Altivar Machine ATV340
Variable Speed Drives

Embedded Safety Function Manual

08/2019



NVE64143.02

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

© 2019 Schneider Electric. All rights reserved.

Table of Contents

	Safety Information	5
	About the Book	9
Chapter 1	**Overview**	13
	Definitions	14
	Basics	15
Chapter 2	**Description**	19
	Safety Function STO (Safe Torque Off)	20
	Limitations	21
	Status of Safety Function	22
Chapter 3	**Technical Data**	23
	Electrical Data	24
	Safety Function Capability	25
Chapter 4	**Certified Architectures**	27
	Introduction	28
	Machine System SF - Case 1	30
	Machine System SF - Case 2	33
	Machine System SF - Case 3	36
Glossary		39

Safety Information

Important Information

NOTICE

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 a drive for three-phase synchronous, reluctance and asynchronous motors and 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

- Only appropriately trained persons who are familiar with and understand the contents of this manual and all other pertinent product documentation and who have received safety 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.
- The system integrator is responsible for compliance with all local and national electrical code requirements as well as all other applicable regulations with respect to grounding of all equipment.
- Many components of the product, including the printed circuit boards, operate with mains voltage.
- Only use properly rated, electrically insulated tools and measuring equipment.
- Do not touch unshielded components or terminals with voltage present.
- Motors can generate voltage when the shaft is rotated. Prior to performing any type of work on the drive system, block the motor shaft to prevent rotation.
- AC voltage can couple voltage to unused conductors in the motor cable. 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.
- Before performing work on the drive system:
  - Disconnect all power, including external control power that may be present. Take into account that the circuit breaker or main switch does not de-energize all circuits.
  - Place a **Do Not Turn On** label on all power switches related to the drive system.
  - Lock all power switches in the open position.
  - Wait 15 minutes to allow the DC bus capacitors to discharge.
  - Follow the instructions given in the chapter "Verifying the Absence of Voltage" in the installation manual of the product.
- Before applying voltage to the drive system:
  - Verify that the work has been completed and that the entire installation cannot cause hazards.
  - If the mains input terminals and the motor output terminals have been grounded and short-circuited, 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.

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.
- If moving loads can result in hazards, for example, slipping or falling loads, operate the drive in closed loop mode.
- 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.

A specific application note *NHA80973* is available on hoisting machines and can be downloaded on *se.com*.

Drive systems 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.

The temperature of the products described in this manual may exceed 80 °C (176 °F) during operation.

⚠ WARNING

HOT SURFACES

- Ensure that any contact with hot surfaces is avoided.
- Do not allow flammable or heat-sensitive parts in the immediate vicinity of hot surfaces.
- Verify that the product has sufficiently cooled down before handling it.
- Verify that the heat dissipation is sufficient by performing a test run under maximum load conditions.

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

At a Glance

Document Scope

The purpose of this document is to provide information about the safety function incorporated in the drive.

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 Machine ATV340 drive.

The technical characteristics of the devices described in the present document also appear online. To access the information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the reference or product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the datasheet.
6	To save or print a datasheet as a .pdf file, click **Download XXX product datasheet**.

The characteristics that are presented in the present document should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the document and online information, use the online information as your reference.

Related Documents

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on www.schneider-electric.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:

(Other option manuals and Instruction sheets are available on *www.schneider-electric.com*)

Title of Documentation	Catalog Number
Digital Catalog for Industrial Automation	*Digit-Cat*
ATV340 Catalog	*DIA2ED2160701EN* (English), *DIA2ED2160701FR* (French)
ATV340 Getting Started - Video	FAQ *FA367923* (English) 
ATV340 Getting Started	*NVE37643* (English), *NVE37642* (French), *NVE37644* (German), *NVE37646* (Spanish), *NVE37647* (Italian), *NVE37648* (Chinese), *NVE37643PT* (Portuguese), *NVE37643TR* (Turkish)
ATV340 Getting Started Annex (SCCR)	*NVE37641* (English)
Wiring Diagrams for Frame Sizes S1, S2, S3	*NVE97896* (English)
ATV340 Installation Manual	*NVE61069* (English), *NVE61071* (French), *NVE61074* (German), *NVE61075* (Spanish), *NVE61078* (Italian), *NVE61079* (Chinese), *NVE61069PT* (Portuguese), *NVE61069TR* (Turkish)
ATV340 Programming Manual	*NVE61643* (English), *NVE61644* (French), *NVE61645* (German), *NVE61647* (Spanish), *NVE61648* (Italian), *NVE61649* (Chinese), *NVE61643PT* (Portuguese), *NVE61643TR* (Turkish)
ATV340 Modbus manual (Embedded)	*NVE61654* (English)
ATV340 Ethernet manual (Embedded)	*NVE61653* (English)
ATV340 PROFIBUS DP manual (VW3A3607)	*NVE61656* (English)
ATV340 DeviceNet manual (VW3A3609)	*NVE61683* (English)
ATV340 PROFINET manual (VW3A3627)	*NVE61678* (English)
ATV340 CANopen manual (VW3A3608, 618, 628)	*NVE61655* (English)
ATV340 POWERLINK manual - (VW3A3619)	*NVE61681* (English)
ATV340 EtherCAT manual - (VW3A3601)	*NVE61686* (English)
ATV340 Sercos III manual (embedded)	*PHA33735* (English), *PHA33737* (French), *PHA33738* (German), *PHA33739* (Spanish), *PHA33740* (Italian), *PHA33741* (Chinese)
ATV340 Communication Parameters	*NVE61728* (English)
ATV340 ATEX manual	*NVE61651* (English)
ATV340 Embedded Safety Function Manual	*NVE64143* (English)
ATV340 Safety Module Manual (VW3A3802) Upcoming commercialization	*NVE61741* (English), *NVE61742* (French), *NVE61745* (German), *NVE61747* (Spanish), *NVE61749* (Italian), *NVE61752* (Chinese)
SoMove FDT	*SoMove_FDT* (English, French, German, Spanish, Italian, Chinese)
Altivar 340: DTM	*ATV340_DTM_Library_EN* (English), *ATV340_DTM_Lang_FR* (French), *ATV340_DTM_Lang_DE* (German), *ATV340_DTM_Lang_SP* (Spanish), *ATV340_DTM_Lang_IT* (Italian), *ATV340_DTM_Lang_CN* (Chinese)
Altivar Application Note for Hoisting (coming soon)	*NHA80973* (English)

You can download these technical publications and other technical information from our website at *www.schneider-electric.com/en/download*

Terminology

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.

Among others, these standards include:

- 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.

Certification for functional safety

The integrated safety function is compatible and certified following IEC 61800-5-2: 2007 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: 2007 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 or the ISO 13849-1, as well as the IEC 62061 for process systems and machinery.

The defined safety function is:

- SIL 3 capability in compliance with IEC 61800-5-2: 2007 and IEC 61508 series Ed.2
- Performance Level **e** in compliance with ISO 13849-1
- Compliant with the Category 3 of European standard ISO 13849-1

Also refer to Safety function capability.

The safety demand mode of operation is considered in high demand or continuous mode of operation according to the IEC 61800-5-2: 2007 standard.

The certificate for functional safety is accessible on *www.schneider-electric.com*

Chapter 1
Overview

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Definitions	14
Basics	15

Definitions

Safety Function In Altivar Machine

The safety function incorporated in Altivar Machine, 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 Machine 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

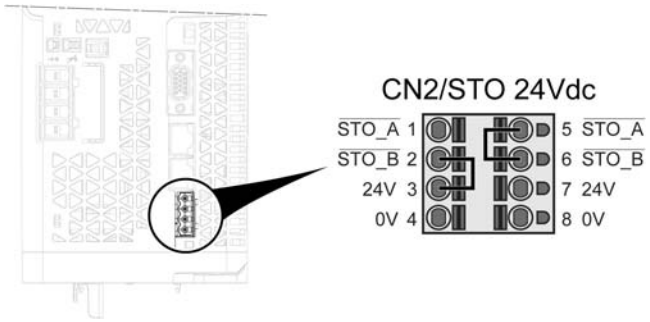
The graphic display terminal menus and parameters are shown in square brackets, with capital letters for the menus and lowercase characters for the parameters.

Example: **[COMMUNICATION]**

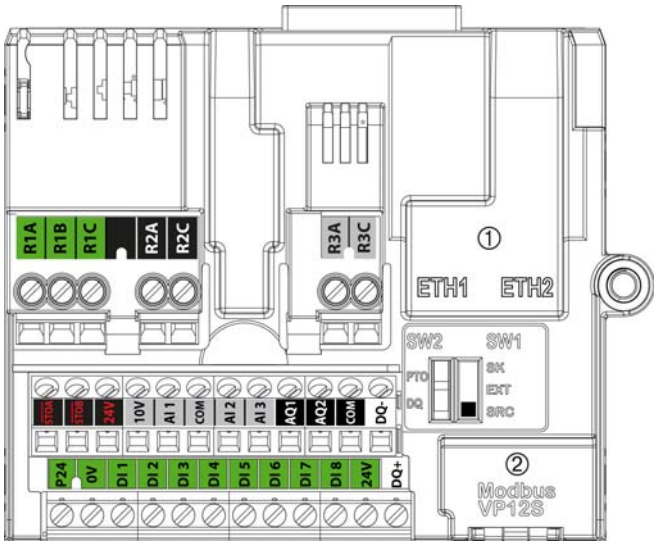
Example: **[Fallback speed]**

STO Terminals Marking

On drives of power ≤ 22 kW STO terminals are marked $\overline{\text{STO_A}}$ and $\overline{\text{STO_B}}$.



On drives of power > 22 kW STO terminals are marked $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$.



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.

ISO 13849 Standard

This 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. 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 a Dangerous Failure Per Hour (According IEC 61508-4:2010)

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 a Dangerous Failure Per Hour) for a safety system.

This is the average frequency of a dangerous failure 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 (SIL)	Average Frequency of a Dangerous Failure of the Safety Function (h^{-1}) (PFH)
4	$10^{-9} \leqslant ... < 10^{-8}$
3	$10^{-8} \leqslant ... < 10^{-7}$
2	$10^{-7} \leqslant ... < 10^{-6}$
1	$10^{-6} \leqslant ... < 10^{-5}$

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	$10^{-8} \leqslant ... < 10^{-7}$
d	$10^{-7} \leqslant ... < 10^{-6}$
c	$10^{-6} \leqslant ... < 3*10^{-6}$
b	$3*10^{-6} \leqslant ... < 10^{-5}$
a	$10^{-5} \leqslant ... < 10^{-4}$

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).

NOTE: SFF Definition: Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:
$SFF = (\Sigma\lambda S_{avg} + \Sigma\lambda Dd_{avg}) / (\Sigma\lambda S_{avg} + \Sigma\lambda Dd_{avg} + \Sigma\lambda Du_{avg})$

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 and dangerous detected 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
(*) IEC62061 standard only considers type B subsystems						

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.

Chapter 2
Description

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Safety Function STO (Safe Torque Off)	20
Limitations	21
Status of Safety Function	22

Safety Function STO (Safe Torque Off)

Overview

⚠⚠ DANGER

ELECTRIC SHOCK CAUSED BY INCORRECT USE

The safety function STO (Safe Torque Off) does not cause electric isolation. The DC bus voltage is still present.

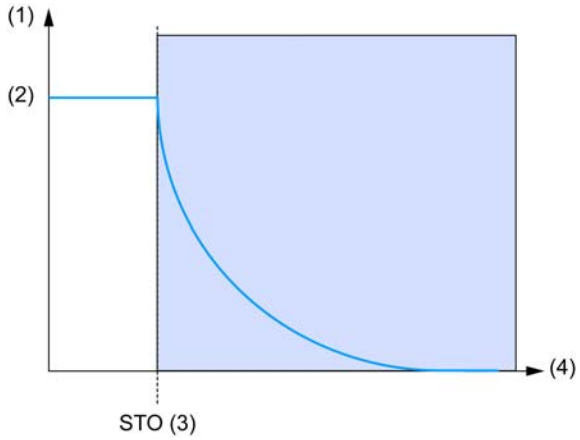
- Turn off the mains voltage using appropriate switch to achieve a voltage-free condition.

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 ($\overline{\text{STO_A}}$ or $\overline{\text{STOA}}$ and $\overline{\text{STO_B}}$ or $\overline{\text{STOB}}$) are always assigned to this function.

The safety function STO status can be displayed by the ASF LED in front of the drive, using the optional display terminal or using the commissioning software.



(1) Speed axis - (2) Motor speed - (3) $\overline{\text{STO_A}}$ or $\overline{\text{STOA}}$ and $\overline{\text{STO_B}}$ or $\overline{\text{STOB}}$ - STO Activation - (4) Time

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

Safety Function STO Standard Reference

The safety function STO is defined in section 4.2.2.2 of standard IEC 61800-5-2: 2007:

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
STO with and without Safety module (such as Preventa module)	SIL3	PL**e**

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

Limitations

Type Of Motor

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

Prerequisites for Using Safety Functions

Following conditions have to be fulfilled for correct operation:

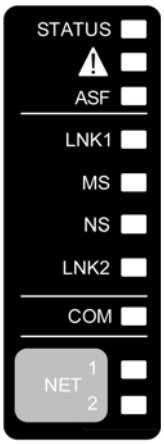
- The motor size is adequate for the application and is not at the limit of its capacity.
- The drive size has been correctly chosen for the supply mains, sequence, motor, and application and is not at the limit of its capacity as stated in the catalog.
- If required, the appropriate options are used.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

Disable Error Detection

When the safety function is used, the error code **[Safety Function Error]** $SAFF$ cannot be disabled by the function **[Disable Error Detection]** inH.

Status of Safety Function

Product LEDs

LEDs on Frame sizes 1...3	LEDs on Frame sizes 4 and 5
	

Description

If...	Then ...
Safe Torque Off (STO) is not active	the orange **ASF** LED is OFF
STO is triggered	the power bridge is locked by redundant hardware the orange **ASF** LED is steady ON if using the optional display terminal, `StO` is displayed
[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 if using the optional display terminal, `StO` then `SAFF` are displayed
(1) Possible causes are exceeded delay between $\overline{\text{STO_A}}$ or $\overline{\text{STOA}}$ and $\overline{\text{STO_B}}$ or $\overline{\text{STOB}}$ signals > 1 s and internal hardware detected error.	

Chapter 3
Technical Data

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Electrical Data	24
Safety Function Capability	25

Electrical Data

Logic Type

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

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

Cabling

Also refer to the Installation manual *NVE61069* and the Getting Started with ATV340 manual *NVE37643* available on *www.schneider-electric.com*

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
Accepted switching delay between $\overline{\text{STO_A}}$ or $\overline{\text{STOA}}$ and $\overline{\text{STO_B}}$ or $\overline{\text{STOB}}$	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	SIL3
IEC 62061 (1)	SIL3 CL
ISO 13849-1 (2)	Category 3 PL**e**
IEC 60204-1 (3)	Category stop 0
(1) Because the IEC 62061 standard concerns integration, this standard distinguishes the overall safety function (which is classified SIL3) from components which constitute the safety function (Altivar Machine is one component which is classified SIL3 CL). **(2)** According to table 3 of ISO 13849-1 (2015). **(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.	

Summary Of The Reliability Study

Standard	Input	ATV340
IEC 61508 Ed.2	SFF	90%
	PFH in /h	3×10^{-10}
	PFD	2×10^{-6}
	Type	A
	HFT	1
	T1 (proof test interval) in hours	8760
	SIL capability	3
IEC 62061	SIL CL capability	3
ISO 13849-1 (1)	PL	e
	Category	3
	MTTFd in years	7000
	DC avg	90%
(1) According to table 3 of ISO 13849-1 (2015)		

Preventive annual activation of the safety function is recommended.

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

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 system integrator has to evaluate the random integrity as well as the systematic integrity at system level according to IEC61508, IEC 62061, ISO13849 or applicable product standard.

Chapter 4
Certified Architectures

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Introduction	28
Machine System SF - Case 1	30
Machine System SF - Case 2	33
Machine System SF - Case 3	36

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:

- Process system SF - Case 1
- Process system SF - Case 2
- Process system SF - Case 3

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 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 +24 Vdc supply voltage is connected with many exposed signal connections in the drive system.

- Use a power supply unit that meets the PELV (Protective Extra Low Voltage) requirements.
- Connect the negative output of the power supply unit to PE (ground).

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 drives.

Please refer to the manual corresponding to the drive:

Drive Range	Documentation
ATV340	*NVE61069*

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.

ATV340 Drive Frame Sizes

The wiring diagrams in next chapters are not the same for drive frame sizes 1...3 and drive frame sizes 4 and 5. The following table shows the drive frame size according to the drive catalog number. Detailed information is also given in the Installation manual *NVE61069*

Catalog Numbers ATV340...	Frame Sizes
ATV340U07N4•... ATV340U40N4•	1
ATV340U55N4•... ATV340U75N4•	2
ATV340D11N4•... ATV340D22N4•	3
ATV340D30N4E... ATV340D37N4E	4
ATV340D45N4E... ATV340D75N4E	5
•: N4 or N4E	

Customer Care Center

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

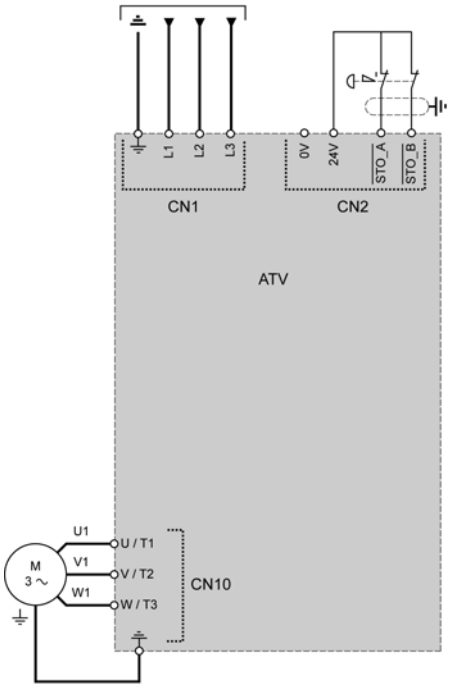
www.schneider-electric.com/CCC.

Machine System SF - Case 1

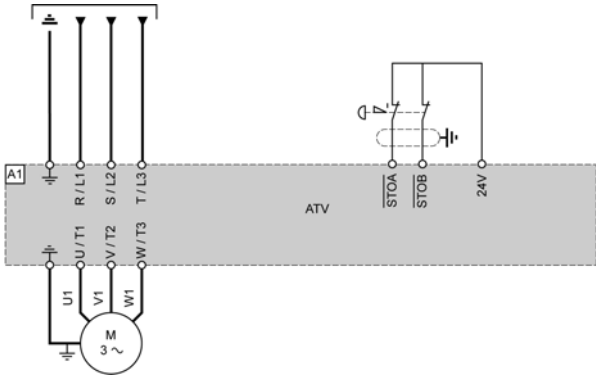
Single Drive Connection Diagram

This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL3, IEC 60204-1 stop category 0 without protection against subsequent rotation after supply interruption or voltage reduction.

Wiring diagram for frame sizes 1...3



Wiring diagram for frame sizes 4 and 5

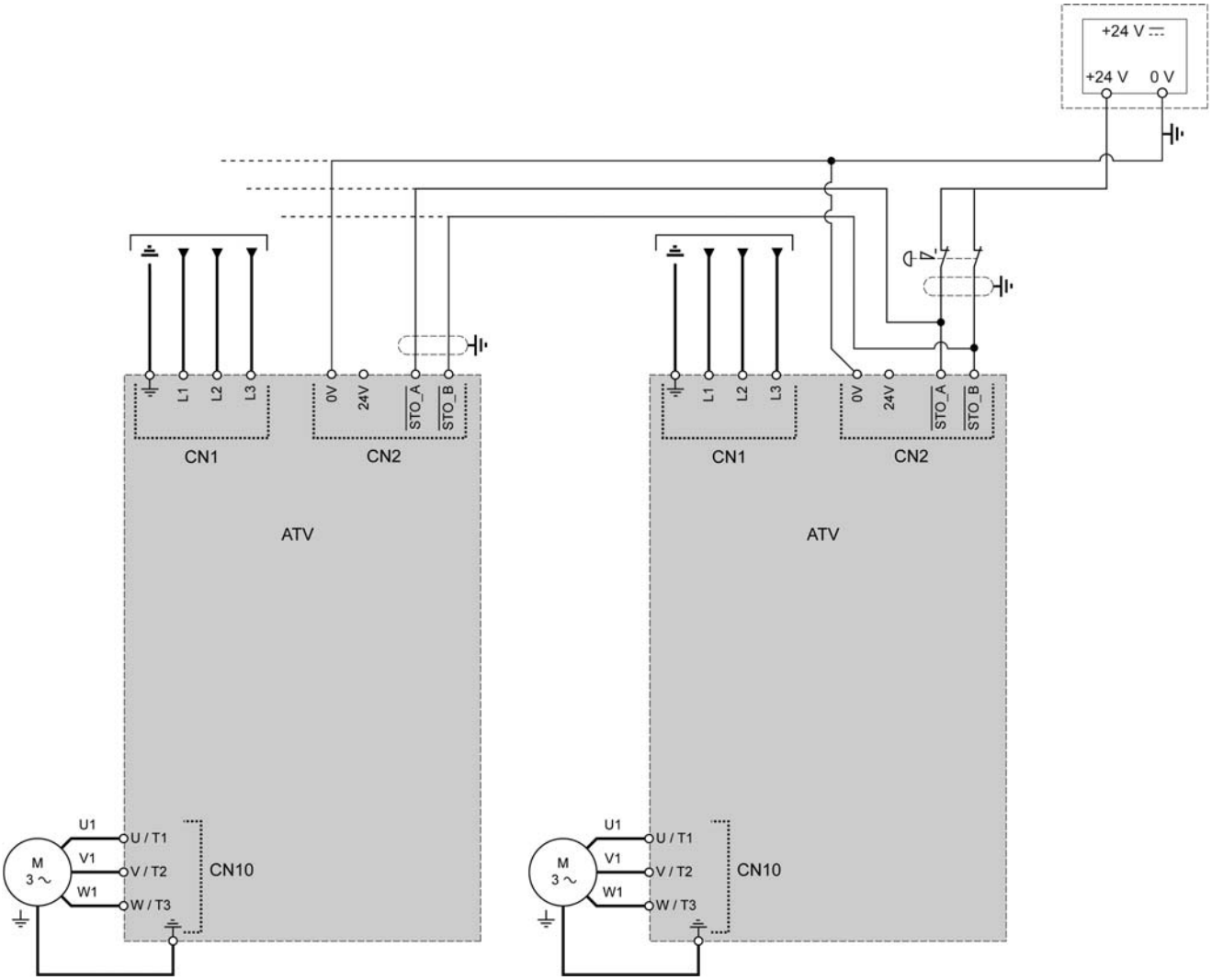


Multidrive Connection Diagram

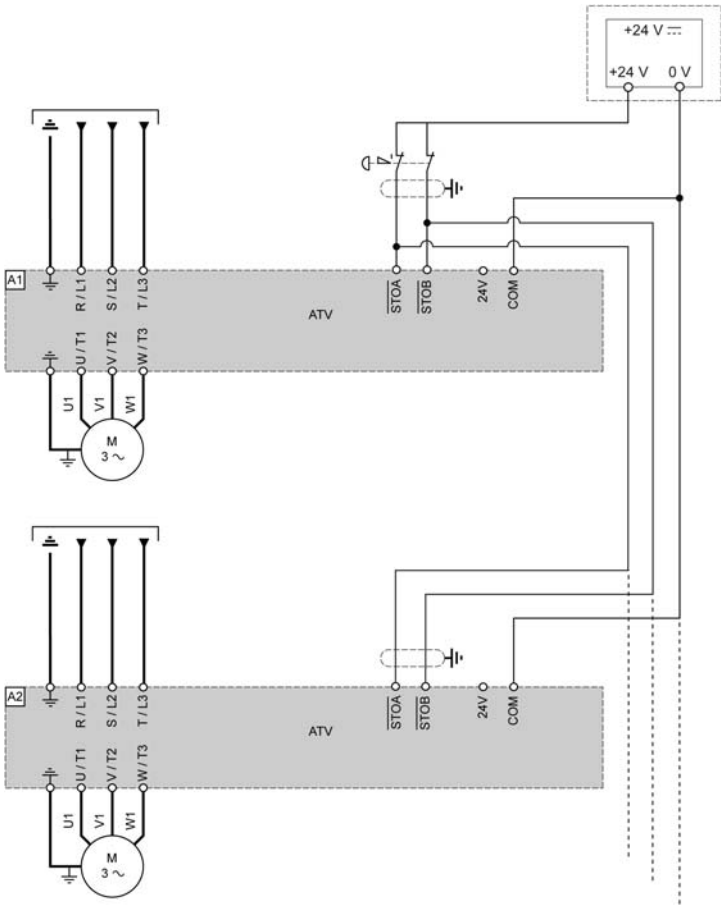
This connection diagram applies for multidrive configuration according to IEC 61508 capability SIL3, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.

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

Wiring diagram for frame sizes 1...3



Wiring diagram for frame sizes 4 and 5

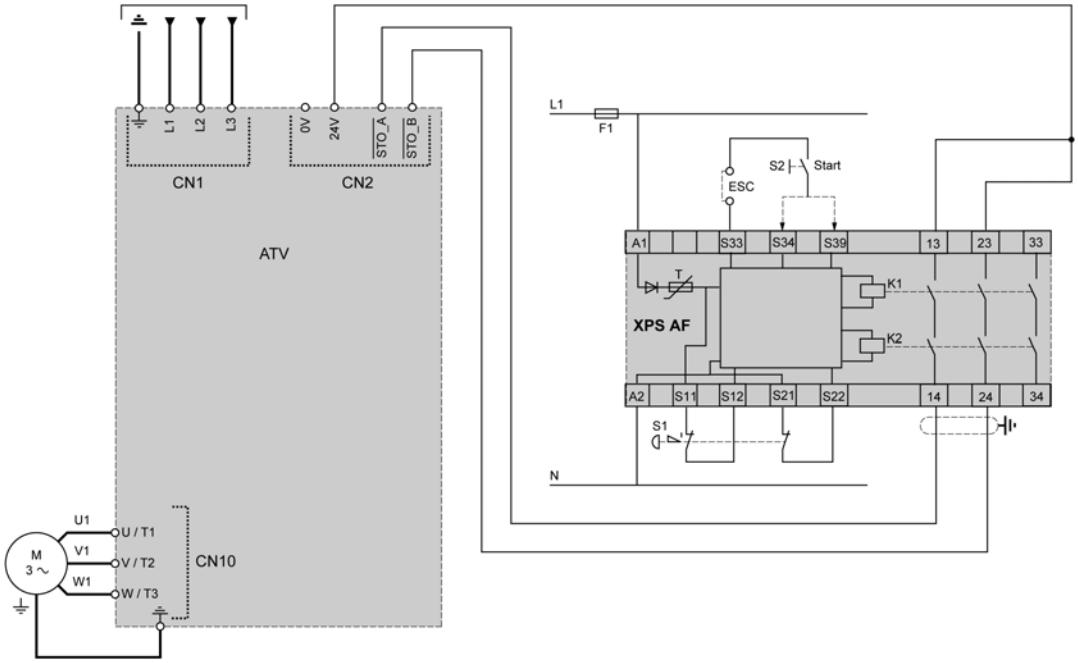


Machine System SF - Case 2

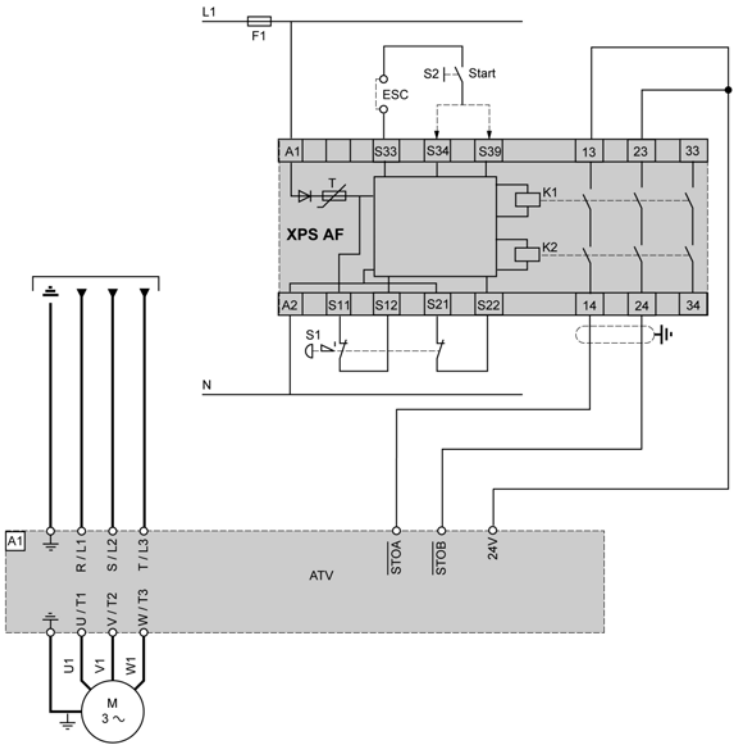
Single Drive with Safety Module Type Preventa XPS-AF Connection Diagram

This connection diagram applies for a single drive configuration with the safety module type Preventa XPS-AF according to ISO 13849-1 category 3 PLe, IEC 62061 and 60204-1 stop category 0.

Wiring diagram for frame sizes 1...3



Wiring diagram for frame sizes 4 and 5

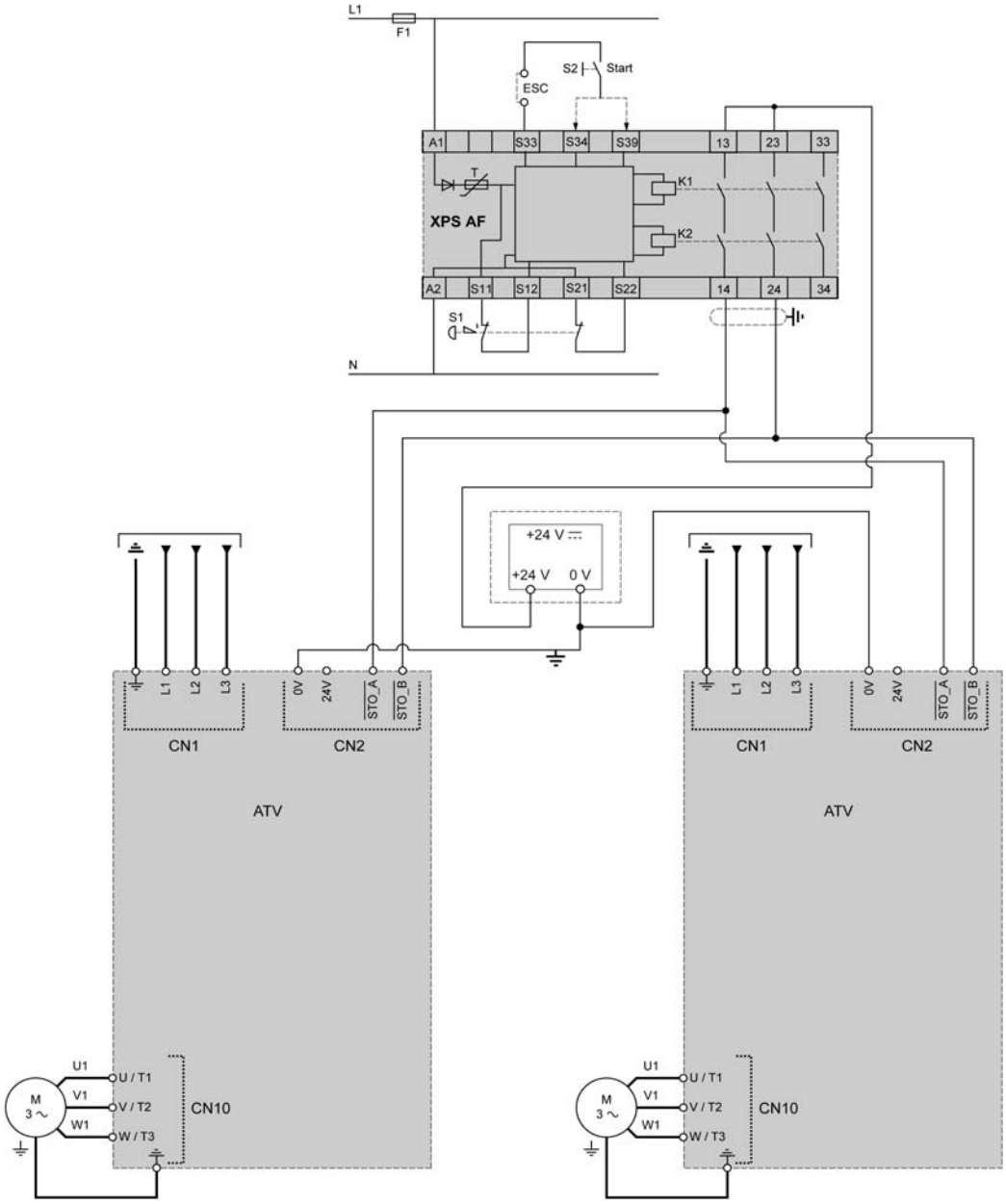


Multidrive with Safety Module Type Preventa XPS-AF Connection Diagram

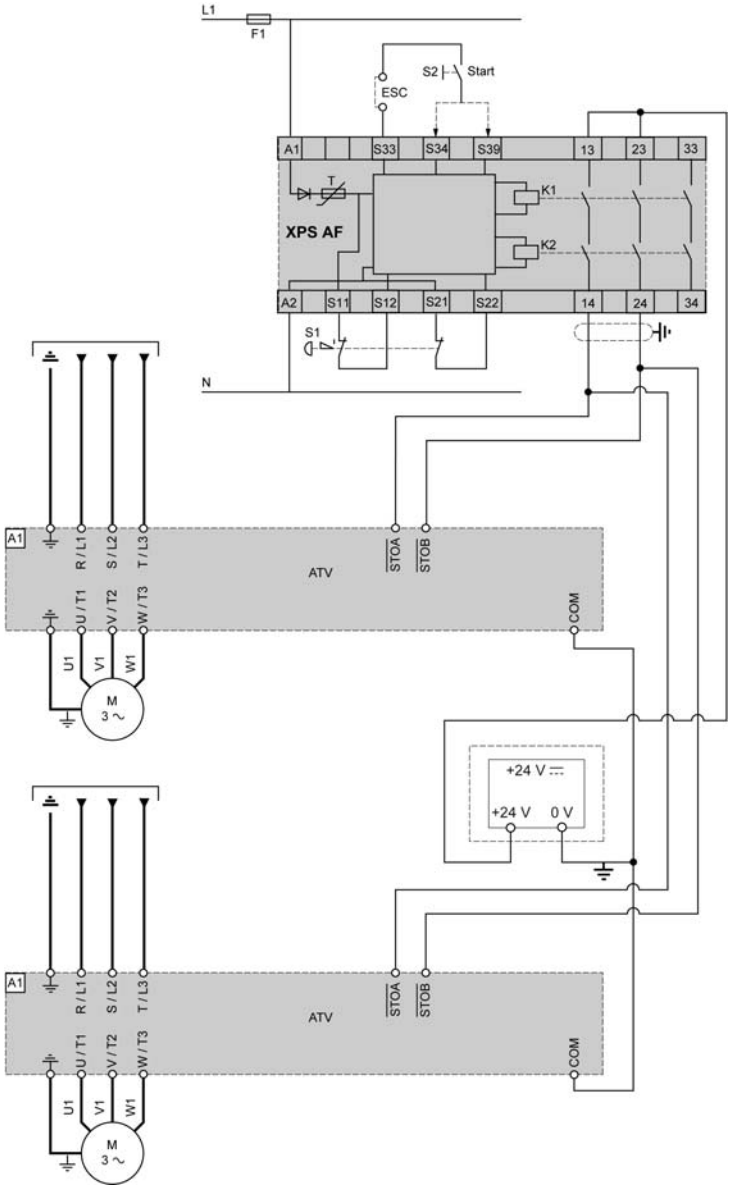
This connection diagram applies for a multidrive configuration with the safety module type Preventa XPS-AF according to ISO 13849-1 category 3 PLe, IEC 62061 and 60204-1 stop category 0.

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

Wiring diagram for frame sizes 1...3



Wiring diagram for frame sizes 4 and 5

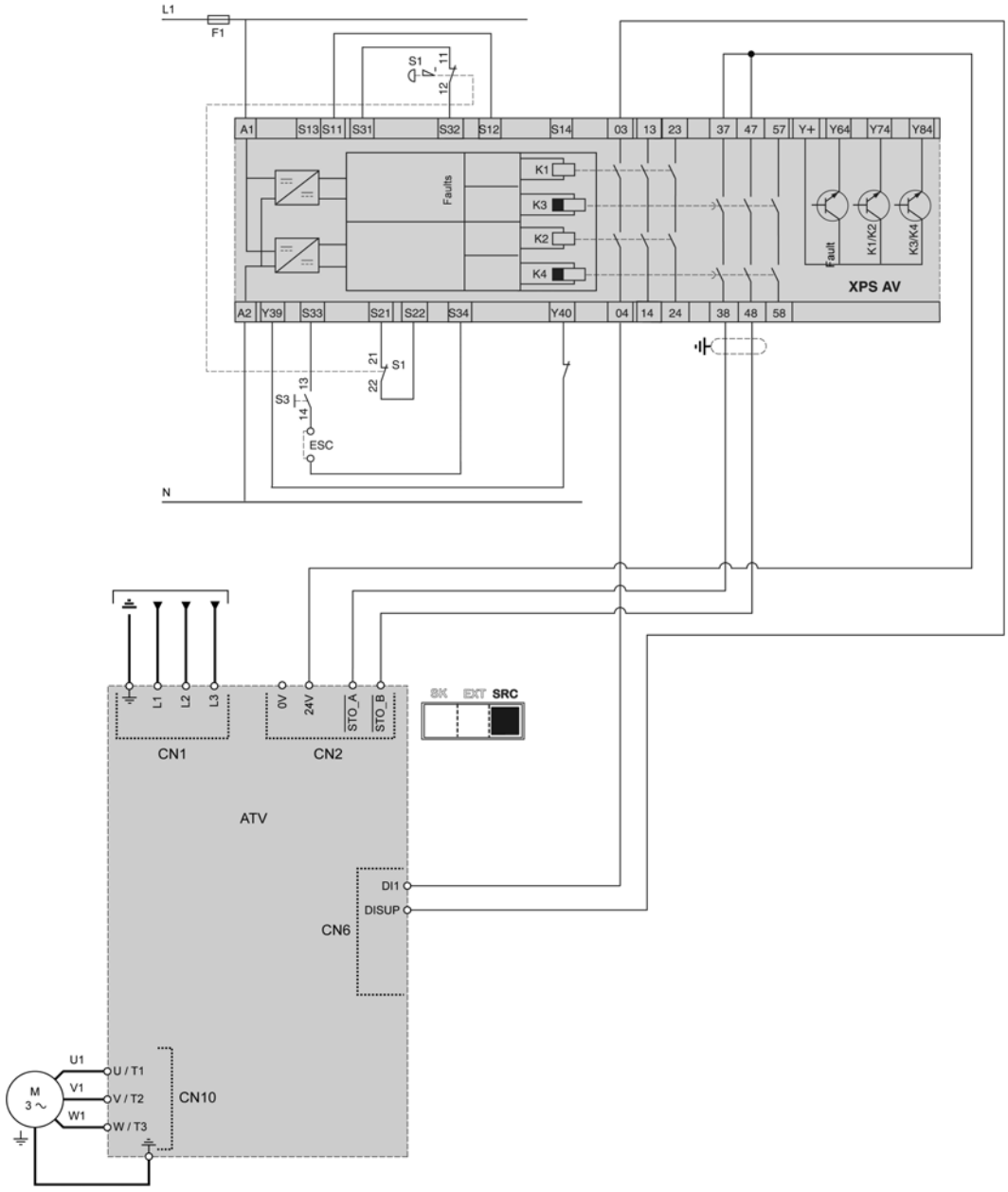


Machine System SF - Case 3

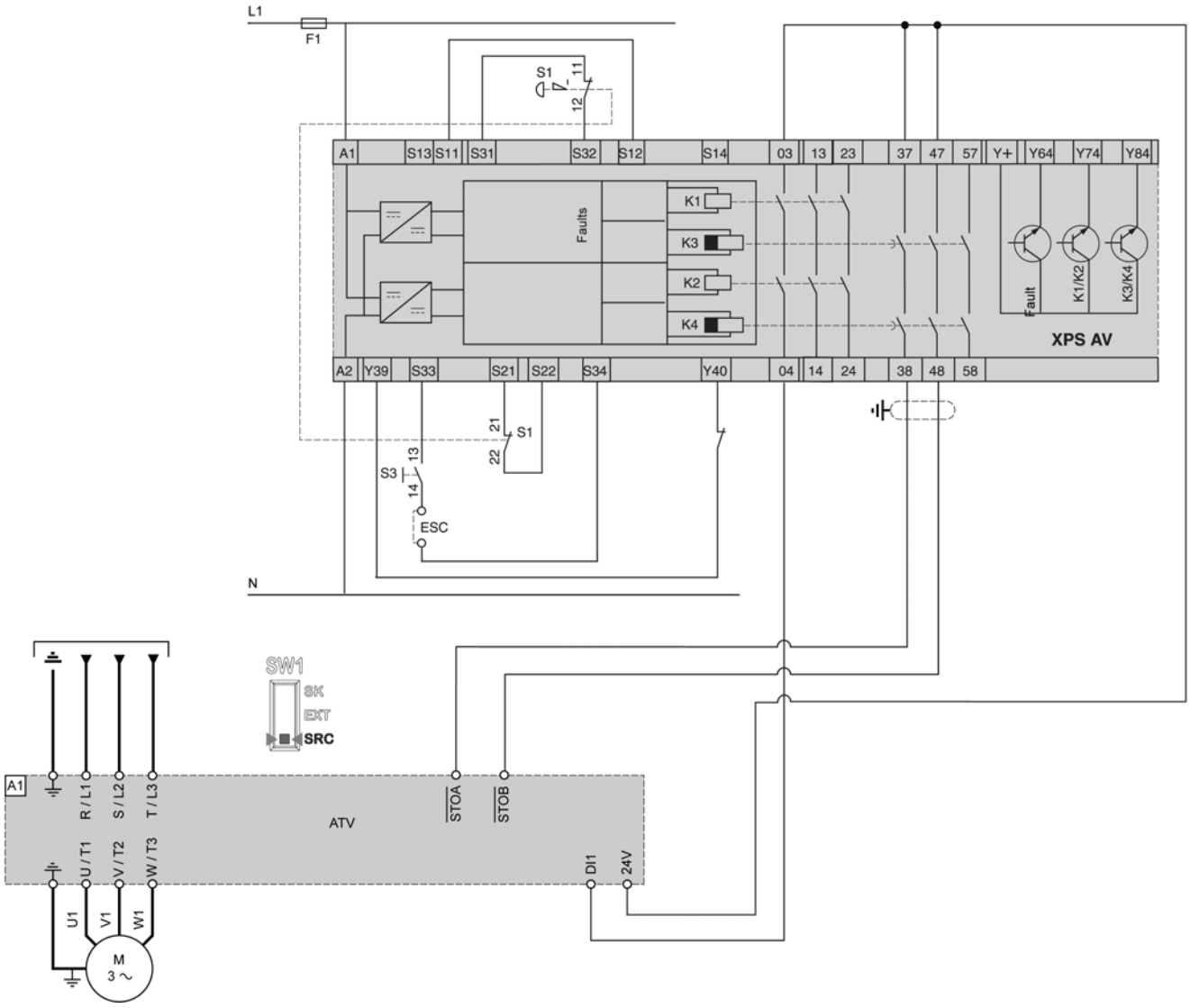
Connection Diagram For Single Drive with Safety Module Type Preventa XPS-AV

This Connection diagram applies for a single drive configuration with the Safety Module Type Preventa XPS AV According to ISO 13849-1 category 3 PLe and IEC 60204-1 stop category 1.

Wiring diagram for frame sizes 1...3



Wiring diagram for frame sizes 4 and 5



NOTE: This diagram is a wiring configuration using DI1 assigned to forward operation.

Glossary

A

AC

Alternating Current

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

Factory settings when the product is shipped

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).

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.

G

GP

General-Purpose

L

L/R

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

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

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.

PTC

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

R

REACh

Registration, Evaluation, Authorisation and restriction of Chemicals regulation

RoHS

Restriction of Hazardous Substances

S

SCPD

Short-Circuit Protective Device

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)

W

Warning

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

