STO circuit manual

Hardware STO implementation in

RoboteQ motor controllers

Revision: 13

Table of contents

1. Revisions of this document:

Revision	Author	Date	Description
01	Kostas Andriotis	02.04.2019	First draft
02	Kostas Andriotis	03.04.2019	Added CH 14, minor changes
03	Kostas Andriotis	04.04.2019	Added !STT command, Added STO levels Minor changes
04	Kostas Andriotis	22.04.2019	Added Constraints when using STO section, minor changes
05	Kostas Andriotis	30.04.2019	Added missing info from FMEDA
06	Kostas Andriotis	07.05.2019	Added release table. Minor changes
07	Kostas Andriotis	09.05.2019	Changes after requirements from auditor
08	Kostas Andriotis	29.11.2019	Added mosfail detection test
09	Kostas Andriotis	06.12.2019	Minor fixes
10	Kostas Andriotis	13.12.2019	Added attention notice for latest firmware to use
11	Kostas Andriotis	17.02.2020	Shorted Mosfets test added
12	Kostas Andriotis	01.06.2020	Shorted Mosfets maintenance test added
13	Kostas Andriotis	11.06.2020	Fixed shorted mosfet test sequence. Deleted release table and company information

2. Scope

This STO manual is the original instruction about the STO circuitry that is implemented in RoboteQ's motor controllers. Describes how the implemented circuit works and how the signals are processed/tested by MCU. Also includes maintenance instructions and commands along with the all the technical data for RoboteQ's STO implementation.

3. Motor controllers

The STO function will be integrated in RoboteQ's motor controllers with STO hardware implementation.

ATTENTION

STO firmware implementation is supported with firmware v2.0 or later. End user need to update to the latest available version. It is also recommended to use the latest version of Roborun+ utility. Please check www.roboteq.com for updates.

4. Safe Torque Off (STO)

Safe Torque Off is a safe method for switching controller in a state where no torque is generated, regardless whether the controller is operating normally or is faulty. This function is a mechanism that prevents the drive from restarting unexpectedly. STO has the immediate effect that the drive cannot supply any torque-generating energy. STO can be used wherever the drive will be brought to a standstill in a sufficiently short time by the load torque or friction or where coasting down of the drive is not relevant to safety. STO enables safe working and has a wide range of use in motion control/ systems with moving axes. The advantage of the integrated STO safety function compared with standard safety technology using electromechanical switchgear is the elimination of separate components and the effort that would be required to wire and service them. Because of the rapid electronic switching times, the function has a shorter switching time than the electromechanical components in a conventional solution.

WARNING

Activating STO does lead to no more torque generation on the motor. The motor will not be actively stopped but run out. It might be possible that the load is turning the motor (e.g. hanging axis). If this can lead to hazards further measures need to be taken (e.g. break). In case of a multiple fault in the power stage a rotation might occur.

5. Safe Torque Off (STO) on Roboteq Controllers

Two digital inputs on the user I/O connector can be used to put the controller in a state where the motor is deprived of energy.

The two inputs, labeled STO1 and STO2 must both be brought and maintained at a logic level 1 for the controller to be active. If any one or both of these lines are at 0, the output is de-energized.

The STO circuit operates independently of the MCU. It will always override the MCU, whether the MCU is processing normally, or is in a hardware of firmware fault condition.

The STO circuit works by controlling the voltage supply to the controller's output MOSFET drivers. When both STO1 and STO2 are at logic 1 level, MOSFET drivers are supplied with power. When either

or both STO1 and STO2 are at logic level 0, the MOSFET driver power is cut, and the MOFETs gates can no longer be above the ON threshold level, regardless of the MCU activity.

Accordingly, the STO circuit is built with redundancy and will continue to function if any one component is faulty, anywhere in the STO circuit or elsewhere in the controller.

6. Activating STO

By factory default STO is disabled. It must be enabled by removing the jumper located on the controller's PCB (depends on model – check datasheet). STO is activated by removing power (logic level 0) to both STO inputs. In order for controller to monitor STO state, this function must be activated through Roborun+ Utility or serial command (check command section). The controller will immediately stop generation of torque in the motor. Hardware STO functionality is only available in the T version of the controller.

7. Deactivating STO

STO is deactivated by applying a voltage (logic level 1) to both STO inputs. After this, a new start/motor command has to be given to turn the motor. It can be disabled by connecting the jumper located on the controller's PCB. After that, user should disable the function through Roborun+ Utility or serial command (check command section).

8. Constraints when using STO

- All voltages attached to the controller need to fulfil SELV or PELV requirements.
- After first installation and at least every 3 months the tests as described in this manual have to be conducted.

9. FAILURE MESSAGES

In case a failure is detected in the STO implementation the following failure message will be visible according on how the user operates the controller.

1- Status LED on Controller
The status LED pattern will be the below in case of STO failure

2- STO Fault LED at Roborun+ utility in failure

This failure can have several internal and external reasons. If the failure is shown, please check the cabling and the signals to STO 1 and STO 2. Both signals much have at all times the same level.

- Check that the STO jumper is set correctly and STO is configured correctly
- Check wiring
- Check cabling for short circuits or open circuits

3- Mosfail LED at Roborun+ utility in Mosfet failure

If the failure persists, contact Roboteq support.

WARNING

Same status LED pattern is used for undervoltage and overvoltage faults and that should not be confusing. If STO fault appear it is normal for the controller voltage to be off and undervoltage fault to trigger. Either way this Status LED pattern indicates a situation that should be treated with caution.

10. STO Firmware implementation

The STO circuit will operate regardless of the MCU activity. However, when operating normally the MCU will perform the following functions:

1. Self-test that the STO circuits and switches are functional. This is done every time the controller is powered on. It can also be done at any time during the controller from external user commands from the system's PC or PLC (check command section). The self-test can also be initiated by the controller itself using its scripting language, at periodic time intervals, or any other user-define rule(s).

   If the self-test fails, the controller will stop driving the MOSFETs and set a fault flag that can be monitored by the PLC/Computer. It can also activate one of its digital outputs to indicate the fault.

2. The STO inputs are monitored continuously every 1ms. If one or both STO inputs are at level zero and the MOSFET driver supply voltage has not dropped, an STO fault is detected. The STO fault flag is set. A user digital output can be activated to indicate the fault.

11. Mosfet Failure Detection Firmware implementation

In order to support STO in RoboteQ brushed motor controllers Mosfet failure detection mechanism is implemented. This way the MCU at every startup will trigger and test each of the Mosfets on the output circuit and identify if they are operating normal or they are shorted. This test is applicable for all RoboteQ controllers that have firmware v2.0 or later. In case of fault/shorted Mosfet, fault is indicated.

ATTENTION

Mosfet Failure test is performed during boot of the controller (< 1sec) and before any power output to Mosfet. This way, if error occurs controller protect the system and stop operation fast enough so that no further damaged happens.

12. STO Commands

STO – STO enabled

Description:

Configure this parameter in order to enable the STO functionality.

Syntax Serial: ^STO nn
~STO
Syntax Scripting: setconfig(_STO, nn)
Number of Arguments: 1

Argument 1: STO Status
Type: Unsigned 8-bit
Min: 0 Max: 1
Default: 0

Where:
nn = STO status
0: Disabled.
1: Enabled.
Example:
^STO 1: Enable STO functionality.

STT – STO Self-Test

Description:

With this command the STO Self-Test/Mosfet failure test process is executed in order to check whether there is a fault. This process is applicable only on motor controllers with latest firmware v2.x installed. The result of the test is returned automatically. In case of fault the Respective STO Fault bit in the Fault Flags is set. The fault is triggered when:

- Any of the transistors or other component of the STO circuit is damaged.
- The respective jumper is placed on the board.
- Only one of the two STO input is set to high.
- Any of the power Mosfets is shorted

Syntax Serial: !STT

Syntax Scripting: setcommand(_STT, 1)
Number of Arguments: 0

STT – STO Self-Test Result

Description:

Returns the status of STO or the result of the latest executed STO Self-Test process after !STT command. This process is applicable only on motor controllers with latest firmware v2.x installed.

Syntax Serial: ?STT

Argument: None

Syntax Scripting: result = getvalue(_STT, cc)

Where:
cc =
1: STO state
Reply:
STT=ff Type Unsigned 8-bit Min: -1 Max: 5
2: Mosfet fail
Reply:
STT = f1 + f2*2 + f3*4 + ... + fn*2^n-1 Type: Signed 32-bit Min: 0 Max: 65535

Where ff=
-1: The test is in process or not applicable
0: Test successful
1: STO1 failed the test
2: STO2 failed the test
3: Test failed using input values
4: Test passed using input values, but cannot continue test since STO is triggered.
5: Mosfet failure

And:
f1 = U1 top fault
f2 = U1 bottom fault
f3 = V1 top fault
f4 = V1 bottom fault
f5 = W1 top fault
f6 = W1 bottom fault
f7 = U2 top fault
f8 = U2 bottom fault
f9 = V2 top fault
f10 = V2 bottom fault
f11 = W2 top fault
f12 = W2 bottom fault

13. Installation – Maintenance

STO Installation test

The STO circuit needs to be tested before first installation and at least every 3 months according to the below sequence:

1. Activate STO (both logic level 0)
2. Check that STO is active (through Roborun+ Utility/Serial)
3. Check that there is no STO fault present (through Roborun+ Utility/Serial)
4. Deactivate STO 1 and STO 2 (both logic level 1)
5. Check that STO is not active and that there is no STO fault present (through Roborun+ Utility/Serial).

Mosfet Fail detection test (optional)

This test can be performed to validate mosfet detection proper operation:

1. Check that ~ZSRM value is a positive number (through Roborun+ utility/Serial)
2. Power off controller
3. Short U phase and GND and boot controller
4. Check that error is correctly detected according to STT result
5. Remove short and reboot controller
6. Check that no error is detected
7. Repeat steps 2-5 with all phases and shorting also to Vmot. Each time, check for the correct error detection reading

Controller should be restarted at least once per 3 months to test the Mosfet fail detection.

SAFETY INSTALLATION

It is required that the controller has to be placed in an enclosure that can provide IP54 protection.

SAFETY REGISTRATION

It is required that STO end user should follow up www.roboteq.com and register to site/forum for any news about safety function.

14. STO Voltage source specification attention

In order to have maximum response at STO implementation, user/installer/integrator should use voltage source with low output capacitance. In any other case, latency in activation might occur.

15. Compliance and Safety Metrics

The STO function is compliant to:

- IEC 61800-5-2:2007, SIL 3
- IEC 61508:2010, SIL 3
- IEC 62061:2005, SIL 3
- ISO 13849-1:2015, Category 3 Performance Level e

Metric acc. To IEC 61508, IEC 61800-5-2, IEC 62061	**Value**
SIL	Up to 3
PFH	5 FIT
Mission Time and Proof Test Interval	20 years
Performance Level	e
Category	3
$MTTF_D$	>100 years

16. Technical Data

Specification	**Value**
STO Input High Level	6V to 30V
STO Input Low Level	0V to 1V
STO Response Time	< 5msec
Operating Temperature	-20°C to 55°C
Storage Temperature	-20°C to 70°C
IP degree	IP40
Humidity	5% to 95% non-condensing
Maximum altitude	2000m
STO cable length	≤ 3m (1)
EMC immunity	According to IEC 61800-3:2017 and IEC 61800-5-2:2007 Annex E
CE Declaration of conformity	Available at www.roboteq.com
(1) All connected cables must have length <3m	