TOSHIBA

E6582067⑥

Industrial Inverter

(For 3-phase motors)

TOSVERT™ VF-AS3

VF-AS3 Safety function manual

"Original instructions"

Toshiba Industrial Products and Systems Corporation

NOTICE

1. Read this manual before installing or operating the inverter. Keep it in a safe place for reference.
2. All information contained in this manual will be changed without notice.

JYT28332-01

- Contents -

Important information 1

I. Safety Information 2

II. About the book 7

1. Before you begin 8
1.1 Safety instructions 8
1.2 Qualification of personnel and use 9

2. Overview 10
2.1 Introduction 10
2.2 Standards and Terminology 10
2.3 Basics 11

3. Description 13
3.1 Safety Function STO (Safe Torque Off) 13
3.2 Limitations 14
3.3 Status of Safety Function 15

4. Technical Data 16
4.1 Electrical Data 16
4.2 Safety Function Capability 17

5. Certified Architectures 19
5.1 Introduction 19
5.2 Process System SF – Case 1 19
5.3 Process System SF – Case 2 21
5.4 Process System SF – Case 3 24

6. Services and maintenance 25
6.1 Maintenance 25

Important information

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 Manufacture nor any of sales or distributors 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.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission.

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 Toshiba 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.

I. Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, 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 Toshiba 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 and asynchronous motors and intended for industrial use according to this manual. The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data. 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. Do not touch. Use only electrically insulated tools.
- 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.
  - Place a **Do Not Turn On** label on all power switches.
  - Lock all power switches in the open position.
  - Wait 15 minutes to allow the DC bus capacitors to discharge. The DC bus LED is not an indicator of the absence of DC bus voltage that can exceed 800 Vdc (1400 Vdc for 500V, 600V(575V), 690V class).
    Measure the voltage on the DC bus between the DC bus terminals (PA/+, PC/-) using a properly rated voltmeter to verify that the voltage is <42 Vdc.
  - If the DC bus capacitors do not discharge properly, contact your Toshiba distributor. Do not repair or operate the product.
- Install and close all covers before applying voltage.

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

⚠ WARNING

UNEXPECTED MOVEMENT

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

- 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 Toshiba 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 metal surfaces of the product may exceed 100 °C (212 °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 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.

II. About the book

At a Glance

Document Scope

The purpose of this document is to provide information about the safety function incorporated in VF-AS3 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 VF-AS3 drives described in the Installation manual.

Related Documents

Title of Documentation	Reference Number
VF-AS3 Instruction manual (Standard model)	E6582062
VF-AS3 Instruction manual (Totally enclosed box type)	E6582162
VF-AS3 Instruction manual (500V, 600V(575V), 690V class)	E6582371
VF-AS3 Instruction manual (Japanese model)	E6582388

1. Before you begin

1.1 Safety instructions

The information provided in this manual supplements the product manuals.
Carefully read the product manuals before using the product.
Read and understand these instructions before performing any procedure with this drive.

■ HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

⚠ WARNING	
Prohibited	• Many parts of this drive, including the printed circuit boards, operate at the line voltage. DO NOT TOUCH. Use only electrically insulated tools. Failure to follow this instruction will result in death or serious injury. • DO NOT touch unshielded components or terminal strip screw connections with voltage present. Failure to follow this instruction will result in death or serious injury. • DO NOT short across terminals PA/+ and PC/– or across the DC bus capacitors. Failure to follow this instruction will result in death or serious injury.
Mandatory action	• Read and understand this manual before installing or operating the drive. Installation, adjustment, repair, and maintenance must be performed by qualified personnel. Failure to follow this instruction will result in death or serious injury. • The user is responsible for compliance with all international and national electrical code requirements with respect to grounding of all equipment. Failure to follow this instruction will result in death or serious injury. • Before servicing the drive: - Disconnect all power, including external control power that may be present. - Place a “DO NOT TURN ON” label on all power disconnects. - Lock all power disconnects in the open position. - WAIT 15 MINUTES to allow the DC bus capacitors to discharge. - Measure the voltage of the DC bus between the PA/+ and PC/- terminals to ensure that the voltage is less than 42 Vdc. - If the DC bus capacitors do not discharge completely, contact your Toshiba distributor. Do not repair or operate the drive. Failure to follow this instruction will result in death or serious injury. • Install and close all covers before applying power or starting and stopping the drive. Failure to follow this instruction will result in death or serious injury.

■ UNINTENDED EQUIPMENT OPERATION

⚠ WARNING	
Mandatory action	• Read and understand this manual before installing or operating the drive. Failure to follow this instruction will result in death or serious injury. • Any changes made to the parameter settings must be performed by qualified personnel. Failure to follow this instruction will result in death or serious injury.

■ **DAMAGED DRIVE EQUIPMENT**

⚠ WARNING	
Prohibited	• Do not operate or install any drive or drive accessory that appears damaged. Failure to follow this instruction can result in death, serious injury, or equipment damage.

■ **LOSS OF CONTROL**

⚠ WARNING	
Mandatory action	• The designer of any wiring scheme must consider the potential failure modes of control channels and, for certain critical control functions, provide a means to achieve a safe state during and after a channel failure. Examples of critical control functions are emergency stop and overtravel stop. Failure to follow this instruction can result in death, serious injury, or equipment damage. • Separate or redundant control channels must be provided for critical control functions. Failure to follow this instruction can result in death, serious injury, or equipment damage. • Each implementation of a control system must be individually and thoroughly tested for proper operation before being placed into service. Failure to follow this instruction can result in death, serious injury, or equipment damage. • System control channels may include links carried out by the communication. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. Failure to follow this instruction can result in death, serious injury, or equipment damage.

■ **INCOMPATIBLE LINE VOLTAGE**

⚠ CAUTION	
Mandatory action	• Before turning on and configuring the drive, ensure that the line voltage is compatible with the supply voltage range shown on the drive nameplate. The drive may be damaged if the line voltage is not compatible. Failure to follow this instruction can result in injury or equipment damage.

1.2 Qualification of personnel and use

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

The functions described in this manual are only intended for use with the basic product; you must read and understand the appropriate product manual.
The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data.
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).

Operate the product only with the specified cables and accessories. Use only genuine accessories and spare parts.
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.
The product must NEVER be operated in explosive atmospheres (hazardous locations, Ex areas).

2. Overview

2.1 Introduction

The safety function incorporated in VF-AS3, allow you to develop applications oriented in the protection of man and machine.
Safety integrated functions provides the following benefits:
- Additional standards-compliant safety functions
- Replacement of external safety equipment
- Reduced wiring efforts and space requirements
- Reduced costs

The VF-AS3 drives are compliant with normative requirements to implement the safety function.

Safety function as per IEC 61800-5-2

STO	Safe Torque Off The function purpose is to bring the motor into a no torque condition so it is relevant in terms of safety since no torque is available at the motor level. Power modules are inhibited and the motor coasts down or prohibits the motor from starting.

2.2 Standards and Terminology

Standards and 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
- EN 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.

EU Declaration of Conformity

The EU Declaration of Conformity for the EMC Directive can be obtained in CD-ROM (E6582090) or attached sheets.

Certification for functional safety

The integrated safety function is compatible and certified following IEC 61800-5-2 Ed.2 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 and 4 of European standard ISO 13849-1

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

2.3 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.

SIL Safety Integrity Level	Probability of a dangerous Failure per Hour (PFH) at high demand or continuous demand
4	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-6} \ldots < 10^{-5}$

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

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.

3. Description

3.1 Safety Function STO (Safe Torque Off)

Overview

⚠ ⚠ DANGER

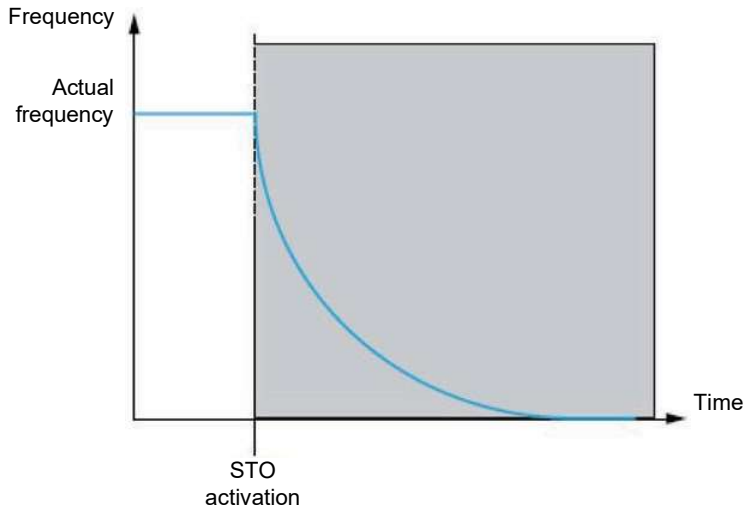
ELECTRIC SHOCK CAUSED BY INCORRECT USE

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 ($\overline{STOA}$ and $\overline{STOB}$) are always assigned to this function.
The safety function STO status can be displayed using the operation panel of the drive or using the commissioning software.



Motor speed - (2) Actual frequency - (3) $\overline{STOA}$ and $\overline{STOB}$ - STO Activation - (4) Time
NOTE: If delay between STOA and STOB is greater than 1 s, the safety function STO is triggered and an error is triggered with the error code **[STO circuit fault] PrF**.

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 61508	PL Performance Level according to ISO-13849
STO with and without Safety module (such as Preventa module)	SIL3	PLe

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 or 3 wires.

3.2 Limitations

Type Of Motor

The safety function STO can be used with synchronous and asynchronous motors.

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.

3.3 Status of Safety Function

Description

If...	Then ...
Safe Torque Off (STO) is not active	ASF yellow LED is OFF
STO is triggered	the power bridge is locked by redundant hardware STO is displayed
[STO circuit fault] detected fault occurs (1)	the power bridge is locked the red LCD is steady ON the Graphic Display terminal displays **PrF**
(1)Possible causes are exceeded delay between $\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ signals > 1 s and internal hardware detected error.	

4. Technical Data

4.1 Electrical Data

Electrical Data

Logic Type

Safety function must only be used in **Source logic**: current flows to input.
$\overline{\text{STOA}}$ and $\overline{\text{STOB}}$ inputs and signal inputs are protected against reverse polarity.

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

4.2 Safety Function Capability

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 (default relay activation, relay of brake logic command, errors 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)	SIL CL 3
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 (VF-AS3 is one component which is classified SIL CL 3). (2) According to table 4 of EN 13849-1 (2008). (3) If protection against supply interruption or voltage reduction and subsequent restoration is needed according to IEC 60204-1, a safety module type Preventa XPS AF or equivalent must be used.	

Process Application Function Configuration

Standard	STO
IEC 61800-5-2 / IEC 61508	SIL3
IEC 62061	SIL CL 3

Summary Of The Reliability Study

Standard	Input	VF-AS3
IEC 61508 Ed.2	SFF	91.5%
	PFH in /h	4.10^{-10}
	PFDavg	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.

5. Certified Architectures

5.1 Introduction

Introduction

Certified Architectures

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

These are the certified architectures:

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

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

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

Also, the output data generated by the use of safety functions (default relay activation, relay of brake logic command, errors 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.

Wire both STO inputs only with the shielded, twisted cables with a pitch of 25...50 mm (1 in. and 2 in.), connecting the shielding to Ground at each end se shielded cables for the signal lines.

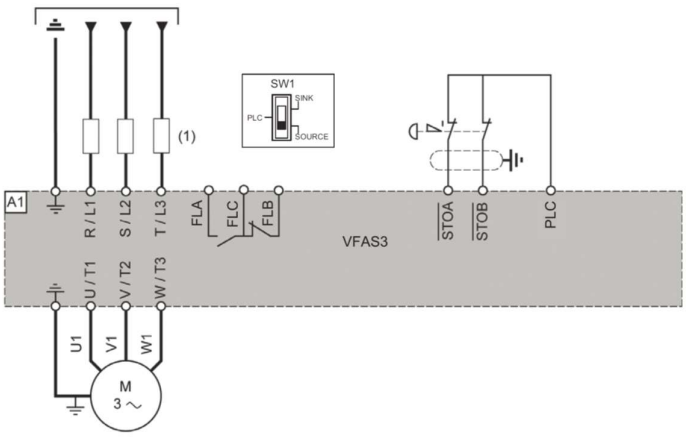
Ground loops may cause problems in machines. In this case the shield has to be connected to ground on drive side only.

5.2 Process System SF – Case 1

Process System SF - Case 1

Single Drive Connection Diagram

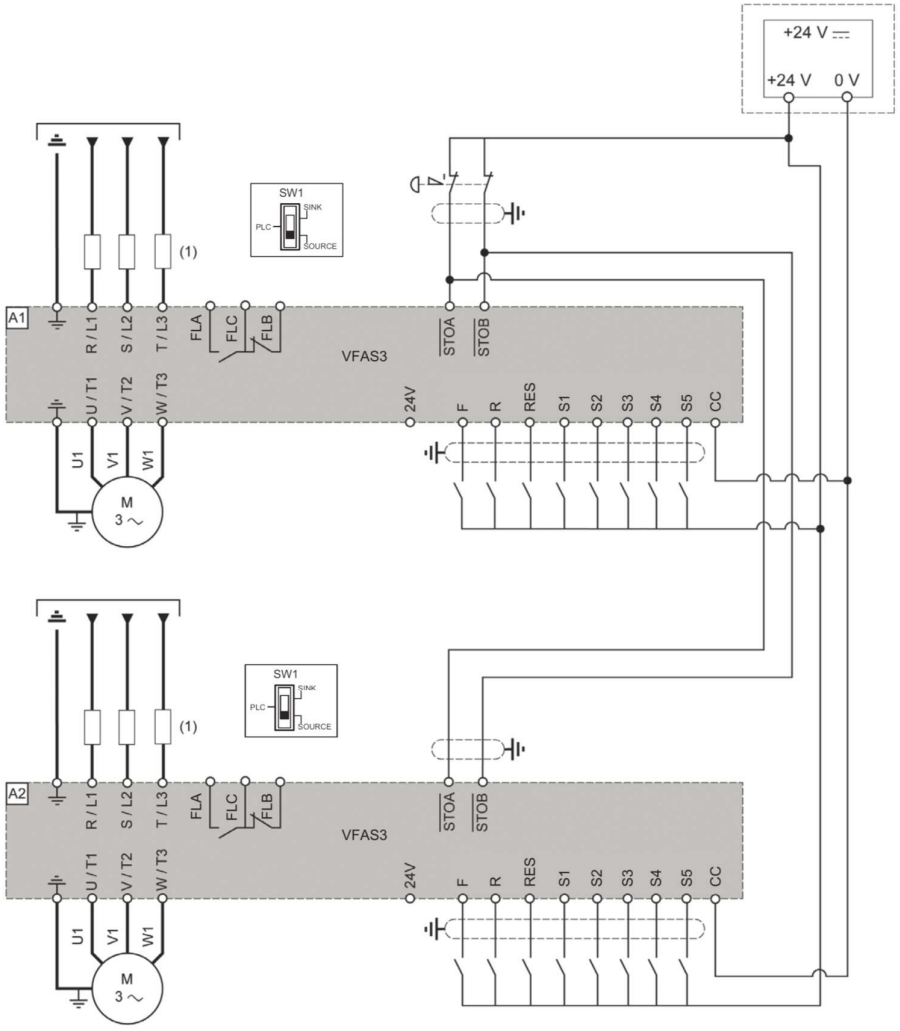
This connection diagram applies for a single drive configuration according to IEC 61508 capability SIL3, IEC 60204-1 stop category 0 without protection against supply interruption or voltage reduction and subsequent rotation.



(1) Line chokes, if used.

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.



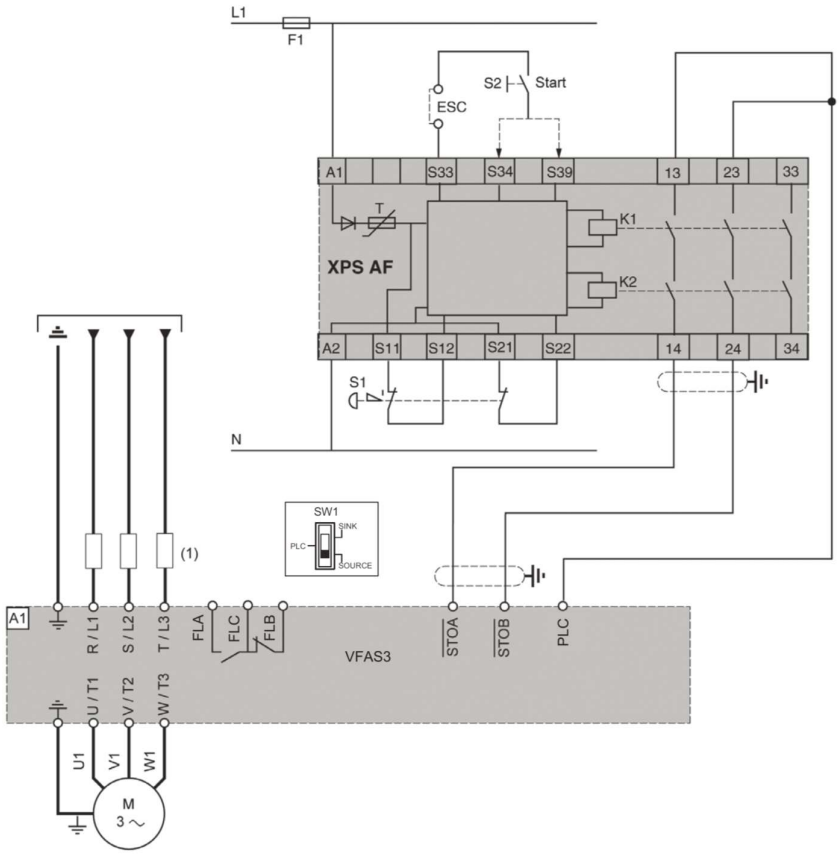
(1) Line chokes, if used.

5.3 Process System SF – Case 2

Process System SF - Case 2

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

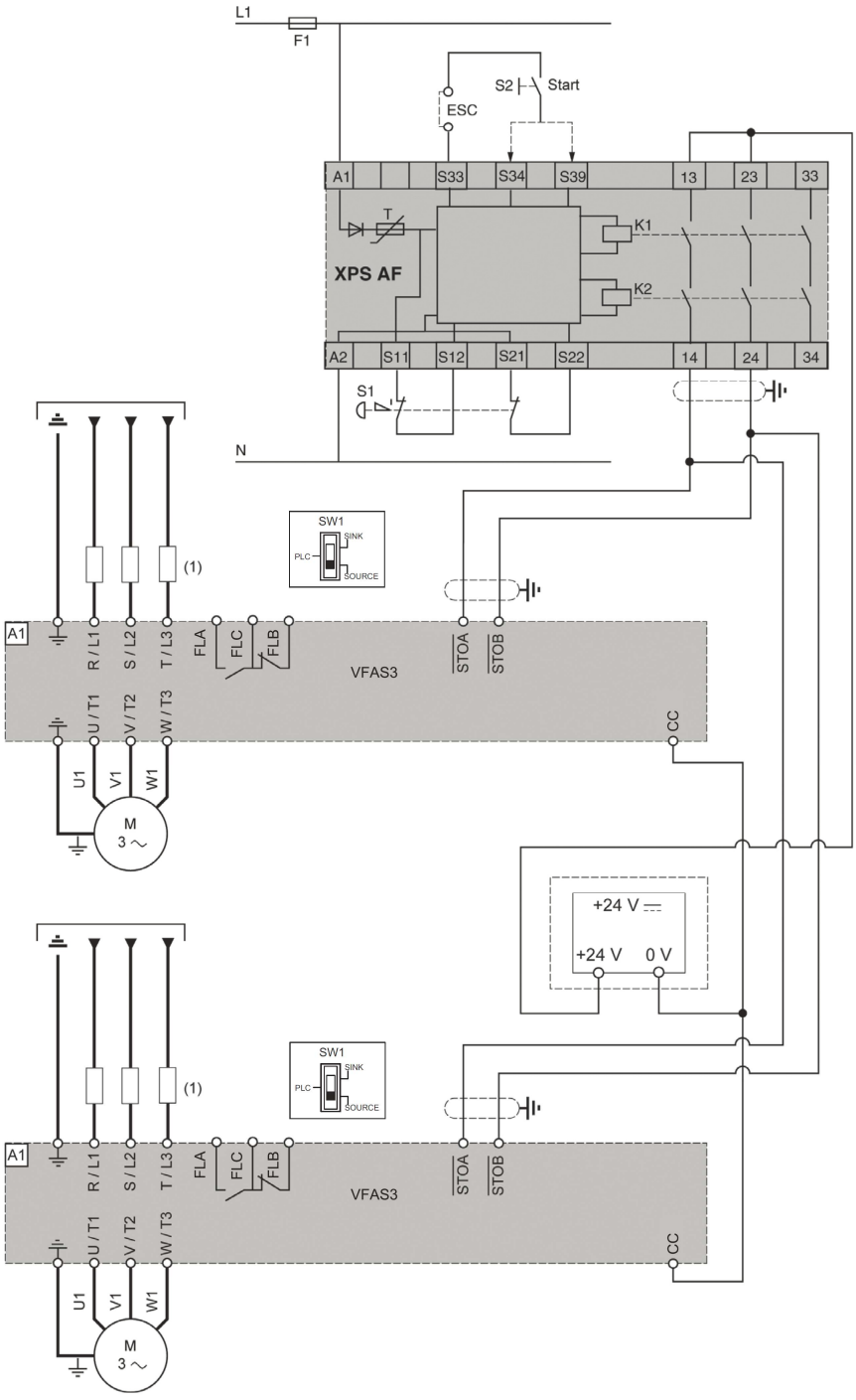
This connection diagram applies for a single drive configuration with the safety module type Preventa XPS- AF according to ISO 13849-1 category 3 PLe, IEC 62061 and 60204-1 stop category 0.



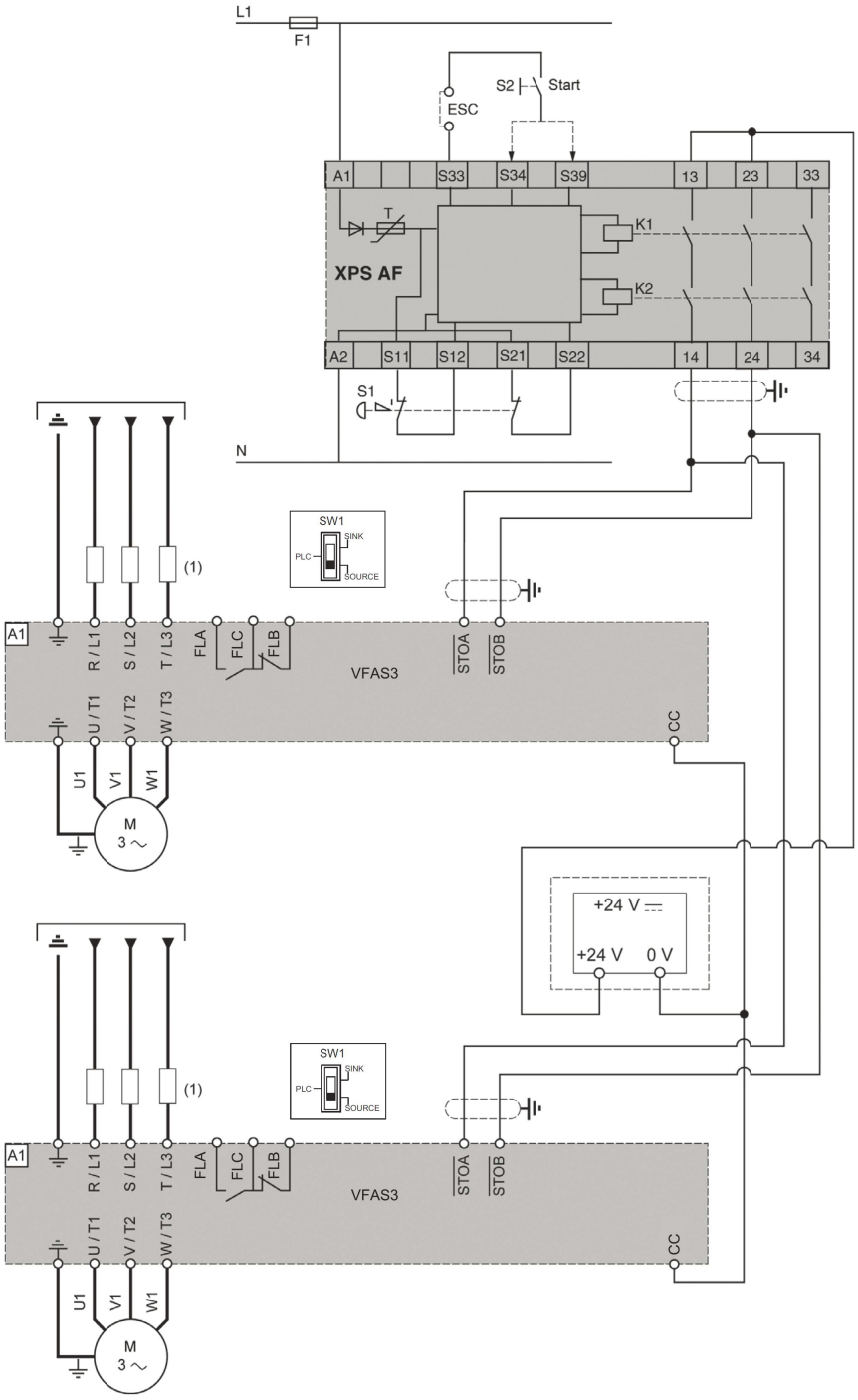
(1) Line chokes, if used.

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.



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.



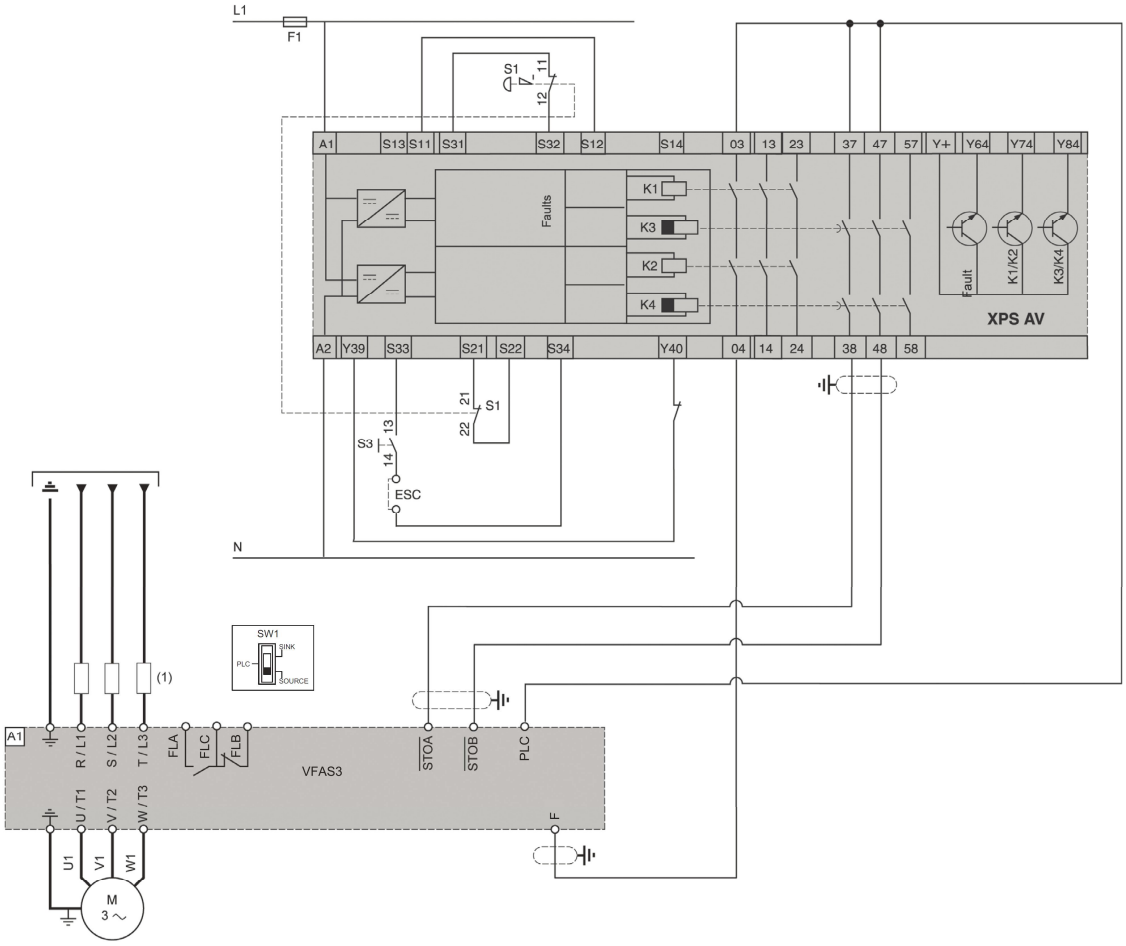
(1) Line chokes, if used.

5.4 Process System SF – Case 3

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 an wiring configuration using [F] assigned to forward operation.
(1) Line chokes, if used.

6. Services and maintenance

6.1 Maintenance

For more product information, see the instruction manual of VF-AS3.

Preventive maintenance

It is recommended to check each year the safety functions.
Example: Open the protective door to see if the drive stops in accordance with the safety function configured.

Changing equipment of the machine

Note: If you need to change any part of the machine out of VF-AS3 (Motor, Emergency stop …) you must redo the Acceptance test.

©Toshiba Schneider Inverter Corporation 2016