

Altivar Process

Variable Speed Drives ATV630, ATV650,
ATV660, ATV680

Embedded Safety Function Manual

06/2017



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.

© 2017 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	17
	Safety Function STO (Safe Torque Off)	18
	Limitations	19
	Status of Safety Function	20
Chapter 3	Technical Data	21
	Electrical Data	22
	Safety Function Capability	23
Chapter 4	Certified Architectures	25
	Introduction	26
	Process System SF - Case 1	28
	Process System SF - Case 2	29
	Process System SF - Case 3	31
	Process System SF - Case 4	32
	Process System SF - Case 5	34
	Process System SF - Case 6	36
	Process System SF - Case 7	38



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, 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. Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel.

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.

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.

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.

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.

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.

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.

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.

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 Process drives and drive systems described in the Installation manual.

The technical characteristics of the devices described in this document also appear online. To access this 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 data sheet.
6	To save or print a data sheet as a .pdf file, click Download XXX product datasheet .

The characteristics that are presented in this manual 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 manual 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
ATV600 Getting Started	EAV63253 (English), EAV63254 (French), EAV63255 (German), EAV63256 (Spanish), EAV63257 (Italian), EAV64298 (Chinese)
ATV600 Getting Started Annex (SCCR)	EAV64300 (English)
ATV630, ATV650 Installation Manual	EAV64301 (English), EAV64302 (French), EAV64306 (German), EAV64307 (Spanish), EAV64310 (Italian), EAV64317 (Chinese)
ATV600 Programming Manual	EAV64318 (English), EAV64320 (French), EAV64321 (German), EAV64322 (Spanish), EAV64323 (Italian), EAV64324 (Chinese)

Title of Documentation	Catalog Number
ATV600 Modbus Serial Link Manual (Embedded)	EAV64325 (English)
ATV600 Ethernet Manual (Embedded)	EAV64327 (English)
ATV600 Ethernet IP - Modbus TCP Manual (VW3A3720, 721)	EAV64328 (English)
ATV600 PROFIBUS DP manual (VW3A3607)	EAV64329 (English)
ATV600 DeviceNet manual (VW3A3609)	EAV64330 (English)
ATV600 PROFINET manual (VW3A3627)	EAV64331 (English)
ATV600 CANopen Manual (VW3A3608, 618, 628)	EAV64333 (English)
ATV600 Communication Parameters	EAV64332 (English)
ATV600 Embedded Safety Function manual	EAV64334 (English)
Altivar Process Drive Systems Installation manual	NHA37119 (English), NHA37121 (French), NHA37118 (German), NHA37122 (Spanish), NHA37123 (Italian), NHA37130 (Chinese), NHA37124 (Dutch), NHA37126 (Polish), NHA37127 (Portuguese), NHA37128 (Russian), NHA37129 (Turkish)
ATV660 Handbook	NHA37111 (English), NHA37110 (German)
ATV680 Handbook	NHA37113 (English), NHA37112 (German)
ATV600F, ATV900F Installation Instruction sheet	NVE57369 (English)
ATV600, ATV900 ATEX manual	NVE42416 (English)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
Altivar Process ATV600: DTM	ATV6xx DTM Library_EN (English), ATV6xx DTM Lang_FR (French), ATV6xx DTM Lang_DE (German), ATV6xx DTM Lang_SP (Spanish), ATV6xx DTM Lang_IT (Italian), ATV6xx DTM Lang_CN (Chinese)

You can download these technical publications and other technical information from our website at <http://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.

EC Declaration of Conformity

The EC Declaration of Conformity can be obtained on www.schneider-electric.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, 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 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 (*see page 23*).

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.schneider-electric.com

Contact Us

Select your country on:

www.schneider-electric.com/contact

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

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 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

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]**

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 - Probability of a Dangerous Hardware Failure Per Hour

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected 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 (Probability of a 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	Probability of a dangerous Failure per Hour (PFH) at high demand or continuous demand
4	$10^{-9} \leq \dots < 10^{-8}$
3	$10^{-8} \leq \dots < 10^{-7}$
2	$10^{-7} \leq \dots < 10^{-6}$
1	$10^{-6} \leq \dots < 10^{-5}$

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	$10^{-8} \leq \dots < 10^{-7}$
d	$10^{-7} \leq \dots < 10^{-6}$
c	$10^{-6} \leq \dots < 3 \times 10^{-6}$
b	$3 \times 10^{-6} \leq \dots < 10^{-5}$
a	$10^{-5} \leq \dots < 10^{-4}$

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

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)	18
Limitations	19
Status of Safety Function	20

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.

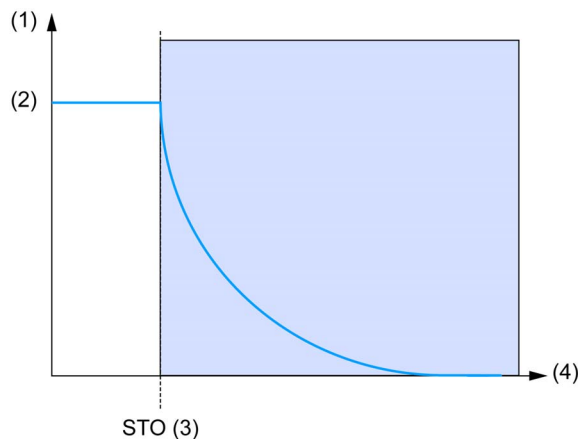
- Turn off the mains voltage using appropriate switch to achieve a voltage-free condition.

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 ($\overline{\text{STOA}}$ 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] 5 H F F**.

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	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.
If the use of an additional safety module is not possible, the drive control must be configured in 2 wires transition ($\overline{L} \overline{C} C = \overline{2} C$ and $\overline{L} \overline{C} \overline{L} = \overline{L} r n$) or 3 wires ($\overline{L} \overline{C} C = \overline{3} C$).

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: 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.

Disable Error Detection

When the safety function is used, the error code **[Safety Function Error] 5 H F F** cannot be disabled by the function **[Disable Error Detection] 1 n H**.

Status of Safety Function

Description

If...	Then ...
Safe Torque Off (STO) is not active	the orange LED is OFF
STO is triggered	the power bridge is locked by redundant hardware the orange LED is steady ON STO is displayed
[Safety Function Error] 5 H F F detected fault occurs (1)	the power bridge is locked the orange LED is steady ON the red LED is steady ON the Graphic Display terminal displays 5 L a then 5 H F F
(1) Possible causes are exceeded delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ signals > 1 s and internal hardware detected error.	

Chapter 3

Technical Data

What Is in This Chapter?

This chapter contains the following topics:

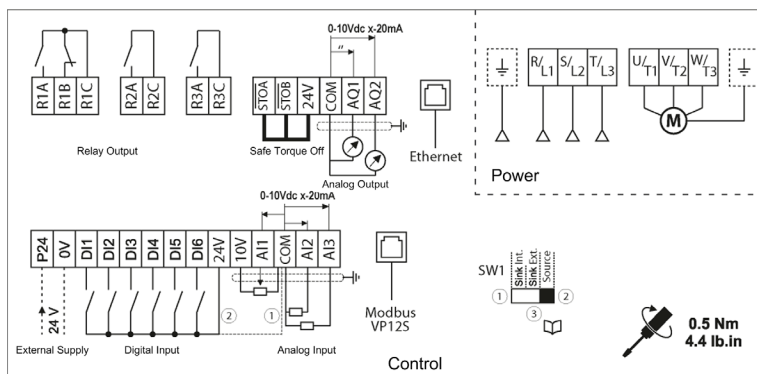
Topic	Page
Electrical Data	22
Safety Function Capability	23

Electrical Data

Logic Type

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

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
Delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$	s	< 1
Response time of safety function	ms	< 10

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 PLe
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 Process 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.	

Process Application Function Configuration

Standard	STO
IEC 61800-5-2 / IEC 61508	SIL3
IEC 62061	SIL3 CL

Summary Of The Reliability Study

Standard	Input	ATV630 ATV650 ATV660 ATV680
IEC 61508 Ed.2	SFF	90.2%
	PFH in /h	4×10^{-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	5000 (2)
	DC avg	90%
(1) According to table 4 of EN 13849-1 (2008) (2) According to ISO13849, the MTTFd has to be reduced to 100 years.		

Preventive annual activation of the safety function is recommended.

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

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

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.

Summary Of The Reliability Study For Drive Systems Options

Standard	Input	ATV660 / ATV680 With Option		
		VW3 AP 1502	VW3 AP 1503	ETO
IEC 61508 Ed.2	PFH in /h	5×10^{-8}	5×10^{-8}	2×10^{-6}
	PFD	2×10^{-6}	4×10^{-4}	4×10^{-5}
	Type	A	A	A
	HFT	1	1	0
	T1 (proof test interval) in hours	8760	8760	8760
	SIL capability	3	3	1
IEC 62061	SIL CL capability	3	3	1
ISO 13849-1 (1)	PL	e	e	c
	Category	3	3	1
	MTTFd in years	> 100 (high)	> 100 (high)	> 100 (high)
	DC avg	> 90% (Medium)	> 90% (Medium)	0%
(1) According to table 4 of EN 13849-1 (2008)				

Preventive annual activation of the safety function is recommended.

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

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

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	26
Process System SF - Case 1	28
Process System SF - Case 2	29
Process System SF - Case 3	31
Process System SF - Case 4	32
Process System SF - Case 5	34
Process System SF - Case 6	36
Process System SF - Case 7	38

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
- Process system SF - Case 4
- Process system SF - Case 5
- Process system SF - Case 6
- Process system SF - Case 7

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, see the ATV630, 650 Installation manual [EAV64301](#) on www.schneider-electric.com.

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

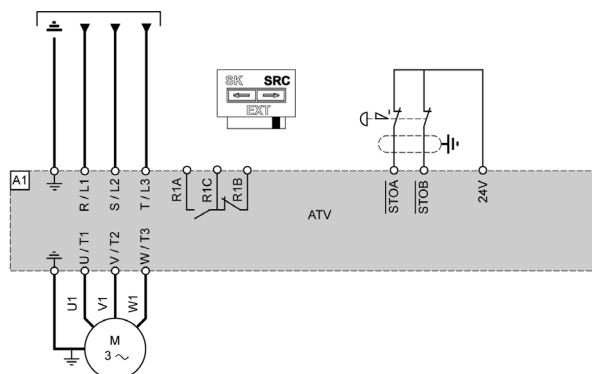
For additional support, you can contact our Customer Care Center on:

www.schneider-electric.com/CCC.

Process System SF - Case 1

Single Drive Connection Diagram

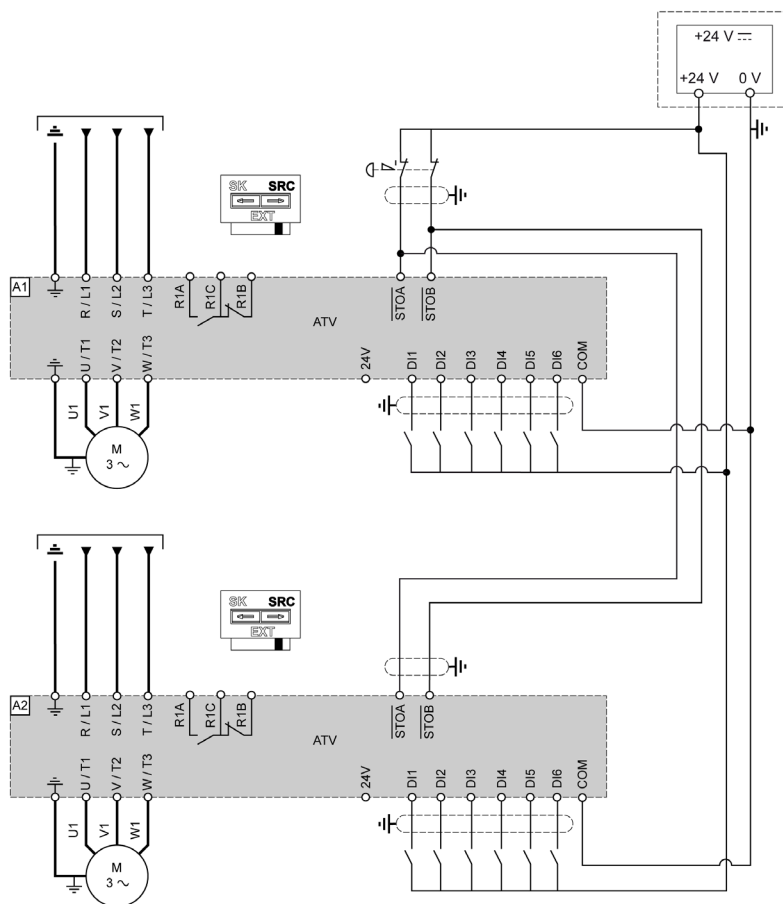
This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL3, IEC 60204-1 stop category 0 without protection against subsequent rotation after supply interruption or voltage reduction.



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).

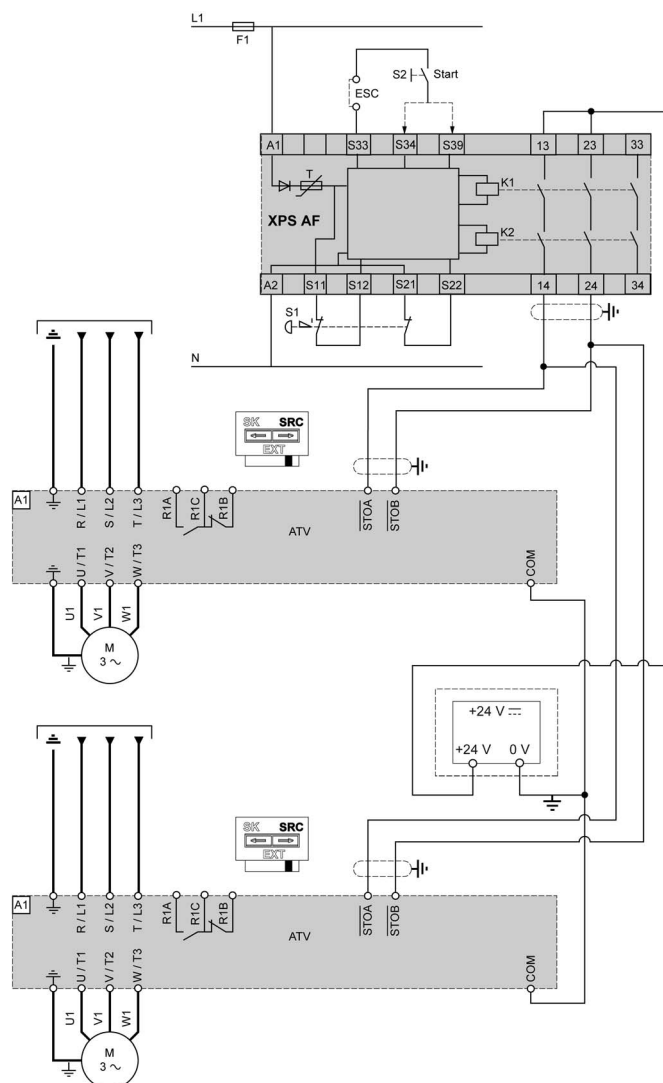


Single Drive with Safety Module Type Preventa XPS-AF Connection Diagram

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.

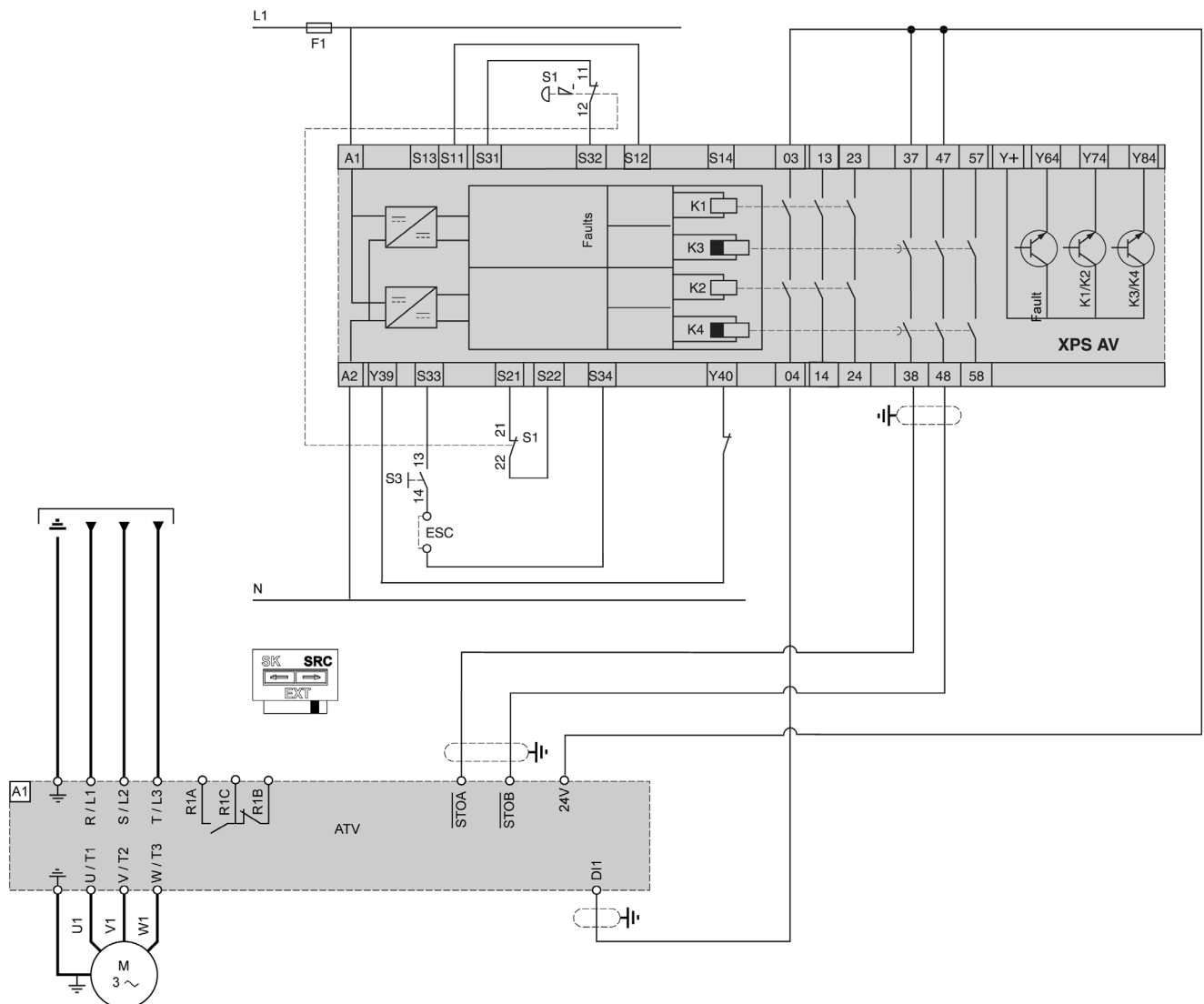
NOTE: The +24VDC power supply must meet the requirements of IEC 61131-2 (PELV standard power supply unit).



Process 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.

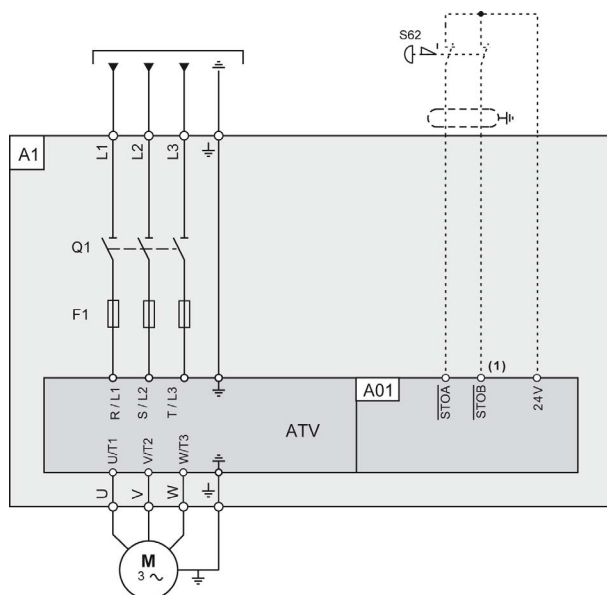


NOTE: This diagram is a wiring configuration using DI1 assigned to forward operation.

Process System SF - Case 4

Single Drive Systems Connection Diagram

This connection diagram applies for a single Altivar Process Drive Systems configuration, without options according to IEC 61508 capability SIL3, ISO 13849-1 category 3 PL e, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



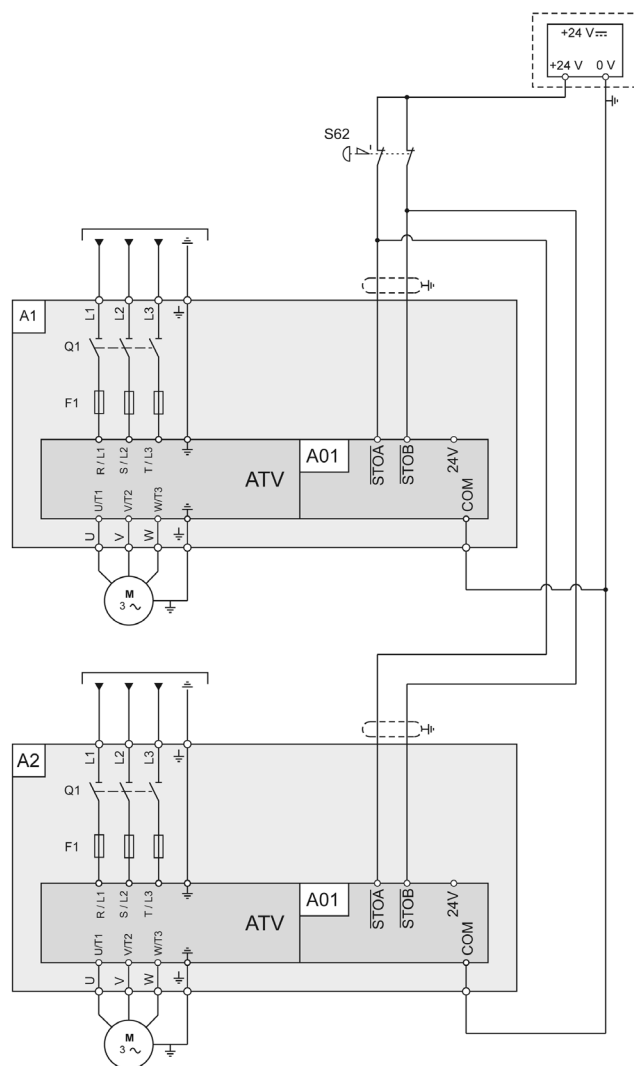
Legend:

- A: Drive Systems enclosure with certified Drive Systems components assembly
 - A01: Control block of the Drive System
- S62: External Emergency Stop button (not included within the certification)
- (1): If S62 external emergency stop is installed, the link between terminals STOA and +24V, and between terminals STOB and +24V has to be removed.

NOTE: An EMERGENCY STOP is requested. This request leads to a category 0 stop. The power stage is immediately disabled via the inputs STOA and STOB of the safety function STO. Power can no longer be supplied to the motor. If the motor has not yet stopped at this point in time, it coasts down in an uncontrolled way (uncontrolled stop).

Multi drive Drive Systems Connection Diagram

This connection diagram applies for multidrive Altivar Process Drive Systems configuration, without options, according to IEC 61508 capability SIL 3, ISO 13849-1 category 3 PL e, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



Legend:

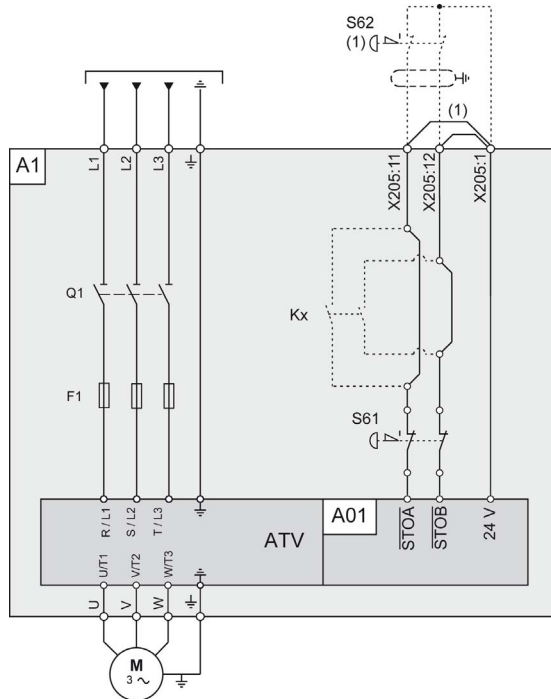
- A1, A2: Drive Systems enclosures with certified Drive Systems components assembly
 - A01: Control block of the Drive System
- S62: External Emergency Stop button (not included within the certification)

NOTE: An EMERGENCY STOP is requested. This request leads to a category 0 stop. The power stage is immediately disabled via the inputs STOA and STOB of the safety function STO. Power can no longer be supplied to the motor. If the motor has not yet stopped at this point in time, it coasts down in an uncontrolled way (uncontrolled stop).

Process System SF - Case 5

Single Drive Systems Connection Diagram with Option Safe Torque Off STO - SIL3 Stop category 0

This connection diagram applies for a single Altivar Process Drive Systems configuration, with option VW3AP1502 (Safe Torque Off STO - SIL 3 Stop Category 0) according to IEC 61508 capability SIL3, ISO 13849-1 category 3 PL e, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



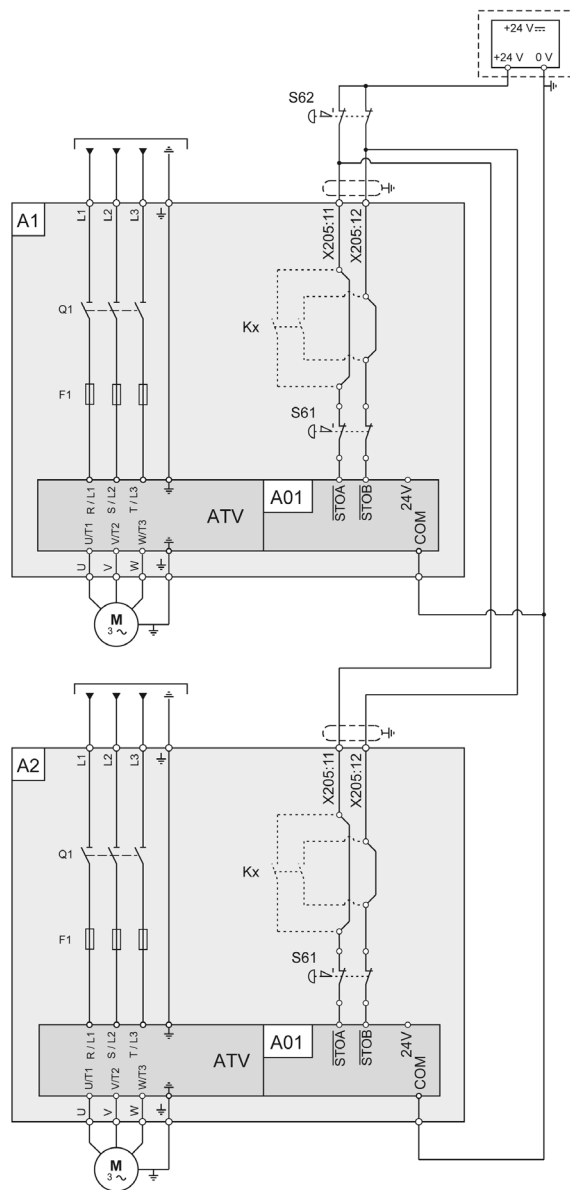
Legend:

- A1: Drive Systems enclosure with certified architecture, with built-in Drive Systems components assembly and with option VW3AP1502.
 - A01: Control block of the Drive System
 - S61: Emergency Stop button mounted in the enclosure door
- S62: External Emergency Stop button (not included within the certification)
- (1): If S62 external emergency stop is installed, the wire link between terminals X205:11 and X205:12, and between terminals X205:12 and X205:1 has to be removed.
- Kx: optional additional contacts within the safety path (not included within the certification). These contacts have to be taken into account separately for the safety path calculation

NOTE: An EMERGENCY STOP is requested. This request leads to a category 0 stop. The power stage is immediately disabled via the inputs STOA and STOB of the safety function STO. Power can no longer be supplied to the motor. If the motor has not yet stopped at this point in time, it coasts down in an uncontrolled way (uncontrolled stop).

Multi drive Drive Systems Connection Diagram

This connection diagram applies for multidrive Altivar Process Drive Systems configuration, with option VW3AP1502 (Safe Torque Off STO - SIL 3 Stop Category 0) according to IEC 61508 capability SIL 3, ISO 13849-1 category 3 PL e, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



Legend:

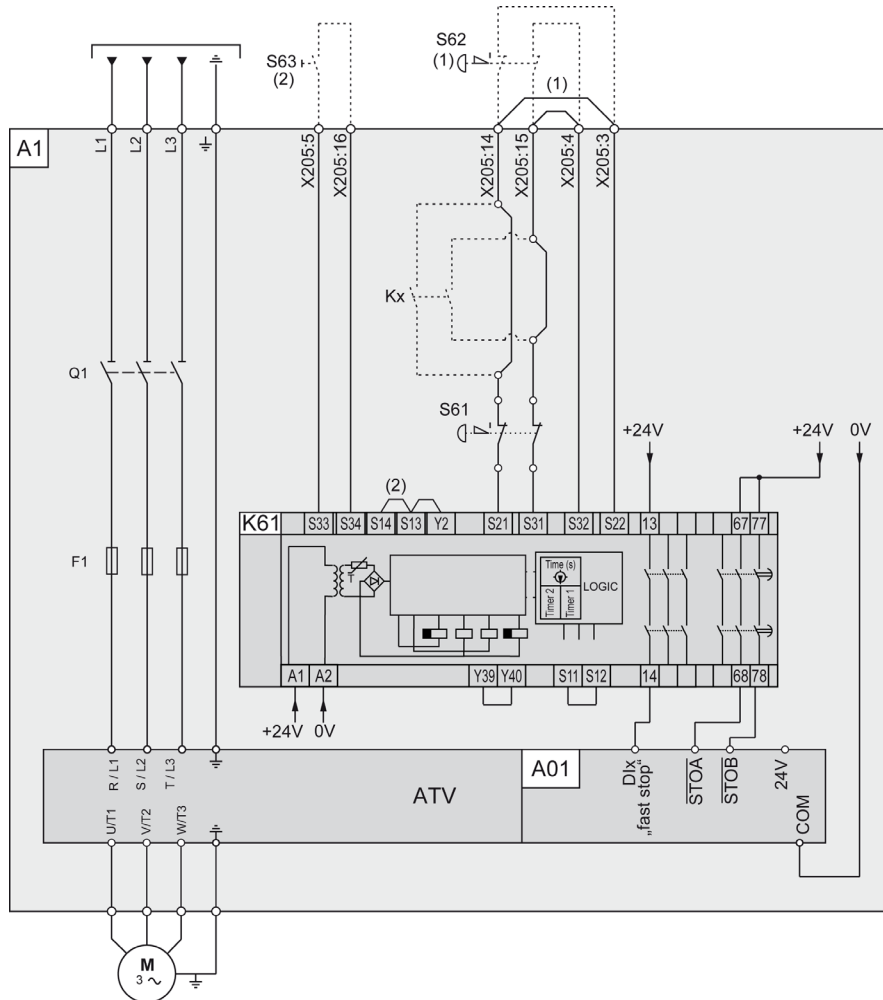
- A1: Drive Systems enclosure with certified architecture, with built-in Drive Systems components assembly and with option VW3AP1502.
 - A01: Control block of the Drive System
 - S61: Emergency Stop buttons mounted in the enclosure door
- S62: External Emergency Stop button (not included within the certification)
- Kx: optional additional contacts within the safety path (not included within the certification). These contacts have to be taken into account separately for the safety path calculation.

NOTE: An EMERGENCY STOP is requested. This request leads to a category 0 stop. The power stage is immediately disabled via the inputs **STOA** and **STOB** of the safety function **STO**. Power can no longer be supplied to the motor. If the motor has not yet stopped at this point in time, it coasts down in an uncontrolled way (uncontrolled stop).

Process System SF - Case 6

Single Drive Systems Connection Diagram with Option Safe Torque Off STO - SIL3 Stop category 1

This connection diagram applies for a single Altivar Process Drive Systems configuration, with option VW3AP1503 (Safe Torque Off STO - SIL 3 Stop Category 1) according to IEC 61508 capability SIL 3, ISO 13849-1 category 3 PL e, IEC 60204-1 stop category 1.



Legend:

- A1: Drive Systems enclosure with certified architecture, with built-in Drive Systems components assembly and with option VW3AP1503.
 - A01: Control block of the Drive System
 - K61: Safety relay for monitoring the Emergency Stop circuit: Preventa XPS-ATR
 - S61: Emergency Stop buttons mounted in the enclosure door
 - Dlx: Internal I/O set to "fast stop"
- S62: External Emergency Stop button (not included within the certification)
- (1): If S62 external emergency stop is installed, the wire link between terminals X205:14 and X205:15, and between terminals X205:15 and X205:4 has to be removed.
- Kx: optional additional contacts within the safety path (not included within the certification). These contacts have to be taken into account separately for the safety path calculation.
- S63: Manual reset button
- (2): If a manual reset button is installed the wire link between the terminals S13/S14 on the safety relay has to be removed.

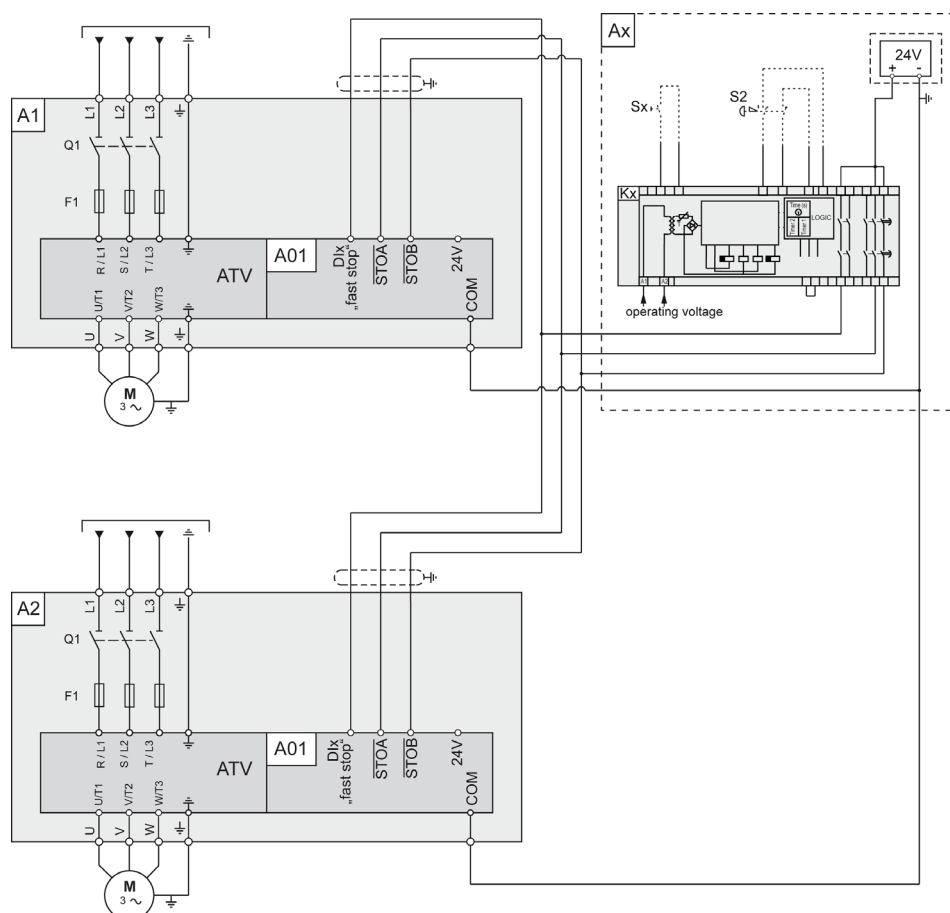
Example

An Emergency Stop is requested. This request leads to a stop category 1:

- The function "fast stop" is immediately started (undelayed) via the digital input DIx (single-channel, not monitored). Any active movement is decelerated via the adjusted ramp.
- The power stage is disabled via the inputs STO_A and STO_B of the safety STO function after the delay time set in the Emergency Stop Safety Module has elapsed. Power can no longer be supplied to the motor. If the motor has not stopped yet when the delay time has elapsed, it coasts down in an uncontrolled way (uncontrolled stop).

Multidrive Drive Systems Connection diagram with Safety Module

This connection diagram applies for a multidrive Altivar Process Drive Systems configuration with a safety module stop category 1.



Legend:

- A1, A2: Drive Systems enclosure without options (certified - see case 4), with certified Drive Systems components assembly.
 - A01: Control block of the Drive System
- Ax: External functional safety path (not included within the certification) with following components:
 - S2: External Emergency Stop button
 - Kx: Safety module
 - Sx: Manual reset button

Example

An Emergency Stop is requested if an Emergency Stop Safety Module, with stop category 1 is used. This request leads to a stop category 1.

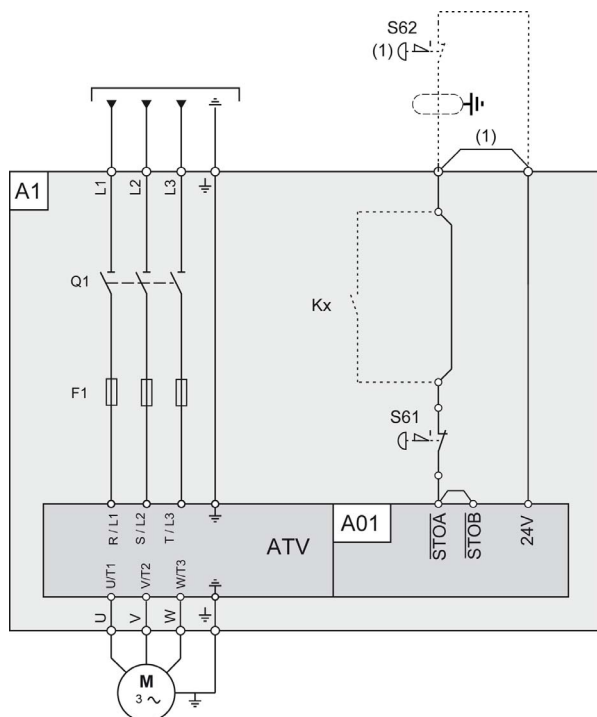
- The function "fast stop" is immediately started (undelayed) via the digital input DIx (single-channel, not monitored). Any active movement is decelerated via the adjusted ramp.
- The power stage is disabled via the inputs STO_A and STO_B of the safety STO function after the delay time set in the Emergency Stop Safety Module has elapsed. Power can no longer be supplied to the motor. If the motor has not stopped yet when the delay time has elapsed, it coasts down in an uncontrolled way (uncontrolled stop).

NOTE: The specified minimum current and the permissible maximum current of the relay outputs of the Emergency Stop Safety Module must be observed.

Process System SF - Case 7

Single Drive Systems Connection Diagram for ETO

This connection diagram applies for a single Altivar Process Drive Systems configuration, within an Engineered to Order (ETO) purchase order. The connection diagram applies according to IEC 61508 capability SIL 1, ISO 13849-1 category 1 PL c, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



Legend:

- A1: Drive Systems enclosure with certified architecture for ETO with built-in Drive Systems components assembly.
 - A01: Control block of the Drive System
 - S61: Emergency Stop button mounted in the enclosure door
- S62: External Emergency Stop button (not included within the certification)
- Kx: Optional additional contacts within the safety path (not included within the certification) These contacts have to be taken into account separately for the safety path calculation.
- (1): If S62 external emergency stop is installed, the wire link has to be removed.

