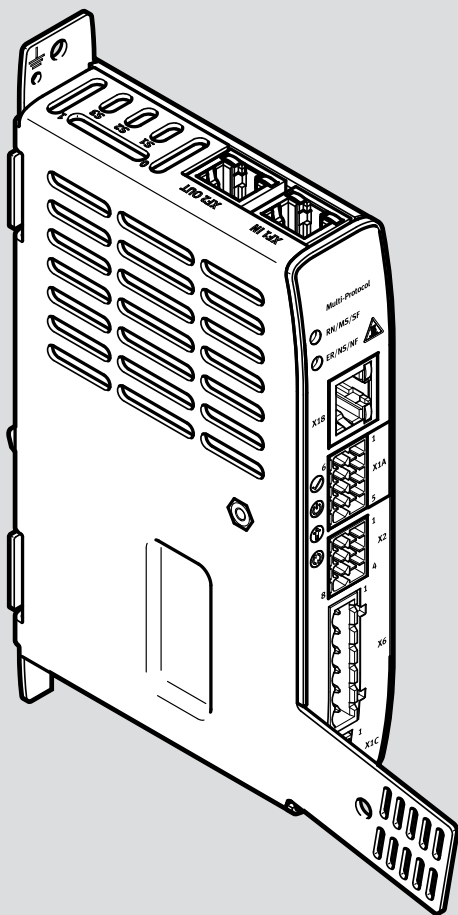


CMMT-ST-C8-1C-MP-S0

Servo drive

FESTO

Manual | Safety sub-
function | STO, SS1-t



8214124

8214124
2024-04a
[8214126]

Original instructions

ET 200, PNOZ, Pilz, SIEMENS, SIMATIC ET 200SP are registered trademarks of the respective trademark owners in certain countries.

Table of contents

1	About this document	5
1.1	Target group	5
1.2	Applicable documents	5
1.3	Product version	5
1.4	Product labelling	5
1.5	Specified standards	5
2	Safety	5
2.1	Safety instructions	5
2.2	Intended use	6
2.2.1	Range of application	6
2.2.2	Permissible components	6
2.3	Foreseeable Misuse	6
2.4	Training of qualified personnel	7
2.5	Product conformity	7
2.6	Safety engineering approval	8
3	Additional information	8
4	Product overview	8
4.1	Safety sub-functions	8
4.1.1	Function and application	8
4.1.2	Safety sub-function STO	8
4.1.3	Safety sub-function SS1-t	12
4.1.4	Cross-wiring of several servo drives	14
4.1.5	Fault exclusion	14
4.1.6	Safety relay unit	14
4.1.7	Interfaces of the PDS	15
5	Installation	15
5.1	Safety	15
5.2	STO installation	16
5.3	SS1-t installation	19
5.4	Installation for operation without safety function	19
5.5	Connection Examples, Cross-wiring	19
6	Commissioning	23
6.1	Safety	23
6.2	Check lists	23
7	Operation	26
8	Malfunctions	26
8.1	Diagnostics via LED	26
8.2	Repair	27

9 **Technical data** 27

9.1 Technical data, safety engineering. 27

9.2 Technical data, general. 29

9.3 Technical data, electrical. 31

 9.3.1 Digital inputs and outputs [X1A]. 31

1 About this document

1.1 Target group

The document is targeted towards individuals who mount and operate the product. It is additionally targeted towards individuals who are entrusted with the planning and application of the product in a safety-oriented system.

1.2 Applicable documents

This document describes the use of the safety sub-function safe torque off (STO/Safe torque off) in accordance with EN 61800-5-2.

The safety sub-function safe stop 1 time controlled (SS1-t/Safe stop 1 time controlled) can be implemented with a suitable external safety relay unit and appropriate servo drive circuitry.

- Observe the safety instructions in the documentation → Operating instruction Assembly Installation Safety sub-function.



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

1.3 Product version

This documentation refers to the following version:

- Servo drive CMMT-ST-...-S0, revision 1 and higher, see product labelling.

1.4 Product labelling

Product labelling → Manual Assembly, Installation.

1.5 Specified standards

Version		
EN ISO 12100:2010-11		EN 61800-5-1:2007+A1:2017+A11:2021
EN ISO 13849-1:2023		EN 61800-3:2023
EN ISO 13849-2:2012-10		EN 61800-5-2:2017
EN ISO 14118:2018-02		EN 61800-2:2015
EN 60204-1:2018-09		EN 61508 Parts 1-7:2010
EN 61131-2:2007		–

Tab. 1: Standards specified in the document

2 Safety

2.1 Safety instructions

The product may generate high frequency interference, which may require interference suppression measures in residential areas.

It is only possible to determine whether the product is suitable for specific applications by also assessing further components of the subsystem.

Analyse and validate the safety function of the entire system.

Check the safety functions at adequate intervals for proper functioning. 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. Time period for cyclical test → 9.1 Technical data, safety engineering.

Prior to initial commissioning, wire the control inputs of the safety sub-function STO. The safety sub-function STO-t is always available without the need for any additional parameterisation.

Keep the documentation available throughout the entire product lifecycle.

2.2 Intended use

The safety function might fail, malfunctions might occur, and the connected actuator technology might move unintentionally if you do not comply with the parameters required for the ambient and connection conditions.

The CMMT-ST-...-S0 supports the following safety sub-functions in accordance with EN 61800-5-2:

- Safe torque off (STO/Safe torque off)
- Safe stop 1 time controlled (SS1-t/Safe stop 1 time controlled) can only be implemented with a suitable safety relay unit and appropriate servo drive circuitry

The safety sub-function STO is intended to switch off the torque of the connected motor, thereby preventing an unexpected restart of the motor.

The safety sub-function SS1-t is intended to perform a fast stop with subsequent torque switch-off.

Ensure that wiring is cross-circuit proof in accordance with EN ISO 13849-1.

2.2.1 Range of application

The device is intended for use in an industrial environment.

Safety sub-functions may only be used for applications for which the stated safety reference values are sufficient → 9 Technical data.

2.2.2 Permissible components

The load and logic power supply must meet the requirements of EN 60204-1 (protective extra-low voltage, PELV).

2.3 Foreseeable Misuse

Foreseeable misuse of the safety sub-function STO

- Use outside the limits of the product defined in the technical data.
- Bypassing of the safety function.
- Cross-wiring of the diagnostic feedback signals of more than 10 servo drives. This applies to all devices that are wired together, regardless of the type of equipment.
- Faults in the cross-wiring of passive diagnostic contacts and active diagnostic outputs will result in incorrect diagnostic feedback. It is therefore important to take extra care when carrying out the cross-wiring. Only wire devices as follows: Always wire all devices with active diagnostic output, e.g. CMMT-AS, in parallel as a group. Connect the signal from the active diagnostic outputs with the first CMMT-ST. Wire the passive diagnostic contacts as a group in series and connect the last passive diagnostic contact directly to the safe controller for evaluation of the diagnostic information.

- Use of the diagnostic contact STA to switch a safety function.
The diagnostic contact STA must not be used to open a secure locking mechanism directly, for example.
The diagnostic contact STA is not part of the safety circuit. The diagnostic contact STA is used to improve diagnostic coverage of the related safety sub-function. The diagnostic contact STA may only be used in combination with the related safe control signals (AND operation) plus a reliable time monitoring function in the safety relay unit for the purpose of switching additional safety-critical functions.
- At low level, the safety relay unit used delivers a higher current than permissible (maximum permissible input current exceeded with low level at STO-/A/B → Tab. 19 Control inputs #STO-A and #STO-B at [X1A]). When this occurs, the device cannot recognise when the safety sub-function is requested.
- Use of the safety sub-function STO without external measures for drive axes influenced by external torques.
If external torques influence the drive axis, use of the safety sub-function STO on its own is not suitable for stopping the axis safely. Additional measures are required to prevent dangerous movements of the drive axis, such as use of a mechanical brake.
- Operation of EC motors requiring a safety classification of SIL 3, cat. 3, Pl e without evaluation of the diagnostic contact STA.
- Operation of the connected motor without the danger zone being restricted or enclosed by suitable means.
The user must not be able to enter the danger zone without triggering the safety function.
- The safety sub-function STO does not provide protection against electric shock, only against dangerous movements.
- The safety sub-function STO cannot prevent non-safety-related sub-functions from failing, e.g. the braking ramp for the SS1-t function or the device's temperature monitoring function.

2.4 Training of qualified personnel

The product may be installed and commissioned only by a qualified electrical engineer who is familiar with:

- The installation, operation and maintenance of electrical control systems
- Applicable regulations for operating safety-related systems

Work on safety engineering systems may only be carried out by qualified personnel trained in safety engineering.

2.5 Product conformity

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

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

Tab. 2: Product conformity

2.6 Safety engineering approval

The product is a safety device in accordance with the EC Machinery Directive. For details of the safety-oriented standards and test values with which the product complies and fulfils, see → 9.1 Technical data, safety engineering. Please note that compliance with the listed standards is limited to the CMMT-ST-...-S0.

3 Additional information

- Contact the regional Festo contact if you have technical problems → www.festo.com.
- Cyber security information → www.festo.com/psirt.

4 Product overview

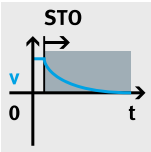
4.1 Safety sub-functions

4.1.1 Function and application

The servo drive CMMT-ST-...-S0 has the following safety-related performance features:

- Safe torque off (STO/Safe torque off)
- Safe stop 1 time controlled (SS1-t/Safe stop 1 time controlled) with use of a suitable external safety relay unit and appropriate servo drive circuitry
- Diagnostic contact STA for feedback of the active safety sub-function STO

4.1.2 Safety sub-function STO



The function described here implements the safety sub-function STO according to EN 61800-5-2 (corresponds to stop category 0 from EN 60204-1).

The safety sub-function STO is used when the power supply to the motor needs to be switched off safely in the application but there are no further requirements for a targeted standstill of the drive (such as stop category 1 from EN 60204-1 → Safety sub-function SS1-t).

Function and application of STO

The safety sub-function STO switches off the driver power supply for the power semiconductor, thus preventing the power output stage from supplying the energy required by the motor. The power supply to the drive is safely disconnected when the safety sub-function STO is active. The drive cannot generate torque and thus cannot perform any dangerous movements.

With suspended loads or other external forces, additional measures must be put in place to prevent movements being performed (e.g. mechanical clamping units). The standstill position is not monitored in the STO state.

The machines must be stopped and locked safely. This especially applies to vertical axes without automatic locking mechanism, clamping unit or counterbalancing.

Functional principle of STO

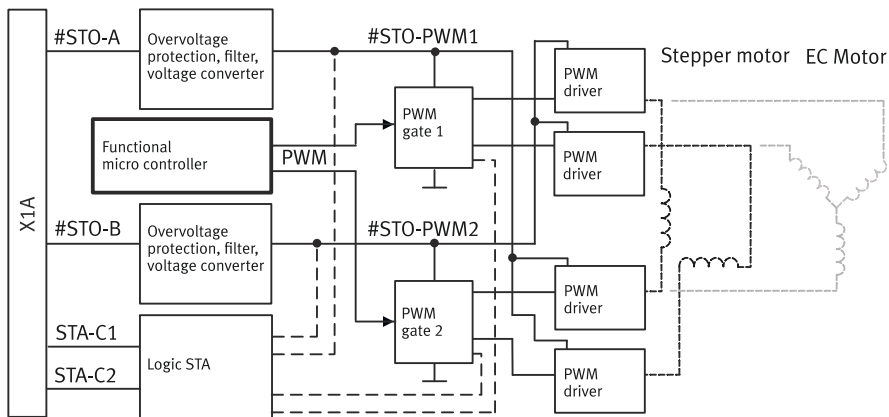


Fig. 1: Functional principle of STO

STO request

The safety sub-function STO is requested on 2 channels by simultaneously switching off the control voltage at both control inputs #STO-A and #STO-B.

The signals of inputs #STO-A/B are low active, so they are marked with #.

The drive responds as follows when the safety sub-function STO is requested:

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

The safe state is achieved after the safety sub-function STO has been requested if all motor coils are switched off and current cannot flow through them.

NOTICE

Detent movement if the power stage fails.

If power stage of the device fails, the drive can move once by the angle of rotation/travel of the pole pitch of the motor used.

- Take the possible movement into account when designing the safety function of the system.

After the safety sub-function STO has been requested and the request completed, the functional controller enable must be activated.

Feedback via diagnostic contact STA

The state of the safety sub-function STO can be reported to the safety relay unit via the diagnostic contact STA.

If the safety classification of SIL 3, cat. 3, Pl e is required for operation with an EC motor, the diagnostic contact STA must be evaluated.

The diagnostic feedback signal STA has been designed as a potential-free contact (Opto relay). The diagnostic contact STA is only closed (conductive) when STO is requested on 2 channels via the control inputs #STO-A and #STO-B. If the contact is closed (conductive), the STO state has been achieved (safe state).

#STO-A	#STO-B	STA-C1/C2
Low level	Low level	Diagnostic contact closed (low resistance)
Low level	High level	Diagnostic contact open (high resistance)
High level	Low level	
High level	High level	

Tab. 3: State of the diagnostic contact STA

If the safety sub-function STO is not requested but protective functions are triggered simultaneously on both channels (#STO-A and #STO-B), e.g. if the voltage at #STO-A and #STO-B is too high, the internal protective functions switch off the channels as if STO had been requested and the diagnostic contact STA is closed (safe state feedback).

Recommendation: the safety relay unit should check the state of the diagnostic contact whenever there is an STO request. The state of STA must change according to the logic table. The safety relay unit can cyclically test the #STO-A and #STO-B signals for high level with low test pulses and for low level with high test pulses, within the specified limits → 4.1.6 Safety relay unit.

The diagnostic contact STA is not evaluated in terms of safety engineering.

STO timing

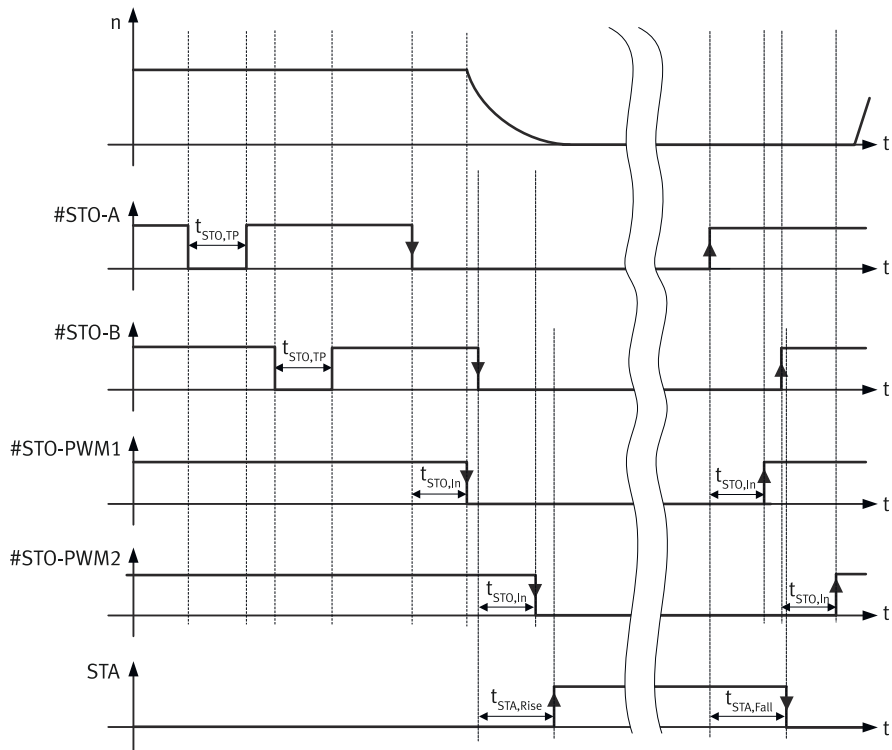


Fig. 2: STO timing graph (example with low test pulses)

Legend for STO timing

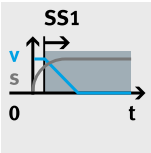
Term/abbreviation	Explanation
#STO-A/#STO-B	2-channel input for STO request
#STO-PWM1/#STO-PWM2	Internal control, PWM driver 1 and 2
$t_{STO,TP}$	Length of low test pulses ¹⁾ at #STO-A/B
$t_{STO,in}$	Max. delay until STO switches off ($\leq$ permissible reaction time when a safety sub-function is requested ¹⁾)
STA	Feedback, STO active
$t_{STA,Rise}$	Maximum permissible delay ¹⁾ for diagnostic feedback after the safety function is requested

Term/abbreviation	Explanation
$t_{STA, Fall}$	Maximum permissible delay ¹⁾ for diagnostic feedback after the safety function request has ended
n	Rotational speed

1) see technical data, safety reference data STO

Tab. 4: Legend for STO timing

4.1.3 Safety sub-function SS1-t



The function described here implements the safety sub-function SS1-t according to EN 61800-5-2. The safety sub-function SS1 is used when the motor needs to be braked and the power supply to the motor then has to be safely switched off in the application but there are no further requirements for a targeted standstill of the drive (controlled stop, stop category 1 according to EN 60204-1).

Together with a suitable safety relay unit, the following can be achieved:

- Safe stop 1 time controlled (SS1-t/Safe stop 1 time controlled); triggering of motor deceleration and, after an application-specific time delay, triggering of the safety sub-function STO

Requirements of SS1-t

- Wire the safety sub-function STO.
- Execute emergency stop command by means of the safety relay unit (either directly by wiring CTRL-EN accordingly or indirectly via a further functional controller).
- The time for executing an emergency stop is known.
- The safety relay unit supports programmable timers and simple logic elements.

Function and Application of SS1-t

The procedure for triggering SS1-t comprises the following steps:

1. Request for a functional emergency stop (e.g. remove CTRL-EN signal)
This causes the servo drive to trigger a braking ramp function and – if present – allows the brake function to engage at the end of the braking ramp. On completion of the braking ramp and once the parameterisable delay time for brake closing has elapsed, the power stage is functionally switched off.
2. Start of a time-delay element for control of STO
3. Request for a safety sub-function STO once the delay time has elapsed

The figure below shows the necessary logic circuits for the safety relay unit:

The delay times are directly included in the reaction time of the system.

SS1-t Feedback

The STA signal can be used as feedback for the safety sub-function SS1-t.

SS1-t Timing

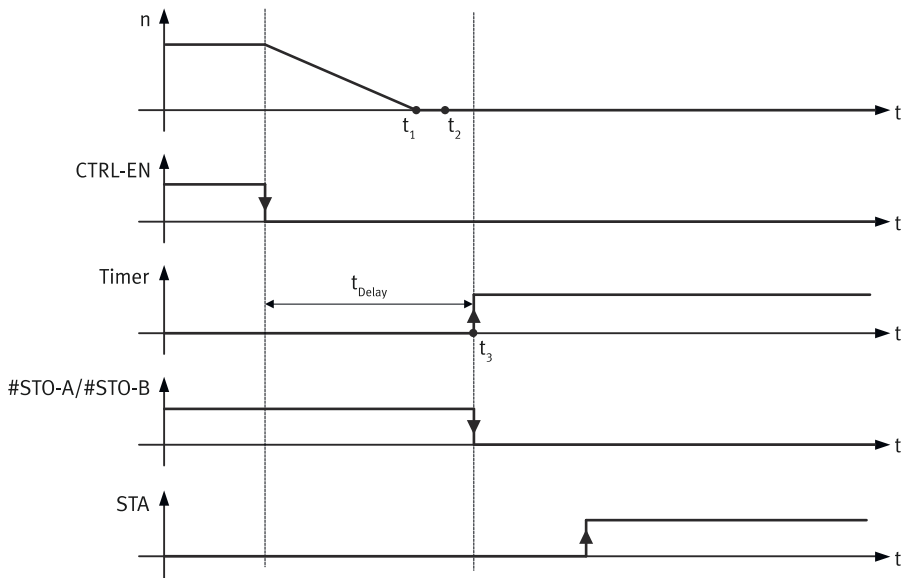


Fig. 3: SS1-t timing graph

Legend for SS1-t timing

Term/abbreviation	Explanation
Timer	Delay element in safety relay unit
CTRL-EN	Enable signal
t_{Delay}	Delay time until STO request
#STO-A/B	2-channel input for STO request
STA	Feedback, STO active
t_1	Braking ramp completed (controlled functionally), rotational speed = 0
t_2	Brake closed (if present) and output stage switched off (functionally)
t_3	$t_3 > t_2$
n	Rotational speed

Tab. 5: Legend for SS1-t timing



- If there are suspended loads and a motor with holding brake is used, they usually drop if STO is requested immediately before the braking ramp has elapsed, because the engagement time of the holding brake plays a significant role.
 - The time t_3 must always be set to a value longer than the total of the braking ramp time t_1 and the brake engagement time ($t_2 - t_1$). This prevents the following:
 - Suspended loads potentially dropping
 - Increased wear on the holding brake
-
- When selecting the delay time t_{Delay} , make sure it is long enough to account for the maximum braking ramp time and brake engagement time.

4.1.4 Cross-wiring of several servo drives

Whether cross-wiring of the diagnostic contact is permissible depends on the safety classification required.

The diagnostic contact must be evaluated separately for EC motors with the classification SIL 3, cat. 3, PL e. It is not permissible to cross-wire the diagnostic contact. In all other cases, the following rules apply when cross-wiring several servo drives:

- Wire inputs #STO-A and #STO-B in parallel in each case.
- Wire diagnostic contacts STA-C1/C2 in series in each case.
- Wire the diagnostic contacts of a maximum of 10 servo drives in series. The maximum cable length applies to the entire line, from the safety relay unit to the final device.

Example of cross-wiring → 5.5 Connection Examples, Cross-wiring.

4.1.5 Fault exclusion

Put suitable measures in place to prevent faulty wiring:

- Exclude wiring faults in accordance with EN 61800-5-2
- Configure the safety relay unit to monitor the outputs of the safety relay unit and wiring up to the servo drive

4.1.6 Safety relay unit

Use suitable safety relay units with the following characteristics:

- 2-channel outputs with
 - Detection of shorts across contacts
 - Required output current (also for STO)
- Evaluation of the diagnostic contact of the servo drive

Safety relay units with test pulses can be used with the following restrictions:

- High test pulses up to a maximum length of 1 ms
- Low test pulses up to a maximum length of 1 ms
- Test pulses are not simultaneous/overlapping on #STO-A/B

The safety relay units Pilz PNOZmulti, Pilz PNOZmulti Mini or SIEMENS SIMATIC ET 200SP with PP-switching output modules, SIEMENS ET 200S, for example, would be suitable.

The Festo input module CPX-F8DE and output module CPX-FVDA-P2 would also be suitable. Comment: the safe output module CPX-FVDA-P2 can only switch potential-free loads. Therefore, it can only be used in combination with an interposed relay, since #STO-A and #STO-B are referred to GND. Detection of shorts across contacts is then only possible as far as the relay. Detection of shorts across contacts is not possible on the CMMT-ST itself, so cross-circuit-proof wiring is required in this case.

4.1.7 Interfaces of the PDS

The interfaces of the PDS(SR) (Power Drive System, safety related in accordance with EN 61800-5-2) to the outside world are:

- Power supply
- Inputs and diagnostic feedback signals
- Movement of the shaft

5 Installation

5.1 Safety

WARNING

Risk of injury due to electric shock.

- For the electrical power supply with extra-low voltages, use only PELV circuits that guarantee a reinforced isolation from the mains network.
- Observe IEC 60204-1/EN 60204-1.



Comprehensive information concerning the electrical installation of the device → 1.2 Applicable documents, Manual Assembly, Installation.

Information for operation with safety function

NOTICE

Check the safety functions to conclude the installation process and after every modification to the installation.

During installation of safety-related inputs and outputs, also observe the following:

- Meet all specified requirements, e.g.:
 - Surrounding area (EMC)
 - Logic and load voltage supply
 - Mating plug
 - Connecting cables
 - Cross-wiring

More information → 1.2 Applicable documents, Manual Assembly, Installation.

- The maximum permissible cable length between the safety relay unit and the plug connector of the I/O interface is 25 m.
- During installation, make sure you meet the requirements of EN 60204-1 relating to the use of PELV fixed power supplies. In the event of a fault, the voltage must not exceed 60 V DC. The safety relay unit must switch off its outputs in the event of a fault.

- A PELV fixed power supply must be used for the safety relay unit and the logic power supply of the CMMT-ST. The GND (0 V) of each fixed power supply must also be connected to each another. The device power supply and the power supply of the STO inputs must be based on the same GND potential.
- The wiring between the safety relay unit and the I/O interface of the servo drive must be installed so as to ensure that the risk of a short circuit between the conductors or to 24 V, as well as a cross circuit can be eliminated; see EN 61800-5-2, Annex D.3.1. Otherwise, the safety relay unit must feature detection of shorts across contacts and, in the event of a fault, must switch off the control signals on 2 channels.
- Only use suitable mating plugs and connecting cables → 1.2 Applicable documents, Manual Assembly, Installation. Use wire end sleeves for multicore wires.
- Prevent conductive contamination between neighbouring plug pins.
- Make sure that bridges or similar items cannot be inserted parallel to the safety wiring. For example, use the maximum wire cross section or appropriate plastic wire end sleeves.
- Use twin wire end sleeves for cross-wiring safety-related inputs. When cross-wiring STA diagnostic contacts, a maximum of 10 devices may be cross-wired → 1.2 Applicable documents, Manual Assembly, Installation.
- The safety relay unit and its inputs and outputs must meet the necessary safety classification of the safety function that is required for the specific case.
- Connect each of the control inputs to the safety relay unit on 2 channels.
- If the STA feedback signal of the STO safety sub-function has to be evaluated: connect diagnostic contact directly to the safety relay unit. The diagnostic contacts must not be connected in parallel, since a device like this with an active safety sub-function would report a safe state for all devices.
- Whether the diagnostic contact needs to be evaluated depends on the type of motor that is connected and the desired safety classification.
- If diagnostic contacts are cross-wired for a device compound: wire diagnostic contacts in series.

Basic circuitry design

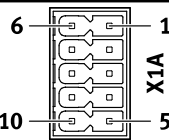
- Safe sensors, e.g. emergency stop switches, light curtains, are routed to the safety relay unit (or the safety PLC).
- The safety relay unit requests the safety sub-function on the servo drive via 2 channels and evaluates the STA feedback signal.

5.2 STO installation

Inputs and outputs for the safety sub-function STO

The 2-channel request for the safety sub-function is made via the digital inputs #STO-A and #STO-B. The digital input #STO-A must not be connected to the digital input #STO-B. Make sure that bridges or the like cannot be used parallel to the safety sub-function.

The diagnostic contact STA indicates whether the safe state has been reached for the safety sub-function STO.

[X1A]	Pin	Type	Identifier	Function
	X1A. 2	Digital input	#STO-A	Safe torque off, channel A
	X1A. 3		#STO-B	Safe torque off, channel B
	X1A. 4	Contact	STA-C1	Safe torque off acknowledge, diagnostic contact
	X1A. 5		STA-C2	

Tab. 6: Inputs and outputs for the safety sub-function STO

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

1. Find out if detection of shorts across contacts is needed for the input circuit and diagnostic contact wiring in the application.
2. If required, use a safety relay unit with detection of shorts across contacts.

STO connection example

In this example, the STO safety sub-function (safe torque off) is triggered by an input device that makes the safety request (e.g. light curtain).

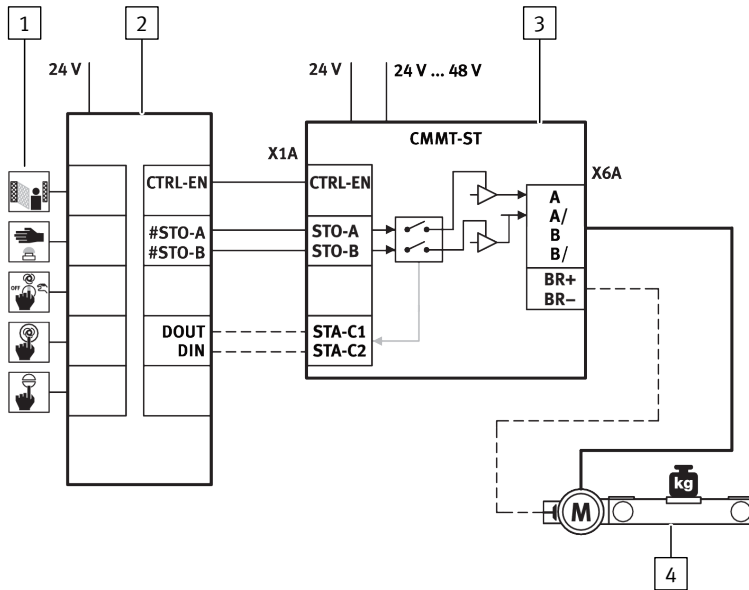


Fig. 4: STO sample circuit

- | | |
|---|--|
| <p>1 Input device for safety request, e.g. light curtain</p> <p>2 Safety relay unit</p> | <p>3 Servo drive</p> <p>4 Drive axis</p> |
|---|--|

Information on the sample circuit

The safety request is passed on to the servo drive on 2 channels via the #STO-A and #STO-B inputs at the connection [X1A]. This safety request results in the 2-channel switch-off of the driver power supply to the servo drive's power output stage.

The safety relay unit can use the STA diagnostic contact to monitor whether the safe state has been reached for the safety sub-function STO.

The CTRL-EN wiring shown is not required for the STO safety sub-function.

Information on using EC and stepper motors

When using stepper motors with a safety classification of SIL 3, cat. 3, PI e and EC motors with a safety classification of SIL 2, cat. 3, PI d, it is not mandatory to have a safety relay unit or to evaluate the feedback signal STA. The following components can be connected to the control inputs #STO-A and #STO-B to request the safety sub-function STO:

- Safe semiconductor outputs (electronic safety relay units, active safety sensors, e.g. light curtains with OSSD signals; OSSD = "Output Signal Switching Device")
- Switch contacts (safety relay units with relay outputs, passive safety sensors, e.g. forced position switches)

When using EC motors that require a safety classification of SIL 3, cat. 3, Pl e, it is necessary to have a safety relay unit and to evaluate the feedback signal STA via the diagnostic contact STA. Direct connection of safe sensors is not permitted.

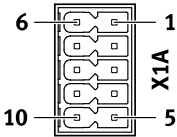
5.3 SS1-t installation

Inputs and outputs for the safety sub-function SS1-t

The safety sub-function SS1-t is wired like the safety sub-function STO but is supplemented by an emergency stop request (either directly by wiring CTRL-EN or indirectly via another functional controller) so that the braking ramp can be activated by the safety relay unit.

5.4 Installation for operation without safety function

For operation without the safety subfunction, wire inputs X1A.2 to X1A.5 as follows:

[X1A]	Pin	Type	Identifier	Function
	1	Digital input	#STO-A	supplies each one with 24 V
	2		#STO-B	
	3	Contact	STA-C1	do not connect
	4		STA-C2	
	5			

Tab. 7: Circuitry of inputs and outputs without safety sub-function

5.5 Connection Examples, Cross-wiring

The following rules apply when cross-wiring several servo drives:

- Wire inputs #STO-A and #STO-B in parallel in each case.
- Wire diagnostic contacts STA-C1/C2 in series in each case.
- Wire the diagnostic contacts of a maximum of 10 servo drives in series.

The maximum cable length applies to the entire line, from the safety relay unit to the final device.

Connection Example for Cross-wiring Several Devices without Checking the Diagnostic Contact

The first diagnostic contact of the CMMT-ST must be supplied with 24 V. The diagnostic contacts of the sequential devices must then be wired in series. Connect the last diagnostic contact for evaluating the diagnostic information to the safe controller.

With this type of wiring, the safe controller cannot perform diagnostics on whether a diagnostic contact of a CMMT-ST is permanently conductive with a short circuit on the output. For this reason, this type of wiring is not permitted for operation with EC motors and the required safety classification in accordance with SIL 3, cat. 3, Pl e.

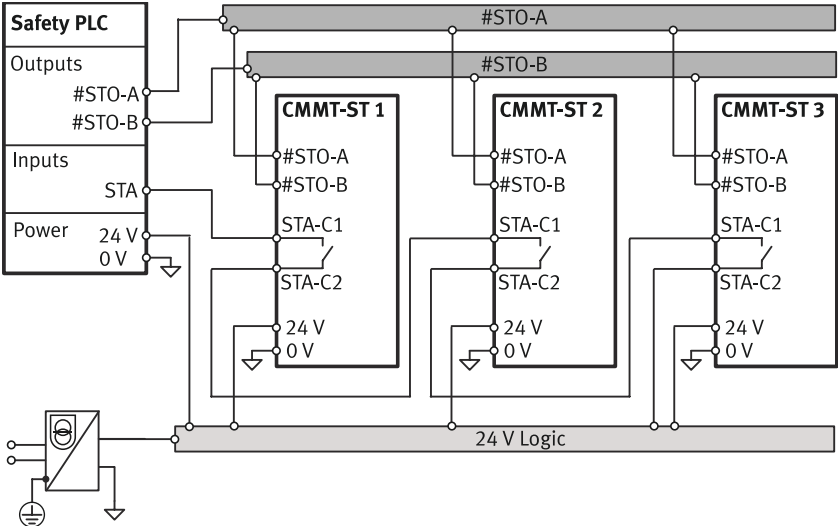


Fig. 5: Connection example for cross-wiring several devices without checking individual diagnostic contacts

Connection Example for Cross-Wiring Several Devices with Checking the Diagnostic Contact

If it is required for the overall assessment of the system that the safe controller can perform diagnostics with diagnostic contacts, the diagnostic contacts may not be connected in series. In these cases, the diagnostic contacts must be individually connected on separate inputs of the safe controller. The inputs #STO-A and #STO-B can continue to be wired in parallel.

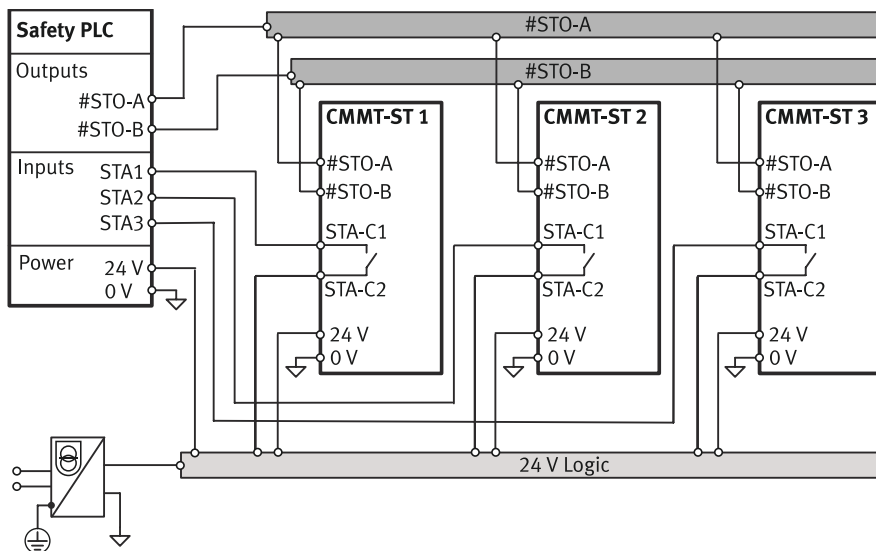


Fig. 6: Connection example for cross-wiring several devices with checking of individual diagnostic contacts

Connection example for mixed cross-wiring of devices with diagnostic contact (CMMT-ST) and diagnostic output (e. g. CMMT-AS)

If errors are made when wiring the diagnostic contacts, they will cause incorrect diagnostic feedback signals. With mixed wiring, special care is therefore needed. Only wire devices as described below. Devices with diagnostic output must always be wired in parallel, e. g. all CMMT-AS. The signal must then be connected to the diagnostic contact of the first CMMT-ST. The diagnostic contacts must then be wired in series. The last CMMT-ST must then be connected to the safe controller for evaluation of the diagnostic information.

This type of wiring is not permitted for operation with EC motors and the required safety classification to SIL 3, cat. 3, Ple (➔ Fig. 6). Here, the diagnostic contacts of the CMMT-ST must be individually evaluated.

The maximum number of 10 devices applies in this case for all devices wired together, regardless of the type.

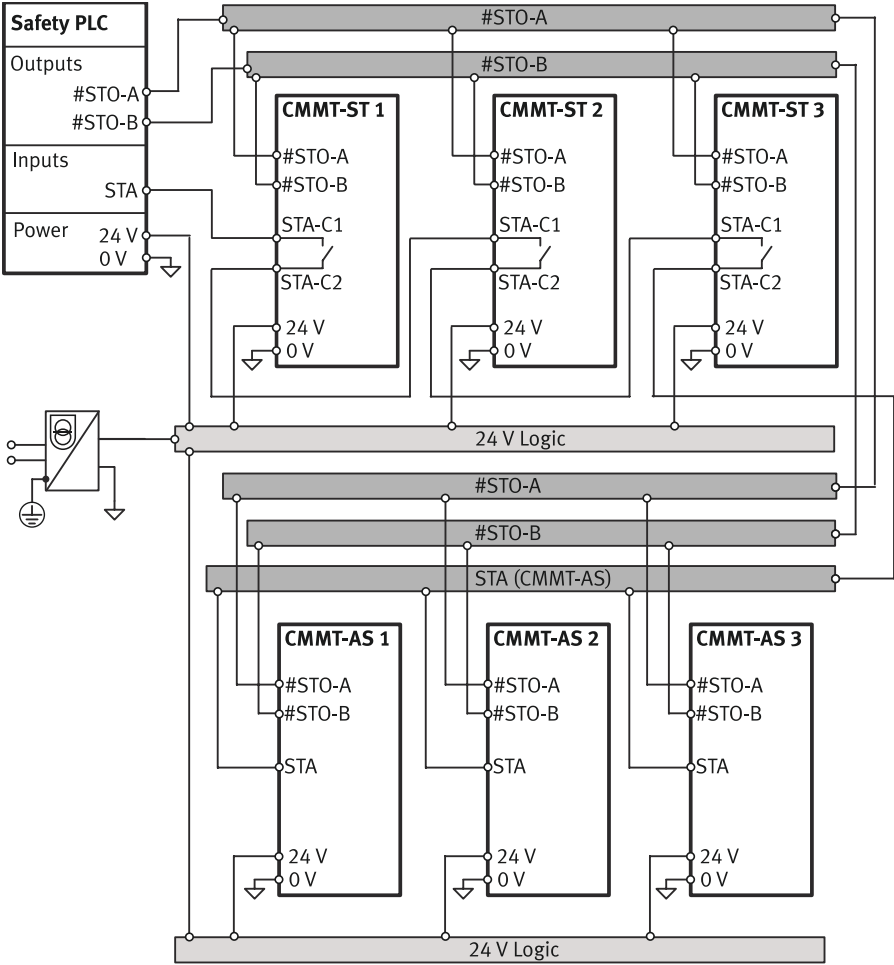


Fig. 7: Connection example for mixed cross-wiring of devices with diagnostic contact (CMMT-ST) and diagnostic output (e. g. CMMT-AS)

6 Commissioning

6.1 Safety

Use of the safety functions

NOTICE

The safety sub-function STO is already available on the servo drive on delivery without the need for any additional parameterisation. Prior to initial commissioning, wire the safety sub-function STO as a minimum.

1. Make sure that each safety function of the system is analysed and validated. It is the responsibility of the operator to determine and verify the required safety classification (safety integrity level, performance level and category) of the system.
 2. Put the servo drive into operation and validate its behaviour in a test run.
- During integration of the PDS, observe the measures stipulated by standard EN ISO 13849-1, Chapter G.4:
- Functional test
 - Project management
 - Documentation
 - Performance of a black-box test

6.2 Check lists

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.

As the CMMT-ST is a catalogue product, possible use cases can only be determined to a limited extent. The system manufacturer must perform a risk analysis on the overall system to calculate the required safety classification for the CMMT-ST and to assess whether the CMMT-ST is suitable for their application.



The following check lists are no substitute for training in safety engineering. The completeness of the check lists cannot be guaranteed.

Questions for validation in accordance with EN ISO 12100 (example)

No.	Questions	Relevant	Done
1	Have all operating conditions and all means of intervention (options for intervening in the operation of the machine but also physical intervention in the machine) 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 possibly additional protective measures, 3. User information about the residual risk?	yes ☐ no ☐	☐

No.	Questions	Relevant	Done
3	Have the hazards been eliminated or the risks of the hazards 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. 8: Questions for validation in accordance with EN ISO 12100 (example)

Questions for the validation in accordance with EN ISO 13849-2 (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 ☐	☐
3a	Inspection of components: is the servo drive described here being used (check using the rating plate)?	yes ☐ no ☐	☐
3b	Is the wiring correct (check the circuit diagram)?	yes ☐ no ☐	☐

No.	Questions	Relevant	Done
3b1	When using an EC motor with a safety classification of SIL 3, cat. 3, Pl e: have the inputs for STO been connected to the safety relay unit via 2 channels? When using a stepper motor with a safety classification of SIL 3, cat. 3, Pl e or an EC motor with a safety classification of SIL 2, cat. 3, Pl d: have the inputs for STO been connected to the safety relay unit or the safe sensor via 2 channels?	yes ☐ no ☐	☐
3b2	When using an EC motor with a safety classification of SIL 3, cat. 3, Pl e: has the diagnostic contact STA been connected to the safety relay unit?	yes ☐ no ☐	☐
3b3	If multiple servo drives have been connected together (linked) via X1A: have the connection instructions been followed? → 4.1.4 Cross-wiring of several servo drives.	yes ☐ no ☐	☐
3c	Functional tests:	yes ☐ no ☐	☐
3c1	Actuation of the system emergency stop: is the drive brought to a standstill in the desired manner?	yes ☐ no ☐	☐
3c2	Is a restart after an emergency stop prevented in the safety relay unit?	yes ☐ no ☐	☐
3c3	Is the safety sub-function STO executed immediately if only one of the assigned inputs #STO-A or #STO-B is requested? Does the diagnostic contact indicate the unsafe state as per the truth table? Truth table → Tab. 3 State of the diagnostic contact STA. Does the functional firmware log an appropriate fault once the discrepancy time has elapsed?	yes ☐ no ☐	☐
3c4	Does the safety relay unit detect a fault based on an evaluation of the diagnostic contact STA when the safety sub-function is requested via 1 channel? Truth table → Tab. 3 State of the diagnostic contact STA.	yes ☐ no ☐	☐
3c5	Only when linking multiple servo drives and connecting the diagnostic contacts: does the safety relay unit detect a fault based on an evaluation of the diagnostic contact STA if the linkage STA is interrupted at a particular point or when the safety sub-function is requested via 1 channel for a servo drive? Truth table → Tab. 3 State of the diagnostic contact STA.	yes ☐ no ☐	☐

Tab. 9: Questions for the validation in accordance with EN ISO 13849-2 (example)

Information on PDS integration

The system manufacturer must guarantee the following steps are taken in order to integrate the safety sub-function of the CMMT-ST into their overall system:

- Provide evidence of a system of project management/functional safety management
- Perform a risk analysis
- Perform a functional test on initial commissioning and during operation, or after a device is replaced (black-box test)
- Document the entire safety function

7 Operation

Check the safety functions at adequate intervals for proper functioning. 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. Time period for cyclical test (PTI) → 9.1 Technical data, safety engineering.

After the safety sub-function STO has been requested and the request completed, the functional controller enable must be reactivated.

Have qualified personnel regularly check and document the function of the diagnostic contact. The machine manufacturer must specify the exact interval, based on their application.

The CMMT-ST is maintenance-free during its period of use and specified service life.

The machine manufacturer must ensure the device is protected against restart according to the EN ISO 14118 standard “Safety of machinery – Prevention of unexpected start-up”.

With suspended axes, additional measures must be put in place to protect against falling loads. The device does not feature a safety sub-function SBC (Safe brake control).

Measures must be put in place to protect against loads that are coasting down.

We recommend decelerating the drive to a standstill before applying a brake. See information on implementing the safety function SS1-t.

8 Malfunctions

8.1 Diagnostics via LED

† Safety LED, functional status of the safety engineering

Malfunctions of the safety sub-function are detected and displayed in the functional device. The following are detected:

- Safety sub-function STO requested via 1 channel (discrepancy monitoring)
- Plausibility check of STO channel switch-off

Malfunctions are externally reported by the functional part, including via the additional communication interfaces (bus, commissioning software).

LED	Meaning
 flashing red	Error in the safety part or a safety condition has been violated.
 yellow light	The safety sub-function has been requested and is active.
 green light	Ready, a safety sub-function has not been requested.

Tab. 10: Safety LED

8.2 Repair

Repair or maintenance of the product is not permissible. If necessary, replace the complete product.

1. If there is a defect: always replace the product.
2. Return the defective product unchanged, together with a description of the fault and application, to Festo for analysis.
3. Check with your regional Festo contact person to clarify the conditions for the return shipment.
4. Validate the safety function after any modification to the installation. Validation check lists → 6.2 Check lists.

9 Technical data

9.1 Technical data, 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.	01/205/5696.01/24
UKCA	
Type-examination	The functional safety engineering of the product has been certified by an independent body, see UK-type examination certificate → www.festo.com/sp
Certificate issuing authority	TUV Rheinland UK Ltd, UK Approved Body No. 2571
Certificate no.	01/205U/5696.01/24

Tab. 11: Approval information, safety engineering

General safety reference data	
Request rate in accordance with EN 61508	High request rate
Reaction time when the safety sub-function is requested ($t_{STO,in}$) [ms]	With stepper motor: maximum 11 With EC motor: maximum 15

Tab. 12: Safety reference data and safety specifications

Safety reference data for the safety sub-function STO			
Circuitry	Stepper motor	EC motor without evaluation of STA	EC motor with evaluation of STA
Safety sub-function in accordance with EN 61800-5-2	Safe torque off (STO)		
Safety integrity level in accordance with EN 61508	SIL 3	SIL 2	SIL 3
Category in accordance with EN ISO 13849-1	Cat. 3		
Performance level in accordance with EN ISO 13849-1	PL e	PL d	PL e
Probability of dangerous failure per hour in accordance with EN 61508, PFH [1/h]	$9.5 \cdot 10^{-11}$	$6 \cdot 10^{-10}$	$3.6 \cdot 10^{-10}$
Mean time to dangerous failure in accordance with EN ISO 13849-1, MTTF _d [a]	2000	1600	
Average diagnostic coverage in accordance with EN ISO 13849-1, DC _{AVG}	medium	low	medium
Operating life (mission time) in accordance with EN ISO 13849-1, T _M [a]	20		

Safety reference data for the safety sub-function STO			
Circuitry	Stepper motor	EC motor without evaluation of STA	EC motor with evaluation of STA
Proof test interval [a] in accordance with EN 61800-5-2, PTI ¹⁾	20 ²⁾	20 ³⁾	20 ⁴⁾
Classification of components in accordance with EN 61508	Type B		
Hardware fault tolerance in accordance with EN 61508, HFT	1		
Common cause factor [%] for dangerous undetected failures β in accordance with EN 61508	2		

- 1) Depending on the desired safety classification, the evaluation of the diagnostic contact STA by the safety relay unit is required or optional.
- 2) The evaluation of the diagnostic contact STA is optional for achieving the safety classification SIL 3 cat. 3, PL e with stepper motor. Testing annually is recommended.
- 3) To achieve the safety classification SIL 2 cat. 3, PL d with EC motor, the evaluation of the diagnostic contact STA is optional. Testing annually is recommended.
- 4) The evaluation of the diagnostic contact STA is required for achieving the safety classification SIL 3 cat. 3, PL e with EC motor. This requires a cyclical test that involves dynamically changing the input signals and then evaluating STA in accordance with EN 13849-1 at least once every 3 months in accordance with EN 61800-5-2.

Tab. 13: Safety reference data for the safety sub-function STO



The technical data for the safety sub-function SS1-t must be calculated individually according to the application. Use the specified safety reference data for STO for the calculation.

9.2 Technical data, general

General technical data	
Certificates, declaration of conformity	➔ www.festo.com/sp
Type ID code	CMMT-ST
Type of mounting	Mounting plate, attached with screws H-rail mounting

General technical data	
Mounting position	vertical, free convection with unhindered air flow from bottom to top
Product weight [kg]	approx. 0.35

Tab. 14: General technical data

Ambient conditions, transport in original packaging or in control cabinet	
Transport temperature [°C]	−25 ... +70
Relative humidity [%]	5 ... 95 (non-condensing)
Max. transportation duration [d]	56 at 70 °C
Permissible altitude [m]	12000 (above sea level) for 12 h
Vibration resistant	Vibration test and free fall in packaging in accordance with EN 61800-2

Tab. 15: Ambient conditions, transport

Ambient conditions, storage in original packaging or in control cabinet	
Storage temperature [°C]	−25 ... +55
Relative humidity [%]	5 ... 95 (non-condensing)
Permissible altitude [m]	3000 (above sea level)

Tab. 16: Ambient conditions, storage

Ambient conditions, operation	
Ambient temperature [°C]	0 ... +50
Relative humidity [%]	5 ... 90 (non-condensing) corrosive media not permitted in the vicinity of the device
Permissible setup altitude above mean sea level [m]	0 ... 2000 Operation above 2000 m is not permitted!
Degree of protection	IP20 Use in a control cabinet with at least IP54, design as “closed electrical operating area” in accordance with EN 61800-5-1, Chap. 3.5
Protection class	III (safety extra-low voltage)
Overvoltage category	I
Pollution degree	2
Vibration resistance in accordance with	EN 61800-5-1 and EN 61800-2

Ambient conditions, operation	
Shock resistance in accordance with	EN 61800-2
EMC in accordance with	EN 61800-5-2

Tab. 17: Ambient conditions, operation

Service life	
Service life of the device at [h] rated load	25000 Dependent on the required current and the ambient temperature in compliance with the necessary mounting clearances and derating, see Manual Assembly, Installation → 1.2 Applicable documents

Tab. 18: Service life

9.3 Technical data, electrical

9.3.1 Digital inputs and outputs [X1A]

Control inputs #STO-A and #STO-B at [X1A]		
Nominal voltage	[V DC]	24; relative to 0 V at X9
Permissible voltage range ¹⁾	[V DC]	–3 ... 30
Max. input voltage, high level ($U_{H \max}$)	[V]	28.8
Min. input voltage, high level ($U_{H \min}$)	[V]	20
Max. input voltage, low level ($U_{L \max}$)	[V]	5
Min. input voltage, low level ($U_{L \min}$)	[V]	–3
Max. input current with high level ($I_{H \max}$)	[mA]	15
Min. input current with high level ($I_{H \min}$)	[mA]	8
Max. input current with low level ($I_{L \max}$)	[mA]	0.5
Tolerance for low test pulses		
Tolerated low test pulses ($t_{STO,TP}$) up to max.	[ms]	1
Min. time between low test pulses	[ms]	50

Control inputs #STO-A and #STO-B at [X1A]		
Tolerance for high test pulses ²⁾		
Tolerated high test pulses ($t_{STO,TP}$) [ms] up to max.		1
Min. time between high test pulses at $U_{STO-A/B} < U_{L\ max}$ [ms]		50

1) Every channel has a separate overvoltage monitor for the power supply at the input. If the voltage at the input exceeds the permissible maximum value, the channel is shut down.

2) High test pulses must never occur simultaneously at inputs #STO-A and #STO-B but only with a time offset.

Tab. 19: Control inputs #STO-A and #STO-B at [X1A]

Diagnostic contact STA at [X1A]		
Design		Potential-free contact
Voltage range [V DC]		18 ... 30
Max. current [mA]		100; not short-circuit proof
Max. internal resistance [Ω]		< 6
Off-state current (contact open) [μ A]		< 2
Closing reaction time $t_{STA,Rise}$ [ms]		< 30
Opening reaction time $t_{STA,Fall}$ [ms]		< 20
Galvanic isolation		Via optocoupler
Protective functions		Overvoltage-resistant up to 60 V DC

Tab. 20: Diagnostic contact STA-C1/C2 at [X1A]

Copyright:
Festo SE & Co. KG
Ruiter Straße 82
73734 Esslingen
Germany

Phone:
+49 711 347-0

Internet:
www.festo.com