

## 6. Safe Torque Off (STO)

### 6.1 Danger analysis and risk assessment

Users of the safety functions (STO/SS1) must strictly comply with the machine directive 98 / 37 / EEC, or the currently valid edition respectively.

The manufacturer or his representative is obliged to perform a danger analysis (acc. to machine directive 98 / 37 / EEC), before the market launch of the machine. He must perform an analysis of dangers arising from the machine and introduce appropriate measures to reduce/eliminate such dangers. With the danger analysis all prerequisites for establishing the required safety functions are fulfilled.

The ServoOne safety function "Safe Torque Off (STO)" has been approved by the accredited certification body "TÜV-Rheinland". Parts of the standard EN951-1 category 51, EN ISO 13849-1, EN 62061, EN 61800-5-1 and EN 615108 were accounted for.

The acceptance applies for servo controller types acc. to the tables in chapters A1.1 and A1.2. as well as for sizes BG1-BG4 from serial number 0729 0001. For size BG5+6 from serial no.: on request



**Qualification:** The operator of the safety related system is trained in accordance with his state of knowledge, as is appropriate for the complexity and safety integrity level of the safety related system. This training includes the study of essential features of the production process and knowledge of the relation between the safety related system and the equipment under control (EUC).

### 6.2 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 should not be able to generate a torque and thus no endangering motion. The rest position is not monitored.

The "STO" function corresponds with stop category 0 acc. to EN 60204-1.

SS1: Safe Stop 1 (stopping acc. to stop category 1)

In case of controlled stopping with reliably monitored delay time the drive is braked by the drive controller. Once the delay time, which is monitored by an external safety circuit, has expired, the power supply for the drive is interrupted (no metallic isolation). The safety function STO is active.

The "SS1" function corresponds with stop category 1 acc. to EN60204-1.

Stop category according to EN 60204-1

Stop category	System behaviour/ requirement
0	<b>Uncontrolled stopping:</b> By direct interruption of power supply to the machine drive elements.
1	<b>Controlled stopping:</b> Power supply to machine drive elements is maintained to achieve stopping. The power supply will only be interrupted when standstill is reached.
2	<b>Controlled stopping:</b> By which the power supply to the machine drive elements is maintained also at standstill.

Table 6.1 Stop category

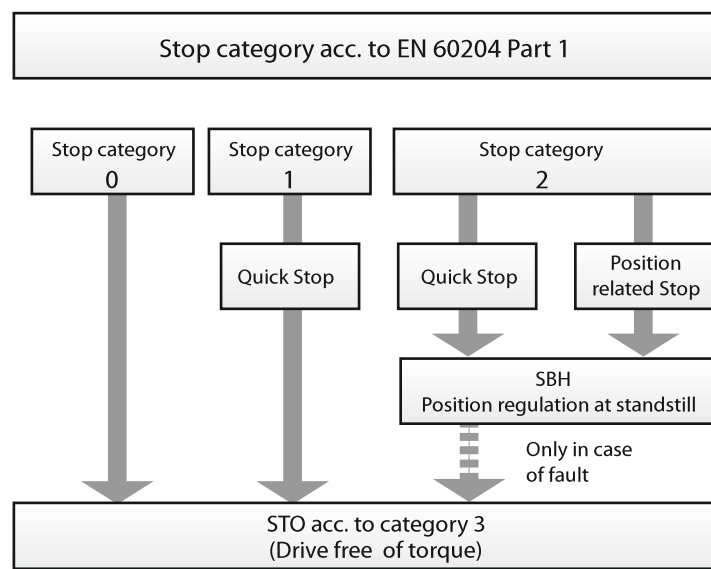


fig. 6.1 Structure of stop categories

## Emergency stop

In compliance with the national and European foreword to EN 60204-1 electrical operating means may also be used for emergency stop facilities, if these e. g. fulfil the standards EN 954-1 and/or IEC 61508. The "STO" function can therefore be used for emergency stop functions.



**Note:** The term "Emergency Stop Facility" was replaced by the new term "Action in Case of Emergency". The term "Emergency Stop" was replaced by "Stopping in Case of Emergency (Emergency Stop)", see paragraph 9.2.5.4.2 in EN60204-1.

EN 954-1 : 1996 / EN ISO 13849-1 : 1999

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.



**Note:** EN954-1 : 1996 is still valid until the end of october 2009, or will then be replaced by EN ISO 13849-1 : 1999.

IEC 62061 : 2006

Standard on safety sectors for the field of machines, emerged from IEC 61508

IEC 61508 : 1998 - 2000

International basic safety standard describing 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 - Operating equipment:**

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 the manufacture, production and processing, transportation, medical or other activities.

**EUC - risk:**

Risk resulting from the EUC or its interaction with the EUC operating equipment.

## Safety function


Function performed by an E / E / PE safety related system, a safety related system of other technology or external facilities for risk minimization, with the goal of reaching and maintaining a safe state for the EUC, under due consideration of a particularly undesired result.

## Validation

Confirmation that the special requirements for a certain purpose of use are fulfilled by examination and the issuing of objective evidence.

Validation describes the activity to proof that the examined safety related system meets the specified safety requirements of the safety related system in every respect, before or after the installation.

## Positive opening operation of a contact element

Symbol for positive opening operation acc. to EN 60947-5-1 appendix K 

In case of 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 spring).

## 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.

## Interlocked separating protective devices

An interlocked separating protective device (EN 1088, paragraph 3.2) is a separating protective device working in connection with an interlocking mechanism. The interlocked separating protective device with tumbler is described in EN 1088, paragraph 3.3.

## Tumbler lock

A tumbler lock (EN 1088, paragraph 3.4) is a device with the function of holding a separating protective device closed, until the risk of injuring has been eliminated.

## 6.2.1 Description of function

The servo controller SO8000 supports the safety function "STO" (Safe Torque Off), acc. to the requirements of EN 954-1 "Category 3", EN ISO 13849-1 "PL d" and EN 61508 / EN 62061 "SIL2".

The safety function "STO" acc. to EN954-1 describes a safety measure in form of an interlocking and control function. Category 3 means that this safety function will remain in place in case a single fault occurs.

The safety relevant parts must be designed in a way that:

- an isolated fault in any of these parts does not result in the loss of the safety function, and
- the isolated fault will be detected, whenever reasonably possible.

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

In comparison with the solution with a motor contactor this variant offers the following advantages:

- Abandonment of the external motor contactor
- Resulting in less wiring work
- Space saving
- Better EMC-compatibility due to the continuous shielding of the motor lead.
- Shorter reaction time

## 6.2.2 Notes on safety

Always formulate 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.



### Danger:

- If the servo controller is in "STO" state all motor and mains lines, brake resistors and d.c.-circuit voltage lines conduct dangerous voltages against PE-conductors.
- With the function "STO" no "shut-down of voltage in case of emergency" is possible without additional measures. There is no metallic isolation between motor and servo controller! There is therefore a risk of electric shock or other risks of electric origin.



### Danger:

- 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.
- By two short circuits each in two offset branches of the power circuit a short-term movement of the axis can be triggered, dependent on the number of poles of the motor.  
Example synchronous motor: With a 6-pole synchronous motor the movement may be max. 30°. With a direct driven ball screw, e.g. 20 mm per revolution, this corresponds with a single linear movement of 1.67 mm.

Example asynchronous motor: Since the exciting field collapses when reverse biasing the inverter and has fully decayed after approx. 1 second, the short circuits in two offset branches of the power section have almost no effect.



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

## 6.2.3 Overview of "STO" connections

ServoOne 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	P.-isolation
<b>Digital inputs</b>			
ENPO (STO)	X4/10	<ul style="list-style-type: none"> <li>• Request input STO = low level</li> <li>• Deactivation of the restart inhibit and release of power stage = high-level</li> <li>• Frequency range &lt; 500 Hz</li> <li>• Reaction time approx. 10 ms</li> <li>• Switching level low/high: &lt;4.8 V / &gt;18 V</li> <li>• for 24 V typ. 3 mA</li> </ul>	Yes
<b>STO "Safe Torque Off"</b>			
ISDSH (STO)	X4/22	<ul style="list-style-type: none"> <li>• Request input STO = low level</li> <li>• Frequency range &lt; 500 Hz</li> <li>• Switching level low/high: &lt;4.8 V / &gt;18 V</li> <li>• for 24 V typically 3 mA</li> </ul>	Yes
RSH RSH	X4/11 X4/12	Diagnose STO, both tripping channels active, one normally open contact with automatically resetting circuit breaker (polyswitch) <div> <div>X4/12</div> <div>X4/11</div> </div> <ul style="list-style-type: none"> <li>• 25 V / 200 mA AC, <math>\cos \varphi = 1</math></li> <li>• 30 V / 200 mA DC, <math>\cos \varphi = 1</math></li> </ul>	Yes
<b>Auxiliary supply</b>			
+ 24 V	X4/2 X4/14	<ul style="list-style-type: none"> <li>• Auxiliary supply to feed the digital control inputs</li> <li>• <math>U_v = 24</math> V DC, no delay in case of short circuit (+24 V → GND), however, short-term shut-down of device possible.</li> <li>• <math>I_{max} = 50</math> mA (per pin) with automatically resetting circuit breaker (polyswitch)</li> </ul>	-
<b>Digital ground</b>			
DGND	X4/1 X4/13	Reference ground for 24 V, with automatically resetting circuit breaker (polyswitch)	-

**X4**

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

Table 6.2 Terminal assignment X4

Digital ground and auxiliary voltage are outputs. The feed for the 24 V auxiliary voltage is accomplished through terminal X9 and X10.

## 6.2.4 Wiring and commissioning

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

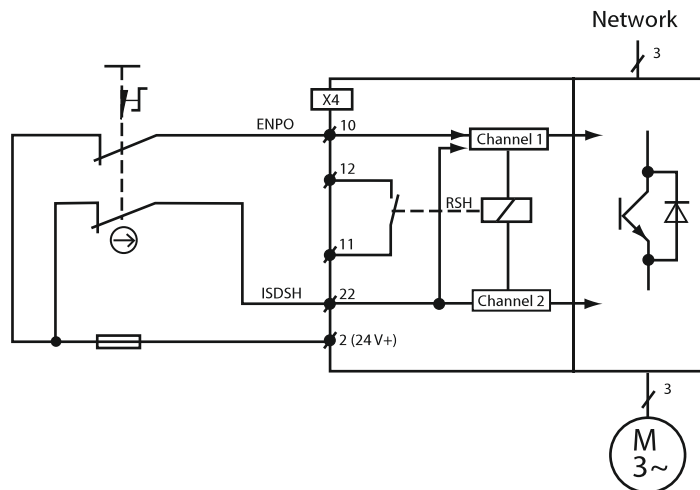


fig. 6.2 "STO" selection of function via switch with two normally closed contacts (positively driven)



**Note:** There is no protection against unexpected restarting after re-establishing the electric power supply in the illustrated exemplary circuitry, unless an external circuitry is used. If ENPO and ISDSH are High when reconnecting the electric power supply (see truth table), the axle may start when Autostart has been programmed. The safety feature on the machine must assure that the ServoOne (the SRP / CS) can reach and maintain the safe state of the machine.



**Note:** In case of a spatially isolated installation of switch and drive controller one must make sure that the leads from closed contact 1 to ENPO (STO) and from normally closed contact 2 to ISDSH (STO) are wired separately, or that possible faults are ruled out by using e.g. a protective tube.

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

ENPO	ISDSH	STO	Restart inhibit	Controller state	RSH <sup>1)</sup>
L	L	ON	ON	Output stage locked via two channels	High
H <sup>3)</sup>	H <sup>3)</sup>	OFF	OFF	Power stage at standby.	Low
(L) ⇒ H <sup>2)</sup>	(L) ⇒ H <sup>2)</sup>	OFF	OFF	Power stage at standby.	Low
H	(H) ⇒ L	ON	ON	Output stage locked via two channels	High
(H) ⇒ L	H	OFF	ON	Output stage locked via one channel	Low
(L) ⇒ H	H	OFF	OFF	Power stage at standby.	Low

( ) previous status  
1)  $3 \times 10^5$  switching cycle at 200mA (rest position: normally open)  
2) In order to deactivate the restart inhibit the control signals must be simultaneously (ENPO max. 5 ms before ISDSH) set to High (H), or ISDSH must be reliably set to High (H) before ENPO.  
3) This only applies when STO has been disabled by the process described in "2)".

Table 6.3 Switching behaviour of the safety function



**Note:** The plausibility between input signals (ENPO, ISDSH) and feedback (RSH) must always be monitored.

### 6.2.5 Checking 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).

The occurrence of an implausible status is a sign for a system fault (installation or servo controller). In this case the drive must be switched off and the fault rectified.



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

- Initial commissioning
- After any intervention in to the wiring of the system
- After replacing one or several appliances in the system.

## 6.3 Stopping acc. to stop category 1 (SS1)

The following example of a circuit represents one of many possibilities which can be realized with ServoOne and an external protective circuit. For the realization of "interlocked separated Protective features" with/without tumbler there are many manufacturers, who offer a vast variety of protective circuits for various applications.

The following example of a circuit is intended to demonstrate, how servo controllers are wired with a typical protective circuit. Here it is the intention to realize controlled stopping acc. to stop category 1 (SS1).

### 6.3.1 Notes on safety

Always formulate a validation plan. The plan specifies which tests and analyses were used by you to determine compliance of the solution (e.g. suggested circuitry) with the requirements of the application.

You should in any case check whether

- all safety related output signals are correctly and logically generated by the input signals
- the behaviour in case of a fault corresponds with the specified circuit categories.
- control and operating means are sufficiently dimensioned for all types of operation and environmental conditions.

After completion of analyses and tests create a validation report. This report should at least contain:

- all objects to be tested
- the reliable personnel for testing
- testing facilities (including details on calibration) and simulation instruments
- performed tests
- problems found and solutions for these problems
- results

Keep the documented results in an understandable form.



**Danger:** Strictly comply with the safety notes in chapters 6.2.2 and 6.2.4.

## 6.3.2 Information on system design

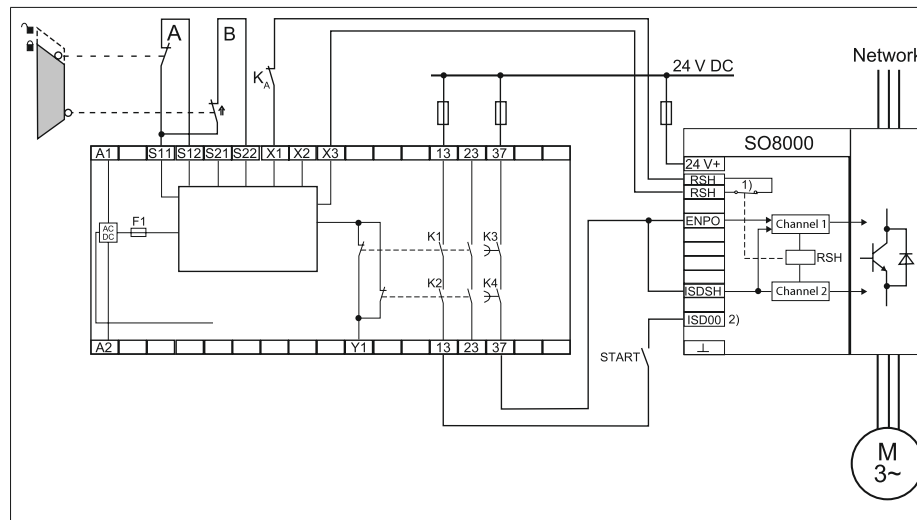
Inform the user about the correct use, the capacity and the limits of safety related parts.

Instruct the user about how he should maintain the capacity of safety related parts, especially if fault exclusions specified by you require special maintenance work.



**Note:** For the determination of safety categories (STO, SS1) we have considered the following fault exclusion.

- Fault exclusion: Bridging within the interconnection in the control cabinet.
- Reason: Protected installation in control cabinet, proven technology



1) In rest position the contact (RSH) is a normally open contact. In relation to the signals in the switching diagram the contact is closed!

2) The exemplary circuitry the input ISD00 is set to "START(1)" (see page 39).

fig. 6.3 Exemplary circuitry "Stopping acc. to stop category 1 (SS1)"

Configuration	EN954-1	EN61508	EN13849-1	EN60204-1
Sensor	Category 3	SIL2	PL d	-
Logic	Category 3	SIL2	PL d	-
Actor*	Category 3 (STO)	SIL2	PL d	Stop category 0
Entire system	Category 3	SIL2	PL d	Stop category 1
With this system solution one achieves a solution SS1 "Safe Stop, Stop Category 1 (with monitored time)". * SO8000				

Table 6.4 Comparison of safety standards