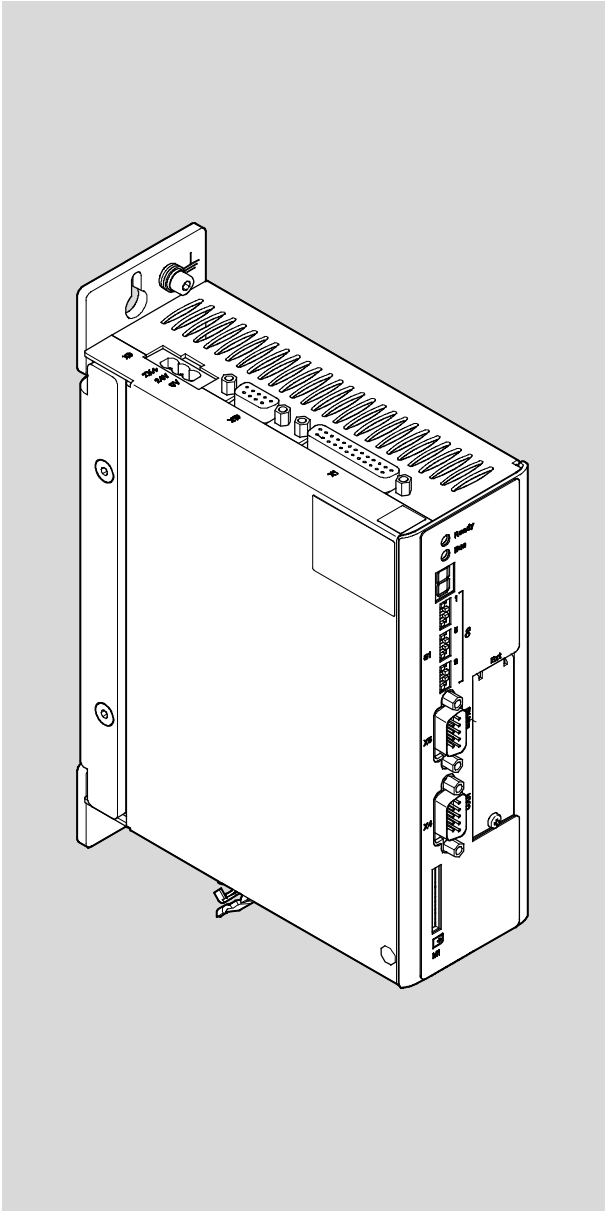
Motor controller

CMMS-ST-C8-7-G2



FESTO

Description

STO safety function
(Safe Torque Off)

8040102
1404NH
[8034464]

Translation of the original instructions
GDCP-CMMS-ST-G2-S1-EN

Identification of hazards and instructions on how to prevent them:

Warning
Hazards that can cause death or serious injuries.

Caution
Hazards that can cause minor injuries or serious material damage.

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.

Table of Contents – CMMS-ST-C8-7-G2

Notes on this documentation

This documentation serves the purpose of safe work with the safety function STO – “Safe Torque Off” with use of the motor controller CMMS-ST-...-G2.

- Always observe in addition the general safety regulations for the CMMS-ST-...-G2.

The general safety regulations for the CMMS-ST-...-G2 can be found in the description Mounting and Installation , GDCP-CMMS-ST-G2-HW-... (➔ Tab. 2).
Observe the information regarding safety and the requirements for product use in chapter 1.

Product identification

This documentation refers to the following versions:
– Motor controller CMMS-ST-...-G2 Rev 05 and higher.
– Firmware FW 1.4.0.1.4 and higher.

The illustration on the rating plate can be found in the description Mounting and Installation, GDCP-CMMS-ST-G2-HW-...

Service

Please consult your regional Festo contact if you have any technical problems.

Issue status of the specified standards

Standard: issue status		
EN 60204-1:2006/A1:2009-02	EN 61800-5-1:2007-09	EN ISO 12100:2010-11
EN 61800-2:1998-04	EN 61800-5-2:2007-10	EN ISO 13849-1:2008-06

Tab. 1 Issue statuses

Documentation

Additional information on the motor controllers can be found in the following documentation:

Documentation		Type of equipment	Contents
Mounting and installation	GDCP-CMMS-AS-G2-HW-...	CMMS-AS	– Mounting – Installation (pin allocation) – Error messages – Technical data
	GDCP-CMMD-AS-HW-...	CMMD-AS	
	GDCP-CMMS-ST-G2-HW-...	CMMS-ST	
Functions and commissioning	GDCP-CMMS/D-FW-...	CMMS-AS CMMD-AS CMMS-ST	– Control interfaces – Operating modes/operational functions – Commissioning with FCT – Error messages
STO safety function	GDCP-CMMS-AS-G2-S1-...	CMMS-AS	– Functional safety engineering with the safety function STO (safe torque off)
	GDCP-CMMD-AS-S1-...	CMMD-AS	
	GDCP-CMMS-ST-G2-S1-...	CMMS-ST	
Device profile FHPP	GDCP-CMMS/D-C-HP-...	CMMS-AS CMMD-AS CMMS-ST	– Description of the interfaces: – CAN bus (CANopen) – Interface CAMC-PB (PROFIBUS) – Interface CAMC-DN (DeviceNet) – Control and parameterisation via the device profile FHPP (Festo profile for handling and positioning) with PROFIBUS, DeviceNet or CANopen.
Device profile CiA 402,	GDCP-CMMS/D-C-CO-...	CMMS-AS CMMD-AS CMMS-ST	– Description of the interface: – CAN bus (CANopen, DriveBus) – Control and parameterisation via device profile CiA 402 (DS 402).
Software Help	Help on the CMMS-AS plug-in	CMMS-AS	– Surface and functions in the Festo Configuration Tool for the plug-in
	Help on the CMMD-AS plug-in	CMMD-AS	
	Help for the CMMS-ST plug-in	CMMS-ST	

Tab. 2 Documentation on the motor controllers

The documentation is available on the following media:
- CD-ROM (scope of delivery)
- Support portal: www.festo.com/sp

1 Safety and requirements for product use

1.1 Safety

1.1.1 General safety instructions

- Always observe in addition the general safety regulations for the CMMS-ST-...-G2.

The general safety regulations for the CMMS-ST-...-G2 can be found in the description Mounting and Installation, GDCP-CMMS-ST-G2-HW-... (➔ Tab. 2, page 6).

Note

Loss of the safety function.

The safety functions might fail if you do not comply with the parameters required for the surroundings and connections.

- In particular, you must provide input voltages which are within the tolerances specified in ➔ Technical data, appendix A.1.

Note

Damage to the motor controller due to incorrect handling.

- Switch off the supply voltage before mounting and installation work. Switch on supply voltage only when mounting and installation work are completely finished.
- Observe the specifications for handling electrostatically-sensitive devices.

1.1.2 Intended use

The CMMS-ST-...-G2 motor controller supports the following safety function:

– “Safe Torque Off” (STO) up to category 3 / PL d in accordance with EN ISO 13849-1.

The motor controller CMMS-ST-...-G2 is a product with safety-relevant functions and is intended for installation in machines or automation systems. Use it only:

– in excellent technical condition,
– in its original state without unauthorised modifications,
– within the product's limits, as defined by the technical data ➔ Appendix A.1,
– within the specified service life of the switching elements ➔ Appendix A.1, Tab. A.6,
– in an industrial environment.

Note
In the event of damage caused by unauthorised manipulation or improper use, the guarantee is invalidated and the manufacturer is not liable for damages.

1.1.3 Foreseeable misuse

The following foreseeable misuses are among those not approved as intended use:
– use outdoors,
– use in non-industrial areas (residential areas),
– use in applications where switching off can result in hazardous movements or conditions.

Note
– The STO function may not be used as the sole safety function for drives subject to permanent torque or force (e.g. suspended loads).
– Bypassing of safety equipment is not allowed.
– Repairs to the motor controller are not allowed!

The STO (Safe Torque Off) function does not provide protection fromelectric shock, but only against hazardous movements (➔ Description, mounting and installation, GDCP-CMMS-ST-G2-HW-...)!

In applications with extremely high requirement rates, the service life of the switching elements must be taken into account in the design (replacement interval for the motor controller, ➔ Appendix A.1, Tab. A.1 and Tab. A.6).

1.1.4 Achievable safety level, safety function in accordance with EN ISO 13849-1

The motor controller CMMS-ST-...-G2 with integrated STO safety function fulfils the requirements of the test regulations for
– Category 3 / PL e in accordance with EN ISO 13849-1
and can be used in applications up to Cat. 3 / PL d in accordance with EN ISO 13849-1.
The achievable safety level depends on the other components used to implement the safety function.

1.2 Requirements for product use

- Make this 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 of the documentation are always complied with. When so doing, also take into account the documentation for the other components (e.g. motors, cables, etc.).
- Take into consideration the legal regulations applicable for the destination, as well as:
  – regulations and standards,
  – regulations of the testing organizations and insurers,
  – national specifications.
- If the safety function is demanded, protection against automatic restart corresponding to the required category must be furnished. Among other means, this can take place through an external safety switching device.

1.2.1 Technical prerequisites

General conditions for the correct and safe use of the product, which must be observed at all times:

- Comply with the connection and environmental conditions of the motor controller (➔ Appendix A.1) and all connected components specified in the technical data.
  Only compliance with the limit values or load limits will enable operation of the product in compliance with the relevant safety regulations.
- Observe the instructions and warnings in this documentation.

1.2.2 Qualification of the specialized personnel (requirements for the personnel)

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

– the installation and operation of electrical control systems,
– the applicable regulations for operating safety-engineered systems,
– the applicable regulations for accident protection and occupational safety, and
– the documentation for the product.

1.2.3 Diagnostic coverage (DC)

Diagnostic coverage depends on the connection between the motor controller and the control loop system as well as the implemented diagnostic measures ➔ Section 5.3.
If a potentially dangerous malfunction is recognised during the diagnostics, appropriate measures must be taken to maintain the safety level.

➔ **Note**
Check whether a fault exclusion of cross circuits in the input circuit and connection wiring is possible in your application.
If not: If applicable, use a safety switching device with cross-circuit detection for control of the safety function as well as an appropriate filter construction group for filtering the test pulses at the control ports of the CMMS-ST-...-G2.

1.2.4 Range of application and certifications

The motor controller with integrated STO safety function is a safety-related part of the control systems.
The motor controller carries the CE marking.
Standards and test values which the product must comply with and fulfils can be found in the section "Technical data" ➔ Appendix A.1. The product-relevant EU directives can be found in the declaration of conformity.

Certificates and declaration of conformity on this product can be found at
➔ www.festo.com/sp.

2 Description of the safety function STO

2.1 Product overview

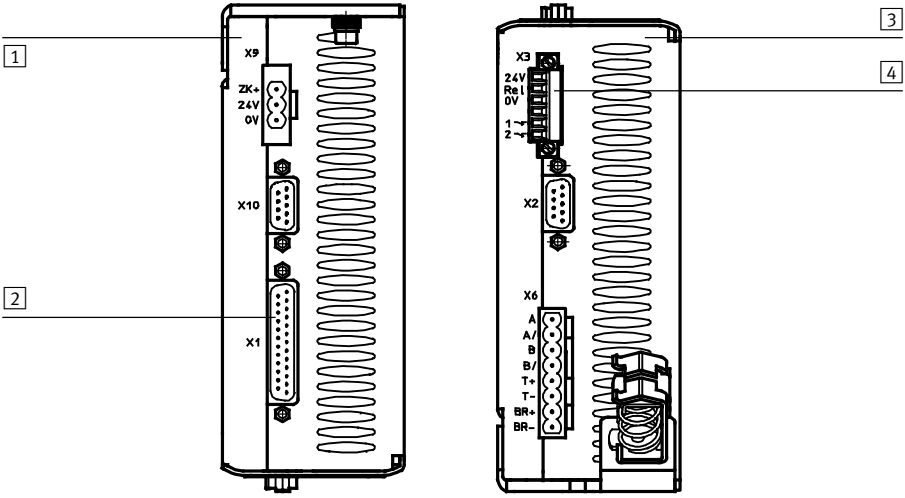
2.1.1 Purpose

As processes become increasingly automated, protecting people from potentially hazardous movements is gaining in importance. Functional safety describes required measures by electrical or electronic equipment to reduce or eliminate malfunction-induced dangers. In normal operation, protective devices prevent human access to hazardous areas. In certain operating modes, during set-up, for example, people need to be in hazardous areas. In such situations, the machine operator must be protected by drive and internal control measures.

The functional safety engineering integrated in the motor controller meets the requirements of the controller and drive for optimised implementation of protective functions. Planning and installation complexity is reduced. The use of integrated functional safety engineering increases machine functionality and availability over the levels achieved by conventional safety technology.

2.1.2 Interfaces

The motor controller CMMS-ST-...-G2 has 2 interfaces for control of the STO safety function.

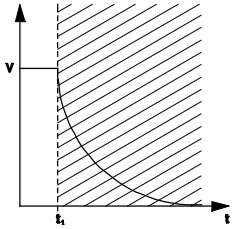
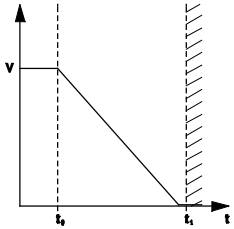


1 Top side of housing
2 I/O interface [X1]
3 Bottom side of housing
4 STO interface [X3]

Fig. 2.1 Motor controller CMMS-ST-...-G2

2.2 Function and application

The CMMS-ST-...-G2 motor controller has the following safetyfeatures:
– “Safe Torque Off” function (STO),
– potential-free acknowledgement contact for the operating status,
The function “Safe Stop 1” (SS1) can be achieved with a suitable external safety switching device and appropriate circuitry of the motor controller CMMS-AS-...-G2.

Safety function		Requirements of the safety switching device[1)]	Switch-off behaviour	Stop category
STO	Safe Torque Off	– 2 safety contacts, non-delayed – Connection option for safety command devices, e.g. emergency stop switch, protective door switch, light curtains, etc.		0
SS1	Safe Stop 1	– 1 safety contact non-delayed – 2 safety contacts relapse delayed – Connection option for safety command devices, e.g. emergency stop switch, protective door switch, light curtains, etc.		1

1) Or comparable safety switching device with corresponding safety contacts

Tab. 2.1 Selection of the safety function

2.2.1 Description of the safety function STO

Use the “Safe Torque Off” function (STO) whenever you have to reliably disconnect the energy supply to the motor in your application.

The safe torque off function switches off the following ➔ Fig. 2.2.:

– driver supply for the power semiconductor.
– activation of the power semiconductor (PWM).

Note

The STO function request must always run in two channels over X3.2 and X1.21 (end stage enable).

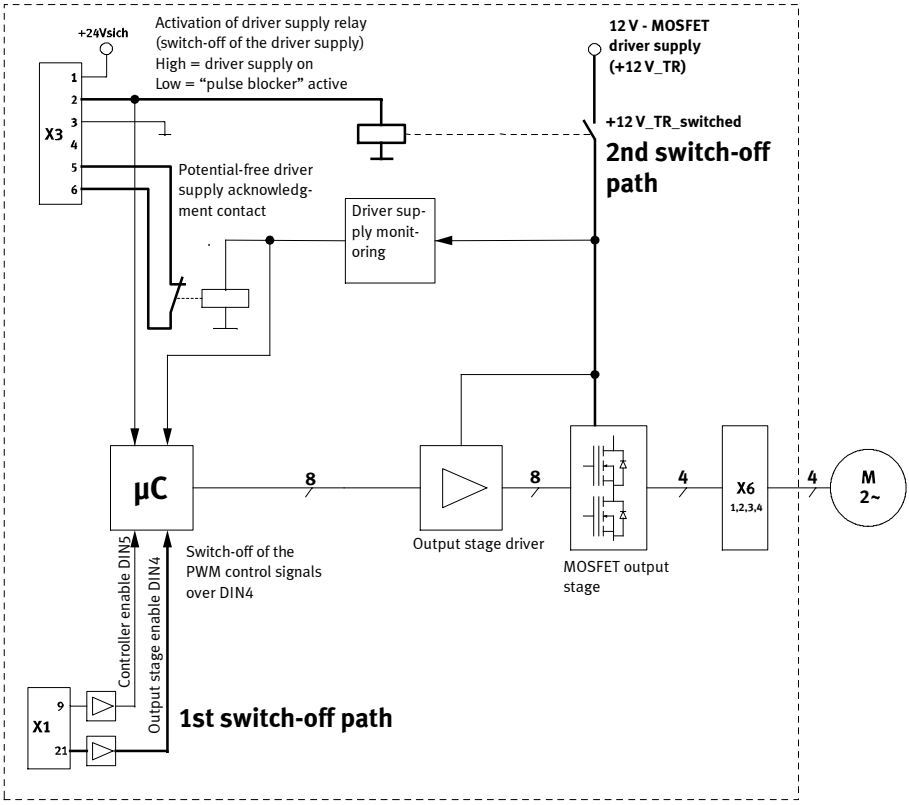


Fig. 2.2 “Safe torque off” - functional principle for CMMS-ST-...-G2

With the Safe Torque Off function (STO), the energy supply to the motor is reliably interrupted by switching off the end stage enable and supply to the final output stage. The drive cannot generate torque or any force and so cannot make 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 holding brakes). In the STO “Safe Torque Off” status, the idle position is not monitored.
The machine must be stopped in a safe manner, e.g. via a safety switching device.
If the STO function is activated with a moving drive, the motor starts to coast uncontrolled after max. 5 ms. After that, the automatic brake control is activated.

Note
If uncontrolled coasting can result in a hazard or damage, additional measures are required.

Note
A clamping unit is actuated by the non-safety-relevant firmware of the motor controller CMMS-ST-...-G2.

If you use motors with a holding brake, the holding brake is worn each time the STO is switched off while the motor is running.
Therefore, when using the “STO” function, do not use motors with holding brakes; use clamping units that permit emergency braking or use automatic locking axis mechanisms.

The holding brakes used by Festo motors are not suitable for active deceleration - only for holding a position!

Application examples for the STO function are manual manipulations during set-up, equipping and fault clearance. Use of the integrated solution offers several advantages:
– fewer external components, e.g. contactors.
– less wiring effort and space requirements in the control cabinet.
– and thus lower costs.
Another advantage is the availability of the system. The integrated solution allows the intermediate circuit of the controller to remain charged. This means no significant waiting time when the system is restarted.

Note
There is a danger that the drive will advance if there are multiple errors in the CMMS-ST-...-G2.
Failure of the motor controller output phase during the STO status (simultaneous short circuit of 2 power semiconductors in different phases) may result in a limited detent movement of the rotor. The rotation angle / path corresponds to a pole pitch. Example: Rotating axis, stepper motor, 50 pin pairs ➔ Movement < 3.6° at the motor shaft.

2.2.2 Overview of interfaces [X1] and [X3]

The motor controller has control ports for requesting the safety function at the following interfaces ➔ Section 3.2:

– 25-pin connection [X1] on the top side with the control port (1st switch-off path) and the controller enable control port (for implementation of the SS1 function in combination with an externally safe time relay).
– 6-pin connection [X3] on the bottom with a control port (2nd switch-off path), an acknowledgment contact and a 24 V auxiliary supply for external sensors.

A safety circuit for additional interfaces on the CMMS-ST-...-G2 motor controller is neither required nor intended.

Tab. A.6 in appendix A.1.3 describes the technical data for the control ports.
Cross-circuit detection in the input circuit is not carried out by the motor controller.
The inputs have no tolerance against test pulses (OSSD).

Interface	Port		Description
	Pin	Designation	
[X1]	6	GND24	Reference potential for digital inputs and outputs
	9	DIN5	Controller enable (high active)
	18	+24 V	24 V supply provided
	21	DIN4	Output stage enable (high active)
[X3]	1	24 V	Auxiliary power supply (24 V DC logic supply of the motor controller provided).
	2	Rel	Activation of driver supply relay High = driver supply switched on Low = “pulse blocker” active, driver supply switched off
	3	0 V	Reference potential for digital inputs and outputs.
	5	1 ⌐ (NC1)	Acknowledgment contact for the status “Safe Torque Off” (STO) – Acknowledgment contact closed = “Safe Torque Off” (STO) active (or controller switched off)
	6	2 ⌐ (NC2)	

Tab. 2.2 Function of the connections

For STO in category 3, PL d in accordance with EN ISO 13849-1, two channels are required, that is, an unintended restart must be reliably prevented through two separate paths that are completely independent of each other. These two paths for interrupting the energy supply to the drive with the reliable impulse block are called switch-off paths:

1st switch-off path:
Output stage enable via [X1] (blocking of the PWM signals; the MOSFET drivers are no longer actuated with pulse patterns).

2nd switch-off path:
Interruption of the supply for the eight drivers for the end stage MOSFETs via [X3] using a relay (the MOSFET drivers are separated from the power supply via a relay, thus preventing the PWM signals from reaching the MOSFETs).

A plausibility check is performed in the µP between the relay control for the output stage driver supply and the monitoring of the driver supply. This serves to provide both error detection of the impulse block and suppression of the error message E 05-2 (“driver supply undervoltage”) occurring in normal operation.

Potential-free acknowledgment contact:
Further, the integrated circuit for “Safe Torque Off” has a potential-free acknowledgment contact ([X3] pin 5 and 6) for the presence of the driver supply. This is an N/C contact. It must be connected to an external safety controller or the higher-order controller, for example. Through this controller, the STO function must be checked regularly (e.g. every 24 hours or at the beginning of the shift, if possible at every STO request).
If an error occurs in the plausibility check, the control system must prevent further operation, for example, by switching off the intermediate circuit voltage or breaking off the output stage enable by the PLC.

The feedback contact has a single channel and may only be used for monitoring.
Tab. A.7 in Appendix A.1.3 describes the electrical data and runtime performance of the acknowledgment contact.
When the 24 V supply to the basic device is turned on and off, the switching status of the relay may - due to the internal supply voltages powering up at a different speed - deviate briefly (approx. 100 ms) from the status of the controller for the driver supply relay Rel [X3.2].

Registration of the status of the acknowledgment contact NC1/NC2 is required at every request of the safety function.
When the safety function has been requested, a change in signal must occur at the acknowledgment contact within an application-specific time. A safety-related reaction must be initiated in the event of a violation.

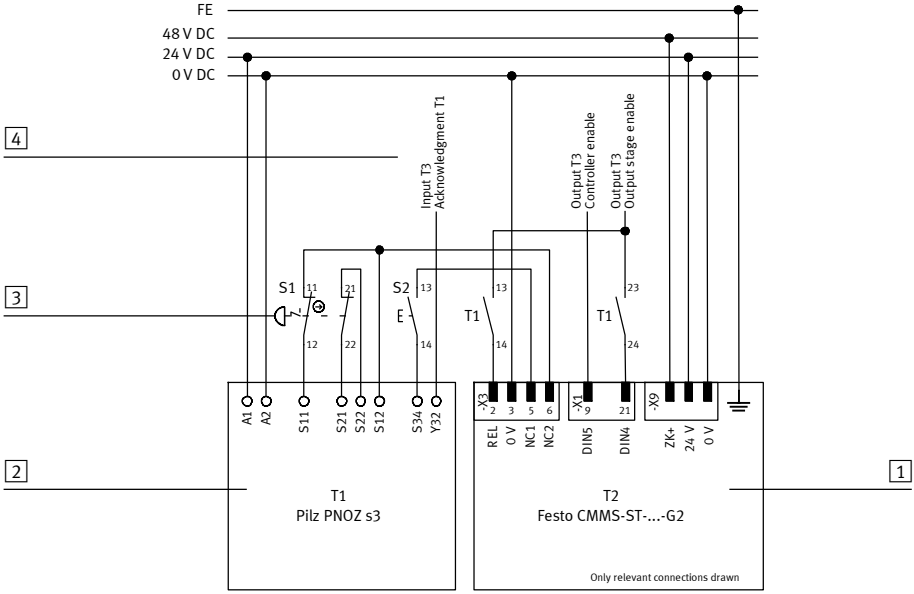
Auxiliary supply 24 V, 0 V [X1] and [X3]
The motor controller CMMS-ST-...-G2 makes available one 24 V auxiliary supply each at [X1] and [X3]. This can be employed when using the acknowledgment contact NC1/NC2 or to supply external, active sensors.

Tab. A.8 in appendix A.1.3 describes the electrical data for the auxiliary supply.

2.2.3 Runtime performance

The runtime performance for typical applications can be found in the sample circuits:
– Sample circuit for STO in ➔ Section 2.3.
– Sample circuit for SS1 ➔ Section 2.4.

2.3 Switching example STO – “Safe Torque Off”



1 Motor controller with safety function (T2, only relevant connections represented)
2 Safety switching device (T1)
3 Emergency stop switches
4 Inputs and outputs of the higher-order controller (T3, 24 V)

Fig. 2.3 Circuit diagram, safety function STO

2.3.1 Explanations of the switching example

The switching example shows a combination of the CMMS-ST-...-G2 with a PNOZ s3 safety switching device from Pilz. A circuit is shown with an emergency stop switch that carries out the safety function “Safe torque switch-off (STO)”. The emergency stop switch (S1) can be replaced by another safety command device, e.g. safety door switch.
You can find technical data, such as max. current, etc., in the data sheet of the safety switching device used.

Due to the drawn circuitry, a two-channel operation with cross-circuit detection is possible. This permits detection of:
– earth faults in the start and input circuit.
– short circuits in the input circuit / start circuit.
– cross circuits in the input circuit.
The removal of output stage enable via DIN4 [X1.21] as well as switching off of the driver supply via Rel [X3.2] results in the motor coasting to a stop.

Note
If external forces (e.g. suspended loads) affect the drive, additional measures (e.g. mechanical holding brakes) are necessary to avoid hazards.

Note
The stop function SS1, “Safe Stop 1”, in which the drive is brought to rest, is fundamentally preferable.

The holding brake of the EMMS-ST-...**B** is not appropriate for braking the motor. It only serves for functional holding of the motor shaft. Additional measures are required for use in safety-oriented applications.

2.3.2 STO request

The following steps describe the process when activating the STO status (➔ Timing diagram section 2.3.4):

a) After actuation of the emergency stop switch (S1), the N/O contacts (13, 14 and 23, 24) of T1 open immediately. As a result, control of the driver supply relay Rel [X3.2] and output stage enable DIN4 [X1.21] are switched off simultaneously – “Safe Torque Off” is activated.
b) With removal of the control signal for the relay to switch off the driver supply, the capacitors are discharged in this voltage branch. After no more than 5 ms (t1), the output stage is no longer active. The motor coasts to a stop.
c) A maximum of 2.5 ms (t2) later, the output for control of the holding brake is switched off.
d) Not later than 12 ms (t_{STO}) after removal of the control of the driver supply relay and output stage enable, the output stage is reliably switched off and the STO status is active.
e) For mechanical reasons, the holding brake requires some time until it is closed - typically after approx. 50 ... 500 ms (t3).
f) Not later than 30 ms (t4) after removal of control of the driver supply Rel [X3.2], the acknowledgment contact NC1/NC2, [X3.5/6] is closed.
g) Not later than 720 ms (t5) after 2-channel calling (DIN4 [X1.21] **and** Rel [X3.2]), “H” is displayed on the 7-segments display of the motor controller.

2.3.3 Restart after termination of the STO status

Before switching it on again, make sure that all hazards have been eliminated and the system can be safely placed in operation again. A manual acknowledgment must be made through the optional S2 pushbutton corresponding to the risk evaluation for the application (see switching example).
To switch the output stage of the motor controller active again and thus operate the connected motor, the following steps must be taken (➔ Timing diagram section 2.3.4):

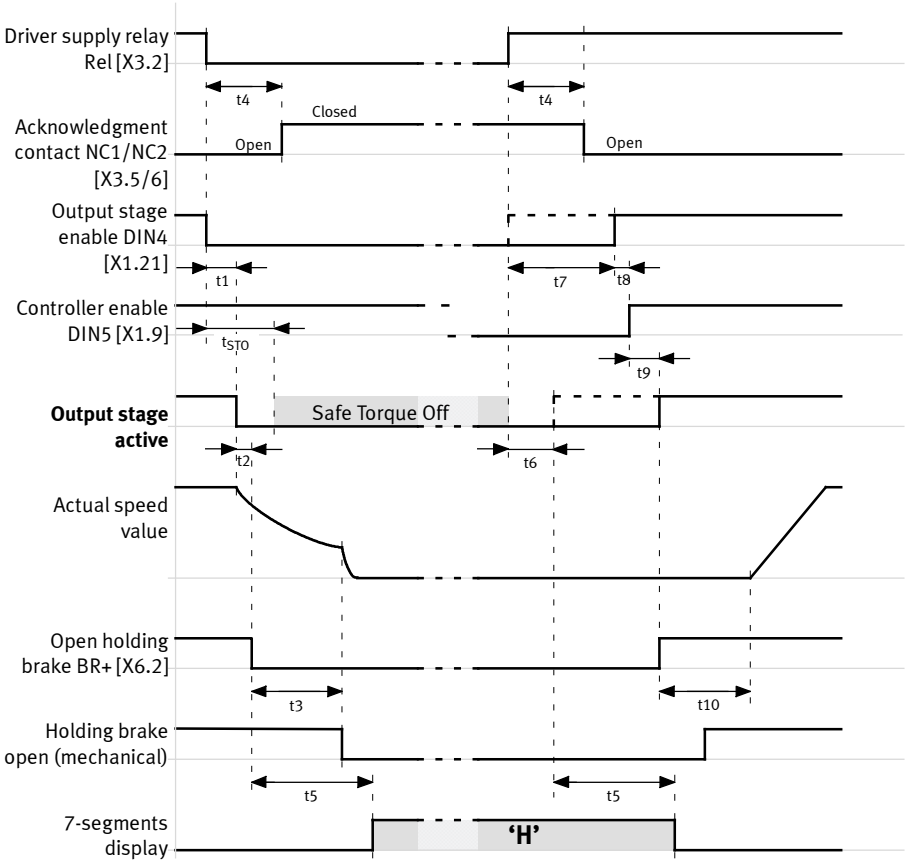
1. First, the control of the relay for switching the supply voltage of the output stage driver (2nd switch-off path) must be switched through 24 V at Rel [X3.2] (related to 0 V [X3.3]).

a) This switches on the internal driver supply. The driver supply is recharged after no more than 20 ms (t6).
b) The potential-free acknowledgment contact NC1/NC2 [X3.5/6] is opened no later than 30 ms (t4) after Rel [X3.2] is switched.

2. The switching time for the output stage enable DIN4 [X1.21] is freely selectable (t7). The release should take place simultaneously with activation of the 2nd switch-off path via Rel [X3.2], but must be present at least 2.5 ms (t8) **before** the rising edge of the controller enable DIN5 [X1.9].

c) With the rising edge of the controller enable, after a time delay ≤ 5 ms (t9), release of the motor holding brake is triggered (if present) and the internal output stage enable takes place. For control via the fieldbus, controller enable via fieldbus is also required beforehand. With FCT, a switch-on delay can be set for the brake (t10), which causes the drive to be regulated to speed “0” for the specified time, and only after this time has elapsed does it run to the set speed.
d) No later than 720 ms (t5) after ending of the 2-channel request, the “H” on the 7-segments display goes out.

2.3.4 STO timing diagram

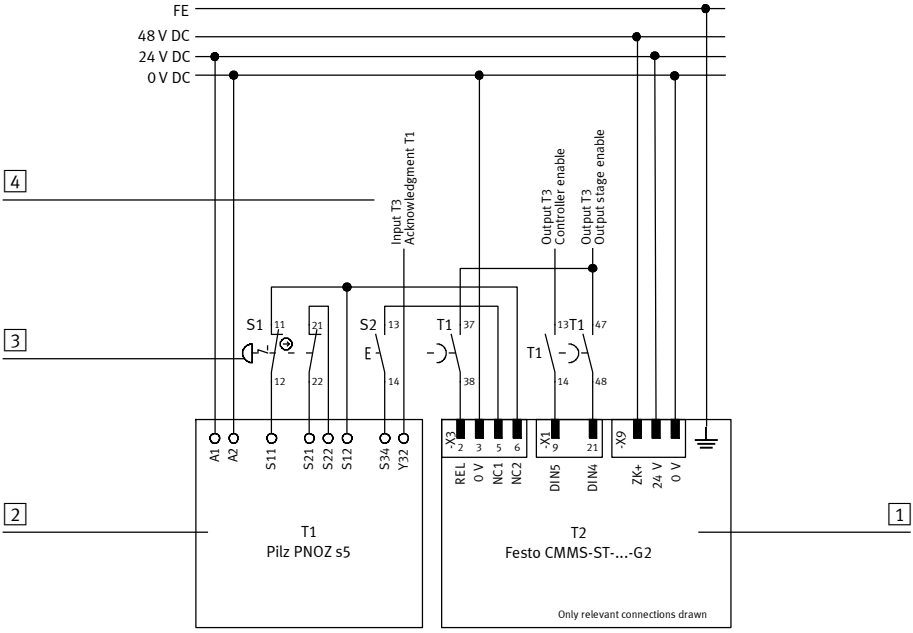


t1 ≤ 5 ms
t2 ≤ 2.5 ms
t_{STO} ≤ 12 ms
t3 ≈ 50 ... 500 ms
(dependent on the brake used)
t4 ≤ 30 ms
t5 ≤ 720 ms
t6 ≤ 20 ms
t7 any
t8 > 2.5 ms
t9 ≤ 5 ms (For control via the fieldbus, controller enable via fieldbus is also required beforehand)
t10 0 ... 6553 ms (with FCT parameterised switch-on delay brake)

Fig. 2.4 STO timing diagram

2.4 Switching example SS1 – “Safe Stop 1”

In the function “Safe Stop 1” (SS1), the drive is run down in a controlled way and, after that, the power supply to the final output stage is switched off. As a result, the drive cannot generate torque or any force at rest and so cannot produce any dangerous movements.



1 Motor controller with safety function (T2, only relevant connections represented)
2 Safety switching device (T1)
3 Emergency stop switches
4 Inputs and outputs of the higher-order controller (T3, 24 V)

Fig. 2.5 Circuit diagram for the safety function SS1

2.4.1 Explanations of the switching example

The switching example shows a combination of the CMMS-ST-...-G2 with a PNOZ s5 safety switching device from Pilz. As a switching device, a safety stop is drawn in combination with an emergency stop switch. There remains the option to use a safety door switch with bolt that holds the safety door closed until the drive is at rest or the “driver supply feedback” signal displays the safe status and the plausibility check is successful.
You can find technical data, such as max. current, etc., in the data sheet of the safety switching device used.

With use of the PNOZ s5 from Pilz, two-channel operation with cross-circuit detection is possible. This permits detection of:
– earth faults in the start and input circuit.
– short circuits in the input circuit / start circuit.
– cross circuits in the input circuit.

Warning
The motor holding brake, supplied as a standard feature, or an external motor holding brake controlled by the motor controller, is not appropriate for personal protection!
- Also secure vertical axes against falling down or dropping after the motor is switched off, such as through:
  – mechanical locking of the vertical axis,
  – external brake/catch/clamping device or
  – sufficient counterbalance of the axis.

The holding brake of the EMMS-ST-...**B** is not appropriate for braking the motor. It only serves for functional holding of the motor shaft. Additional measures are required for use in safety-oriented applications.

Note
The time delay of the PNOZ relay must be adapted to the application (see section 2.4.5). If this delay time is set too short, the drive carries out an STO function after this time has expired. This can result in wear of the brake.

Note
The ramp function of the motor controller's Quick Stop delay is not monitored.

2.4.2 Request SS1

The following steps describe the process when requesting the SS1 safety function (➔ Timing diagram Section 2.4.4):

a) After actuation of the S1 switch (emergency stop switch or opening of the protective doors), the N/O contact of T1 (13, 14) opens immediately. This results in the immediate removal of controller enable DIN5 [X1.9]. The brake ramp is begun after no more than 5 ms (t1).
b) The delay of the brake ramp is adjustable via FCT, depending on the application (“Stop-delays” – “Quick stop”). Dependent on the actual speed value and quick-stop delay, the brake ramp requires between 0 ms and maximum approx. 10 s (t2).
   Determination of the brake time ➔ Section 2.4.5.
c) After speed 0 is reached, the holding brake output BR+ [X6.2] is switched off and the drive is still regulated down to this setpoint for a time “Times brake” – “Switch-off delay” (t3) that can be parameterised. This adjustable time is the delay with which the holding brake of the motor comes down. This time is dependent on the respective holding brake and must be parameterised by the user, typically 150 ms.
   For applications without holding brake, the time is set to 0 ms.
d) The brake is mechanically closed after the time t11 (50 .. 500 ms), after the electric holding brake output BR+ [X6.2] has been switched off.

The holding brake is always activated when the “brake ramp time” + set “switch-off delay” has expired and the drive could not stop until then.

e) After the switch-off delay (t3) has expired, the internal output stage enable is switched off after no more than 5 ms (t4).
f) The time delay of the PNOZ (t5) must be set greater than t1 + t2 + t3 + t4. After the time delay of the PNOZ has expired, open the two delay contacts of T1 (37, 38 and 47, 48). As a result, control of the driver supply relay Rel [X3.2] and output stage enable DIN4 [X1.21] are switched off simultaneously.
g) After no more than 12 ms (t_{STO}), the output stage is reliably switched off and the STO status is active.
h) Not later than 30 ms (t6) after removal of control of the driver supply relay Rel [X3.2], the acknowledgment contact NC1/NC2, [X3.5/6] is closed.
i) Not later than 720 ms (t7) after 2-channel request (DIN4 [X1.21] **and** Rel [X3.2]), “H” is displayed on the 7-segments display of the motor controller.

2.4.3 Restart after termination of the SS1 function and STO status

Before switching it on again, make sure that all hazards have been eliminated and the system can be safely placed in operation again. A manual acknowledgment must be made through the optional S2 pushbutton corresponding to the risk evaluation of the application (see switching example).
This timing diagram is based on the example of speed regulation using the controller enable via DIN 5 at [X1]. For fieldbus applications, the controller enable is additionally controlled via the respective fieldbus. Depending on the application, the operating mode can also be parameterised using the parameterisation software.
To end the safety function SS1 and switch the output stage of the motor controller active again, the following steps must be taken (➔ Timing diagram section 2.4.4):

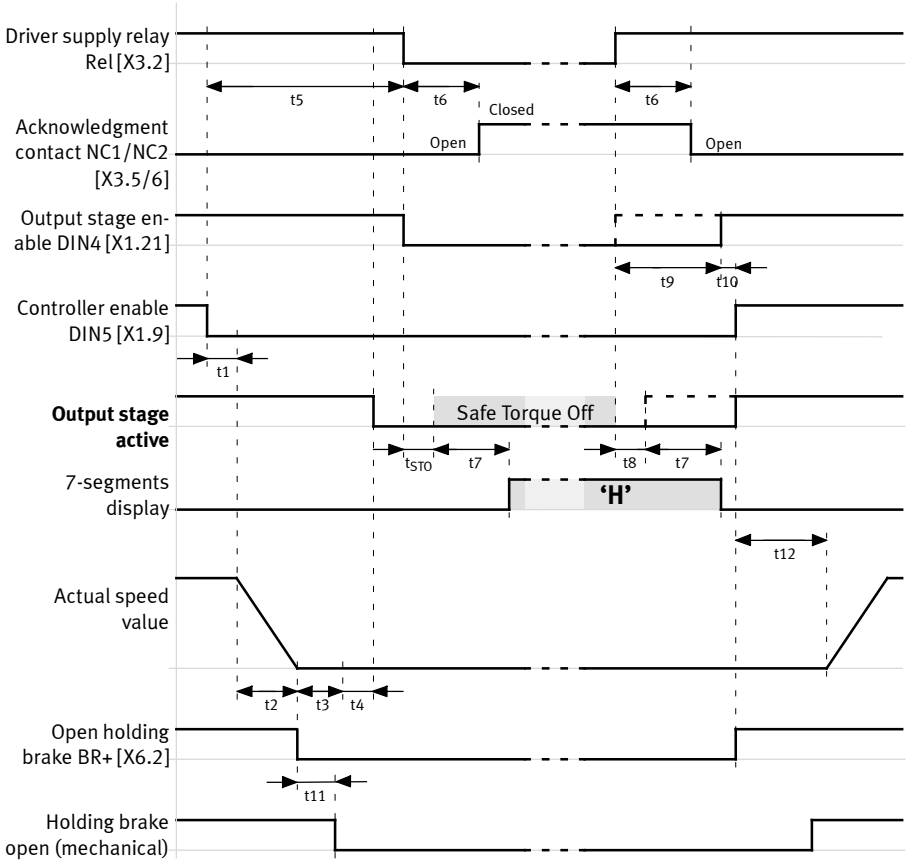
1. First, the control of the relay for switching the supply voltage of the output stage driver (2nd switch-off path) must be switched through 24 V at Rel [X3.2] (related to 0 V [X3.3]).
   This switches on the internal driver supply.

a) The driver supply is recharged after no more than 20 ms (t8).
b) The potential-free acknowledgment contact NC1/NC2 [X3.5/6] is opened no later than 30 ms (t6) after Rel [X3.2] is switched.

2. The switching time for the output stage enable DIN4 [X1.21] is freely selectable (t9). The release should take place simultaneously with activation of the 2nd switch-off path via Rel [X3.2], but must be present at least 2.5 ms (t10) **before** the rising edge of the controller enable DIN5 [X1.9].

c) The rising edge of the controller enable releases the motor holding brake (if present) and the internal end stage enable occurs.
   With FCT, a switch-on delay can be set for the brake (t12). During this time, the drive is regulated to speed “0”. After that, it is regulated to the set speed.
   The time t12 is chosen so large that the brake can open mechanically within t12.
d) No later than 720 ms (t7) after ending of the 2-channel request, the “H” on the 7-segments display goes out.

2.4.4 Timing diagram SS1



t1 ≤ 5 ms
t2 = 0 ms...10 s (dependent on the actual speed value and quick-stop delay parameterised with FCT)
t3 = 0...6553 ms (switch-off delay brake parameterised with FCT)
t4 ≤ 5 ms
t5 time delay PNOZ (> t1 + t2 + t3 + t4)
t_{STO} ≤ 12 ms
t6 ≤ 30 ms
t7 ≤ 720 ms
t8 ≤ 20 ms
t9 any
t10 > 2.5 ms
t11 = 50...500 ms (dependent on the brake used)
t12 = 0...6553 ms (with FCT parameterised switch-on delay brake)

Fig. 2.6 Timing diagram SS1

2.4.5 Parameterisation example

Setting the switch-off delay

The switch-off delay of the holding brake must be set in the FCT on the “Motor” page , “Brake control” tab. The set time is necessary, as the brake does not close immediately due to the mechanics. If this set time = 0 or <= 10 ms, vertically hanging loads can briefly slip through.

Determination of the brake time

The brake time can be determined with the FCT Trace Function. The brake time can vary greatly due to different travel speeds and delays. Determine the values for the maximum brake time with maximum travel speed.

To do this, select the actual actual value in the FCT on the “Configure measurement data”.

Then perform a measurement (“Start trace”).

During the measurement, remove the controller enable and so determine the brake time from the measurement curve on the “Measurement data” page. A typical measurement curve can look as follows.

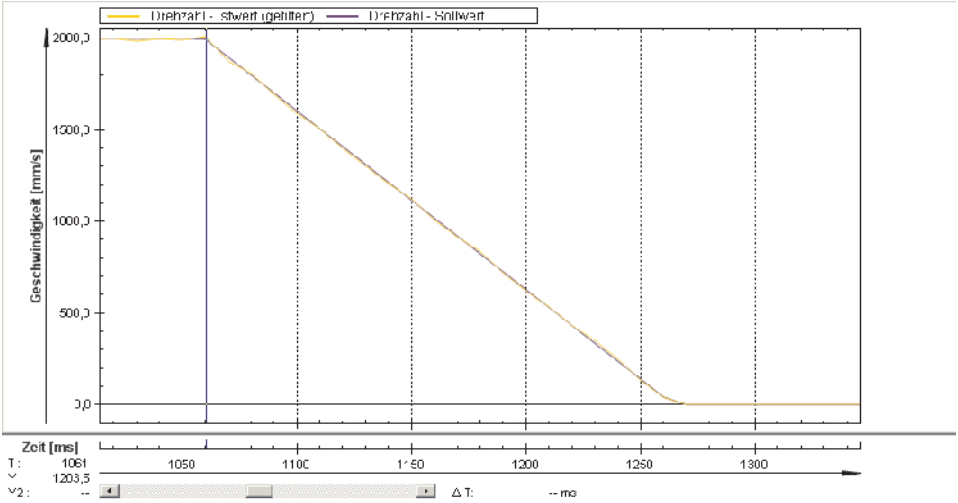


Fig. 2.7 Typical measurement curve for determination of brake time

Calculation example:

- graphically read brake time (t2): 210 ms
- parameterised switch-off delay for the brake: 150 ms (from FCT)
- time delay until output stage from (t4): 5 ms (fixed)
- sum: 210 ms + 150 ms + 5 ms = 365 ms
- safety reserve for dispersion of the brake times (example): 10 %
- time delay of the PNOZ (t5): 400 ms

Time delay of the PNOZ s5 from Pilz

The time delay of the PNOZ s5 from Pilz must be set greater than the determined brake time; see calculation example. Otherwise, the drive would not brake in the defined manner, but would run out uncontrolled.

- Plan a safety reserve for dispersion of the brake times, e.g. 10 %.

2.5 Testing the safety function

At each On-Off cycle of the machine, the safety switching devices PNOZ from Pilz check whether the relays of the safety device open and close properly.

Since the safety switching devices can check all required functions only during activation and request of the safety function, the safety function must be activated regularly and its function checked.

In addition, the “Acknowledgment of driver supply” signal must be checked for plausibility.

If a performance test does not take place in the process through regular actuation of the protective device:

- Perform a performance test at least once a week.
- Perform a performance test each time the machine is switched on.

3 Mounting and installation

3.1 Mounting / dismantling

The protection circuit is integrated into the CMMS-ST-...-G2 motor controller and cannot be dismantled.

Information on mounting the motor controller ➔ Description, mounting and installation, GDCP-CMMS-ST-G2-HW-... (➔ Tab. 2).

3.2 Electrical installation

3.2.1 Safety instructions

In the installation, the requirements of EN 60204-1 must be fulfilled.

Warning

Danger of electric shock from voltage sources without safeguarding.

- Use only PELV circuits in accordance with EN 60204-1 for the electric logic supply (Protective Extra-Low Voltage, PELV).
  Also take into account the general requirements for PELV circuits in accordance with EN 60204-1.
- Only use power sources which guarantee reliable electrical isolation of the operating voltage in accordance with EN 60204-1.

Through the use of PELV circuits, protection from electric shock (protection from direct and indirect contact) in accordance with EN 60204-1 is ensured (Electrical equipment of machines. General requirements). A 24 V power supply unit used in the system must meet the requirements of EN 60204-1 for DC power supply units (behaviour in case of voltage interruptions, etc.).
The cable is connected with plugs; this makes it easier to replace the motor controller.

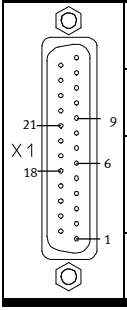
Make sure that no jumpers or the like can be inserted parallel to the safety wiring, e.g. through the use of the maximum wire cross section of 1.5 mm² or suitable wire end sleeves with insulating collars.
Use twin wire end sleeves for looping through lines between neighbouring devices.

ESD protection

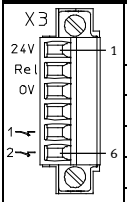
On unoccupied plug connectors, there is the danger that damage can occur to the device or other system parts from electrostatic discharge (ESD). Earth the system parts prior to installation and use suitable ESD equipment (e.g. shoes, earthing straps, etc.).

3.2.2 Ports [X1] and [X3]

The motor controller CMMS-ST-...-G2 has digital inputs for the integrated safety function at the plug connectors [X1] and [X3].

Plug connector [X1]	Pin	Allocation	Value	Description
	6	GND24	0 V	Reference potential for digital inputs and outputs
	9	DIN5	0 V / 24 V	Controller enable (high active)
	18	24 V	+24 V DC	Auxiliary power supply (24 V DC logic supply of the motor controller provided)
	21	DIN4	0 V / 24 V	Output stage enable (high active)

Tab. 3.1 Pin allocation [X1], only for connections relevant for the safety function (representation of the plug connector on the device)

Plug connector [X3]	Pin	Designation	Value	Description
	1	24 V	+24 V DC	Voltage output (24 V DC logic supply carried out as auxiliary voltage)
	2	Rel	0 V / 24 V	Driver supply relay control
	3	0 V	0 V	Reference potential for digital inputs and outputs
	4	–	–	–
	5	1 ⌒ (NC1)	Max. 25 V AC, 30 V DC, 2 A	Acknowledgment contact for the status “Safe Torque Off” (STO)
	6	2 ⌒ (NC2)		

Tab. 3.2 Pin allocation [X3] (representation with plug connector on the device in the scope of delivery)

To ensure the function STO “Safe Torque Off”, the control ports DIN4 [X1.21] and Rel [X3.2] must be connected in two channels through parallel wiring ➔ Section 2.3, Fig. 2.3.
This interface can be part of an emergency stop circuit or a protective door arrangement, for example. Carry out the connection corresponding to section A.1.3, Tab. A.9.

You will find switching examples in section 2.3 and 2.4.

4 Commissioning

Note
The term “commissioning” does not mean the first intended use by the end customer, but the commissioning by the machine manufacturer during set-up of the machine.

Note
Failure of the safety function!
Lack of the safety function can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuators.
- Place the motor controller in operation only if all safeguarding, including the safety function, has been introduced.
- The safety function must be tested and a corresponding validation procedure must be carried out prior to intended use ➔ Section 4.2.

Incorrect wiring or the use of incorrect external components, which have not been selected in accordance with the safety category, can result in a loss of the safety function.

- Carry out a risk assessment for your application and select the circuitry and components correspondingly.
- Observe the examples ➔ sections 2.3 and 2.4.

4.1 Prior to commissioning

Carry out the following steps in preparation for commissioning:
1. Make sure the motor controller is correctly mounted (➔ Section 3.1).
2. Check the electrical installation (connecting cable, pin allocation ➔ Section 3.2). All FU conductors connected?

4.2 Performance test, validation

Note
The STO function must be validated after installation and after every change in installation. This validation must be documented by the person performing commissioning. To assist you with the commissioning, questions for risk minimisation are summarised below in the form of sample checklists.

The following checklists are no substitute for safety training.
No guarantee can be provided for the completeness of the checklists.

No.	Questions	Applicable	Completed
1.	Were all operating conditions and interventions taken into account?	Yes ☐ No ☐	☐
2.	Has the “3-step method” for risk minimisation been applied, i.e. 1. Inherently safe design, 2. Technical and poss. additional safety measures, 3. User information about the residual risk?	Yes ☐ No ☐	☐
3.	Were the hazards eliminated or the hazard risk reduced as far as practically possible?	Yes ☐ No ☐	☐
4.	Can it be guaranteed that the implemented measures will not pose new hazards?	Yes ☐ No ☐	☐
5.	Have the users been adequately informed and warned about the residual risks?	Yes ☐ No ☐	☐
6.	Can it be guaranteed that the operators’ working conditions have not deteriorated due to the safeguarding taken??	Yes ☐ No ☐	☐
7.	Are the safeguardings mutually compatible?	Yes ☐ No ☐	☐
8.	Was adequate consideration given to the potential consequences of using a machine designed for commercial/ industrial purposes in a non-commercial/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. 4.1 Questions for validation in accordance with EN ISO 12100 (example)

No.	Questions	Applicable	Completed
1.	Has a risk assessment been conducted?	Yes ☐ No ☐	☐
2.	Have an error list and a validation plan been drawn up?	Yes ☐ No ☐	☐
3.	Was the validation plan, including analysis and inspection, processed and a validation report compiled? The validation procedure must include the following inspections as a minimum:	Yes ☐ No ☐	☐
	e) Inspection of components: Is a CMMS-ST-...-G2 used (inspection using the rating plates)	Yes ☐ No ☐	☐
	f) Is the wiring correct (check against the wiring diagram)?	Yes ☐ No ☐	☐
	Have any short-circuit bypasses been removed?	Yes ☐ No ☐	☐
	Has a safety switching device been wired to X1 and X3?	Yes ☐ No ☐	☐
	Is the safety switch device certified and wired in accordance with the application's requirements?	Yes ☐ No ☐	☐
	g) Functional tests:	Yes ☐ No ☐	☐
	Actuation of the emergency stop button on the unit. Is the drive switched free of torque?	Yes ☐ No ☐	☐
	If only Rel (X3.2) is activated – is the drive switched torque-free immediately?	Yes ☐ No ☐	☐
	If only DIN4 (X1.21) is activated – is the drive switched torque-free immediately?	Yes ☐ No ☐	☐
	Has a short circuit been detected between Rel (X3.2) and DIN4 (X1.21) or is a suitable fault exclusion defined?	Yes ☐ No ☐	☐
	Check of the safety switching device with evaluation of the acknowledgment contact NC1/NC2: Is the drive switched torque-free if there is a short circuit from NC1 to NC2?	Yes ☐ No ☐	☐
	Is a restart inhibited? That is, no movement occurs when the emergency stop button is pressed and the enable signals are active unless a start command is acknowledged beforehand.	Yes ☐ No ☐	☐

Tab. 4.2 Questions for validation in accordance with EN ISO 13849-1 and -2 (example)

5 Operation

5.1 Obligations of the operator

The functionality of the safety equipment is to be checked at adequate intervals. It is the responsibility of the operator to choose the type of check and time intervals in the specified time period. The check is to be conducted so the excellent function of the safety equipment in interaction with all the components can be verified.
Recommendation: Carry out a performance test at least every 24 hours.

5.2 Maintenance and care

The CMMS-ST-...-G2 motor controller with integrated safety function is maintenance-free.

Note
Please observe the permissible number of switching cycles for the relays used in the device ➔ Section A.1.3, Tab. A.7.

5.3 Diagnostics and fault clearance

5.3.1 Status indicators

Display on the motor controller

Display	Description
	"H": STO is called up over two channels. If this is not the case, the normal status displays of the motor controller are shown..

Tab. 5.1 Seven-segment display on the motor controller

5.3.2 Error messages

When an error occurs, the motor controller shows an error message cyclically in the seven-segment display on the front of the motor controller. The error message consists of an "E" (for Error), a main index (xx) and a sub-index (y), e.g.: E 5 1 0.
Warnings have the same number as an error message. The difference is that a warning is displayed with a prefixed and suffixed hyphen, e.g. - 1 7 0 -.
In the following tables, the error messages relevant for the functional safety in relationship to the STO safety function are listed. The "Code" column includes the CiA 402 error code.

For the complete list of error messages ➔ Description, mounting and installation, GDCP-CMMS-ST-G2-HW-....

Where 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 eliminated.

Error group 05		**Internal power supply**		
No.	Code	Message		Reaction
05-2	8000h	**Error in driver supply**		PS off
		Cause	Error in the plausibility check of the driver supply (safe stop)	
		Action	• Separate device from the entire peripheral equipment and check whether the error is still present after reset. If so, an internal defect is present ➔ Repair by the manufacturer.	

Error group 45		**STO error**		
No.	Code	Message		Reaction
45-0	8000h	**Error in driver supply**		PS off
		Cause	Driver supply is still active despite the STO requirement.	
		Action	The internal logic for the STO requirement may be disturbed due to high-frequency switching operations at the input. • Check activation; the error must not recur. • If the error occurs again when STO is required: Check firmware ➔ Section “Product identification”? If all the named options have been excluded, the hardware of the motor controller is defective.	
45-1	8000h	**Error in driver supply**		PS off
		Cause	The driver supply is active again, although STO is still required.	
		Action	The internal logic for the STO requirement may be disturbed due to high-frequency switching operations at the input. • Check activation; the error must not recur. • If the error occurs again when STO is required: Check firmware ➔ Section “Product identification”? If all the named options have been excluded, the hardware of the motor controller is defective.	
45-2	8000h	**Error in driver supply**		PS off
		Cause	The driver supply is not active again, although STO is no longer required.	
		Action	If the error occurs again after the STO requirement is ended, the hardware of the motor controller is defective.	
45-3	8087h	**DIN4 plausibility error**		PS off
		Cause	Output stage no longer switches off ➔ Hardware defective	
		Action	Repair by the manufacturer	

6 Modification and replacement of the motor controller

6.1 Repair or replacement of the integrated protection circuit

Repair of the integrated protection circuit is not permissible. If required, replace the complete motor controller.

6.2 De-commissioning and waste management

Observe the local regulations for environmentally appropriate disposal of electronic modules.

A Technical appendix

A.1 Technical data

A.1.1 Safety engineering

Safety function STO in accordance with EN 61800-5-2: STO, Safe Torque Off

Safety reference data			
Category		3	Grading in categories as per EN ISO 13849-1
Performance Level		PL d	Performance level in accordance with EN ISO 13849-1
PFH_d	[h^{-1}]	4.53×10^{-8}	Probability of dangerous failure per hour
T	[Years]	20	Proof test interval Operating life in accordance with EN ISO 13849-1
			Maximum proof test interval; depending on switching frequency, considerably shorter proof test intervals may be required. Please take into account the maximum service life of the relay contact ➔ Tab. A.6.
$MTTF_d$	[Years]	2521	Mean time to dangerous failure.

Tab. A.1 Technical data: safety reference data

Due to the service life of the internal switching relay (➔ Tab. A.6), the safety data for the STO function apply for an annual actuation rate of:

– CMMS-ST-...-G2 up to Rev 05: n_{op} = 500 / a
– CMMS-ST-...-G2 from Rev 06: n_{op} = 500000 / a

Safety information	
Type test	The functional safety engineering of the product has been certified by an independent testing body in accordance with section 1.1.4, see certificate ➔ www.festo.com
Reliable component	Yes, for the STO safety function

Tab. A.2 Technical data: safety information

A.1.2 General, operating and environmental conditions CMMS-ST-...-G2

The complete technical data on CMMS-ST-...-G2 can be found in the description Mounting and Installation, GDCP-CMMS-ST-G2-HW-....
Please observe the restrictions of the environmental conditions, specifically the required output nominal power.

General technical data	
Product conformity and certifications	
CE marking (see declaration of conformity)	in accordance with EC Machinery Directive 2006/42/EC
	In accordance with EU EMC Directive 2004/108/EC
	The device is intended for use in an industrial environment. Outside of industrial environments, e.g. in commercial and mixed-residential areas, actions to suppress interference may have to be taken.

Tab. A.3 Technical data: general

Operating and environmental conditions		
Permissible setup altitude above sea level		
with nominal power	[m]	1000
with power reduction10 % each 1000 m	[m]	1000 ... 3000
Air humidity	[%]	0 ... 90 (non-condensing)
Degree of protection		IP20
Protection class		III
Overvoltage category		III
Degree of contamination in accordance with EN 61800-5-1		2
Ambient temperature		
with nominal power	[°C]	0 ... +40
with power reduction: 4 % per [K]	[°C]	+40 ... +50
Storage temperature	[°C]	–25 ... +70
Vibration and resistance to shocks		
Operation		in accordance with EN 61800-5-1, section 5.2.6.4
Transport		in accordance with EN 61800-2, section 4.3.3

Tab. A.4 Technical data: operating and environmental conditions

A.1.3 Electrical data [X1], [X3]

Control ports DIN4, DIN5 [X1.21, X1.9]		
Nominal voltage	[V DC]	24 (related to 0 V)
Voltage range	[V DC]	19.2 ... 28.8
Nominal current	[mA]	2.5 (typical; maximum 3)
Input voltage threshold		
Switch on	[V DC]	≥ 13.1
Switch off	[V DC]	≤ 3.4
Switching time from High to Low	[ms]	≤ 3
Switching time from Low to High	[ms]	≤ 8
Maximum test impulse length	[µs]	Not specified; no tolerance against test impulses

Tab. A.5 Technical data: electrical data for the digital inputs at [X1]

Control port Rel [X3.2]		
Nominal voltage	[V DC]	24 (related to 0 V)
Voltage range	[V DC]	19.2 ... 28.8
Nominal current	[mA]	20 (typical; maximum 30)
Input voltage threshold		
Switch on	[V DC]	≥ 17.9
Switch off	[V DC]	≤ 2.5
Switching time from High to Low	[ms]	≤ 12
Switching time from Low to High	[ms]	≤ 20
Maximum test impulse length	[µs]	Not specified; no tolerance against test impulses
Service life of relay input, switching cycles n_{op}		
CMMS-ST up to Rev 05	[n_{op}]	10 000
CMMS-ST from Rev 06	[n_{op}]	10 x 10^6

Tab. A.6 Technical data: electrical data of the control port Rel [X3]

Acknowledgment contact NC1, NC2 [X3.5, X3.6]		
Design		Relay contact, normally closed
Max. voltage	[V DC]	< 30
Nominal current	[mA]	< 2000 at 30 V
Switching time closing	[ms]	< (Switching time from High to Low[1)] + 9 ms)
Switching time opening	[ms]	< (Switching time from Low to High [1)] + 9 ms)
Service life of acknowledgment contact, switching cycles n_{op} (at 24 V and $I_{Contact}$ = 10 mA; the service life is reduced with higher load currents)		
CMMS-ST up to Rev 05	[n_{op}]	10 000
CMMS-ST from Rev 06	[n_{op}]	10 x 10^6

1) Switching time ➔ Tab. A.6

Tab. A.7 Technical data: electrical data of the acknowledgment contact NC1/NC2 [X3]

Auxiliary supply 24 V, 0 V – output [X3.1, X3.3]		
Design		Logic supply voltage routed out of the motor controller (fed in at [X9], not additionally filtered or stabilised).
Nominal voltage	[V DC]	24
Nominal current	[mA]	100 (not short-circuit proof)
Voltage drop	[V]	≤ 1 (at nominal current)

Tab. A.8 Technical data: electrical data of the auxiliary supply output [X3]

Cabling [X3]		
Max. cable length	[m]	30
Screening		When wiring outside the control cabinet, use screened cable. Guide screening into the control cabinet / attach to the side of the control cabinet.
Cable 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 M2	[Nm]	0.22 ... 0.25

Tab. A.9 Technical data: cabling at [X3]

B Glossary

Term/abbreviation	Description
Cat.	Category in accordance with EN ISO 13849-1, steps 1-4.
Emergency off	In accordance with EN 60204-1: Electrical safety in case of emergency by switching off the electrical energy to all or part of the installation. EMERGENCY STOP 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 in an emergency by bringing a machine or moving parts to a stop. Emergency stop is used to stop a process or a movement if this creates a hazard.
FCT	Festo Configuration Tool, software for configuration and commissioning.
$MTTF_d$	Mean Time To Failure (dangerous): Time in years until the first dangerous failure will have occurred with 100 % probability, in accordance with EN ISO 13849-1.
PFH	Probability of Dangerous Failures per Hour
PL	Performance Level in accordance with EN ISO 13849-1: steps a ... e.
Safety switching device	Device for execution of safety functions or achievement of a safe status of the machine through switching off of the energy supply to dangerous machine functions. The desired safety function is achieved only in combination with other measures for risk reduction, although switch-off can occur on a motor controller, for example.
STO	Safe Torque Off.
T	Duration of use in accordance with EN ISO 13849-1.

Tab. B.1 Terms and abbreviations

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