

Altivar Soft Starter ATS490

Soft Starter for Asynchronous Motors

Embedded Safety Function Manual

Original Instructions

PKR63419.01

10/2024



Legal Information

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

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

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

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

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

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

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

Table of Contents

| | |
|--|----|
| Safety Information..... | 5 |
| Qualification of Personnel | 6 |
| Intended Use..... | 6 |
| Product related information | 6 |
| About the Book..... | 11 |
| Document scope | 11 |
| Validity note | 11 |
| Related Documents | 12 |
| Terminology | 14 |
| EC Declaration of Conformity | 14 |
| Certification for functional safety | 14 |
| Contact us | 15 |
| Overview | 16 |
| Definition | 16 |
| Basics | 17 |
| Description | 21 |
| Safety Function STO (Safe Torque Off) | 21 |
| Limitations | 23 |
| Status of Safety Function | 25 |
| Technical Data..... | 26 |
| Electrical Data..... | 26 |
| Safety Function Capability..... | 27 |
| Certified Architectures..... | 28 |
| Introduction..... | 28 |
| Process System FuSa - Case 1 - Suitable for Altivar Soft Starter ATS490 offer according to IEC 61508 capability SIL1 | 30 |
| Single Soft Starter Connection Diagram..... | 30 |
| Multi Soft Starter Connection Diagram..... | 31 |
| Process System FuSa- Case 2 - Suitable for Altivar Soft Starter ATS490 offer according to ISO 13849–1 category 2 PLc IEC 62061 and IEC 60204–1 stop category 0 | 32 |
| Single Soft Starter with Safety Module Type Preventa XPSUAB or Equivalent Connection Diagram | 32 |
| Multi Soft Starters with Safety Module Type Preventa XPSUAB or Equivalent Connection Diagram | 33 |
| Process System FuSa Case 3 - Suitable for Altivar Soft Starter ATS490 offer according to ISO 13849-1 category 2 PLc, IEC 60204-1 stop category 1 and IEC 61800-5-2 SS1-A (2007) or SS1-t (2016)..... | 35 |
| Glossary | 37 |

Safety Information

Important Information

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



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



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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

Please Note

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

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

Qualification of Personnel

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

Intended Use

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

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

Product related information

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

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

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

⚡⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

Before performing work on the equipment:

- Use all required personal protective equipment (PPE).
- 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 equipment.
- Lock all power switches in the open position.
- Verify the absence of voltage using a properly rated voltage sensing device.

Before applying voltage to the equipment:

- 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.

⚡⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

- Never operate energized switch with door open.
- Turn off switch before removing or installing fuses or making load side connections.
- Do not use renewable link fuses in fused switches.

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 soft starter being just one part of the application. The soft starter 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 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 soft starter 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.
- Verify that the service life of all individual components used in your application is sufficient for the intended service life of your overall application.
- Perform extensive commissioning tests for all potential error situations to verify the effectiveness of the safety-related functions and monitoring functions implemented, for example, but not limited to, speed monitoring by means of encoders, short circuit monitoring for all connected equipment, correct operation of brakes and guards.
- Perform extensive commissioning tests for all potential error situations to verify that the load can be brought to a safe stop under all conditions.

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

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

⚠ WARNING

UNANTICIPATED EQUIPMENT OPERATION

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

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

⚠ WARNING

LOSS OF CONTROL

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

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

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

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

⚠ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

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

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

⚠ WARNING

LOSS OF CONTROL

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

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

This product meets the EMC requirements according to the standard IEC 60947-4-2. This device has been designed for environment A. Use of this product in a domestic environment (B environment) may cause unwanted radio interference.

⚠ WARNING

RADIO INTERFERENCE

- In a domestic environment (B environment), this product may cause radio interference in which case supplementary mitigation measures may be required.

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

NOTICE

DESTRUCTION DUE TO INCORRECT MAINS VOLTAGE

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

Failure to follow these instructions can result in equipment damage.

About the Book

Document scope

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

The soft starter supports the STO safety function according to the IEC 61508 standard.

Validity note

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

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.

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.se.com . |
| 2 | In the Search box type the reference of the product or the name of a product range. <ul style="list-style-type: none">• 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 . |

Related Documents

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on www.se.com The Internet site provides the information you need for products and solutions:

- The whole catalog for detailed characteristics and selection guides
- The CAD files to help design your installation, available in over 20 different file formats
- All software and firmware to maintain your installation up to date
- A large quantity of White Papers, Environment documents, Application solutions, Specifications... to gain a better understanding of our electrical systems and equipment or automation
- And finally all the User Guides related to your soft starter, listed below:

Catalog

| Title of documentation | Reference number |
|--------------------------------------|---|
| Catalog: Altivar Soft Starter ATS490 | DIA2ED2240603EN (English) DIA2ED2240603FR (French) |

Documentations

| Title of documentation | Reference number |
|--|---|
| ATS490 Getting Started | PKR63410 (English), PKR63411 (French) PKR63412 (Spanish), PKR63413 (Italian) PKR63414 (German), PKR63415 (Chinese) PKR63416 (Portuguese), PKR63417 (Turkish) |
| ATS490 Getting Started Manual Annex for UL | PKR63418 (English) |
| ATS490 User Manual | PKR52680 (English), PKR52681 (French) PKR52682 (Spanish), PKR52683 (Italian) PKR52684 (German), PKR52685 (Chinese) PKR52686 (Portuguese), PKR52687 (Turkish) |
| ATS490 Embedded Safety Function Manual | PKR63419 (English) |
| ATS490 ATEX Manual | BQT74920 (English) |
| ATS490 Embedded Modbus RTU Manual | PKR63421 (English) |
| ATS490 EtherNet Manual | PKR63423 (English) |
| ATS490 PROFIBUS DP Manual (VW3A3607) | PKR63425 (English) |
| ATS490 CANopen Manual (VW3A3608, VW3A3618, VW3A3628) | PKR63426 (English) |
| ATS490 Communication Parameter Addresses | PKR63420 (English) |
| Recommended Cybersecurity Best Practices | CS-Best-Practices-2019–340 (English) |

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

Videos

| Title of documentation | Reference number |
|------------------------------------|------------------------|
| Video: Getting Started with ATS490 | FAQ000263202 (English) |

Software

| Title of documentation | Reference number |
|------------------------|---|
| SoMove: FDT | SoMove FDT (English, French, German, Spanish, Italian, Chinese) |
| ATS490: DTM | ATS490 DTM Library EN (English – to be installed first) ATS490 DTM Lang FR (French) ATS490 DTM Lang SP (Spanish) ATS490 DTM Lang IT (Italian) ATS490 DTM Lang DE (German) ATS490 DTM Lang CN (Chinese) |

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 soft starters 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:

- 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
- IEC 60947–1 Low–Voltage Switchgear and Control Gear – General rules
- IEC 60947–4-2 Semiconductor Motor controllers, Starters and Soft Starters
- IEC 61508–1 Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61508–2 Functional safety of electrical/electronic/programmable electronic safety-related systems
 - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61508–3 Functional safety of electrical/electronic/programmable electronic safety-related systems
 - Part 3: Software requirements
- IEC 62061 Safety of machinery - Functional safety of safety-related control systems
- IEC 62443: Security for industrial automation and control systems

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.

Also see the glossary at the end of this manual.

EC Declaration of Conformity

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

Certification for functional safety

Compliance with 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-1 capability in compliance with IEC 61508 series Ed.2
- Performance Level **c** in compliance with ISO 13849–1
- *Compliant with Category 2 of International standard ISO 13849–1*

Also refer to **Safety function capability** Chapter in the ATS490 Embedded Safety Manual PKR63419.

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

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

Contact us

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

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

Overview

Definition

Safety Function In Altivar Soft Starter

Definition according to standard IEC 61800–5–2:

- **STO Safe Torque Off**: This function prevents force-producing power from being provided to the motor
- **SS1–t Safe Stop 1 type t**: Initiates the motor deceleration and performs the STO function after an application specific time delay

Notation

The graphic display terminal menus and parameters are shown in square brackets.

Example: **[Communication]**

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 International 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 EN 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.

IEC 62061 Standard

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines. It is applicable to control systems used, either singly or in combination, to carry out safety functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

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 ISO 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 |

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 | 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 | 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 - 1,000,000,000 |

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

Fault Avoidance Measures

Systematic errors in the specifications, in the hardware and the software, usage faults and maintenance faults in the safety system must be avoided to the maximum degree possible. To meet these requirements, IEC 61508 specifies a number of measures for fault avoidance that must be implemented depending on the required SIL. These measures for fault avoidance must cover the entire life cycle of the safety system, i.e. from design to decommissioning of the system.

Description

Safety Function STO (Safe Torque Off)

Overview

The safety function incorporated in ATS490 helps to prevent force-producing power from being provided to the motor.

In some cases, further safety-related systems external to the soft starter (for example a mechanical brake) may be necessary to maintain the safe condition when electrical power is removed.

The safety function STO (Safe Torque Off) does not remove electrical power from the product.

DANGER

HAZARD OF ELECTRIC SHOCK

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

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

This function brings the machine safely into a no-torque state and / or prevents it from starting accidentally. The safe torque-off (safety function STO) function can be used to effectively implement the prevention of unexpected start-up functionality, thus making stops safe by preventing the power only to the motor, while still maintaining power to the soft starter control circuits. The principles and requirements of the prevention of unexpected start-up are described in the standard NF EN ISO 14118.

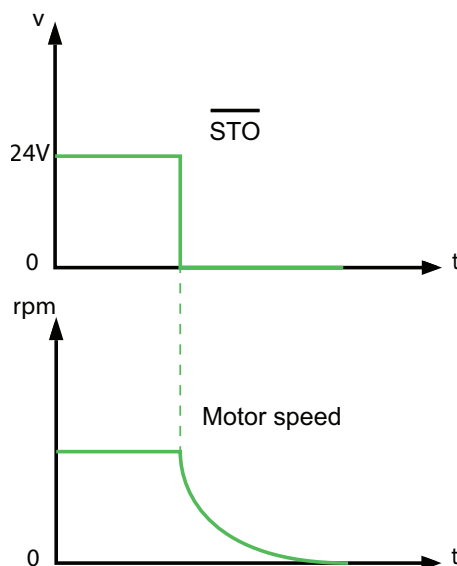
Safety integrated function provides the following benefits:

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

ATS490 is compliant with normative requirements to implement the safety function.

The logic input $\overline{\text{STO}}$ is always assigned to this function.

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



Safety Function STO Standard Reference

The safety function STO is defined in section 4.2.2.2 of standard IEC 61800-5-2:2007 and section 4.2.3.2 of standard IEC 61800-5-2:2016

Power that can cause rotation is not applied to the motor. The soft starter suitable for use in safety-related applications will not provide energy to the motor which can generate torque.

- **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.

Safe Stop 1 SS1 Standard Reference

The SS1 function is defined in section 4.2.2.2 of standard IEC 61800-5-2:2007 and 4.2.3.3 of standard IEC 61800-5-2 : 2016 Safe Stop 1 time controlled

SS1-A (version 2007) or **t** (version 2016) Initiates the motor deceleration and performs the STO function after an application specific time delay.

Safety Function Level Capability for Safety Function STO

| Configuration | SIL Safety Integrity Level according to IEC 61508 | PL Performance Level according to ISO-13849-1 |
|---|---|---|
| STO with and without Safety module (such as Preventa module) | SIL1 | PL c |

Emergency Operations

Standard IEC 60204-1 introduces 2 emergency operations:

- **Emergency switching-off:**

This function requires external switching components, and cannot be accomplished with soft starter 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 as a stop category 0.

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).

Limitations

ISO 13849–1 category 2 PLc IEC 62061 and IEC 60204–1

An additional safety module (such as the Preventa module) is required to maintain these certifications.

IEC 61508 capability SIL1

If the use of an additional safety module is not possible, the soft starter control must be configured in:

- 2 wires transition ([**2/3-Wire Control**] set to [**2-Wire Control**] and [**2-wire type**] set to [**Transition**]).
- 3 wires ([**2/3-Wire Control**] set to [**3-Wire Control**]).

Type Of Motor

The safety function STO can be used with all motors supported by soft starter.

Type Of Wiring

The safety function STO is not compatible with **[Inside Delta]** **DLT** function.

If the safety function STO is enabled while **[Inside Delta]** **DLT** function is set to **[Yes]**, the soft starter will trigger the **[STO On Inside Delta]** **DLTF** error.

WARNING

INEFFECTIVE SAFETY FUNCTION

- Never use the safety function STO when the function **[Inside Delta]** **DLT** is activated.
- Always consider that enabling the safety function STO when the **[Inside Delta]** **DLT** function is set to **[Yes]** does not provide any Safety Integrity Level (SIL), Performance Level (PL), or any other capacity related to the safety of your machine or process.

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

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 soft starter 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.
- **[Phase Loss Monit]** **PHP** should be set to **[Yes]** for correct operation. Refer to the ATS490 User Manual PKR52680 (Chapter "Phase Loss") for additional information.

Maximum Operation Altitude

The maximum operating altitude for the ATS490 safety function is 2000 m above sea level.

Error Code Description

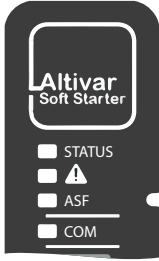
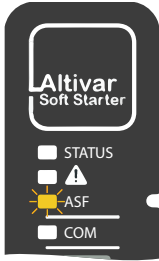
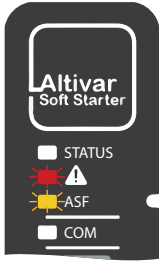
When an error is detected by the safety function, the soft starter displays **[Safety Function Error]** **SAFF**. This detected error can only be reset after powering the soft starter OFF/ON once the root cause is cleared.

Disable Error Detection

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

Status of Safety Function

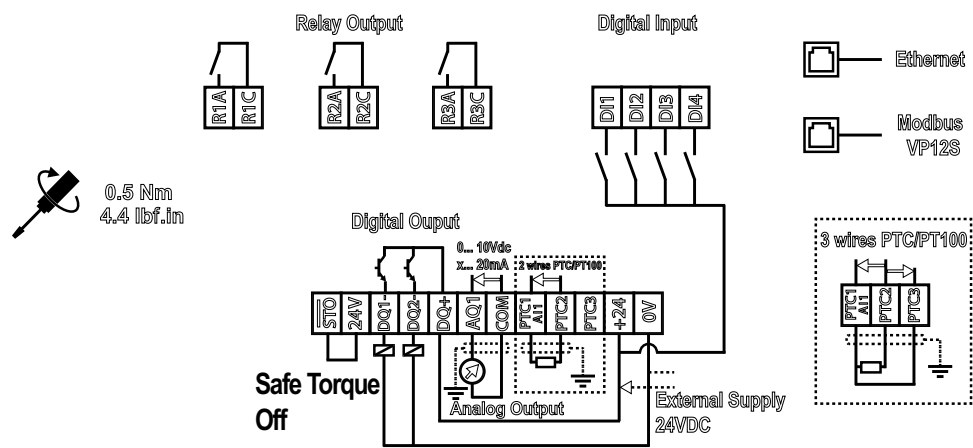
Description

| If... | Then ... | |
|--|---|--|
| Safe Torque Off (STO) is not active | <ul style="list-style-type: none"> the orange LED is OFF |  |
| STO is triggered | <ul style="list-style-type: none"> the power stage is open by safety channel the orange LED is steady ON STO is displayed on the Graphic Display Terminal |  |
| [Safety Function Error] SAFF detected fault occurs | <ul style="list-style-type: none"> the power stage is open the orange LED is steady ON the red LED is steady ON the Graphic Display terminal displays SAFF |  |

Technical Data

Electrical Data

Cabling Label



Input Signal Safety Function

| Input Signals Safety Function | Units | Value for \overline{STO} |
|---------------------------------------|----------|----------------------------|
| Logic 0 (Ulow) | Vdc | < 5 or open |
| Logic 1 (Uhigh) | Vdc | > 11 |
| Current (at 19 Vdc) | mA | 10 |
| Debounce time (*) | ms | 1 |
| Response time of safety function (**) | ms | < 50 |
| Maximum wire length (***) | m (ft) | 30 (98.43) |
| Maximum wire resistance | Ω | < 100 |

(*) A pulse shorter than “Debounce time” will be ignored.

(**) Time between STO activation and the moment when the motor no longer has torque.

(***) The maximum wire length between the safety-related input and a sensor/device for a cable cross section equal to 1.5 mm² / AWG17.

Safety Function Capability

Machine Application Function Configuration

| Standard | STO |
|---------------------------|-----------------|
| IEC 61800-5-2 / IEC 61508 | SIL1 |
| IEC 62061 (1) | SIL1 CL |
| ISO 13849-1 (2) | Category 2 PLc |
| 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 SIL1) from components which constitute the safety function (ATS490 is one component which is classified SIL1 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 XPSUAB or equivalent must be used.

Summary Of The Reliability Study

| Safety Standards | Parameter | ATS490D17Y...C11Y | ATS490C14Y...C17Y | ATS490C21Y...C41Y | ATS490C48Y...M12Y |
|------------------|-------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| | Safety function | STO | STO | STO | STO |
| | PST | 6050ms | 6050ms | 6050ms | 6050ms |
| IEC 61508 | HFT | 0 | 0 | 0 | 0 |
| | Type | B | B | B | B |
| | PFH | 3×10^{-7} | 3×10^{-7} | 3×10^{-7} | 3×10^{-7} |
| | PTI | 1 year | 1 year | 1 year | 1 year |
| | PFDavg | 3×10^{-3} | 4×10^{-3} | 3×10^{-3} | 3×10^{-3} |
| | SIL | 1 | 1 | 1 | 1 |
| IEC 62061 | SIL capability | 1 | 1 | 1 | 1 |
| ISO 13849 | MTTFd | > 30 years | > 30 years | > 30 years | > 30 years |
| | Category | 2 | 2 | 2 | 2 |
| | Performance Level | c | c | c | c |
| | Lifetime | 10 years | 10 years | 10 years | 10 years |
| | Hypothesis | 87600 nop/year B10d: 500000 | 87600 nop/year B10d: 418684 | 52560 nop/year B10d: 340174 | 52560 nop/year B10d: 340174 |

Preventive annual activation of the safety function is recommended but mandatory for safety machine systems only.

For the machine environment, a safety module type Preventa XPSU or equivalent is required for the STO function.

NOTE: The table above is not sufficient to evaluate the PL of a safety-related system. 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.

NOTE: The reliability of the SS1-t function required to add the values of this table to the Preventa reliability table values.

Certified Architectures

Introduction

Certified Architectures

NOTE: For certification relating to functional aspects, only the safety related function of the soft starter will be considered, not the complete system into which it is integrated to help to ensure the functional safety of a machine or a system/process.

These are the certified architectures:

- Case 1 - Suitable for Altivar Soft Starter according to IEC 61508 capability SIL1, IEC 60204–1 stop category 0
- Case 2 - Suitable for Altivar Soft Starter according to ISO 13849–1 category 2 PLc IEC 62061 and IEC 60204–1 stop category 0
- Case 3 - Suitable for Altivar Soft Starter according to ISO 13849-1 category 2 PLc, IEC 60204-1 stop category 1 and IEC 61800-5-2 SS1-A (2007) or SS1-t (2016).

The safety function of the soft starter 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 soft starter is responsible for these additional changes.

Also, the output data generated by the use of the safety function (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 1 input. This circuit has to be wired according to protective cable insulation.

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

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

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

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

Power Supply Unit

DANGER

ELECTRIC SHOCK CAUSED BY INCORRECT POWER SUPPLY UNIT

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

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

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

Acceptance Test

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

Ambient Conditions

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

Please refer to the ATS490 User Manual PKR52680.

External Forces

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

⚠ WARNING

INSUFFICIENT DECELERATION OR UNINTENDED EQUIPMENT OPERATION

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

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

Degree of Protection When the Safety Function Is Used

⚠ WARNING

LOSS OF SAFETY FUNCTION CAUSED BY FOREIGN OBJECTS

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

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

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

Customer Care Center

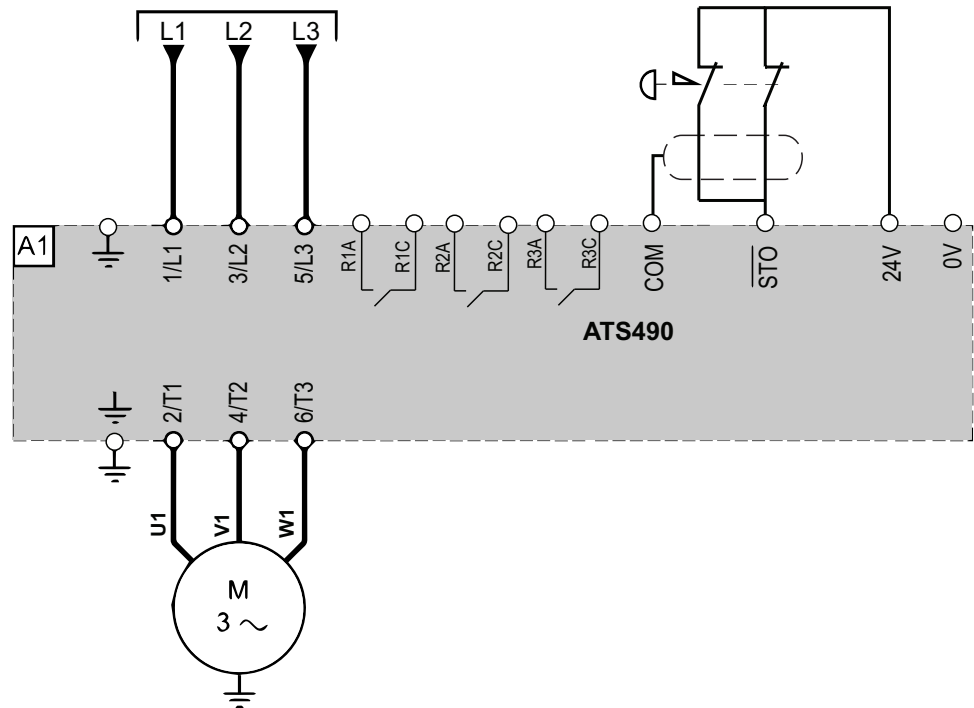
For additional support, you can contact our Customer Care Center on:

www.se.com/CCC.

Process System FuSa - Case 1 - Suitable for Altivar Soft Starter ATS490 offer according to IEC 61508 capability SIL1

Single Soft Starter Connection Diagram

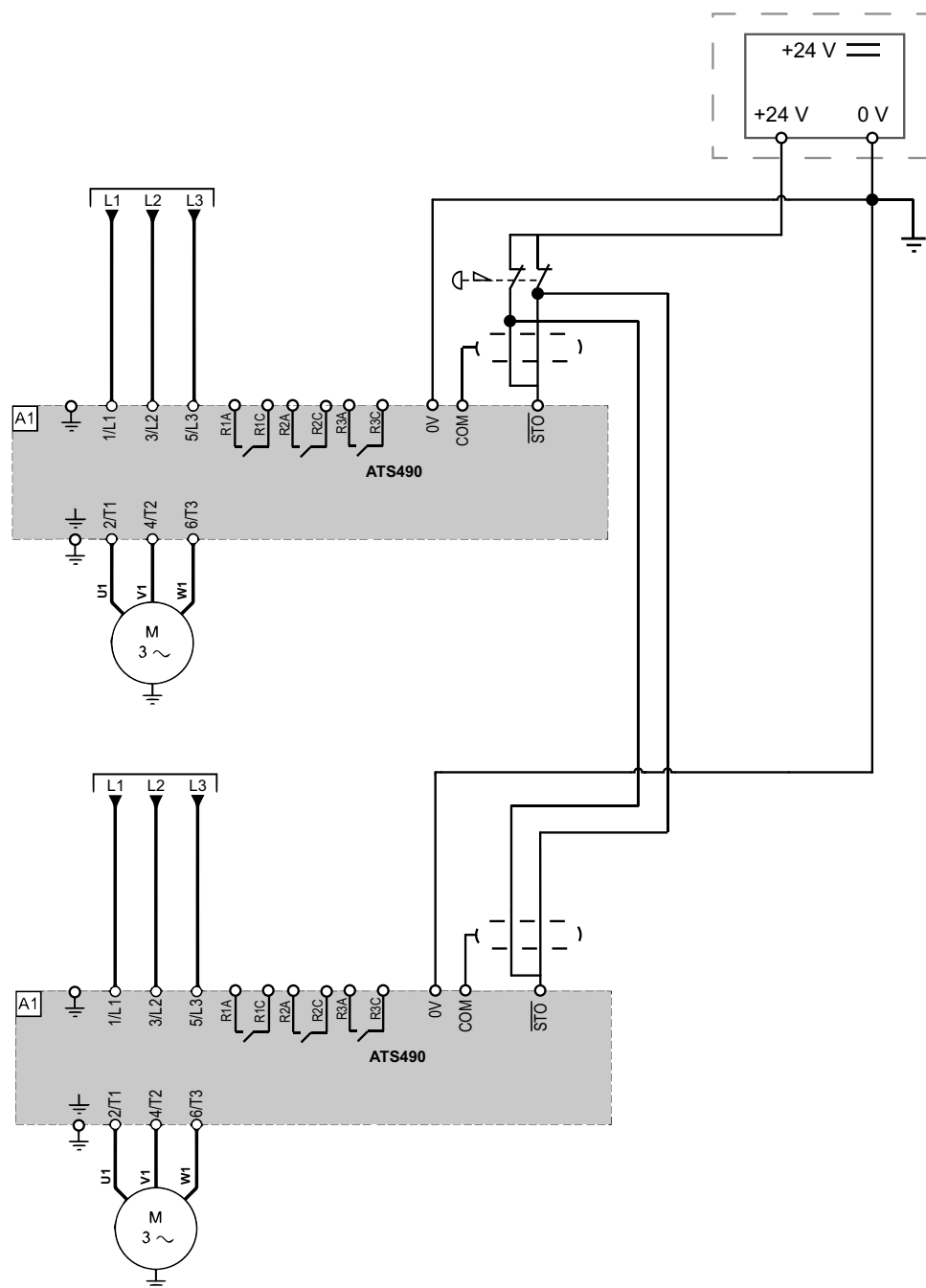
This connection diagram applies for a single soft starter configuration according to IEC 61508 capability SIL1.



Multi Soft Starter Connection Diagram

This connection diagram applies for multi soft starter configuration according to IEC 61508 capability SIL1.

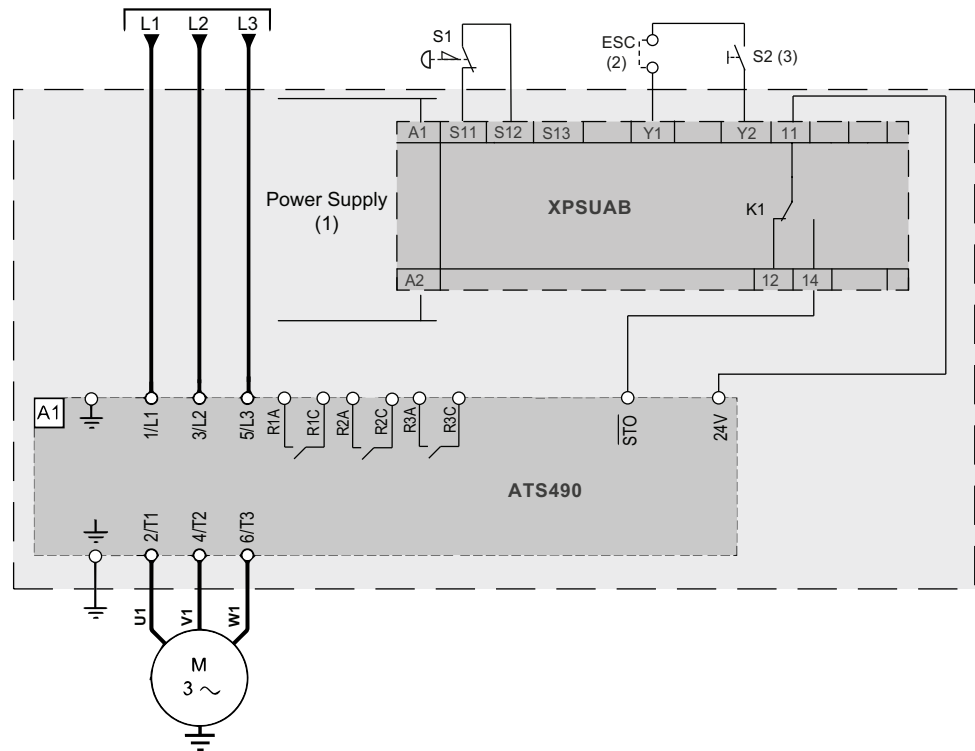
NOTE: The +24VDC power supply must meet the requirements of IEC 61131-2 (PELV standard power supply unit).



Process System FuSa- Case 2 - Suitable for Altivar Soft Starter ATS490 offer according to ISO 13849–1 category 2 PLc IEC 62061 and IEC 60204–1 stop category 0

Single Soft Starter with Safety Module Type Preventa XPSUAB or Equivalent Connection Diagram

This connection diagram applies for a single soft starter configuration with the safety module type Preventa XPSUAB or equivalent according to ISO 13849-1 category 2 PLc, IEC 62061 and 60204-1 stop category 0.



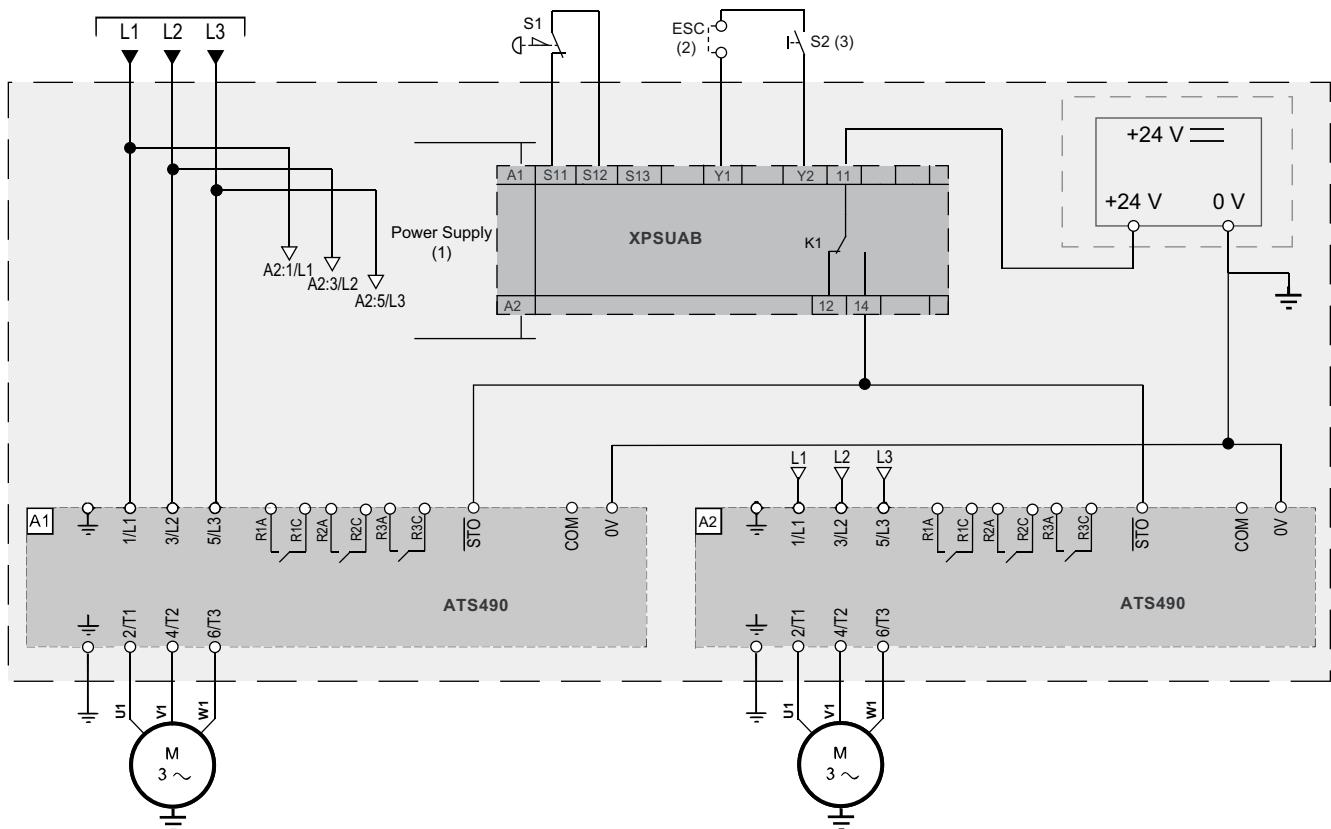
1. Refer to the XPSUAB Safety Module User Manual EIO0000003454 for more information on the power supply.
2. External Start Condition **ESC** is used to add external starting conditions.
3. On power-up or after an emergency stop, rearm the XPSUAB safety module using push-button S2.

Multi Soft Starters with Safety Module Type Preventa XPSUAB or Equivalent Connection Diagram

This connection diagram applies for a multi soft starter configuration with the safety module type Preventa XPSUAB or equivalent according to ISO 13849-1 category 2 PLc, IEC 62061 and 60204-1 stop category 0.

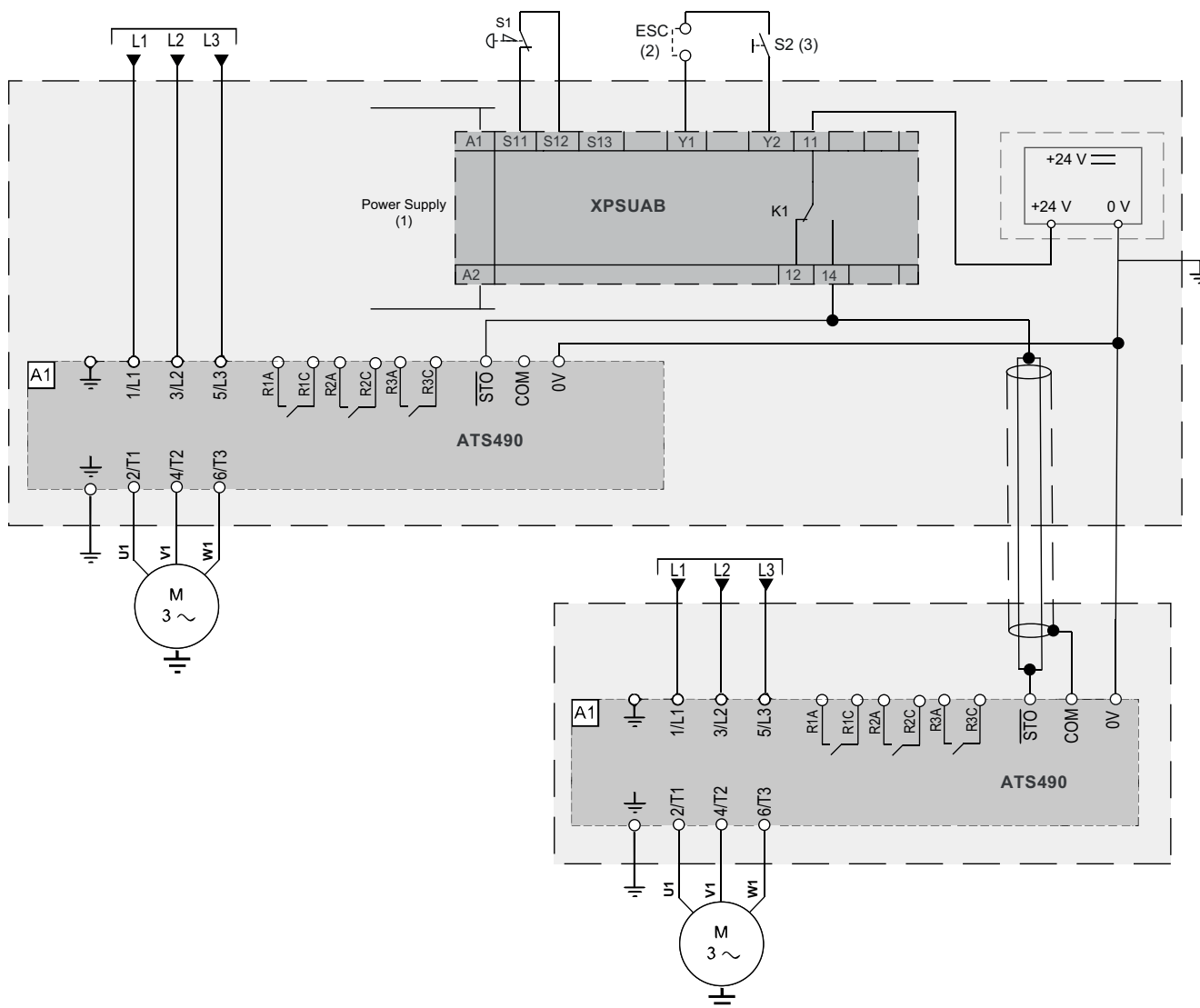
NOTE: The +24 Vdc power supply must meet the requirements of IEC 61131-2 (PELV standard power supply unit).

Multi Soft Starters with Safety Module in the same enclosure



- Refer to the XPSUAB Safety Module User Manual EIO0000003454 for more information on the power supply.
- External Start Condition **ESC** is used to add external starting conditions.
- On power-up or after an emergency stop, rearm the XPSUAB safety module using push-button S2.

Multi Soft Starters with Safety Module in separate enclosures

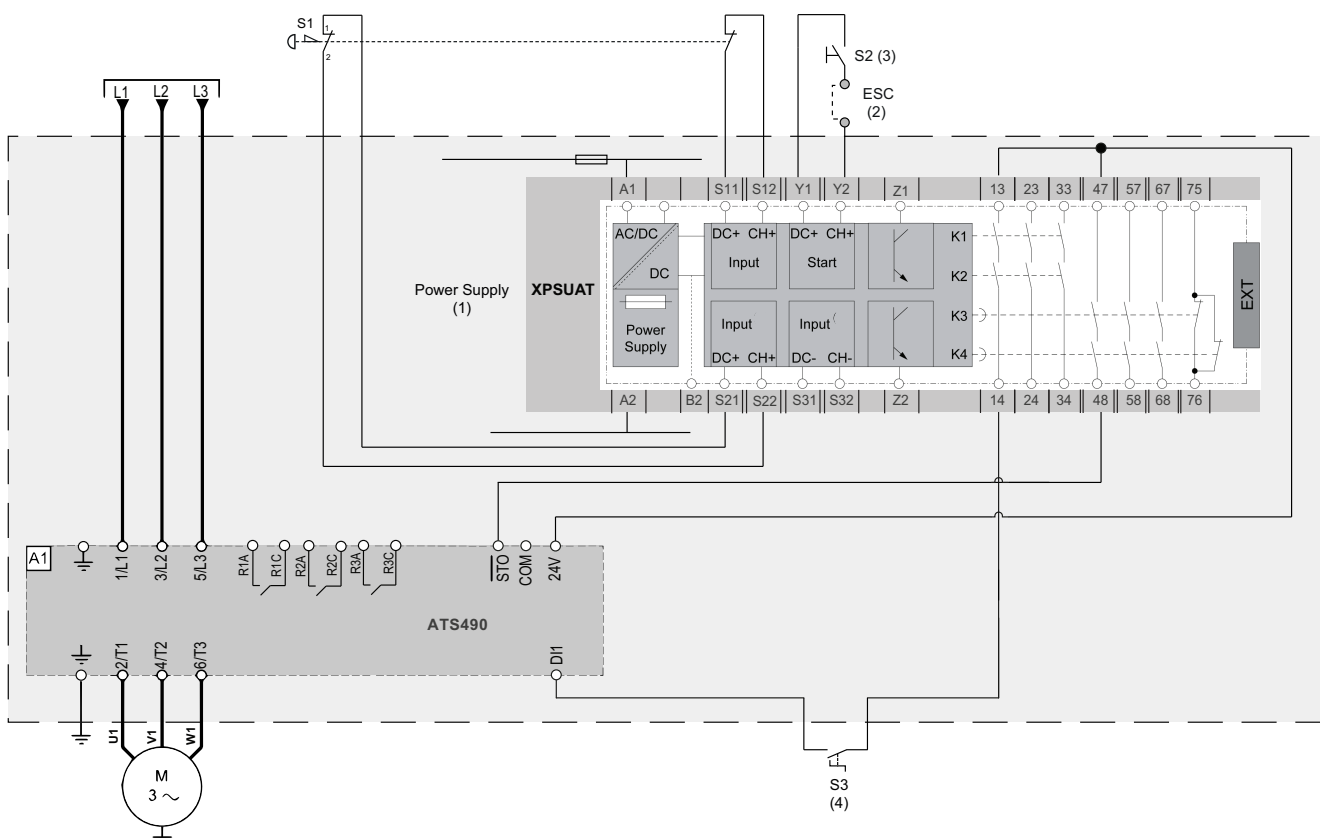


1. Refer to the XPSUAB Safety Module User Manual EIO0000003454 for more information on the power supply.
2. External Start Condition **ESC** is used to add external starting conditions.
3. On power-up or after an emergency stop, rearm the XPSUAB safety module using push-button S2.

Process System FuSa Case 3 - Suitable for Altivar Soft Starter ATS490 offer according to ISO 13849-1 category 2 PLc, IEC 60204-1 stop category 1 and IEC 61800-5-2 SS1-A (2007) or SS1-t (2016)

Connection Diagram For Single Soft Starter with Safety Module Type Preventa XPSUAT or Equivalent

This Connection diagram applies for a single soft starter configuration with the Safety Module Type Preventa XPSUAT or equivalent, according to ISO 13849-1 category 2 PLc, IEC 60204-1 stop category 1 and IEC 61800-5-2 SS1-A (2007) or SS1-t (2016).



NOTE: This diagram cannot be used with display terminal or fieldbus configuration.

1. Refer to the XPSUAT Safety Module User Manual EIO0000003443 for more information on the power supply.
2. External Start Condition **ESC** is used to add external starting conditions.
3. On power-up or after an emergency stop, re-arm the XPSUAT safety module using push-button S2.
4. This diagram is a wiring configuration using 2 wires control by transition:
 - a. **[2/3-Wire Control]** set to **[2-Wire Control]**
 - b. **[2-wire type]** set to **[Transition]**

NOTE: In 3 wire command (**[2/3-Wire Control]** set to **[3-Wire Control]**), S3 become a push button normally closed to apply **STOP command**. For more information, refer to the chapter *RUN and STOP Management* in the user manual.

NOTE: This wiring diagram is not compatible in:

- **[Hardwired ctrl mode]**
- **[2-Wire Control]** when **[2-wire type]** is set to **[Level]**.

Glossary

A

ASF:

Angle Safety Fault

B

B10d:

Number of cycles until 10% of bypass relays have failed dangerously (IEC 61810-2-1)

H

HFT:

(Hardware Fault Tolerance) A hardware fault tolerance of N means that N + 1 faults could cause a loss of the Safety Function, for instance :

- HFT = 0: The 1st failure could cause a loss of the Safety Function
- HFT = 1: 2 faults in combination could cause a loss of the Safety Function. (There are 2 different paths to go to a Safe state. Loss of the Safety Function means that a Safe state cannot be entered. (IEC 61508)

M

MTTFd:

Mean Time To Failure dangerous

N

nop/year:

Number of operations by year

P

PELV:

(Protective Extra-Low Voltage) Electric system in which the voltage cannot exceed the value of extra low voltage

PFD:

Probability of Failure on Demand

PFH:

Probability of Failure by Hour

PST:

(Process Safety Time) The process safety time is defined as the period of time between a failure occurring in EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed. (IEC 61508)

PTI:

(Proof Test Interval) Periodic test performed to detect failures in a safety-related system

S

SFF:

Safe Failure Fraction

T

Type A / Type B:

An element can be regarded as type A if, the failure modes of all constituent components are well defined; and the behavior of the element under fault conditions can be completely determined (example: passive components)

An element shall be regarded as type B if, the failure mode of at least one constituent component is not well defined, or the behavior of the element under fault conditions cannot be completely determined. (example : microcontroller)

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

© 2024 – 2024 Schneider Electric. All rights reserved.

PKR63419.01