Catalog

Version Change Log

Date	Version	Content
2023- 10	V1.0	First version released

SD700-STO Safety Torque Off

1. Safety Standards and Regulations

Safety standards

Item	Reference
Safety function	EN/ISO 13849-1: 2021 EN/IEC 61508: 2010, Parts 1-7 EN/IEC 62061: 2021 EN/IEC 61800-5-2: 2017
EMC	EN/IEC 61326-3-1: 2017

Safety parameter

Item	Parameter
SIL (Safety integrity level)	SIL3
PFH (Average frequency of dangerous failure per hour)	7.60×10-10[1/h]
PL (Performance level)	PLe/Cat.3
MTTFD (Mean time to dangerous failure)	High
DC (Average diagnostic coverage (%))	Medium
Service life	20 years
HFT (Hardware fault tolerance)	1
Response time	5ms

Note

To meet the requirements of SIL3/PLe/Cat.3, the servo drive must trigger the STO function at least once every three months for troubleshooting.

2. Safety Function

2.1 STO Description

Safety Torque Off (STO) is a safety function in accordance with IEC 61800-5-2: 2016. It is integrated in the VEICHI SD700-EA/NA/PA drive.

STO disables the PWM gate signal of the drive to close the output of the power devices and cut off the motor torque, making the motor safely enter a torque-free state and preventing accidental start-up. When the STO function is activated, if the motor is running, it will stop freely.

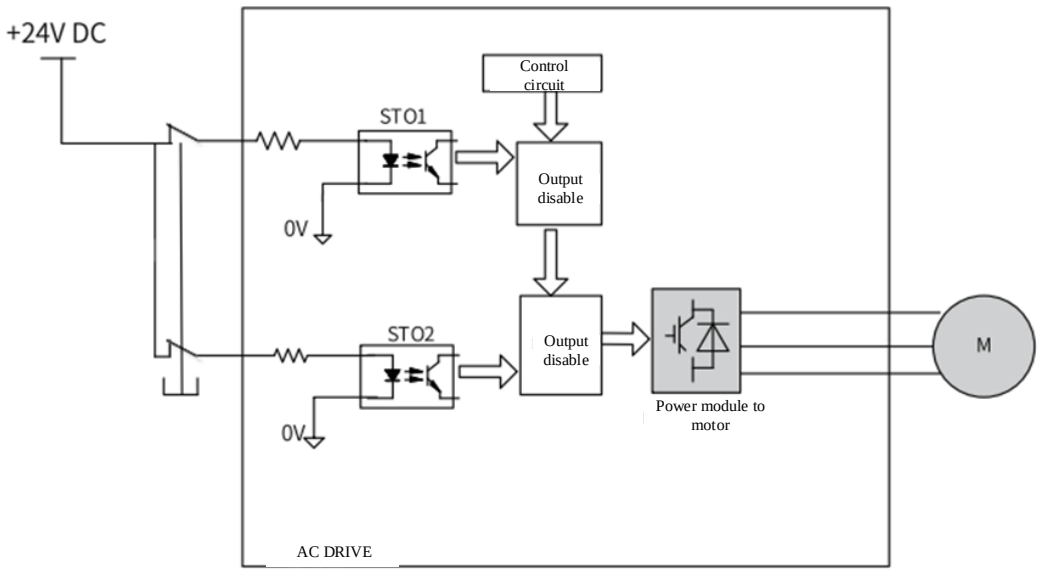
The STO function blocks the PWM signal output to the power device through external redundant hardware terminals STO1 and STO2, thus preventing the motor from moving.

STO1 and STO2 terminal input signals must both be active (high or set to "1") to enable the drive to operate properly.

STO functions are as follows:

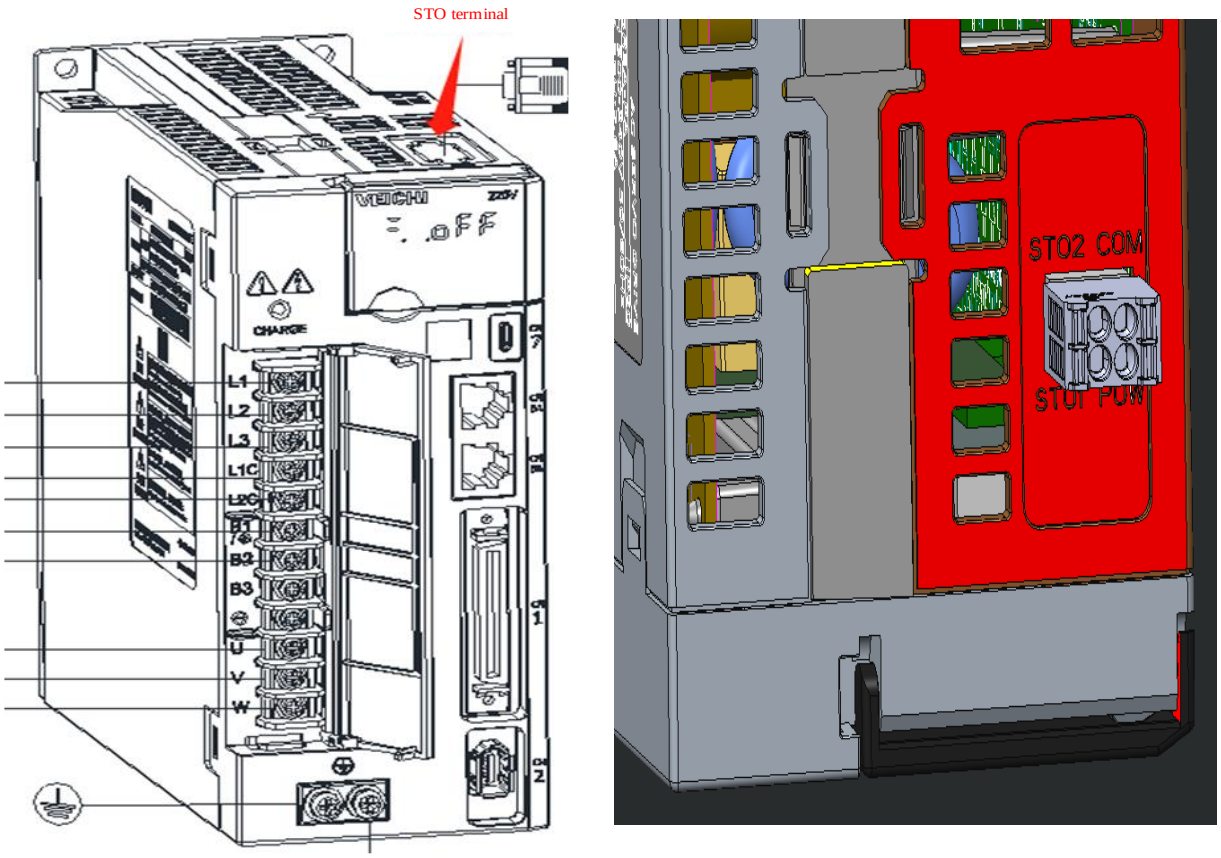
STO1	STO2	PWM Output
High	High	Normal
Low	High	Disable
High	Low	Disable
Low	Low	Disable

The diagram of STO circuit is shown in the following figure:



2.2 STO Terminal Wiring

STO terminal are shown in the figure below:



Definition	Description
COM	STO reference ground
POW	Internal power supply
STO1	STO1 input
STO2	STO2 input

Configure two separate inputs for the STO function: STO1/STO2.

In order to be more user-friendly during debugging, the pin of power supply voltage (+ 24V) is added. If the safety circuit is installed, but the STO function is not required, STO1/STO2 needs to be connected to 24V.

The electrical characteristics of the safety request input signal are as follows:

Item	Characteristic
Voltage range	24VDC(±10%)
Input current	7mA
DI resistance	4KΩ

Diagram of wiring with external 24V power supply:

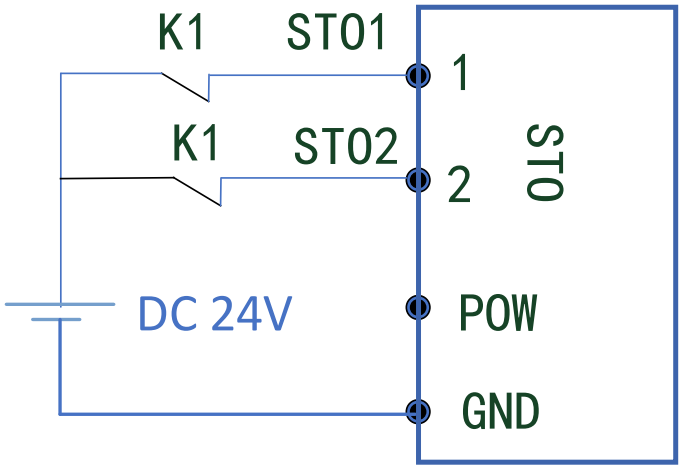
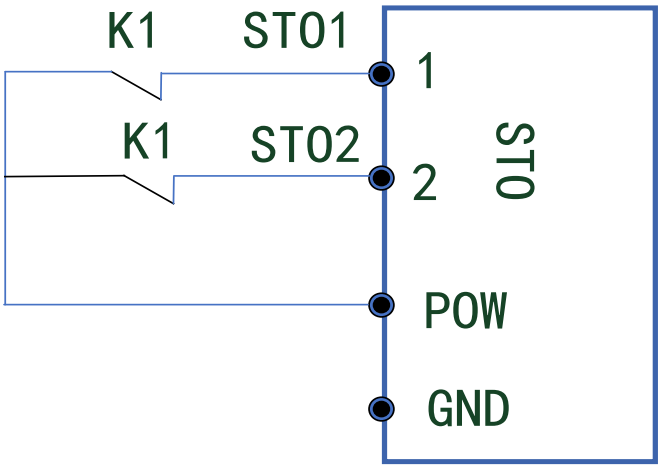


Diagram of wiring of internal power supply:



Note

- When users use the STO function, it is recommended to use twisted pair, due to its stronger immunity.
- When using an external 24V power supply, please do not connect the 24V power supply to

the POW terminal, otherwise the STO function will fail.

2.3 STO Alarm Description

When the STO terminal is disconnected, report Er.7AA or AL.9F1, please check whether the STO terminal is disconnected. Or please check Bit8, Bit9 and Bit14 of Un230 (Bit8: STO2 disconnection, Bit9: STO1 disconnection and Bit14: STO disconnection at the same time). When the STO terminal is connected, Bit8, Bit9 and Bit14 will be 0 or it will report Er.7AA and needs to be re-powered. If there is any fault during repower, please contact the manufacturer.

Parameter description: PnE0D

Function of bit5:

- 0: Manual reset of STO disconnection fault.
- 1: Auto reset of STO disconnection fault.

Function of bit6:

- 0: Report fault when STO is not enabled
- 1: Report warning when STO is not enabled

Note: Bit13 (STO Output Failure Alarm) of Un231 should be checked when the fault is reset. If it is set to 1, then fault can’t be reset.

STO fault is shown in the following table:

Fault code	Bus code	Name	Remark
Er.7AA	0x6021	STO fault	Report STO alarm, please check Un230, Un231 for details (Category 1 Alarm)

STO warning is shown in the following table:

Fault code	Bus code	Name	Remark
AL.9F1	0x09F1	STO warning	Report STO disconnection warning, please check Un230, Un231 for details.

2.4 STO Monitoring

Un230 is STO_L, and its Bit8 indicates STO2 disconnection fault; Bit9 indicates STO1 disconnection fault; Bit14 indicates the communication fault code 1; Bit8, Bit9, and Bit14 indicate resettable fault, and others are not, see the table below for details.

Name	Bit	Remark
Un230 STO_L	Bit0	Channel 1 optocoupler error
	Bit1	Channel 2 optocoupler error
	Bit2	Channel 1 inverter error
	Bit3	Channel 2 inverter error
	Bit4	Channel 1 buffer error
	Bit5	Channel 2 buffer error
	Bit6	Reserved
	Bit7	Reserved
	Bit8	Channel 2 error
	Bit9	Channel 1 error
	Bit10	PWM signal block
	Bit11	Comparator undervoltage/power down
	Bit12	ADC sampling circuit power down
	Bit13	Watchdog reset pin RST power down
	Bit14	24V emergency stop button disconnection (resettable)
	Bit15	Reserved

Un231 is STO_H, where Bit8 is STO undervoltage or program out of control; Bit9 means STO hardware not supported; Bit13 means STO output fault 1; Bit14 is a hardware signal block; l; Bit15 means STO monitoring off/on; Please refer to the following table for details.

Name	Bit	Remark
Un231 STO_H	Bit0	CPU detection error
	Bit1	RAM detection error
	Bit2	FLASH detection error
	Bit3	STACK detection error
	Bit4	Reserved
	Bit5	Reserved
	Bit6	Reserved
	Bit7	Reserved
	Bit8	When overvoltage and undervoltage is detected on +5V or when the program operation is out of control, STO reports to the general control board (0: abnormal; 1:normal)
	Bit9	hardware not supported, set control board hardware to (0: hardware not supported, 1: hardware supported)
	Bit10	Communication timeout, MCU module detects RXD signal of STO
	Bit11	Reserved
	Bit12	Reserved
	Bit13	STO output error
	Bit14	Hardware signal block

	Bit15	STO function off (0: OFF, 1: ON) (for monitoring)

2.5 STO Reset

Abnormal operation refers to drive starting, initialization, and STO exit.

During MCU initialization, the MCU disables the PWM buffer by setting the enable pin to 1, thus disabling the PWM signals. Until the initialization phase is completed, the MCU will set the enable pin to 0, the PWM buffer is enabled, and the servo drive operates normally.

When the servo drive system enters the safe state through STO, it can exit when the following conditions are met at the same time, and the normal operation can be resumed after the drive is reset.

1. The request input status of STO must be "1".
2. Servo drive starting or operation command must be invalid.
3. There are no dangerous faults.

Fault reset process goes as follows: connect STO terminal, auto detects that Bit13 of Un231 is 0, and auto resets the drive fault.

3. Commissioning, Operation and Maintenance Requirements

3.1 Basic Requirements

Technicians must be trained to understand the requirements and principles of safety-related system design and commissioning.

Operation and maintenance personnel must be trained to understand the requirements and principles of safety-related system design and commissioning.

Operators must be trained to understand the requirements and principles of safety-related system design and commissioning.

If the safety-related circuits on the control board do not work, a new control board must be replaced.

3.2 Test Operation Procedures and Acceptance Checklist

Start-up Test and Verification

The final assembler verifies the operation of the safety functions by means of acceptance tests in accordance with IEC 61508, EN/IEC 62061 and EN ISO 13849.

The stages below must pass the acceptance tests:

- When the safety function is initially started.
- When any changes related to safety functions (wiring, components, settings, etc.)are changed.
- When any maintenance work related to safety functions is completed. Acceptance tests of safety functions must be carried out by personnel with professional knowledge of safety functions. And the tests must be recorded and signed by the testers.

Procedure and Check

The signed acceptance test reports must be kept in the log. And it should include documentation of start-up activities and test results, reference to fault reports and troubleshooting. Any new acceptance tests due to changes or maintenance shall be also recorded in the log.

Step	Method	Result
1	Ensure that the drive is free to run and stop during debugging.	
2	Stop the drive (if running), turn off the input power, and isolate the drive from the power cord by a circuit breaker.	
3	Check the STO circuit connection according to the circuit diagram.	

4	Close the circuit breaker and turn on the power supply.	
5	When the motor stops, test STO signal # 1: Set STO1 and STO2 to H Issue the drive stop command (if running) and wait for the motor shaft to stop Trigger the STO function by disconnecting (under low state or open loop) STO input signal # 1 and issue a start command for the drive. Ensure that the motor remains still and the drive displays "ER7AA"	
	Set STO1 to "H" to disable the drive's ON/RUN command, then drive is automatically restarted, and the drive's ON/RUN command is enabled again. Please check whether the motor is running properly.	
	When the motor stops, test STO signal # 2: Set STO1 and STO2 to "H". Issue the drive stop command (if running) and wait for the motor shaft to stop Trigger the STO function by disconnecting (under low state or open loop) STO input signal 2 and issue a startup command for the drive. Ensure that the motor remains still and the drive displays "ER7AA"	
	Set STO2 to "H" to disable the drive's ON/RUN command,then drive is automatically restarted, and the drive's ON/RUN command is enabled again. Please check whether the motor is running properly.	
6	When the motor is running, test STO channel # 1: Set STO1 and STO2 to "H". Start the drive and make sure the motor runs Trigger the STO function by disconnecting (under low state or open loop) STO input signal # 1 Make sure the motor stops and the drive trips. Reset the fault and try to start the drive. Ensure that the motor remains still and the drive displays "ER7AA"	
	Set STO1 to "H" to disable the drive's ON/RUN command, then drive is automatically restarted, and the drive's ON/RUN command is enabled again. Please check whether the motor is running properly.	
	When the motor is running, test STO channel # 2: Set STO1 and STO2 to "H". Start the drive and make sure the motor runs	

	Trigger the STO function by disconnecting (under low state or open loop) STO input signal # 2 Ensure that the motor stops and the drive trips Reset the fault and try to start the drive. Ensure that the motor remains still and the drive displays "ER7AA"	
	Set STO2 to "H" to disable the drive's ON/RUN command, then drive is automatically restarted, and the drive's ON/RUN command is enabled again. Please check whether the motor is running properly.	
7	Record and sign the acceptance test reports to prove that the safety function is safe and can be put into operation.	

4. Preventive Measures

4.1 Safety Protection Measures

When this function, please carefully read the following important precautions and follow them carefully:

- The STO function is not a substitute for the emergency stop. If other measures are not taken, the power supply cannot be cut off in case of emergency, and the strong electric parts of motors and drivers are still charged, so there is the risk of electric shock or other risks caused by electricity. Therefore, the maintenance of electrical parts of the drive or motor can only be carried out after the drive system is isolated from the main power supply.
- STO may be used as a part of an emergency stop system depending on the standards and requirements of a particular application. But it is mainly used for safety controls dedicated to preventing hazards from occurring instead of emergency stop.
- Emergency stop function is often used in machines to enable operators to take actions to prevent accidents in face of accidents.
- Emergency stop requirements are different from those of safety interlock. Generally speaking, the emergency stop function requires independence from any complex or intelligent control. It may use purely electromechanical devices, either cutting off the power supply or using other means (dynamic braking or regenerative braking) for rapid shutdown control.
- Professional knowledge is required to design safety-related systems to ensure the safety of a complete control system, the whole system should be designed according to the safety principles. Safety torque-off function for some sub-systems, although intentionally designed for safety-related applications, does not ensure the safety of the entire system.
- In case of emergency stop, the safety torque off function can be used to stop the drive.
- It is recommended not to use STO function to stop the drive in the processes without personal protections. If stop a running drive by STO, the drive will gradually stop.

4.2 Risk Assessment

- When using safety functions, it is necessary to conduct risk assessment of servo system in advance. to ensure compliance with standard safety integrity levels.
- Even when STO is on, risks may still exist. Therefore, security must always be considered when making risk assessment.
- If external forces (such as gravity perpendicular to the axis) are applied during the operation of the safety function, the motor will rotate due to these external forces, so it is necessary to provide a separate mechanical brake to fix the motor.
- In the event of multiple IGBT power tube failures, the servo drive generates an alignment torque so that whether or not the STO function is enabled, which may cause the motor shaft to rotate in a maximum range of 180 ÷p (180 ÷2p if synchronous reluctance motors).
- p: Motor pole pair no.
- Safety Torque Off (STO) only cuts off the torque of the motor but it does not cut off the power supply to the servo drive/inverter. When overhauling the servo drive/inverter, please cut off the power supply and confirm that the servo/inverter is dead.