetyTool and if parameters are backed up in the safety module.	
		Action	– Note SafetyTool information for complete validation; check parameterisation closely.	
58-1	–	**General parameterisation error**		configurable
		Cause	Parameterisation session active for > 8 hrs. The safety module has thus terminated the parameterisation session The error message is saved in the diagnostic memory.	
		Action	– Terminate parameterisation session within 8 h. If necessary, start a new parameterisation session and continue.	
58-4	80E9h	**Buffer internal communication**		Fixed [8]
		Cause	– Communication connection faulty. – Timeout/data error/incorrect sequence (packet counter) in data transfer between basic unit and safety module. – Too much data traffic, new requests are being sent to safety module before old ones have been responded to.	

Error group 58		Error during communication/parameterisation		
No.	Code	Message		Reaction
58-4	80E9h	Action	– Check communication interfaces, wiring, shield etc. – Check whether other devices have read access to the motor controller and safety module during a parameterisation session - this may overload the communication connection. – Check whether the firmware versions of the safety module and basic unit and the versions of the FCT plug-in and SafetyTool are compatible.	
58-5	80EAh	**Communication safety module - basic unit**		Fixed [8]
		Cause	– Packet counter error during transmission µC1 ←➔ µC2. – Checksum error during transmission µC1 ←➔µC2.	
		Action	– Internal malfunction in the motor controller. – Check whether the firmware versions of the safety module and basic unit and the versions of the FCT plug-in and SafetyTool are compatible.	
58-6	80EBh	**Cross-comparison error processors 1 - 2**		Fixed [8]

Error group 58		Error during communication/parameterisation		
No.	Code	Message		Reaction
58-6	80EBh	Cause	Timeout during cross-comparison (no data) or cross-comparison faulty (data for µC1 and µC2 are different). – Error in cross-comparison for digital I/O. – Error in cross-comparison for analogue input. – Error in cross-comparison for internal operating voltage measurement (5 V, 3.3 V, 24 V) and reference voltage (2.5 V). – Error in cross-comparison for SIN/COS angle encoder analogue values. – Error in cross-comparison for programme sequence monitoring. – Error in cross-comparison for interrupt counter. – Error in cross-comparison for input map. – Error in cross-comparison for violation of safety conditions. – Error in cross-comparison for temperature measurement.	
		Action	This is an internal error in the module that should not occur during operation. – Check the operating conditions (temperature, humidity, condensation). – Check the EMC wiring as specified and shield design; are there any external interference sources? – Safety module may be faulty – is error eliminated after replacing the module? – Check whether new firmware for the motor controller or a new version of the safety module is available from the manufacturer.	

Tab. 131

Error group 59		Internal safety module error		
No.	Code	Message		Reaction
59-1	80F1h	**Fail-safe power supply/safe pulse inhibitor**		Fixed [8]
		Cause	– Internal error in module in fail-safe power supply circuit section or in the driver supply for the upper and lower switches.	
		Action	– Module faulty, replace.	
59-2	80F2h	Cause	– Reference voltage 2.5 V outside tolerance. – Logic supply overvoltage +24 V detected.	
		Action	– Module faulty, replace.	
59-3	80F3h	**Internal power supply error**		Fixed [8]
		Cause	– Voltage (internal 3.3 V, 5 V, ADC reference) outside permissible range.	

Error group 59		Internal safety module error		
No.	Code	Message		Reaction
59-3	80F3h	Action	– Module faulty, replace.	
59-4	80F4h	**Error management: too many errors**		Fixed [8]
		Cause	– Too many errors have occurred simultaneously.	
		Action	– Clarify: what is the status of the installed safety module - does it contain a valid parameter set? – Read out and analyse the log file of the basic unit via FCT. Eliminate causes of error step by step. – Install safety module with “delivery status” and perform commissioning of basic unit. – If this is not available: reset safety module to factory settings, then copy data from the basic unit and perform complete validation. Check whether the error occurs again.	
59-5	80F5h	**Diagnostic memory writing error**		Fixed [8]
		Cause	Consecutive error if internal communication is disrupted. – Basic unit not ready for operation, faulty or memory error.	
		Action	– Check the function of the basic unit – Generate an error in the basic unit, e.g. by unplugging the position encoder, and check whether the basic unit writes an entry to the log file. – Module or basic unit faulty; replace.	
59-6	80F6h	**Error saving parameter set**		Fixed [8]
		Cause	– Voltage interruption/power off while parameters were being saved.	
		Action	– Maintain a power supply of 24 V throughout the parameterisation session. – Once the error has occurred, parameterise the module again and validate the parameter set again.	
59-7	80F7h	**FLASH checksum error**		Fixed [8]
		Cause	– Voltage interruption/power off while parameters were being saved. – FLASH memory in safety module corrupted (e.g. by extreme malfunctions).	
		Action	Check whether the error recurs after a reset. If it does – parameterise the module again and validate the parameter set again. If error persists: – Module faulty, replace.	
59-8	80F8h	**Internal monitoring processor 1 - 2**		Fixed [8]

Error group 59		Internal safety module error		
No.	Code	Message		Reaction
59-8	80F8h	Cause	– Serious internal error in the safety module: error detected during dynamisation of internal signals – Disrupted programme sequence, stack error or OP code test failed, processor exception/interruption.	
		Action	Check whether the error recurs after a reset. If it does – Module faulty, replace.	
59-9	80F9h	**Other unexpected error**		Fixed [8]
		Cause	Triggering of internal programme sequence monitoring.	
		Action	– Check the firmware version of the basic unit and the version of the safety module – update available? – Safety module faulty; replace.	

Tab. 132

7 Maintenance, repair, replacement, disposal

7.1 Maintenance

The safety module does not contain any parts requiring maintenance.

7.2 Repair

ⓘ

Repair or maintenance of the safety module is not permissible. If necessary, replace the entire safety module.

- Always replace the safety module in the event of an internal fault.
- Send the unchanged, faulty safety module with a description of the error and the application back to Festo for analysis.
- Please contact your technical consultant to discuss the return.

7.3 Replacement of the safety module

If a safety module fails and has to be replaced, organisational measures must be taken to ensure that an unsafe status is not created. To do this,

- the safety module must not be replaced by another module type without safety function (switch module).
- the safety module must not be replaced by another module type with reduced function range (CAMC-G-S3 for CAMC-G-S1).
- the revision status of the new safety module must match or be compatible with that of the old safety module.
- the parameterisation of the new safety module must match the parameterisation of the faulty safety module.

ⓘ

The order reference of the safety module and the revision status can be found on the rating plate
➔ Product identification.

Observe required organisational measures to avoid errors when replacing the module.
For example, always generate a new validation report due to the different serial number of the safety module and the new validation code.

7.3.1 Disassembly and installation

Prior to a module replacement, the compatibility between the safety module and basic unit must be checked, see also ➔ “Versions” at the front of this document.

ⓘ

For information on removing and installing the safety module, see Safety module assembly/disassembly ➔ 4.1 Mounting/removal.

Tip: if the safety module to be replaced can be addressed from the SafetyTool, we recommend saving a safe parameter set from the validated actual status (start SafetyTool in online mode - display parameterisation - then create safe parameter set).

7.3.2 Accept safety module

After replacing the module, the new safety module must first be accepted in the FCT CMMP-AS plug-in.

ⓘ

Accept the serial number of the replaced safety module ➔ 5.3.4 Accepting the safety module.

7.3.3 Recommissioning with the SafetyTool

After accepting the replaced safety module, you must transfer the desired parameterisation to the safety module and then validate it.

ⓘ

Basic information can be found in the following sections:
SafetyTool ➔ 5.5 Safe parameterisation with the SafetyTool
Parameterisation ➔ 5.4 Basic principles for parameterisation of the safety module
Function test and validation ➔ 5.8 Function test, validation

To do this, you must first start the SafetyTool in online mode.
You then have the following options, depending on the data available from the safety module that is to be replaced:
a) Safe parameter set is available for the safety module that is to be replaced:
- Open the parameter set in the SafetyTool and upload it to the safety module. This requires that the basic information of the basic unit matches that of the parameter set.

b) A saved SafetyTool project is available that conforms to the parameterisation:
- Set the safety module to the factory setting if it is not in the delivery status.
- Open the SafetyTool project.
- The basic information of the basic unit must match. Otherwise they must be synchronised.
- You can then validate the individual parameter screens and upload them to the safety module.

c) If there is no safe data available for the safety module that is to be replaced:
- Set the safety module to the factory setting if it is not in the delivery status.
- Then proceed as for initial commissioning.

Regardless of variant a), b) or c), you must generate a new validation report with a new validation code and new serial number for the safety module.

7.4 Decommissioning and disposal

Observe the information for removal of the safety module ➔ 4.1 Mounting/removal.

Disposal

Observe the local regulations for environmentally appropriate disposal of electronic modules. The safety module is RoHS-compliant.
The material used in the packaging has been specifically chosen for its recyclability.

8 Technical appendix

8.1 Technical data

8.1.1 Safety engineering

Approval information, safety engineering	
CE	
Type-examination	The functional safety engineering of the product has been certified by an independent testing body, see EC-type examination certificate ➔ www.festo.com/sp
Certificate issuing authority	TÜV Rheinland, Certification Body of Machinery, NB 0035
Certificate no.	01/205/5165.03/24

Tab. 133: Approval information, safety engineering

The following table contains the maximum attainable classification. Restrictions are dependent on the safety function ➔ 2.1.4 Achievable safety level/safety function in accordance with EN ISO 13849-1/EN 61800-5-2 and ➔ 8.2 Safety reference data.

Safety reference data			
Safety functions according to EN 61800-5-2		STO	Safe Torque Off
		SS1	Safe Stop 1
		SS2	Safe Stop 2
		SOS	Safe Operating Stop
		SLS	Safely Limited Speed
		SSR	Safe Speed Range
		SSM	Safe Speed Monitor
		SBC	Safe Brake Control
Values in accordance with EN 61800-5-2			
SIL		SIL 3	Safety integrity level
PFH	[h^{-1}]	9.5×10^{-9}	Probability of a dangerous random hardware failure per hour
DC	[%]	97.5	Diagnostic coverage
HFT		1	Hardware fault tolerance
SFF	[%]	99.5	Safe failure fraction
T	[years]	20	Proof Test Interval
Values in accordance with EN 62061			

Safety reference data			
SIL		SIL CL 3	SIL claim limit for a subsystem
PFH_D	[h^{-1}]	9.5×10^{-9}	Probability of dangerous failure per hour
DC	[%]	97.5	Diagnostic coverage
HFT		1	Hardware fault tolerance
SFF	[%]	99.5	Safe failure fraction
T	[years]	20	Proof Test Interval
Values in accordance with EN 61508			
SIL		SIL 3	Safety integrity level
PFH	[h^{-1}]	9.5×10^{-9}	Average frequency of dangerous failure
DC	[%]	97.5	Diagnostic coverage
HFT		1	Hardware fault tolerance
SFF	[%]	99.5	Safe failure fraction
T	[years]	20	Proof test interval
Values according to EN ISO 13849-1			
Category		4	Category
Performance Level		PL e	Performance level
PFH		9.5×10^{-9}	Average probability of a dangerous failure per hour
DC		97.5	Diagnostic coverage
$MTTF_d$		8700	Mean time to dangerous failure
T_M		20	Mission time

Tab. 134: Technical data: safety reference data

Safety specifications	
Well-tried component	Yes

Tab. 135: Technical data: safety specifications

8.1.2 General

Mechanical system		
length/width/height	[mm]	112.2 x 99.1 x 28.7
Weight	[g]	220

Mechanical system	
Slot	Slot Ext3 for safety modules
Note on materials	RoHS-compliant

Tab. 136: Technical data: mechanical

Approvals (safety module CAMC-G-S3 for motor controller CMMP-AS-...-M3)	
Certificates, declaration of conformity	➔ www.festo.com/sp
The device is intended for use in an industrial environment. Measures for interference suppression may be required in residential areas.	

Tab. 137: Technical data: approvals

8.1.3 Operating and environmental conditions

Transport		
Temperature range	[°C]	–25 ... +70
Humidity	[%]	0 ... 95, at max. 40 °C ambient temperature
Maximum transportation duration		maximum 4 weeks over the entire product lifecycle

Tab. 138: Technical data: transport

Storage		
Storage temperature	[°C]	–25 ... +55
Humidity	[%]	5 ... 95, non-condensing or protected against condensation
Permissible altitude	[m]	< 3000 (above sea level)[1)]

1) Note additional limitations, such as the permissible setup altitude for the motor controller (usually < 2000 m above mean sea level)

Tab. 139: Technical data: storage

Ambient conditions CMMP-AS-...-M3 with safety module CAMC-G-S3 in Ext3					
CMMP-AS-...		C2-3A-M3	C5-3A-M3	C5-11A-P3-M3	C10-11A-P3-M3
Ambient temperature[1)]	[°C]	0 ... +35	0 ... +40	0 ... +40	0 ... +40
		+35 ... +40	+40 ... +50	+40 ... +50	+40 ... +45
Ambient temperature with power reduction[)]	[°C]	An overtemperature switch-off will take place if the power output of the basic unit and/or the load of the control unit and the I/Os is too high.			
Cooling		Via the ambient air in the motor controller, no forced ventilation			

Ambient conditions CMMP-AS-...-M3 with safety module CAMC-G-S3 in Ext3					
CMMP-AS-...		C2-3A-M3	C5-3A-M3	C5-11A-P3-M3	C10-11A-P3-M3
Humidity	[%]	0 ... 90 (non-condensing).			
		No corrosive media permitted in the environment of the device.			
Permissible setup altitude above mean sea level					
at nominal power	[m]	1000			
with power reduction	[m]	1000 ... 2000			
Degree of protection		IP20 (mounted in the CMMP-AS-...-M3).			
Vibration/shock		Requirements of EN 61800-5-1 and EN 61800-2 are fulfilled.			

1) The maximum permissible operating temperature depends on a wide range of parameters, including the number of switched inputs and the load of the outputs in the CAMC-G-S3, the presence of additional modules in EXT1 and EXT2 in the CMMP-AS-M3, the load on the power output stage in the CMMP-AS-M3 and also the air flow conditions in the control cabinet. The specified values apply to a typical device configuration. The CAMC-G-S3 has separate temperature monitoring, which switches the safety module and the basic unit off if the electronics temperature becomes too high (error 57-6).

Tab. 140: Technical data: ambient conditions

Electrical operating conditions		
Galvanically isolated potential areas		Control voltage of the basic unit
		24 V control voltage (all inputs and outputs)
		Potential-free signal contact C1/C2
System voltage	[V]	< 50 (24V PELV power supply in accordance with EN 60204-1)
		The 24 V fixed power supply unit used must be able to handle the voltage interruption defined in EN 60204-1.
System voltage		3
Pollution degree in accordance with EN 61800-5-1		2
		It must always be ensured by taking appropriate measures, e.g. by installation in a control cabinet.

Tab. 141: Technical data: electrical operating conditions

EMC operating conditions	
Immunity to interference	Requirements for “second environment” in accordance with EN 61800-3 (PDS of category C3) Requirements in accordance with EN 61326-3-1
Interference emission	Requirements for “first environment with restricted availability” in accordance with EN 61800-3 (PDS of category C2)

Tab. 142: Technical data: EMC operating conditions

8.1.4 Digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40]

Digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49[1]		
Input		Type 3 in accordance with IEC 61131-2
Nominal voltage	[V DC]	24
Permissible voltage range	[V]	-3 … 30
Maximum input voltage “HI” $U_{H,max}$	[V]	30
Minimum input voltage “HI” $U_{H,min}$		
typical	[V]	11
maximum	[V]	13[2]
Maximum input voltage “LO” U_{Lmax}	[V]	5
Minimum input voltage “LO” $U_{L,min}$	[V]	–3
Maximum input current “HI” $I_{H,max}$	[mA]	15
Minimum input current “HI” $I_{H,min}$	[mA]	2
Maximum input current “LO” $I_{L,max}$	[mA]	15
Minimum input current “LO”} “HI” $IT_{,min}$	[mA]	1.5[3]
Switching delay to port pin (Low-High transition)	[ms]	< 1
Tolerance for test pulses	[ms]	0 … 10 (parameterisable ➔ 3.4.2 Two-channel safe inputs DIN40 … DIN43 [X40] and ➔ 3.4.3 Single-channel (partially safe) digital inputs DIN44 … DIN49 [X40])

1) Data designations according to IEC 61131-2
2) Taking all the tolerances in the series into account, the minimum required input voltage UH, min = 13 V, which deviates from the requirement of IEC 61131.
3) The compliance of IT, min cannot be tested in the context of self-diagnostics. When using active two-wire sensors on DIN40A/B… DIN43A/B to request safety functions, cyclical tests are required (every 24 h).

Tab. 143: Technical data: digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40]

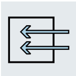


Fig. 103: Input, two-channel

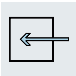


Fig. 104: Input, single-channel

The digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 comply with the EMC requirements of EN 61326-3-1.

8.1.5 Digital outputs DOUT40A/B to DOUT42A/B [X40]

Digital outputs DOUT40A/B to DOUT42A/B		
Output		High-side switch with pull-down
Voltage range	[V DC]	18 … 30
Permissible output current $I_{L,nom}$ (nominal)	[mA]	< 50
Voltage loss at $I_{L,nom}$	[V]	≤1 V
Residual current with switch OFF[1]	[µA]	< 100 µA
Pull down resistor $R_{pull down}$	[kΩ]	< 50 (approx. 0.6 mA at 24 V)
Short circuit/overcurrent protection		Short circuit-proof, feedback-proof, overvoltage-resistant up to 60 V
Temperature protection		Shutdown of all outputs of a group (DOUT40A to DOUT42A or DOUT40B to DOUT42B) in the event of overtemperature T_J > 150°
Supply		Protection against inductive loads
Loads		
Resistive load	[Ω]	> 500
Inductive load	[mH]	< 10
Capacitive load[2]	[nF]	< 10

Digital outputs DOUT40A/B to DOUT42A/B		
Switching delay from port pin	[ms]	< 1
Test pulse output	[ms]	0.4 … 10 (parameterisable ➔ 3.9.1 Two-channel safe outputs DOUT40 ... DOUT42 [X40])

1) In specific error cases (e.g. device-internal interruption of the 24 V reference potential), the residual current may still be considerably above 100 µA. If the output is connected to an IEC 61131-compatible Type 3 input, the range of the Low status is not violated, even if there is an error.

2) Requires connection of the output to a Type 3 input and a test pulse length ≥ 400 µs. Longer test pulses may be required for other input types.

Tab. 144: Technical data: digital outputs DOUT40A/B to DOUT42A/B [X40]

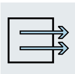


Fig. 105: Output, two-channel

The digital outputs DOUT40A/B to DOUT42A/B comply with the EMC requirements in accordance with EN 61326-3-1.

8.1.6 Signal contact C1/C2 [X40]

Signal contact C1/C2		
Design		Relay contact, N/O contact
Voltage range	[V DC]	18 … 30
Output current $I_{L,nom}$ (nominal)	[mA]	< 200
Voltage loss at $I_{L,nom}$	[V]	≤ 1
Residual current with switch OFF	[µA]	< 10
Short circuit/overcurrent protection		Not short-circuit-proof, overvoltage-proof up to 60 V
Switching delay	[ms]	< 20
Service life of feedback contact	[n_{op}]	10×10^6 (at 24 V and $I_{contact}$ = 10 mA; the service life is reduced at higher load currents)

Tab. 145: Technical data: signal contact C1/C2 [X40]

8.1.7 24 V auxiliary power supply [X40]

24 V auxiliary power supply		
Design		Logic supply voltage routed via the motor controller (fed in at [X9], not additionally filtered or stabilised). Reverse-polarity protected, overvoltage-proof up to 60 V DC
Nominal voltage	[V]	24
Output current $I_{L,nom}$ (nominal)	[mA]	100
Voltage loss at $I_{L,nom}$		≤ 1
Reverse polarity protection		Via series diode 100 V/1 A
Short circuit/overcurrent protection		Protective PTC with tripping current typ. 300 mA, overvoltage-resistant up to 60 V

Tab. 146: Technical data: 24 V auxiliary supply [X40]

8.1.8 Design of the connecting cable [X40]

Cabling [X40]		
Max. cable length	[m]	< 30
Max. cable length		Use shielded cable for wiring outside the control cabinet. Guide shielding into the control cabinet/attach to the side of the control cabinet
Conductor cross section (flexible conductors, wire end sleeve with insulating collar)		
one conductor	[mm²]	0.25 … 0.5
two conductors	[mm²]	2 x 0.25 (with twin wire end sleeves)
Tightening torque of mating plug MC1.5_12ST3.81BK – M2	[Nm]	0.22 … 0.25

Tab. 147: Technical data: cabling [X40]

8.1.9 Digital output for a holding brake on the basic unit [X6]

Digital output BR+/BR-		
Output		High-side switch for BR + Low-side switch for BR-
Voltage range	[V DC]	18 … 30
Permissible output current $I_{L,nom}$ (nominal)	[mA]	< 2000

Digital output BR+/BR-		
Voltage loss at $I_{L,nom}$	[V]	≤ 1 V
Pull down resistor $R_{pull\ down}$	[kΩ]	Approx. 2.5 (approx. 10 mA at 24 V) between BR + and BR-
Short circuit/overcurrent protection		Short circuit proof to 24 V, 0 V and PE
Temperature protection		Switch-off of the power driver in event of overtemperature
Supply		Protection against inductive loads
Loads		
Resistive load	[Ω]	> 12
Inductive load	[mH]	< 1000
Capacitive load	[nF]	< 10
Switching delay from port pin	[ms]	< 1
Test pulse output	[ms]	0.4 … 10 (parameterisable ➔ 3.9.2 Internal brake control of the motor controller [X6])

Tab. 148: Technical data: digital outputs for a holding brake [X6]

The digital output of the basic unit for a holding brake, BR +, BR-, corresponds to the EMC requirements in accordance with EN 61326-3-1.

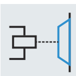


Fig. 106: Holding brake

NOTICE

When the safety module is delivered, the SBC function is always configured in conjunction with the output [X6], even if you do not wish to use the SBC function.
In the following application, an interference coupling into the open brake lines can cause the safety module to report error 57-0:

- The brake control cables are routed in the motor cable.
- A holding brake is not connected on the motor side.

In this case:

- Disconnect brake control cables at [X6]
- Connect brake control cables to [PE].

8.2 Safety reference data

8.2.1 Safety functions

Allocation of safety function - classification

The following table shows the classification of the safety functions in accordance with EN 61800-5-2

Function	Cat., PL[1]	SIL[2]	Note
STO	Cat. 4, PL e	SIL 3	–
SBC			–
SS2	Cat. 3, PL d or Cat. 3, PL e	SIL 2 or SIL 3	The classification is dependent on the combination of position encoders used. When a single encoder is used with SIL classification, a safe shaft connection is required; depending on the encoder configuration, only Cat. 3, PL d or SIL 2 is achieved ➔ 8.2.3 Encoder systems. Note that the accuracy of position detection is limited ➔ 8.3 System precision and reaction time.
SS1			
SLS			
SSR			
SSM			
SOS			

1) Classification category and performance level according to EN ISO 13849-1

2) Safety Integrity Level classification according to EN 62061

Tab. 149: Classification of the safety functions and notes

ⓘ

Some of the information on selected, prequalified encoder combinations is available separately. Please consult your regional Festo contact as necessary.

ⓘ

For a “safe shaft connection”, fault exclusion is achieved e.g. using positive-locking and/or appropriately overdimensioned attachment elements.

Take the whole drive train up to the location of the hazard into account.

ⓘ

If the movement of the motor shaft is monitored solely by a single rotary or linear encoder with a two-channel structure, then it must have a certificate from a notified body relating to the desired degree of risk reduction.

ⓘ

When using two encoders, the resolution limit for the motion detection for the safety functions is specified by the encoder with the lower resolution limit.

Position encoders used for standstill position monitoring, e.g. SOS, and that show static output signals at standstill require dynamisation by the user, i.e. the drive must be moved once within every 10 day period.

The safe brake control of the CAMC-G-S3 is designed for SIL 3/EN 61800-5-2. Please check whether the clamping unit in use achieves PL e corresponding to SIL 3. The clamping unit itself usually has a lower classification, meaning that the safety function SBC, in combination with the clamping unit, only achieves the lower classification.

8.2.2 Digital inputs

The relevant standards for command devices which request safety functions must be observed, e.g. EN ISO 13850 for emergency stop.

Sensor type	Switch type	Classification category, PL[1)]	Classification SIL[2)]
1: General 2-channel input	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
2: Emergency stop switching device	2 N/C contacts	Cat. 4, PL e	SIL 3
3: Enabling button	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
4: Two-handed operator unit	2: 1 N/C contact 1 N/O contact	Cat. 4, PL e	SIL 3
5: Start button	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
6: Door lock	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
7: Reliable reference switch	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
8: Light curtain	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
9: Brake feedback	1 N/C contact or 2 N/C contacts	only as feedback for SBC	

Sensor type	Switch type	Classification category, PL[1]	Classification SIL[2]
10: General single-channel input	1 N / C contact or 1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Cat. 2, PL d	SIL 2
11: Mode selector switch	1 of n	Cat. 4, PL e	SIL 3
12: Acknowledge errors	1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Cat. 2, PL d	SIL 2
13: Terminate safety function	1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Kat. 2, PL d	SIL 2

1) according to EN ISO 13849-1
2) according to EN 61800-5-2

Tab. 150: Safety reference data for digital inputs

NOTICE

- The following data on measures and DC is based on the specifications of EN ISO 13849-1.
- The manufacturer's specifications must be used for safety engineering assessment of the sensors.
- The listed DC values are only valid if the specified measures and the specified additional conditions are in compliance.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

Measure	DC	Comment	Use
Cyclical test pulse created by dynamically changing the input signals	90	Only effective if allocation of test pulses is active.	Cross-circuit monitoring for 1-channel sensors
Cross-comparison of input signals with dynamic test if short circuits cannot be detected (for multiple inputs/outputs)	90	Without allocation of test pulses. Cyclical change of input signals required, e.g. by the process or regular actuation.	Monitoring 2-channel sensors

Measure	DC	Comment	Use
Cross-comparison of input signals with immediate and intermediate results in the logic (L) and time-based and logic program sequence monitoring and detection of static failures and short circuits (for multiple inputs/outputs).	99	Only with allocation of test pulses	Monitoring 2-channel sensors
Plausibility check, e.g. use of normally open and normally closed contacts.	99	Only when using antivalent signals	Monitoring 2-channel sensors

Tab. 151: Measures for digital inputs

8.2.3 Encoder systems

The relevant standards for the functional safety of electrical drives must always be observed, e.g. EN 61800-5-2.

The following table shows the approved encoder combinations and the maximum achievable Performance Level and Safety Integrity Level.

P06.00: selection of position encoder 1	P06.01: selection of position encoder 2	Information	Achievable safety level	
			EN 61800-5-2	ISO 13849
Resolver (X2A)= [1]	Other encoder (X2B) = [4][1)]	–	SIL 3	Cat. 3/PL d or Cat. 3/PL e
Resolver (X2A)= [1]	Incremental encoder [X10] = [5]	–	SIL 3	Cat. 3/PL e
Resolver (X2A)= [1]	None = [6]	Requires a safe shaft connection. Resolver must satisfy the SIL 2 requirements (MTTFd value, etc.)	SIL 2	Cat. 3/PL d
SINCOS/Hiperface (X2B) = [2]	Incremental encoder [X10] = [5]	–	SIL 3	Cat. 3/PL e
SINCOS/Hiperface (X2B) = [2]	None = [6]	Requires a safe shaft connection. Requires a SIL 2-certified encoder	SIL 2	Cat. 3/PL d
SINCOS/Hiperface (X2B) = [2]	None = [6]	Requires a safe shaft connection. Requires a SIL 3-certified encoder	SIL 3	Cat. 3/PL e

P06.00: selection of position encoder 1	P06.01: selection of position encoder 2	Information	Achievable safety level	
			EN 61800-5-2	ISO 13849
EnDat SIL (X2B) = [3]	Incremental encoder [X10] = [5]	Not a part of PS1	SIL 3	Cat. 3/PL e
EnDat SIL (X2B) = [3]	None = [6]	Not a part of PS1. Requires a safe shaft connection. Requires a SIL 2-certified encoder	SIL 2	Cat. 3/PL d
EnDat SIL (X2B) = [3]	None = [6]	Not a part of PS1. Requires a safe shaft connection. Requires a SIL 3-certified encoder	SIL 3	Cat. 3/PL e
Other encoder (X2B) = [4][1)]	Incremental encoder [X10] = [5]	Please note the following.	SIL 2	Cat. 3/PL d
Other encoder (X2B) = [4][1)]	None = [6]	Invalid, is blocked by the CAMC-G-S3 and Safety Tool	–	–

1) Other encoder (X2B) = [4]: EnDat encoder without SIL certification, BISS encoder, incremental encoder with A/B/N signals, incremental encoder with SINCOS signals, Hiperface encoder without SIL

Tab. 152: Safety reference data for evaluation of encoder systems

NOTICE

The actually achievable safety level for the system, consisting of CAMC-G-S3, motor, axis and possibly a second position encoder, must be calculated using the safety reference data of the CAMC-G-S3 ➔ 8.1.1 Safety engineering and the safety reference data of the remaining components.
Please consult your regional Festo contact if you required precalculated application suggestions.

Note the additional information:

- General information on encoder analysis and the supported position encoders ➔ 3.2.5 Overview of supported position encoders
- Information on the encoder configuration ➔ 3.3.2 Configuration of the encoders
- Example of encoder configuration in the SafetyTool ➔ 5.6.4 Checking the data migration

NOTICE

The suitability of the “standard encoder” and the “digital incremental encoder” for use in safe systems up to SIL3 (EN 61800-5-2, EN 61508) as well as PL e (EN ISO 13849) must be confirmed separately (for example, diversity of encoder systems with regard to CCF, $MTTF_d$ etc. and suitability of the encoders for the operating and ambient conditions, EMC, etc.).

NOTICE

- The following information on measures and DC is based on the data of EN 61800-5-2, table in Appendix D.16.
- The manufacturer's specifications must also always be used for a safety engineering assessment of the position encoder.
- The DC values given for the evaluation of the encoder systems in the safety module are only valid if the specified measures and the specified additional conditions are in compliance.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

SIN/COS encoder/Hiperface encoder

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2)]
Interruption of any conductor of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2)]
Static “0” or “1” signal at inputs and outputs, individually or simultaneously at multiple inputs/outputs	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2)]
Interruption or high-impedance status on a single input/output or multiple inputs/outputs simultaneously	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2)]
Reduction or increase of the output amplitude	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Parasitic oscillation at one or more outputs	None	Individual signal monitoring and vector length monitoring[1]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2] If a signal oscillates, maximum motor movement in the tolerance window of the amplitude monitoring
Change of phase shift between output signals	None	Individual signal monitoring and vector length monitoring[1]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2] e.g. by a soiled encoding disc
Mounting becomes loose at standstill: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Required! According to the manufacturer's data sheet for the encoder	Not possible safely! However, the period of the SOS request is monitored: A switch-off and error message occur after 10 days	Use fault exclusion for the motor-encoder system, or a second measuring system for position comparison.
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)			
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2]
Additional requirements for rotary encoders with sin/cos output signals, analogue signal generation			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Static signal at inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2]
Change in the signal shape	None	Individual signal monitoring and vector length monitoring[1]	In accordance with ➔ 8.3 System precision and reaction time; DC › 90%[2]
Swapping of the sin and cos output signal	Yes	Safety module has sufficiently separated signal processing without multiplexer	–
Supplementary requirements for shaft encoders with incremental and absolute signals			
Simultaneous incorrect position change of incremental and absolute signal	None	None, the safety module only evaluates the analogue sin/cos signals	With Hiperface interface only: the basic unit runs a cyclical plausibility check by cross-comparison of the sin/cos signals with the absolute position read via the data interface.
Supplementary requirements for rotary encoders with synthetically generated output signals			
Any falsification of the output signal	None	Not possible in all cases if both output signals are falsified simultaneously.	Use fault exclusion for the encoder, or a second measuring system for position comparison.
Supplementary requirements for linear encoders			
Mounting of read head broken	Required! According to the manufacturer's data sheet for the encoder	Not possible safely! However, the duration of the SOS request is monitored: after 10 days, the function is switched off and an error message appears.	Use fault exclusion for the motor-encoder system, or a second measuring system for position comparison.
Static offset of the material measure (e.g. visual code strip)			
Damaged material measure (e.g. visual code strip)			
Supplementary requirements for evaluation of SIL position encoders			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Supply voltage monitoring of the encoder	None	Not present. This must be ensured at the encoder.	The basic unit includes regulation of the supply voltage for the encoder. In the case of a fault (overvoltage, overcurrent), the encoder supply can be switched off functionally.
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder.	The basic unit has an input for monitoring the motor temperature. In the case of fault, the drive can be switched off functionally.

1) Sensitivity and DC dependent on the parameterised error limits; specification applies to factory setting

2) Position information is "static" if there is a fault => fixed commutating position, motor at standstill/voltage of a channel static => commutating position changes by max +/-90° of a signal period of the encoder, motor only moves in this range

Tab. 153: SIN/COS encoder, Hiperface encoder

Classification of the safety module in conjunction with the SIN/COS encoder, Hiperface encoder:
Detection of encoder fault: DC › 90%
Classification in accordance with EN 61800-5-2/EN 13849-1:

- SIL2/Cat. 3/PL d (safe positioning incl. standstill)
- SIL3/Cat. 3/PL e (safe speed and acceleration)

Resolver

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Interruption of any conductor of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Static "0" or "1" signal at inputs and outputs, individually or simultaneously at multiple inputs/outputs	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Interruption or high-impedance status on a single input/output or multiple inputs/outputs simultaneously	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reduction or increase of the output amplitude	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Parasitic oscillation at one or more outputs	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Change of phase shift between output signals	None	Not applicable for resolver	–
Mounting becomes loose at standstill: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Required! According to the manufacturer's data sheet for the encoder	Not possible safely! However, the duration of the SOS request is monitored: after 10 days, the function is switched off and an error message appears	Use fault exclusion for the motor-encoder system, or a second measuring system for position comparison.
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)	None	Not applicable for resolver	–
No light from transmitter diode	None	Not applicable for resolver	–
Supplementary requirements for resolvers with signal processing/reference generator			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
– Central timer fails – No Conversion Start for analogue-digital converter – Sample & Hold occurs at the wrong time	None	Failure monitoring of the SYNC signal	Error is reliably detected (DC_{AV} of the safety module)
Analogue-digital converter generates incorrect values	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Analogue-digital converter does not generate values	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reference generator does not supply frequency	None	Failure monitoring of the SYNC signal	Error is reliably detected (DC_{AV} of the safety module)
Reference generator supplies incorrect frequency	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reference generator does not supply periodic reference signal	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Amplification error during signal processing (reference, sin, cos signal), oscillation	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Magnetic interference at the installation location	Sufficient screening for the installation location	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Supplementary requirements for evaluation of SIL position encoders			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/ comments
Supply voltage monitoring of the encoder	None	Indirect monitoring of the resolver carrier via vector length monitoring	Error is reliably detected (DC_{AV} of the safety module)
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of fault, the drive can be switched off functionally.

1) DC = 60% applies to factory setting, DC = 90% for restricted tolerances of vector length monitoring corresponding to section "System accuracy and reaction time"

Tab. 154: Resolver

ⓘ

Classification of the safety module in conjunction with resolver:
Detection of encoder fault: DC > 90%
Classification in accordance with EN 61800-5-2/EN 13849-1:

- SIL2/Cat. 3/PL d (safe positioning incl. standstill)
- SIL3/Cat. 3/PL e (safe speed and acceleration)

Combined encoder systems:

Encoder 1: resolver [X2A] or SIN/COS encoder [X2B]

Encoder 2: incremental encoder [X10]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
Interruption of any conductor of the connecting cable			
Static “0” or “1” signal at inputs and outputs, individually or simultaneously at multiple inputs/outputs			
Interruption or high-impedance status on a single input/output or multiple inputs/outputs simultaneously			
Reduction or increase of output amplitude - parasitic oscillation at one or more outputs			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Change of phase shift between output signals	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2)]
Mounting becomes loose at standstill: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2)]
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Material measure comes loose (e.g. optical encoding disc)			
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2)]
Supplementary requirements for rotary encoders with sin/cos output signals, analogue signal generation			
Static signal at inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1)]	DC “high”[2)]
Change in the signal shape			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Swapping of the sin and cos output signal	None	Individual signal monitoring and vector length monitoring[1]	DC “high”[2]
Supplementary requirements for rotary encoders with square wave output signals (encoder 2)			
Parasitic oscillation at output	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2]
Output signal terminates			
Zero pulse fails, is too short, too long or occurs multiple times			
Supplementary requirements for rotary encoders with synthetically generated output signals (encoder 1 or encoder 2)			
Any falsification of the output signal	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2]
Supplementary requirements for rotary encoders with position determination using a counter (encoder 2)			
Incorrect position value due to faulty count	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2]
Supplementary requirements for resolvers with signal processing/reference generator			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2]
Central timer fails, no Conversion Start for analogue/digital converter, Sample & Hold occurs at the wrong time	None		
Analogue-digital converter generates incorrect values	None		
Analogue-digital converter does not generate values	None		
Reference generator does not supply frequency	None		

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Reference generator supplies incorrect frequency	None	Individual signal monitoring and vector length monitoring[1] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC “high”[2]
Reference generator does not supply periodic reference signal	None		
Amplification error during signal processing (reference, sin, cos signal), oscillation	None		
Magnetic interference at the installation location	Sufficient screening for the installation location		
Supplementary requirements for evaluation of SIL position encoders			
Supply voltage monitoring of the encoder	None	Separate generation of the supply voltage for: – resolver [X2A] – SIN/COS encoder [X2B] – incremental encoder [X10]	–
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of fault, the drive can be switched off functionally

1) Sensitivity and DC dependent on the parameterised error limits; specification applies to factory setting.

2) Position information is “static” if there is a fault => fixed commutating position, motor at standstill/voltage of a channel static => commutating position changes by max +/-90° of a signal period of the encoder, motor only moves in this range.

Tab. 155: Combined encoder systems: encoder 1: resolver [X2A] or SIN/COS encoder [X2B], encoder 2: incremental encoder [X10]

ⓘ

Classification of the safety module in conjunction with the basic unit in the encoder combination encoder 1: resolver [X2A] or SIN/COS encoder [X2B], encoder 2: incremental encoder [X10] (without taking the actual encoder into account):
Detection of encoder fault: DC > 95%
Classification in accordance with EN 61800-5-2: SIL3
Classification in accordance with EN ISO 13849: Cat. 4/PL e

Combined encoder systems:

Encoder 1: resolver [X2A] or incremental encoder [X10]

Encoder 2: other encoder [X2B] (evaluation via basic unit)

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x “low” (basic unit)[2)]
Interruption of any conductor of the connecting cable	None	Individual signal monitoring and vector length monitoring [1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Static “0” or “1” signal at inputs and outputs, individually or simultaneously at multiple inputs/outputs	None	Individual signal monitoring and vector length monitoring 1) Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)
Interruption or high-impedance status on a single input/output or multiple inputs/outputs simultaneously	None	Individual signal monitoring and vector length monitoring 1) Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)
Reduction or increase of the output amplitude	None	Individual signal monitoring and vector length monitoring 1) Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Parasitic oscillation at one or more outputs	None	Individual signal monitoring and vector length monitoring [1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Change of phase shift between output signals	None	Individual signal monitoring and vector length monitoring [1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Mounting becomes loose at standstill: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Supplementary requirements for rotary encoders with sin/cos output signals, analogue signal generation			
Static signal at inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Change in the signal shape	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Swapping of the sin and cos output signal	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Supplementary requirements for resolvers with signal processing/reference generator (encoder 1)			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
– Central timer fails – No Conversion Start for analogue-digital converter – Sample & Hold occurs at the wrong time	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Analogue-digital converter generates incorrect values	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
Analogue-digital converter does not generate values	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
Reference generator does not supply frequency	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Reference generator supplies incorrect frequency	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
Reference generator does not supply periodic reference signal	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
Amplification error during signal processing (reference, sin, cos signal), oscillation	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Magnetic interference at the installation location	Sufficient screening for the installation location	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x “high” (safety module) + 1 x “low” (basic unit)[2)]
Supplementary requirements for rotary encoders with square wave output signals (encoder 1)			
Parasitic oscillation at output	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Output signal terminates			
Zero pulse fails, is too short, too long or occurs multiple times			
Supplementary requirements for rotary encoders with synthetically generated output signals (encoder 1 or encoder 2)			
Any falsification of the output signal	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Supplementary requirements for rotary encoders with position determination using a counter (encoder 1 or encoder 2)			
Incorrect position value due to faulty count	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Supplementary requirements for linear encoders (encoder 1 or encoder 2)			
Mounting of read head broken	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)[2)]
Static offset of the material measure (e.g. visual code strip)			
Damaged material measure (e.g. visual code strip)			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Supplementary requirements for rotary encoders with computer interface (encoder 2)			
Transmission errors: – repetition; – loss; – insertion; – incorrect sequence; – message falsification; – delay	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit)2)
Supplementary requirements for evaluation of SIL position encoders			
Supply voltage monitoring of the encoder	None	Separate generation of the supply voltage for: – resolver [X2A] – SIN/COS encoder [X2B] – incremental encoder [X10]	–
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder.	The basic unit has an input for monitoring the motor temperature. In the case of fault, the drive can be switched off functionally.

1) Sensitivity and DC dependent on the parameterised error limits; specification applies to factory setting.
2) Limitation by DCAV of the module by DC of the basic unit

Tab. 156: Combined encoder systems: encoder 1: resolver [X2A] or incremental encoder [X10], encoder 2: other encoder [X2B] (evaluation via basic unit)

ⓘ

Classification of the safety module in conjunction with the basic unit in the encoder combination, encoder 1: resolver [X2A] or incremental encoder [X10], encoder 2: other encoder [X2B] (without taking the actual encoder into account):

Angular detection of the basic unit:

- MTTF of each channel: ›100 a, “high”
- DC of the channel: = 50% “low"

Safety module: MTTF of each channel: ›100 a, “high”

Detection of encoder error DC: ›95% “high”

System classification (safety module + basic unit):

- Classification in accordance with EN 61800-5-2: SIL3
- Classification in accordance with EN ISO 13849: Cat. 3/PL d

8.2.4 Digital outputs

The relevant standards for the control of external safety relay units must always be observed.

Output type	**Switch type**	**Classification category, PL**[1)]	**Classification SIL**[2)]
1: integrated safe pulse inhibitor	2 N/C contacts	Cat. 4, PL e	SIL 3
2: general 2-channel output DOUT40 … DOUT42	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
2: general 2-channel output	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
3: control of the holding brake via [X6] in the basic unit CMMP-AS	2 N/C contacts	Cat. 3, PL d, for directly connected clamping units, requested via SBC.	SIL 2
	2 N/C contacts	Cat. 1, PL c, for indirectly connected clamping units (e.g. pneumatically opening), requested via SBC.	SIL 1

Output type	Switch type	Classification category, PL[1]	Classification SIL[2]
3: control of the holding brake via [X6] in the basic unit CMMP-AS	2 N/C contacts	Cat. 3, PL d, for indirectly connected clamping units (e.g. pneumatically opening), requested via SBC.	SIL 2
10: potential-free feedback contact (diagnostics)	1 N/O contact	Only as feedback for higher-level safety relay unit.	

1) In accordance with EN ISO 13849-1
2) In accordance with EN 61508, EN 61800-5-2, EN 62061

Tab. 157: Safety reference data, digital outputs

NOTICE

- The following data on measures and DC is based on the specifications of EN ISO 13849-1.
- The manufacturer's specifications must be used for a safety engineering assessment of the switching devices.
- The listed DC values are only valid if the specified measures and the specified additional conditions are in compliance.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

Measure	DC	Comment	Use
Cyclic test pulse by dynamic change of the output signals.	90	Always effective in the safety module, since the test pulses for the safe pulse inhibitor and for DOUT40 … 42 cannot be switched off.	Cross-circuit monitoring for 2-channel outputs
Cross-comparison of output signals with dynamic test if short circuits cannot be detected (for multiple inputs/outputs).	90	Without allocation of test pulses. Cyclic change of input signals required, e.g. by the process or regular actuation.	Monitoring 2-channel outputs

Measure	DC	Comment	Use
Cross-comparison of output signals with immediate and intermediate results in the logic (L) and time-based as well as logic program sequence monitoring and detection of static failures and short circuits (for multiple inputs/outputs).	99	Always effective in the safety module, since the test pulses for the safe pulse inhibitor and for DOUT40 … 42 cannot be switched off	Monitoring 2-channel outputs
Plausibility check, e.g. use of outputs switching antivalently.	99	Only applicable for DOUT40 … 42, switching “antivalent” in configuration.	Monitoring 2-channel outputs

Tab. 158: Measures for digital outputs

8.3 System precision and reaction time

The following sections consider the system precision requirements of functional safety engineering, with regard to safely monitoring movement functions for position and speed.

ℹ

The achievable system accuracy is primarily dependent on the system structure, consisting of: Motor – Gear unit – Axis
It can be increased particularly by the use of a gear unit or by the selection of an axis with a reduced feed ➔ 8.3.7 Basis for observation of system accuracy.

The specified accuracies and reaction times of the safety module always represent a compromise between:
- the resolution and the accuracy of the connected position sensors and the allocated electronic evaluation unit in the safety module,
- the desired high precision for monitoring limit values for position and speed,
- the reaction time until violation of a condition is detected,
- the system availability during operation in an industrial environment (malfunctions, EMC etc.).

For this reason, the accuracies and reaction times should be as high as necessary from a safety point of view but not excessive.

NOTICE

The factory settings of the safety module for encoder evaluation, speed detection and position monitoring are correct for most applications. They are adapted to the resolution of the position encoders and to the electronic evaluation unit in the safety module.
They should only be changed if there are proven problems, because they influence the reaction time of the safety module when dangerous movements are detected or during error detection. These are so-called “expert parameters”.
Alternatively, check to see if the mechanical system can be changed (e.g. axis with reduced feed).
Use the data migration (➔ 3.3 Data migration from the motor controller) to ensure that the safety module has the correct parameters for the feed constant and the gear ratios before parametrisation of safety functions.

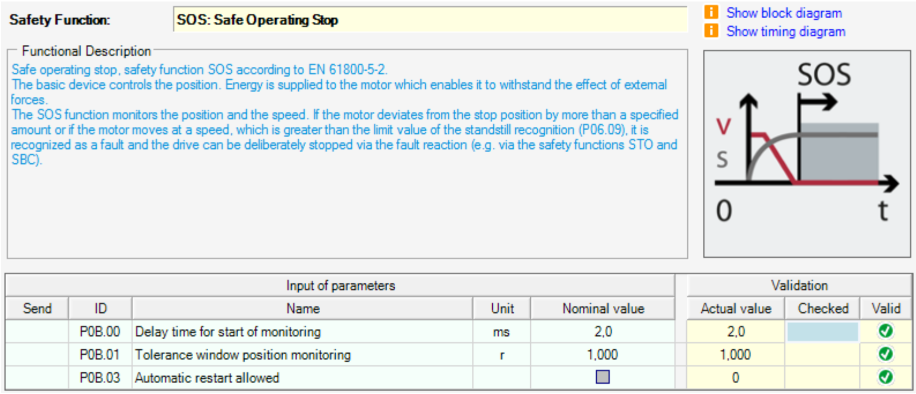
8.3.1 Accuracy of position monitoring (SOS) from the point of view of the application

When the SOS safety function is requested, the current position is detected and saved to x_sample.
Monitoring takes place in a position window of:
(x_sample – x_max) ≤ x_actual ≤ (x_sample + x_max)
Application-specific requirements for x_max (for SOS) ➔ 8.3.7 Basis for observation of system accuracy. X_max is set via P0B.01 ➔ 3.5.5 SOS – Safe Operating Stop.

Parameters	Name	min.	typical	max.	Note
x_max	Position tolerances for SOS	–	1 mm	1.8 mm	Position limits ➔ 8.3.7 Basis for observation of system accuracySection
phi_max	Angle tolerances on the motor shaft for SOS	Typical values, SOS	4.0°	7.2°	Sample calculation, based on a feed of 90 mm/rev

Tab. 159: Typical values, SOS

The safety module is parameterised as follows for this:



Safety Function: SOS: Safe Operating Stop

Show block diagram
Show timing diagram

Functional Description

Safe operating stop, safety function SOS according to EN 61800-5-2.
The basic device controls the position. Energy is supplied to the motor which enables it to withstand the effect of external forces.
The SOS function monitors the position and the speed. If the motor deviates from the stop position by more than a specified amount or if the motor moves at a speed, which is greater than the limit value of the standstill recognition (P06.09), it is recognized as a fault and the drive can be deliberately stopped via the fault reaction (e.g. via the safety functions STO and SBC).

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0B.00	Delay time for start of monitoring	ms	2,0	2,0		✓
	P0B.01	Tolerance window position monitoring	r	1,000	1,000		✓
	P0B.03	Automatic restart allowed		☐	0		✓

Fig. 107: Sample specification of the relevant parameters for Safe Operation Stop (SOS)

This sample data is converted from translational to rotational variables based on the following:
- motor without gear unit,
- axis EGC-80 with a feed of 90 mm/rev.

8.3.2 Accuracy of speed monitoring (SLS, SSR) from the point of view of the application

When the safety function with speed monitoring is requested, e.g. SLS, SSR, the current speed v_act is detected continuously and monitored for compliance with specific limit values.
The limit values can change dynamically, e.g. on requesting SLS, if the system first brakes to the safely limited speed.
Monitoring takes place in a speed window of:
v_min ≤ v_act ≤ v_max
Application-specific requirements for v_max (for SLS) ➔ 8.3.7 Basis for observation of system accuracy.
The acceptable filter time constant t_filter_v in the speed monitoring is the result of the quality of the analogue signal processing on the safety module (for position encoders with analogue signals, such as resolvers or Hiperface encoders) and the position resolution (number of angle steps per motor revolution).
In addition, on dynamic changes, there is a transient status until the speed settles into the new setpoint value. The length of time depends on the bandwidth of the rotational speed regulation circuit. To ensure a high level of system availability, short transient statuses in the range of the bandwidth of the rotational speed regulation circuit should not lead to a response of the monitoring system.
An allowable time t_tol_v is provided for that. During the length of time t_tol_v, v_act may move outside the speed window without triggering the violation of the safety condition.

Parameters	Name	Min.	typical	max.	Note
v_max	Speed limit for SLS	4 mm/s	250 mm/s	≥ 10 m/s	Speed limits ➔ 8.3.7 Basis for observation of system accuracy
n_max	Minimum speed limit on the motor shaft for SLS	2.1 rpm	167 rpm	–	Sample calculation, based on a feed of 90 mm/rev
t_filter_v	Filter time constant, speed detection	2 ms	8 ms	≥ 100 ms	Position limits ➔ 8.3.7 Basis for observation of system accuracySec-tion
t_tol_v	Allowable time for v_act outside the approved speed range	0 ms	10 ms	≥ 100 ms	Typical bandwidth of the speed control f_gr = 100 Hz

Tab. 160: Typical values, SLS

The resolution of the speed signal is primarily determined by the quality of the encoders used and the parameterised filter time of the speed filter. Monitoring for n_typ_min should be possible with standard rotary encoders, such as resolvers or SIN/COS encoders, if the speed filter is parameterised in the range of 20 ms (at 4 mm/s, the axis moves exactly 0.08 mm in 20 ms).

8.3.3 Specification of the relevant parameters for Safe Speed Function (with SLS, SSR)

The safety module is parameterised as follows for the requirements determined in ➔ 8.3.2 Accuracy of speed monitoring (SLS, SSR) from the point of view of the application:

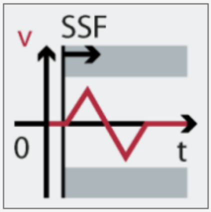
Standard Parameters | Expert Parameters

Safety Function: **SSF0: Safe Speed**

Show block diagram
Show timing diagram

Functional Description

Safe speed function - collective function for safety functions regarding control or monitoring rotational speed or speed. The characterisation as safety function SLS, SSR or SSM according to EN 61800-5-2 is done through the parametrisation as follows:
SLS = Safe Limited Speed: setting a symmetrical speed range around zero
SSR = Safe Speed Range: setting an arbitrary speed window
SSM = Safe Speed Monitor: like SSR; the fault reaction of the SSF is parametrised to "none".



Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.00	Activate SSF		☑	1		✓
	P0E.01	Delay time for start of monitoring	ms	10,0	10,0		✓
	P0E.07	Safe speed - upper limit	rpm	225,000	225,000		✓
	P0E.08	Safe speed - lower limit	rpm	-225,000	-225,000		✓
	P0E.02	Brake ramp time	ms	100,0	100,0		✓
	P0E.03	Tolerance time for limit exceed	ms	10,0	10,0		✓
	P0E.09	Limit speed in base device		☑	1		✓
	P0E.0B	Automatic restart allowed		☐	0		✓

Fig. 108: Sample specification of the relevant parameters for Safe Speed Function (SLS, SSR)

Standard Parameters | Expert Parameters

Safety Function: **SSF0: Safe Speed**

Show block diagram
Show timing diagram

Please note!

Editing the listet parameters is reserved only for experts!

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.0D	Speed ramp - Delay time monitoring	ms	2,0	2,0		✓
	P0E.06	Brake ramp - start delay	ms	6,0	6,0		✓
	P0E.04	Brake ramp - starting value factor		0,10	0,10		✓
	P0E.05	Brake ramp - starting value offset	rpm	0,000	0,000		✓
	P0E.0C	Offset speed limit	rpm	50,000	50,000		✓
	P0E.0A	Activate quick stop ramp in base device		☐	0		✓

Fig. 109: Sample specification of the expert parameters for Safe Speed Function (SLS, SSR)

8.3.4 Requirements for encoder errors from the point of view of the application

The evaluation of the position sensors on the safety module is based on one of the following basic principles:

a) Two redundant items of position information are available, which are also analysed redundantly and separately by two micro controllers, i.e. also two independent speed signals. Example: motor with EnDat encoder + second incremental position sensor on the axis.

b) Only one item of position information is “reliably” available. The information is sent along the same cables and via partially identical circuit sections (e.g. differential amplifiers for the input signals) and evaluated redundantly by two micro controllers on the safety module.

Example: resolver (SIL2) or SIN/COS encoder with SIL 2/SIL 3.

- Case a) The detection of encoder errors and position deviations between position encoders 1 and 2 is “non-time critical”, as monitoring is always guaranteed by the other encoder even if one of the encoders fails.
- Case b) The detection of position deviations between micro controller 1 and micro controller 2 is “non-time critical”, as monitoring is always guaranteed by the other micro controller.
  The detection of errors in the transmission channel (e.g. cable) and in the shared circuit sections for encoder analysis must be performed as quickly as possible within an error reaction time to be specified.
  The detection of encoder errors is based primarily on the monitoring of analogue signals. The limits of signal monitoring influence the resulting accuracy of the monitoring and the diagnostic coverage ➔ 8.2.3 Encoder systems.

Monitoring of the position difference does not need to be more accurate than in other cases of error. The worst case for uncontrolled movement of the axis is the failure of two power semiconductors in the power stage of the CMMP-AS-M3. In the worst case, this error leads to an electrical advance of the axis by up to 180° (== 45° on the shaft in the case of an 8-pole motor).
Note: of course, the system must be designed in such a way that this error does not lead to an impermissible position difference - e.g. by selection of a suitably low feed or gear unit.

NOTICE

There is a danger that the drive will advance if there are multiple errors in the CMMP-AS-...-M3.
If the power stage of the motor controller fails during the STO state (simultaneous short circuit of 2 power semiconductors in different phases), this can result in a limited detent movement of the rotor. The rotation angle/travel corresponds to one pole pitch. Examples:

- rotary axis, synchronous machine, 8-pole ➔ movement < 45° at the motor shaft.
- Linear motor, pole pitch 20 mm ➔ movement < 20 mm at the moving part.

Determination of angle difference (dynamic)	
Detection of signal errors in the “shared” transmission path (resolver, SIN/COS encoder)	≤ 2 ms
Position offset on “failure” of two power semiconductors (worst case)	approx. 60° on the shaft
Position offset because micro controller 1 and micro controller 2 did not detect the position at the same time	approx. 1° on the shaft
Dynamic position offset on accelerating	typ. 30 ° on the shaft
Duration of the compensation operation	typ. ≤ 10 ms
Resulting total position difference	approx. 0.167 U

Tab. 161: Observation of the possible position difference between micro controllers 1 and 2

Monitoring the speed difference depends on the resolutions in the encoder evaluation and the possible time offset in detection between micro controller 1 and micro controller 2 at maximum acceleration. The permissible filter time constant is calculated according to ➔ 8.3.7 Basis for observation of system accuracy (➔ Further information).

Determination of total rotational speed difference (dynamic)	
Resolution of encoder evaluation (raw) (important for standstill detection, P06.09)	approx. 20 rpm
Rotational speed offset on accelerating	approx. 120 rpm
Time offset	1 basic cycle =› ≤ 200 µs
Maximum acceleration	0 → 5000 rpm within 1 ms
Rotational speed offset on accelerating	200 µs x 6000 rpm/10 ms
Resulting total rotational speed difference	approx. 150 rpm
Filter time constant for speed signals	typ. 8 ms

Tab. 162: Observation of the possible dynamic rotational speed difference between micro controllers 1 and 2

Due to the high reliability (PFH) of the circuit, the maximum allowable time for encoder monitoring can be increased to 100 ms without any problems.
As a result, the encoder configuration of the safety module is parameterised as follows:

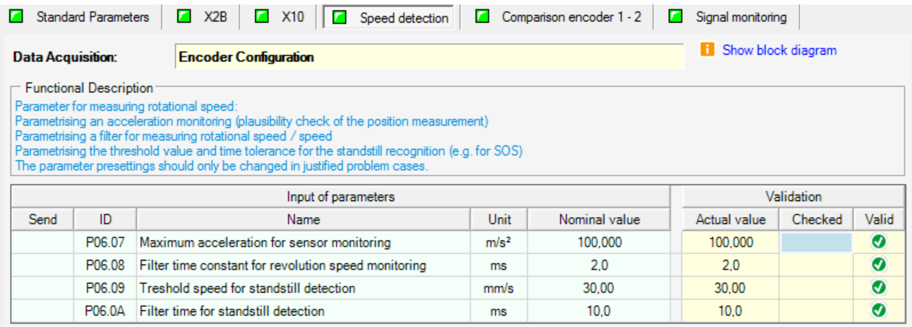
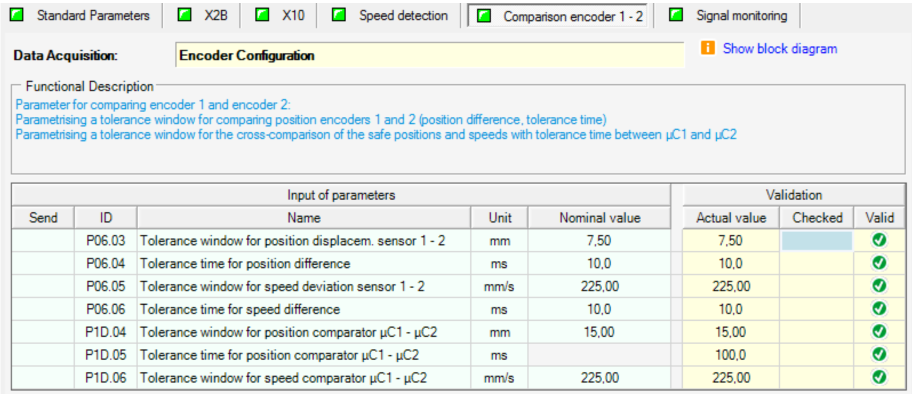


Fig. 110: Parameter setting for rotational speed detection


Standard Parameters | X2B | X10 | Speed detection | Comparison encoder 1 - 2 | Signal monitoring

Data Acquisition: Encoder Configuration

Show block diagram

Functional Description

Parameter for comparing encoder 1 and encoder 2:
Parametrising a tolerance window for comparing position encoders 1 and 2 (position difference, tolerance time)
Parametrising a tolerance window for the cross-comparison of the safe positions and speeds with tolerance time between µC1 and µC2

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.03	Tolerance window for position displacem. sensor 1 - 2	mm	7,50	7,50		✓
	P06.04	Tolerance time for position difference	ms	10,0	10,0		✓
	P06.05	Tolerance window for speed deviation sensor 1 - 2	mm/s	225,00	225,00		✓
	P06.06	Tolerance time for speed difference	ms	10,0	10,0		✓
	P1D.04	Tolerance window for position comparator µC1 - µC2	mm	15,00	15,00		✓
	P1D.05	Tolerance time for position comparator µC1 - µC2	ms		100,0		✓
	P1D.06	Tolerance window for speed comparator µC1 - µC2	mm/s	225,00	225,00		✓

Fig. 111: Parameter setting for comparing encoders 1 - 2

8.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder)

The safety module monitors the analogue encoder signals of a SIN/COS encoder or resolver:

– The tracking signals ex (corresponds to COS signal of a SIN/COS encoder/resolver) and ey (corresponds to SIN signal of a SIN/COS encoder/resolver) are measured.
– Every individual signal is monitored (compliance with the permissible signal range). Short circuits of individual signals against GND/VCC and impermissibly high signal levels are detected.
– The vector length is also calculated:
  $e = \sqrt{e_x^2 + e_y^2}$
– The currently measured vector length e is checked for compliance with parameterisable limit values: $e_{min} < e < e_{max}$ (parameters P06.0F, P06.10, P06.1A, P06.1B)
– If an individual signal (e_x, e_y) or the vector (e) is outside the permitted range, an encoder error is triggered and the error response is initiated (error of group 55-x).

Vector length monitoring is used to detect various errors of the encoder and for detection of errors in the analogue signal recording ➔ 8.2.3 Encoder systems:

– failure of a signal due to short circuit, interruption etc.
– amplitude and phase errors
– Stuck-At errors
– drift and oscillation

The maximum error angle until the vector length monitoring responds is calculated on the basis of the nominal vector length e_{rated}, including the limit values as follows:

$$\Delta e = acos\left(\frac{e_{min}}{e_{rated}}\right) + acos\left(\frac{e_{min}}{e_{max}}\right)$$

Diagnostic coverage of vector length monitoring:

The diagnostic coverage can be calculated from the ratio of the voltage areas in the x-y coordinate space, assuming a homogeneous distribution list of the voltage errors, as follows:

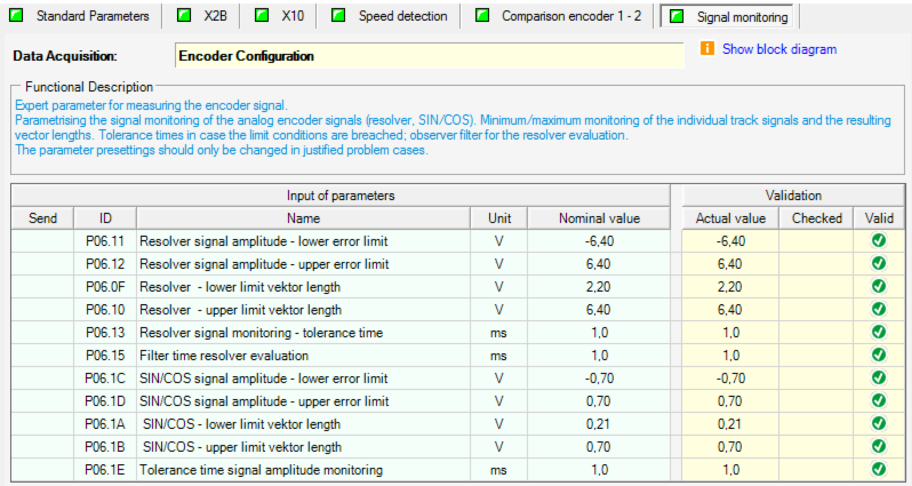
Value	SIN/COS encoder	Resolver
Voltage range of the encoder signals e_x, e_y	$0.5\ V \le e_x, e_y \le 4.5\ V$	$-6.7\ V \le e_x, e_y \le 6.7\ V$
Total area of voltage space F_{total}	$F_{total} = (4.50\ V - 0.50\ V)^2$	$F_{total} = (6.7\ V - (-6.7\ V))^2$

Value	**SIN/COS encoder**	**Resolver**
Proportion of the “permitted” Voltage range F_{valid} $F_{valid} = \pi(e_{max}^2 - e_{min}^2)$	$F_{valid} = \pi(0.70\ V^2 - 0.21\ V^2)$ 1) $F_{valid} = \pi(0.60\ V^2 - 0.40\ V^2)$ 2)	$F_{valid} = \pi\ (2.20\ V^2 - 6.40\ V^2)$ 1) $F_{valid} = \pi\ (5.20\ V^2 - 6.40\ V^2)$ 2)
Diagnostic coverage DC_{vl} $DC_{vl} = 1 - F_{valid}/F_{total}$	DCvl =91% 1) DCvl =95% 2)	DC_{vl} = 37% DC_{vl} =76% 2)

1) factory setting
2) setting with reduced tolerance

Tab. 163: Calculation of diagnostic coverage

The diagnostic coverage of the vector length monitoring DC_{VL} goes through the FMEA of possible encoder errors into the total diagnostic coverage DC_{AV} for the encoder system. DC_{AV} is mostly markedly higher than DC_{VL}.
When the device is delivered, the parameters for vector length are “relatively roughly” parameterised to enable operation with many different encoders and to achieve maximum availability in the case of external interference:



Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.11	Resolver signal amplitude - lower error limit	V	-6,40	-6,40		✓
	P06.12	Resolver signal amplitude - upper error limit	V	6,40	6,40		✓
	P06.0F	Resolver - lower limit vektor length	V	2,20	2,20		✓
	P06.10	Resolver - upper limit vektor length	V	6,40	6,40		✓
	P06.13	Resolver signal monitoring - tolerance time	ms	1,0	1,0		✓
	P06.15	Filter time resolver evaluation	ms	1,0	1,0		✓
	P06.1C	SIN/COS signal amplitude - lower error limit	V	-0,70	-0,70		✓
	P06.1D	SIN/COS signal amplitude - upper error limit	V	0,70	0,70		✓
	P06.1A	SIN/COS - lower limit vektor length	V	0,21	0,21		✓
	P06.1B	SIN/COS - upper limit vektor length	V	0,70	0,70		✓
	P06.1E	Tolerance time signal amplitude monitoring	ms	1,0	1,0		✓

Fig. 112: Parameter setting for analogue signal monitoring and error detection

The following table summarises the other data for encoders in the Festo motor series. It specifies the nominal values of the vectors, the frequencies of the encoders, the values for e_{min}, e_{max} (see above), the resulting maximum angle errors until the error detection responds, DC_{VL} and the resulting overall diagnostic coverage DC_{AV} for the motor with encoder system.

Motor series	Encoder 1	p_0	e_{min}	e_{rated}	e_{max}	$\Delta\varepsilon_{mech}$	Position error during feed [mm/rev]		DC_{VL}	DC_{AV}
							100	20		
EMMS-AS with resolver	Resolver	1	2.20 V	5.80 V	6.40 V	138°	38 mm	7 mm	36 %	91 %
EMME-AS	Hiperface encoder (SIN/COS encoder)	16	0.21 V	0.50 V	0.70 V	8.6°	2.4 mm	0.5 mm	91%	93%
Servo motor with Hiperface encoder SKS 36/SKM 36	Hiperface encoder (SIN/COS encoder)	128	0.21 V	0.50 V	0.70 V	1.1°	0.3 mm	0.06 mm	91%	93%

Tab. 164: Position error up to response of vector length monitoring, as well as corresponding DC (factory setting)

If the diagnostic coverage is too small, then a restriction is possible by changing e_{min} and e_{max} to the following limit values (possibly at the expense of system availability in an industrial environment with interference):

Motor series	Encoder 1	p_0	e_{min}	e_{rated}	e_{max}	$\Delta\varepsilon_{mech}$	Position error during feed [mm/rev]		DC_{VL}	DC_{AV}
							100	20		
EMMS-AS with resolver	Resolver	1	5.20 V	5.80 V	6.40 V	62°	17 mm	3.4 mm	75%	91%
EMME-AS	Hiperface encoder (SIN/COS encoder)	16	0.40 V	0.50 V	0.60 V	5.3°	1.5 mm	0.3 mm	95%	96%
Servo motor with Hiperface encoder SKS 36/SKM 36	Hiperface encoder (SIN/COS encoder)	128	0.40 V	0.50 V	0.60 V	0.7°	0.2 mm	0.04 mm	95%	96%

Tab. 165: Position errors up to the response of the vector length monitoring as well as the associated DC (restricted tolerances)

The diagnostic coverage of vector length monitoring DC_{VL} is included in the overall diagnostic coverage for operation of the CAMC-G-S3 with the appropriate encoder system. However, many errors are reliably detected even with “relatively roughly” set vector length monitoring or are also detected with other mechanisms for error detection. As a result, the total DC_{AV} is higher than DC_{VL}.
Example: resolver with factory settings for monitoring → DC_{VL} = 37%, but DC_{AV} = 91% is reached in the system.

NOTICE

Please check your application critically:

- What are the requirements for the accuracy of position and standstill monitoring?

Take the limitations listed in this chapter into account when selecting your system.

8.3.6 Effect of an angle error within the error limits of vector length monitoring on the speed signal

Assume the following case: there is an error in an encoder signal e_x or e_y, which could be an amplitude error, for example. However, the error is small enough so vector length monitoring does not respond. If the axis moves at a constant speed or the shaft rotates at a constant rotational speed, the error will lead to “fluctuations” in the currently measured speed. However, the speed averaged over an encoder period corresponds to the actual speed of movement.

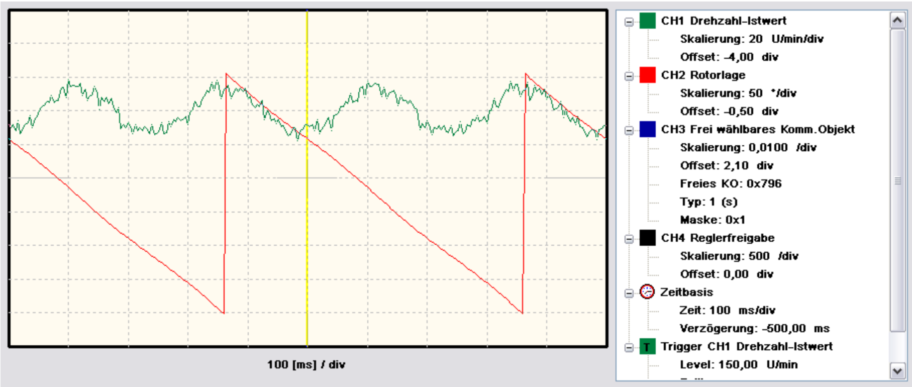


Fig. 113: Error curves on the speed signal (CH1) at a reduction of the signal amplitude of ex by 10%. This also produces a speed ripple of 10%. The measurement took place on an external drive of the shaft with a constant rotational speed.

Position encoder 1 is normally also evaluated in the basic unit and used for rotational speed adjustment. The basic unit now adjusts the current speed to the fluctuations. At least at low frequencies, below the cut-off frequency of the rotational speed control circuit, the supposed fluctuation is compensated, the axis no longer travels at a constant speed, but the actual rotational speed fluctuates and the angle and speed signal now look "OK"

The option of detection of speed errors in safety functions, such as SLS or SSR, is therefore dependent on multiple factors:

a) If, in addition, a second measuring system is used at the output, the fluctuation is detected safely. The speed fluctuation is detected correctly using the second measuring system, the safety module detects an excessively high current rotational speed and switches to the safe status.

b) Only one encoder system is used with a high number of periods per revolution:
Even at low speeds, there is a relatively high frequency, which is no longer corrected, the speed fluctuation is detected by the safety module and it switches to the safe state.

c) Only one encoder system is used with a low number of periods per revolution:
At low speeds, there is a low frequency of the speed fluctuation, which is largely corrected.

c1) The safety module is able to detect excessive mean speed safely over an encoder period.

c2) The monitoring limit must be reduced to ensure that the current rotational speed is also monitored.

Example for c2): monitoring of the resolver vector length with +/- 20% => The rotational speed to be monitored must be lowered by the expected amount of the rotational speed fluctuation, i.e. also by 20% => If monitoring at v = 200 mm/s is requested, then monitoring is set to v = 160 mm/s.

NOTICE

Please check your application critically:

- What are the requirements for speed monitoring?
- Is monitoring of the mean speed over one motor revolution sufficient?

Take the limitations listed in this chapter into account when selecting your system.

8.3.7 Basis for observation of system accuracy

SOS position limits	
Position monitoring	
Example of the maximum tolerance, required value must be specified in the risk assessment	1.8 mm is the upper limit for SOS, i.e. the axis may move max. 1.8 mm in the direction of the hazard.
Speed monitoring	
Standard max. filter times	64 ms
Typical default value	Immediate detection with 8 ms monitoring cycle
Summary	
Typical approved position tolerance	+/- 1 mm
Typical filter time	8 ms filter, 2 ms sampling time

Tab. 166: SOS position limits, filter times

SLS speed limits	
DIN EN 12417:2009-07 Machine tools – Safety – Machining centres	
Limited speed in special operating mode	
– Open, guards	5 m/min = 83.3 mm/s
Limit speed during tool changing, maintenance or setting work	
– Risk of impact only	15 m/min = 250 mm/s
– Risk of crushing	2 m/min = 33.3 mm/s
DIN EN 23125:2010-10 Machine tools – Safety – Lathes	
Limited speed in manual operation	
– For small lathes	6 m/min = 100 mm/s
– For large lathes	10 m/min = 166.7 mm/s
– Closing speed, jaw chucks	4 mm/s
– Axis movement	2 m/min = 33.3 mm/s
– Feed motion, spindle sleeve	1.2 m/min = 20 mm/s
EN 10218-1:2012-01 Industrial robots – Safety requirements – Part 1: Robots	
Limited speed	250 mm/s
Summary	
Value range “Limited speed”	
– Minimum	4 mm/s

SLS speed limits	
– Maximum	250 mm/s
– Typical filter time	8 ms filter, 2 ms sampling time.

Tab. 167: SLS speed limits

Typical data of some Festo linear axes							
Toothed belt axes EGC-TB-KF, with recirculating ball bearing guide							
Size		50	70	80	120	185	
Pitch	[mm]	2	3	3	5	8	
Extension (max. force)	[%]	0.094	0.08	0.24	0.13	0.29	
Effective diameter	[mm]	18.46	24.83	28.65	39.79	73.85	
Feed constant	[mm/ rev]	58	78	90	125	232	
Ball screw axes EGC-BS-KF, with recirculating ball bearing guide							
Size		70	80	120	185		
Diameters	[mm]	12	15	25	40		
Slope	[mm/ rev]	10	10, 20	10, 25	40		
Toothed belt axes DGE-ZR (high speed, up to 10 m/s depending on the type)							
Size		8 -	12	18	25	40	63
Pitch	[mm]	2	2	2	3	5	8
Extension (max. force)	[%]	0.04	0.1	0.2	0.11	0.1	0.15
Effective diameter	[mm]	10.18	12.09	16.55	20.05	31.83	56.02
Feed constant	[mm/ rev]	32	28	52	63	100	176
Toothed belt axes ELGA-TB-G							
Size		70	80	120			
Pitch	[mm]	3	5	5			
Extension (max. force)	[%]	0.31	0.19	0.23			
Effective diameter	[mm]	28.65	39.79	52.52			
Feed constant	[mm/ rev]	90	125	165			

Typical data of some Festo linear axes	
Linear drives, e.g. ELGL-LAS, air bearings and linear motor	
Typical pole pitches	In the range 20 mm ... 80 mm == 40 mm ... 160 mm feed
Summary	
Value range “Feed”	Z : 20 mm/rev .... 300 mm/rev

Tab. 168: Typical Festo linear axes - feed constants to be observed

$$\text{position factor} = \frac{\text{gear ratio} * \text{increments/revolution}}{\text{feed constant}}$$

Fig.114

8.4 Status messages, diagnostics via fieldbus

8.4.1 Output of status messages via the digital outputs of the basic unit

The motor controller can output important status signals of the safety module to digital outputs DOUT0 to DOUT3 via the I/O interface [X1].
The digital outputs are configured with the Festo Configuration Tool.
The following common messages are available for output (cf. ➔ 3.10.2 Status display on the safety module):

VOUT	Signal	Name	Function
40	VOUT_PS_EN	Power stage enable approval	Status bit specifies whether the motor controller can switch on the power stage.
41	VOUT_WARN	Warning	At least one error with the priority “Warning” has occurred.
42	VOUT_SCV	Safety condition violated	At least one safety condition was violated.
43	VOUT_ERROR	Errors	The safety module has detected an internal error.
44	VOUT_SSR	Safe state reached	Global bit “Safe state reached”, all the requested safety functions are indicating a safe status.
45	VOUT_SFR	Safety function requested	Global bit “Safety function requested”, at least one safety function is requested. It remains active until all requests have been reset.

VOUT	Signal	Name	Function
46	VOUT_SERVICE	Service status	“Service” status, no parameters present, parameter invalid or parameterisation session is running.
47	VOUT_READY	Ready for operation	“Ready for operation” status, no safety function requested.

Tab. 169: Status signals of the safety module for output via DOUTx of the basic unit

The status messages of the CAMC-G-S3 are compatible with those of the CAMC-G-S1 (safety module with safety function “Safe Torque Off”).
This achieves standardised feedback to the controller for applications with mixed use of the safety module.

8.4.2 Status signals via fieldbus – protocol CiA 402

The motor controller has all the key information of the safety module (status, modes, errors, IO). The following information is primarily relevant for transfer of data to bus systems, in order to create a detailed map of the system in a function controller:

- Common status messages on the status of the safety module (normal operation, safety function requested, errors, etc.) (cf. ➔ 3.10.2 Status display on the safety module).
- Status of the individual safety functions (which ones have been requested, which ones have been implemented).
- Status of the digital inputs and outputs.

The corresponding CiA 402 objects are listed below that contain information on the safety module and that the CMMP-AS-...- M3 supports.

Object 2000h: manufacturer_statuswords

The object group manufacturer_statuswords was introduced in order to map additional controller statuses which do not need to be present in the status word, which is queried often in the cycle. The object group manufacturer_statuswords has been extended for the safety module.

Index	**2000$_h$**
Name	manufacturer_statuswords
Object code	RECORD
No. of elements	2

Tab. 170

Subindex	**00$_h$**
Description	manufacturer_statuswords
Data Type	UINT8
Access	ro

PDO mapping	No
Units	–
Value Range	–
Default Value	1

Tab. 171

Subindex	**01_h**
Description	manufacturer_statusword_1
Data Type	UINT32
Access	ro
PDO mapping	yes
Units	–
Value Range	–
Default Value	–

Tab. 172

manufacturer_statusword_1		
Bit	Signal	Description
Bit 0	IS_REFERENCED	Drive is referenced
Bit 1	COMMUTATION_ VALID	Commutation valid
Bit 2	READY_FOR_ENABLE	The bit is set when all conditions are present to enable the controller and only the controller enable itself is missing. The following conditions must be present: – The drive is error-free. – The intermediate circuit is loaded. – Angle encoder evaluation is ready. No processes (e.g. serial transmission) that prevent enabling are active. – No blocking process is active (e.g. the automatic motor parameter identification). – STO is not active or a safety function is active, which permits enabling.
Bit 3	IPO_IN_TARGET	Positioning generator has completed the profile.
Bit 4 … 7	CAM	Reserved and used for the cam.
Bit 8	SAFE_STANDSTILL	“Safe Stop” “H” on the 7-segment display. Use by safety module CAMC-G-S1.

manufacturer_statusword_1		
Bit	Signal	Description
Bit 9 ... 11	–	Reserved for extensions.
Bit 12	VOUT_PS_EN	Displays that the drive can be switched on (no limitations by safety module).
Bit 13	VOUT_WARN	Corresponds to VOUT_WARN (VOUT41) of the safety module. There is at least one error, whose error response is parameterised as “Warning”.
Bit 14	VOUT_SCV	Corresponds to VOUT_SCV (VOUT 42) of the safety module. At least one safety condition was violated.
Bit 15	VOUT_ERROR	Corresponds to VOUT_ERROR (VOUT 43) of the safety module. An internal error was detected.
Bit 16	VOUT_SAVE_STAT	Corresponds to VOUT_SSR (VOUT 44) of the safety module. The bit is set if a safety function was requested in the safety module and the safe state has been reached.
Bit 17	VOUT_SFR	Corresponds to VOUT_SFR (VOUT 45) of the safety module. The bit is set if at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
Bit 18	VOUT_SERVICE	No parameters present, parameter invalid or parameterisation session is running (not supported by CAMC-G-S1). Status is assumed if the safety module was replaced with another type.
Bit 19	VOUT_READY	Normal status: VOUT_READY= NOT(VOUT_SFR)
Bit 20 ... 31	–	Reserved.

Tab. 173: Bit allocation for manufacturer_statusword_1

Object 2600h: FSM_VOUT

These objects map the status of the VOUT (0..64).

Index	**2600h**
Name	FSM_vout
Object code	RECORD
No. of elements	2

Tab. 174

Subindex	**01h**
Description	FSM_vout_0_31
Data Type	UINT32
Access	ro
PDO mapping	yes
Units	–
Value Range	–
Default Value	–

Tab. 175

Bits 0..31 = VOUT0..31 of the safety module

Subindex	**02h**
Description	FSM_vout_32_63
Data Type	UINT32
Access	ro
PDO mapping	yes
Units	–
Value Range	–
Default Value	–

Tab. 176

Bits 0..31 = VOUT32..63 of the safety module

Object 2602h: FSM_IO

Read the level at the inputs of the safety module

Index	**2602h**
Name	FSM_io
Object code	RECORD
No. of elements	1

Tab. 177

Subindex	**01h**
Description	FSM_dig_io
Data Type	UINT32
Access	ro
PDO mapping	yes

Units	–
Value Range	–
Default Value	–

Tab. 178

FSM_dig_io		
Bit	Signal	Description
Bit 0	LOUT48	Logic state DIN40 A/B
Bit 1	LOUT49	Logic state DIN41 A/B
Bit 2	LOUT50	Logic state DIN42 A/B
Bit 3	LOUT51	Logic state DIN43 A/B
Bit 4	LOUT52	Logic state DIN44
Bit 5	LOUT53	Logic state DIN45; mode selector switch (1 of 3)
Bit 6	LOUT54	Logic state DIN46; mode selector switch (1 of 3)
Bit 7	LOUT55	Logic state DIN47; mode selector switch (1 of 3)
Bit 8	LOUT56	Error acknowledgement via DIN48
Bit 9	LOUT57	Terminate safety function via DIN49
Bit 10	LOUT58	Logic state, two-handed operator unit (pair of 2 x DIN4x)
Bit 11	LOUT59	Feedback, holding brake
Bit 12 … 15	LOUT60 … 63	Not assigned
Bit 16	LOUT64	Status of output DOUT40
Bit 17	LOUT65	Status of output DOUT41
Bit 18	LOUT66	Status of output DOUT42
Bit 19	LOUT67	Status of signal relay
Bit 20	LOUT68	Brake control
Bit 21	LOUT69	Status of SS1 control signal
Bit 22 … 31	LOUT70 …	Not assigned

Tab. 179: Bit allocation FSM_dig_io

8.4.3 Status signals via fieldbus – protocol FHPP

The motor controller has all the key information of the safety module (status, modes, errors, I/O).
The following information is primarily relevant for transfer of data to bus systems, in order to create a detailed map of the system in a function controller:

- Common status messages on the status of the safety module (normal operation, safety function requested, errors, etc.) (cf. ➔ 3.10.2 Status display on the safety module).
- Status of the individual safety functions (which ones have been requested, which ones have been implemented).
- Status of the digital inputs and outputs.

The corresponding objects for the communication protocol FHPP (Festo Handling and Positioning) that contain information about the safety module are listed below.

FSM_STATE via FHPP

PNU 280	**Safety status**			
Subindex 01	Class: Var	Data type: uint32	From FW 4.0.1501.2.1	Access: ro
Status word of the safety function.				

Bit	Name	Value	Meaning
0 … 7	–	0x0000 00FF	Reserved.
8	VOUT_PS_EN	0x0000 0100	Power stage enable possible.
			CAMC-G-S3: VOUT_PS_EN = NOT (VOUT_SFR).
			CAMC-G-S1: none of the inputs STO-A or STO-B has been switched.
9	VOUT_WARN	0x0000 0200	Warning. There is at least one error, whose error response is parameterised as “Warning”.
			CAMC-G-S3: VOUT_WARN (VOUT41).
			CAMC-G-S1: Reserved.
10	VOUT_SCV	0x0000 0400	At least one safety condition was violated.
			CAMC-G-S3: VOUT_SCV (VOUT 42).
			CAMC-G-S1: Reserved.
11	VOUT_ERROR	0x0000 0800	Internal error (common error message) of the safety module.
			CAMC-G-S3: VOUT_ERROR (VOUT 43).
			CAMC-G-S1: Discrepancy time violated.
12	VOUT_SSR	0x0000 1000	Safety status reached (common message).

PNU 280	**Safety status**				
Subindex 01	Class: Var	Data type: uint32	From FW 4.0.1501.2.1	Access: ro	

12	VOUT_SSR	0x0000 1000	CAMC-G-S3: VOUT_SSR (VOUT 44) the bit is set if the safe state has been reached in the safety module with all requested safety functions.
			CAMC-G-S1: STO active.
13	VOUT_SFR	0x0000 2000	Safety function requested.
			CAMC-G-S3: VOUT_SFR (VOUT 45): The bit is set if at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
			CAMC-G-S1: at least one of the inputs STO-A or STO-B has been switched.
14	VOUT_SERVICE	0x0000 4000	Service message.
			CAMC-G-S3: Status is assumed,... ...... after a module replacement ...... in delivery status, ... during a parameterisation session.
			CAMC-G-S1: Reserved.
15	VOUT_READY	0x0000 8000	Ready. Normal status, no safety function requested.
			CAMC-G-S3: VOUT_READY = NOT (VOUT_SFR).
			CAMC-G-S1: no STO requested.
16... 31	–	0xFFFF 0000	Reserved.

Tab. 180

PNU 281	**FSM status word**		
Subindex 01 ... 02	Class: array	Data type: uint32	From FW 4.0.1501.2.1
CAMC-G-S3: contents of the status word VOUT (0 ... 63).			
Subindex 01	Lower bytes		
Bits 0 ... 31 = VOUT_0 ... 31 of the safety module CAMC-G-S3.			

PNU 281	FSM status word
Subindex 02	Upper bytes
Bits 0 ... 31 = VOUT_32 ... 63 of the safety module CAMC-G-S3.	

Tab. 181: PNU 281

PNU 282	FSM IO (FSM IO)			
Subindex 01	Class: Var	Data type: uint32	From FW 4.0.1501.2.1	Access: ro
CAMC-G-S3: level at the inputs of the safety module.				

Bit	Signal	Meaning
0	LOUT48	Logic state DIN40 A/B
1	LOUT49	Logic state DIN41 A/B
2	LOUT50	Logic state DIN42 A/B
3	LOUT51	Logic state DIN43 A/B
4	LOUT52	Logic state DIN44
5	LOUT53	Logic state DIN45; mode selector switch (1 of 3)
6	LOUT54	Logic state DIN46; mode selector switch (1 of 3)
7	LOUT55	Logic state DIN47; mode selector switch (1 of 3)
8	LOUT56	Logic state, error acknowledgement via DIN48
9	LOUT57	Logic state, terminate safety function via DIN49
10	LOUT58	Logic state, two-handed operator unit (pair of 2 x DIN4x)
11	LOUT59	Feedback, holding brake
12 . 15	LOUT60 ... 63	Not assigned
16	LOUT64	Logic state of output DOUT40
17	LOUT65	Logic state of output DOUT41
18	LOUT66	Logic state of output DOUT42
19	LOUT67	Logic state of the signal relay
20	LOUT68	Logic state of the brake control
21	LOUT69	Logic state of the SS1 control signal
22 ... 31	LOUT70 ... 79	Not assigned.

Tab. 182: PNU 282

8.5 Record measurement data - “Trace”

8.5.1 Overview

For diagnostics purposes, you can use the trace function (oscilloscope function) of the FCT plug-in CMMP-AS to record measurement data of the safety module in addition to the normal data of the motor controller.

ⓘ

The recorded measurement data is used for troubleshooting. They are not safety relevant.

The measurement data and recording are parameterised via FCT (➔ 8.5.2 Configuring).
You can record up to four numerical or digital data in parallel. The following data is available for the safety module:

Data	Description
Numerical data	
Upper limit of speed[1)]	Current upper speed limit in the basic unit, limit set by the safety module.
Lower limit of speed setpoint value[1)]	Current lower speed limit in the basic unit, limit set by the safety module.
CAMC-G-S3: speed - actual value	Actual rotational speed value from the safety module.
CAMC-G-S3: position - actual value	Actual position value from the safety module.
CAMC-G-S3: currently monitored speed upper limit	Current upper speed limit monitored by the safety module.
CAMC-G-S3: currently monitored speed lower limit	Current lower speed limit monitored by the safety module.
Freely selectable CO ...	With this selection, any parameters can be recorded ➔ 8.5.2 Configuring.
Digital data	
CAMC-G-S3: ...	Status bits of the safety module
CAMC-G-S3: DIN40A	Physical status of input DIN40A
...	Physical statuses of the other inputs ...
CAMC-G-S3: DOUT40A	Physical status of output DOUT40A
...	Physical statuses of the other outputs ...
CAMC-G-S3: C1/C2	Physical status of relay contact C1 / C2

1) Data from basic unit

Tab. 183: Measurement data for the safety module

8.5.2 Configuring

The recorded data is specified as usual in the FCT plug-in CMMP-AS on the “Configure trace data” page.
For the safety module, the additional numerical and digital data contained in ➔ Further information are available.

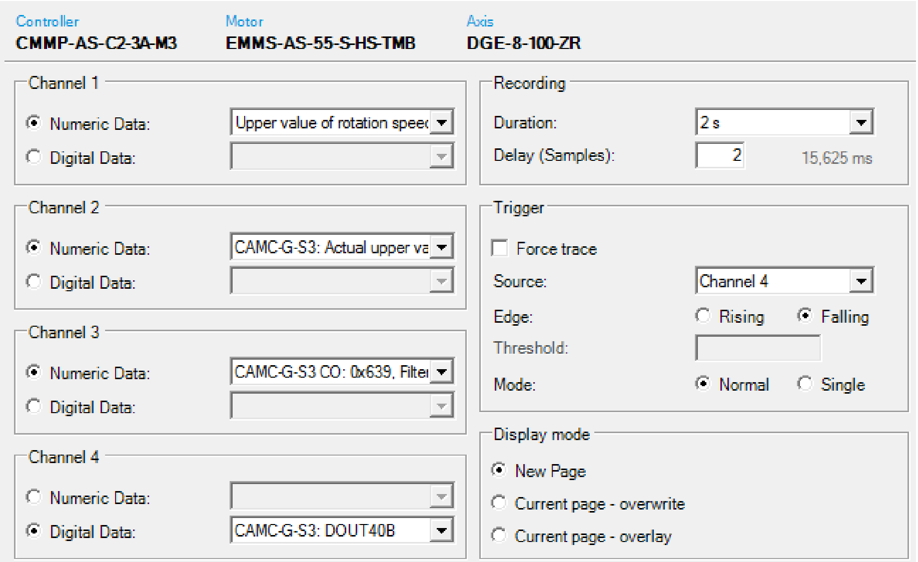


Fig. 115: Configure measurement data

With the exception of “Freely selectable CO...”, you can set the entries directly.
A special dialogue box is opened for the freely selectable COs (communication objects):

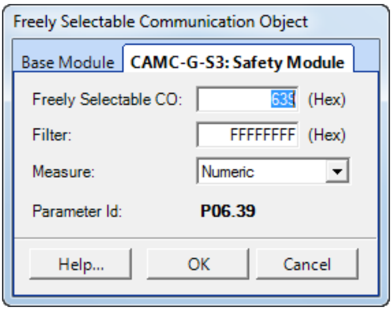


Fig. 116: Freely selectable communication object

1. First, activate the “CAMC-G-S3: Safety module” tab for the measurement data of the safety module.

2. Under “Freely selectable CO”, enter the number as a hexadecimal value. The number corresponds to the parameter number without “P” and the full stop. In the example, “639” stands for P06.39 – actual value of the safe speed. The parameter number is displayed below.
   Useful parameters can be found for example in ➔ 9.2 List of additional parameters, ➔ Further information.
3. You can specify a mask under “Filter”, e.g. for bit arrays or other digital data.
4. Under “Unit of measurement”, select the correct entry for the measured variable so that it is displayed correctly later in the diagram.

To change the settings, simply select the entry “Freely selectable CO...” again.

8.5.3 Starting the trace

Normally, the settings of the “Configure trace data” page are sent to the motor controller automatically when the trace is started. This is not possible if a safety module CAMC-G-S3 is installed because the measurement data determined by the safety module only become effective after a restart.
For this reason, the FCT plug-in displays the following dialogue box as soon as one or more items of data contained in "➔ Further information" are selected (with the exception of data marked as from the basic unit).

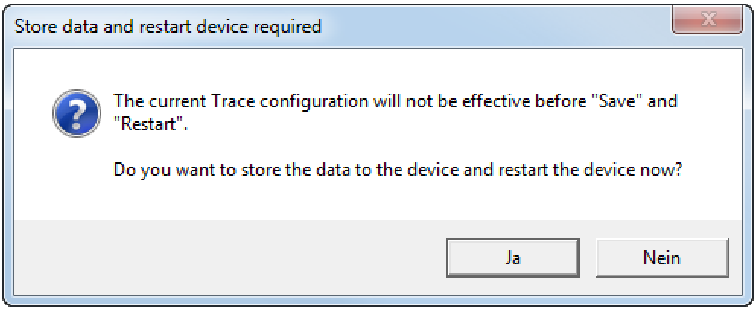


Fig. 117: Save data and restart

This is necessary once after opening the CMMP-AS plug-in in the FCT or after every change to the measurement data.
After restart of the motor controller, you can start the trace normally.

8.5.4 Example

A violation of the safety condition on SS1 should be recorded. As a trigger, DOUT42 is requested by VOUT_SCV “Safety Condition Violated”.

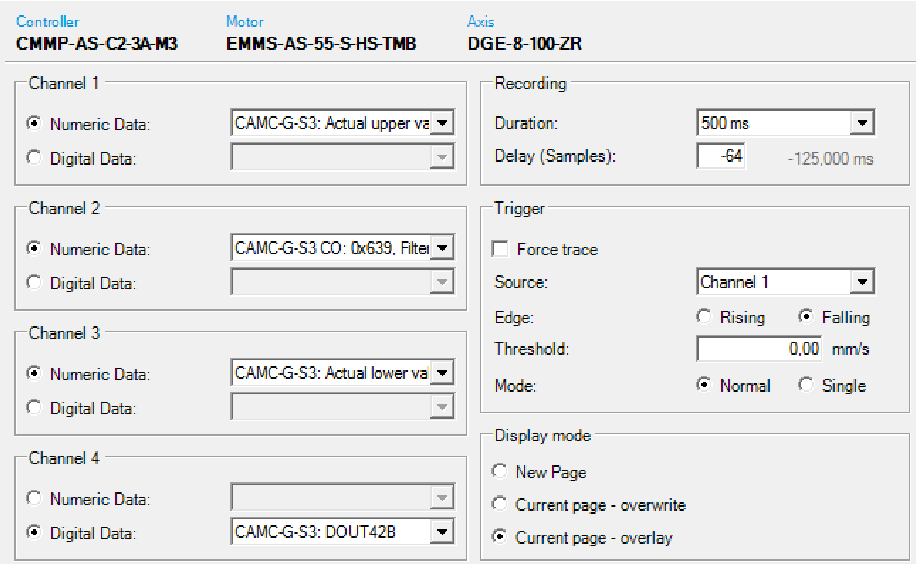


Fig. 118: Example of configuring measurement data

As can be seen in the figure, the following data is set:

- Trace channel 1 - numerical data - CAMC-G-S3: currently monitored speed upper limit
- Trace channel 2 - numerical data - CAMC-G-S3: KO: 0x639, filter 0xFFFFFFFF (P06.39 – actual value of the safe speed)
- Trace channel 3 - numerical data - CAMC-G-S3: currently monitored speed lower limit
- Trace channel 4 - digital data - CAMC-G-S3: DOUT42B

For example, this results in the following graph:

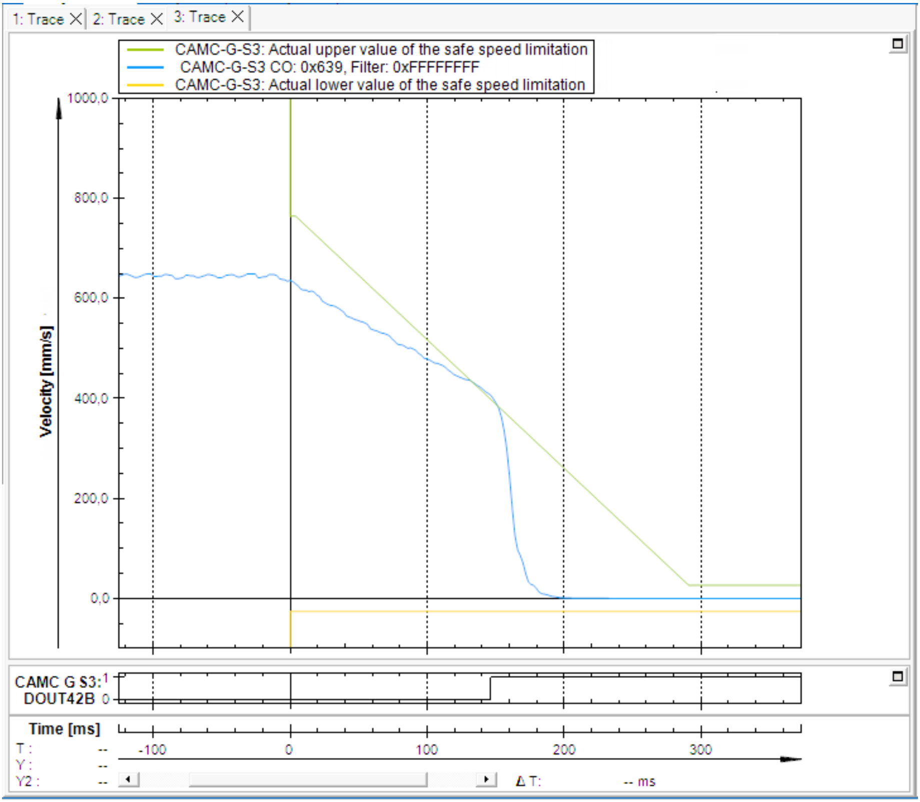


Fig. 119: Sample graph

9 Reference list for control signals and parameters

9.1 List of all logic signals

9.1.1 Logical inputs LIN

The logical inputs are combined into a bit vector with a length of 128 bits. The bit vector has the following structure:

LIN	Name	Function
0	–	Reserved for later expansion of the functionality of the safety module, always zero.
...	...	
63	–	
64	LIN_USF0_SSR	Returned virtual output signals VOUT (status signals of the safety functions, common messages). This means that they can be linked logically with the input signals.
...	...	
95	LIN_READY	
96	LIN_D40	Logic state of digital inputs DIN40...DIN49, as well as output signals of the logic functions and some auxiliary statuses.
...	...	
127	LIN_STATIC_ONE	

Tab. 184: Structure of the bit vector of the logical inputs

The current status of the bit vector LIN can be read via the communication objects:
- Bit 00 ... Bit 31: P04.20
- Bit 32 ... Bit 63: P04.21
- Bit 64 ... Bit 95: P04.22
- Bit 96 ... Bit 127:P04.23

Mapping of the physical inputs to the logical inputs

The physical inputs are mapped to the logical inputs as follows (the stationary status after filtering, test pulse analysis, etc. is stated):

LIN	Name	Function
96	LIN_D40	Bit LIN_D40 set if DIN40 A/B = 0 V (quiescent current principle)[1)]
97	LIN_D41	Bit LIN_D41 set if DIN41 A/B = 0 V (quiescent current principle)[1)]
98	LIN_D42	Bit LIN_D42 set if DIN42 A/B = 0 V (quiescent current principle)[1)]
99	LIN_D43	Bit LIN_D43 set if DIN43 A/B = 0 V (quiescent current principle)[1)]
100	LIN_D44	Bit LIN_D44 set if DIN44 = 24 V
101	LIN_D45	Bit LIN_D45 set if DIN47 = 0 V and DIN46 = 0 V and DIN45 = 24 V

LIN	Name	Function
102	LIN_D46	Bit LIN_D46 set if DIN47 = 0 V and DIN46 = 24 V and DIN45 = 0 V
103	LIN_D47	Bit LIN_D47 set if DIN47 = 24 V and DIN46 = 0 V and DIN45 = 0 V
104	LIN_D48	Bit LIN_D48 set, if DIN48 = 24 V
105	LIN_D49	Bit LIN_D49 set, if DIN49 = 24 V

1) Valid for configuration as equivalent input. Configuration as antivalent input accordingly: LIN_DIN4x set, if D4xA = 0 V and D4xB = 24 V.

Tab. 185: Logical inputs, level assignment to the physical inputs

i

Please note that LIN_D40 ... LIN_D43 have a special allocation to the voltage levels. This means that the logical inputs can be fed to the safety functions (e.g. request STO) without inversion, implementing the quiescent current principle (input 0 V = STO requested).

Logical inputs after preliminary processing and auxiliary functions

Mapping of the physical inputs after preliminary processing (time expectation, 1-of-n etc.)

LIN	Name	Function
96	LIN_D40	Logic state DIN40 A/B
97	LIN_D41	Logic state DIN41 A/B
98	LIN_D42	Logic state DIN42 A/B
99	LIN_D43	Logic state DIN43 A/B
100	LIN_D44	Logic state DIN44
101	LIN_D45	Logic state DIN45; mode selector switch (1 of 3) Logic state DIN45 - 47 (1 of 3) DIN45
102	LIN_D46	Logic state DIN45 - 47 (1 of 3) DIN46
103	LIN_D47	Logic state DIN45 - 47 (1 of 3) DIN47
104	LIN_D48	Logic state DIN48
105	LIN_D49	Logic state DIN49
106	LIN_2HAND_CTRL	Logic state, two-handed operator unit (pair of 2 x DIN4x)
107	LIN_BRAKE_X6_FB	Feedback, holding brake
117	LIN_PWSTG_ON	Basic unit power stage active
121	LIN_D45_SAFE	Logic state DIN45 after mode selector switch evaluation
122	LIN_D46_SAFE	DIN46 after mode selector switch evaluation
123	LIN_D47_SAFE	DIN47 after mode selector switch evaluation

LIN	Name	Function
124	LIN_D49_RISING_EDGE	Logic “1” pulse with approx. 2 ms – 10 ms length after each rising edge of the signal LIN_D49. Intended for edge-sensitive termination of the safety function.
125	LIN_AFTER_RST_PULSE	Logic “1” pulse with approx. 2 ms – 10 ms length after every RESET. Intended for first automatic setting of a safety function request after Power ON or after a system RESET.
126	LIN_STATIC_ZERO	Always "0"
127	LIN_STATIC_ONE	Always "1"

Tab. 186: Logical inputs after preliminary processing

Virtual outputs returned as logical inputs

LIN	Name	Function
64	LIN_USF0_SSR	Safe state USF0 reached
65	LIN_USF1_SSR	Safe state USF1 reached
66	LIN_USF2_SSR	Safe state USF2 reached
67	LIN_USF3_SSR	Safe state USF3 reached
75	LIN_SBC_SSR	Safe state SBC reached
76	LIN_SS2_SSR	Safe state SS2 reached
77	LIN_SOS_SSR	Safe state SOS reached
78	LIN_SS1_SSR	Safe state SS1 reached
79	LIN_STO_SSR	Safe state STO reached
80	LIN_ALF0_OUT	"Additional Logic Function" for feedback or own logic
81	LIN_ALF1_OUT	"Additional Logic Function" for feedback or own logic
82	LIN_ALF2_OUT	"Additional Logic Function" for feedback or own logic
83	LIN_ALF3_OUT	"Additional Logic Function" for feedback or own logic
84	LIN_ALF4_OUT	"Additional Logic Function" for feedback or own logic
85	LIN_ALF5_OUT	"Additional Logic Function" for feedback or own logic
86	LIN_ALF6_OUT	"Additional Logic Function" for feedback or own logic
87	LIN_ALF7_OUT	"Additional Logic Function" for feedback or own logic
88	LIN_PS_EN	Status bit specifies whether the motor controller can switch on the power stage.
89	LIN_WARN	At least one error with the priority “Warning” has occurred.
90	LIN_SCV	At least one of the safety conditions was violated.

LIN	Name	Function
91	LIN_ERROR	The safety module has detected an internal error.
92	LIN_SSR	Global bit “Safe State Reached”, when at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
93	LIN_SFR	Global bit “Safety function requested”, at least one safety function has been requested but not yet reached.
94	LIN_SERVICE	“Service” status, no parameters present, parameter invalid or parameterisation session is running.
95	LIN_READY	“Ready for operation” status, no safety function requested

Tab. 187: Virtual outputs returned as logical inputs

9.1.2 Virtual inputs VIN

The virtual inputs are the inputs of the safety functions and the additional logic functions (ALF = additional logic function). The following abbreviations apply:

– “RSF” = Request Safety Function
– "CSF" = Clear Safety Function, terminates safety function after safety condition has been violated

The virtual inputs are combined into a bit vector with a length of 64 bits.

ⓘ

The current status of the bit vector VIN can be read via the communication objects:

- Bit 00 ... Bit 31: P04.24
- Bit 32 ... Bit 63: P04.25

Mapping of the virtual inputs

VIN	Name	Function
0	VIN_USF0_RSF	Request safety function USF0
1	VIN_USF1_RSF	Request safety function USF1
2	VIN_USF2_RSF	Request safety function USF2
3	VIN_USF3_RSF	Request safety function USF3
4	–	Reserved, always zero
...	...	
10	–	
11	VIN_SBC_RSF	Request safety function SBC
12	VIN_SS2_RSF	Request safety function SS2
13	VIN_SOS_RSF	Request safety function SOS
14	VIN_SS1_RSF	Request safety function SS1

VIN	Name	Function
15	VIN_STO_RSF	Request safety function STO
16	VN_USF0_CSF	Terminate USF0 request
17	VIN_USF1_CSF	Terminate USF1 request
18	VIN_USF2_CSF	Terminate USF2 request
19	VIN_USF3_CSF	Terminate USF3 request
27	VIN_SBC_CSF	Terminate SBC request
28	VIN_SS2_CSF	Terminate SS2 request
29	VIN_SOS_CSF	Terminate SOS request
30	VIN_SS1_CSF	Terminate SS1 request
31	VIN_STO_CSF	Terminate STO request
32	VIN_ALF0_IN	Input, additional logic function ALF0
33	VIN_ALF1_IN	Input, additional logic function ALF1
34	VIN_ALF2_IN	Input, additional logic function ALF2
35	VIN_ALF3_IN	Input, additional logic function ALF3
36	VIN_ALF4_IN	Input, additional logic function ALF4
37	VIN_ALF5_IN	Input, additional logic function ALF5
38	VIN_ALF6_IN	Input, additional logic function ALF6
39	VIN_ALF7_IN	Input, additional logic function ALF7
40	–	Reserved for extensions of ALF, always zero
...	...	
47	–	
48	–	Reserved for later expansion of the functionality of the safety module, always zero
...	...	
59	–	
60	VIN_ERR_QUIT	Acknowledge error
61	–	Reserved, always zero
62	–	Reserved, always zero
63	VIN_BRK_ACK	Feedback, holding brake

Tab. 188: Virtual inputs

9.1.3 Virtual outputs VOUT

The virtual outputs are the outputs of the safety functions and the additional logic functions. They are defined in terms such as “SS1_Safe_State_Reached”. The following abbreviations apply:

SSR = Safety Function Requested
SSR = Safe State Reached
The virtual outputs are combined into a bit vector with a length of 64 bits. Selected virtual output signals are fed back into the processing as logical inputs, cf. ➔ Virtual outputs returned as logical inputs.

ⓘ

The current status of the bit vector VIN can be read via the communication objects:
- Bit 00 ... Bit 31: P05.10
- Bit 32 ... Bit 63: P05.11

VOUT	Name	Function
0	VOUT_USF0_SFR	Safety function USF0 requested
1	VOUT_USF1_SFR	Safety function USF1 requested
2	VOUT_USF2_SFR	Safety function USF2 requested
3	VOUT_USF3_SFR	Safety function USF3 requested
4	–	Reserved, always zero
...	...	
10	–	
11	VOUT_SBC_SFR	Safety function SBC requested
12	VOUT_SS2_SFR	Safety function SS2 requested
13	VOUT_SOS_SFR	Safety function SOS requested
14	VOUT_SS1_SFR	Safety function SS1 requested
15	VOUT_STO_SFR	Safety function STO requested
16	VOUT_USF0_SSR	safe state USF0 reached
17	VOUT_USF1_SSR	safe state USF1 reached
18	VOUT_USF2_SSR	safe state USF2 reached
19	VOUT_USF3_SSR	safe state USF3 reached
20	–	Reserved, always zero
...	...	
26	–	
27	VOUT_SBC_SSR	safe state SBC reached
28	VOUT_SS2_SSR	safe state SS2 reached
29	VOUT_SOS_SSR	safe state SOS reached
30	VOUT_SS1_SSR	safe state SS1 reached

VOUT	Name	Function
31	VOUT_STO_SSR	safe state STO reached
32	VOUT_ALF0_OUT	Output, additional logic function ALF0
33	VOUT_ALF1_OUT	Output, additional logic function ALF1
34	VOUT_ALF2_OUT	Output, additional logic function ALF2
35	VOUT_ALF3_OUT	Output, additional logic function ALF3
36	VOUT_ALF4_OUT	Output, additional logic function ALF4
37	VOUT_ALF5_OUT	Output, additional logic function ALF5
38	VOUT_ALF6_OUT	Output, additional logic function ALF6
39	VOUT_ALF7_OUT	Output, additional logic function ALF7
40	VOUT_PS_EN	Status bit specifies whether the motor controller can switch on the power stage
41	VOUT_WARN	At least one error with the priority "Warning" has occurred
42	VOUT_SCV	At least one safety condition was violated
43	VOUT_ERROR	The safety module has detected an internal error
44	VOUT_SSR	Global bit "Safe state reached", all the requested safety functions are indicating a safe status
45	VOUT_SFR	Global bit "Safety function requested", at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
46	VOUT_SERVICE	"Service" status, no parameters present, parameter invalid or parameterisation session is running
47	VOUT_READY	"Ready for operation" status, no safety function requested
48	–	Reserved, always zero
...	...	
62	–	
63	VOUT_SBC_BRK_ON	Engage holding brake

Tab. 189: Virtual output signals

9.1.4 Logical outputs LOUT

Like the logical inputs, the status of the logical outputs is represented by 1 bit. This also applies for two-channel outputs.
Equivalence/antivalence and test signals are processed during the conversion of the logical outputs into physical outputs.
The logical outputs are combined into a bit vector with a length of 96 bits.

ⓘ

The current status of the bit vector LOUT can be read via the communication objects:
- Bit 00 ... Bit 31: P05.12
- Bit 32 ... Bit 63: P05.13
- Bit 64 ... Bit 95: P05.14

Mapping of the logical outputs

LOUT	Name	Function
0	–	Logical outputs for diagnostics via fieldbus ➔ 8.4 Status messages, diagnostics via fieldbus
...	...	
63	–	
64	LOUT_D40	Status of output DOUT40
65	LOUT_D41	Status of output DOUT41
66	LOUT_D42	Status of output DOUT42
67	LOUT_RELAY	Status of signal relay C1/C2
68	LOUT_BRAKE_CTRL	Brake control
69	LOUT_SS1_RQ	SS1 control signal (fixed wiring)
70	–	Reserved, always zero
...	...	
95	–	

Tab. 190: Logical outputs, mapping the physical outputs

The physical outputs are assigned to logical outputs LOUT64 ... LOUT69.

9.1.5 Status words for the data exchange/diagnostics via fieldbus

The safety module and the basic unit exchange data on a regular basis.
In this way, important data from the safety module are sent to the basic unit and are available for data exchange with a function controller and for diagnostic functions.
The data of the communication objects in the safety module are "mirrored" in corresponding communication objects in the basic unit.
The data is used for:
- status messages via fieldbus and digital outputs,
- recording data with the trace function of the basic unit.

The following table lists the corresponding diagnostic communication objects. This means that the data of the safety module can be read out in the basic unit via communication objects 0794h to 0797h.

CO basic unit	Name of CO in the basic unit	CO safety module	Trans-mitted value[1)]	Meaning/value sent to the basic unit
0782	ioh_fsm_mov_vout_ 0_31	P05.10	---	Actual value of virtual outputs VOUT00...VOUT31
0783	ioh_fsm_mov_vout_ 32_63	P05.11	---	Actual value of virtual outputs VOUT32...VOUT63
079B	ioh_fsm_limit_speed _upper			Current upper speed limit in the basic unit
079C	ioh_fsm_limit_speed _lower			Current lower speed limit in the basic unit
0790	ioh_fsm_diag_ch0	---	P06.39	Selection of the CO sent to diagnostic channel 0
0791	ioh_fsm_diag_ch1	---	P04.23	Selection of the CO sent to diagnostic channel 1
0792	ioh_fsm_diag_ch2	---	P05.10	Selection of the CO sent to diagnostic channel 2
0793	ioh_fsm_diag_ch3	---	P05.11	Selection of the CO sent to diagnostic channel 3
0794	ioh_fsm_dat_ch0	P1D.00	P06.39	Safe actual speed of the safety module
0795	ioh_fsm_dat_ch1	P1D.01	P04.23	Status of logical inputs LIN96...LIN127
0796	ioh_fsm_dat_ch2	P1D.02	P05.10	Status of virtual outputs VOUT0... VOUT31
0797	ioh_fsm_dat_ch3	P1D.03	P05.11	Status of virtual outputs VOUT32... VOUT63

1) Default setting

Tab. 191: List of the diagnostic information for the basic unit

The diagnostic outputs can be revised if needed. Use the trace function of the FCT plug-in CMMP-AS ➔ 8.5 Record measurement data - “Trace” for this purpose. The following settings are made here:

1. The COs of the safety module that are to be recorded are entered in basic unit COs nos. 0790h to 0793h.
2. The setting is saved in the basic unit and it is restarted. The settings are then sent to the safety module.

Example:

CO 0790h → value: 0639h transmission of safe speed

CO 0791h → value: 0423h status of LIN96... LIN127 (LIN_D40... LIN_D49 etc.)

CO 0792h → value: 1D09h upper monitoring limit of speed
CO 0793h → value: 1D0Ah lower monitoring limit of speed
RESET/restart:
CO 0794h ← value: 0639h transmission of safe speed
CO 0795h ← value: 0423h status of LIN96... LIN127 (LIN_D40... LIN_D49 etc.)
CO 0796h ← value: 1D09h upper monitoring limit of speed
CO 0797h ← value: 1D0Ah lower monitoring limit of speed
The corresponding data is shown in the basic units in COs 0794h to 0797h (time resolution approx. 2 ms)

9.2 List of additional parameters

The menu item Options/Parameter overview in SafetyTool allows experts the option to view or change the parameters of the safety module. Filters can be used to select the parameters which you want to see. This means, for example, that those parameters can be found quickly whose settings are different in the Safety Tool and the safety module.

ⓘ

Most parameters are described in the context of the appropriate function:

- Basic information ➔ 3.3.1 Basic information
- Encoder configuration ➔ 3.3.5 List of all parameters for encoder configuration
- Two-channel digital inputs ➔ 3.4.2 Two-channel safe inputs DIN40 ... DIN43 [X40]
- Single-channel digital inputs ➔ 3.4.2 Two-channel safe inputs DIN40 ... DIN43 [X40]
- STO: Safe Torque Off ➔ 3.5.1 STO – Safe Torque Off
- SS1: Safe Stop 1 ➔ 3.5.3 SS1 – Safe Stop 1
- SS2: Safe Stop 2 ➔ 3.5.4 SS2 – Safe Stop 2
- SOS: Safe Operating Stop ➔ 3.5.5 SOS – Safe Operating Stop
- SSF: Safe Speed ➔ 3.5.7 Safe speed functions SSF
- SBC: Safe Brake Control ➔ 3.5.2 SBC – Safe Brake Control
- Logic functions, mode selector switch ➔ 3.6.1 Mode selector switch
- Logic functions, two-handed control unit ➔ 3.6.2 Two-hand control unit
- Logic functions, additional logic functions➔ 3.6.3 Additional logic functions - ALF
- Digital outputs ➔ 3.9 Digital outputs

The following tables contain a list of all parameters that have not yet been explained above.

Error management		
No.	Name	Description
P20.00	[53-0] USF0: safety condition violated	Error response of error 53-0
P20.01	[53-1] USF1: safety condition violated	Error response of error 53-1
P20.02	[53-2] USF2: safety condition violated	Error response of error 53-2
P20.03	[53-3] USF3: safety condition violated	Error response of error 53-3
P20.0A	[54-0] SBC: safety condition violated	Error response of error 54-0

Error management		
No.	Name	Description
P20.0C	[54-2] SS2: safety condition violated	Error response of error 54-2
P20.0D	[54-3] SOS: safety condition violated	Error response of error 54-3
P20.0E	[54-4] SS1: safety condition violated	Error response of error 54-4
P20.0F	[54-5] STO: safety condition violated	Error response of error 54-5
P20.10	[54-6] SBC: Brake not released for > 10 days	Error response of error 54-6
P20.11	[54-7] SOS: SOS requested > 10 days	Error response of error 54-7
P20.14	[55-0] Rotational speed/actual position value not available or standstill > 10 days	Error response of error 55-0
P20.15	[55-1] SINCOS encoder [X2B] - tracking signal errors	Error response of error 55-1
P20.16	[55-2] SINCOS encoder [X2B] - standstill > 10 days	Error response of error 55-2
P20.17	[55-3] Resolver [X2A] - signal error	Error response of error 55-3
P20.18	[55-4] EnDat encoder [X2B] - sensor error	Error response of error 55-4
P20.19	[55-5] EnDat encoder [X2B] - incorrect sensor type	Error response of error 55-5
P20.1A	[55-6] Incremental encoder [X10] - tracking signal error	Error response of error 55-6
P20.1B	[55-7] Other encoder [X2B] - faulty angle information	Error response of error 55-7
P20.26	[56-8] Rotational speed/angle difference encoder 1 - 2	Error response of error 56-8. The error is triggered when one of the two micro controllers detects an impermissible position or speed difference between encoder 1 and encoder 2
P20.27	[56-9] Error cross-comparison encoder evaluation	Error response of error 56-9. The error is triggered if an impermissible position difference is detected during cross-comparison of the safe position values between micro controller 1 and micro controller 2
P20.28	[57-0] Self-test I/O error (internal/external)	Error response of error 57-0
P20.29	[57-1] Digital inputs - signal level error	Error response of error 57-1
P20.2A	[57-2] Digital inputs - test pulse error	Error response of error 57-2
P20.2E	[57-6] Electronic temperature too high	Error response of error 57-6

Error management		
No.	Name	Description
P20.32	[58-0] Plausibility check parameters	Error response of error 58-0
P20.33	[58-1] General parameterisation error	Error response of error 58-1
P20.36	[58-4] Buffer internal communication	Error response of error 58-4
P20.37	[58-5] Communication safety module - basic unit	Error response of error 58-5
P20.38	[58-6] Cross-comparison error processors 1 - 2	Error response of error 58-6. The error is triggered if an impermissible deviation occurs during cross-comparison of micro controllers 1 and 2. Examples: different statuses of the inputs and outputs, or different safe speed values. Error 56-9 is triggered in special cases where position values deviate.
P20.3D	[59-1] Fail-safe power supply/safe pulse inhibitor	Error response of error 59-1
P20.3E	[59-2] External power supply error	Error response of error 59-2
P20.3F	[59-3] Internal power supply error	Error response of error 59-3
P20.40	[59-4] Error management: too many errors	Error response of error 59-4
P20.41	[59-5] Diagnostic memory writing error	Error response of error 59-5
P20.42	[59-6] Error saving parameter set	Error response of error 59-6
P20.43	[59-7] FLASH checksum error	Error response of error 59-7
P20.44	[59-8] Internal monitoring processor 1 - 2	Error response of error 59-8
P20.45	[59-9] Other unexpected error	Error response of error 59-9

Tab. 192: Error management

Diagnostic parameters		
No.	Name	Description
P00.00	Parameter set version	Parameter set version
P20.46	Error status, group 53 and 54:	Main error number 53 and 54 in the error field
P20.47	Error status, group 55 and 56:	Main error number 55 and 56 in the error field
P20.48	Error status, group 57 and 58:	Main error number 57 and 58 in the error field

Diagnostic parameters		
No.	Name	Description
P20.49	Error status, group 59:	Main error number 59 in the error field
Expert parameters		
P02.2F	Status of the digital inputs	Status of the digital inputs
P02.38	Status of the digital outputs	Status of the digital outputs
P02.39	Status of the digital outputs B	Status of the digital outputs
P02.3A	Status of the digital inputs B	Status of the digital inputs
P05.10	Status VOUT0VOUT31	Actual values of VOUT0..VOUT31
P05.11	Status VOUT32VOUT63	Actual values of VOUT32..VOUT63
P05.12	Status LOUT0LOUT31	Actual values of LOUT0..LOUT31
P05.13	Status LOUT32LOUT63	Actual values of LOUT32..LOUT63
P05.14	Status LOUT64LOUT95	Actual values of LOUT64..LOUT95
P06.39	Actual value of the safe speed	Actual rotational speed value
P06.3A	Safe position	Actual position value shortened to 32 bits
P06.3B	Safe acceleration	Acceleration from angle encoder
P06.3C	Angle from encoder 1	Angle from encoder 1 (without gear unit)
P06.3D	Angle from encoder 2	Angle from encoder 2 (without gear unit)
P06.56	Position from encoder 1	Calculated position of encoder 1 (contains gear unit conversion)
P06.57	Position from encoder 2	Calculated position of encoder 2 (contains gear unit conversion)
P1D.00	CO for diagnostics channel 0	CO for output as diagnostics channel 0
P06.58	Speed from encoder 1	Calculated speed of encoder 1 (including gear unit conversion)
P1D.01	CO for diagnostics channel 1	CO for output as diagnostics channel 1
P06.59	Speed from encoder 2	Calculated speed of encoder 2 (including gear unit conversion)
P1D.02	CO for diagnostics channel 2	CO for output as diagnostics channel 2
P1D.03	CO for diagnostics channel 3	CO for output as diagnostics channel 3

Diagnostic parameters		
No.	Name	Description
P0E.50	Current upper speed limit	Current upper speed limit in the safety module
P0E.51	Current lower speed limit	Current lower speed limit in the safety module

Tab. 193: Diagnostic parameters

Mapping		
No.	Name	Description
P04.00	Product term	Mapping and allocation for product term 0
P04.01	Product term	Mapping and allocation for product term 1
P04.02	Product term	Mapping and allocation for product term 2
P04.03	Product term	Mapping and allocation for product term 3
P04.04	Product term	Mapping and allocation for product term 4
P04.05	Product term	Mapping and allocation for product term 5
P04.06	Product term	Mapping and allocation for product term 6
P04.07	Product term	Mapping and allocation for product term 7
P04.08	Product term	Mapping and allocation for product term 8
P04.09	Product term	Mapping and allocation for product term 9
P04.0A	Product term	Mapping and allocation for product term 10
P04.0B	Product term	Mapping and allocation for product term 11
P04.0C	Product term	Mapping and allocation for product term 12
P04.0D	Product term	Mapping and allocation for product term 13
P04.0E	Product term	Mapping and allocation for product term 14
P04.0F	Product term	Mapping and allocation for product term 15
P04.10	Product term	Mapping and allocation for product term 16
P04.11	Product term	Mapping and allocation for product term 17
P04.12	Product term	Mapping and allocation for product term 18
P04.13	Product term	Mapping and allocation for product term 19
P04.14	Product term	Mapping and allocation for product term 20
P04.15	Product term	Mapping and allocation for product term 21
P04.16	Product term	Mapping and allocation for product term 22

Mapping		
No.	Name	Description
P04.17	Product term	Mapping and allocation for product term 23
P04.18	Product term	Mapping and allocation for product term 24
P04.19	Product term	Mapping and allocation for product term 25
P04.1A	Product term	Mapping and allocation for product term 26
P04.1B	Product term	Mapping and allocation for product term 27
P04.1C	Product term	Mapping and allocation for product term 28
P04.1D	Product term	Mapping and allocation for product term 29
P04.1E	Product term	Mapping and allocation for product term 30
P04.1F	Product term	Mapping and allocation for product term 31
P05.00	Function selection DOUT40	Output mapping for LOUT64 (DOUT40)
P05.01	Function selection DOUT41	Output mapping for LOUT65 (DOUT41)
P05.02	Function selection DOUT42	Output mapping for LOUT66 (DOUT42)
P05.03	Function select, feedback contact C1/C2	Output mapping for LOUT67 (signal relay)
Expert parameters		
P04.20	Status LIN0..LIN31	Actual values of LIN0..LIN31
P04.21	Status LIN32..LIN63	Actual values of LIN32..LIN63
P04.22	Status LIN64..LIN95	Actual values of LIN64..LIN95
P04.23	Status LIN96..LIN127	Actual values of LIN96..LIN127
P04.24	Status VIN0..VIN31	Actual values of VIN0..VIN31
P04.25	Status VIN32..VIN63	Actual values of VIN32..VIN63
P05.04	Function selection, brake output of basic unit	Output mapping for LOUT68 (holding brake of the basic unit)

Tab. 194: Mapping

Internal/hidden parameters		
No.	Name	Description
P06.14	Resolver, phase offset	Phase offset between pulse-width modulation toggling and sampling instant
P06.20	Single turn resolution in bits	Number of bits per angle value
P06.21	Number of measurable revolutions (Multi-turn)	Number of measurable revolutions (Multi-turn)

Internal/hidden parameters		
No.	Name	Description
P06.22	Serial number of the EnDat encoder (Part 1)	Serial number of the EnDat encoder (Part 1)
P06.23	Serial number of the EnDat encoder (Part 2)	Serial number of the EnDat encoder (Part 2)
P06.24	Serial number of the EnDat encoder (Part 3)	Serial number of the EnDat encoder (Part 3)
P06.25	ID number of the EnDat encoder (Part 1)	ID number of the EnDat encoder (Part 1)
P06.26	ID number of the EnDat encoder (Part 2)	ID number of the EnDat encoder (Part 2)
P06.27	ID number of the EnDat encoder (Part 3)	ID number of the EnDat encoder (Part 3)
P06.38	Allowable time for incorrectly sent angle data	Maximum time for which the basic unit angle can be sent incorrectly.
P09.00	Filter for common message SFR or SSR	Mask, in order to exclude status reports for individual safety functions from the calculation of the common message
P09.01	Time between two sync pulses (basic cycle)	Time between two sync pulses (basic cycle)
P12.01	Switch-on delay	Time delay in case of a switch-on delay
P12.02	Switch-off delay	Time delay in case of a switch-off delay
P12.04	Switch-on delay	Time delay in case of a switch-on delay
P12.05	Switch-off delay	Time delay in case of a switch-off delay
P12.07	Switch-on delay	Time delay in case of a switch-on delay
P12.08	Switch-off delay	Time delay in case of a switch-off delay
P12.0A	Switch-on delay	Time delay in case of a switch-on delay
P12.0B	Switch-off delay	Time delay in case of a switch-off delay
P12.0D	Switch-on delay	Time delay in case of a switch-on delay
P12.0E	Switch-off delay	Time delay in case of a switch-off delay
P12.10	Switch-on delay	Time delay in case of a switch-on delay
P12.11	Switch-off delay	Time delay in case of a switch-off delay
P12.13	Switch-on delay	Time delay in case of a switch-on delay
P12.14	Switch-off delay	Time delay in case of a switch-off delay
P12.16	Switch-on delay	Time delay in case of a switch-on delay
P12.17	Switch-off delay	Time delay in case of a switch-off delay
P1C.00	Software revision (main revision)	Software revision (main revision)
P1C.01	Software revision (application number)	Software revision (application number)
P1C.02	Software revision (KM/subrevision)	Software revision (KM/subrevision)

Internal/hidden parameters		
No.	Name	Description
P20.06	[53-6] SDI 0: safety condition violated	Error response of error 53-6
P20.07	[53-7] SDI 1: safety condition violated	Error response of error 53-7
P20.08	[53-8] SLI0: safety condition violated	Error response of error 53-8
P20.09	[53-9] SLI1: safety condition violated	Error response of error 53-9
P20.0B	[54-1] SBT: safety condition violated	Error response of error 54-1
P20.0B	[57-3] Error, analogue input (value range)	Error response of error 57-3
P20.2C	[57-4] Error in current measurement	Error response of error 57-4
P20.2D	[57-5] Error, motor voltage measurement	Error response of error 57-5
P20.4A	Request for safety function logging	If set: log safety function request
PFF.00	Operating status:	Current status of the parameterisation session
PFF.01	Identification “Delivery status” 1 = YES	Identification “Delivery status”
PFF.02	Identification “Complete validation” 1 = YES	Identification “Complete validation”
Expert parameters		
PFF.03	Validation code:	Validation code of the parameterisation session

Tab. 195: Internal/hidden parameters

9.3 List of important communication objects in the basic unit

Reference list of the communication objects in the motor controller that provide information on the safety module.

CO no.	**Name**	**Type**	**Unit**	**Description**
0750	ioh_fsm_ctrl	RW	UINT32	Control word for the safety module
0751	ioh_fsm_stat	RO	UINT32	Status word for the safety module
0752	ioh_fsm_sto_disc rep_time	RW	UINT32	Discrepancy time, within which briefly differing levels may occur at the STO inputs of the CAMC-G-S1 without an error being triggered
0753	ioh_fsm_config	RW	UINT32	Configuration word for the safety module

CO no.	Name	Type	Unit	Description
0760	srvc_fsm_act_art _hi	RO	UINT32	Current manufacturer-specific product number of the safety module: ASCII coding of the upper 4 places, e.g. 0x39313030 = '9100'
0761	srvc_fsm_act_art _mid	RO	UINT32	Current manufacturer-specific product number of the safety module: medium longword
0762	srvc_fsm_act_art _lo	RO	UINT32	Current manufacturer-specific product number of the safety module: lower longword
0763	srvc_fsm_act_typ	RO	UINT32	Current type of the connected safety module:
0764	srvc_fsm_act_ser _hi	RO	UINT32	Manufacturer-specific serial number of the connected safety module: ASCII coding of the upper 4 places, e.g. 0x30303134 = '0014'
0765	srvc_fsm_act_ser _mid	RO	UINT32	Manufacturer-specific serial number of the connected safety module: medium longword
0766	srvc_fsm_act_ser _lo	RO	UINT32	Manufacturer-specific serial number of the connected safety module: lower longword
0767	srvc_fsm_act_rev _idx	RO	UINT32	Revision of the hardware of the con-nected safety module
0768	srvc_fsm_act_sof t_ref_idx	RO	UINT32	Revision of the software of the con-nected safety module
0769	ioh_fsm_proj_art _hi	RW	UINT32	Manufacturer-specific product number of the safety module planned using the parameterisation program: ASCII coding of the upper 4 places, e.g. 0x39313030 = '9100'
076A	ioh_fsm_proj_art _mid	RW	UINT32	Planned manufacturer-specific product number of the safety module: medium longword
076B	ioh_fsm_proj_art _lo	RW	UINT32	Planned manufacturer-specific product number of the safety module: lower longword

CO no.	Name	Type	Unit	Description
076C	ioh_fsm_proj_typ	RW	UINT32	Planned type of the connected safety module.
076D	ioh_fsm_proj_ser _hi	RW	UINT32	Manufacturer-specific serial number of the planned safety module: ASCII coding of the upper 4 places, e.g. 0x30303134 = '0014'
076E	ioh_fsm_proj_ser _mid	RW	UINT32	Manufacturer-specific serial number of the planned safety module: medium longword
076F	ioh_fsm_proj_ser _lo	RW	UINT32	Manufacturer-specific serial number of the planned safety module: lower longword
0770	ioh_fsm_proj_rev _idx	RW	UINT32	Revision of the hardware of the planned safety module
0771	ioh_fsm_proj_sof t_rev_idx	RW	UINT32	Revision of the software of the planned safety module
0772	srvc_fsm_dip_val _std	RO	UINT32	Supplies the value of the DIL switches read on the safety module/ switch module after reset
0773	ioh_fsm_num_en try_act	RO	UINT32	Supplies the number of entries in the error log memory of the basic unit
0774	ioh_fsm_num_en try_max	RO	UINT32	Supplies the maximum number of possible entries in the error log memory of the basic unit
0780	ioh_7segment_fsm_ctrl	RW	UINT32	Control word to control the 7-seg- ment display of the safety module.
0781	ioh_7seg- ment_fsm_data	RW	UINT32	Controls the 7-segment display of the safety module
0782	ioh_fsm_mov_vo ut_0_31	RW	UINT32	Internal status of the safety module (64 bits of the system bus) low word (Tab. B.6, VOUT 0... 31)
0783	ioh_fsm_mov_vo ut_32_63	RW	UINT32	Internal status of the safety module (64 bits of the system bus) high word (Tab. B.6, VOUT 32... 64)
0784	ioh_fsm_mov_ms cfct_rx	RW	UINT32	Received character from FCT. Input from USB, Ethernet. Tracking read index, FIFO-SYSTEM

CO no.	Name	Type	Unit	Description
0785	ioh_fsm_mov_ms cfct_tx	RW	UINT32	Character to be sent to FCT. Output to USB, Ethernet FIFO-SYSTEM
0786	ioh_fsm_mscfct_ rx_cnt	RO	UINT32	Number of characters from FCT in the USB buffer, Ethernet FIFO-SYSTEM
0787	ioh_fsm_mscfct_ tx_cnt	RO	UINT32	Number of characters from the safety module for FCT in the USB buffer, Ethernet FIFO-SYSTEM
0788	ioh_fsm_din_dou t	RO	UINT32	Reading of the digital inputs from the safety module
0789	ioh_fsm_mov_sta t_arb	RW	UINT32	Set/read the safety module state machine
078B	srvc_fsm_act_gesant_re v_idx	RO	UINT16	--
078C	ioh_fsm_proj_gesamt_r ev_idx	RW	UINT16	--
0790	ioh_fsm_diag_ch 0	RW	UINT32	Safety module diagnostic channel 1: selection of the CO in the safety module
0791	ioh_fsm_diag_ch 1	RW	UINT32	Safety module diagnostic channel 2: selection of the CO in the safety module
0792	ioh_fsm_diag_ch 2	RW	UINT32	Safety module diagnostic channel 3: selection of the CO in the safety module
0793	ioh_fsm_diag_ch 3	RW	UINT32	Safety module diagnostic channel 4: selection of the CO in the safety module
0794	ioh_fsm_dat_ch0	RO	UINT32	Safety module diagnostics channel 1: date, dynamically updated by the safety module
0795	ioh_fsm_dat_ch1	RO	UINT32	Safety module diagnostics channel 2: date, dynamically updated by the safety module
0796	ioh_fsm_dat_ch2	RO	UINT32	Safety module diagnostics channel 3: date, dynamically updated by the safety module

CO no.	Name	Type	Unit	Description
0797	ioh_fsm_dat_ch3	RO	UINT32	Safety module diagnostics channel 4: date, dynamically updated by the safety module
0798	ioh_fsm_log_entr y_0	RW	UINT32	Input of a log entry in the diagnostic memory of the safety module. Writing only takes place after the third entry
0799	ioh_fsm_log_entr y_1	RW	UINT32	Input of a log entry in the diagnostic memory of the safety module. Writing only takes place after the third entry
079A	ioh_fsm_log_entr y_2	RW	UINT32	Input of a log entry in the diagnostic memory of the safety module. Writing only takes place after the third entry
079B	ioh_fsm_limit_sp eed_upper	RW	INT32	Limiting of rotational speed setpoint value, upper limit › 0
079C	ioh_fsm_limit_sp eed_lower	RW	INT32	Limiting of rotational speed setpoint value, lower limit only ‹ 0 permitted
079D	ioh_fsm_limit_torque_u pper	RW	INT32	Limiting of torque setpoint value, upper limit only › 0 permitted
079E	ioh_fsm_limit_torque_l ower	RW	INT32	Limiting of torque setpoint value, lower limit only ‹ 0 permitted
079F	ioh_fsm_deccelramp	RW	INT32	STOP ramp of the safety module

Tab. 196: List of important communication objects in the basic unit

10 Glossary

10.1 Safety terms and abbreviations

Term/abbreviation	Description
ALF	Additional Logic Function. Not a safety function. Enables the logical interconnection of internal inputs and outputs.
CCF	Common Cause Failure in accordance with EN ISO 13849-1.
DC avg	Average Diagnostic Coverage, diagnostic coverage in accordance with IEC 61508 and EN 61800-5-2.
FCT	Festo Configuration Tool, software for configuration and commissioning.
HFT	Hardware Fault Tolerance in accordance with IEC 61508.
Cat.	Category in accordance with EN ISO 13849-1, levels 1 … 4.
MTTFd	Mean Time To Failure (dangerous): time in years until the first dangerous failure occurs with 100% probability according to EN ISO 13849-1.
Emergency off	In accordance with EN 60204-1: electrical safety is ensured in case of emergency by switching off the electrical power to all or part of the installation. Emergency off is to be used where a risk of electric shock or other electrical risk exists.
Emergency stop	In accordance with EN 60204-1: functional safety is ensured in an emergency by bringing a machine or moving parts to standstill. Emergency stop is intended to stop a movement that can result in a hazard.
OSSD	“Output Signal Switching Device”: output signals with 24 V level cycle rates for error detection.
PFH	Probability of dangerous failures per hour in accordance with IEC 61508.
PL	Performance Level in accordance with EN ISO 13849-1: levels a … e.
SBC	Safe Brake Control in accordance with EN 61800-5-2.
SFF	Safe Failure Fraction [%], ratio of the failure rates of safe and dangerous (but detectable) failures to the sum of all failures in accordance with IEC 61508.
Safety relay unit	Device for execution of safety functions or achievement of a safe status of the machine by switching off the power supply to dangerous machine functions. The desired safety function is only achieved in combination with other measures for risk reduction.
SIL	Safety Integrity Level, discrete levels for determining the safety integrity requirements of safety functions in accordance with IEC 61508, EN 62061 and EN ISO 13849.
SILCL	Maximum SIL that can be used by a subsystem.

Term/abbreviation	Description
SLS	Safely Limited Speed in accordance with EN 61800-5-2.
SOS	Safe Operating Stop in accordance with EN 61800-5-2.
SS1	Safe Stop 1 in accordance with EN 61800-5-2.
SS2	Safe Stop 2 in accordance with EN 61800-5-2.
SSF	"Safe Speed Function", summarised safety functions with regard to speed monitoring and control.
SSM	Safe Speed Monitor in accordance with EN 61800-5-2.
SSR	Safe Speed Range in accordance with EN 61800-5-2.
STO	Safe Torque Off in accordance with EN 61800-5-2.
T	Service life in accordance with EN ISO 13849-1.
USF	"Universal Safety Function", combined safety functions.

Tab. 197: Terms and abbreviations

10.2 Terms for the SafetyTool and for safe parameterisation

Term	Meaning/function
Display unit	Unit in which the respective parameters are displayed. The desired display units for position values, speed values and acceleration values are specified by the program invoking start-up of the SafetyTool.
Display value	The value of a parameter converted to the desired display unit.
Basic unit	Motor controller as carrier of the safety module, in this case a CMMP-AS-...-M3.
Actual value	The current value of a parameter in the safety module, converted to the display unit
Communication object	Individual data element that can be read, written and validated by the SafetyTool.
Offline parameterisation	Operation of the SafetyTool without connection to the device (at the desk)
Online parameterisation	Operation of the SafetyTool with connection to the safety module (via the basic unit).

Term	Meaning/function
Product term	In order to configure switching conditions of the safety module, logic operations between the logical inputs and the virtual outputs and between the virtual outputs and the logical outputs are configured in the form of so-called product terms. A product term is an AND operation with or without inversion with a maximum of 7 inputs. Maximum of 4 product terms can be combined as an OR operation. The product terms (AND operation) and OR operations are generally termed gates.
Project	See SafetyTool project.
Check sum	Measure for guaranteeing the integrity of data that is sent or stored. Check sums are generated from the data and guarantee data parity sufficient under normal circumstances.
Quantisation	Some parameters are quantised (rasterised) by the safety module, e.g. if the value must be a multiple of a cycle time. In such cases, when reading out the safety module, a value can be fed back which is different from the written value. However, the specified quantisation ranges do not create any relevant deviations.
Quantisation range	Permissible deviation between the written value and the read value of a parameter. Values within the quantisation limit can be viewed as identical. The quantisation limit is read from the safety module during writing parameter access.
SafetyTool project	The SafetyTool allows the user to save the locally available parameterisation as a “SafetyTool project”. This file contains the parameters as display values (in contrast to the safe parameter set, to which device values are saved). The SafetyTool project can be sent to the safety module in an online session. The user must validate the sent parameters individually.
SCV	Safety Condition Violated.
SFR	Safety Function Requested.
Safe basic status	If the parameterisation is missing, invalid or not fully validated, the safety module switches to the safe basic status: power stage switched off, clamping unit or holding brake closed, outputs DOUT4x switched off at the safety module

Term	Meaning/function
Safe parameter set	The sum of all the parameters of the safety module forms a parameter set. If this parameter set contains a valid validation code, then it is a “safe parameter set”. The safe parameter set of an application is thus always located in a safety module that is ready for operation. In addition, it can be read out with the SafetyTool and stored on a storage medium, together with the validation code generated by the safety module. It is protected against changes on the storage medium with a check sum.
Safety module	CAMC-G-S3 as a plug-in module in the basic unit, which is responsible for the safety of the drive application. The parameterisation of this safety module takes place with the SafetyTool.
Setpoint value	The display value of a parameter specified by the user.
SSR	Safe State Reached.
Validation code	Content of a special communication object that is generated by the safety module when all parameters are validated.

Tab. 198: Terms for the SafetyTool and for safe parameterisation

Copyright:
Festo SE & Co. KG
Ruiter Straße 82
73734 Esslingen
Germany

Phone:
+49 711 347-0

Internet:
www.festo.com