

3.13 Safe Torque Off (STO)

Applicable to all devices CDE3x.003,W to CDE3x.208,W and CDE34.044,L to CDE34.208,L as well as to all special variants CDB3x.003,SH,W2.4 to CDB3x.208,SH,W2.4 and CDB34.044,SH,L2.4 to CDB34.208,SH,L2.4 (W2.4 = hardware index for wall-mounted, L2.4 = hardware index for liquid-cooled).

3.13.1 Danger analysis and risk assessment

Users of the safety functions (STO) must comply with the EU Machinery Directive 2006/42/EEC, or the latest applicable version as appropriate.

The manufacturer or its representative is obliged to undertake a danger analysis (in accordance with the applicable Machinery Directive) before the market launch of a machine. An analysis of hazards posed by the machine must be conducted and appropriate measures instigated to reduce/eliminate such hazards.

With the danger analysis all prerequisites for establishing the required safety functions are fulfilled.

The CDE/CDB3000 safety function "Safe Torque Off (STO)" has been approved by the accredited certification body "TÜV-Rheinland". Conformance to parts of EN954-1 category 4, EN ISO 1384949-1, EN62061, EN61800-5-1 and EN61508 is ensured.



Qualification: The operators of the safety-related system are trained in accordance with their state of knowledge, appropriate to the complexity and safety integrity level of the safety-related system concerned. This training includes the study of essential features of the production process and knowledge of the relationship between the safety-related system and the equipment under control (EUC).

3.13.2 Definition of terms

STO = Safe Torque OFF

With the safety function STO the power supply to the drive is reliably interrupted (no metallic isolation). The drive must not be able to generate a torque and so perform any hazardous movement. The standstill position is not monitored.

The "STO" function conforms to stop category 0 according to EN60204-1.



Note: see section 3.13.5: Electrical hazard and see section 3.13.6: Hazard posed by axis movement on the motor.

Emergency stop

In accordance with the national and European preface to EN 60204-1, electrical equipment may also be used for emergency stop devices provided they comply with relevant standards, such as EN954-1 and/or IEC 61508. "STO" can thus be used for emergency stop functions.

EN 954-1:1996 / EN ISO 13849-1:2008

Safety of machines, safety related parts of controls. The standard EN ISO 13849 emerged from EN954-1, supplemented by the aspects of quality management and reliability.



Qualification: EN954-1: 1996 is still valid until 31.12.2012, and will then be replaced by EN ISO 13849-1:2008.

IEC 62061:2006

Safety sector standard for machinery, originating from IEC 61508.

IEC 61508:1998-2000

International basic safety standard specifying the status of safety technology in all its aspects.

EN 61800-5-1: 2003

Electrical drives with variable speed. Part 5-1: Requirements concerning electrical, thermal and function safety.

EUC (Equipment Under Control)

EUC system:

A system that responds to the input signals from the process and/or a user and generates output signals which enable the EUC to work as desired.

EUC equipment:

Equipment, machine, apparatus or plant used for manufacture, production and processing, transportation, medical or other activities.

EUC risk:

Risk resulting from the EUC or its interaction with the EUC system.

PFH (Probability of dangerous Failure per Hour)

Probability of Failure per Hour, in respect of a hazardous random hardware failure.

Safety function

Function performed by an E/E/PE (electrical/electronic/programmable electronic) safety-related system, a safety-related system of other technology or external equipment for risk minimization, with the goal of attaining and maintaining a safe state for the EUC, taking into account a particular undesired event.

Validation

Affirmation that the special requirements for a certain purpose of use are fulfilled by investigation and the submission of objective proof.

Validation describes the activity to prove that the safety-related system under investigation meets the specified safety requirements of the safety-related system in every respect, before or after installation.

Positive opening operation of a contact element

Symbol for positive opening operation to EN 60947-5-1 annex K 

In a positive opening operation of a contact element, the contact separation is achieved as a direct result of a certain movement of the actuating element caused by non-elastic links (no springs).

Safety circuit

A safety circuit is designed with two channels and has been approved by accredited testing bodies on the basis of the standards. There is a large number of manufacturers offering a vast variety of safety circuits for various applications.

3.13.3 Description of function

The positioning controllers CDE3000 and CDB3000,SH support the "STO" (Safe Torque Off) safety function in accordance with the requirements of EN 61800-5-2, EN 954-1 "Category 4", EN ISO 13849-1 "PL e" and EN 61508 / EN 62061 "SIL 3" (PFH rating to be provided subsequently).

The "STO" safety function to EN61800-5-2 describes a safety measure in the form of an interlock and control function. "Category 4" signifies that the safety function will remain in place in the event of a single fault.

The safety-related parts must be designed in such a way that:

- a single fault in any of the said parts does not result in loss of the safety function and
- the single fault is detected on or before the next request to the safety function. If this is not possible, a series of faults does not then lead to loss of the safety function.

For the "STO" function the positioning controllers are equipped with additional logic circuits and a feedback contact. The logic cuts the power supply to the pulse amplifiers to activate the power stage. In combination with the controller release "ENPO" the system uses two channels to prevent the motor creating a torque.

This variant offers the following advantages over the solution with a motor contactor:

- No need for the external motor contactor
- So less wiring
- Space-saving
- Better EMC performance due to the all-over shielding of the motor cable
- Shorter reaction time

3.13.4 Fundamentals

Always draw up a validation plan. The plan specifies which tests and analyses were used by you to determine compliance of the solution with the requirements of the application.

3.13.5 Electrical hazard



- When the drive controller is in the "STO" state all motor and mains cables, braking resistors and DC link voltage cables are carrying dangerous voltages against protective conductors.
- With the "STO" function no "voltage shut-off in case of emergency" is possible without additional measures. There is no electrical isolation between the motor and the drive controller! This means there is a risk of electric shock or other electrical hazard.

3.13.6 Hazard posed by axis movement on the motor



- If an external effect of forces can be expected in safety function "STO", e.g. with suspended load, this motion must be reliably prevented by additional measures, e.g. by a mechanical brakes, safety bolts or clamping device with brake.
- Short-circuits in two remote branches of the power section may activate a short-time axis movement depending on the number of poles of the motor.

Example – synchronous motor:

With a 6-pole synchronous motor the movement may be max. 30°. For a directly driven ball screw, e.g. 20 mm per revolution, this corresponds to a one-time maximum linear movement of 1.67 mm.

Example – asynchronous motor:

The short-circuits in two offset branches of the power section have almost no effect, since the exciter field collapses when the inverter is blocked and has fully decayed after about 1 second.



Note: The safety circuitry connected to the drive controller should be designed in such a way that in case of a loss of electrical supply the safe state of the machine can be reached or maintained.

3.13.7 Overview of "STO" connections for CDB,SH

	X2
OSD02 normally open	20
OSD02 +24 V Relay	19
OSD02 normally closed	18
DGND	17
OSD01	16
OSD00	15
DGND	14
+24 V	13
ISD03	12
ISD02	11
ISD01	10
ISD00	9
ENPO	8
+24 V	7
+24 V	6
OSA0	5
AGND	4
ISA01	3
ISA00	2
+10,5 V	1

The drive controller CDB3000,SH offers a separate input for the "STO" request, a facility to deactivate the restart inhibit and a separate relay contact for feedback.

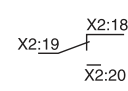
Des.	Term.	Specification	Floating	
Digital inputs				
ISD00 (STO)	X2-9	<ul style="list-style-type: none"> Request input STO = low level OSSD-capable* Switching level Low/High: < 5 V / > 18 V DC $I_{max} = 10 \text{ mA}$ (at 24 V) $U_{in \text{ max}} = 24 \text{ V} + 20\%$ $R_{in \text{ nom.}} = 3 \text{ k}\Omega$ Internal signal delay time $\approx 2 \text{ ms}$ Terminal scan cycle = 1 ms 	Yes	
ENPO (STO)	X2-8	<ul style="list-style-type: none"> Request input STO = low level OSSD-capable* Power stage enable = High level Switching level Low/High: < 5 V / > 18 V DC $I_{max} = 10 \text{ mA}$ (at 24 V) $U_{in \text{ max}} = 24 \text{ V} + 20\%$ $R_{in \text{ nom.}} = 3 \text{ k}\Omega$ Internal signal delay time $\approx 10 \text{ ms}$ Terminal scanning cycle = 1 ms 	Yes	
Relay output: Feedback (NO contact) "STO"				
OSD02 (RSH)	X2-18 X2-19 X2-20	<ul style="list-style-type: none"> Diagnose STO, both tripping channels active, one NO contact with automatically resetting circuit-breaker (polyswitch) 25 V / 200 mA AC, usage category AC1 30 V / 200 mA DC, usage category DC1 Operating delay approx. 10 ms 3×10^6 switching cycles 		Yes
Voltage supply				
<p>Note: In the range > 5 V / < 18 V the response of the inputs is undefined. *OSSD: (Output Signal Switching Device) Tested semiconductor outputs. Test pulses are suppressed up to a length of 300 μs.</p>				

Table 3.21 X2 terminal assignment – CDB3000,SH

3.13.8 Overview of "STO" connections for CDE

The drive controller CDE3000 offers a separate input for the "STO" request, a facility to deactivate the restart inhibit and a separate relay contact for feedback.

X2

REL	←	24	12	→	RSH
REL	→	23	11	←	RSH
ISDSH	→	22	10	←	ENPO
ISD06	→	21	9	→	OSD02
ISD05	→	20	8	→	OSD01
ISD04	→	19	7	→	OSD00
ISD03	→	18	6	←	ISA1-
ISD02	→	17	5	←	ISA1+
ISD01	→	16	4	←	ISA0-
ISD00	→	15	3	←	ISA0+
+24V	↔	14	2	↔	+24V
DGND	↔	13	1	↔	DGND

Des.	Term.	Specification	Floating	
Digital inputs				
ENPO (STO)	X2-10	<ul style="list-style-type: none"> Request input STO = low level OSSD-capable* Switching level Low/High: < 5 V / > 18 V DC $I_{max} = 5 \text{ mA}$ (at 24 V) typically 3 mA $U_{In max} = 24 \text{ V} \pm 20\%$ $R_{In nom.} = 3 \text{ k}\Omega$ Internal signal delay time approx. 10 ms 	Yes	
ISDSH (STO)	X2-22	<ul style="list-style-type: none"> Request input STO = low level OSSD-capable* Terminal scanning cycle = 1 ms Switching level Low/High: < 5 V / > 18 V DC $I_{max} = 5 \text{ mA}$ (at 24 V) typically 3 mA $U_{In max} = 24 \text{ V} \pm 20\%$ $R_{In nom.} = 3 \text{ k}\Omega$ Internal signal delay time approx. 1 ms 	Yes	
Relay outputs				
RSH	X2-11 X2-12	<ul style="list-style-type: none"> Diagnose STO, both tripping channels active, one NO contact with automatically resetting circuit-breaker (polyswitch) 25 V / 200 mA AC, $\cos \varphi = 1$ 30 V / 200 mA DC, $\cos \varphi = 1$ 	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> X2:12 X2:11 </div>	Yes
REL	X2-23 X2-24	<ul style="list-style-type: none"> Relay, 1 NO contact 25 V / 1 A AC, usage category AC1 30 V / 1 A DC, usage category DC1 Operating delay approx. 10 ms Cycle time 1 ms 	Yes	
Note: In the range > 5 V / < 18 V the response of the inputs is undefined. *OSSD: (Output Signal Switching Device) Tested semiconductor outputs. Test pulses are suppressed up to a length of 300 μs .				

Table 3.22 X2 terminal assignment – CDE3000

3.13.9 Wiring and commissioning

For the "STO" function the positioning controllers are equipped with additional logic circuits and a feedback contact. The logic cuts the power supply to the pulse amplifiers to activate the power stage. In combination with the controller release "ENPO" the system uses two channels to prevent the motor creating a torque.

The internal device functionality and connections are illustrated in Figure 3.27 for CDB3000,SH and in Figure 3.28 for CDE3000.

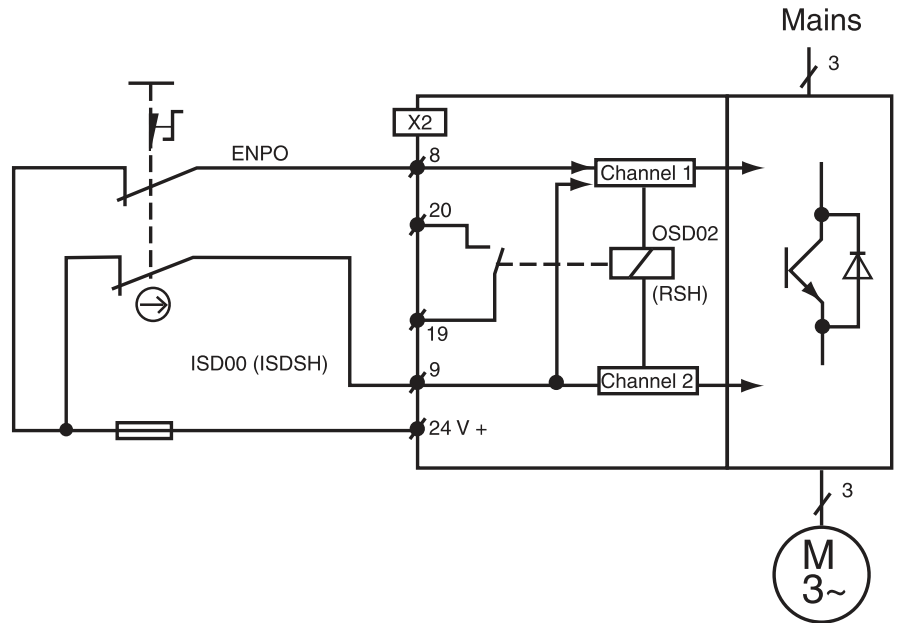


Figure 3.27 "STO" request on CDB3000,SH for shutdown in case of emergency (emergency stop)

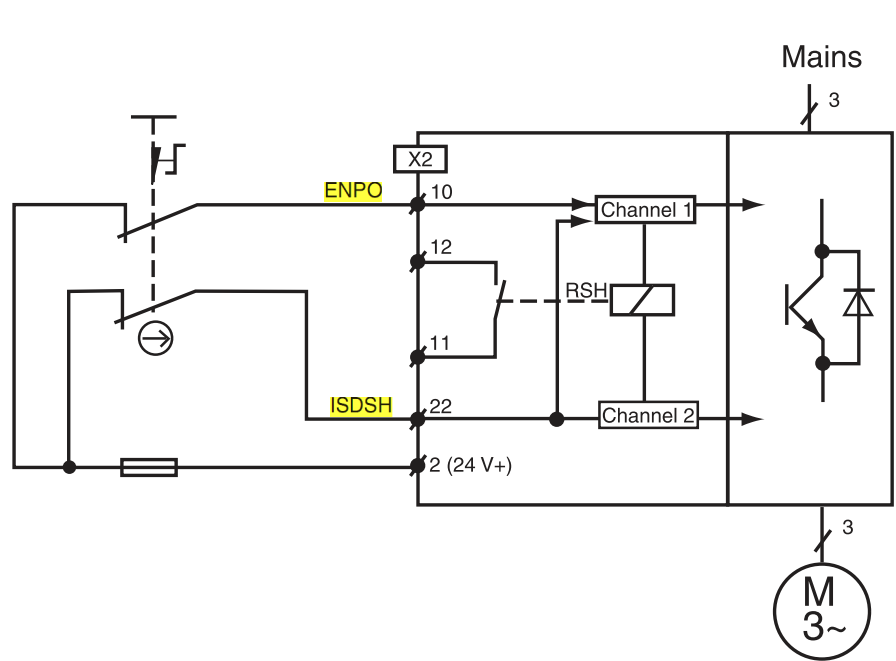


Figure 3.28 "STO" request on CDE3000 for shutdown in case of emergency (emergency stop)

ENPO	ISD00 (CDB,SH) ISDSH (CDE)	STO	Restart inhibit	Controller state	Relay ¹⁾ OSD02 / (CDB,SH) RSH (CDE)
L	L	ON	ON	Power stage disabled over two channels.	high
H ³⁾	H ³⁾	OFF	OFF	Power stage ready	low
(L) → H ²⁾	(L) → H ²⁾	OFF	OFF	Power stage ready	low
H	(H) → L	ON	ON	Power stage disabled over two channels.	high
(H) → L	H	OFF	OFF	Power stage disabled over one channel.	low
(L) → H	H	OFF	OFF	Power stage ready.	low

() Previous state

1) 3 x 10⁶ switching cycles at 200 mA (resting: NO contact)

2) In order to deactivate the restart inhibit the control signals must be simultaneously (ENPO max. 5 ms before ISDSH/ISD00) set to High (H), or ISDSH/ISD00 must be safely set to High (H) before ENPO.

3) This only applies when STO has been disabled by the process described in "2)".

Table 3.23 Logic table for use of "STO"

3.13.10 Testing the STO function



The applied control signals "ISDSH" and "ENPO" must always be checked by the operator or a superimposed control for plausibility to the feedback (RSH).

If an implausible state occurs, this indicates an error in the system (installation or positioning controller). In this case the drive must be switched off and the fault rectified.

Attention: The "STO" (Safe Torque Off) function must be checked for correct functioning:

- on initial commissioning;
- after any modification of the system wiring;
- after any replacement of one or more items of system equipment.

Note: There is no protection against unexpected restarting after re-establishing the electrical power supply in the illustrated example circuit, unless an external circuit is used. **If ENPO and ISDSH are High when the power is restored (see truth table), the axis may start up if autostart is programmed, particularly if an external 24V feed is connected to supply the control electronics in the event of power failure.** The connected safety circuit on the machine must ensure that the drive controller (the SRP/CS) can attain and maintain the safe state of the machine.

Note: If the switch and drive controller are installed in separate locations, it must be ensured that the cables from NC contact 1 to ENPO (STO) and from NC contact 2 to ISDSH (STO) are wired separately, or that possible faults are prevented by using a protective tube for example.

In order to cancel the STO safety function and deactivate the restart inhibit, the ISDSH signal must be set to High before the ENPO signal, or simultaneously with it.

**3.13.11 Safety
characteristics****Safety characteristics are:**

PFH: To be determined and submitted by TÜV

MTTF: To be determined and submitted by TÜV

Min. service life: xx years

Max. service life: 20 years