

Altivar 320

Variable Speed Drives

Safety Functions Manual

04/2019



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

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

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

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

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

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

© 2019 Schneider Electric. All rights reserved.

Table of Contents



Safety Information	5
About the Book	11
Chapter 1 General Information	15
Introduction	16
Certifications	18
Basics	19
Chapter 2 Description	23
Safety Function STO (Safe Torque Off)	24
Safety Function SS1 (Safe Stop 1)	26
Safety Function SLS (Safely-Limited Speed)	28
Safety Function SMS (Safe Maximum Speed)	35
Safety Function GDL (Guard Door Locking)	37
Chapter 3 Calculation of Safety Related Parameters	39
SLS Type 1	40
SLS Type 2, Type 3, Type 4, Type 5, and Type 6	42
SS1	46
SMS	49
GDL	50
Chapter 4 Behavior of Safety Functions	51
Limitations	52
Detected Fault Inhibition	53
Priority Between Safety Functions	53
Factory Settings	53
Configuration Download	53
Priority Between Safety Functions and No Safety-Related Functions	54
Monitoring of The Stator Frequency Consistency	57
Chapter 5 Safety Functions Visualization via HMI	59
Status of Safety Functions	60
Dedicated HMI	60
Error Code Description	61
Chapter 6 Technical Data	69
Electrical Data	70
Getting and Operating the Safety Function	71
Safety Function Capability	72
Debounce Time and Response Time	75
Chapter 7 Certified Architectures	77
Introduction	78
Multi-drive with the Safety Module Type Preventa XPS AF - Case 1	79
Multi-drive with the Safety Module Type Preventa XPS AF - Case 2	80
Multi-drive Without the Safety Module	81
Single Drive with the Safety Module Type Preventa XPS AV - Case 1	82
Single Drive with the Safety Module Type Preventa XPS AV - Case 2	83
Single Drive with the Safety Module Type Preventa XPS AF - Case 1	84
Single Drive with the Safety Module Type Preventa XPS AF - Case 2	85
Single Drive According to IEC 61508 and IEC 60204-1 - Case 1	86
Single Drive According to IEC 61508 and IEC 60204-1 - Case 2	87
Single Drive According to IEC 61508 and IEC 62061 with Safety Function GDL	88
Multi-drive Chaining According to IEC 61508 and IEC 62061 with Safety Function GDL	89

Chapter 8	Commissioning	91
Safety Functions Tab		92
Configure Safety Functions Panel		93
Visualization and Status of Safety Functions		98
Copying Safety Related Configuration from Device to PC and from PC to Device		99
Machine Signature		102
Chapter 9	Services and Maintenance	105
Maintenance		106
Power and MCU Replacement		106
Changing Machine Equipment		106

Safety Information



Important Information

NOTICE

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



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



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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

PLEASE NOTE

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

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

Qualification Of Personnel

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

Intended Use

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

Product Related Information

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

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

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

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

Damaged products or accessories may cause electric shock or unanticipated equipment operation.

DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

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

Contact your local Schneider Electric sales office if you detect any damage whatsoever.

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

DANGER

POTENTIAL FOR EXPLOSION

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

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

Your application consists of a whole range of different interrelated mechanical, electrical, and electronic components, the drive being just one part of the application. The drive by itself is neither intended to nor capable of providing the entire functionality to meet all safety-related requirements that apply to your application. Depending on the application and the corresponding risk assessment to be conducted by you, a whole variety of additional equipment is required such as, but not limited to, external encoders, external brakes, external monitoring devices, guards, etc.

As a designer/manufacturer of machines, you must be familiar with and observe all standards that apply to your machine. You must conduct a risk assessment and determine the appropriate Performance Level (PL) and/or Safety Integrity Level (SIL) and design and build your machine in compliance with all applicable standards. In doing so, you must consider the interrelation of all components of the machine. In addition, you must provide instructions for use that enable the user of your machine to perform any type of work on and with the machine such as operation and maintenance in a safe manner.

The present document assumes that you are fully aware of all normative standards and requirements that apply to your application. Since the drive cannot provide all safety-related functionality for your entire application, you must ensure that the required Performance Level and/or Safety Integrity Level is reached by installing all necessary additional equipment.

WARNING

INSUFFICIENT PERFORMANCE LEVEL/SAFETY INTEGRITY LEVEL AND/OR UNINTENDED EQUIPMENT OPERATION

- Conduct a risk assessment according to EN ISO 12100 and all other standards that apply to your application.
- Use redundant components and/or control paths for all critical control functions identified in your risk assessment.
- If moving loads can result in hazards, for example, slipping or falling loads, operate the drive in closed loop mode.
- Verify that the service life of all individual components used in your application is sufficient for the intended service life of your overall application.
- Perform extensive commissioning tests for all potential error situations to verify the effectiveness of the safety-related functions and monitoring functions implemented, for example, but not limited to, speed monitoring by means of encoders, short circuit monitoring for all connected equipment, correct operation of brakes and guards.
- Perform extensive commissioning tests for all potential error situations to verify that the load can be brought to a safe stop under all conditions.

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

A specific application note [NHA80973](#) is available on hoisting machines and can be downloaded on [se.com](#).

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

WARNING

UNANTICIPATED EQUIPMENT OPERATION

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

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

WARNING

LOSS OF CONTROL

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

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

(1) For USA: Additional information, refer to NEMA ICS 1.1 (latest edition), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control and to NEMA ICS 7.1 (latest edition), Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems.

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

WARNING

HOT SURFACES

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

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

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).
- 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.

WARNING

LOSS OF CONTROL

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

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

NOTICE

DESTRUCTION DUE TO INCORRECT MAINS VOLTAGE

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

Failure to follow these instructions can result in equipment damage.

About the Book



At a Glance

Document Scope

The purpose of this document is to provide information about safety functions incorporated in Altivar 320. These functions allow you to develop applications oriented in the protection of man and machine.

FDT/DTM (field device tool / device type manager) is a new technology chosen by several companies in automation.

To install the Altivar 32 DTM, you can download and install our FDT: SoMove lite on www.schneider-electric.com. It is including the Altivar 320 DTM.

The content of this manual is also accessible through the ATV320 DTM online help.

Validity Note

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

This documentation is valid for the Altivar 320 drives.

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

Step	Action
1	Go to the Schneider Electric home page www.schneider-electric.com .
2	In the Search box type the reference of a product or the name of a product range. <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 datasheet.
6	To save or print a datasheet as a .pdf file, click Download XXX product datasheet .

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

Related Documents

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

The internet site provides the information you need for products and solutions

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

Title of Documentation	Reference Number
Altivar 320 Getting Started	NVE21763 (English) , NVE21771 (French) , NVE21772 (German) , NVE21773 (Spanish) , NVE21774 (Italian) , NVE21776 (Chinese)
Altivar 320 Getting Started Annex (SCCR)	NVE21777 (English)
Altivar 320 Installation Manual	NVE41289 (English) , NVE41290 (French) , NVE41291 (German) , NVE41292 (Spanish) , NVE41293 (Italian) , NVE41294 (Chinese)
Altivar 320 Programming manual	NVE41295 (English) , NVE41296 (French) , NVE41297 (German) , NVE41298 (Spanish) , NVE41299 (Italian) , NVE41300 (Chinese)
Altivar 320 Modbus Serial Link manual	NVE41308 (English)
Altivar 320 Ethernet IP/Modbus TCP manual	NVE41313 (English)
Altivar 320 PROFIBUS DP manual (VW3A3607)	NVE41310 (English)
Altivar 320 DeviceNet manual (VW3A3609)	NVE41314 (English)
Altivar 320 CANopen manual (VW3A3608, 618, 628)	NVE41309 (English)
Altivar 320 POWERLINK Manual - VW3A3619	NVE41312 (English)
Altivar 320 EtherCAT manual - VW3A3601	NVE41315 (English)
Altivar 320 Communication Parameters	NVE41316 (English)
Altivar 320 PROFINET manual	NVE41311 (English)
Altivar 320 Safety Functions manual	NVE50467 (English) , NVE50468 (French) , NVE50469 (German) , NVE50470 (Spanish) , NVE50472 (Italian) , NVE50473 (Chinese)

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

Terminology

The technical terms, terminology, and the corresponding descriptions in this manual normally use the terms or definitions in the relevant standards.

In the area of drive systems this includes, but is not limited to, terms such as **error**, **error message**, **failure**, **fault**, **fault reset**, **protection**, **safe state**, **safety function**, **warning**, **warning message**, and so on.

Among others, these standards include:

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

In addition, the term **zone of operation** is used in conjunction with the description of specific hazards, and is defined as it is for a **hazard zone** or **danger zone** in the EC Machinery Directive (2006/42/EC) and in ISO 12100-1.

Contact Us

Select your country on:

www.schneider-electric.com/contact

Schneider Electric Industries SAS

Head Office
35, rue Joseph Monier
92500 Rueil-Malmaison
France

Chapter 1

General Information

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Introduction	16
Certifications	18
Basics	19

Introduction

Overview

WARNING

INEFFECTIVE SAFETY FUNCTIONS

- Verify that a risk assessment as per ISO 12100-1 and/or any other equivalent assessment has been performed before this product is used.
- Verify that only persons who are trained and certified experts in safety engineering and who are familiar with all safety-related standards, provisions, and regulations such as, but not limited to, IEC 61800-5-2 work with this product.
- Verify that only persons who are thoroughly familiar with the safety-related applications and the non-safety-related applications as well as the hardware used to operate the machine/process, work with this product.

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

WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Only start the machine/process if there are no persons or obstructions in the zone of operation.
- Only make modifications of any type whatsoever, including, but not limited to, parameters, settings, configurations, hardware, if you fully understand all effects of such modifications.
- Verify that modifications do not compromise or reduce the Safety Integrity Level (SIL), Performance Level (PL) and/or any other safety-related requirements and capabilities defined for your machine/process.
- After modifications of any type whatsoever, restart the machine/process and verify the correct operation and effectiveness of all functions by performing comprehensive tests for all operating states, the defined safe state, and all potential error situations.
- If you have to commission or recommission the machine/process, perform a commissioning test pursuant to all regulations, standards, and process definitions applicable to your machine/process.
- Document all modifications in compliance with all regulations, standards, and process definitions applicable to your machine/process.

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

WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Connect the drive to be configured directly to the PC.
- Do not establish a connection via network/Fieldbus protocols from the PC to the drive to be configured.

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

The safety functions incorporated in ATV320 are intended to maintain the safe condition of the installation or prevent hazardous conditions arising at the installation. In some cases, further safety-related systems external to the drive (for example a mechanical brake) may be necessary to maintain the safe condition when electrical power is removed.

The safety functions are configured with SoMove software.

Integrated safety functions provide the following benefits:

- Additional standards-compliant safety functions
- No need for external safety-related devices
- Reduced wiring effort and space requirements
- Reduced costs

The ATV320 drives are compliant with the requirements of the standards in terms of implementation of safety functions.

Safety Functions as Defined by IEC 61800-5-2

Definitions

Acronym	Description
STO	Safe Torque Off No power that could cause torque or force is supplied to the motor.
SLS	Safely-Limited Speed The SLS function prevents the motor from exceeding the specified speed limit. If the motor speed exceeds the specified speed limit value, safety function STO is triggered.
SS1	Safe Stop 1 <ul style="list-style-type: none">● initiates and monitors the motor deceleration rate within set limits to stop the motor● initiates the Safe Operating Stop function when the motor speed is below the specified limit

Safety Function Not Defined in IEC 61800-5-2

Definitions

Acronym	Description
SMS	Safe Maximum Speed The SMS function prevents the speed of the motor from exceeding the specified speed limit. If the motor speed exceeds the specified speed limit value, safety function STO is triggered. The SMS can only be activated or deactivated with the commissioning software. When activated, the stator frequency is constantly monitored irrespective of the mode of operation.
GDL	Guard Door Locking The GDL function allows you to release the guard door lock when the motor power is turned off.

Notation

The graphic display terminal (to be ordered separately - reference VW3A1101) menus are shown in square brackets.

The integrated 7-segment display terminal menus are shown in round brackets.

Parameter names are displayed on the graphic display terminal in square brackets.

Parameter codes are displayed on the integrated 7-segment display terminal in round brackets.

Certifications

EC Declaration of Conformity

The EC Declaration of Conformity for the EMC Directive can be obtained on www.schneider-electric.com.

ATEX Certification

The ATEX certificate can be obtained on www.schneider-electric.com.

Functional Safety Certification

The integrated safety functions are compatible and certified according to IEC 61800-5-2 Ed.1 Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional.

IEC 61800-5-2, as a product standard, sets out safety-related considerations of Power Drive System Safety Related PDS (SR)s in terms of the framework of the IEC 61508 Ed.2 series of standards.

Compliance with the IEC 61800-5-2 standard, for the safety functions described below, will facilitate incorporation of a PDS (SR) (Power Drive System suitable for use in safety-related applications) into a safety-related control system using the principles of IEC 61508, or IEC 13849-1, as well as IEC 62061 for process systems and machinery.

The defined safety functions are:

- SIL2 and SIL3 capability in compliance with IEC 61800-5-2 and the IEC 61508 Ed.2 series.
- Performance Level d and e in compliance with IEC 13849-1.
- Compliant with Category 3 and 4 of European standard IEC 13849-1 (EN 954-1).

Also refer to safety function Capability.

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

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

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.

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 faults, depending on the required SIL.

All components of a safety function must be subjected to a probability assessment to evaluate the effectiveness of the measures implemented for controlling detected faults.

This assessment determined the PFH (Average frequency of dangerous failure) 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.

Performance level	Average frequency of dangerous failure (PFH) at high demand or continuous demand
4	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-6} \dots < 10^{-5}$

PL - Performance Level

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

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 frequency of dangerous failure.

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

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 and dangerous detected failures to the total failure rate of the system.

$$SFF = (\Sigma \lambda_s + \Sigma \lambda_{Dd}) / (\Sigma \lambda_s + \Sigma \lambda_{Dd} + \Sigma \lambda_{Du})$$

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
60% ... < 99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

PFD - Probability of Failure on Demand

The standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum Safe Failure Fraction. The concept of 'dangerous failure' must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

The PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) of low demand operation for different SILs are defined in IEC 61508 are as follows:

SIL	PFD	PFD (power)	RRF
1	0.1 - 0.01	$10^{-1} - 10^{-2}$	10 - 100
2	0.01 - 0.001	$10^{-2} - 10^{-3}$	100 - 1000
3	0.001 - 0.0001	$10^{-3} - 10^{-4}$	1000 - 10,000
4	0.0001 - 0.00001	$10^{-4} - 10^{-5}$	10,000 - 100,000

In high demand or continuous operation, these changes to the following:

SIL	PFH	PFH (power)	RRF
1	0.00001 - 0.000001	$10^{-5} - 10^{-6}$	100,000 - 1,000,000
2	0.000001 - 0.0000001	$10^{-6} - 10^{-7}$	1,000,000 - 10,000,000
3	0.0000001 - 0.00000001	$10^{-7} - 10^{-8}$	1000 - 10,000
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.

Chapter 2

Description

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Safety Function STO (Safe Torque Off)	24
Safety Function SS1 (Safe Stop 1)	26
Safety Function SLS (Safely-Limited Speed)	28
Safety Function SMS (Safe Maximum Speed)	35
Safety Function GDL (Guard Door Locking)	37

Safety Function STO (Safe Torque Off)

Overview

The safety function STO (Safe Torque Off) does not remove power from the DC bus. The safety function STO only removes power to the motor. The DC bus voltage and the mains voltage to the drive are still present.

DANGER

HAZARD OF ELECTRIC SHOCK

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

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

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

WARNING

INSUFFICIENT DECELERATION OR UNINTENDED EQUIPMENT OPERATION

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

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

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.

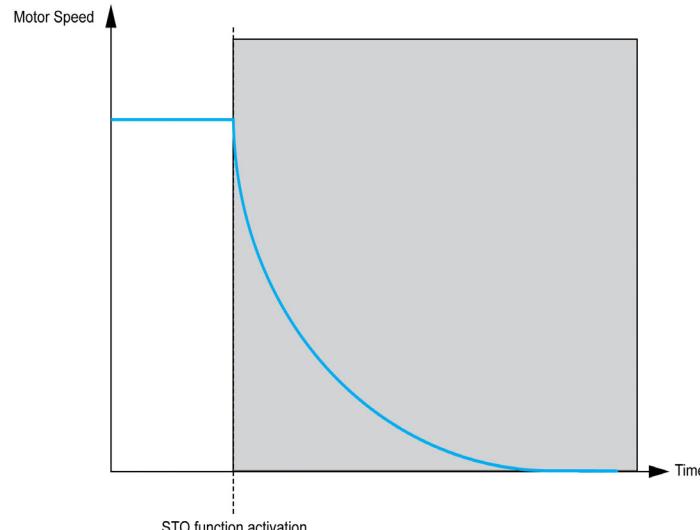
The principles and requirements of the prevention of unexpected start-up are described in the standard EN 1037:1995+A1.

The digital input STO is assigned to this safety function and cannot be modified.

If a paired terminal line in 2 channels is required to trigger safety function STO, the function can also be enabled by the safety-related digital inputs.

The safety function STO is configured with the commissioning software.

The safety function STO status can be displayed using the HMI of the drive 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 (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 13849-1
STO with or without safety module	SIL 2	PL d
STO & DI3 with or without safety module	SIL 3	PL e
DI3 and DI4	SIL 2	PL d
DI5 and DI6	SIL 2	PL d

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). This is the reason why an additional safety module is required if the machine restarts automatically after the safety function STO has been deactivated.

Safety Function SS1 (Safe Stop 1)

Overview

The safety function SS1 (Safe Stop 1) monitors the deceleration according to a dedicated deceleration ramp and safely shuts off the torque once standstill has been achieved.

When the safety function SS1 is triggered, it overrides all other functions (except STO function that has priority) and operations in all modes.

The unit of the SS1 deceleration ramp is in Hz/s. The setting of the ramp is done with two parameters:

[SS1 ramp unit] 5 5 r u (Hz/s) to give the unit of the ramp in 1 Hz/s, 10 Hz/s, and 100 Hz/s

[SS1RampValue] 5 5 r E (0.1) to set the value of the ramp

Ramp calculation:

$$\text{Ramp} = \text{SSrU} * \text{SSrt}$$

Example: If SSrU = 10 Hz/s and SSrt = 5.0 the deceleration ramp is 50 Hz/s.

The safety function SS1 is configured with the commissioning software, for more information see Commissioning ([see page 91](#)).

The safety function SS1 status can be displayed using the HMI of the drive or using the commissioning software.

Behavior on Activation of the SS1 Function

When SS1 function is triggered, it monitors the deceleration of the motor according to the specified monitoring ramp until standstill is reached and verifies if the motor speed is not above a monitored limit value depending on the specified monitoring ramp and the parameter [SS1 trip threshold] 5 5 E E .

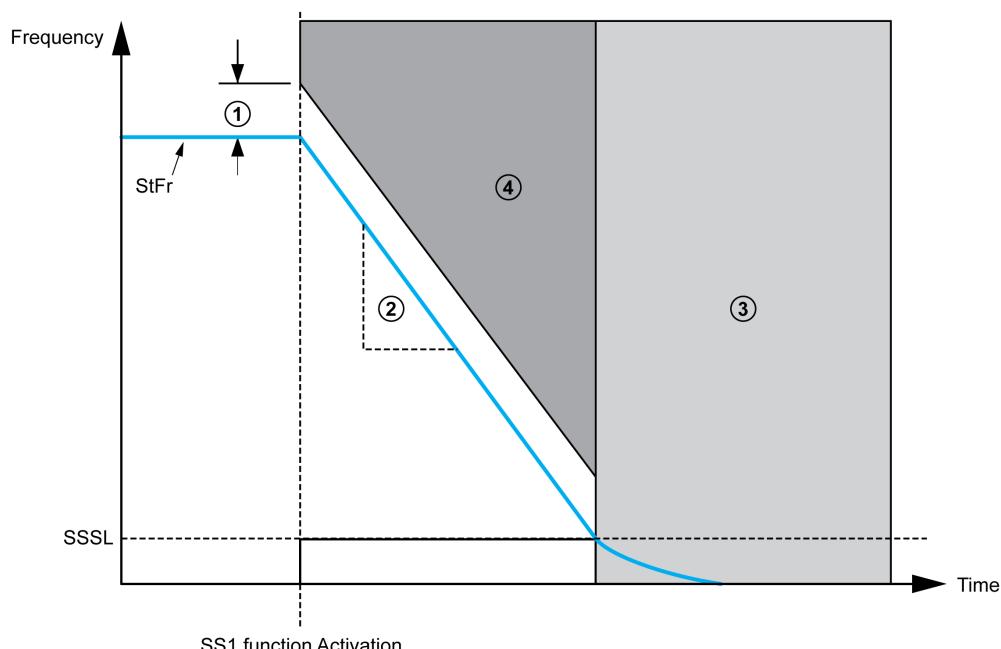
If the monitored limit value is exceeded:

- An error is triggered and the error code [Safety function fault] 5 R F F is displayed.
- Safety function STO is triggered.

After the [Standstill level] 5 5 S L has been reached, the safety function STO is triggered.

SS1 function continues to be active if the request has been removed before the standstill has been reached.

NOTE: The error detection depends on [Stator Frequency] 5 E F r .



(1): SS1 trip threshold, (2): SS1 deceleration ramp (dV/dT), (3): STO function triggered, (4): Error and STO function triggered

Behavior on Deactivation of the SS1 Function

After an SS1 stop, send a new run command (even if the run command is set on level command).

SS1 Standard Reference

The SS1 function is defined in section 4.2.2.2 of standard IEC 61800-5-2:

The PDS(SR) (Power drive system suitable for use in safety-related applications) either:

- Initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function (see 4.2.2.2) when the motor speed is below a specified limit; or
- Initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or
- Initiates the motor deceleration and initiates the STO function after an application-specific time delay.

NOTE: This safety function corresponds to a controlled stop in accordance with stop category 1 of IEC 60204-1.

Safety Function (SF) Level Capability for Safety Function SS1

Function	Configuration	SIL Safety Integrity Level According to IEC 61508	PL Performance Level According to ISO 13849-1
SS1 type C	STO with Preventa module	SIL2	PL d
	STO and DI3 with Preventa module	SIL 3	PL e
SS1 type B	DI3 and DI4	SIL 2	PL d
	DI5 and DI6	SIL 2	PL d

Emergency Stop Category 1

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 1 is a controlled shut-down, whereby the energy supply to the motor is maintained to perform the shut-down, and the energy supply is only interrupted when the shut-down has been completed.

Stop category 1 is equivalent to the **[Safe Stop 1] 5 5 /** 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 SS1 is used to manage an emergency stop category 1, the motor must not restart automatically when safety function SS1 has been triggered and deactivated (with or without a power cycle). This is the reason why an additional safety module is required if the machine restarts automatically after the safety function SS1 has been deactivated.

Safety Function SLS (Safely-Limited Speed)

Overview

This function is used to limit the speed of a motor.

There are 6 types of SLS function:

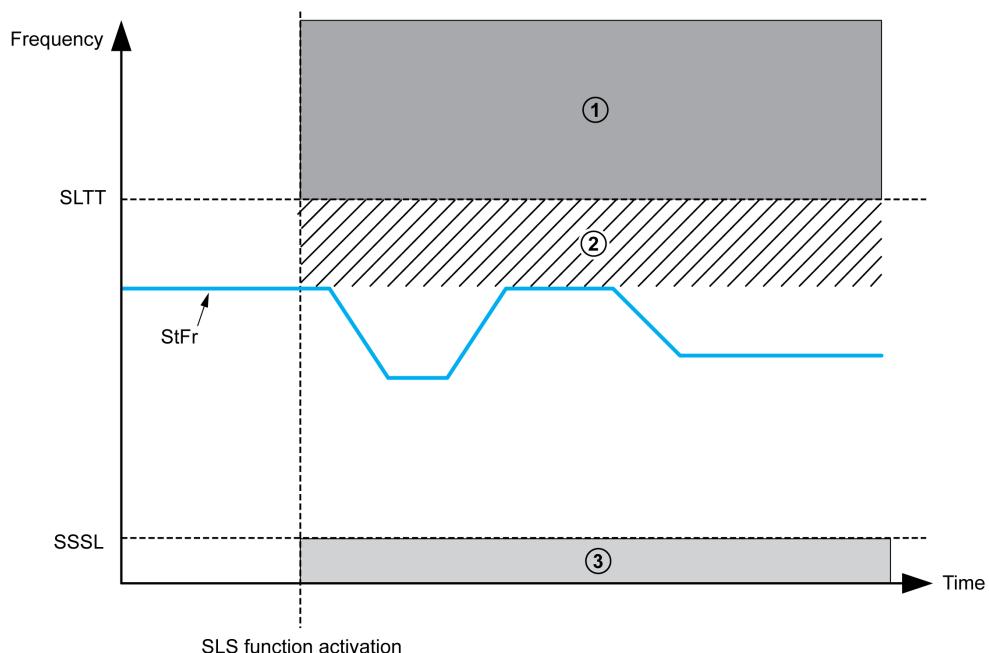
- SLS type 1: Limits the motor speed to the actual motor speed.
- SLS type 2: Limits the motor speed to a value set using a parameter.
- SLS type 3: Same as type 2 with specific behavior if the motor speed is above threshold value set using a parameter.
- SLS type 4: Limits the motor speed to a value set using a parameter. The direction of rotation can be changed while the safety function is active.
- SLS type 5: Same as type 4 with the specific behavior if the motor speed is above threshold value set using a parameter.
- SLS type 6: Same as type 4 with specific behavior if the motor speed is above threshold value set using a parameter.

NOTE: SLS types 2 and 3 use (SLwt) [SLS Wait time] parameter to allow the motor to run under the [standstill level] 5 5 L for a given time after the safety function SLS has been activated.

The safety function SLS is configured with the commissioning software, for more information see commissioning ([see page 91](#)).

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

Behavior on Activation of the Safety Function SLS Type 1



①: Error and STO function triggered, ②: Reference upper limit, ③: STO function triggered

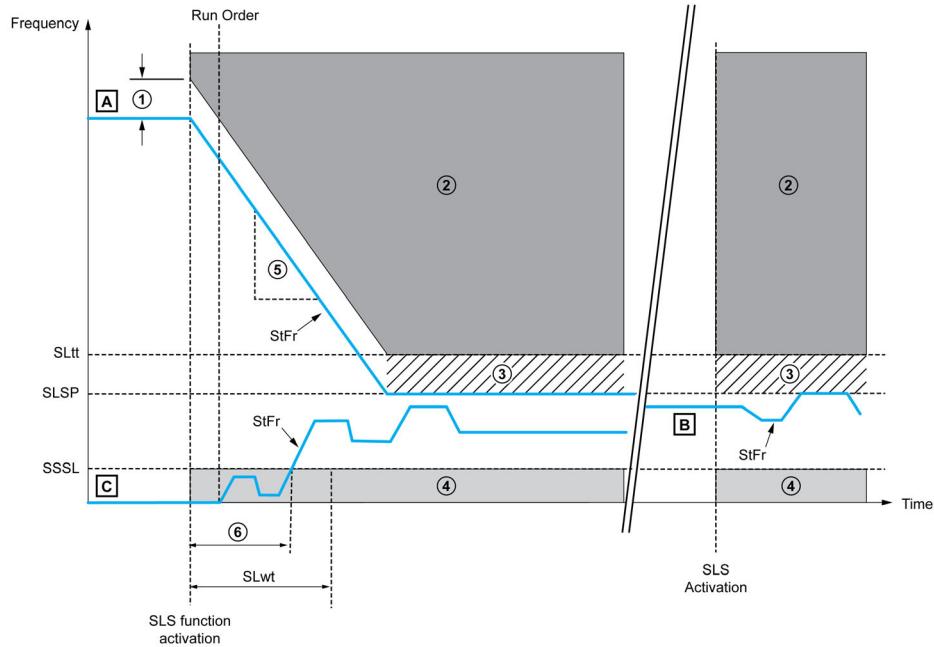
When the safety function is activated:

- If the [Stator Frequency] 5 E F r is above the [SLS tolerance threshold] 5 L E E, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] 5 R F F.
- If the [Stator Frequency] 5 E F r is under the [SLS tolerance threshold] 5 L E E, the stator frequency is limited to the actual stator frequency. The reference frequency will only vary between this value and the standstill level SSSL.

While the function is activated:

- If the [Stator Frequency] 5 E F r decreases and reaches the [Standstill level] 5 5 L frequency, the safety function STO is triggered.
- If the [Stator Frequency] 5 E F r increases and reaches [SLS tolerance threshold] 5 L E E, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] 5 R F F.

Behavior on Activation of the Safety Function SLS Type 2



- ①: SS1 trip threshold, ②: Error and STO function triggered, ③: Reference upper limit, ④: STO function triggered, ⑤: SS1 deceleration ramp (dV/dT), ⑥: Time taken for the [Stator Frequency] $S E F r$ to become greater than SSSL

A: [Stator Frequency] $S E F r$ is above [Set Point] $S L S P$

B: [Stator Frequency] $S E F r$ is between [Standstill level] $S S S L$ and [Set Point] $S L S P$

C: [Stator Frequency] $S E F r$ is below [Standstill level] $S S S L$ and [SLS wait time] (SLwt) $\neq 0$

When the function is activated:

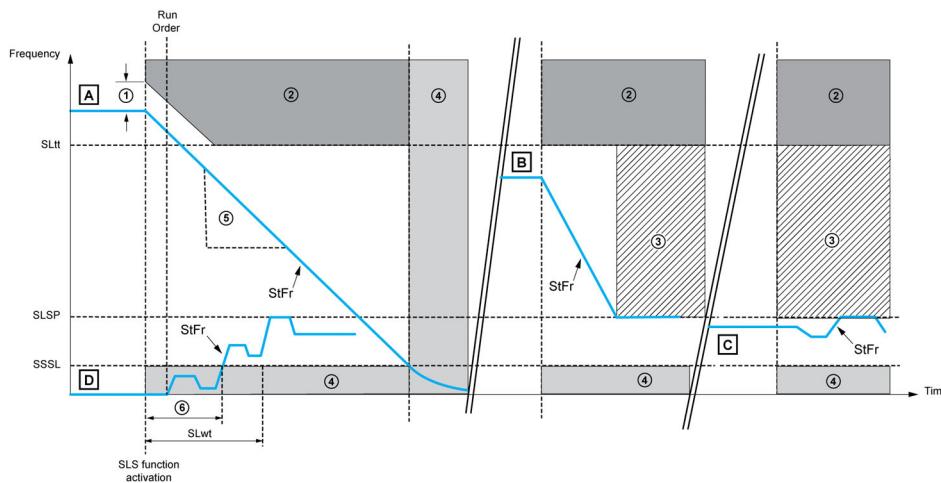
- If the [Stator Frequency] $S E F r$ is above the [Set point] $S L S P$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ is reached.(see case A)
- If the [Stator Frequency] $S E F r$ is below the SLSP the current reference is not changed but limited to the [Set point] $S L S P$.(see case B)
- If the [Stator Frequency] $S E F r$ is still below the [Standstill level] $S S S L$ frequency after [SLS wait time] (SLwt) has elapsed, the safety function STO will be triggered.(see case C)

While the function is activated:

- The reference frequency can only vary between the [Set point] $S L S P$ and the standstill level SSSL.
- If the [Stator Frequency] $S E F r$ decreases and reaches the [Standstill level] $S S S L$ frequency, safety function STO is triggered.
- If the [Stator Frequency] $S E F r$ increases and reaches the [SLS tolerance threshold] $S L E E$, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] $S R F F$.

Behavior on Activation of the Safety Function SLS Type 3

SLS type 3 has the same behavior as SLS type 2 except that If the [Stator Frequency] $S E F r$ is above the [SLS tolerance threshold] $S L E E$, the safety function SS1 is triggered instead of decelerating to the [Set point] $S L S P$ (see case A)



①: SS1 trip threshold, ②: Error and STO function triggered, ③: Reference upper limit, ④: STO function triggered, ⑤: SS1 deceleration ramp (dV/dT), ⑥: Time taken for the [Stator Frequency] $S E F r$ to become greater than SSSL

- A**: [Stator Frequency] $S E F r$ is above [SLS tolerance threshold] $S L E E$
- B**: [Stator Frequency] $S E F r$ is between [Set Point] $S L S P$ and [SLS tolerance threshold] $S L E E$
- C**: [Stator Frequency] $S E F r$ is between [Standstill level] $S S S L$ and [Set Point] $S L S P$
- D**: [Stator Frequency] $S E F r$ is below [Standstill level] $S S S L$ and [SLS wait time] (SLwt) ≠ 0

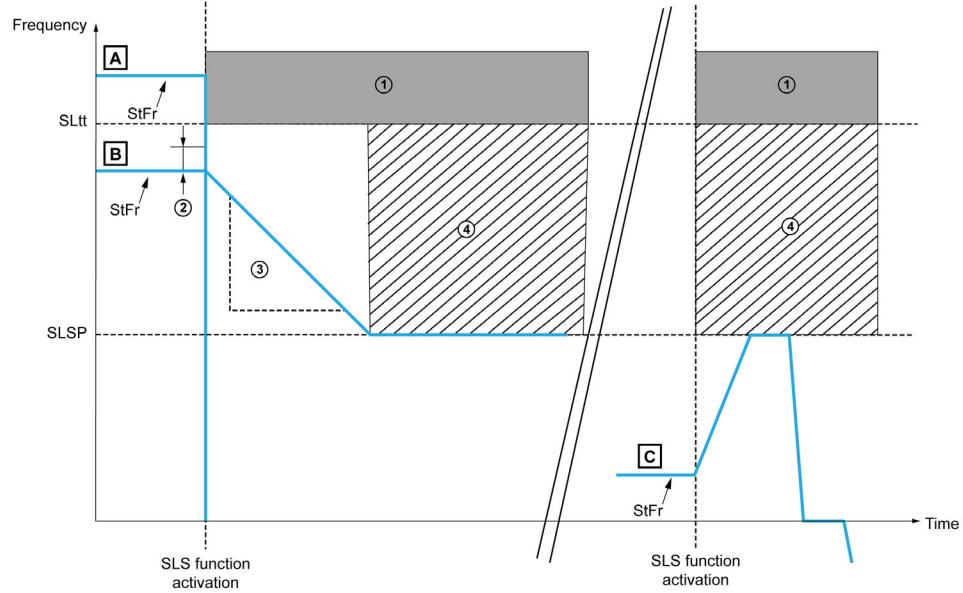
When the function is activated:

- If the [Stator Frequency] $S E F r$ is above the [SLS tolerance threshold] $S L E E$, the safety function SS1 is triggered. (see case A).
- If the [Stator Frequency] $S E F r$ is between the [SLS tolerance threshold] $S L E E$ and the [Set point] $S L S P$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ has been reached.(see case B).
- If the [Stator Frequency] $S E F r$ is below the [Set point] $S L S P$ the current reference is not changed but limited to the [Set point] $S L S P$.(see case C)
- If the [Stator Frequency] $S E F r$ is still below the [Standstill level] $S S S L$ frequency after [SLS wait time] $S L W E$ has elapsed, the safety function STO will be triggered.(see case D)

While the function is activated:

- The reference frequency can only vary between the [Set point] $S L S P$ and the [Standstill level] $S S S L$.
- If the [Stator Frequency] $S E F r$ decreases and reaches the [Standstill level] $S S S L$ frequency, the safety function STO is triggered.
- If the [Stator Frequency] $S E F r$ increases and reaches the [SLS tolerance threshold] $S L E E$, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] $S R F F$.

Behavior on Activation of the Safety Function SLS Type 4



- ① Error and STO function triggered, ② SS1 trip threshold, ③ SS1 deceleration ramp (dv/dt), ④ reference upper limit

A: [Stator Frequency] $S E F r$ is above [SLS tolerance threshold] $S L E E$

B: [Stator Frequency] $S E F r$ is between [Set Point] $S L S P$ and [SLS tolerance threshold] $S L E E$

C: [Stator Frequency] $S E F r$ is below [Set Point] $S L S P$

NOTE: If the $SLTT \leq SLSP$ for SLS type 4, SAFF fault is triggered.

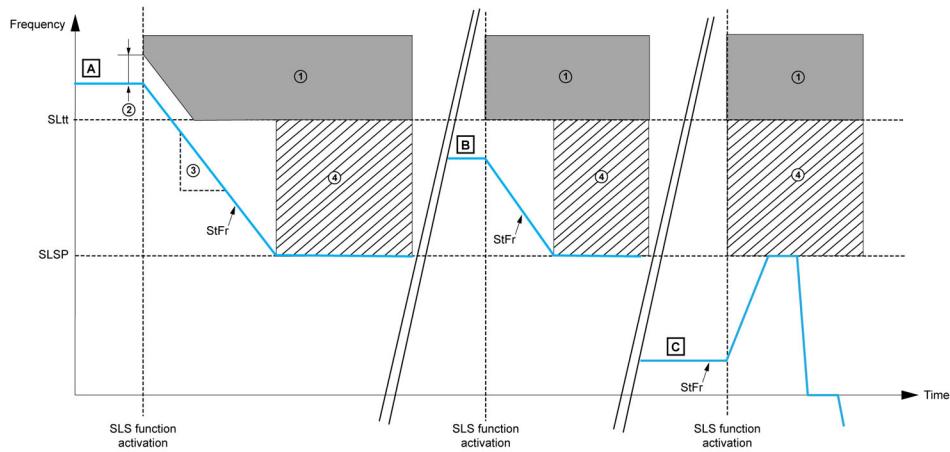
When the function is activated:

- If the [Stator Frequency] $S E F r$ is above the [SLS tolerance threshold] $S L E E$, the safety function STO is triggered with the error code [Safety function fault] $S R F F$. (see case A)
- If the [Stator Frequency] $S E F r$ is between the [SLS tolerance threshold] $S L E E$ and the [Set point] $S L S P$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ has been reached.(see case B)
- If the [Stator Frequency] $S E F r$ is below the [Set point] $S L S P$, the current reference is not changed but limited to the [Set point] $S L S P$.(see case C).

While the function is activated:

- The reference frequency can vary between the [Set point] $S L S P$ in both forward and reverse directions.
- If the [Stator Frequency] $S E F r$ increases and reaches [SLS tolerance threshold] $S L E E$, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] $S R F F$.

Behavior on Activation of the Safety Function SLS Type 5



①: Error and STO function triggered, ②: SS1 trip threshold, ③: SS1 deceleration ramp (dv/dt), ④: Reference upper limit

A: [Stator Frequency] $S E F r$ is above [SLS tolerance threshold] $S L E E$

B: [Stator Frequency] $S E F r$ is between [Set Point] $S L S P$ and [SLS tolerance threshold] $S L E E$

C: [Stator Frequency] $S E F r$ is below [Set Point] $S L S P$

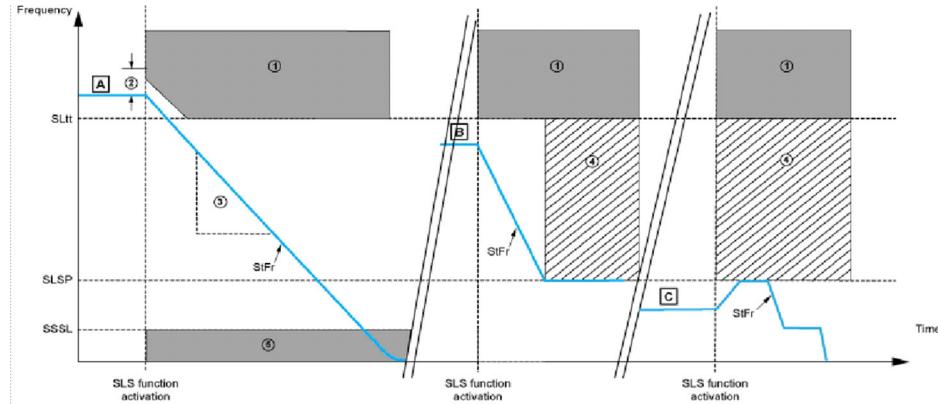
When the function is activated:

- If the [Stator Frequency] $S E F r$ is above the [SLS tolerance threshold] $S L E E$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ has been reached. (see case A)
- If the [Stator Frequency] $S E F r$ is between the [SLS tolerance threshold] $S L E E$ and the [Set point] $S L S P$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ has been reached.(see case B)
- If the [Stator Frequency] $S E F r$ is below the [Set point] $S L S P$, the current reference is not changed but limited to the [Set point] $S L S P$.(see case C).

While the function is activated:

- The reference frequency can vary between the [Set point] $S L S P$ in both forward and reverse directions.
- If the [Stator Frequency] $S E F r$ increases and reaches [SLS tolerance threshold] $S L E E$, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] $S R F F$.

Behavior on Activation of the Safety Function SLS Type 6



①: Error and STO function triggered, ②: SS1 trip threshold, ③: SS1 deceleration ramp (dV/dT) ④: Reference upper limit, ⑤: STO function triggered.

A: [Stator Frequency] $S E F_r$ is above [SLS tolerance threshold] $S L E E$

B: [Stator Frequency] $S E F_r$ is between [Set Point] $S L S P$ and [SLS tolerance threshold] $S L E E$

C: [Stator Frequency] $S E F_r$ is below [Set Point] $S L S P$

When the function is activated:

- If the [Stator Frequency] $S E F_r$ is above the [SLS tolerance threshold] $S L E E$, the drive decelerates according to SS1 deceleration ramp until $S S S L$ is reached then the safety function STO is triggered (see case A).
- If the [Stator Frequency] $S E F_r$ is between the [SLS tolerance threshold] $S L E E$ and the [Set point] $S L S P$, the drive decelerates according to SS1 deceleration ramp until the [Set point] $S L S P$ has been reached.(see case B)
- If the [Stator Frequency] $S E F_r$ is below the [Set point] $S L S P$, the current reference is not changed but limited to the [Set point] $S L S P$.(see case C).

While the function is activated:

- The reference frequency can vary between the [Set point] $S L S P$ in both forward and reverse directions.
- If the [Stator Frequency] $S E F_r$ increases and reaches [SLS tolerance threshold] $S L E E$, the safety function STO is triggered and an error is triggered with the error code [Safety function fault] $S R F F$.

Behavior on Deactivation of the Safety Function SLS for All SLS Types

If...	Then ...
The drive is still running when the function is deactivated	The reference frequency of the active channel is applied.
Safety function STO has been triggered and the drive is not in fault state.	A new run command must be applied.
The safety function SLS type 2, 3, 4 is deactivated while the drive decelerates to the [Set point] 5 L 5 P according to SS1 deceleration ramp. The safety function SLS type 3 is deactivated while the safety function SS1 has been triggered	The safety function SLS remains activated until the [Set point] 5 L 5 P has been reached. STO is triggered when [Standstill level] 5 5 5 L is reached and a new run command must be applied.
a stop command is applied	The safety function SLS remains active and the drive decelerates until standstill is reached. For SLS type 1, 2, or 3 STO function is triggered when the [Stator Frequency] 5 E F r decreases and reaches the [Standstill level] 5 5 5 L frequency.
an error is detected	The safety function SLS remains active and the drive stops according to the configured error response. For SLS type 1, 2, or 3 STO function will be triggered after the [Standstill level] 5 5 5 L frequency has been reached. The drive can be reset after the cause is cleared.

SLS Standards References

The safety function SLS is defined in section 4.2.3.4 of standard IEC 61800-5-2 The SLS function helps to prevent the motor from exceeding the specified speed limit.

Safety Function (SF) Level for Safety Function SLS

Configuration	SIL Safety Integrity Level According to IEC 61508	PL Performance level According to ISO 13849-1
DI3 and DI4	SIL 2	PL d
DI5 and DI6	SIL 2	PL d

Safety Function SMS (Safe Maximum Speed)

Overview

This function prevents the speed of the motor from exceeding the specified safe maximum speed limit.

The safety function SMS is configured using commissioning software, for details, refer commissioning (*see page 91*).

[SMS Activation] $S\pi S R$ parameter is used to activate or deactivate the SMS function.

Two speed limits can be set using the following parameters

- [SMS Low Limit] $S\pi L L$: To select the lower speed limit.
- [SMS High Limit] $S\pi L H$: To select the higher speed limit

[SMS Low Limit] $S\pi L L$ or [SMS High Limit] $S\pi L H$ is considered as safe maximum speed limit based on the [SMS Assignment] $S\pi L S$ selection.

When [SMS Assignment] $S\pi L S$ is selected as L34 or L56 (digital input 3 and 4 or digital input 5 and 6),

- If the digital inputs are in low state (0), [SMS Low Limit] $S\pi L L$ is considered as the safe maximum speed limit.
- If the digital inputs are in high state (1), [SMS High Limit] $S\pi L H$ is considered as the safe maximum speed limit.

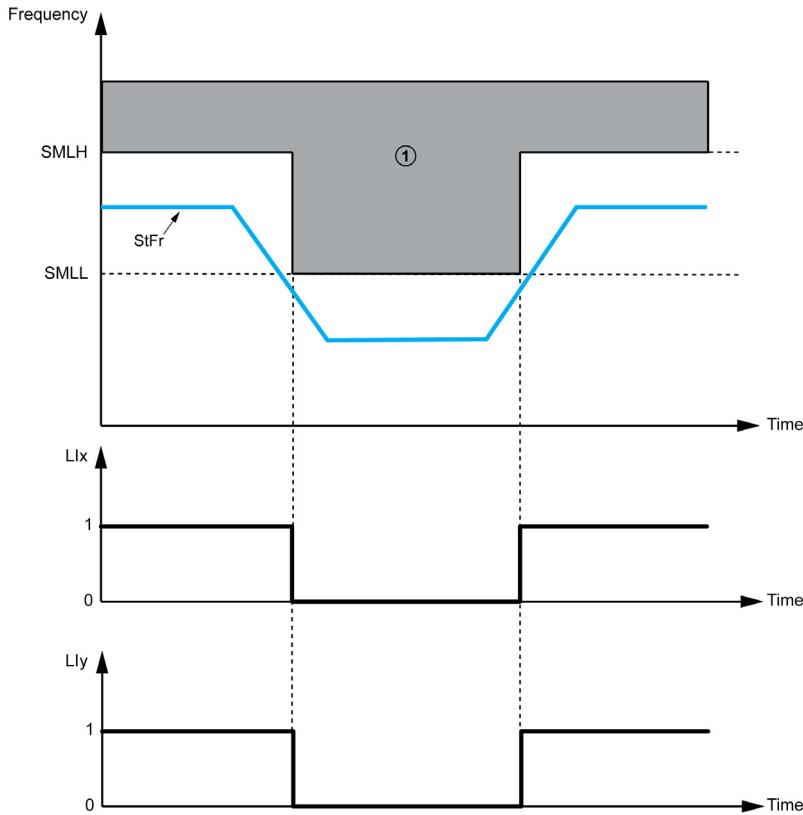
When [SMS Assignment] $S\pi L S$ is selected as NO, [SMS Low Limit] $S\pi L L$ is considered as the safe maximum speed limit.

NOTE:

- The SMS function does not adjust the speed reference.
- The speed reference should be adjusted through an active speed reference channel according to [SMS Low Limit] $S\pi L L$ or [SMS High Limit] $S\pi L H$.

The status of safety function SMS is displayed on graphical display terminal of the drive and **Monitoring** tab of the commissioning software.

Behavior on Activation of the Safety Function SMS



① Error and STO function triggered

While the function is activated

- If digital inputs (Dlx and Dly) are in low state (0) and [Stator Frequency] $S E F r$ increases and reaches [SMS Low Limit] $S \pi L L$, STO is triggered and an error is triggered with an error code [Safety function fault] $S R F F$.
- If digital inputs (Dlx and Dly) are in high state (1) and [Stator Frequency] $S E F r$ increases and reaches [SMS High Limit] $S \pi L H$, STO is triggered and an error is triggered with an error code [Safety function fault] $S R F F$.
- If digital inputs (Dlx and Dly) are not assigned and [Stator Frequency] $S E F r$ increases and reaches [SMS Low Limit] $S \pi L L$, STO is triggered and an error is triggered with an error code [Safety function fault] $S R F F$.

SMS Standard References

The safety function SMS is not defined in IEC 61800-5-2. The SMS function prevents the speed of the motor from exceeding the specified speed limit. If the motor speed exceeds the specified speed limit value, safety function STO is triggered. The SMS can only be activated or deactivated with the commissioning software. When activated, the stator frequency is constantly monitored irrespective of the mode of operation.

Safety Function (SF) Level for Safety Function SMS

Configuration	SIL Safety Integrity Level According to IEC 61508	PL Performance level According to ISO 13849-1
DI3 and DI4	SIL 2	PL d
DI5 and DI6	SIL 2	PL d
No	SIL 2	PL d

Safety Function GDL (Guard Door Locking)

Overview

This function allows you to release the guard door lock after specified delay when the motor power is turned off. The front door of the machine can be opened only after the motor is stopped, this function helps to ensure the safety of the machine operator.

For details on certified wiring diagram, refer Single Drive According to IEC 61508 and IEC 62061 for GDL Function ([see page 88](#)).

[**GDL Assignment**] $G d L R$ parameter is used to activate or deactivate the GDL function.

GDL function uses $L \Delta I$ parameter.

Two delays can be configured using following parameters.

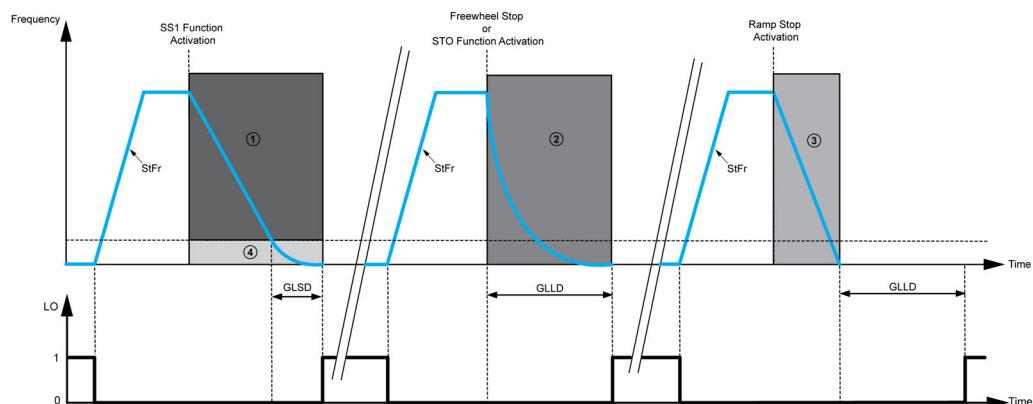
- [**Guard Door Locking Long Delay**] $G L L d$: Long delay after any stop command (such as STO, ramp stop, DC injection, and so on) other than SS1 stop to make sure that the machine is stopped.
- [**Guard Door Locking Short Delay**] $G L S d$: Short delay after SS1 ramp to make sure that the machine is stopped.

NOTE: [**Guard Door Locking Long Delay**] $G L L d$ and [**Guard Door Locking Short Delay**] $G L S d$ are defined based on the characteristics of the machine.

The safety function GDL is configured using the commissioning software, for details, refer Commissioning ([see page 91](#)).

The status of the safety function GDL is displayed on graphical display terminal of the drive and **Monitoring** tab of the commissioning software.

Behavior on Activation of the Safety Function GDL



① SS1 stop, ② Freewheel stop, ③ Ramp stop, ④ STO function triggered

While the function is activated,

- If the safety function SS1 is triggered, digital output (DQ) changes to high state (1) after [**GDL Short Delay**] $G L S d$ and guard door lock is released.
- If the freewheel stop or safety function STO is triggered, digital output (DQ) changes to high state (1) after [**GDL Long Delay**] $G L L d$ and guard door lock is released.
- If the ramp stop is triggered, digital output (DQ) changes to high state (1) after [**GDL Long Delay**] $G L L d$ and guard door lock is released.

GDL Standard References

The safety function GDL is not defined in IEC 61800-5-2. The GDL function allows you to release the guard door lock when the motor power is turned off.

Safety Function (SF) Level for Safety Function GDL

Configuration	SIL Safety Integrity Level According to IEC 61508	PL Performance level According to ISO 13849-1
STO with safety module	SIL 1	PL c

Chapter 3

Calculation of Safety Related Parameters

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
SLS Type 1	40
SLS Type 2, Type 3, Type 4, Type 5, and Type 6	42
SS1	46
SMS	49
GDL	50

SLS Type 1

Collect Application Data

Before starting to configure the SLS function, you must collect the following data:

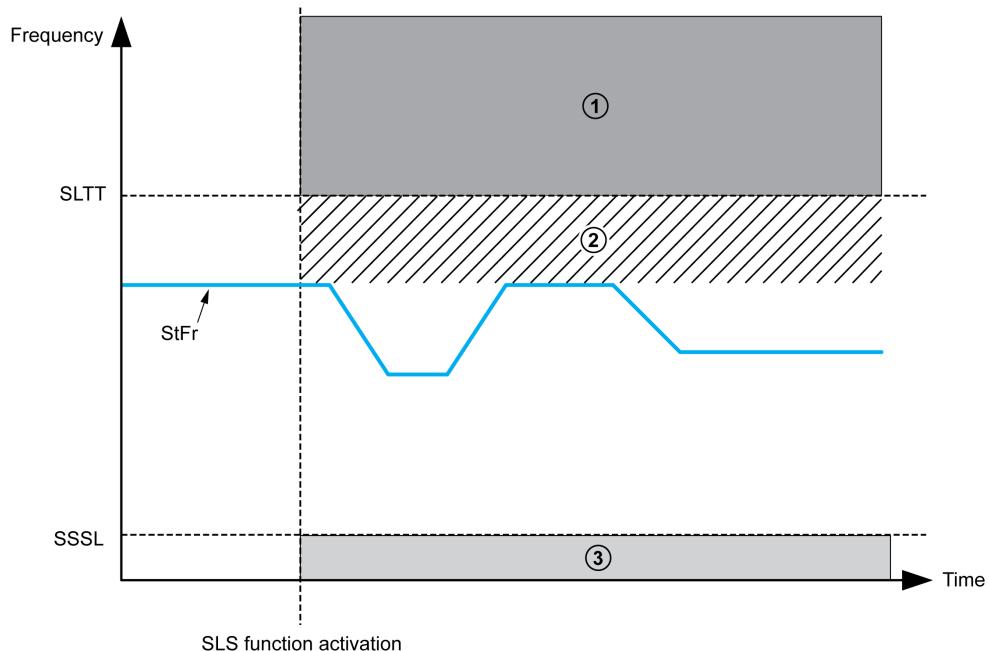
Code	Description	Unit	Comment
<i>F r S</i>	[Rated motor freq.]	Hz	See motor nameplate
<i>n SP</i>	[Rated motorspeed]	rpm	See motor nameplate
ppn	Motor pole pair number	-	See motor nameplate
Max Frequency	Maximum motor frequency for normal operation	Hz	This value is equal to [High speed] <i>H SP</i> or lower

Calculate the rated motor slip frequency *Fslip* (Hz):

$$F_{slip} = F_{rS} - \frac{N_{sp} \times ppn}{60}$$

To Configure the Function

Overview of diagram



① : Error and STO function triggered, ② : Reference upper limit, ③ : STO function triggered

Standstill Level

The recommended standstill level is: $SSSL = F_{slip}$

If the application requires a different standstill level, it can be set accordingly with the *SSSL* parameter.

Motor Frequency Limit Threshold

The recommended value of the parameter is $SLtt = 1.2 \times \text{Max Frequency} + F_{slip}$

Testing and Adjusting the Configuration

When configuration is complete, test the SLS function to verify it behaves as expected.

If an error is triggered with the error code **[Safety function fault] 5 RFF** apply the following troubleshooting rules

Context	Drive Status	Adjustment
SLS activated and motor running at the fixed setpoint frequency	<ul style="list-style-type: none">SAFF error codeSFFE.7 = 1	Motor frequency has reached the motor frequency limit threshold. The cause of the detected error can be due to frequency instability. Investigate and correct the cause. The value of SLtt can be modified to increase the tolerance threshold to the instability of the drive system.

Example

Code	Description	Unit
F r S	[Rated motor freq.]	50 Hz
n 5 P	[Rated motorspeed]	1350 rpm
ppn	Motor pole pair number	2
Max Frequency	Maximum motor frequency on normal operation. This value is generally equal to [High speed] H 5 P or lower	50 Hz

With these numerical values, the configuration of SLS type 1 is:

$$F_{slip} = 50 - \frac{1350 \times 2}{60} = 5 \text{ Hz}$$

$$SSSL = F_{slip} = 5 \text{ Hz}$$

$$SLtt = 1.2 \times \text{Max Frequency} + F_{slip} = 1.2 \times 50 + 5 = 65 \text{ Hz}$$

SLS Type 2, Type 3, Type 4, Type 5, and Type 6

Collect Application Data

Before starting to configure the SLS function, you must collect the following data:

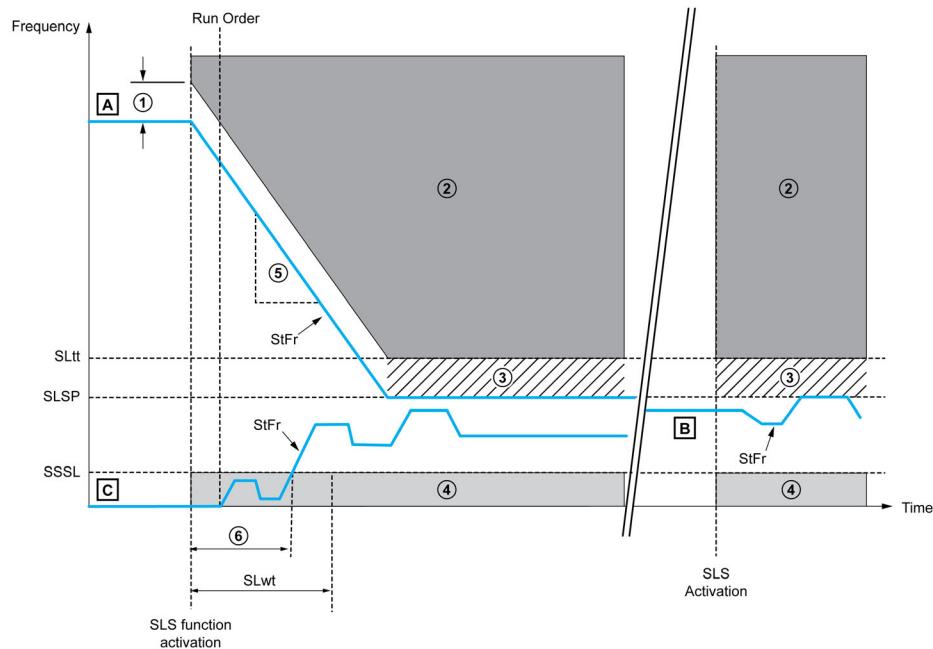
Code	Description	Unit	Comment
<i>F r S</i>	[Rated motor freq.]	Hz	See motor nameplate
<i>n S P</i>	[Rated motor speed]	rpm	See motor nameplate
ppn	Motor pole pair number	–	See motor nameplate
Max Frequency	Maximum motor frequency on normal operation	Hz	This value is equal to [High speed] <i>H S P</i> or lower.
SS1 deceleration ramp	Deceleration ramp to apply when SS1 ramp is triggered	Hz	–

Calculate the rated motor slip frequency *Fslip* (Hz).

$$F_{slip} = FrS - \frac{N_{sp} \times ppn}{60}$$

To Configure the Function

Overview of diagram



- ①: SS1 trip threshold, ②: Error and STO function triggered, ③: Reference upper limit, ④: STO function triggered, ⑤: SS1 deceleration ramp (dV/dT), ⑥: Time taken for the [Stator Frequency] *S E F r* to become greater than SSSL

A: [Stator Frequency] *S E F r* is above [Set Point] *S L S P*

B: [Stator Frequency] *S E F r* is between [Standstill level] *S S S L* and [Set Point] *S L S P*

C: [Stator Frequency] *S E F r* is below [Standstill level] *S S S L* and [SLS wait time] (SLwt) ≠ 0
Standstill Level

The recommended standstill level is: $SSSL = F_{slip}$

If the application requires a different standstill level, it can be set accordingly with the SSSL parameter.

Ramp Value and Ramp Unit

Set SSrt (ramp value) and SSru (ramp unit) parameters according to the deceleration ramp to apply when the safety function SS1 is triggered.

Ramp calculation: Ramp = SSru * SSrt

Example 1: If SSru = 1 Hz/s and SSrt = 500.0 the deceleration ramp is 500.0 Hz/s and the accuracy is 0.1 Hz

Example 2: If SSru = 10 Hz/s and SSrt = 50.0 the deceleration ramp is 500 Hz/s and the accuracy is 1 Hz

Use the table to set the correct accuracy according to the deceleration ramp to apply when the safety function SS1 is triggered:

Min	Max	Accuracy	SSrt	SSru
0.1 Hz/s	599 Hz/s	0.1 Hz/s	1 Hz/s	SS1 deceleration ramp
599 Hz/s	5990 Hz/s	1 Hz/s	10 Hz/s	SS1 deceleration ramp/10
5990 Hz/s	59900 Hz/s	10 Hz/s	100 Hz/s	SS1 deceleration ramp/100

SLS Setpoint

Set the SLS setpoint parameter (SLSP) to: *SLSP = Fsetpoint (SLS)*

Motor Frequency and ramp Limit Threshold

The recommended motor frequency limit threshold is $SLtt = 1.2 \times SLSP + Fs/10$ and the recommended SS1 ramp limit threshold is: $SStt = 0.2 \times Max\ Frequency$

SLS Wait time

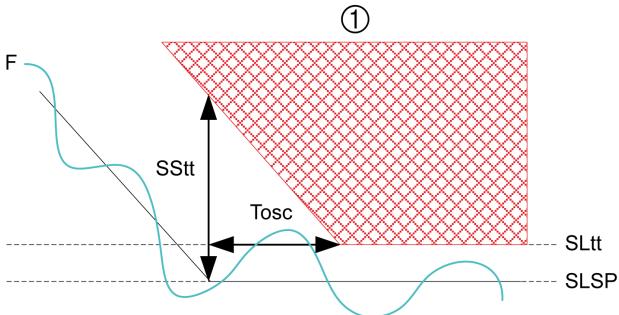
Set the **[SLS wait time]** (SLwt) greater than 0 ms to allow the motor to run under the **[standstill level] 5 5 5 L** for a given time after the safety function SLS has been activated.

NOTE: When SLS Type 4 is configured, **[SLS wait time]** (SLwt) must be set to 0 otherwise an error is triggered and the error code **[Safety function fault] 5 A F F** is displayed

Testing and Adjusting the Configuration

When configuration is complete, test the SLS function to verify that it behaves as expected.

If an error is triggered with the error code **[Safety function fault] 5 R F F**, apply the following troubleshooting rules

Context	Drive Status	Adjustment
SLS activated and deceleration ramp in progress	<ul style="list-style-type: none"> SAFF error code SFFE.3 = 1 	<p>Motor frequency has reached the motor frequency limit threshold. The cause of the detected error can be due to frequency instability. Investigate and correct the cause. The value of SLtt can be modified to increase the tolerance threshold to the instability of the drive system.</p>
SLS activated and end of ramp at SLSP frequency	<ul style="list-style-type: none"> SAFF error code SFFE.3 = 1 or SFFE.7 = 1 	<p>Motor frequency stabilization at SLSP takes too long and has reached the safety function error detection condition.</p>  <p>①: Safety function error detection, Tosc: T oscillation, F: Frequency The oscillations must be lower than SLtt before the time T(oscillation) elapses. If the condition is not followed, an error is triggered and the error code [Safety function fault] 5 R F F is displayed The relationship between SSSt and T(oscillation) is: $T(\text{osc}) = \frac{SSTT - (SLTT - SLSP - F_{\text{slip}})}{SSRT \times SSRU}$</p> <p>Motor frequency has reached the motor frequency limit threshold. The cause of the detected error can be due to frequency instability. Investigate and correct the cause. The value of SSSt can be modified to increase the tolerance threshold to the oscillations of the drive system.</p>
SLS activated and motor running at SLSP frequency	<ul style="list-style-type: none"> SAFF error code SFFE.7 = 1 	<p>Motor frequency has reached the motor frequency limit threshold. The cause of the detected error can be due to frequency instability. Investigate and correct the cause. The value of SLtt can be modified to increase the tolerance threshold to the instability of the drive system.</p>

Example

Code	Description	Unit
<i>F r S</i>	Rated motor frequency	50 Hz
<i>n S P</i>	Rated motor speed	1350 rpm
ppn	Motor pole pair number	2
Max Frequency	Maximum motor frequency on normal operation. This value is equal to [High speed] <i>H S P</i> or lower	50 Hz
Fsetpoint(SLS)	Motor frequency setpoint	15 Hz
SS1 deceleration ramp	Deceleration ramp to apply when SS1 is triggered	20 Hz/s

With these numerical values, the configuration of SLS type 2, 3, and 4 is:

$$F_{slip} = 50 - \frac{1350 \times 2}{60} = 5 \text{ Hz}$$

$$SSSL = F_{slip} = 5 \text{ Hz}$$

$$SSrU = 1 \text{ Hz/s} \text{ and } SSrt = 20.0 \text{ for } SS1 \text{ deceleration ramp} = 20 \text{ Hz/s (accuracy is 0.1 Hz)}$$

$$SLSP = Fsetpoint(SLS) = 15 \text{ Hz}$$

$$SLtt = 1.2 \times SLSP + F_{slip} = 1.2 \times 15 + 5 = 23 \text{ Hz}$$

$$SStt = 0.2 \times \text{Max Frequency} = 0.2 * 50 = 10 \text{ Hz}$$

$$T(\text{oscillation}) = \frac{SSSI - (SLtt - SLSP - F_{slip})}{SSrt \times SSrU} = \frac{10 - (23 - 15 - 5)}{20 \times 1} = 350 \text{ ms}$$

In this example, the frequency oscillations are allowed to be higher than SLtt for 350 ms.

SS1

Collect Application Data

Before configuring the SS1 function, you must collect the following data:

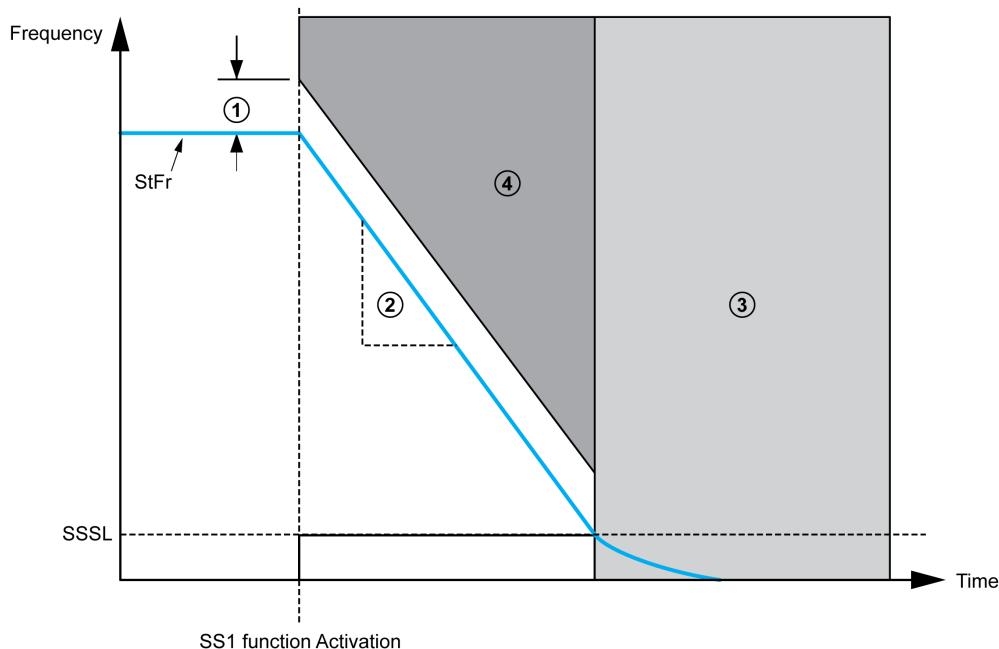
Code	Description	Unit	Comment
<i>F r S</i>	Rated motor frequency	Hz	From motor
<i>n S P</i>	Rated motor speed	rpm	From motor
ppn	Motor pole pair number	–	From motor
Max Frequency	Maximum motor frequency on normal operation	Hz	This value is equal to [High speed] <i>H S P</i> or lower

Calculate the rated motor slip frequency Fslip (Hz).

$$F_{slip} = FrS - \frac{N_{sp} \times ppn}{60}$$

To Configure the Function

Overview of diagram



① : SS1 trip threshold, ② : SS1 deceleration ramp (dV/dT), ③ : STO function triggered, ④ : Error and STO function triggered

Standstill Level

The recommended standstill level is: $SSSL = F_{slip}$

If the application requires a different standstill level, it can be set accordingly with the SSSL parameter.

Ramp Value and Ramp Unit

Set SSrt (ramp value) and SSru (ramp unit) parameters according to the deceleration ramp to apply when the safety function SS1 is triggered.

Ramp Calculation: Ramp = SSru * SSrt

Example 1: If SSru = 1 Hz/s and SSrt = 500.0 the deceleration ramp is 500.0 Hz/s and the accuracy is 0.1 Hz

Example 2: If SSru = 10 Hz/s and SSrt = 50.0 the deceleration ramp is 500 Hz/s and the accuracy is 1 Hz

Use the table to set the correct accuracy according to the deceleration ramp to apply when the safety function SS1 is triggered:

Min	Max	Accuracy	SSru	SSrt
0.1 Hz/s	599 Hz/s	0.1 Hz/s	1 Hz/s	SS1 deceleration ramp
599 Hz/s	5990 Hz/s	1 Hz/s	10 Hz/s	SS1 deceleration ramp/10
5990 Hz/s	59900 Hz/s	10 Hz/s	100 Hz/s	SS1 deceleration ramp/100

Ramp Limit Threshold

The SS1 ramp trip threshold is calculated by: $SStt = 0.2 \times \text{Max Frequency}$

This value is equal to [High speed] HSP or lower

Testing and Adjusting the Configuration

When configuration is complete, test the safety function SS1 to verify that it behaves as expected.

If an error is triggered with the error code **[Safety function fault] 5 F F F**, apply the following troubleshooting rules

Context	Drive Status	Adjustment
SS1 activated and the [Standstill level] 5 S L has not yet been reached	<ul style="list-style-type: none">SAFF error codeSFFE.3 = 1	<p>Motor frequency has reached the motor frequency limit threshold.</p> <p>The cause of the detected error can be due to frequency instability. Investigate and correct the cause. The value of SS1t can be modified to increase the tolerance threshold to the instability of the drive system.</p>

Example

Code	Description	Unit
F r 5	Rated motor frequency	50 Hz
n S P	Rated motor speed	1350 rpm
ppn	Motor pole pair number	2
Max Frequency	Maximum motor frequency on normal operation	50 Hz
SS1 deceleration ramp	Deceleration ramp to apply when SS1 is triggered	20 Hz/s

With these numerical values, the configuration of SS1 is:

$$F_{slip} = 50 - \frac{1350 \times 2}{60} = 5 \text{ Hz}$$

$$SSSL = F_{slip} = 5 \text{ Hz}$$

$$SSrU = 1 \text{ Hz/s} \text{ and } SSrt = 20.0 \text{ for SS1 deceleration ramp} = 20 \text{ Hz/s (accuracy is 0.1 Hz)}$$

$$SS1t = 0.2 \times \text{Max Frequency} = 0.2 \times 50 = 10 \text{ Hz}$$

SMS

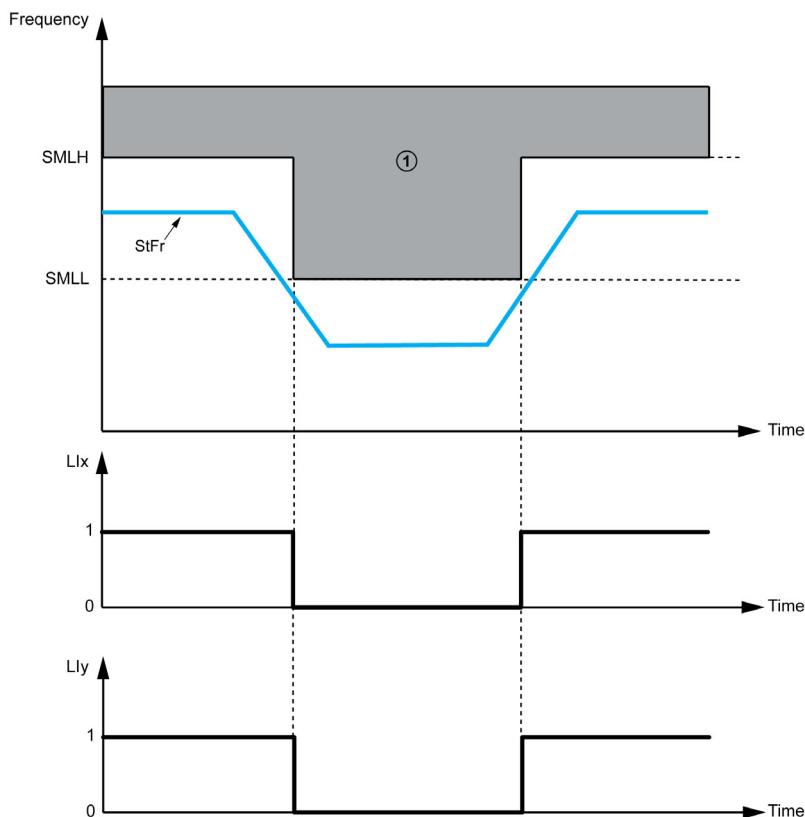
Collect Application Data

Before starting to configure the SMS function, you must collect the following data:

Code	Description	Unit	Comment
PPn	Motor pole pair number	-	See motor nameplate

Max output frequency in Hz = ((Max velocity in rpm)/60)* PPn

To Configure the Function



① Error and STO function triggered

SMLL > Max output frequency

SMLH > Max output frequency

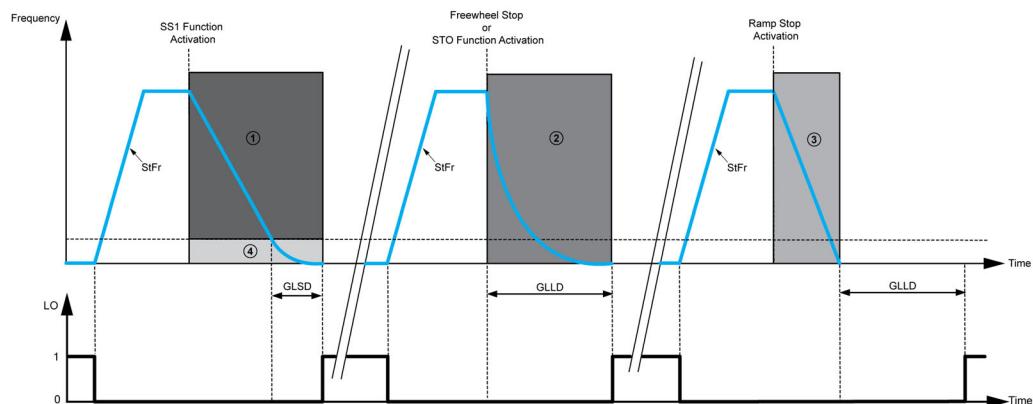
GDL

Collect Application Data

Before starting to configure the GDL function, you must collect the following data:

Code	Description	Unit	Comment
G L S d	[GDL Short Delay]	s	Maximum delay after SS1 ramp to stop the machine.
G L L d	[GDL Long Delay]	s	Maximum delay after STO function activation or normal deceleration ramp command to stop the machine.

To Configure the Function



① SS1 stop, ② Freewheel stop, ③ Ramp stop, ④ STO function triggered

Testing and Adjusting the Configuration

When GDL configuration is complete

- Activate safety function SS1 and verify that digital output changes to high state (1) when the machine is stopped.
- Activate safety function STO and verify that the digital output changes to high state (1) when the machine is stopped.

Chapter 4

Behavior of Safety Functions

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Limitations	52
Detected Fault Inhibition	53
Priority Between Safety Functions	53
Factory Settings	53
Configuration Download	53
Priority Between Safety Functions and No Safety-Related Functions	54
Monitoring of The Stator Frequency Consistency	57

Limitations

Type of Motor

The safety function STO and GDL (long delay) can be used for synchronous and asynchronous motors. On ATV320, the safety functions SLS, SS1, SMS and GDL (short delay) are only applicable for asynchronous motors. For the possible [Motor Control Type] *L E E* settings, refer to the Priority Table (see page 54).

Prerequisites for Using Safety Functions

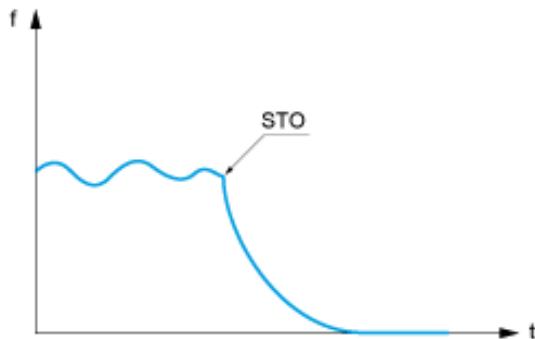
Following conditions have to be fulfilled for correct operation:

- 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 line supply, sequence, motor, and application and is not at the limit of their capacities as stated in the catalog.
- If required, the appropriate options are used.
Example: dynamic braking resistor or motor choke.
- 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.
- The maximum output frequency is 200 Hz.

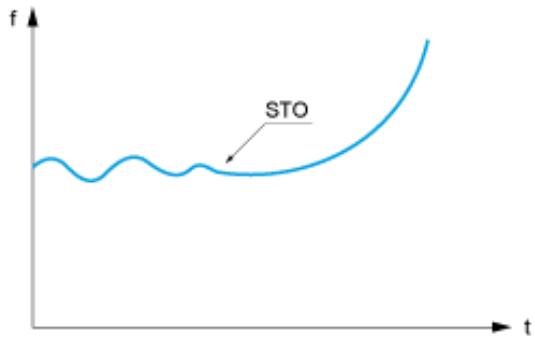
Allowed and Unallowed Application for Safety Function

Applications with acceleration of the load after disabling the output power bridge are not allowed (for example, applications with long/permanent regenerative braking cycles).

Typical allowed application



Typical unallowed application



Examples: Vertical Conveyors, Vertical hoist, Lifts, or Winders.

Requirements on Digital Inputs

- Sink mode is not used with the safety function. If you use the safety function, you need to wire the digital inputs in source mode.
- PTC on DI6 is incompatible with the safety function set on this input. If you are using the safety function on DI6, do not set the PTC switch to PTC
- If you are using the pulse input, you cannot set the safety function on DI5 at the same time.
- If an output signal switching device (OSSD) is used with ATV320, the outputs of the device can only be wired to DI3/DI4 or DI5/DI6 if [DI response time] *L r E* is set to a value higher than 1 ms. STO/DI3 cannot be wired to OSSD outputs.

Detected Fault Inhibition

When a safety function has been configured, the error **[Safety Function Fault] S F F** cannot be inhibited by the function **[Fault Inhibit assign.] , n H**

Priority Between Safety Functions

1. The safety function STO has the highest priority. If the safety function STO is triggered, a Safe Torque Off is performed regardless of which other functions are active.
2. The safety function SS1 has medium priority in relation to the other safety functions.
3. The safety function SLS and GDL has the lowest priority.

Factory Settings

If the safety functions are configured and you restore the factory settings, only the parameters which are not safety-related will be reset to the factory setting. The settings of safety-related parameters can only be reset using the commissioning software, for more information see Commissioning (*see page 91*).

Configuration Download

You can transfer a configuration in all situations. If a safety function has been configured, the functions using these same digital inputs will not be configured.

For example: If the downloaded configuration has functions (Preset speed,...) on DI3-4-5-6 and if the drive has a safety function configured on these digital inputs, safety function will not be erased. It is the functions that have the same digital input as safety functions that are not transferred. Multiconfiguration/multimotor and macro configuration obey the same rules.

Priority Between Safety Functions and No Safety-Related Functions

Priority Table

o: Compatible functions

x: Incompatible functions

↑ ⇌: The function indicated by the arrow has priority over the other.

Drive Function	SLS	SS1	STO	SMS	GDL
[HIGH SPEED HOISTING] H S H -	↑	↑	↑	↑	o
[+/- SPEED] u P d -	↑	↑	↑	↑	o
[Skip Frequency] J P F	↑	o	o	↑	o
[Low speed time out] L L S	o	o	↑	o	o
[MULTIMOTORS] M M L -	Configuration must be consistent with the 3 motors			o	Configuration must be consistent with the 3 motors
[PRESET SPEEDS] P S S -	↑	o	↑	↑	o
[PID REGULATOR] P r d -	↑	o	o	↑	o
[RAMP] r P E - profile	↑	↑	↑	o	o
[Freewheel stop ass.] n S E	⇒	⇒	↑	o	o
[Fast stop assign.] F S E	↑: SLS ramp ⇒: SLS steady	↑	↑	o	o
[TRAVERSE CONTROL] E r D -	↑	↑	↑	↑	o
[EXTERNAL FAULT] E E F -	⇒: NST x: DCI ↑: fast, ramp, fallback, maintain	⇒: NST x: DCI ↑: fast, ramp, fallback, maintain	⇒: NST ↑: DCI ↑: fast, ramp, fallback, maintain	⇒: NST x: DCI ↑: fast, ramp, fallback, maintain	o
[AUTOMATIC RESTART] R E r -	↑	↑	↑	↑	o
[FAULT RESET] r S E -	↑	↑	↑	↑	o
[JOG] J o G -	↑	↑	↑	↑	o
[STOP CONFIGURATION] S E E -					
[Ramp stop] r P P	↑: SLS ramp ⇒: SLS steady	↑	↑	↑	o
[Fast stop] F S E	↑: SLS ramp ⇒: SLS steady	↑	↑	⇒	o
[DC injection] d C i	x	x	↑	x	o
[+/-SPEED AROUND REF.] S r E -	↑	↑	↑	↑	o
[POSITIONING BY SENSORS] L P o -	↑: SLS ramp & position is not respected	↑: Position is not respected	↑	↑	o
[RP input] P F r C	o: if the safety function is not assigned to DI5	o: if the safety function is not assigned to DI5	o: if the safety function is not assigned to DI5	o: if the safety function is not assigned to DI5	o
[Underload Detection] u L F	↑	↑	↑	↑	o

Drive Function	SLS	SS1	STO	SMS	GDL
[Overload Detection] $\square L C$	↑	↑	↑	↑	o
[Rope slack config.] $r S d$	x	x	x	x	o
[UnderV. prevention] $S t P$	x	x	↑	↑	o
[AUTO DC INJECTION] $R d C -$	x	x	↑	x	o
[DC injection assign.] $d C i$	x	x	↑	x	o
[Load sharing] $L b R$	o: If the [Stator Frequency] $S t F r$ is above the frequency limit threshold, the error SAFF is triggered.		↑	↑	↑
[Motor control type] $C E E$					
[Standard] $S t d$	x	x	o	x	o
[SVC V] $u u C$	o	o	o	o	o
[V/F Quad.] $u F q$	x	x	o	x	o
[Energy Sav.] $n L d$	x	x	o	x	o
[Sync. mot.] $S y n$	x	x	o	x	o: long delay x: short delay
[V/F 5pts] $u F s$	x	x	o	x	
[OUTPUT PHASE LOSS] $\square P L$	x: Motor output phase loss is detected by the safety function		o	x: Motor output phase loss is detected by the safety function	
[Output cut] $\square R C$	x	x	x	x	o
[Dec ramp adapt.] $b r R$	o: If the [Stator Frequency] $S t F r$ is above the Frequency limit threshold, the error SAFF is triggered.		↑	o	o
[REF. OPERATIONS] $\square R i -$	↑	↑	o	↑	o
[2 wire] $z C$	o: Run command on transition ↑ Run command on level is not compatible		o: Run command on transition ↑ Run command on level is not compatible	o: Run command on transition ↑ Run command on level is not compatible	o: Run command on transition ↑ Run command on level is not compatible
[PTC MANAGEMENT] $P t C -$	o: inactive if the safety function is not assigned to DI6		o: inactive if the safety function is not assigned to DI6	o: inactive if the safety function is not assigned to DI6	o: inactive if the safety function is not assigned to DI6
[FORCED LOCAL] $L C F -$	↑	↑	o	↑	o
[LI CONFIGURATION]	o: inactive if the safety function is assigned to digital input		o: inactive if the safety function is assigned to digital input	o: inactive if the safety function is assigned to digital input	o: inactive if the safety function is assigned to digital input

Drive Function	SLS	SS1	STO	SMS	GDL
[MULTIMOTORS/CONFIG] ΠΠC -	o: except safety-related parameters	o			
[FAULT INHIBITION] ,nH	x	x	x	x	o
[Profile] C H C F	Digital input used by safety function cannot be switched	Digital input used by safety function cannot be switched	Digital input used by safety function cannot be switched	Digital input used by safety function cannot be switched	o
[Macro configuration] C F G	↑: Macro configuration could be overlapped if safety function use a digital input requested by the macro configuration	↑: Macro configuration could be overlapped if safety function use a digital input requested by the macro configuration	↑: Macro configuration could be overlapped if safety function use a digital input requested by the macro configuration	↑: Macro configuration could be overlapped if safety function use a digital input requested by the macro configuration	o
[Motor short circuit] 5 C F I	↑	↑	o	↑	o
[Ground short circuit] 5 C F 3	↑	↑	o	↑	o
[Overspeed] 5 o F	↑	↑	o	↑	o
[Sync. mot.] 5 Y n	x	x	o	x	o
[Configuration Transfer]	o: except safety-related parameters	o: except safety-related parameters			
[Energy Sav.] n L d	x	x	o	x	o

For more information about these functions, see Programming manual.

Monitoring of The Stator Frequency Consistency

Description

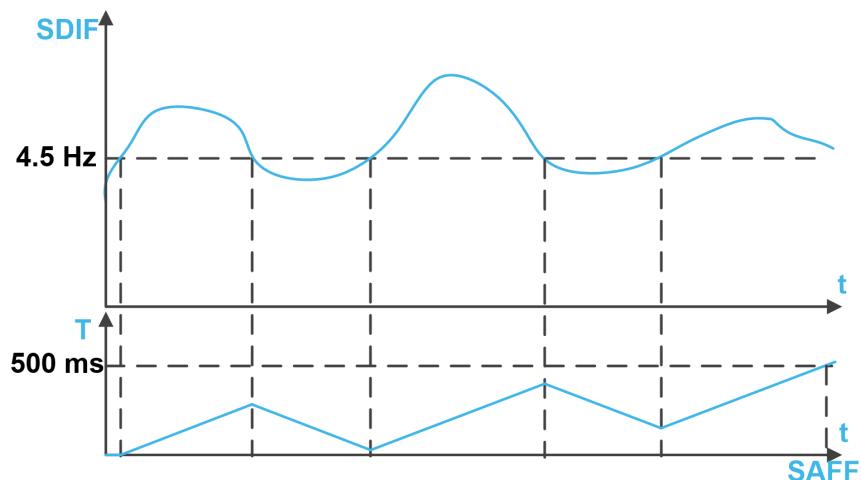
If at least one of the safety function SS1, SLS and SMS is configured, the drive monitors the difference between the estimated stator frequency and the internal computed stator frequency, in order to control the consistency.

If this frequency difference, displayed by the parameter **5 d , F**, reaches 4.5 Hz (absolute value), an internal timer is activated.

While the difference remains higher than 4.5 Hz, the timer increases.

If the difference decreases below 4.5 Hz, the timer decreases (the timer is not reset).

If the timer reaches 500 ms, a **5 AFF F** error is triggered and the bit 0 of the **5 AFF Z** register is raised.



NOTE: The parameter **5 d , F** can be displayed on the scope of the DTM. **5 d , F** displays 0 Hz if SS1, SLS and SMS are not configured..

Remedies

Verify the settings of the drive such as, the acceleration (**A C C**), the deceleration (**d E C**), the motor nameplate, the autotuning, etc.

Verify the configuration of the motor control parameters in order to reduce the oscillations of **5 d , F** value.

If this error is triggered without running the motor, an internal hardware error is the probable cause. Contact your local Schneider Electric representative.

Chapter 5

Safety Functions Visualization via HMI

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Status of Safety Functions	60
Dedicated HMI	60
Error Code Description	61

Status of Safety Functions

Description

The status of the safety functions can be displayed using the HMI of the drive or using the commissioning software. HMI of the drive can be the local HMI on the product or the graphic display terminal or the remote display terminal. There is one register for each safety function. See introduction ([see page 16](#)) for more information about the safety functions.

To access these registers with an HMI: [2 MONITORING] $\pi \alpha n - \rightarrow$ [MONIT. SAFETY] $S A F -$

- **[STO status]** $S E \alpha S$: Status of the safety function STO (Safe Torque Off)
- **[SLS status]** $S L S S$: Status of the safety function SLS (Safely-Limited Speed)
- **[SS1 status]** $S S 1 S$: Status of the safety function SS1 (Safe Stop 1)
- **[SMS status]** $S M S S$: Status of the safety function SMS (Safe Maximum Speed)
- **[GDL status]** $G D L S$: Status of the safety function GDL (Guard Door Locking)

The status registers are not approved for any type of safety-related use.

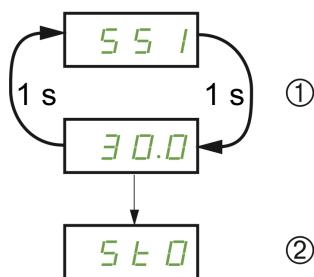
For more information about these registers, see ATV320 Visualization and Status of Safety Functions ([see page 98](#)) on www.schneider-electric.com.

Dedicated HMI

Description

When a safety function has been triggered, some information is displayed.

Example with the local HMI of the product when the safety function SS1 has been triggered:



①: Display alternately the name of the safety function SS1 and the current display parameter as long as the motor decelerates according to the specified monitoring ramp until standstill is reached, ② After the **[Standstill level]** $S S S L$ has been reached, the safety function STO is triggered and displayed

Error Code Description

Description

When an error is detected by the safety function, the drive displays **[Safety function fault] (S F F F)**. This detected error can only be reset after powering the drive OFF/ON.

for more information, you can access to the registers to find out the possible reasons for triggering.

These registers can be displayed using the graphic display terminal or the commissioning software:

[DRIVE MENU] --> [MONITORING] --> [DIAGNOSTICS] --> [MORE FAULT INFO]

S F F E [Safety Function Error Register]

Bit	Description
Bit0=1	Digital inputs debounce time-out (verify value of debounce time LIDT according to the application)
Bit1	Reserved
Bit2=1	Motor speed sign has changed during SS1 ramp
Bit3=1	Motor speed has reached the frequency limit threshold during SS1 ramp.
Bit4	Reserved
Bit5	Reserved
Bit6=1	Motor speed sign has changed during SLS limitation
Bit7=1	Motor speed has reached the frequency limit threshold during SLS.
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13=1	Not possible to measure the motor speed (verify the motor wiring connection)
Bit14=1	Motor ground short-circuit detected (verify the motor wiring connection)
Bit15=1	Motor phase to phase short-circuit detected (verify the motor wiring connection)

This register is reset after powering OFF/ON.

This register can also be accessed from **[DRIVE MENU] --> [MONITORING] --> [MONIT. SAFETY]**

5 F F 1 [Safety Fault Register 1]

This is an application control error register.

Bit	Description
Bit0=1	PWRM consistency detected error
Bit1=1	Safety functions parameters detected error
Bit2=1	Application auto test has detected an error
Bit3=1	Diagnostic verification of safety function has detected an error
Bit4=1	Digital input diagnostic has detected an error
Bit5=1	SMS or GDL safety function detected error, for details refer 5 F D 4 [Safety Fault Subregister 04] (see page 65).
Bit6=1	Application watchdog management active
Bit7=1	Motor control detected error
Bit8=1	Internal serial link core detected error
Bit9=1	Digital input activation detected error
Bit10=1	Safe Torque Off function has triggered an error
Bit11=1	Application interface has detected an error of the safety functions
Bit12=1	Safe Stop 1 function has detected an error of the safety functions
Bit13=1	Safely Limited Speed function has triggered an error
Bit14=1	Motor data is corrupted
Bit15=1	Internal serial link data flow detected error

This register is reset after powering OFF/ON.

5 F F 2 [Safety Fault Register 2]

This is a motor control error register.

Bit	Description
Bit0=1	Consistency stator frequency verification has detected an error (see page 57).
Bit1=1	Stator frequency estimation detected error
Bit2=1	Motor control watchdog management is active
Bit3=1	Motor control hardware watchdog is active
Bit4=1	Motor control auto test has detected an error
Bit5=1	Chain testing detected error
Bit6=1	Internal serial link core detected error
Bit7=1	Direct short-circuit detected error
Bit8=1	PWM driver detected error
Bit9=1	GDL safety function internal error
Bit10	Reserved
Bit11=1	Application interface has detected an error of the safety functions
Bit12	Reserved
Bit13	Reserved
Bit14=1	Motor data is corrupted
Bit15=1	Internal serial link data flow detected error

This register is reset after powering OFF/ON.

S F D 0 [Safety Fault Subregister 00]

This is an application auto test error register.

Bit	Description
Bit0	Reserved
Bit1=1	Ram stack overflow
Bit2=1	Ram address integrity detected error
Bit3=1	Ram data access detected error
Bit4=1	Flash checksum detected error
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9=1	Fast task overflow
Bit10=1	Slow task overflow
Bit11=1	Application task overflow
Bit12	Reserved
Bit13	Reserved
Bit14=1	PWRM line is not activated during initialization phase
Bit15=1	Application hardware watchdog is not running after initialization

This register is reset after powering OFF/ON.

S F D 1 [Safety Fault Subregister 01]

This is a digital input diagnostics error register

Bit	Description
Bit0=1	Management - state machine detected error
Bit1=1	Data required for test management are corrupted
Bit2=1	Channel selection detected error
Bit3=1	Testing - state machine detected error
Bit4=1	Test request is corrupted
Bit5=1	Pointer to test method is corrupted
Bit6=1	Incorrect test action provided
Bit7=1	Detected error in results collecting
Bit8=1	DI3 detected error. Cannot activate safety function
Bit9=1	DI4 detected error. Cannot activate safety function
Bit10=1	DI5 detected error. Cannot activate safety function
Bit11=1	DI6 is detected error. Cannot activate safety function
Bit12=1	Test sequence updated while a diagnostic is in progress
Bit13=1	Detected error in test pattern management
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 2 [Safety Fault Subregister 02]

This is an application watchdog management detected error register.

Bit	Description
Bit0=1	Fast task detected error
Bit1=1	Slow task detected error
Bit2=1	Application task detected error
Bit3=1	Background task detected error
Bit4=1	Safety function fast task/input detected error
Bit5=1	Safety function slow task/input detected error
Bit6=1	Safety function application task/inputs detected error
Bit7=1	Safety function application task/treatment detected error
Bit8=1	Safety function background task detected error
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 3 [Safety Fault Subregister 03]

Bit	Description
Bit0=1	Debounce time out
Bit1=1	Input not consistent
Bit2=1	Consistency verification - state machine detected error
Bit3=1	Consistency verification - debounce timeout corrupted
Bit4=1	Response time data detected error
Bit5=1	Response time corrupted
Bit6=1	Undefined consumer queried
Bit7=1	Configuration detected error
Bit8=1	Inputs are not in nominal mode
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

5 F 0 4 [Safety Fault Subregister 04]

This is a [Safe Torque Off] 5 E 0 detected error register

Bit	Description
Bit0=1	No signal configured
Bit1=1	State machine detected error
Bit2=1	Internal data detected error
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8=1	SMS overspeed detected error
Bit9=1	SMS internal detected error
Bit10	Reserved
Bit11	Reserved
Bit12=1	GDL internal detected error 1
Bit13=1	GDL internal detected error 2
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

5 F 0 5 [Safety Fault Subregister 05]

This is a [Safe Stop 1] 5 S 1 detected error register

Bit	Description
Bit0=1	State machine detected error
Bit1=1	Motor speed sign has changed during stop
Bit2=1	Motor speed has reached the frequency limit threshold.
Bit3=1	Theoretical motor speed corrupted
Bit4=1	Unauthorized configuration
Bit5=1	Theoretical motor speed computation detected error
Bit6	Reserved
Bit7=1	Speed sign verification: consistency detected error
Bit8=1	Internal SS1 request corrupted
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 6 [Safety Fault Subregister 06]

This is a **[Safely Limited Speed] S L S** detected error register

Bit	Description
Bit0=1	State machine detected error
Bit1=1	Motor speed sign changed during limitation
Bit2=1	Motor speed has reached the frequency limit threshold
Bit3=1	Data corruption
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 7 [Safety Fault Subregister 07]

This is an application watchdog management detected error register.

Bit	Description
Bit0	Reserved
Bit1	Reserved
Bit2	Reserved
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 8 [Safety Fault Subregister 08]

This is an application watchdog management detected error register

Bit	Description
Bit0=1	PWM task detected error
Bit1=1	Fixed task detected error
Bit2=1	ATMC watchdog detected error
Bit3=1	DYNFCT watchdog detected error
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

S F D 9 Safety Fault Subregister 09

This is a motor control auto test detected error register.

Bit	Description
Bit0	Reserved
Bit1=1	Ram stack overflow
Bit2=1	Ram address integrity detected error
Bit3=1	Ram data access detected error
Bit4=1	Flash checksum error
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9=1	1 ms task overflow
Bit10=1	PWM task overflow
Bit11=1	Fixed task overflow
Bit12	Reserved
Bit13	Reserved
Bit14=1	Unwanted interruption
Bit15=1	Hardware WD is not running after initialization

This register is reset after powering OFF/ON.

5F 10 [Safety Fault Subregister 10]

This is a motor control direct short-circuit detected error register

Bit	Description
Bit0=1	Ground short circuit - configuration detected error
Bit1=1	Phase to phase short circuit - configuration detected error
Bit2=1	Ground short circuit
Bit3=1	Phase to phase short circuit
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

5F 11 [Safety Fault Subregister 11]

This is a motor control dynamic verification of activity detected error register

Bit	Description
Bit0=1	Application requested a diagnostic of direct short-circuit
Bit1=1	Application requested consistency verification of stator frequency estimation (voltage and current)
Bit2=1	Application requested diagnostic of SpdStat provided by motor control
Bit3	Reserved
Bit4	Reserved
Bit5	Reserved
Bit6	Reserved
Bit7	Reserved
Bit8=1	Motor control diagnostic of direct short circuit is enabled
Bit9=1	Motor control consistency verification of stator frequency estimation is enabled
Bit10=1	Motor control diagnostic of SpdStat provided by motor control is enabled
Bit11	Reserved
Bit12	Reserved
Bit13	Reserved
Bit14	Reserved
Bit15	Reserved

This register is reset after powering OFF/ON.

Chapter 6

Technical Data

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Electrical Data	70
Getting and Operating the Safety Function	71
Safety Function Capability	72
Debounce Time and Response Time	75

Electrical Data

Logic Type

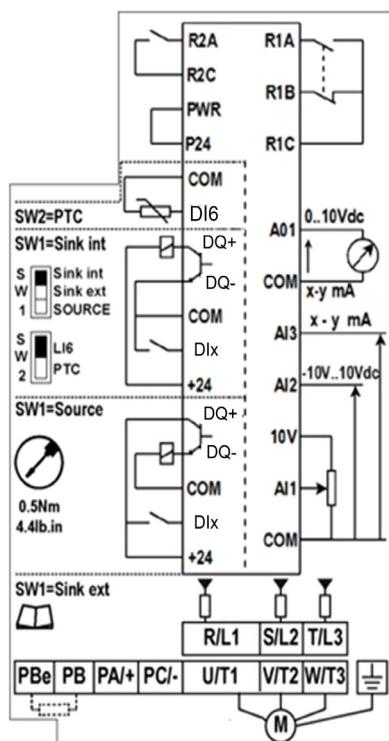
The drive digital inputs and digital outputs can be wired for logic type 1 or logic type 2.

Logic Type	Active State
1	The output draws current (Sink) Current flows to the input
2	The output supply flows from the input current Current (Source)

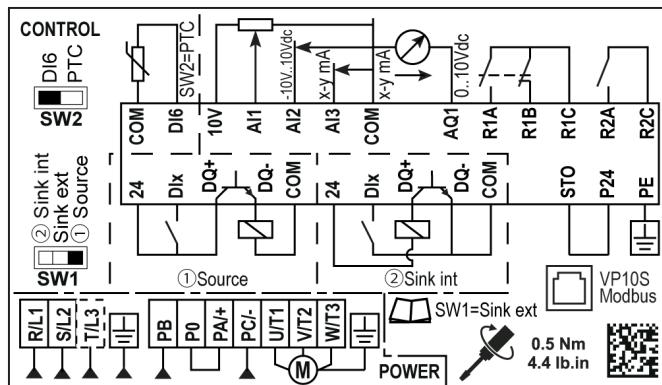
Safety functions must only be used in source mode.

Signal inputs are protected against reverse polarity, outputs are protected against short-circuits. The inputs and outputs are galvanically isolated.

ATV320B Cabling Label



ATV320C Cabling Label



Getting and Operating the Safety Function

Digital Input

General-purpose digital inputs can be used to trigger a safety function. Digital inputs have to be combined in pairs to obtain a redundant request. There are only 4 general-purpose digital inputs that can be linked to safety functions (DI3, DI4, DI5, DI6). The pairs of digital inputs are fixed and are:

- DI3 and DI4
- DI5 and DI6
- Another combination is only possible for the STO function: DI3 and STO

Pairs of digital inputs can only be assigned once when they are linked to a safety function. When you set a safety function on an digital input you cannot set another function (safety or other) on this digital input. If you set a non-safety function on an digital input you cannot set a safety function on this digital input.

The SISTEMA Software

The SISTEMA software allows machine developers and testers of safety-related machine controls to evaluate the safety standard or level of their machine in the context of IEC 13849-1. The tool allows you to model the structure of safety-related control components based on the designated architectures, allowing automated calculation of the reliability standards with various levels of detail, including that of the Performance Level (PL).

The ATV320 Libraries are available from www.schneider-electric.com.

Preventa Safety Relays

Used for the creation of complex safety functions in machines, allowing management of the I/O, and also for protecting both the operator and the machine.

The Preventa range of products feature microprocessor-based technology using the redundancy principle, and are essential to ensure safe operation of dangerous machinery.

Input Signal Safety Functions

Input signals safety functions	Units	Value for DI3 to DI6	Value for STO
Logic 0 (Ulow)	V	< 5	< 2
Logic 1 (Uhigh)	V	> 11	> 17
Impedance (24V)	kΩ	3.5	1.5
Debounce time	ms	< 1	< 1
Response time of safety function	ms	< 10	< 10

Summary of the Reliability Study

Function	Standard	STO input	STO input & DI3	DI3 & DI4 or DI5 & DI6
STO SS1 type C (With Preventa XPS ATE or XPS AV or equivalent) (3)	IEC 61508 Ed.2	SFF	96%	95%
		PFD _{10y}	8.10 ⁻⁴	5.10 ⁻⁴
		PFD _{1y}	8.10 ⁻⁵	5.10 ⁻⁵
		PFH _{equ_1y}	9 FIT (1)	6 FIT (1)
		Type	B	B
		HFT	1	0
		DC	92%	88%
		SIL capability	2	2
	IEC 62061 (2)	SIL CL capability	2	2
	IEC 60204-1	Category stop	0 for STO 1 for SS1 Type C	0 for STO 1 for SS1 Type C
SS1 type B SLS SMS	ISO 13849-1 (4)	PL	d	e
		Category	3	3
		MTTFd in years	14000	"L1" 3000 "L2" 31000
				4000
				90%
				4.10 ⁻³
				43 FIT (1)
				B
				0
				74%
	IEC 62061 (2)	SIL CL capability		2
	IEC 60204-1	Category stop		2
	ISO 13849-1 (4)	PL		1 for SS1 Type B
		Category		d
		MTTFd in years		3
				2000

Function	Standard		DQ	R1 and R2
GDL	IEC 61508 Ed.2	SFF	91%	94%
		PFD _{equ1y}	2.10 ²	2.10 ⁻²
		PFD _{equ10y}	2.10 ⁻³	2.10 ⁻³
		PFH	52 FIT(1)	37 FIT(1)
		Type	B	B
		HFT	0	0
		DC	72%	78%
		SIL capability	1	1
	IEC 62061 (2)	SIL CL capability	1	1
	ISO 13849-1 (4)	PL	c	c
		Category	2	2
	MTTFd in years		600	600

(1) FIT: Failure In Time = 10⁻⁹ failure per hour.

(2) Because the IEC 62061 standard concerns integration, this standard distinguishes the overall safety function (which is classified SIL2 or SIL3 for ATV320 according to diagrams Process system SF - Case 1 and Process system SF - Case 2, from components which constitute the safety function (which is classified SIL2 CL or SIL3 CL for ATV320).

(3) The SS1 Type C values are only given for the drive modules.

(4) According to EN 13849-1:2015.

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.

To avoid the use of a safety module, the Restart function parameters must be part of the safety function.

Please refer to the description of advantages of the safety module.

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 fitter or the integrator of the BDM (Basic Drive Module) has to do the system PL evaluation by including sensors data with numbers from the table above.

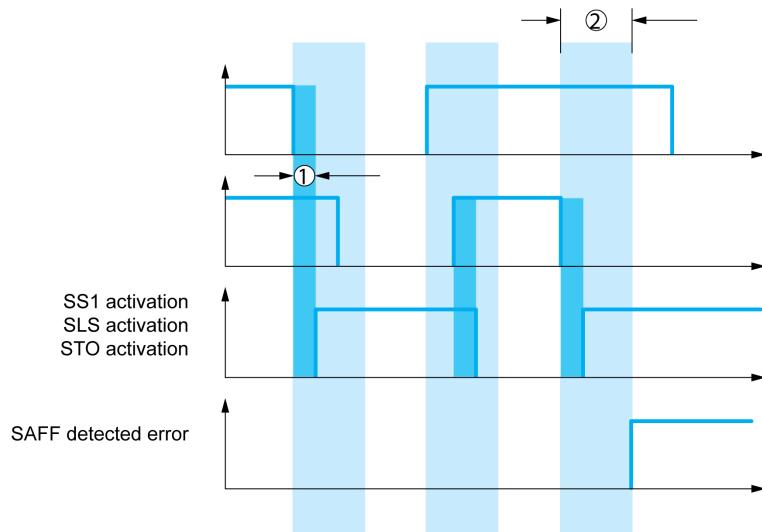
Debounce Time and Response Time

Description

On the ATV320 there are 2 parameters to configure digital inputs for safety function (DI3, DI4, DI5, DI6). The consistency of each pair of digital input is verified continuously.

[DI debounce time] L_{deb} : A logical state difference between DI3/DI4 or DI5/DI6 is allowed during debounce time, otherwise a detected error is activated.

[DI response time] L_{res} : The digital input response time manages the safety function activation shift.



① : Digital input Response Time

② : Digital input Debounce Time

Chapter 7

Certified Architectures

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Introduction	78
Multi-drive with the Safety Module Type Preventa XPS AF - Case 1	79
Multi-drive with the Safety Module Type Preventa XPS AF - Case 2	80
Multi-drive Without the Safety Module	81
Single Drive with the Safety Module Type Preventa XPS AV - Case 1	82
Single Drive with the Safety Module Type Preventa XPS AV - Case 2	83
Single Drive with the Safety Module Type Preventa XPS AF - Case 1	84
Single Drive with the Safety Module Type Preventa XPS AF - Case 2	85
Single Drive According to IEC 61508 and IEC 60204-1 - Case 1	86
Single Drive According to IEC 61508 and IEC 60204-1 - Case 2	87
Single Drive According to IEC 61508 and IEC 62061 with Safety Function GDL	88
Multi-drive Chaining According to IEC 61508 and IEC 62061 with Safety Function GDL	89

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:

- Multi-drive with the Safety module type Preventa XPS AF - Case 1
- Multi-drive with the Safety module type Preventa XPS AF - Case 2
- Multi-drive without the Safety module
- Single drive with the Safety module type Preventa XPS AV - Case 1
- Single drive with the Safety module type Preventa XPS AV - Case 2
- Single drive with the Safety module type Preventa XPS AF - Case 1
- Single drive with the Safety module type Preventa XPS AF - Case 2
- Single drive according to IEC 61508 and IEC 60204-1 - Case 1
- Single drive according to IEC 61508 and IEC 60204-1 - Case 2

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 (fault relay activation, error codes or information on the display, etc.) is not considered to be a safety-related data.

Multi-drive with the Safety Module Type Preventa XPS AF - Case 1

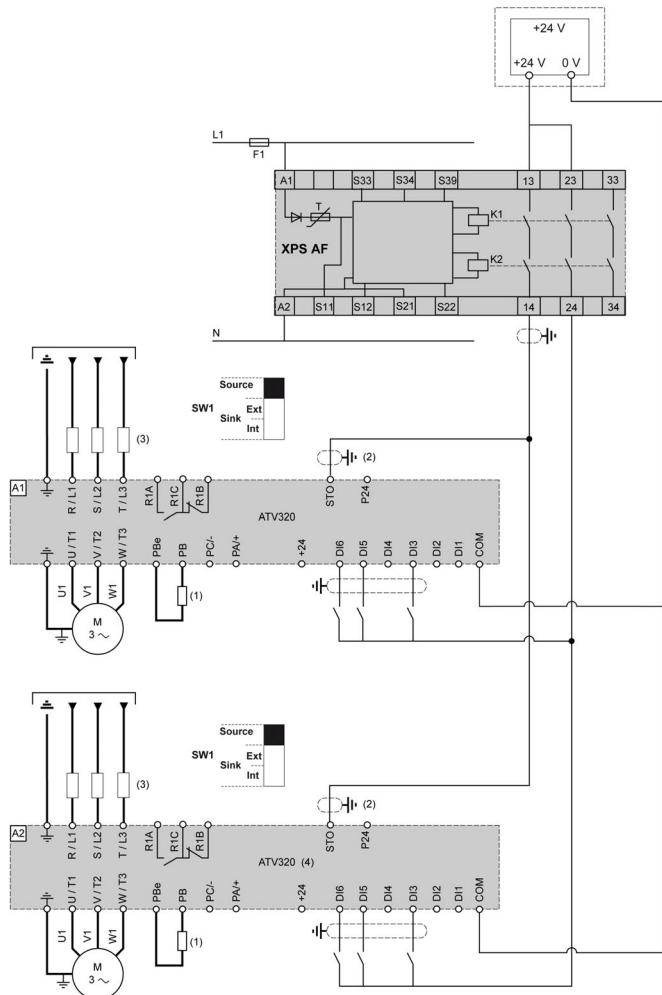
Multi-drive with the Safety Module Type Preventa XPS AF According to EN 954-1, IEC 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram:

- STO category 4, PL e/SIL3 Machine with Safety module type Preventa XPS AF or equivalent and DI3 set to STO
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI5/DI6

Or

- STO category 4, PL e/SIL3 Machine with Safety module type Preventa XPS AF or equivalent and DI3 set to STO
- DI4 and DI5/DI6 not set to a safety function



(1) Braking resistor, if used, (2) Cable and wiring following IEC60079-14. STO cables must be shielded and run apart from the supply cable. (3) Line choke, if used, (4) Multi-drives is possible with another drive (For Example: ATV71 with PWR connection or Lexium servo drives).

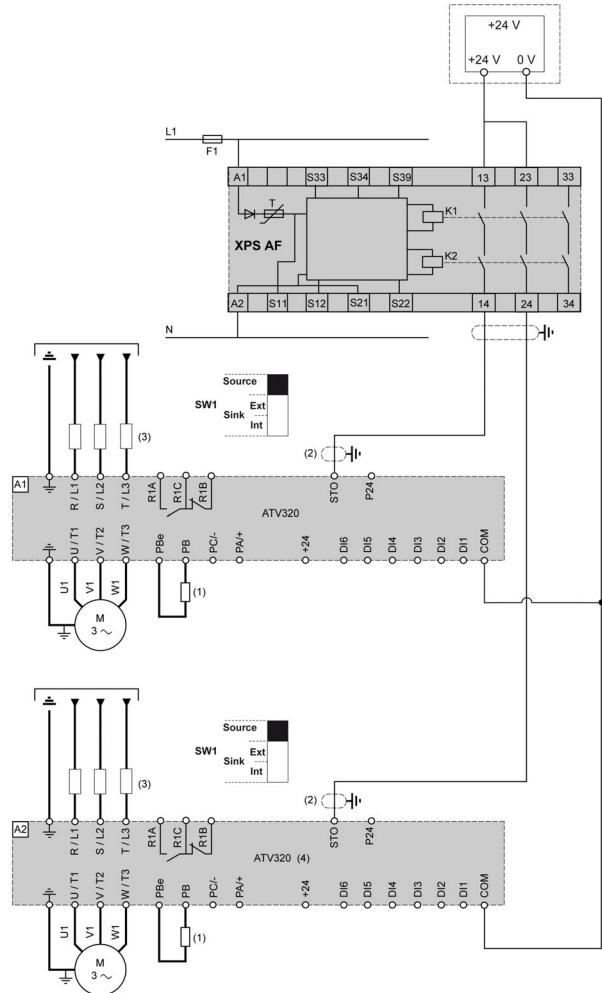
NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Multi-drive with the Safety Module Type Preventa XPS AF - Case 2

Multi-drive with the Safety Module Type Preventa XPS AF According to EN 954-1, IEC 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- STO category 3, PL d/SIL2 Machine with Safety module type Preventa XPS AF or equivalent
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI3/DI4 or DI5/DI6



(1) Braking resistor, if used, (2) Cable and wiring following IEC60079-14. STO cables must be shielded and run apart from the supply cable. (3) Line choke, if used, (4) Multi-drives is possible with another drive (For Example: ATV71 with PWR connection or Lexium servo drives).

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Multi-drive Without the Safety Module

Multi-drive Without the Safety Module Type Preventa XPS AF According to IEC 61508

The following configurations apply to the diagram below:

- STO SIL2 on STO
- SLS SIL2 or SS1 type B SIL2 on DI3/DI4 or DI5/DI6

Or

- STO SIL2 on STO
- SLS or SS1 type B on DI3/DI4
- DI5/DI6 not set to a safety function

Or

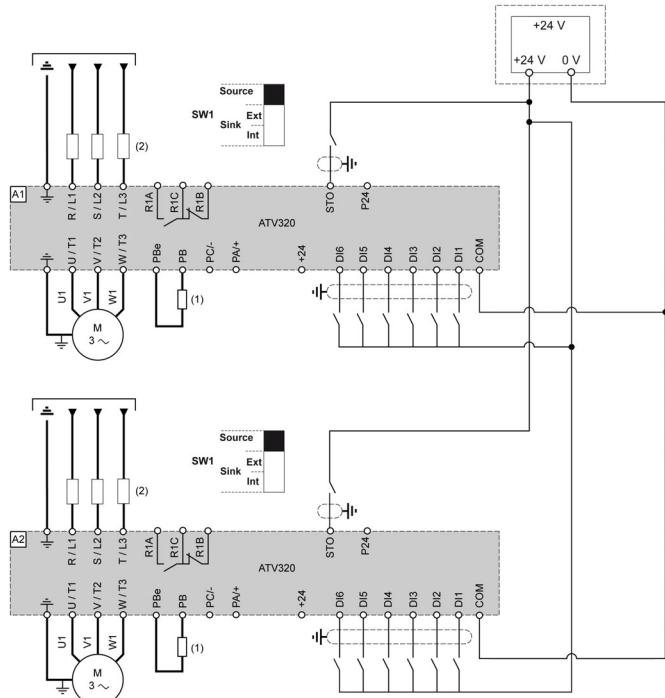
- STO SIL2 on STO
- DI3/DI4 and DI5/DI6 not set to a safety function

Or

- STO SIL3 on STO and DI3
- SLS SIL2 or SS1 type B SIL2 on DI5/DI6
- DI4 not set to a safety function

Or

- STO SIL3 on STO and DI3
- DI4 and DI5/DI6 not set to a safety function



(1) Braking resistor, if used, (2) Line chokes, if used.

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive with the Safety Module Type Preventa XPS AV - Case 1

Single Drive with the Safety Module Type Preventa XPS AV According to EN 954-1, IEC 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- SS1 type C category 3, PL d/SIL2 on STO with Safety module type Preventa XPS AV or equivalent

Or

- SS1 type C category 3, PL d/SIL2 on STO with Safety module type Preventa XPS AV or equivalent

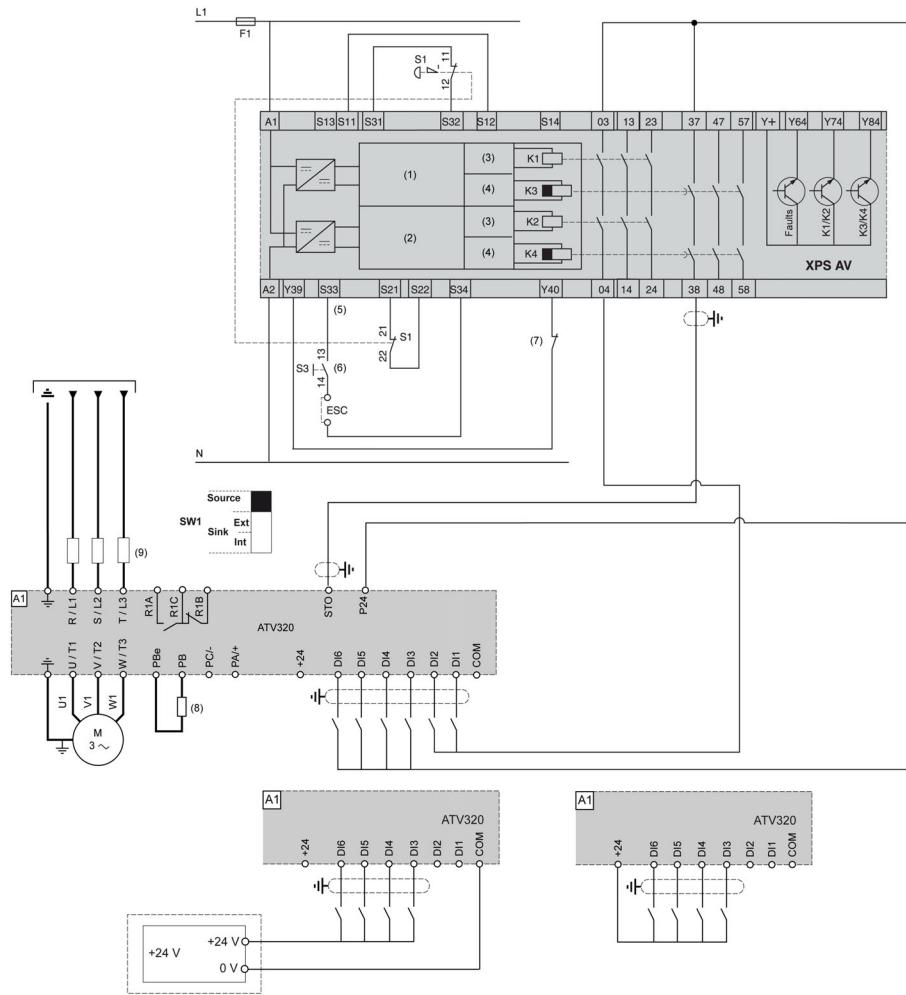
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI3/DI4

- DI5/DI6 not set to a safety function

Or

- SS1 type C category 3, PL d/SIL2 on STO and DI3 with Safety module type Preventa XPS AV or equivalent

- DI3/DI4 and DI5/DI6 not set to a safety function



(1) Channel 1 logic, (2) Channel 2 logic, (3) Output 1, (4) Output 2, (5) Emergency stop, (6) Start, (7) Time delay stop, (8) Braking resistor, if used, (9) Line chokes, if used

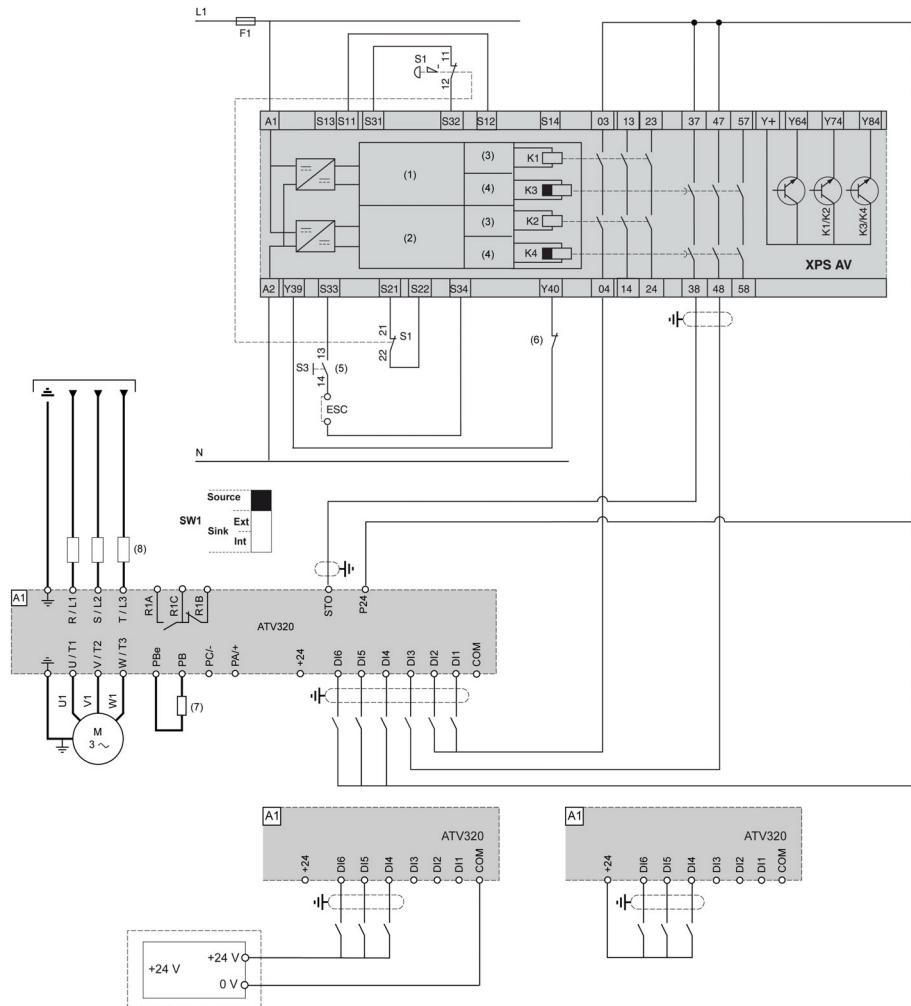
NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive with the Safety Module Type Preventa XPS AV - Case 2

Single Drive with the Safety Module Type Preventa XPS AV According to EN 954-1, IEC 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- SS1 type C category 4, PL e/SIL3 on STO and DI3 with Safety module type Preventa XPS AV or equivalent
- SLS category 3, PL d/SIL2 or SS1 type B category 3 PL d/SIL2 on DI5/DI6
- DI4 not set to a safety function



(1) Channel 1 logic, (2) Channel 2 logic, (3) Output 1, (4) Output 2, (5) Emergency stop, (6) Time delay stop, (7) Braking resistor, if used, (8) Line chokes, if used.

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive with the Safety Module Type Preventa XPS AF - Case 1

Single Drive with the Safety Module Type Preventa XPS AF According to EN 954-1, IEC 13849-1, IEC 62061 and 60204-1 (Machine)

The following configurations apply to the diagram below:

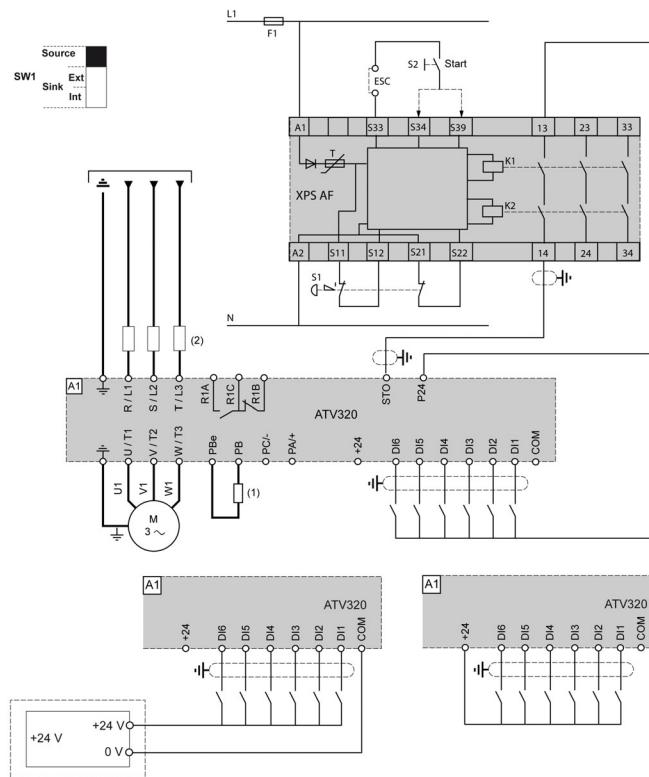
- STO category 3, PL d/SIL2 on STO with Safety module type Preventa XPS AF or equivalent
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI3/DI4 or DI5/DI6

Or

- STO category 3, PL d/SIL2 on STO with Safety module type Preventa XPS AF or equivalent
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI3/DI4
- DI5/DI6 not set to a safety function

Or

- STO category 3, PL d/SIL2 on STO with Safety module type Preventa XPS AF or equivalent
- DI3/DI4 and DI5/DI6 not set to a safety function



(1) Braking resistor, if used, (2) Line chokes, if used.

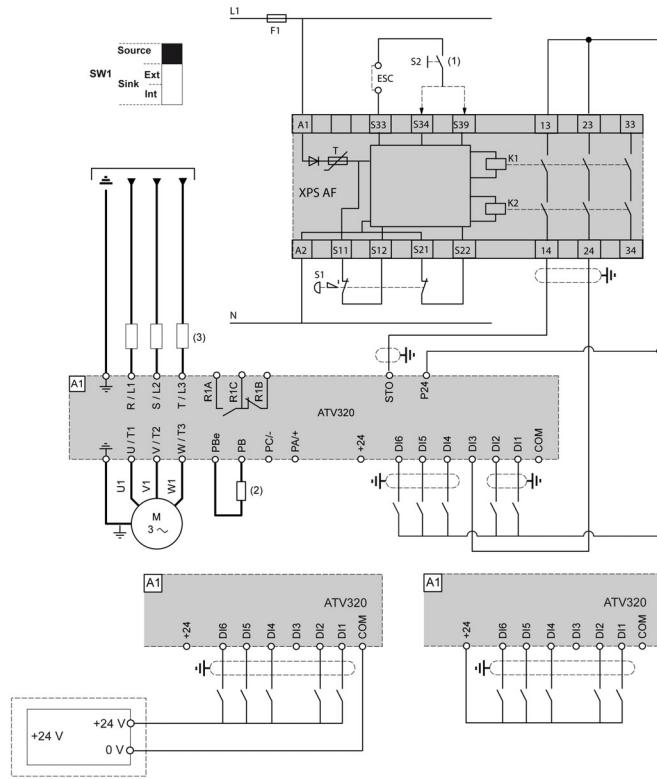
NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive with the Safety Module Type Preventa XPS AF - Case 2

Single Drive with the Safety Module Type Preventa XPS AF According to EN 954-1, IEC 13849-1, IEC 62061 and 60204-1 (Machine)

The following configurations apply to the diagram below:

- STO category 4, PL e/SIL3 on STO with Safety module type Preventa XPS AF or equivalent and DI3 set to STO
- SLS category 3, PL d/SIL2 or SS1 type B category 3 on DI5/DI6
- DI4 not set to a safety function



(1) Start, (2) Braking resistor, if used, (3) Line chokes if used.

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive According to IEC 61508 and IEC 60204-1 - Case 1

Single Drive According to IEC 61508 and IEC 60204-1 Without Protection Against Supply Interruption or Voltage Reduction and Subsequent Rotation

The following configurations apply to the diagram below:

- STO SIL2 on STO
- STO or SLS SIL2 or SS1 type B SIL2 on DI3/DI4 or DI5/DI6

Or

- STO SIL2 on STO
- STO or SLS or SS1 type B on DI3/DI4
- DI5/DI6 not set to a safety function

Or

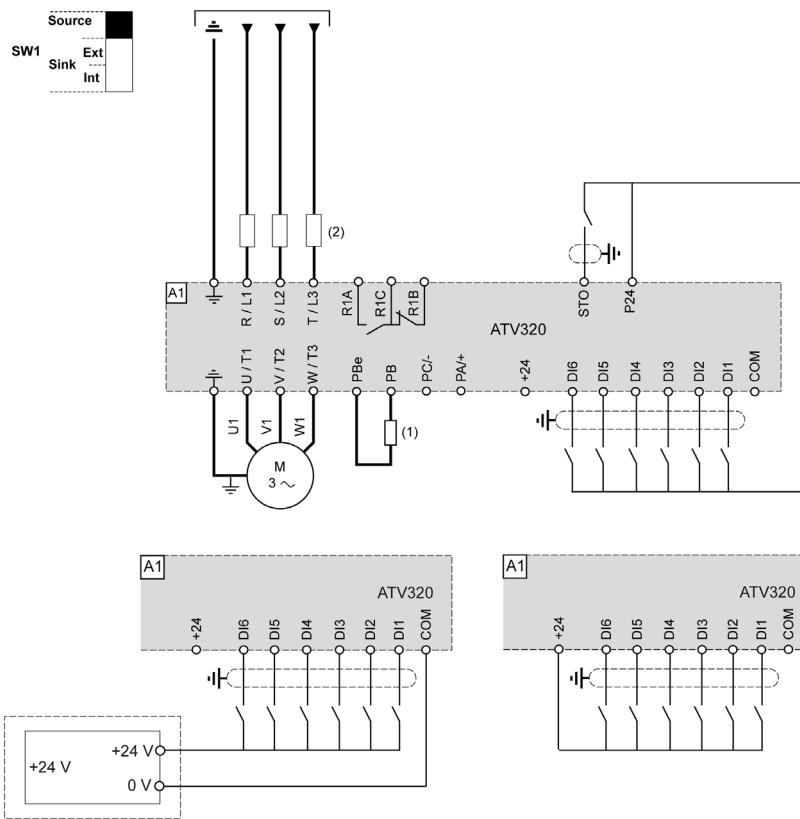
- STO SIL2 on STO
- DI3/DI4 and DI5/DI6 not set to a safety function

Or

- STO SIL3 on STO and DI3
- SLS SIL2 or SS1 type B SIL2 on DI5/DI6
- DI4 not set to a safety function

Or

- STO SIL3 on STO and DI3
- DI4 and DI5/DI6 not set to a safety function



(1) Braking resistor, if used, (2) Line chokes if used.

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive According to IEC 61508 and IEC 60204-1 - Case 2

Single Drive According to IEC 61508 and IEC 60204-1 Without Protection Against Supply Interruption or Voltage Reduction and Subsequent Rotation

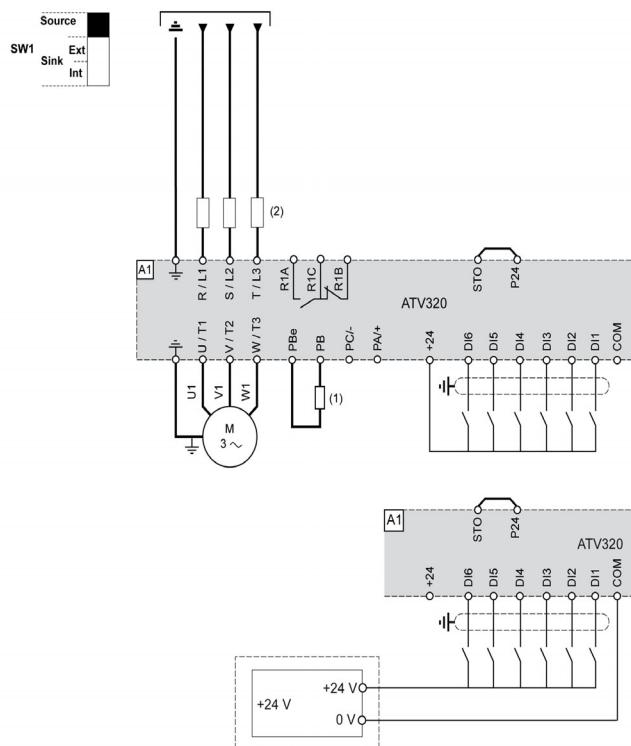
The following configurations apply to the diagram below:

- STO SIL2 on DI3 and DI4
- SLS SIL2 or SS1 type B SIL2 on DI5/DI6

Or

- STO SIL2 on DI3 and DI4
- DI5/DI6 not set to a safety function

Wiring Diagram



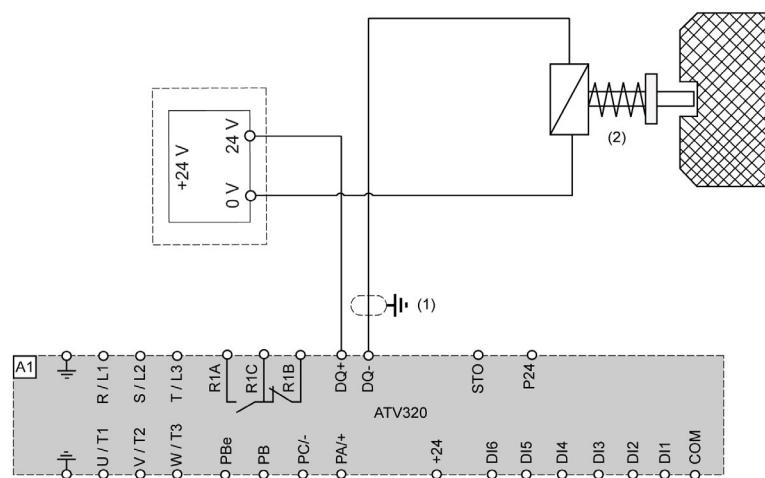
(1) Braking resistor, if used, (2) Line chokes, if used.

NOTE: For more information about the control terminal characteristics, please refer to the installation manual.

Single Drive According to IEC 61508 and IEC 62061 with Safety Function GDL

Certified Wiring Diagram

GDL category 2, PL c/SIL1 is applicable to the following wiring diagram.

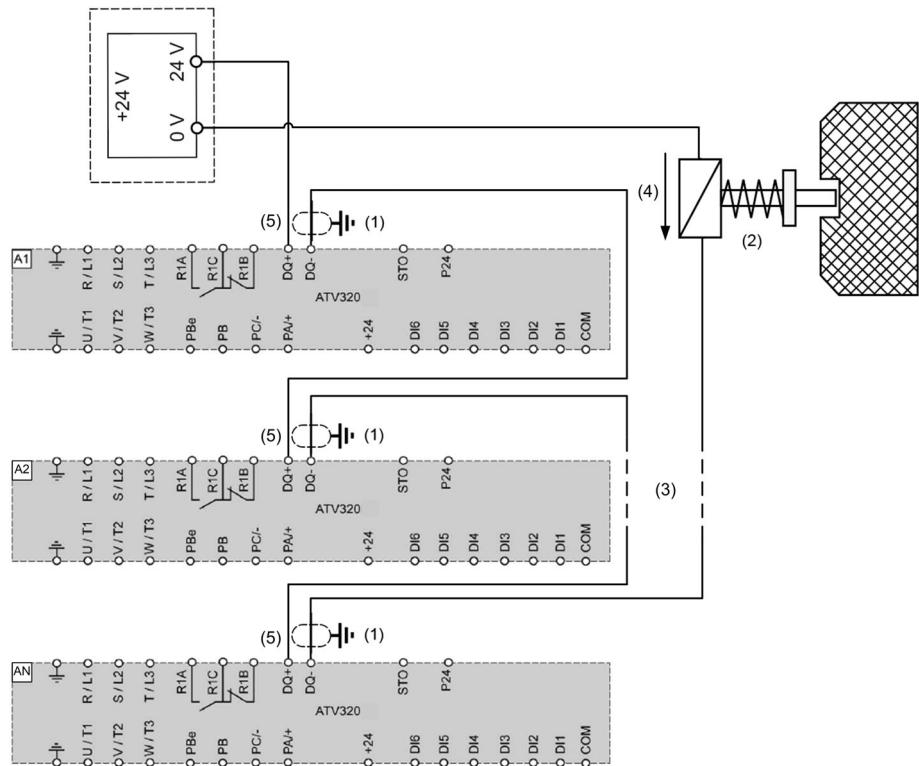


- (1) Cable wiring following IEC60079-14. STO cables must be shielded and run apart from the supply cable.
(2) Guard door lock. The maximum current for the interlock system is 100 mA.

Multi-drive Chaining According to IEC 61508 and IEC 62061 with Safety Function GDL

Certified Wiring Diagram

GDL category 2, PL c/SIL1 is applicable to the following wiring diagram.



(1): Cable wiring following IEC60079-14. STO cables must be shielded and run apart from the supply cable.

(2): Guard door lock. The maximum current for the interlock system is 100 mA.

(3): Chaining of a total of N ATV320 drives.

(4): The maximum ATV320 voltage drop is 2.5 V. With N ATV320 drives and a 24 V supply voltage, the guard door lock operating voltage must be lower than (24 V - 2.5 V x N).

(5): The maximum voltage between DQ+ and DQ- is 30 V.

NOTE: For more information about the control terminal characteristics, refer to the installation manual.

Chapter 8

Commissioning

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Safety Functions Tab	92
Configure Safety Functions Panel	93
Visualization and Status of Safety Functions	98
Copying Safety Related Configuration from Device to PC and from PC to Device	99
Machine Signature	102

Safety Functions Tab

Introduction

To access the safety function configuration, click the **Safety Functions** tab. This screen is read-only, allowing you to see all current safety function configurations.

The **Safety Functions** tab provides access to:

- an outline of the safety function features available on the ATV320 (accessible Online/Offline)
- the status of all I/O in connected mode
- general information about the machine (Online/Offline).

It also provides access to the following dialog boxes:

- **Configuration**
 - **Configure** (only available in connected mode)
 - **Reset Configuration**
 - **Copy from DEVICE to PC**
 - **Copy from PC to DEVICE**
- **Password Configuration**
 - **Modify Password**
 - **Reset Password**

Pre-Condition

Before configuring the safety-related parameters, make sure that the device firmware and the DTM version are the same.

Steps to Configure the Safety Functions

If...	Then ...
you are not in Online mode	In the menu bar, click Communication → Connect to Device or click the Connect to Device icon
you are Online mode	Click the Configure button in the Safety Functions tab.

Once connected:

Step	Action	Comment
1	Click the Configure button in the Safety Functions tab.	A Define Configuration Password dialog box appears: <ul style="list-style-type: none">• Type the new configuration password in Enter New Password box• Retype the new configuration password in Confirm New Password box.• Click OK NOTE: Your password: <ul style="list-style-type: none">• Should have only numeric value, choose the value between 1...9999.• Should not exceed more than 4 digits.• Should not have the value 0. Result: Opens the Configuration of Safety Functions window.

If...	Then ...
you have already defined the password	type your safety function configuration password in Enter Configuration Password box, click OK . Result: Opens the Configuration of Safety Functions window.

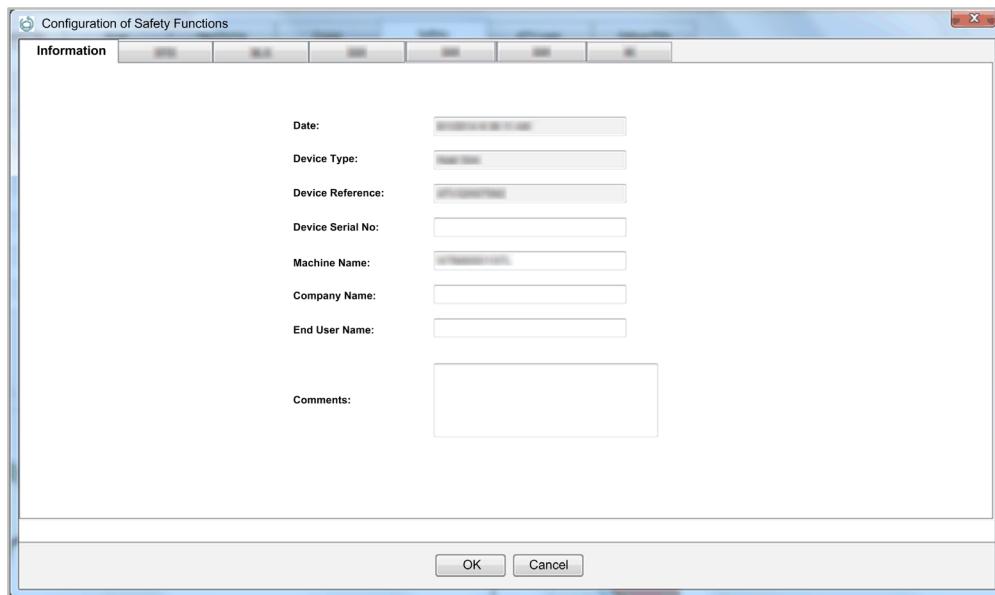
Configure Safety Functions Panel

Overview

The Configuration of Safety Functions panel includes the **Information**, **STO**, **SLS**, **SS1**, **SMS**, **GDL**, and **Input/Output** tabs.

Information Tab

The **Information** tab allows you to define and display product system information



Information filled in automatically by SoMove:

- **Date** (format depends on the PC local and linguistic options)
- **Device Type**
- **Drive Reference**

Information filled in manually:

- **Device Serial No** (number)
- **Machine Name**
- **Company Name**
- **End-User Name**
- **Comments**

Safe Torque Off (STO) Tab

For more information about **STO** function, see STO description ([see page 24](#)).

For this function, only the associated set of inputs should be selected in the box. The parameter to be managed is: STOA.

Code	Name/Description	Factory Setting
S E O	[Safe Torque Off]	
S E O R	[STO function activation]	[No]
n o	[No: Not assigned]	
L 3 4	[DI3 and DI4]: digital input 3/4 low state	
L 5 6	[DI5 and DI6]: digital input 5/6 low state	
L 3 P W	[DI3 and STO]: digital input 3/STO low state This parameter is used to configure the channel used to trigger the STO function. If you set STOA=No, STO function is always active but just on STO input	

Safely Limited Speed (SLS) Tab

For more information about **SLS** function, see SLS description ([see page 28](#)).

Code	Name/Description	Adj. Range	Factory Setting
5 L 5	[Safely-Limited Speed]		
5 L 5 R L 3 4 L 5 6	[SLS function activation] [No]: Not assigned [DI3 and DI4]: digital input 3/4 low state [DI5 and DI6]: digital input 5/6 low state This parameter is used to configure the channel used to trigger the SLS function.		[No]
5 L E	[Safely Limited speed Type Element] This parameter is used to select the SLS type. [Type1] : SLS type 1 [Type2] : SLS type 2 [Type3] : SLS type 3 [Type4] : SLS type 4 [Type5] : SLS type 5 [Type6] : SLS type 6 Refer to function description to have information about behavior of different type.		[Type1]
5 L 5 P	[SLS set point] parameter This parameter is only visible if SLT = Type2 or SLT = Type3 or SLT = Type 4 SLSP is used to set the maximum speed	0...599 Hz	0 Hz
5 L E E	[SLS tolerance threshold] parameter The behavior of this parameter depends on the value of SLT, see above	0...599 Hz	0 Hz
5 L W E	[SLS Wait Time] parameter This parameter is used to set the maximum time for 5 E F r to be greater than 5 S S L . When SLwt is reached, STO function is triggered. Unit of this parameter is 1 ms. For example If the value is set to 2000 units, then the SLS wait time in second is: 2000*1 ms = 2 s This parameter can be modified only if SLT = Type 2 or SLT = Type 3 For SLS type 1 and SLS type 4, SLwt is always set to 0	0...5000 ms	0 Hz
5 S r E	[SS1 ramp value] parameter The unit depends on the SSRU parameter. Use this parameter to set the value of the SS1 deceleration ramp. SS1 ramp = SSRT*SSRU example: If SSRT = 250 and SSRU = 1 Hz/s then the deceleration ramp = 25 Hz/s. This parameter is similar to the SS1 safety function, for more information see SS1 (see page 46).	1 to 5990	1
5 S r u I H I O H I O O H	[SS1 ramp unit] parameter [1 Hz/s] [10 Hz/s] [100 Hz/s] This parameter is used to set the SSrt unit. This parameter is similar to the SS1 safety function configured, for more information see SS1 (see page 46).	[1 Hz/s]	
5 S E E	[SS1 trip threshold] This parameter sets the tolerance zone around the deceleration ramp in which the frequency may vary. This parameter is similar to the SS1 safety function configured in another tab.	0...599 Hz	0 Hz
5 S S L	[SLS/SS1 standstill level] parameter This parameter adjusts the frequency at which the drive should go into STO state at the end of the SS1 ramp. This parameter is similar to the SS1 safety function configured in another tab.	0...599 Hz	0 Hz

Safe Stop 1 (SS1) Tab

For more information about **SS1** function, see SS1 description ([see page 26](#)).

Code	Name/Description	Adj. Range	Factory Setting
5 5 1	[Safe Stop 1]		
5 5 1 R	[Safe Stop 1 Activation]		[No]
n o	[No]: Not assigned		
L 3 4	[DI3 and DI4]: digital input 3/4 low state		
L 5 6	[DI5 and DI6]: digital input 5/6 low state		
	These parameters are used to configure the channel used to trigger the SS1 function.		
5 5 r t	[SS1 ramp value]	1 to 5990	1
	The unit depends on the SSRU parameter. Use this parameter to set the value of the SS1 deceleration ramp. SS1 ramp = SSRT*SSRU example: If SSRT = 250 and SSRU = 1 Hz/s then the deceleration ramp = 25 Hz/s.		
	This parameter is similar to the SLS safety function configured in another tab.		
5 5 r u	[SS1 ramp unit]		[1 Hz/s]
1 H	[1 Hz/s]		
10 H	[10 Hz/s]		
100 H	[100 Hz/s]		
	This parameter is used to set the SSRT unit.		
	This parameter is similar to the SLS safety function configured in another tab.		
5 5 t t	[SS1 trip threshold] parameter	0...599 Hz	0 Hz
	This parameter sets the tolerance zone around the deceleration ramp in which the frequency may vary.		
	This parameter is similar to the SLS safety function configured,		
5 5 s L	[SLS/SS1 standstill level] parameter	0...599 Hz	0 Hz
	This parameter adjusts the frequency at which the drive should go into STO state at the end of the SS1 ramp.		
	This parameter is similar to the SLS safety function configured in another tab.		

Safe Maximum Speed (SMS) Tab

For more information about **SMS** function, see SMS description ([see page 35](#)).

Code	Name/Description	Adj. Range	Factory Setting
5 n 5	[Safe Maximum Speed]		
5 n 5 R	[SMS Activation]		[No]
n o	[No]: SMS function is not active.		
Y E 5	[Yes]: SMS function is active		
	This parameter is used to configure the channel used to trigger the SMS function.		
5 n L 5	[SMS Assignment]		[NO]
	This parameter is used to select the safe maximum speed limit.		
n o	[No]: [SMS Low Limit] 5 n L L is selected as the safe maximum speed limit.		
L 3 4	[DI3 and DI4]		
	● If digital inputs 3/4 are in low state (0), [SMS Low Limit] 5 n L L is selected as the safe maximum speed limit.		
	● If digital inputs 3/4 are in high state (1), [SMS High Limit] 5 n L H is selected as the safe maximum speed limit.		
L 5 6	[DI5 and DI6]		
	● If digital inputs 5/6 are in low state (0), [SMS Low Limit] 5 n L L is selected as the safe maximum speed limit.		
	● If digital inputs 5/6 are high state (1), [SMS High Limit] 5 n L H is selected as the safe maximum speed limit.		
5 n L L	[SMS Low Limit]	0...599 Hz	0 Hz
	This parameter is used to set the lower speed limit.		
5 n L H	[SMS High Limit]	0...599 Hz	0 Hz
	This parameter is used set the higher speed limit.		

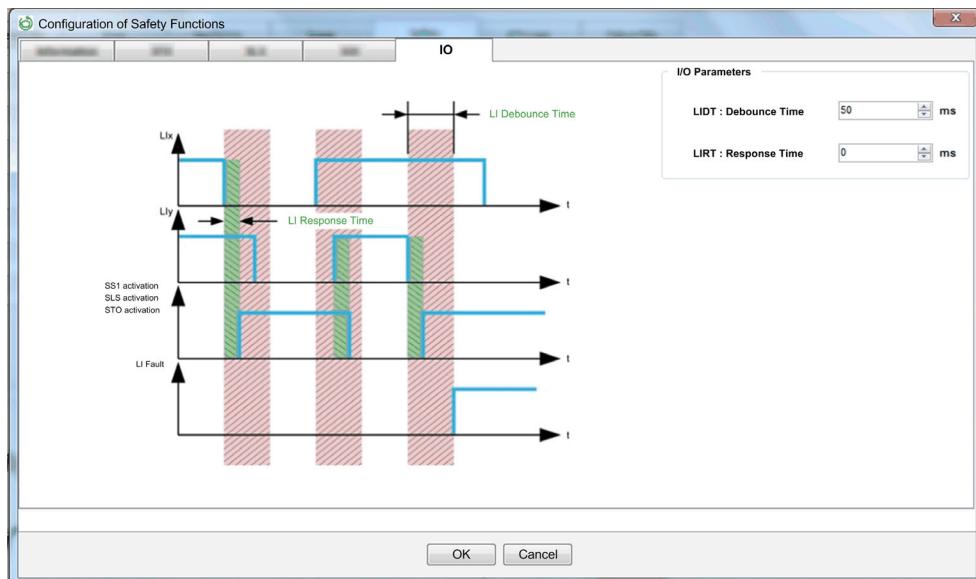
Guard Door Locking (GDL) Tab

For more information about GDL function, see GDL description ([see page 37](#)).

Code	Name/Description	Adj. Range	Factory Setting
<i>G d L</i>	[Guard Door Locking]		
<i>G d L A</i>	[GDL Assignment] <i>n o</i> : [No]: Guard door locking is not assigned <i>Y E S</i> : [Yes]: Guard door locking is assigned NOTE: <i>G d L A</i> can be set to [yes] only if <i>L o I</i> parameter is set to [NO]. This parameter is used to configure the channel used to trigger the GDL function.		[No]
<i>G L L d</i>	[GDL Long Delay] This parameter is used to set the long delay for triggering the safety function GDL. Maximum delay after STO function activation or normal deceleration ramp command to stop the machine. NOTE: GDL long delay should be greater than GDL short delay.	1...3600 s	1 s
<i>G L S d</i>	[GDL Short Delay] This parameter is used to set the short delay for triggering the safety function GDL. Maximum delay after SS1 ramp to stop the machine.	1...3600 s	1 s

Input/Output Configuration

The figure shows the Input/Output tab:



Code	Name/Description	Adj. Range	Factory Setting
<i>I o</i>	[Input/Output]		
<i>L i d t</i>	[DI debounce time]	0...2000 ms	50
	In most cases, the two digital inputs in a pair used for a safety function (DI3-DI4 or DI5-DI6 or STO-DI3) will not be 100% synchronized. They will not change state at the same time. There is a small delta between the two digital input transitions. <i>L i d t</i> is the parameter used to set this delta. If the two digital inputs change state with a delta lasting less than <i>L i d t</i> it is considered to be simultaneous transition of the digital inputs. If the delta lasts longer than <i>L i d t</i> , the drive considers the digital Inputs are no longer synchronized and detected error is triggered.		
<i>L i r t</i>	[DI response time]	0...50 ms	0
	This parameter is used to filter short impulses on the digital input (only for DI3-DI4 or DI5-DI6, STO not concerned). Some applications send short impulses on the line to test it. This parameter is used to filter these short impulses. Commands are only taken into account if the duration is longer than <i>L i r t</i> . If the duration is shorter the drive considers that there is no command: the command is filtered.		

Password Configuration - Modify Password

This function allows you to modify the configuration password in the drive.

To modify the configuration password

Step	Action
1	In Safety Functions tab, click the Modify Password button Result: opens the Modify Configuration Password dialog box.
2	In the Modify Configuration Password dialog box: <ul style="list-style-type: none">● Type the existing configuration password in Enter Current Password box● Type the new configuration password in Enter New Password box● Retype the new configuration password in Confirm New Password box● Click Ok NOTE: The password typed in Enter New Password box and Confirm New Password box should be same. NOTE: Your password: <ul style="list-style-type: none">● Should contain only numeric value, choose the value between 1...9999.● Should not exceed more than 4 digits.● Should not have the value 0. Result: modifies the configuration password.

Password Configuration - Reset Password

If you cannot remember the configuration password defined in the drive, you need to know the universal password to reset the drive. To obtain this password, contact your Schneider Electric contact.

After this operation, the device reverts to no defined configuration password and the session is automatically closed.

However, the function configuration remains unchanged.

Reset Configuration

This function is used to reset the configuration of the safety function to the factory settings.

To access the function, click the **Reset Configuration** button in the **Safety Functions** tab.

First enter the password, then confirm your choice.

After this action, all safety-related parameters are set to factory settings.

Visualization and Status of Safety Functions

Code	Name/Description
<i>Mon -</i>	[Monitoring] menu - Visible on SoMove and keypad
<i>S t F r</i>	[Stator Frequency] Displays the estimated stator frequency in Hz
<i>S d , F</i>	[Stator Freq Consist] Stator Frequency Consistency. Displays the difference between the estimated stator frequency and the internal computed stator frequency in Hz.
<i>S R F -</i>	[MONIT. SAFETY] menu - Visible on SoMove and keypad
<i>S t o S</i>	[STO status] Status of the Safe Torque Off safety function [IdLE]: STO not in progress [Safe torque off]: STO in progress [Fault]: STO in detected error
<i>S L S S</i>	[SLS status] Status of the Safely limited speed safety function [Not config]: SLS not configured [IdLE]: SLS not in progress [Safe stop 1]: SLS ramp in progress [Safe torque off]: SLS safe torque off request in progress [Fault]: SLS in detected error [wAIT]: SLS waiting for activation [Started]: SLS in transient state
<i>S M S S</i>	[SMS status] Status of the Safe Maximum Speed safety function [Not Set]: SMS is not configured [Active]: SMS is in active state [Internal Err.]: SMS in internal detected error [Max Speed]: SMS in overspeed detected error
<i>G d L S</i>	[GDL status] Status of the guard door locking safety function [Not Set]: GDL is not configured [Inactive]: GDL is in inactive state [Short delay]: GDL in Short delay state. [Long delay]: GDL in long delay state. [Active]: GDL is in active state. [Internal Err.]: GDL in internal detected error.
<i>S S 1 S</i>	[SS1 status] Status of the Safe Stop 1 safety function [Not config]: SS1 not configured [IdLE]: SS1 not in progress [Safe stop 1]: SS1 ramp in progress [Safe torque off]: SS1 Safe Torque Off request in progress [Fault]: SS1 in detected error
<i>S R F -</i>	[MONIT. SAFETY] menu - Visible ONLY on SoMove
<i>S F t Y</i>	[Safety drive status] Safety function status of the drive [Standard drive]: Standard product without safety function configured [Safety drive]: product with at least 1 safety function configured

Copying Safety Related Configuration from Device to PC and from PC to Device

Overview

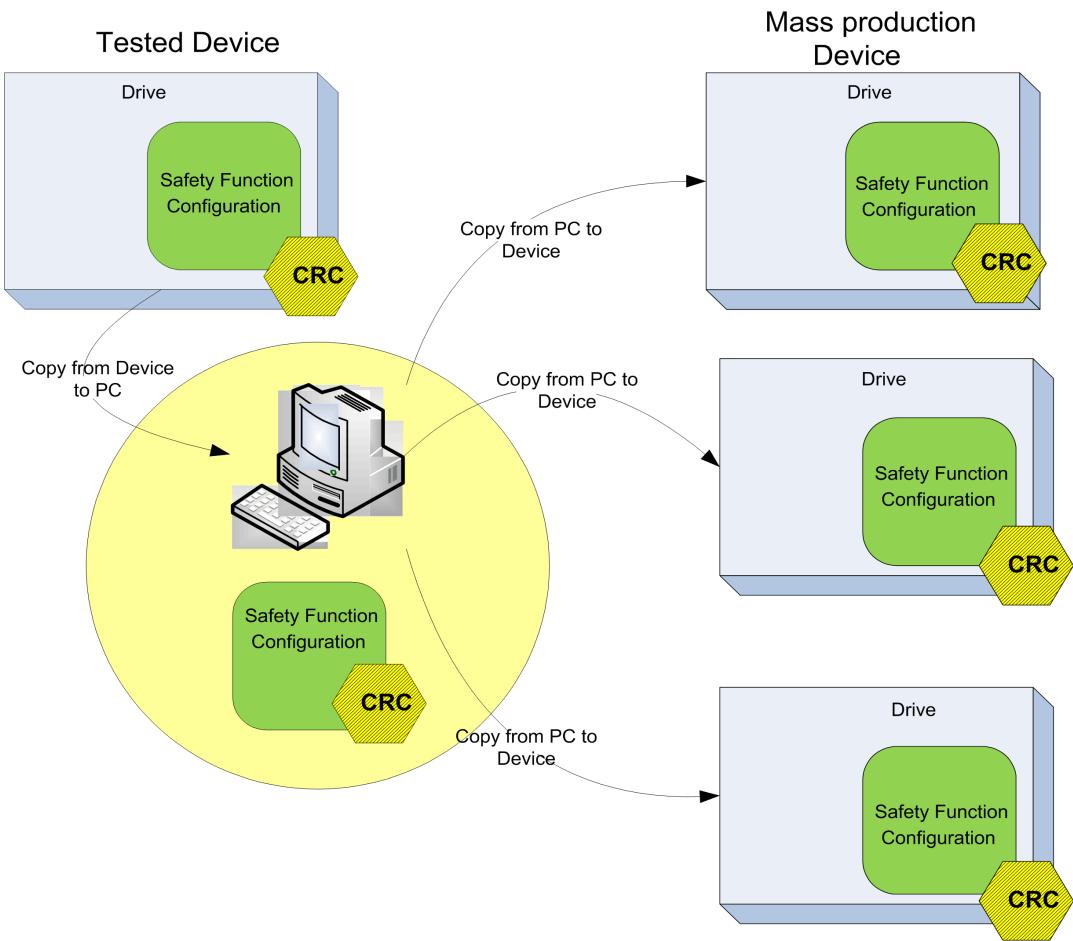
This feature is used to copy/paste the tested safety-related configuration in several drives.

This feature allows you to:

- identify unique safety-related configuration on the drive
- copy the safety-related configuration file from drive to PC.
- copy the safety-related configuration file from PC to drives

Architecture

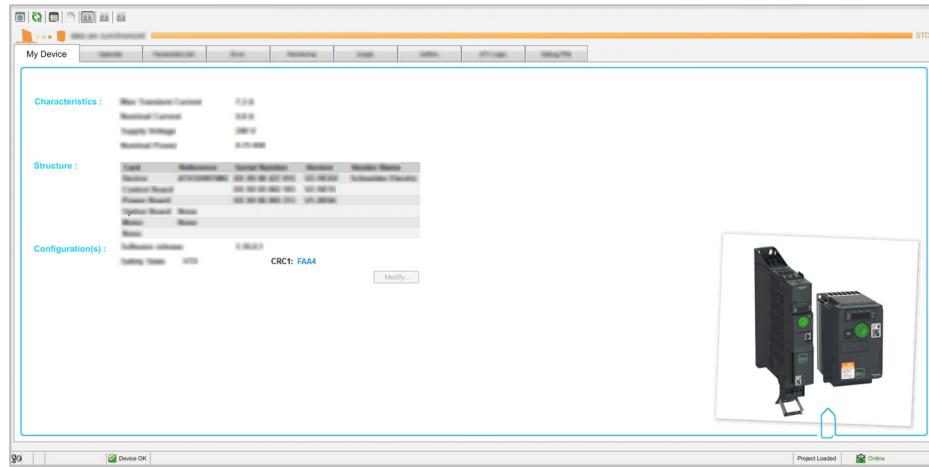
The figure shows the architecture for copying the safety-related configuration from device to PC and PC to device:



Identify Unique Safety Related Configuration

The identification of the safety-related configuration is done by using CRC, calculated using all safety-related parameters

You can get the CRC value from **My Device** tab. Note down the CRC value after the drive is fully tested.



Copy from Device to PC

To copy a configuration file from device to PC:

Step	Action
1	<p>In the Safety Functions tab, click the Copy from DEVICE to PC button</p> <p>Result: opens the Copy from Device to PC dialog box.</p>
2	<p>Type the configuration password in Enter configuration Password box, click Ok.</p> <p>Result: Displays the CRC1 value</p>
3	<p>Note the CRC1 value, click Save.</p> <p>Result: opens the Save File... window.</p>
4	<p>In the Save File.. Window:</p> <ul style="list-style-type: none"> Select/create the folder Type the name of the file in File name box. Click Save, <p>Result: Safety-related Parameters Successfully saved message appears on the screen, which confirms that the file has been saved successfully in the desired path.</p>

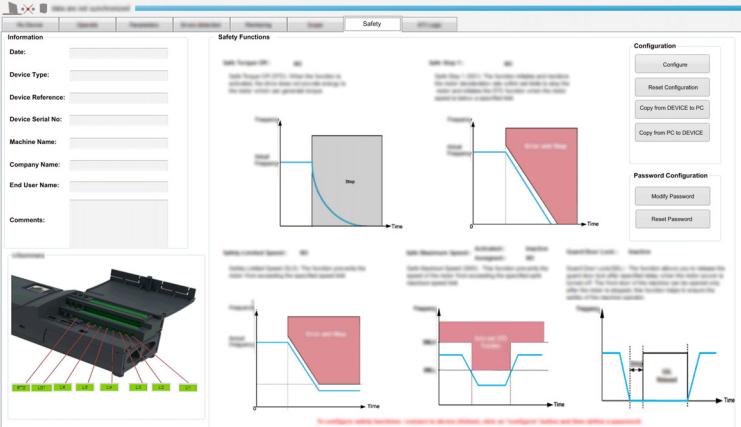
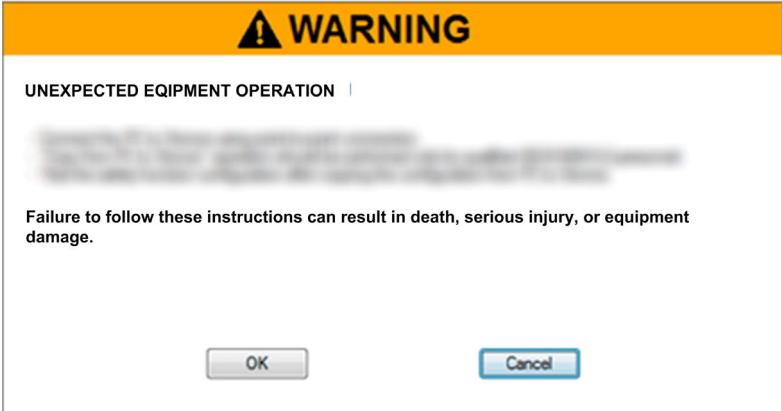
NOTE:

You cannot copy the configuration from device to PC if:

- the motor is powered.
- a function block is in **Run** state.
- the function **Forced Local** is active.
- a safety function is triggered.

Copy from PC to Device

To copy a file from PC to device:

Step	Action
1	<p>In the Safety Functions tab, click the Copy from PC to DEVICE button</p>  <p>Result: Warning box appears, read the following instruction before proceeding with copy from PC to device operation.</p>
2	 <p>Click Ok Result: Opens the Open File... window.</p>
3	<p>In the Open File... Window</p> <ul style="list-style-type: none"> Select .sfty file. Click Open <p>Result: Displays the CRC1 value</p>
4	<p>Verify whether the CRC1 value is same as the CRC1 value noted while copying the configuration from device to PC if both CRC1 values are same then click Continue.</p> <p>Result: Opens the Copy from PC to Device dialog box.</p>
5	<p>Type the password (49157) in the Enter copy password box, click Ok.</p> <p>Result: Configuration is successfully copied from PC to device. A commissioning test must be done on the safety function.</p>

NOTE:

You cannot copy the configuration from PC to device if:

- the motor is powered.
- a function block is in **Run** state.
- the function **Forced Local** is active.
- the configuration of the safety function is already present in the device

Machine Signature

Overview

The purpose of the test is to verify proper configuration of the defined safety functions and test mechanisms and to examine the response of dedicated monitoring functions to explicit input of values outside the tolerance limits.

The test must cover all drive-specific Safety configured monitoring functions and global Safety integrated functionality in ATV320.

Condition Prior to Acceptance Test

- The machine is wired up correctly.
- All safety-related devices such as protective door monitoring devices, light barriers, and emergency stop switches are connected and ready for operation.
- All motor parameters and command parameters must be correctly set on the drive.

Acceptance Test Process

The acceptance test is configured with SoMove software.

Step	Action	Comment
1	Select the Device → Safety Function → Machine Signature menu and follow the five steps below	
2	General Information To add this step to the final report select Add to the machine signature Click Next .	The information displayed here corresponds to the Identification section in the Safety Functions tab.
3	Function Summary To add a function to the final report select Add to the machine signature Click Next	This step is composed of sub-steps. Each sub-step relates to one of the following safety functions: <ul style="list-style-type: none">• STO• SLS• SS1 In a function, sub-step the function diagram and parameters values are displayed. A text box allows you to enter additional text in this step.
4	I/O Summary To add a function to the final report select Add to the machine signature Click Next	The information displayed here corresponds to the Digital Input summary folder of the Safety Functions tab: <ul style="list-style-type: none">• The digital input that is assigned to a safety function are displayed in red and show the related safety function• The digital input that is not assigned to a safety function do not show any assignment and are displayed in green
5	Test To add a function to the final report select Add to the machine signature Click Next	In this step, you tick the box when you have tested the safety functions to confirm that you have verified the correct behavior of the functions for all devices.
6	Key Click Finish to create the report	The checksum of the safety-related configuration is displayed as it is calculated for transmission to the connected device when you click Apply . This allows you to compare the checksum value with the one displayed in the identification menu on the graphic display terminal

Acceptance Report

SoMove creates the acceptance report.

This function provides a final report when one or several safety functions have been configured and verified. This report is deemed to be a machine signature and certifies that all the safety functions are operational. The acceptance report has been added as an optional document to be printed to a printer or to a PDF file.

If the drive configuration is modified (not only applicable on the safety related parameters), you must repeat the acceptance test.

Chapter 9

Services and Maintenance

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Maintenance	106
Power and MCU Replacement	106
Changing Machine Equipment	106

Maintenance

Overview

By way of preventive maintenance, the Safety functions must be activated at least once a year. The drive power supply must be turned off and then on again before carrying out this preventive maintenance. The drive digital output signals cannot be considered to be safety-related signals. Install interference suppressors on all inductive circuits near the drive or coupled to the same circuit (relays, contactors, solenoid, valves, etc.).

NOTE: For more product information, see the installation manual and programming manual on www.schneider-electric.com.

Power and MCU Replacement

Overview

You can replace the MCU (Motor Control Unit) part (APP + HMI card) and the power part.

Depending on the drive configuration (safety function active or not), the drive response will differ.

If you replace the power and you keep your MCU, you won't lose the configuration of the safety functions but you need to repeat the Acceptance Test to avoid incorrect wiring or incorrect behavior of the safety function.

If you replace the MCU you will lose your safety-related configuration. You need to reinstall your Configuration on the new MCU and then repeat the Acceptance Test.

NOTE: For more product information, see the installation manual and programming manual www.schneider-electric.com.

Changing Machine Equipment

Overview

If you need to change any part of the drive system (Motor, Emergency stop, etc.) you must repeat the Acceptance Test.

NOTE: For more product information, see the installation manual and programming manual www.schneider-electric.com.



www.schneider-electric.com/contact

ATV320_Safety_Function_manual_EN_NVE50467_03
04/2019