Altivar HVAC ATH200

Variable Speed Drives

Safety Functions Manual

Original Instructions written in English

JPS43226.01
12/2025

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Qualification of Personnel

Only appropriately trained persons who are familiar with and understand the contents of this manual and all other pertinent product documentation are authorized to work on and with this product. In addition, these persons must have received safety training to recognize and avoid hazards involved. These persons must have sufficient technical training, knowledge and experience and be able to foresee and detect potential hazards that may be caused by using the product, by changing the settings and by the mechanical, electrical and electronic equipment of the entire system in which the product is used. All persons working on and with the product must be fully familiar with all applicable standards, directives, and accident prevention regulations when performing such work.

Intended Use

This product is intended for industrial use according to this manual.

The product may only be used in compliance with all applicable safety standard and local regulations and directives, the specified requirements and the technical data. The product must be installed outside the hazardous ATEX zone. Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented. Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design). Any use other than the use explicitly permitted is prohibited and can result in hazards.

About the document

Document Scope

The purpose of this document is to provide information about safety functions incorporated in Altivar HVAC ATH200. These functions allow you to develop applications oriented in the protection of man and machine.

The content of this manual is also accessible through the ATH200 DTM online help.

Validity Note

Original instructions and information given in the present document have been written in English (before optional translation).

This documentation is valid for the Altivar HVAC ATH200 drives.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Product Related Information

Read and understand these instructions before performing any procedure with this device.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Only appropriately trained persons who are familiar with and fully understand the contents of the present manual and all other pertinent product documentation and who have received all necessary training to recognize and avoid hazards involved are authorized to work on and with this device system.
- Installation, adjustment, repair and maintenance must be performed by qualified personnel.
- Verify compliance with all local and national electrical code requirements as well as all other applicable regulations with respect to grounding of all equipment.
- Only use properly rated, electrically insulated tools and measuring equipment.
- Do not touch unshielded components or terminals with voltage present.
- Prior to performing any type of work on the device system, block the motor shaft to prevent rotation.
- Insulate both ends of unused conductors of the motor cable.
- Do not short across the DC bus terminals or the DC bus capacitors or the braking resistor terminals.

Failure to follow these instructions will result in death or serious injury.

Damaged products or accessories may cause electric shock or unanticipated equipment operation.

⚠⚠DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

Failure to follow these instructions will result in death or serious injury.

Contact your local Schneider Electric sales office if you detect any damage whatsoever.

Your application consists of a whole range of different interrelated mechanical, electrical, and electronic components, the device being just one part of the application. The device by itself is neither intended to nor capable of providing the entire functionality to meet all safety-related requirements that apply to your application. Depending on the application and the corresponding risk assessment to be conducted by you, a whole variety of additional equipment is required such as, but not limited to, external encoders, external brakes, external monitoring devices, guards, etc.

As a designer/manufacturer of machines, you must be familiar with and observe all standards that apply to your machine. You must conduct a risk assessment and determine the appropriate Performance Level (PL) and/or Safety Integrity Level (SIL) and design and build your machine in compliance with all applicable standards. In doing so, you must consider the interrelation of all components of the machine. In addition, you must provide instructions for use that enable the user of your machine to perform any type of work on and with the machine such as operation and maintenance in a safe manner.

The present document assumes that you are fully aware of all normative standards and requirements that apply to your application. Since the device cannot provide all safety-related functionality for your entire application, you must ensure that the required Performance Level and/or Safety Integrity Level is reached by installing all necessary additional equipment.

⚠WARNING

INSUFFICIENT PERFORMANCE LEVEL/SAFETY INTEGRITY LEVEL AND/OR UNINTENDED EQUIPMENT OPERATION

- Conduct a risk assessment according to EN ISO 12100 and all other standards that apply to your application.
- Use redundant components and/or control paths for all critical control functions identified in your risk assessment.
- Implement all monitoring functions required to avoid any type of hazard identified in your risk assessment, for example, slipping or falling loads.
- Verify that the service life of all individual components used in your application is sufficient for the intended service life of your overall application.
- Perform extensive commissioning tests for all potential error situations to verify the effectiveness of the safety-related functions and monitoring functions implemented, for example, but not limited to, speed monitoring by means of encoders, short circuit monitoring for all connected equipment, correct operation of brakes and guards.
- Perform extensive commissioning tests for all potential error situations to verify that the load can be brought to a safe stop under all conditions.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Product may perform unexpected movements because of incorrect wiring, incorrect settings, incorrect data or other errors.

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Carefully install the wiring in accordance with the EMC requirements.
- Do not operate the product with unknown or unsuitable settings or data.
- Perform a comprehensive commissioning test.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop, overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines (1).
- Each implementation of the product must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

(1) For USA: Additional information, refer to NEMA ICS 1.1 (latest edition), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control and to NEMA ICS 7.1 (latest edition), Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems.

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.

⚠WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

- In your hazard and risk analysis, consider all hazards that result from access to and operation on the network/fieldbus and develop an appropriate cybersecurity concept.
- Verify that the hardware infrastructure and the software infrastructure into which the machine is integrated as well as all organizational measures and rules covering access to this infrastructure consider the results of the hazard and risk analysis and are implemented according to best practices and standards covering IT security and cybersecurity (such as: ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/ IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security, SE recommended Cybersecurity Best Practices*).
- Verify the effectiveness of your IT security and cybersecurity systems using appropriate, proven methods.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

(*) : SE Recommended Cybersecurity Best Practices can be downloaded on SE.com.

⚠WARNING

LOSS OF CONTROL

Perform a comprehensive commissioning test to verify that communication monitoring properly detects communication interruptions.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

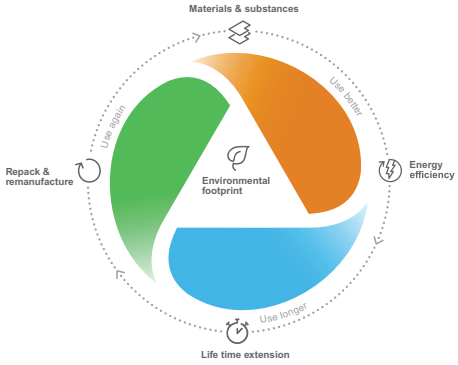
- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

The Environmental Data Program is a framework for how we measure, categorize, and compare the environmental attributes and footprint of our products.

Using a rigorous, fact-based methodology, the program provides environmental data from across the product lifecycle.

Five data categories across the product lifecycle



Use Better: How sustainable a product is, including environmental footprint, materials and substances, packaging, and energy efficiency.

Use Longer: How a product's life time can be effectively extended in terms of repairability and updatability.

Use Again: How a product can be reused, from dismantling and remanufacturing to recyclability and manufacturer take back.

With this transparent, verified data, customers and partners are empowered to make conscious environmental choices and accurately evaluate and report on sustainability performance.

All our hardware offers have an associated environmental data available on se.com product pages.

Refer to Environmental Data Program for more information.

Related Documents

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on www.se.com.

The internet site provides the information you need for products and solutions:

- The whole catalog for detailed characteristics and selection guides,
- The CAD files to help design your installation, available in over 20 different file formats,
- All software and firmware to maintain your installation up to date,

- A large quantity of White Papers, Environment documents, Application solutions, Specifications... to gain a better understanding of our electrical systems and equipment or automation,
- And finally all the User Guides related to your drive, listed below:

Title of Documentation	Reference Number	
Catalog: Altivar Building ATH200	DIA2ED2250901EN (English)	DIA2ED2250901FR (French)
ATH200 Getting Started	JPS43191 (English), JPS43192 (French), JPS43193 (German), JPS43194 (Spanish)	JPS43198 (Italian), JPS43199 (Chinese), JPS43197 (Portuguese), JPS43195 (Turkish)
ATH200 Getting Started Annex (SCCR)	JPS43196 (English)	
ATH200 Installation manual	JPS43203 (English), JPS43204 (French), JPS43202 (German), JPS43201 (Spanish),	JPS43200 (Italian), JPS43208 (Chinese), JPS43205 (Portuguese), JPS43209 (Turkish)
ATH200 Programming manual	JPS43207 (English), JPS43206 (French), JPS43212 (German), JPS43211 (Spanish),	JPS43210 (Italian), JPS43213 (Chinese), JPS43214 (Portuguese), JPS43215 (Turkish)
ATH200 ATEX manual	JPS43218 (English)	
ATH200 Modbus manual	JPS43217 (English)	
ATH200 BACnet manual	JPS43216 (English)	
ATH200 Communication Parameters	JPS43219 (English)	
ATH200 Safety Functions manual	JPS43226 (English), JPS43227 (French), JPS43229 (German),	JPS43233 (Spanish), JPS43231 (Italian), JPS43232 (Chinese)
ATH200 - ATV Logic manual	JPS43234 (English), JPS43230 (French), JPS43236 (German),	JPS43238 (Spanish), JPS43237 (Italian), JPS43235 (Chinese)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)	
ATH200: DTM	ATH200 DTM Library (English, French, Spanish, Italian, German, Chinese)	
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019-340 (English)	

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Terminology used in this document

The technical terms, terminology, and the corresponding descriptions in this manual normally use the terms or definitions in the relevant standards.

Among others, these standards include:

- ISO 13849: The Foundation of Functional Safety in the Machinery
- IEC 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements.
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC 61508 Ed.2 series: Functional safety of electrical/electronic/ programmable electronic safety-related.
- IEC 61784 series: Industrial communication networks - Profiles.
- IEC 61800 series: Adjustable speed electrical power drive systems.
- IEC 62443: Security for industrial automation and control systems.

In the area of drive systems this includes, but is not limited to, terms such as **error, error message, failure, fault, fault reset, protection, safe state, safety function, warning, warning message**, and so on.

In addition, the term **zone of operation** is used in conjunction with the description of specific hazards, and is defined as it is for a **hazard zone** or **danger zone** in the EC Machinery Directive (2006/42/EC) and in ISO 12100-1.

Contact us

Select your country on www.se.com/contact.

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

General Information

What’s in This Part

Introduction

Overview

⚠WARNING

INEFFECTIVE SAFETY FUNCTIONS

- Verify that a risk assessment as per ISO 12100-1 and/or any other equivalent assessment has been performed before this product is used.
- Verify that only persons who are trained and certified experts in safety engineering and who are familiar with all safety-related standards, provisions, and regulations such as, but not limited to, IEC 61800-5-2 work with this product.
- Verify that only persons who are thoroughly familiar with the safety-related applications and the non-safety-related applications as well as the hardware used to operate the machine/process, work with this product.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Only start the machine/process if there are no persons or obstructions in the zone of operation.
- Only make modifications of any type whatsoever, including, but not limited to, parameters, settings, configurations, hardware, if you fully understand all effects of such modifications.
- Verify that modifications do not compromise or reduce the Safety Integrity Level (SIL), Performance Level (PL) and/or any other safety-related requirements and capabilities defined for your machine/process.
- After modifications of any type whatsoever, restart the machine/process and verify the correct operation and effectiveness of all functions by performing comprehensive tests for all operating states, the defined safe state, and all potential error situations.
- If you have to commission or recommission the machine/process, perform a commissioning test pursuant to all regulations, standards, and process definitions applicable to your machine/process.
- Document all modifications in compliance with all regulations, standards, and process definitions applicable to your machine/process.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Connect the drive to be configured directly to the PC.
- Do not establish a connection via network/Fieldbus protocols from the PC to the drive to be configured.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The safety functions incorporated in ATH200 are intended to maintain the safe condition of the installation or prevent hazardous conditions arising at the installation. In some cases, further safety-related systems external to the drive (for example a mechanical brake) may be necessary to maintain the safe condition when electrical power is removed.

The safety functions are configured with SoMove software.

Integrated safety functions provide the following benefits:

- Additional standards-compliant safety functions
- No need for external safety-related devices
- Reduced wiring effort and space requirements
- Reduced costs

The ATH200 drives are compliant with the requirements of the standards in terms of implementation of safety functions.

Safety Functions as Defined by IEC 61800-5-2

Definitions

Acro-nym	Description
STO	**Safe Torque Off** No power that could cause torque or force is supplied to the motor.

Notation

The graphic display terminal (to be ordered separately - reference WV3A1111 and VW3A1006) menus are shown in square brackets.

The integrated 7-segment display terminal menus are shown in round brackets.

Parameter names are displayed on the graphic display terminal in square brackets.

Parameter codes are displayed on the integrated 7-segment display terminal in round brackets.

Certifications

EU Declaration of Conformity

The EU Declaration of Conformity, which includes compliance with the EMC Directive and other applicable EU legislation, can be obtained at www.se.com.

ATEX Certification

The ATEX certificate can be obtained on www.se.com.

Functional Safety Certification

The integrated safety functions are compatible and certified according to certified according to IEC 61800-5-2 Ed.1 (2007) and Ed.2 (2016) Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional.

IEC 61800-5-2, as a product standard, sets out safety-related considerations of Power Drive System Safety Related PDS (SR)s in terms of the framework of the IEC 61508 Ed.2 series of standards.

Compliance with the IEC 61800-5-2 standard, for the safety functions described below, will facilitate incorporation of a PDS (SR) (Power Drive System suitable for use in safety-related applications) into a safety-related control system using the principles of IEC 61508, or IEC 13849-1, as well as IEC 62061 for process systems and machinery.

The defined safety functions are:

- SIL2 and SIL3 capability in compliance with IEC 61800-5-2 and the IEC 61508 Ed.2 series.
- Performance Level d and e in compliance with IEC 13849-1.
- Compliant with Category 3 and 4 of European standard IEC 13849-1.

Also refer to safety function Capability.

The safety demand operating mode is considered to be high demand or continuous mode of operation according to the IEC 61800-5-2 standard.

The functional safety certificate is accessible on www.se.com.

Basics

Functional Safety

Automation and safety engineering are two areas that were completely separate in the past but have recently become more and more integrated.

The engineering and installation of complex automation solutions are greatly simplified by integrated safety functions.

Usually, the safety engineering requirements depend on the application.

The level of requirements results from the risk and the hazard potential arising from the specific application.

IEC 61508 Standard

The standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems covers the safety-related function.

Instead of a single component, an entire function chain (for example, from a sensor through the logical processing units to the actuator) is considered as a unit.

This function chain must meet the requirements of the specific safety integrity level as a whole.

Systems and components that can be used in various applications for safety tasks with comparable risk levels can be developed on this basis.

SIL - Safety Integrity Level

The standard IEC 61508 defines 4 safety integrity levels (SIL) for safety functions.

SIL1 is the lowest level and SIL4 is the highest level.

A hazard and risk analysis serves as a basis for determining the required safety integrity level.

This is used to decide whether the relevant function chain is to be considered as a safety function and which hazard potential it must cover.

PFH - Probability of a Dangerous Hardware Failure Per Hour

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected faults, depending on the required SIL.

All components of a safety function must be subjected to a probability assessment to evaluate the effectiveness of the measures implemented for controlling detected faults.

This assessment determined the PFH (Average frequency of dangerous failure) for a safety system.

This is the probability per hour that a safety system fails in a hazardous manner and the safety function cannot be correctly executed.

Depending on the SIL, the PFH must not exceed certain values for the entire safety system.

The individual PFH values of a function chain are added. The result must not exceed the maximum value specified in the standard.

Performance level	Average frequency of dangerous failure (PFH) at high demand or continuous demand
4	$\geq 10^{-9} ... < 10^{-8}$
3	$\geq 10^{-8} ... < 10^{-7}$
2	$\geq 10^{-7} ... < 10^{-6}$
1	$\geq 10^{-6} ... < 10^{-5}$

PL - Performance Level

The standard ISO 13849-1 defines 5 Performance levels (PL) for safety functions.

a is the lowest level and e is the highest level.

Five levels (a, b, c, d, and e) correspond to different values of Average frequency of dangerous failure.

Performance level	Probability of a dangerous Hardware Failure per Hour
e	$\geq 10^{-8} ... < 10^{-7}$
d	$\geq 10^{-7} ... < 10^{-6}$
c	$\geq 10^{-6} ... < 3 * 10^{-6}$
b	$\geq 3 * 10^{-6} ... < 10^{-5}$
a	$\geq 10^{-5} ... < 10^{-4}$

HFT - Hardware Fault Tolerance and SFF - Safe Failure Fraction

Depending on the SIL for the safety system, the IEC 61508 standard requires a specific hardware fault tolerance HFT in connection with a specific proportion of safe failures SFF (Safe Failure Fraction).

The hardware fault tolerance is the ability of a system to execute the required safety function in spite of the presence of one or more hardware faults.

The SFF of a system is defined as the ratio of the rate of safe failures and dangerous detected failures to the total failure rate of the system.

$SFF = (\Sigma\lambda_s + \Sigma\lambda_{Dd})/(\Sigma\lambda_s + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$

According to IEC 61508, the maximum achievable SIL of a system is partly determined by the hardware fault tolerance HFT and the safe failure fraction SFF of the system.

IEC 61508 distinguishes two types of subsystem (type A subsystem, type B subsystem).

These types are specified on the basis of criteria which the standard defines for the safety-relevant components.

SFF	HFT type A subsystem			HFT type B subsystem		
	0	1	2	0	1	2
< 60%	SIL1	SIL2	SIL3	----	SIL1	SIL2
60% ...< 90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
60% ...< 99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

PFD - Probability of Failure on Demand

The standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum Safe Failure Fraction. The concept of 'dangerous failure' must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

The PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) of low demand operation for different SILs are defined in IEC 61508 are as follows:

SIL	PFD	PFD (power	RRF
1	0.1 - 0.01	10^{-1} - 10^{-2}	10 - 100
2	0.01 - 0.001	10^{-2} - 10^{-3}	100 - 1000
3	0.001 - 0.0001	10^{-3} - 10^{-4}	1000 - 10,000
4	0.0001 - 0.00001	10^{-4} - 10^{-5}	10,000 - 100,000

In high demand or continuous operation, these changes to the following:

SIL	PFH	PFH (power	RRF
1	0.00001 - 0.000001	10^{-5} - 10^{-6}	100,000 - 1,000,000
2	0.000001 - 0.0000001	10^{-6} - 10^{-7}	1,000,000 - 10,000,000
3	0.0000001 - 0.00000001	10^{-7} - 10^{-8}	1000 - 10,000
4	0.00000001 - 0.000000001	10^{-8} - 10^{-9}	100,000,000 - 1,000,0000,000

The hazards of a control system must be identified then analyzed in a risk analysis. These risks are gradually mitigated until their overall contribution to the hazard is deemed to be acceptable. The tolerable level of these risks is specified as a safety requirement in the form of a target probability of a dangerous failure over a given period, stated as a discrete SIL level.

Fault Avoidance Measures

Systematic errors in the specifications, in the hardware and the software, usage faults and maintenance faults in the safety system must be avoided to the maximum degree possible. To meet these requirements, IEC 61508 specifies a

number of measures for fault avoidance that must be implemented depending on the required SIL. These measures for fault avoidance must cover the entire life cycle of the safety system, i.e. from design to decommissioning of the system.

Description

What’s in This Part

Safety Function STO (Safe Torque Off)

Overview

The safety function STO (Safe Torque Off) does not remove power from the DC bus. The safety function STO only removes power to the motor. The DC bus voltage and the mains voltage to the drive are still present.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK

- Do not use the safety function STO for any other purposes than its intended function.
- Use an appropriate switch, that is not part of the circuit of the safety function STO, to disconnect the drive from the mains power.

Failure to follow these instructions will result in death or serious injury.

When the safety function STO is triggered, the power stage is immediately disabled. In the case of vertical applications or external forces acting on the motor shaft, you may have to take additional measures to bring the motor to a standstill and to keep it at a standstill when the safety function STO is used, for example, by using a service brake.

⚠ WARNING

INSUFFICIENT DECELERATION OR UNINTENDED EQUIPMENT OPERATION

- Verify that using the safety function STO does not result in unsafe conditions.
- If standstill is required in your application, ensure that the motor comes to a secure standstill when the safety function STO is used.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This function brings the machine safely into a no-torque state and / or prevents it from starting accidentally.

The safe torque-off (safety function STO) function can be used to effectively implement the prevention of unexpected start-up functionality, thus making stops safe by preventing the power only to the motor, while still maintaining power to the main drive control circuits.

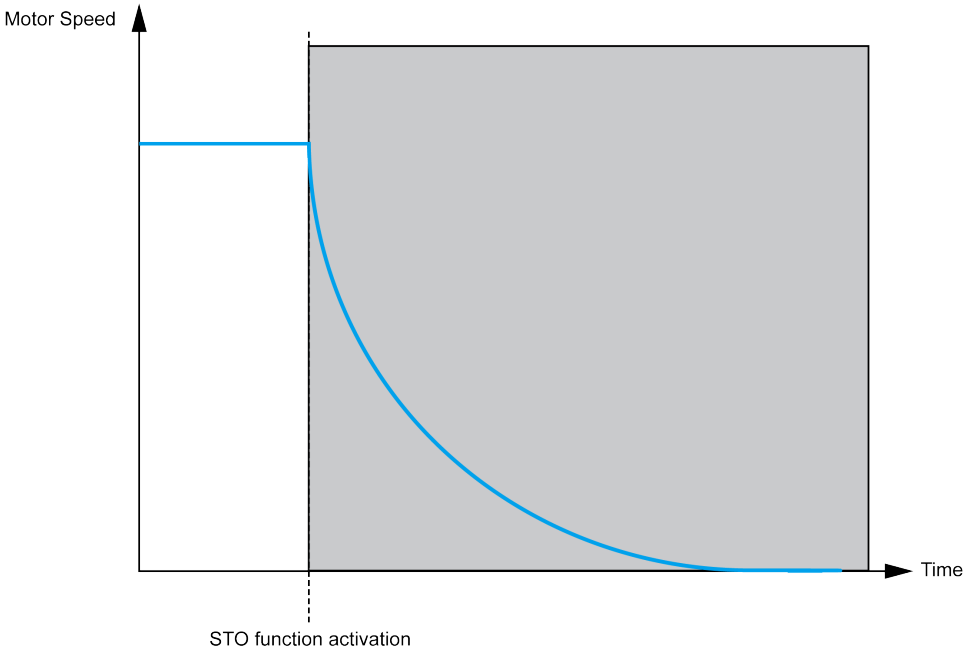
The principles and requirements of the prevention of unexpected start-up are described in the standard EN 1037:1995+A1.

The digital input STO is assigned to this safety function and cannot be modified.

If a paired terminal line in 2 channels is required to trigger safety function STO, the function can also be enabled by the safety-related digital inputs.

The safety function STO is configured with the commissioning software.

The safety function STO status can be displayed using the HMI of the drive or using the commissioning software.



Safety Function STO Standard Reference

The safety function STO is defined in section 4.2.2.2 of standard IEC 61800-5-2 (edition 1.0 2007.07) and in section 4.2.3.2 of edition 2.0 (2016-04):

Power, that can cause rotation (or motion in the case of a linear motor), is not applied to the motor.The PDS(SR) (power drive system suitable for use in safety-related applications) will not provide energy to the motor which can generate torque (or force in the case of a linear motor).

- NOTE 1: This safety function corresponds to an uncontrolled stop in accordance with stop category 0 of IEC 60204-1.
- NOTE 2: This safety function may be used where power removal is required to prevent an unexpected start-up.
- NOTE 3: In circumstances where external influences (for example, falling of suspended loads) are present, additional measures (for example, mechanical brakes) may be necessary to prevent any hazard.
- NOTE 4: Electronic equipment and contactors do not provide adequate protection against electric shock, and additional insulation measures may be necessary.

Safety Function (SF) Level Capability for Safety Function STO

Configuration	**SIL** **Safety Integrity Level according to IEC 61508**	**PL** **Performance Level according to ISO 13849-1**
STO with or without safety module	SIL 2	PL d
STO & LI3 with or without safety module	SIL 3	PL e
LI3 and LI4	SIL 2	PL d
LI5 and LI6	SIL 2	PL d

Emergency Operations

Standard IEC 60204-1 introduces 2 emergency operations:

- **Emergency switching-off**:

  This function requires external switching components, and cannot be accomplished with drive based functions such as safe torque-off (STO).

- **Emergency stop**:

  An emergency stop must operate in such a way that, when it is activated, the hazardous movement of the machinery is stopped and the machine is unable to start under any circumstances, even after the emergency stop is released.

  An emergency stop shall function either as a stop category 0 or as a stop category 1.

  Stop category 0 means that the power to the motor is turned off immediately. Stop category 0 is equivalent to the safe torque-off (STO) function, as defined by standard EN 61800-5-2.

  In addition to the requirements for stop (see 9.2.5.3 of IEC 60204-1), the emergency stop function has the following requirements:

  - it shall override all other functions and operations in all modes.
  - This reset shall be possible only by a manual action at that location where the command has been initiated. The reset of the command shall not restart the machinery but only permit restarting.
  - For the machine environment (IEC 60204-1 and machinery directive), when safety function STO is used to manage an emergency stop category 0, the motor must not restart automatically when safety function STO has been triggered and deactivated (with or without a power cycle). This is the reason why an additional safety module is required if the machine restarts automatically after the safety function STO has been deactivated.

Behavior of Safety Functions

What’s in This Part

Limitations

Prerequisites for Using Safety Functions

Following conditions have to be fulfilled for correct operation:

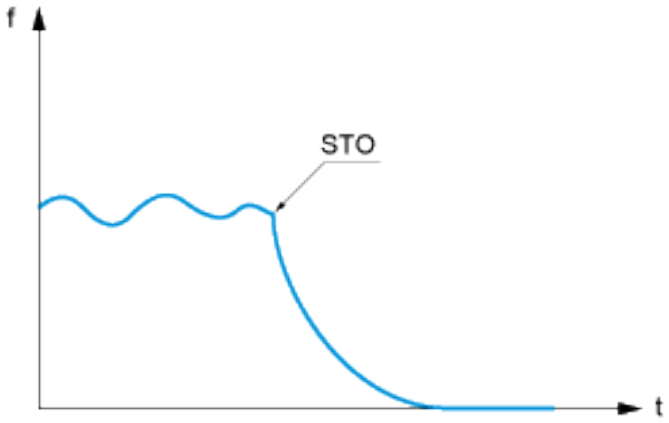
- The motor size is adequate for the application and is not at the limit of its capacity.
- The drive size has been correctly chosen for the line supply, sequence, motor, and application and is not at the limit of their capacities as stated in the catalog.
- If required, the appropriate options are used.

  Example: dynamic braking resistor or motor choke.
- The drive is correctly set up with the correct speed loop and torque characteristics for the application; the reference frequency profile applied to the drive control loop is followed.

Allowed and Unallowed Application for Safety Function

Allowed Application

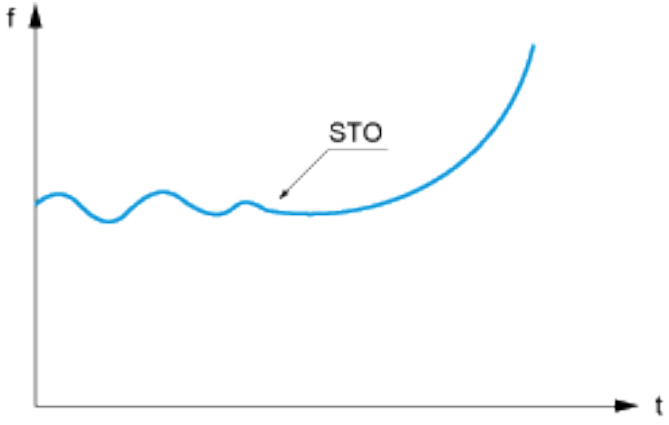
Allowed sharp of stop after STO request or freewheel stop.



Unallowed Application

Applications with acceleration of the load after drive shut down or where there are long/permanent regenerative braking cycles are not allowed.

Sudden stopping is not allowed after an STO request or freewheel stop.



Examples: Vertical Conveyors, Vertical hoist, Lifts, or Winders.

Requirements on Digital Inputs

- Sink mode is not used with the safety function. If you use the safety function, you need to wire the digital inputs in source mode.
- PTC on DI6 is incompatible with the safety function set on this input. If you are using the safety function on DI6, do not set the PTC switch to PTC
- If you are using the pulse input, you cannot set the safety function on DI5 at the same time.

Detected Fault Inhibition

When a safety function has been configured, the error **[Safety Function Fault]** SAFF cannot be inhibited by the function **[Fault Inhibit assign.]** InH

Priority Between Safety Functions

The safety function STO has the highest priority. If the safety function STO is triggered, a Safe Torque Off is performed regardless of which other functions are active.

Factory Settings

If the safety functions are configured and you restore the factory settings, only the parameters which are not safety-related will be reset to the factory setting. The settings of safety-related parameters can only be reset using the commissioning software, for more information see Commissioning, page 59.

Configuration Download

You can transfer a configuration in all situations. If a safety function has been configured, the functions using these same digital inputs will not be configured.

For example: If the downloaded configuration has functions (Preset speed,...) on LI3-4-5-6 and if the drive has a safety function configured on these digital inputs, safety function will not be erased. It is the functions that have the same digital input as safety functions that are not transferred. Multiconfiguration/multimotor and macro configuration obey the same rules.

Safety Functions Visualization via HMI

What’s in This Part

Status of Safety Functions

Description

The status of the safety functions can be displayed using the HMI of the drive or using the commissioning software. HMI of the drive can be the local HMI on the product or the graphic display terminal or the remote display terminal. There is one register for each safety function. See introduction, page 15 for more information about the safety functions.

To access these registers with an HMI: **[2 MONITORING]** `MON-` --> **[MONIT. SAFETY]** `SAF-`

- **[STO status]** `STOS`: Status of the safety function STO (Safe Torque Off)

The status registers are not approved for any type of safety-related use.

For more information about these registers, see ATH200 Visualization and Status of Safety Functions, page 65 on www.se.com.

Error Code Description

Description

When an error is detected by the safety function, the drive displays **[Safety function fault]** (SAFF). This detected error can only be reset after powering the drive OFF/ON.

for more information, you can access to the registers to find out the possible reasons for triggering.

These registers can be displayed using the graphic display terminal or the commissioning software:

[DRIVE MENU] --> **[MONITORING]** --> **[DIAGNOSTICS]** --> **[MORE FAULT INFO]**

SFFE [Safety Function Error Register]

Bit	Description
Bit0=1	Logic inputs debounce time-out (verify value of debounce time LIDT according to the application)
Bit1	Reserved
Bit2=1	Motor speed sign has changed
Bit3=1	Motor speed reached trip area
Bit4	Reserved
Bit5	Reserved
Bit6=1	Motor speed sign has changed
Bit7=1	Motor speed reached trip area
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13=1	Motor speed measurement is not possible
Bit14=1	Motor ground short-circuit detected (verify the motor wiring connection)
Bit15=1	Motor phase to phase short-circuit detected (verify the motor wiring connection)

This register is reset after powering OFF/ON.

This register can also be accessed from **[DRIVE MENU]** --> **[MONITORING]** --> **[MONIT. SAFETY]**

SAFI [Safety Error Register 1]

This is an application control error register.

Bit	Description
Bit0=1	PWRM consistency detected error
Bit1=1	Safety functions parameters detected error

Bit	Description
Bit2=1	Application auto test has detected an error
Bit3=1	Diagnostic verification of safety function has detected an error
Bit4=1	Logical input diagnostic has detected an error
Bit5=1	Extended detected error, for details refer { SF04} Safety Fault Subregister 04, page 39.
Bit6=1	Application watchdog management active
Bit7=1	Motor control detected error
Bit8=1	Internal serial link core detected error
Bit9=1	Logical input activation detected error
Bit10=1	Safe Torque Off function has triggered an error
Bit11=1	Application interface has detected an error of the safety functions
Bit12=1	Detected an error of the safety functions
Bit13=1	Safely Limited Speed function has triggered an error
Bit14=1	Motor data is corrupted
Bit15=1	Internal serial link data flow detected error, for details refer to **[Safety Subcode 11]**, page 42.

This register is reset after powering OFF/ON.

SAF2 [Safety Error Register 2]

This is a motor control error register.

Bit	Description
Bit0=1	Consistency stator frequency verification has detected an error
Bit1=1	Stator frequency estimation detected error
Bit2=1	Motor control watchdog management is active
Bit3=1	Motor control hardware watchdog is active
Bit4=1	Motor control auto test has detected an error
Bit5=1	Chain testing detected error
Bit6=1	Internal serial link core detected error
Bit7=1	Direct short-circuit detected error
Bit8=1	PWM driver detected error
Bit9=1	Stop power detected error
Bit10	Reserved
Bit11=1	Application interface has detected an error of the safety functions
Bit12	Reserved
Bit13	Reserved
Bit14=1	Motor data is corrupted
Bit15=1	Internal serial link data flow detected error

This register is reset after powering OFF/ON.

SF00 [Safety Subcode 0]

This is an application auto test error register.

Bit	Description
Bit0	Reserved
Bit1=1	Ram stack overflow
Bit2=1	Ram address integrity detected error
Bit3=1	Ram data access detected error
Bit4=1	Flash checksum detected error
Bit5	Reserved
Bit6=1	Consistency verification - ram address variables
Bit7 Bit7=1	Consistency verification - ram data access variables
Bit8 Bit8=1	Consistency verification - DMA channels variables
Bit9=1	Fast task overflow
Bit10=1	Slow task overflow
Bit11=1	Application task overflow
Bit12	Reserved
Bit13	Reserved
Bit14=1	PWRM line is not activated during initialization phase
Bit15=1	Application hardware watchdog is not running after initialization

This register is reset after powering OFF/ON.

SF01 [Safety Subcode 1]

This is a digital input diagnostics error register

Bit	Description
Bit0=1	Management - state machine detected error
Bit1=1	Data required for test management are corrupted
Bit2=1	Channel selection detected error
Bit3=1	Testing - state machine detected error
Bit4=1	Test request is corrupted
Bit5=1	Pointer to test method is corrupted
Bit6=1	Incorrect test action provided
Bit7=1	Detected error in results collecting
Bit8=1	DI3 detected error.Cannot activate safety function
Bit9=1	DI4 detected error. Cannot activate safety function
Bit10=1	DI5 detected error. Cannot activate safety function
Bit11=1	DI6 is detected error. Cannot activate safety function
Bit12=1	Test sequence updated while a diagnostic is in progress
Bit13=1	Detected error in test pattern management

Bit	Description
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF02 [Safety Subcode 2]

This is an application watchdog management detected error register.

Bit	Description
Bit0=1	Fast task detected error
Bit1=1	Slow task detected error
Bit2=1	Application task detected error
Bit3=1	Background task detected error
Bit4=1	Safety function fast task/input detected error
Bit5=1	Safety function slow task/input detected error
Bit6=1	Safety function application task/inputs detected error
Bit7=1	Safety function application task/treatment detected error
Bit8=1	Safety function background task detected error
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF03 [Safety Subcode 3]

Bit	Description
Bit0=1	Debounce time out
Bit1=1	Input not consistent
Bit2=1	Consistency verification - state machine detected error
Bit3=1	Consistency verification - debounce timeout corrupted
Bit4=1	Response time data detected error
Bit5=1	Response time corrupted
Bit6=1	Undefined consumer queried
Bit7=1	Configuration detected error
Bit8=1	Inputs are not in nominal mode
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved

Bit	Description
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF04 [Safety Subcode 04]

This is a **[Safe Torque Off]** STo detected error register

Bit	Description
Bit0=1	No signal configured
Bit1=1	State machine detected error
Bit2=1	Internal data detected error
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8=1	SMS overspeed detected error
Bit9=1	SMS internal detected error
Bit10	Reserved
Bit11	Reserved
Bit12=1	SFO SAFF Internal detected error
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF05 [Safety Subcode 5]

Bit	Description
Bit0=1	State machine detected error
Bit1=1	Motor speed sign has changed during stop
Bit2=1	Motor speed has reached the frequency limit threshold.
Bit3=1	Theoretical motor speed corrupted
Bit4=1	Unauthorized configuration
Bit5=1	Theoretical motor speed computation detected error
Bit6	Reserved
Bit7=1	Speed sign verification: consistency detected error
Bit8=1	Internal SS1 request corrupted
Bit9	Reserved
Bit10	Reserved

Bit	Description
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

5F06 [Safety Subcode 6]

Bit	Description
Bit0=1	Reserved
Bit1=1	Reserved
Bit2=1	Reserved
Bit3=1	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

5F07 [Safety Subcode 7]

This is an application watchdog management detected error register.

Bit	Description
Bit0	Reserved
Bit1	Reserved
Bit2	Reserved
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved

Bit	Description
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF08 [Safety Subcode 8]

This is an application watchdog management detected error register

Bit	Description
Bit0=1	PWM task detected error
Bit1=1	Fixed task detected error
Bit2=1	ATMC watchdog detected error
Bit3=1	DYNFCT watchdog detected error
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SF09 Safety Subcode 9

This is a motor control auto test detected error register.

Bit	Description
Bit0	Reserved
Bit1=1	Ram stack overflow
Bit2=1	Ram address integrity detected error
Bit3=1	Ram data access detected error
Bit4=1	Flash checksum error
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved

Bit	Description
Bit9=1	1 ms task overflow
Bit10=1	PWM task overflow
Bit11=1	Fixed task overflow
Bit12	Reserved
Bit13	Reserved
Bit14=1	Unwanted interruption
Bit15=1	Hardware WD is not running after initialization

This register is reset after powering OFF/ON.

SFI0 [Safety Subcode 10]

This is a motor control direct short-circuit detected error register

Bit	Description
Bit0=1	Ground short circuit - configuration detected error
Bit1=1	Phase to phase short circuit - configuration detected error
Bit2=1	Ground short circuit
Bit3=1	Phase to phase short circuit
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

SFI1 [Safety Subcode 11]

This is a motor control dynamic verification of activity detected error register

Bit	Description
Bit0=1	Application requested a diagnostic of direct short-circuit
Bit1=1	Application requested consistency verification of stator frequency estimation (voltage and current)
Bit2=1	Application requested diagnostic of SpdStat provided by motor control
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved

Bit	Description
Bit6	Reserved
Bit7	Reserved
Bit8=1	Motor control diagnostic of direct short circuit is enabled
Bit9=1	Motor control consistency verification of stator frequency estimation is enabled
Bit10=1	Motor control diagnostic of SpdStat provided by motor control is enabled
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

Technical Data

What’s in This Part

Electrical Data

Logic Type

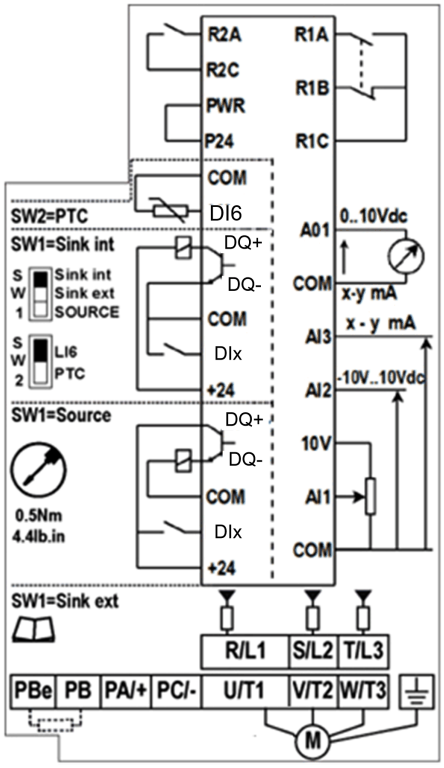
The drive digital inputs and digital outputs can be wired for logic type 1 or logic type 2.

Logic Type	Active State
1	The output draws current (Sink) Current flows to the input
2	The output supply flows from the input current Current (Source)

Safety functions must only be used in source mode.

Signal inputs are protected against reverse polarity, outputs are protected against short-circuits. The inputs and outputs are galvanically isolated.

Cabling Label



Getting and Operating the Safety Function

Digital Input

General-purpose digital inputs can be used to trigger a safety function. Digital inputs have to be combined in pairs to obtain a redundant request. There are only 4 general-purpose digital inputs that can be linked to safety functions (DI3, DI4, DI5, DI6).The pairs of digital inputs are fixed and are:

- DI3 and DI4
- DI5 and DI6
- Another combination is only possible for the STO function: DI3 and STO

Pairs of digital inputs can only be assigned once when they are linked to a safety function. When you set a safety function on an digital input you cannot set another function (safety or other) on this digital input. If you set a non-safety function on an digital input you cannot set a safety function on this digital input.

The SISTEMA Software

The SISTEMA software allows machine developers and testers of safety-related machine controls to evaluate the safety standard or level of their machine in the context of ISO 13849-1. The tool allows you to model the structure of safety-related control components based on the designated architectures, allowing automated calculation of the reliability standards with various levels of detail, including that of the Performance Level (PL).

The ATH2xx Libraries are available from www.se.com.

Preventa Safety Relays

Used for the creation of complex safety functions in machines, allowing management of the I/O, and also for protecting both the operator and the machine.

The Preventa range of products feature microprocessor-based technology using the redundancy principle, and are essential to ensure safe operation of dangerous machinery.

Safety Function Capability

PDS (SR) safety functions are part of an overall system

If the qualitative and quantitative safety objectives determined by the final application require some adjustments to ensure safe use of the safety functions, the integrator of the BDM (Basic Drive Module) is responsible for these additional changes (for example, managing the mechanical brake on the motor).

Also, the output data generated by the use of safety functions (fault relay activation, error codes or information on the display, etc.) is not considered to be safety-related data.

Machine Application Function Configuration

		STO		**STO**	
		STO	STO and DI3	DI3 DI4	DI5 DI6
Standard	IEC 61800-5-2 / IEC 61508 /	SIL2	SIL3	SIL2	
	IEC 62061 (1)	Maximum SIL2	Maximum SIL3	Maximum SIL2	
	ISO 13849-1 (2)	Category 3	Category 4	Category 3	
		PL d	PL e	PL d	
	IEC 60204-1 (3)	Category stop 0	Category stop 0	Category stop 0	

(1) Because the IEC 62061 standard concerns integration, this standard distinguishes the overall safety function (which is classified SIL2 or SIL3 for ATH200 according to the diagrams Process system SF - Case 1 and Process system SF - Case 2 from components which constitute the safety function (which is classified SIL2 CL or SIL3 CL for ATH200).

(2) According to table 4 of EN 13849-1 (2008).

(3) If protection against supply interruption or voltage reduction and subsequent restoration is needed according to IEC 60204-1, a safety module type Preventa XPS AF or equivalent must be used.

Process Application Function Configuration

		STO		**STO (3)**	
		STO	STO and DI3	DI3 DI4	DI5 DI6
Standard	IEC 61800-5-2 IEC 61508	SIL2	SIL3	SIL2	
	IEC 62061 (1)	SIL2 CL	SIL3 CL	SIL2 CL	

(1) Because the IEC 62061 standard concerns integration, this standard distinguishes the overall safety function (which is classified SIL2 or SIL3 for ATH200 according to diagrams CASE 1 and CASE 2 from components which constitute the safety function (which is classified SIL2 CL or SIL3 CL for ATH200).

(2) SS1 type C: the power drive initiates the motor deceleration and initiates the STO function after an application specific time delay.

(3) SS1 type B: the power drive initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit.

Input Signal Safety Functions

Input signals safety functions	Units	Value for DI3 to DI6	Value for STO
Logic 0 (Ulow)	V	< 5	< 2
Logic 1 (Uhigh)	V	> 11	> 17
Impedance (24V)	kΩ	3.5	1.5
Debounce time	ms	< 1	< 1
Response time of safety function	ms	< 10	< 10

Summary of the Reliability Study

Function	Standard	Input	STO input	STO input & DI3	DI3 & DI4 or DI5 & DI6
STO	IEC 61508	SFF	96.7%	96%	94.8%
		PFD_{10y}	$7.26.10^{-4}$	$4.00.10^{-4}$	$2.44.10^{-3}$
		PFD_{1y}	$7.18.10^{-5}$	$3.92.10^{-5}$	$2.33.10^{-4}$
		PFH_{equ_1y}	8.20 FIT (1)	4.47 FIT (1)	26.6 FIT (1)
		Type	B	B	B
		HFT	1	1	0
		SIL capability	**2**	**3**	**2**
	IEC 62061 (2)	Maximum SIL	2	3	2
	IEC 60204–1	Category stop	0	0	0
	ISO 13849-1 (3)	PL	d	e	d
		Category	3	4	3
		DC	93.1%	91.5%	90%
		MTTFd in years	13900	“L1” 3850 “L2” 29300	4290

(1) FIT: Failure In Time = 10^{-9} failure per hour.

(2) Because the IEC 62061 standard concerns integration, this standard distinguishes the overall safety function (which is classified SIL2 or SIL3 for ATH200 according to diagrams Process system SF - Case 1 and Process system SF - Case 2, from components which constitute the safety function (which is classified SIL2 CL or SIL3 CL for ATH200).

(3) According to table 4 of EN 13849-1 (2008).

Preventive annual activation of the safety function is recommended.

However, the safety levels can be obtained (with lower margins) without annual activation.

For the machine environment, a safety module is required for the STO function.

To avoid the use of a safety module, the Restart function parameters must be part of the safety function.

Please refer to the description of advantages of the safety module.

NOTE: The table above is not sufficient to evaluate the PL of a PDS. The PL evaluation has to be done at the system level. The fitter or the integrator of the BDM (Basic Drive Module) has to do the system PL evaluation by including sensors data with numbers from the table above.

Debounce Time and Response Time

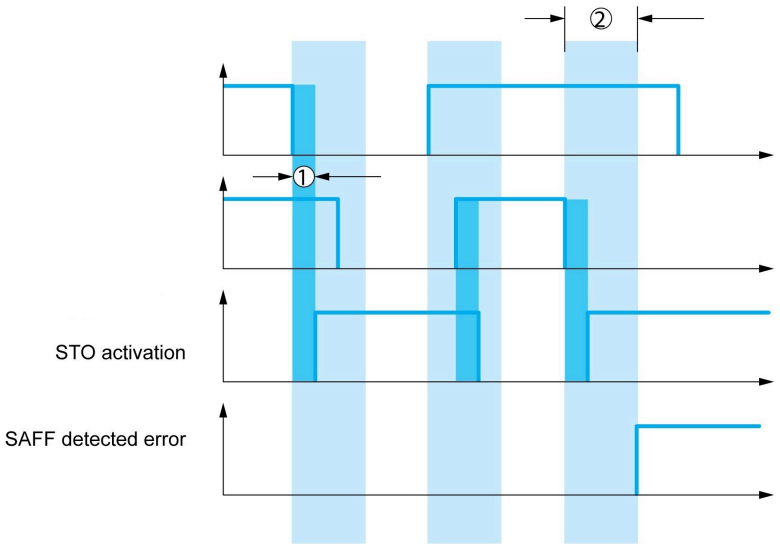
Description

On the ATH2xx, there are 2 parameters to configure digital inputs for safety function (DI3, DI4, DI5, DI6).

The consistency of each pair of digital input is verified continuously.

[LI debounce time] L id E : A logical state difference between DI3/DI4 or DI5/DI6 is allowed during debounce time, otherwise a detected error is activated.

[LI response time] L rE : The digital input response time manages the safety function activation shift.



① : Digital input Response Time

② : Digital input Debounce Time

Certified Architectures

What’s in This Part

Introduction

Certified Architectures

NOTE: For certification relating to functional aspects, only the PDS(SR) (Power Drive System suitable for use in safety-related applications) will be considered, not the complete system into which it is integrated to help to ensure the functional safety of a machine or a system/process.

Dedicated cabling examples will be provided for the following configurations:

- STO SIL2: Single STO input.
- STO SIL3: STO input combined with one digital input (DI).
- Functions using two digital inputs (DI): Applicable to STO.

These configurations can also be integrated with cabling compliant with ISO 13849 and IEC 60204-1, including a certified restart function using a safety relay.

Additionally:

- A safety relay can be used with the STO function.
- The system supports a choice of power supply: either provided by the drive or from an external PELV-compliant source.

Protected Cable Insulation

The STO safety function is triggered via 1 input. This circuit has to be wired according to protective cable insulation.

If short circuits and cross circuits can occur with safety-related signals and if they are not detected by upstream devices, protected cable installation as per ISO 13849-2 (Table D.4) is required.

In the case of an unprotected cable installation, the signal of a safety function in short circuit state may be connected to external voltage if a cable is damaged. In this case, the safety function is no longer operative.

For correct operation of Functional Safety "SAFE TORQUE OFF" circuit, adherence to the following conditions must be ensured:

- The cables and connectors must not be damaged.
- Correct contact between connector and socket must be guaranteed.

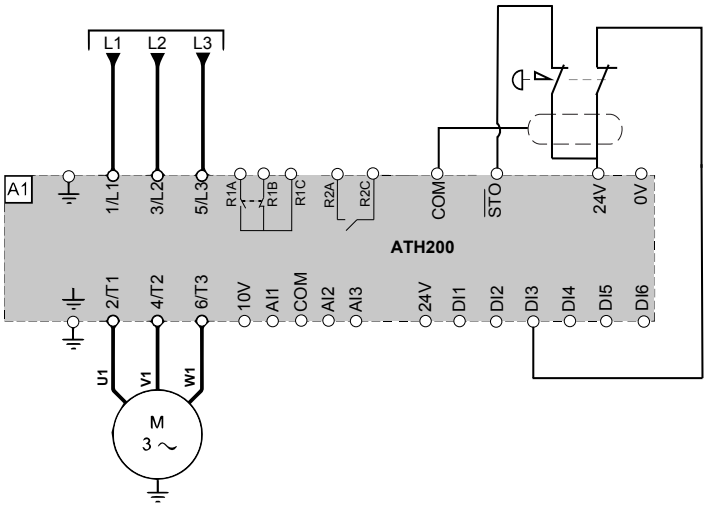
STO Supply

The Safe Torque Off (STO) inputs can be powered using one of the following methods:

- Internal 24 V Supply: Provided by the drive (subject to specific limitations).
- External 24 V Supply: Must be a PELV-compliant source (Protective Extra Low Voltage).

Drive Supply

Cabling example for STO SIL3 with STO and DI3 input:

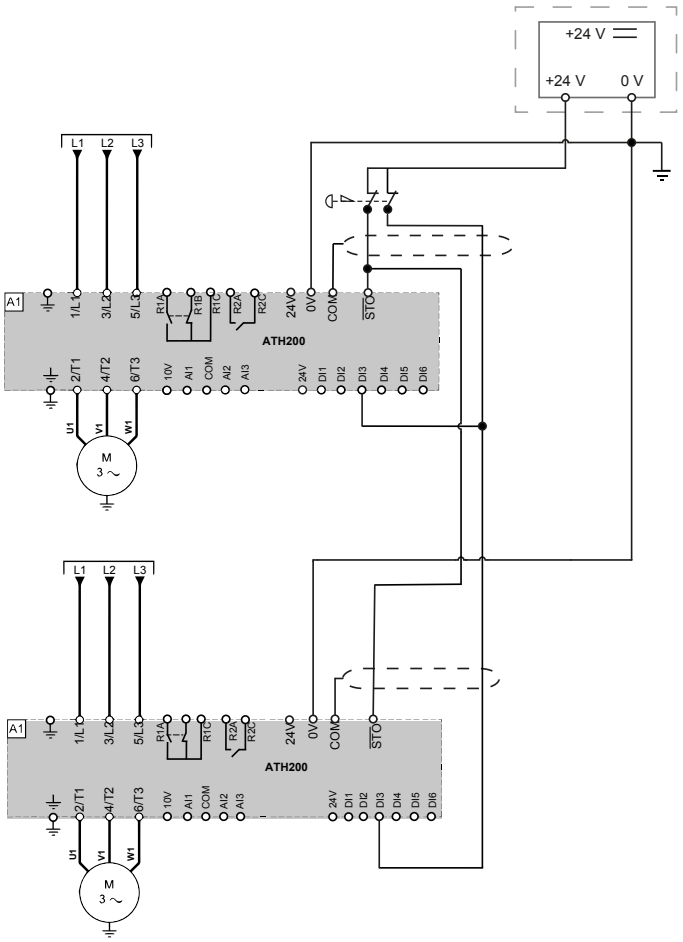


P24V current limit is 100 mA.

STO inputs drain 16 mA (impedance of 1.5 kOhm) and DI inputs drain 7 mA (impedance of 3.5 kOhm). Refer to Getting and Operating the Safety Function, page 46.

External Supply

Cabling example for STO SIL3:

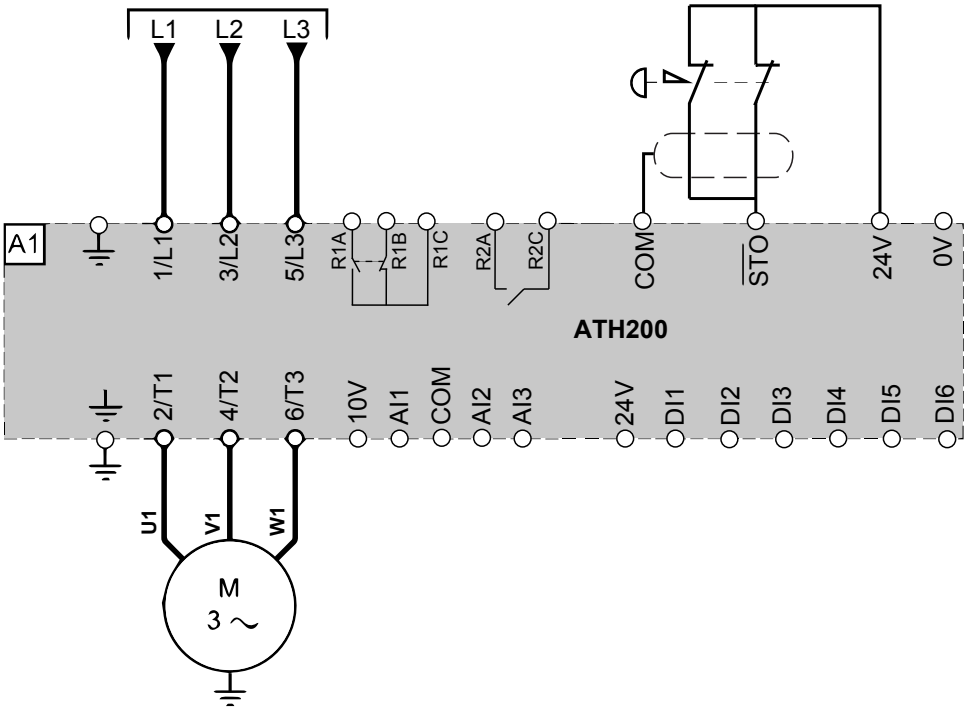


NOTE: The +24VDC power supply must meet the requirements of IEC 61131-2 (PELV standard power supply unit).

Cabling for STO SIL2

Single Drive Connection Diagram

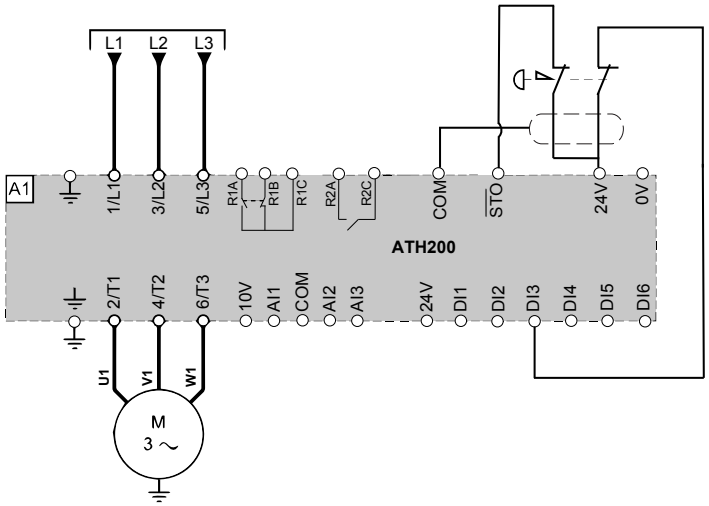
This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL2.



Cabling for STO SIL3

Single Drive Connection Diagram

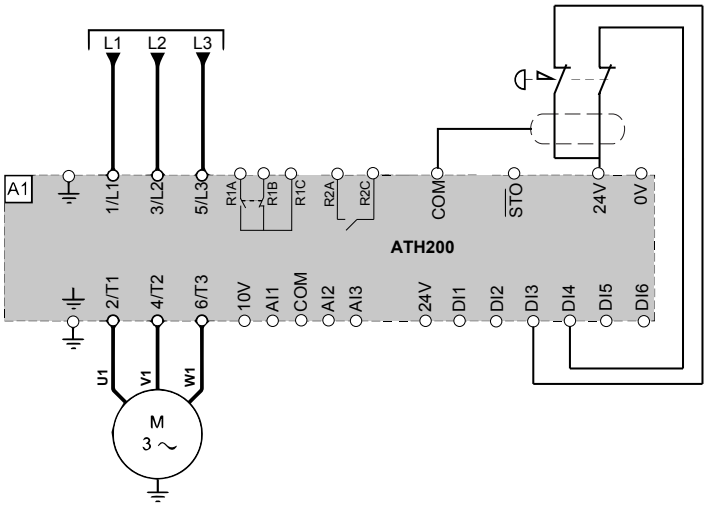
This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL3.



Cabling for Functions On DI

Single Drive Connection Diagram

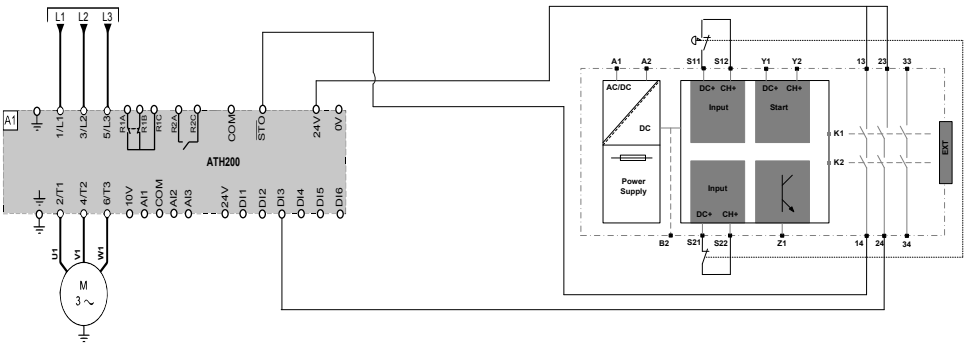
This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL2.



Cabling for Restart Function

Single Drive Connection Diagram

This connection diagram applies for a single drive configuration with the safety module type Preventa XPSUAF or equivalent according to according to ISO 13849 and IEC60204-1.



Refer to the XPSUAF Safety Module User Guide EIO0000003465 for more information on the power supply.

Commissioning

What's in This Part

Safety Functions Tab

Introduction

To access the safety function configuration, click the **Safety Functions** tab. This screen is read-only, allowing you to see all current safety function configurations.

The **Safety Functions** tab provides access to:

- an outline of the safety function features available on the ATH2xx (accessible Online/Offline)
- the status of all I/O in connected mode
- general information about the machine (Online/Offline).

It also provides access to the following dialog boxes:

- **Configuration**
  - **Configure** (only available in connected mode)
  - **Reset Configuration**
  - **Copy from DEVICE to PC**
  - **Copy from PC to DEVICE**
  - **Convert...**
- **Password Configuration**
  - **Modify Password**
  - **Reset Password**

Pre-Condition

Before configuring the safety-related parameters, make sure that the device firmware and the DTM version are the same.

Steps to Configure the Safety Functions

If...	Then ...
you are not in Online mode	In the menu bar, click **Communication** > **Connect to Device** or click the **Connect to Device** icon
you are Online mode	Click the **Configure** button in the **Safety Functions** tab.

Once connected:

Step	Action	Comment
1	Click the **Configure** button in the **Safety Functions** tab.	A **Define Configuration Password** dialog box appears: • Type the new configuration password in **Enter New Password** box • Retype the new configuration password in **Confirm New Password** box. • Click **OK** **NOTE:** Your password: • Should have only numeric value, choose the value between 1...9999. • Should not exceed more than 4 digits. • Should not have the value 0. **Result**: Opens the **Configuration of Safety Functions** window.

If...	Then ...
you have already defined the password	type your safety function configuration password in **Enter Configuration Password** box, click **OK**. **Result**: Opens the **Configuration of Safety Functions** window.

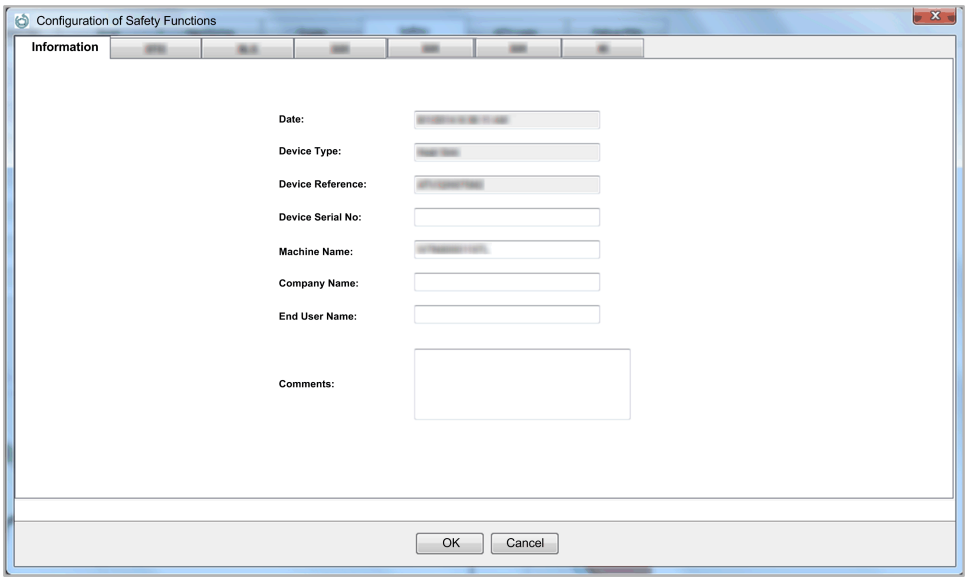
Configure Safety Functions Panel

Overview

The **Configuration of Safety Functions** panel includes the **Information**, **STO** tabs.

Information Tab

The **information** tab allows you to define and display product system information



Information filled in automatically by SoMove:

- **Date** (format depends on the PC local and linguistic options)
- **Device Type**
- **Drive Reference**

Information filled in manually:

- **Device Serial No** (number)
- **Machine Name**
- **Company Name**
- **End-User Name**
- **Comments**

Safe Torque Off (STO) Tab

For more information about **STO** function, see STO description, page 23.

For this function, only the associated set of inputs should be selected in the box. The parameter to be managed is: STOA.

Code	Name/Description	Factory Setting
StO	**[Safe Torque Off]**	
StoA	**[STO function activation]**	**[No]**
no	**[No: Not assigned]**	
L34	[LI3 and LI4]: digital input 3/4 low state	
L56	[LI5 and LI6]: digital input 5/6 low state	
L3PW	[LI3 and STO]: digital input 3/STO low state	
	This parameter is used to configure the channel used to trigger the STO function. If you set STOA=No, STO function is always active but just on STO input	

Password Configuration - Modify Password

This function allows you to modify the configuration password in the drive.

To modify the configuration password

Step	Action
1	In **Safety Functions** tab, click the **Modify Password** button **Result**: opens the **Modify Configuration Password** dialog box.
2	In the **Modify Configuration Password** dialog box: • Type the existing configuration password in **Enter Current Password** box • Type the new configuration password in **Enter New Password** box • Retype the new configuration password in **Confirm New Password** box • Click **Ok** **NOTE:** The password typed in **Enter New Password** box and **Confirm New Password** box should be same. **NOTE:** Your password: • Should contain only numeric value, choose the value between 1...9999. • Should not exceed more than 4 digits. • Should not have the value 0. **Result**: modifies the configuration password.

Password Configuration - Reset Password

If you cannot remember the configuration password defined in the drive, you need to know the universal password to reset the drive. To obtain this password, contact your Schneider Electric contact.

After this operation, the device reverts to no defined configuration password and the session is automatically closed.

However, the function configuration remains unchanged.

Reset Configuration

This function is used to reset the configuration of the safety function to the factory settings.

To access the function, click the **Reset Configuration** button in the **Safety Functions** tab.

First enter the password, then confirm your choice.

After this action, all safety-related parameters are set to factory settings.

Visualization and Status of Safety Functions

Code	Name/Description
SAF-	**[MONIT. SAFETY]** menu - **Visible** on **SoMove and keypad**
STFr	**[Stator Frequency]** Displays the estimated stator frequency in Hz
StoS	**[STO status]** Status of the Safe Torque Off safety function
idLE	**[IdLE]**: STO not in progress
Sto	**[Safe torque off]**: STO in progress
FLt	**[Fault]**: STO in detected error
SAF-	**[MONIT. SAFETY]** menu - **Visible** ONLY on **SoMove**
SFty	**[Safety drive status]** Safety function status of the drive
iStd	**[Standard drive]**: Standard product without safety function configured
SAFE	**[Safety drive]**: product with at least 1 safety function configured

Copying Safety Related Configuration from Device to PC and from PC to Device

Overview

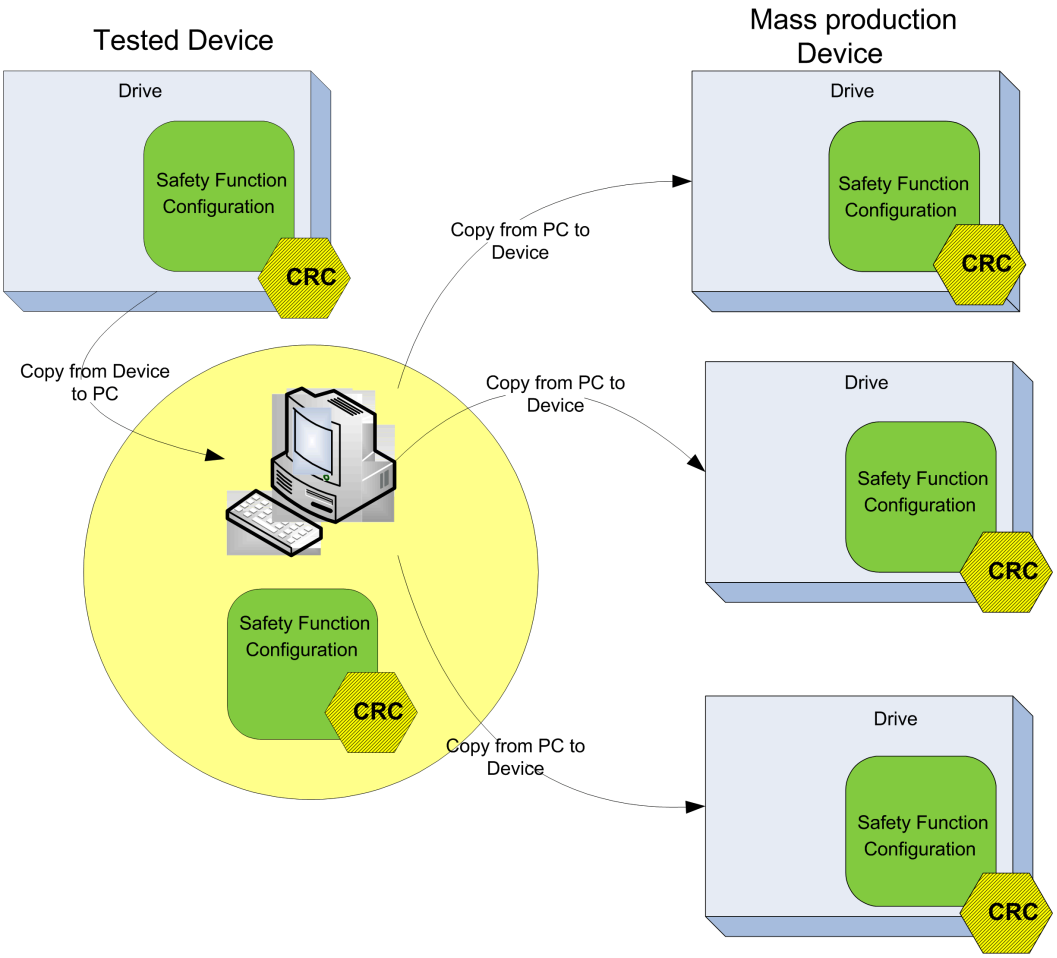
This feature is used to copy/paste the tested safety-related configuration in several drives.

This feature allows you to:

- identify unique safety-related configuration on the drive
- copy the safety-related configuration file from drive to PC.
- copy the safety-related configuration file from PC to drives

Architecture

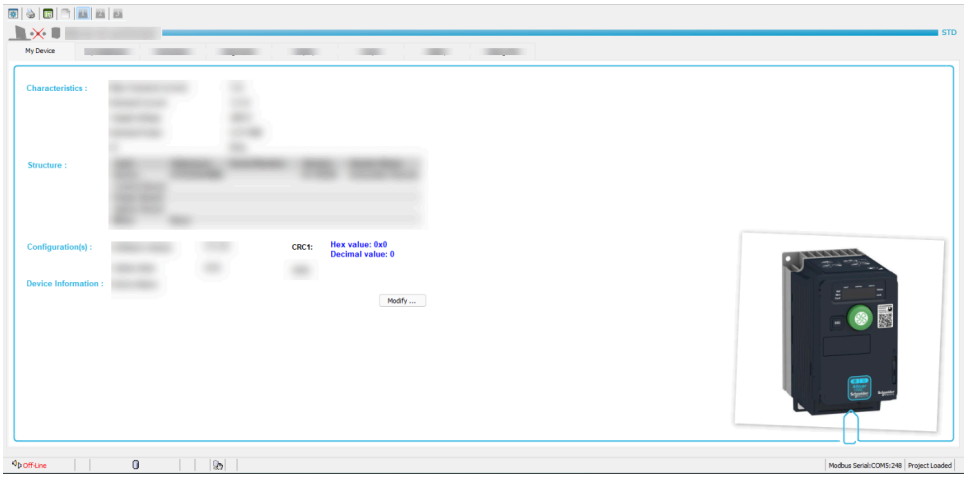
The figure shows the architecture for copying the safety-related configuration from device to PC and PC to device:



Identify Unique Safety Related Configuration

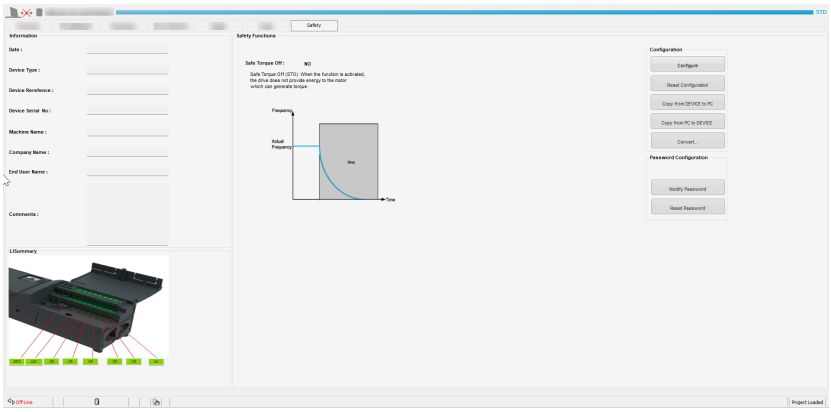
The identification of the safety-related configuration is done by using CRC, calculated using all safety-related parameters

You can get the CRC value from **My Device** tab. Note down the CRC value after the drive is fully tested.



Copy from Device to PC

To copy a configuration file from device to PC:

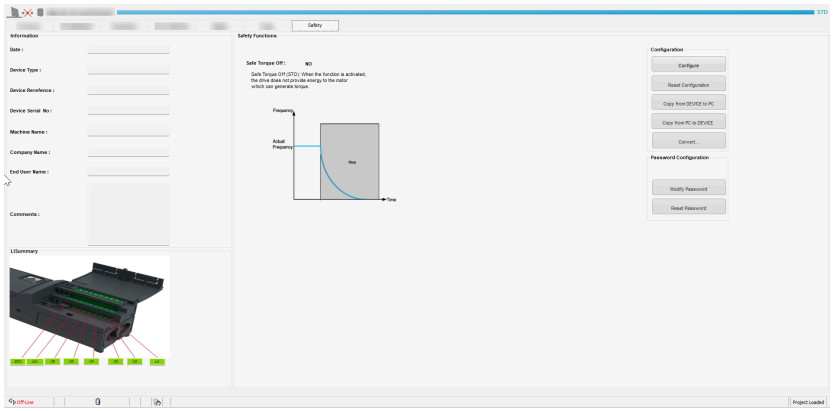
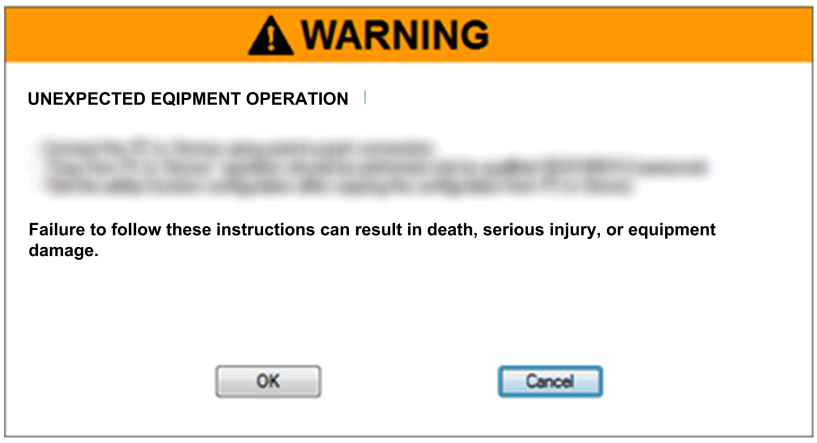
Step	Action
1	In the **Safety Functions** tab, click the **Copy from DEVICE to PC** button  **Result**: opens the **Copy from Device to PC** dialog box.
2	Type the configuration password in **Enter configuration Password** box, click **Ok**. **Result**: Displays the CRC1 value
3	Note the CRC1 value, click **Save**. **Result**: opens the **Save File...** window.
4	In the **Save File..** Window: • Select/create the folder • Type the name of the file in **File name** box. • Click **Save**, **Result**: **Safety-related Parameters Successfully saved** message appears on the screen, which confirms that the file has been saved successfully in the desired path.

NOTE: You cannot copy the configuration from device to PC if:

- the motor is powered.
- a function block is in **Run** state.
- the function **Forced Local** is active.
- a safety function is triggered.

Copy from PC to Device

To copy a file from PC to device:

Step	Action
1	In the **Safety Functions** tab, click the **Copy from PC to DEVICE** button  **Result**: **Warning** box appears, read the following instruction before proceeding with copy from PC to device operation.
2	 Click **Ok** **Result**: Opens the **Open File...** window.
3	In the **Open File...** Window • Select `.sfty` file. • Click **Open** **Result**: Displays the CRC1 value
4	Verify whether the CRC1 value is same as the CRC1 value noted while copying the configuration from device to PC if both CRC1 values are same then click **Continue**. **Result**: Opens the **Copy from PC to Device** dialog box.
5	Type the password (49157) in the **Enter copy password** box, click **Ok**. **Result**: Configuration is successfully copied from PC to device. A commissioning test must be done on the safety function.

NOTE: You cannot copy the configuration from PC to device if:

- the motor is powered.
- a function block is in **Run** state.
- the function **Forced Local** is active.
- the configuration of the safety function is already present in the device

Device and DTM Firmware Compatibility

You can copy a configuration file to the device, only if the device and DTM firmware versions are the same.

NOTE: This function is available in Online Mode.

To copy a configuration file from the DTM with different firmware version, follow the steps:

- Connect the DTM with the same firmware version to the device and copy the configuration file using the **Copy from Device to PC** option.
- Connect the DTM to the device on which you need to copy the configuration file, and use the **Copy from PC to Device** option.

Machine Signature

Overview

The purpose of the test is to verify proper configuration of the defined safety functions and test mechanisms and to examine the response of dedicated monitoring functions to explicit input of values outside the tolerance limits.

The test must cover all drive-specific Safety configured monitoring functions and global Safety integrated functionality in ATH200.

Condition Prior to Acceptance Test

- The machine is wired up correctly.
- All safety-related devices such as protective door monitoring devices, light barriers, and emergency stop switches are connected and ready for operation.
- All motor parameters and command parameters must be correctly set on the drive.

Acceptance Test Process

The acceptance test is configured with SoMove software.

Step	Action	Comment
1	Select the **Device** > **Safety Function** > **Machine Signature** menu and follow the five steps below	
2	**General Information** To add this step to the final report select **Add to the machine signature** Click **Next**.	The information displayed here corresponds to the **Identification** section in the **Safety Functions** tab.
3	**Function Summary** To add a function to the final report select **Add** to the machine signature Click **Next**	This step is composed of sub-steps. Each sub-step relates to one of the following safety functions: • STO In a function, sub-step the function diagram and parameters values are displayed. A text box allows you to enter additional text in this step.
4	**I/O Summary** To add a function to the final report select **Add** to the machine signature Click **Next**	The information displayed here corresponds to the **Digital Input summary** folder of the **Safety Functions** tab: • The digital input that is assigned to a safety function are displayed in red and show the related safety function • The digital input that is not assigned to a safety function do not show any assignment and are displayed in green
5	**Test** To add a function to the final report select **Add** to the machine signature Click **Next**	In this step, you tick the box when you have tested the safety functions to confirm that you have verified the correct behavior of the functions for all devices.
6	**Key** Click **Finish** to create the report	The checksum of the safety-related configuration is displayed as it is calculated for transmission to the connected device when you click **Apply**. This allows you to compare the checksum value with the one displayed in the identification menu on the graphic display terminal

Acceptance Report

SoMove creates the acceptance report.

This function provides a final report when one or several safety functions have been configured and verified.This report is deemed to be a machine signature and certifies that all the safety functions are operational.The acceptance report has been added as an optional document to be printed to a printer or to a PDF file.

If the drive configuration is modified (not only applicable on the safety related parameters), you must repeat the acceptance test.

Services and Maintenance

What's in This Part

Maintenance

Overview

By way of preventive maintenance, the Safety functions must be activated at least once a year. The drive power supply must be turned off and then on again before carrying out this preventive maintenance. The drive digital output signals cannot be considered to be safety-related signals. Install interference suppressors on all inductive circuits near the drive or coupled to the same circuit (relays, contactors, solenoid, valves, etc.).

NOTE: For more product information, see the installation manual and programming manual on www.se.com.

Power and MCU Replacement

Overview

You can replace the MCU (Motor Control Unit) part (APP + HMI card) and the power part.

Depending on the drive configuration (safety function active or not), the drive response will differ.

If you replace the power and you keep your MCU, you won't lose the configuration of the safety functions but you need to repeat the Acceptance Test to avoid incorrect wiring or incorrect behavior of the safety function.

If you replace the MCU you will lose your safety-related configuration. You need to reinstall your Configuration on the new MCU and then repeat the Acceptance Test.

NOTE: For more product information, see the installation manual and programming manual www.se.com.

Changing Machine Equipment

Overview

If you need to change any part of the drive system (Motor, Emergency stop, etc.) you must repeat the Acceptance Test.

NOTE: For more product information, see the installation manual and programming manual www.se.com.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© 2025 Schneider Electric. All rights reserved.

JPS43226.01