



Functional Safety

User's Manual

Version C

ETEL

THIS PAGE IS INTENTIONALLY LEFT BLANK

Table of contents

1	Introduction	6
1.1	Functional Safety availability	6
1.2	Certified safety functions	6
1.3	Proper and intended operation	7
1.4	Qualified personnel	7
1.5	Safety precautions and general information	8
1.6	Safety information for various life phases of the controllers	10
2	Directives and standards	11
2.1	Basic guidelines	11
2.2	Basis for Functional Safety certification	11
3	Implementation and safety functions	12
3.1	Description of the safety/monitoring functions	12
3.1.1	Safe torque off (STO)	12
3.1.2	Response times and definitions	12
3.2	Implementation of the ETEL safety system	12
3.2.1	Schematics	12
3.2.2	Configuration examples	13
3.2.3	Limits of the safety-related architectures	15
3.2.4	Fault exclusions	16
3.2.5	Interfaces	16
3.2.6	Safety-related hardware signals	16
3.2.7	Safety-related operating modes	16
3.2.8	Non-safety related firmware signals	16
3.2.9	Activation of Functional Safety	17
3.3	SIL and target failure measures	17
3.4	Use duration	17
3.5	Remaining risks	18
4	Integration into a safety system	19
4.1	Integration requirements	19
4.2	Operating and environmental requirements	20
5	Testing	21
5.1	Complete acceptance test	21
5.2	Acceptance test of series-manufactured machines	21
5.3	Test intervals	21
5.4	Procedure	21

6	Service and support	22
----------	----------------------------------	-----------

Record of revisions:




Document revisions		
Version	Date	Main modifications
Ver A	08.07.20	First version
Ver B	18.09.20	Updated version: - Controller designation updated (refer to §1.1)
Ver C	10.03.23	Updated version: - Minor changes

Documentation concerning the Functional safety related products:

- | | |
|--|--|
| <ul style="list-style-type: none"> • Functional Safety User's Manual • AccurET Modular Operation & Software Manual • AccurET Modular 300 Hardware Manual | <ul style="list-style-type: none"> • Functional Safety implementation • AccurET setup, use & programming manual • Specifications & electrical interfaces |
|--|--|

Acronyms/definitions:

- **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
- **MTTFd:** Mean Time to Dangerous Failure
- **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
- **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, ...

	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, only.





The Safe Torque Off (STO) function described in [§2.2](#) has been successfully tested and evaluated as part of AccurET Modular 300 controller listed in [§1.1](#).

1 Introduction

This manual provides information about the Functional Safety features related to the AccurET Modular 300 controller (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 page 5 before carrying out any operation on the system. Please contact ETEL S.A. or authorized distributors in case of questions regarding the installation procedures, safety or any other issues.
	ETEL S.A. disclaims all responsibility for accidents and damages if the safety instructions, the procedures and the usage described in this manual are not followed (including the ones given in the manuals listed page 5).

1.1 Functional Safety availability

The Functional Safety features documented in this manual are only available on the following controllers.


Controller designation	Part number
EA-P2M-300-4/7.5A-0101-01	716932-11
EA-P2M-300-4/7.5A-0001-01	716936-11
EA-P2M-300-4/7.5A-0003-01	716936-12
EA-P2M-300-07/15A-0101-01	716935-11
EA-P2M-300-07/15A-0001-01	716938-11
EA-P2M-300-07/15A-0003-01	716938-12

Remark: The other ETEL controllers are not certified about Functional Safety.

1.2 Certified safety functions

The following certified safety function is available for the products mentioned in [§1.1](#):

- Safe Torque OFF (STO)

Danger	
	<p>ETEL only assumes responsibility for the safety functions stated and described in this manual. Functional safety can reduce the inherent risks of EUC.</p> <p>However, it is impossible to implement safety measures that ensure that nothing will ever go wrong with an EUC.</p> <p>In order for functional safety to take effect, the User must do the following:</p> <ul style="list-style-type: none"> - 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 documentations 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.

1.3 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.

1.4 Qualified personnel

Trained 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 Functional Safety standards. This trained personnel is also the target group of the manuals listed [page 5](#) and is generally named as "User" in the document.

Furthermore, electrical engineering work on the system may be carried out only by trained electrical engineering technicians or persons trained specifically for the respective application.

- **General requirements**

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

- Completion of a training for the appropriate ETEL components or in-house instruction from training course participants
- Training or instruction in the standards of safety engineering (state-of-the-art technology)
- Use of appropriate safety equipment (clothing, measuring systems, etc.)
- Completion of first aid training

- **Operator**

The operator uses and operates the product within the framework specified for the intended use. He or she is informed by the operating company about the special tasks and the potential hazards resulting from incorrect behavior.

- **Qualified personnel**



The qualified personnel are trained by the operating company to perform advanced operation and parameterization. The qualified personnel have the required technical training, knowledge and experience and know the applicable regulations, and are thus capable of performing the assigned work regarding the application concerned and of pro-actively identifying and avoiding potential risks.

- **Electrical specialist**

The electrical specialist has the required technical training, knowledge and experience and knows the applicable standards and regulations, and is thus capable of performing work on electrical systems and of pro-actively identifying and avoiding potential risks. Electrical specialists have been specially trained for the environment they work in.

Electrical specialists must comply with the provisions of the applicable legal regulations on accident prevention.

1.5 Safety precautions and general information

Danger	
	<p>Live parts Electric shock upon contact.</p> <ul style="list-style-type: none"> - Work on electrical components can be performed only if the User is sufficiently qualified for this. The minimum qualifications in accordance with this manual are described in §1.4. - The User must always comply with the applicable local safety rules and regulations while working. - Before working on the machine and/or performing other work on electrical components, the User must disconnect the EUC from the power supply, check that the power is disconnected, and take precautions against restart of the EUC. - The User must ensure that the main switch of the control or EUC is switched off when engaging or disengaging connecting elements or connection clamps and/or perform other work on electrical components. - Before starting with the work, the User must allow for at least a 10 minute discharge period after the supply voltage has been switched off and ensure that the equipment is free of potential. - The User must ensure that the circuit protective conductor (CPC) is correctly connected. The circuit protective conductor is used to provide protection from electric shock and to allow sufficient current to flow so that the protective devices can trip. Interruptions in the protective conductor may cause damage to persons or property.
	<p>Moving parts or EUC components Personal injury due to mechanical influence.</p> <p>The User must ensure that the main switch of the control or the EUC is switched off before starting work on devices and components in the electrical cabinet or in the housing of the EUC. 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.</p>
	<p>Faulty machine performance Collision with persons, property and damage to machine.</p> <ul style="list-style-type: none"> - Incorrect or non-optimized use of the controllers can lead to faulty EUC performance and therefore to serious injury to persons, damage to equipment and to processed parts. Modifications of the EUC configuration should be done with caution and uncontrolled axes motions should be taken into account. - Please note that faulty wiring or assembly, a defective component or an external force, and/or damage may lead to inadvertent movements of the EUC parts. - If a defect is found on the EUC, in which ETEL components and/or ETEL devices are installed, or if an ETEL component and/or ETEL device is defective, then the machine must be turned off and secured against restarting.
Warning	
	<p>Faulty machine performance Collision with persons, property damage to machine.</p> <p>In order to be able to judge 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.</p>

Warning

Live parts

Electric shock upon contact.

- Refer to the system's control's circuit diagrams and grounding diagrams for the various supply voltages in the control system.
- Please note that the following may cause dangerous touch voltages: faulty wiring or assembly of a defective component, an external force, and/or damage.
- The components described in this manual may only be installed and operated in suitable housings, such as enclosures and electrical cabinets.
- Repair and start-up of systems, into which ETEL components, as described in this manual are installed, may only be performed by trained personnel.
- Repair of an ETEL component as described in this manual may only be performed by ETEL. Do not open the housing of the ETEL components.
- The +24 V supply voltage can also be used to supply machine components or (S)PLC components that are not from ETEL. It must be ensured, however, that PELV ("low voltage electrical separation") according to EN 61800-5-1 is compliant for the +24 V supply voltage of the control system from ETEL. If this is not the case, those components must be supplied from an individual power supply unit and be electrically isolated.
- Safely separated voltages or circuits (protective low voltage, PELV) must not be connected to circuits with basic insulation.
- Prior to the start-up of an EUC, it must be ensured by means of measurement that the connection of 0 V to the protective conductor connection of the machine is at low resistance according to the applicable sector's standard.
- EN 61800-5-1 must be observed for the +24 V voltage cables and cable routing. Therefore, cables for safely separated electric circuits must have double or reinforced insulation between the wire and the surface if they are routed without spatial separation from other cables. The insulation must then be chosen correspondingly to the maximum possible voltage that can be generated.



Faulty machine performance or live parts

Property damage to the machine or electric shock upon contact.

The User must refer to the technical manual for its control and the corresponding "Hardware Manual" from ETEL.

- Cables and terminals for the power connection and DC link must be arranged to be safe to touch in the electrical cabinet.
- The housing of the devices (e.g. the electrical cabinet), in particular the housing of power stages, must be designed in accordance with the fire prevention regulations at the place of installation. The User is responsible for fire protection.
- The use of suitable gloves to avoid injury from sharp edges during handling is recommended.
- All of the ETEL control components or devices must be operated only in enclosures suitable for this purpose, such as electrical cabinets or panels. The enclosures must also provide protection against electric shock.
- The mounting surface for the devices must be chosen such that it does not deform under the weight of all devices. In addition, a permanently electrically conductive material must be used and connected to the protective conductor.
- The User must ensure that no small parts enter inside the devices through any housing openings.
- ETEL components or ETEL devices must not come into contact with chemicals, acids or bases.
- Detergents for cleaning ETEL components or devices must not be used.
- The use of lubricants and contact grease is not permitted for screw and clamp connections on ETEL controllers.
- In certain cases of failure, the power stages are switched off or the current to the power stages is cut off without the axes being decelerated. In these cases, axes without mechanical brakes can move to a stop without braking. The User must take this into account in the risk analysis of the EUC.
- Radio transmission devices must be kept at least 50 cm away from ETEL components or ETEL devices.

Warning

- Measurement must be taken at regular intervals of the resistance of all protective ground connections, in particular from the ETEL components to the building's electrical installations and from the motors to the inverters.
 - To measure the insulation resistance of the system or to perform a voltage test on the insulation of the system, the User must first disconnect the ETEL controllers. Failure to do so could result in damage to the devices.
 - The vibrations in EUC can eventually loosen screw connections. The User must regularly check the torque of screws on terminals and mounting screws.
- The User must ensure that the machine and the devices can easily be accessed at the mounting and installation location during operation, commissioning, maintenance and servicing. Sufficient clearance must be provided from adjacent parts and walls. The space required for cables, installation and servicing mentioned in the corresponding "Hardware Manual" must be taken into account.

Notice

- The following points must be observed during mounting and electrical connection:
- National regulations for low-voltage installations at the operating site of the machine or components.
 - National regulations regarding interference and noise immunity at the operating site of the EUC or components.
 - National regulations regarding electrical safety and operating conditions at the operating site of the EUC or components.
 - Specifications for the installation position.
- Information on the documentation:
- This technical manual is addressed to EUC builders, commissioning technicians and service personnel who implement ETEL control technology.
 - Refer to the corresponding "Hardware Manual" for more information about assembly, installation and commissioning.
 - For ETEL products, the safety-related characteristics (such as failure rates, statements on fault exclusion, etc.) of the individual products are available on request from the ETEL contact person.
 - The User must ensure that the latest documents version is used when planning the EUC.

1.6 Safety information for various life phases of the controllers

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

- Transport and storage;
- Unpacking and handling;
- Installation and initial operation;
- Maintenance operation;
- Service.

The user must also refer to the safety precautions and general information provided in [§1.5](#).

2 Directives and standards

2.1 Basic guidelines

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

Directives	Directives took effect on
Machinery Directive 2006/42/EC	December 29, 2009
EMC Directive 2014/30/EU	April 20, 2016
EC Low Voltage Directive 2014/35/EC	April 20, 2016

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 Basis for Functional Safety certification

The safety functions and devices for controllers with functional safety (FS) 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	Applicable since
EMC Directive 2014/30/EU	April 20, 2016
EC Low Voltage Directive 2014/35/EU	April 20, 2016

- **Functional safety**

Safety standards	Requirement (*)	Meaning / Designation
IEC 61508-1:2010 IEC 61508-2:2010 IEC 61508-4:2010	SIL 2	Functional safety of electrical/electronic/programmable electronic safety related systems
ISO 13849-1:2015	Cat 2 / 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 mentioned in [§1.1](#) when used in a single-channel architecture. The achievement of the highest safety level depends on the implementation of the safety function by the User. [§3.2](#) provides information about possible implementations.

Due to the applications of the device or system, the following directives and standards are also valid:

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	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.

3 Implementation and safety functions


3.1 Description of the safety/monitoring functions

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.

Danger	
	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.

3.1.1 Safe torque off (STO)

The purpose of the STO function is to safely cut the power to the motors. This is to prevent the motors to generate a torque or force. When the STO is activated, the controller is unable to control the motion of the motors, but also unable to hold moving parts. The safety function is achieved by disabling the transistors of the power bridge (PWM signals).

Danger	
	<p>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:</p> <ul style="list-style-type: none"> - 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.

3.1.2 Response times and definitions

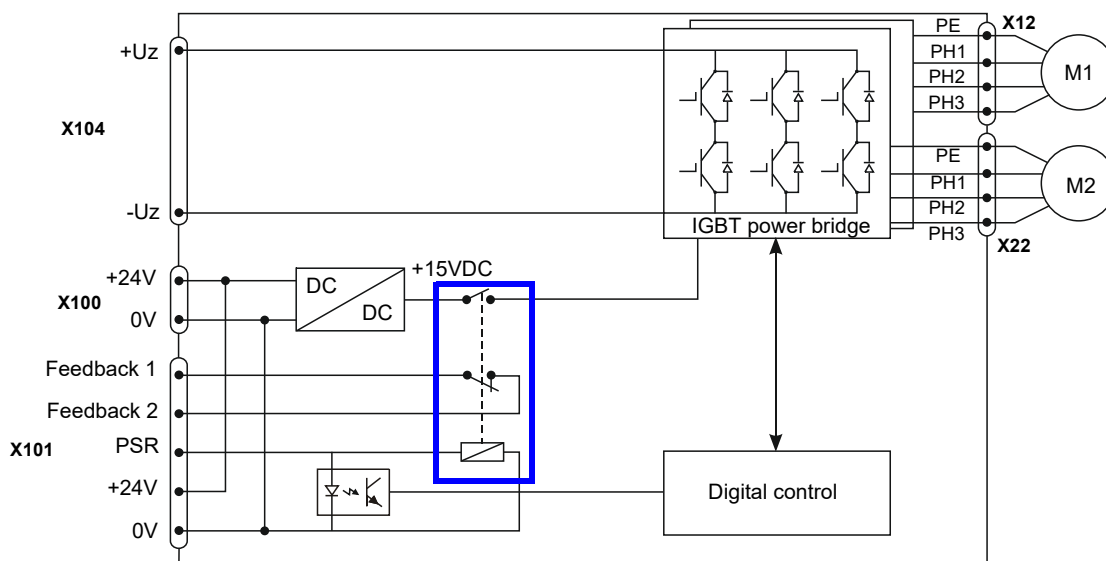
The following reaction times indicate delay between a command to enable the STO mode and the occurring of a stable status of the feedback contact:

- Maximum response time at 24V and +23°C (including bounce time): 28 ms.
- These delays must be taken into account by the User and added to the timings of the other involved parts.

3.2 Implementation of the ETEL safety system

3.2.1 Schematics

Internal relay principle: the STO function simultaneously manages all the motor outputs of the controller. Both motors' outputs are enable or both are disabled at the same time.



The STO circuit contains a relay (internal relay highlighted in blue in the above figure) including a main contact (+15VDC) to allow power transmission to motors and a feedback contact to detect anomalies. The main and feedback contacts are mechanically linked.

The feedback contact [Normally Closed] is closed when the internal relay is not powered and open when relay is powered. The main contact is a Normally Open type, meaning that without current in the coil the motors cannot receive power. The two contacts are mechanically linked.

The table below gives all possible combinations between the values of the command of the internal relay and of the feedback signal and provides the related interpretation.

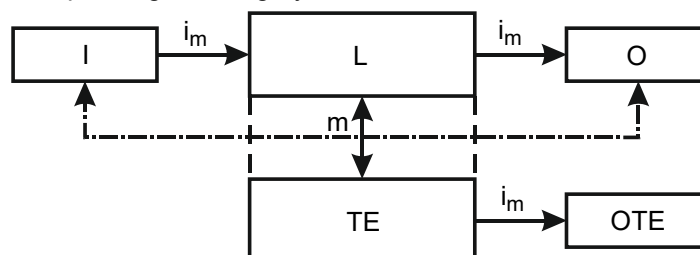
Main contact status	Feedback contact status	Status	Interpretation
Open (PSR = 0 V)	Open	Anomaly	Damaged relay, damaged feedback circuit or issue related to the connection. As the main contact is not powered, the system is in a safe state. However, the STO must be tested before restarting the application.
Open (PSR = 0 V)	Closed	Ok	STO active, i.e. no power to the motors.
Closed (PSR = 24 V)	Open	Ok	STO inactive, i.e. power provided to the motors.
Closed (PSR = 24 V)	Closed	Anomaly	Damaged relay, damaged feedback circuit or issue related to the connection. As the main contact is potentially powered, the system is possibly not in the safe state. The EUC main controller must initiate the safe state.

3.2.2 Configuration examples

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

3.2.2.1 Configuration with diagnostic

Here is a diagram corresponding to Category 2 from ISO 13849-1:



With

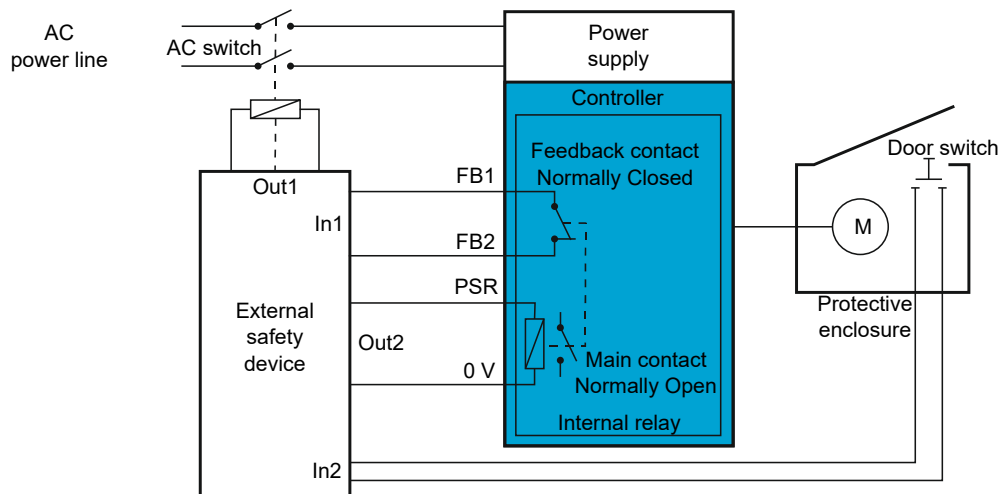
- i_m = interconnecting means
- I = Input device (e.g. sensor)
- L = Logic
- O = Output device (e.g. main contactor)
- m = monitoring
- TE = Test Equipment
- OTE = Output of TE

Dashed lines represent reasonably practicable fault detection

Below is a configuration example with diagnostic for SIL2 (IEC61508-1) Cat.2 PLd according to ISO 13849-1. The STO reaches its highest safety level when the signal from feedback contact is used to trigger an automated reaction in case of detected anomaly.

By comparing the feedback signal with the command of the internal relay, the external safety device can detect dangerous failures and react safely (refer to the table in §3.2.1).

The diagram below describes an example of a configuration with an external safety device that controls the STO function and the main AC power line feeding the controller.



The illustrated external Safety Device has two inputs and two outputs:

- one output to control the internal relay (Out 2),
- one output to connect and disconnect the AC power line (Out 1),
- one input to check the internal relay feedback contact (In 1),
- one input to check the door switch (In 2); The door switch is an example of use of a device that triggers the use of the STO.

When the AC switch is closed, the power supply unit is powered. If the door switch is closed, the external Safety Device can apply voltage on the internal relay coils and this allows the controller to send power to the motor. When the main contact closes, the feedback contact must open. If it is not the case, a possibly dangerous situation is occurring (refer to the table in §3.2.1) and the AC switch shall be opened by the external safety device to disconnect the power line.

When the door opens, the external safety device must stop supplying the internal relay, which releases its main contact. Then the external safety device must check that the feedback contact is closed. If it is not the case, a possibly dangerous situation is occurring (refer to the table in §3.2.1) and the AC switch shall be opened by the external safety device to disconnect the power line.

Warning

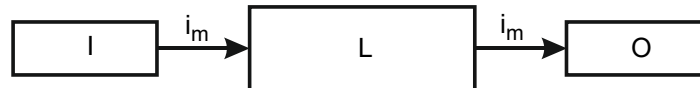


Achievement of the Category 2 and SIL 2 requirements

- It is the responsibility of the system manufacturer to verify that the requirements of Category 2 and SIL 2 are satisfied for the designed system.

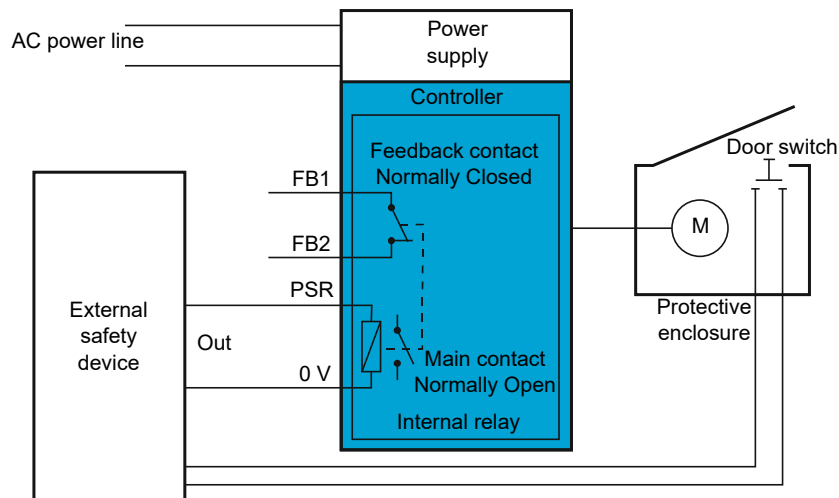
3.2.2.2 Configuration without diagnostic

Here is a diagram corresponding to Category 1 of ISO 13849-1:



With
 I_m = interconnecting means
 I = Input device (e.g. sensor)
 L = Logic
 O = Output device (e.g. main contactor)

Below is a configuration example without diagnostic Coverage for SIL1 (IEC61508-1) Cat.1 PLc according to ISO 13849-1.



A limited safety level is obtained when the feedback contact is not used or simply used to indicate an anomaly without reacting automatically. The resulting layout matches the category 1 as per ISO 13849-1.

3.2.3 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 (Type A as per 7.4.4.1.2 of IEC 61508-2).

The diagnostic time interval must either be lower than the process safety time (including the time required to perform the safe state achievement action) or be 100 times lower than the demand rate. This requirement comes from IEC 61508-2, 7.4.4.1.4: for HFT=0.

- **Without diagnostic, category 1 (ISO 13849-1, §6.2.4), SIL1 (IEC 61508)**

PFH is $\geq 10^{-6}$ to $< 10^{-5}$

SFF is $< 60\%$ for type A components

MTTFd must be high.

Maximum achievable PL with category 1 is PL=c.

No diagnostic coverage.

Common Cause Failures (CCF) not relevant for this category.

When a fault occurs it can lead to the loss of the safety function.

- **With diagnostic, category 2 (ISO 13849-1, §6.2.5), SIL2 (IEC 61508)**

PFH is $\geq 10^{-7}$ to $< 10^{-6}$

SFF is $\geq 60\% - < 90\%$ for type A components

For PLr = d the output (OTE) must initiate a safe state which is maintained until the fault is cleared.

The diagnostic coverage (DCavg) of the functional channel must be at least low.

The MTTFd of each channel must be low-to-high, depending on the required performance level (PLr).

Measures against CCF must be applied.

The maximum PL achievable with category 2 is PL = d.

The occurrence of a fault can lead to the loss of the safety function between tests.

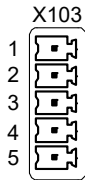
The loss of safety function is detected by the diagnostic channel.

3.2.4 Fault exclusions

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

- **Relay:** Use of positively mechanically linked contacts for, e.g. monitoring function in Category 2, 3, and 4 systems (see EN 50205, IEC 60947-4-1:2001, Annex F, IEC 60947-5-1:2003 + A1:2009, Annex L).
- **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 to at 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 covering all conductor paths.

3.2.5 Interfaces

Phoenix Contact MC 1.5/5-G-3.81 (plastic connector)			
Relay	Pin #	Signal	Function
	1	FB1 (Feedback 1)	Feedback control 1 of the relay (24 V / 0.8 A max)
	2	FB2 (Feedback 2)	Feedback control 2 of the relay (24 V / 0.8 A max)
	3	PSR	Relay supply input (+24VDC ±10%) from control input
	4	+24V	Control supply output (+24VDC). 40 mA max. To bypass the STO function, connect this pin to pin 3 (PSR), otherwise let this pin not connected.
	5	0V	Control supply (0VDC) internally connected to GNDaux (pin 2 of X100)

Remark: The +24V (pin 4) is internally connected to +24V (pin 1 of X100).
Pin 4 must not be used to power for something else other than the power relay.
The associated connector can be ordered through the connector kit (refer to the "Hardware Manual" for more information).
Always use a connector compatible with the above-mentioned one.
The relay connector is located on the top of the controller.

3.2.6 Safety-related hardware signals

The controller STO feature is activated using the PSR signal (X103 pin 3) as input and the Feedback Contact (X103 pin 1 / pin 2) as output.

The controller STO feature does not involve any software or firmware. The wiring of the controller determines the behavior of the safety function.

3.2.7 Safety-related operating modes

The controller is designed to operate in high or continuous demand mode.

Only one operating mode is available with the ETEL controller: standard operation mode. It must be noted that, during switch on, booting, working, switch off, the STO function is available.

3.2.8 Non-safety related firmware signals

The controller FW provides a non-safe signal that monitors the PSR input of the relay (warning M66 = 12 and error M64 = 132 : refer to "Operating and Software Manual" for more information).

3.2.9 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, the relay must be activated through the PSR channel (X103 pin 3). The bypass of the safety function is possible by connecting X103 pin 3 (PSR) and X103 pin 4 (+24 V).

Danger



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.

3.3 SIL and target failure measures

Fundamentally 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. Refer to [§3.2](#) for applicable requirements.

Standard	Parameters	Without diagnostic	With diagnostic
IEC 61508-1:2010	SIL	1	2
ISO 13849-1:2015	Category	1	2
ISO 13849-1:2015	PL	c	d
IEC 61508-1:2010	PFH	$\geq 10^{-8}$ to $< 10^{-7}$ [1/h]	$< 10^{-8}$ [1/h]
ISO 13849-1:2015	MTTFd	High	High

The safety functions and hardware components for Functional Safety (FS) 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).

3.4 Use duration

An average mission time of 10 years (24/24h, 360d/y) is assumed for ETEL controls with integrated safety design.


Mechanical endurance of the relay is 10×10^6 operations (data from manufacturer).

Electrical endurance is 1×10^6 with 0.8A in the feedback contact.

This maximum value is not reached after 10 years (24/24h, 360d/y) with 10 switch cycles per hours.

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.

3.5 Remaining risks

Warning	
	This chapter describes the risk that can exist even in the case of a correct use of the product and that can lead to dangerous situation.
	The User have 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.

- **Vibrations**

Excessive vibrations might lead to the instability of the relay. In such cases, the relay might not be able to guarantee the safe state. In order to limit such risk, the controller was tested up to 1G for vibrations (according to IEC 60068-2-6) and up to 5G for shocks (according to IEC 60068-2-27). In addition, the monitoring of the diagnostic signals by the system manufacturer, according to the procedure documented in [§3.2](#), allows to detect this situation.

- **Broken relay**

If the relay breaks (e.g. soldered contacts), the safe state triggering might not be controllable and therefore lead to a dangerous situation. Due to the construction of the relay according to EN61810-3 (formerly EN50205), the reading of the feedback signal allows to detect more than 99% of the failures of the relay. The monitoring of the diagnostic signals by the system manufacturer, according to the procedure documented in [§3.2](#), allows to detect this situation.

- **Connector**

In case of a short circuit of one pin of the connector to the ground, the corresponding signal provides the wrong value. In the case a feedback-related pin is concerned, the real state of the relay would be unknown. This case could lead to dangerous situations. The monitoring of the diagnostic signals by the EUC manufacturer, according to the procedure documented in [§3.2](#), allows to detect this situation.

- **Brake**

When the STO is enabled, the moving parts are no longer controlled by the ETEL controllers. 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 (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 on one magnetic period.

- **Connector lost**

In order to improve troubleshooting, or/and to detect a disconnected cable, the current in the coil of the internal relay could be externally monitored to check that the value measured is compatible with the coil resistance ($823R \pm 10\%$). If the cable is disconnected, the voltage is present but there is no current.

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 2 as per ISO 13849-1 and SIL 2 as per IEC 61508. Achievement of such safety level is possible if the implementation by the system integrator of the diagnostic channel is executed according to the recommendations provided in [§3](#) of this manual.

The basis of the ETEL safety concept is its single-channel architecture. According to ISO 13849-1, the occurrence of a fault can lead to the loss of the safety function. If the system developed by the User requires the safety function to be functional despite the failure of one component, a dual-channel architecture, matching Category 3 must be designed. In this case, the ETEL controller can be included in the safety control system as one of the two channels.

The system manufacturer uses the ETEL controller's interface diagram (refer to [§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 [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 "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 "medium" 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 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

5.4 Procedure

The comparison of the diagnostic signals with the STO command input (PSR signal) allows to check the correct behavior of the STO function according to the situations detailed in [§3.2.1](#).

- Without voltage present on the PSR signal, the STO function is active and the motors cannot be enabled. The feedback contact must be closed, otherwise a possible failure might be occurring.
- With 24V present on the PSR signal, the STO function is not active and the motor can be enabled. The feedback contact must be opened, otherwise a possible failure might be occurring.

Both lines must be checked successively to fulfil the test procedure.

Additional measurements can be added to increase further the confidence of the test:

- Reaction time measurement according to [§3.1.2](#).
- Connector disconnection detected by current measurement following the note in [§3.5](#).

Further important notes on the acceptance test:

- The responsibility for the acceptance, above all for the contents of the test and its conductance lies solely with the system manufacturer.
- The results of the acceptance test, the behavior and response times of the machine (e.g. braking behavior) should be documented in a suitable form.
- The acceptance test should be conducted and recorded in the test report only by qualified persons. On the basis of their specialist training and knowledge, this person should be capable of conducting the acceptance test in an appropriate manner. The machine should be deemed "non-safe" until final completion of the acceptance test. The test report should be signed by the person who conducted the acceptance test.

Danger



The sequence and procedure for each step of the test should be evaluated before performance, always in the same way. Otherwise situations may occur during the test where careless or imprudent handling may cause danger to the operator or damage to the machine.

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 our website (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.