3 Functional Safety

3.1 STO - Safe Torque Off

Option

3.1.1 Introduction

This section provides information for use of MIS stepper motors in functional safety applications. The section includes information about functional safety standards, the STO function, the related installation and commissioning and service and maintenance for STO.

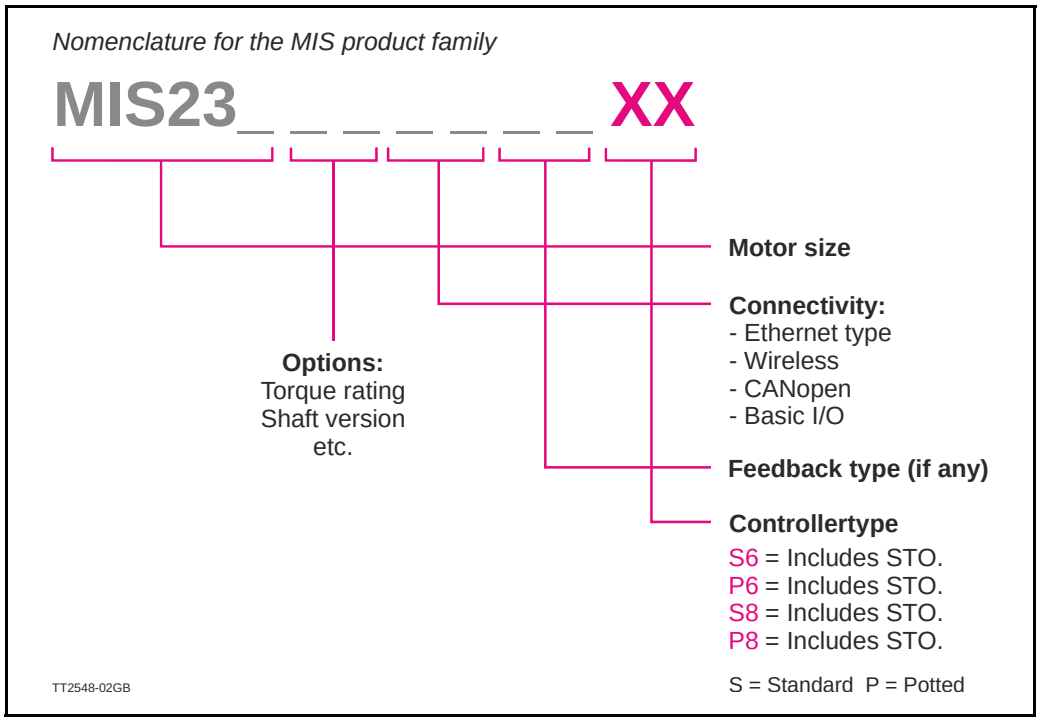
3.1.2 Functional overview

Introduction

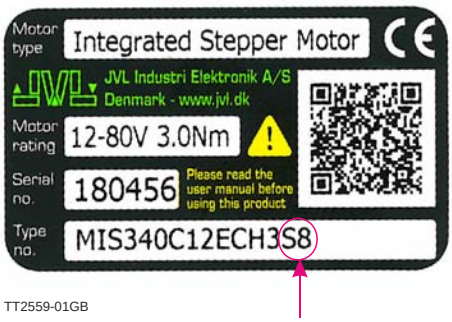
As an option the MIS motor can be delivered with the so-called STO function which to a certain extend can simplify the safety system in the actual application. If the STO option is present in the motor an extra 4-pin M8 connector is available with 2 inputs. These 2 inputs need to be applied with a 24V (nom.) voltage in order to let the motor be energized and thereby operate. If one or both of the inputs are not supplied, the motor will be de-energized and no movement will happen regardless which commands are sent to the motor. The STO input simply overrule any other attempts to let the motor run. The default settings require manual restart of the motor when the STO signals are re-applied.

Products covered and identification

The whole range of MIS and MIL stepper motors offers the STO option. To identify whether a motor has the STO option installed, please check the last 2 digits of the type number:



Example of the physical label on the motor where the S8 is identified and marked with a red circle:



3.1.3 Abbreviations

Abbreviation	Reference	Description
Cat.	ISO13849-1	Category, level “1-4”
DC	-	Diagnostic coverage
FIT	-	Failure in time: 1E-9/hour
HFT	IEC61508	Hardware fault tolerance: HFT = n means that n+1 faults cause a loss of the safety function.
MTTFd	ISO13849-1	Mean time to failure – dangerous. Unit: Years
PFH	IEC61508	Probability of dangerous failures per hour. Consider this value if the safety device is operated in high demand or continuous mode of operation, where the frequency of demands for operation made on a safety-related system is greater than once per year.
PFD	IEC61508	Average probability of failure on demand, value used for low demand operation.
PL	ISO13849-1	Performance level, used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. Levels a–e.
SIL	IEC61508 IEC62061	Safety integrity level
STO	IEC61800-5-2	Safe Torque Off
SRECS	IEC62061	Safety related electrical control system
SRP/CS	ISO13849-1	Safety related parts of control systems
PDS/SR	IEC61800-5-2	Power drive system (safety related)

3.2.1 Qualified personnel

Only persons with proven skills are allowed to assemble, install, program, commission, maintain, and decommission the products.

Persons with proven skills

- Are qualified electrical engineers, or persons who have received training from qualified electrical engineers and are suitably experienced to operate devices, systems, plant, and machinery in accordance with the general standards and guidelines for safety technology.
- Are familiar with the basic regulations concerning health and safety/accident prevention.
- Have read and understood the safety guidelines given in this section and also the instructions given in the general operating instructions of the stepper motor.
- Have a good knowledge of the generic and specialist standards applicable to the specific application.

Users of power drive systems (safety related) (PDS(SR)) are responsible for:

- Hazard and risk analysis of the application.
- Identifying safety functions required and allocating SIL or PLr to each of the functions.
- Other subsystems and the validity of signals and commands from them.
- Designing appropriate safety-related control systems (hardware, software, parameterization, and so on).

Protective measures

- Only qualified and skilled personnel is allowed to install and commission safety engineering systems.
- Check the ingress protection (IP) level of the motor before installation in wet, humid environments - Ordering information, page 353.
- Ensure short-circuit protection of the STO cable between the motor and the external safety device according to ISO 13849-2 table D.4.
- When external forces influence the motor axis (for example suspended loads), extra measures (for example a safety holding brake) are required to eliminate hazards.

3.2.2 Safety precautions

CAUTION

After installation of STO, perform a commissioning test as specified in chapter STO commissioning test, page 70. A passed commissioning test is mandatory after first installation and after each change to the safety installation. In case that the test of STO fails: DO NOT use the motor, return it to JVL Industri Elektronik A/S for service.
The motor control electronics including the safety related parts must only be serviced and repaired by JVL Industri Elektronik A/S. Access to the inner parts of the motor will violate the guarantee.

WARNING
RISK OF DEATH AND SERIOUS INJURY
If external forces act on the motor, for example in case of vertical axis (suspended loads), and an unwanted movement, for example caused by gravity, could cause a hazard, the motor must be equipped with extra measures for fall protection. For example, install extra mechanical brakes.

WARNING
STO is suitable for performing mechanical work on the system or affected area of a machine only. It does not provide electrical safety.

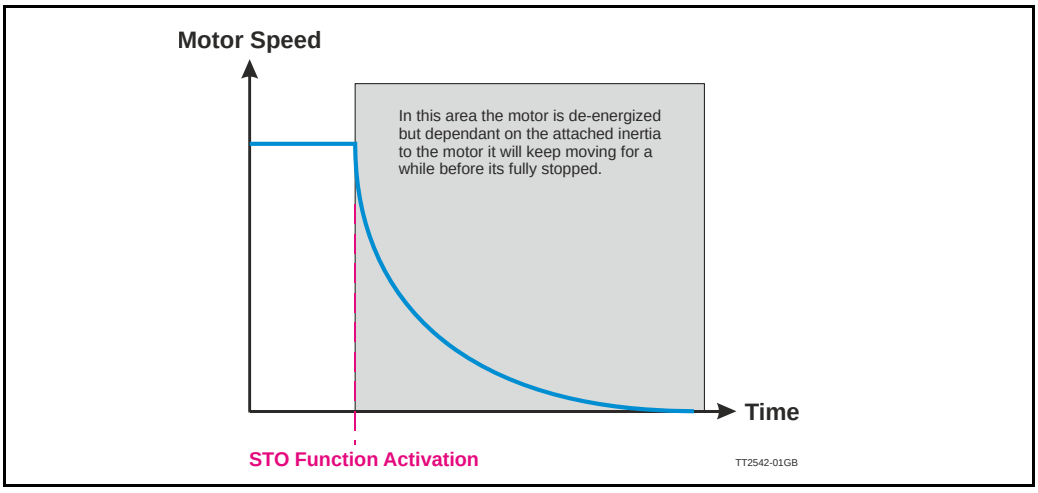
NOTICE
Perform a risk assessment for each stop function to determine the selection of a stop category in accordance with EN 60204-1:

- Stop Category 0 is achieved with immediate removal of power to the actuator, resulting in an uncontrolled coast to stop.
  The STO according to EN 61800-5-2 accomplishes a Stop Category 0 stop.

This is the only category available for the MIS motors alone. Other measures must be made to achieve stop category 1 or 2:

- Stop Category 1 is achieved with power available to the machine actuators to achieve the stop. Power is removed from the actuators when the stop is achieved according to EN 61800-5-2 Safe Stop 1 (SS1).
- Stop Category 2 is a controlled stop with power available to the machine actuators. A holding position under power follows the stop.

NOTICE
When designing the machine application, timing and distance must be considered for a coast to stop (Stop Category 0 or STO). For more information regarding stop categories, refer to EN 60204-1.



3.2.3 Important general information.

If the motor is used outside the environmental limits given in this instruction the motor can not be expected to perform a safe stop when there is a demand on the STO-safety function.

3.3.1 Safety instructions

CAUTION - ELECTRICAL HAZARD
The operator or electrical installer is responsible for proper grounding and compliance with all applicable national and local safety regulations. Please see Power Supply Grounding and Earthing, page 14.

3.3.2 STO installation

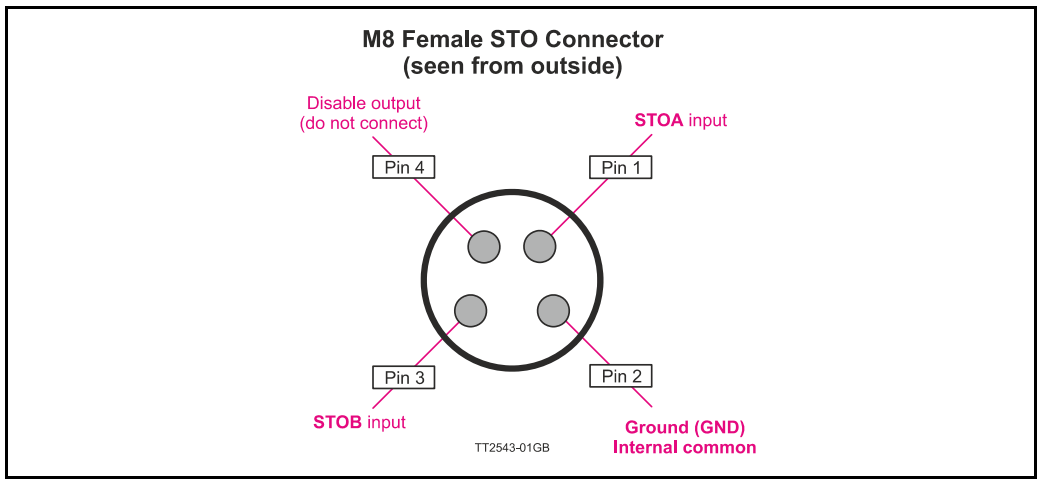
Installation must be in accordance with the following steps and must be carried out by competent personnel, see Qualified personnel, page 60. The Safe Torque Off option is intended to be part of the safety related control system. Before installation, perform a risk assessment that compares the Safe Torque Off option specifications and all foreseeable operational and environmental characteristics of the control system. A safety analysis of the machine section controlled by the drive is required to determine how often to test the safety function for proper operation during the life of the machine.

3.3.3 Enabling the STO function

NOTE: The MIS motors must be ordered with the STO option installed.
The STO option is enabled when the NON-STO plug is not inserted, please see Disabling the STO function, page 71 to learn more about the NON-STO plug.

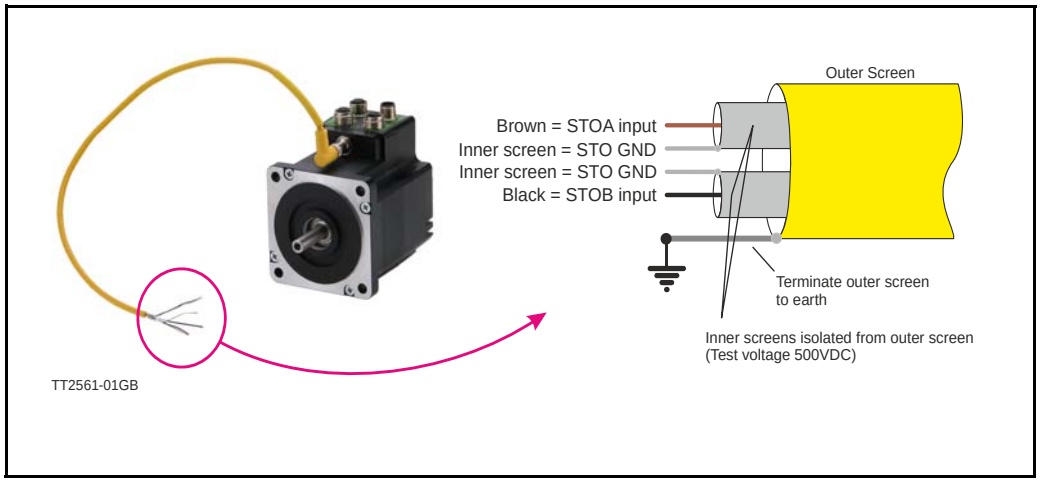
3.3.4 Cables and connectors

The STO connector contains the two enable inputs STOA and STOB. Both inputs must be applied nominal +24VDC in order to energize the motor and make any motor movement possible. STO-signals must originate from a safety isolating transformer in accordance with IEC 61558-1 and IEC 61558-2-6 or from a switch mode power supply with equivalent property. If only one of the inputs is not applied +24VDC the internal STO circuit will remove the energy from the motor. The illustration below shows the pinout of the connector. A 100 mA fuse must be inserted in each channel.



Use only the standard cable for the STO function: JVL stock no. **WI1010-M08M4V05P**.

The standard STO cable is yellow to signal “safety”, and by using this official cable, the disable output (pin 4) is not connected inside. If using another standard cable, pin 4 might be connected and therefore 24 V is inside the cable and could be a risk in safety applications.



3.3.5 Functional Proof tests

The functional safety standards require that functional proof tests be performed on the equipment used in the system. Proof tests are performed at user-defined intervals and are dependent upon PFD and PFH values.

IMPORTANT
The specific application determines the time frame for the proof test interval. Verify operation of safety function after drive installation, modification, or maintenance. Refer to for more information about how to test the safety function.

3.4.1 Safety instructions

CAUTION - ELECTRICAL HAZARD
The operator or electrical installer is responsible for proper grounding and compliance with all applicable national and local safety regulations.
Please see Power Supply Grounding and Earthing, page 14.

3.4.2 Activation of STO

The STO is activated by removing either signal STO_A, STO_B or both. In all 3 cases the STO will be active and the motor will not be energized.

3.4.3 Parameter settings for STO (auto./manual restart behavior)

AUTOMATIC RESTART
Automatic restart behavior is only allowed in 1 of the 2 situations:

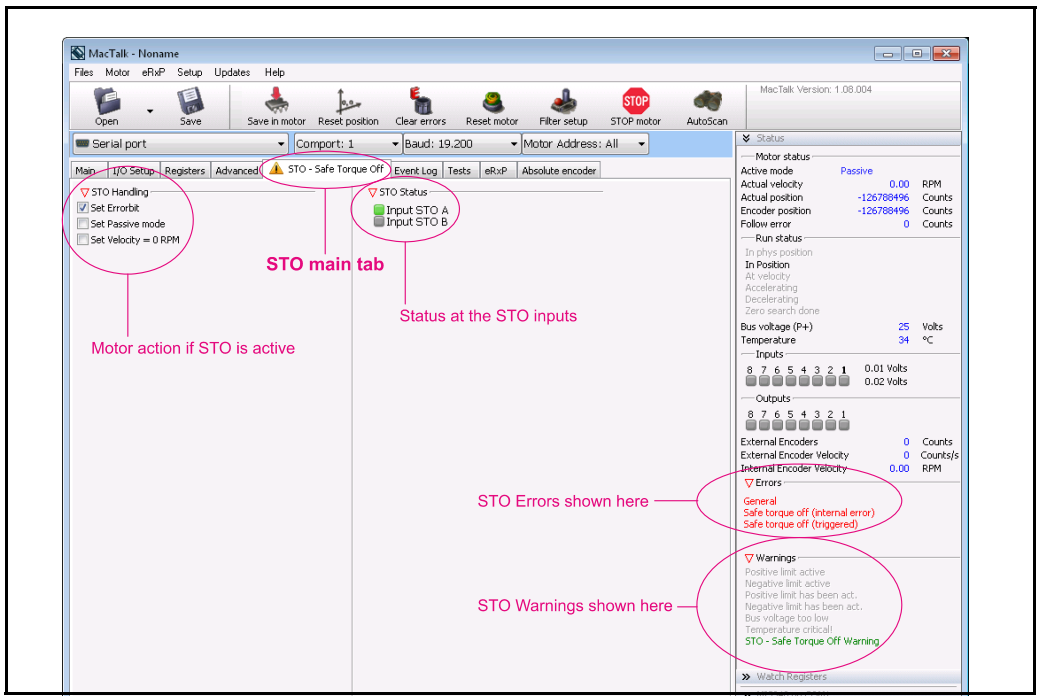
- The unintended restart prevention is implemented by other parts of the STO installation.
- A presence in the dangerous zone can be physically excluded when STO is not activated. In particular, paragraph 6.3.3.2.5 of ISO 12100: 2010 must be observed.

3.4.4 Operating the STO feature using MacTalk

If the motor has the Safe Torque Off option installed, The “STO – Safe Torque Off” tab will be shown in MacTalk.
The actual status of both channels can be monitored on this tab. When green, the channel is ON. Both channels must be ON at the same time in order to enable the motor.

When one or both of the channels are OFF, the Safe Torque Off is active and the motor is disabled. The motor will behave according to the settings made:

Below the STO tab in MacTalk.



3.4.5 Motor action if STO is active

Below a description of the 3 possible actions that can be done if the STO is activated. They refer to the screen dump above.

Set Errorbit
Default = OFF
The motor will set both the General (bit 0) and the STO (bit 29) error bit. To get the motor back in normal operation the STO channels must be ON, the error must be cleared and an active operation mode must be selected.

Set Passive mode
Default = ON
The motor will go to passive mode. To get the motor back in normal operation the STO channels must be ON and an active operation mode must be selected.

Set Velocity = 0 RPM
Default = OFF
The motor stays in the actual mode and the requested velocity will be set to 0 RPM. After the STO channels are ON, a velocity value (>0 RPM) must be written into the velocity register to get the motor moving again.

3.4.6 STO Error messages

2 error messages exist:

- **Safe torque off (triggered)**
  When the Safe Torque Off is or has been active and the **Set Errorbit** setting, the STO Error bit is set, and in MacTalk this can be monitored on the right status panel as **"Safe torque off (triggered)"**. The error will only be cleared by sending the "Clear errors" command.

- **Safe Torque off (internal error)**
  Will only be set if the STO self-diagnostic circuit has detected an internal error. In this case, the motor must be returned to the manufacturer (JVL) for repair. This error can not be cleared.

3.4.7 STO Warning messages

Warnings
When the Safe Torque Off is active, the STO Warning bit is set, and in MacTalk this can be monitored on the right status panel as "STO- Safe Torque Off Warning".

3.4.8 Safe Torque Off without using MacTalk

If MacTalk is not used for monitoring the status of the STO function it must be done as follows:

The motor contains a number of registers which can be accessed from various protocols depending on which options the motor has.
Protocols available are for example Ethernet (EthernetIP, PROFINET etc.) and CAN-open, Modbus or the MacTalk protocol.
The status of the STO function is also available using above protocols.

Each field in MacTalk described earlier in this chapter can be monitored/read from a register in the motor.

The registers that are relevant for the STO function are:

R25 STATUS_BITS — Status bits related to the STO function.
Note that other bits for many other functions in the motor are also represented in this register.

- Bit 23: Input status for the STOA input.
  Reading "0" means that the input is inactive (no voltage applied).

- Bit 24: Input status for the STOB input.
  Reading "0" means that the input is inactive (no voltage applied).

See also: *Status bits*, page 198

R35 ERROR_BITS — Error bits related to the STO function.
Note that other bits for many other functions in the motor are also represented in this register.

- Bit 27: STO_ALARM.
  Will be set if there is an internal hardware defect in the STO circuitry.

  Important
  The STO_ALARM will only be set if the STO self-diagnostic circuit has detected an internal error.
  In this case, the motor must be returned the manufacturer (JVL) for repair.

- Bit 29: STO - This bit will be set if one of the 2 STO inputs are off (not applied an voltage). Also STO is set if the STO_ACTION_ERROR bit is set.

See also: *Err_Bits*, page 201

R36 WARNING_BITS

Warning bits related to the STO function.
Note that other bits for many other functions in the motor are also represented in this register.

- Bit 9: STO Warning
  The STO warning bit is always set if one of the STO channels are off (no voltage applied to the STOA and/or STOB input)

See also: *Warn_Bits*, page 202

R124 SETUP_BITS

Setup bits related to the STO function.
Note that other bits for many other functions in the motor are also represented in this register.
If one or more of the following bits are set, the motor will behave as described when the STO function is activated:

- Bit 29:STO_ACTION_ERROR
  The motor will set both the General (bit 0) and the STO (bit 29) error bit.

- Bit 30:STO_ACTION_PASSIVE
  The motor will go to passive mode.

- Bit 31:STO_ACTION_V_ZERO
  The motor stays in the actual mode and the requested velocity will be set to 0 RPM.

See also: *Setup_Bits*, page 213

3.4.9 STO commissioning test

After installation and before first operation, perform a commissioning test of the installation, using STO. Perform the test again after each modification of the installation or application involving the STO.

NOTICE
A successful commissioning test of the STO function is required after the initial installation, and after each subsequent change to the installation.

To perform a commissioning test:

- Follow the instructions in chapter Restart prevention for STO application, page 70 for applications without automatic restart after a safe stop, or
- Follow the instructions in chapter Automatic restart of STO application, page 71 for applications with automatic restart after a safe stop.

3.4.10 Restart prevention for STO application

Application where SETUPBITS are set to default values STO_ACTION_ERROR=1, STO_ACTION_PASSIVE=0, STO_ACTION_V_ZERO=0:

1. Set the motor in an active mode where it runs at well-defined velocity.
2. Remove STO channel A.
3. Check that:
   - 3a The motor coasts until stop.
   - 3b If any monitoring is connected, then check that ERRORBIT 0 and 29 are set. If MacTalk is connected, it shows “Safe Torque Off – triggered”.
4. Reapply 24 V DC to STO channel A.
5. Verify that the motor remains stopped.
6. Clear the ERRORBITS either with MacTalk (“Clear errors” button”) or by sending command 97 to register 24.
7. Set the motor in the active mode.
8. Check that the motor runs at the defined velocity.

Repeat the procedure with STO channel B.

The commissioning test is successfully completed when all the given steps are passed.

3.4.11 Automatic restart of STO application

Application where SETUPBITS are set to STO_ACTION_ERROR=0, STO_ACTION_PASSIVE=0, STO_ACTION_V_ZERO=0:

1. Set the motor in an active mode where it runs at well-defined velocity.
2. Remove STO channel A.
3. Check that the motor coasts until stop.
4. Reapply 24 V DC to STO channel A.
5. Check that the motor runs at the defined velocity.

Repeat the procedure with STO channel B.

The commissioning test is successfully completed when all the given steps are passed.

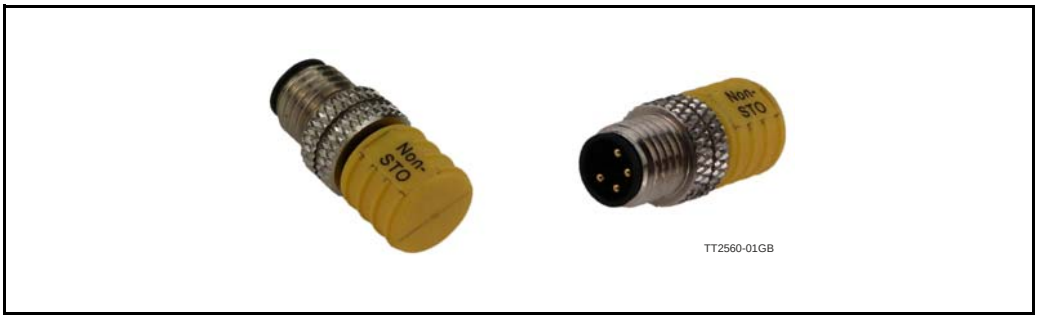
NOTICE
See the warning on the restart behavior in chapter Parameter settings for STO (auto./ manual restart behavior), page 65

3.4.12 Disabling the STO function

If the STO function is not needed the plug JVL type **WI1010-M08M4SSTO** must be inserted in the STO connector at the motor.

The reason for this external plug to disable the STO function is to obtain a high safety level and make sure that no misunderstandings will occur concerning whether the STO function is active or not.

Pictures of the 4 pin M8 plug



3.4.13 Service and maintenance

For PL e or SIL3, it is a must, for lower PL or SIL it is recommended to conduct a functional test every 12 months to detect any failure or malfunction of the STO functionality. To conduct the functional test, perform the following steps (or a similar method suitable for the application):

1. Remove the 24 V DC voltage supply from the STO A and B.
2. Check if the monitoring gives an error message.
3. Verify that the motor is coasting and comes to a complete stop.
4. Verify that the motor cannot be started by re-applying the 24 V DC to STO A and B.
5. Verify that the motor is not started automatically until errors are cleared and the motor is set in an active mode.

3.4.14 Capabilities

Safe Torque Off performs a safety function such that when one of the STO inputs is not active, (i.e. open-circuit or set at nominally 0V), the motor will not develop torque. The STO function is implemented purely in simple solid state hardware for which substantial failure data exists, allowing meaningful quantitative FMEA to be carried out. The function does not use software or complex hardware. The probability of failure of the safety function due to a hardware fault has been estimated by JVL Industri Elektronik A/S as 1,38e-10 per hour (IEC61508/IEC62061/IEC61800-5-2) or 4,29e-8 per hour (ISO13849), and assessed by the independent notified body TÜV NORD (pending). The input is compatible with self-testing digital outputs of controllers such as PLCs, where the test pulse is a maximum of 1 ms. This means that the drive is not disabled by logic-low input pulses with a maximum of 1 ms duration.

3.4.15 Limitations

- STO uses solid-state techniques, it does not provide physical separation of electrical connections and is not intended to provide electrical isolation.

- STO does not provide braking, it disables the motor so no motor electrical braking is available. If motor braking is a requirement then an external arrangement must be made to stop the motor conventionally and then to safely remove the STO inputs to activate STO. Braking by the drive is not a high-integrity function, if braking is a safety requirement then an independent fail-safe brake must be provided.

3.4.16 STO Technical Data

NOTICE : The STO signal must be SELV or PELV supplied.

European directives	Machinery Directive (2006/42/EC)	EN ISO 13849-1/2	
		EN IEC 62061	
		EN IEC 61800-5-2	
	EMC Directive (2014/30/EU)		
		EN 61000-6-3	
		EN 61800-3	
	Low Voltage Directive (2014/35/EU)		
		EN 61800-5-1	
Safety standards	Safety of Machinery	EN ISO 13849-1/2, IEC 62061, IEC 60204-1	
	Functional Safety	IEC 61508-1/2, IEC 61800-5-2	
Safety function		IEC 61800-5-2	IEC 60204-1
		Safe Torque Off (STO)	Stop Category 0
Safety performance	**ISO 13849-1**		
	Category	Cat 3	
	Diagnostic Coverage	DCavg: 98,5 % (Medium)	
	Mean Time to Dangerous Failure (per channel)	MTTFd: 100 years (High)	
	PFHd	4,29e-8/h	
	Performance Level	PLe	
	IEC 61508 / IEC 62061 / IEC61800-5-2		
	Safety Integrity Level	SIL 3, SIL CL3	
	Systematic capability (systematic integrity level)	SIL 3	
	Probability of Dangerous Failure per Hour	PFHd: 1,38e-10/h (High Demand Mode)	
	Diagnostic Coverage	DC: 96 %	
	Safe Failure Fraction	SFF: 96 %	
	Common Cause Failure Factor	CCF 5 %	
	Hardware Fault Tolerance	HFT: 1 (1oo2)	
	Proof Test Interval T1	20 Years	
	Mission time TM	20 Years	
Reaction time	Input to output response time	Maximum 8 ms.	
	Response time (internal fault)	Maximum 200 ms.	

The following temperature profile is used in safety value calculations:

- 1000 on/off cycles per year with T = 85 °C
- 85 °C board temperature at 100 % of time.
- The STO is a type A safety component as defined in IEC 61508-2.
- Relevant failure modes:
  1. The STO trips spuriously (safe failure)
  2. The STO does not activate when requested

The analysis is based on an assumption that one failure occurs at one time. No accumulated failures have been analyzed. The conclusion gives that no single dangerous failures can remain undetected, and therefore the motor will always go to safe state in case of one dangerous failure at a time.

- Reaction times are described in section STO function activation and indication response times in the table above.

3.5 Specifications and Certifications

Option

3.5.1 General specifications

Attribute	Value
Standards	EN 60204-1, IEC 61508, EN 61800-3, EN 61800-5-1, EN 61800-5-2, EN 62061, EN ISO 13849-1
Safety category	Cat. 3 and PL e per EN ISO 13849-1; SIL CL3 per IEC 61508 and IEC 62061
Power supply (user I/O)	24V DC ±10%, 0.8…1.1 x rated voltage PELV or SELV
STO A	24 V DC, max. 10 mA
STO B	24 V DC, max. 10 mA
STO input ON voltage, min	5 V
STO input OFF voltage, max	2 V
STO input **absolute max** rating	60 V
Conductor type	Multi-conductor shielded cable
Conductor size	24 AWG
Strip length	10 mm

3.5.2 Environmental specifications

The installation must comply with all environmental, pollution degree, and drive enclosure rating specifications required for the operating environment.

Category		Specification
Ambient temperature		0…40 °C
Storage temperature		-40…70 °C
Relative humidity		5..93 % non-condensing
Shock		15 g, 30ms. (EN/IEC 60068-2-27)
Vibration		5 - 25 Hz: ±1.6mm, 25 - 500Hz: 4 g, 1.0 oct./min. (EN/IEC 60068-2-6)
Surrounding environment		The ingress protection (IPxx) depends on the specific motor type number. Please see Ordering information, page 353
EMC	Emission	IEC61800-3 (Category 2)
	Noise immunity	IEC61000-6-2

ATTENTION:
Failure to maintain the specified ambient temperature can result in a failure of the safety function.

3.5.3 Certifications

Certification	Value
TÜV	Certified by TÜV NORD for Functional Safety: up to SIL CL3, according to IEC 61800-5-2, IEC 61508, and EN 62061; up to Performance Level PLe and Category 3, according to EN ISO 13849-1; when used as described in this User Manual.