Chapter 6  Safe Torque Off
SIL3 / PLe

This chapter describes the Safe Torque Off (STO) function, with advice on how to use it, install, test and maintain it in various applications.

- General Information
- STO Functional Description
- Alignment to European Standards
- Safety Specification
- EMC Specification
- User Connections
- STO Technical Specification
- STO Input Timing Diagrams
- STO State Transition Diagram
- STO Trip Annunciation
- Safety Warnings and Limitations
- Example User Wiring
- STO Function Checking
- Troubleshooting
General Information

THIS EQUIPMENT IF USED INCORRECTLY IS POTENTIALLY DANGEROUS. THEREFORE UNDER NO CIRCUMSTANCES SHOULD IT BE USED BEFORE THESE INSTRUCTIONS HAVE BEEN READ AND UNDERSTOOD BY THE END USER WHO SHOULD BE APPROPRIATELY QUALIFIED TO OPERATE THE EQUIPMENT.

This section provides general information about STO.

Two safety functions can be implemented with the 890: Safe Torque Off (STO) and Safe Stop 1 (SS1). In order to meet all aspects of STO and SS1, an external safety control unit should be used.

To implement Safe Stop 1 (SS1), the external safety control unit causes the drive to decelerate to rest. Once at rest, it invokes STO in the 890. Please refer to EN61800-5-2:2007 para 4.2.2.3 for the formal definitions.

It is the user’s responsibility to:

1) Risk assess the machine.

2) Design, implement and assess an appropriate solution for each application to meet all relevant safety requirements.

Note: STO is an electronic inhibit intended for use during normal operation of the machine. It is not intended for use during machine maintenance, repair, replacement or other similar activities. For these activities recognised electrical power isolation devices and lock-off procedures should be used.
STO Functional Description

STO is a means of preventing an 890 drive from delivering power to its connected electric motor. Please refer to EN61800-5-2:2007 para 4.2.2.2 for the formal definition.

To ensure a high degree of safety, two independent STO control channels are implemented in hardware. The STO circuit in the 890 is designed such that a fault in one control channel will not affect the other channel’s ability to prevent the drive from starting, i.e. the STO function of the 890 drive is tolerant to any single fault. It may not be tolerant to an accumulation of faults. This is in keeping with its declared safety ratings.

STO always overrides any attempt to start the drive. If one or both STO control inputs is requesting the STO function, the drive will not start, even if for example, the drive’s software malfunctions and tries to cause the motor to turn.

The STO function is implemented in hardware; it overrides all software activities. The only software involvement is to report STO status to the user via an MMI, serial communications link or user terminal on the 890 control board as defined by the drive configuration.

WARNING

THE DECLARED SIL CAPABILITY OF THIS STO PRODUCT CAN BE ACHIEVED ONLY WHEN THE TWO STO USER INPUTS ARE DRIVEN INDEPENDENTLY. THEY MUST NOT BOTH BE DRIVEN FROM A COMMON SOURCE; OTHERWISE THE SINGLE FAULT DETECTION WILL BE COMPLETELY INOPERATIVE.

USE OF THE PRODUCT IN THIS “COMMON SOURCE” CONDITION INVALIDATES THE STO PRODUCT SPECIFICATION AND IS ENTIRELY AT THE USER’S OWN RISK.
**Alignment to European Standards**

EN ISO13849-1:2006

(Safety of machinery – Safety-related parts of control systems)

STO aligns internally to the following aspects of this standard:

- **Architecture according to Category 3:**

![Diagram]

Solid lines represent the STO control paths.

Dashed lines represent reasonably practicable fault detection.

**Key:**

- I1, I2 = user terminal
- L1, L2 = logic
- O1, O2 = methods of enabling or disabling output power devices
- \( i_{mxy} \) = interconnecting means
- \( m_x \) = monitoring
- \( c \) = cross monitoring
**Category 3 general requirements are:**

A single failure, and any consequential failures, will not lead to loss of the STO safety function.

Failure of more than one component can lead to the loss of the STO safety function.

Most but not all single component failures will be detected. Diagnostic Coverage (DC) is required to be at least 60% (i.e. the minimum required for ‘low’ diagnostic coverage).

Detected component failures will result in the STO function being applied without intervention from the user.

The risk associated with the loss of STO safety function caused by multiple failures must be understood and accepted by the user.

The user must undertake a risk analysis and specify suitable components that, when connected together, meet the required risk assessment requirements.

Mean Time To Failure (dangerous) (MTTFd) of each STO channel must be ≥ 30 years.

Common Cause Failure (CCF) score must be ≥ 65 according to Annex F of the standard.

**Performance Level e:**

Average probability of dangerous failure per hour (PFH) must be ≤ $10^{-7}$
EN61800-5-2:2007 and EN61508

(Aboutlce speed electrical power drive systems) and
(Functional safety of electrical/electronic/programmable electronic safety-related systems)

STO aligns to the following aspects of this standard:

- Safety Integrity Level 3
  - Probability of dangerous random hardware failures per hour (PFH) must be $\leq 10^{-7}$
  - Subsystems type A according to EN61508-2:2001 para 7.4.3.1.2
  - Hardware Fault Tolerance (HFT) = 1
  - Safe Failure Fraction (SFF) must be $\geq 90\%$
Safety Specification

As assessed to EN ISO13849 and EN61800-5-2 and certified by BGIA (a German trade association for industrial safety) the 890 frames B to F have the following related safety values:-

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Requirement</th>
<th>Value achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL3</td>
<td>For type A subsystems, HFT = 1: SFF ≥ 60%</td>
<td>98%</td>
</tr>
<tr>
<td>SIL3</td>
<td>10^{-1} ≥ PFH ≥ 10^{-8}</td>
<td>1 x 10^{-9}</td>
</tr>
<tr>
<td>PLe</td>
<td>SIL3</td>
<td>SIL3</td>
</tr>
<tr>
<td>PLe</td>
<td>10 years ≤ MTTFd &lt; 30 years</td>
<td>100 years¹</td>
</tr>
<tr>
<td>PLe</td>
<td>DC = medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Mission Time</td>
<td>20 years</td>
<td>20 years</td>
</tr>
</tbody>
</table>

Note: all values quoted in this table are valid only when the two STO user inputs are driven independently. This is as required by EN ISO 13849 category 3. See the Alignment to European Standards section in this chapter for the required architecture which must be used throughout the machine design relevant to the drive under consideration.

EMC Specification

In addition to the mandatory requirements of EN61800, the STO functionality has been subjected to testing for immunity at higher levels. In particular it has been tested for radiated immunity up to 3GHz which includes frequencies used by mobile telephones and walkie-talkies.

¹ EN ISO13849 limits MTTFd to 100 years.
User Connections

The STO terminals are on a 6-way terminal block X11. This is mounted on the front of the 890 control housing. Terminal designations are:

<table>
<thead>
<tr>
<th>Terminal Number</th>
<th>Terminal Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X11/01</td>
<td>STO A Input</td>
<td>0V = drive will not run, STO is active on channel A. 24V = drive is enabled to run if X11/03 is also 24V. This input is optically isolated from all the other 890 terminals.</td>
</tr>
<tr>
<td>X11/02</td>
<td>STO Common*</td>
<td>Signal return for STO A and STO B inputs. Connected internally to X11/04. This terminal or X11/04 must be connected to earth at one common point in the drive system.</td>
</tr>
<tr>
<td>X11/03</td>
<td>STO B Input</td>
<td>0V = drive will not run, STO is active on channel B. 24V = drive is enabled to run if X11/01 is also 24V. This input is optically isolated from all the other 890 terminals.</td>
</tr>
<tr>
<td>X11/04</td>
<td>STO Common*</td>
<td>Signal return for STO A and STO B inputs. Connected internally to X11/02. This terminal or X11/02 must be connected to earth at one common point in the drive system.</td>
</tr>
<tr>
<td>X11/05</td>
<td>STO Status Negative</td>
<td>Together with X11/06, this terminal forms an isolated volt-free status output. Although formed from semiconductor</td>
</tr>
</tbody>
</table>

* Do not connect both X11/02 and X11/04 to earth, otherwise an earth loop could be created.
components and therefore sensitive to voltage polarity, it is equivalent to a pair of relay contacts.
This output is on (equivalent to closed relay contacts) when the STO circuit is in the ‘safe’ state, i.e. the drive will not cause its motor to produce torque.
However, this output should be used primarily as an indication. In the unlikely event of a fault in the STO circuit, this output could turn on erroneously to give a false indication of the STO status. It must not be used as a guarantee that the motor will not produce torque.

| X11/06 | STO Status Positive | Together with X11/05, this terminal forms a volt-free status output. See the description for X11/05. |
Examples of wiring to X11/05 and X11/06.

Active high output: The load is energised and X11/05 is high when STO is in the intended safe STO state.

Active low output: The load is energised and X11/06 is low when STO is in the intended safe STO state.

The examples show the use of the 24V supply provided on X14/03 (+24V) and X14/04 (0V) as source of power to a load. Alternatively an external 24V supply could be used.
STO Technical Specification

Inputs Specification
STO A Input and STO B Input comply with IEC61131-2. Note: inputs do not have hysteresis.
- Recommended input voltage for low level: 0V to +5V
- Recommended input voltage for high level: +21.6V to +26.4V
- Typical input threshold voltage: +10.5V
- Absolute maximum input voltage: -30V to +30V
- Typical input current @ 24V: 9mA
- Indeterminate input range: +5V to +15V. Function is undefined.

Output Specification
OFF state:
- Maximum applied voltage: +30V (X11/06 relative to X11/05)
- Reverse voltage protection: Up to -30V X11/06 relative to X11/05
- Leakage current: Less than 1mA when output is off.

ON state:
- Maximum output current: 150mA
- Voltage drop X11/06 to X11/05: Less than 2.5V
- Overcurrent protection: Included
**WARNING**

WIRED CONNECTIONS TO TERMINALS X11/01, X11/03, X11/05 AND X11/06 MUST BE LESS THAN 25 METRES IN LENGTH AND REMAIN WITHIN THE CUBICLE OR DRIVE ENCLOSURE. PARKER SSD DRIVES IS NOT LIABLE FOR ANY CONSEQUENCES IF EITHER CONDITION IS NOT MET.

### Truth Table

<table>
<thead>
<tr>
<th>Overview</th>
<th>STO Input A X11/01</th>
<th>STO Input B X11/03</th>
<th>Drive Function</th>
<th>STO Status Output X11/05, X11/06</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STO Active</strong></td>
<td>0V</td>
<td>0V</td>
<td>Drive cannot start or supply power to its motor. STO trip reported.</td>
<td><strong>ON</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This is the intended safe state of the product with correct dual-channel operation.</td>
<td></td>
</tr>
<tr>
<td><strong>Abnormal one-channel operation detection</strong></td>
<td>24V</td>
<td>0V</td>
<td>Drive cannot start or supply power to its motor. STO trip reported. If either of these conditions persists for more than 2.3 seconds (nominal), the STO function will lock into a fault state. The drive cannot start until the fault is rectified, power is removed and reapplied.</td>
<td><strong>OFF</strong></td>
</tr>
<tr>
<td></td>
<td>0V</td>
<td>24V</td>
<td>This is single channel operation and thus deemed not as intended for category 3 structure implementation.</td>
<td></td>
</tr>
<tr>
<td><strong>STO Inactive</strong></td>
<td>24V</td>
<td>24V</td>
<td>Drive is enabled to run under software control. The drive can supply power to its motor.</td>
<td><strong>OFF</strong></td>
</tr>
</tbody>
</table>
**STO Input Timing Diagrams**

**Ideal Operation**

In ideal operation, both inputs X11/01 and X11/03 should change state simultaneously reflecting true dual-channel operation as intended.

<table>
<thead>
<tr>
<th>STATE</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CH A</td>
<td>24V</td>
<td>0V</td>
<td>24V</td>
</tr>
<tr>
<td>CH B</td>
<td>24V</td>
<td>0V</td>
<td>0V</td>
</tr>
<tr>
<td>Output</td>
<td>ON</td>
<td>OFF</td>
<td>ON</td>
</tr>
</tbody>
</table>

**States:**

1. Both inputs are low. Drive is tripped and STO prevents the drive from starting. User output is ON. This is the “safe torque off” state of the drive.

2. Both outputs are high. Drive is able to run under software control. User output is OFF.
**Normal Operation**

In normal operation, there can be a small time difference between changes of state on X11/01 and X11/03, due to different delays in the operation of two sets of relay contacts.

**States:**

1. Both inputs are low. Drive is tripped and STO prevents the drive from starting. User output is ON. This is the “safe torque off” state of the drive.
2. Both outputs are high. Drive is able to run under software control. User output is OFF.
3. One input is high and the other input is low. Drive is tripped and cannot start due to STO action. User output is OFF. Normal operation allows this state to persist for up to 2.3 seconds (nominal). Usually this period will be in the order of tens of microseconds to tens of milliseconds. These delays are caused by external equipment, not the 890.
Fault Operation

A fault is detected when X11/01 and X11/03 are in opposite states for more than 2.3 seconds.

States:

1. Both inputs are low. Drive is tripped and STO prevents the drive from starting. User output is ON. This is the “safe torque off” state of the drive.

3. One input is high and the other input is low. Drive is tripped and STO prevents the drive from starting. In this example, this state persists for more than 2.3 seconds, after which time the STO logic transitions to state 4 without further changes in input state. The 890 has detected single-channel operation. The user must correct this situation immediately as it implies a first fault has been detected and subsequent second faults may not be detected.
DANGER

OPERATION OF THE 890 UNIT SHOULD CEASE IMMEDIATELY AND THE UNIT SHOULD BE INSPECTED AND REPAIRED AS NECESSARY BY APPROPRIATELY QUALIFIED PERSONNEL. FAILURE TO DO SO COULD RESULT IN INJURY, DEATH OR DAMAGE.

FURTHER OPERATION OF THE 890 WITHOUT RESOLVING THIS FAILURE IS ENTIRELY AT THE USER’S OWN RISK.

SEE SAFETY CATEGORY DEFINITIONS AND LIMITATIONS, REFER TO EN ISO 13849-1:2008.

The fault state (one input high, the other input low) has persisted for longer than 2.3 seconds (nominal). The STO hardware logic locks into state 4. The drive is tripped and the STO function prevents the drive from starting. User output is OFF. To exit from state 4, the drive must be powered off and on due to this hardware lockout safety feature.
Pulsed Inputs

Some safety equipment, e.g. safety PLCs, regularly pulse the two STO inputs independently in order to detect a short circuit between them. This is commonly known as OSSD (Output Signal Switch Device). The 890STO inputs are immune to such pulses when these are less than 2ms in width. The product will not react to such pulses and therefore will not inadvertently invoke the STO function.

States:
1. Both inputs are low. Drive is tripped and STO prevents the drive from starting. User output is ON. This is the “safe torque off” state of the drive.
2. Both inputs are high, but regularly pulse low independently. External equipment can thus detect a short circuit between the two STO user inputs. Each input must remain low for 6ms (typical) before the 890 reacts to it.
6-18 Safe Torque Off

**STO State Transition Diagram**

The flow chart below shows how the drive responds to STO inputs, start and stop commands.

**Key:**
- Normal state
- Transitional state. User should avoid remaining in this state
- Fault state
  - * = One channel operation
  - ** = Two channel operation

**Out-of-box state**
- Normal startup state
  - X11/01 high
  - X11/03 low

**Fault state**
- Drive cannot run
  - Power must be cycled
  - 2.3 seconds

**X11/01 high**
- X11/01 high
  - X11/03 low
  - Drive cannot run

**X11/03 high**
- X11/03 high
  - X11/01 low
  - Drive cannot run

**STOP command**
- X11/03 low
- Drive enabled but not running

**START command**
- X11/03 high
- Drive runs

**Fault state**
- X11/01 low
- X11/03 high
- Drive cannot run
STO Trip Annunciation

The MMI will display a STO trip message when STO becomes active, i.e. STO prevents the drive from running, thus:

*** TRIPPED ***
SAFE TORQUE OFF

This message is displayed immediately if:

- One or both STO user inputs X11/01 or X11/03 is low, or
- The 890 drive has detected a fault in the STO circuit.

Note that an out-of-box 890 drive will report this trip if the drive, as supplied, has no connections to X11. Appropriate connections must be made to X11 to prevent this trip from occurring, as described elsewhere in this chapter. The user must decide if STO is to be permanently inactive, or to make use of the STO feature. See elsewhere within this chapter for details.

Safe Torque Off is inserted into the trips history buffer (see Chapter 11) if STO becomes active while the drive is running, indicating an abnormal condition. The trips history buffer is not updated if STO becomes active while the drive is not running.

Note: The intended method of operation is for STO to become active while the drive is not running and the motor is intended not to rotate.
Safety Warnings and Limitations

- Only appropriately qualified professional personnel are permitted to install the STO function and commission it. They must disseminate and make available all appropriate instructions and documentation to all personnel who may come into contact with or operate the STO and provide suitable training on the 890 to ensure it is operated in the correct manner and to avoid loss of life, injury or damage.

- The 890 STO function is a factory-fitted and factory-tested feature. Repairs to 890 STO featured-product are to be carried out only by Parker SSD Drives. Any unauthorised attempt to repair or disassemble the product will render any warranty null and void. Upgrading of non-STO product to STO product is strictly prohibited. PARKER SSD DRIVES WILL NOT ACCEPT ANY LIABILITY FOR FAILING TO OBEY THESE INSTRUCTIONS OR FOR ANY CONSEQUENTIAL LOSS OR DAMAGE.

- It is important that the 890 product environment including all aspects of its CE conformance and IP etc., specified elsewhere in this manual, is maintained to ensure the safety integrity of the STO function.

- Should synchronous motors be operated in the field weakening range, operation of the STO function may lead to overspeed and destructive life-threatening overvoltages as well as explosions in the drive. Therefore, the STO function must NEVER be used with synchronous drives in the field-weakening range. The user must ensure this condition is prevented.

- When using synchronous permanent magnet motors, shaft movement over a small angle is possible if two faults occur simultaneously in the power section of the drive. This depends on the number of motor poles. The maximum angle is:
  - Rotary motors: 360° / number of poles
  - Linear motors: 180° electrically.
  It is the user’s responsibility to assess, validate and safeguard as necessary against this potential hazard.

- If external forces can act on the motor and/or load to cause it to move, additional measures must be taken by the user to restrain it, for example mechanical brakes. Examples of external forces are suspended loads (effect of gravity), and other web-tensioning devices.
The 890 STO feature does not provide or guarantee any galvanic isolation in accordance with EN 60204-1 Section 5.5. This means that the entire system must be isolated from the mains power supply with a suitable electrical isolation device before any drive or motor maintenance or replacement procedures are attempted. Note that even after the power has been isolated, dangerous electrical voltages may still be present in the 890 drive. Safe discharge times and details are specified elsewhere in this manual.

The STO function must not be used for electrical isolation of the 890 drive and power. Whenever any personnel require to work on the drive, associated motor or other power items, they must always use recognised and suitable electrical isolation devices and lock-off procedures as appropriate.

Terminal X11/02 or X11/04 must be connected to earth at one common point in the drive system. For multi-drive systems this can be a shared earth point.

The STO user output, serial communications or MMI messages relating to accessing or viewing any safety monitoring statuses are for information only and should not be relied on. They are not part of the drive module safety system and its associated PL/SIL declared rating. Any customer use of these must be appropriately risk assessed by the customer in accordance with any relevant standards or regulations.

The STO safety function must be tested regularly. The frequency should be determined by the machinery builder. An initial frequency of once per week is suggested.

When using an external safety control unit with adjustable time delay, for example when implementing an SS1 function, the time delay must be protected to prevent unauthorized adjustment. The adjustable time delay on the safety control unit must be set to a value greater than the duration of the braking ramp controlled by the 890 with maximum load inertia and from maximum speed. Any external forces must also be considered, e.g. effects due to gravity.

When implementing a SS1 function with the 890, the user is responsible for ensuring the drive’s configuration will allow a controlled braking ramp to be initiated by the external safety device. This is particularly important when using serial link communications for normal control of the drive.

During the active braking phase of SS1 or Stop category 1 (controlled stop with safely monitored time delay according to EN60204-1), faulty operation of the drive must be allowed for. If a fault in the drive system occurs during the active braking phase, the load may coast to a stop or might even actively
accelerate until expiration of the defined time delay. It is not the remit of this document to specify these measures. This is for the user to assess.

- When the 890 detects either an internal STO fault or an external single-channel user fault, the user must immediately fully resolve the fault. The user must ensure dual-channel operation has been fully restored before attempting to use the 890 STO safety feature.

**DANGER**

FAILURE TO DO SO COULD RESULT IN STO NOT BEING ACHIEVABLE, AND THUS THE MOTOR MAY ROTATE UNEXPECTEDLY AND COULD RESULT IN INJURY, DEATH OR DAMAGE.

- It is the user’s responsibility to ensure that their overall control implementation recovers safely from supply loss or dips.
- In all instances it is the user’s responsibility formally to perform suitable risk assessments, and invoke and fully validate the necessary risk reduction measures after having thoroughly understood the application, the drive product and its features.
Example User Wiring

**WARNING**

THE WIRING EXAMPLES SHOWN IN THIS SECTION ARE FOR ILLUSTRATION ONLY. THEY ARE NOT TO BE CONSIDERED FINAL DESIGNS, NOR AS AN ATTEMPT TO CREATE A DESIGN FOR SPECIFIC SOLUTIONS.

THE USER / INSTALLER IS RESPONSIBLE FOR DESIGNING A SUITABLE SYSTEM TO MEET ALL REQUIREMENTS OF THE APPLICATION INCLUDING ASSESSING AND VALIDATING IT. PARKER SSD DRIVES WILL NOT ACCEPT ANY LIABILITY FOR FAILURE TO DO THIS OR FOR ANY CONSEQUENTIAL LOSS OR DAMAGE.
Applications that do not require STO function

STO inputs X11/01 and X11/03 must be connected to 24VDC with respect to terminals X11/02 or X11/04.

STO Status output on X11/05 and X11/06 may be left disconnected.

All wiring shown is within the control cubicle.

Here the STO inputs X11/01 and X11/03 have been set to the inactive state (tied to +24V). Drive control is performed solely through software with no inherent safety function. The drive is controlled with its own start and stop pushbuttons.

Note: Only X11/02 or X11/4 must be earthed, i.e. they should not both be earthed otherwise it is possible to create an earth loop.
Minimum STO Implementation

This example shows the minimum connections required. To reset from STO requires that STO Request contacts are closed to permit normal drive operation. The user must do a risk assessment to ensure that all safety requirements are met. The user must select and assess appropriate equipment.

To run the drive:
Ensure the STO Request contacts are closed.
Press the DRIVE START button.

To perform operational (not STO) stop:
Press the DRIVE STOP button.
Wait for the motor to come to rest.

To invoke STO:
Press the DRIVE STOP button.
Wait for the motor to come to rest.
Open the STO Request contacts simultaneously. The contacts must remain open for the entire duration that STO is required, they must not be momentary action switches. The drive will confirm via X11/05 that STO has been invoked by the lamp being ON.
If the lamp is OFF, do not access the machine as a fault may be present.
Note: if the STO Request contacts open while the motor is rotating, the motor will coast to rest (unless external forces act on it).

Note: all wiring shown is within the control cubicle.
**STO Implementation with Safety Control Unit**

This example improves on the previous one by showing the resetting from a STO stop. The example shows wiring and terminal numbering for a Siemens 3TK2827, but similar products are available from other vendors. The use of this Siemens part does not imply it is suitable for the user’s application. The user must select and assess appropriate equipment.

Note: On power-up, the safety control unit outputs are OPEN; thus the STO state is requested of the 890. The latter responds by energising KA1 if both channels are active and healthy. KA1 is used as a self-check for the reset cycle of the safety control unit. If a reset cannot be achieved due to KA1 being de-energised, a fault may be present and must be resolved by the user before relying on the STO function. See Fault Operation on page 6-15.
To start the drive:
Ensure the Safety Demand switch is reset (contacts closed). Press the RESET button to ensure the Safety Control Unit is reset; its contacts to the 890 should close making the STO function inactive, the 890 STO output should then turn OFF. Then press the DRIVE START button.

To perform operational stop (non STO):
Press the DRIVE STOP button.
Wait for the motor to come to rest.

To invoke STO:
Press the DRIVE STOP button.
Wait for the motor to come to rest.
Operate the Safety Demand (contacts open) that causes the safety control unit to open its output contacts together. In response, the drive will confirm, by energising KA1 via X11/05, that STO has been invoked. The user may wish / require that this is verified by mechanisms not shown on this drawing.

DANGER

IF KA1 IS DE-ENERGISED, DO NOT ACCESS THE MACHINE AS A FAULT MAY BE PRESENT.

THE USER MUST RESOLVE THE DETECTED FAULT BEFORE USING THE STO FEATURE. FAILURE TO DO SO COULD RESULT IN STO NOT BEING ACHIEVABLE, AND THUS THE MOTOR MAY ROTATE UNEXPECTEDLY AND COULD RESULT IN INJURY, DEATH OR DAMAGE. PARKER SSD DRIVES WILL NOT ACCEPT ANY LIABILITY FOR FAILURE TO DO THIS OR FOR ANY CONSEQUENTIAL LOSS OR DAMAGE.

Note: if either channel of the Safety Demand is requested while the motor is rotating, the motor will coast to rest unless external forces act on it.
SS1 Implementation using Safety Control Unit

This Safe Stop 1 (SS1) implementation causes the drive to come to rest in a controlled manner, and STO is actioned after a time delay determined by the safety delay relay. This conforms to SS1 defined in EN61800-5-2:2007 para 4.2.2.3 c). The example shows wiring and terminal numbering for a Siemens 3TK2827, but similar products are available from other vendors. The user must select and assess appropriate equipment.

POWER SUPPLY

SAFETY DEMAND

SAFETY CONTROL UNIT

890 STO

DRIVE START

DRIVE STOP

RESET

KA1

SAFETY DEMAND

24VDC

A1 Y10 Y11 Y12 Y21 Y22 13
A2 PE Y33 Y34 14

X15/02 X15/03 X11/01 X11/03 X11/06 X14/03

X11/02 X11/04 X11/05 X14/04

X15/05

K11/02 K11/04 K11/06 K14/09

K11/01 K11/03 K11/08 K14/09

KA1

X14/09

THIS WIRING MUST BE WITHIN THE CONTROL CUBICLE.
Note: On power-up, the Safety Control Unit outputs are OPEN; thus STO is requested of the 890. This responds by energising KA1 if both channels are active and healthy. KA1 is used as a self-check for the reset cycle of the Safety Control Unit. If a reset cannot be achieved due to KA1 being de-energised, a fault may be present and must be resolved by the user before relying on the STO function. See Fault Operation on page 6-6-15.

**To start the drive:**
Ensure the Safety Demand switch is reset (contacts closed). Press the RESET button to ensure the Safety Control Unit is reset; its contacts to the 890 should close making the STO function inactive, the 890 STO output should then turn OFF. Then press the DRIVE START button.

**To perform operational stop (non STO):**
Press the DRIVE STOP button.
Wait for the motor to come to rest.

**To invoke STO:**
Operate the Safety Demand (contacts open). This should cause the Safety Control Unit to open its instantaneous output, shown here as a single channel. This causes the drive to decelerate to rest using its own software which is not safety critical in this instance. Note: the drive’s block diagram must be configured to provide this ramp to rest functionality.

After a time delay set in the Safety Control Unit, the pair of delayed OFF output contacts open together. This time delay must be set longer than the worst case time for the motor to come to rest.

In response, the drive will confirm, by energising KA1 via X11/05, that STO has been invoked. The user may wish / require that this is verified by mechanisms not shown on this drawing.
DANGER

IF KA1 IS DE-ENERGISED, DO NOT ACCESS THE MACHINE AS A FAULT MAY BE PRESENT.

THE USER MUST RESOLVE THE DETECTED FAULT BEFORE RELYING FURTHER ON THE STO FEATURE. FAILURE TO DO SO COULD RESULT IN STO NOT BEING ACHIEVABLE, AND THUS THE MOTOR MAY ROTATE UNEXPECTEDLY AND COULD RESULT IN INJURY, DEATH OR DAMAGE. PARKER SSD DRIVES WILL NOT ACCEPT ANY LIABILITY FOR FAILURE TO DO THIS OR FOR ANY CONSEQUENTIAL LOSS OR DAMAGE.

Note: if either of the delayed OFF output contacts in the Safety Control Unit open while the motor is rotating, the motor will coast to rest (unless external forces act on it).
STO Function Checking

Two levels of checking are required. A comprehensive check, and a regular check.

It is for the user / machine builder to determine the frequency of these checks based on their knowledge, use of the machine, appropriate standards and any legal requirements.

**DANGER**

ALL TESTS MUST PASS. IF ANY TEST FAILS, IT MUST BE INVESTIGATED AND RECTIFIED BEFORE ATTEMPTING TO PUT THE EQUIPMENT INTO SERVICE.

FURTHER OPERATION OF THE 890 WITHOUT RESOLVING THIS FAILURE IS ENTIRELY AT THE USER’S OWN RISK. FAILURE TO DO SO COULD RESULT IN INJURY, DEATH OR DAMAGE. PARKER SSD DRIVES WILL NOT ACCEPT ANY LIABILITY FOR FAILURE TO DO THIS OR FOR ANY CONSEQUENTIAL LOSS OR DAMAGE.

SEE SAFETY CATEGORY DEFINITIONS AND LIMITATIONS, REFER TO EN ISO 13849-1:2008.

When STO becomes active during any test, power to the motor must be seen by the user to be quenched instantaneously. Note: the drive should respond in less than 10 milliseconds.

All STO checks should be performed after the 890 has been commissioned for speed control.
Comprehensive check

A comprehensive check of the STO function ensures the overall integrity of the STO functionality. It proves the independent operation of each individual channel (including during the normal dual channel operation), the STO user feedback operation, and the essential single fault detection.

It must always be performed:

- During factory test
- During commissioning activities
- After repair or replacement of the 890
- After any hardware or software design changes which may affect the 890 concerned.
- After each intervention into the system and control wiring.
- At defined maintenance intervals as determined by the machine builder and/or user risk assessments and associated verification assessments.
- If the machine has been idle for more than a period of time determined by the machinery builder and user risk assessments.
- The check must be made by suitably qualified professional personnel following all necessary safety precautions. They must be fully conversant with all equipment concerned.
The following test steps must be performed:

<table>
<thead>
<tr>
<th>STO test</th>
<th>Comprehensive Action, activity</th>
<th>Expected reaction and effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that no harm can come to personnel or equipment if the motor turns.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Apply +24V DC to terminals X11/01 and X11/03.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Switch on power and 24V supply voltage.</td>
<td>No error must be present in the drive system. X11/05 and /06 must be OFF.</td>
</tr>
<tr>
<td>4</td>
<td>Configure the drive and associated equipment if necessary so that it can be started and stopped, and a speed setpoint provided.</td>
<td>No error must be present in the drive system. X11/05 and /06 must be OFF.</td>
</tr>
<tr>
<td>5</td>
<td>Try to start the drive with a non-zero setpoint. This setpoint value will be referred to as SPT1 for brevity in these tests. Leave this set throughout all tests.</td>
<td>Drive must start and motor must turn at SPT1. X11/05 and /06 must be OFF.</td>
</tr>
</tbody>
</table>

Channel A Check:

<table>
<thead>
<tr>
<th>STO test</th>
<th>Comprehensive Action, activity</th>
<th>Expected reaction and effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>With drive running and motor turning, momentarily disconnect terminal X11/01 (maximum duration of disconnect = 1 second), while retaining +24V at terminal X11/03.</td>
<td>Motor must immediately coast to rest. Drive must report STO trip immediately. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Channel B Check:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Ensure terminals X11/01 and X11/03 are both 24V. Try to restart the drive.</td>
<td>Drive must restart at SPT1. STO trip must clear. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td>8</td>
<td>With drive running and motor turning, momentarily disconnect terminal X11/03 (maximum duration of disconnect = 1 second), while retaining +24V at terminal X11/01.</td>
<td>Motor must immediately coast to rest. Drive must report STO trip immediately. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td>9</td>
<td>Ensure terminals X11/01 and X11/03 are both 24V. Try to restart the drive.</td>
<td>Drive must restart at SPT1. STO trip must clear. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td><strong>Channel A Fault Check:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Ensure the drive is running and the motor is turning. Disconnect terminal X11/01 for approximately 5 seconds (must exceed 3 seconds).</td>
<td>Motor must immediately coast to rest. Drive must report STO trip immediately. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>The STO function has latched in hardware to disable the drive. Re-apply 24V to terminal X11/01, and then try to restart drive.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Drive must not start. Drive must continue to report STO trip. X11/05 and /06 must remain OFF.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Remove and re-apply power to the drive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X11/05 and /06 must be OFF.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Try to start drive.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Drive must start at SPT1. X11/05 and /06 must remain OFF.</td>
<td></td>
</tr>
</tbody>
</table>

**Channel B Fault Check:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Ensure the drive is running and the motor is turning. Disconnect terminal X11/03 for approximately 5 seconds (must exceed 3 seconds).</td>
</tr>
<tr>
<td></td>
<td>Motor must immediately coast to rest. Drive must report STO trip immediately. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td>15</td>
<td>The STO function has latched in hardware to disable the drive. Re-apply 24V to terminal X11/03, and then try to restart drive.</td>
</tr>
<tr>
<td></td>
<td>Drive must not start. Drive must continue to report STO trip. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td>16</td>
<td>Remove and re-apply power to the drive</td>
</tr>
<tr>
<td></td>
<td>X11/05 and /06 must be OFF.</td>
</tr>
<tr>
<td>17</td>
<td>Try to restart drive.</td>
</tr>
<tr>
<td></td>
<td>Drive must start at SPT1.</td>
</tr>
<tr>
<td>18</td>
<td>Stop the drive.</td>
</tr>
<tr>
<td></td>
<td>Drive must decelerate to rest.</td>
</tr>
</tbody>
</table>
### Safe Torque Off

**User Output Check:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Requirement</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Remove connections to X11/01 and X11/03 within 1 second of each other.</td>
<td>Drive must report STO trip immediately. X11/05 and /06 must be ON.</td>
</tr>
<tr>
<td>20</td>
<td>Try to restart the drive. Wait for at least 10 seconds with the run command active.</td>
<td>Drive must not start while run command is given. STO trip must remain. X11/05 and /06 must remain ON.</td>
</tr>
<tr>
<td>21</td>
<td>Reconnect X11/01 and X11/03 to 24V.</td>
<td>X11/05 and /06 must turn OFF immediately.</td>
</tr>
<tr>
<td>22</td>
<td>Try to restart the drive.</td>
<td>STO trip must clear. The drive must restart at SPT1.</td>
</tr>
<tr>
<td>23</td>
<td>Stop the drive. Test is complete.</td>
<td>Drive must stop.</td>
</tr>
</tbody>
</table>

The performance of the individual test steps of the STO function should be logged.

The tests specified above are the minimum set; further test steps may be required depending on the application, for example a controlled stop should be verified in a SS1 application.

**Regular check**

A comprehensive check must take precedence if it coincides with a regular check.

A regular check is intended only to demonstrate the STO is functional. It will not always detect the loss of a single channel. It is therefore important for the user and / or machinery builder to determine the frequency of the comprehensive checks based on their knowledge and application of the machine.
The following tests should be performed.

<table>
<thead>
<tr>
<th>STO test</th>
<th>Regular Action, activity</th>
<th>Expected reaction and effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that no harm can come to personnel or equipment if the motor turns.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Apply +24V DC to terminals X11/01 and X11/03.</td>
<td>No error must be present in the drive system</td>
</tr>
<tr>
<td>3</td>
<td>Apply power to the drive.</td>
<td>X11/05 and /06 must be OFF. The STO trip message should not be present.</td>
</tr>
<tr>
<td>4</td>
<td>Try to start the drive with a non-zero setpoint. This setpoint value will be referred to as SPT1 for brevity in these tests. Leave this set throughout all tests.</td>
<td>The drive should start and the motor should turn at SPT1. X11/05 and /06 must remain OFF.</td>
</tr>
<tr>
<td>5</td>
<td>Remove connections to X11/01 and X11/03 within 1 second of each other.</td>
<td>Drive must stop immediately, and report STO trip. X11/05 and /06 must be ON.</td>
</tr>
<tr>
<td>6</td>
<td>Re-apply 24V to X11/01 and X11/03.</td>
<td>STO trip indication must remain. X11/05 and /06 must turn OFF.</td>
</tr>
<tr>
<td>7</td>
<td>Try to restart drive.</td>
<td>STO trip indication should clear. Drive must restart at SPT1.</td>
</tr>
<tr>
<td>8</td>
<td>Stop the drive.</td>
<td>Drive must stop.</td>
</tr>
<tr>
<td></td>
<td>Test is complete.</td>
<td></td>
</tr>
</tbody>
</table>
## Troubleshooting

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Examines:</th>
<th>6901 MMI display</th>
<th>User output</th>
<th>User inputs</th>
<th>Probable cause</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive won’t start when given a start command</td>
<td>*** TRIPPED *** SAFE TORQUE OFF</td>
<td>On</td>
<td>Both &lt; 15V</td>
<td></td>
<td>STO is invoked.</td>
<td>When safe to do so, connect X11.01 and X11.03 to 24V ± 10%</td>
</tr>
<tr>
<td></td>
<td>*** TRIPPED *** SAFE TORQUE OFF</td>
<td>Off</td>
<td>Both &gt;15V and &lt; 30V</td>
<td>Fault latch might have tripped</td>
<td>Remove all power from drive and re-apply. If symptom persists, immediately return the 890 for repair. See the DANGER box below.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>Both &gt;15V and &lt; 30V</td>
<td>Faulty hardware</td>
<td>Reset the trip, and remove its cause. If symptom persists, return the 890 for repair.</td>
<td></td>
</tr>
<tr>
<td>Any other message</td>
<td>Off</td>
<td>Both &gt;15V and &lt; 30V</td>
<td>Faulty hardware</td>
<td>Return for repair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drives starts unexpectedly</td>
<td>Don’t care</td>
<td>Don’t care</td>
<td>Both &lt; 5V</td>
<td>Faulty hardware</td>
<td>Immediately return the 890 for repair. See the DANGER box below.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Don’t care</td>
<td>Off</td>
<td>Both &gt; 5V</td>
<td>STO not invoked by the user.</td>
<td>Use STO according to instructions elsewhere in this chapter.</td>
<td></td>
</tr>
<tr>
<td>Drive fails comprehensive or regular STO test</td>
<td>Don’t care</td>
<td>Don’t care</td>
<td>Don’t care</td>
<td>Faulty hardware</td>
<td>Immediately return the 890 for repair. See the DANGER box below.</td>
<td></td>
</tr>
</tbody>
</table>

---

3 Continuity through X11.05 and X11.06
4 Measure X11.03 and X11.03 relative to X11.02 or X11.04
The above table is only a guide. It may not be a comprehensive list of all possible symptoms relating to STO. Parker SSD Drives will not accept responsibility for any consequences arising from its incompleteness or inaccuracy.

**Important note:**
- There are no user-serviceable parts in the 890 drive. Refer to the Safety Warnings and Limitations section of this chapter.

---

**DANGER**

IF ANY FAULTY OPERATION OF THE STO FUNCTION IS OBSERVED OR SUSPECTED, OPERATION OF THE 890 SHOULD CEASE IMMEDIATELY AND THE UNIT SHOULD BE RETURNED TO PARKER SSD DRIVES FOR INVESTIGATION AND REPAIR. FAILURE TO DO SO COULD RESULT IN INJURY, DEATH OR DAMAGE.

FURTHER OPERATION OF THE 890 WITHOUT RESOLVING THIS FAILURE IS ENTIRELY AT THE USER’S OWN RISK.

SEE SAFETY CATEGORY DEFINITIONS AND LIMITATIONS. REFER TO EN ISO 13849-1:2008