Altivar Process ATV6000

Variable Speed Drives

Embedded Safety Function Manual

BQT43422.01
07/2024

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

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, ARC FLASH OR UNEXPECTED EQUIPMENT OPERATION

- This manual is not intended to be used by end users.
- This manual may only be used by qualified personnel. These qualified personnel are limited to Schneider Electric Field Service personnel and to partners who have been trained by Schneider Electric to install components in variable speed drives.
- The qualified Schneider Electric personnel and its partners are trained in servicing variable speed drives and know how to recognize and avoid the hazards involved. They are authorized to install component and to service variable speed drives.

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

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.

Product Related Information

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

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

Before performing work on the drive system:

- Follow the instructions given in the section ”Complete drive system power Off procedure” of the installation manual.

Before applying voltage to the drive system:

- Verify that the work has been completed and that the entire installation cannot cause hazards.
- Remove the ground and the short circuits on the mains input terminals and the motor output terminals.
- Verify proper grounding of all equipment.
- Verify that all protective equipment such as covers, doors, grids is installed and/or closed.

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

⚠⚠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 drive 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 drive system, block the motor shaft to prevent rotation.
- Insulate both ends of unused conductors of the motor cable
- Do not create short circuits across the DC bus terminals or the DC bus capacitors.

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

Many components of the equipment, including the printed circuit board, operate with mains voltage, or present transformed high currents, and/or high voltages.

The motor itself generates voltage when the motor shaft is rotated.

AC voltage can couple voltage to unused conductors in the motor cable.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Verify compliance with all safety information, different electrical requirements, and standards that apply to your machine or process in the use of this equipment.
- Verify compliance with all applicable standards and 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 drive system, block the motor shaft to prevent rotation.
- Do not create short circuits across the DC bus terminals or the DC bus capacitors or the braking resistor terminals, if present.

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.

This equipment has been designed to operate outside of any hazardous location. Only install this equipment in zones known to be free of a hazardous atmosphere.

⚠DANGER

POTENTIAL FOR EXPLOSION

Install and use this equipment in non-hazardous locations only.

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

Your application consists of a whole range of different interrelated mechanical, electrical, and electronic components, the drive being just one part of the application. The drive 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 drive 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 cyber security 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 cyber security (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 cyber security 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.

NOTICE

DESTRUCTION DUE TO INCORRECT MAINS VOLTAGE

Before switching on and configuring the product, verify that it is approved for the mains voltage.

Failure to follow these instructions can result in equipment damage.

About the Book

Document Scope

The purpose of this document is to provide information about the supported safety function.

The drive supports the STO safety function according to the IEC 61800-5-2 standard.

Validity Note

Original instructions and information given in this manual have been written in English (before optional translation).

This documentation is valid for the Altivar Process ATV6000 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.

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 Handbook for detailed characteristics and selection guides,
- The CAD files to help design your installation,
- All software and firmware to maintain your installation up to date,
- Additional documents for better understanding of drive systems and applications
- And finally all the User Guides related to your drive, listed below:

Title of Documentation	Reference number
Altivar Process range brochure	998-20307132 (English)
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019-340 (English)
ATV6000 Handbook	QGH83255 (English), PHA51119 (French), PHA51121 (German), PHA51120 (Spanish), GDE94089 (Italian), PHA51122 (Russian), PHA51118 (Chinese)
ATV6000 Installation Manual	QGH83258 (English), QGH83259 (French), QGH83261 (German), QGH83260 (Spanish), GDE94087 (Italian), QGH83257 (Chinese)
ATV6000 Programming Manual for Operator and Advanced Operator	QGH83265 (English), QGH83266 (French), QGH83268 (German), QGH83267 (Spanish), GDE94088 (Italian)
ATV6000 Embedded Safety Function Manual	BQT43422 (English)
ATV6000 Communication Parameters	MFR82761 (English)
ATV6000 Embedded Ethernet Manual	PHA30472 (English)
ATV6000 Modbus SL Manual	MFR24213 (English)
ATV6000 PROFIBUS Manual	PHA30474 (English)
ATV6000 DeviceNet Manual	PHA30471 (English)
ATV6000 EtherCat Manual	PHA30473 (English)
ATV6000 Profinet Manual	PHA30475 (English)
ATV6000 CANopen Manual	PHA30470 (English)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
Altivar Process ATV6000: DTM	ATV6000 DTM Library EN (English)

You can download these technical publications and other technical information from our website at www.se.com/en/download

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.

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.

This terminology is used and defined, among others, in these following standards:

- IEC 61800 series: Adjustable speed electrical power drive systems
- IEC 61508 Ed.2 series: Functional safety of electrical/electronic/ programmable electronic safety-related
- EN 954-1 Safety of machinery - safety-related parts of control systems
- ISO 13849-1 & 2 Safety of machinery - safety related parts of control systems
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC 61784 series: Industrial communication networks - Profiles
- IEC 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements

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.

EC Declaration of Conformity

The EC Declaration of Conformity can be obtained on www.se.com.

Certification for Functional Safety

The integrated safety function is compatible and certified following IEC 61800-5-2 Ed.1 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 Systems Safety Related PDS (SR) s in terms of the framework of IEC 61508 series Ed.2 of standards.

Compliance with IEC 61800-5-2 standard, for the following described safety function, will facilitate the incorporation of a PDS(SR) (Power Drive System with safety-related functions) into a safety-related control system using the principles of IEC 61508, 60204 or the ISO 13849-1 for process-systems and machinery.

The defined safety function is

- SIL 2 capability in compliance with IEC 61800-5-2 and IEC 61508 series Ed.2

Also refer to Safety function capability, page 36.

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

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

Contact Us

Select your country on:

www.se.com/contact

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

Cyber Security

Overview

The objective of Cybersecurity is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

No single Cybersecurity approach is adequate. Schneider Electric recommends a defense-in-depth approach. Conceived by the National Security Agency (NSA), this approach layers the network with security features, appliances, and processes.

The basic components of this approach are:

- Risk assessment
- A security plan built on the results of the risk assessment
- A multi-phase training campaign
- Physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- System access control
- Device hardening
- Network monitoring and maintenance

This chapter defines the elements that help you configure a system that is less susceptible to cyber-attacks.

Network administrators, system integrators and personnel that commission, maintain or dispose of a device should:

- Apply and maintain the device's security capabilities. See Device Security
- Capabilities sub-chapter for details
- Review assumptions about protected environments. See Protected
- Environment Assumptions sub-chapter for details
- Address potential risks and mitigation strategies. See Product Defense-in-Depth sub-chapter for details
- Follow recommendations to optimize cybersecurity

For detailed information on the system defense-in-depth approach, refer to the TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room (STN V2) on se.com.

To submit a Cybersecurity question, report security issues, or get the latest news from Schneider Electric, visit the Schneider Electric website.

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default password to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least rights, separation of duties) to help prevent unauthorized exposure, loss or modification of data and logs, interruption of services, or unintended operation.

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

Protected Environment Assumptions

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 cyber security 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 cyber security (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 cyber security 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.

Before considering cybersecurity practices on the device, please pay attention to following points:

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company.
- Perimeter security – installed devices, and devices that are not in service, are in an access-controlled or monitored location.

- Emergency power – the control system provides the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
- Firmware upgrades – the ATV6000 upgrades are implemented consistently to the current version of firmware available on request from Schneider Electric Customer Care Center.
- Controls against malware – detection, prevention, and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Physical network segmentation – the control system provides the capability to:
  - Physically segment control system networks from non-control system networks.
  - Physically segment critical control system networks from non- critical control system networks.
- Logical isolation of critical networks – the control system provides the capability to logically and physically isolate critical control system networks from non-critical control system networks. For example, using VLANs.
- Independence from non-control system networks – the control system provides network services to control system networks, critical or non-critical, without a connection to non-control system networks.
- Encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.
- Zone boundary protection – the control system provides the capability to:
  - Manage connections through managed interfaces consisting of appropriate boundary protection devices, such as: proxies, gateways, routers, firewalls, and encrypted tunnels.
  - Use an effective architecture, for example, firewalls protecting application gateways residing in a DMZ.
  - Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site, for example, data centers.
- No public internet connectivity – access from the control system to the internet is not recommended. If a remote site connection is needed, for example, encrypt protocol transmissions.
- Resource availability and redundancy – ability to break the connections between different network segments or use duplicate devices in response to an incident.
- Manage communication loads – the control system provides the capability to manage communication loads to mitigate the effects of information flooding types of DoS (Denial of Service) events.
- Control system backup – available and up-to-date backups for recovery from a control system failure

Security Policy

⚠WARNING

ACCESSIBILITY LOSS

- Setup a security policy to your device and backup the device image with security administrator user account.
- Define and regularly review the password policy.
- Periodic change of the passwords, Schneider Electric recommends a modification of the password each 90 days.

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

Cybersecurity helps to provide:

- Confidentiality (to help prevent unauthorized access)
- Integrity (to help prevent unauthorized modification)
- Availability/authentication (preventing the denial of service and assuring authorized access)
- Non-repudiation (preventing the denial of an action that took place)
- Traceability/detection (logging and monitoring)

For an efficient security, the instructions and procedures should structure the roles and responsibilities in terms of security within the organization, in other words, who is authorized to perform what and when? These should be known by the users.

The anti-intrusion and anti-physical access to any sensitive installation should be set up.

All the security rules implemented in the ATV6000 are in complement of the points above.
The device does not have the capability to transmit data encrypted using the CIP Safety protocolfollowing protocols: HTTP, Modbus slave over serial, Modbus slave over Ethernet, EtherNet/IP, SNMP, SNTP. If other users gained access to your network, transmitted information can be disclosed or subject to tampering.

⚠WARNING

CYBERSECURITY HAZARD

- For transmitting data over an internal network, physically or logically segment the network, the access to the internal network needs to be restricted by using standard controls such as firewalls.
- For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

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

The access through the digital inputs is not controlled.

Any computer using SoMove, DTM, Webserver or EcoStruxure Control Expert should have an updated anti-virus, anti-malware, anti-ransomware application activated during the use.

The ATV6000 have the capability to export its settings and files manually or automatically. It is recommended to archive any settings and files (device backup images, device configuration, device security policies) in a secure area.

For detailed information about cybersecurity policy for the CIP safety environment, please refer to the .

Product Defense-in-Depth

Use a layered network approach with multiple security and defense controls in your IT and control system to minimize data protection gaps, reduce single-points of failure and create a strong cybersecurity posture. The more layers of security in your network, the harder it is to breach defenses, take digital assets or cause disruption.

Device Security Capabilities

ATV6000 offers the following security features:

Threats	Desired security property on Embedded Device	security features
Information disclosure	Confidentiality	Password encrypted in a non-reversible way
		User access control
Denial of Service	Availability	Device backup/restore
		Achilles Level 2
Spoofing/Elevation of privilege	User Authenticity / Authorization	Strong password policy
		Access control commissioning tools Modbus TCP
		Access control commissioning tools Web Server

Confidentiality
Information confidentiality capacity prevents unauthorized access to the device and information disclosure.

- The user access control helps on managing users that are authorized to access the device. Protect user credential at usage.
- The user's passwords are encrypted in non-reversible way at rest

Information affecting the security policy of the device is encrypted in transit.

Device Integrity Protection
The device integrity protection prevents unauthorized modification of the device with tampered or spoofed information.
This security capability helps protect the authenticity and integrity of the firmware running on the ATV6000 and facilitates protected file transfer: digitally signed firmware is used to help protect the authenticity of the firmware running on the ATV6000 and only allows firmware generated and signed by Schneider Electric.

- Cryptographic signature of the firmware package executed at the firmware update

Availability
The control system backup is essential for recovery from a control system failure and/or misconfiguration and participate on preventing denial of service. It also helps ensure global availability of the device by reducing operator overhead on security application/deployment.

These security capabilities help manage control system backup with the device:

- Complete device backup/restore available on local HMI, DTM and FDR. Regarding the communication robustness, the ATV6000 embedded Ethernet fieldbus successfully passed the certification Achilles L2.

User Authenticity and Authorization
The user authentication helps prevent the repudiation issue by managing user identification and prevents information disclosure and device integrity issues by unauthorized users.

These security capabilities help enforce authorizations assigned to users, segregation of duties and least rights:

- User authentication is used to identify and authenticate software processes and devices managing accounts
- Device Password policy and password strength configurable using SoMove, DTM or EcoStruxure Control Expert
- Authorization managed according to channels

In line with user authentication and authorization, the device has access control cryptographic features to check user credential before access is granted to the system.

In the ATV6000, the control of accessibility to the settings, parameters, configuration, and logging database is done with a user authentication after "Log in", with a name and password.

The ATV6000 controls the access through:

- SoMove DTM (Ethernet connection)
- The webserver
- EcoStruxure Control Expert

Potential Risks and Compensating Controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating controls
User accounts.	Default account settings are often the source of unauthorized access by malicious users.	If you do not change default password or disable the user access control, unauthorized access can occur.	Ensure User access control is enabled on all the communication ports and change the default passwords to help reduce unauthorized access to your device.
Secure protocols.	Modbus serial, Modbus TCP, EtherNet/IP, SNMP, SNTP, HTTP protocols are insecure. The device does not have the capability to transmit data encrypted using these protocols.	If a malicious user gained access to your network, they could intercept communication.	For transmitting data over internal network, physically or logically segment your network. For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution. See Protected Environment Assumptions, page 17.

Data Flow Restriction

A firewall device is required to secure the access to the device and limit the data flow.

For detailed information, refer to the TVDA: How Can I Reduce Vulnerability to.

Cyber Attacks in the Control Room (STN V2) on the Schneider Electric website.

Password

Changing Password

The user password can be changed from the DTM Admin options screen.

Reset Password

User and password are stored during commissioning, before reset password, contact your local Schneider representative.

If user forgets or has lost the user authentication password, user can restore the default password regarding his access level control .

- Standard Level access: contact your local Schneider representative
- Expert Level access: reset password using HMI Panel

Using HMI panel:
Go to the menu **Settings > My preferences > Webserver** and push the Reset button to reset the embedded Ethernet password.

Note: Upon first use, the commissioning tools and webserver requests the user to change this password prior to connecting. The cybersecurity policy does not change when the password is reset.
Note: When password is reset, the old password saved during commissioning (and also available at your Local Schneider Electric Representative) does not work anymore.

Password Policy

By default, the password policy of the ATV6000 complies with IEEE 1686–2013 as following:

- 8 characters minimum with ASCII [32 to 122] characters
- At least one digit (0-9)
- At least one special character (for example @, $)

In addition, for password changes, the password history is saved and help prevent the reuse of a password that has been set at least once in the last 5 times.

The password policy can be customized or totally disabled to match with password policy in place in the system of which the device is part.

The following settings are available:

- Password policy: enabled/disabled. If disabled, a password is requested as authentication factor but there is no specific rule defined regarding the password robustness
- Password history: No restriction, Exclude last 3, Exclude last 5
- Special character required: YES/NO
- Numeric character required: YES/NO
- Alphabetic character required: YES/NO
- Minimum password length: any value between 6 and 20

This password policy customization can only be done with SoMove, DTM or EcoStruxure Control Expert. Please refer to DTM online help for details.

Upgrades Management

When the ATV6000 firmware is upgraded, security configuration remains the same until changed, including usernames and passwords.

It is recommended that security configuration is reviewed after an upgrade to analyze rights for new or changed device features and revoke or apply them according to your company’s policies and standards.

Overview

Definitions

Safety Function In Altivar Process

The safety function incorporated in Altivar Process, helps to detect unsafe conditions of the installation and 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.

Safety integrated function provides the following benefits:

- Replacement of external safety-related equipment
- Reduced wiring efforts and space requirements
- Reduced costs

The Altivar Process drives are compliant with normative requirements to implement the safety function.

STO (Safe Torque Off)

No power that could cause torque or force is supplied to the motor.

Notation

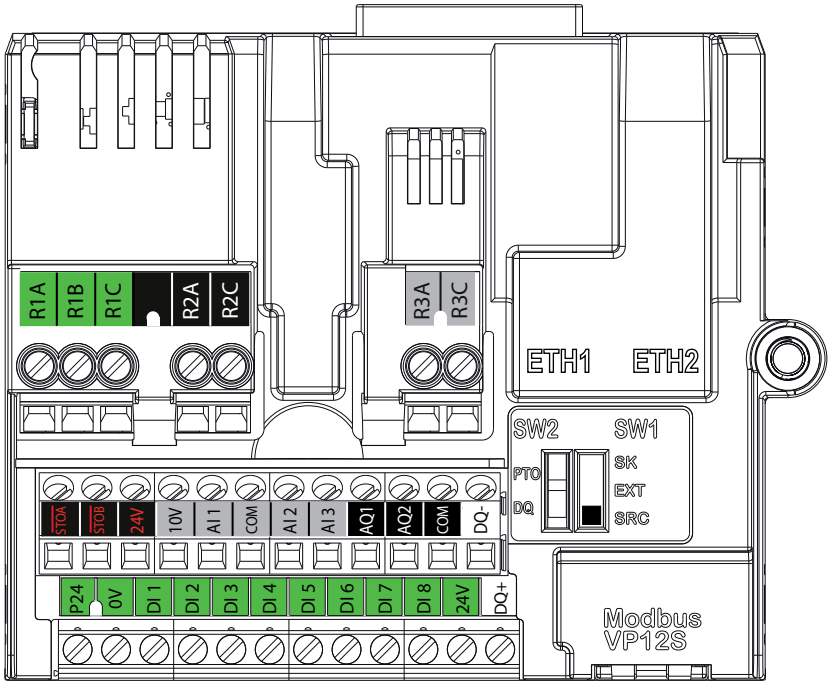
Parameters described in this document are based on the ATV6000 HMI and ATV6000 DTM.

The parameter are shown in square brackets.

Example: **[STO active]** `STO`.

STO Terminals Marking

With the Safety function, control block terminals on master controller are marked with STO_A and STO_B.



All safety relays, extension modules and push buttons are described to the Certified Architectures, page 39. Refer to case 1 as standard configuration or case 4 for the drive power stage only. (master controller and power cells).

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.

EN ISO 13849 Standard

This European Standard specifies the validation process, including both analysis and testing, for the safety functions and categories for the safety-related parts of control systems. Descriptions of the safety functions and the requirements for the categories are given in ISO 13849-1 which deals the general principles for design. Some requirements for validation are general and some are specific to the technology used. EN ISO 13849-2 also specifies the conditions under which the validation by testing of the safety-related parts of control systems should be carried out.

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 - Average Frequency of Dangerous Failure Per Hour.

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected errors, 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 per hour.) 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.

Safety Integrity Level	Average frequency of dangerous failure per hour (PFH) at high demand or continuous demand
4	$10^{-9} \leq ... < 10^{-8}$
3	$10^{-8} \leq ... < 10^{-7}$
2	$10^{-7} \leq ... < 10^{-6}$
1	$10^{-6} \leq ... < 10^{-5}$

PL - Performance Level

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

Level **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 probability of dangerous failure per hour.

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

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 to the total failure rate of the system.

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
90% <... < 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}	10,000,000 - 100,000,000
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

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

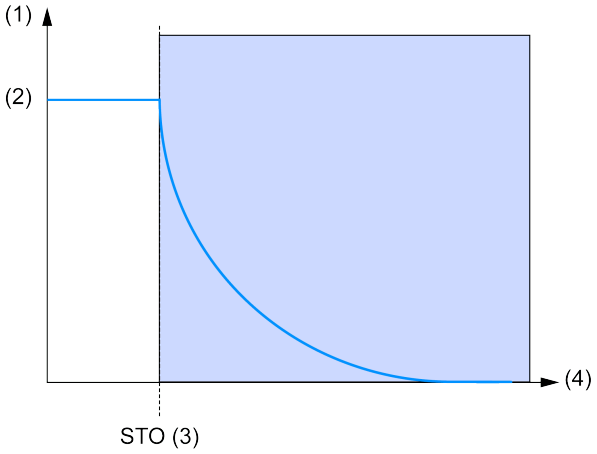
- Do not use the safety function STO for any other purposes than its intended function.
- Use an appropriate switch, that is not part of the circuit of the safety function STO, to disconnect the drive from the mains power.

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

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 logic inputs ($\overline{\text{STOA}}$ and $\overline{\text{STOB}}$) are always assigned to this function.

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



(1) Motor speed - (2) Actual speed - (3) $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ - STO Activation - (4) Time

NOTE: If delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ is greater than 1 s, the safety function STO is triggered and an error is triggered with the error code **[Safety Function Error]** $5AFF$.

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):

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 61-508
STO with and without Safety module (such as Preventa module)	SIL2

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).

    If the drive configuration enables automatic machine restart after the safety function STO has been deactivated, an additional safety module (such as Preventa module) is required.

    If the use of an additional safety module is not possible, the drive control must be configured in 2 wires transition (**[2/3-Wire Control]** `TCC` = **[2-Wire Control]** `2C` and **[2-wire type]** `TCT` = **[Transition]** `TRN`) or 3 wires (**[2/3-Wire Control]** `TCC` = **[3-Wire Control]** `3C`).

Limitations

Type Of Motor

The safety function STO can be used with all motors supported by the drive.

Prerequisites for Using Safety Functions

The STO safety function can be used only with the ATV6000 MASTER CONTROLLER STO.
Master controller STO requiring a software version equal or higher to V2.0 to support the STO safety function according to the IEC 61800-5-2 standard. (see below "Master Controller Identification")

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 supply mains, sequence, motor, and application and is not at the limit of its capacity as stated in the catalog.
- If required, the appropriate options are used.

  Example: output filter.
- 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.

Master Controller Identification

The sticker located on the Master Controller shows STO naming. Confirm that STO function is available on your system through this sticker.

The Safe torque off (STO) function is managed during the commissioning, status of the STO function is displayed though HMI Panel, for more details refer to the Product LEDs and HMI Status, page 34.

High Altitude

The safety function STO can be used with drive installed up to 4800 m, refer to the table: Maximum PoC admissible depending on altitude, page 37.

Bypassed Drive

The Safe Torque Off (STO) SIL certification apply at the product level:

- It is only valid for
  - ATV6000 as a single source for the motor
  - Applications of ATV6000 use cases, described inside the Certified Architectures, page 39.
- Any additional equipment (e.g. drive bypass circuit), connected to motor terminals, is NOT part of ATV6000 Safe Torque Off (STO) SIL certification.

Using any kind of drive bypass (see below figure for possible, non-exhaustive examples),

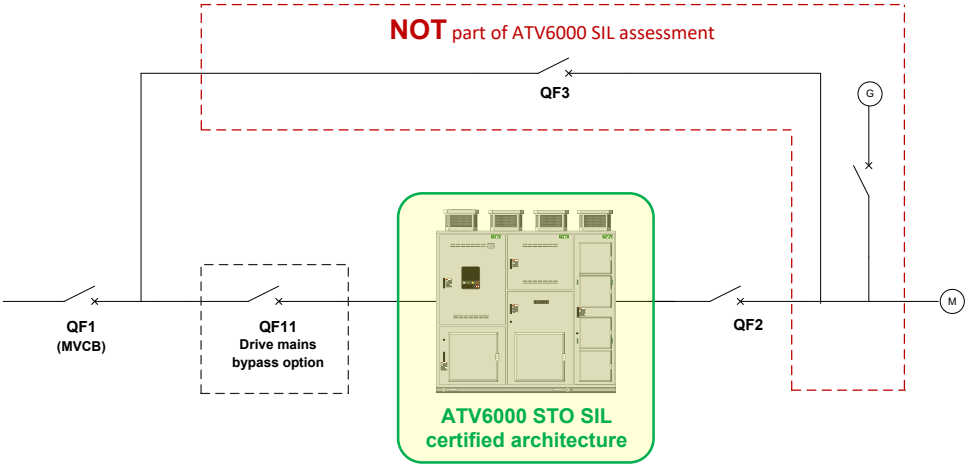
- manual, automatic or synchronous, including the ones controlled by the ATV6000 itself,
- or any scheme where the motor can be supplied by a source different than the drive at any moment,

will constitute a new safety system consisting of the ATV6000 and the bypass equipment.

ATV6000 STO function becomes only a part of this system and cannot ensure the safety level of the whole system when the motor is supplied by another source.

NOTE: It is mandatory to assess the safety level of this whole system.

It must be ensured that the activation/deactivation of any additional switching devices connecting the motor to another power source and ATV6000 STO function are interlocked to prevent unintended motor operation with the required safety level in all conditions.



QF1: Mains medium voltage Circuit Breaker
QF11: Bypass circuit breaker DRIVE (Optional)
QF2: Bypass circuit breaker MOTOR
QF3: Bypass circuit breaker DOL
G: Generator
M: Motor

Power Cell Topology

It is recommended to have a power cell bypass option for critical process, in which case a reduction in capacity is preferable to a complete shutdown. When a power cell goes to error, the drive automatically bypasses the power cells in order to keep the VSD system running. This prevents production downtime or unexpected interruption.

Additionally, when utilizing the safety function STO, **a minimum of 3 PoCs per phase must remain in operation**. Therefore additional PoCs must be added to cover this limitation, taking into account bypassed stages and PoCs in degraded mode.

NOTE: The **[Bypass PoC Error]** `BYPF` occur when the number of Power Cell in operation is less than 3 PoCs per phase.

NOTE: The setting and functionality of the system are managed during the commissioning process. For further information, refer to your local Schneider representative.

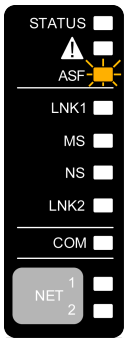
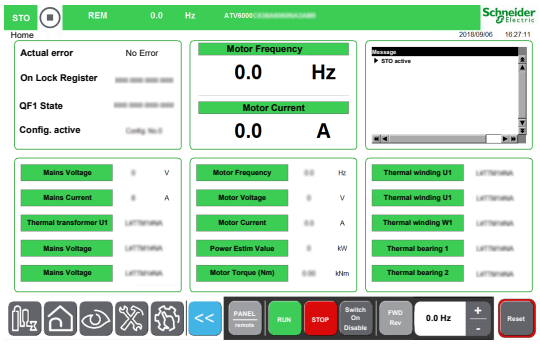
Disable Error Detection

When the safety function is used, the error code **[Safety Function Error]** `SAFF` cannot be disabled by the function **[Inhibited Errors]** `INH`, this detected error can only be reset after a power reset.

Status of Safety Function

Product LEDs and HMI Status

The following figures describes the LEDs status and HMI Panel status of safety function:

LED indicator on control block	Status on HMI (1)
	

(1): Refer to the ATV6000 Programming manual for operator and advanced operator.

Description

If...	Then ...
Safe Torque Off (STO) is not active	the orange **ASF** LED is OFF no error are detected and the green banner from HMI is displayed
STO is triggered	the power bridge is locked by redundant hardware the orange **ASF** LED is steady ON the green banner from the HMI Panel is displayed with the drive status **[STO active]** `STO`.
[Safety Function Error] `SAFF` detected fault occurs (1)	the power bridge is locked the orange **ASF** LED is steady ON the red ⚠ LED is steady ON the red banner from the HMI Panel is displayed with the drive status **[STO active]** `STO`, then the detected error **[Safety Function Error]** `SAFF` is triggered .

(1): Possible causes are exceeded delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ signals > 1 s and internal hardware detected error.

Technical Data

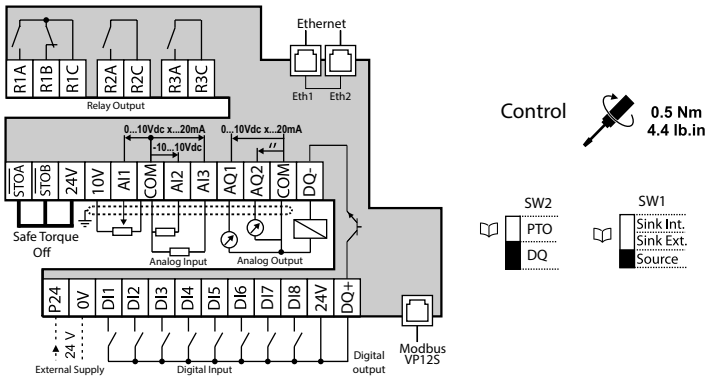
Electrical Data

Logic Type

Safety function must only be used in **Source mode**: current flows to input.

$\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ inputs and signal inputs are protected against reverse polarity.

Cabling Label



Input Signal Safety Function

Input Signals Safety Function	Units	Value for STO
Logic 0 (Ulow)	Vdc	< 5 or open
Logic 1 (Uhigh)	Vdc	> 11
Current (at 19 Vdc)	mA	11
Debounce time (*)	ms	> 1
Delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$	s	< 1
Response time of safety function	ms	< 10
(*) A pulse shorter than “Debounce time” will be ignored.		

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 help 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 (activation of the digital input set to **[Operating State Fault]**, error codes or information on the display, etc.) is not considered to be a safety-related data.

Machine Application Function Configuration

Standard	STO
IEC 61800-5-2 / IEC 61508 (2)	SIL2
IEC 60204-1 (1)	Category stop 0

(1) 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.

(2) Even if the performance level is not provided (PL Spec), the power stage can also be applied based on the architecture specified in ISO 13849-1.

Process Application Function Configuration

Standard	STO
IEC 61800-5-2 / IEC 61508	SIL2

PDS (SR) - Summary Of The Reliability Study

Refer to the Certified Architectures, page 39. (ATV6000 Power stage: case 4)

Up to 2000 m

Standard	Input	ATV6000 (Master controller and Power Cells only)
IEC 61508 Ed.2	PFH in /h	7.0×10^{-07}
	PFD	4.0×10^{-03}
	T1 (proof test interval) in hours	8760
	SIL capability(1)	SIL2

> 2000 m to 4800 m

Standard	Input	ATV6000 (Master controller and Power Cells only)
IEC 61508 Ed.2	PFH in /h	8.3×10^{-07}
	PFD	5.0×10^{-03}
	T1 (proof test interval) in hours	8760
	SIL capability(1)	SIL2

(1): Even if the performance level is not provided (PL Spec), the power stage can also be applied based on the architecture specified in ISO 13849-1 (see ATV6000 Drive Assembly - Summary Of The Reliability Study, page 38).

Preventive annual activation of the safety function is recommended.

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

Maximum PoC admissible depending on altitude

Altitude	Maximum PoC per phase (Total)
Up to 3000 m	12 (36)
Up to 4000 m	7 (21)
Up to 4800 m	4 (12)

NOTE: The safety function STO can be used with drive installed up to 4800 m.

ATV6000 Drive Assembly - Summary Of The Reliability Study

Refer to the Certified Architectures, page 39 for:

- Mains Power OFF (Including STO) - (As standard configuration): Case 1
- Mains Power OFF (Including STO) + SP06 (STO stop category 0 (SS0)) - SP06: Case 2
- Mains Power OFF (Including STO) + SP07 (STO Stop Category 1 (SS1)): Case 3
- ATV6000 Power stage (Master controller and Power cells only): Case 4

NOTE: For more details regarding the options, please refer to the Handbook manual QGH83255.

Up to 2000 m

Standard	Input	Case 1	Case 2	Case 3	Case 4
		ATV6000 as standard configuration	ATV6000 with Option		ATV6000 Power stage
		Mains power off (STO)	SP06 (STO)	SP07 (SS1)	
IEC 61508 Ed.2	PFH in /h	7.1 x10^{-07}	7.1 x10^{-07}	7.1 x10^{-07}	7.0 x10^{-07}
	PFD	4.2 x10^{-03}	4.2 x10^{-03}	4.2 x10^{-03}	4.0 x10^{-03}
	T1 (proof test interval) in hours	8760	8760	8760	8760
	SIL capability	SIL2	SIL2	SIL2	SIL2
ISO 13849-1	PL	d	d	d	NA
	PFH_D	7.1 x10^{-07}	7.1 x10^{-07}	7.1 x10^{-07}	NA

> 2000 m to 4800 m

Standard	Input	Case 1	Case 2	Case 3	Case 4
		ATV6000 as standard configuration	ATV6000 with Option		ATV6000 Power stage
		Mains power off (STO)	SP06 (STO)	SP07 (SS1)	
IEC 61508 Ed.2	PFH in /h	8.3 x10^{-07}	8.3 x10^{-07}	8.3 x10^{-07}	8.3 x10^{-07}
	PFD	5.2 x10^{-03}	5.2 x10^{-03}	5.2 x10^{-03}	5.0 x10^{-03}
	T1 (proof test interval) in hours	8760	8760	8760	8760
	SIL capability	SIL2	SIL2	SIL2	SIL2
ISO 13849-1	PL	d	d	d	NA
	PFH_D	8.3 x10^{-07}	8.3 x10^{-07}	8.3 x10^{-07}	NA

Preventive annual activation of the safety function is recommended.

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

Maximum PoC admissible depending on altitude.

Altitude	Maximum PoC per phase (Total)
Up to 3000 m	12 (36)
Up to 4000 m	7 (21)
Up to 4800 m	4 (12)

Certified Architectures

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.

These are the certified architectures:

- Case 1 - Mains Power OFF (Including STO) - (As standard configuration)
- Case 2 - Mains Power OFF (Including STO) + SP06 (STO stop category 0 (SS0))
- Case 3 - Mains Power OFF (Including STO) + SP07 (STO Stop Category 1 (SS1))
- Case 4 - ATV6000 Power stage (Master controller and Power cells only)

For all certified architecture, refer to the Safety Function Capability, page 36.

The safety functions of a PDS(SR) (Power Drive System suitable for use in safety-related applications) are part of an overall system.

If the qualitative and quantitative safety-related 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 (activation of the digital input set to **[Operating State Fault]**, error codes or information on the display, etc.) is not considered to be a safety-related data.

Protected cable insulation

The STO safety function is triggered via 2 redundant inputs. These two circuits have 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 two signals (both channels) 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 EMC purpose, both STO inputs have to be shielded with twisted cables with a pitch of 25...50 mm (1 in. and 2 in.), connecting the shielding to Ground at each end of the shielded cables for the signal lines.

Ground loops may cause problems in machines. In this case the shield has to be connected to ground on drive side only.

Power Supply Unit

⚠⚠DANGER

ELECTRIC SHOCK CAUSED BY INCORRECT POWER SUPPLY UNIT

The +24VDC supply voltage is connected with many exposed signal connections in the device.

- Use a power supply unit that meets the PELV (Protective Extra Low Voltage) requirements.

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

Acceptance Test

The system integrator/machine manufacturer must perform an acceptance test of the safety function STO to verify and document the correct functionality of the safety function. The system integrator/machine manufacturer hereby certifies to have tested the effectiveness of the safety functions used. The acceptance test must be performed on the basis of the risk analysis. All applicable standards and regulations must be adhered to.

Ambient Conditions

The ambient conditions to be met for the safety function STO correspond to the ambient conditions for the drive.

Please refer to the table **General Technical Data** available to the handbook manual or the installation manual.

Vertical Axis and External Forces

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.

Degree of Protection When the Safety Function Is Used

⚠WARNING

LOSS OF SAFETY FUNCTION CAUSED BY FOREIGN OBJECTS

Conductive foreign objects, dust or liquids may cause safety functions to become inoperative.

- Do not use a safety function unless you have protected the system against contamination by conductive substances.

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

Customer Care Center

For additional support, you can contact our Customer Care Center on:

www.se.com/CCC.

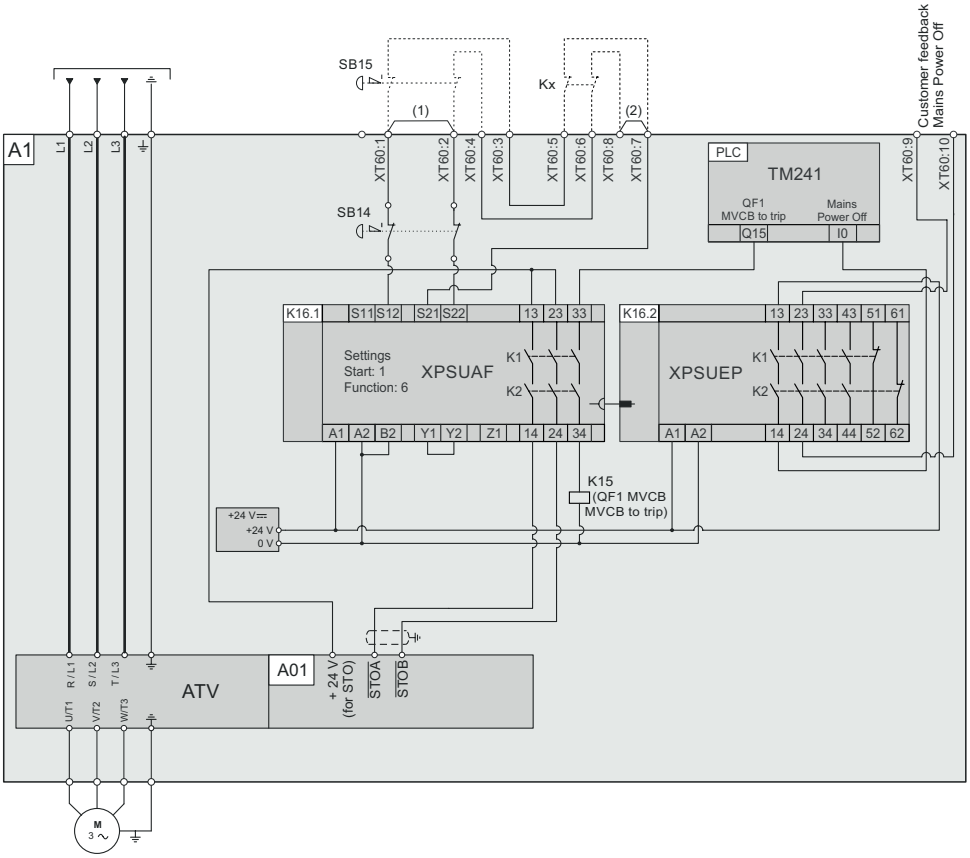
Case 1

Mains Power OFF (Including STO) - (As standard configuration)

This connection diagram applies for a drive configuration according to ISO 13849-1 PLd, IEC 61508 capability SIL2, IEC 60204-1 stop category 0 without protection against subsequent rotation after supply interruption or voltage reduction.

In this certified architecture, the drive incorporates safety modules and an emergency stop button on the enclosure door. These are used to activate the Safe Torque Off (STO) and turn off the mains power.

There is also a possibility to include an additional external emergency stop button to trigger STO and mains power off.(not included within the certification and safety path reliability calculation)



Legend:

- A1: ATV6000 Drive enclosure (certified architecture)
  - A01: Control Block
  - ATV: ATV6000 Power stage
  - K16.1: Safety relay for monitoring of the Emergency Stop circuit: Harmony XPSUAF13A type
  - K16.2: Safety relay extension module. Harmony XPSUEP14A type
  - SB14: Emergency Stop button in the enclosure door to trigger STO and Mains OFF (via K15)
  - PLC: Embedded logic controller
- SB15: Additional optional external Emergency Stop button to trigger STO and Mains OFF (via K15) (not included within the certification and safety path reliability calculation)
- Kx: Additional optional external contacts within safety path (not included within the certification and safety path calculation)

- (1): The fixed wire bridge XT60/1-XT60/2 needs to be used for single channel architectures (SIL1) on external safety components (SB15, Kx)
- (2): The fixed wire bridge XT60/7-XT60/8 (standard configuration) needs to be used for dual channel architectures (SIL2) on external safety components (SB15, Kx)

Case 2

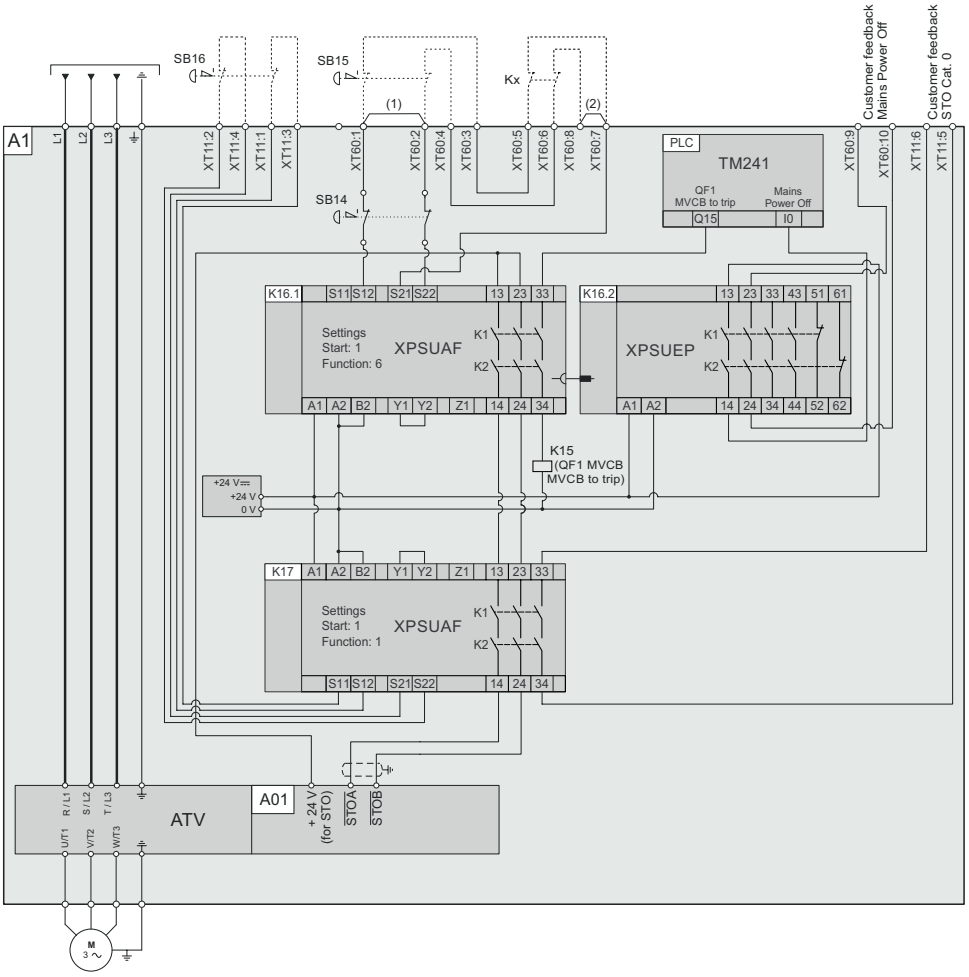
Mains Power OFF (Including STO) + SP06 (STO stop category 0 (SS0))

This connection diagram applies for a drive configuration according to ISO 13849-1 PLd, IEC 61508 capability SIL2, IEC 60204-1 stop category 0 without protection against subsequent rotation after supply interruption or voltage reduction.

In this certified architecture, the drive incorporates safety modules and an emergency stop button on the enclosure door. These are used to activate the Safe Torque Off (STO) and turn off the mains power.

There is also a possibility to include an additional external emergency stop button to trigger STO and mains power off.(not included within the certification and safety path reliability calculation)

There is also an option to include an external emergency stop button to trigger STO category 0 without turning off the mains power.



Legend:

- A1: ATV6000 Drive enclosure (certified architecture)
  - A01: Control Block
  - ATV: ATV6000 Power stage
  - K16.1: Safety relay for monitoring of the Emergency Stop circuit: Harmony XPSUAF13A type
  - K16.2: Safety relay extension module. Harmony XPSUEP14A type
  - K17 : Safety relay for monitoring of additional external Emergency Stop circuit Harmony XPSUAF13A type
  - SB14: Emergency Stop button in the enclosure door to trigger STO and Mains OFF (via K15)
  - PLC: Embedded logic controller
- SB15: Additional optional external Emergency Stop button to trigger STO and Mains OFF (via K15) (not included within the certification and safety path reliability calculation)
- SB16: Additional optional external Emergency Stop button to trigger STO only (Stop Category 0) (not included within the certification and safety path reliability calculation)
- Kx: Additional optional external contacts within safety path (not included within the certification and safety path calculation)
- (1): The fixed wire bridge XT60/1-XT60/2 needs to be used for single channel architectures (SIL1) on external safety components (SB15, Kx)
- (2): The fixed wire bridge XT60/7-XT60/8 (standard configuration) needs to be used for dual channel architectures (SIL2) on external safety components (SB15, Kx)

Case 3

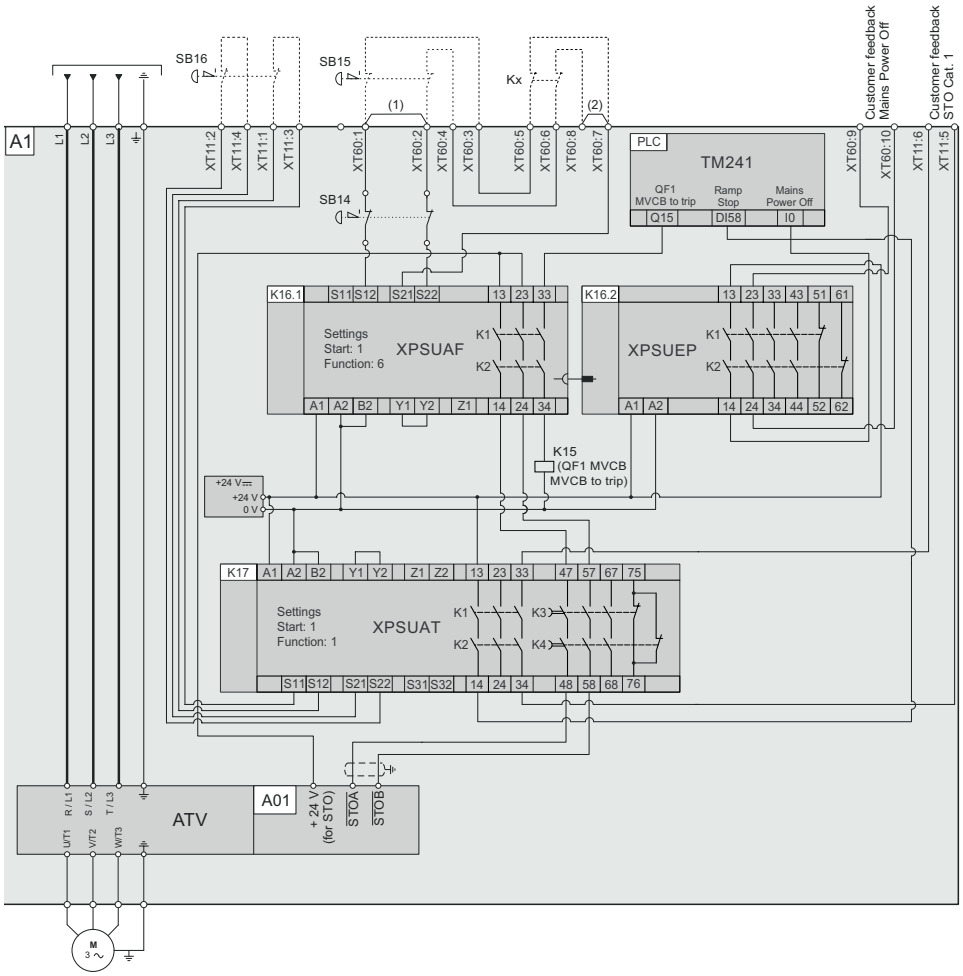
Mains Power OFF (Including STO) + SP07 (STO Stop Category 1 (SS1))

This connection diagram applies for a drive configuration according to ISO 13849-1 PLd, IEC 61508 capability SIL2, IEC 60204-1 stop category 1 without protection against subsequent rotation after supply interruption or voltage reduction.

In this certified architecture, the drive incorporates safety modules and an emergency stop button on the enclosure door. These are used to activate the Safe Torque Off (STO) and turn off the mains power.

There is also a possibility to include an additional external emergency stop button to trigger STO and mains power off.(not included within the certification and safety path reliability calculation)

There is also an option to include an external emergency stop button to trigger STO category 1 without turning off the mains power. Additionally, a stop mode is configured for the digital input (DI58)



Legend:

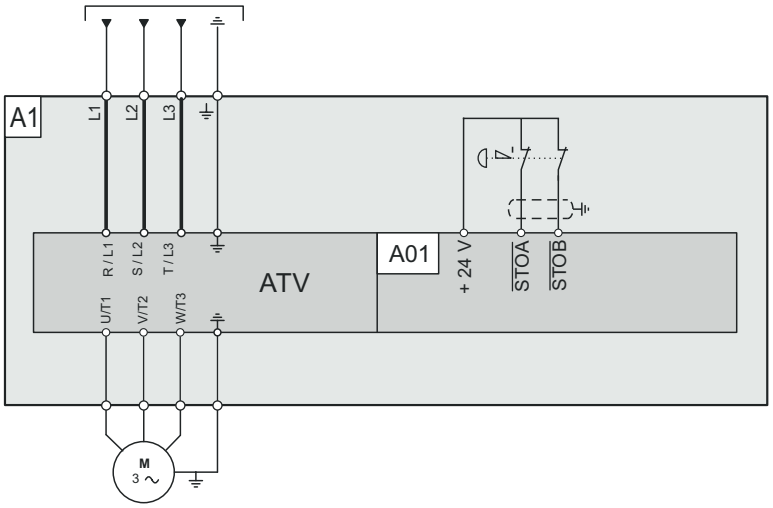
- A1: ATV6000 Drive enclosure (certified architecture)
  - A01: Control Block
  - ATV: ATV6000 Power stage
  - K16.1: Safety relay for monitoring of the Emergency Stop circuit: Harmony XPSUAF13A type
  - K16.2: Safety relay extension module. Harmony XPSUEP14A type
  - K17: Safety relay for monitoring of additional external Emergency Stop circuit Harmony XPSUAT13A type
  - SB14: Emergency Stop button in the enclosure door to trigger STO and Mains OFF (via K15)
  - PLC: Embedded logic controller
  - DI58: Internal I/O set to "Monitor Circuit D" (Ramp Stop)
- SB15: Additional optional external Emergency Stop button to trigger STO and Mains OFF (via K15) (not included within the certification and safety path reliability calculation)
- SB16: Additional optional external Emergency Stop button to trigger STO only (Stop Category 1) (not included within the certification and safety path reliability calculation)
- Kx: Additional optional external contacts within safety path (not included within the certification and safety path calculation)
- (1): The fixed wire bridge XT60/1-XT60/2 needs to be used for single channel architectures (SIL1) on external safety components (SB15, Kx)
- (2): The fixed wire bridge XT60/7-XT60/8 (standard configuration) needs to be used for dual channel architectures (SIL2) on external safety components (SB15, Kx)

Case 4

ATV6000 Power stage (Master controller and Power cells only)

This connection diagram applies for a drive configuration according to IEC 61508 capability SIL2, IEC 60204-1 stop category 0 without protection against subsequent rotation after supply interruption or voltage reduction.

In this configuration, the user takes care of managing the architecture, including safety modules, extension modules, and push buttons.



Legend:

- A1: ATV6000 Drive enclosure (certified architecture)
  - A01: Control Block
  - ATV: ATV6000 Power stage

Glossary

A

AC:

Alternating Current

AFE :

Active Front End

APM :

Altivar Process Modular

D

DC:

Direct Current

E

ELV:

Extra-Low Voltage. For more information: IEC 60449

Error :

Discrepancy between a detected (computed, measured, or signaled) value or condition and the specified or theoretically correct value or condition.

F

Factory setting:

Machine status in factory settings when the product was shipped.

Fault Reset:

A function used to restore the drive to an operational state after a detected error is cleared by removing the cause of the error so that the error is no longer active.

Fault:

Fault is an operating state. If the monitoring functions detect an error, a transition to this operating state is triggered, depending on the error class. A "Fault reset" is required to exit this operating state after the cause of the detected error has been removed. Further information can be found in the pertinent standards such as IEC 61800-7, ODVA Common Industrial Protocol (CIP).

G

GP:

General-Purpose

H

HHP:

High Horse Power (75 kW...800 kW)

HiPot test:

High Potential Test.

L

L/R:

Time constant equal to the quotient of inductance value (L) over the resistance value (R).

LHP:

Low Horse Power (< 15 kW)

M

MHP:

Medium Horse Power (15 kW...75 kW)

N

NC contact:

Normally Closed contact

NO contact:

Normally Open contact

O

OEM:

Original Equipment Manufacturer

OVCII:

Overvoltage Category II, according IEC 61800-5-1

P

PA/+:

DC bus terminal

PC/-:

DC bus terminal

PDS (SR):

PDS(SR) (Power Drive System with safety-related functions)

PDS:

PDS (Power Drive System)

PELV:

Protective Extra Low Voltage, low voltage with isolation. For more information: IEC 60364-4-41.

PLC:

Programmable logic controller.

Power stage:

The power stage controls the motor. The power stage generates current for controlling the motor.

PRM:

Partner Relationship Management

PTC:

Positive Temperature Coefficient. PTC thermistor probes integrated in the motor to measure its temperature

PVZ:

.PVZ is a Creo View Express™ software file format used to display the integration sequences to build Altivar Process Modular drives

R

REACh:

Registration, Evaluation, Authorisation and restriction of Chemicals regulation

RoHS:

Restriction of Hazardous Substances

S

SCPD:

Short-Circuit Protective Device

STD:

Standard

STO:

Safe Torque Off: No power that could cause torque or force is supplied to the motor

T

TVS Diode:

Transient Voltage Suppression Diode

V

VHP:

Very High Horse Power (> 800 kW)

VSD:

Variable Speed Drive

W

Warning:

If the term is used outside the context of safety instructions, a warning alerts to a potential error that was detected by a monitoring function. A warning does not cause a transition of the operating state.

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.

© 2024 Schneider Electric. All rights reserved.

BQT43422.01