



This safety manual was translated from the original user manual

### Introduction

This safety manual applies to the drive controllers:

- mcDSA-E25XC revision DF.1, P/N 1512840\*
- mcDSA-E27XC revision DF.1, P/N 1512841\*
- mcDSA-E27XC-STO revision DF.1, P/N 1513167 \*

the safety firmware version (SI\_STO\_Version):

- 1.04.00.00 \*\*

and the respective safety function:

- "Safe torque off (STO)"

The user of the safety function (STO) must observe the latest version of the European Machinery Directive 2006/42/EC.



The manufacturer of the end product or the manufacturer's authorized representative must carry out a hazard analysis in line with the Machinery Directive before placing any machinery on the market.

An analysis of the hazards posed by the machinery must be performed and the necessary actions taken to reduce potential risks. The safety function must be selected according to the actions demanded and the degree of risk minimization required.

**The devices may only be installed and adjusted by fully qualified staff in accordance with the relevant standards.**

Always ensure compliance with the relevant regional standards in the area of component application. Also observe the safety information for the devices and machines being controlled.



A fully qualified person is someone who

- is capable of identifying and avoiding possible hazards due to their experience,
- is familiar with the accident prevention regulations for the employed devices,
- is capable of installing and putting into operation electric circuits and devices according to relevant standards.



**Querying the revision and safety firmware version via the parameters:**

- \*) 3020.01h DeviceSubCode
- \*\*) 3868.23h. SI\_STO\_Version

## Safe torque off (STO) - description of the safety function

### Designation

Safe torque off (STO)

### Description

This function ensures that no torque-generating energy can reach the motor. This safety sub-function corresponds to an uncontrolled stop according to IEC 60204-1, stop category 0.



This safety sub-function can be used when energy shutdown is required to prevent unexpected start-up according to ISO 14118.



In circumstances where external influences (e.g. falling suspended loads) are present, further actions (e.g. mechanical brakes) may be necessary to prevent hazards.



The safety function as an electronic device does not provide adequate protection against electric shock or other electrical risks.



The safety function is only approved for controlling brushless DC motors (BLDC). The drive controllers with this safety function do not have an operating mode for controlling brushed DC motors (DC).



If this function is activated, limited movement (180° maximum electric movement of the axis) is still possible in the event of a failure in the power section of the drive controller.

The safety-related section of the drive controller is designed in such a way that:

- a single fault in the electronics does not lead to the loss of the safety function
- the single fault is detected by the internal diagnostic function during or before the next safety function request and a fault is signalled

### Safety factors

The STO function meets the requirements of DIN EN 61800-5-2:2017.

The STO function supports:

- SIL 3 according to EN 61508:2010 and/or EN 62061:2016
- PL e according to EN ISO 13849-1:2015

SSafety factors according to EN 62061 / EN 61508	Safety factors according to EN ISO 13849
SIL = 3	PL = e
PFH = 5,74*10 <sup>-9</sup> 1/h	MTTFd = 2581 years
SFF <sub>Channel1</sub> = 99,5 % SFF <sub>Channel2</sub> = 99,3 % SFF <sub>PowerSupply</sub> = 99,75 %	Category = Cat. 3 DC <sub>Avg</sub> = 98,9 %

### Operating conditions

Property	Unit	Value	Remarks
Supply voltage		PELV / SELV	Applies to drive controller and safety function
Temperature range	°C	-40 ... 55	gApplies to drive controller and safety function
Relative humidity (non-condensing)	%	5 ... 90	Applies to drive controller and safety function
Operating altitude	m	< 2000	Applies to drive controller and safety function
Electromagnetic compatibility (EMC)		EN 61800-3:2011 - Category C3 device intended for use in the second environment (industrial areas) EN 61800-5-2:2017 - Safety requirements - Functional	

## Properties of the STO inputs

Input description:

Signal name	Description	Specification
STO-A	STO channel A	Low level = STO function request High level = power amplifier release Switching level Low = $-30V < U_{IN} < 5V$ Switching level High = $8V < U_{IN} < 30V$ (60V) Current consumption = 3,5mA @ $U_{IN} = 24V$ $U_{IN Max} = 60V$ Galvanic isolation = no OSSD compatible = ja OSSD filter = 5ms Max. cable length < 30m
STO-B	STO channel B	Low level = STO function request High level = power amplifier release Switching level low = $-30V < U_{IN} < 5V$ Switching level high = $8V < U_{IN} < 30V$ (60V) Current consumption = 3,5mA @ $U_{IN} = 24V$ $U_{IN Max} = 60V$ Galvanic isolation = nein OSSD compatible = ja OSSD filter = 5ms Max. cable length < 30m

- The maximum response time of the STO function is 50ms
- Behaviour of the inputs is indeterminate between  $U_{IN} = 5V$  and 8V
- Output signal switching device (OSSD) semiconductor outputs with test signal

Terminal configuration (mcDSA-E25XC, E27XC):

Signal name	Description	Specification
X4.4	STO-A	STO channel A
X4.6	STO-B	STO channel B

Logic table:

STO-A	STO-B	Controller status	Description
L	L	STO activated, power amplifier blocked	Safety function activated, no diagnostic error
L	H	STO activated, power amplifier blocked	Safety function activated, diagnostic error = -5209/-5229 **
H	L	STO activated, power amplifier blocked	Safety function activated, diagnostic error = -5208/-5228 *
H	H	STO not activated, power amplifier operable	Safety function not activated, no diagnostic error

\*) Errors are indicated by the red error LED, the error code can also be queried via CAN bus and an output can be activated as an error output (see also mcManual „3060.00h Output assignment - error“)

### Automatic restart

Automatic restart determines whether the controller restarts immediately with the movement when the safety function is switched off or whether the user must enable its release. Automatic restart is activated by default.

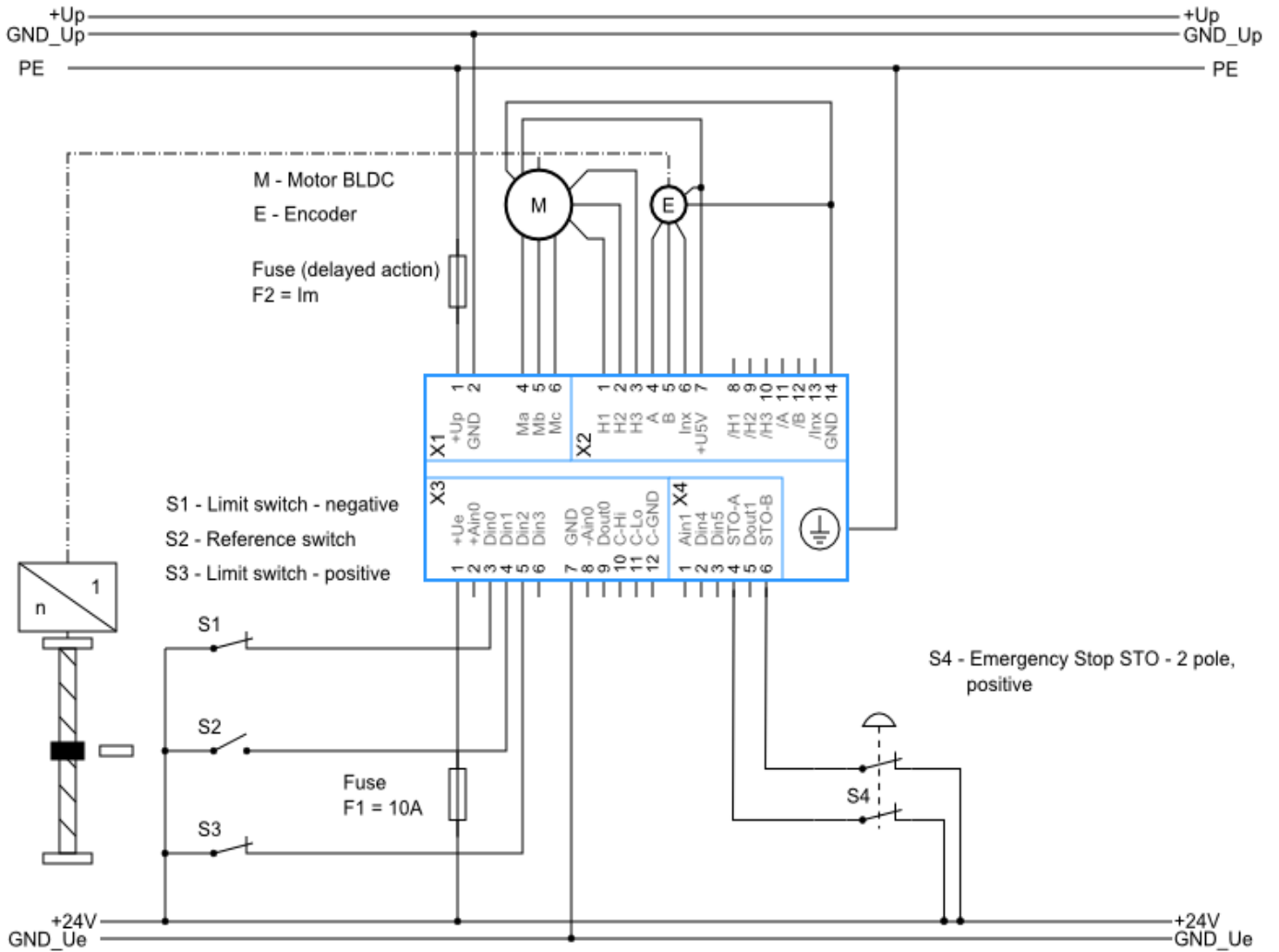
This function is set via bit 4 of the parameter “3868.05h STO configuration”. If bit 4 = 0, automatic restart is activated. If bit 4 = 1, renewed release via CAN bus is required. The movement is released via the parameter “3868.00h STO command” along with the command “0x43495053”.

## Wiring of the STO inputs

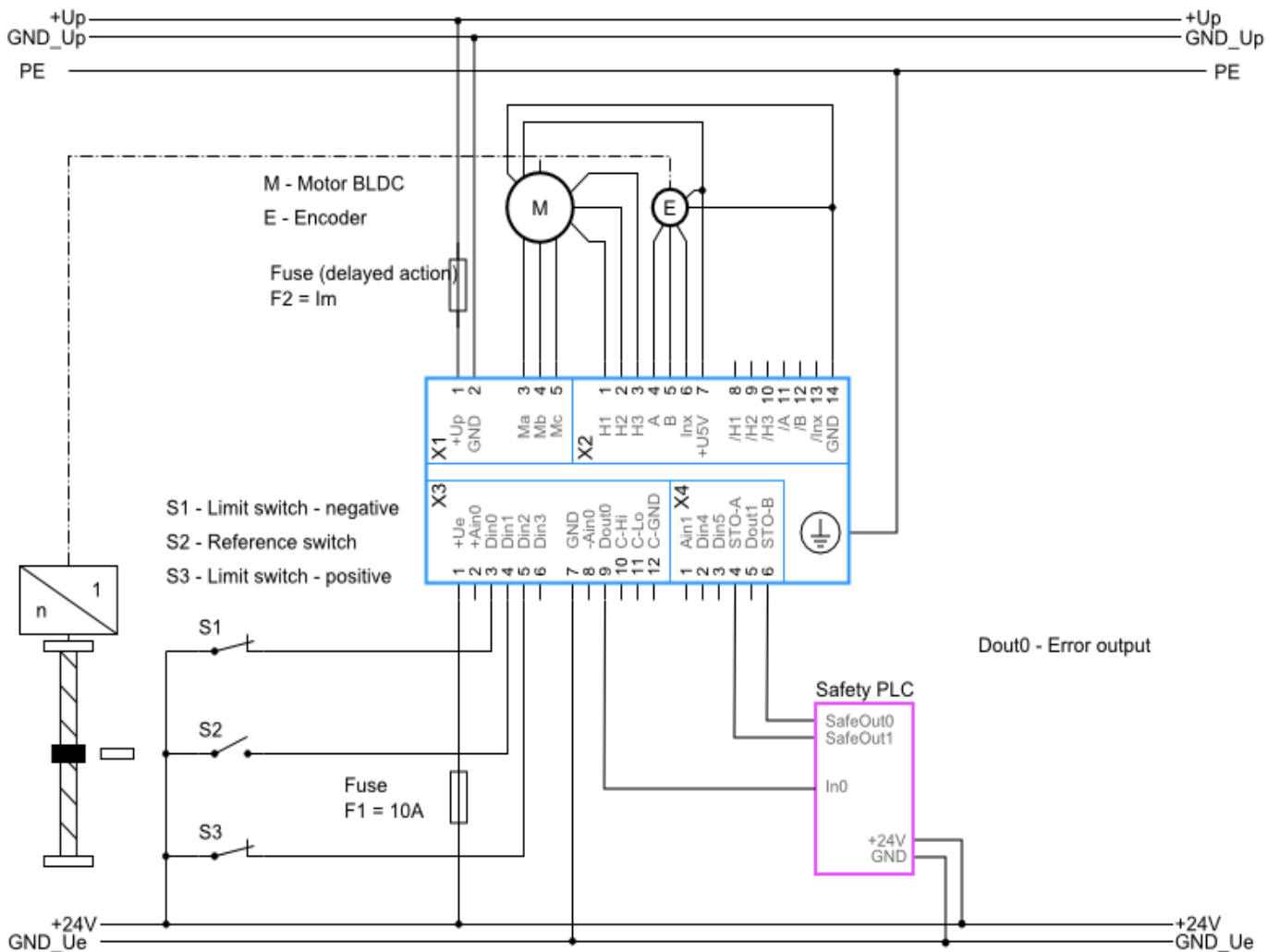
Wiring examples for:

- Simple Emergency Stop circuit
- Safety PLC

Wiring with Emergency Stop button:



Wiring with safety PLC:



## Testing the STO function

Use the following procedure to test the STO function:

- Run the motor
- Activate the STO function
- Check whether the motor stops
  - if yes, eliminate the error and perform the STO test again
- Deactivate STO
- Check whether error messages are output
  - if yes, eliminate the error and perform the STO test again
- Run the motor

If all the test steps are performed without errors, the STO function is correct

## Maintaining the STO function

Correct functioning of the STO function must be checked once every three months.

## Service life

The estimated service life of the STO circuit is 20 years.

## Troubleshooting

The automatic diagnostic function performs a cross comparison between STO-A and STO-B as well as between the input and the output of the circuit each time the STO function is requested. In addition, the diagnostic software is monitored for internal errors. The following error codes can be generated:

Error code	Description/Meaning	Action
-5208	Input STO-B is low and input STO-A is high	Check cabling, perform STO test, replace devices
-5209	Input STO-A is low and input STO-B is high	Check cabling, perform STO test, replace devices
-5228	Output STO-B is low and output STO-A is high	Check cabling, perform STO test, replace devices
-5229	Output STO-A is low and output STO-B is high	Check cabling, perform STO test, replace devices
-5230	Input signals are not stable (oscillation)	Check cabling, perform STO test, replace devices
-30101	Internal error (input and output STO-A not identical)	Replace device
-30102	Internal error (input and output STO-A not identical)	Replace device
-30103	Internal error (input and output STO-B not identical)	Replace device
-30104	Internal error (input and output STO-B not identical)	Replace device
-30105	Internal error (input and output STO-A and STO-B not identical)	Replace device
-30110	Internal error (Diagnosis failed when switching on at STO-B)	Replace device
-30111	Diagnosis failed when switching on at STO-A	Replace device
-30112	Diagnosis failed when switching on at STO-A and STO-B	Replace device
-30114	Internal error in the diagnostic software	Update firmware, replace device
-30115	Internal error in the diagnostic software	Update firmware, replace device
-30116	Internal error in the diagnostic software	Update firmware, replace device

## Declaration of Conformity

<https://www.micontrol.de/de/download>

Version of the safety manual: 08