



Functional Safety on ACCURET+ family

User's Manual

THIS PAGE IS INTENTIONALLY LEFT BLANK

Table of contents

1	Introduction.....	7
1.1	General safety information.....	7
1.2	Functional Safety availability.....	7
1.3	Certified safety functions.....	7
1.4	Proper and intended operation.....	8
1.5	Personnel qualification.....	8
1.6	Safety information for various life phases of the controllers.....	9
2	Directives and standards.....	10
2.1	Basic guidelines.....	10
2.2	Basics for Functional Safety certification.....	10
3	Safe Torque Off (STO) implementation.....	12
3.1	SIL and target failure measures.....	12
3.2	Dual channel architecture.....	12
3.3	Circuit description.....	13
3.4	Interfaces.....	15
3.5	Activation of Functional Safety.....	15
3.6	Configuration example.....	15
3.7	Use duration.....	16
3.8	Response time.....	16
3.9	User-supplied diagnostic.....	16
3.10	Limits of the safety-related architectures.....	17
3.11	Fault exclusions.....	17
3.12	Remaining risks.....	18
3.13	Safety-related operating modes.....	18
3.14	Safety-related hardware signals.....	18
3.15	Non-safety related firmware signals.....	18
3.16	Bypass of Functional Safety.....	19
4	Integration into a safety system.....	20
4.1	Integration requirements.....	20
4.2	Operating and environmental requirements.....	20
5	Testing.....	22
5.1	Complete acceptance test.....	22
5.2	Acceptance test of series-manufactured machines.....	22
5.3	Test intervals.....	22

6	Service and support.....	23
----------	---------------------------------	-----------

Record of revisions

Version	Date	Main modifications
Ver. 1.0	10.03.23	First version

Associated documentation

- | | |
|---|--|
| ■ Functional Safety User's Manual: | Functional Safety implementation |
| ■ ACCURET+ Operation & Software Manual: | ACCURET+ setup, use and programming manual |
| ■ ACCURET+ Hardware Manual: | Specifications & electrical interfaces |

NOTICE

- The content of the present manual is applicable only to ACCURET+ controllers that mention the Functional Safety feature in their corresponding "Hardware Manual". Please contact ETEL or authorized distributors to obtain the latest version of the documentation.



The Safe Torque Off (STO) function described in [§2.2](#) has been successfully tested and evaluated as part of ACCURET+ controllers listed in [§1.2](#).

Acronyms

CCF	Common Cause Failure.
Control system	Terminology from the IEC 61508-4 standard. System that responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner. The EUC control system includes input devices and final elements.
DC	Diagnostic Coverage.
EUC	Equipment Under Control. This document adopts the terminology from the IEC 61508- 4 standard. This general term indicates any equipment, machinery, apparatus or plant that is controlled through a control system.
FS	Functional Safety.
FW	Firmware.
HFT	Hardware Fault Tolerance.
MTTFd	Mean Time to Dangerous Failure.
PELV	Protective Extra Low Voltage.
PFH	Probability of Failure per Hour.
PL	Performance Level according to ISO 13849-1.
PLC	Programmable Logic Controller.
PLr	Required Performance Level according to ISO 13849-1.
SELV	Separated Extra Low Voltage.
SFF	Safe Failure Fraction.
SPLC	Safety-related PLC.
(S)PLC	Indicates either a PLC or a SPLC, depending on the context.
STO	Safe Torque Off.
SW	Software.
System	A system is a general term that indicates the combination of an EUC, a control system and any other part that is shipped with a product.
User	The term 'user' is used in this manual to indicate the person or company that integrates or uses the controller within a safety system. Alternative terms, depending on the use context, are EUC manufacturers, machine integrators, service engineers, etc.



- Signals a danger of electrical shock to the operator. Can be fatal for a person.



- Signals a danger for the controller and the power supply. Can be destructive for the material. A danger for the operator can result from this.



- Indicates electrostatic discharges (ESD), dangerous for the controller and the power supply. The components must be handled in an ESD protected environment.

1 Introduction

This manual provides information about the Functional Safety features related to the ACCURET+ controllers (also called “controller” in this document).

- The following topics are covered in this document: Information about safety;
- List of safety functions implemented in the controller and illustration of their use;
- Requirements for the integration of the controller into a safety system.



- The user must have read and understood this documentation as well as those listed in ["page 5"](#) before carrying out any operation on the system. ETEL S.A. disclaims all responsibility for accidents and damages if it is not done. Please contact ETEL S.A. or authorized distributors in case of missing information or question regarding the installation procedures, safety or any other issue.
-

1.1 General safety information



- The user must ensure that moving parts cannot be set in motion dangerously due to external forces such as gravity, remaining inertia, shock, vibrations, contact with other moving parts, etc.
 - Please note that faulty wiring or assembly, defective component(s), external force(s), and/or damage(s) may lead to inadvertent movements of the EUC parts.
 - Work on electrical components can be performed by qualified personnel. The minimum qualifications in accordance with this manual are described in [§1.5](#).
 - For judging the behavior of an EUC, the user needs to have fundamental knowledge about all the elements belonging to the control of the EUC (drives, inverters, controls and encoders). Inappropriate use may cause considerable damage to persons or property. ETEL does not accept any responsibility for direct or indirect damage caused to persons or property through improper use or incorrect operation of the EUC.
-

1.2 Functional Safety availability

The Functional Safety features documented in this manual are applicable to ACCURET+ controllers mentioning the Functional Safety feature in their respective "Hardware Manual".

1.3 Certified safety functions

- Safe Torque OFF (STO)



ETEL only assumes responsibility for the safety functions stated and described in this manual. Functional safety can reduce the inherent risks of EUC. However, it is impossible to implement safety measures that ensure 'the zero risk' when using an EUC.

In order for functional safety to take effect, the user must do the following:

- Verify the theoretical and actual setup of the EUC, the necessary (S)PLC programs and the system-parameter settings with a thoroughly documented acceptance test. This acceptance test must be performed by qualified personnel.
- Thoroughly understand the information contained in this manual and other documentation for the control and other electronic components being used (such as inverters and motors), as well as understand and enforce the safety instructions, constraints and relevant standards.
- Draw up a risk analysis, as required by the relevant machinery directive.
- Implement all measures deemed necessary based on the risk analysis of the system. These measures may be implemented as a part of Functional Safety, or with other suitable equipment or procedures. All measures must be validated.

1.4 Proper and intended operation

The controllers are not designed or intended for use in the on-line control of air traffic, aircraft navigation and communications as well as critical components in life support systems or in the design, construction, explosive atmosphere, operation and maintenance of any nuclear facility. Refer to the corresponding "Hardware Manual" for more information.

The described controllers may only be installed and operated as described in the corresponding "Hardware Manual". Commissioning, maintenance, inspection and operation are only to be performed by trained personnel.

The implementation of safety features in an EUC shall be designed according to the relevant sector, national and international standards and must be validated and verified by competent and independent personnel, in accordance with the requirements of the relevant standards.

The safety features of the described controllers are intended as contributing elements of a complete safety system. The use of the safety features in a non-safe control system is not recommended and may prevent the proper functioning of the safety functions when demanded.

1.5 Personnel qualification

Qualified personnel in the sense of this manual means persons who are familiar with the installation, mounting, commissioning, and operation of the ETEL components and with the requirements and specifications of the relevant sector, national and international standards. These trained personnel are also the target group of the manuals listed in the associated documentation listed ["page 5"](#) and is generally named as 'user' in the document.

Basically, persons who perform work on ETEL components must meet the following requirements:

- Completion of a training for the appropriate ETEL components.
- Training or instruction in the standards of safety engineering (state-of-the-art technology).
- Training, education or instruction related to the work to be performed.
- Use of appropriate safety equipment (clothing, measuring systems, etc.).
- Completion of first aid training.

To perform machine integration design, advanced operation or parameterization of ETEL products, qualified personnel must satisfy the following requirements:

- Have the required technical training, knowledge and experience to perform the assigned work.
- Know and understand the applicable legal regulations related to safety.
- Be able to proactively identify and avoid potential risks.

1.6 Safety information for various life phases of the controllers

Information about the following life cycle of the controllers are provided in the "Hardware Manual":

- Transport conditions;
- Storage conditions;
- Handling;
- Installation and operation;
- Maintenance operation.

The user must also refer to the safety precautions and general information provided in the corresponding "Hardware Manual".

2 Directives and standards

2.1 Basic guidelines

Compliance with the following directives is mandatory for the design of safety-related systems:

Directives
Machinery Directive: 2006/42/EC
EMC Directive: 2014/30/EU
EC Low Voltage Directive: 2014/35/EC

ETEL controllers with integrated safety design fulfill their share of the requirements as specified in the above directives, thus enabling the user as the manufacturer to produce EUCs in accordance with the Machinery Directive. The user is responsible for checking all indicated standards and directives for their validity. Furthermore, the user must ensure that all standards and directives applicable to his product are available in their currently valid version and are implemented in the product accordingly.

2.2 Basics for Functional Safety certification

The safety functions and devices for controllers with Functional Safety described are certified by TÜV Süd. The directives and standards serving as the basis for the Functional Safety certification are listed below:

■ European directives

Directives
EMC Directive: 2014/30/EU
EC Low Voltage Directive: 2014/35/EU

■ Functional Safety

Safety standards	Requirement (*)	Meaning / designation
IEC 61508-1:2010 IEC 61508-2:2010 IEC 61508-4:2010	SIL 3	Functional Safety of electrical / electronic / program-mable electronic safety related systems
ISO 13849-1:2015	Cat 3 / PL d	Machine safety - Safety-related parts of control systems

(*): The requirements reported in this table refer to the highest safety integrity level that can be achieved with the products when used in a dual-channel architecture. The achievement of the highest safety level depends on the implementation of the safety function by the User.

In addition, the integration of the ACCURET+ position controller into a safety-related machine requires that this machine also fulfills the safety-related standards. The table below provides examples of such standards.

Safety standards	Meaning / designation
IEC 61800-5-2: 2016	Adjustable Speed Electrical Power Drive Systems – Part 5-2: Safety requirements – Functional
IEC 60204-1:2016	Safety of machinery – Electrical equipment of machines – Part 1: General requirements

■ Primary safety

Safety standards	Meaning / designation
EN 61800-5-1: 2007/A11:2021	Adjustable Speed Electrical Power Drive Systems – Part 5-1: Safety requirements – Electrical, thermal and energy
UL 61800-5-1: 2012/R:2021-02	Adjustable Speed Electrical Power Drive Systems – Part 5-1: Safety requirements – Electrical, thermal and energy

■ **Electromagnetic compatibility**

Safety standards	Meaning / designation
EN 61800-5-2: 2016	Annex E provides the requirements and the specifications of the EMC tests to be executed
IEC 61800-3:2017	Adjustable speed electrical power drive systems - Part 3: EMC requirements and specific test methods

3 Safe Torque Off (STO) implementation

All components (e.g. control hardware, control software, emergency stop button, safety relays, etc.) that are involved in the individual safety functions must meet the requirements for the safety function. The hardware of the individual safety functions, including the wiring, must also be structured according to the determined requirements.



- The risk analysis that must be carried out for the system must state the requirements to be fulfilled by the individual safety functions. Before using the controller, a check must be made as to whether the safety functions realized by ETEL's controller meet the requirements of the risk analysis.

The purpose of the STO function is to safely shut off the power to the motors. This prevents the motors from generating a torque or a force. When the STO function is activated, the controller is unable to control the motion of the motors, but also unable to hold moving parts.



When the STO function is activated, the motor can no longer generate a torque or a force. This can result in a hazardous movement, such as may occur with:

- Axes without mechanical holding brakes (moving to a stop);
- Vertical and inclined axes without weight compensation;
- Direct drives with low friction and self-retention;
- External force on the drive axes;

It is the duty of the user to carry out a risk analysis and use it as a basis to minimize the risks by taking suitable measures.

3.1 SIL and target failure measures

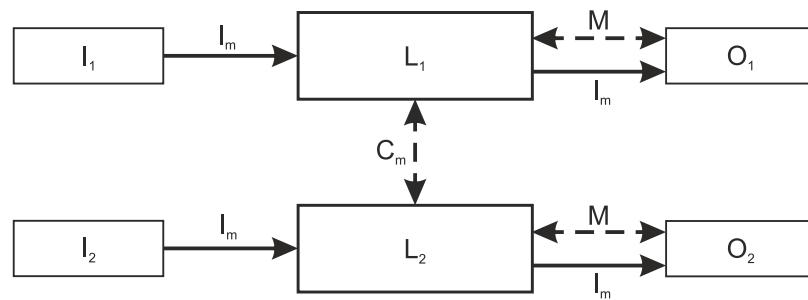
Only the specific manufacturer of a device or component may issue statements about whether these devices or components are suitable for safety-relevant applications. Furthermore, the key values of the control system do not take any external assemblies or devices into account. The following table reports the achieved safety level for the STO function of the controller and the related parameters.

Standard	Parameters	2-channel
IEC 61508-1:2010	SIL	3
ISO 13849-1:2015	Category	3
ISO 13849-1:2015	PL	d
IEC 61508-1:2010	PFH	$< 10^{-7}$ [1/h]
ISO 13849-1:2015	MTTFd	High

The safety functions and hardware components for Functional Safety are certified by an independent institute. Upon request, your contact partner at ETEL can provide you with the safety-related characteristic values needed for calculations as per EN ISO 13849-1 and IEC 61508. Please contact your ETEL representative if you require failure rates and statements for safety-related examination or risks analysis purposes concerning fault exclusions or ETEL products (e.g. control components, motors and power stages).

3.2 Dual channel architecture

The following figure represents the two-channel architecture required to achieve Category 3 as per ISO 13849-1.



with:

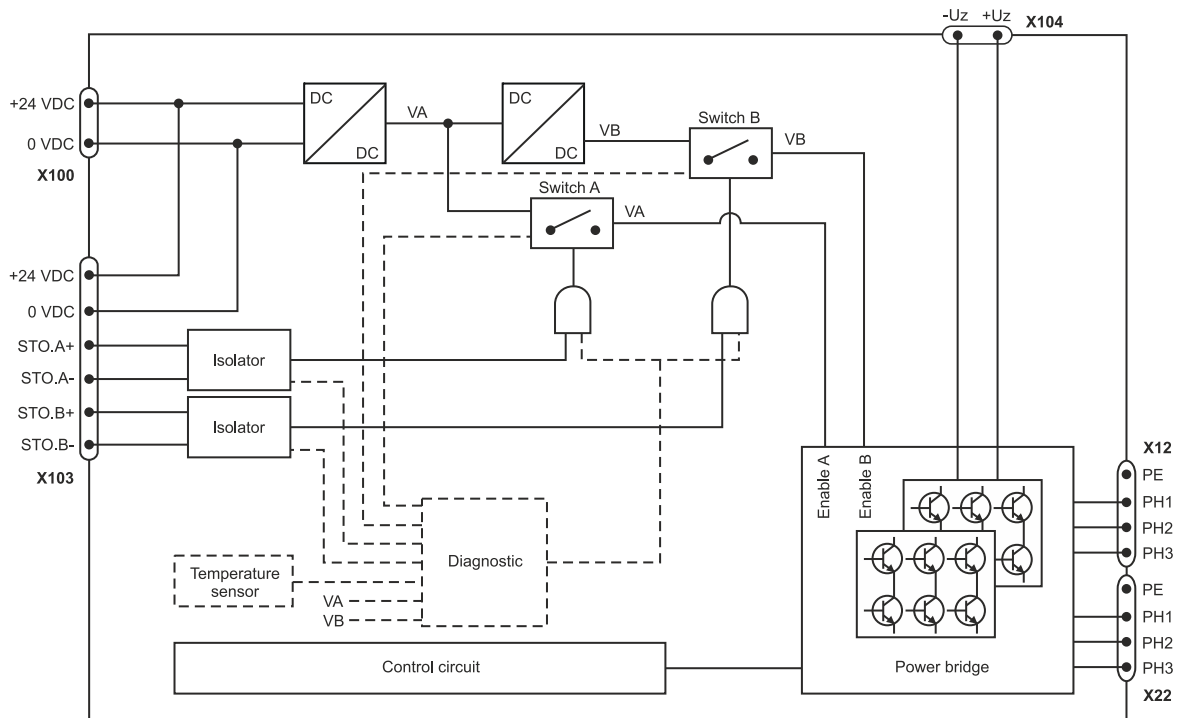
I_1, I_2	Input device (e.g. sensor)
I_m	Interconnecting means
C_m	Cross monitoring
L_1, L_2	Logic
M	Monitoring
O_1, O_2	Output device (e.g. main contactor)

Dashed line arrows represent practicable fault detection.

Inputs I_1 and I_2 correspond to the STO.A and STO.B inputs as reported in the figure in §3.3. O_1 and O_2 represent VA and VB after the respective switches.

3.3 Circuit description

The following figure shows the architecture of the STO circuit.



The STO circuit is composed by two separate channels (STO.A and STO.B) that act on two separate auxiliary internal voltages (refer to the above figure). The inputs of the STO circuit are controlled via the connector X103 and are insulated (functional insulation) through an isolator. When +24 VDC are respectively applied on STO.x input (where x stands for channel A and/or B), the switches of the respective channel are closed and the voltages VA and/or VB (generated, after due transformation, from the +24 VDC control input X100) are transmitted to the power bridge through the Enable A and/or B inputs.

The diagnostic channel continuously monitors the state of the A and B channels, as well as other parameters, like input voltages, temperature and other internal signals. When an anomaly is detected, the diagnostic channel acts on both A and B switches preventing to enable the power bridge.

When both VA and VB are available, the power coming from the connector X104 can be transmitted to the motors through the power bridge, for example with a PWR command sent by the control circuit (refer to the ACCURET+ "Operation & Software Manual" for more information about the PWR command). If any of the VA or VB voltages is missing (i.e. if any of the channel A or B of the STO circuit are not powered), the power transmission to the motors is shut off, leading the controller to the safe state.

The STO function simultaneously manages all the motor outputs of the controller. All motors' outputs are enabled or both are disabled at the same time.

The following table gives all possible combinations between the values of the inputs of the STO circuit, of the output signals and provides the related interpretation.

STO.A input	STO.B input	Switch A status	Switch B status	Status	Interpretation
L	L	Open	Open	Ok, safe state	STO function active. No power can be transmitted to the motors
L	H	Open	Close	Ok, safe state	STO active (channel A is disabled), i.e. no power to the motors
H	L	Close	Open	Ok, safe state	STO active (channel B is disabled), i.e. no power to the motors
H	H	Close	Close	Ok, power on is possible	STO inactive, i.e. power can be provided to the motors
H	X	Open	Any	Anomaly, safe state	Detected faulty component on channel A. As VA switch is disabled, the controller is in the safe state. If the failure persists after switch off and on, please contact an ETEL representative (refer to §6)
X	H	Any	Open	Anomaly, safe state	Detected faulty component on channel B. As VB switch is disabled, the controller is in the safe state. If the failure persists after switch off and on, please contact an ETEL representative (refer to §6)

With:

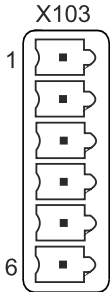
- STO.x input = L → 0 V between pin STO.x+ and pin STO.x- (or unconnected)
- STO.x input = H → +24 VDC between pin STO.x+ and pin STO.x-
- STO.x input = X → any of H or L: 0 V or 24 VDC between pin STO.x+ and pin STO.x-

NOTICE

- STO.A and STO.B must be high (24 VDC) before a command PWR is sent otherwise the error 132 occurs (refer to the errors reference list in the "ACCURET+ Operation & Software Manual").

3.4 Interfaces

Phoenix Contact MC 0.5/ 6-G-2.54 SMD R44 (plastic connector)

STO	Pin #	Signal	Function
	1	+24 VDC	Control supply output (+24 VDC). The current is limited by a resettable fuse of 160 mA.
	2	0 VDC	Control supply output (0 VDC)
	3	STO.A+	STO channel A + input
	4	STO.A-	STO channel A - input
	5	STO.B+	STO channel B + input
	6	STO.B-	STO channel B - input

NOTICE

- Refer to the corresponding "Hardware Manual" for more information about this connector.

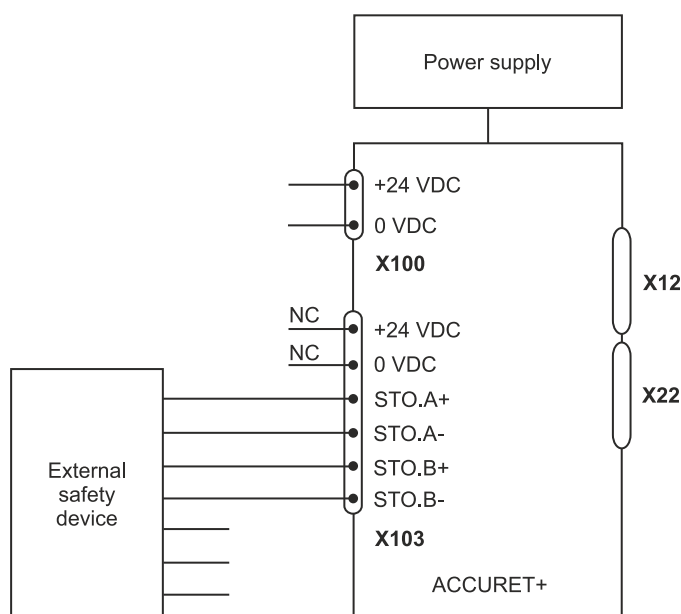
3.5 Activation of Functional Safety

Functional Safety is not a software option that must be enabled, as only hardware components of the controller are involved in the safety function. The wiring between the controller and the machine determines the behavior of the safety function. The STO is active by default, preventing the controller to provide power to the motors. To deactivate the STO function, STO.A+, STO.A-, STO.B+, STO.B- (on pin 3, 4, 5, 6 of connector X103) must be energized.

3.6 Configuration example

The STO architecture of the ETEL controllers allows the user to implement applications matching the following architectures according to ISO 13849-1.

Below is a configuration example with diagnostic for SIL3 (IEC61508-1) Cat.3 PLd according to ISO 13849-1. The STO reaches its highest safety level when both input signals STO.A and STO.B are used and connected by two separated cables: one cable for STO.A and one cable for STO.B. The external safety device can detect dangerous failures and react safely (refer to the table in [§3.3](#)).



Achievement of the Category 3 PLd and SIL 3 requirements

- It is the responsibility of the system manufacturer to verify that the requirements of Category 3 PLd and SIL 3 are satisfied for the designed system.

3.7 Use duration

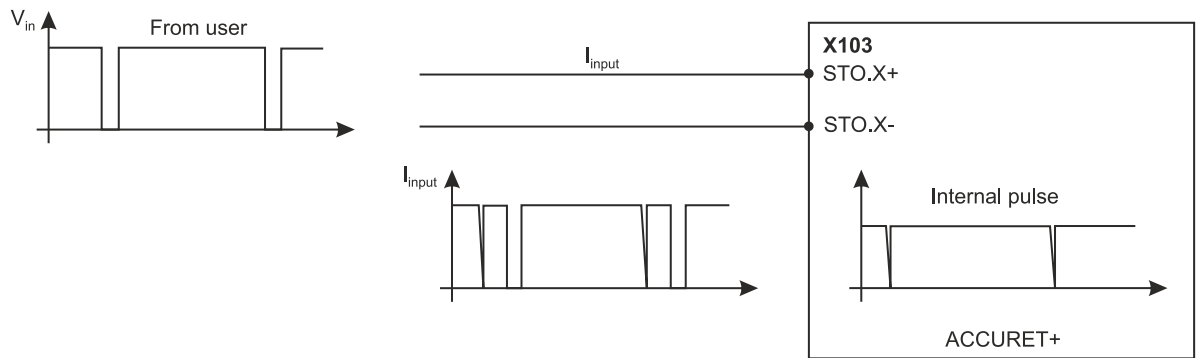
An average mission time of 10 years (24/24h, 360d/y) and a duty cycle of 80 % is assumed for ETEL controls with integrated safety design. For an application with a higher cycle's rate, the expected mission time must be adapted accordingly. The user is responsible for planning the replacement of the controller in accordance to the calculated mission time.

3.8 Response time

The following reaction times indicates the delay between a command on the inputs to activate the STO function and the achievement of the safe state (i.e. power to the motors is shut off). The maximum response time at 24 V and +23 °C is 30 ms. These delays must be taken into account by the user and must be added to the timings of any other part involved in the execution of the safety function.

3.9 User-supplied diagnostic

The STO.A and STO.B inputs have been designed to accept external pulses sent for user-diagnostic purposes. Such pulses can be used to detect stuck-at one STO.A or STO.B inputs (shorts 0V pulses are injected on +24 VDC signal) and connector disconnection (X103). The width of the pulse must be lower than 1 ms while its frequency must be lower than 100 Hz.



V_{in} is the user signal applied to STO.A and STO.B inputs. This +24 VDC signal could contain 0 V pulses (< 1 ms; < 100 Hz) to detect 'stuck-at one' failure. The current I_{input} shows the same pulses. Their presence indicates that the connector (X103) is correctly plugged in. If X103 is not connected there is no circulating current. The current I_{input} shows also smaller pulses coming from an internal signal of ACCURET+. These shorter pulses of $200 \mu s / 100 Hz$ are used internally to check continuously STO circuit and to detect anomaly.

3.10 Limits of the safety-related architectures

■ General limits:

- Electromagnetic compatibility with IEC 61800-3.
- Immunity requirements as per IEC 61000-6-2.
- Use of well-tried components as per IEC 61508-2, table B.2 and ISO 13849-2, table D.3.
- Use of Type A components as per IEC 61508-2, §7.4.4.1.2.

■ Category 3 (ISO 13849-1, §6.2.6), SIL3 (IEC 61508)

- PFH is $\geq 10^{-8}$ to $< 10^{-7}$.
- SFF is $\geq 90\%$ – $< 99\%$ for type A components and HFT=1.
- For PL_r = d the outputs (O₁ and O₂, refer to §3.2) must initiate a safe state which is maintained until the fault is cleared. The diagnostic coverage (DC_{avg}) of the functional channel must be at least low.
- The MTTF_d of each channel must be at least Medium.
- Measures against CCF must be applied.

The maximum PL achievable with category 3 is PL = d.

Due to the dual-channel architecture, the occurrence of a fault does not lead to the loss of the safety function between tests. The single fault should generally be detected at or before the next demand upon the safety function. It must however be noted that not all faults can be detected.

3.11 Fault exclusions

This section lists the fault exclusions implemented in the STO circuit.

■ Connector:

Short circuit between adjacent pins in accordance with the following remark:

By using ferrules or other suitable means for multi-stranded wires, creepage distances, clearances and all gaps should be dimensioned according to IEC 60664-1 standards with overvoltage category III.

■ PCB:

Short circuits between adjacent conductors in accordance with the following remarks:

As base material, EP GC according to IEC 60893-1 is used as a minimum. The clearances and creepage distances are dimensioned to at least IEC 60664-5 (IEC 60664-1 standard for distances greater than 2 mm) with pollution degree 2/overvoltage category III; if both tracks are powered by

a SELV / PELV power supply, pollution degree 2 / overvoltage category II applies, with a minimum clearance of 0,1 mm. The assembled board is mounted in an enclosure giving protection against conductive contamination, e.g. an enclosure with a protection of at least IP54, and the printed side(s) is (are) coated with an ageing-resistant varnish or a protective layer (solder mask) covering all conductor paths.

3.12 Remaining risks



- This chapter describes the residual risk that can lead to dangerous situation.
- The user has to take into account all following remarks when conducting the mandatory risk analysis. The risk analysis must also focus on others non-mentioned remaining risks, specific to the related system that can impact safety.

■ Brake

When the STO is enabled, the moving parts are no longer controlled by the ETEL controller. The machine manufacturer is responsible for the safety of the machine and must add some additional component(s) (ex: brake) to stop the movements.

■ Live parts

STO disables torque / force in the motor but does not disconnect the controller power outputs from the power supply. Switch off the power and wait for the complete discharge (up to 10 minutes) are mandatory before touching electrical parts.

■ Components failure

Components failure cannot be excluded. In case of component failure (ex: IGBT), a transient torque / force can produce an uncontrolled movement (e.g. on one magnetic period).

■ Connector lost

In order to improve troubleshooting, or / and to detect a disconnected cable, the current in the STO.x signals could be externally monitored. If the cable is disconnected, the input voltage is present but there is no current.

3.13 Safety-related operating modes

The controller is designed to operate in high or continuous demand mode. Only one operating mode is available with the ACCURET+ controller: standard operation mode. It must be noted that, during switch on, booting, working and switch off, the STO function is available.

3.14 Safety-related hardware signals

The controller STO function is activated using the STO.A and STO.B signals as inputs and does not involve any software or firmware. The wiring of the controller determines the behavior of the safety function.

3.15 Non-safety related firmware signals

The controller firmware provides a non-safe signal that monitors the STO.A and STO.B inputs of the STO function thanks to M66 and M272 (refer to the "Operating and Software Manual" for more information).

STO.A	STO.B	Internal STO diagnostic	M66	M272
H	H	Ok	0	0
L	H	Ok	12	1
H	L	Ok	12	2
H	H	Ok	12	3
X	X	Not ok	12	>3

NOTICE

- Refer to §3.3 for the meaning of H, L and X.
- When STO is enabled, a warning is indicated by the firmware monitoring M66=12. In addition, if the user tries to power on the motor (with PWR command), an error 142 (STO error) is raised. The power on of the motors is not possible..
- The error 132 is also raised by the firmware if the STO (A or B) is enabled as the motor was already powered on.

3.16 Bypass of Functional Safety

The bypass of the safety function is possible by connecting:

- Pin 3 and pin 5 of connector X103, together with pin 1
- And pin 4 and pin 6 of connector X103, together with pin 2



Bypass of the safety function:

- ETEL disengages from any consequence of the bypass of the safety function by the customer.
- The user must ensure that the effects of bypassing safety function are fully understood.

4 Integration into a safety system

This section provides information about the integration of the ETEL controllers into a safety control system for the control of EUC.

4.1 Integration requirements

Every EUC operator is exposed to certain risks. Although protective devices can prevent access to dangerous areas, the operator must also be able to work on the machine without such protection (e.g. protective door opened). Guidelines and regulations to minimize these risks have to be developed by the system integrator in the safety control system or with other safety measures.

Machinery Directive 2006/42/EC requires the system integrator to perform detailed risk assessments in order to prove operator safety during the various operating phases of the system. The combination of hazard analysis and risk evaluation leads to the determination of how much risks must be reduced by design measures or control methods in order to achieve an appropriate level of safety.

According to ISO 12100-1 and -2 (Safety of Machinery), it is important for safe operation of the machine that the safety measures permit simple and continuous use of the machine and that they do not impair its correct and intended operation. If this is not the case, it can lead to the safety measures being circumvented in order to attain the simplest possible operation of the machine.

The ETEL safety design complies with category 3 as per ISO 13849-1 and SIL 3 as per IEC 61508. Achievement of such safety level is possible if the implementation by the system integrator make use of the two channels as described in [§3](#).

The system manufacturer uses the ETEL controller's interface diagram (refer to [§3.3](#)) as a basis for wiring. This is a non-binding proposal, and must be adapted by the user to the requirements of the designed system. The user is responsible for adhering to the relevant standards and safety regulations.

It is imperative that the following requirements be fulfilled:

- The demand rates placed on the safety functions must be checked on the machine and documented.
- A comprehensive test of all safety-relevant functions must be performed before commissioning. The results of this functional test must be documented.
- The safety tests, including the test of the motor brakes and motor brake control, must be repeated within the interval required by the adopted architecture. The requirements are specified in [§5.3](#).
- For each specific system, a calculation of the safety characteristic numbers is to be performed in accordance with ISO 13849-1 and / or IEC 61508 for all components used, including external safety components.
- When installing and operating ETEL components, please refer to the corresponding documents mentioned in ["page 5"](#).
- External devices used in safety functions of the control must meet the following requirements:
 - Only devices that correspond to at least the same category as per EN ISO 13849-1 or at least the same SIL as per IEC 61508 may be used as part of a safe control system.
 - If parts with a lower category or SIL are used in combination with the ETEL controller, the overall safety level of the control system will be limited by the level of such components.
 - The power supply used for STO related signals must be PELV or SELV.

4.2 Operating and environmental requirements

The integration of the ETEL controllers must satisfy the operating and environmental requirements defined in the corresponding "Hardware Manual". In addition, the following operating conditions must also be satisfied:

- Appropriate measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, etc.) must be implemented according to the classification 'High' as stated in section A.14 of IEC 61508-7.
- Appropriate modification protections are implemented according to the classification 'high' as stated in section B.4.8 of IEC 61508-7.
- Appropriate measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as A.C. power supply frequency variation that can lead to dangerous failure are implemented according to the classification 'Medium' as stated in section A.8 of IEC 61508-7.
- ETEL controllers must be installed in an IP54 enclosure for dust and water splash protection.

5 Testing

The safety of the machine is ensured only by successful acceptance, i.e. a complete acceptance test, of the EUC.

5.1 Complete acceptance test

A complete acceptance test must be performed before operating the system, e.g. during commissioning, and if changes have been made to the hardware or to the software of the safety control system.

During a complete acceptance test, all provided safety functions (such as the compliance with limit values, functions of control units, functions of actuators, etc.) are checked. The fault reaction physically takes effect. The correct functioning of the safety functions is tested.

The acceptance test must be carried out by personnel authorized by the system manufacturer. Passing of the complete acceptance test and any modifications must be documented in a suitable manner.

5.2 Acceptance test of series-manufactured machines

A complete acceptance test does not need to be repeated for series manufactured machines if a complete acceptance test has been conducted on one of these machines, and the hardware match exactly those of the tested machine. The user must refer to the standards and requirements relevant for the system. However, the basic safety functions, such as emergency stop, the effectiveness of guard door contacts and interlocking devices, etc. must be tested for every machine.

5.3 Test intervals

The test interval requirements are defined in the following standards:

- ISO13849-1, §6.2.5
- IEC 61508-2, §7.4.4.1.4
- IEC 61800-5-2, §6.2.2.1.5

6 Service and support

For any inquiry regarding technical, commercial and service information relating to ETEL S.A. products, please contact your ETEL S.A. representative listed on www.etel.ch.

The technical hotline, based in ETEL S.A.'s headquarters, can be reached by:

- Phone: +41 (0)32 862 01 12.
- Fax: +41 (0)32 862 01 01.
- E-mail: support@etel.ch.

Please refer to your corresponding ETEL S.A. representative for more information about the technical documentation. ETEL S.A. organizes training courses for customers on request, including theoretical presentations of our products and practical demonstrations at our facilities.