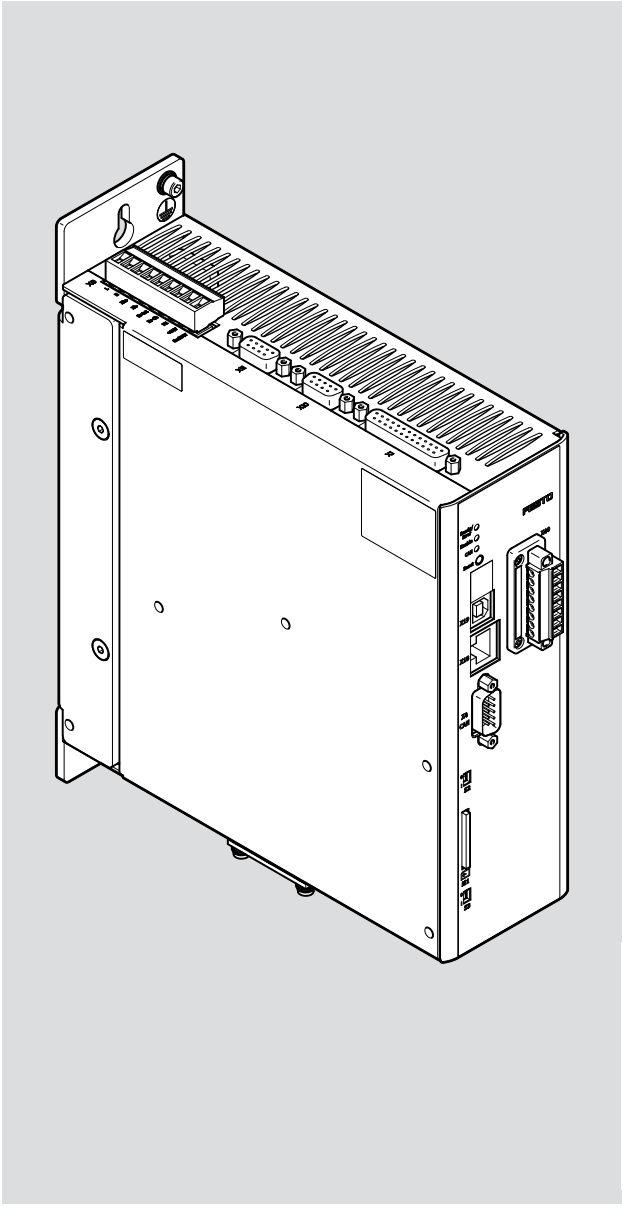
CMMP-AS-...-M0

Motor controller



FESTO

Manual | Safety function, STO

8219384

8219384
2024-07d

Original instructions

Table of contents

1 About this document

Notes regarding this documentation

This documentation is a guide to safe working with the STO – "Safe Torque Off" safety function in accordance with EN 61800-5-2 with use of the motor controller CMMP-AS-...-M0.

– In addition, always observe the general safety regulations for the motor controller CMMP-AS-...-M0.

The general safety regulations for the CMMP-AS-...-M0 can be found in the hardware documentation, GDCP-CMMP-M0-HW-... ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M0.
Observe the information regarding safety and the requirements for product use in ➔ 2.2 Requirements for product use.

Product identification

This documentation refers to the following versions:

- Motor controller CMMP-AS-...-M0, firmware from rev. 04.
- Firmware from 4.0.1501.1.2

You can find the information on the rating plate in the hardware description, GDCP-CMMP-M0-HW-...

Service

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

Specified standards/directives

Version		
EN 61800-5-1:2007 + A1:2017		EN ISO 12100-1:2010
EN 61800-5-2:2017		EN ISO 13849-1:2015
EN 60204-1:2006 + A1:2009 + AC:2010		IEC 61131-2:2007
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015		IEC 61508-1/.../-7:2010

Tab. 1: Standards/directives specified in the document

Documentation

You will find additional information on the motor controller in the following documentation:

User documentation for the motor controller CMMP-AS-...-M0	
Name, type	Contents
Hardware manual, GDCP-CMMP-M0-HW-...	Assembly and installation for all variants/performance classes (1-phase, 3-phase), pin allocations, error messages, maintenance.
Commissioning manual, GDCP-CMMP-M0-FW-...	Commissioning with FCT + functional description (firmware), overview of FHPP, fieldbus, safety engineering.

User documentation for the motor controller CMMP-AS-...-M0	
Name, type	Contents
FHPP manual, GDCP-CMMP-M0/-M0-C-HP-...	Control and parameterisation of the motor controller via the Festo FHPP profile.
CiA 402 (DS 402) manual, GDCP-CMMP-M3/-M0-C-CO-...	Control and parameterisation of the motor controller via the device profile CiA 402 (DS 402)
CAM Editor manual, P.BE-CMMP-CAM-SW-...	Cam disc function (CAM) of the motor controller.
STO safety function manual, GDCP-CMMP-AS-M0-S1-...	Functional safety engineering for the motor controller with the STO safety function.
Help for the FCT CMMP-AS plug-in	User interface and functions of the CMMP-AS plug-in for the Festo Configuration Tool ➔ www.festo.com/sp.

Tab. 2: Documentation for the motor controller CMMP-AS-...-M0

2 Safety and requirements for product use

2.1 Safety

2.1.1 General safety instructions

– Also always observe the general safety regulations for the motor controller CMMP-AS-...-M0.

The general safety regulations for the CMMP-AS-...-M0 can be found in the hardware documentation GDCP-CMMP-M0-HW-.... ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M0.

NOTICE

Loss of the safety function!

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

- Observe the specified environmental and connection conditions, in particular the input voltage tolerances ➔ 8.1.1 Technical data.

NOTICE

Damage to the motor controller due to incorrect handling.

Incorrect handling may cause damage.

- Switch off the power supply before mounting and installation work. Do not switch on the supply voltages until mounting and installation work is completely finished.
- Observe the handling specifications for electrostatically sensitive devices.

2.1.2 Intended use

The motor controller CMMP-AS-...-M0 supports the following safety function:

– Safe Torque Off (STO) with SIL 3 in accordance with EN 61800-5-2/EN 62061/IEC 61508 and/or category 4/PL e in accordance with EN ISO 13849-1.

The motor controller CMMP-AS-...-M0 is intended for installation in machines or automation systems and to be used as follows:

– in excellent technical condition,
– in its original condition, without unauthorised modifications,
– within the limits of the product defined by the technical data ➔ 8.1.1 Technical data
– in an industrial environment.

NOTICE

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

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

The motor controller CMMP-AS-...-M0 with integrated STO safety function fulfils the requirements for

– Category 4/PL e in accordance with EN ISO 13849-1,
– SIL CL 3 in accordance with EN 62061,

and can be used in applications up to cat. 4/PL e in accordance with EN ISO 13849-1 and SIL 3 in accordance with EN 61800-5-2/EN 62061/IEC 61508.

The achievable safety level depends on the other components used to implement a safety function.

2.2 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 in the documentation are observed at all times. When so doing, also take into account the documentation for the other components and modules (e.g. motor controller, cables etc.).
- Take into account the legal regulations applicable for the location as well as:
  - instructions and standards,
  - regulations of testing organisations and insurers,
  - national specifications.
- If the safety function is required, protection against automatic restart in accordance with the required category must be installed. For example, an external safety relay unit can be used.

2.2.1 Technical prerequisites

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

- Observe the connection and ambient conditions of the motor controller (➔ 8.1.1 Technical data) and all connected components as specified in the technical data.
  Only compliance with the limit values and/or load limits will enable operation of the product in accordance with the relevant safety directives.
- Observe the notes and warnings in this documentation.

2.2.2 Qualification of the specialist technicians (requirements for staff)

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

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

2.2.3 Diagnostic coverage (DC)

Diagnostic coverage depends on the integration of the motor controller into the control loop system as well as the implemented diagnostics measures ➔ 6.4.1 Diagnostics and fault clearance.
If a potentially dangerous malfunction is recognised during diagnostics, appropriate measures must be taken to maintain the safety level.

NOTICE

Check whether detection of shorts across contacts of the input circuit and the connection wiring is required in your application.
If necessary, use a safety relay unit with detection of shorts across contacts to control the safety function.

2.2.4 Range of application and approvals

The motor controller with integrated safety function is a safety-related part of controllers. For details of the safety-oriented standards and test values that the product complies with and fulfils, see ➔ 8.1.1 Technical data.
The product-relevant directives are listed in the declaration of conformity ➔ www.festo.com/sp.

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

Tab. 3: Product conformity

3 Description of the safety function STO

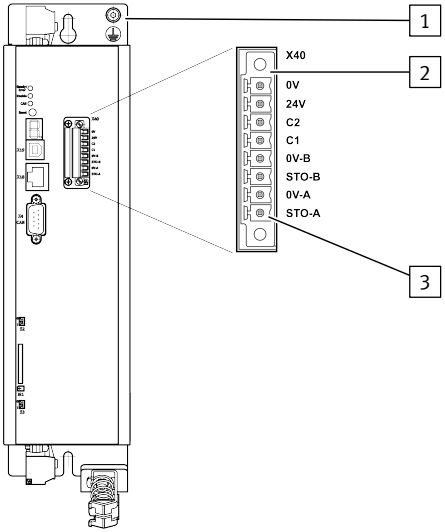
3.1 Product overview

3.1.1 Purpose

As processes become increasingly automated, protecting people from potentially hazardous movements is becoming ever more relevant. Functional safety refers to measures required of electrical or electronic equipment to reduce or eliminate dangers due to malfunctions. In normal operation, protective devices prevent human access to hazard zones. In certain operating modes, e.g. during set-up, people need to have access to danger zones. In such situations, the operator must be protected by measures incorporated into the drive and control system.
The functional safety engineering integrated 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 engineering.

3.1.2 Interface

The motor controller CMMP-AS-...-M0 has a digital I/O interface [X40] for control of the STO safety function.



1 Motor controller CMMP-AS-...-M0
2 Digital I/O interface [X40] for controlling the STO function
3 Pin 1 of the interface [X40]

Fig. 1: Motor controller CMMP-AS-...-M0

3.2 Function and application

The motor controller CMMP-AS-...-M0 has the following safety-related performance feature.
– Achieving the “Safe Torque Off” (STO) function,
– Potential-free feedback contact for the operating status,

The “Safe Stop 1” (SS1) function can be implemented with a suitable external safety relay unit and appropriate circuitry for the motor controller CMMS-AS-...-M0.

3.2.1 Description of the STO safety function

Use the “Safe Torque Off” function (STO) whenever you need to disconnect the energy supply to the motor reliably in your application.
The “Safe Torque Off” function switches off the driver power supply for the power semiconductor, thus preventing the power output stage from supplying the power required by the motor; see the diagram below.

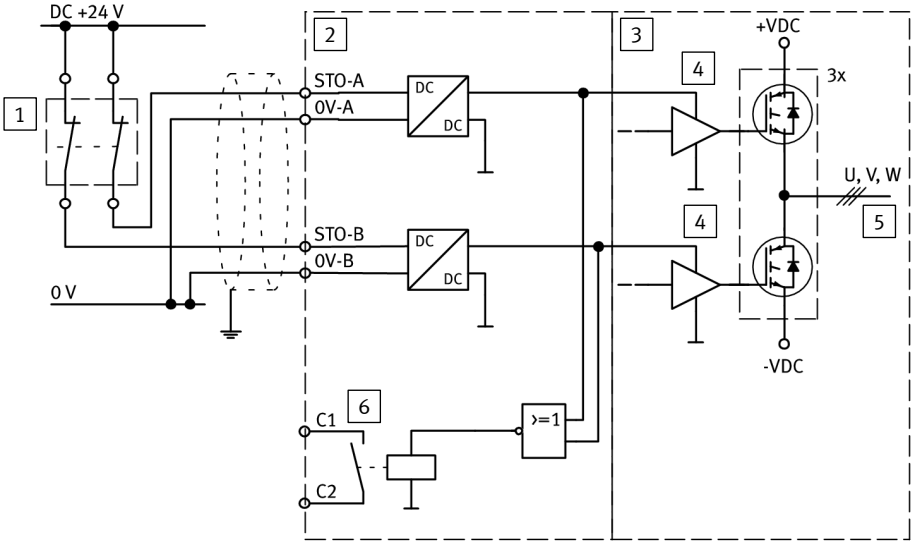


Fig. 2: “Safe torque off” - functional principle for the CMMP-AS-...-M0

1 Safety command device (e.g. switch, relay, safety relay unit)
2 STO integrated safety function
3 Power output stage in the CMMP-AS-...-M0 (only one phase shown)
4 Driver power supply
5 Motor connection
6 Feedback contact

The power supply to the drive is safely disconnected when the STO “Safe Torque Off” safety function is active. The drive cannot generate torque or force and so cannot perform any dangerous movements. With suspended loads or other external forces, additional measures must be taken to ensure that the load does not drop (e.g. mechanical holding brakes). The standstill position is not monitored in the STO “Safe Torque Off” state.
The machine must be brought to a standstill in a safe manner and secured, e.g. with a safety relay unit.

NOTICE

There is a danger that the drive will advance if there are multiple errors in the CMMP-AS-...-M0.
If the power stage of the motor controller fails during the STO state (simultaneous short circuit of 2 power semiconductors in different phases), this can result in a limited detent movement of the rotor.
The rotation angle/travel corresponds to one pole pitch. Examples:

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

3.2.2 Overview of interface [X40]

The front of the motor controller has an 8-pin connection [X40] for control inputs, feedback contact and a 24 V auxiliary supply for external sensors ➔ 4.2.1 Electrical installation.
The STO safety function is requested exclusively via the two digital control inputs STO-A and STO-B.
Safety circuitry for additional interfaces on the CMMD-AS-...-M0 motor controller is neither required nor intended.

ⓘ

Cross-circuit detection in the input circuit is not carried out by the motor controller.

The status of the motor controller is sent to an external safety relay unit via a potential-free feedback contact (N/O contact). This means that a downward compatible interface can be implemented in a mixed configuration consisting of CMMP-AS (previous series with the “safe stop” function via the [X3] connection) and the CMMP-AS-...-M0 ➔ 7.3 Replacement of the previous CMMP-AS series with the CMMP-AS-...-M0.
The interface [X40] allows direct connection of active and passive sensors, because a 24 V supply voltage (auxiliary supply) with associated reference potential is connected.

Ports		Description
STO-A 0V-A	(Pin 1) (Pin 2)	Control input A for the STO function with the associated reference potential – "Safe Torque Off" (STO) request at low (logic 0), together with STO_B. Control input 24 V, high active, based on EN 61131-2, signal level deviating from ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs.
STO-B 0V-B	(Pin 3) (Pin 4)	Control input B for the STO function with the associated reference potential. – "Safe Torque Off" (STO) request at low (logic 0), together with STO_A. Control input 24 V, high active, based on EN 61131-2, signal level deviating from ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs.
C1 C2	(Pin 5) (Pin 6)	Feedback contact for the "Safe Torque Off" status (STO), e.g. to an external controller.
		– Feedback contact open: "Safe Torque Off" (STO) not active
		– Feedback contact closed: "Safe Torque Off" (STO) active
24V 0V	(Pin 7) (Pin 8)	Auxiliary power supply, e.g. for safety-oriented peripherals (24 V DC logic power supply of the motor controller).

Tab. 4: Function of the connections [X40]

The connections are galvanically isolated from one another in groups and from the 24 V power supply of the motor controller ➔ Tab. 22 Technical data: electrical data of the auxiliary supply output.

3.2.3 Control inputs STO-A, 0V-A/STO-B, 0V-B [X40]

The STO (Safe Torque Off) safety function is requested via two channels with the two control inputs STO-A and STO-B. They allow the direct connection of safe semiconductor outputs (electronic safety relay units, active safety sensors, e.g. light curtains with OSSD signals) and switching contacts (safety relay units with relay outputs, passive safety sensors, e. g. positively driven position switches) ➔ 4.3.1 Safe Torque Off (STO).
In order to request the STO (Safe Torque Off) safety function, the 24 V control voltage is switched off at both control inputs STO-A and STO-B (0 V).
If the two control ports are switched off simultaneously or within a defined discrepancy time, the STO safety function is active. If both channels are not actuated simultaneously, the STO is still active on the first request. If a channel is not switched off, this is interpreted as an error and results in an error message.
Undervoltage monitoring is integrated for the STO-A and STO-B control inputs in order to rule out invalid voltage ranges for the downstream electronics, as well as overvoltage monitoring to protect against overvoltage.

ⓘ

Technical data of the control inputs ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs.

Tolerance ranges are defined for the input voltage range of the STO-A and STO-B control inputs.
The amount of energy stored in the components of the motor controller (e.g. capacitors) depends on the level of the input voltage. This amount of energy must be charged or discharged during switching operations. The input voltage-dependent values are thus derived for the switch-off time for the transition to the safe state (STO) and the tolerance time for OSSD signals (buffer time).
The requirements for the time response are derived from the technical data ➔ 8.1.3 Electrical data [X40]. The time response itself is described here ➔ 3.4 Time response.

Discrepancy time

The transition between a safe and an unsafe state is initiated by level changes at the control inputs STO-A and STO-B of the motor controller. According to the specification of the safety function, both levels must be identical, otherwise an error message is generated. The state machine in the motor controller internally monitors the driver supply voltages as a result of the control of the control inputs. The level changes do not usually take place exactly simultaneously, for example, because of component tolerances or bouncing outputs of safety controls. The firmware tolerates this so long as the second input follows within a defined time, the so-called discrepancy time. If the time is exceeded, the motor controller generates an error message.
A discrepancy time of 100 ms is the default.
Recommendation: always switch STO-A and STO-B simultaneously.

Test pulses

Test pulses from safety controllers are tolerated in a specific range and thus do not lead to the request of the STO function.

The tolerance to test pulses from sensors with OSSD signals depends on the operating range ➔ Tab. 20 Typical switch-off time and minimum tolerance time for test pulses (OSSD signals). The permissible test pulse length depends on the control voltage level at the STO-A and STO-B inputs. Example: input voltage for STO-A and STO-B = 24 V ➔ OSSD signals with a test pulse length of 3.5 ms are tolerated.

3.2.4 Feedback contact C1, C2 [X40]

If **the STO function is not active**, the feedback contact is opened. This is the case if the control voltage is present at STO-A and STO-B, if only one of the two control voltages STO-A or STO-B is present, if the 24 V logic supply voltage is switched off or if the supply voltage fails.
When **the STO function is active**, the relay contact is closed.

ⓘ

The feedback contact has a single channel and may only be used for monitoring.
Electrical data of the feedback contact ➔ Tab. 21 Technical data: electrical data of the feedback contact C1/C2. Time response of the feedback contact ➔ Tab. 20 Typical switch-off time and minimum tolerance time for test pulses (OSSD signals).
When the 24 V supply of the basic unit is switched on and off, the switching status of the relay may deviate briefly (approx. 100 ms) from the status of the STO-A and STO-B control inputs due to the difference in speed at which the internal supply voltage starts up.

ⓘ

In order to ensure the DC and SFF values specified in the technical data, the status of the feedback contact C1/C2 must be registered whenever the safety function is requested.
After the safety function has been requested, there must be a signal change at the feedback contact within an application-specific time. In the event of a violation, a safety-oriented reaction must take place.

3.2.5 24 V, 0 V auxiliary power supply [X40]

The motor controller CMMP-AS-...-M0 supplies a 24 V auxiliary power supply at [X40]. This can be employed when using the C1/C2 feedback contact or for power to external active sensors.

ⓘ

Electrical data of the auxiliary power supply ➔ 8.1.3 Electrical data [X40], ➔ Tab. 22 Technical data: electrical data of the auxiliary supply output.

3.3 Functions in the motor controller CMMP-AS-...-M0

The following functions in the motor controller CMMP-AS-...-M0 are not certified according to EN 61800-5-2. They are functional supplements and offer additional diagnostic options.
Error messages generated by the integrated safety circuit, e. g. exceeding the discrepancy time, are recorded and evaluated by the non-safety-related state machine of the motor controller. If the conditions for an error status are detected, an error message is generated. In this case, it cannot be guaranteed under all circumstances that the power output stage has been safely switched off.

The integrated safety circuit exclusively controls the provision of the driver supply for the motor controller CMMP-AS-...-M0. The levels of the input voltage are monitored area by area, but the integrated safety circuit does not have its own error evaluation mechanisms or the option of an error display.

NOTICE

When error messages are acknowledged, all acknowledgeable errors regarding functional safety are also acknowledged ➔ 6.4.2 Error messages.

The motor controller CMMP-AS-M0 monitors the status of the STO-A and STO-B control inputs. As a result, the request for the STO (Safe Torque Off) safety function is detected by the firmware of the motor controller and various non-safety-related functions are then executed:
- detection of the shutdown of the driver supply for the power semiconductors by the integrated safety circuit,
- switching off the drive control and the control of the power semiconductors (PWM),
- the holding brake control is switched off (if configured),
- state machine on the motor controller side with evaluation of the control (discrepancy time),
- detection of application-related error states,
- hardware diagnostics,
- status and error indication via display, digital outputs, fieldbuses etc.

NOTICE

If one of the control inputs STO-A or STO-B is deactivated while the output stage is active, this leads to the drive coasting down without braking.
If uncontrolled coasting could result in a hazard or damage, additional measures are required.

NOTICE

A clamping unit is actuated by the non-safety-relevant firmware of the motor controller CMMP-AS-...-M0.

ⓘ

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

A safe state with active control of the power semiconductors (PWM) can be requested. The status of both driver supply voltages is recorded and evaluated in a 10 ms cycle. If they are unequal over a longer period of time, an error message is triggered ➔ 6.4.2 Error messages. The safety function assumes that both signals have the same status. Unequal signals are only tolerated during a transition period, the so-called "discrepancy time" ➔ 3.2.3 Control inputs STO-A, 0V-A/STO-B, 0V-B [X40].
This status machine in the motor controller CMMP-AS-...-M0 has its own status parallel to the integrated safety circuit. Due to the assessment of the discrepancy time, this state machine may only reach the "safe state" with a significant delay. Accordingly, this state can only be signaled with a significant delay via digital outputs or a fieldbus. The power output stage itself is then already "safely switched off". This status machine is processed in a 10 ms cycle.
This results in a staggered reaction speed according to the following table:

Function	Reaction time	Reaction
Switching time from high to low	T_STO-A/B_OFF	➔ 8.1.3 Electrical data [X40], ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs
Switching time from low to high	T_STO-A/B_ON	
Detection of failure Driver power supply	$t_{Reaction} \leq 125$ µs	Control of the power semiconductors (PWM) is switched off
Activate holding brake	$t_{Reaction} \leq 10$ ms	Actuation of the holding brake after detecting the failure of the driver power supply
Signal evaluation and status indicator	$t_{Reaction} \leq 10$ ms	Status transitions in the internal status machine, triggering of an error message if necessary and showing the status on the display

Tab. 5: Driver supply voltage acquisition and reaction times

3.4 Time response

The STO-A and STO-B inputs are functionally absolutely equivalent, therefore the switching sequence of STO-A/STO-B is interchangeable in all diagrams.

3.4.1 STO basic time response

The figure below shows the basic time response of the integrated safety circuit. The times can be found in the table below.

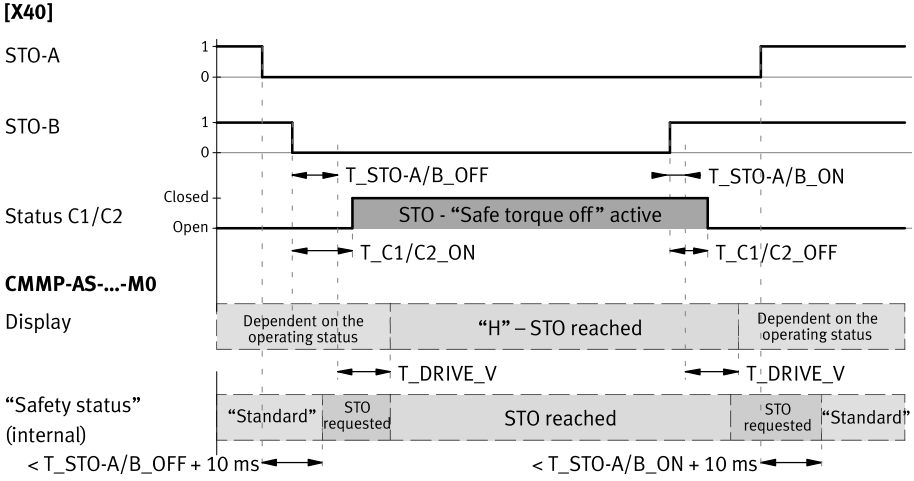


Fig. 3: Basic time response when activating and deactivating the STO safety function

Time	Description	Value
T_STO-A/B_OFF	STO-A/B – switching time from high to low	➔ 8.1.3 Electrical data [X40], ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs
T_STO-A/B_ON	STO-A/B – switching time from low to high	
T_C1/C2_ON	C1/2 – switching time for closing	➔ 8.1.3 Electrical data [X40], ➔ Tab. 21 Technical data: electrical data of the feedback contact C1/C2
T_C1/C2_OFF	C1/2 – switching time for opening	
T_DRIVE_V	Delay of the CMMP-AS-M0	0 ... 10 ms

Tab. 6: Time specifications for the basic time response

3.4.2 Time response of activation of STO in operation with restart

The figure below shows the time response from switching off the control voltage at STO-A/B and the process required to restart the device. The times can be found in the table below. Notes:
- The holding brake is controlled via the motor controller, not safety-related.
- The coasting of the motor is shown, independent of activation/deactivation of the brake.
- The setpoint value is only enabled when the holding brake delay T_BRAKE_V has expired.

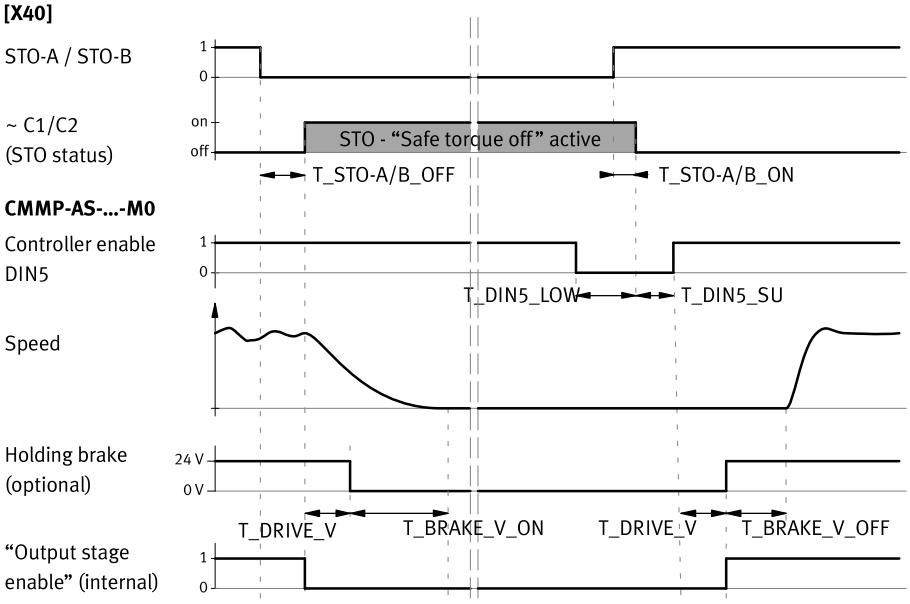


Fig. 4: Time response when activating the STO safety function with restart

Time	Description	Value
T_STO-A/B_OFF	STO-A/B – switching time from high to low	➔ 8.1.3 Electrical data [X40], ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs
T_STO-A/B_ON	STO-A/B – switching time from low to high	
T_DIN5_LOW	Time that DIN5 must be low before STO-A/B is switched on again	0 ms
T_DIN5_SU	Time that DIN5 must still be low after switching on STO-A/B again and changing the status of the STO module	> 20 ms
T_DRIVE_V	Delay of the CMMP-AS-M0	0 ... 10 ms
T_BRAKE_V_ON	Switch-off delay of the holding brake	Depending on the brake [1)]
T_BRAKE_V_OFF	Switch-on delay of the holding brake	Depending on the brake [2)]

1) Physical delay time until the brake is activated.
2) Minimum time: physical delay time until the brake is released. This time can be parameterised with a higher value in the controller.

Tab. 7: Times for the time response when activating the STO safety function with restart

3.4.3 Time response of activation of SS1 in operation with restart

The time response in the figure below is based on the sample circuit for SS1 in, based on the control signal S1 for K1 ➔ 4.3.2 Deceleration and Safe Torque Off (SS1, "Safe Stop 1"). The times can be found in the table below.

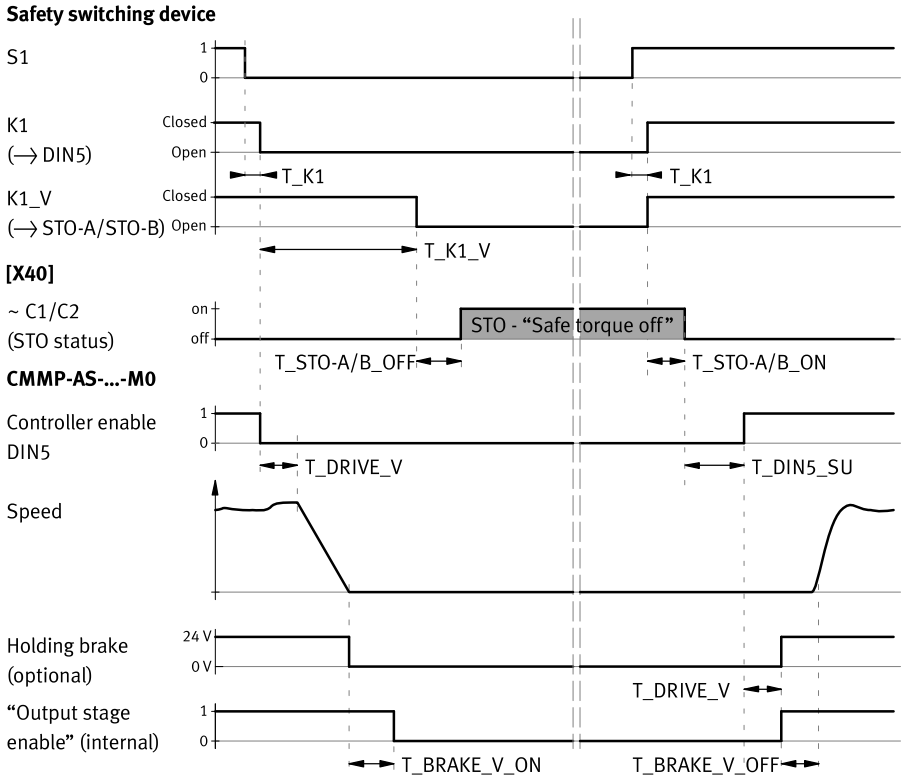


Fig. 5: Time response when activating the SS1 safety function (external circuitry) with restart

Time	Description	Value
T_K1	Delay time between switching S1 and closing instantaneous contact K1	➔ Data sheet of the safety relay unit
T_K1_V	Delay time between S1 and opening of the off-delayed contacts K1	Adjustable on the safety relay unit
T_STO-A/B_OFF	STO-A/B – switching time from high to low	➔ 8.1.3 Electrical data [X40], ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs
T_STO-A/B_ON	STO-A/B – switching time from low to high	
T_DRIVE_V	Delay of the CMMP-AS-M0	0 ... 10 ms
T_DIN5_SU	Time that DIN5 must still be low after switching on STO-A/B again and changing the status of the STO module	>20 ms

Time	Description	Value
T_BRAKE_V_ON	Switch-off delay of the holding brake	Depending on the brake [1]
T_BRAKE_V_OFF	Switch-on delay of the holding brake	Depending on the brake [2]

1) Physical delay time until the brake is activated.
2) Minimum time: physical delay time until the brake is released. This time can be parameterised with a higher value in the controller.

Tab. 8: Times for the time response when activating the SS1 safety function

4 Assembly and installation

4.1 Mounting/removal

The safety circuit is integrated in the motor controller CMMP-AS-...-M0 and cannot be removed.

Information on installing the CMMP-AS-...-M0 can be found in the hardware documentation, GDCP-CMMP-M0-HW-... ➔ Tab. 2 Documentation for the motor controller CMMP-AS-...-M0.

4.2 Electrical installation

4.2.1 Safety instructions

The requirements of EN 60204-1 must be fulfilled for the installation.

⚠ WARNING

Danger of electric shock from voltage sources without protective measures.

- Use only PELV circuits in accordance with EN 60204-1 (protective extra-low voltage, PELV) for the electrical logic power supply. Also take into account the general requirements for PELV circuits in accordance with EN 60204-1.
- Only use power sources that guarantee reliable electrical isolation of the operating voltage from the mains in accordance with EN 60204-1.

Protection from electric shock (protection from direct and indirect contact) in accordance with EN 60204-1 (Electrical equipment of machines, General requirements) is guaranteed with the use of PELV circuits. A 24 V fixed power supply used in the system must satisfy the requirements of EN 60204-1 for DC power supplies (behaviour during power interruptions, etc.).
The cable is connected to a plug, which makes it easier to replace the motor controller.

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

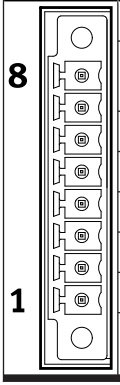
ESD protection

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

4.2.2 Connection [X40]

The motor controller CMMP-AS-...-M0 has a combined interface for open-loop control and feedback via the plug [X40] for the integrated safety function.

– Version on the device: PHOENIX MINICOMBICON MC 1.5/8-GF-3.81 BK
– Connector (in scope of delivery): PHOENIX MINICOMBICON MC 1.5/8-STF-3.81 BK, connection according to section ➔ 8.1.3 Electrical data [X40], ➔ Tab. 24 Technical data: wiring at [X40].

Plugs	Pin	Designation	Value	Description
	8	0V	0 V	Reference potential for auxiliary supply voltage.
	7	24V	+24 V DC	Auxiliary supply voltage (from the 24 V DC logic supply of the motor controller).
	6	C2	–	Feedback contact for the “STO” status on an external controller.
	5	C1		
	4	0V-B	0 V	Reference potential for STO-B.
	3	STO-B	0 V / 24 V	Control input B for the STO function.
	2	0V-A	0 V	Reference potential for STO-A.
	1	STO-A	0 V / 24 V	Control input A for the STO function.

Tab. 9: Pin allocation [X40] (diagram of the plug on the device)

The STO-A and STO-B control inputs must be connected in parallel over two channels to ensure the STO “Safe Torque Off” function ➔ 4.3.1 Safe Torque Off (STO), ➔ Fig. 6.
For example, this interface can be part of an emergency stop circuit or a safety door installation.

4.2.3 Minimum wiring for initial start-up [X40]

For initial commissioning of the motor controller without safety engineering, the motor controller CMMP-AS-...-M0 can be wired with a minimum circuit in accordance with ➔ Fig. 6 with an emergency stop switch ([2]).

NOTICE

Safety functions must never be bypassed.

Install the minimum circuits for the STO-A/STO-B and 0V-A/0V-B inputs for initial commissioning in such a way that they must be removed when the final safety circuitry is installed.

4.3 Sample circuits

4.3.1 Safe Torque Off (STO)

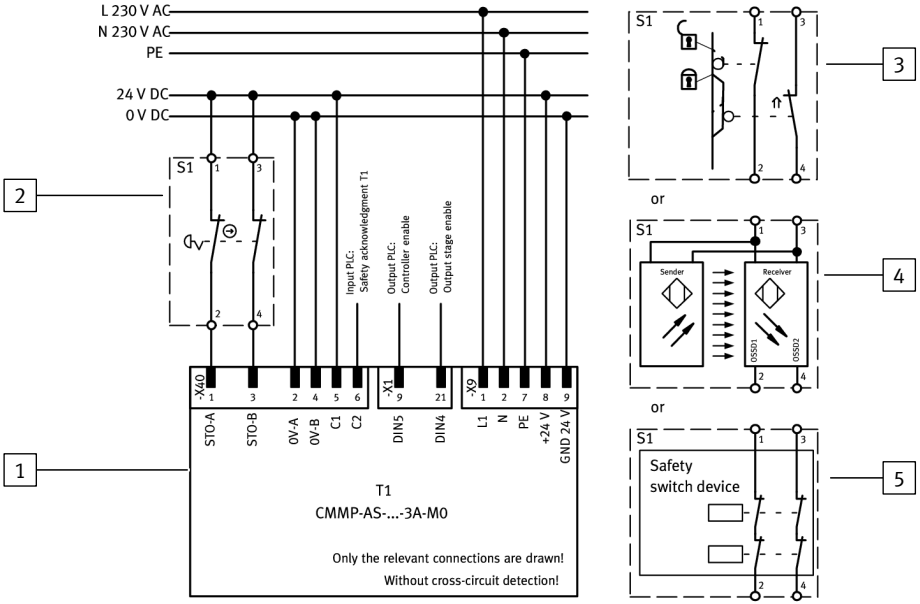


Fig. 6: Connection of the integrated safety function, example single-phase motor controller CMMP-AS-...-3A-M0

1 Motor controller with safety function (only relevant connections represented)

2 Emergency stop switch

3 Safety door

4 Light curtain

5 Safety relay unit

The "Safe Torque Off" (STO) safety function can be requested by various devices. For example, the switch S1 may be an emergency stop switch, a safety door switch, a light curtain or a safety relay unit. The security requirement is made in 2 channels via the S1 switch and leads to the 2-channel switch-off of the power stage. If the power stage has been switched off, it is output by the potential-free contact C1/C2.

Information on the sample circuit:

- Detection of shorts across contacts is not integrated in the motor controller with integrated safety function.
  The direct wiring of light curtains means that detection of shorts across contacts is implemented by the light curtain, if it is designed for this purpose.
- When using safety relay units, contact C1, C2 can be integrated into the feedback circuit of the safety relay unit.

- The sample circuit has a 2-channel structure that is suitable for categories 3 and 4 with additional measures.
- The additional measures required depends on the area of application and the safety concept of the machine.

4.3.2 Deceleration and Safe Torque Off (SS1, "Safe Stop 1")

The "Safe Stop 1" (SS1, Type C) safety function can be requested by various devices, see the following figure. For example, the S1 switch in the following figure can be an emergency stop switch, a safety door switch or a light curtain. The security requirement is made in 2 channels via the S1 switch and to the safety relay unit. The safety relay unit switches off the controller release. If the controller release of the motor controller is switched off, the movement is automatically delayed, the activation of the brake is delayed if the brake is configured and the control loop is then switched off. After a time set in the safety relay unit, the output stage is switched off via 2 channels via STO-A/B. If the power stage has been switched off, it is output by the potential-free contact C1-C2.

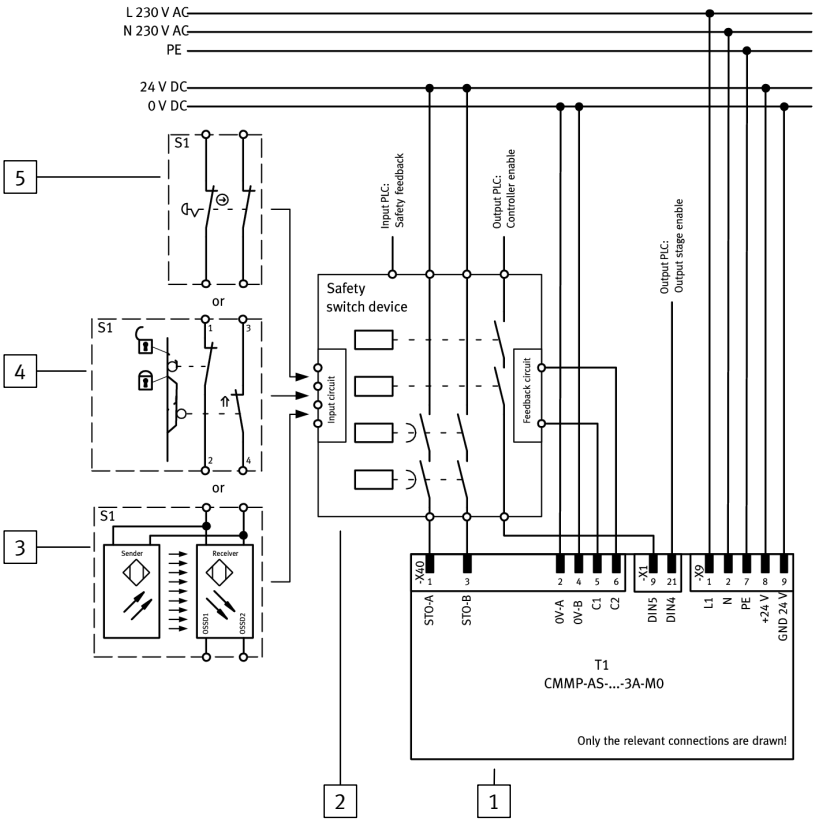


Fig. 7: Sample circuit "Decelerating and safe torque off" (SS1, "Safe Stop 1") with the example of single-phase motor controller CMMP-AS-...-3A-M0

1 Motor controller with safety function (only relevant connections represented)

2 Safety relay unit

3 Light curtain

4 Safety door

5 Emergency stop switch

Information on the sample circuit:

- The safety relay unit must switch off the controller enable (X1-9, DIN5) without time delay and the inputs STO-A and STO-B (X40-1, -3) with time delay.
- The required time delay depends on the application and must be determined specific to the application. The time delay must be designed in such a way that the drive is braked to zero even at the highest speed via the quick stop ramp in CMMP-AS...-M0 before STO-A/B are switched off.

- The electrical installation has been carried out in accordance with the requirements of EN 60204-1. For example, the safety relay unit and the motor controller are located in the same control cabinet to enable fault exclusion for a cross or earth fault between the cables (acceptance test of the control cabinet for fault-free wiring).
- The sample circuit has a 2-channel structure that is suitable for categories 3 and 4 with additional measures.
- The additional measures required depends on the area of application and the safety concept of the machine.

5 Commissioning

NOTICE

The term “commissioning” does not mean the first intended use by the end customer. It refers to commissioning by the manufacturer during setup of the machine.

NOTICE

Failure of the safety function!

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

- Only operate the safety function if all protective measures have been initiated.
- The safety function must be tested and a corresponding validation procedure must be carried out prior to intended use ➔ 5.3 Function test, validation.

Incorrect wiring or the use of incorrect external components that have not been selected in accordance with the safety category can result in failure of the safety function.

– Carry out a risk assessment for your application and select the circuitry and components accordingly.
– Observe the examples ➔ 4.3.1 Sample circuits.

5.1 Prior to commissioning

Carry out the following steps in preparation for commissioning:

1. Make sure that the motor controller is correctly mounted ➔ 4.1 Mounting/removal.
2. Check the electrical installation (connecting cables, contact assignment ➔ 4.2.1 Electrical installation). All PE conductors connected?

5.2 FCT support

Parameterisation is not required for the safety function integrated in the motor controller.

5.2.1 Status display of the safety function

The status of the safety function is displayed in the FCT, see the following table.

Characteristics	Display	Status
Status: Display of the module status	Green	Normal operation (STO not requested)
	Yellow	STO requested and achieved
	Red	Safety circuit error
Input X40.STO-A: Display of the input status	Grey	Safety function requested, STO-A = Low
	Green	Safety function not requested, STO-A = High

Characteristics	Display	Status
Input X40.STO-B: Display of the input status	Grey	Safety function requested, STO-B = Low
	Green	Safety function not requested, STO-B = High
Output X40.C1/C2: Display of the relay contact	Orange	Safety function active, relay contact closed
	Grey	Safety function inactive, relay contact open

Tab. 10: Status of the safety function

5.2.2 Displaying log file of the motor controller

Error and status messages are logged non-volatile in the permanent diagnostic memory of the CMMPAS-...-M0. You can read this out in the online 'Diagnostics' tab ➔ Fig. 8.

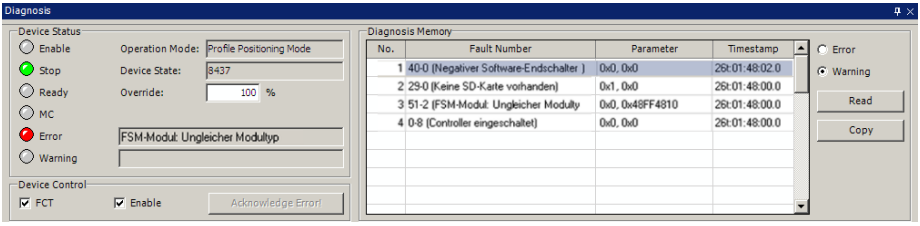


Fig. 8: FCT plug-in CMMP-AS: "Diagnostics" tab

5.3 Function test, validation

NOTICE

The STO function must be validated after installation and after changes to the installation.
This validation must be documented by the person who commissions the device. To assist you with the commissioning, questions for risk reduction are summarised below in the form of sample check lists.

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

No.	Questions	Relevant	Done
1.	Have all operating conditions and interventions been taken into account?	Yes ☐ No ☐	☐
2.	Has the 3-step method for risk reduction been applied, i.e.: 1. Inherently safe design, 2. Technical and any additional protective measures, 3. User information about the residual risk?	Yes ☐ No ☐	☐
3.	Have the hazards been eliminated or the hazard risks reduced as far as practically possible?	Yes ☐ No ☐	☐

No.	Questions	Relevant		Done
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. 11: Questions for the validation in accordance with EN ISO 12100-1:2010 (example)

No.	Questions		Relevant		Done
1.	Has a risk assessment been carried out?		Yes ☐	No ☐	☐
2.	Have a list of issues and a validation plan been drawn up?		Yes ☐	No ☐	☐
3.	Has the validation plan – including analysis and inspection – been worked through and has a validation report been created? The following must be inspected as a minimum as part of the validation:		Yes ☐	No ☐	☐
	a)	Check the components: is the CMMP-AS-...-M0 being used (check the rating plates).	Yes ☐	No ☐	☐
	b)	Is the wiring correct (check the circuit diagram)?	Yes ☐	No ☐	☐
		Have any jumpers been removed?	Yes ☐	No ☐	☐
		Has a safety relay unit been wired to X40?	Yes ☐	No ☐	☐
		Is the safety relay unit certified and wired in accordance with the application requirements?	Yes ☐	No ☐	☐
	c)	Functional tests:	Yes ☐	No ☐	☐
		Actuation of the emergency stop button of the system. Is the drive stopped?	Yes ☐	No ☐	☐

No.	Questions		Relevant	Done
3.	c)	If only STO-A is activated - is the drive shut down immediately and is the "Discrepancy time violation" error (display 52-1) reported in the CMMP-AS-...-M0 after the discrepancy time has expired?	Yes ☐ No ☐	☐
		If only STO-B is activated – is the drive shut down immediately and is the "Discrepancy time violation" error (display 52-1) reported in the CMMP-AS-...-M0 after the discrepancy time has expired?	Yes ☐ No ☐	☐
		Is a short circuit detected between STO-A and STO-B or is a suitable fault exclusion defined?	Yes ☐ No ☐	☐
		Only when using a safety relay unit with evaluation of the feedback contact C1/C2: Is the drive shut down if there is a short circuit from C1 to C2?	Yes ☐ No ☐	☐
		Is the restart inhibited? That means that there is no movement when the emergency stop button is actuated and the enable signals are active unless a start command is acknowledged beforehand.	Yes ☐ No ☐	☐

Tab. 12: Questions for validation in accordance with EN ISO 13849-1 and -2 (example)

6 Operation and use

6.1 Obligations of the operator

The functionality of the safety device must be tested at appropriate intervals. It is the responsibility of the operator to choose the type and frequency of the checks within the specified time period.
The manner in which the test is conducted must make it possible to verify that the safety device is functioning perfectly in interaction with all components.

6.2 Maintenance and care

The motor controller CMMP-AS-...-M0 with integrated safety function is maintenance-free.

6.3 Protective functions

6.3.1 Voltage monitoring

The input voltages at STO-A and STO-B are monitored. If the input voltage at STO-A or STO-B is too low or too high, the driver supply for the power semiconductors of the motor controller is switched off safely. This switches off the power output stage (PWM).

6.3.2 Overvoltage and reverse polarity protection

The STO-A and STO-B control inputs are protected against overvoltage and reverse polarity of the control voltage ➔ 8.1.3 Electrical data [X40], ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs.
The 24 V DC supply voltage of the motor controller connected to [X40] is short-circuit proof.

6.4 Diagnostics and fault clearance

6.4.1 Status display

Display on the motor controller

Display	Description
	“H”: the motor controller is in the “safe status”. This does not have the same meaning as the information on the status of the STO safety function (Safe Torque Off). There is no special display for the "unsafe status"; the normal status indicators of the motor controller are displayed.

Tab. 13: 7-segment display on the motor controller

6.4.2 Error messages

When an error occurs, the motor controller shows an error message cyclically in the 7-segment display on the front of the motor controller. The error message consists of an "E" (for Error), a main index (xx) and a subindex (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 -.
The error messages relevant for the functional safety in connection with the STO safety function are listed in the following tables.

The complete list of error messages can be found in the hardware documentation GDCP-CMMP-M0-HW-... of the motor controller.

If an error message cannot be acknowledged, the cause must first be remedied in accordance with the recommended measures. Then reset the motor controller and check whether the cause of the error and thus the error message have been eliminated.

Errors	Cause	Actions
51-0[1)]	Reserved	–
51-1[1)]	Safety function: driver function defective – Internal voltage error of the STO circuit	– Safety circuit defective. No action possible, please contact Festo. If possible, replace with another motor controller.
51-2[1)]	Reserved	–
51-3[1)]	Reserved	–
52-1	Safety function: discrepancy time expired	– Control inputs STO-A and STO-B are not actuated simultaneously. – Control inputs STO-A and STO-B are not wired in the same direction. – Check discrepancy time.
52-2	Safety function: driver supply failure with active PWM control	– The safe status was requested with power output stage enabled. Check integration into the safety-oriented interface.

1) The messages of error group 51 cannot be acknowledged.

Tab. 14: Error messages related to the safety function

7 Modification and replacement of the motor controller

7.1 Repair or replacement of the integrated safety circuit

Repair or maintenance of the integrated safety circuit is not permissible. If necessary, replace the entire motor controller.

7.2 Decommissioning and disposal

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

7.3 Replacement of the previous CMMP-AS series with the CMMP-AS-...-M0

CMMP-AS

The devices of the previous CMMP-AS series have a safety function STO "Safe Torque Off" permanently integrated in the device in accordance with EN ISO 13849-1, Cat. 3/PL d. The required two-channel nature of the STO function is achieved via two independent switch-off paths:

- 1st switch-off path: output stage enable via [X1.21], switch-off of the power output stage (blocking of the PWM signals). The drivers for the power semiconductors are no longer controlled with pulse patterns.
- 2nd switch-off path: interruption of the power supply to the six output stage power semiconductors (IGBTs) via [X3] using a relay. The driver supply for the power semiconductors (IGBT optocoupler) is separated with a relay. This prevents pulse patterns (PWM signals) from reaching the power semiconductors.

In addition, the CMMP-AS has a potential-free feedback contact ([X3] pin 5 and 6), which, as a diagnostic output, indicates the presence of the driver supply.

CMMP-AS-...-M0

The devices of the CMMP-AS-...-M0 series have the safety function STO "Safe Torque Off" in accordance with EN 61800-5-2 SIL3, or EN ISO 13849-1, Cat. 4/PL e. The two switch-off paths are implemented via the control inputs STO-A [X40.1] and STO-B [X40.3]. The potential-free feedback contact ([X40] pin 5 and 6) is also available.

Changes to connection wiring

In order to convert an existing application with STO from CMMP-AS to CMMP-AS-M0, the following changes in the connection wiring are required:

- 1. Shutdown path:
  Retain the wiring of the power stage enable [X1.21] and route it parallel to STO-A [X40.1]. Connect GNDA [X40.2] to 0 V [X40.8] to connect the reference potential.
- 2. Shutdown path:
  Now run the driver supply wiring [X3.RELAY] to STO-B [X40.3].
  Connect GNDB [X40.4] to 0 V [X40.8] to connect the reference potential.
- Feedback contact:
  Switch the connection for the feedback contact [X3.5] and [X3.6] to [X40.5] and [X40.6].

NOTICE

During operation, the feedback contacts behave compatibly with CMMP-AS and CMMP-AS-M0.
The response is different if the logic supply (24 V) is switched off:

- CMMP-AS: contact closed.
- CMMP-AS-...-M0: contact open.

Notes on project engineering

The CMMP-AS-...-M0 has a higher peak power than the CMMP-AS. This enables higher travel speeds depending on the application. If this is applied, it is a major change to the machine.

NOTICE

The parameter set of CMMP-AS must be transferred to the parameter set of CMMP-AS...-M0 with the same values. If these values increase and the risk increases as a result, a new risk assessment of the machine must be carried out.

NOTICE

After replacing the motor controller, the safety function must be validated in accordance with the machine manufacturer's specifications.

8 Technical appendix

8.1 Technical data

8.1.1 Safety engineering

Approval information, safety engineering	
CE	
Type-examination	The functional safety engineering of the product has been certified by an independent testing body, see EC-type examination certificate ➔ www.festo.com/sp
Certificate issuing authority	TÜV Rheinland, Certification Body of Machinery, NB 0035
Certificate no.	01/205/5262.03/25

Tab. 15: Approval information, safety engineering

Safety engineering			
Safety reference data			
Safety function		STO	– Safe restart interlock (STO, Safe Torque Off) in accordance with EN 61800-5-2 with SIL 3 – Safe restart interlock (STO, Safe Torque Off) in accordance with EN ISO 13849-1 with category 4 and PL e
SIL		SIL 3	Safety integrity level in accordance with EN 61800-5-2/IEC 61508
		SIL CL 3	SIL Claim Limit for a subsystem in accordance with EN 62061
Category		4	Classification in category in accordance with EN ISO 13849-1
PL		PL e	Performance level in accordance with EN ISO 13849-1
DCavg	[%]	97	Average diagnostic coverage
HFT		1	Hardware fault tolerance
SFF	[%]	99.2	Safe failure fraction
PFH		1.27×10^{-10}	Probability of dangerous failure per hour
PFD		2.54×10^{-5}	Probability of dangerous failure on demand
T	[years]	20	Proof test interval Service life in accordance with EN ISO 13849-1
$MTTF_d$	[years]	1370	Mean time to dangerous failure.

Safety engineering	
Safety specifications	
Well-tried component	Yes, for the STO safety function

Tab. 16: Safety engineering

8.1.2 General, operating and environmental conditions CMMP-AS-...-M0

The complete technical data for the CMMP-AS-...-M0 can be found in the hardware documentation GDCP-CMMP-M0-HW-...

General technical data	
Approvals	
Certificates, declaration of conformity	➔ www.festo.com/sp
The device is intended for use in an industrial environment. Measures for interference suppression may be required in residential areas.	

Tab. 17: General technical data

Operating and environmental conditions for CMMP-AS-...-M0		
Permissible setup altitude above mean sea level		
– at nominal power	[m]	1000
– with power reduction	[m]	1000 ... 2000
Humidity	[%]	0 ... 90 (non-condensing)
Degree of protection		IP20
Pollution degree in accordance with EN 61800-5-1		2 The integrated safety-engineering equipment requires compliance with pollution degree 2 and thus a protected installation space (IP54). It must always be ensured by taking appropriate measures, e.g. by installation in a control cabinet.
Operating temperature	[°C]	0 ... +40
Operating temperature with power reduction 2.5% per K	[°C]	+40 ... +50
Storage temperature	[°C]	-25 ... +70
Vibration and shock resistance		

Operating and environmental conditions for CMMP-AS-...-M0	
– 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. 18: Operating and environmental conditions

8.1.3 Electrical data [X40]

Control inputs STO-A, 0V-A/STO-B, 0V-B		
Nominal voltage	[V]	24 (related to 0V-A/B)
Voltage range	[V]	19.2 ... 28.8
Permissible residual ripple	[%]	2 (based on nominal voltage 24 V)
Overvoltage shutdown	[V]	31 (shutdown in case of fault)
Nominal current	[mA]	20 (typical; maximum 30)
Starting current	[mA]	450 (typical, duration approx. 2 ms; max. 600 at 28.8 V)
Input voltage threshold		
– Switching on	[V]	approx. 18
– Switching off	[V]	approx. 12.5
Switching time from high to low (STO-A/B_OFF)	[ms]	10 (typical; maximal 20 at 28.8 V)
Switching time from low to high (STO-A/B_ON)	[ms]	5 (typical; maximum 7)
Maximum positive test pulse length with logic 0	[µs]	< 300 (related to nominal voltage 24 V and intervals > 2 s between pulses)

Tab. 19: Technical data: electrical data of the STO-A and STO-B inputs

Switch-off time to power output stage inactive and maximum tolerance time for test pulses											
Input voltage (STO-A/B)	[V]	19	20	21	22	23	24	25	26	27	28
– Typical switch-off time (STO-A/B_OFF)	[ms]	4.0	4.5	5.0	6.0	6.5	7.0	7.5	8.0	8.5	9.5
– Maximum tolerance time for test pulses with 24 V signal	[ms]	< 2.0	< 2.0	2.0	2.5	3.0	3.5	4.5	5.0	5.5	6.0

Tab. 20: Typical switch-off time and minimum tolerance time for test pulses (OSSD signals)

Feedback contact C1, C2		
Design		Relay contact, N/O contact
Max. voltage	[V DC]	< 30 (overvoltage-proof up to 60 V DC)
Nominal current	[mA]	< 200 (not short-circuit-proof)
Voltage drop	[V]	≤ 1
Off-state current (contact open)	[µA]	< 10
Switching time for closing (T_C1/C2_ON)	[ms]	< (STO-A/B_OFF + 5 ms) STO-A/B_OFF ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs
Switching time for opening (T_C1/C2_OFF)	[ms]	< (STO-A/B_ON + 5 ms) STO-A/B_ON ➔ Tab. 19 Technical data: electrical data of the STO-A and STO-B inputs

Tab. 21: Technical data: electrical data of the feedback contact C1/C2

Auxiliary supply 24V, 0V – output		
Design		Logic supply voltage routed out of the motor controller (fed in at [X9], not additionally filtered or stabilised). Protected against reverse polarity, overvoltage-proof up to 60 V DC.
Nominal voltage	[V]	24
Nominal current	[mA]	100 (short-circuit-proof, max. 300 mA)
Voltage drop	[V]	≤ 1 (at nominal current)

Tab. 22: Technical data: electrical data of the auxiliary supply output

Galvanic isolation	
Galvanically isolated potential areas	STO-A/0V-A
	STO-B/0V-B
	C1/C2
	24 V/0 V (logic supply of the motor controller)

Tab. 23: Electrical data [X40]

Wiring		
Max. cable length	[m]	30
Shielding		Use shielded cable for wiring outside the control cabinet. Guide shielding into the control cabinet/attach to the side of the control cabinet.
Conductor cross section (flexible conductors, wire end sleeve with insulating collar)		
– one conductor	mm^2	0.25 ... 0.5
– two conductors	mm^2	2 x 0.25 (with twin wire end sleeves)
Tightening torque M2	[Nm]	0.22 ... 0.25

Tab. 24: Technical data: wiring at [X40]

9 Glossary

Term/abbreviation	Description
CCF	Common Cause Failure in accordance with EN ISO 13849-1.
DC avg	Average Diagnostic Coverage, diagnostic coverage in accordance with IEC 61508 and EN 61800-5-2.
FCT	Festo Configuration Tool, software for configuration and commissioning.
HFT	Hardware Fault Tolerance in accordance with IEC 61508.
Cat.	Category in accordance with EN ISO 13849-1, steps 1-4.
$MTTF_d$	Mean Time To dangerous Failure: time in years until the first dangerous failure occurs with 100% probability, in accordance with EN ISO 13849-1.
Emergency off	In accordance with EN 60204-1: electrical safety is ensured in case of emergency by switching off the electrical power to all or part of the installation. Emergency off is to be used where a risk of electric shock or other electrical risk exists.
Emergency stop	In accordance with EN 60204-1: functional safety is ensured in an emergency by bringing a machine or moving parts to standstill. Emergency stop is intended to stop a process or a movement if this has created a hazard.
OSSD	“Output Signal Switching Device”: output signals with 24 V level cycle rates for error detection.
PFD	Probability of Failure on Demand according to IEC 61508.
PFH	Probability of dangerous failures per hour in accordance with IEC 61508.
PL	Performance Level in accordance with EN ISO 13849-1: steps a … e.
SFF	Safe Failure Fraction [%], ratio of the failure rates of safe and dangerous (but detectable) failures to the sum of all failures in accordance with IEC 61508.
Safety relay unit	Device for execution of safety functions or achievement of a safe status of the machine by switching off the power supply to dangerous machine functions. The desired safety function is only achieved in combination with further risk reduction measures, whereby the shutdown can be a motor controller, for example.
SIL	Safety Integrity Level, discrete levels for determining the safety integrity requirements of safety functions in accordance with IEC 61508, EN 62061 and EN ISO 13849.
SIL CL	SIL claim limit for a subsystem.

Term/abbreviation	Description
STO	Safe Torque Off in accordance with EN 61800-5-2.
T	Service life in accordance with EN ISO 13849-1.

Tab. 25: Terms and abbreviations

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

Phone:
+49 711 347-0

Internet:
www.festo.com