atos
the smart electrohydraulics

USER MANUAL

S-MAN-STO

SMART SERVOPUMP SYSTEM
SAFETY TORQUE OFF INSTRUCTIONS

INDEX

1 GENERAL

This manual describes the Safe Torque Off (STO) functionality combined to Atos Smart ServopPump (SSP) system.

This manual must be used in conjunction with any other instruction, document, checklist furnished with the machinery, also related to single equipment or parts of the machine.
Atos disclaims any liability for damage and / or injury to persons, animals or property resulting from the requirements contained in this document.

The manufacturer has the right to update products and manuals for future products without any obligation to update this manual.

THE USER IS ADVISED THAT THE AMENDMENT OF THE CHARACTERISTICS, TAMPERING OF THE SAFETY DEVICES, FAILURE TO FULFILL THE REQUIREMENTS LISTED IN THE INSTRUCTIONS AND MAINTENANCE PLANNED, THE EXECUTION OF WORK OR UNAUTHORIZED MODIFICATIONS AND ANY IMPROPER USE OF THE MACHINE, WILL RESULT IN VOID OF THE WARRANTY; THE USER WILL IN ALL THESE CASES BE LIABLE FOR ANY DAMAGE CAUSED TO PERSONS OR ANIMALS OR THINGS.

1.1 Documentation

Additional information about electronic drives, motor, pump and Atos software can be found into the Atos web site or in the My Atos - Download Area.

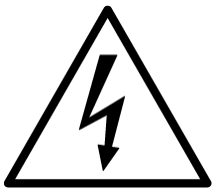
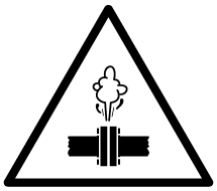
Related documentations

- S-MAN-S-SW SSP programming software – user manual
- S-MAN-HW SSP system installation - user manual
- AS050 Basics for Smart Servopumps - SSP - technical table
- AS100 Smart Servopumps - SSP- technical table
- AS200 Sizing criteria for Servopumps - technical table
- AS300 PGI - Cast iron internal gear pumps for SSP servopumps- technical table
- AS350 PGIL - Aluminium internal gear pumps for SSP servopumps - technical table
- AS400 PMM – Electric motors for SSP servopumps - technical table
- AS500 D-MP – Digital electronic drives for SSP servopumps - technical table
- AS800 Programming tools for pumps & servopumps – technical table
- AS810 Accessories for SSP servopumps - technical table
- AS910 Operating and maintenance information for SSP servopumps - technical table
- GS510 Fieldbus features
- S-MAN-S-BC Drive programming instruction CANopen protocol
- S-MAN-S-BP Drive programming instruction PROFIBUS DP protocol
- S-MAN-S-EH Drive programming instruction EtherCAT protocol
- S-MAN-S-EP Drive programming instruction PROFINET protocol

1.2 Safety pictograms

Residual risks are risks that remain in the system also after the implementation of all the security measures taken by the manufacturer.

The residual risks due to any shortcomings of the protection measures taken, if any, are described on the machine with proper signage and pictograms.

Risk of electrocution in the vicinity of electrical equipment. Do not open when energized or before adequately isolated the source of electricity	
Risk of limb injury: do not open the protective removable during processing and not ever operate the machine when a user is in the vicinity of the station. Only one operator at a time can work on the station	
High temperature risk: do not touch cold parts of the machinery for prolonged period	
Low temperature risk: do not touch cold parts of the machinery for prolonged period	
High pressure risk: do not open when in functions or when pressurized	

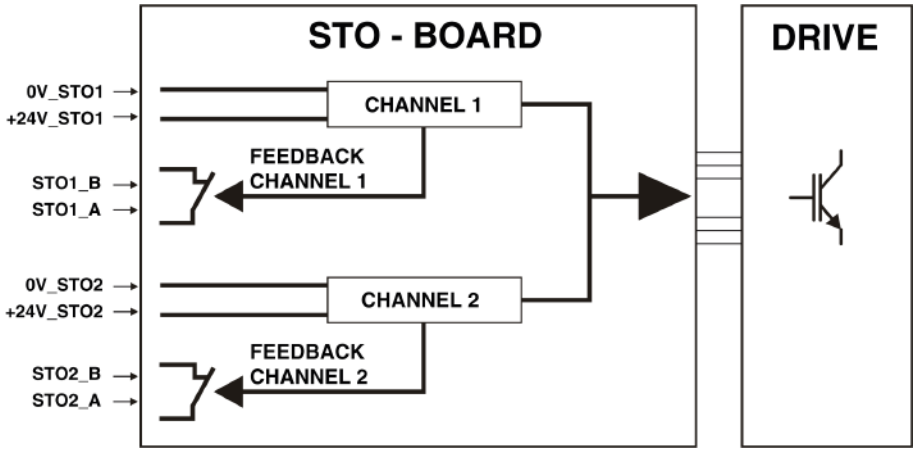
1.3 Personal Protective Equipment

In the use of the machine everyone is obliged to use the following PPE:

Safety boots	
Chemical resistant gloves	
Safety goggle	

2 STO FUNCTION

The Atos drive implements the Safe Torque Off (STO) function as a prevention of unexpected starts according to the EN 61800-5-2 standard. The function prevents the generation of a rotating magnetic field by removing the control voltage of the power semiconductors. Thanks to this function, short-term operations such as cleaning and / or maintenance on non-electrical parts of the machine can be performed without disconnecting either the power supply of the drive or the connection between the converter and the motor. The STO function is implemented using two redundant channels each having its own feedback signal accessible from the outside. The principle scheme is as follows:



Channel 1 has **+24V_STO1** as input and **STO1** signal as feedback.

Channel 2 has **+24V_STO2** as input and **STO2** as feedback.

The feedbacks refer each to an N.C. contact which can be read by an external logic that manages the STO function at the machine level.

3 LIMIT OF USE

The environmental limits of use of the D-MP drive are indicated in part in the installation manual and refer to the normal operation of the converter.

The following are better specified limits of use of the converter so that the correct functioning of the converter is guaranteed even when the STO function is active.

3.1.1 Climatic Class

3K3 climatic class according to EN 60721-3-3

Environmental parameter	**Limits**	**Measure unit**
Working temperature **(1)**	0 ÷ 40	°C
Humidity	5 ÷ 85	%
Atmospheric pressure	70 ÷ 106 **(2)**	kPa
Maximum movement of the surrounding air	1	m/s
Maximum temperature gradient	0.5	°C/min
Maximum thermal radiation	700	W/ m^2
Condensation	-	-
Precipitation with wind	- **(3)**	-
Water of origin other than rain	-	-
Ice formation	-	-

(1) The 3K3 climatic class has an operating limit of 5 ÷ 40 °C, but the drive is able to work with ambient temperatures down to 0 °C. The maximum operating temperature of the drive reaches 45 °C. In this case, downgrade the rated current to 88%.

(2) The atmospheric pressure limits correspond to an operating range of 0 ÷ 3000m above sea level. In reality, over 1000m above sea level, the rated current of the drive will have to be downgraded by 1% each 100m.

(3) The drive must be installed inside an electrical panel and therefore not outside.

3.1.2 Resistance to chemically active substances

3C1R climatic class according to EN 60721-3-3

Environmental parameter	**Max value**	**Measure unit**
Sea salts	-	-
Sulfur dioxide	0.01 0.0037	mg/m^3 cm^3/m^3
Hydrogen sulphide	0.0015 0.001	mg/m^3 cm^3/m^3
Chlorine	0.001 0.00034	mg/m^3 cm^3/m^3
Hydrochloric acid	0.001 0.00066	mg/m^3 cm^3/m^3
Hydrofluoric acid	0.001 0.0012	mg/m^3 cm^3/m^3
Ammonia	0.03 0.042	mg/m^3 cm^3/m^3
Ozone	0.004 0.002	mg/m^3 cm^3/m^3
Nitric oxide	0.01 0.005	mg/m^3 cm^3/m^3

3.2 Vibration resistance

Following the D-MP drive vibration limits:

10Hz ≤ frequency ≤ 57Hz	0.075	mm (amplitude)
57Hz ≤ frequency ≤ 150Hz	1	g

In the case of vibrations exceeding the indicated limits, it is necessary to adopt the appropriate damping solutions.

3.3 IP protection degree and pollution

Ingress protection	IP20
Degrees of pollution	2 **(1)**

(1) Non-conductive pollution and, occasionally and temporarily, conductive pollution generated by condensation.

4 STORAGE

4.1 Environmental storage conditions

Temperature	-10 ÷ 60	°C
Humidity	5 ÷ 95	%
Condensation	-	-

ATTENTION: every 6 months / 1 year it is necessary to regenerate the power bus capacitors: power up operation through terminals L1, L2, L3 for 2 hours without giving the run consent.

4.2 Recovery procedure after storage

The drive cannot be used immediately after a storage period.

To avoid breakdowns it is necessary adopt the following recovery procedure.

Step 1:

Drive not powered		
Temperature	15 ÷ 35	°C
Humidity	5 ÷ 75	%
Condensation	-	-
Atmospheric pressure	86 ÷ 106	kPa
Recovery time **(1)**	1	h

(1) After this recovery time no trace of condensation inside or outside the drive must be present (well-ventilated environment).

Step 2:

ATTENTION: if the time of the last regeneration of the power bus electrolytic capacitors is between 6 months and 1 year, it is mandatory to perform the regeneration of the bus capacitors again of power. Power the drive through terminals L1, L2, L3 for 2 hours without giving the run consent.

ATTENTION: if the time from the purchase or from the last regeneration of the electrolytic capacitors of the bus power is greater than 1 year, their regeneration cannot be performed by powering simply the drive, but it is necessary to request the operating procedure to be adopted from Atos.

Once the recovery procedure has been completed after storage and, if necessary, the regeneration process has been carried out of the power bus electrolytic capacitors, the drive can work normally.

5 POWER SUPPLY CONTROL LOGIC AND STO CHANNELS

5.1.1 X3 connector - 24VDC input power supply

Drive type: 022 ÷ 060

Connector	PIN	SIGNAL	Description
X3  drives type **022 ÷ 060**	1	**V+_IN**	V+_IN = +24V input power supply (22V ÷ 26V) V0_IN = 0V input power supply Current: min 800mA (type 022) min1A (types 033 – 046 – 060) Through the pins 1 and 2 of the X3 connector is possible to power up: - drive logic (mandatory for drives type 022 ÷ 060 no self powered) - motor sensor (mandatory for drives type 022 ÷ 060 no self powered)
	2	**V0_IN**	

Drive type: 090 ÷ 210

Connector	PIN	SIGNAL	Description
X3  drives type **090 ÷ 210**	1	**V+_IN**	V+_IN = +24V input power supply (±10%) V0_IN = 0V input power supply Current: min 500mA (for type 090 ÷ 140) min1A (types 165 ÷ 210) Through the pins 1 and 2 of the X3 connector is possible to power up: - drive logic - motor sensor The drives type 090 ÷ 210 generates internally an 24 VDC auxiliary supply through the main power supply; the drive logic can be supplied through X3 connector with an external 24 VDC without produce conflict between the internally generated voltage and the auxiliary power supplied externally (it is used the source with higher voltage level). This feature allows to configure the drive without main power supply and keep the drive logic switched on even in the absence of the drive main power supply.
	2	**V0_IN**	

5.1.2 X6 connector - 24VDC output power supply - only for drives type 090 ÷ 210

Drive type: 090 ÷ 210

Connector	PIN	SIGNAL	Description
X6  drives type **090 ÷ 210**	1	**V+_OUT**	V+_IN = +24V output power supply (±10%) V0_IN = 0V output power supply Current: min 500 mA Through the pins 1 and 2 of the X6 connector is possible to power up: - drive digital I/O - two channels of the STO function (the power supply must be interrupted by safety contacts)
	2	**V0_OUT**	

5.1.3 S1 connector - Safe Torque Off (STO) - only for /K option

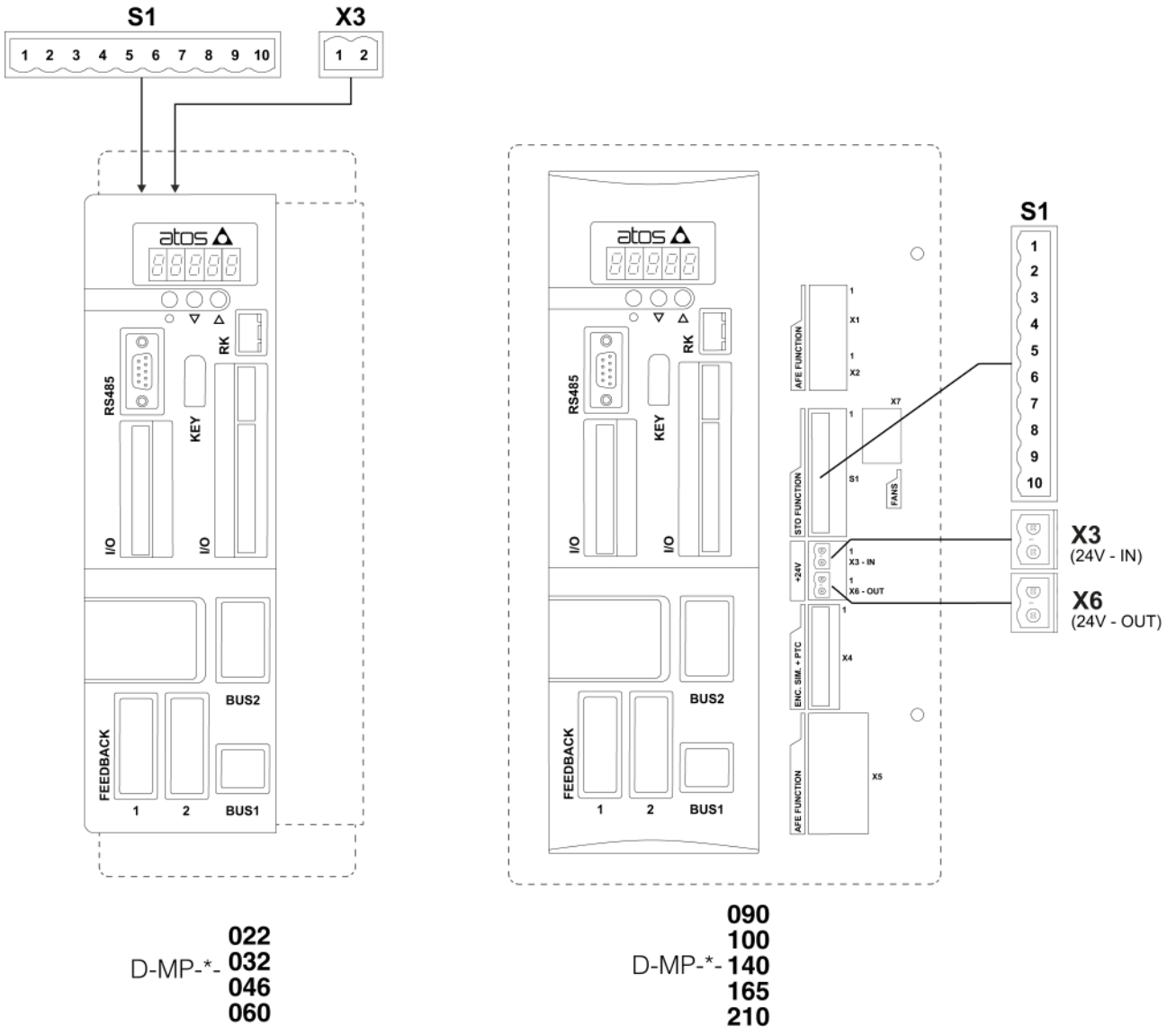
Drive type: 022 ÷ 060

Connector	PIN	SIGNAL	Description
S1  drives type **022 ÷ 060**	1	**STO2_A**	Monitor for STO2 – second safety system channel When the terminal board is powered, the contact is open Voltage: max 60 VDC – Current: max 0,5 mA
	2	**STO2_B**	
	3	**NC**	
	4	**+24V_STO2**	+24V_STO2 = +24V power supply (22V ÷ 26V) 0V_STO2 = 0V power supply Current: min 40 mA This channel supply the relay which interrupts the IGBT driver commands. To normal drive operating the + 24V_STO2 voltage must be supplied. To enable the STO function it is necessary to remove the + 24V_STO2 voltage.
	5	**0V_STO2**	
	6	**NC**	
	7	**STO1_A**	Monitor for STO1 – first safety system channel When the terminal board is powered, the contact is open Voltage: max 60 VDC – Current: max 0,5 mA
	8	**STO1_B**	
	9	**+24V_STO1**	+24V_STO1 = +24V power supply (22V ÷ 26V) 0V_STO1 = 0V power supply Current: min 40 mA This channel supply the relay which interrupts the IGBT driver commands. To normal drive operating the + 24V_STO1 voltage must be supplied. To enable the STO function it is necessary to remove the + 24V_STO1 voltage.
	10	**0V_STO1**	

Drive type: 090 ÷ 210

Connector	PIN	SIGNAL	Description
S1  drives type **090 ÷ 210**	1	**STO2_A**	Monitor for STO2 – second safety system channel When the terminal board is powered, the contact is open Voltage: max 60 VDC – Current: max 0,5 mA
	2	**STO2_B**	
	3	**NC**	
	4	**+24V_STO2**	+24V_STO2 = +24V power supply (±10%) 0V_STO2 = 0V power supply Current: min 10 mA Input for STO2 – second safety system channel This channel cuts the command of the high power IGBT. To normal drive operating the + 24V_STO2 voltage must be supplied. To enable the STO function it is necessary to remove the + 24V_STO2 voltage.
	5	**0V_STO2**	
	6	**NC**	
	7	**STO1_A**	Monitor for STO1 – first safety system channel When the terminal board is powered, the contact is open Voltage: max 60 VDC – Current: max 0,5 mA
	8	**STO1_B**	
	9	**+24V_STO1**	+24V_STO1 = +24V power supply (22V ÷ 26V) 0V_STO1 = 0V power supply Current: min 40 mA Input for STO1 – first safety system channel This channel cuts the command of the high power IGBT. To normal drive operating the + 24V_STO1 voltage must be supplied. To enable the STO function it is necessary to remove the + 24V_STO1 voltage.
	10	**0V_STO1**	

5.1.4 X3 – X6 – S1 terminal boards



D-MP-*- **022 032 046 060**

D-MP-*- **090 100 140 165 210**

6 EXTERNAL CONNECTIONS

The connection instructions for the Atos drive will be provided below only for the parts concerning the power supply of the regulation board and the STO safety function.

For the remaining connections refer to the installation manual (S-MAN-HW).

The regulation board can be powered through X3 terminal board (V+_IN). Only for drives 090 ÷ 210 an auxiliary voltage (V+_OUT) is available on X6 terminal board.

Each of the + 24V_STO1 (referred to 0V_STO1) and + 24V_STO2 (referred to 0V_STO2) signals is referred to a channel of the STO safety function. Pay attention to the wiring of these signals from the OPEN DRIVE to the module safety used in the electrical panel.

a) If using the output voltage V + _OUT present on X6 to power the safety channels, use a cable with two-way shielded whose braid must be connected to the V0_OUT signal. The choice to use a shielded cable is to avoid that, due to any faults on the power cables, the safety function is lost. This because:

- terminal X6 is located near terminal S1

- the power cables of X6 and those of S1 will reach the converter inside the same conduit

b) To connect X3 use a two-way shielded cable whose braid must be connected to the V0_IN signal. A shielded power cable is not normally required regulation. The choice to use a shielded cable is to avoid that due to any faults on the power cables, the safety function is lost. This because:

- terminal X3 is located near terminal S1

- the power cables of X3 and those of S1 will reach the converter inside the same conduit

c) To connect the first channel (+ 24V_STO1 and 0V_STO1) use a two-way cable whose shield must be connected to the 0V_STO1 (S1-10) signal. The use of a cable shielded with the braid connected to 0V_STO1 is used to avoid losing the function of safety in case of failure of the wiring external to the converter. An example, could be the loss of insulation and subsequent accidental contact between a cable connected to the 24V of the panel electric and + 24V_STO1.

d) To connect the second channel (+ 24V_STO2 and 0V_STO2) use a two-way cable whose shield must be connected to the 0V_STO2 (S1-5) signal. The use of a cable shielded with the braid connected to 0V_STO2 is used to avoid losing the function of safety in case of failure of the wiring external to the converter. An example, could be the loss of insulation and subsequent accidental contact between a cable connected to the 24V of the panel and the + 24V_STO2 signal.

e) To connect the two monitors, the type of cable to use depends on how the diagnostic test of the safety chain performed. Some security modules do not specify the type of cable adapted for connecting the signals used for the diagnostic function. This because within them, they are able to discriminate if there is a failure. In the event that, the diagnostic test of the safety channels is carried out directly by the manufacturer of the electrical panel, it is necessary to understand if this test can detect a fault on the cables. In the diagnostic test, a failure on the monitor signal cables causes the monitor to fail diagnostic test. It is not possible to distinguish where the fault is: on the chain of security or on the monitor. By providing a two-way shielded cable for each of the monitors, at least the failure on the monitor signal connections can be excluded.

7 STO FUNCTION ACTIVATION

7.1 Drive 022 ÷ 140

In the normal working conditions of the drive (STO function deactivated), it is necessary to supply in addition to the + 24V (V+_IN of X3), the + 24V_STO1 and the + 24V_STO2.

In this situation the contacts of monitors (STO1 and STO2) must both be open.

To activate the STO safety function, the following procedure must be followed:

a) stop the motor

b) remove the run enabling command **(1)**

c) remove the + 24V_STO1 **(2)**

d) remove + 24V_STO2 **(2)**

(1) in presence of external influences (e.g. falling suspended loads), it may be necessary to use additional measures to prevent

any risk (for example mechanical brakes)

(2) respect the points sequence **c)** and **d)**

ATTENTION: activating the STO function while the drive is running can cause total loss of control of the motor. Activate the STO function only with the drive already stopped following the procedure indicated above.

ATTENTION: the STO safety function implemented in the drive allows the prevention against unexpected starts only for horizontal axes in which the axis is not stressed by external forces. In the case of vertical axes or in cases where external forces or loads can generate movement, additional means of immobilization (e.g. mechanical brakes) conforming to the required SIL or PL level are required.

DANGER: terminals +, -, U, V, W, F remain active.

Maintenance work on the equipment or access to electrical parts are not permitted.

ATTENTION: from the moment when supply voltage is interrupted, both safety channels require a time to enter the safe state condition. Times are shown below.

Channel 1	Maximum time from interruption of +24V_STO1	1 s
Channel 2	Maximum time from interruption of +24V_STO2	20 ms

DANGER: in brushless permanent magnet motors, the simultaneous failure of two power switches, can cause motor movement up to 180° electrical equal to [180/n° pole pairs of the motor] mechanical degrees.

In this situation the feedback contacts (STO1 and STO2) must both be closed.

A discrepancy of only one of the monitor contacts with respect to the drive status corresponds to a fault. In this case the safety function may not work properly and an immediate repair is necessary.

In addition to the feedback contacts available externally, there is a logic output ("STO Active") managed via S-SW-SETUP software and Fieldbus (see S-MAN-SW software manual) to signal the status of STO.

Note:

- for drives up to size 060, the output (“STO Active”) only monitors channel 1.

- for drives 090 to 140, the output (“STO Active”) monitors both channels of the safety function.

If the STO function is activated, the drive goes into the “Switch On Disable” state.

7.2 Drive 165 ÷ 210

In the normal working conditions of the converter (STO function deactivated), it is necessary to supply the + 24V_STO1 and + 24V_STO2 signals. In this situation, the contacts of the monitor must both be open.

To activate the STO safety function, the following procedure must be followed:

a) stop the engine

b) remove the run enabling command **(1)**

c) simultaneously remove the + 24V of the two safety channels (+ 24V_STO1 and + 24V_STO2) **(2)**

(1) with presence of external influences (for example falling suspended loads), it may be necessary to use additional measures to prevent any risk (e.g. mechanical brakes).

(2) the diagnostics performed by the control logic admits a maximum delay time between the activation of one channel and the other of 70ms (a higher delay generates an alarm described in chapter 9).

ATTENTION: activating the STO function while the drive is running causes total loss of control of the motor. Activate the STO function only with the drive already stopped following the procedure indicated above.

ATTENTION: The STO safety function implemented in the drive allows prevention against unexpected starts only for horizontal axes in which the axis is not stressed by external forces. In the case of vertical axes or in cases where external forces or loads can generate movement, additional means of immobilization (e.g. mechanical brakes) conforming to the required SIL or PL level are required.

DANGER: terminals +, -, U, V, W, F remain active.

Maintenance work on the equipment or access to electrical parts are not permitted.

ATTENTION: from the moment of power failure, both safety channels require a time to enter the safe state condition. Times are shown below.

Channel 1	Maximum activation time of the first STO channel	5 ms
Channel 2	Maximum activation time of the second STO channel	5 ms

DANGER: in brushless permanent magnet motors, the simultaneous failure of two power switches, can cause motor movement up to 180° electrical equal to [180/n° pole pairs of the motor] mechanical degrees.

The STO safety function diagnostics is performed by:

a) hardware monitor for each of the two safety channels (STO1 and STO2)

b) control logic

The diagnostic performed both through the hardware monitors of the two safety channels (STO1 and STO2) and through the control logic, has a delay with respect to the falling edge of the signals input (+ 24V_STO1 and + 24V_STO2). The delay times are shown below.

Channel 1	Maximum hardware monitor delay time of the first STO channel	10 ms
Channel 2	Maximum hardware monitor delay time of the second STO channel	10 ms
Channels 1 and 2	Maximum diagnostic delay time performed by the control logic	80 ms

After the delay times described above, the feedback contacts (STO1 and STO2) must both be closed.

Any discrepancy of only one of the monitor contacts with respect to the converter status indicates the presence of a failure. In this case, the STO safety function may not work properly and it is necessary to proceed to one immediate repair.

If there are no dangerous faults (alarms code A13.3, A13.4, A13.5, A13.6 are considered dangerous – see 9.2.3), the drive activates the "STO Active" logic output, while the "STO Corrupted" output remains disabled. In this case the drive goes to the “Switch On Disable” state.

8 STO FUNCTION DEACTIVATION

8.1 Drive 022 ÷ 140

To exit the STO safety state it is sufficient to supply the voltages again.

ATTENTION: from the moment the voltage is switched on, both safety channels require a time to exit the safe state condition. The times are shown below.

Channel 1	Maximum time from activation of +24V_STO1	100 ms
Channel 2	Maximum time from activation of +24V_STO2	20 ms – drive 022 ÷ 060 1.1 s – drive 090 ÷ 140 **(*)**

(*) For drives 090 - 140, to calculate the exit maximum time from the safety function, the recharge time of the power stage must be considered.

In the standard configuration the pre-charge time is 500ms.

In this situation, the feedback contacts (STO1 and STO2) must both be open.

A possible discrepancy of only one of the monitor contacts with respect to the drive status corresponds to a fault. In this case the safety function may not work properly and is immediate repair is necessary.

To return to normal operating conditions, proceed as indicated below:

- wait at least 100ms from the insertion of the + 24V_STO1 and + 24V_STO2 (for drives 022 ÷ 060)
- wait at least 1,1s from the insertion of the + 24V_STO1 and + 24V_STO2 (for drives 090 ÷ 210)
- the “STO_Active” output is disabled
- the "Drive ready - Ok" logic output is active
- the drive is ready to work

ATTENTION: If the run command is given before the maximum exit time from the STO function, the drive shows alarm A12 (see S-MAN-SW software manual).

8.2 Drive 165 ÷ 210

To exit the STO safety state it is sufficient to supply the voltages again +24V_STO1 and +24V_STO2.

Note: the diagnostics performed by the control logic admits a maximum delay time between the activation of one channel and the other of 70ms (a higher delay generates an alarm described in chapter 9.2.3).

ATTENTION: from the moment the voltage +24V_STO1 and +24V_STO2 are switched on, both safety channels require a time to exit the safe state condition. The times are shown below.

Channel 1	Maximum time from activation of +24V_STO1	5 ms
Channel 2	Maximum time from activation of +24V_STO2	5 ms

The STO safety function diagnostics is performed by:

a) hardware monitor for each of the two safety channels (STO1 and STO2)

b) control logic

The diagnostics performed both through the hardware monitors of the two safety channels (STO1 and STO2) and through the control logic, has a delay with respect to the falling edge of the signals input (+ 24V_STO1 and + 24V_STO2). The delay times are shown below.

Channel 1	Maximum hardware monitor delay time of the first STO channel	10 ms
Channel 2	Maximum hardware monitor delay time of the second STO channel	10 ms
Channels 1 and 2	Maximum diagnostic delay time performed by the control logic	80 ms

After the delay times described above, the feedback contacts (STO1 and STO2) must both be open.

Any discrepancy of only one of the monitor contacts with respect to the converter status indicates the presence of a failure. In this case the STO safety function may not work properly and it is necessary to proceed to one immediate repair.

If there are no dangerous faults (alarms code A13.3, A13.4, A13.5, A13.6 are considered dangerous – see 9.2.3), the "STO Corrupted" logic output of the drive remains always disabled.

To return to normal operating conditions, proceed as indicated below:

- wait at least 80ms from the insertion of the + 24V_STO1 and +24V_STO2

- the “STO_Active” output is disabled

- the "Drive ready - Ok" logic output is active

- the drive is ready to work

ATTENTION: before giving the start command it is necessary to wait for the delay time of the control diagnostics. In case the run command is given too soon, the drive ignore the run command until diagnostics recognize that the safety function is disabled.

9 DIAGNOSTIC SYSTEM

9.1 Drive 022 ÷ 140

When the STO safety function is activated, the feedback signals indicate if the safety function has been correctly performed (it is therefore necessary to monitor these feedback signals).

For this purpose, a distinction is made between:

- Basic diagnostics (mandatory)
- Smart diagnostics (optional)

9.1.1 Basic diagnostic

The basic diagnostic is mandatory and must be always performed as it represents a basic check of the correct operating of the STO function. To satisfy the basic diagnostics it is necessary that:

a) the feedback signals and the "STO Corrupted" digital output are monitored at each start of the machine on which the drive will be mounted. The machine must be started only if the STO1 and STO2 feedback contacts are both closed (both "active" feedback signals) and if the "STO Corrupted" output is disabled;

b) the reset command that brings the machine out of the "emergency stop" condition is enabled only if, during the emergency stop state, the feedback contacts are both closed and the "STO Corrupted" digital output is disabled.

See a connection example that meet these requirements at paragraph 10.

Note: for drives up to 140A, the "STO Corrupted" output only signals a dangerous fault in the power part through alarm A3.0.

9.1.2 Smart diagnostic

Smart diagnostics is optional and can be used when the STO function is managed by a PLC or other smart system.

It consists to perform periodically:

a) Diagnostic test: two test sequences, one for each of the two channels, which make it possible to detect any faults in the STO safety function before it is activated;

b) "STO Corrupted" logic output status check

Diagnostic test

By observing the congruence between the feedback signals and the presence or absence of the control voltage at the input of the two channels of the STO function, it is possible to perform control sequences that allow to detect some faults on the safety channels.

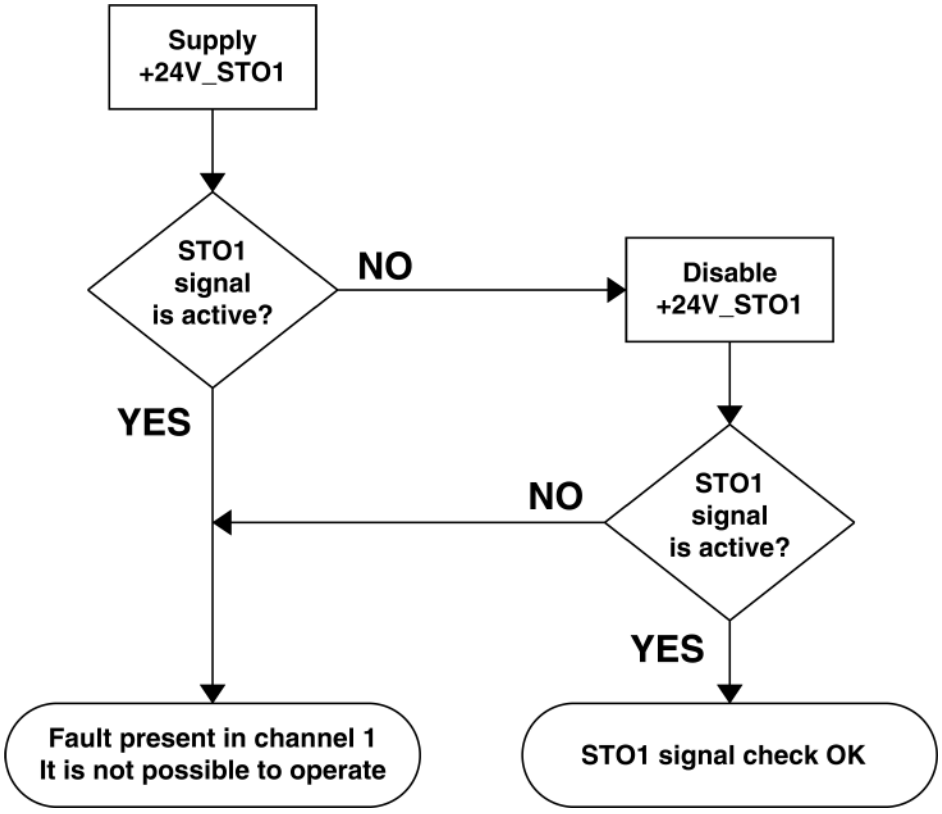
ATTENTION: The control sequences of the two safety channels must be performed one at a time and NOT simultaneously.

The maximum entry and exit times from the safety condition are shown in the table below. These data refer to the maximum time that elapses between the change of state of the safety channel input and the switching of the relative monitor.

Channel 1	Maximum time from interruption of +24V_STO1 to the commutation of STO1	1 s
	Maximum time from activation of +24V_STO1 to the commutation of STO1	100 ms

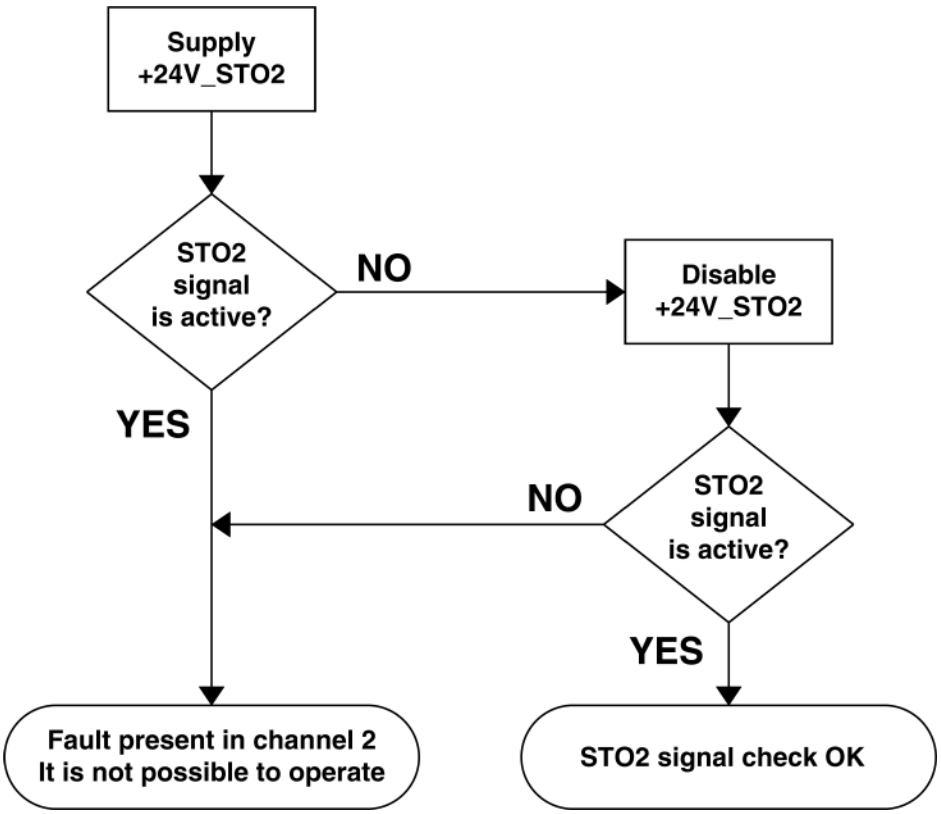
Channel 2	Maximum time from interruption of +24V_STO2 to the commutation of STO2	1 s
	Maximum time from activation of +24V_STO2 to the commutation of STO2	20 ms – drive 022 ÷ 060 1.1 s – drive 090 ÷ 140

Safety channel 1 sequence:



ATTENTION: for drives 090 ÷ 140, the diagnostic function of channel 1 must be performed with the second safety channel NOT active (+ 24V on the + 24V_STO2 input). For Atos sizes 22 ÷ 60A, the status of the second safety channel is not relevant.

Safety channel 2 sequence:



If the diagnostic test detects a fault, the drive must be subjected to immediate repair, otherwise the safety function may malfunction in the next intervent request.

We recommend to perform these tests periodically with the machine in stop status.

In any case, it is mandatory that the basic diagnostics requirements are observed (see 9.1.1).

ATTENTION: the status of the first safety channel is not relevant for the diagnostic test of the second safety channel.

"STO Corrupted" logic output status check

The "STO Corrupted" logic output check allows to verify the presence of some dangerous faults. To perform the check, it is necessary to verify that the logic output is disabled (logic state low), keeping safety channels 1 and 2 powered (see 7 for connection examples).

9.2 Drive 165 ÷ 210

When the safety function is activated, both the two hardware monitors (STO1 and STO2) and the control board signal if the safety function has been correctly performed or if there are dangerous faults. The activation of the safety function allows to perform a diagnostic test on the integrity of the two safety channels that must be performed periodically.

NOTE: the diagnostics performed by the control logic is sufficient to identify the correct functionality of the two safety channels. It is not necessary to perform the diagnostic test using the two hardware monitors. The following paragraphs show the sequences to be followed to perform the test procedures using two types of diagnostics. The diagnostic test must be performed every time the machine is started.

ATTENTION: the maximum diagnostic time interval of the STO safety function (Diagnostic Test Interval) must be 2160h (3 working months). If the safety function is never activated for 2160h the drive display with code A13.6 (diagnostic test necessary).

ATTENTION: if the diagnostic test detects a fault, the drive must be subjected to immediate repair, to avoid possible incorrect operation of the safety function in the subsequent request for intervention.

WARNING: after 720 hours (1 working month) from the last activation of the safety function, the drive activates the logic output (also present at the S-SW-SETUP software and Fieldbus level) "STO test suggested". The logic output is intended to alert the end user that the diagnosti test must be performed, in order to comply with the requirements of the Machinery Directive 2006/42 / EC.

9.2.1 Diagnostic test – without feedback channels

The starting conditions to perform the diagnostic test are the following:

a) Control logic powered

b) Safety channels not active (+ 24_STO1 and + 24_STO2 powered)

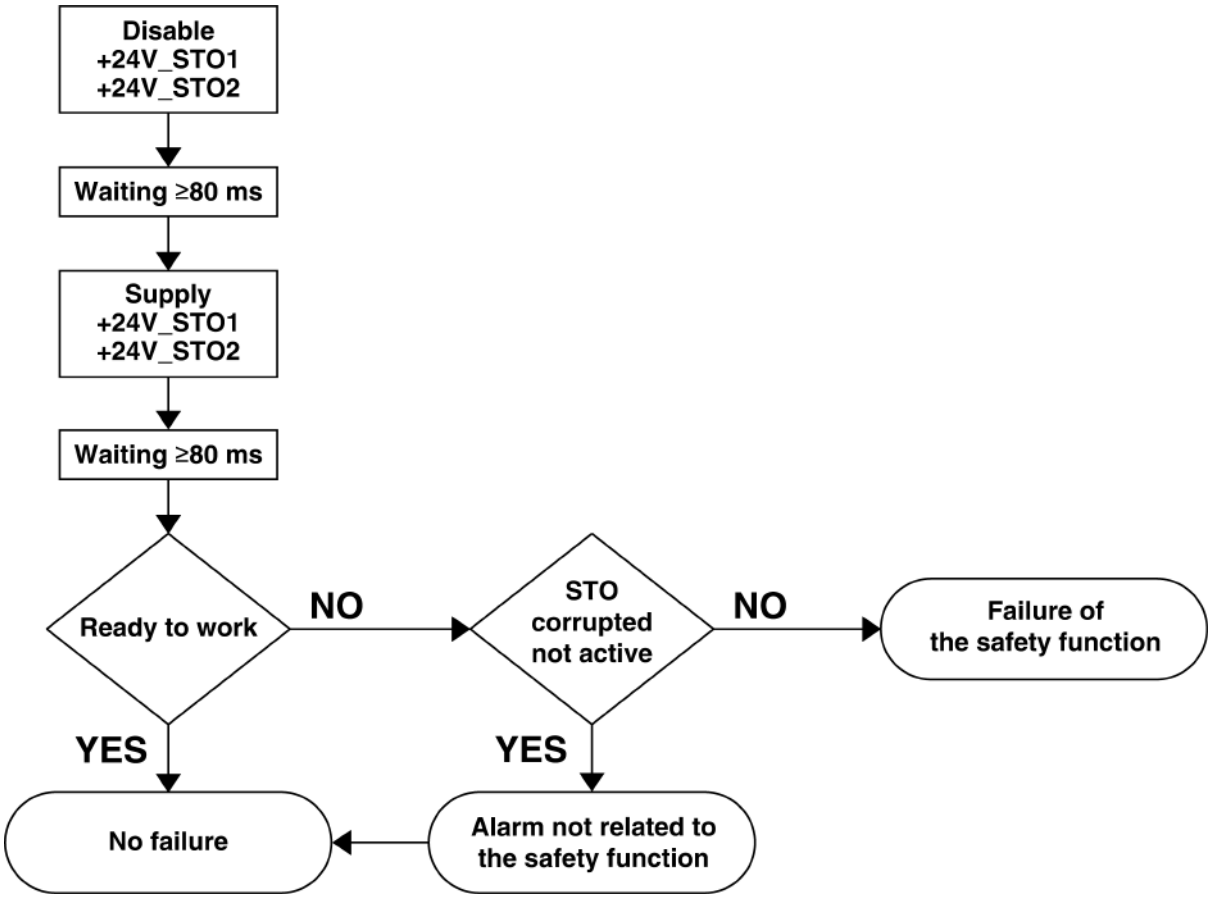
c) No alarms present

The sequence to be adopted is shown in the picture below. The diagnostic test, if the drive resumes working normally after the described sequence, does not require any verification by the user. Only if the drive remains in alarm it is necessary to check the alarm code to verify to verify if it is related to the STO safety function.

To quickly verify if the drive does not work due to a failure of the safety function, it is possible to use the "STO Corrupted" logic output. This configurable logic output indicates the presence of a fault in the channels of the safety function and it is the summary of the alarms code A13.3, A13.4, A13.5 and A13.6 (see 9.2.3).

The logic output is disabled when are not failures on the STO channels.

Sequence to be adopted:



9.2.2 Diagnostic test – with feedback channels

The diagnostic test performed using only the STO1 and STO2 monitor contacts is not able to detect all failures of the STO safety function.

It is therefore necessary to use the "STO Corrupted" logic output. This configurable logic output indicates the presence of a dangerous fault in the channels of the STO safety function and it is the summary of the alarms code A13.3, A13.4, A13.5 and A13.6 (see 9.2.3).

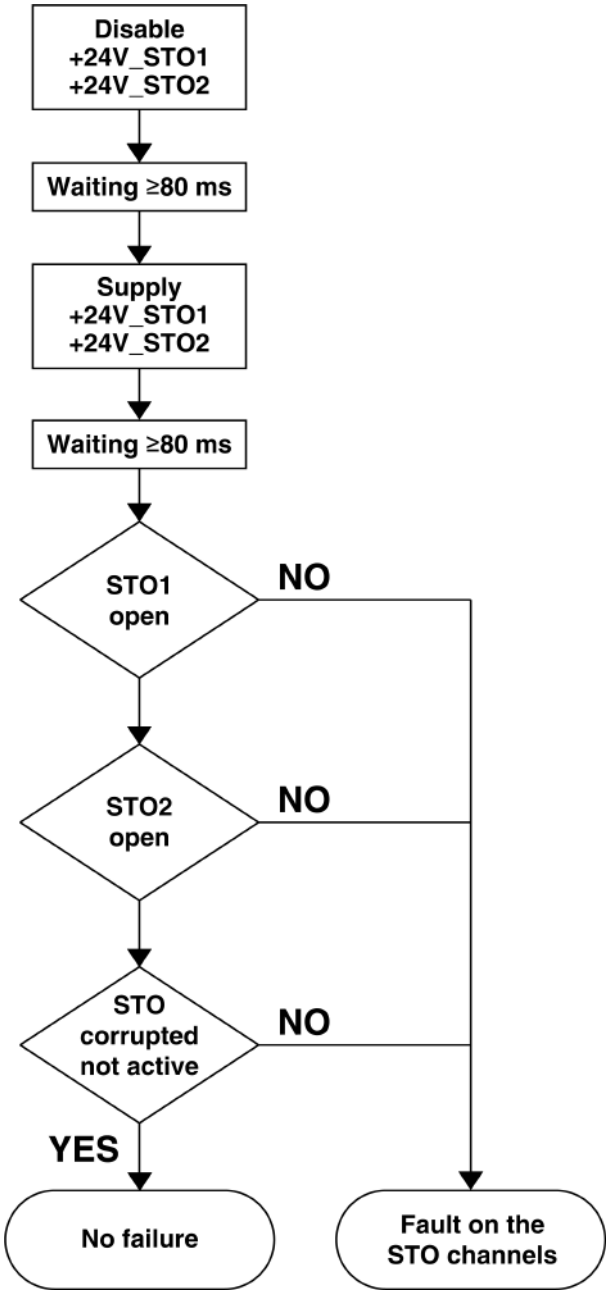
The starting conditions to perform the diagnostic test are the following:

a) Control logic powered

b) Safety channels not active (+ 24V_STO1 and + 24V_STO2 powered)

c) No alarms present

Sequence to be adopted:



9.2.3 Alarms code

The drive control logic knows the status of the STO safety function. An alarm is associated with each status and consequently a reaction of the same control logic.

CODE	CONDITION	DRIVE STATUS
-	STO not active	Ready to work / on run
A13.3	Only one channel active. Commutation time upper than 70 ms. Failure on one of the two STO channels.	Only one channel active
A13.4	Failure of at least one STO channel	Failure on at least one safety channel
A13.5	Interruption of the switching channel between the control logic and the STO function management card	Internal communication channel failure
A13.6	Excessive time span (greater than 2160h) from the last STO activation	Need to execute a diagnostic test

9.2.4 STO safety function not active

When the STO safety function is not active, in the absence of other alarms, the control logic:

a) do not show any type of alarm

b) activates the "Drive Ready - Ok" logic output

c) disables the "STO Corrupted" logic output

d) disables the "STO Active" logic output

e) allows the PWM commands to be transferred to the board that perform the STO safety function

The drive can work normally.

9.2.5 STO safety function active

When the STO safety function is active, in the absence of other alarms, the control logic:

a) do not show any type of alarm

b) set the drive in "Switch on disable" condition (it will not be allowed to exit this status as long as the STO safety function is active)

c) disables the "Drive Ready - Ok" logic output

d) disables the "STO Corrupted" logic output

e) activates the "STO Active" logic output

f) inhibits PWM commands transfer to the board that perform the STO safety function

9.2.6 Only one channel active of the STO safety function

When:

- only one of the two safety channels is active

- the time between the switching of the two channels is higher than 70ms

- there is a fault on one of the two safety channels

The control logic:

a) provides alarm A13.3 (only one STO channel active)

b) disables the "Drive Ready - Ok" logic output

c) activates the "STO Corrupted" logic output

d) disables the "STO Active" logic output

e) inhibits the PWM commands transfer to the board that perform the STO safety function

The alarm code A13.3 cannot be reset either by logic input, or via serial or via field bus because indicates that there may be a fault on the STO safety function. It is necessary to remove the drive power and check if the fault is external to the drive.

If not, replace the drive.

9.2.7 Failure of at least one STO channel

In the event of a failure on one of the two safety channels, the control logic is unable to understand on which one of the two channels there is the problem. Similarly, it cannot distinguish a failure of only one channel from a failure of both channels. The control logic only recognizes that at least one of the two safety channels is faulty and reacts as follows:

a) provides alarm A13.4 (failure on at least one safety channel)

b) disables the "Drive ready - OK" logic output

c) activates the "STO Corrupted" logic output

d) disables the "STO Active" logic output

e) inhibits the PWM commands transfer to the board that perform the STO safety function

It is not important how many or which safety channels are in failure: the reaction to failures of the control logic is always the same.

The alarm code A13.4 cannot be reset either by logic input, or via serial or via field bus because it indicates that there may be a fault on the STO safety function.

It is necessary to replace the drive.

9.2.8 Internal communication channel interruption

The control logic knows the status of the safety function through a communication channel that connects it with the board that manages the STO safety function. In the event that this communication channel is interrupted, the control logic:

a) provides alarm A13.5 (Internal communication channel failure)

b) disables the "Drive ready - Ok" logic output

c) activates the "STO Corrupted" logic output

d) disables the "STO Active" logic output

e) inhibits the PWM commands transfer to the board that perform the STO safety function

The alarm code A13.5 cannot be reset either from logic input, or via serial or via field bus because indicates that the control logic is no longer able to perform the diagnostic function on the STO safety function.

It is necessary to replace the converter.

9.2.9 Diagnostic test

Test mandatory

In the control logic there is a counter that indicates the time elapsed since the last activation of the STO safety function and, consequently, the time elapsed since the last diagnostic test. When it reaches 2160 h from the last activation of the safety function, the control logic:

a) provides alarm A13.6 (Diagnostic test required)

b) disables the "Drive ready - Ok" logic output

c) activates the "STO Corrupted" logic output

d) disables the "STO Active" logic output

e) inhibits the PWM commands transfer to the board that perform the STO safety function

The alarm code A13.6 can be reset from logic input, from serial or from field bus only after the STO safety function is activated.

Test recommended

In the control logic there is a counter that indicates the time elapsed since the last activation of the STO safety function and, consequently, the time elapsed since the last diagnostic test. When it reaches 720 h from the last activation of the safety function, the control logic:

a) activates the "STO: test suggested" logic output

b) leaves the "Drive ready - Ok" logic output unchanged

c) leaves the "STO Corrupted" logic output unchanged

d) leaves the "STO Active" logic output unchanged (which will be inactive since the STO safety function has not been activated for the least 720 hours)

e) allows the PWM commands to be transferred to the board that carries out the STO safety function. In this way the drive can work normally.

WARNING: the "STO: test suggested" logic output activation is intended to indicate that, to meet the requirements of the Machinery Directive 2006/42/EC, a diagnostic test must be performed.

10 APPLICATION EXAMPLE

In the below example, a Pilz PNOZ XV2 safety module is used which includes two relays each having two immediate contacts and two timed contacts that trip after an adjustable delay.

The motor must be stopped by pressing the emergency button.

The enable command is removed.

The PLC receives the communication that the emergency has been pressed through the connection to its digital input.

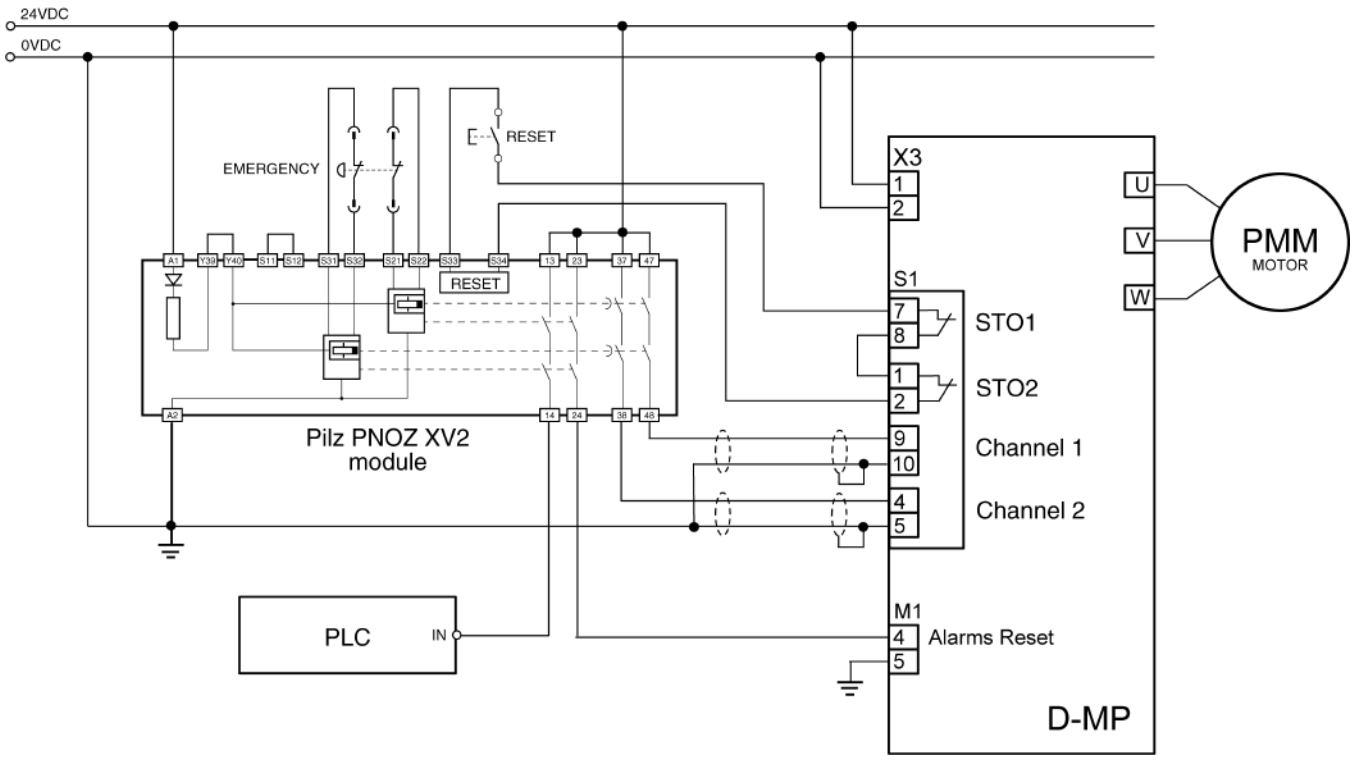
After a certain delay time, the timed contacts of the Pilz module also open and cause the activation of the two channels of the STO function, which occurs when the engine is already stopped.

The feedback contacts of the STO function are connected in series to the reset button (this button allows you to exit the emergency stop condition).

The reset is enabled only if the feedback contacts are closed when the STO function is activated.

If this does not happen, it means that an internal fault has occurred of the converter and the feedback contact will remain open.

This allows you to perform a feedback check of the STO function each time the reset is performed.



11 TECHNICAL DATA

11.1 Drive 022 ÷ 140

EN 61800-5-2		
	DRIVE 022 ÷ 060	**DRIVE 90 ÷ 140**
SIL capability	2	2
PFH	$8{,}4 \cdot 10^{-8}$ h^{-1}	$2{,}8 \cdot 10^{-8}$ h^{-1}
Hardware Fault Tolerance	1	1
Lifetime	10 years	10 years

EN ISO 13849-1		
	DRIVE 022 ÷ 060	**DRIVE 90 ÷ 140**
PL	d	d
Class	3	3
$MTTF_d$	39,6 years	342,7 years

11.2 Drive 165 ÷ 210

EN 61800-5-2	
	DRIVE 165 ÷ 210
SIL capability	3
PFH	$4{,}45 \cdot 10^{-9}$ h^{-1}
Hardware Fault Tolerance	1
Lifetime	20 years

EN ISO 13849-1	
	DRIVE 165 ÷ 210
PL	e
Class	3
PFH	$4{,}45 \cdot 10^{-9}$ h^{-1}
$MTTF_d$	100 years

12 STO SAFETY FUNCTION AND RELATED DIGITAL OUTPUTS

	22A a 60A						90A a 140A						165A – 210A						
	+24V_ STO1	*STO 1*	*+24V_ STO2*	*STO 2*	*STO Active*	*STO Corrupted*	*+24V_ STO1*	*STO 1*	*+24V_ STO2*	*STO 2*	*STO Active*	*STO Corrupted*	*+24V_ STO1*	*STO 1*	*+24V_ STO2*	*STO 2*	*STO Active*	*STO Corrupted*	*STO Test Suggested*
STO disabled	+24V	O	+24V	O	L	L	+24V	O	+24V	O	L	L	+24V	O	+24V	O	L	L	NR
STO active	+24V	O	0V	C	L	L	+24V	O	0V	C	H	L	0V	C	0V	C	H	L	NR
	0V	C	+24V	O	H	L	0V	C	+24V	O	H	L							NR
	0V	C	0V	C	H	L	0V	C	0V	C	H	L							NR
Diagnostic Test Feedback Channel 1 (*)	+24V	C	NR	NR	H	NR	+24V	C	+24V	C	H	NR	+24V	C	+24V	O	L	H	NR
	0V	O	NR	NR	L	NR	0V	O	+24V	C	L	NR							NR
Diagnostic Test Feedback Channel 2	NR	NR	+24V	C	NR	NR	NR	NR	+24V	C	H	NR	+24V	O	+24V	C	L	H	NR
	NR	NR	0V	O	NR	NR	NR	NR	0V	O	H	NR							NR
Recommended Diagnostic Test (**)	NA						NA						NR	NR	NR	NR	NR	NR	H
Power circuit failure (Alarm A3.0)	NR	NR	NR	NR	NR	H	NR	NR	NR	NR	NR	H	NR	NR	NR	NR	NR	H	NR
Failure of one of the channels (**) (Alarm A13.4)	NW		CW		H	L	NW		CW		H	L	NW		CW		L	H	NR
	0V	C	NW		H	L	CW		NW		H	L							
	+24V	O	NW		L	L							CW		NW		L	H	NR
Internal communication channel failure (**) (Alarm A13.5) and mandatory diagnostic test (**) (Alarm A13.6)	NA						NA						NR	NR	NR	NR	L	H	NR

(*) For drives 090 ÷ 140 the diagnostic test must be performed with channel 2 not active: + 24V present on the **+24V_STO2** input

(**) Only for drives 165 and 210

LEGEND:

C: Contact Closed
O: Contact Open
NR: State not Relevant
NA: Not Available
NW: Not Working
CW: Correctly Working
L: Low State
H: High State


atos
the smart electrohydraulics