Altivar 32

Variable speed drives
for synchronous and asynchronous motors

Safety integrated functions manual

03/2010

S1A45606

www.schneider-electric.com

Schneider Electric

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.

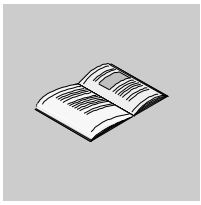
All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

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

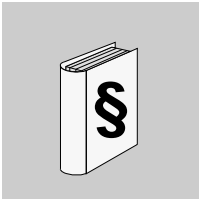
Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

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

Table of contents



Safety Information



Important Information

NOTICE

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

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

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

⚠ DANGER

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

⚠ WARNING

WARNING indicates a potentially hazardous situation, which, if not avoided, **can result** in death, serious injury or equipment damage.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation, which, if not avoided, **can result** in injury or equipment damage.

CAUTION

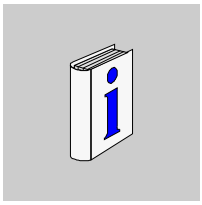
CAUTION, used without the safety alert symbol, indicates a potentially hazardous situation which, if not avoided, **can result** in equipment damage.

PLEASE NOTE

The word "drive" as used in this manual refers to the controller portion of the adjustable speed drive as defined by NEC.

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 product.

About the book



At a Glance

Document Scope

The purpose of this document is to provide information about safety functions incorporated in Altivar32. These functions allow you to develop applications oriented in the protection of man and machine.

Validity Note

This documentation is valid for the Altivar 32 drive.

Related Documents

Title of Documentation	Reference Number
ATV32 Quick Start	S1A41715
ATV32 Installation manual	S1A45686
ATV32 Programming manual	S1A28692
ATV32 Modbus manual	S1A28698
ATV32 CANopen manual	S1A28699
ATV32 Communication parameters	S1A44568
ATV32 Atex manual	S1A45605
ATV32 other option manuals: see www.schneider-electric.com.	

You can download the latest versions of these technical publications and other technical information from our website at www.schneider-electric.com.

Before you begin

1

What's in this Chapter?

This chapter contains the following topics:

Safety instructions

The information provided in this manual supplements the product manuals.

Carefully read the product manuals before using the product.

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

⚠⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

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

⚠ DANGER

UNINTENDED EQUIPMENT OPERATION

- Read and understand this manual before installing or operating the drive.
- Any changes made to the parameter settings must be performed by qualified personnel.

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

⚠WARNING

DAMAGED DRIVE EQUIPMENT

Do not operate or install any drive or drive accessory that appears damaged.

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

⚠WARNING

LOSS OF CONTROL

- The designer of any wiring scheme must consider the potential failure modes of control channels and, for certain critical control functions, provide a means to achieve a safe state during and after a channel failure. Examples of critical control functions are emergency stop and overtravel stop.
- Separate or redundant control channels must be provided for critical control functions.
- Each implementation of a control system must be individually and thoroughly tested for proper operation before being placed into service.
- System control channels may include links carried out by the communication. Consideration must be given to the implications of unanticipated transmission delays or failures of the link[1].

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

1. For 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.”

⚠CAUTION

INCOMPATIBLE LINE VOLTAGE

Before turning on and configuring the drive, ensure that the line voltage is compatible with the supply voltage range shown on the drive nameplate. The drive may be damaged if the line voltage is not compatible.

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

CAUTION

RISK OF DERATED PERFORMANCE DUE TO CAPACITOR AGING

The product capacitor performances after a long time storage above 2 years can be degraded.
In that case, before using the product , apply the following procedure:

- Use a variable AC supply connected between L1 and L2 (even for ATV32●●●N4 references).
- Increase AC supply voltage to have:
  - 25% of rated voltage during 30 min
  - 50% of rated voltage during 30 min
  - 75% of rated voltage during 30 min
  - 100% of rated voltage during 30 min

Failure to follow these instructions can result in equipment damage.

Qualification of personnel and use

Qualification of personnel

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

All persons working on and with the product must be fully familiar with all applicable standards, directives, and accident prevention regulations when performing such work.

Intended use

The functions described in this manual are only intended for use with the basic product; you must read and understand the appropriate product manual.

The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data.

Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented.

Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design).

Operate the product only with the specified cables and accessories. Use only genuine accessories and spare parts.

Any use other than the use explicitly permitted is prohibited and can result in hazards.

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

The product must NEVER be operated in explosive atmospheres (hazardous locations, Ex areas).

Overview

2

What's in this Chapter?

This chapter contains the following topics:

Introduction

The safety functions incorporated in Altivar32, allow you to develop applications oriented in the protection of man and machine. The safety functions are configured with SoMove software.

Safety integrated functions provides the following benefits:

- Additional standards-compliant safety functions
- Replacement of external safety equipment
- Reduced wiring efforts and space requirements
- Reduced costs

The Altivar 32 drives are compliant with normative requirements to implement the safety functions

Safety functions as per IEC 61800-5-2

STO	**Safe Torque Off** The function purpose is to bring the motor into a no torque condition so it is relevant in terms of safety since no torque is available at the motor level. Power modules are inhibited and the motor coasts dow or prohibits the motor from starting.
SLS	**Safely Limited Speed** SLS monitors an adjustable speed limit. In case of exceeding the limit speed, the drive is shut down safely.
SS1	**Safe Stop 1** SS1 consists of: • Monitored deceleration of the movement according a specified ramp. • STO (triggered after standstill has been reached).

Notation

The graphic display terminal (to be ordered separately - reference VW3 A1 101) menus are shown in square brackets.

Example: **[COMMUNICATION]**

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

Example: (COM-)

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

Example: **[Fallback speed]**

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

Example: (LFF)

Standards and Terminology

Technical terms, terminology and the corresponding descriptions in this manual are intended to use the terms or definitions of the pertinent standards.

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

Among others, these standards include:

- IEC 61800 series: "Adjustable speed electrical power drive systems"
- IEC 61508 series Ed.2: "Functional safety of electrical/electronic/programmable electronic safetyrelated systems"
- EN 954-1 Safety of machinery - Safety related parts of control systems
- EN ISO 13849-1 & 2 Safety of machinery - Safety related parts of control systems

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

Certification for functional safety

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

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

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

The defined safety functions are:

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

Also refer to Safety function capability, page 46.

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

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

Basics

Functional Safety

Automation and safety engineering are two areas that were completely separated in the past but recently have become more and more integrated.

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 the 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 determines the PFH (probability of a dangerous failure per hour) for a safety system. This is the probability per hour that a safety system fails in a hazardous manner and the safety function cannot be correctly executed. Depending on the SIL, the PFH must not exceed certain values for the entire safety system. The individual PFH values of a function chain are added. The result must not exceed the maximum value specified in the standard.

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

PL - Performance level

The standard IEC 13849-1 defines 5 Performance levels (PL) for safety functions. “a” is the lowest level and “e” is the highest level. Five level (a, b, c, d, e) correspond to different values of average probability of dangerous failure per hour.

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

HFT - hardware detected fault tolerance and SFF - Safe Failure Fraction

Depending on the SIL for the safety system, the IEC 61508 standard *and SFF, Safe Failure Fraction* requires a specific hardware detected fault tolerance HFT in connection with a specific proportion of safe failures SFF (safe failure fraction).
The hardware detected fault tolerance is the ability of a system to execute the required safety function in spite of the presence of one or more hardware detected faults.
The SFF of a system is defined as the ratio of the rate of safe failures to the total failure rate of the system.
According to IEC 61508, the maximum achievable SIL of a system is partly determined by the hardware detected fault tolerance HFT and the safe failure fraction SFF of the system.
IEC 61508 distinguishes two types of subsystems (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	

Detected fault avoidance measures

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

Description

3

What's in this Chapter?

This chapter contains the following topics:

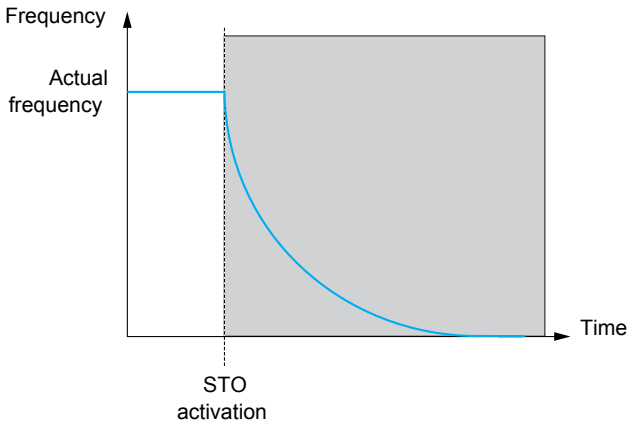
(STO) Safe Torque Off

The purpose of this function is to bring the motor into a no torque condition with motor coasts down or prohibits the motor from starting. So it is relevant in terms of safety since no torque is available at the motor level.

The logic input “STO” is always assigned to this function.

If a paired terminal line in two channels is required for control of STO, the function can be enabled also by the safe logic inputs.

The STO status is accessible with the drive or with SoMove.



STO Normative reference

The normative definition of STO function is in §4.2.2.2 of the IEC 61800-5-2:

"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 with safety-related functions) 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 help 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 help prevent any hazard.

NOTE 4 Electronic means and contactors are not adequate for protection against electric shock, and additional measures for isolation may be necessary."

Safety function (SF) level required for STO function

Configuration	**SIL** *(Safety Integrity Level)* according to IEC 61-508	**PL** *(Performance Level)* according to ISO-13849
STO with or without Preventa module	SIL 2	PL "d"
STO & LI3 with or without Preventa module	SIL 3	PL "e"
LI3 & LI4	SIL 2	PL "d"
LI5 & LI6	SIL 2	PL "d"

The Preventa module is required for the machine environment because:

- For the machine environment (IEC60204-1 & Machine Directive), reset shall not initiate a restart in any cases. One of the most constringent case is when STO is activated, then the power supply is switch off. In this case, if STO is deactivated during the loss of supply, the motor do not have to restart automatically. The Preventa module can prevent a spurious restart in the previous condition. So the Preventa module is mandatory for machine applications.
- E_stop of several BDM in a PDS: the Preventa module has some safety outputs for application which requires one or several safety outputs.

For other environments, the Preventa module is not required, except if the application requires it: System fallback position.

(SS1) Safe Stop 1

Description

This function is used to stop the motor following a dedicated down ramp. The motor speed is monitored during the down ramp. STO is initiated when the motor speed is below a specified threshold.

The unit of SS1 down ramp is in Hz/s to get the shape of the ramp you need to configure 2 parameters

[SS1 ramp unit] (S S r U) (Hz/s) to give the unit of the ramp 1 Hz/s, 10Hz/s and 100 Hz/s.

[SS1RampValue] (S S r t) (0,1) to set the value of the ramp

Ramp calculation: ramp = SSRU*SSRT

Example: if SSRU = 10 Hz/s and SSRT= 50 the down ramp is 50 Hz/s.

When the function is activated, the SS1 function has the reference priority over all other reference channels.

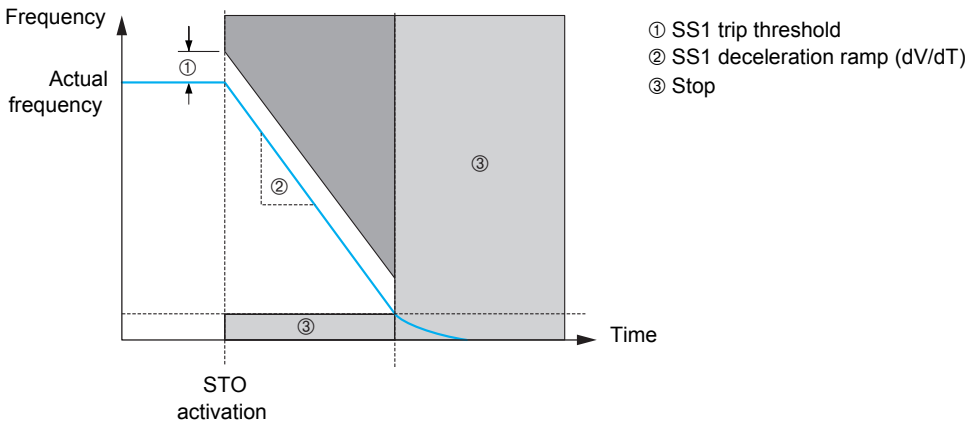
When a fault is detected within the safety function, the drive will trip and stop using the internal STO command.

This safety function is configured with SoMove software, see Commissioning page 55.

The SS1 status is accessible with the drive or with SoMove

Behavior at the activation of SS1 function

The SS1 function monitors the Motor Speed and check the **[SS1 trip threshold]** (S S t t)
During the SS1 ramp, if the trip area is reached, drive trip in S A F F and the drive stop in free wheel.
When the Motor Speed reaches the **[Standstill level]** (S S S L) a STO is set.
The protections depend on the stator frequency.



Behavior at the deactivation of SS1 function

After a SS1 stop, give a new run order (even if the run order is set as level)

If the SS1 request disappeared before the end of safe function, the safe function continues to run until STO is reached.

SS1 Normative reference

The normative definition of SS1 function is in §4.2.2.2 of the IEC 61800-5-2:

"The PDS(SR) (Power Drive System with safety-related functions) either
Type B. 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
Type C. 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.

In accordance with the IEC 60204-1, the SS1 function generates a stop category 1 for the PDS generates a stop category 0 after:

- the motor stop (when the motor speed is below a specified limit)
- or an application specific time delay.

Safety function (SF) level required for SS1 function

Function	**Configuration**	**SIL Level** *(Safety Integrity Level* **)** according to IEC 61-508	**PL** *(Performance Level)* according to ISO-13849
SS1 Type C	STO with Preventa module	SIL 2	PL "d"
	STO and LI3 with Preventa module	SIL 3	PL "e"
SS1 Type B	LI3 and LI4	SIL 2	PL "d"
	LI5 and LI6	SIL 2	PL "d"

(SLS) Safely Limited Speed

Description

This function is used to limit a machine speed. The main goal is to monitor the motor speed and to adjust the speed to a set point.

This function offers 3 types:

- SLS type 1: used to monitor the motor speed and trips in STO in case of over speed.
- SLS type 2: used to limit the motor speed to a set point and trips in STO in case of over speed.
- SLS type 3: Same as type 2 with a dedicated behavior when the motor speed is above the tolerance threshold. Trips in STO in case of over speed.

When the function is activated, the SLS function has the reference priority to all others reference channel. This safety function is configured with SoMove software, see commissioning. The SS1 status is accessible with the drive or with SoMove

Behavior at the activation of SLS function

SLS type 1

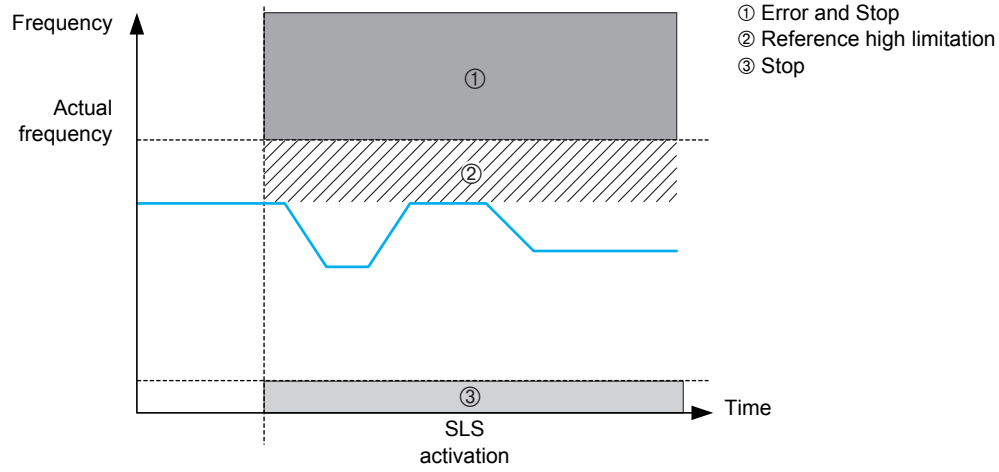
When the function is activated,

- if the current frequency or stator frequency is above the **[SLS tolerance threshold]** (S L t t), the SAFF detected fault is trigged,
- if the current frequency or stator frequency is under the **[SLS tolerance threshold]** (S L t t), the speed is limited to the actual speed. The main reference channel can only decrease the speed reference.

While the function is activated

- If the current frequency decrease and reach the **[Standstill level]** (S S S L) frequency, STO is activated.

If the current frequency or stator frequency increase and reach the **[SS1 trip threshold]** (S L t t), drive trips in SAFF detected fault



SLS type 2

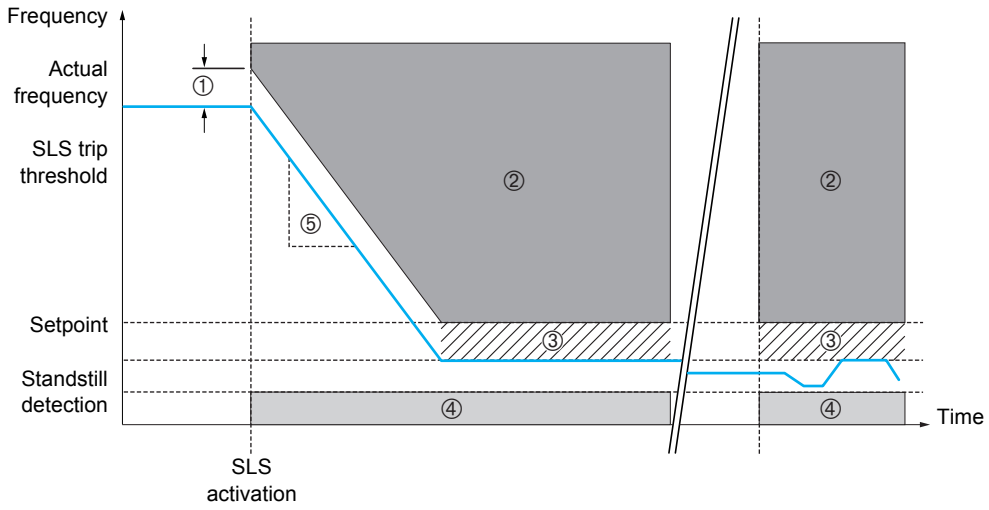
When the function is activated,

- If the current frequency is above the **[SLS tolerance threshold]** (S L t t), the drive decelerates until the **[Set point]** (S L S P) frequency with the same ramp as SS1 function.
- If the current frequency is under the **[SLS tolerance threshold]** (S L t t) and upper the **[Set point]** (S L S P), the drive decelerates until the **[Set point]** (S L S P) frequency with the same ramp as SS1 function.
- If the current frequency is under the **[Set point]** (S L S P), the speed is high limited by the set point.

Once the **[Set point]** (S L S P) is reached, is it still possible to vary the reference speed between [Standstill level] (SSSL) and the **[Set point]** (S L S P).

While the function is activated

- If the current frequency decrease and reach the **[Standstill level]** (S S S L) frequency, STO is activated.
- If the current frequency or stator frequency increase and reach the **[SS1 trip threshold]** (S L t t), drive trips in SAFF detected fault



① SS1 trip threshold
② Error and Stop
③ Reference high limitation
④ Stop
⑤ SS1 deceleration ramp (dV/dT)

SLS type 3

When the function is activated,

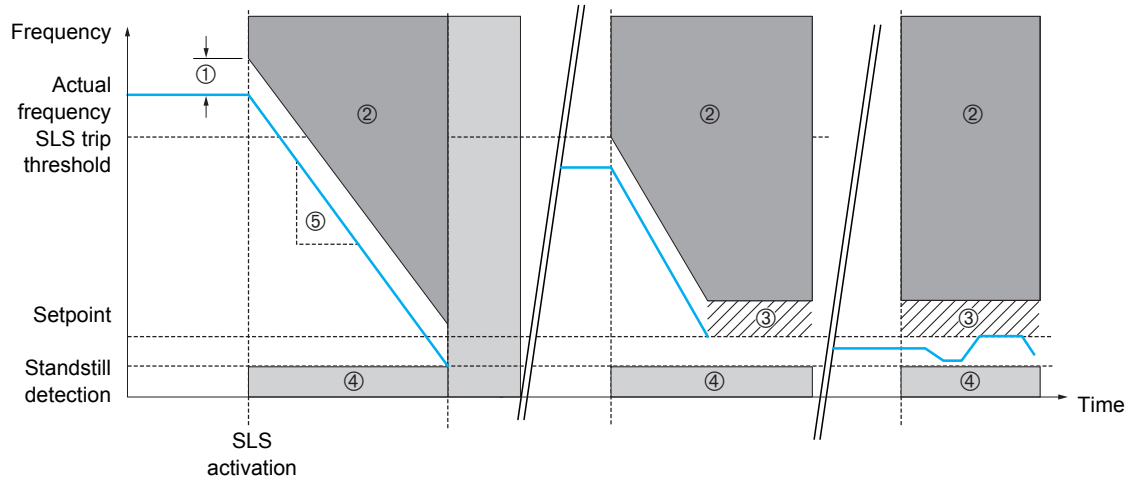
- If the current frequency is above the **[SLS tolerance threshold]** (SLtt) the drive decelerates until the [Standstill level] (SSSL) frequency with the same ramp as SS1 function.
- If the current frequency is under the **[SLS tolerance threshold]** (SLtt) and upper the **[Set point]** (SLSP), the drive decelerates until the **[Set point]** (SLSP) frequency with the same ramp as SS1 function.
- If the current frequency is under the **[Set point]** (SLSP), the current reference is not changed but limited to the **[Set point]** (SLSP).

While the function is activated,

- If the current frequency decrease and reach the **[Standstill level]** (SSSL) frequency, STO is activated.
- If the current frequency or stator frequency increase and reach the **[SS1 trip threshold]** (SLtt), drive trips in SAFF detected fault.

The **[Set point]** (SLSP), is linked to the rotor frequency.

.



① SS1 trip threshold
② Error and Stop
③ Reference high limitation
④ Stop
⑤ SS1 deceleration ramp (dV/dT)

Behavior at the deactivation of SLS function

For all SLS types

If the drive is still running when the function is deactivated, the main reference and the current run order is applied.

If the drive is already stopped (STO or end of SS1) a new run order must be set to restart.

If the SLS request disappeared before the end of SS1 deceleration, the safe function continues to run until **[Set point]** (SLSP) or **[Standstill level]** (SSSL) are reached.

When a stop order appeared, the drive stops even if a safe function is activated (but the safe function stays active and continues to monitor the trip area). A stop order has the priority to safe function.

If a detected fault appeared when a safe function is configured, the drive stops following the detected fault reaction configured and a new run order must be set to restart.

SLS Normative reference

The normative definition of SLS function is in §4.2.3.4 of the IEC 61800-5-2 "The SLS function helps to prevent the motor from exceeding the specified speed limit".

The safety function (SF) level required for SLS function is:

Configuration	**SIL** *(Safety Integrity Level* **)** according to IEC 61-508	**PL** *(Performance Level)* according to ISO-13849
LI3 & LI4 : SLS	SIL 2	PL "d"
LI5 & LI6 : SLS	SIL 2	PL "d"

Formulas for calculation of safety parameters

4

What's in this Chapter?

This chapter contains the following topics:

SLS type 1

Collect application data

Before beginning the configuration of the SLS function, you must collect the following data:

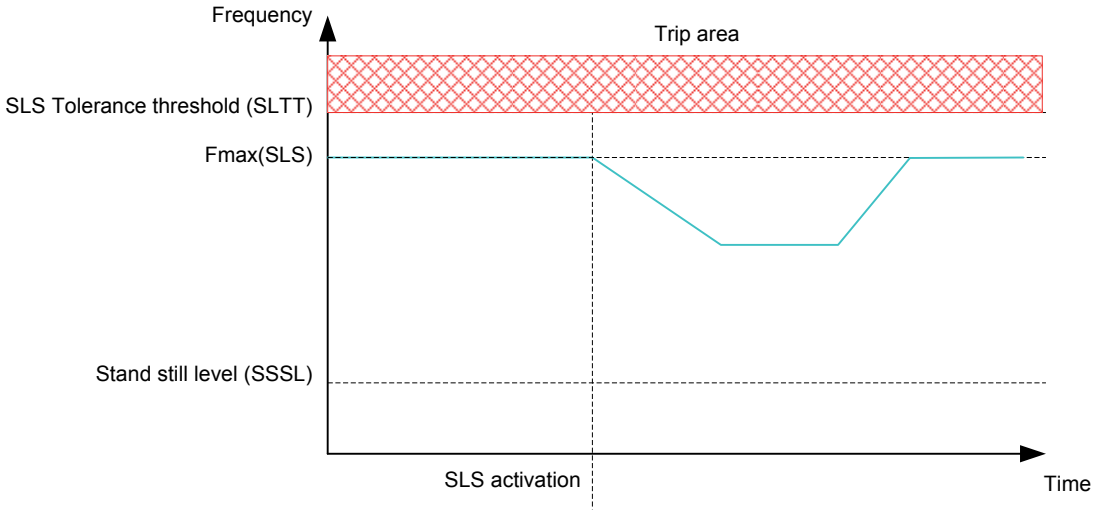
Code	Description	Unit	Comment
Fn	Rated motor frequency	Hz	From motor
Nsp	Rated motor speed	rpm	From motor
Np	Motor pole pair number	Ø	From motor
Fmax(SLS)	Maximum motor frequency during SLS type 1	Hz	Maximum motor frequency when the SLS type 1 function: ● is about to be activated ● is used

First, compute the rated motor slip frequency Fslip (Hz). It will be used afterward:

$$Fslip = Fn - \frac{Nsp \times Np}{60}$$

Configure the function

Overview diagram



Standstill level

The recommended standstill level is:

$$SSSL = Fslip$$

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

Protection threshold

The SLS tolerance threshold is computed by:

$$SLTT = 1,2 \times Fmax(SLS) + Fslip$$

Test & adjust configuration

When the configuration is done, test the SLS function to check if the behaviour is as expected.

If a SAFF detected fault happens during the test, check with the following troubleshooting rules:

Context	Problem	Adjustment
SLS activated and motor running at the frozen set-point frequency	- SAFF detected fault - SFFE.7 = 1	Motor frequency reached the tolerance threshold. Increase SLTT by steps of 1Hz and test again until the SAFF no longer happens: $SLTT > 1,2 \times Fmax(SLS) + Fslip$ If the difference between the corrected SLTT and the recommended one is important, investigate the cause of the frequency instability.

Example

Code	Description	Value
Fn	Rated motor frequency	50 Hz
Nsp	Rated motor speed	1350 rpm
Np	Motor pole pair number	2
Fmax(SLS)	Maximum motor frequency during SLS type 1	50 Hz

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

$$Fslip = 50 - \frac{1350 \times 2}{60} = 5Hz$$

$$SSSL = Fslip = 5Hz$$

$$SLTT = 1,2 \times Fmax(SLS) + Fslip = 1,2 \times 50 + 5 = 65Hz$$

SLS type 2 & type 3

Collect application data

Before beginning the configuration of the SLS function, you must collect the following data:

Code	Description	Unit	Comment
Fn	Rated motor frequency	Hz	From motor
Nsp	Rated motor speed	rpm	From motor
Np	Motor pole pair number	Ø	From motor
Fmax(SLS)	Maximum motor frequency when SLS type 2/3 is activated	Hz	Maximum motor frequency when the SLS type 2/3 function is about to be activated
Fsetpoint(SLS)*	Motor frequency set-point	Hz	User defined. Frequency set-point that the SLS type 2/3 function must reach.
D*	Ramp deceleration	Hz/s	User defined. Ramp deceleration used on SLS activation

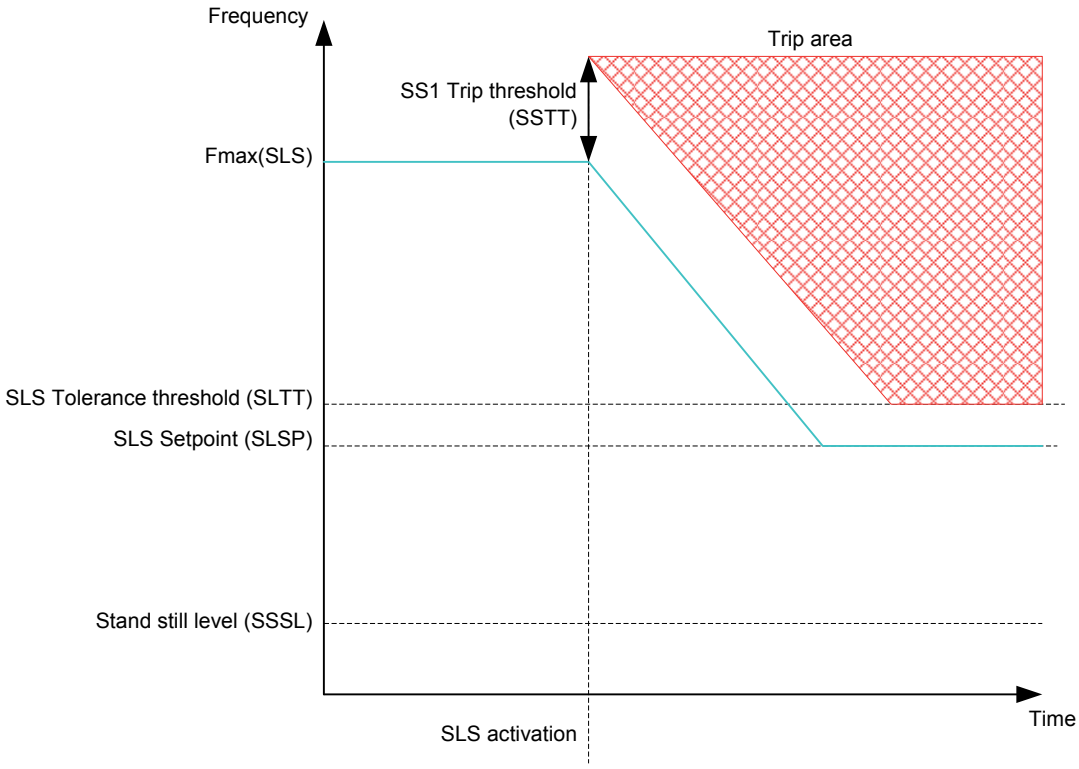
* Before configuring the SLS function, Fsetpoint(SLS) and D must be defined by you.

First, compute the rated motor slip frequency Fslip (Hz). It will be used afterward:

$$Fslip = Fn - \frac{Nsp \times Np}{60}$$

Configure the function

Overview diagram



Standstill level

The recommended standstill level is:

$$SSSL = Fslip$$

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

Ramp value and ramp unit

Depending on the your selected deceleration, set SSRT (ramp value) and SSRU (ramp unit) parameters according to the deceleration range which includes D and the available accuracy:

Min	Max	Accuracy	SSRU	SSRT
0.1 Hz/s	599 Hz/s	0.1 Hz/s	[1 Hz/s]	D
599 Hz/s	5990 Hz/s	1 Hz/s	[10 Hz/s]	D/10
5990 Hz/s	59900 Hz/s	10 Hz/s	[100 Hz/s]	D/100

SLS set-point

Set the SLS set-point parameter (SLSP) to:

$SLSP = Fsetpoint(SLS)$

Protection thresholds

The SLS tolerance threshold is computed by:

$SLTT = 1,2 \times SLSP + Fslip$

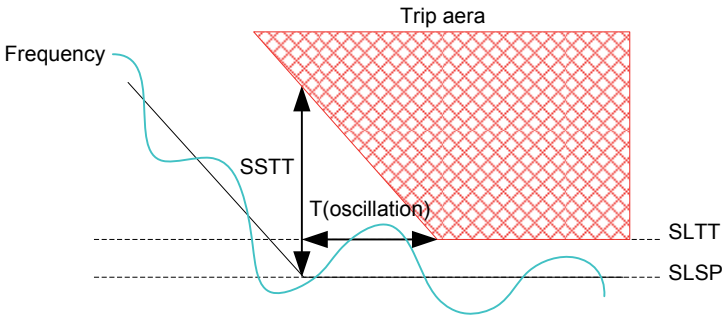
And the SS1 ramp trip threshold is computed by:

SLTT = 0.2 x *Fmax (SLS) + (SLTT – SLSP – Fslip)*

Test & adjust configuration

When the configuration is done, test the SLS function to check if the behaviour is as expected.

If a SAFF detected fault happens during the test, check with the following troubleshooting rules:

Context	Problem	Adjustment
SLS activated and deceleration ramp in progress	- SAFF detected fault - SFFE.3 = 1	Motor frequency reached the trip area. Increase SSTT by steps of 1Hz and test again until the SAFF no longer happens: *SLTT* > 0.2 x *Fmax (SLS) + (SLTT – SLSP – Fslip)* If the difference between the corrected SSTT and the recommended one is important, investigate the cause of the frequency instability.
SLS activated and end of ramp at SLSP frequency	SAFF detected fault SFFE.3 = 1 or SFFE.7 = 1	Motor frequency stabilization at SLSP takes too much time and reached the trip aera  The oscillations must be lower than SLTT before the time T(oscillation) is elapsed. If it is not, the frequency will reach the trip area and an detected SAFF fault will be triggered. The relationship between SSTT and T(oscillation) is: $T(oscillation) = \frac{SSTT - (SLTT - SLSP - Fslip)}{SSRT \times SSRU}$ If more time is required for stabilization, increase SSTT by steps of 1 Hz and test again until the SAFF no longer happens. If the elapsed time required for oscillations to be under SLTT is known, compute SSTT directly: $SSTT = T(oscillation)_{new} \times SSRT \times SSRU + (SLTT - SLSP - Fslip)$ If the difference between the corrected SSTT and the recommended one is important, investigate the cause of the frequency instability.

Context	Problem	Adjustment
SLS activated and motor running at SLSP frequency	SAFF detected fault SFFE.7 = 1	Motor frequency reached the tolerance threshold. Increase SLTT by steps of 1Hz and test again until the SAFF no longer happens: $SLTT > 1,2 \times SLSP + Fslip$ If the difference between the corrected SSTT and the recommended one is important, investigate the cause of the frequency instability.

Example

Code	Description	Value
Fn	Rated motor frequency	50 Hz
Nsp	Rated motor speed	1350 rpm
Np	Motor pole pair number	2
Fmax(SLS)	Maximum motor frequency when SLS type 2/3 is activated	50 Hz
Fsetpoint(SLS)	Motor frequency set-point	15 Hz
D	Ramp deceleration	20 Hz/s

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

$$Fslip = 50 - \frac{1350 \times 2}{60} = 5Hz$$

$$SSSL = Fslip = 5Hz$$

D = 20 *Hz*/*s* which is between 0.1 *Hz*/*s* and 599 *Hz*/*s* so SSRU = [1 *Hz*/*s*] and *SSRT* = 20.0

$$SLSP = Fsetpoint(SLS) = 15Hz$$

$$SLTT = 1,2 \times SLSP + Fslip = 1,2 \times 15 + 5 = 23Hz$$

$$SSTT = 0,2 \times Fmax(SLS) + (SLTT - SLSP - Fslip) = 0,2 \times 50 + (23 - 15 - 5) = 13Hz$$

$$T(oscillation) = \frac{SSTT - (SLTT - SLSP - Fslip)}{SSRT \times SSRU} = \frac{13 - (23 - 15 - 5)}{20 \times 1} = 500ms$$

In this example, the frequency oscillations are allowed over SLTT during 500ms.

SS1

Collect application data

Before beginning the configuration of the SS1 function, you must collect the following data:

Code	Description	Unit	Comment
Fn	Rated motor frequency	Hz	From motor
Nsp	Rated motor speed	rpm	From motor
Np	Motor pole pair number	Ø	From motor
Fmax(SS1)	Maximum motor frequency when SS1 is activated	Hz	Maximum motor frequency when the SS1 function is about to be activated
D*	Ramp deceleration	Hz/s	User defined. Ramp deceleration used on SLS activation

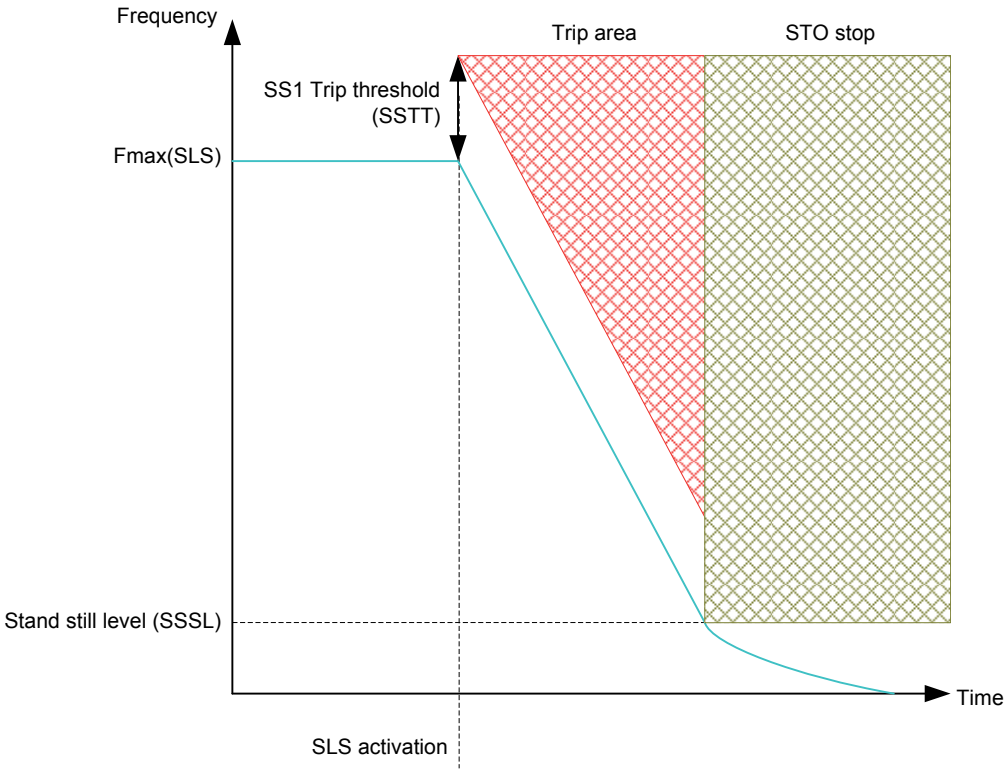
* Before configuring the SS1 function, D must be defined by you.

First, compute the rated motor slip frequency Fslip (Hz). It will be used afterward:

$$Fslip = Fn - \frac{Nsp \times Np}{60}$$

Configure the function

Overview diagram



Standstill level

The recommended standstill level is:
$SSSL = Fslip$

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

Ramp value and ramp unit

Depending on the user-selected deceleration, set SSRT (ramp value) and SSRU (ramp unit) parameters according to the deceleration range and available accuracy:

Min	Max	Accuracy	SSRU	SSRT
0.1 Hz/s	599 Hz/s	0.1 Hz/s	[1 Hz/s]	*D*
599 Hz/s	5990 Hz/s	1 Hz/s	[10 Hz/s]	*D*/10
5990 Hz/s	59900 Hz/s	10 Hz/s	[100 Hz/s]	*D*/100

Protection threshold

The SS1 ramp trip threshold is computed by:
$SSTT = 0,2 \times Fmax(SS1)$

Test & adjust configuration

When the configuration is done, test the SS1 function to check if the behaviour is as expected.

If a SAFF detected fault happens during the test, check with the following troubleshooting rules:

Context	Problem	Adjustment
SS1 activated and deceleration ramp in progress	- SAFF detected fault - SFFE.3 = 1	Motor frequency reached the trip area. Increase SSTT by steps of 1Hz and test again until the SAFF no longer happens: $SSTT > 0,2 \times Fmax(SS1)$ If the difference between the corrected SSTT and the recommended one is important, investigate the cause of the frequency instability.

Example

Code	Description	Value
Fn	Rated motor frequency	50 Hz
Nsp	Rated motor speed	1350 rpm
Np	Motor pole pair number	2
Fmax(SS1)	Maximum motor frequency when SS1 is activated	50 Hz
D	Ramp deceleration	20 Hz/s

With these numerical values, the configuration of SS1 is:

$$Fslip = 50 - \frac{1350 \times 2}{60} = 5Hz$$

$SSSL = Fslip = 5Hz$

D = 20 *Hz*/*s* which is between 0.1 *Hz*/*s* and 599 *Hz*/*s* so SSRU = [1 *Hz*/*s*] and *SSRT* = 20.0

$SSTT = 0,2 \times Fmax(SS1) = 0,2 \times 50 = 10Hz$

Incompatibility with safety functions

5

What's in this Chapter?

This chapter contains the following topics:

Limitations

Type of Motor

SLS and SS1functions on ATV32 are applicable only for asynchronous motors without encoder.

STO can be used with synchronous and asynchronous motors.

Prerequisites for using safety functions

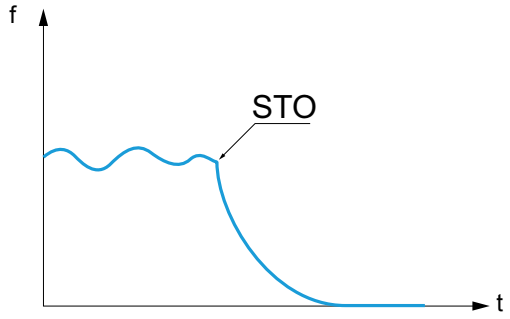
Some parameters have to be fulfilled for a proper operation:

- Motor size is adequate to the application and is not in the limit of its capacity
- Speed drive size has been properly chosen for the electrical mains, sequence, motor and application and it is not in the limit of their catalogued capacities.
- If required, the adequate options are used. Example: like dynamic brake resistor or motor inductor.
- The drive is properly setting up for the right speed loop and torque characteristics for the application; the speed profile of the reference is mastered by the drive control loop.

Allowed and unallowed application for safety function

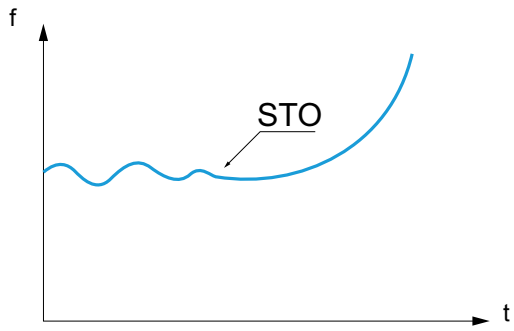
Allowed application

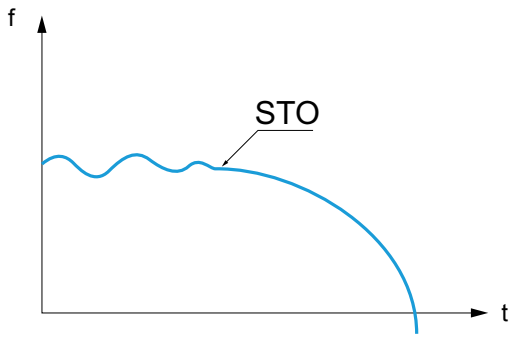
Allowed sharp of stop after STO request or freewheel stop



Unallowed application

Application with acceleration of the load after shut down of the drive or where there are long/permanent regenerative braking cycles are not allowed. Unallowed sharp of stop after STO request or freewheel stop.





Examples: vertical conveyors, vertical hoist, lifts or winders.

Limitation on logical input

- The sink mode is incompatible with safety function. If you use safety function, you need to wire your logical input in source mode.
- PTC on LI6 is incompatible with safety function set on this input. If you use functional safety on LI6 don’t set PTC switch on PTC.
- If you use the pulse input, you can’t set safety function on LI5 at the same time.

Fault Inhibition

For some kind of detected fault, **[Fault inhibit assign.]** (InH) can be requested to avoid the drive to stop when the fault occurred. The fault inhibition goal is not compatible with the safe function behavior.

When a safe function is activated, detected fault generated by the safe function SAFF can't be inhibited.

Configuration download

In order to protect people and machine the configuration download of safe parameters is impossible with any kind of tools. Configuration download as SoMove, keypad, Simple-loader, Multi-loader, Ethernet or mobile phone are not possible.

With a configuration download, the parameters are downloaded in the drive, except the safe parameters.The user can transfer a configuration in all situations. If a safety function has been activated, the functions using these same LI are no longer configured.

Note: If the downloaded configuration have functions (Preset speed,...) on LI3-4-5-6 and if the drive has a safety function configured on LI, safety function will not be erased. It is the functions that have the same LI as safety functions that are not transfered. Multiconfiguration/multimotor and macroconfiguration obey the same rules.

Factory settings

If the drive is in safe mode and you active the factory settings only non safety parameters will be downloaded in the drive. Safe parameters are not impacted by factory settings.

Priority between safety functions

1 STO has the higher priority. If the STO function is trigged, a safe torque off is managed whatever the others active functions.
2 SS1 has the medium priority to the other safe functions
3 SLS has the lower priority

Priority between safety and drive functions

o : Compatible functions

x : Incompatible functions

▲◄: The function indicated by the arrow has priority over the other.

Drive function	SLS	SS1	STO
[BRAKE LOGIC CONTROL] bLC -	x	x	x
[HIGH SPEED HOISTING] HSH -	▲	▲	▲
[+/- SPEED] UPd -	▲	▲	▲
[Skip Frequency] JPF	▲	o	o
[Low speed time out] tLS	▲	▲	▲
[MULTIMOTORS] MMC -	Configuration must be consistent with the 3 motors		o
[PRESET SPEEDS] PSS -	▲	▲	▲
[PID REGULATOR] PId -	▲	o	o
[RAMP] rPt -	▲	▲	▲
[Freewheel stop ass.] nSt	◄	◄	▲
[Fast stop assign.] FSt	◄	▲	▲
[TRAVERSE CONTROL] trO -	**o** : both function's configurations mustn't overlap. **o** : motor frequency can exceed SLS set-point (but not the trip area)	▲	▲
[FAULT MANAGEMENT] FLt -	◄ : NST, fast, ramp **x** : DCI ▲: fallback, maintain	◄ : NST **x** : DCI ▲: fast, ramp, fallback, maintain	◄ : NST ▲: DCI ▲: fast, ramp, fallback, maintain
[EXTERNAL FAULT] EtF -	◄ : NST **x** : DCI ▲: fast, ramp, fallback, maintain	◄ : NST **x** : DCI ▲: fast, ramp, fallback, maintain	◄ : NST ▲: DCI ▲: fast, ramp, fallback, maintain
[AUTOMATIC RESTART] Atr -	▲	▲	▲
[FAULT RESET] rSt -	▲	▲	▲
[JOG] JOG -	▲	▲	▲
[STOP CONFIGURATION] Stt -			
[Ramp stop] rMP	▲ : SLS ramp ◄ : SLS steady	▲	▲

Drive function	SLS	SS1	STO
[Fast stop] F S t	▲ : SLS ramp ◄ : SLS steady	▲	▲
[DC injection] d C I	x	x	▲
[Freewheel] n S t	◄	◄	▲
[+/-SPEED AROUND REF.] S r E -	▲	▲	▲
[POSITIONING BY SENSORS] L P O -	▲ : SLS ramp & position is not respected	▲ : Position is not respected	▲
[RP input] P F r C	**o** : if LI5 is not use by the safety function	**o** : if LI5 is not use by the safety function	**o** : if LI5 is not use by the safety function
[Underload Detection] U L F	▲	▲	▲
[Overload Detection] O L C	▲	▲	▲
[Rope slack config.] r S d	x	x	x
[UnderV. prevention] S t P	x	x	▲
[AUTO DC INJECTION] A d C -	x	x	▲
[DC injection assign.] d C I	x	x	▲
[Load sharing] L b A	**o** : if the adapted load sharing frequency reaches the trip area, SAFF fault is trigged	▲	▲
[Motor control type] C t t			
[Standard] S t d	x	x	o
[SVC V] U U C	o	o	o
[V/F Quad.] U F 9	x	x	o
[Energy Sav.] n L d	x	x	o
[Sync. mot.] S Y n	x	x	o
[V/F 5pts] U F S	x	x	o
[OUTPUT PHASE LOSS] O P L	**x** : Motor output phase loss is detected by the safe function	**x** : Motor output phase loss is detected by the safe function	o
[Output cut] O A C	x	x	x
[Dec ramp adapt.] b r A	**o** : if ramp adaptation reaches a trip area, SAFF fault is triggered	**o** : if ramp adaptation reaches a trip area, SAFF fault is triggered	▲
[REF. OPERATIONS] O A I -	▲	▲	o
[2 wire] 2 C	**o** : Run order on transition ▲Run order on level is not compatible	**o** : Run order on transition ▲Run order on level is not compatible	**o** : Run order on transition ▲Run order on level is not compatible
[PTC MANAGEMENT] P t C -	**o** : if LI6 is not use by the safety function	**o** : if LI6 is not use by the safety function	**o** : if LI6 is not use by the safety function
[FORCED LOCAL] L C F -	▲	▲	o
[LI CONFIGURATION]	**o** : inactive if LI is used by safety fct	**o** : inactive if LI is used by safety fct	**o** : inactive if LI is used by safety fct
[MULTIMOTORS/CONFIG.] n n C-	**o** : except safety parameters	**o** : except safety parameters	**o** : except safety parameters
[FAULT INHIBITION] I n H	x	x	x
[Profile] C H C F	LI used by safety fct can not be switched	LI used by safety fct can not be switched	LI used by safety fct can not be switched
[Macro configuration] C F G	▲: Macro configuration could be overlaped if safety function use a logical input requested by the macro conf	▲: Macro configuration could be overlaped if safety function use a logical input requested by the macro conf	▲: Macro configuration could be overlaped if safety function use a logical input requested by the macro conf
[RAMP] r P t -	▲ : SLS ramp ◄ : SLS steady	▲	o
[Motor short circuit] S C F I	▲	▲	o
[Ground short circuit] S C F 3	▲	▲	o
[Overspeed] S O F	▲	▲	o
[Sync. mot.] S Y n	x	x	o
ConfigurationTransfer	**o** : except safety parameters	**o** : except safety parameters	**o** : except safety parameters
[Energy Sav.] n L d	x	x	o

For more information about those functions see ATV32 Programming manual.

Safety monitoring

6

What's in this Chapter?

This chapter contains the following topics:

Status of safety functions

With the HMI on the drive you can't configure safety functions, only monitoring can be done. There is one monitoring parameter for each safety function. See Introduction for more information of safety function.

To access this parameter by keypad or HMI: **[2 MONITORING]** (MOn-) => **[MONIT. SAFETY]** (SAF-)

- **[STO status]** (StOS): Status of the Safe Torque Off safety function
- **[SLS status]** (SLSS): Status of the Safe Limit speed safety function
- **[SS1 status]** (SS1S): Status of the Safe Stop 1 safety function

These statuses are not certified safety, they are informative.

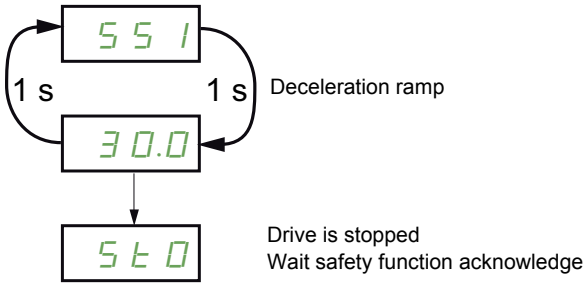
For more information see the ATV32 programming manual on www.schneider-electric.com.

Dedicated HMI

When a safe function is activated, some dedicated messages can be displayed and some status word can be set.

Embedded keypad and LED keypad: Display the active safe function (STO, SS1, SLS) alternate with monitoring parameter.

LED display on SS1 function:



Detected fault given by the drive

When fault is detected on safety function drive trips in **[Safety fault]** (SAFF). Drive can only be reseted by a power OFF/ON.

For further information you can access the register to know possible cause of trip,

Safety Function detected Fault Error register (SFFE) accessible with graphic keypad:

DRIVE MENU -> MONITORING -> DIAGNOSTIC -> MORE FAULT INFO -> Safety Function detected Fault Error register

Or

DRIVE MENU -> MONITORING -> MONIT. SAFETY -> Safety Function detected Fault Error

It is also accessible with the integrated display terminal DRI -> MON -> SAF -> SFFE

SFFE register

Bit0=1	logical input debounce time out (check value of Debounce time LIDT in accordance with the application)
Bit1	Reserved
Bit2=1	Motor speed sign change during SS1 ramp
Bit3=1	Motor speed reached SS1 trip area
Bit4	Reserved
Bit5	Reserved
Bit6=1	Motor speed sign change during SLS limitation
Bit7=1	Motor speed reached SS1 trip area
Bit8	Reserved
Bit9	Reserved
Bit10	Reserved
Bit11	Reserved
Bit12	Reserved
Bit13=1	Motor speed measurement is not possible (check wiring motor connection)
Bit14=1	Motor ground short circuit detected (check wiring motor connection)
Bit15=1	Motor phase to phase short circuit detected (check wiring motor connection)

This parameter is reset after Power OFF/ON.

Technical data

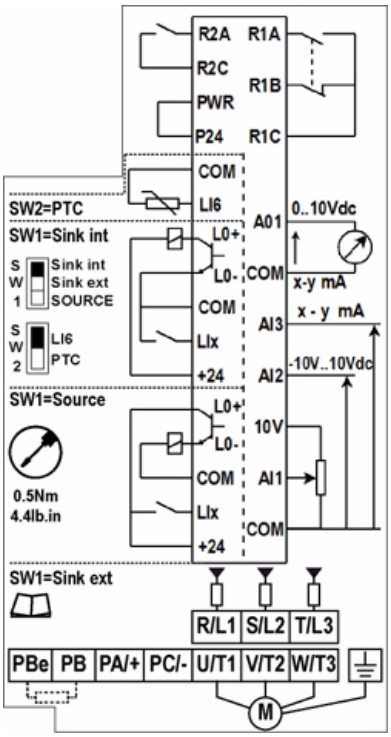
7

What's in this Chapter?

This chapter contains the following topics:

Electrical Data

The Logic inputs and Logic outputs of the drive can be wired for logic type 1 or logic type 2.



Logic Type	Active state
1	Output draws current (Sink) Current flows to the input
2	Output supplies flows from the input Current Current (Source)

Safe function only used in source mode, sink is not compatible with safe functions.

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

Logical input for safety function

General logical inputs can be used to trig a safe function. Logical inputs have to be combined by pair to get a redundant request. There are only 4 general logical inputs linkable to safety functions (LI3, LI4, LI5, LI6). The pairs of logical inputs are fixed and are:

- LI3 and LI4,
- LI5 and LI6,
- An other combination is possible only for STO function: LI3 and STO.

The pairs of logical inputs are mono assignable when they are linked to a safety function. When you set a safety function on a LI you can’t set an other function (safe or not safe) on this LI. If you set a non safe function on a LI you can’t set a safe function on this LI.

Safety function capability

Safety functions of PDS (SR) are part of a global system.

If qualitative and quantitative objectives of safety set by the final application requires to make some adjustments to use the safety functions in a safe way, then the integrator of the BDM is responsible of these complementary evolutions (for example management of the mecanichal brake on the motor).

Also, the output information generated by the utilization of safety functions (default relay activation, relay of brake logic command, errors codes or information on the display, …) aren't considering safety informations.

Machine application

Function	**STO**		**SS1 type C**		**SLS**	
Configuration / **Standard**	**STO with Preventa XPS AF or equivalent**	**STO and LI3 with Preventa XPS AF or equivalent**	**STO with Preventa XPS ATE or XPS AV or equivalent**	**STO and LI3 with Preventa XPS ATE or XPS AV or equivalent**	**LI3 LI4**	**LI5 LI6**
IEC 61800-5-2 / IEC 61508 /	SIL2	SIL3	SIL2	SIL3	SIL2	
IEC 62061 (1)	SIL2 CL	SIL3 CL	SIL2 CL	SIL3 CL	SIL2 CL	
EN 954-1 (2)	Category 3	Category 4	Category 3	Category 4	Category 3	
ISO 13849-1 (3)	Category 3 PL "d"	Category 4 PL "e"	Category 3 PL "d"	Category 4 PL "e"	Category 3 PL "d"	
IEC 60204-1	Category stop 0	Category stop 0	Category stop 1	Category stop 1		

(1) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 or SIL3 for ATV32 according to diagrams Process system SF - Case 1, page 50 and Process system SF - Case 2, page 51) from components which constitute the safety function (which is classify SIL2 CL or SIL3 CL for ATV32)

(2) According to table 6 of IEC 62061 (2005)

(3) According to table 4 of EN13849-1 (2008)

Process application

Function	**STO**		**SS1 type C**		**SLS SS1 type B STO**	
Configuration / **Standard**	**STO**	**STO and LI3**	**STO with Preventa XPS ATE or XPS AV or equivalent**	**STO and LI3 with Preventa XPS ATE or XPS AV or equivalent**	**LI3 LI4**	**LI5 LI6**
IEC 61800-5-2 / IEC 61508 /	SIL2	SIL3	SIL2	SIL3	SIL2	
IEC 62061 (1)	SIL2 CL	SIL3 CL	SIL2 CL	SIL3 CL	SIL2 CL	

(1) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 or SIL3 for ATV32 according to diagrams Process system SF - Case 1, page 50 and Process system SF - Case 2, page 51) from components which constitute the safety function (which is classify SIL2 CL or SIL3 CL for ATV32)

Input signals safety functions

Input signals safety functions	**Units**	Value for LI3 to LI6	**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

Synthesis of the dependability study

Function	Standard	Input	STO input	STO Input & LI3	LI3 & LI4 or LI5 & LI6
STO	IEC 61508 Ed.2	SFF	96.7%	96%	94.8%
		PFD_{10y}	$7.26.10^{-4}$	$4.00.10^{-4}$	$2.44.10^{-3}$
		PFD_{1y}	$7.18.10^{-5}$	$3.92.10^{-5}$	$2.33.10^{-4}$
		PFH_{equ_1y}	8.20 FIT (1)	4.47 FIT (1)	26.6 FIT (1)
		Type	B	B	B
		HFT	1	1	0
		DC	93.1%	91.5%	90%
		SIL capability	**2**	**3**	**2**
	IEC 62061 (2)	SIL CL capability	2	3	2
	EN 954-1 (3)	Category	3	4	3
	ISO 13849-1 (4)	PL	d	e	d
		Category	3	4	3
		MTTFd in years	13900	"L1" 3850 "L2" 29300	4290
SS1 type B SLS	IEC 61508 Ed.2	SFF			93.3%
		PFD_{10y}			$2.72.10^{-3}$
		PFH_{equ_10y}			31.1 FIT (1)
		Type			B
		HFT			0
		DC			78.7%
		SIL capability			**2**
	IEC 62061 (2)	SIL CL capability			2
	EN 954-1 (3)	Category			3
	ISO 13849-1 (4)	PL			d
		Category			3
		MTTFd in years			3670

(1) FIT : Failure In Time = Failure/10^{-9} hours

(2) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 or SIL3 for ATV32 according to diagrams Process system SF - Case 1, page 50 and Process system SF - Case 2, page 51) from components which constitute the safety function (which is classify SIL2 CL or SIL3 CL for ATV32)

(3) According to table 6 of IEC 62061 (2005)

(4) According to table 4 of EN13849-1 (2008)

Preventive annual activation of the safety function is recommended. However the safety levels are reached with lower margins without annual activation.

For the machine environment, Preventa module is required for the STO function. To free from the Preventa module, the "Restart" function parameters have to be part of the safety function. Please refer to the Preventa usefullness details, page 20.

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 has to do the system PL evaluation by including sensors data with numbers from the table above.

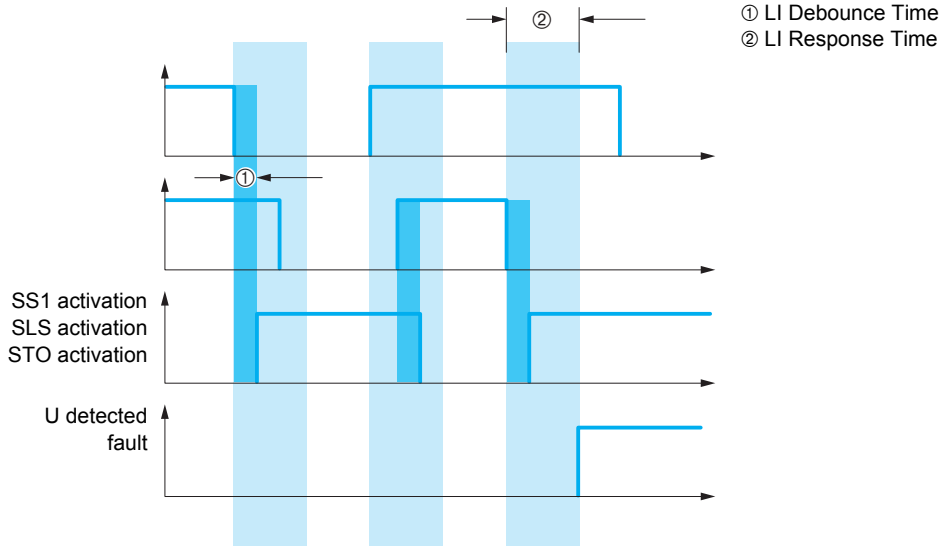
Debounce time and response time

On the ATV32 there are 2 parameters to configure LI for safety function (LI3, LI4, LI5, LI6).

The consistency of each pair of logical input is checked continuously.

LI Debounce Time (LIdt): A logical state difference between LI3-LI4 or LI5-LI6 is allowed during debounce time.

LI Response Time (LIrt): A response time is managed to enable a safe function activation shift.



Several certified architectures

NOTE: For the certification relative to functional aspects, only the PDS(SR) (Power Drive System with safety-related functions) will be in consideration, and not the complete system in which fits into to help to ensure the functional safety of a machine or a system/process.

Here are the architectures certified:

- Process system SF - Case 1, page 50
- Process system SF - Case 2, page 51
- Process system SF - Case 3, page 52
- Process system SF - Case 4, page 53

Safety functions of PDS(SR) (Power Drive System with safety-related functions) are part of a global system.

If qualitative and quantitative objectives of safety set by the final application require to make some adjustments to use the safety functions in a safe way, then the integrator of the BDM (background debug module) is responsible of these complementary evolutions (for example management of the mechanical brake on the motor).

Also, the output information generated by the utilization of safety functions (default relay activation, relay of brake logic command, errors codes or information on the display, …) are not considering safety informations.

Process system SF - Case 1

Safety according to EN 954-1, ISO 13849-1 and IEC 60204-1(Machine)

The following configurations apply to the diagram below:

- STO category 3 Machine with Safety controller module type Preventa XPS AF or equivalent
- SLS category 3 or SS1 type B category 3 on LI3/LI4 or LI5/LI6

Or

- STO category 3 Machine with Safety controller module type Preventa XPS AF or equivalent
- SLS category 3 or SS1 type B category 3 on LI3/LI4

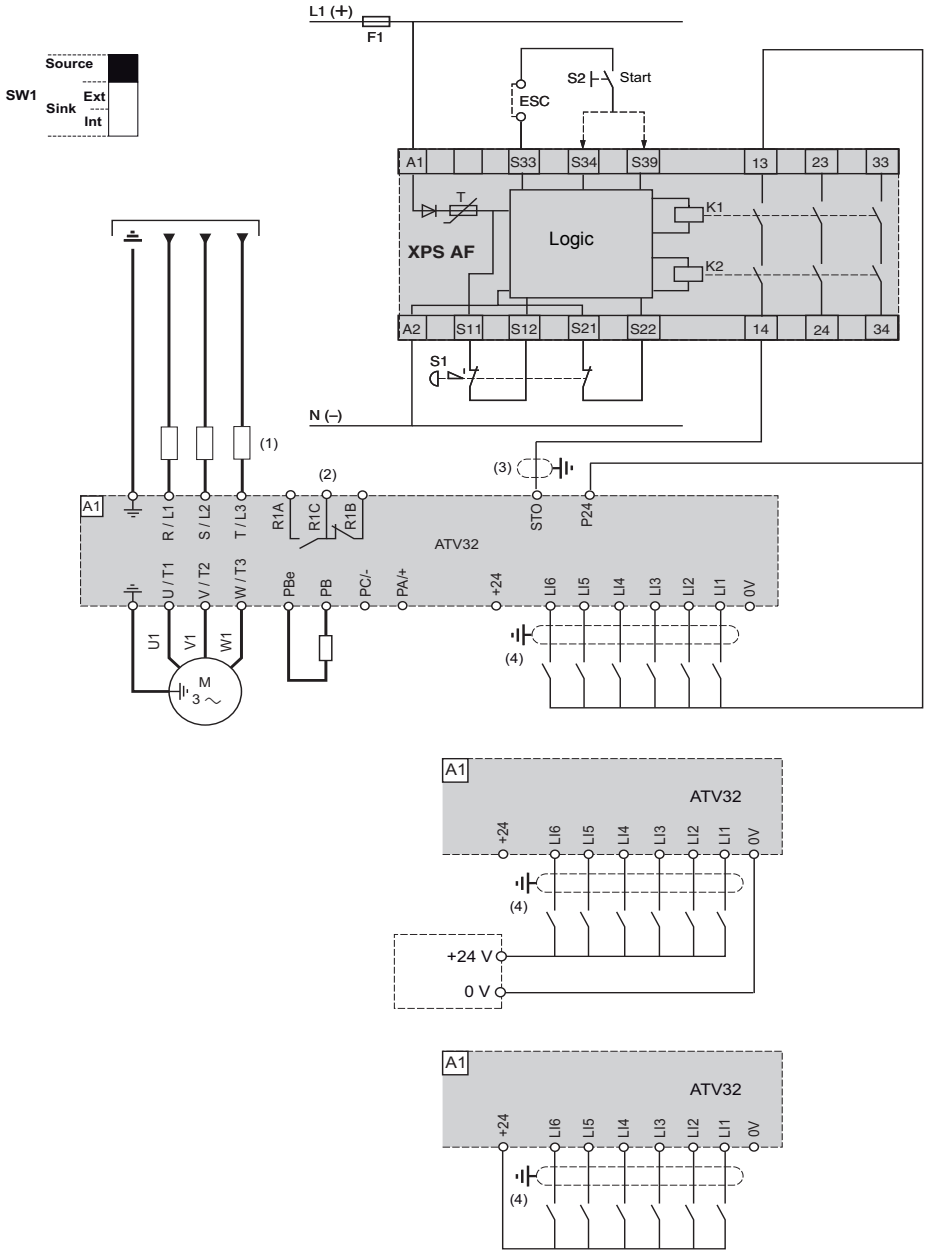
LI5/LI6 not set to a safety function

Or

- STO category 3 Machine with Safety controller module type Preventa XPS AF or equivalent
- LI3/LI4 and LI5/LI6 not set to a safety function

Or

- STO category 4 Machine with Safety controller module type Preventa XPS AF or equivalent and LI3 sets to STO
- SLS cat 3 or SS1 type B category 3 on LI3/LI4 or LI5/LI6
- LI4 not set to a safety function



Process system SF - Case 2

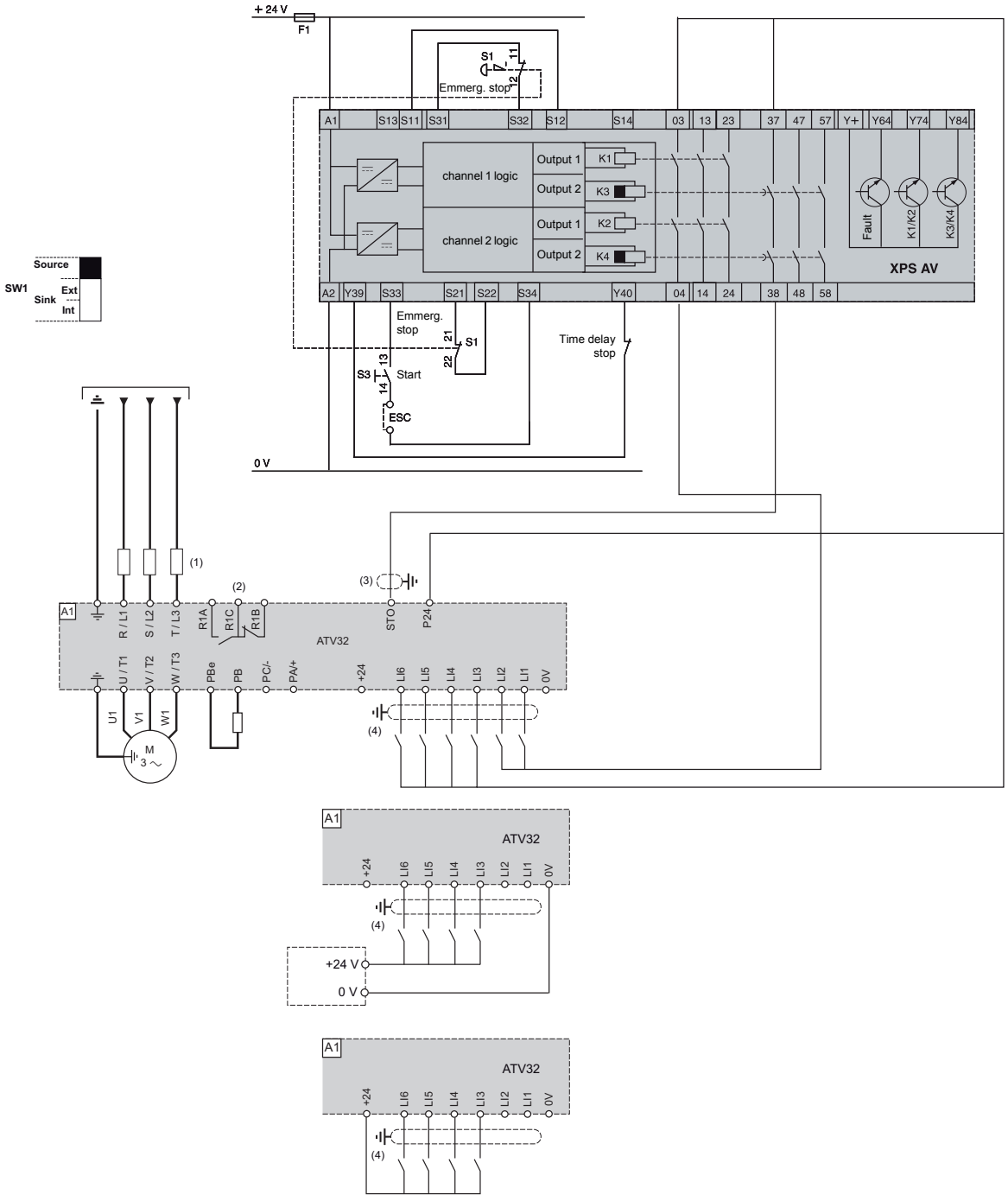
Safety according to EN 954-1, ISO 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- SS1 type C category 3 Machine with Safety controller module type Preventa XPS AV or equivalent
- SLS category 3 on LI3/LI4
- LI5/LI6 not set to a safety function

Or

- SS1 type C category 3 Machine with Safety controller module type Preventa XPS AV or equivalent
- LI3/LI4 and LI5/LI6 not set to a safety function



Process system SF - Case 3

Safety according to IEC 61508

The following configurations apply to the diagram below:

- STO SIL 2 on STO (also SIL1)
- SLS SIL2 or SS1 type B SIL2 on LI3/LI4 or LI5/LI6

Or

- STO SIL 2 on STO (also SIL1)
- SLS or SS1 type B on LI3/LI4
- LI5/LI6 not set to a safety function

Or

- STO SIL 2 on STO (also SIL1)
- LI3/LI4 and LI5/LI6 not set to a safety function

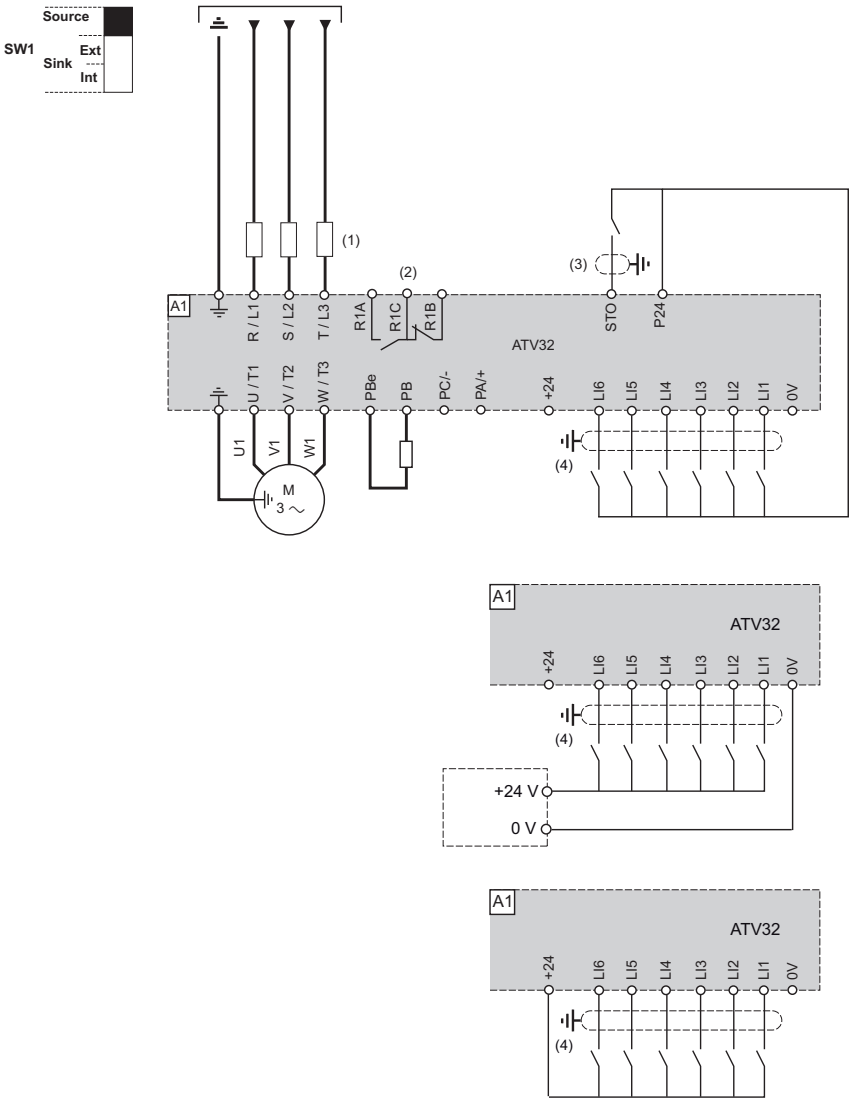
Or

- STO SIL 3 on STO and LI3
- SLS SIL2 or SS1 type B SIL2 on LI5/LI6
- LI4 not set to a safety function

Or

- STO SIL 3 on STO and LI3

LI4 and LI5/LI6 not set to a safety function



Process system SF - Case 4

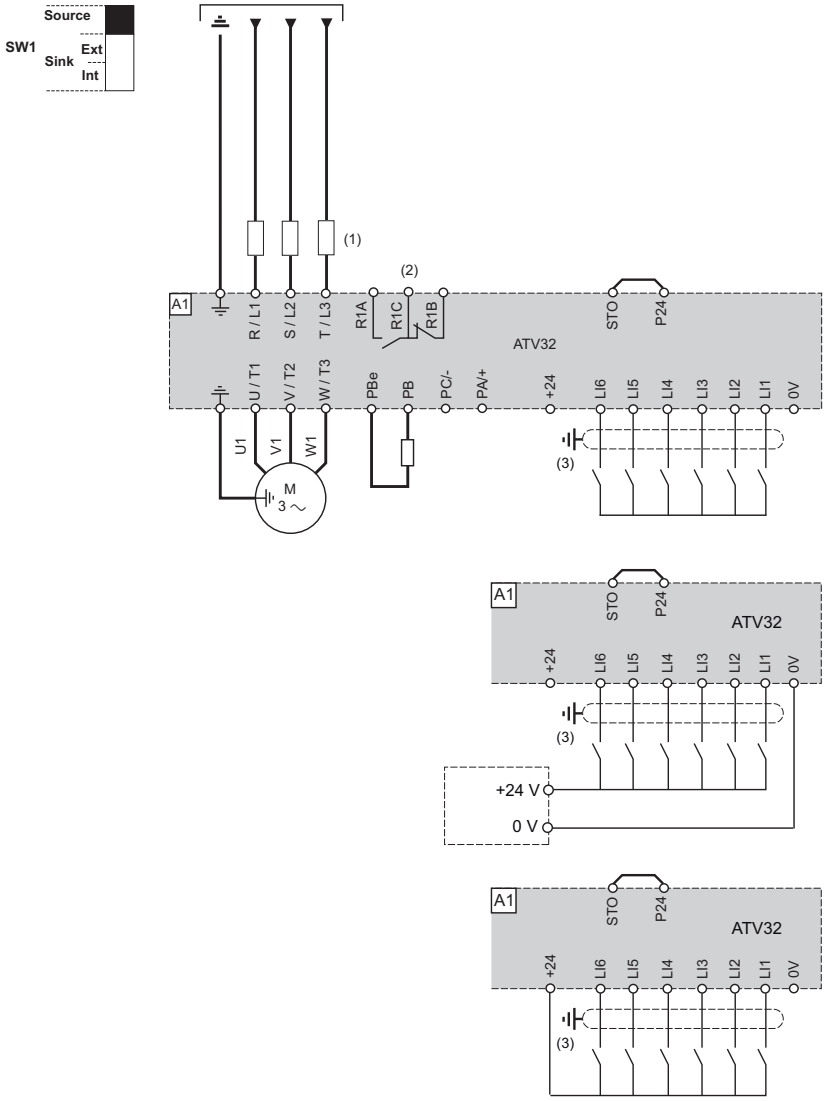
Safety according to IEC 61508

The following configurations apply to the diagram below:

- STO SIL 2 on LI3 and LI4
- SLS SIL2 or SS1 type B SIL2 on LI5/LI6

Or

- STO SIL 2 on LI3 and LI4
- LI5/LI6 not set to a safety function



Commissioning

8

What's in this Chapter?

This chapter contains the following topics:

Starting SoMove configuration

Note

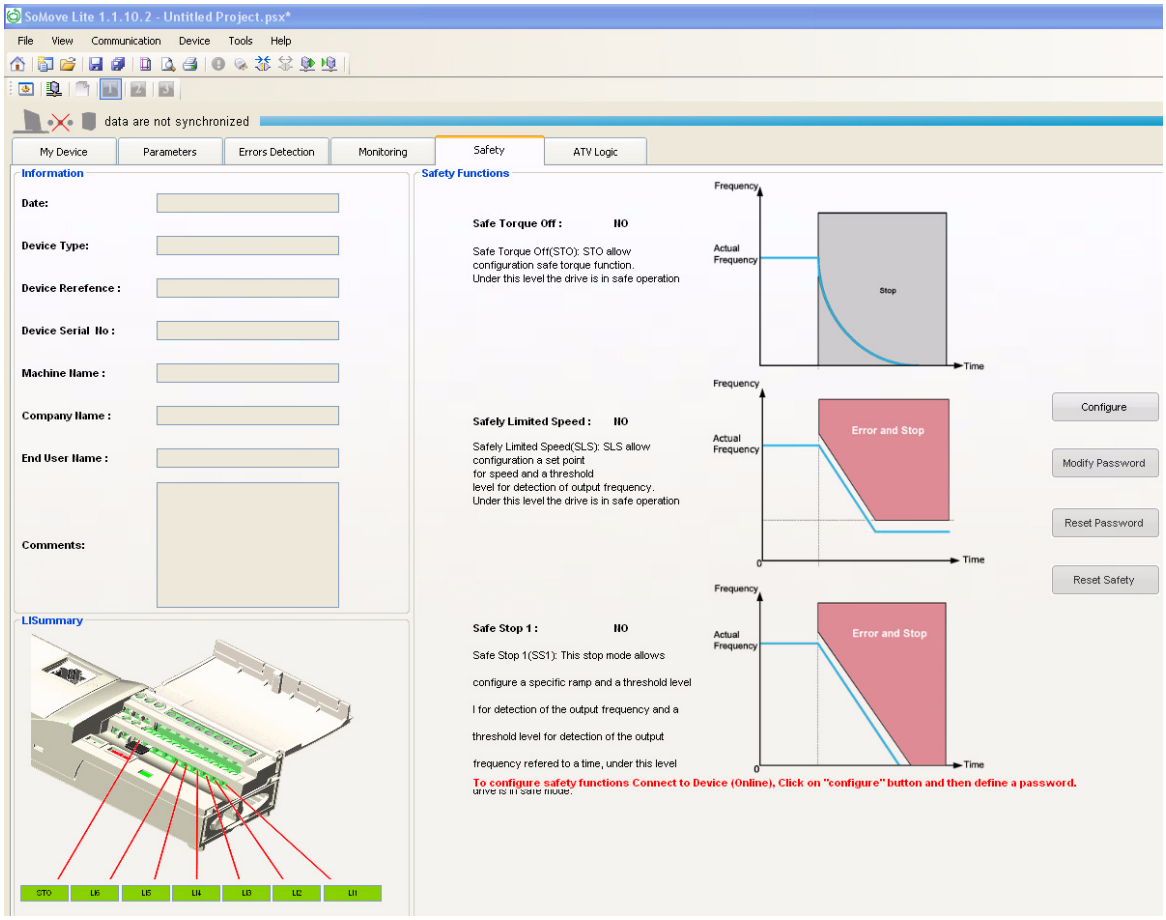
Before commissioning the ATV32 refer to the installation manual on www.schneider-electric.com.

The safety functions are configured with SoMove software.

Safety tab

To access safety configuration, click on safety tab ①.

This screen is in read-only, you can see all current safety configurations.



The Safety tab gives access to:

- an outline of the safety features available on the ATV323 (accessible online/offline)
- the status of all I/O in connected mode
- general information about the machine (online/offline).

It also gives access to the following dialogue boxes:

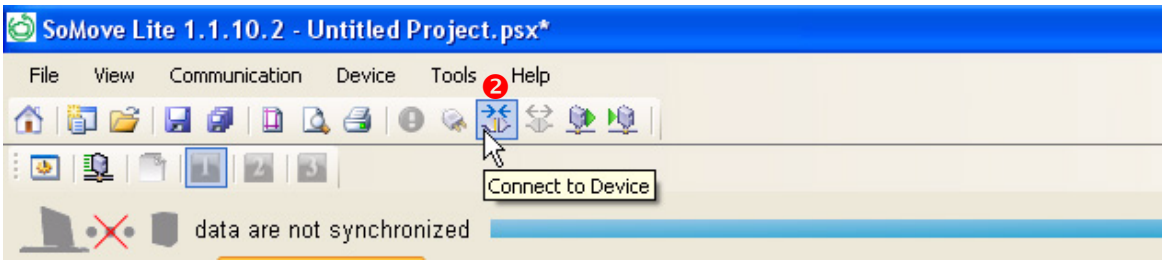
configure (only available in connected mode)

- safety password
- reset password
- reset safety

Steps to configure safety functions

First of all, you need to be in online mode.

If not, go in "Communication->Connect to Device" or click on Connect to Device icon ❷



When you are online you can click on “configure” button in the safety tab panel.

At this time a dialog box appears, to write or set your password.

First case

you have already entered a password: write your defined password:

Second case

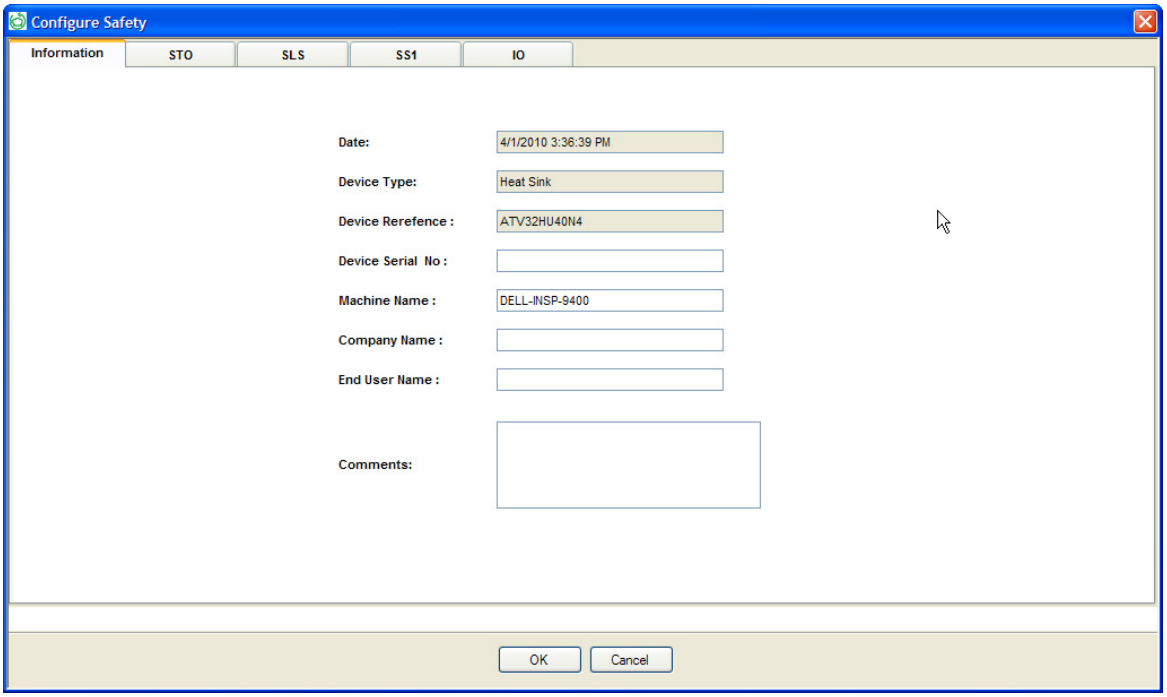
you never have entered a password: you need to choose a value between 1 and 65535. The value 0 is forbidden for the password.

Once this is done, you enter the Configure safety window.

The Configure Safety panel

The Configure Safety panel includes the Information, STO, SLS, SS1 and I/O tabs.

Information tab



The information tab provides the way to define safety information.

The Safety Information data is displayed in the "Information" tab of the "Safety" HMI.

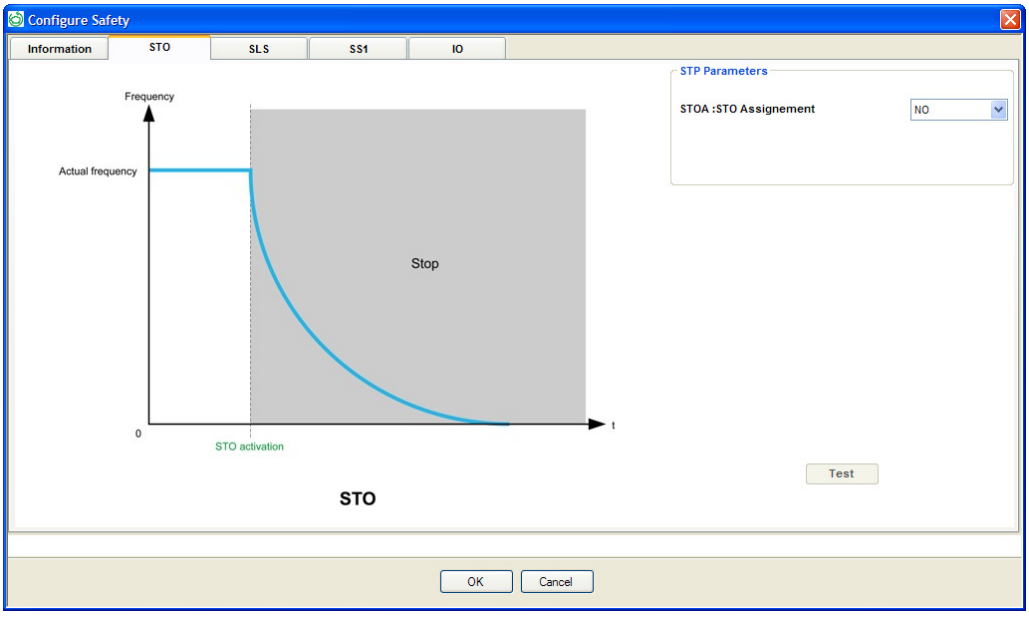
Information automatically filled by SoMove:

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

Information filled manually:

- Device serial number
- Machine name
- Company name
- End user name
- Comments

Safe Torque Off (STO) tab



For this function, only the associated set of inputs has to be selected in the combo box.

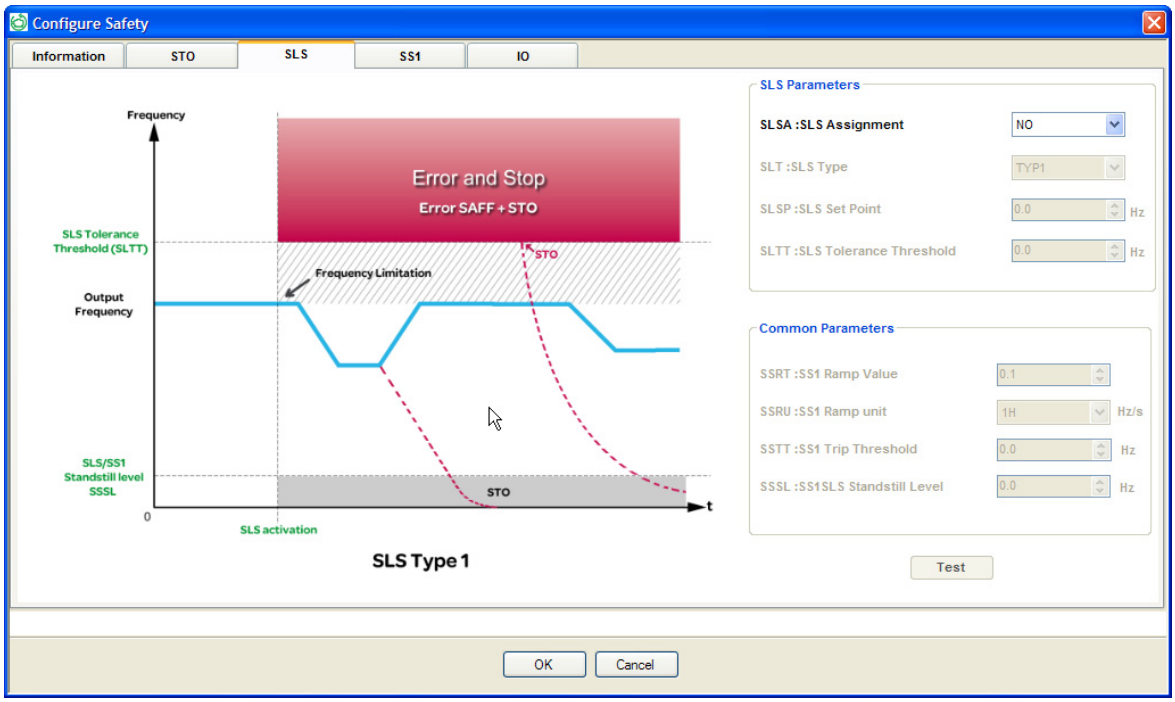
The parameter to be managed is the parameter: STOA.

Code	Name / Description	Adjustment range	Factory setting
StO	**[Safe Torque Off]**		
StOA	**[SLO function activation]**		No
nO	**[No]**: Not assigned		
LI3P.	**[LI3 and STO]**: LI 3/STO Low state		
LI34	**[LI3 and LI4]**: LI 3/4 Low state		
LI56	**[LI5 and LI6]**: LI 5/6 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		

For more information about STO function see page 20.

Safely Limited speed (SLS) tab

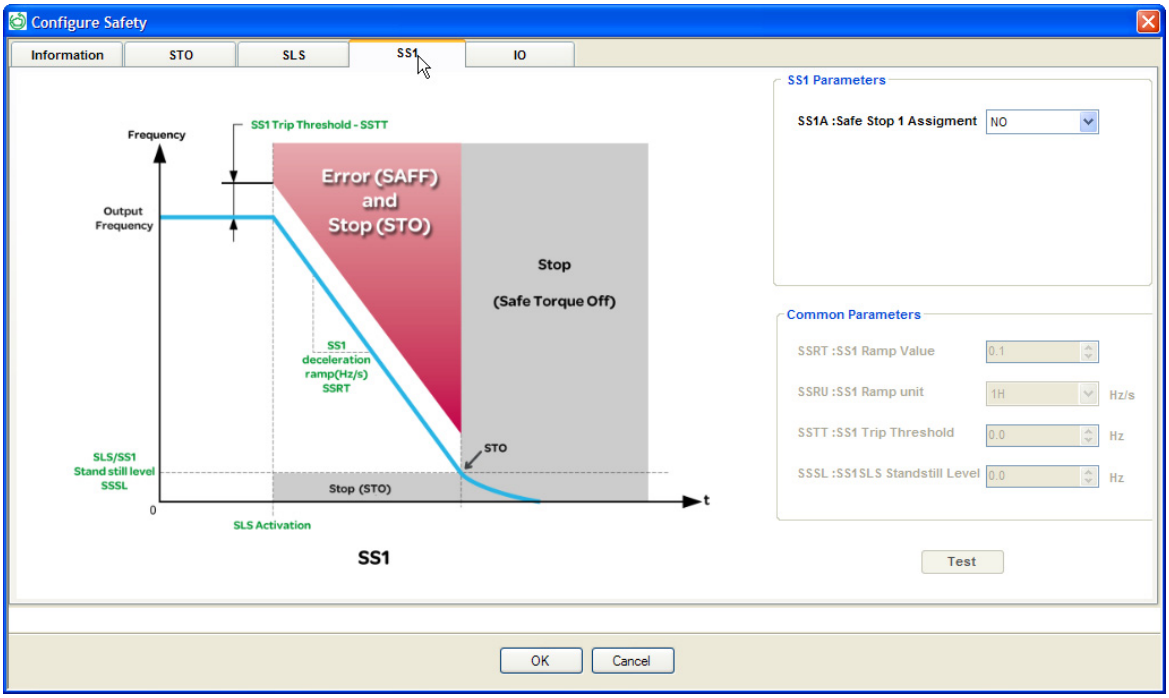
For more information see (SLS) Safely Limited Speed, page 23.



Code	Name / Description	Adjustment range	Factory setting
SLS	**[Safely Limited Speed]**		
SLSA	**[SLS function activation]**		No
nO	**[No]**: Not assigned		
LI3_4	**[LI3 and LI4]**: LI 3/4 Low state		
LI5_6	**[LI5 and LI6]**: LI 5/6 Low state		
	This parameter is used to configure the channel used to trigger the SLS function.		
SLt	**[Safe Limited speed Type Element]**		Type 1
tYP1	**[Type 1]**: SLS type 1		
tYP2	**[Type 2]**: SLS type 2		
tYP3	**[Type 3]**: SLS type 3		
	This parameter is used to select the SLS type. Refer to functions description to have information about behavior of different types.		
SLSP	**[SLS set point]**	0 to 599 Hz	0
	This parameter is only visible if SLT = TYPE2 or SLT=TYPE3 SLSP is used to set the limit speed		
SLtt	**[SLS tolerance threshold]**	0 to 599 Hz	0
	The behavior of this parameter depend of the value of SLT.		
SSrt	**[SS1 ramp value]**	1 to 5990	1
	Unit depends on SSRU parameter. Use this parameter to set the value of SS1 ramp. SS1 ramp = SSRT*SSRU. Example: SSRT=250 and SSRU=1 Hz/s then speed of the ramp = 25 Hz/s. This parameter is specific. Indeed, they are common with the safety function SS1 configured in another tab.		
SSrU	**[SLS type]**		1 Hz/s
1H	**[1 Hz/s]**		
10H	**[10 Hz/s]**		
100H	**[100 Hz/s]**		
	With this parameter you can set the unit of SSRT. This parameter is specific. Indeed, they are common with the safety function SS1configured in another tab.		

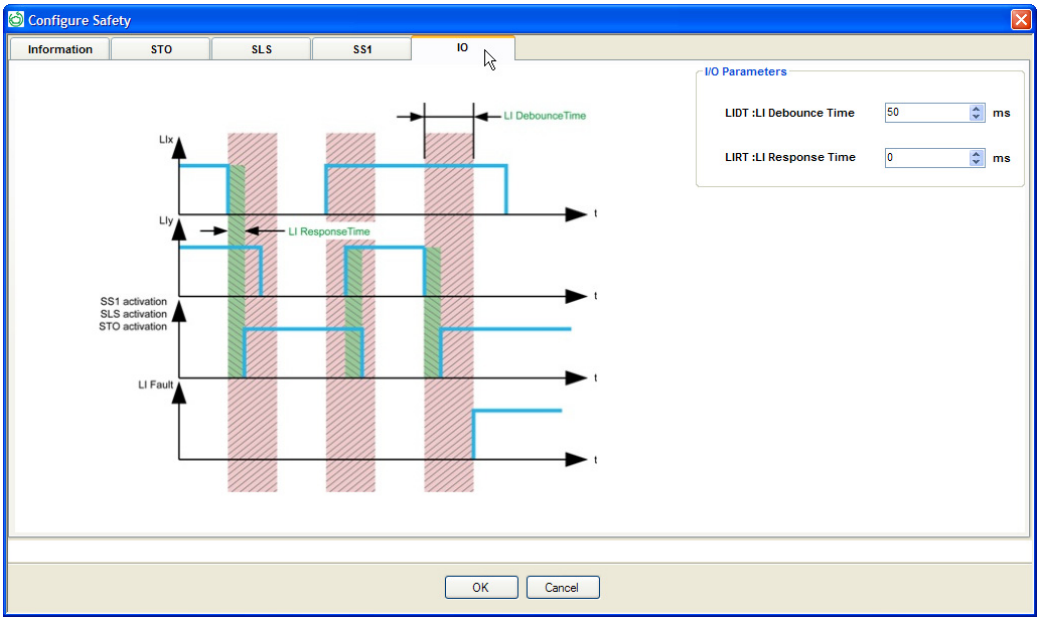
Code	Name / Description	Adjustment range	Factory setting
SSTt	**[SS1 trip threshold]** This parameter sets the tolerance zone around the deceleration ramp in which the frequency may vary. This parameter is specific. Indeed, they are common with the safety function SS1 configured in another tab.	0 to 599 Hz	0
SSSL	**[SLS/SS1 standstill level]** This parameter adjusts the frequency to which the drive should go into state STO at the end of the ramp SS1. This parameter is specific. Indeed, they are common with the safety function SS1 configured in another tab.	0 to 599 Hz	0

Safe Stop 1 (SS1) tab



Code	Name / Description	Adjustment range	Factory setting
SS 1	**[Safe Stop 1]**		
SS 1A	**[SS1 function activation]**		No
nO	**[No]**: Not assigned		
L I3_4	**[LI3 and LI4]**: LI 3/4 Low state		
L I5_6	**[LI5 and LI6]**: LI 5/6 Low state		
	This parameter is used to configure the channel used to trigger the SS1 function.		
SSrt	**[SS1 ramp value]**	1 to 599	1
	Unit depends on SSRU parameter. Use this parameter to set the value of SS1 ramp. SS1 ramp = SSRT*SSRU. Example: SSRT=250 and SSRU=1 Hz/s then speed of the ramp = 25 Hz/s. This parameter is specific. Indeed, they are common with the safety function SS1 configured in another tab.		
SSrU	**[SL1 ramp unit]**		1 Hz/s
1H	**[1 Hz/s]**		
10H	**[10 Hz/s]**		
100H	**[100 Hz/s]**		
	With this parameter you can set the unit of SSRT. This parameter is specific. Indeed, they are common with the safety function SLS configured in another tab.		
SStt	**[SS1 trip threshold]**	0 to 599 Hz	0
	This parameter sets the tolerance zone around the deceleration ramp in which the frequency may vary. This parameter is specific. Indeed, they are common with the safety function SLS configured in another tab.		
SSSL	**[SLS/SS1 standstill level]**	0 to 599 Hz	0
	This parameter adjusts the frequency to which the drive should go into state STO at the end of the ramp SS1. This parameter is specific. Indeed, they are common with the safety function SLS configured in another tab.		

I/O Configuration tab

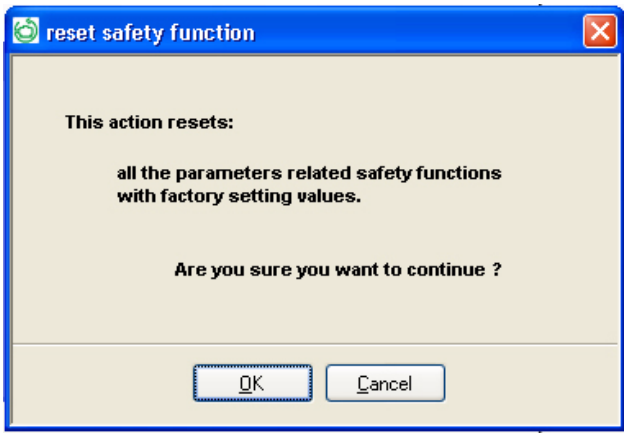


Code	Name / Description	Adjustment range	Factory setting
IO	**[I/O parameters]**		
LIdt	**[LI debounce time]**	1 to 2000 ms	50
	In most of the case, both LI of a safe LI couple (LI3 and LI4, LI5 and LI6) will not be 100% synchronized. They will not change of state in the same time. There is a small delta between both LI transition. LIDT is the parameter used to set this delta. If both LI change states with a delta in time smaller than LIDT it is considered as a simultaneous transition of the LI. If delta in time is greater than LIDT, drive considers that LI are no more synchronized and a Safe detected fault is triggered.		
LIrt	**[LI response time]**	0 to 50 ms	0
	This parameter is used to filter shirt impulse on LI. In some application automaton sends short impulse on the line to test it. This parameter is used to filter these short impulses. Orders are taken into account only if the duration is greater than LIRT. If duration is smaller drive considers that there is no order: order is filtered.		

Reset Safety

This function is used to remove the safety function in the device. To access the function, click the «Reset Safety» function button in the Safety tab panel, see page 56.

First, enter the password, and after confirm your choice.



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

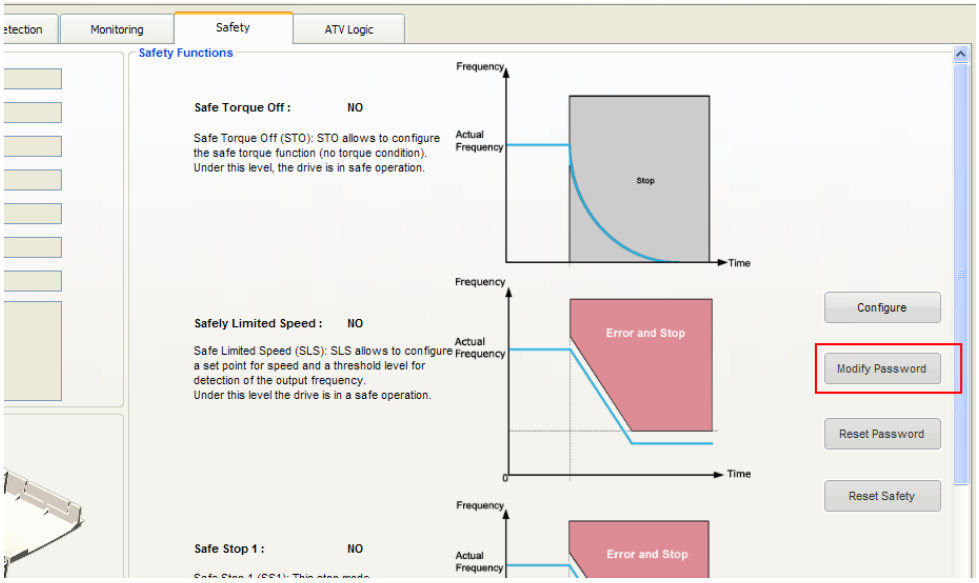
Password management

Modify Password

This function allows to modify the safety password in the drive.

This tool is launched from the “Safety” tab using the button “Modify Safety Password”.

To modify the safety password, a session must be opened in the drive. Opening a safety session means providing to the Drive the good safety password.



You need to choose a value between 1 and 65535. The value 0 is forbidden for the password. Use only digits to create the password. Any other character will not be taken into account.

Reset password

If you don’t remember the safety password defined in the drive.

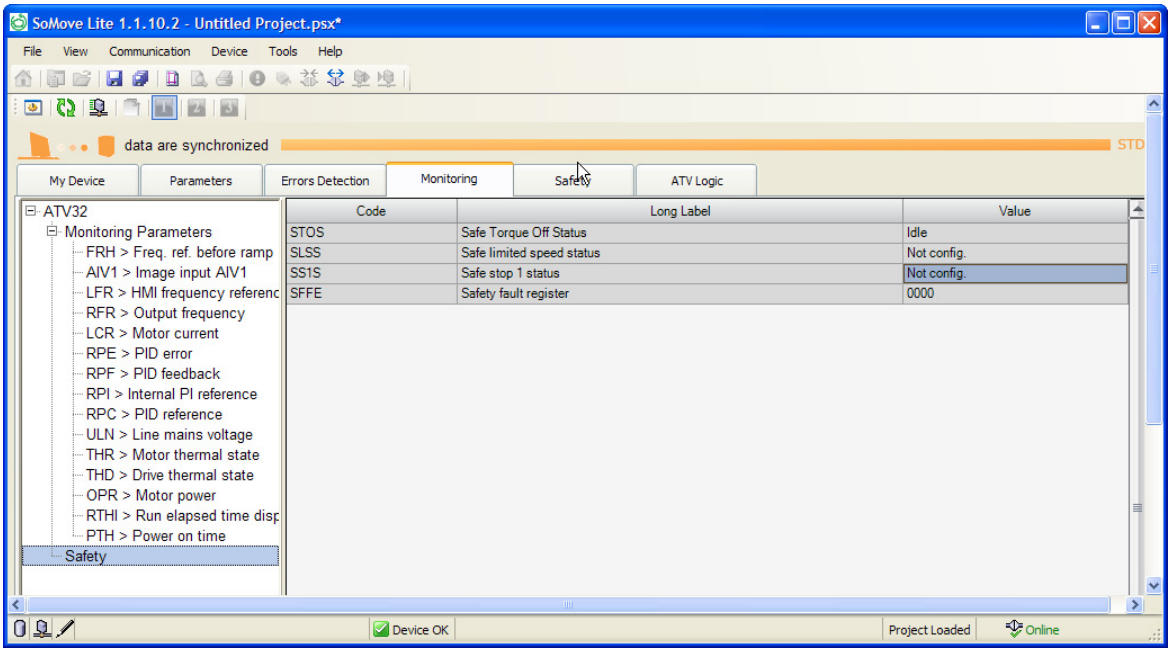
Resetting the drive requires the knowledge of the universal password.

To get this password, contact your Schneider Electric support.

After this operation, the device goes back to undefined safety password and the safety session is automatically closed.

Function configuration however remains unchanged.

Monitoring and status of safety function



A parameter shows if the drive is in safe state or not (safety function configured):

- No safety function configured: STD
- Safety function configured : SFTY

Safety Status

Code	Name / Description
SAF-	**[MONIT. SAFETY] Visible on SoMove and keypad**
STOS	**[STO status]** Status of the Safe Torque Off safety function. IdLE [IdLE] STO not in progress. Sto [Safe stop] STO in progress FLt [Fault] STO in detected fault
SLSS	**[SLS status]** Status of the Safe Limit speed safety function. nO [Not config.]: SLS not configured IdLE [IdLE]: SLS not in progress SSI [Safe ramp]: SLS ramp in progress SLS [Speed limited]: SLS speed limitation in progress Sto [Safe stop]: SLS safe torque off request in progress FLt [Fault]: SLS in detected fault
SS1S	**[SLS status]** Status of the Safe Stop 1 safety function nO [Not config.]: SS1 not configured IdLE [IdLE]: SS1 not in progress SS1 [Safe ramp]: SS1 ramp in progress Sto [Safe stop]: SS1 safe torque off request in progress FLt [Fault]: SS1 in detected fault
SAF-	**[MONIT. SAFETY] Visible ONLY on SoMove**
SFTY	**[Safe drive Status]** Safe Status of the Drive Std [Standard drive]: standard product without safe function configured. SAFE [Safe drive]: safe product with at least 1 safe function configured.

Machine signature

9

What's in this Chapter?

This chapter contains the following topics:

Introduction

The acceptance test for systems with Safety Integrated Functions is focused on validating the functionality of Safety Integrated monitoring and stop functions configured in the drive system.

The test objective is to verify proper configuration of the defined safety functions and of test mechanisms and to examine the response of specific monitoring functions to the explicit input of values outside tolerance limits. The test must cover all drive-specific Safety configured monitoring functions and global Safety Integrated functionality of ATV32.

Condition before acceptance test

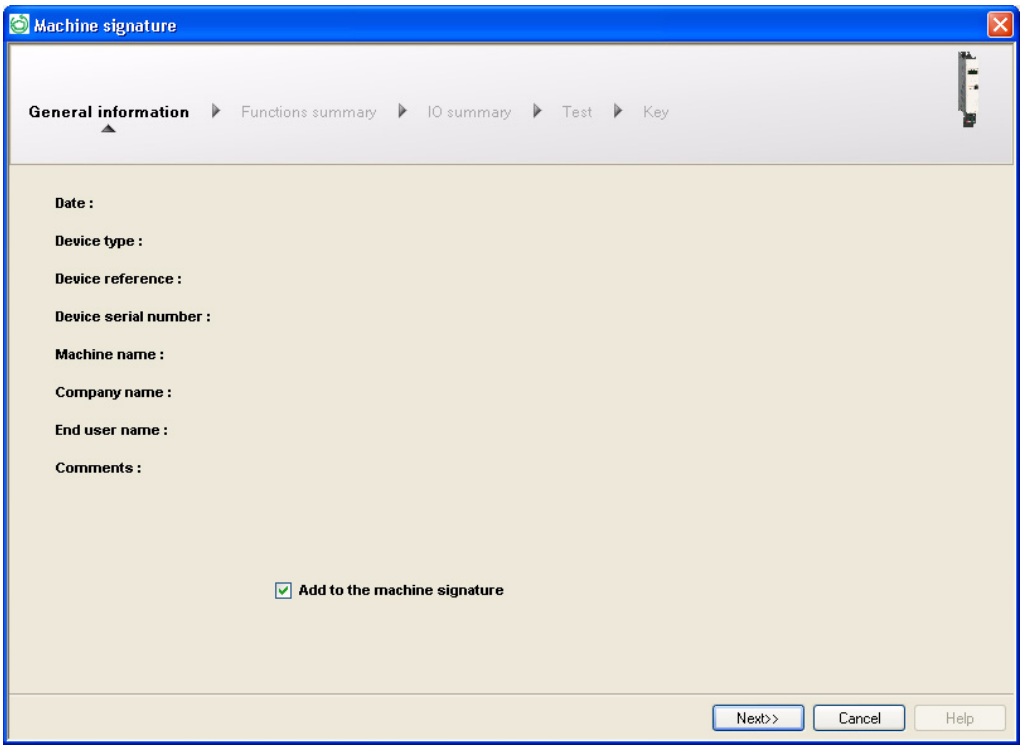
- The machine is properly wired.
- All safety equipment such as protective door monitoring devices, light barriers or emergency stop switches are connected and ready for operation.
- All motor parameters and command parameters shall be correctly set on the drive.

Acceptance test process

The configuration of Acceptance test is done with SoMove software.

Select the menu: Device -> Safety function -> Machine signature and follow the 5 steps below.

Step 1: General information



The information that is displayed is the one defined in the "Identification" folder of the "Safety" tab. They cannot be modified here.

To add this step to the final report select "Add to the machine signature".

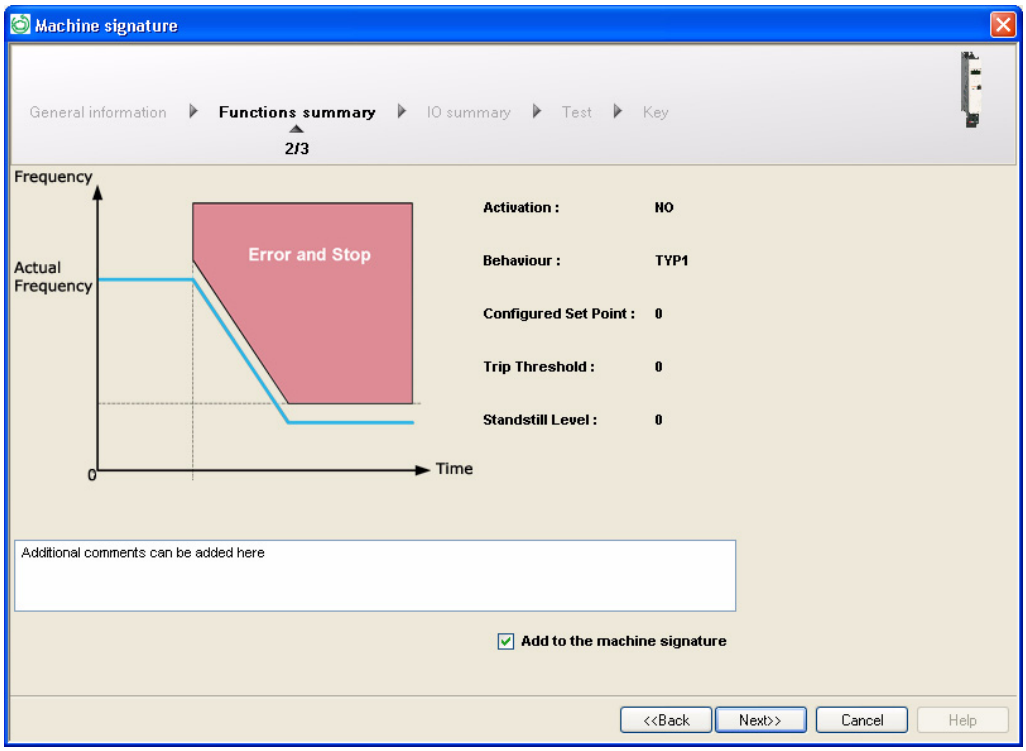
Click on "next" button

Step 2: Functions summary

This step is composed of sub steps.

Each sub step is a safety function between:

- STO
- SLS
- SS1

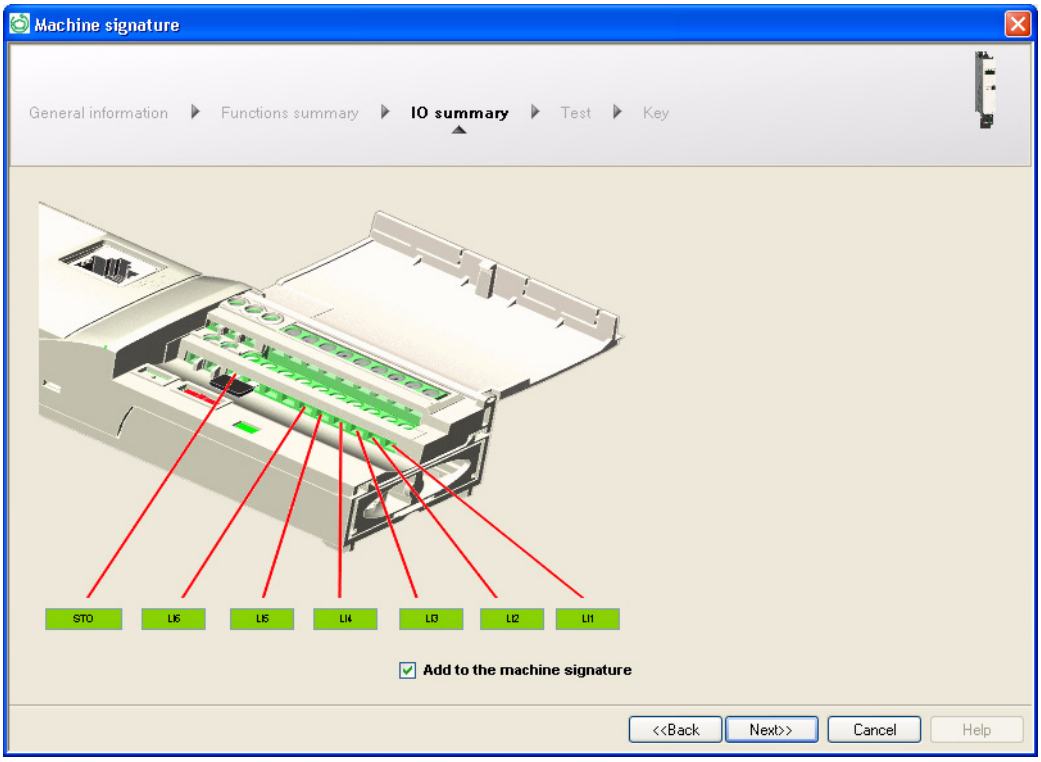


In a function sub step the function diagram and parameters values are displayed. A text box allows you to enter some additional text in this step.

To add a function to the final report select "Add to the machine signature".

Click on "next" button

Step 3: I/O summary



The information that is displayed is the one defined in the "LI summary" folder of the "Safety" tab.

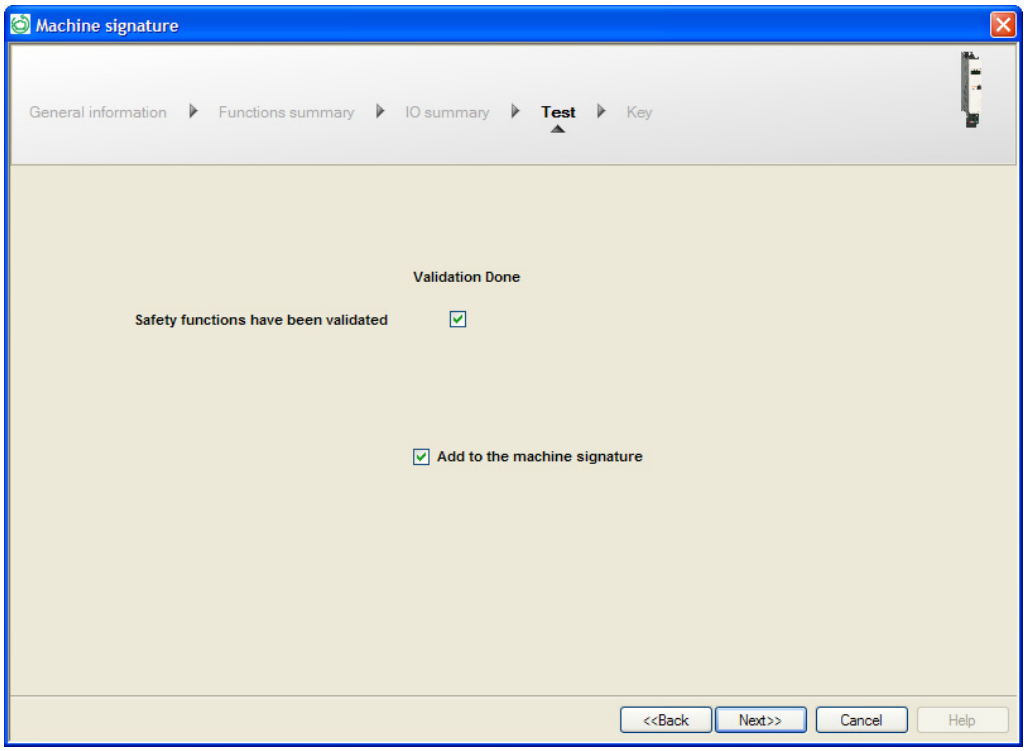
- The LI that are assigned to a safety function are displayed in red and show the related safety function.
- LI that is not assigned to a safety function does not show any assignment and are displayed in green.

To add this step to the final report select "Add to the machine signature".

Click on "next" button

Step 4: Test

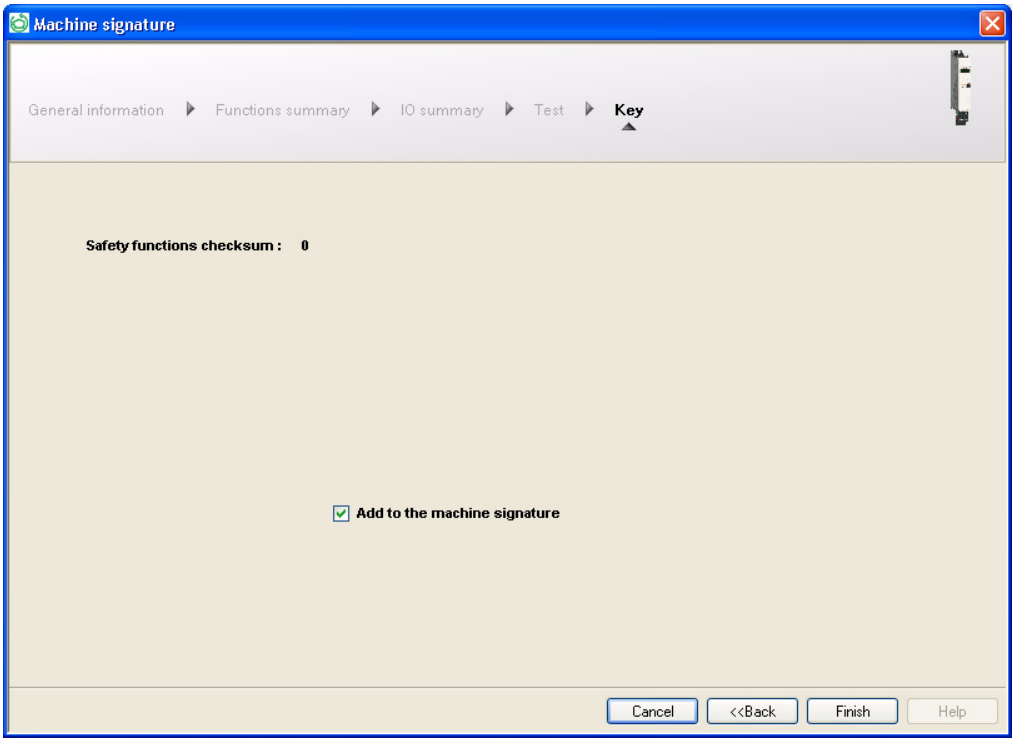
In this step you tick the box when you have done test on your safety functions to guarantee you have check the correct behaviour of the functions with all the equipments.



To add this step to the final report select "Add to the machine signature".

Click on "next" button.

Step 5: Key



The check sum of the safety parameters is displayed as it is calculated to be sent to the connected device when "Apply".

This allows you to compare the checksum value, with the one that displayed on the graphic terminal, in identification menu.

Click on Finish button to create the report.

Acceptance report

SoMove creates the Acceptance report.

It can generate the drive safety signature. This function provides a final private report when the drive has been configured as “Safe” and declared “Safe in operation”.

This report is considered as a machine signature and certifies that all the “Safety functions” are operational.

The Safety report is added as a possible document to be printed to printer or into a PDF file.

In case of modification of drive configuration (not only safety parameter), you must redo the acceptance test.

Services and maintenance

10

What's in this Chapter?

This chapter contains the following topics:

Maintenance

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

Preventive maintenance

It is recommended to check each year the safety functions.

Example: Open the protective door to see if the drive stops in accordance with the safety function configured.

Power and MCU replacement

You can change the MCU (Motor Control Unit) part (APP + HMI card) and the power part. Following the drive configuration (safety function active or not), the drive reaction could be different.

In case of power replacement and if you keep your MCU, you don't loose your safety configuration but you need to redo the Acceptance test in case of wrong wiring or incorrect behavior of safety function.

In case of MCU replacement you will lose your safety configuration, you need to do again your configuration on the new MCU (page 56) and after you redo the the Acceptance test

Changing equipment of the machine

Note: If you need to change any part of the machine out of ATV32 (Motor, Emergency stop …) you must redo the Acceptance test.