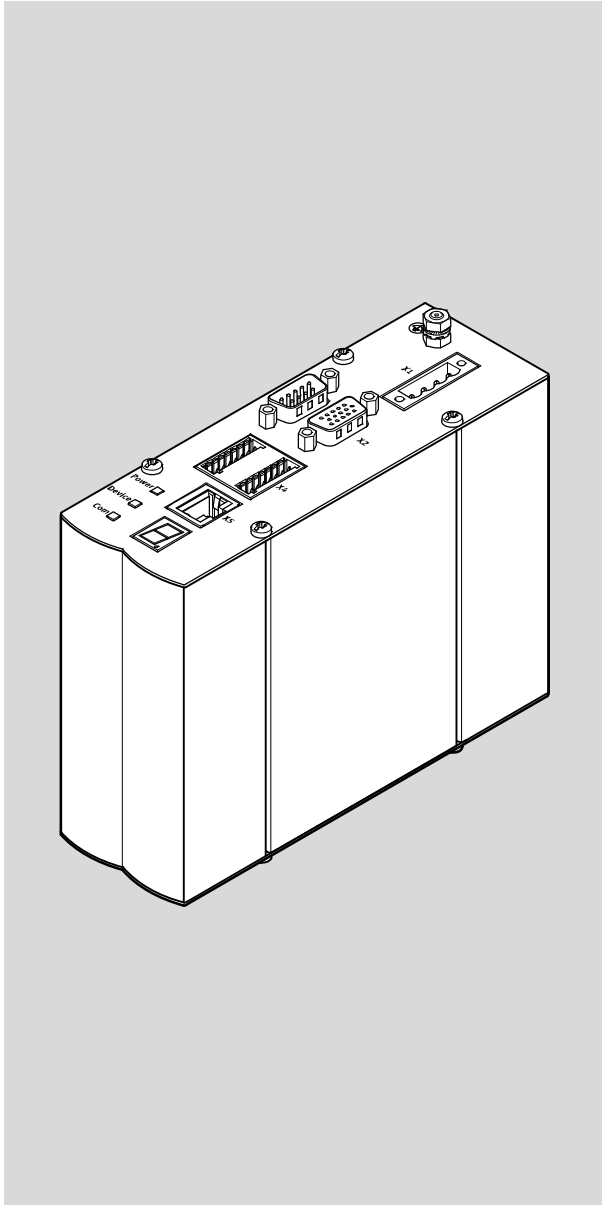


Controller

CMXH



FESTO

Description
STO

Safe Torque Off
(STO)

8067357
1612a
[8067359]

Identification of hazards and instructions on how to prevent them:



Danger

Immediate dangers which can lead to death or serious injuries



Warning

Hazards that can cause death or serious injuries



Caution

Hazards that can cause minor injuries

Other symbols:



Note

Material damage or loss of function



Recommendations, tips, references to other documentation



Essential or useful accessories



Information on environmentally sound usage

Text designations:

- Activities that may be carried out in any order
- 1. Activities that should be carried out in the order stated
- General lists
- Result of an action/References to more detailed information

Table of Contents – CMXH

Instructions on this documentation	4
1 Safety and requirements for product use	5
1.1 Safety	5
1.1.1 Safety instructions for use of the STO safety function (Safe torque off)	5
1.1.2 Intended use of the STO function	6
1.1.3 Safety characteristics	6
1.1.4 Foreseeable misuse of the STO function	6
1.1.5 Diagnostic coverage (DC) of the controller	6
1.2 Requirements for product use	7
1.2.1 Qualification of specialized personnel	7
1.2.2 Range of application	7
1.2.3 Specified standards	7
2 Function and application	8
2.1 Circuitry of the STO inputs	9
2.2 Functional description	10
2.3 STO function of the interface [X4]	11
2.3.1 Switching statuses	11
2.3.2 Switching times	12
2.3.3 Logic supply 24 V logic	12
3 Electrical installation	13
3.1 Installation	13
3.2 Notes on commissioning	14
3.3 Diagnostics	15
3.4 Obligations of the machine operator	15
A Technical appendix	16
A.1 Technical data	16
A.1.1 Safety engineering	16
A.1.2 Electrical data	17
A.2 Product conformity and certifications	18

Instructions on this documentation

This document only describes the utilisation of the safety function STO – “Safe Torque Off” in accordance with EN 61800-5-2, which is implemented in the controller CMXH, in combination with the related planar surface gantry EXCM-30/-40.

Documentation

The complete description of the system, comprising controller and gantry, includes the following documents:

Designation	Contents
Assembly instructions CMXH	Notes on mechanical installation of the CMXH.
Description EXCM-30/-40	Description of the mechanical installation of the planar surface gantry EXCM-30/-40
Description EXCM-30/40-...-PF-...	Commissioning of the planar surface gantry EXCM-30/-40 with the CMXH controller
Help system for the FCT plug-in CMXH	Help system in the FCT for support of commissioning and parameterisation of the CMXH controller
Description CMXH	Use of the STO safety function (“Safe Torque Off”).

Tab. 1 Documentation for the system EXCM-30/-40 with CMXH

Product identification, versions

This documentation refers to the following software versions:

CMXH firmware version	Required CMXH plug-in
V1.2 or later	V2.0 or later

Tab. 2 Software versions



The hardware version, firmware version and serial number are displayed in the software with an active online connection (➔ Configuration software FCT, “Controller” page).
If an online connection is currently unavailable, information relating to the last connection will be displayed.



Additional information about the product:
– Overview of accessories (catalogue) ➔ www.festo.com/catalogue
– Certificates, declaration of conformity ➔ www.festo.com/sp



Note
Before using a newer firmware version:
• Check whether a newer corresponding version of the FCT plug-in or user documentation is available ➔ www.festo.com/sp.

1 Safety and requirements for product use

1.1 Safety

When commissioning electrical drives:

- Always observe the safety instructions and warnings in the documentation of the controller (→ Tab. 1) and the documentation of the components used.
- Before mounting and installation work: Switch off the supply voltage. Secure against accidental reactivation. Only switch on the supply voltage again when mounting and installation work is complete.
- Never remove or insert a plug when the motor controller is powered.
- Observe the handling specifications for electrostatically sensitive devices.
- Only enable the controller if the drive has been professionally installed and fully parameterised.
- Do not carry out repairs on the controller. In the event of a defect: Replace the complete controller.

1.1.1 Safety instructions for use of the STO safety function (Safe torque off)



Caution

In order to achieve safety characteristics according to EN ISO 13849-1:

- Conduct a risk assessment of the application.
- Select the components and their wiring corresponding to the required category according to EN ISO 13849-1.



Caution

Failure of the safety function can result in serious, irreversible injuries, e.g. due to unexpected movements of the actuators.

- Do not bypass the connections for safety equipment.
- Observe the input voltage ranges of the controller → Chapter A.1.
- Only use the STO function when all of the necessary safeguards have been set up and are functional.
- Validate the STO function to complete commissioning.



Caution

Severe injuries as a result of uncontrolled movement of the passive actuators when switching off the power output stage. The STO function is insufficient as the sole safety function for drives that are subject to permanent torque (e.g. through suspended loads).

- Shut down the passive actuators mechanically if required, e.g. via a brake, to ensure that movements are prevented. This especially applies to vertical axes without automatic locking mechanics, clamping units or counterbalancing.

1.1.2 Intended use of the STO function

The controller supports the STO safety function (STO, Safe Torque Off) in accordance with EN 61800-5-2. The STO function is intended to shut down the torque from a motor that is connected to the CMXH, thereby preventing an unexpected restart of the motors. The STO function may only be used for applications in which the specified safety characteristics suffice.

1.1.3 Safety characteristics

The STO function of the CMXH fulfils requirements for the following characteristic safety values:

- PL e/Cat. 3 according to EN ISO 13849-1
- SIL CL 3 in accordance with EN 61800-5-2 / in accordance with EN 62061 / IEC 61508

The achievable safety level of the complete system depends on the other components that are used to implement the safety function.

To protect against unintended start-up, the controller must be activated via the connection [X4] with the category required for the application according to EN ISO 13849-1, e.g. via an external safety relay.

1.1.4 Foreseeable misuse of the STO function

Unintended use includes the following misuses:

- Bypassing of the safety function
- Use in applications where switching off can result in hazardous movements or conditions.

The STO function does not provide protection against electric shock, only against dangerous movements!

1.1.5 Diagnostic coverage (DC) of the controller

The diagnostic coverage (➔ Chapter A.1) is influenced by the interconnection of the controller in the control chain as well as the measures implemented for diagnostics.

In order to achieve the diagnostic coverage, the status of the diagnostic contacts must be evaluated by the control system with each request of the STO function.

If the signal does not correspond to the expected value, it can allude to a potentially dangerous malfunction, e.g. a wire break. In this case, appropriate measures must be implemented to maintain the safety level.



Note

The controller cannot detect a cross circuit in the input circuit by itself.

- Find out if cross-circuit detection is needed for the input circuit and wiring in your application.
- If required, use a safety switching device with cross-circuit detection.

1.2 Requirements for product use

For correct and safe use of the product in a machine or system:

- Provide the complete product documentation to the following specialists
 - the design engineer and installer of the machine or system
 - the personnel responsible for commissioning
- Keep the documentation safe throughout the entire product lifecycle.
- Ensure compliance with all of the specifications in the documentation for the controller (→ Tab. 1 Documentation for the system EXCM-30/-40 with CMXH).
- Also take into consideration the documentation for the other components (e.g. motors, cables, etc.).
- Take into consideration all of the legal regulations that are applicable for the installation site, as well as the following documents:
 - regulations and standards
 - regulations of the testing organisations and insurers
 - national specifications

For correct and safe use of the STO function:

- Conduct a risk assessment for your machine or system.
- Comply with the specified safety characteristics (→ Chapter A.1, Technical data).
- Comply with the connection and environmental conditions, in particular the voltage ranges of the product and all connected components. Only compliance with the limit values and load limits will enable operation of the product in compliance with the specified safety regulations.

1.2.1 Qualification of specialized personnel

The function should only be integrated into the machine by a qualified electrical technician of the machine manufacturer. The qualified technician must be familiar with:

- Installation and operation of electrical control systems
- the applicable regulations for operating safety-engineered systems
- the applicable regulations for accident prevention and occupational safety
- the documentation for the product

1.2.2 Range of application

The controller has the CE marking. The product-relevant EU directives can be found in the declaration of conformity. Additional information:

- Certificates and the declaration of conformity (→ www.festo.com/sp)
- Standards and test values (→ Chapter A.1, Technical data)

1.2.3 Specified standards

EN ISO 13849-1:2015
EN 60204-1:2006/AC:2010
IEC 61508-1...2/4...7:2010-04
EN 61800-5-2:2007-10
EN 62061:2005/A2

Tab. 1.1 Standards specified in the document

2 Function and application



Caution

Unexpected movement of the vertically built-in planar surface gantry when the output stage is shut down.

Risk of impact and crushing injuries.

- Only planar surface gantries with holding brakes may be installed vertically.
- Note the mechanical inertia of the holding brake.



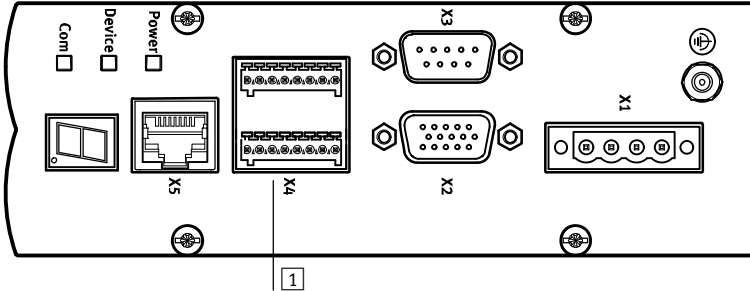
Note

Failure of the output stage.

If the output stage of the controller fails when an STO function is active, it may result in the drive jerking through a limited detent movement of the rotor. The rotation angle/ travel corresponds to the pole pitch of the motor used.

The STO function (“Safe Torque Off”) enables 2-channel, secure disconnection of the power supply to both motors connected to the controller.

The safety function is requested solely via the control ports of the switch-off functions interface [X4] on the controller. Safety-oriented circuitry for additional interfaces of the controller is not required.



1 Switch-off functions interface [X4]

Fig. 2.1 Switch-off functions interface [X4]

2.1 Circuitry of the STO inputs



To protect against unintended start-up, the controller must be activated via the connection [X4] with the category required for the application in accordance with EN ISO 13849-1. Attainable safety level of the STO function → Chapter 1.1.3.

The following components for requesting the STO function, for example, can be connected to the STO inputs (→ Tab. 3.1 Switch-off functions interface [X4]):

- Semiconductor safety outputs (electronic safety switching devices, active safety sensors, e.g. light curtains with OSSD signals) (OSSD = “Output Signal Switching Device”)
- Switch contacts (safety switching devices with relay outputs, passive safety sensors, e.g. forced position switches)

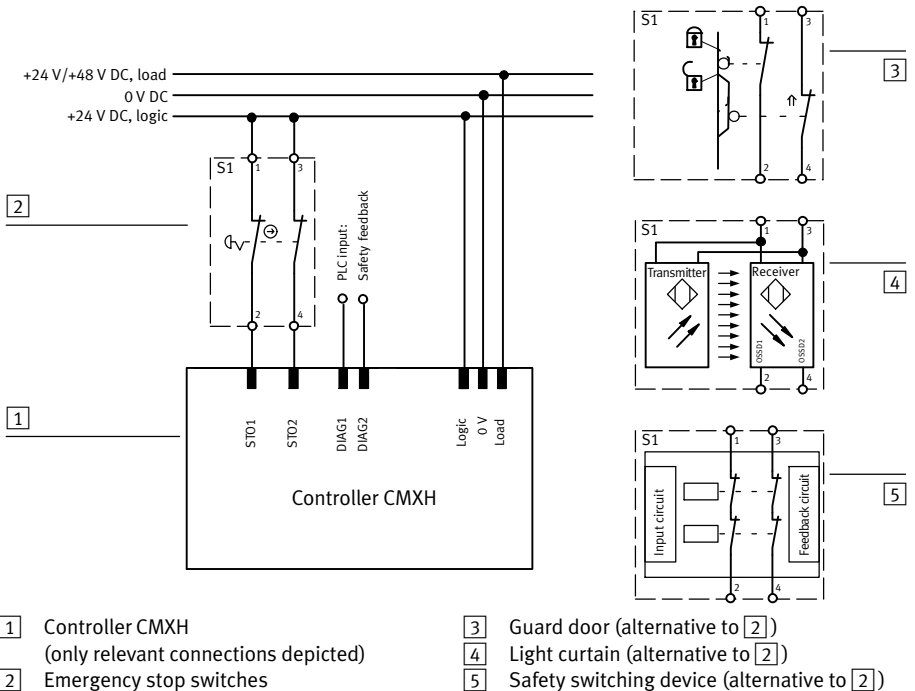


Fig. 2.2 Switching example (without cross-circuit detection)

2.2 Functional description

The STO function is requested over 2 channels via switch S1, whereby the control voltage (+24 V DC, logic → Fig. 2.2) is switched off at both inputs STO1 and STO2.

The STO inputs are of equal value, i.e. it makes no difference in which sequence they are connected.

The controller monitors the status of the STO inputs and switches off the driver supply for the output stages as soon as logic 0 (0 V) is present at **one** of the STO inputs. Power supply of the motors is interrupted via the power output stages:

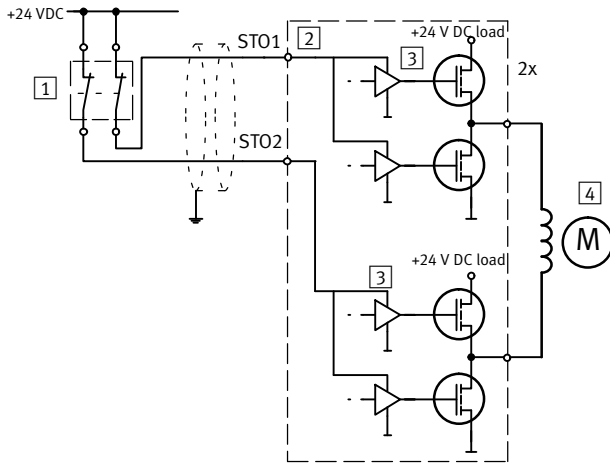
- Behaviour of the drive with running motors: The movement of the drive is not decelerated via a braking ramp of the controller. The drive continues to move uncontrolled due to inertia or external forces until it comes to a standstill by itself.
- Behaviour of the drive with a stopped motor: The drive is uncontrolled and can move due to external forces.



Note

For motors with integrated holding brake, the holding brake is activated by the non-safety-relevant firmware of the device. When the output stage is switched off, there is no deceleration of the drive via a braking ramp. The holding brake is closed immediately. If the motor is running, this results in increased wear and can lead to damage to the motors if it occurs repeatedly.

The **2-channel** disconnection of the output stages is indicated by the DIAG1/DIAG2 diagnostic contact. The status of the STO function can be reported to an external safety switching device for diagnostics, for example, via the diagnostics contact. The diagnostics contact is not evaluated in terms of safety engineering.



1 Input circuit (e.g. safety relay)

2 Power output stage in CMXH
(only one phase shown)

3 Driver supply

4 Motor (only one phase shown)

Fig. 2.3 “Safely switched off torque” functional principle

2.3 STO function of the interface [X4]

2.3.1 Switching statuses



The STO inputs do not have voltage monitoring.
If required, voltage monitoring must be achieved through additional measures.

Inputs STO1/STO2:

As long as a logic 1 (+24 V DC) is present at both STO inputs, the motors can be operated. If there is a logic 0 (0 V DC) at one or both of the STO inputs, the voltage supply to the motors is interrupted. At the same time, error 0x34 is triggered. When both STO inputs receive logic 1 again, the error 0x34 must first be acknowledged before the drive can be enabled again.

Diagnostic contacts DIAG1/DIAG2:

The diagnostic contacts are closed when the STO function is active.

The diagnostic contacts are opened:

- in the event of a failure of the logic voltage or supply voltage
- if the STO function is inactive

STO1	STO2	DIAG1/DIAG2	Status
1	1	High impedance (open)	Normal operation – Output stages are switched on. – STO function is inactive.
1	0	High impedance (open)	The STO function has been requested on one channel, e.g. in the event of a failure of a channel: – Output stages are switched off through 1 channel. – The motors can no longer be operated. – STO function is inactive.
0	1		
0	0	Low impedance (closed)	The STO function has been requested on 2 channels. – Output stages are switched off through 2 channels. – The motors can no longer be operated. – The STO function is active.

Tab. 2.1 Switching logic of the inputs STO1/STO2

Switching statuses [X4]			
Inputs STO1/STO2 ¹⁾			
Logic 1	[V DC]	>	20.4
0-signal	[V DC]	<	5
Diagnostic contacts DIAG1/DIAG2			
Closed: Max. internal resistance	[Ω]	≤	40
Open: off-state current	[μA]	≤	2

1) Intermediate area is undefined

Tab. 2.2 Electrical data of switching statuses [X4]

2.3.2 Switching times

The amount of energy stored in the components of the STO function (e.g. capacitors) depends on the input voltage level. These amounts of energy must be charged or discharged depending on the switching operation. Depending on the input voltage, this results in different values for the transition to the safe status (STO) and the tolerance time (buffer time) compared to signals of safety-relevant output switching elements of Electro-Sensitive Protective Equipment (Output Signal Switching Device = OSSD).

Signal¹⁾	Switching time¹⁾		
STO1/STO2	Activate STO	[ms]	≤ 2
	Deactivate STO	[ms]	> 8
DIAG1/DIAG2	Close diagnostics contact	[ms]	≤ 10
	Open diagnostics contact	[ms]	≤ 20

1) Other electrical data → Chapter A.1.2

Tab. 2.3 Switching times

2.3.3 Logic supply 24 V logic

A 24 V auxiliary supply is available at [X4.1] and [X4.16].

The reference potential (0 V) is [X4.8].

The logic supply can be optionally used to supply external, active sensors.

Other electrical data → Chapter A.1.2.

3 Electrical installation



Warning

Electric shock from voltage sources without safeguarding.

- For the electrical power supply, only use PELV circuits compliant with EN 60204-1 (Protective Extra-Low Voltage, PELV).
- Observe the general requirements of EN 60204-1 for PELV circuits.
- Use only voltage sources which guarantee reliable electrical isolation of the operating and load voltage in accordance with IEC 60204-1.

3.1 Installation



Caution

Unexpected and unintended movement of the drive during mounting, installation and maintenance work.

- Before starting work: Switch off power supplies. Cancelling the enable signal on the controller is not sufficient.
- Secure the power supplies against accidental reactivation.

Installation instructions:

- Observe all of the information on electrical installation of the controller → Tab. 1.
- Comply with the handling specifications for electrostatically sensitive devices.
- Use the plug connector [X4] included in the scope of delivery of the controller.
- Connect the STO inputs in 2 channels with parallel wiring.



Note

Damage to the device in the event of an overload.

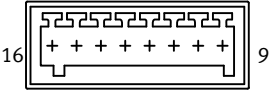
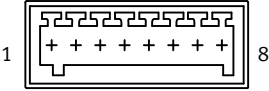
Pin [X4.1] and [X4.16] (24-V logic) are not overload-proof! Max. 100 mA permissible.



Note

The STO function must never be bridged.

- Make sure that no jumpers etc. can be used parallel to the safety wiring, e.g. by using the maximum cable cross section of 0.5 mm².

Connection X4		Pin	Function	
Top row 	16	24 V logic	Output	Logic voltage +24 V
	15	ESTOP ¹⁾	Input	External stop, trigger braking ramp (at 0 V)
	14	RB ²⁾	Input	With +24 V: Release brake With 0 V: Brake control via the control word CCON ³⁾
	13	–		Reserved
	12	–		
	11	–		
	10	–		
	9	–		
Bottom row 	1	24 V logic	Output	Logic voltage +24 V
	2	STO1	Input	Safe Torque Off function: With 0 V: safely switching off supply voltage to the motors
	3	STO2	Input	
	4	–		Reserved
	5	FAULT ⁴⁾	Output	With +24 V: Fault is present
	6	DIAG1		Potential-free diagnostic contacts (Low impedance if the STO function has been requested and activated via 2 channels.)
	7	DIAG2		
	8	0 V GND		GND (reference potential)

- 1) At rest, the output stage is switched off and any motor brakes present are closed.
- 2) Detailed information about the brake function (→ Description for the module EXCM-30/-40-...-PF)
- 3) If no controller has master control, the brake remains in its last status when 0 V is applied.
- 4) The output is high impedance. To signal errors, a low impedance consumer is used.

Tab. 3.1 Switch-off functions interface [X4]

3.2 Notes on commissioning



Note

It is recommended that at least the STO function should be wired at initial start-up. The complete commissioning of the controller by the machine manufacturer is described in the description EXCM-30/-40-...-PF and in the Online Help for the CMXH plug-in of the FCT software.



Caution

Incorrect wiring or use of inappropriate components will result in failure of the STO function or non-compliance with the requirements of EN ISO 13849-1 (category).

Prior to commissioning:

- Make sure that components are used and wired in accordance with the required category according to EN ISO 13849-1.
- Check the electrical installation (connecting cable, pin allocation).
- Validate the STO function to conclude the installation process and after every modification to the installation.
- Only use the STO function when all of the necessary safeguards have been set up and are functional.

For a performance test of the STO function:

1. Switch off each channel individually, and check the reaction of the motors and diagnostics contacts.
2. Switch off both channels and check the reactions.

3.3 Diagnostics

Diagnostics	Description
Potential-free diagnostic contacts ¹⁾	The potential-free diagnostic contacts of the STO function (DIAG1/DIAG2) can be evaluated by a higher-order controller. Closed diagnostic contacts show that the STO function is active.
Error message 0x34	When the STO function is requested, the error "Safe torque off" (0x34) is generated and displayed cyclically on the 7-segments display of the controller. An entry of the error in the diagnostic memory is optional.

1) This diagnosis is **not** evaluated in terms of safety.

Tab. 3.2 Diagnostics options of the STO function



For additional information on the 7-segment display and complete error lists (→ Description EXCM-30/-40-...-PF)

3.4 Obligations of the machine operator

The implemented safety function must be subjected to a regular and documented performance test by a specialist during the machine's period of use. The frequency of these tests must be determined by the machine operator based on the specifications of the machine manufacturer. An inspection of the controller is recommended at least once a year.

A Technical appendix

A.1 Technical data



The general technical data, operating and ambient conditions and additional connection data can be found in the commissioning of the planar surface gantry EXCM-30/-40 with the controller CMXH (→ Description EXCM-30/-40-...-PF).

A.1.1 Safety engineering

Safety reference data and safety specifications			
Safety function		STO	Safe Torque Off (safely switched-off torque)
Category		3	In accordance with EN ISO 13849-1
Performance Level		PL e	In accordance with EN ISO 13849-1
Safety Integrity Level		SIL CL 3	In accordance with EN 61800-5-2 (Safety integrity level)
SIL Claim Limit		SIL CL 3	In accordance with EN 62061 (SIL Claim Limit)
Systematic Capability		SC 3	In accordance with IEC 61508 (Systematic suitability)
DCavg	[%]	90	Average Diagnostic Coverage (Average degree of diagnostic coverage) → Chapter 1.1.3
SSF	[%]	99	Safe Failure Fraction (Proportion of safe failures)
MTTF _d	[Years]	5700	Mean Time To dangerous Failure (Mean time until a dangerous failure)
HFT		1	Hardware Failure Tolerance (hardware fault tolerance)
PFH	[1/hr]	2×10^{-9}	Probability of Dangerous Failure per Hour (Probability of a dangerous failure per hour)
T			
Proof Test Interval	[Years]	20	Inspection interval
Service life	[years]	20	In accordance with EN ISO 13849-1
Type test	The STO function has been certified by an independent testing body. Certificate CMXH → www.festo.com/sp		

Tab. A.1 Safety reference data and safety specifications

A.1.2 Electrical data

Inputs STO1/STO2 [X4.2]/[X4.3]		
Nominal voltage	[V DC]	24 (relative to 0 V at [X1.3])
Voltage range	[V DC]	21.6 ... 28.8
Permissible residual ripple	[%]	5 (relative to nominal voltage 24 V)
Nominal current	[mA]	20
Starting current	[mA]	200
Input voltage thresholds (intermediate range is undefined)		
Logic 1	[V DC]	> 20.4
Logic 0	[V DC]	< 5
Activate STO function switching time	[ms]	≤ 2
Deactivate STO function switching time	[ms]	> 8

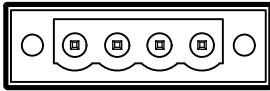
Tab. A.2 Electrical data for inputs STO1 and STO2

Potential-free diagnostic contacts DIAG1/DIAG2 [X4.6]/[X4.7]		
Version		Semiconductor relay
Max. voltage	[V DC]	≤ 30
Nominal current	[mA]	100
Max. internal resistance (contact closed)	[Ω]	≤ 40
Residual current (contact open)	[μA]	≤ 2
Switching time closing	[ms]	≤ 10
Switching time opening	[ms]	≤ 20
Galvanic separation		Via optocoupler
Protective function		Overvoltage resistant to 60 V DC (checked)

Tab. A.3 Electrical data of the diagnostic contacts

Logic voltage 24 V logic [X4.1]/[X4.16]		
Nominal voltage	[V DC]	24
– Supply via [X1.4] – Not additionally filtered or stabilised		
Nominal current	[mA]	100 (max.)
Overload protection		Not overload-proof

Tab. A.4 Electrical data of the 24 V logic output

Connection [X1]	Pin	Function		
	1	GND	0 V	Reference potential for load voltage
	2	Load voltage	+24 V ±10 % or +48 V ±10 %	Power supply of the power output stages of the motors
	3	GND	0 V	Reference potential for logic voltage
	4	Logic voltage	+24 V ±15 %	Power supply for the control electronics and brakes

Tab. A.5 Voltage supply [X1] connection

Signal lines		
Max. cable length	[m]	30
Cable cross section	[mm ²]	0.14 ... 0.5

Tab. A.6 Technical data of the cabling at [X4]

A.2 Product conformity and certifications

Product conformity and certifications	
CE marking (see declaration of conformity → www.festo.com)	In accordance with EU EMC Directive ¹⁾ In accordance with EU Machinery Directive
Approvals	RCM (Regulatory Compliance Mark)

1) The component is intended for industrial use. Outside of industrial environments, e.g. in commercial and mixed-residential areas, actions to suppress interference may have to be taken.

Tab. A.7 Product conformity and certifications

Reproduction, distribution or sale of this document or communication of its contents to others without express authorization is prohibited. Offenders will be liable for damages. All rights reserved in the event that a patent, utility model or design patent is registered.

Copyright:
Festo AG & Co. KG
Postfach
73726 Esslingen
Germany

Phone:
+49 711 347-0

Fax:
+49 711 347-2144

E-mail:
service_international@festo.com

Internet:
www.festo.com

Original: de