SIEMENS

SINUMERIK

SINUMERIK ONE Safety Integrated

Commissioning Manual

Valid for:

CNC Shopfloor Management Software
Create MyVirtual Machine V1.1
SINUMERIK ONE V6.15
SINUMERIK ONE STEP 7 Toolbox V17

07/2021
A5E47278158B AE

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E47278158B AE
Ⓟ 07/2021 Subject to change

Table of contents

Introduction 1

1.1 About SINUMERIK

From simple, standardized CNC machines to premium modular machine designs – the SINUMERIK CNCs offer the right solution for all machine concepts. Whether for individual parts or mass production, simple or complex workpieces – SINUMERIK is the highly dynamic automation solution, integrated for all areas of production. From prototype construction and tool design to mold making, all the way to large-scale series production.

Visit our website for more information SINUMERIK (https://www.siemens.com/sinumerik).

1.2 About this documentation

The "Safety Integrated (plus)" safety solution combines various safety functions in the SINUMERIK control system:

- F-I/O are connected via the F-capable PLC of the SINUMERIK control system:
- F-blocks are programmed with F-logic using F-FBD or F-LAD editors
- Configurations and the F-library are handled in the same way as for SIMATIC F-CPUs
- Configuration using the Safety Administration Editor (Page 58)
- Controlling the safety functions integrated in the drive (via SINAMICS Integrated):
  – Safety Integrated Basic Functions
  – Safety Integrated Extended Functions

Purpose of the documentation

This documentation provides a description of functions and data about the Safety Integrated mode - as well as more general information relating to commissioning, acceptance, maintenance and diagnostics with SINUMERIK Operate and the TIA Portal.

This includes the Safety Integrated Extended Functions and the Safety Integrated Basic Functions in conjunction with the integrated drives of the SINUMERIK ONE or PLC-controlled NC axes - or external drives, which are assigned to an NC axis.

Drives without NC axis assignment are not taken into account in this documentation.

Information about F-PLC, F-I/O, the safety program and/or SIMATIC Safety in this manual serves as entry-level information only - and describes the special features relating to SINUMERIK.

Note

Important additional information

For space reasons, the information described in this manual cannot replace a complete SIMATIC Safety Manual.

Therefore, when configuring these safety programs, it is crucial that you carefully follow the information provided in the TIA Portal help on SIMATIC Safety or in manual "SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126)".

Note

Validity and scope of the information about SIMATIC STEP 7 Safety

This handling overview provided as example only serves as an introduction to configuring and programming of SIMATIC STEP 7 Safety with SINUMERIK in the TIA Portal. It cannot always be used in regular and effective operation.

The following documentation is the main source of all information regarding functional safety relating to configuring and programming in the TIA portal:

- Programming and operating manual - SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/de/view/54110126)

This also applies in the case of discrepancies between this manual and the SIMATIC STEP 7 Safety manual.

The warnings and other notes contained in that manual must be observed, even when they are not repeated in this document!

Note

Carefully comply with the applicable standards and regulations

Depending on the application area, the SINUMERIK ONE, being part of plants and systems, requires that special standards and regulations be carefully observed. It is absolutely crucial that you observe the appropriate safety and accident prevention regulations, e.g. IEC 60204-1 (general requirements placed on the safety of machines).

Note

Important additional information

Note also the information in the SINAMICS S120 Safety Integrated Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109760403).

Standard scope

This documentation only describes the functionality of the standard version. This may differ from the scope of the functionality of the system that is actually supplied. Please refer to the ordering documentation only for the functionality of the supplied drive system.

It may be possible to execute other functions in the system which are not described in this documentation. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include all of the detailed information on all product types. Further, this documentation cannot take into consideration every conceivable type of installation, operation and service/maintenance.

The machine manufacturer must document any additions or modifications they make to the product themselves.

Websites of third-party companies

This document may contain hyperlinks to third-party websites. Siemens is not responsible for and shall not be liable for these websites and their content. Siemens has no control over the information which appears on these websites and is not responsible for the content and information provided there. The user bears the risk for their use.

1.3 Documentation on the internet

1.3.1 Documentation overview SINUMERIK ONE

Comprehensive documentation about the functions provided in SINUMERIK ONE Version 6.13 and higher is provided in the Documentation overview SINUMERIK ONE (https://support.industry.siemens.com/cs/ww/en/view/109768483).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Functions
- Manufacturer/Service: Hardware
- Manufacturer/Service: Configuration/Setup
- Manufacturer/Service: Safety Integrated
- Information and training
- Manufacturer/Service: SINAMICS

1.3.2 Documentation overview SINUMERIK operator components

Comprehensive documentation about the SINUMERIK operator components is provided in the Documentation overview SINUMERIK operator components (https://support.industry.siemens.com/cs/document/109783841/technische-dokumentation-zu-sinumerik-bedienkomponenten?dti=0&lc=en-WW).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- Operator Panels
- Machine control panels
- Machine Pushbutton Panel
- Handheld Unit/Mini handheld devices
- Further operator components

An overview of the most important documents, entries and links to SINUMERIK is provided at SINUMERIK Overview - Topic Page (https://support.industry.siemens.com/cs/document/109766201/sinumerik-an-overview-of-the-most-important-documents-and-links?dti=0&lc=en-WW).

1.4 Basic knowledge requirements

General basic knowledge of automation engineering is needed to understand this documentation. Basic knowledge of the following is also necessary:

- Failsafe automation systems
- S7-1500 automation systems
- Distributed I/O systems on PROFIBUS DP/PROFINET IO
- Totally Integrated Automation Portal, including:
  - Hardware configuration with hardware and network editor
  - Programming in the LAD and FBD programming languages using the program editor
  - Communication between CPUs
  - Configuring and programming failsafe systems with SIMATIC Safety
  - Configuring and programming with SINUMERIK hardware and the SINUMERIK PLC basic program
- Commissioning the SINUMERIK ONE with SINUMERIK Operate
- Commissioning drives with SINUMERIK Operate

1.5 Notation

Notation used

The following notation and abbreviations are used in this documentation:

Synonyms of terminology used

This documentation uses terms "Safety technology" and "F-technology" synonymously. The same applies to terms "failsafe" and "F-" process.

The term "Safety program" designates the failsafe part of the user program - and is used instead of "failsafe user program", "F-program", etc. To make a differentiation, the non-safety-related part of the user program is called "Standard user program".

Notations for SINAMICS parameters (examples):

- p0918 — Adjustable parameter 918
- r1024 — Display parameter 1024
- p1070[1] — Adjustable parameter 1070, index 1
- p2098[1].3 — Adjustable parameter 2098, index 1 bit 3
- p0099[0...3] — Adjustable parameter 99, indices 0 to 3
- r0945[2](3) — Display parameter 945, index 2 of drive object 3
- p0795.4 — Adjustable parameter 795, bit 4

Notation for SINUMERIK machine data (examples):

- MD36933 — Machine data 36933
- $MA_SAFE_DES_VELO_LIMIT — Machine data type and symbolic name of the machine data
- MD15068[1] — Machine data 15068 index 1
- MD15068[1].3 — Machine data 15068 index 1 bit 3
- MD15068[0...3] — Machine data 15068 index 0 to 3
- MD15068.4 — Machine data 15068 bit 4

Note

Term "Control Unit" in this documentation

In the Safety Integrated environment and in this documentation the term "Control Unit" designates the SINUMERIK NCU.

1.6 SINUMERIK-conformal telegram configuring

Rules for SINUMERIK-conformal telegram configuring of SINAMICS drives

To configure the data exchange between a SINUMERIK 828D, SINUMERIK 840D sl, SINUMERIK ONE or SINUMERIK MC and SINAMICS S120 drives, the following rules must be observed for the PROFIBUS/PROFINET configuration of the drives:

- For the SINAMICS drives (CU3xx) on PROFIBUS/PROFINET, the PROFIBUS/PROFINET configuration must be identical to the standard configuration of the telegrams of the drives on the integrated PROFIBUS (SINAMICS Integrated or NX) of a SINUMERIK 828D, SINUMERIK 840D sl or SINUMERIK ONE with regard to the structure of the telegrams.
- The identical structure of the telegrams refers specifically to the sequence of telegrams for a drive (CU3xx). The telegrams must be configured in the following order:
  - Telegrams for SERVO or HLA drive objects
  - Telegram for the control unit drive object
  - Telegram for the infeed drive object
- The following rules must be observed for the telegrams of the individual drive objects:
  - The input and output address of a telegram must have the same value.
    Exception: User-specific telegrams that only have input or output values.
  - The input and output data of a telegram are generally transferred via the same slot. If two different slots are used for data exchange (for PROFIBUS or PROFIBUS Integrated), make sure that the input slot is defined first. The output slot must have the following slot number.

1.7 Feedback on the technical documentation

If you have any questions, suggestions or corrections regarding the technical documentation which is published in the Siemens Industry Online Support, use the link "Send feedback" link which appears at the end of the entry.

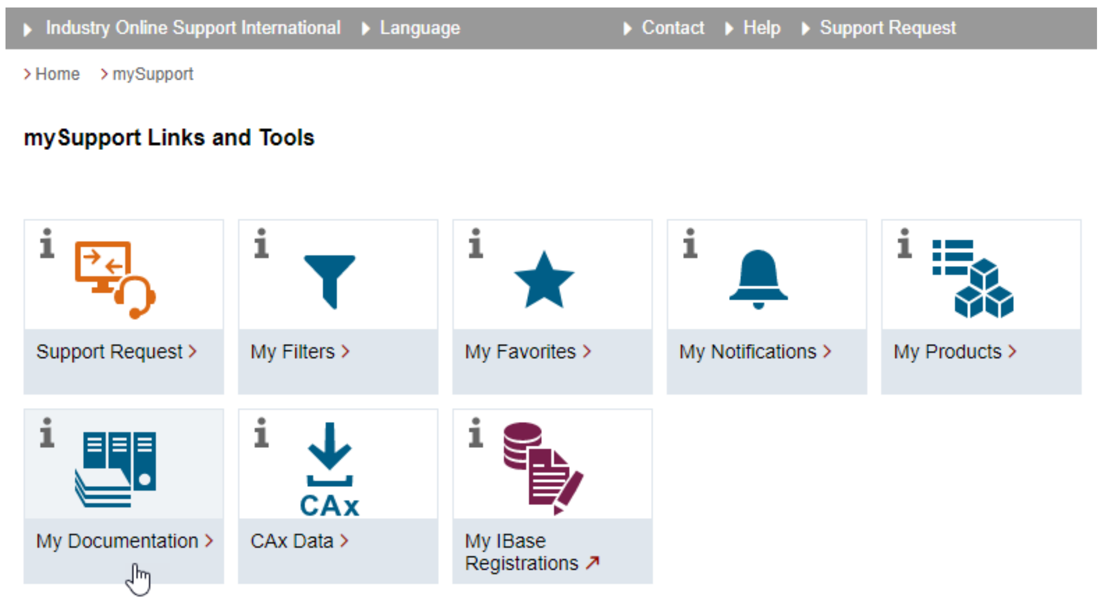
See also

Send feedback (mailto:docu.motioncontrol@siemens.com)

1.8 mySupport documentation

With the "mySupport documentation" web-based system you can compile your own individual documentation based on Siemens content, and adapt it for your own machine documentation.

To start the application, click on the "My Documentation" tile on the mySupport homepage (https://support.industry.siemens.com/cs/ww/en/my):



The configured manual can be exported in RTF, PDF or XML format.

Note

Siemens content that supports the mySupport documentation application can be identified by the presence of the "Configure" link.

1.9 Service and Support

Product support

You can find more information about products on the internet:

Product support (https://support.industry.siemens.com/cs/ww/en/)

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs (frequently asked questions)
- Manuals
- Downloads
- Newsletters with the latest information about your products
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via our Contacts at Siemens database (→ "Contact")
- Information about field services, repairs, spare parts, and much more (→ "Field Service")

Technical support

Country-specific telephone numbers for technical support are provided on the internet at address (https://support.industry.siemens.com/cs/ww/en/sc/4868) in the "Contact" area.

If you have any technical questions, please use the online form in the "Support Request" area.

Training

You can find information on SITRAIN at the following address (https://www.siemens.com/sitrain).
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go

With the award-winning "Siemens Industry Online Support" app, you can access more than 300,000 documents for Siemens Industry products – any time and from anywhere. The app can support you in areas including:

- Resolving problems when implementing a project
- Troubleshooting when faults develop
- Expanding a system or planning a new system

Furthermore, you have access to the Technical Forum and other articles from our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product announcements and much more

The "Siemens Industry Online Support" app is available for Apple iOS and Android.

Data matrix code on the nameplate

The data matrix code on the nameplate contains the specific device data. This code can be read with a smartphone and technical information about the device displayed via the "Industry Online Support" mobile app.

1.10 Important product information

Using OpenSSL

This product can contain the following software:

- Software developed by the OpenSSL project for use in the OpenSSL toolkit
- Cryptographic software created by Eric Young.
- Software developed by Eric Young

You can find more information on the internet:

- OpenSSL (https://www.openssl.org)
- Cryptsoft (https://www.cryptsoft.com)

Compliance with the General Data Protection Regulation

Siemens observes standard data protection principles, in particular the data minimization rules (privacy by design).

For this product, this means:

The product does not process or store any personal data, only technical function data (e.g. time stamps). If the user links this data with other data (e.g. shift plans) or if he/she stores person-related data on the same data medium (e.g. hard disk), thus personalizing this data, he/she must ensure compliance with the applicable data protection stipulations.

Fundamental safety instructions 2

2.1 General safety instructions

⚠ **WARNING**

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ **WARNING**

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.2 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. Application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.3 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity (https://new.siemens.com/global/en/products/services/cert.html#Subscriptions).

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, or worms, can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- On completion of commissioning, check all security-related settings.

Fundamentals 3

3.1 Safety functions of the F-PLC

The safety functions of the F-PLC are predominantly implemented in the software. The safety functions are executed by the F-system to bring the system into a safe state if a hazardous event takes place – and to maintain it in this safe state.

These safety functions are mainly included in the following components:

- **In the safety-relevant user program (safety program) in the PLC with active F-capability (F-PLC)**
  Users only program the user safety function. The safety function for the process itself can be implemented using a user safety function - or a fault response function. If, in the case of a fault, the F-system can no longer execute the actual user safety function, then it executes the fault response function: for example, the associated outputs are shut down, and the F-PLC goes into the STOP mode, if necessary.
- **In the failsafe inputs and outputs (F-I/O)**
  The F-I/O guarantees the safety-relevant processing of information from the field (sensors: e.g. EMERGENCY STOP pushbuttons, light barriers; actuators, e.g. motor controls). It has all of the necessary hardware and software components for safety-relevant processing, corresponding to the specified safety class.

3.2 Safety functions integrated in the drive

Safety Integrated supports, through SINAMICS Integrated (as subcomponent of the SINUMERIK control system), the SINAMICS Safety Integrated Functions (Page 103). These safety functions integrated in the drive can communicate with the process via safety-related input/output signals. They can be implemented for each individual axis and spindle.

Differentiation by scope

Based on the scope of the available functions and the licensing required, a distinction is made between "Basic Functions" and "Extended Functions":

- Safety Integrated Basic Functions are always included as part of the standard scope of the drive, and can be used without an additional license. These functions do not require an encoder and/or do not place any special requirements on the encoder used.
- Safety Integrated Extended Functions require an additional license (Page 45). Extended Functions with encoder require a safety-related encoder concept (Page 208).

Differentiation by application

Based on the specific application, safety functions integrated in the drive can be split up into three main classes:

- Functions for safely stopping the drive, without having to disconnect the power from the line supply
- Functions for safely monitoring the motion of a drive
- Functions for safely monitoring the position of a drive

Listing of all functions by application

Table 3-1 Functions for safely stopping the drive, without having to disconnect the power from the line supply

Safety Function	Scope	Brief description	Configuration via
Safe Torque Off (STO)	Basic/ Extended	Safe Torque Off is a safety function that prevents the drive from restarting unexpectedly in accordance with EN- 60204-1. STO prevents the supply of power to the motor, which can produce a torque. This is equivalent to stop Category 0.	STO (Basic/Extended) (Page 115)
Safe Stop 1 (SS1, time-controlled)	Basic	Safe Stop 1 is based on the "Safe Torque Off" function. This means that a Category 1 stop in accordance with EN 60204-1 can be implemented.	SS1 Basic (Page 104)
Safe Stop 1 (SS1, time and acceleration controlled)	Extended		SS1 Extended (Page 108)
Safe Brake Control (SBC)	Basic/ Extended	Safe Brake Control is used to safely control a holding brake.[1) 2)]	SBC (Basic/Extended) (Page 121)
Safe Brake Test (SBT)	Extended	The diagnostic function "Safe Brake Test" function (SBT) checks the required holding torque of a brake (operating or holding brake). [3)] This function is in conformance with SIL 1 according to IEC 61508 and to PLd/Cat. 2 according to EN ISO 13849-1.	SBT (Page 185)
Safe Stop 2 (SS2)	Extended	Safe Stop 2 is used to safely brake the motor with a subsequent transition into the "Safe Operating Stop" state (SOS). This means that a Category 2 stop in accordance with EN 60204-1 can be implemented.	SS2 (Page 128)

Safety Function	Scope	Brief description	Configuration via
Safe Stop 2 with external stop (SS2E)	Extended	The 'Safe Stop 2 with external stop' (SS2E) safety function is used to brake the motor safely. The drive does not automatically brake the motor, but instead follows the specified speed setpoint.	SS2E (Page 131)
Safe Stop 2 Extended Stop and Retract (SS2ESR)	Extended	The "Safe Stop 2 Extended Stop and Retract (SS2ESR)" safety function is used to brake the motor safely. The drive does not automatically brake the motor, but instead follows the specified speed setpoint. This can also result in fast retraction motion. During the delay time p9554, the brake ramp (SBR) and the acceleration (SAM) are not monitored, and there is no standstill detection. SOS becomes active after delay time p9554 has expired.	SS2ESR (Page 135)
Safe Operating Stop (SOS)	Extended	Safe Operating Stop is used to protect against unintentional movement. The drive is in closed-loop control mode and is not disconnected from the power supply.	SOS (Page 139)

1) Note regarding Power/Motor Modules in the chassis format:
For the chassis format, SBC is only supported by Power/Motor Modules with the number 3 or higher at the last position of the Article number. For this design, a Safe Brake Adapter is also required.

2) Note regarding Power/Motor Modules in blocksize format:
blocksize Power Modules additionally require a Safe Brake Relay for this function.

3) The Safe Brake Test is purely a diagnostic function, but for organizational reasons is included in the list of Safety Integrated Extended Functions.

Table 3-2 Functions for safely monitoring the motion of a drive

Safety Function	Scope	Brief description	Configuration via
Safely-Limited Speed (SLS)	Extended	Safely-Limited Speed monitors that the drive does not exceed a preset speed/velocity limit.	SLS (Page 143)
Safely-Limited Acceleration (SLA)	Extended	Safely-Limited Acceleration monitors (the same as SLS) the acceleration, and intervenes when a limit value is violated.	SLA (Page 200)
Safe Speed Monitor (SSM)	Extended	Safe Speed Monitor is used for safely identifying when a speed limit is fallen below in both directions of motion, e.g. to identify zero speed. A failsafe output signal is available for further processing.	SSM (Page 156)
Safe Direction (SDI)	Extended	Safe Direction is used to safely monitor the direction of motion.	SDI (Page 168)

Table 3-3 Functions for safely monitoring the position of a drive

Safety Function	Scope	Brief description	Configuration via
Safely-Limited Position (SLP)	Extended	Safely-Limited Position ensures that a freely definable traversing range is not left.	SLP (Page 176)
Transferring safe position values (SP)	Extended	The "Transfer safe position values (SP)" function enables you to transfer a safe position to a higher-level control via PROFIsafe.	SP (Page 181)
Safe cams (SCA)	Extended	Safe electronic cams enable a secure, axis-specific range detection or a work zone / protection zone delimitation.	SCA (Page 197)

Note

In SINAMICS as "Advanced"

The 3 position monitoring functions in SINUMERIK belong to Extended Functions. However, in SINAMICS they are encrypted and belong there to the Advanced Functions (which require their own license). For reasons of transparency, in this manual they are still called Extended Functions.

3.3 Approvals

The "Safety Integrated" safety system with the "F-PLC" and "SINAMICS Integrated" safety-related components can be used up to the following safety requirements:

- SINAMICS Safety Integrated Functions:
  - SIL2 - safety class (Safety Integrity Level) according to IEC 61508
  - Performance level (PL) d according to DIN EN ISO 13849-1
  - Category 3 to DIN EN ISO 13849-1
- F-PLC:
  - SIL3 - safety class (Safety Integrity Level) according to IEC 61508

Note

F-system SIMATIC Safety/Safety Integrated is used to control processes, where a safe state can be immediately achieved by shutting down.

It is only permissible to use SIMATIC Safety/Safety Integrated to control processes, where an immediate shutdown does not represent any risk to persons and the environment.

Additional information

Information about the maximum safety requirements that can be achieved for the individual safety-related components is provided in the relevant documentation.

- Programming and Operating Manual - SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126)
- SINAMICS S120 Safety Integrated Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109760403)

3.4 Safety-relevant processing using SINUMERIK ONE components

In the "SINUMERIK Safety Integrated (F-PLC)" mode, safety-relevant internal and external signals are processed in the safety-relevant user program (safety program) of the F-PLC:

- F-I/O is connected to the F-PLC, and directly controlled via PROFIsafe.
  The safety functions are mainly embedded in the safety program (F-PLC) - and in the failsafe inputs and outputs (F-I/O).
- Safety functions integrated in the drive are also controlled via PROFIsafe:
  The PROFIsafe telegrams (for example, SIEMENS telegram 903) are transferred to the DP Integrated interface from the PLC to the SINAMICS Integrated (DRIVE) for this purpose.

Status and control information is transferred with SIC/SCC (Safety Info Channel / Safety Control Channel) between the integrated subcomponents of the SINUMERIK ONE (PLC, NC and SINAMICS Integrated).

PROFIsafe communication is only possible between F-components. With the SINUMERIK ONE, PROFIsafe communication is performed between the following components:

- F-PLC as PROFIsafe host
- SINAMICS Integrated (DRIVE) as PROFIsafe slave/device
- F-I/O as PROFIsafe slave/device

Details on internal processing of safety-related communication

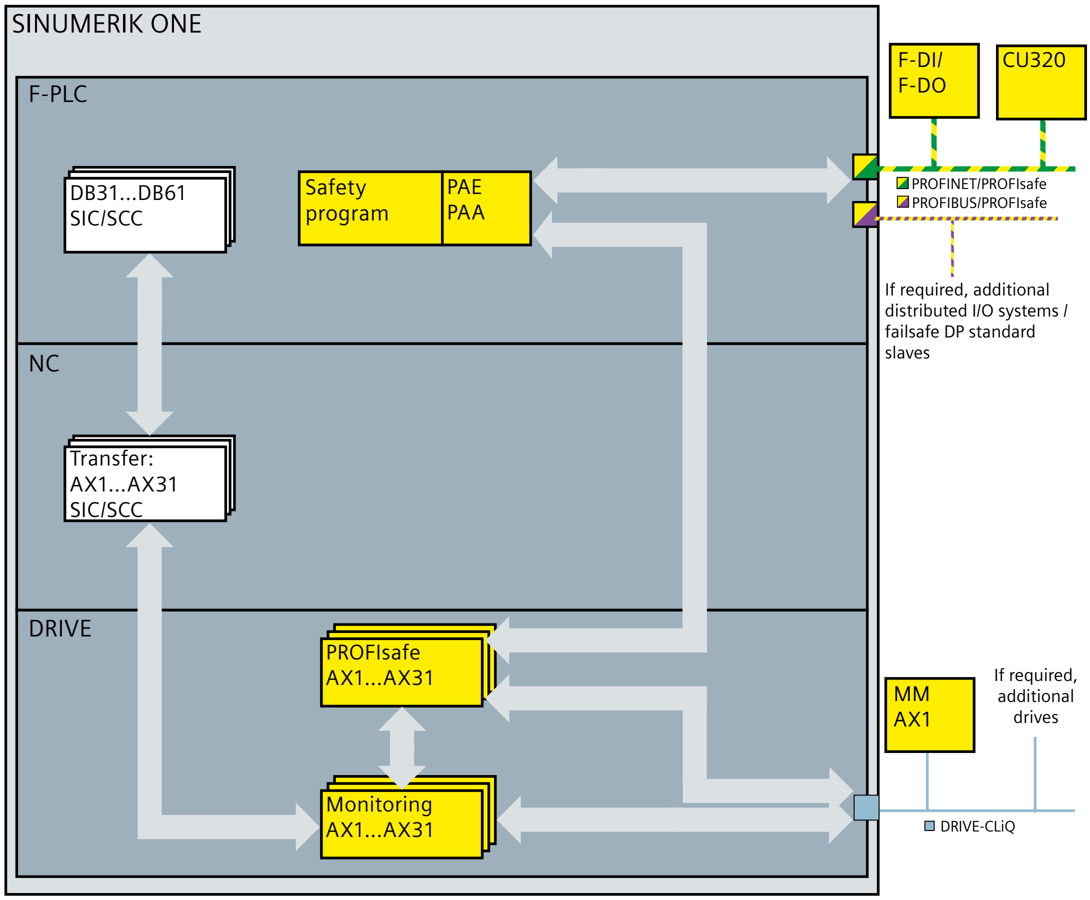


Figure 3-1 Component diagram for processing safety-relevant information and data

Table 3-4 Subcomponents of the SINUMERIK ONE

F-PLC PROFIsafe host	• Processing safety-relevant internal and external signals in the safety-relevant user program (safety program) See: Safety program of the F-PLC (Page 51) • Processing status and control signals (SIC/SCC) via the corresponding axis DB (LBP_Axis1 [DB31] ... LBP_Axis31 [DB61]) See: PLC user interface (DB3x) (Page 232), SIC/SCC (Page 231)
NC	• Transfers status and control information (SIC/SCC, axis DB) between the F-PLC and DRIVE • Reads-in safety-relevant messages from the message buffers of SINAMICS Integrated to the NC alarm buffer

HMI	• Displays safety-relevant messages/alarms from the NCK alarm buffer • Reads out and displays additional safety-relevant diagnostics information directly from the drive • Displays a safety delete symbol for active safety messages • Displays safety-relevant diagnostic information (alarms) of the F-PLC and F-I/O See: Diagnostics (Page 347)
DRIVE (SINAMICS Integrated) PROFIsafe slave	• Safety-relevant motion monitoring of NC-controlled drives (connected at the DRIVE-CLiQ interface) See: Safety functions integrated in the drive (Page 30) • Executes fault response functions or user safety functions

Table 3-5 I/O and drives

F-I/O PROFIsafe slave	The F-I/O guarantees the safety-relevant processing of information from the field (sensors: e.g. EMERGENCY STOP pushbuttons, light barriers; actuators, e.g. motor controls). The safety function for the process itself can be implemented using a user safety function - or a fault response function. See: Safety program of the F-PLC (Page 51), F-I/O for PROFIBUS DP (Page 38), F-I/O for PROFINET IO (Page 38)
NC-controlled drives	For each individual axis and spindle, safety functions integrated in the drive can be implemented, which can communicate via safety-relevant input/output signals with the process. See: Safety functions integrated in the drive (Page 30), drive components (Page 37)

3.5 Hardware components

The Safety Integrated safety solution places specific requirements on the hardware components that are used.

Independent of the scope of the Safety Functions used, you can use failsafe SIMATIC and standard I/O for PROFIBUS DP (Page 38) or PROFINET IO (Page 38) - as known from SIMATIC Safety.

The drive system that you can use (Page 39) depends on whether a safety-relevant encoder is used - and which axis type is to be used.

Hardware components

The following diagram shows an overview of a possible structure with failsafe hardware components.

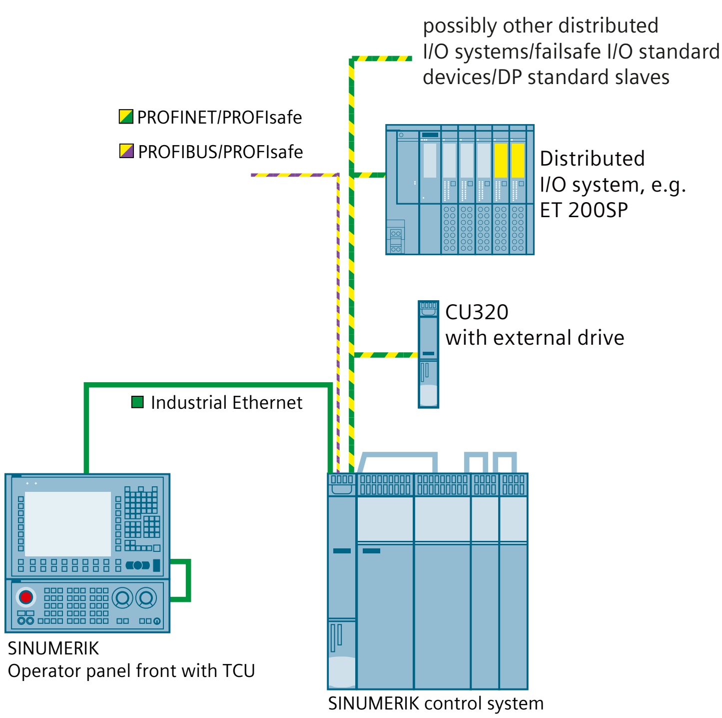


Figure 3-2 Configuration diagram: Hardware structure with Safety Integrated

3.5.1 F-I/O for PROFIBUS DP

You can use the following failsafe components in SINUMERIK Safety F-systems on PROFIBUS DP:

- F-CPUs with DP interface
- Failsafe inputs and outputs (F-I/O), such as:
  - S7-1500/ET 200MP failsafe modules
  - ET 200SP failsafe modules
  - ET 200S failsafe modules
  - ET 200pro failsafe modules
  - ET 200AL failsafe I/O module
  - ET 200iSP failsafe modules
  - ET 200eco failsafe I/O module
  - Failsafe GSD based DP slaves (light grid, laser scanner, etc.)

You have the option to expand the configuration with standard I/O.

3.5.2 F-I/O for PROFINET IO

You can use the following failsafe components in SINUMERIK Safety F-systems on PROFINET IO:

- F-CPUs with PN interface
- Failsafe inputs and outputs (F-I/O), such as:
  - S7-1500/ET 200MP failsafe modules
  - ET 200SP failsafe modules
  - ET 200S failsafe modules
  - ET 200pro failsafe modules
  - ET 200iSP failsafe modules
  - ET 200eco PN failsafe I/O modules
  - ET 200AL failsafe I/O module
  - Failsafe GSD based I/O devices (light grid, laser scanner, etc.)

You have the option to expand the configuration with standard I/O.

3.5.3 Drive components

The drive system that you can use depends on whether a safety-relevant encoder is used - and which axis type is to be used.

Table 3-6 Supported axis types as a function of the drive type and the use of a safety-relevant encoder

	Spindle	Rotary axis	Linear axis
Induction motor with encoder	Yes	Yes	Yes
Induction motor without encoder	Yes	No	No
Synchronous motor with encoder	Yes	Yes	Yes
Synchronous motor without encoder	No	No	No
SINAMICS HLA with encoder	No	No	Yes[1)]
SINAMICS HLA without encoder	No	No	No

[1)] Not all Basic or Extended Functions are supported, see SINAMICS HLA (Page 42) or SINAMICS HLA (Page 42).

3.5.3.1 Interconnecting DRIVE-CLiQ components

For Safety Integrated Functions, the general DRIVE-CLiQ rules apply as a basic principle. You will find these rules in Chapter "Rules for connection with DRIVE-CLiQ" in the following Manual:

- "SINAMICS S120 Drive Functions" Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109771805)

Beyond this, the following rules also apply to Safety Integrated:

Rules for Safety Integrated Basic Functions

- Maximum of 4 drives per DRIVE-CLiQ line for control via PROFIsafe

Rules for Safety Integrated Extended Functions

- Maximum of 6 servo axes for default clock cycle settings (safety monitoring clock cycle = 12 ms; current controller cycle = 125 μs); of which a maximum of 4 servo axes are in one DRIVE-CLiQ line
- Maximum of 6 vector axes for the following clock cycle settings (safety monitoring cycle = 12 ms; current controller cycle = 500 μs)
- One Double Motor Module corresponds to 2 DRIVE-CLiQ participants.

- On Double Motor Modules, on the drive objects, different values for p9511 are not permitted, even if the values in p0115[0] are different.
- You can operate a maximum of 4 Motor Modules with Safety Extended Functions on one DRIVE-CLiQ line. The following condition applies in this regard: T_{IReg} (current controller sampling time) = 125 μs for all axes. In addition to the 4 Motor Modules with Safety Extended Functions, you can also operate the following modules on a DRIVE-CLiQ line:
  – A Line Module if T_{IReg} (current controller sampling time) ≥ 250 μs
  – A Motor Module if T_{IReg} (current controller sampling time) ≥ 125 μs
  – A maximum of 7 Sensor Modules or DRIVE-CLiQ encoders

3.5.3.2 Drive monitoring with or without encoder

In the Safety Integrated system, encoderless safety operation is only supported for spindles with induction motors.

If motors without a (safety-capable) encoder are being used, not all Safety Integrated Functions can be used.

Note

Definition: "Without encoder"

When "without encoder" is used in this manual, then this always means that either no encoder or no safety-capable encoder is being used.

In operation without encoder the actual speed values are calculated from the measured electrical actual values. Therefore, speed monitoring is also possible during operation without encoder.

The configuration of the Safety Integrated Functions and the selection of monitoring with or without encoder is realized in the startup (commissioning) area of SINUMERIK Operate.

The safety functions integrated in the drive that are actually supported depends on the drive components used (drive and axis type, and whether a safety-relevant encoder is used).

Table 3-7 Safety Integrated Functions in operation with or without encoder

Function	Basic	Extended	HLA	Electric drive		Brief description
				With encoder	Without encoder	
STO/SS1 Basic Safe Torque Off/Safe Stop 1	x	-	x3)	x	x1)	Safe Torque Off / Safe Stop according to Stop Category 1 of DIN EN 60204-1.
STO Extended Safe Torque Off	-	x	x3)	x	x1)	Safe Torque Off
SBC Safe Brake Control	x	x	-	x	x1)	Safe brake control
SS1 Extended Safe Stop 1	-	x	x3)	x	x1)	Safe Stop according to Stop Category 1 of DIN EN 60204-1.

Function	Basic	Extended	HLA	Electric drive		Brief description
				With encoder	Without encoder	
SOS Safe Operating Stop	-	x	x[3]	x	-	Safe monitoring of the standstill position
SS2 Safe Stop 2	-	x	x[3]	x	-	Safe stopping process in accordance with stop Category 2
SS2E SS2 with external stop	-	x	x[3]	x	x[1]	SS2 with external stop
SS2ESR Safe Stop 2 Extended Stop and Retract	-	x	x[3]	x	x[1]	Safe Stop 2 Extended Stop and Retract
SLS Safely-Limited Speed	-	x	x[3)]	x	x[1)]	Safely-Limited Speed
SSM Safe Speed Monitor	-	x	x[3)]	x	x[1)]	Safe Speed Monitoring
SAM Safe Acceleration Monitor	-	x	-	x	x[1, 2)]	Safe Acceleration Monitoring
SBR Safe Brake Ramp	-	x	-	x	x[1)]	Safe brake ramp monitoring
SDI Safe Direction	-	x	x[3)]	x	x[1)]	Safe motion direction
SLP/SP Safely-Limited Position/ Safe Position	-	x	x[3)]	x	x[1)]	Safely-Limited Position/Safe Position
SLA Safely-Limited Acceleration	-	x	x[3)]	x	x[1)]	Safely-Limited Acceleration
SBT (diagnostic function) Safe Brake Test	-	x	-	x	-	Safe Brake Test SBT is a pure **diagnostic function** - but for organizational reasons is included in the list of Safety Integrated Extended Functions.
SCA Safe Cam	-	x	x	x	-	Safe Cam

1) Safety operation without encoder is only supported for spindles equipped with induction motors, see also Table 3-6 Supported axis types as a function of the drive type and the use of a safety-relevant encoder (Page 39).

2) Only for the function setting "Safety without encoder with accel_monitoring".

3) Encoderless Safety mode with SINAMICS HLA is not supported either for Basic Functions or for Extended Functions, see also SINAMICS HLA (Page 42).

See also

Drive components (Page 39)

3.5.3.3 Induction motors and synchronous motors

Approved encoders

Motors with sin/cos encoder and encoder evaluation with DRIVE-CLiQ interface or via Sensor Module SMC20, SME20/25/120/125.

A list of approved encoders is provided in Siemens Industry Online Support under Entry ID 33512621 (https://support.industry.siemens.com/cs/document/33512621?dti=0&dl=en).

3.5.3.4 SINAMICS HLA

Safety operation without encoder with HLA is neither supported for Basic nor for Extended Functions. When operating SINAMICS HLA in a safety mode, you require encoder types that have been approved for SINAMICS HLA.

Note

Comparison, description of electric ↔ hydraulic drives

In this Safety Integrated commissioning manual, Safety Integrated Functions are described from the perspective of an electric drive. However, these descriptions essentially also apply in the same way for hydraulic systems. You can find parameters and messages for the HLA drive object in the SINAMICS S120/S150 List Manual.

Encoder types supported by SINAMICS HLA

The following encoder types are permissible for SINAMICS HLA:

- Single-encoder systems
  - DRIVE-CLiQ encoder with safety capability
  - sin/cos encoder connected via SME20/25, SME120/125 or SMC20 (1Vss, pure analog signal processing)
- 2-encoder systems
  - Encoders with DRIVE-CLiQ connection
  - sin/cos encoder connected via SME20/25, SME120/125 or SMC20 (1Vss, pure analog signal processing)

Basic Functions supported by SINAMICS HLA

SINAMICS HLA supports the following Safety Integrated Basic Functions:

- Basic Functions
  These functions are part of the standard scope of the drive and can be used without requiring an additional license. These functions are always available. These functions do not require an encoder and/or do not place any special requirements on the encoder used.
  - Safe Torque Off (STO)
    Safe Torque Off is a safety function that prevents the drive from restarting unexpectedly in accordance with EN- 60204-1. STO prevents the supply of power to the valve, which can produce a force. It is equivalent to stop Category 0.
  - Safe Stop 1 (SS1, time-controlled)
    Safe Stop 1 is based on the "Safe Torque Off" function. This means that a Category 1 stop in accordance with EN 60204-1 can be implemented.

These functions are part of the standard scope of the drive and can be used without requiring an additional license.

Extended Functions supported by SINAMICS HLA

SINAMICS HLA supports the following Safety Integrated Extended Functions:

- Safe Torque Off (STO)
  Safe Torque Off is a safety function that prevents the drive from restarting unexpectedly according to EN- 60204-1.
- Safe Stop 1 (SS1, time and acceleration controlled)
  Safe Stop 1 is based on the "Safe Torque Off" function. This means that a Category 1 stop in accordance with EN 60204-1 can be implemented.
- Safe Operating Stop (SOS)
  Safe Operating Stop is used to protect against unintentional movement. The drive is in closed-loop control mode and is not disconnected from the power supply.
- Safe Stop 2 (SS2)
  Safe Stop 2 is used to safely brake the valve with a subsequent transition into the "Safe Operating Stop" state (SOS). This means that a Category 2 stop in accordance with EN 60204-1 can be implemented.
- Safe Stop 2 with external stop (SS2E)
  The 'Safe Stop 2 with external stop' (SS2E) safety function is used to brake the motor safely. The drive does not automatically brake the motor, but instead follows the specified speed setpoint.
- Safe Stop 2 Extended Stop and Retract (SS2ESR)
  The "Safe Stop 2 Extended Stop and Retract (SS2ESR)" safety function is used to brake the motor safely. The drive does not automatically brake the motor, but instead follows the specified speed setpoint. This can also result in fast retraction motion.
- Safely-Limited Speed (SLS)
  Safely-Limited Speed ensures that the drive does not exceed a preset speed limit.

- Safe Speed Monitor (SSM)
  Safe Speed Monitor is used for safely identifying when a speed limit is undershot in both directions of motion, e.g. to identify zero speed. A failsafe output signal is available for further processing.
- Safe Direction (SDI)
  Safe Direction is used to safely monitor the direction of motion.
- Safely-Limited Acceleration (SLA)
  Safely-Limited Acceleration monitors (the same as SLS) the acceleration, and intervenes when a limit value is violated. However, SLA cannot prevent that the acceleration threshold is briefly exceeded.
- Safely-Limited Position (SLP)
  Safely-Limited Position ensures that a freely definable traversing range is not left.
- Transferring safe position values (SP)
  The "Transfer safe position values (SP)" function enables you to transfer a safe position to a higher-level control via PROFIsafe.
- Safe Cam (SCA)
  Safe electronic cams enable a secure, axis-specific range detection or a work zone / protection zone delimitation.

These functions require an additional Safety Integrated license (Page 45).

3.6 Safety components and licensing

3.6.1 Software components required

When configuring the system, the STEP 7 Safety Advanced option package is required. This option package is integrated in package "SIMATIC STEP 7 Professional V17". The software can be immediately used once the license for the option package has been installed.

Engineering system:

- TIA Portal V17
- SIMATIC STEP 7 Professional V17
  – SIMATIC STEP 7 Safety Advanced V17
- SINUMERIK ONE STEP 7 Toolbox V17

CNC software:

- SINUMERIK CNC software V6.15
- SINUMERIK Operate V4.95

3.6.2 Licensing of axes/spindles and F-PLC

To use Safety Integrated, you require in addition to the license for SIMATIC STEP 7 Safety Advanced (TIA Portal), the appropriate software options for the RT function:

Table 3-8 Software options when using Safety Integrated

Software option	Article No.	Purpose
SINUMERIK ONE Safety Integrated - F-PLC	6FC5800-0BS60-0YB0	Activate the F-PLC in the SINUMERIK control system to process the failsafe sensors and actuators in an F-program.
SINUMERIK ONE Safety Integrated - axis/spin-dle	6FC5800-0BK00-0YB0	Use the motion control functions of the SINAMICS Integrated in the "SINUMERIK Safety Integrated (F-PLC)" mode. License for 1 axis/spindle, multiple licensing in or-der to be able to use additional axes/spindles.
SINUMERIK ONE Safety Integrated - multi axis packet	6FC5800-0BS61-0YB0	Use the motion control functions of the SINAMICS Integrated in the "SINUMERIK Safety Integrated (F-PLC)" mode. License for any number of axes/spindles.

Depending on the functions used, you must license the appropriate software options and set in the machine data:

- MD19500 $MN_SAFE_PLC_LOGIC: Safety Integrated basic option - F-PLC
- MD19121 $MN_NUM_DRIVEBASED_SAFE_AXES: Number of axes/spindles in the "SINUMERIK Safety Integrated (F-PLC)" mode

Additional licensing information:

You can find additional information about licensing in:

SINUMERIK ONE Commissioning Manual: Work steps for configuring and commissioning (https://support.industry.siemens.com/cs/de/en/view/109777606)

3.7 Components and basic configuration in the TIA Portal

3.7.1 Structure of a project view in the TIA Portal

Overview

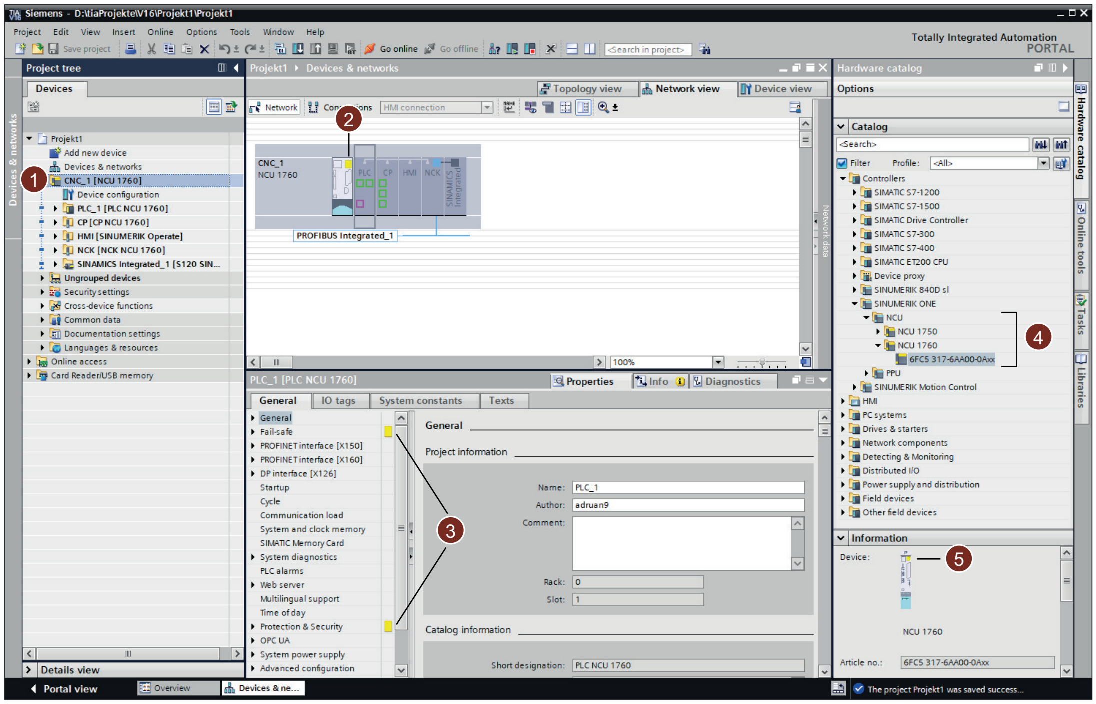
All safety-related resources are marked yellow in the TIA Portal, e.g. in the following views:

- Network view, device view, topology view
- Project tree
- Hardware catalog
- Inspector window or object properties
- Program editor

This also applies to the SINUMERIK components:

- NCU
  Because the subcomponents PLC and SINAMICS Integrated support Safety Integrated Functions, the higher-level NCU is marked as safety-oriented resource.
- Integrated PLC
- Integrated SINAMICS Integrated
- NX

Marking failsafe components in the TIA Portal



① The project tree shows which components of your project are F-components.

② In the network view, device view or topology view, the Safety Integrated marking is on the NCU, representative for the integrated components. External devices, e.g. NX, may have their own Safety Integrated marking.

③ Safety-related settings are marked in the "Properties" inspector window.

④ Folders and the devices themselves are marked in the hardware catalog. You can therefore see whether Safety Integrated is supported before inserting the device.

⑤ Failsafe devices are also marked in the information area of the hardware catalog.

Figure 3-3 Marking failsafe components in the TIA Portal

EMERGENCY STOP button symbol when using Safety Integrated

If you activate the "SINUMERIK Safety Integrated (F-PLC)" mode and therefore use PROFIsafe telegrams, all devices with failsafe modules (PROFIsafe telegrams) also have an EMERGENCY STOP button symbol in the network and topology view:

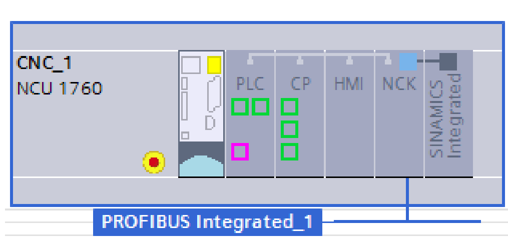


Figure 3-4 NCU with EMERGENCY STOP button symbol

3.8 Overview, SafeUserData

With SafeUserData (SUD), at a SINUMERIK control, safety-related configuration data can be entered and retentively saved using the HMI of the SINUMERIK Commissioning Tool. The configuration data is available to the safety program in an F-DB defined by the OEM, and can be evaluated and processed in the safety program.

The following properties and constraints apply to SafeUserData:

- Up to 32 instances (data sets) can be created.
- "Bool", "Int" and "DInt" data types are supported. When doing this, a data set with 16 signals of the same type can always be configured.
- OEMs can assign the SUD tag names.
- Any change to the SUD requires the "Manufacture" protection level and must be authorized using a safety-related enable signal defined by the OEM.
- Entering and confirming the SUD is only possible via SINUMERIK Operate (or the SINUMERIK ONE Commissioning Tool).
- The SUD become active immediately after confirmation.
- Every SUD instance has its own signature to identify the active net data. For a complete identification of the safety program, in addition to the program signature, all signatures of the SafeUserData must also be compared.
- The signatures and setting values of the SUD instances are documented in the SINUMERIK acceptance test report.
- The SUD program parts are implemented in the standard and F-component of the PLC.

Integrating SafeUserData

The following diagram provides an overview of the integration of SafeUserData in the system.

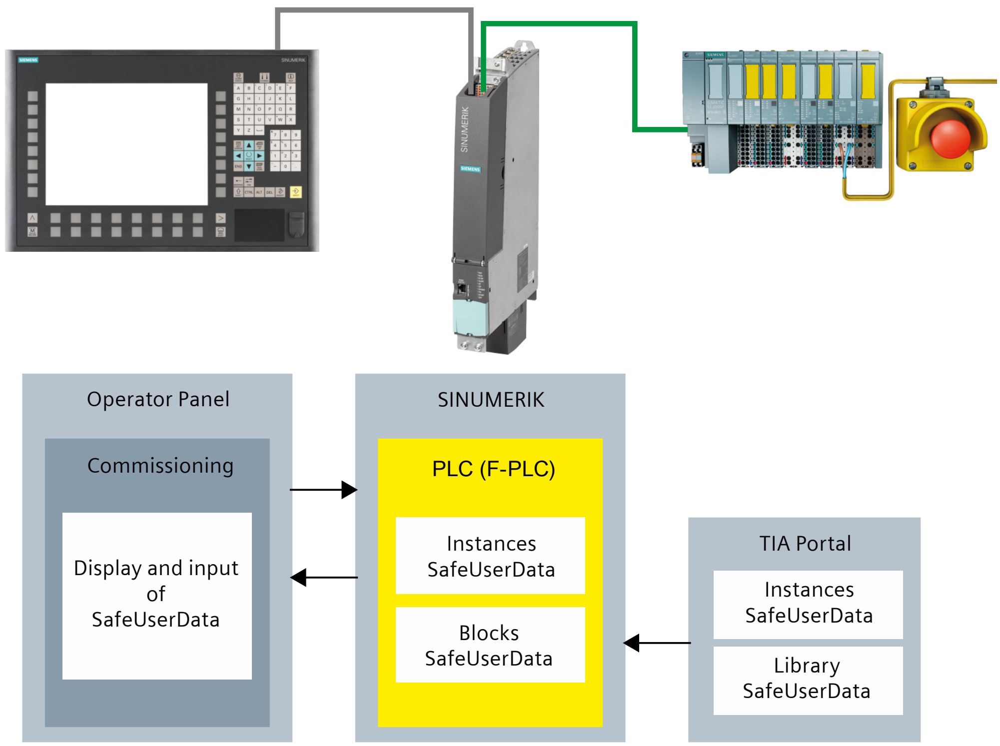


Figure 3-5 Arranging SUD entries in the system

See also

Integrating SUD program components in the TIA Portal (Page 81)

Configuring SafeUserData in the SINUMERIK Commissioning Tool (Page 283)

Safety program of the F-PLC 4

Information about F-PLC, F-I/O, the safety program and/or SIMATIC Safety in this manual serves as entry-level information only - and describes the special features relating to SINUMERIK.

Note

Important additional information

For space reasons, the information described in this manual cannot replace a complete SIMATIC Safety Manual. Therefore, when configuring these safety programs, it is crucial that you carefully follow the information provided in the TIA Portal help on SIMATIC Safety or in the "SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126)" Manual.

Principle of operation of the F-PLC safety functions

The safety functions of the F-PLC are mainly implemented in the software. The safety functions are executed by the F-system to bring the system into a safe state if a hazardous event takes place – and maintain it in this safe state. Safety functions are contained mainly in the following components:

- in the safety-related user program (safety program) in the PLC with active F-capability (F-PLC)
- in the failsafe inputs and outputs (F-I/O)
- in the safety functions integrated in the drive (drive components)

The F-I/O guarantees the safety-related processing of information from the field (sensors: e.g. EMERGENCY STOP pushbuttons, light barriers; actuators, e.g. motor controls). They have all of the required hardware and software components for safe processing, in accordance with the required Safety Integrity Level. The user only has to program the user safety function. The safety function for the process itself can be implemented using a user safety function - or a fault response function. In the event of an error, if the F-system can no longer execute its actual user safety function, it executes the fault reaction function; for example, the associated outputs are shut down, and the F-PLC goes into the STOP mode, if necessary.

Example of user safety function and fault reaction function

In the event of overpressure, the F-system will open a valve (user safety function). For a hazardous F-PLC fault, all outputs are shutdown (fault response function); the overpressure valve opens, and also the other actuators go into a safe state. For a non-faulty F-system, only the valve would be opened.

Safety program

If you activate (Page 240) Safety Integrated in the properties of the NCU, then the F-capability of the PLC is activated and an F-runtime group is created. The F-runtime group, together with the associated F-blocks, is known as the safety program.

You generate a safety program in the program editor. You program failsafe FBs and FCs in the FBD and LAD programming languages with operations from the option package - creating failsafe DBs.

Safety checks are automatically performed when compiling the safety program, and additional failsafe blocks are integrated for fault detection and fault response. This ensures that failures and faults are detected, and the appropriate responses triggered to keep the safety system in a safe state - or to transition it into a safe state.

In addition to the safety program, a standard user program can also be executed in the F-PLC. Standard and safety programs can coexist in an F-PLC. This is because the safety-related data of the safety program are protected against being inadvertently influenced by data of the standard user program.

Data can be exchanged between the safety and standard user program in the F-PLC using bit memories, data of a standard DB - and by accessing the process image of inputs and outputs.

Additional information

Programming Guidelines Safety for SIMATIC S7-1200/1500 (https://support.industry.siemens.com/cs/document/81318674/programming-guidelines-and-programming-styleguide-for-simatic-s7-1200-and-s7-1500?dti=0&lc=en-WW)

4.1 Program structure of the safety program (S7-1500)

Representation of program structure

For structuring purposes, a safety program consists of one or two F-runtime groups.

Each F-runtime group contains:

- F-blocks that you create using FBD or LAD or that are inserted from the project library or global libraries
- F-blocks that are added automatically (F-system blocks F-SBs, automatically generated F-blocks, F-runtime DB, and F-I/O DBs)

The following diagram shows the schematic structure of a safety program and/or an F-runtime group for an F-CPU S7-1500.

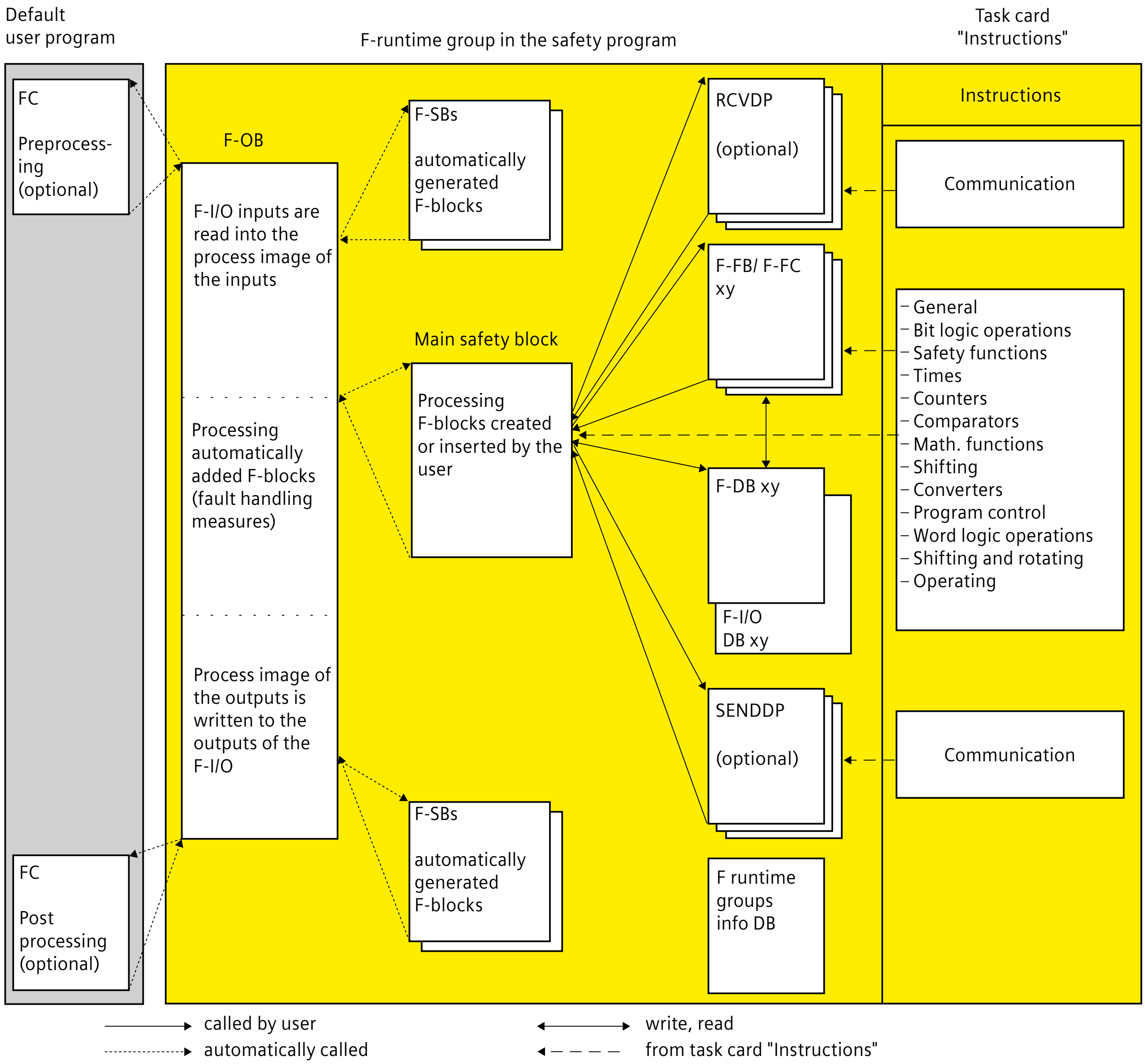


Figure 4-1 Schematic structure of a safety program and/or an F-runtime group for an F-CPU S7-1500

Main safety block

The main safety block is the first F-block of the safety program that you program yourself.

You must assign an F-runtime group to the main safety block.

The main safety block is called in an F-CPU S7-1500 using the F-OB assigned to the F-runtime group.

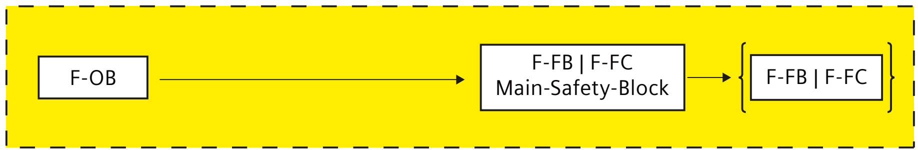


Figure 4-2 Calling the main safety block

F-runtime groups

To improve handling, a safety program consists of one or two "F-runtime groups". An F-runtime group is a logical construct of several related F-blocks that is formed internally by the F-system.

An F-runtime group consists of the following:

- An F-OB which calls the main safety block
- A main safety block (an F-FB/F-FC that you assign to the F-OB)
- Any additional F-FBs or F-FCs that you program using FBD or LAD and call from the main safety block
- One or more F-DBs, as needed
- F-I/O DBs
- F-runtime group information DB
- F-blocks from the project library or global libraries
- F-system blocks F-SBs
- Automatically generated F-blocks

Structuring the safety program in two F-runtime groups

You can divide your safety program into two F-runtime groups. By having parts of the safety program (one F-runtime group) run in a faster priority class, you achieve faster safety circuits with shorter response times.

Block types of the safety program

When the "SINUMERIK Safety Integrated (F-PLC)" mode is activated, then automatically an F-runtime group is created together with all the associated blocks:

- Calling block: FOB_RTG1
- Main safety block: Main_Safety_RTG1
- I-DB for the main safety block: Main_Safety_RTG1_DB

Note

Generate default failsafe program

In the STEP 7 safety settings you can define whether a safety program should be automatically created:

Procedure when defining an F-runtime group (Page 73)

4.2 Fail-Safe Blocks

F-blocks of an F-runtime group

The following table shows the F-blocks that you use in an F-runtime group:

F-block	Function
Main safety block	The first step in programming of the safety program is the main safety block. In F-CPU S7-1500, the main safety block is an F-FC or F-FB (with instance-DB), which is called by the F-OB.
F-FB/F-FC	Both in the main safety block as well as additional F-FBs and F-FCs, you can perform the following: • Program the safety program with the instructions available for F-blocks in FBD or LAD • Call other created F-FBs/F-FCs for structuring the safety program • Insert F-blocks from the project library or global libraries
F-DB	Optional failsafe data blocks that can be read- and write-accessed within the entire safety program.
F-I/O DB	An F-I/O DB is automatically generated for each F-I/O when it is configured. You can or you must access the variables of the F-I/O DB in conjunction with F-I/O accesses.
F-runtime group information DB	An F-runtime group information DB is created when you create an F-runtime group. The F-runtime group information DB provides information on the F-runtime group and on the safety program as a whole.

Note

You are not permitted to insert F-system blocks from the "System blocks" folder in a main safety block/F-FB/F-FC.

Instructions for the safety program

In task card "Instructions", depending on the F-CPU being used, you can find instructions that you can use to program the safety program.

You can find instructions that you know from the standard user program, such as bit logic operations, mathematical functions, functions for program control, and word logic operations.

Moreover, there are instructions with safety functions, e.g. for two-hand monitoring, discrepancy analysis, muting, emergency STOP/emergency OFF, safety door monitoring, feedback monitoring and instructions for safety-related communication between F-CPUs.

Additional information

A detailed description of the instructions for the safety program are provided in Chapter Instructions for the safety program (Page 70).

4.3 Safety Administration Editor

In the "SINUMERIK Safety Integrated (F-PLC)" mode, the "Safety Administration Editor" is available in the project tree.

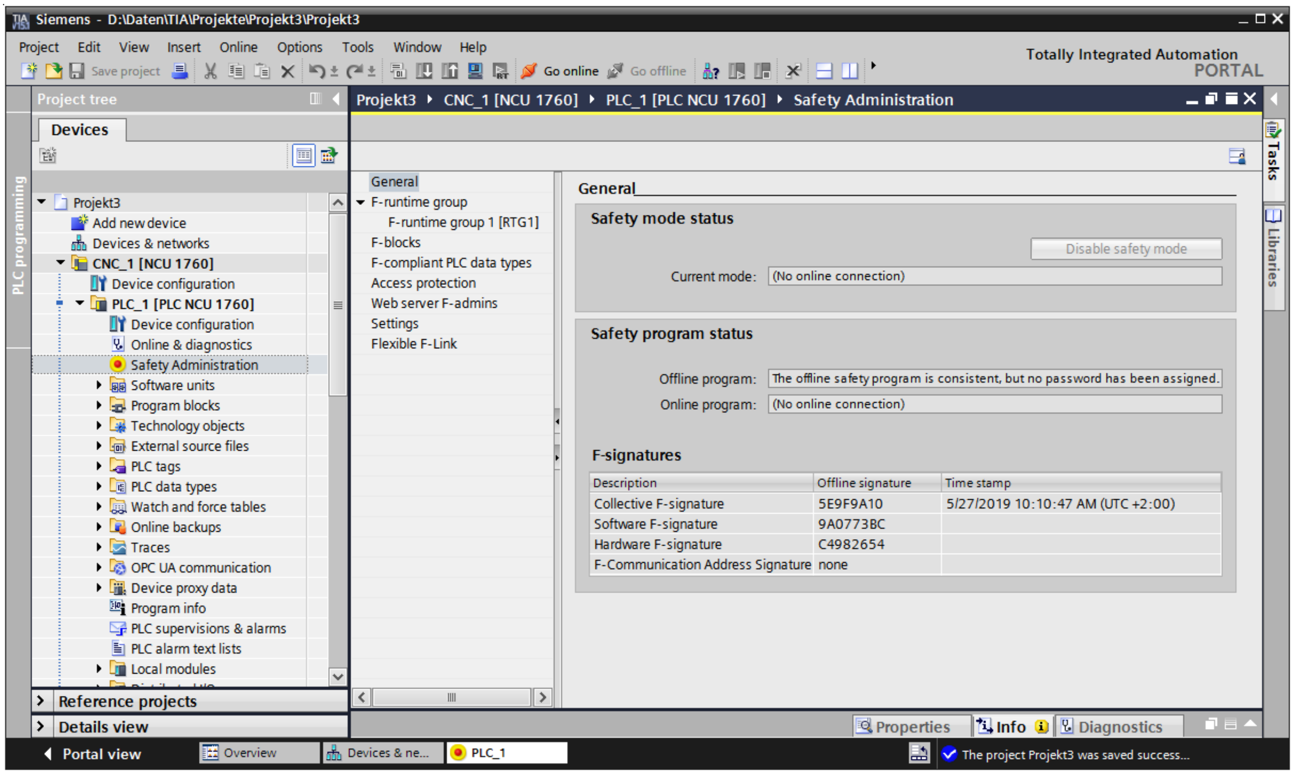


Figure 4-3 Safety Administration Editor

The Safety Administration Editor supports you when carrying out the following tasks:

- Display of the safety program status
- Deactivating safety operation
- Display of the collective signature
- Software F-signature
- Hardware F-signature (S7-1500)
- F-communication address signature
- Display of the safety mode status
- Creation/organization of F-runtime groups
- Display of information on the F-blocks
- Display information about F-conform PLC data types (UDT)
- Information for users with F-admin authorization
- Definition/change of the access protection

- Definition/change of the general settings for the safety program
- Creating/displaying/deleting F-communication via Flexible Link

The Safety Administration Editor is divided into the following sections:

- General
- F-runtime groups (Page 72)
- F-blocks
- F-conform PLC data types
- Access protection
- Web server F-admins
- Settings
- Flexible F-Link

Name for the F-I/O DBs

You can define whether the names of the F-I/O DBs are displayed with or without prefix (address of the I/O/of the module). The prefix is displayed as default.

Note

F-I/O DBs with prefix

The block name is not affected when shifting the axis-drive assignment, assuming that you do not change the address assignment. You do not have to change the F-program.

Proceed as follows to change the default setting:

1. In the Project Navigator, click on "Safety Administration".
2. In screen form "Settings" under "System generated objects", activate option "Create F-I/O DBs without prefix".

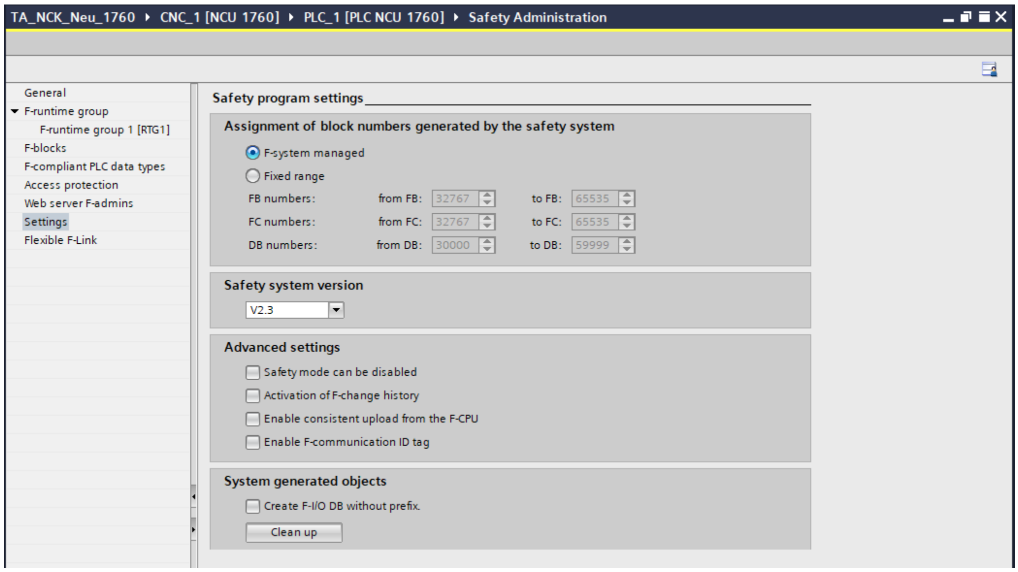


Figure 4-4 Settings for the safety system - objects created by the system

Examples:

- with prefix: e.g. F06700_DriveAxis01FIODB
- without prefix: e.g. DriveAxis01FIODB

More information

More information is provided in the help for SIMATIC STEP 7 Safety Advanced in Chapter "Safety Administration Editor".

4.4 Restrictions in the programming languages FBD/LAD

LAD and FBD programming languages

The user program in the F-CPU typically consists of a standard user program and a safety program.

The standard user program is created using standard programming languages such as SCL, STL, LAD, or FBD.

For the safety program, LAD or FBD may be used with certain restrictions in the instructions and the applicable data types and operand areas. Please also take into account the information regarding restrictions relating to individual instructions.

Supported instructions

The instructions that are supported are listed in the description of the instructions (Instructions for the safety program (Page 70)).

Note

It is not possible to connect the enable input EN and/or the enable output ENO.

Exception:

For the following instructions, by connecting enable output ENO, you can program an overflow detection:

- ADD (addition)
- SUB (subtraction)
- MUL (multiplication)
- DIV (dividing)
- NEG (generated a two's complement)
- ABS (generate absolute value)
- CONVERT (convert value)

Supported data types and parameter types

Only the following data types are supported:

- BOOL
- INT
- WORD
- DINT
- TIME

- ARRAY, ARRAY[*] when using instructions RD_ARRAY_I (read value from INT F-array) and RD_ARRAY_DI (read value from DINT F-array).
  Restrictions:
  - ARRAY only in F-global DBs
  - ARRAY limits: 0 up to max. 10000
  - ARRAY[*] only as in-out parameter (InOut) in F-FCs and F-FBs
  - ARRAY of UDT
  - ARRAY of bool
  - ARRAY of word
  - ARRAY of time
- F-conform PLC data types (UDT) (S7-1500)

Note

If the result of an instruction is located outside the permitted range for this data type, the F-CPU may switch to STOP. The cause of the diagnostics event is entered in the diagnostics buffer of the F-CPU.
You must therefore ensure that the permitted range for the data type is observed when creating the program, or select a matching data type or use the ENO output.

Observe the description of the individual instructions.

Non-permitted data and parameter types

The following types are **not** permitted:

- All of the types not listed under Section "Supported data and parameter types" (e.g. BYTE, REAL)
- Grouped data types (e.g. STRING, STRUCT)
- Parameter types (e.g. BLOCK_FB, BLOCK_DB, ANY)

Supported operand areas

The system memory of an F-CPU is divided into the same operand areas as the system memory of a standard CPU. You can access the operand areas listed in the table below from within the safety program.

Table 4-1 Supported operand areas

Operand area	Description
Process image of the inputs	
• Of F-I/O	Only read-only access to input channels of F-I/O is possible. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. The process image of the inputs of F-I/O is updated prior to the start of the main safety block.
• Of standard I/O	Input channels of standard I/O can only be accessed read-only. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. In addition, a process-specific validity check is required. See the *STEP 7 help* for the update times of the process image of the inputs of standard I/O.
Process image of the outputs	
• Of F-I/O	Only write-only access to output channels of F-I/O is possible. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. In the safety program, the values for the outputs of the F-I/O are calcu-lated and stored in the process image of the outputs. The process image of the outputs for F-I/O is updated after the end of the main safety block.
• Of standard I/O	Output channels of standard I/O are write-only channels. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. In the safety program, the values for the outputs of the standard I/O are also calculated and stored in the process image of the outputs, if needed. See the *STEP 7 help* for the update times of the process image of the outputs of standard I/O.
Bit memory	This area is used for data exchange with the standard user program. In addition, read access requires a process-specific validity check. A particular element of the bit memory can be either read- or write-ac-cessed in the safety program. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. Note that it is only permitted to use bit memory for connecting the standard user program and the safety program; it must not be used as a buffer for F-data.
Data blocks	

Operand area	Description
• F-DB	Data blocks store information for the program. They can either be defined as global data blocks such that all F-FBs, F-FCs, or main safety blocks can access them or assigned to a particular F-FB or main safety block (instance DB). A tag of a shared DB can only be accessed from one F-runtime group, and an instance DB only from the F-runtime group in which the corresponding F-FB/instruction is called.
• DB	This area is used for data exchange with the standard user program. In addition, read access requires a process-specific validity check. For a tag of a DB, either read access or write access is possible in the safety program. Transfer to IN_OUT parameters of an F-FB or F-FC is therefore not valid either. Please note that the tags of a DB can only be used for transferring data between the standard user program and the safety program; DBs must not be used as a buffer for F-data.
Temporary local data	This memory area holds the temporary tags of a block (or F-block) while the (F-) block is being executed. The local data stack also provides memory for transferring block parameters and for saving intermediate results.

File type conversion

Just as with the standard user program, there are two possibilities for file type conversion in the safety program.

- Implicit conversion
  The implicit conversion is executed as in the standard user program with the following restrictions: The bit length of the source data type has to match the bit length of the destination data type.
- Explicit conversion
  You use an explicit conversion instruction before the actual instruction is carried out.

Slice access

Slice access is not possible in the safety program.

Non-permitted operand areas

Access via units other than those listed in the table above is **not** permitted. The same applies to access to operand areas not listed, in particular:

- Data blocks that were automatically added
  Exception: certain tags in the F-I/O DB and in the F-runtime group information DB
- I/O area: Inputs
- I/O area: Outputs

Boolean constants "0" or "FALSE" and "1" or "TRUE" (S7-1500)

For F-CPUs S7-1500, Boolean constants "0" or "FALSE" and "1" or "TRUE" are available to supply parameters for block calls.

You can also create "1" or "TRUE" in a tag using instruction "Assignment".

To do this, in FBD, leave the box input of instruction "Assignment" unconnected. In LAD, you interconnect the input directly with the supply rail.

You obtain a tag with "0" or "FALSE" by subsequent inversion using instruction "Invert result of logic operation".

Example FBD:

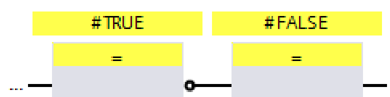


Figure 4-5 Example FBD

Example LAD:

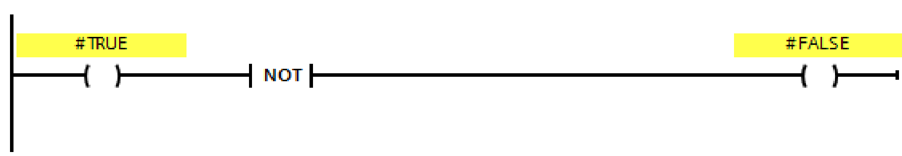


Figure 4-6 Example LAD

Operand area of temporary local data: Particularities

Note

Note when using the operand area of temporary local data that the first access of a local data element in a main safety block/F-FB/F-FC must always be a write access. This initializes the local data element.

Make sure that a temporary local data element is initialized prior to the first JMP, JMPN, or RET instruction.

The "local data bit" should be initialized with the Assign ("=") (FBD) or ("--( )") (LAD) instruction. Assign the local data bit a signal state of "0" or "1" as a Boolean constant.

Local data bits cannot be initialized with the Flip Flop (SR, RS), Set Output (S) or Reset Output (R) instructions.

The F-CPU can go to STOP if this is not observed. The cause of the diagnostic event is entered in the F-CPU diagnostics buffer.

"Fully qualified DB access"

Access to tags of a data block in an F-FB/F-FC is "fully qualified DB access". This also applies to initial access to tags of a data block after a jump label.

Example of "fully qualified DB access":

Assign a name for the F-DB, e.g. "FData1". Use the names assigned in the declaration of the F-DB instead of the absolute addresses.

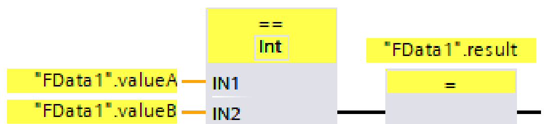


Figure 4-7 Example with fully-qualified access

Access to instance DBs

You can also access instance DBs of F-FBs with fully qualified access, e.g., for transfer of block parameters. It is not possible to access static local data in single/multi-instances of other F-FBs.

Note that accessing instance DBs of F-FBs that are not called in the safety program can cause the F-CPU to go to STOP mode.

Note

If you program global access operations to instance DBs or F-DBs, then you must ensure that the associated F-FB is called in the safety program.

4.5 F-conform PLC data types F (UDT)

Introduction

You declare and use F-conform PLC data types (UDT) as you would standard PLC data types (UDT). You can use F-conform PLC data types (UDT) in the safety program as well as in the standard user program.

Differences to standard PLC data types (UDT) are described in this chapter.

Information on using and declaring standard PLC data types (UDT) is provided in the help for *STEP 7* under "Declaring PLC data types".

Declaring F-conform PLC data types (UDT)

You declare F-conform PLC data types (UDT) as you would PLC data types (UDT).

In F-conform PLC data types (UDT), you can use all data types (Page 61), which you can also use in your safety program. Exception: ARRAY.

Proceed as follows for declaration:

1. In the project tree, in folder "PLC data types", click on "Add new data type".
2. To create F-conform PLC data types (UDT), in dialog "Add new data type", activate option "Create F-conform PLC data types".
3. Proceed as described in the help for *STEP 7* under "Programming the structure of PLC data types".

You specify default values for F-conform PLC data types (UDT) during the declaration.

Using F-conform PLC data types (UDT)

You use F-conform PLC data types as you would standard PLC data types (UDT).

Nesting depth for F-conform PLC data types

For F-conform PLC data types, the maximum nesting depth when compared to standard PLC data types (maximum nesting depth = 8) is restricted. There is a dependency on the call sequence of the block, in which a tag of the nested F-conform PLC data type is declared. Each call level of F-FCs or multi-instance of F-FBs reduces the maximum nesting depth of the F-conform PLC data types used. For multi-instance F-FBs, the caller counts as an additional level.

If a tag of a nested F-conform PLC data type is declared in a global F-data block, then its maximum nesting depth = 7.

Example 1

The main safety block (level 1) calls an F-FB as multi-instance (level 2), which in turn calls an F-FC (level 3), in which a tag with nested F-conform PLC data type is declared. This means a maximum nesting depth of 5 is available for the F-conform PLC data type used by the tag.

Example 2

The main safety block calls an F-FB as single instance (level 1), which in turn calls an F-FC (level 2), in which a tag with nested F-conform PLC data type is declared. This means a maximum nesting depth of 6 is available for the F-conform PLC data type used by the tag.

Changes to F-conform PLC data types (UDT)

You need the password for the safety program to change F-conform PLC data types (UDT). Regardless if you are using the F-conform PLC data type (UDT) in an F-block, in a standard block or not at all.

4.5.1 Grouping PLC variables for inputs and outputs of F-I/O in structures (S7-1500)

You group PLC tags for inputs and outputs of F-I/O in structures (structured PLC tag) as you would for inputs and outputs of standard I/O.

Use F-conform PLC data types (UDT).

Rules

When creating structured PLC tags for inputs and outputs of F-I/O, you must also observe the following rules in addition to the rules in the standard:

- You must not group inputs/outputs of standard I/O and F-I/O at the same time in a structured PLC tag.
- You may only group inputs/outputs of actually existing channels (channel value and value status) in a structured PLC tags.
  See also Access to SI-drives and F-I/O (Page 94)
- You may only group inputs/outputs of channels (channel value and value status) that are enabled in the hardware configuration in a structured PLC tag.
  See also Access to SI-drives and F-I/O (Page 94)
- In a structured PLC tag, you may only group inputs of channels (channel value and value status) that when "1oo2 (2v2) evaluation of the encoder" is set, provide the result of the "1oo2 (2v2) evaluation of the encoder".
  See also Access to SI-drives and F-I/O (Page 94)
- You should combine all inputs and/or outputs of an F-IO in a structured PLC tag. Then these can only start at a multiple of 16 bits for a distribution across several structured PLC tags. This is also applicable for nested F-conform PLC data types (UDT). See the rules in the standard. The F-CPU can go to STOP mode if this is disregarded. The cause of the diagnostics event is entered in the diagnostics buffer of the F-CPU.
- A structured PLC tag that groups outputs of an F-I/O must not overlap with other PLC tags. The F-CPU can go to STOP mode if this is disregarded. The cause of the diagnostics event is entered in the diagnostics buffer of the F-CPU.

Note

To observe these rules, you must declare the F-conform PLC data type that is used for the structured PLC tag accordingly.

You can identify which addresses can be occupied by a structured PLC tag from tab "I/O tags" in the configuration of an F-I/O.

4.6 Instructions for the safety program

When programming an F-block, in task card "Instructions", you can find all the instructions that you can use to program an F-block in LAD or FBD with the configured F-PLC. These instructions have a yellow background, as is already the case for as a safety-relevant functions.

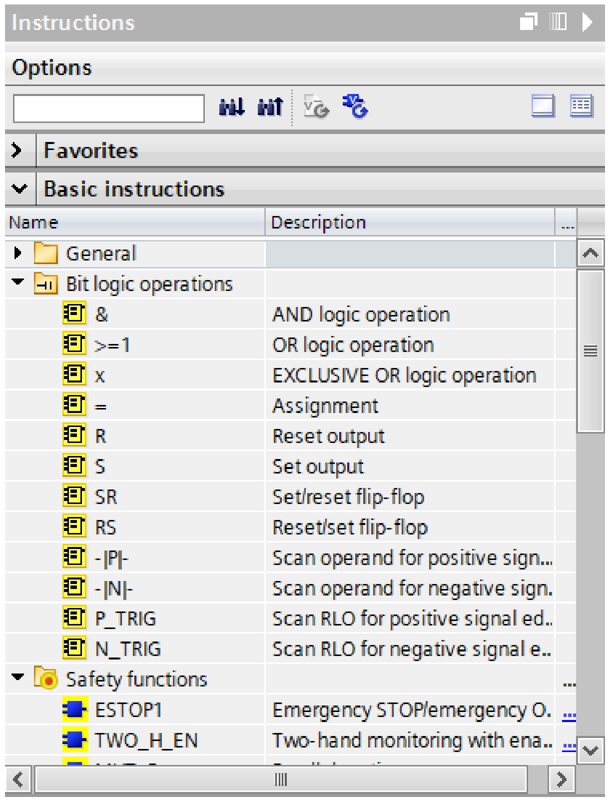


Figure 4-8 Task Card "Instructions"

In addition to the known operations, there are special safety functions, e.g. for two-hand monitoring, discrepancy analysis, muting, E STOP, protective door monitoring and feedback circuit monitoring.

Additional information

A detailed description of the instructions for the safety program provided in the Programming and Operating Manual SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126).

Alternatively, you can call up these descriptions directly in the TIA Portal by moving the tooltip over a specific instruction.

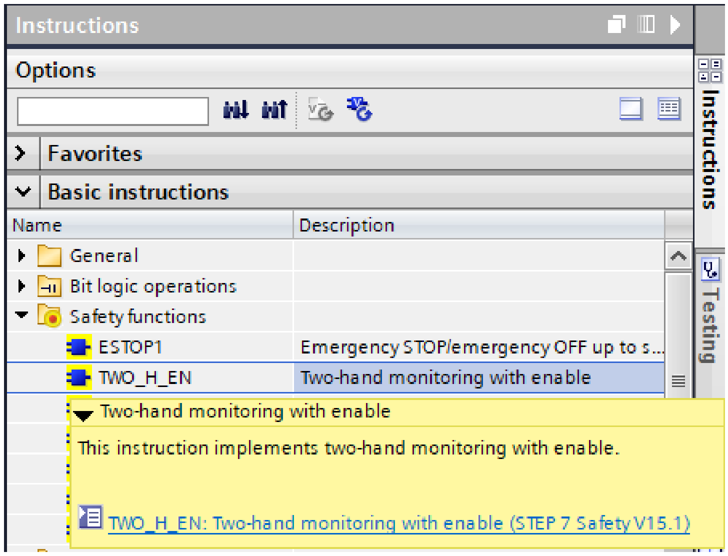


Figure 4-9 Tooltip of an instruction

4.7 F-runtime groups

4.7.1 Rules for F-Runtime Groups of the Safety Program

Rules

Note the following:

- The channels (channel values and value status) of an F-I/O can only be accessed from a single F-runtime group.
- Tags of the F-I/O DB of an F-I/O can only be accessed from one F-runtime group and only from that F-runtime group from which the channels or value status of this F-I/O are also accessed (if access is made).
- F-FBs can be used in more than one F-runtime group but they must be called with different instance DBs.
- Instance DBs of F-FB can only be accessed from the F-runtime group in which the associated F-FB is called.
- It is only permissible to access a tag of a global F-DB from an F-runtime group. However, it is permissible to use a global F-DB in several F-runtime groups.
- It is not permissible that you call the main safety block. It is automatically called by the assigned F-OB.

  Note

  F-OBs are protected by F-system know-how. The OB start information of F-OBs therefore cannot be evaluated.

- The F-OB should be created with the highest priority of all OBs.

  Note

  The cycle time/runtime of the F-OB can be extended, for instance, as a result of communication load levels, processing higher priority alarms and test and commissioning functions.

- The process image of the inputs and outputs of the standard I/O, bit memories and tags of DBs of the standard user program may be read or write accessed from several F-runtime groups.
- F-FCs can generally be called in more than one F-runtime group.

Note

You can improve performance by writing sections of the program that are not required for the safety function in the standard user program.

When determining which elements to include in the standard user program and which to include in the safety program, you should keep in mind that the standard user program can be modified and downloaded to the F-CPU more easily. In general, changes in the standard user program do not require an acceptance.

4.7.2 Procedure when defining an F-runtime group

An F-runtime group comprises a block (F-OB), which calls the main safety block (FB or FC).

Automatically creating the safety program

An F-runtime group is automatically created when you activate the "SINUMERIK Safety Integrated (F-PLC)" mode.

You can adapt this response in the menu under "Options > Settings > STEP 7 Safety".

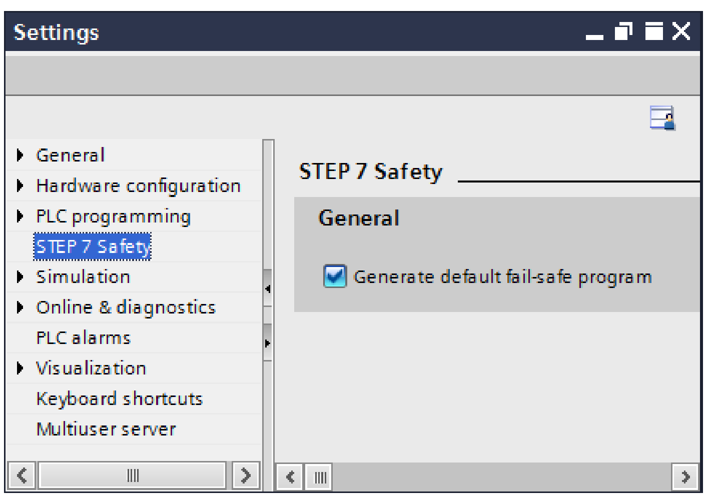


Figure 4-10 Settings for STEP 7 Safety

Archiving the F-blocks

The automatically created F-blocks of the F-runtime group are in folder "Program blocks": FOB_RTG1, Main-Safety_RTG1 and Main-Safety_RTG1_DB.

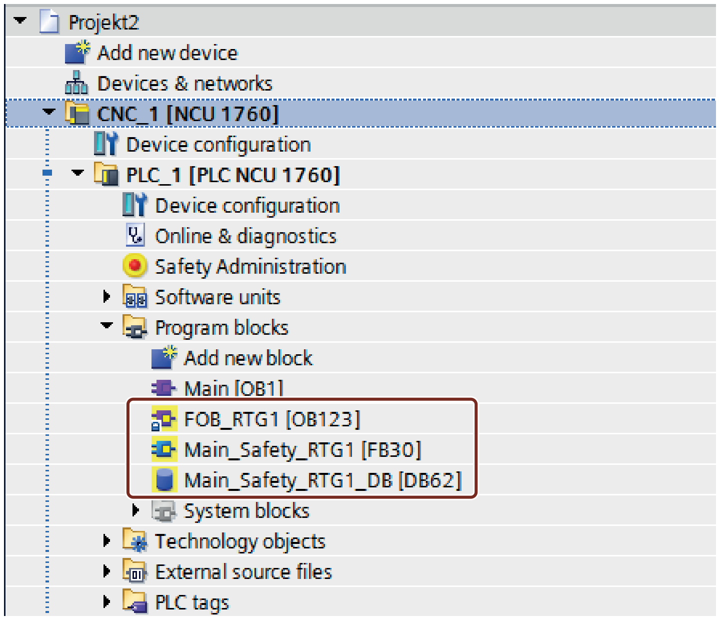


Figure 4-11 F-runtime group blocks in the project navigator

Open the "F-runtime group" work cell

If you wish to adapt the automatically created F-runtime group or configure F-runtime groups, in the Safety Administration Editor, open the "F-runtime group" work cell.

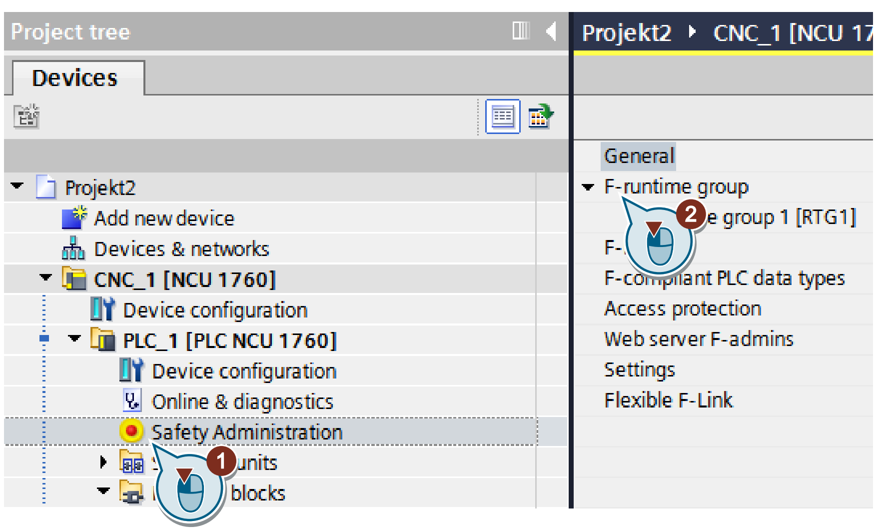


Figure 4-12 Displaying the "F-runtime group" work cell

"F-runtime group" work cell

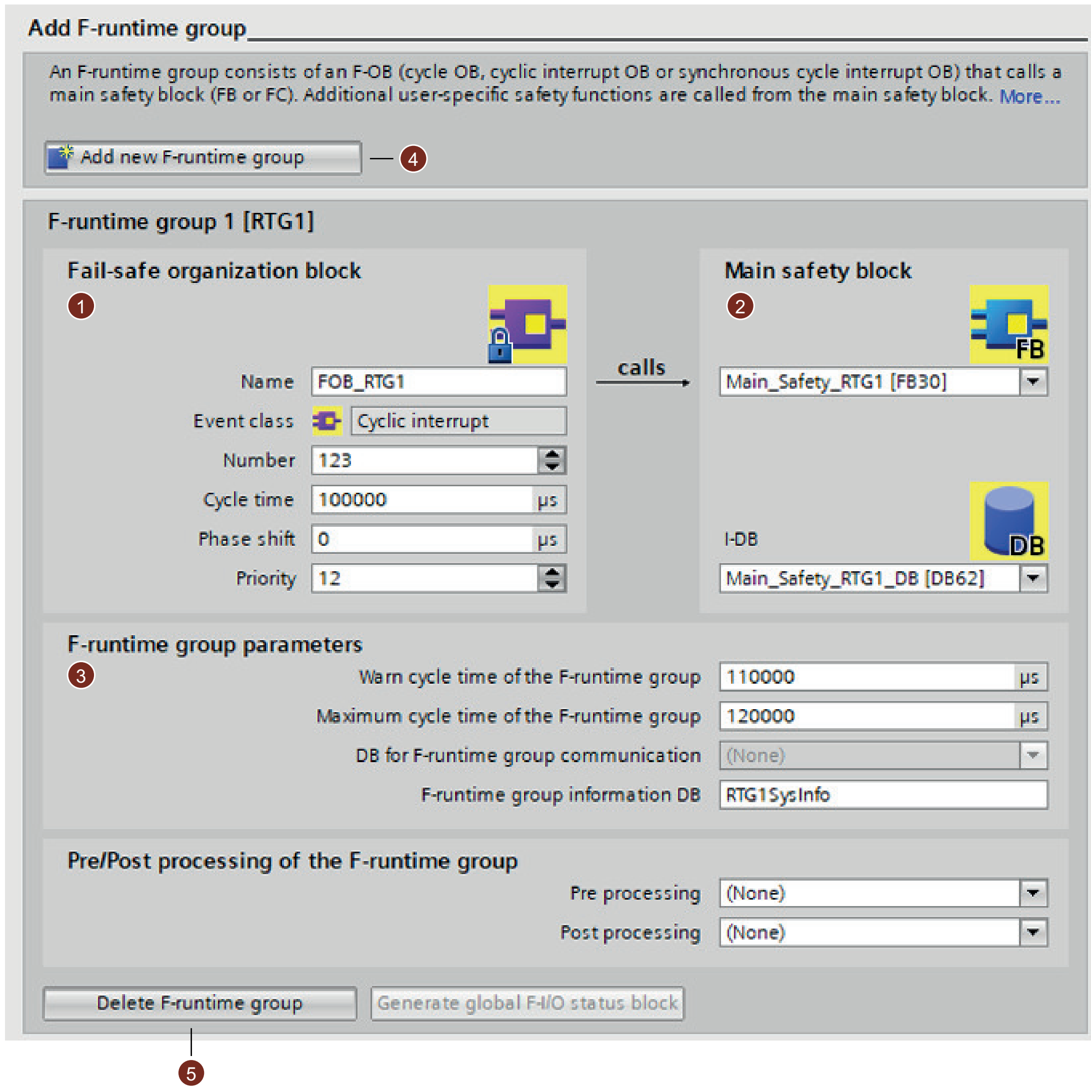


Figure 4-13 Safety Administration Editor, "F-runtime group" work cell

① Failsafe organization block (F-OB)

1. Under "F-OB" assign a name for the F-OB; the default value is "FOB_RTG1".
2. For the F-runtime group created as default, the F-OB has the event class "Cyclic interrupt". To change the event class of the F-OB of an already created F-runtime group, you must delete the F-runtime group and recreate it.

Note

We recommend that you create the F-OB with event class "Cyclic interrupt" as "Cyclic interrupt OB". As a consequence, the safety program is called at fixed time intervals.

3. If necessary, you can manually change the F-OB number that the system suggests. When doing this, observe the number ranges permissible for the particular event class.
4. For F-OBs with event class "Cyclic interrupt", parameterize cycle time, phase shift and priority.
   - Select a cycle time that is less than the "Maximum cycle time of the F-runtime group" and less than the "Warning limit cycle time of the F-runtime group".
   - Select a phase offset that is less than the cycle time.
   - If possible, select a priority that is higher than the priority of all other OBs.

   Note

   The higher F-OB priority means that you can ensure that the runtime of the safety program and the response time of your safety functions is influenced as little as possible by the standard user program.

② **Main safety block**

Assign the main safety block to be called to the F-OB. If the main safety block is an FB, then you must also assign an instance DB. As default value, Main_Safety_RTG1 and Main_Safety_RTG1_DB are suggested.

③ Runtime group parameters

1. The F-CPU monitors the F-cycle time of the F-runtime group. Two parameters are available to do this.
   – If the "Warning limit cycle time of the F-runtime group" is exceeded, then an entry is written to the diagnostics buffer of the F-CPU. You can use these parameters to define whether the cycle time can exceed a specified value without the F-CPU going into the STOP state.
   – If the "Maximum cycle time of the F-runtime group" is exceeded, then the F-CPU goes into the STOP state. For "Maximum cycle time of the F-runtime group", select the maximum time that can elapse between two calls of this F-runtime group (max. 20000000 µs).

   Note

   The call interval of the F-runtime group is monitored against a maximum value; this means it is monitored as to whether the call is performed frequently enough, but not whether too frequently or e.g. isochronously. Therefore, failsafe times must be implemented using instructions TP, TON or TOF from the task card "Instructions" and not using a counter (OB calls).

   Note

   The response time of your safety function is also dependent on the cycle time of the F-OB, the runtime of the F-runtime group - and when using distributed F-I/O - the parameterization of PROFINET/PROFIBUS. As a consequence, the configuration/parameterization of the standard system also influences the response time of your safety function.

   If you do not prevent changes being made to the configuration/parameterization of the standard system that can influence the response time by applying the appropriate organizational measures, when calculating the maximum response time of the safety function, you must always apply the monitoring times.

   You must parameterize the "Warning limit cycle time of the F-runtime group" lower or the same as the "Maximum cycle time of the F-runtime group".
2. When required, under "F-runtime group information DB", you can change the name for the F-runtime group information DB suggested by the system.

④ Creating new F-runtime groups

Using this command, you can create a second F-runtime group; for example, to organize safety-related program sections that are executed quickly, in their own dedicated F-runtime group.

⑤ Delete F-runtime group

This command deletes the assignment of the F-blocks to an F-runtime group. You may have to carry out additional steps if you wish to delete your safety program.

See also

Response time calculation (https://support.industry.siemens.com/cs/ww/en/view/93839056)

4.7.3 F-runtime group information DB

Introduction

The F-runtime group information DB provides key information on the corresponding F-runtime group and on the safety program as a whole.

The F-runtime group information DB is generated automatically when an F-runtime group is created. In so doing, a symbol is assigned for the F-runtime group information DB, e.g. "RTG1SysInfo". You have the option of changing the name in the Safety Administration Editor.

Information in the F-runtime group information DB

The F-runtime group information DB provides the following information:

Name		Data type	For processing in the safety program	For processing in the standard user program	Description
MODE		BOOL	x	x	1 = Disabled safety mode
F_SYSINFO					
	MODE	BOOL	—	x	1 = Disabled safety mode
	TCYC_CURR	DINT	—	x	Current cycle time of the F-runtime group, in ms
	TCYC_LONG	DINT	—	x	Longest cycle time of the F-runtime group, in ms
	TRTG_CURR	DINT	—	x	Current runtime of the F-runtime group, in ms
	TRTG_LONG	DINT	—	x	Longest runtime of the F-runtime group, in ms
	T1RTG_CURR	DINT	—	x	Not supported by STEP 7 Safety V16.
	T1RTG_LONG	DINT	—	x	Not supported by STEP 7 Safety V16.
	F_PROG_SIG	DWORD	—	x	Collective F-signature of the safety program
	F_PROG_DAT	DTL	—	x	Compilation date of the safety program
	F_RTG_SIG	DWORD	—	x	F-runtime groups signature
	F_RTG_DAT	DTL	—	x	Compilation date of the F-runtime group
	VERS_S7SAF	DWORD	—	x	Version identifier of STEP 7 Safety

You access the content of the F-runtime group information DB with fully qualified addressing. Either collectively with the F_SYSINFO PLC data type (UDT), for example, "RTG1SysInfo.F_SYSINFO", provided by the F-system or individual information, for example, "RTG1SysInfo.F_SYSINFO.MODE".

4.8 Creating F-blocks

Introduction

In order to create F-FBs, F-FCs, and F-DBs for the safety program, you should follow the same basic procedure as for standard blocks. In the following, only the deviations from the procedure for standard blocks are presented.

Creating F-FBs, F-FCs, and F-DBs

You create F-blocks in the same way as for standard blocks. Proceed as follows:

1. In the project tree under "Program blocks", double-click on "Add new block".
2. In the dialog that appears, specify the type, name, and language and select the "Create F-block" check box. (If you do not select the check box, a standard block is created.)
3. After confirming the dialog, the F-block is opened in the program editor.

Note the following

Note the following important instructions:

Note

- It is not permissible that you declare any block parameters in the block interface of the main safety block as they cannot be supplied.
- You can edit start values in the instance DBs.
- Function "Accept actual values" is not supported.
- It is not permissible that you access static local data in individual or multi-instances of other F-FBs.
- You must always initialize F-FC outputs.
  If you do not comply with this, then the F-CPU can go into the STOP state. The cause of the diagnostic event is entered in the F-CPU diagnostics buffer.
- A block may only have read access to its inputs and only write access to its outputs.
  Use an in/out if you wish to have both read and write access.
- For reasons of transparency, assign meaningful names to the F-blocks that you create.

Copying/pasting F-blocks

You can copy F-FBs, F-FCs, and F-DBs in exactly the same was as blocks of the standard user program.

Exception:

You cannot copy blocks from folder "Program blocks > System blocks".

Nesting depth for F-FBs and F-FCs

We recommend that you do not exceed a nesting depth of 8 levels.

4.9 Using libraries

Introduction

As with standard blocks, you have the option of storing F-blocks which you wish to reuse as master copy or types in global libraries or in the project library.

Additional information can be found in the help for STEP 7 under "Using libraries".

Reusing F-blocks which have already been tested and accepted

Please note the following when reusing F-blocks which have already been tested and if applicable also accepted:

- Document the signature and start value signature of the F-block after you have compiled, tested and possibly accepted the F-block.
- Document the version set for "Instructions (without their own version)" in the Safety Administration Editor under "Settings"/"System library elements used in safety program". For documentation purposes, you can create a safety summary of the safety program you used to create the F-block.
- When re-using the F-block, carefully ensure that the signature and start value signature of the F-block have not been changed.

For F-blocks with instructions for which a version is indicated in the "Version" column of the "Instructions" task card, you must also note the following:

- Document the versions of these instructions that were set at the time the F-block was compiled and on the basis of which the F-block was tested and, if applicable, approved. You can use the safety summary for documentation purposes.
- When using the F-block again make sure that the documented versions are set for these instructions in the "Instructions" task card.
- If versions other than the documented versions are set for these instructions, you must check yourself whether the F-block still works with these versions as intended.
  To do so, identify any differences between the versions based on the online help on the instructions.
  You need to have the F-block retested and accepted. Additional information on the instruction versions can be found in the help for STEP 7 under "Fundamentals for instruction versions".

To help you manage F-blocks that you wish to reuse and that have already been tested and if applicable accepted, we recommend that you save these blocks as types in a global library.

4.10 Integrating SUD program components in the TIA Portal

4.10.1 Structure of a SafeUserData instance

The following diagram schematically shows the interaction between all blocks of a SafeUserData instance.

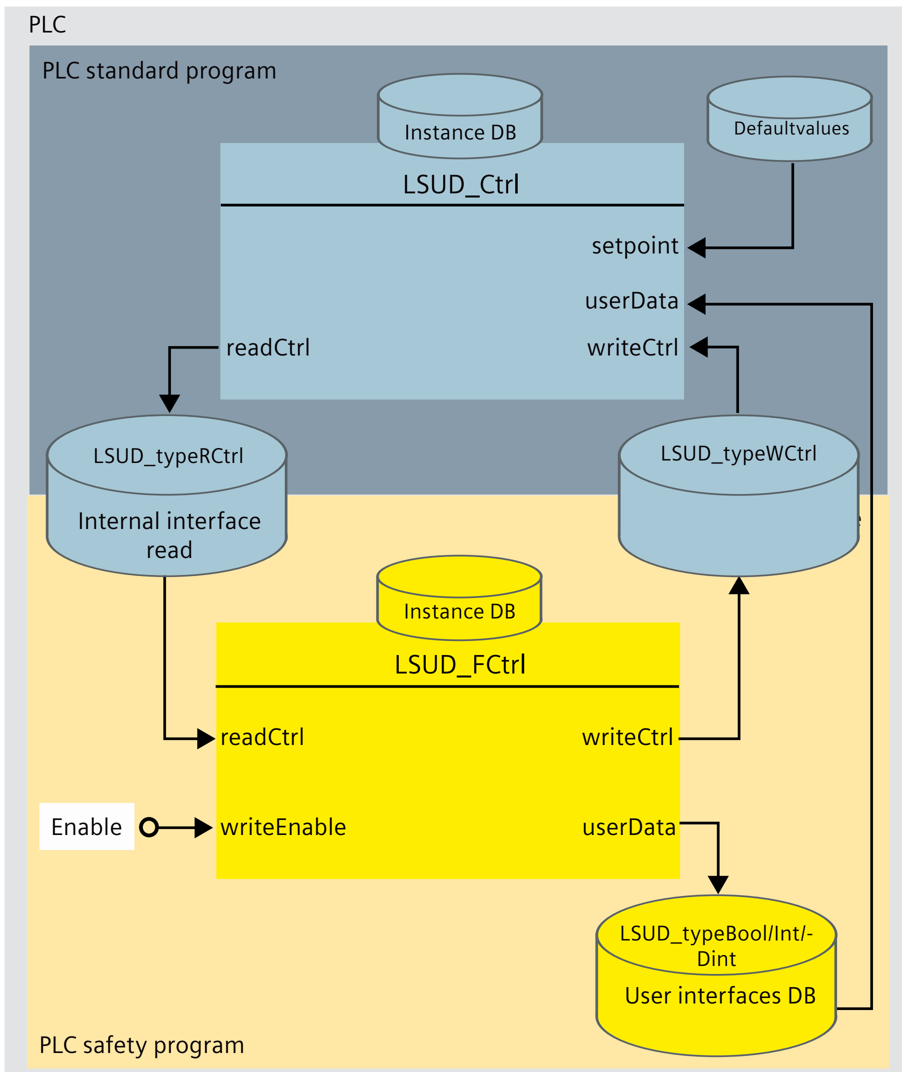


Figure 4-14 Interaction between all blocks of a SafeUserData instance.

An F-DB implements the interface to the safety program (in the diagram above: User interfaces DB).

This F-DB contains 16 net data of a data type (Bool, Int oder DInt). The number of net data is fixed.

4.10.2 Transferring SafeUserData data types and libraries into the project

To integrate SafeUserData instances in the PLC program, you must open the SUD library in the TIA Portal, and copy SUD data types and SUD library blocks into the project.

Preconditions

- As a minimum, safety system version V2.4 is set in the project.
- For SINUMERIK ONE: The Safety Integrated mode "SINUMERIK Safety Integrated (F-PLC)" was activated at the NCU in the project.

Procedure

1. Save library "SINUMERIK ONE SafeUserData Vx.y" to your file system.
2. In the TIA Portal, load library "SINUMERIK ONE SafeUserData Vx.y" as global library into your SINUMERIK project.

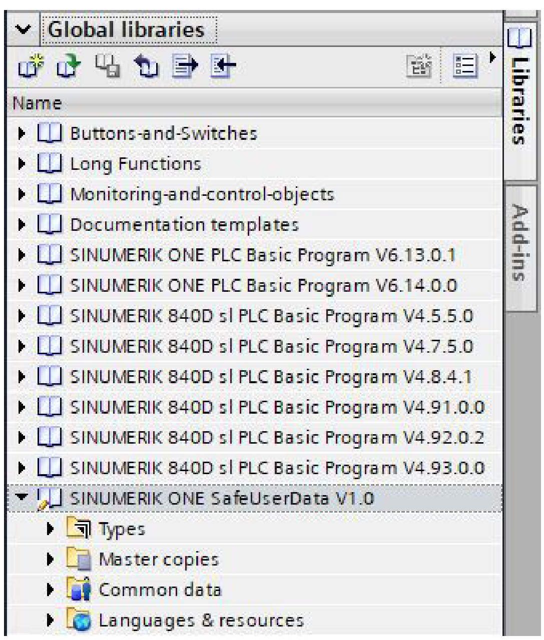


Figure 4-15 SafeUserData library opens

3. Open folder "Copy templates > SINUMERIK ONE SafeUserData" into the library.

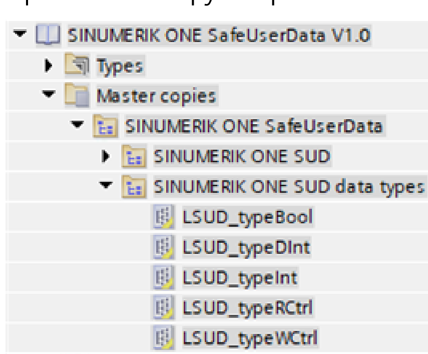


Figure 4-16 SUD data types in the library

4. Copy folder "SINUMERIK ONE SUD data types" of the library to folder "PLC data types" of the PLC.

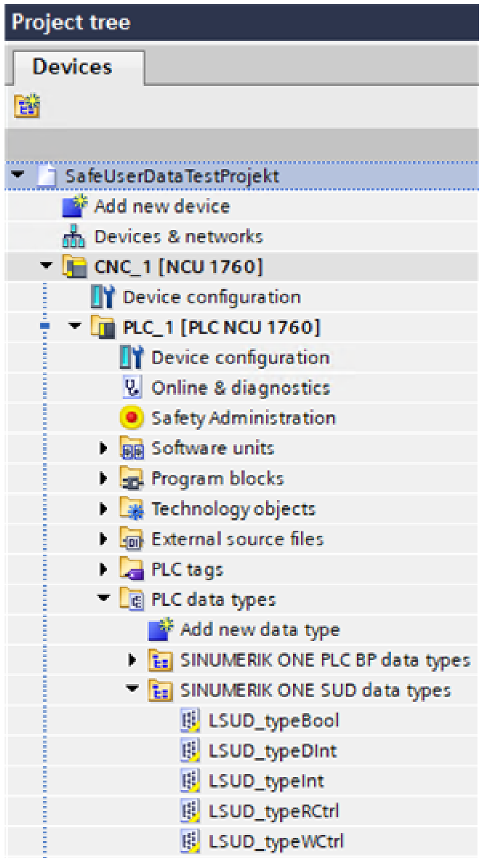


Figure 4-17 Transferring SUD data types into the PLC project tree

5. Open folder "Copy templates > SINUMERIK ONE SafeUserData" into the library.

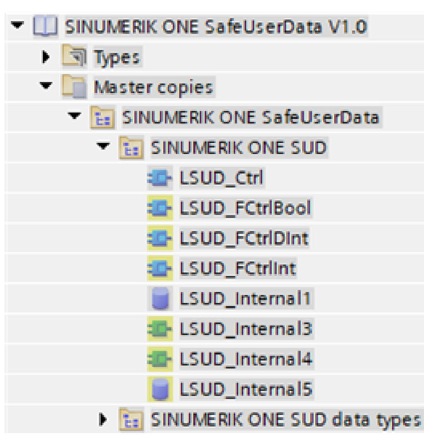


Figure 4-18 SUD library blocks

6. Copy folder "SINUMERIK ONE SUD" of the library to folder "Program blocks" or a PLC subfolder.

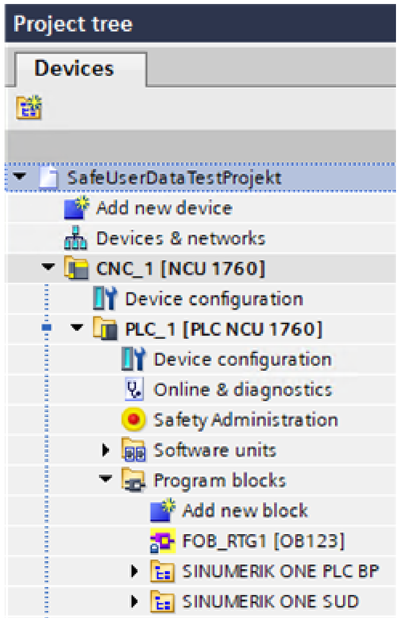


Figure 4-19 Transferring the SUD library into the PLC project tree

7. Save your SINUMERIK project in the TIA Portal.

4.10.3 Creating a SafeUserData instance

4.10.3.1 Creating SafeUserData data blocks

For a SafeUserData instance you require a:

- Failsafe user interface
- Internal user interface "readCtrl" (LSUD_typeRCtrl)
- Internal interface "writeCtrl" (LSUD_typeWCtrl)
- Optional: Default interface "setpoint"

For every SafeUserData instance/data set, create a dedicated failsafe user interfaces DB. Interfaces "readCtrl" and "writeCtrl" are required for the internal communication. This and interface "setpoint" should be created without F-attribute, and do not necessarily have to be located in their own DBs.

Precondition

- A SafeUserData data type - either provided or user-defined - is available.

See also

Creating a failsafe user interface (Page 85)

Transferring SafeUserData data types and libraries into the project (Page 82)

4.10.3.2 Creating a failsafe user interface

A defined data type is required for the user interfaces DB to be subsequently created. You can directly use the data types provided (LSUD_typeBool, LSUD_typeInt or LSUD_typeDInt). A user-defined data type must be derived from the data type provided to integrate user-specific symbols into the user interfaces DB.

Rules

Strictly comply with the procedure described and follow the subsequent rules.

- Do not delete or shift elements, not even temporarily!
- Do not sort the elements.
- Do not make any adaptations to data types and initial values.

Note

If these rules are violated, then inconsistencies in the data type result in data entries being interchanged in SINUMERIK Operate (or in the SINUMERIK ONE Commissioning Tool).

After the values have been transferred into the PLC and subsequent activation by the HMI, any interchanged data is identified and data storage is inhibited.

- In this case, restore the previous values by restarting the SINUMERIK. The problem can only be subsequently resolved by recreating the data type in the TIA Portal.

The element names in the subsequent diagram have been selected as example only:

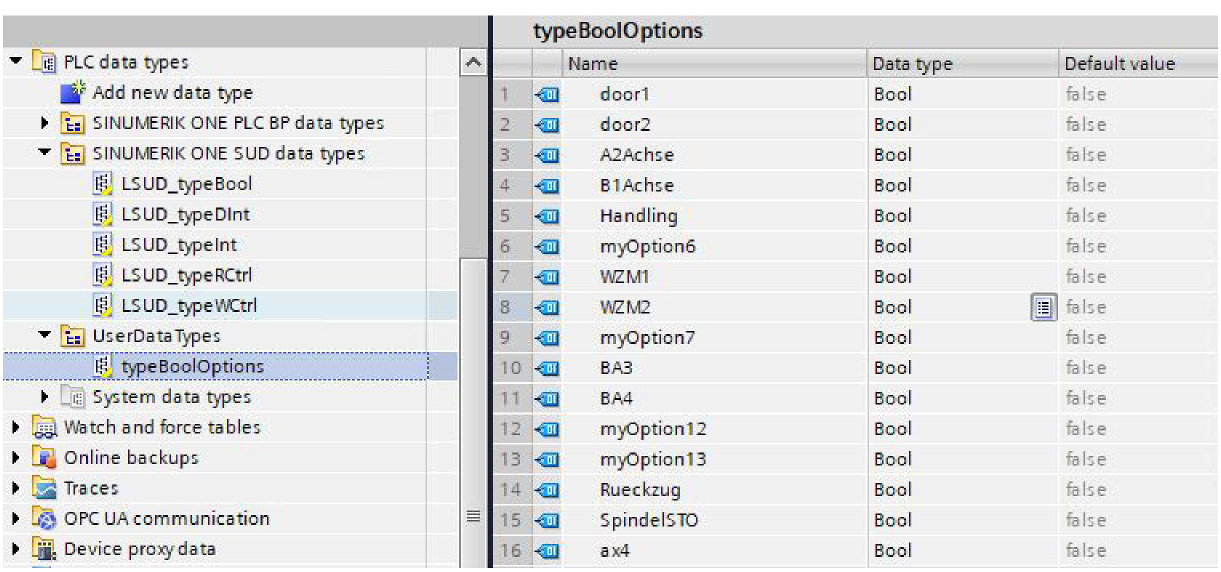


Figure 4-20 Example: SINUMERIK ONE: SafeUserData - User data type

Procedure for creating a SafeUserData data type with user symbols

1. Copy the required data type from folder "SINUMERIK ONE SUD data types" and save the data type under a dedicated name, e.g. "typeBoolOptions" in folder "PLC data types".
2. Adapt the name of the elements "data1" to "data16" to address your specific requirements.
3. Save the SUD data type that has been created and configured in the project.

Creating the user interface as DB

1. In the project tree under "Program blocks", double-click on "Add new block".
   Dialog "Add new block" opens.
2. Select "Data block" as block type and assign it a name, e.g. "sudMyOptions".
3. Under "Type", select the SafeUserData data type - either the one provided or a user-defined one (see "Procedure for creating..."), which you wish to use in this data set.
4. Under "Failsafe", select option "Create F-block".
5. Confirm your entries with "OK".
   The new SUD data blocks are inserted in the project navigation under "Program blocks".
6. For each additional instance, create an additional user interfaces DB in the same way.

Adding internal interface "readCtrl"

1. In the project tree under "Program blocks", double-click on "Add new block".
   Dialog "Add new block" opens.
2. Select "Data block" as block type and assign it a name.
3. Under "Type", select SafeUserData data type "LSUD_typeRCtrl".
4. Under "Failsafe", deactivate option "Create F-block".
5. Confirm your entries with "OK".
   The new interfaces DB is inserted in the project tree under "Program blocks".
6. For each additional instance, create an additional interface in the same way.

Adding internal interface "writeCtrl"

1. In the project tree under "Program blocks", double-click on "Add new block".
   Dialog "Add new block" opens.
2. Select "Data block" as block type and assign it a name.
3. Under "Type", select SafeUserData data type "LSUD_typeWCtrl".
4. Under "Failsafe", deactivate option "Create F-block".
5. Confirm your entries with "OK".
   The new interfaces DB is inserted in the project tree under "Program blocks".
6. For each additional instance, create an additional interface in the same way.

Optional: Adding default interface

To reduce the time required to make entries when changing data, using SINUMERIK Operate, new data can be transferred to Operate via a default interface as suggested values. The default interface should be created in the PLC as data block or as part of a data block and applied to parameter "setpoint" of FB LSUD_Ctrl.

It should be carefully noted that the default interface must have the same structure and use the same symbols as the user interface DB of the particular instance. This is best ensured by using the same type when creating the two interfaces.

The complete data set must always be transferred; no subsets can be accepted in the data set. The default can be realized using initial values in the TIA Portal or in the operational PLC by changing actual values.

1. In the project tree under "Program blocks", double-click on "Add new block".
   Dialog "Add new block" opens.
2. Select "Data block" as block type and assign it a name.
3. Select the data type that you also use for the user interfaces DB.
   Important: The tags in the data type must use the same symbols as those of the user interface.
   Under "Failsafe", deactivate option "Create F-block".
4. Confirm your entries with "OK".
   The new default interface is inserted as data block in the project tree under "Program blocks" and opened in the block editor.
5. If required, set the default values as initial values.
6. For each additional instance, create a default interface in the same way.

See also

Transferring SafeUserData data types and libraries into the project (Page 82)

4.10.3.3 Programming the call of SUD blocks

Precondition

- The SUD data blocks (Page 84) required for the SafeUserData instance are created in the project under "Program data blocks".

Programming SUD blocks in the standard program

To call the instance from the standard program, program the call of the FB "LSUD_Ctrl" in a cyclic execution level. For example, use the OB1 or use the preprocessing/postprocessing of the F-runtime group, which should use the instance.

1. Drag data block "LSUD_Ctrl" from folder "SINUMERIK ONE SUD" in folder "Program blocks " (or where relevant, a subfolder) and drop at the selected call position - and in so doing create the associated instance DB or a multi-instance.
2. Assign a suitable name to the instance DB or the multi-instance, which clearly identifies the assignment to the data set (e.g. "InstBoolMyOptionsStd").
3. As "LSUD_Ctrl" is a block that must be continually executed asynchronously, if possible, permanently interconnect input "enable" to value "true".
4. Parameterize the associated interface "writeCtrl" (e.g. "myOptionsWCtrlDb") at input "writeCtrl" of function block "LSUD_Ctrl".
5. Parameterize the associated interface "readCtrl" (e.g. "myOptionsRCtrlDb") at input "readCtrl" of function block "LSUD_Ctrl".
   This signal should depend both on a machine status that is safe for the modification (e.g. emergency stop) and on a suitable authorization mechanism. Please note: this signal may only be simultaneously active at one instance.
6. Parameterize the user interfaces DB (e.g. "sudMyOptions") associated with the instance at input "userData" of function block "LSUD_Ctrl".
7. Optional: If an interface with default values exists (e.g. "myOptionsSetpoint"), parameterize this at input "setpoint" of function block "LSUD_Ctrl" (see Creating a failsafe user interface (Page 85)).
8. Optional: Outputs "valid", "busy", "error", "status" and "diagnostics" can be used for diagnostic purposes or to control downstream processes. See Tables "LSUD_Ctrl parameters" and "LSUD_Ctrl status and diagnostics".

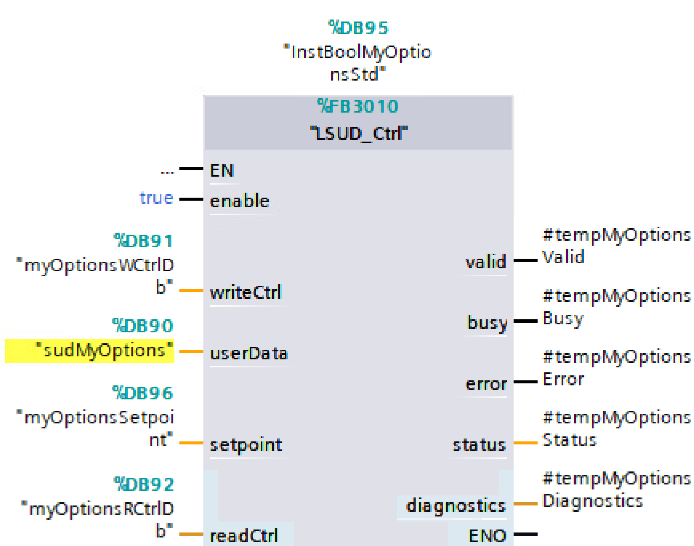


Figure 4-21 Example of calling the standard instance (LSUD_Ctrl)

Table 4-2 LSUD_Ctrl parameters

Parameter	Declaration	Data type	Description
enable	Input	BOOL	Activates the function; should be permanently assigned the value "true" because of the continuous execution.
writeCtrl	Input	LSUD_typeWCtrl	Internal interface "writeCtrl"
userData	Input	Variant	User interface
setpoint	Input	Variant	Interface for default values when entering data at the HMI
readCtrl	InOut	LSUD_typeRCtrl	Internal interface "readCtrl"
valid	Output	BOOL	Executed without errors
busy	Output	BOOL	Being executed
error	Output	BOOL	Error when executed
status	Output	WORD	Status information about the execution
diagnostics	Output	DWORD	Extended status and diagnostic information

Table 4-3 LSUD_Ctrl status and diagnostics

Status (W#16#...)	Diagnosis (W#16#...)	Explanation
7000	70000000	FB LSUD_Ctrl inactive (parameter "enable" = "false")
7001	70010000	Function called for the first time with "enable" = "true"
7001	70010001	Function called for the first time with "enable" = "true", wait for instance ID
7002	70020000	Subsequent call
7002	70020001	Subsequent call, waiting for instance ID, F cycle not yet been run
7002	70020200	Subsequent call, LSUD_FCtrl<DATA_TYPE> in initialization phase
7002	70020201	Subsequent call, waiting for LSUD_FCtrl<DATA_TYPE> instance ID in initialization phase
7002	70020A00	Subsequent call, LSUD_FCtrl<DATA_TYPE> waiting for retentive data
7002	70020B00	Subsequent call, LSUD_FCtrl<DATA_TYPE> waiting for memory identification
7002	70020C00	Subsequent call, LSUD_FCtrl<DATA_TYPE> waiting for change counter
7002	70021100	Subsequent call, LSUD_FCtrl<DATA_TYPE> operation with substitute values
7002	70021300	Subsequent call call, LSUD_FCtrl<DATA_TYPE> operation with net data
7002	70021400	Subsequent call, LSUD_FCtrl<DATA_TYPE> data change mode active
7002	70021900	Subsequent call, LSUD_FCtrl<DATA_TYPE> storing new data part 1
7002	70021C00	Subsequent call, LSUD_FCtrl<DATA_TYPE> storing new data part 2
9000	90000000	More than 32 instances/data sets were created.
9001	90010000	Multiple use of the internal interfaces (readCtrl/writeCtrl) identified
9002	90020000	Multiple use of an instance ID was identified

Status (W#16#...)	Diagnosis (W#16#...)	Explanation
9003	90030000	Error when preparing the diverse memory archive
9004	900400xx	Error, net data type not identified (xx=incorrect data type code)
9005	90050000	Library block comparison error
9010	9010xxxx	Error when reading the system identifier (xxxx=fine code of the subordinate system function)
9011	9011xxyy	Error when converting the system identifier (xx=incorrect code, yy=position of the code)
9100	9100xxxx	Error when reading from the diverse memory archive (xxxx=fine code of the subordinate system function)
9200	9200xxxx	Error when writing to the diverse memory archive (xxxx=fine code of the subordinate system function)
9300	9300xxxx	Error when preparing/processing data from the diverse memory archive (xxxx=fine code of the subordinate system function)
9400	9400xxxx	Error when preparing/processing data for the diverse memory archive (xxxx=fine code of the subordinate system function)

Configuring the call in the F-program

To call the failsafe instance in the safety program, program the call of the FB "LSUD_FCtrl<DATA_TYPE>" that corresponds to the data type (i.e. for <Bool>, for <Int> and for <DInt>). The call must be made in the runtime group that SafeUserData should use. It is recommended that the call is made at the start of the runtime group. The following example refers to data type <Bool>. Proceed in the same way for data types <Int> and <DInt>.

1. Drag FB "LSUD_FCtrlBool" from folder "SINUMERIK ONE SUD" in folder "Program blocks " (or where relevant, a subfolder) and drop at the selected call position - and in so doing create the associated instance DB or a multi-instance.
   Assign a suitable name to the instance DB or the multi-instance, which clearly identifies the assignment to the data set (e.g. "InstBoolMyOptionsF").
2. Parameterize the associated interface "readCtrl" (e.g. "myOptionsRCtrlDb") at input "readCtrl" of function block "LSUD_FCtrl".
3. Parameterize the associated interface "writeCtrl" (e.g. "myOptionsWCtrlDb") at input "writeCtrl" of function block "LSUD_Ctrl".
4. Parameterize the user interfaces DB (e.g. "sudMyOptions") associated with the instance at input "userData" of function block "LSUD_FCtrl".
5. At input "writeEnable" parameterize a safety-related signal that enables the modification. This signal should depend both on a machine status that is safe for the modification (e.g. emergency stop) and on a suitable authorization mechanism. Carefully observe that this signal may only be simultaneously active at one instance.
6. At input "instanceID", for every data set, parameterize a dedicated, unique numerical value > 0 to internally identify the data set.
7. Optional: You can use outputs "valid" and "error" for diagnostic purposes or to control downstream processes. See also table "LSUD_FCtrl parameters".
8. Optional: You can use output "signature" to identify active net data.

⚠ WARNING

Avoiding an unsafe status of the machine when changing SafeUserData

Safety functions can be modified or deactivated by changing SafeUserData. An incorrect parameterization can mean that safety functions are not executed as expected. This can also result in personal injury. An incorrect parameterization can mean that incorrect values are assigned and/or values are assigned to an incorrect parameter.

- As OEM, ensure that the machine is in a safe state that permits a change to SafeUserData. Only under this precondition is activation permissible using the safety-related "writeEnable" enable signal.
- Only activate the safety-related "writeEnable" enable signal simultaneously for one instance to prevent data from being changed in another instance.
- Immediately after being changed, carefully check the entered and active values to ensure that they are correct, and perform a function or acceptance test for all of the safety functions that were influenced.

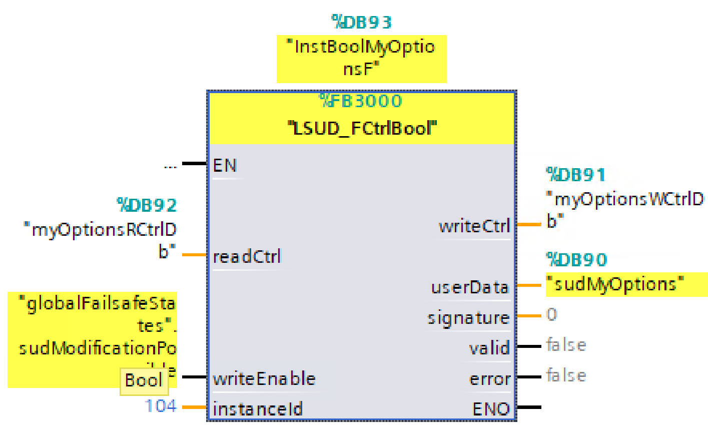


Figure 4-22 Example of calling the failsafe instance (LSUD_FCtrlBool)

Table 4-4 LSUD_FCtrl parameters

Parameter	Declaration	Data type	Description
readCtrl	Input	LSUD_typeRCtrl	Internal interface "readCtrl"
writeEnable	Input	BOOL	Safety-related enable signal (machine state for modification is safe and authorized)
instanceID	Input	INT	Identification of the data set, numerical value > 0, must be different for each instance.
writeCtrl	Output	LSUD_typeWCtrl	Internal interface "writeCtrl"
userData	Output	LSUD_type<DA-TA_TYPE>	User interface, type <BOOL/INT/DINT>
signature	Output	DINT	Net data signature to identify the active SafeUserData

Parameter	Declaration	Data type	Description
valid	Output	BOOL	Initialization phase completed
error	Output	BOOL	Error when executing, at the same time, SafeUserData is output with the value 0 or false.

4.11 Safety-relevant communication

Introduction

Here, you can obtain an overview of the possibilities of safety-related communication in SIMATIC Safety F-systems.

Options for safety-related communication

Safety-related communication	On subnet	Additional hardware required
Safety-related CPU-CPU communication:		
IO controller-IO controller communication	PROFINET IO	PN/PN coupler
Master-master communication	PROFIBUS DP	DP/DP coupler
IO controller-I-device communication	PROFINET IO	—
Master-I-slave communication	PROFIBUS DP	—
IO controller-I-slave communication	PROFINET IO and PROFIBUS DP	IE/PB link
IO-controller-IO-controller communication for *S7 Distributed Safety*	PROFINET IO	PN/PN coupler
Master-master communication for *S7 Distributed Safety*	PROFIBUS DP	DP/DP coupler

Note

Flexible F-Link

From STEP 7 Safety V15.1, a new failsafe CPU-CPU communication "Flexible F-Link" is available for the F-CPU S7-1500.

More information

More detailed information is provided in the "SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126)" Manual.

4.12 Access to SI-drives and F-I/O

Overview

A description is subsequently provided as to how you can address F-I/O and safety-related drive telegrams in the safety program - and which rules you must observe.

Addressing via the process image

You address F-I/O and safety-related drive telegrams just the same as for standard I/O using the process image (PAE and PAA).

Directly reading (with I/O access identifier ":P") inputs or writing to outputs is not possible in the safety program.

Updating the process image

The process image of inputs of the F-I/O and safety-related drive telegrams is updated at the start of the F-runtime group. The process image of outputs of the F-I/O and safety-related drive telegrams is updated at the end of the F-runtime group (see Program structure of the safety program (Page 53)).

The communication between the F-CPU (process image) and the F-I/O required to update the process image is realized using a special safety protocol according to PROFIsafe.

.

Rules

- It is only permissible that you address a channel (channel value and value status) of an F-I/O or a drive telegram in an F-runtime group. You define the assigned F-runtime group with the first programmed addressing.
- It is only permissible that you address a channel (channel value and value status) of an F-I/O or a drive telegram with the unit, which corresponds to the data type of the channel.
  Example: It is only permissible that you access input channels, data type BOOL using unit "Input (bit)" (Ix.y). It is not possible to access 16 consecutive input channels, data type BOOL using unit "Input word " (IWx).
- Only address inputs and outputs that reference a real existing channel (channel value and value status) - (e.g. for an F-DO 10xDC24V with start address 10, only outputs Q10.0 to Q11.1 for the channel values, and inputs I10.0 to I11.1 for the value status). Also note that as a result of the special safety protocol, the F-I/O and/or drive telegrams occupy a larger area in the process image than is required for the real channels (channel values and value status) on the F-I/O and/or the drive telegram.
  Refer to the appropriate manuals for the F-I/O and/or the drive telegram regarding the area of the process image in which the channels (channel values and value status) are saved (channel structure). See also Sections Telegram structure and data (Page 395) and Process data (Page 398).

- Channels can be deactivated for certain F-I/O (e.g. failsafe modules ET 200SP or failsafe modules S7-1500/ET 200MP). Only address channels (channel value and value status) that are activated in the hardware configuration. If you address channels, which are deactivated in the hardware configuration, then when compiling the safety program, an alarm is output.
- For certain F-I/O (e.g. failsafe modules ET 200SP or failsafe modules S7-1500/ET 200MP), a "1oo2 (2v2) evaluation of the encoder" can be set. In so doing, two channels are grouped together to create a channel pair, and the result of the "1oo2 (2v2) evaluation of the encoder" is generally made available under the address of the channel with the lower channel number (see the corresponding manuals for the F-I/O). Only address this channel (channel value and value status) of the channel pair. If you address the other channel, then an alarm is output when compiling the safety program.

Additional information

Additional information is provided in the help for SIMATIC STEP 7 Safety Advanced in the following chapters:

- Data transfer from the safety to the standard user program
  (Information on updating the process image)
- Safety-relevant I-slave-slave communication - F-I/O access

Also observe the documentation on the relevant F-I/O - as well as on the safety-relevant drive telegrams.

4.13 Programming startup protection

Introduction

Initiating a STOP state, e.g. using PG/PC operator action, mode switch, communication function or "STP" instruction - as well as maintaining a STOP state - are not safety relevant. This STOP state can be very simply (also inadvertently) withdrawn, e.g. with an appropriate operator action at the PG/PC.

When an F-CPU is switched from STOP to RUN mode, the standard user program starts up in the usual way. When the safety program is started up, all F-DBs are initialized with the values from the load memory - as is the case with a cold restart. This means that saved error information is lost. The F-system automatically reintegrates the F-I/O. If your process does not allow such a startup, you must program a restart/startup protection in the safety program: The output of process data must be blocked until manually enabled. It is only permissible to issue the enable after process values can be output without incurring any risk, and faults have been removed.

Example of restart/startup prevention

In order to implement a restart/startup prevention, it must be possible to detect a startup. To detect a startup, in an F-DB declare a variable, data type BOOL with start value "TRUE".

Block the output of the process values if this variable has the value "1", e.g. by passivating F-I/O using variable PRESS_ON in the F-I/O DB.

To manually enable the output of process data, you reset this tag by means of a user acknowledgment.

Additional information

Additional information is provided in the help for SIMATIC STEP 7 Safety Advanced in the following chapters:

- F-I/O DB
- Implementing a user acknowledgment

4.14 Implementing a user acknowledgment

Send data must be reintegrated after communication, channel and F-I/O faults.

The existing operations provide the following options:

- Parameter "ACK_REI":
  Special acknowledgment for the reintegration for each F-I/O
- Safety function "ACK_GL":
  Acknowledgment to simultaneously reintegrate all F-I/O of an F-runtime group

In your safety program, you must always provide the possibility of acknowledging the reintegration of F-I/O. You can implement the user acknowledgment as follows:

- User acknowledgment using an operating control and monitoring system
- User acknowledgment using an acknowledgment button at one of the F-I/O
  - Assigning the inputs to the F-CPU of the I-Slaves/I-Devices
  - Assigning the inputs to the F-CPU of the DP master / I/O controller

Additional information

- Implementing user acknowledgment for global reintegration (Page 256)
- You can find additional information and examples in the help for SIMATIC STEP 7 Safety Advanced under keywords "ACK_REI", "ACK_GL" as well as in Chapter "Implementing a user acknowledgment".

4.15 Data exchange between the standard user program and safety program

You have the option of transferring data between the safety program and the standard user program. Tags can be transferred using DBs, F-DBs and bit memory:

	From the standard user program		From the safety program	
	Read access	**Write access**	**Read access**	**Write access**
Tag from DB	Permitted	Permitted	A tag from the DB can be read-accessed *or* write-accessed	
Tag from F-DB	Permitted	**Not permitted**	Permitted	Permitted
Bit memory	Permitted	Permitted	Bit memory can be read-accessed *or* write-accessed	

You can also access the process image of the standard I/O and F-I/O:

		From the standard user program		From the safety program	
		Read access	**Write access**	**Read access**	**Write access**
Process image standard I/O	PII	Permitted	Permitted	Permitted	**Not permitted**
	PIQ	Permitted	Permitted	**Not permitted**	Permitted
Process image F-I/O	PII	Permitted	**Not permitted**	Permitted	**Not permitted**
	PIQ	Permitted	**Not permitted**	**Not permitted**	Permitted

Decoupling of the safety program from the standard program in case of data transfer

We recommend that you define special data blocks (transfer data blocks) for exchanging data between the standard user program and safety program, in which data to be exchanged is stored. This measure means that you have decoupled blocks from the standard user program from those of the safety program. As long as these data blocks are not changed, changes in the standard user program do not impact the safety program (and vice versa).

4.15.1 Data transfer from the safety program to the standard user program

Overview

The standard user program can read out all data of the safety program, e.g. using symbolic (fully qualified) access operations to:

- The instance DBs of the F-FBs ("Name of instance DB".Signal_x)
- F-DBs (for example "Name of F_DB".Signal_1)
- The process image of the inputs and process image of the outputs of F-I/O (for example "Emergency_Stop_Button_1" (I 5.0))

Note

Valid for F-CPUs S7-1200/1500

The process image of the inputs of the F-I/O is updated before processing the main safety block.

Further, you have the option of directly writing safety program data to the standard user program (see also table of the supported operand areas in: Restrictions in the programming languages FBD/LAD (Page 61)):

Data block/bit memory

In the safety program, you can write to data blocks of the standard user program in order that the safety program data can be directly written to the standard user program (e.g. output DIAG of instruction SENDDP). However, a written tag must not be read in the safety program itself.

You can also write to bit memory in the safety program. However, written bit memory must not be read in the safety program itself.

Process image of the outputs

You can write to the process image of the outputs (PIQ) of standard I/O in the safety program, for example for display purposes. The PIQ must not be read in the safety program.

4.15.2 Data transfer from standard user program to the safety program

Overview

It is only permissible that fail-safe data or fail-safe signals from the F-I/O and other safety programs (in other F-CPUs) are processed in the safety program, as all variables from the standard program are not secured.

If you have to process tags from a standard user program in the safety program, then you can either evaluate bit memories from the standard user program, tags from a standard DB or the process image of the inputs (PII) from the standard I/O in the safety program (see also the table of the supported operand areas in: Restrictions in the programming languages FBD/LAD (Page 61)).

However, note that structural changes to standard DBs, which are used in the safety program, can result in inconsistencies of the safety program so that the password is possibly queried as a consequence. In this case, the F-collective signature after compilation corresponds to the original one. To avoid this effect, use "Coupling data blocks" between the standard user program and the safety program.

> ⚠ **WARNING**
>
> **Unexpected machine motion when using non-failsafe data**
>
> Bit memories from the standard user program, variables of a standard DB or the process image of inputs (PAE) of the standard I/O are not failsafe data. Hazardous states can occur in the machine if you evaluate non-failsafe data in the safety program. This can put people in dangerous situations or cause material damage.
>
> - Check the standard data in the safety program for plausibility.
> - If you use standard data in both F-runtime groups, then separately check the plausibility in both F-runtime groups.

To make checking easier, when printing out the safety program, all PLC variables from the standard user program, which are evaluated in the safety program, are printed out.

Bit memory

In order to process tags of the standard user program in the safety program, you can also read bit memory in the safety program. However, read bit memory must not be written in the safety program itself.

Data block

In order to process tags of the standard user program in the safety program, you can read tags from data blocks of the standard user program in the safety program. However, a read tag must not be written in the safety program itself.

Note

It is not possible to access static local data in single/multi-instances of the FBs of the standard user program.

Process image of the inputs

You can read the process image of the inputs (PII) of standard I/O in the safety program. The PII must not be written in the safety program.

Examples: Programming validity checks

- Check non-safety relevant tags from the standard user program using operations to compare whether a permissible upper/lower limit is violated (exceeded/fallen below). You can then influence your safety function with the result of the comparison.
- With non-safe variables from the standard user program, e.g. using instructions "S: set output", "R: reset output" or "SR: set/reset flip-flop" only allow the motor to be switched off, but do NOT allow it to be switched on.
- For switch-on sequences, use the AND logic operation instruction, for example, to logically combine unsafe tags from the standard user program with switch-on conditions that you derive from failsafe tags.

If you want to process standard tags in the safety program, please bear in mind that there is not a sufficiently simple method of checking validity for all unsafe tags.

Reading tags from the standard user program that can change during the runtime of an F-runtime group

If, in the safety program, you wish to read variables from the standard user program (bit memories, variables of a standard DB or PII of the standard I/O), which - during the runtime of the F-runtime group in which they are being read - can be changed by the standard user program or an HMI system – for example, because your standard user program is processed by a higher priority cyclic interrupt – then you must use separate bit memories or variables of a standard DB.

You must create the standard DB with the same priority as the F-OB. You must call the standard OB with a phase offset with respect to the F-OB, and write to the variables in this.

We recommend that you select the phase offset so that the standard OB is processed immediately before the F-OB.

You are then permitted to access only this bit memory or these tags of a standard DB in the safety program.

Also note that the **clock memory**, which you defined under tab "Properties" when configuring the F-CPU, can change during the runtime of the F-runtime group. This is because the clock memory runs asynchronously to the F-CPU cycle.

Note

If this is not complied with, then the F-PLC can go into STOP. The cause of the diagnostic result is entered in the diagnostics buffer of the F-PLC.

Safety functions integrated in the drive 5

This chapter provides the following information on the individual safety functions integrated in the drive:

- Basic principle of operation
- Example of how they are used
- Details and parameterization required, for example when commissioning using the parameter list/parameter view.

A shorter description on how to commission the safety functions using SINUMERIK Operate screen forms is available at Configuring safety functions integrated in the drive (Page 299).

Note

Difference between Basic Functions and Extended Functions

Basic Functions are designated as such in the chapter headings. Chapters that are not designated as Basic Functions, refer to Extended Functions.

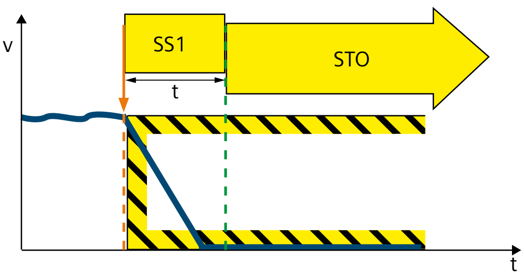
Note

Term "Control Unit" in this documentation

In the Safety Integrated environment and in this documentation the term "Control Unit" designates the SINUMERIK NCU.

5.1 SS1 Basic:

Definition according to EN 61800-5-2:
"The SS1 function brakes the motor and initiates the STO function after a delay time."



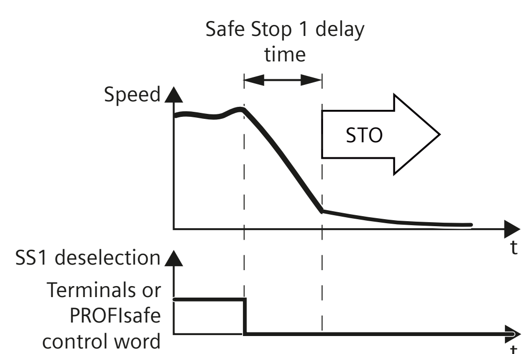
Example of how the function can be used

Example	Possible solution
A central Emergency Stop button ensures that several drives are braked as quickly as possible and brought into the STO state.	• Evaluating an Emergency Stop pushbutton in an F-PLC • Select SS1 via PROFIsafe.

How does SS1 function in detail?

Overview

The drive decelerates once "Safe Stop 1" has been selected, and goes into the "Safe Torque Off" (STO) state once the delay time has expired.



Select SS1

As soon as the converter identifies that SS1 has been selected via a terminal or via PROFIsafe safe communication, the following happens:

- If, when selecting SS1, the motor is already switched off, then until the SS1 delay time expires, there is no response. STO becomes active after the time expires.
- If the motor is switched on when SS1 is selected, the converter brakes the motor with the OFF3 ramp-down time. STO is automatically initiated after the delay time has expired.

5.1.1 Details and parameterization

5.1.1.1 SS1 with OFF3

The "Safe Stop 1" (SS1) function allows the drive to be stopped in accordance with EN 60204-1, Stop Category 1. The drive decelerates with the OFF3 ramp (p1135) once "Safe Stop 1" is selected and switches to "Safe Torque Off" once the delay time set in p9652 has elapsed.

Note

Selection via terminals

The selection of the "Safe Stop 1" (time-controlled) function via terminals is parameterized by setting a delay > 0 in p9652. In this case, the STO function can no longer be selected directly via terminals, i.e. either STO or SS1 can be selected via terminals.

If the "Safe Stop 1" (time-controlled) function has been selected by parameterizing a delay time in p9652, STO can no longer be selected directly via terminals.

Functional features of Safe Stop 1

SS1 is enabled by p9652 (delay time) ≠ 0.

- Setting parameter p9652 has the following effect:
  - p9652 = 0
    SS1 is not enabled. Only STO can be selected via the onboard terminals and PROFIsafe.
  - p9652 > 0
    SS1 is enabled. Only SS1 can be selected via the onboard terminals; with PROFIsafe, a selection of SS1 and STO is possible.
- When SS1 is selected, the drive is braked along the OFF3 ramp (p1135) and STO/SBC is automatically initiated after the delay time has expired (p9652).
  After the function has been selected, the delay timer runs down - even if the function is deselected during this time. In this case, after the delay time has expired, the STO/SBC function is selected and then again deselected immediately.

Note

Setting the delay time

So that the drive is able to travel down the OFF3 ramp completely and any motor holding brake present can be applied, before the pulses have been safely deleted, the delay time should be set as follows:

- Motor holding brake parameterized: Delay time p9652 ≥ p1135 + p1228 + p1217
- Motor holding brake not parameterized: Delay time p9652 ≥ p1135 + p1228
- The setting of parameter p1135 must be oriented towards the actual braking capability of the drive.

- The timer (p9652) after whose expiration STO is activated, is implemented with two channels, although deceleration along the OFF3 ramp is only one channel.
- Effect on "Setpoint speed limit effective" (r9733[0...2]):
  For SS1 (≙ STOP B), setpoint 0 is specified in r9733[0...2].

Requirement

- The Basic Functions are enabled via terminals and/or PROFIsafe:
  - p9601 = 1, 8 or 9 (hex).
- In order that the drive can brake down to a standstill even when selected through one channel, the time in p9652 must be shorter than the sum of the parameters for the crosswise data comparison (p9650 and p9658). Otherwise the drive will coast down after the time p9650 + p9658 has elapsed.

Status of Safe Stop 1

You can check the status in the SI diagnostics screens via "MENU SELECT > Diagnostics > Menu forward key > Safety".

5.1.1.2 SS1 with external stop (SS1E)

In drive line-ups (e.g. drives that are mechanically connected via the material), the drive-independent braking on the respective OFF3 ramp can cause problems. If the SS1E function is used, the safe delay time (p9652) is started when the function is selected, but no OFF3 is triggered. The higher-level controller still enters the setpoint.

Note

The function is configurable - however, the braking behavior using SS1E is not supported by the NC (path stop).

⚠ WARNING

Axis motion that is not monitored

During the unmonitored delay time, for "Safe Stop 1 (time-controlled) with external stop", axis motion is possible that is not monitored. This motion can result in death or severe injury.

- If there is a hazard due to undesirable motion in your application, take measures to counter it, for example, by using a brake with safe monitoring. For additional information, see Chapter "SBC (Basic/Extended) (Page 121)".

Differences between "SS1 with OFF3" and "SS1 with external stop"

"SS1 with OFF3" and "SS1 with external stop" have the following differences:

- In order to activate "Safe Stop 1 with external stop", **additionally** set p9653 to 1.
- When SS1E is selected, the drive is **not** braked along the OFF3 ramp, but after the delay time has expired (p9652), only STO/SBC is automatically initiated.

5.1.1.3 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2810 SI Basic Functions - STO (Safe Torque Off), SS1 (Safe Stop 1)
- 2811 SI Basic Functions - STO (Safe Torque Off), safe pulse cancellation

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p1135[0...n] OFF3 ramp-down time
- p1217 Motor holding brake closing time
- p1228 Pulse cancellation delay time
- p9601 SI enable functions integrated in the drive (Control Unit)
- p9652 SI Safe Stop 1 delay time (Control Unit)
- r9772.0...23 CO/BO: SI Status (Control Unit)
- r9773.0...23 CO/BO: SI Status (Control Unit + Motor Module)
- r9774.0...23 CO/BO: SI Status (group STO)

Only for "Safe Stop 1 (time-controlled) with external stop"

- p9653 SI Safe Stop 1 drive-based braking response

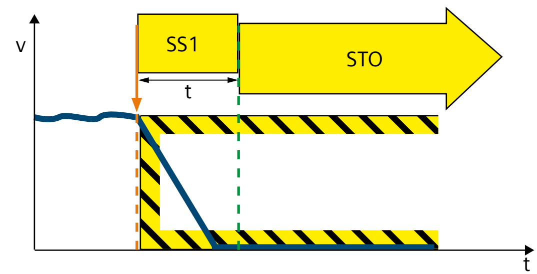
5.2 SS1

Definition according to EN 61800-5-2:

The "SS1" function causes the motor to brake (this function is integrated in the drive) and initiates the "Safe Torque Off" (STO) function after a predefined time interval has elapsed. The following variants are possible:

- SS1-a with acceleration monitoring (SAM)
- SS1-r with braking ramp monitoring (SBR)
- Manually set delay time until STO is activated.

This function corresponds to stop category 1 to EN 60204-1.



Example of how the function can be used

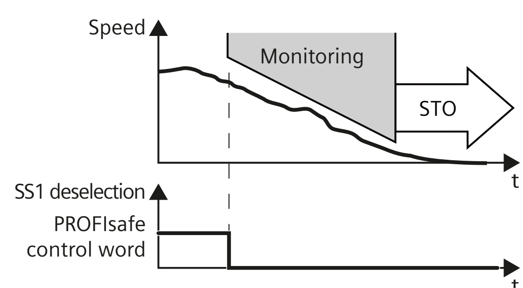
Example	Possible solution
A central Emergency Stop button ensures that several drives are braked as quickly as possible and brought into the STO state.	• Evaluating an Emergency Stop pushbutton in an F-PLC • Select SS1 via PROFIsafe. • SS1 brakes the drives and then brings them into the STO state.

How does SS1 function in detail?

Overview

Using the SS1 function, the converter brakes the motor and monitors the absolute speed.

If the motor speed is low enough or the delay time has expired, the converter safely switches off the motor torque using STO.



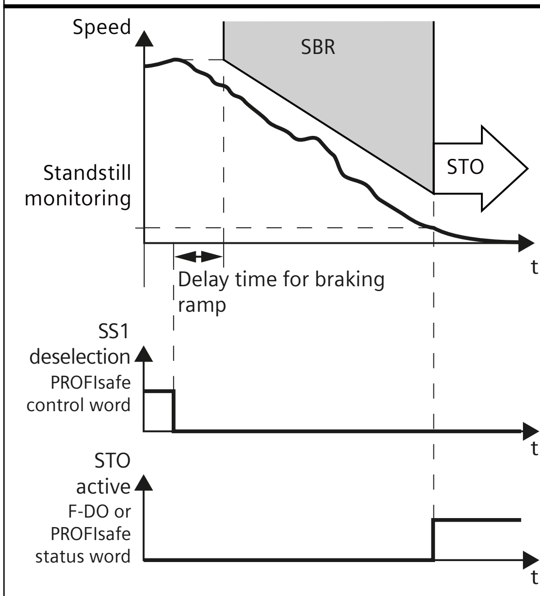
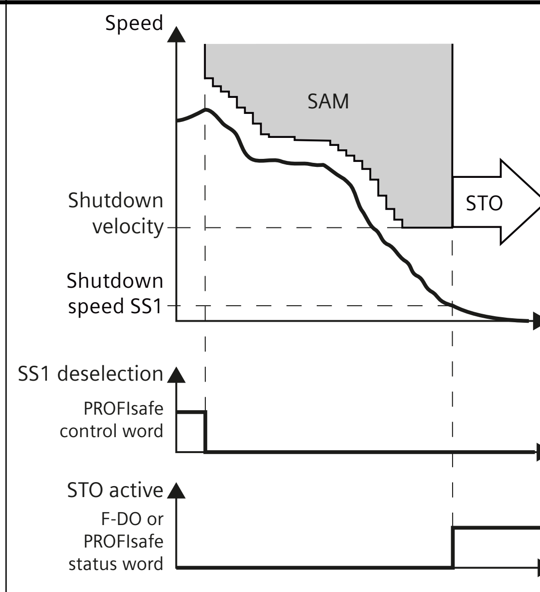
Select SS1

As soon as the converter identifies that SS1 has been selected via the PROFIsafe safe communication, the following happens:

- If the motor has already been switched off when selecting SS1 then the converter safely switches off the motor torque (STO).
- If the motor is switched on when SS1 is selected, the converter brakes the motor with the AUS3 ramp-down time.

Monitoring modes

- For the Extended Functions with or without encoder, you can choose between 2 different monitoring modes of the function SS1:
  - Safe Brake Ramp (SBR)
  - Safe Acceleration Monitor (SAM)

<table>
<tr><th>Brake ramp monitoring
(with or without encoder)</th><th>Acceleration monitoring
(with or without encoder)</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>
Using the SBR (Safe Brake Ramp) function, the converter monitors whether the motor speed decreases.
The gradient of the SBR function can be set via the reference velocity and the ramp-down time. The SBR function only starts after the "Delay for braking ramp".
The SBR function starts with the speed setpoint, which was present at the instant in time that SS1 was selected.
If the converter detects that the speed has fallen below the speed threshold (standstill monitoring), it safely switches off the motor torque (STO).
</td><td>
The converter monitors the speed of the motor with the SAM function.
The converter prevents the motor from accelerating again by having the monitoring function continuously track the speed as it decreases.
The converter reduces the monitoring threshold until the "Shutdown speed" has been reached.
The converter safely switches off the motor torque (STO), if one of the following conditions is fulfilled:

The speed has fallen below the shutdown speed SS1.
The maximum time until the torque is switched off has expired.

</td></tr>
</table>

Note

SS1 with external stop (SS1E)

If you use "SS1 with external stop", neither of the two monitoring functions (SBR, SAM) is active. For SS1E, the drive must be stopped within the delay time, for example via the PLC program. STO becomes active after the delay time expires.

5.2.1 Details and parameterization

5.2.1.1 Safe Stop 1 (SS1, time and acceleration controlled)

For function SS1 of the Extended Safety Functions, braking monitoring is included.

- **For p9506 = 0, the following applies:**
  Braking is monitored with the "Safe Acceleration Monitor" function (see Chapter "SAM (Page 162)").
  In this case, we also talk about "SS1 (time and acceleration controlled)".
- **For p9506 = 2, the following applies:**
  Braking is monitored using the "Safe Brake Ramp" function (see Chapter "SBR (Page 164)").
  In this case, we also talk about "SS1 (speed controlled)".

The "Safe Stop 1" (SS1) function allows the drive to be stopped according to EN 60204-1, Stop Category 1. The drive brakes with the OFF3 ramp (p1135) once "Safe Stop 1" is selected and switches to "Safe Torque Off" (STO) once the delay time has elapsed (p9556) or when the shutdown speed is fallen below (p9560).

Functional features of Safe Stop 1 with encoder

- The delay time starts after the function has been selected. If SS1 is deselected again within this time, the STO function is selected and deselected immediately again after the delay time has expired or if the speed drops below the shutdown speed; i.e. the SS1 function is terminated normally. It cannot be interrupted.
- Selection and monitoring of the acceleration (SAM) or the monitoring function "Safe Brake Ramp" are implemented in two channels, but braking along the OFF3 ramp is only implemented in one channel.
- Effect on "Setpoint speed limit effective" (r9733[0...2]):
  For SS1 (≙ STOP B), setpoint 0 is specified in r9733[0...2].

Commissioning

The delay time (SS1 time) is set by entering parameter p9556. The wait time until safe pulse cancellation (STO) can be shortened by defining a shutdown speed in p9560.

To enable the drive to brake to standstill after selection, the time in p9556 must be selected to be long enough for the drive to be able to brake along the OFF3 ramp (p1135) from any speed of the underlying process to below the shutdown speed (p9560).

Note

Setting the delay time

So that the drive is able to travel down the OFF3 ramp completely and any motor holding brake present can be applied, the delay time should be set as follows:

- Motor holding brake parameterized: Delay time ≥ p1135 + p1228 + p1217
- Motor holding brake not parameterized: Delay time ≥ p1135 + p1228

The shutdown speed defined in p9560 must be set in such a way that coasting down (due to the subsequent STO function) does not represent any risk for man and machine.

Responses

System fault:

1. STOP F with subsequent STOP B, followed by STOP A
2. Safety message C01711

Status of Safe Stop 1

You can check the status in the SI diagnostics screens via "MENU SELECT > Diagnostics > Menu forward key > Safety".

5.2.1.2 Safe Stop 1 without encoder

Two encoderless Safe Stop 1 (SS1) monitoring functions can be set with parameter p9506:

- p9506 = 3: Safe monitoring of acceleration (SAM) / delay time
  The function is identical to "Safe Stop 1" with encoder (Page 110).
  In this case, we also talk about "SS1 (time and acceleration controlled)".
- p9506 = 1: Safe brake ramp monitoring (SBR)
  In this case, there is no SS1 delay time active. The transition from SS1 to STO depends entirely on the speed falling below the shutdown speed (p9560). You will find more information on the function "Safe Brake Ramp (SBR)" in Chapter "SBR (Page 164)." In this case, we also talk about "SS1 (speed controlled)".

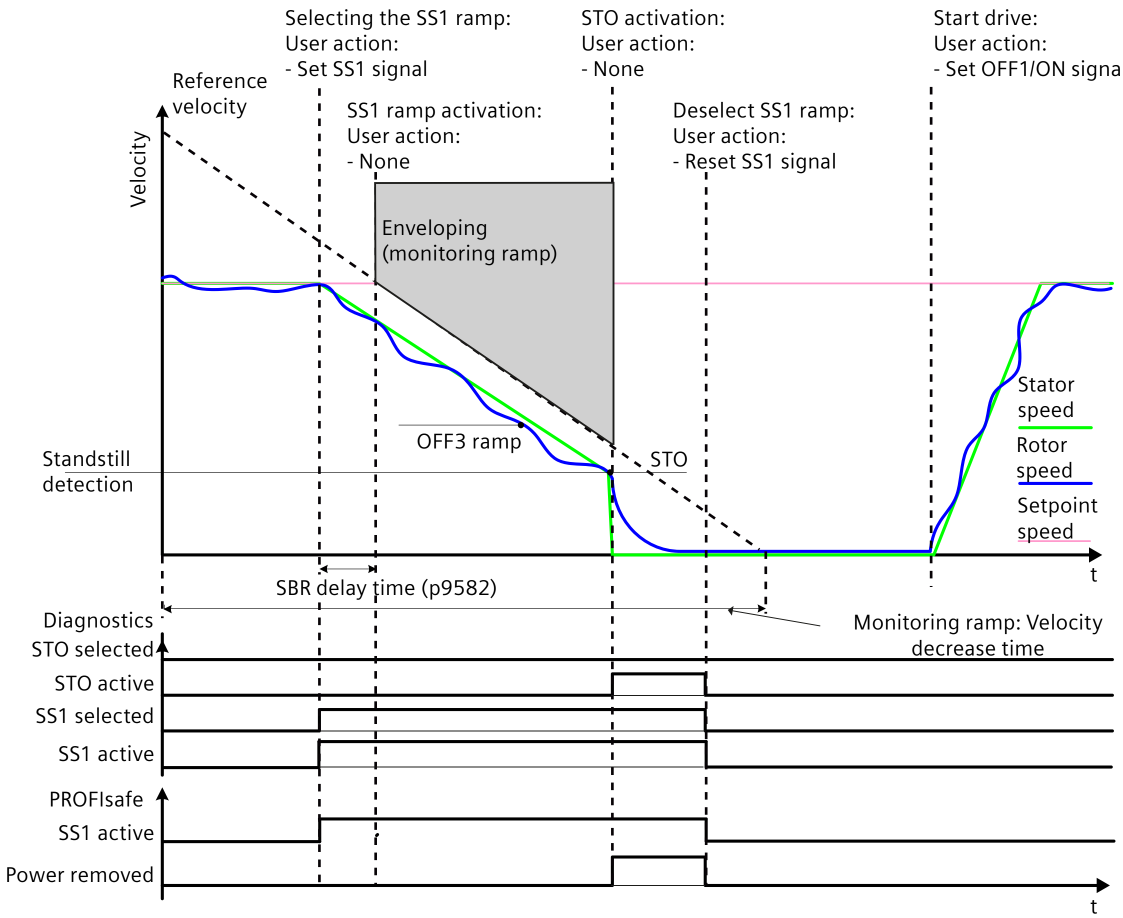


Figure 5-1 Sequence for "Safe Stop 1" without encoder with SBR monitoring (p9506 = 1)

Functional feature of Safe Stop 1 without encoder

- Selection and monitoring of the brake ramp (SBR) or the acceleration (SAM) are implemented in two channels, however braking at the OFF3 ramp is only through one channel.

5.2.1.3 SS1 (Extended Functions) with external stop

General description

WARNING

Unexpected axis motion when the SS1E function is active

When the SS1E function is active, during the monitored delay time, axis motion that is not monitored can occur. This can result in death or severe injury.

- Prevent persons from entering the hazardous area around the axis, e.g. by providing protective doors or other suitable protective equipment.

With external stop, "Safe Stop 1" basically works exactly as described in the previous Chapters "Safe Stop 1 with encoder (time and acceleration controlled)" and "Safe Stop 1 without encoder (speed controlled)." Note, however, the following differences:

Differences between "Safe Stop 1 with OFF3" and "SS1 with external stop"

- In order to activate "Safe Stop 1 with external stop", **additionally** set p9507.3 = 1.
- When SS1 with external stop is selected, the drive is **not** braked along the OFF3 ramp: You are responsible in applying suitable measures to brake the drive. After the delay time has expired (p9556), only STO/SBC are automatically initiated. After the function has been selected, the delay timer runs down - even if the function is deselected during this time. In this case, after the delay time has expired, the STO/SBC function is selected and then again deselected immediately.
- The brake ramp (SBR) and the acceleration (SAM) are not monitored and there is no standstill detection.
- With this configuration, STO becomes active after the SS1 timer p9556 has expired; this also applies if SBR has been configured.
- Further information can be found in Section Extended Functions (Page 368).

Constraint

Note

The function is configurable - however, the braking behavior using SS1E is not supported by the NC (path stop).

5.2.1.4 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2819 SI Extended Functions - SS1, SS2, SOS, internal STOP B, C, D, F

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p1135[0...n] OFF3 ramp-down time
- p9501 SI Motion enable safety functions (Control Unit)
- p9506 SI Motion function specification (Control Unit)
- p9556 SI Motion STOP A delay time (Control Unit)
- p9560 SI Motion STO shutdown speed (Control Unit)
- r9722.0...15 CO/BO: SI Motion drive-integrated status signals

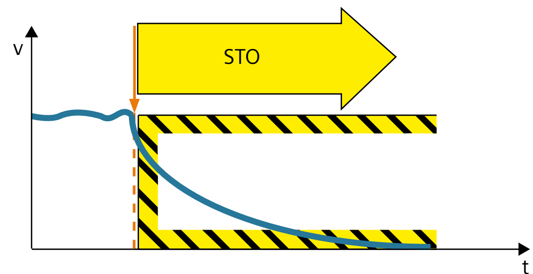
Only for SS1 (Extended Functions) with external stop

- p9507 SI Motion function configuration (Control Unit)

5.3 STO (Basic/Extended)

Definition according to EN 61800-5-2:

"The STO function prevents energy from being supplied to the motor, which can generate a torque."



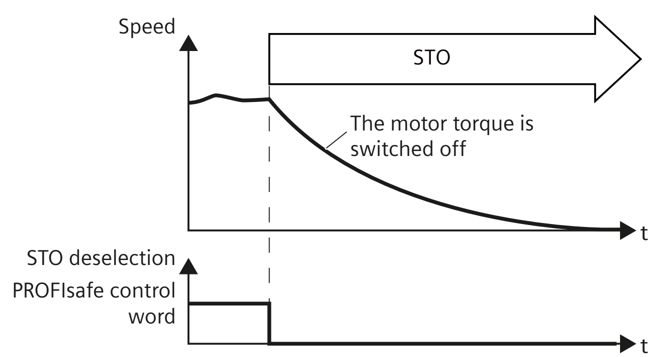
Examples of how the function can be used

Example	Possible solution
It is only permissible to open a protective door if the motor torque has been switched off.	• Select STO in the converter. • The pulses are suppressed and the motor coasts to a standstill.

How does STO function in detail?

The converter recognizes the selection of STO via a failsafe input or via the safe communication PROFIsafe.

The converter then safely switches off the torque of the connected motor.



5.3.1 Details and parameterization

In conjunction with a machine function or in the event of a fault, the "Safe Torque Off" (STO) function is used to safely disconnect the torque-generating energy supply to the motor.

A restart is prevented by the two-channel pulse suppression. The switching on inhibited prevents an automatic restart after deselection of STO.

The two-channel pulse suppression function integrated in the Motor Modules / Power Modules is the basis for this function.

Functional features of "Safe Torque Off"

- The function is completely integrated in the drive. It can be selected via terminals or PROFIsafe from an external source.
- The function is drive-specific, i.e. it is available for each drive and must be individually commissioned.
- The function must be enabled via parameter.
- When the "Safe Torque Off" function is selected, the following applies:
  - The motor cannot be started accidentally.
  - The pulse suppression safely disconnects the torque-generating energy supply to the motor.
  - The power unit and motor are not electrically isolated.
- The selection/deselection of the STO function also acknowledges the safety faults when the Basic Functions are used. The standard acknowledgment mechanism must also be performed.
- Extended acknowledgment:
  The selection/deselection of STO can also acknowledge the safety messages of the extended safety functions. This means that you must configure the extended message acknowledgment (p9507.0 = 1).
  If in addition to the "Extended Functions", the "Basic Functions via terminals" are also enabled, in addition to selection/deselection of STO via PROFIsafe (Page 377), acknowledgement is also possible by selection/deselection of STO via terminals.
- The status of the "Safe Torque Off" function is displayed using parameters (r9772, r9872, r9773 and r9774).
- Effect on "Setpoint speed limit effective" (r9733[0...2]):
  For STO (≙ STOP A), a setpoint of 0 is specified in r9733[0...2].

⚠ WARNING

Unexpected machine motion when STO is active

After the energy feed has been disconnected (STO active) the motor can undesirably move (e.g. the motor can coast down), therefore presenting risk to persons.

- Take suitable measures to prevent undesirable movement, e.g. by using a brake with safety-relevant monitoring. You can find additional information in Chapter "SBC (Basic/Extended) (Page 121)".

⚠ WARNING

Unexpected motor movement as a result of defective power transistors

Undesirable motor motion[1)] can occur if 2 power transistor simultaneously become defective (breakdown of the depletion layer). This can result in accidents leading to death or severe injury.

- Take suitable measures to prevent undesirable movement, e.g. by using a brake with safety-relevant monitoring. You can find additional information in Chapter "SBC (Basic/Extended) (Page 121)".

[1)] The maximum movement can involve:

- Synchronous rotary motors: Max. movement = 180° / no. of pole pairs
- Synchronous linear motors: Max. movement = pole width

Enabling the "Safe Torque Off" function

The "Safe Torque Off" function is enabled via parameter p9601:

- STO for the Safety Integrated Basic Functions:
  - p9601 = 1 hex (Basic Functions via onboard terminals)
  - p9601 = 8 hex (Basic Functions via PROFIsafe)
  - p9601 = 9 hex (Basic Functions via PROFIsafe and onboard terminals)
- STO for the Safety Integrated Extended Functions:
  - p9601 = C hex (Extended Functions via PROFIsafe)
  - p9601 = D hex (extended functions via PROFIsafe and basic functions via onboard terminals)
  - p9601 = 25 hex (Extended Functions without selection and Basic Functions via onboard terminals)

Selecting/deselecting "Safe Torque Off"

The following is executed when "Safe Torque Off" is selected:

- Each monitoring channel triggers safe pulse cancellation via its switch-off signal path.
- A motor holding brake is closed (if connected and configured).

Deselecting "Safe Torque Off" represents an internal safety acknowledgment. The following is executed if the cause of the fault has been removed:

- Each monitoring channel cancels safe pulse cancellation via its switch-off signal path.
- The Safety requirement "Close motor holding brake" is canceled.
- Any pending STOP F or STOP A commands are canceled (see r9772).
- The messages in the fault memory must also be reset using the general acknowledgment mechanism.

Note

No message for selection/deselection within the tolerance time (p9650)

If "Safe Torque Off" is selected and deselected through one channel within the tolerance time p9650, the pulses are suppressed without a message being output.

However, if you want a message to be displayed, then you must reconfigure N01620 as an alarm or fault using p2118 and p2119.

Restart after the "Safe Torque Off" function has been selected

1. Deselect the function.
2. Set drive enables.

Status for "Safe Torque Off"

You can check the status in the SI diagnostics screens via "MENU SELECT > Diagnostics > Menu forward key > Safety".

Internal armature short-circuit with the "Safe Torque Off" function

The function "internal armature short-circuit" can be configured together with the "STO" function.

The "STO" safety function has the higher priority when simultaneously selected. If the "STO" function is initiated, then an activated "internal armature short-circuit" is disabled.

5.3.1.1 Safe Torque Off (STO) for SINAMICS HLA

For the HLA module, Safe Torque Off (STO) corresponds to shutting off a safety-related shutoff valve.

Special features of STO for HLA

- The shutoff valve controls the infeed to the hydraulic circuit. The shutoff valve is controlled via an F-DO of SINAMICS HLA.
- For Safety Integrated Functions, it is absolutely necessary that a shutoff valve is connected with the associated feedback signals.
- You configure the feedback signal contacts of the shutoff valve using parameter p9626.
- You can take into account the response times of the feedback signals using parameter p9625.

- The shutoff valve is safely closed by selecting STO. If the shutoff valve signals a safe state via the feedback signal(s), the "STO active/Power removed" state is displayed, and is output at the configured safety-related output (PROFIsafe feedback signal telegram).

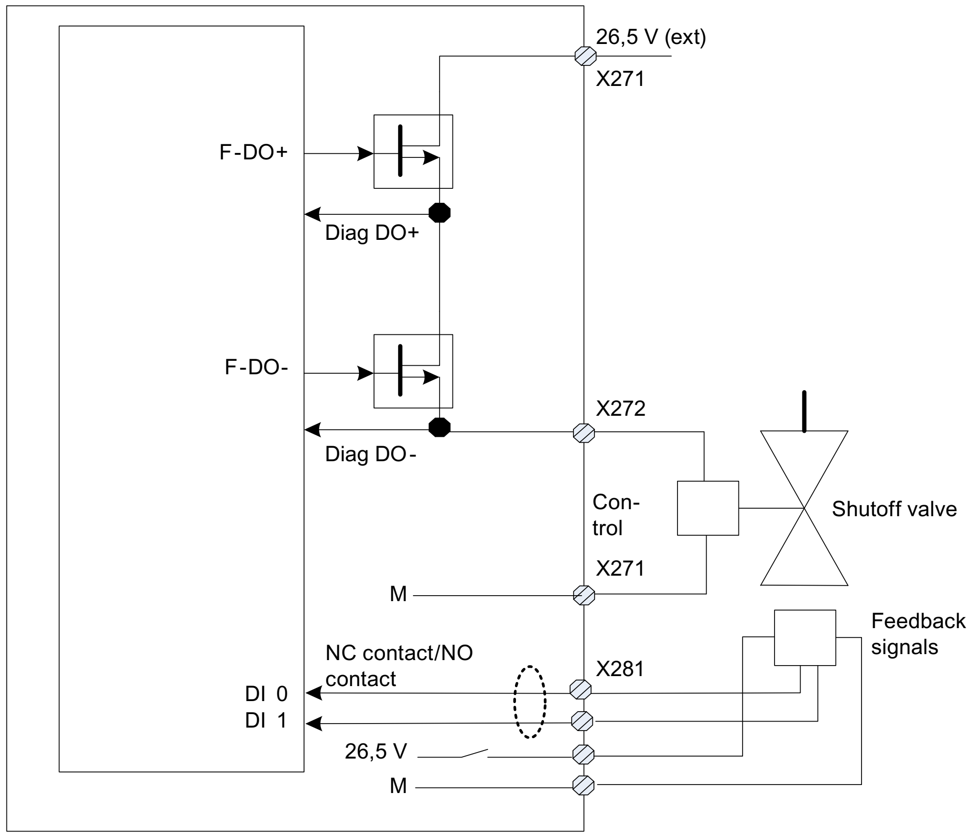


Figure 5-2 Interconnecting the shutoff valve (for an axis)

- F-DO is dynamized each time that STO is selected/deselected: "Diag DO+" and "Diag DO-" are checked when switching F-DO+ and F-DO-.
- It is not necessary to explicitly select a test stop/forced checking procedure.
- If, for test stop/forced checking procedure, a fault occurs, then the converter outputs fault F01632 or F30632.

5.3.1.2 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2810 SI Basic Functions - STO (Safe Torque Off), SS1 (Safe Stop 1)
- 2811 SI Basic Functions - STO (Safe Torque Off), safe pulse cancellation

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9601 SI enable functions integrated in the drive (Control Unit)
- r9720 CO/BO: SI Motion drive-integrated control signals
- r9772 CO/BO: SI Status (Control Unit)
- r9773 CO/BO: SI Status (Control Unit + Motor Module)
- r9774 CO/BO: SI Status (group STO)

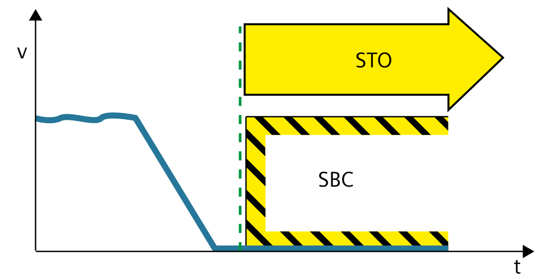
HLA parameters

- p9625[0...1] SI HLA shutoff valve wait time (CU)
- p9626 SI HLA shutoff valve feedback contacts configuration (CU)
- r9773 CO/BO: SI Status (Control Unit + Motor Module)
- r9774 CO/BO: SI Status (group STO)
- r9780 SI monitoring cycle (Control Unit)

5.4 SBC (Basic/Extended)

Definition according to EN 61800-5-2:

"The SBC function supplies a safe output signal to control a holding brake."



Safe Brake Control (SBC)

Example of how the function can be used

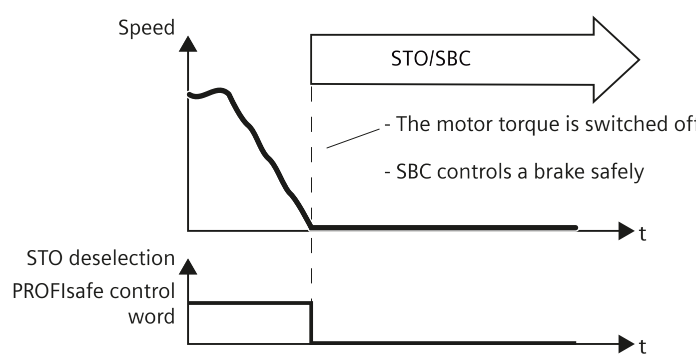
Example	Possible solution
The safe control of a motor holding brake must be guaranteed in order to guarantee the motor is at a standstill.	SBC is (if configured) initiated together with STO. The Motor Module / Safe Brake Relay / Safe Brake Adapter then carries out the action and safely controls the outputs for the brake.

How does SBC function in detail?

The converter recognizes the selection of STO via a failsafe input or via the safe communication PROFIsafe.

The converter then safely switches off the torque of the connected motor.

SBC is (if configured) initiated together with STO. The Motor Module / Safe Brake Relay / Safe Brake Adapter then carries out the action and safely controls the outputs for the brake.



5.4.1 Hardware required

- Safe Brake Relay
  The command for releasing or applying the brake is transferred to the Motor Module / Power Module via DRIVE-CLiQ. The Motor Module / Safe Brake Relay then carries out the action and appropriately activates the outputs for the brake.

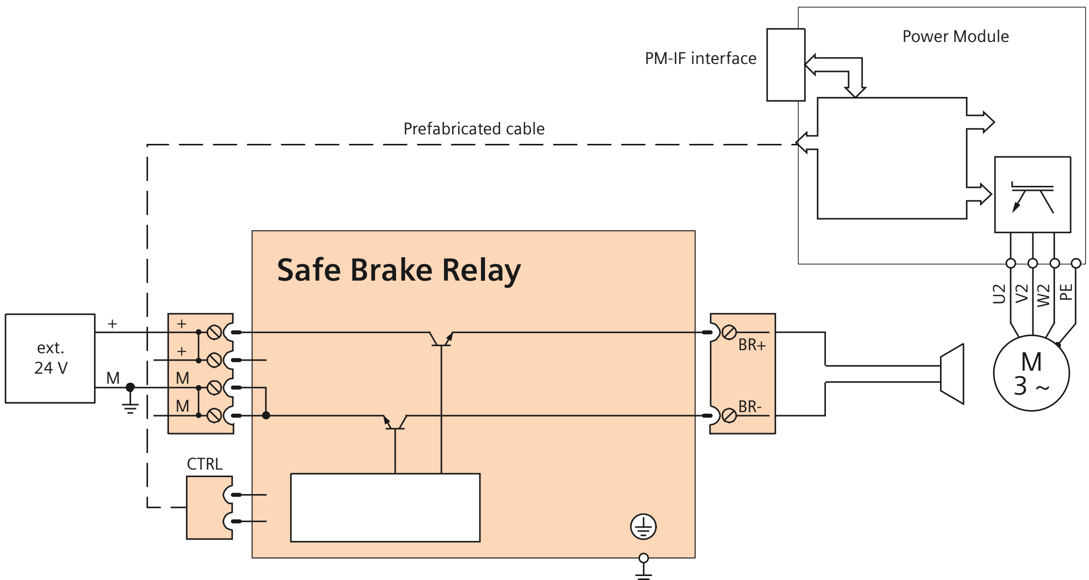


Figure 5-3 Interconnecting the Safe Brake Relay using Blocksize as an example

The brake cannot be directly connected to the Motor Module in the chassis format. The connection terminals are only designed for 24 VDC with 150 mA; the Safe Brake Adapter is required for higher currents and voltages.

Note

Additionally required hardware for other formats

A Safe Brake Relay is also required for the "Safe Brake Control" in the blocksize format. A Safe Brake Adapter is required in the chassis format (starting with order numbers with the ending ...xxx3). The Safe Brake Adapter is available for a 230 V AC brake control voltage.

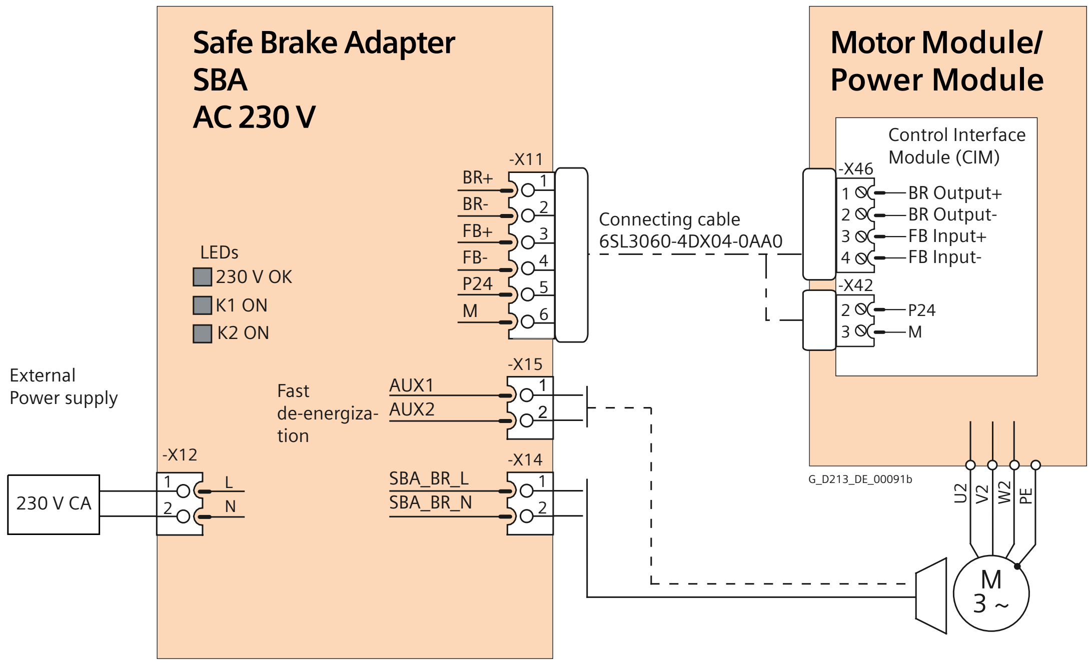


Figure 5-4 Interconnecting the Safe Brake Adapter

5.4.2 Details and parameterization

Note

No SBC for SINAMICS HLA

SINAMICS HLA does not support Safe Brake Control.

The "Safe Brake Control" function (SBC) is used to safely control holding brakes that function according to the closed-circuit principle (e.g. motor holding brake).

The opening and closing of the brake is controlled by the Motor Module / Power Module. Terminals are available for this on the device in booksize format. A Safe Brake Relay is also required for the "Safe Brake Control" in the blocksize format. With the chassis format (article numbers ending 3 or higher), a Safe Brake Adapter is required. When the Power Module is configured automatically, the Safe Brake Relay is detected and the motor holding brake type is defaulted (p1278 = 0).

Brake activation via the brake connection on the Motor Module / Safe Brake Relay (SBR) / Safe Brake Adapter (SBA) involves a safe, two-channel method.

Note

Controlling the brake via a relay for "Safe Brake Control":

If you use the "Safe Brake Control (SBC)" function, the use of relays/contactors can cause faults in the brake control when brakes are switched. For this reason, this type of control is not generally enabled.

An interrupted cable or a short-circuit in the brake winding is only detected when the state changes, i.e. when the brake either opens or closes. For devices in the chassis format with connected Safe Brake Adapter, the connecting cable between the Safe Brake Adapter and the motor brake is not monitored for an interrupted cable or short-circuit.

WARNING

Undesirable motor motion due to a defective brake

The "Safe Brake Control" function does not detect mechanical defects of the brake. A defective brake can result in unwanted motor motion, which may result in injury or death.

- Test the brake using the Safety Integrated diagnostics function "Safe Brake Test (SBT)" (for further information, see Section "Enabling the function (Page 189)").

Functional features of "Safe Brake Control"

- SBC is executed when "Safe Torque Off" (STO) is selected.
- In contrast to conventional brake control, SBC is executed via two channels.
- SBC is executed regardless of the brake control or mode set in p1215. SBC is not recommended, however, when 1215 = 0 or 3.
- The function must be enabled using parameters.
- When the state changes, electrical faults, such as a short-circuit in the brake winding or wire breakage can be detected.

Enabling the "Safe Brake Control" function

The "Safe Brake Control" function is enabled via parameter p9602.

The "SBC" function can be used only together with STO (i.e. p9501 ≠ 0 and/or p9601 ≠ 0). It is not possible to just select SBC.

Two-channel brake control

Note

Connecting the brake

The brake cannot be directly connected to the Motor Module in chassis format: A Safe Brake Adapter is also required.

The brake is controlled from the Control Unit. Two signal paths are available for applying the brake.

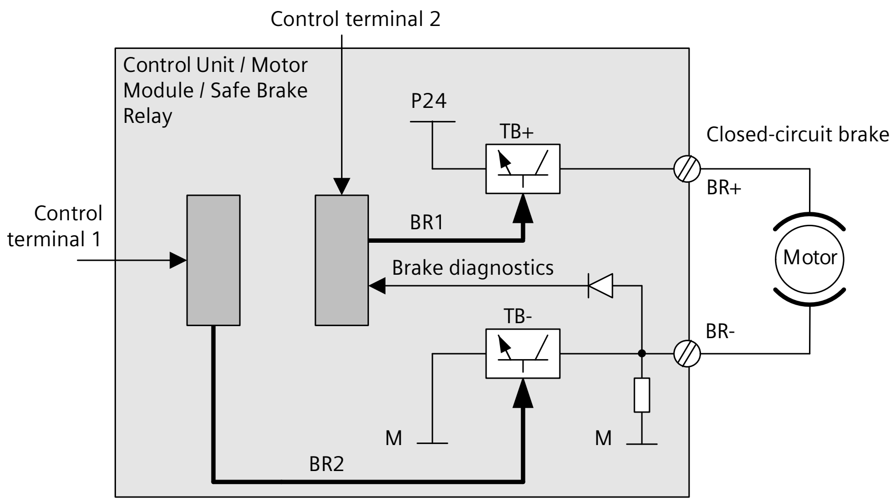


Figure 5-5 Two-channel brake control, blocksize (example)

For the "Safe Brake Control" function, the Motor/Power Module assumes a monitoring function to ensure that when the Control Unit fails or malfunctions, the brake current is interrupted therefore closing the brake.

The brake diagnosis can only reliably detect a malfunction in either of the switches (TB+, TB-) when the status changes, i.e. when the brake is released or applied.

If the Motor Module or Control Unit detects a fault, the brake current is switched off. The brake then closes and a safe state is reached.

5.4.2.1 SBC for Motor Modules in the chassis format

To be able to set higher power in the brakes of devices of this format, an additional Safe Brake Adapter (SBA) module is needed. For more information about connecting and wiring the Safe Brake Adapter, refer to the "SINAMICS G130/G150/S120 Chassis/S120 Cabinet Modules/S150 Safety Integrated" Function Manual.

Using parameter p9621, you can define via which digital input the relay (NO contacts) feedback signal of the Safe Brake Adapter is routed to the Control Unit.

To evaluate the feedback signal contacts, you must maintain the wait times caused by the SBA. Parameter p9622 is pre-assigned with the SBA-relay wait times:

- p9622[0] ≙ wait time, switching on
- p9622[1] ≙ wait time, switching off

Further functionality and the activation of the brake, i.e. reaching the safe status, are in this case the same as the above described procedure for booksize devices.

Safe Brake Control with power units in a parallel connection

Note

SBC for parallel connection of power units

Safe Brake Control with power units in a parallel connection is available if r9771.14 = 1.

If you wish to use SBC with SBA for chassis format power units connected in parallel, then it is only permissible that you connect precisely one SBA to a power unit in the parallel connection. The Safe Brake Adapter and therefore the brake are controlled via this power unit.

There are two options for registering this power unit with the system:

- Automatic brake identification when commissioning the system for the first time
  - Requirements:
    - No Safety Integrated Functions enabled
    - p1215 = 0 (no motor holding brake available)
  - During the first commissioning, SINAMICS checks at which power unit an SBA is connected. If precisely one SBA is found, the number of the power unit is entered into parameter p7015.
    If several SBAs are found at the parallel-connected power units, message "F07935 drive: Motor holding brake configuration error" is output.
  - For devices in the chassis format, if the SBA feedback signal (SBA_DIAG) is read in via an input of the power unit, then in addition, this digital input is automatically entered into parameter p9621.
- Manually defining the power unit
  - Enter the component number of the power unit, to which the SBA is connected, into parameter p7015. If no SBA is connected to the power unit, faults are detected when controlling the motor holding brake and fault F01630 is output.
  - In parameter p9621 (p9621 = BICO interconnection to r9872.3), enter the digital input of the power unit to which the SBA is connected and via which the SBA feedback signal (SBA_DIAG) is read in.

Note

Disconnecting the brake cable for service purposes

As long as the brake is permanently released and not actuated, it is possible to briefly disconnect the brake cable, e.g. for service purposes, and not receive fault messages. In the case of a fault, message F07935 is only output when the brake is controlled.

5.4.2.2 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2814 SI Basic Functions - SBC (Safe Brake Control), SBA (Safe Brake Adapter)

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p0799 CU inputs/outputs, sampling time
- p1215 Motor holding brake configuration
- p7015 Par_circuit holding brake power unit data set
- p9602 SI enable safe brake control (Control Unit)
- p9621 BI: SI Safe Brake Adapter signal source (Control Unit)
- p9622[0...1] SI SBA relay wait times (Control Unit)
- r9771.14 SI common functions (Control Unit): SBC supported for parallel connection
- r9780 SI monitoring cycle (Control Unit)

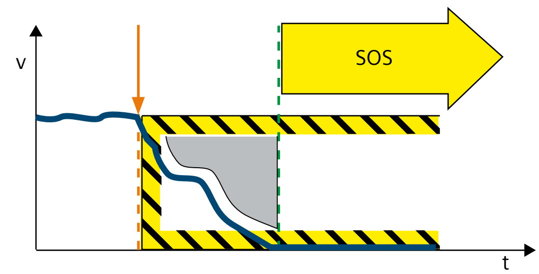
5.5 SS2

Definition according to EN 61800-5-2:

The "SS2" function brings the motor to a standstill with subsequent safe monitoring of the standstill position. If SS2 is selected, the drive brakes the motor along a braking ramp. The following variants are possible:

- SS2-a with acceleration monitoring (SAM)
- SS2-r with braking ramp monitoring (SBR)
- Manually set delay time until SOS is activated.

This function corresponds to stop category 2 to EN 60204-1.

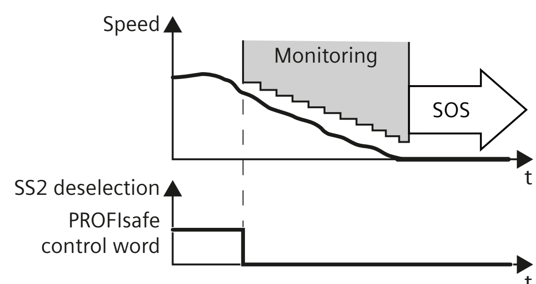


Example of how the function can be used

Example	Possible solution
A protective door must only be opened if a motor is in the safe standstill state.	• Select SS2 in the converter via a terminal or via PROFIsafe . • After braking, the converter goes into the SOS state. Only then may the protective door be released.

The safety function SS2 monitors the load speed and initiates the SOS function if the SS2 delay time has expired.

With SS2, braking is monitored on the OFF3 ramp. A faulty acceleration is detected and the drive then shuts down with STO.



If you are operating the motor with closed-loop torque control, the converter switches to the closed-loop speed control mode when SS2 is selected.

How does SS2 function in detail?

The failsafe logic (e.g. F-PLC) selects the SS2 safety function via a failsafe input or via the PROFIsafe safe communication.

- If, when selecting SS2, the motor is already at a standstill, after a delay time, the converter activates function "Safe Operating Stop (SOS)".
- If the drive is not at standstill when SS2 is selected, it is braked along the OFF3 ramp. Braking is monitored with one of the following functions, depending on the setting in p9506:
  - Safe Acceleration Monitor (SAM)
    A faulty acceleration is therefore detected.
  - Safe Brake Ramp (SBR)
    In this way, a violation of the braking ramp is detected.

  After a delay time, the converter activates function "Safe Operating Stop (SOS)". This function monitors the safe standstill of the drive.

Braking behavior

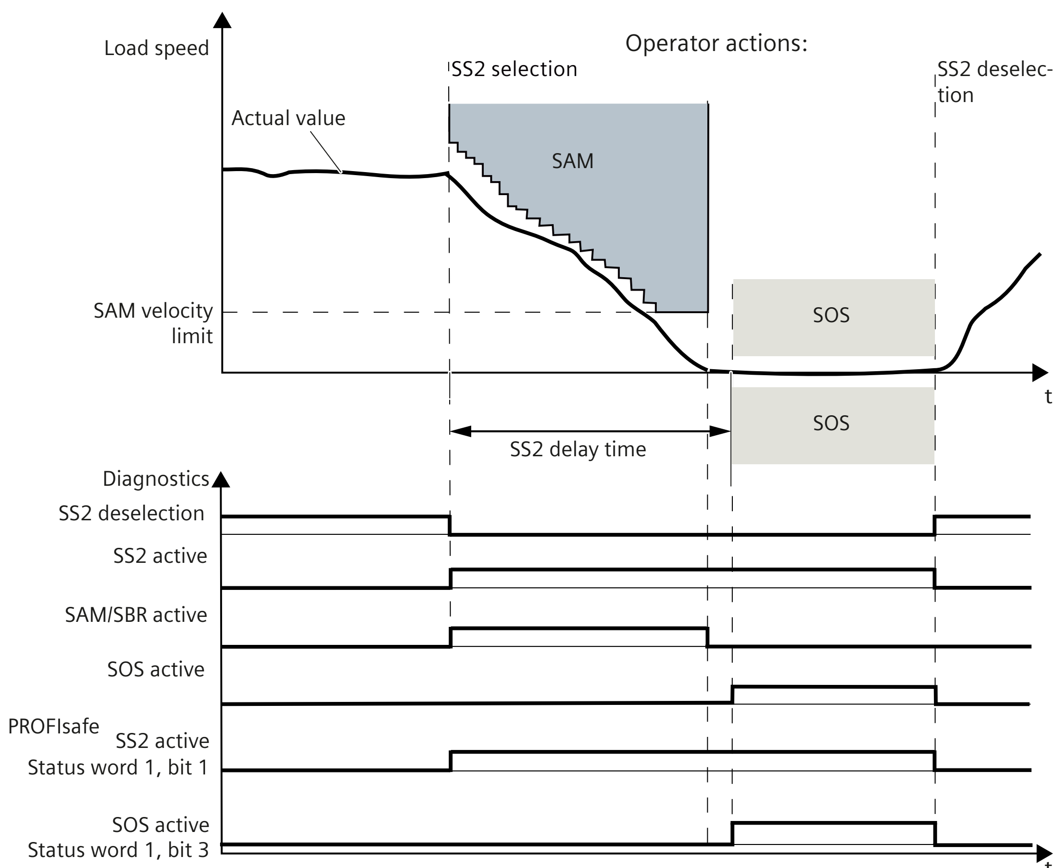


Figure 5-6 Braking behavior and diagnostics (example for SS2 with SAM)

Note

SS2 with external stop (SS2E)

If you use SS2E, neither of the two monitoring functions (SBR, SAM) is active. The drive is decelerated by interpolation (SIC/SCC is required for this). SOS becomes active after the delay time expires.

5.5.1 Details and parameterization

Note

SS2 only with encoder

The "Safe Stop 2" (SS2) safety function can only be used with an encoder.

The "Safe Stop 2" (SS2) function is used to brake the motor safely along the OFF3 deceleration ramp (p1135) with subsequent transition to the SOS state (see Chapter "Safe Operating Stop (Page 139)") after the delay time expires (p9552). The delay time set must allow the drive to brake to a standstill from every speed of the operating process within this time. The standstill tolerance (p9530) may not be violated after this time.

After braking, the drives remain in speed control mode with the speed setpoint n = 0. The full torque is available.

When braking, one of the following functions is active:

- **For p9506 = 0, the following applies:**
  Braking is monitored with the "Safe Acceleration Monitor" function (see Chapter SAM (Page 162)).
- **For p9506 = 2, the following applies:**
  Braking is monitored using the "Safe Brake Ramp" function (see Chapter SBR (Page 164)).

The selection and monitoring of the acceleration (SAM) are realized through two channels – however, braking along the OFF3 ramp, only through one channel.

- Effect on "Setpoint speed limit effective" (r9733[0...2]):
  If SS2 (≙ STOP C), a setpoint of 0 is specified in r9733[0...2].

Responses

- **Speed limit violated (SAM):**
  - STOP A
  - Safety message C01706
- **Standstill tolerance violated in p9530 (SOS):**
  - STOP B with subsequent STOP A
  - Safety message C01707
- **System fault:**
  - STOP F with subsequent STOP A
  - Safety message C01711

5.5.1.1 SS2 with external stop (SS2E)

> **WARNING**
>
> **Unexpected axis motion when the "SS2E" function is activated**
>
> When the "SS2E" function is active, during the safety delay time, until SOS is reached, axis motion that is not monitored can occur. This can result in death or severe injury.
>
> - During this time, prevent persons from entering the hazardous area around the axis, e.g. by providing protective doors or other suitable protective equipment.

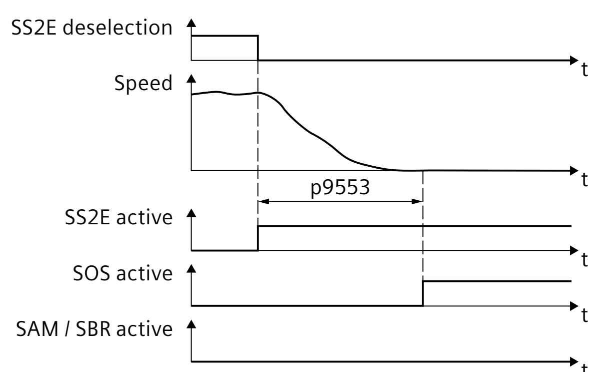


Figure 5-7 Selecting function SS2E

With external stop, "Safe Stop 2" functions in principle exactly the same way as described in the previous sections. Note, however, the following differences:

Differences between "Safe Stop 2 with OFF3" and "SS2 with external stop (SS2E)"

- When SS2 is selected with external stop, the drive does not automatically brake the motor, but instead, follows the specified speed setpoint.
- During delay time p9553, the brake ramp (SBR) and the acceleration (SAM) are not monitored and there is no standstill detection.

- SOS becomes active after the delay time p9553 expires.
P9553 must be set in such a way that the axes are braked to a standstill with the set dynamics.
- In order to activate "Safe Stop 2 with external stop", set p9501.18 = 1.
- The PROFIsafe control word S_STW2.28 selects the SS2E function. PROFIsafe S_STW2.28 is contained in telegrams 31, 901, 902 and 903.
- The PROFIsafe status word S_ZSW2.28 indicates whether the SS2E function is active. The PROFIsafe status word S_ZSW2.28 is contained in telegrams 31, 901, 902 and 903. The associated diagnostics parameter is r9722.28.
In the "Safety Info Channel", status word S_ZSW3B.11 indicates whether function SS2E is active. The associated diagnostics parameter is r10234.11.
Diagnostic parameters p9722.28 and p10234.11 are also set during an internal STOP D.

Deselecting function SS2E while SS2E is active

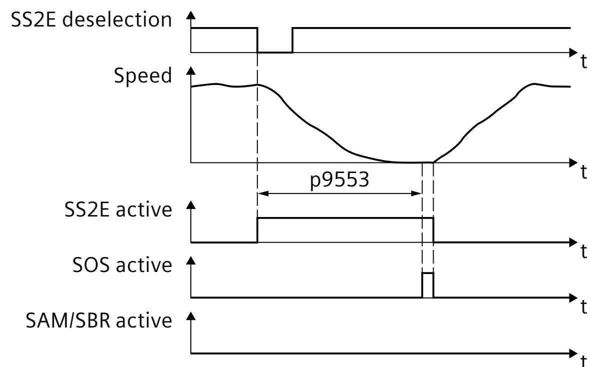


Figure 5-8 Deselecting function "SS2E" while SS2E is active

After the function has been selected, the delay time starts to elapse - even if the function is deselected during this time. In this case, after the delay time has expired, the "SOS" function is briefly active. Afterwards, it is permissible that the drive accelerates the motor back to the speed setpoint.

Interruption of the active "SS2E" function by functions "SS1" and "SS2"

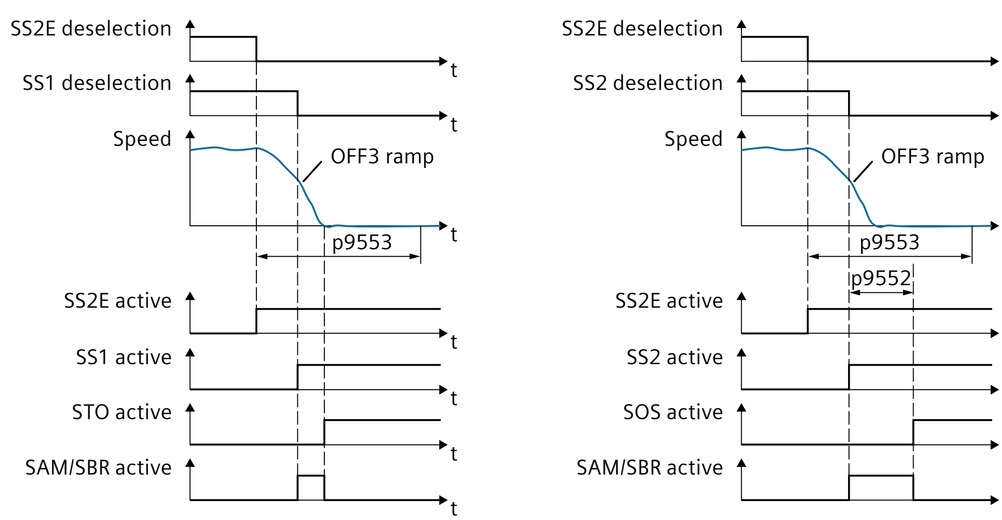


Figure 5-9 Interruption of function "SS2E" by functions "SS1" (shown at the left) and "SS2" (shown at the right)

When selecting SS1, the drive brakes the motor along the OFF3 ramp and monitors the speed using the "SAM" function. Function "STO" becomes active when the motor is at a standstill.

When selecting SS2, the drive also brakes the motor along the OFF3 ramp and monitors the speed using the "SAM" function. Function "SOS" becomes active after time p9552.

5.5.1.2 Dynamic response adaptation for SS2E

Adaptation of the dynamic response for axes

For axes, the acceleration characteristic is adapted dynamically so that the axes stop within the time saved in p9553 "SI Motion transition time STOP D to SOS". Therefore, ensuring stopping with low associated stress on the machine.

In order that the stop D time, parameterized in p9553, is used as basis to determine the braking time and possibly issue an alarm, this must be enabled by setting bit 2 in MD37950 $MA_SAFE_INFO_ENABLE.

When powering up, for all axes with SIC/SCC connection - where the bit to take into account the stop D/SS2E transition times in the braking response (MD37950.2 $MA_SAFE_INFO_ENABLE) is set, the control system checks whether the braking time set in p9553 is sufficient for the active acceleration characteristic of the axis. When violated, suppressible alarm 22001 "Channel %1 block %2 axis %3: braking time %6 [s] longer than the stop D time. Reason: %5" is output.

If the acceleration/deceleration behavior is changed, the axes brake for STOP D with the shortest transition time of all path axes. It is recommended that the transition times are set the same in p9553 for all axes of an interpolation group.

Adaptation of the dynamic response for spindles

For spindles, the actual acceleration characteristic is not adapted. The control checks whether the braking time set in p9553 is sufficient for all spindle operating modes and configured gear stages. When violated, suppressible alarm 22002 "Channel %1 Spindle %2: Braking time %6 [s] longer than the stop D time gearbox stage %3. Reason: %5" is output.

If the spindle is in axis operation, then it behaves just like an axis.

Adaptation of the dynamic response for coupling

For an active axis or spindle coupling (with the exception of the synchronous spindle coupling), the coupling is no longer taken into consideration, if synchronous stopping of the coupled group is no longer safely possible within the time parameterized in p9553. For a coupled group, this is the reason why a STOP D must be set for all axes of the coupled group.

For the synchronous spindle coupling, when synchronous operation is reached, the coupling is always maintained. The coupling group is always braked via the leading spindle. If the following spindle requires a longer braking time than the leading spindle, then p9553 must be appropriately increased for the leading spindle.

When a synchronous spindle is active, STOP D should also be initiated for the leading and following spindle.

Endlessly rotating axes are braked at the acceleration limit.

The SOS function is automatically activated after the time set in p9553 expires.

Configuring support

The braking time of the active acceleration characteristic is available in the OPI tag "diagSlopeTime".

The displayed time is the maximum expected braking time that has been determined, and is used as diagnostic information for parameterizing the STOP D time. It is possible that it can have a higher value than the braking time displayed in alarm A22001/A22002 (dependent on the dynamic response settings). The determined time is displayed in commissioning screen form SS2E.

Note

Irrespective of the reason, the longest braking time to be expected is always displayed in the OPI tag. The OPI tag is only output when Safety Integrated is activated for the particular axis.

Triggering alarms

The following formulas are applied to trigger alarm 22001/22002:

METRIC:	p9553 > MAX_AX_VELO * 1/60000 / MAX_AX_ACCEL
INCH/ROT/SPINDLE:	p9553 > MAX_AX_VELO * 1/60 / MAX_AX_ACCEL

For axes with jerk limitation, the minimum braking time is increased by the additional component:

2 * MAX_AX_ACCEL / MAX_AX_JERK

The check is made for NEWCONF, RESET, unparking an axis and for programming ACC or JERKLIM.

The MD names contained in the formulas must, corresponding to the alarm situation (the alarm occurs when parameterizing or when programming), be replaced by other values when required.

MD	Alternative MD	Gearbox stage-specific MD spindle	Program command
MAX_AX_VELO	min(JOG_VELO, JOG_VELO_RAPID)	$MA_GEAR_STEP_MAX_VELO_LIMIT[0...max] $MA_GEAR_STEP_PC_MAX_VELO_LIMIT[0...max]	-
MAX_AX_ACCEL	MAX_AX_ACCEL	$MA_GEAR_STEP_SPEEDCTRL_ACCEL[0...max] $MA_GEAR_STEP_POSCTRL_ACCEL[0...max]	ACC
MAX_AX_JERK	JOG_AND_POS_MAX_JERK		JERKLIM

Notes:

The calculated value should be rounded off to one decimal place so that for an INCH-METRIC switchover, internal rounding effects can be compensated and no undesirable alarms are initiated.

With the parameterization of the STOP D braking time in p9553 via the HMI IBN screen forms and subsequent update by means of the operator panel reset, alarm 22001 or 22002 is triggered when the specified calculation rules are violated.

The braking time of the active acceleration characteristic is available in the NC tag "diagSlopeTime", and can be used as basis to parameterize the Stop D braking time.

The braking time is only calculated using static parameterized values for VELO, ACCEL, JERK. This is only applicable for the current motion type and dynamic response level "DYNNORM".

The values for other dynamic response levels are only taking into account at the time of switchover (e.g. in the part program).

Alarms 22001/22002 can be suppressed via MD 11415 bit 13. The dynamic response is adapted as described.

When evaluating the alarm output, the conditions that are required to initiate the alarm are checked. The first condition that is satisfied initiates the alarm; other conditions are no longer checked. The braking time for the first condition that is satisfied is displayed in the alarm.

When switching over the dynamic response level (e.g. in the part program), if other values of the axis dynamic response (VELO, ACCEL, JERK) are accessed, then the conditions to initiate Alarm 22001 no longer exist. For an NC start (NCSTARTCLEAR), the alarm is then automatically hidden. A reset (CANCELCLEAR) is required to facilitate a new alarm output.

5.5.1.3 Safe Stop 2 Extended Stop and Retract (SS2ESR)

> ⚠ **WARNING**
>
> **Unexpected axis motion**
>
> When function "SS2ESR" is active, during the delay time (p9554) the speed follows the setpoint issued from the higher-level control system. As a consequence, unexpected axis motion is possible, which can lead to severe injury and death.
>
> - Prevent persons from entering the danger zone of the machine or system during the delay time (p9554), for example, by keeping protective devices closed and interlocked.

In principle, Safe Stop 2 Extended Stop and Retract (SS2ESR) functions in exactly the same way as SS2 described in the previous sections. Note, however, the following differences:

Select SS2ESR

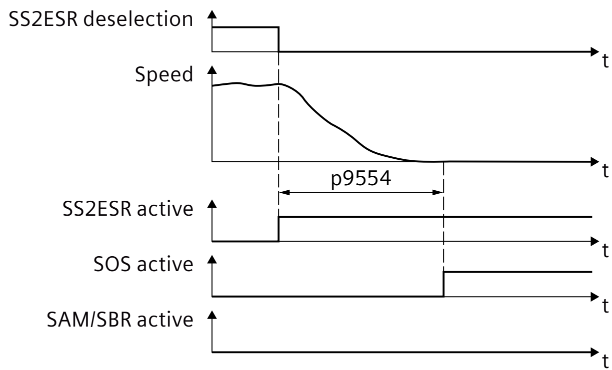


Figure 5-10 Selecting function SS2ESR

Differences between "Safe Stop 2 with OFF3" and SS2ESR

- If SS2ESR with external stop is selected, the drive does not brake the motor automatically, but instead, follows the defined speed setpoint: This can also result in fast retraction motion.
- During the delay time p9554, the brake ramp (SBR) and the acceleration (SAM) are not monitored, and there is no standstill detection.
- SOS becomes active after delay time p9554 has expired. If function SS2ESR is active, the higher-level control system must define the speed setpoint such that the motor is stopped no later than after the delay time p9554 has expired.
- To enable SS2ESR, set p9501.4 = 1.
- PROFIsafe control word S_STW2.29 selects function "SS2ESR". PROFIsafe S_STW2.29 is contained in telegrams 31, 901, 902 and 903.
- PROFIsafe status word S_ZSW2.27 indicates whether function "SS2ESR" is active. PROFIsafe status word S_ZSW2.27 is contained in telegrams 31, 901, 902 and 903. The associated diagnostics parameter is r9722.27. In the "Safety Info Channel," status word S_ZSW3B.12 indicates whether the "SS2ESR" function is active. The associated diagnostics parameter is r10234.12.
- In addition, in the "Safety Info Channel", status word S_ZSW1B.14 = 1 is set. This bit corresponds to diagnostic parameter r9734.14.
- You can use p0890[1] to interconnect to an ESR integrated in the drive.
- SS2ESR has no effect on the "Setpoint speed limit effective" (r9733[0...2]). If SS2ESR is enabled in p9501.4, then a STOP E also has no effect on r9733[0...2].

Deselecting SS2ESR while SS2ESR is active

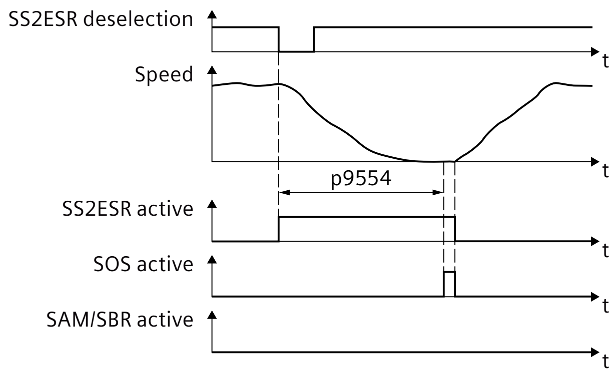


Figure 5-11 Deselecting SS2ESR while SS2ESR is active

After the function has been selected, the delay time starts to elapse - even if the function is deselected during this time. In this case, after the delay time has expired, the "SOS" function is briefly active. Afterwards, it is permissible that the drive accelerates the motor back to the speed setpoint.

Interrupting active SS2ESR with SS1 and SS2

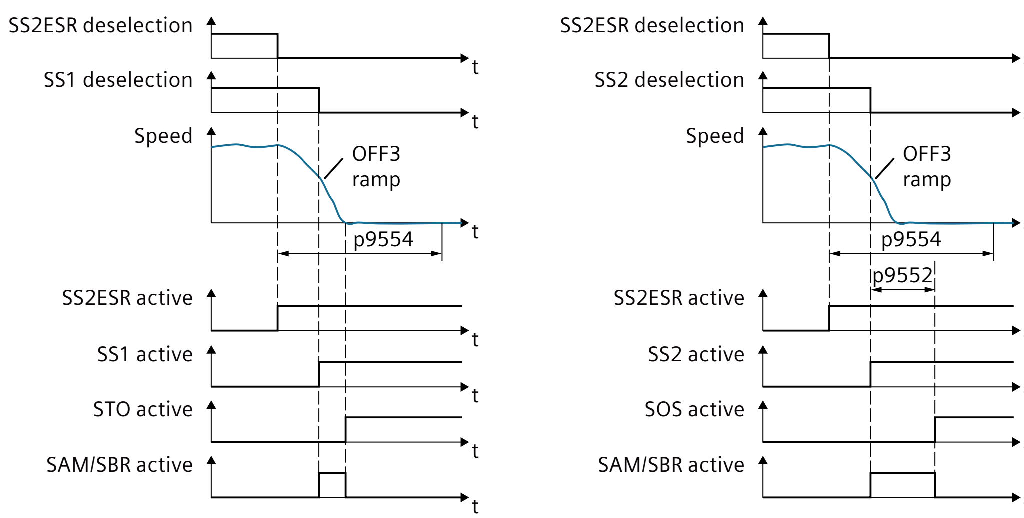


Figure 5-12 Interrupting function "SS2ESR" by functions "SS1" (shown at the left) and "SS2" (shown at the right)

When selecting SS1, the drive brakes the motor along the OFF3 ramp and monitors the speed using function "SAM/SBR". Function "STO" becomes active when the motor is at a standstill.

When selecting SS2, the drive also brakes the motor along the OFF3 ramp and monitors the speed using the "SAM" function. Function "SOS" becomes active after time p9552.

5.5.1.4 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2819 SI Extended Functions - SS1, SS2, SOS, internal STOP B, C, D, F

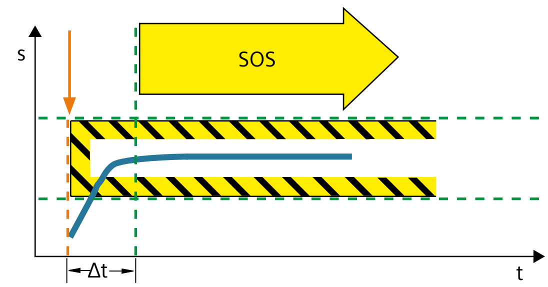
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p1135[0...n] OFF3 ramp-down time
- p9501 SI Motion enable safety functions (Control Unit)
- p9530 SI Motion standstill tolerance (Control Unit)
- p9548 SI Motion SAM actual speed tolerance (Control Unit)
- p9552 SI Motion transition time STOP C to SOS (SBH) (Control Unit)[1)]
- p9553 SI Motion transition time STOP D to SOS (SBH) (Control Unit)
- p9554 SI Motion transition time STOP E to SOS (SBH) (Control Unit)
- r9722.0...15 CO/BO: SI Motion drive-integrated status signals

[1)] STOP C corresponds to SS2.

5.6 SOS

Definition according to EN 61800-5-2:
"The SOS function is used to safely monitor the standstill position of a drive."



Example of how the function can be used

Example	Possible solution
A protective door must only be opened if a motor is in the safe standstill state.	• Select SOS • A higher-level controller brakes the axis (e.g. position-controlled) down to standstill within the configured time between the selection of SOS and when it becomes active. • Standstill is then safely monitored via the SOS function.

5.6.1 Safe Operating Stop (SOS)

The protected machine areas can be entered without having to shut down the machine as long as SOS is active.

After SOS has been selected it becomes active after the parameterizable delay time has expired. The drive must be braked to standstill within this delay time (e.g. by the controller).

Drive stopping is monitored using an SOS tolerance window. When this function is activated, the current actual position is saved as a comparative position, until SOS is deselected again. Any delay time is cleared after SOS is deselected and the drive can be immediately moved.

The drive is stopped with SS1 when the standstill tolerance window is violated.

Note

Contrary to SS1 and SS2, SOS does not automatically brake the drive

The control still enters the setpoint.

This means that in the user program of the control system, the system must respond to the "SOS selected" bit so that the control system brings the drive to a standstill within the delay time.

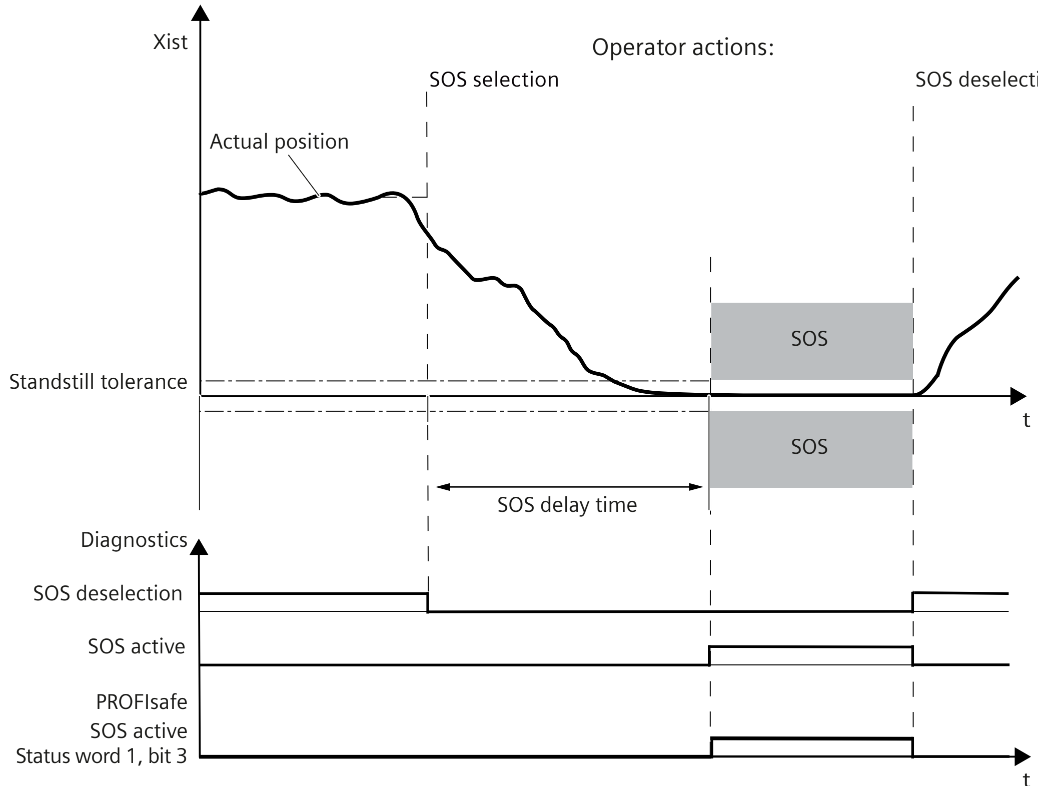


Figure 5-13 Standstill tolerance

5.6.2 Details and parameterization

> **WARNING**
>
> **Drive can be forced out of the SOS position by mechanical forces**
>
> A drive in position control can be forced out of the Safe Operating Stop (SOS, stop Category 2 according to 60204-1) position by mechanical forces that are greater than the maximum torque of the drive. This unexpected drive motion then initiates a Category 1 stop function according to EN 60204-1. The alarms for SS1 and STO must be carefully observed. This unexpected drive motion can result in death and serious injury.
>
> - To rule out any unexpected motion, use a brake with safe monitoring (see SBC (Page 121)).

This function serves for failsafe monitoring of the standstill position of a drive.

- Drive stopping is monitored using an SOS tolerance window (p9530).
- Effect on "Setpoint speed limit effective" (r9733[0...2]):
  If SOS is selected, setpoint 0 is specified in r9733[0...2].

Note

Size of the tolerance window

The size of the tolerance window should be slightly above the standard standstill monitoring limit, otherwise the standard monitoring functions will no longer be effective.

Parameter r9731 indicates the safe position accuracy (load side) that can be achieved as a maximum, based on the acquisition of the actual value for the safe motion monitoring functions.

STOP B is the stop response after the standstill tolerance window has been violated.

The "SOS" function becomes active in the following cases:

- After SOS is selected and the delay time in p9551 has elapsed
  The drive must be braked to standstill within this delay time (e.g. by the controller).
- As a consequence of SS2, SS2E or SS2ESR
- As a consequence of STOP C (corresponds to selection of SS2)
- As a consequence of STOP D (corresponds to selection of SOS)
- As a consequence of STOP E (corresponds to selecting SOS with additional activation of the standard "Extended stop and retract (ESR)" function)

Responses

- **Standstill tolerance violated in p9530**
  - STOP B with subsequent STOP A
  - Safety message C01707
- **System error**
  - STOP F
  - Safety message C01711

5.6.2.1 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

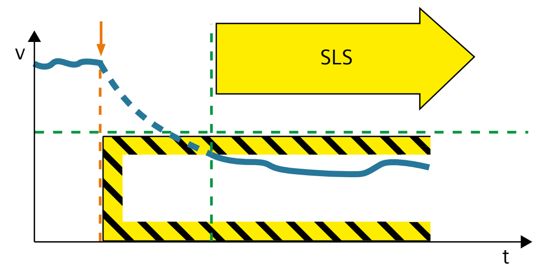
- 2819 SI Extended Functions - SS1, SS2, SOS, internal STOP B, C, D, F

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9501.23 Enable deactivation of SOS/SLS during an external STOP A
- p9530 SI Motion standstill tolerance (Control Unit)
- p9551 SI Motion SLS(SG) switchover/SOS(SBH) delay time (CU)
- p9567 Switchover speed to SOS/SLS
- p9569 Transition time to SOS after standstill
- r9722.0...31 CO/BO: SI Motion drive-integrated status signals
- r9731 SI Motion safe positioning accuracy

5.7 SLS

Definition according to EN 61800-5-2:
"The "SLS" function prevents the motor from exceeding the defined speed limit."



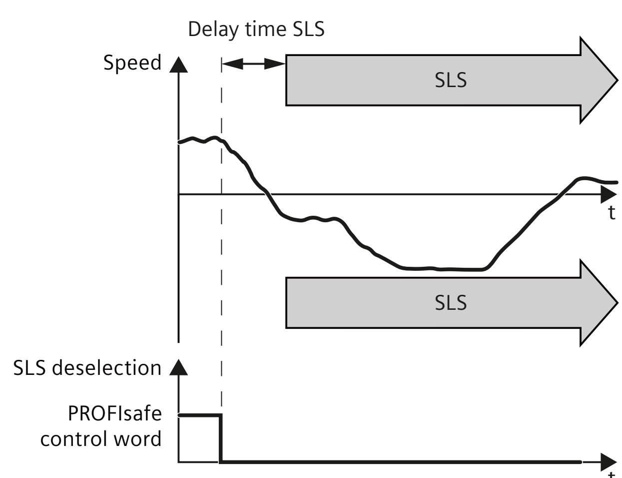
Examples of how the function can be used

Example	Possible solution
After opening a protective door, the machine operator must enter the machine and in the hazardous zone, operate a horizontal conveyor belt running at a slow speed using an acknowledgment button.	• Select SLS in the converter using a failsafe input or PROFIsafe . • The converter limits and monitors the velocity of the horizontal conveyor.
A spindle drive, depending on the selection of the cutting tool, must not exceed a specific maximum velocity.	• Select SLS and the corresponding SLSlevel in the converter via PROFIsafe.

How does SLS function in detail?

Overview

1. The inverter recognizes the selection of SLS via a failsafe input or via the PROFIsafe safe communication.
2. SLS allows a motor to reduce its possibly inadmissibly high speed within a defined time.
3. SLS monitors the absolute value of the actual velocity.
   The SLS setpoint limit can be transferred to the F-PLC, where the speed setpoint can be limited.
   In addition, you can configure the setpoint limit provided by SLS as maximum speed in the ramp-function generator. In this case, SLS limits the speed setpoint.



Note

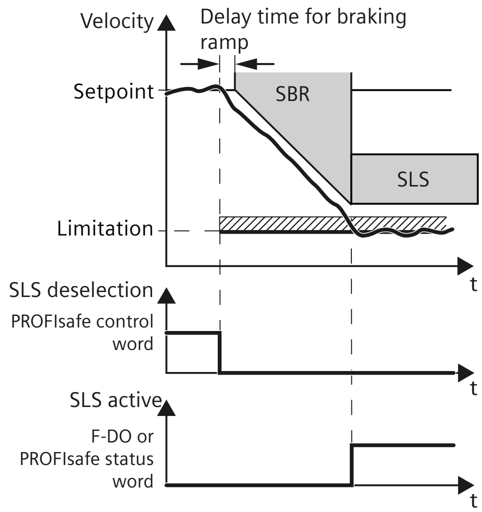
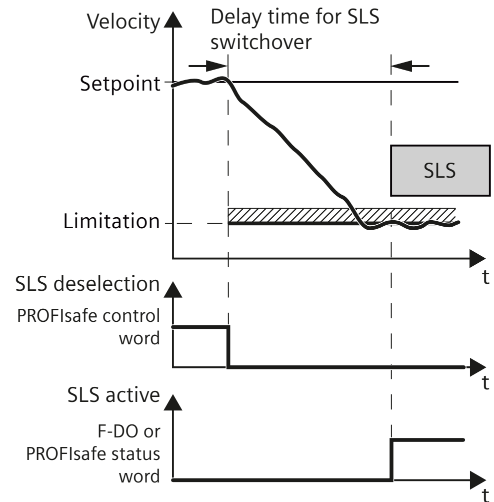
SLS without selection

As an alternative to controlling via terminals and/or PROFIsafe, there is also the option to parameterize the "SLS" function without selection. In this case, the "SLS" function is permanently active after POWER ON. You can find details about this in Section "Safely-Limited Speed without selection (Page 154)".

Selecting SLS when the motor is switched on

As soon as the converter detects the selection of SLS via a failsafe input or via PROFIsafe safe communication, the following happens:

- To avoid a limit value being violated, the setpoint limit can be transferred to the F-PLC This can then limit the velocity setpoint.
- If the speed setpoint limitation is interconnected to the ramp-function generator, the converter limits the speed to a value below the SLS monitoring.
- For SLS without encoder, you can select whether or not the converter monitors motor braking using the function "SBR (Safe Brake Ramp)" or "SAM (Safe Acceleration Monitor)" . For SLS with encoder, function "SBR" cannot be selected.

<table>
<tr><th>With braking ramp monitoring[1)]
(only without encoder)</th><th>Without braking ramp monitoring
(with or without encoder)</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>After the adjustable "delay time for the braking ramp", using the "SBR (Safe Brake Ramp)" function, the converter monitors whether the velocity decreases.
The converter switches from SBR to SLS as soon as one of the following two conditions is fulfilled:
The SBR monitoring ramp has reached the value of the SLS monitoring.
This case is shown in the diagram above.
After the actual velocity has reached the value of the SLS monitoring threshold, the system again waits for the "delay time for braking ramp" until SLS becomes active.</td><td>The converter monitors the load velocity after the "delay time for SLS switchover" has expired.</td></tr>
<tr><td>Advantages:
Already when braking, the converter detects as to whether the load velocity decreases too slowly.
The feedback signal "SLS active" generally comes earlier than without acceleration monitoring.</td><td>Advantage:
Commissioning is simplified, because instead of the subfunction SBR or SAM of the alternative brake ramp monitoring, you only have to set the delay time.</td></tr>
</table>

1) The automatic reduction of the speed only takes effect when the ramp-function generator is interconnected to the speed setpoint limitation.

Selecting SLS at low velocities

If the motor velocity when selecting SLS is less than the SLSlimit, then the drive responds as follows:

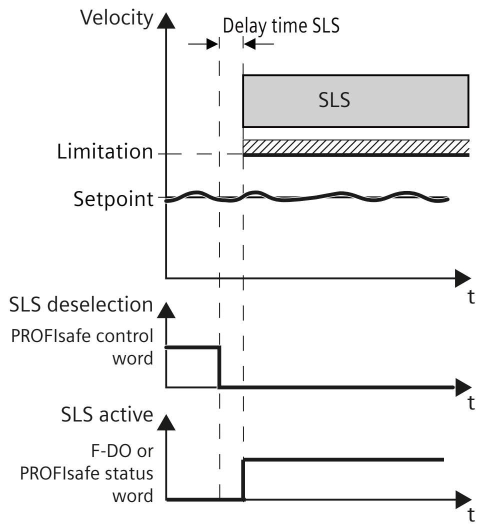


Figure 5-14 Selecting SLS at low velocities

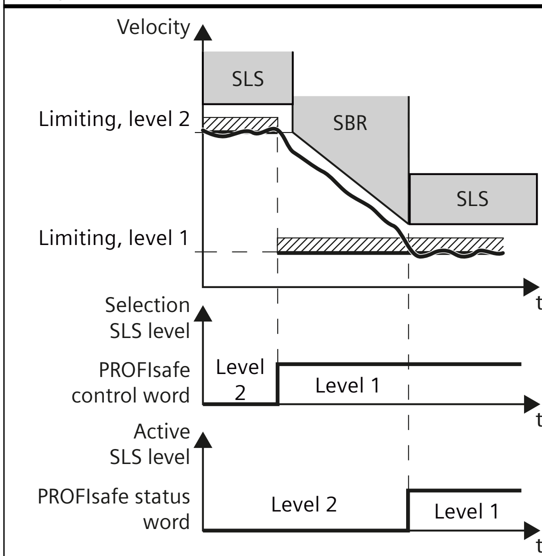
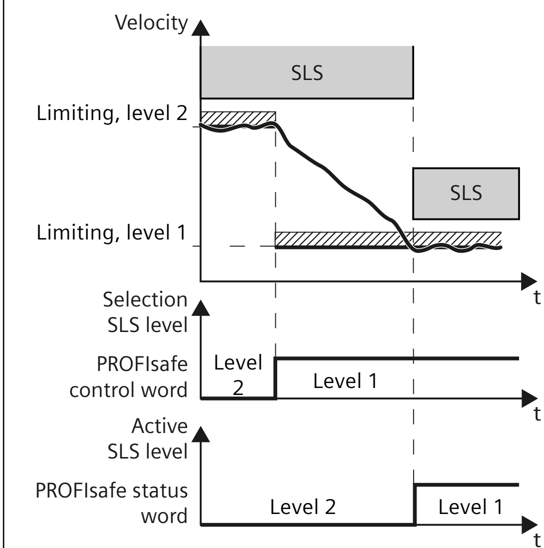
Deselecting SLS

If the higher-level controller deselects SLS , then the converter deactivates limiting and monitoring.

Switching over the monitoring limits

When SLS is active, you can switchover between 4 different speed levels. An exception is "SLS without selection": In this case, there is only one limit.

Switching to a lower speed level

<table>
<tr><th>With braking ramp monitoring[1)]
(only without encoder)</th><th>Without braking ramp monitoring
(with or without encoder)</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>

- Once the "delay time for braking ramp" has elapsed, the converter monitors the motor velocity using the function SBR (Safe Brake Ramp).
- The converter switches over from SBR monitoring to level 2 of SLS monitoring as soon as one of the following conditions is fulfilled:
  - The SBR monitoring ramp has reached the value of the SLS monitoring.
This case is shown in the diagram above.
  - The load velocity has decreased down to the value SLS monitoring and the "delay time for braking ramp" has expired.

</td><td>

- The converter monitors the velocity with the lower SLS level after the "delay time for SLS changeover" has expired (this is the same delay time that applies after selecting the function SLS).

</td></tr>
</table>

1) The automatic reduction of the speed only takes effect when the ramp-function generator is interconnected to the speed setpoint limitation.

Switching to a higher speed level

If you switch over from a lower to a higher speed level, the converter immediately monitors the actual velocity against the higher velocity.

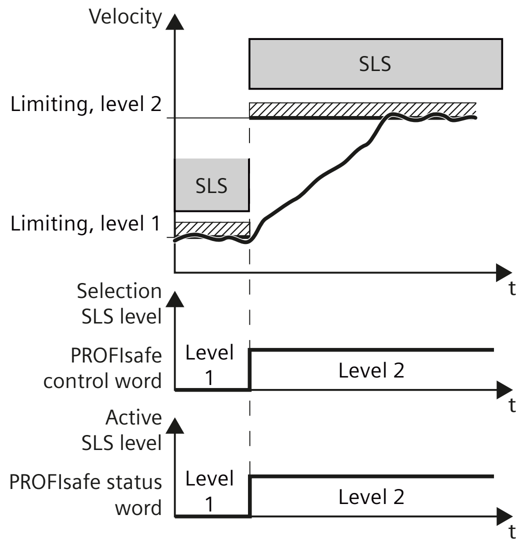


Figure 5-15 Switching to a higher speed level

5.7.1 Details and parameterization

The "Safely-Limited Speed" (SLS) function is used to protect a drive against unintentionally high speeds in both directions of rotation. This is achieved by monitoring the current drive speed up to a speed limit.

Safely-Limited Speed prevents a parameterized speed limit from being exceeded. Limits must be specified based on results of the risk analysis. Up to four different SLS speed limits can be parameterized using parameter p9531[0..3]; it is possible to switch between them even if the SLS is activated.

An override can also be added to SLS limit value 1. In operation, this override can be varied using a PROFIsafe telegram.

Note

Deviation of the displayed speed limit

The SLS speed limit displayed in r9714[2] can deviate slightly from the specified SLS speed limit. The reason for this is the internal resolution (r9732) of the speed values.

Note

Response in the event of a communication error

If p9580 ≠ 0 and SLS is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SLS response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9563[0...3] ≥ 10).

Note

Setpoint speed limit and SLS

- When parameterizing SLS, it also makes sense to configure the setpoint speed limiting. This is done in a higher-level controller that evaluates the Safety Info Channel, for example, or by wiring r9733[0/1] to the speed limits of the ramp-function generator (p1051/p1052).
- It does not make sense to use the positive and negative setpoint limiting for SLS in conjunction with standard telegram 105 and others: With this combination, the velocity setpoint of the standard telegram is only effective after the setpoint limiting.

5.7.1.1 Connection to the motion control in the NC

The following status bits or values from the SIC/SCC send data are linked to the NC so that for safety functions integrated in the drive, subsequent responses or alarms do not occur in the NC:

- SI Motion Safety Info Channel status word: S_ZSW1B (Page 415)
  - Bit 4 SLS_ACTIVE (SLS active)
  - Bit 6 SLS_SELECTED (SLS selected)
- Speed setpoint limit in 32-bit resolution with sign bit: S_V_LIMIT_B (Page 418)

If the SLS function is selected or is active, then the corresponding bits are set in S_ZSW1B. The currently selected velocity limit value of the SLS function integrated in the drive is then entered in S_V_LIMIT_B.

After rescaling, S_V_LIMIT_B is multiplied with the value from MD36933 $MA_SAFE_DES_VELO_LIMIT[0...3], and is transferred to the motion control in the NC as setpoint speed limit.

If a value of 0% or 100% is entered in MD36933, then the value from S_V_LIMIT_B is transferred as speed setpoint limit.

When SOS or a STOP A to F is selected, then S_V_LIMIT_B contains a setpoint of 0. When the "SLS" or "SOS" function is not selected in the drive, then the velocity/speed limit value in S_V_LIMIT_B corresponds to the value for the maximum velocity/maximum speed (Vmax).

5.7.1.2 Safely Limited Speed (SLS)

Features

- When SLS is selected, the monitoring only takes effect after the configured delay time has expired (p9551). Within this time, the actual speed must be below the (selected) limit. The delay time is not effective when SLS is deselected.
- After switching to a lower limit value (p9531), the actual speed of the drive must have dropped below the new limit within the delay time (p9551). The existing limit remains active during the delay time. The lower limit value becomes active after the delay time expires. This also applies to a reduction of the limit value via PROFIsafe.
- After the delay time has elapsed, if the actual speed of the drive is higher than the new Safely-Limited Speed limit then a message is generated with the parameterized stop response.

- The stop response (STOP A, STOP B, STOP C, STOP D or STOP E) is parameterized with p9563.
- During changeover to a higher limit value, the delay time is not active and the high limit value becomes immediately active. This also applies to increasing the limit value via PROFIsafe.
- 4 parameterizable limit values p9531[0...3]
- The first limit value can be entered via PROFIsafe telegrams 901, 902 and 903 (for p9501.24 = 1)
- In parameter p9533 enter the weighting factor to determine the setpoint limit from the selected actual speed limit in percent. The active limit value is evaluated using this factor, and is provided as setpoint limit in r9733.
  - r9733[0] = p9531[x] x p9533 (converted from the load to the motor side)
  - r9733[1] = - p9531[x] x p9533 (converted from the load to the motor side)
    [x] = selected SLS stage

  Conversion factor from the motor to the load side:
  - Motor type = rotary and axis type = linear: p9522/(p9521 × p9520)
  - Otherwise: p9522/p9521
- Limit value
  - r9733[0] = p9531[x] x p9533; x = selected SLS limit value
  - r9733[1] = -p9531[x] x p9533; x = selected SLS limit value

  r9733 is used, for example, for transferring values to a higher-level controller, which can then, for example, adjust traversing speeds to the SLS levels or at the setpoint channel (p1051). r9733 is a part of the Safety Info Channel (SIC).
- The currently monitored limit value is displayed in parameter r9714[2].

Changeover of SLS limit values

The changeover is executed binary-coded via 2 F-DIs or 2 PROFIsafe control bits. The speed selection status can be checked using parameters r9720.9/r9720.10. Parameters r9722.9 and r9722.10 indicate the actual speed limit, bit r9722.4 must carry a "1" signal.

Table 5-1 Changeover of speed limits:

F-DI for bit 1 (r9720.10)	F-DI for bit 0 (r9720.9)	Speed limit	SLS level
0	0	p9531**[0]**	1
0	1	p9531**[1]**	2
1	0	p9531**[2]**	3
1	1	p9531**[3]**	4

Excessively high speed during incorrect control of the Safely-Limited Speed limits via F-DI

For all control options except PROFIsafe, limit SLS1 is activated after 2 discrepancy errors that have not been acknowledged. This means that for the 2 F-DIs for selecting the velocity levels, the value 0 is the "safe state" (failsafe value).

- Therefore parametrize the SLS limits in ascending order, i.e. with limit SLS1 as the lowest speed and limit SLS4 as the highest speed.

Responses

Speed limit value exceeded:

- Configured subsequent stop STOP A/B/C/D/E via p9563
- Safety message C01714

System fault:

- STOP F
- Safety message C01711

Transferring the first limit value via SIEMENS telegram 901, 902 or 903

You have the option of influencing the first SLS limit value via PROFIsafe:

- The transfer of the first SLS limit value via PROFIsafe is active if the speed level 1 in the PROFIsafe telegram is selected and the bit "Enable transfer SLS (SG) limit via PROFIsafe" (p9501.24) is set.
- S_SLS_LIMIT_A has the value range 1 ... 32767; the following applies:
  - 32767 ≙ 100 % of the 1st SLS level
  - The actually monitored limit value is calculated as follows:
    SLS limit value = (S_SLS_LIMIT_A/32767) × p9531[0]
- Also in this case, speed levels 2, 3 and 4 can be parameterized and selected.
- In operation, the selected delay time cannot be changed. If you require various delay times in your application, then you must realize this using a time-delayed transfer of the SLS limit value using the F-PLC.
- If an incorrect SLS limit value is transferred, then the converter responds with the stop response of speed level 1 parameterized in p9563.

5.7.1.3 Safely Limited Speed without encoder

Functions

2 different encoderless Safely-Limited Speed monitoring functions can be set with parameter p9506:

- p9506 = 3: Safe monitoring of acceleration (SAM) / delay time
  The function is identical to "Safely-Limited Speed with encoder" which was described in the previous section.
- p9506 = 1: Safe brake ramp monitoring (SBR)

Note

Defaults

- When commissioning, also note the description provided in the SINAMICS Safety Integrated Function Manual, Chapter "Default settings for commissioning Safety Integrated Functions without encoder".
- Information about setting the SBR monitoring function can be found in Chapter "SBR (Page 164)".

Monitoring the brake ramp

- If the speed setpoint limitation (r9733) was connected to the setpoint channel (p1051/ p1052) and then SLS was selected – or if you change over to a lower SLS level – the motor is decelerated from the actual speed to below the value defined with r9733 along the OFF3 ramp. In this case, the drive may no longer follow the setpoint of the higher-level motion controller.
- Parameter p9582 is used to set the delay time for the braking ramp monitoring.
- Monitoring of the brake ramp is activated once the delay time in p9582 has elapsed. If the actual speed of the drive violates the brake ramp (SBR) during braking, safety message C01706 is output and the drive is stopped with STOP A.
- The newly selected SLS limit value is also taken over as the new limit speed, if either
  - The SBR ramp has reached the new SLS limit value, or
  - The actual speed of the drive was below the new SLS limit value for at least the time set in p9582.
- The "Safely-Limited Speed without encoder" function then monitors whether the actual speed remains below the newly selected SLS limit value.
- The parameterized stop response (p9563[x]) is initiated if the SLS limit value is exceeded.

Configuring the limits

- The speed limits for Safely-Limited Speed without encoder are configured in exactly the same way as described for Safely-Limited Speed with encoder.
- Only STOP A and STOP B may be configured as stop responses for "Safely-Limited Speed" (SLS) without encoder.

Restart after OFF2/STO

If the drive has been switched off via STO, the following steps need to be carried out before a restart can be performed:

1. Case	• State after switching on	
		• SLS selected
		• STO selected
		• Pulse suppression active
	• Deselect STO	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
2. Case	• Situation	
		• Traversing to standstill with SLS selected
		• OFF1 is initiated, pulse cancellation becomes active (internal selection STO)
	• Select STO	
	• Deselect STO STO activated internally via pulse suppression: This activation must be undone by selection/deselection.	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
3. Case	• Situation	
		• Traversing to standstill with SLS selected
		• OFF1 is initiated, pulse cancellation becomes active (internal selection STO)
	• Deselect SLS STO activated internally via pulse suppression: This activation must be undone by selecting/deselecting SLS.	
	• Select SLS The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
4. Case	• Situation	
		• All Safety Integrated functions are deselected.
	• After this the drive enable must be given by a positive edge at OFF1.	
	• In this case, the motor is not started safely.	

5.7.1.4 Safely-Limited Speed without selection

Differences between Safely-Limited Speed with and without selection

- As an alternative to controlling via terminals and/or PROFIsafe, there is also the option to parameterize the "SLS" function without selection.
- The function "SLS without selection" is selected with p9512.4 = 1.
- For "SLS without selection", only one SLS limit value can be parameterized (p9531[0]).
- The stop response is parameterized with p9563[0].
- For Safely-Limited Speed without selection there is no delay time. The function is always active (with encoder), or it becomes active when switching on (without encoder).

Switching the motor on and off (without encoder)

The time response and diagnostic options are as follows in this SLS version:

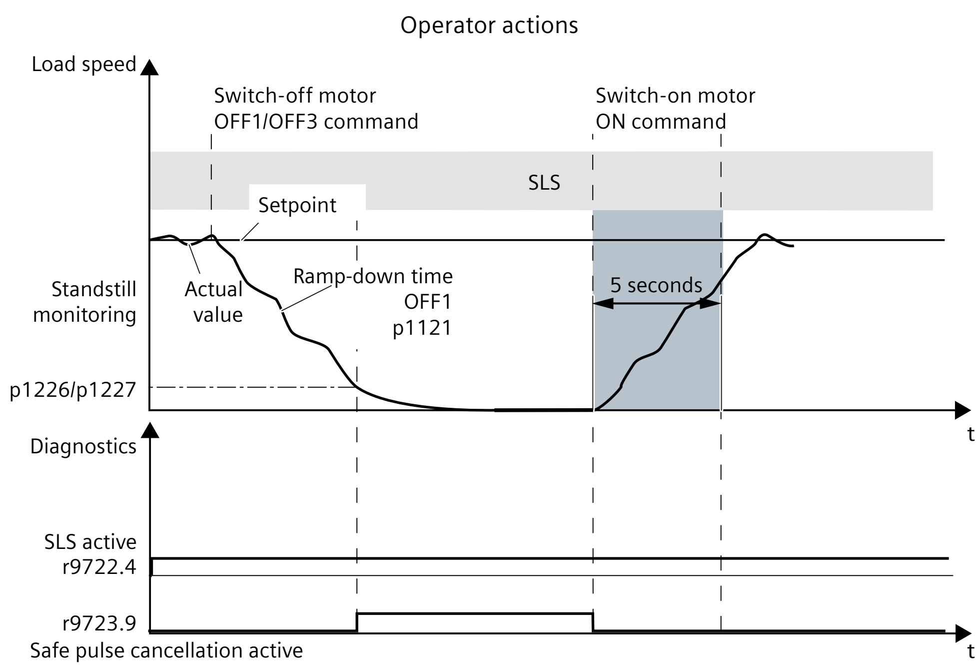


Figure 5-16 Time response of SLS without selection (example: Switching the motor on and off (without encoder))

"SLS without selection" behaves as follows when switching off and switching on again:

- After switch-off, the motor behaves in accordance with the canceled signal (OFF1, OFF2 or OFF3).
- The "safe pulse cancellation" becomes active after the standstill limit is undershot. If a brake has been parameterized, it is also closed.

- After the ON command, the converter cancels the "safe pulse cancellation" state and the start procedure is initiated.
- If the minimum current has not been reached after 5 s, the converter returns into the "safe pulse suppression" state and initiates alarm C01711.

5.7.1.5 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

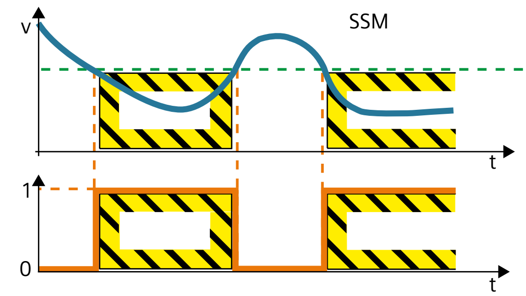
- 2820 SI Extended Functions - SLS (Safely-Limited Speed)

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501.0 SI Motion enable safety functions (Control Unit)
- p9512 Select SI Motion safety functions without selection (CU)
- p9531[0...3] SI Motion SLS (SG) limits (Control Unit)
- p9551 SI Motion SLS(SG) switchover/SOS(SBH) delay time (CU)
- p9563[0...3] SI Motion SLS (SG)-specific stop response (Control Unit)
- p9580 SI Motion STO delay bus failure (Control Unit)
- p9581 SI Motion braking ramp reference value (Control Unit)
- p9582 SI Motion braking ramp delay time (Control Unit)
- p9583 SI Motion braking ramp monitoring time (Control Unit)
- p9601 SI enable functions integrated in the drive (Control Unit)
- r9707[0...2] CO: SI Motion diagnostics actual position value GX_XIST1
- r9714[0...2] CO: SI Motion diagnostics velocity
- r9720.0...27 CO/BO: SI Motion drive-integrated control signals
- r9721.0...15 CO/BO: SI Motion status signals (Control Unit)
- r9722.0...31 CO/BO: SI Motion drive-integrated status signals (Control Unit)

5.8 SSM

Definition according to EN 61800-5-2:
"The "SSM" function supplies a safe output signal to indicate whether the motor speed is below a specified limit value."



Example of how the function can be used

Example	Possible solution
A centrifuge may only be filled below a velocity defined by the user.	• SSM is active through the configuration of the Safety Integrated Extended Functions. • The converter safely monitors the centrifuge speed and enables the process to advance to the next step using the "Status SSM" status bit.

Note

SSM is a pure signaling function

Contrary to other safety functions integrated in the drive, a violation of the SSM limit does not result in a drive-based stop response.

5.8.1 Details and parameterization

The "Safe Speed Monitor" (SSM) function provides a reliable method for detecting when a speed limit has been fallen below in both directions of rotation, e.g. for zero speed detection. A failsafe output signal is available for further processing.

Features

- Safe monitoring of the specified speed limit
- Parameterizable hysteresis
- Adjustable filter time (PT1 filter)

- Safe output signal
- No stop response

Note

Unexpected response of STOP F for SSM

A STOP F is indicated by safety message C01711. STOP F only results in the subsequent response STOP B / STOP A if one of the safety functions is active. If only the SSM function without hysteresis (that is, p9501.16 = 0) is active, a STOP F cross-checking error does not result in a STOP B / STOP A follow-up response.

- The monitoring function is considered to be active as soon as "SSM with hysteresis" is activated.

How does SSM function in detail?

Requirements

The safety function "SSM" cannot be selected or deselected using external control signals. SSM is active if, for the drive involved, the following settings have been made:

- Extended Functions are selected as safety function scope.
- The velocity limit for SSM is parameterized > 0.

Evaluating the speed

The converter compares the load speed with the speed limit and signals if the limit value is undershot to the high-level control.

Parameterizable hysteresis

The parameterizable hysteresis ensures that the SSM output signal does not jump between the values "0" and "1" in the limit range.

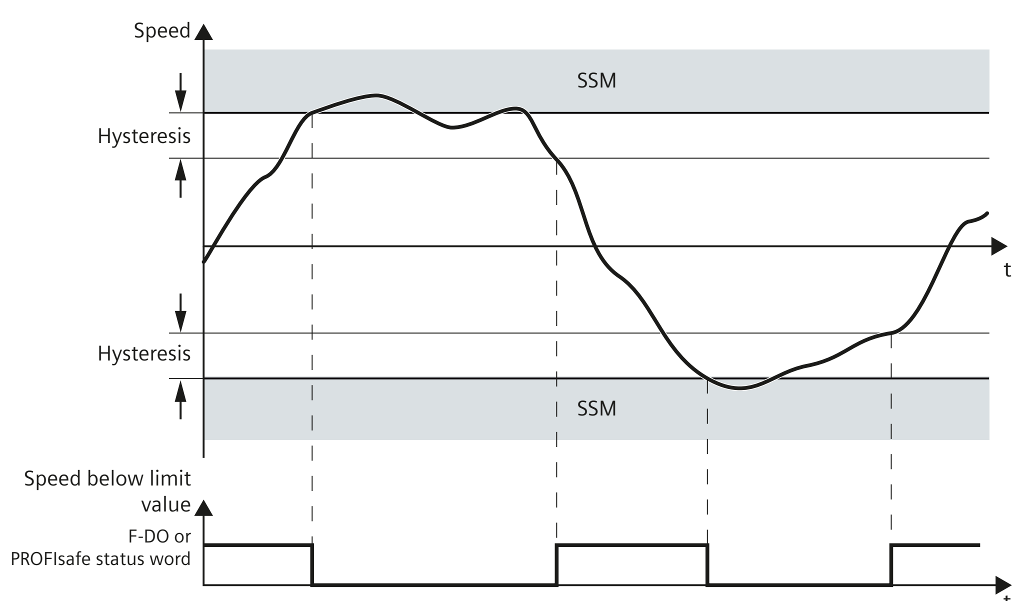


Figure 5-17 Time response of the safety function SSM (Safe Speed Monitor)

5.8.1.1 Signal characteristic (with encoder)

Functional features of "Safe Speed Monitor" with encoder

A hysteresis can be configured for the SSM function using (p9547). In this way, a more stable signal characteristic of SSM can be achieved at velocities close to the velocity limit (p9546).

The following diagram shows the characteristic of the safe output signal SSM when the hysteresis is active:

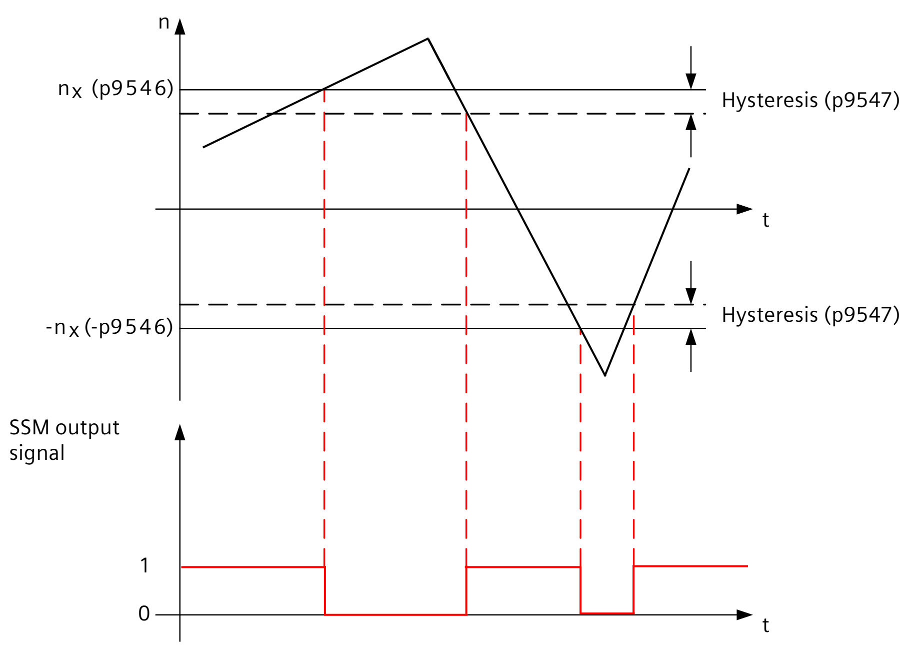


Figure 5-18 Safe output signal for SSM with hysteresis

5.8.1.2 Differences in operation without encoder

In operation, safety function SSM makes a distinction without encoder as a result of the following features:

- Due to the less precise speed sensing, "Safe Speed Monitor without encoder" requires a higher hysteresis (p9547) and, where applicable, a filter time (p9545) compared with the function with encoder.
- For Safe Speed Monitor without encoder, after pulse suppression the drive is unable to determine the current speed. For this operating state, the additional setting "Feedback signal SSM for pulse inhibit" is available (see below)

Note

Setting of the OFF1 or OFF3 ramp-down time

If the OFF1 or OFF3 ramp-down time is too short or the difference between the SSM limit speed and the shutdown speed is too small, the "speed below limit value" signal may not change to 1, because no actual speed value could be determined below the SSM limit before pulse suppression occurred. In this case, the OFF1 or OFF3 ramp-down time or the margin between SSM speed limit and shutdown speed should be increased.

5.8.1.3 Signal characteristic (without encoder)

Procedure when the "Feedback signal SSM for pulse inhibit" setting is activated

The following diagram shows the signal characteristic if property "Feedback signal SSM for pulse inhibit" is activated. (p9509.0 = 0)

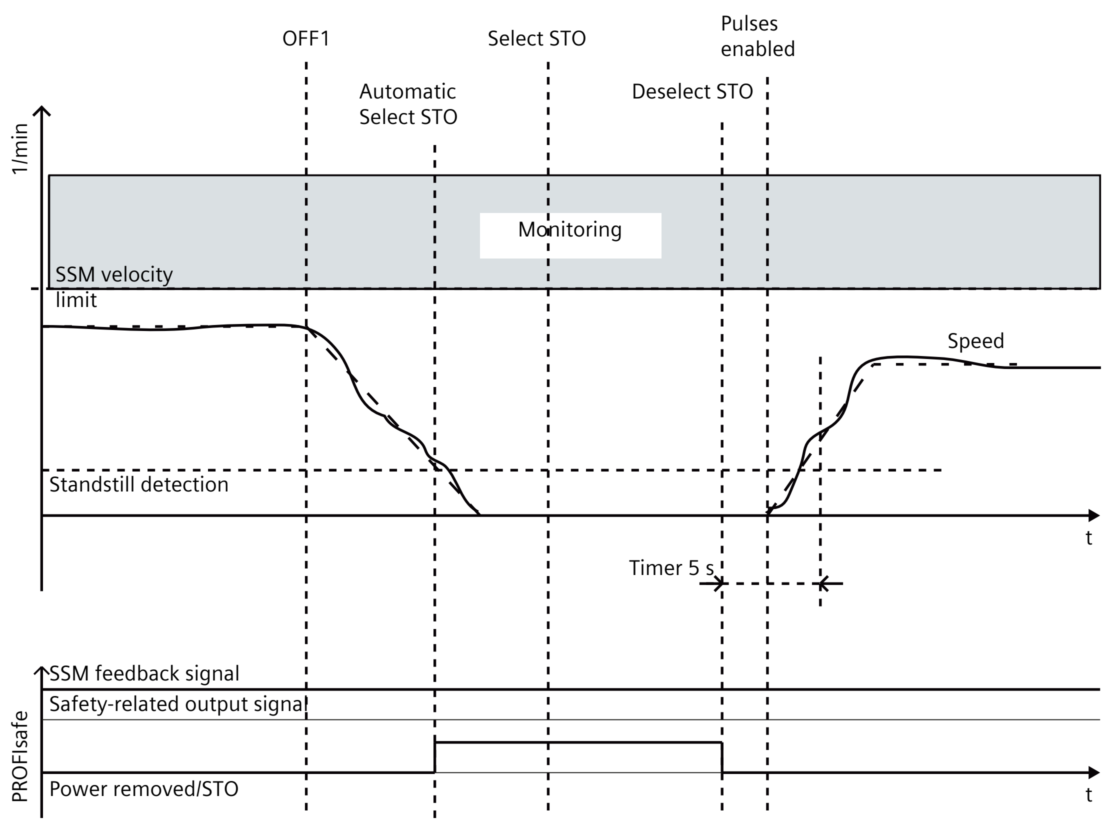


Figure 5-19 Flow chart: SSM without encoder with feedback signal SSM for pulse inhibit (p9509.0 = 0)

The speed remains below the speed limit throughout the entire monitoring period. This is the reason that status signal "SSM (Speed below limit value)" goes to 1 (r9722.15 = 1). After the command for pulse suppression, the motor speed drops. The internal STO is set when the speed drops below the zero speed detection level.

In this case, the SSM status signal remains HIGH; it is frozen. The drive cannot accelerate again, due to the internal STO selection.

To restart the motor safely, the STO must be selected manually and deselected once more. After the STO has been deselected, a 5 second time window is opened. If the pulse enable takes place within this time window, the motor starts. If the pulse enable does not take place within this 5 second time window, the internal STO becomes active once more.

Procedure when the "Feedback signal SSM for pulse inhibit" setting is deactivated

If property "Feedback signal SSM for pulse inhibit" is deactivated (p9509.0 = 1), then SSM monitoring is exited after pulse cancellation. Status signal "SSM (Speed below limit value)" goes to 0 (r9722.15 = 0). The SSM monitoring is only reactivated after a new pulse enable. In this case, STO must not be selected and deselected to start the drive.

Restart after pulse cancellation for p9509.0 = 0

If the drive pulses have been suppressed using OFF1/OFF2/STO, the following steps must be carried out for a restart:

1. Case	• State after switching on	
		• SSM active
		• STO selected
		• Pulse suppression active
	• Deselect STO	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
2. Case	• Situation	
		• SSM active
		• Motor turning
		• OFF1 triggered, pulses are suppressed
	• Select STO	
	• Deselect STO STO activated internally via pulse suppression: This activation must be undone by selecting/deselecting STO.	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	

5.8.1.4 Function diagrams and parameters

Function diagrams

- 2823 SI Extended Functions - SSM (Safe Speed Monitor)
- 2840 SI Extended Functions - SI Motion drive-integrated control signals/status signals

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9501.16[1)] Enable SSM (n < nx) hysteresis and filtering
  Screen form: "SSM with hysteresis"
- p9506 SI Motion function specification (Control Unit)
- p9509 SI Motion behavior during pulse suppression (Control Unit)
- p9509.1[1)] SSM during pulse cancellation and with no encoder
  Screen form: "Feedback signal SSM active for pulse inhibit"
- p9545[1)] SI Motion SSM (SGA n < nx) filter time (Control Unit)
  Screen form: "Filter time"
- p9546[1)] SI Motion SSM (SGA n < nx) speed limit (CU)
  Screen form: "Velocity limit"
- p9547[1)] SI Motion SSM (SGA n < nx) speed hysteresis n_x (CU)
  Screen form: "Hysteresis"
- r9722.0...14 CO/BO: SI Motion drive-integrated status signals
- r9722.15[1)] SSM (speed below limit value)
  Screen form: "Velocity below limit value SSM"

[1)] You can parameterize this parameter using the additional screen form mentioned.

All other parameters that have not been specifically marked, are either part of the general NC and drive-specific settings (Page 265), or can only be configured using the parameter list. The parameter list can be accessed in the function-specific screen forms of the safety functions by pressing softkey "Parameter list".

Additional information

You can find a complete description of all SINAMICS parameters - as well as the associated function diagrams - in the SINAMICS S120/S150 List Manual.

5.9 SAM

The "Safe Acceleration Monitor" (SAM) function is used to safety monitor braking along the OFF3 ramp. The function is active for SS1, SS2 or STOP B and STOP C.

Features

As long as the speed is less, the converter continuously adds the adjustable tolerance p9548 to the actual speed so that the monitoring tracks the speed. If the speed is temporarily higher, the monitoring remains at the last value. The converter reduces the monitoring threshold until the "Shutdown speed" has been reached.

SAM recognizes if the drive accelerates beyond the tolerance defined in p9548 during the ramp-down phase, and generates a STOP A. The monitoring function is activated for SS1 (or STOP B) and SS2 (or STOP C) and is deactivated after the speed drops below the value set in p9568.

Note

Relationship between SSM and SAM

If 0 is entered for p9568, the speed limit of the SSM function (p9546) is also used as minimum limit value for the SAM function (Safe Acceleration Monitoring). If the speed is below this limit, SAM no longer triggers a response from the drive.

In this case, the effects of Safe Acceleration Monitoring are therefore significantly restricted if a relatively high SSM velocity limit is set when using the SS1 and SS2 stop functions.

Note

No direct selection of SAM

SAM is part of the Safety Integrated Extended Functions SS1 and SS2 or STOP B and STOP C. SAM cannot be individually selected.

Calculating the SAM tolerance of the actual speed

- The following applies when parameterizing the SAM tolerance:
  - The maximum speed increase after SS1 or SS2 is triggered results from the effective acceleration (a) and the duration of the acceleration phase.
  - The duration of the acceleration phase is equivalent to one monitoring cycle (MC p9500) (delay from detecting an SS1 / SS2 until $n_{set} = 0$)
- Calculating the SAM tolerance:
  Actual speed for SAM = acceleration × acceleration duration
  The following setup rule is derived thereof:
  - For linear axes:
    SAM tolerance [mm/min] = a [m/s^2] x MC [s] x 1000 [mm/m] x 60 [s/min]
  - For rotary axes:
    SAM tolerance [rpm] = a [rev/s^2] x MC [s] x 60 [s/min]

- Recommendation
  The SAM tolerance value entered should be approx. 20% higher than the calculated value.
- You set the tolerance such that the "overshoot" is tolerated that necessarily occurs when standstill is reached after braking along the OFF3 ramp. However, it cannot be calculated as to just how high this is.

Note

First monitoring cycle

For SAM, in the first "SI Motion monitoring cycle" (p9500) a higher SAM tolerance is taken into account in order to compensate for possible settling operations without resulting in an incorrect initiation. The increase factor is calculated as follows:
SI Motion monitoring cycle (p9500) / SI Motion actual value acquisition cycle (p9511)

Example:
SI Motion monitoring cycle (p9500) = 12 ms
SI Motion actual value acquisition cycle (p9511) = 1 ms
SAM tolerance (p9548) = 300 rpm
Actual speed = 250
Rotary axis

In the first cycle after activation of the monitoring, the SAM limit value is therefore:

Actual speed + SAM tolerance · (12 ms/1 ms) =
250 rpm + 300 rpm · 12 =
approx. 3850 rpm

Responses

- **Speed limit violated (SAM):**
  - STOP A
  - Safety message C01706
- **System fault:**
  - STOP F with subsequent STOP A
  - Safety message C01711

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9546 SI Motion SSM (SGA n < nx) speed limit (CU)
- p9548 SI Motion SAM actual speed tolerance (Control Unit)
- p9568 SI Motion SAM speed limit (Control Unit)

5.10 SBR

The "Safe Brake Ramp (SBR)" function provides a safety-related method for monitoring the brake ramp. The "Safe Brake Ramp (SBR)" function is used to monitor braking with the functions "SS1 with/without encoder" and "SLS without encoder" as well as for STOP B / STOP C (for Safety Integrated with encoder). For SLS, the setpoint limiting of the Safety Integrated Functions (r9733) must be connected to the ramp-function generator (p1051/p1052).

Features

The motor is immediately braked along the OFF3 ramp as soon as SS1, SS2, or SLS is triggered. Monitoring of the brake ramp is activated once the delay time in p9582 has elapsed. Monitoring ensures that the motor does not exceed the set brake ramp (SBR) when braking. The safe monitoring of the brake ramp is deactivated

- For SS1:
  - As soon as the speed drops below the shutdown speed (p9560).

  Or:
  - As soon as the SS2 delay time (p9552) has elapsed.
- For SLS:
  - As soon as the set brake ramp has reached the new SLS level

  Or:
  - As soon as the actual speed drops below the newly selected SLS level and has remained there for the time parameterized in p9582.

Additional specific functions (e.g. STO, new SLS speed limit, etc.) are activated at this point, depending on the Safety Integrated Function used.

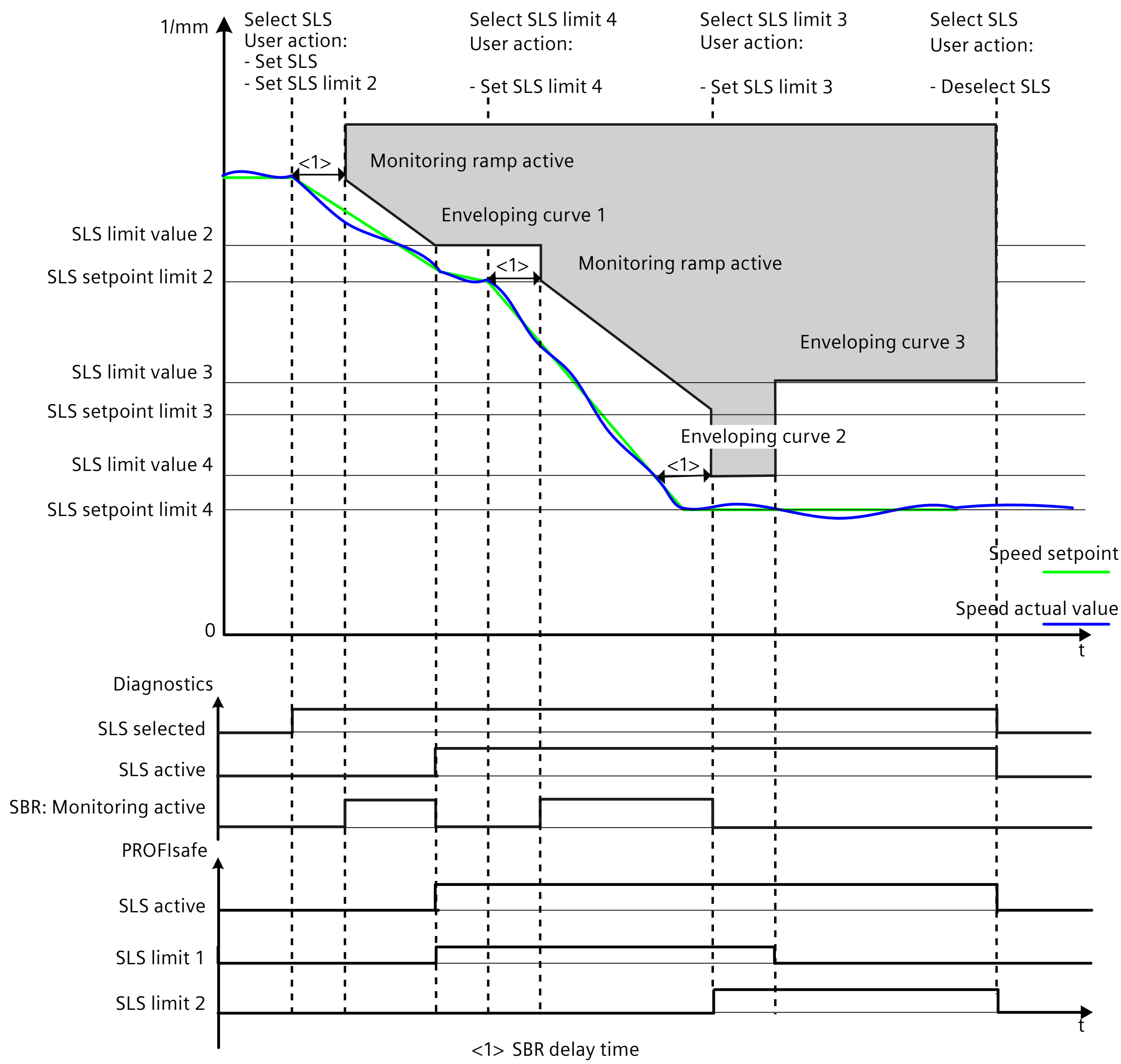


Figure 5-20 Safe Brake Ramp without encoder (for SLS)

Parameterization of the brake ramp

p9581 (SI Motion braking ramp reference value) and p9583 (SI Motion brake ramp monitoring time) are used to set the gradient of the brake ramp. Parameter p9581 determine the reference speed and parameter p9583 define the ramp-down time. Parameter p9582 is used to set the time which passes after the triggering of SS1, selection of SLS or SLS level changeover and the start of brake ramp monitoring.

Note

SBR and OFF3 curve

The SBR curve should be aligned to the OFF3 curve. In addition, you should check that under every load condition, the drive can follow this OFF3 ramp.

Note

Limitation of the SBR delay time

The SBR delay time (p9582) is limited to a minimum value of 2 SI Motion monitoring cycles (2 · p9500), i.e. even if a value less than 2 · p9500 is parameterized for the delay time (p9582), SBR only takes effect 2 safety cycles after an active SS1.

If a value greater than 2 · p9500 is parameterized for the delay time (p9582), SBR takes effect after active SS1 after the time p9582. Ensure that you round off the SBR delay time to an integer multiple of the safety cycle (p9500).

Responses to brake ramp violations (SBR)

- Safety message C01706 (SI Motion: SAM/SBR limit exceeded)
- Drive is stopped with STOP A
- For an encoder fault in a 1-encoder system, the "Safe Acceleration Monitoring" function is not active. A Category 0 or 1 stop response (EN 60204-1) can be set with parameter p9516.4.

Features

- Part of the "SS1 with/without encoder", "SS2 with encoder", "SLS without encoder" and "STOP B/STOP C (for safety with encoder)" functions.
- Parameterizable safe brake ramp

5.10.1 Important parameters

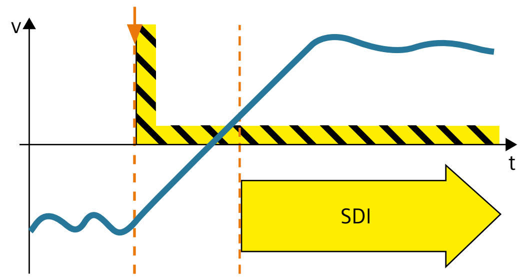
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9560 SI Motion STO shutdown speed (Control Unit)
- p9581 SI Motion braking ramp reference value (Control Unit)
- p9582 SI Motion braking ramp delay time (Control Unit)
- p9583 SI Motion braking ramp monitoring time (Control Unit)

5.11 SDI

Definition according to EN 61800-5-2:

The "SDI" function prevents that the motor shaft rotates in the unintended direction.



Examples of how the function can be used

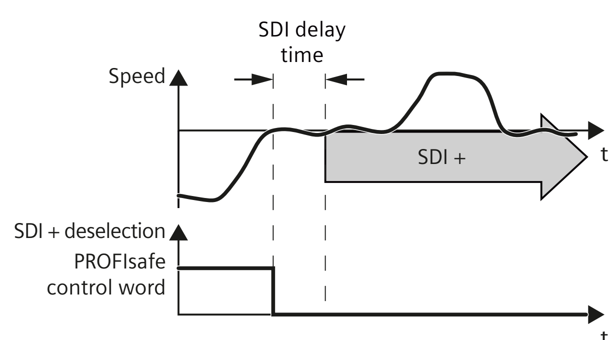
Example	Possible solution
A protective door must only be opened if a drive moves in the safe direction (away from the operator).	• Select SDI in the converter using a failsafe input or PROFIsafe . • Enable the locking mechanism of the protective doors via the PROFIsafe status bit of the converter.
When replacing the pressure cylinders of the plates, the drive must only move in the safe direction of rotation.	• Select SDI in the converter using a failsafe input or PROFIsafe . • In the converter, inhibit the direction of rotation that is not permitted.
Once the protection against jamming has been triggered, a roller shutter gate must only be able to start moving in one direction.	
At an operational limit switch, the trolley of a crane must only be able to start in the opposite direction.	

How does SDI function in detail?

SDI (Safe Direction) monitors the actual direction of rotation.

The SDI setpoint limit can be transmitted to the F-PLC to enable limitation of the velocity setpoint.

In addition, you can configure the setpoint limit provided by SDI as maximum speed in the ramp-function generator. In this case, SDI limits the speed setpoint to the permissible direction.



You can select to block either the positive or the negative direction of rotation via 2 fail-safe signals (F-DIs or PROFIsafe).

Selecting and deselecting SDI

As soon as the converter identifies that SDIhas been selected via a failsafe input or via PROFIsafe safe communication, the following happens:

- You can also set a delay time, within which you can ensure that the converter moves in the enabled (safe) direction.
- You can also set a tolerance, within which the converter tolerates movement in the direction that has not been enabled (unsafe). You can avoid the triggering of faults during braking (overshoot) as well as in controlled standstill.
- After the delay time has expired, the converter monitors the direction of rotation of the motor.
- If the drive now moves more than the configured tolerance in the blocked direction, a message is output and the defined stop response is initiated.

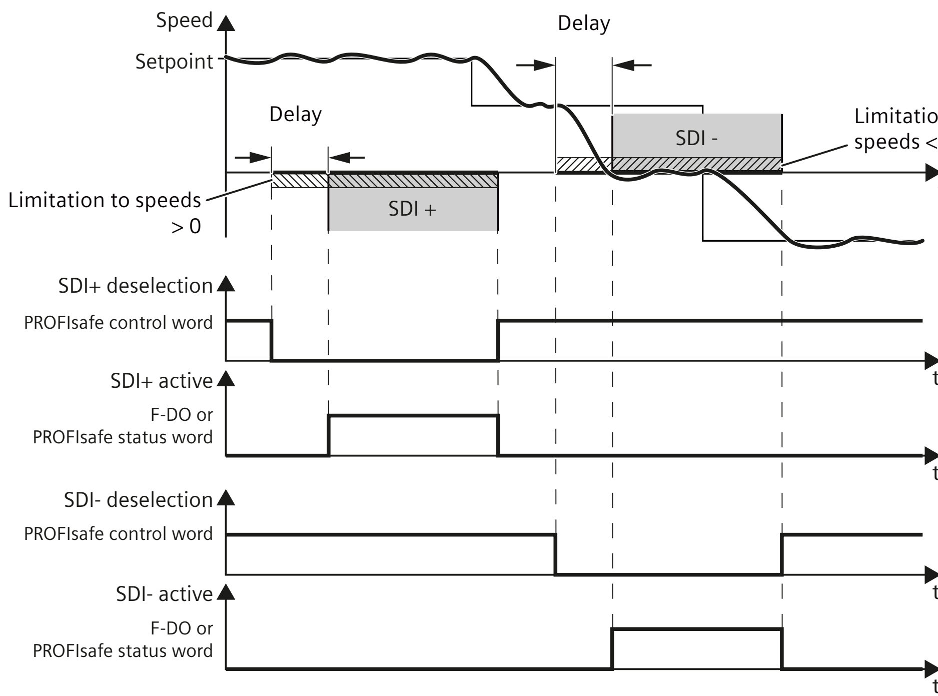


Figure 5-21 Time response of the safety function SDI (Safe Direction)

Note

SDI without selection

As an alternative to controlling via terminals and/or PROFIsafe, there is also the option of parameterizing SDI without selection. In this case, SDI will be permanently active after POWER ON. You can find details about this in section "Safe Direction without selection (Page 173)".

5.11.1 Details and parameterization

Note

Response to bus failure

If p9580 ≠ 0 and SDI is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SDI response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9566[0...3] ≥ 10).

5.11.1.1 Safe Direction with encoder

The "Safe Direction (SDI)" function allows a safe monitoring of the motion direction of the drive. If this function is activated, the drive can only move in the enabled direction.

Principle of operation

After SDI has been selected via terminals or PROFIsafe, the delay time p9565 is started. During this time, you have the option of ensuring that the drive is moving in the enabled direction. After this, the "Safe Direction (SDI)" function is active and the direction of motion is monitored.

If the drive now moves more than the configured tolerance (p9564) in the disabled direction, message C01716 is output and the stop response defined in p9566 is initiated. To acknowledge the messages, you must first deselect SDI, correct the fault cause and then safely acknowledge (Page 377) the messages. Only then can you reselect SDI.

Features

- Parameters r9720.12 and r9720.13 display whether the SDI function is selected.
- Parameters r9722.12 and r9722.13 display whether the SDI function is active.
- Parameter p9564 are used to set the tolerance within which a movement in a non-enabled (non-safe) direction is tolerated.
- Parameter p9566 define the stop response in the case of a fault.
- If "SDI positive" is selected, the following value is set automatically:
  - r9733[1] = 0 (setpoint limitation negative)
- If "SDI negative" is selected, the following value is set automatically:
  - r9733[0] = 0 (setpoint limitation positive)
- The absolute setpoint speed limit is available in r9733[2].

Enabling function "Safe Direction"

The "Safe Direction" function is enabled with p9501.17 = 1.

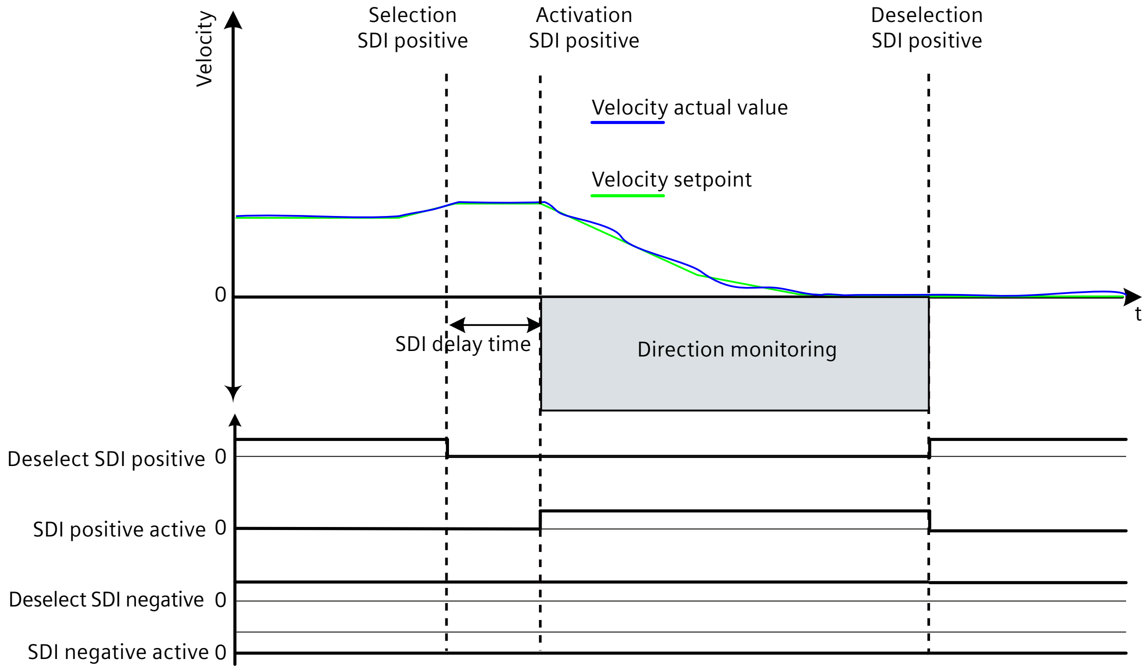


Figure 5-22 Functional principle SDI with encoder

5.11.1.2 Safe Direction without encoder

Note

You can find the parameterization for operation without encoder (p9506 = 1 or p9506 = 3) in the commissioning screen form for the safety functional scope (Page 267).

Differences between Safe Direction with encoder and Safe Direction without encoder

- For Safe Direction without encoder, after pulse suppression the drive is unable to determine the current speed. For this operating state, the behavior is defined using parameter p9509.8:
  - p9509.8 = 1
    The status signal displays "inactive".
  - p9509.8 = 0
    The status signal displays "active", and the drive takes on the state STO.
- Due to the less precise position recognition, "Safe Direction without encoder" requires a larger tolerance (p9564) compared with the function with encoder.

Note

No detection of a change of direction with the aid of p1820 or p1821

If the direction of rotation is reversed via p1820 or p1821, then safe monitoring is still possible: However, in this case, the setpoint limitation r9733 is calculated with the wrong direction of rotation. A reversal of the rotational direction with p1820 or p1821 therefore does not make sense.

Restart after pulse cancellation for p9509.8 = 0

If the drive has been switched off via OFF1/OFF2/STO etc., the following steps need to be carried out before a restart can be performed:

1. Case	• State after switching on	
		• SDI selected
		• STO selected
		• Pulse suppression active
	• Deselect STO	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
2. Case	• Situation	
		• Traversing to standstill with SDI selected
		• Initiate OFF1
		• Pulses are canceled; internal selection STO becomes active
	• Select STO	
	• Deselect STO STO activated internally via pulse suppression: This activation must be undone by selecting/deselecting STO.	
	• The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	
3. Case	• Situation	
		• Traversing to standstill with SDI selected
		• Initiate OFF1
		• Pulses are canceled; internal selection STO becomes active
	• Deselect SDI STO activated internally via pulse suppression: This activation must be undone by deselecting SDI.	
	• Select SDI The drive enable must be issued within 5 seconds via a positive edge at OFF1, otherwise STO is reactivated.	

4. Case	• Situation	
		• All Safety Integrated functions are deselected.
	• After this the drive enable must be given by a positive edge at OFF1.	
	• In this case, the motor is not started safely.	

When acknowledging SDI with STOP C, you must maintain the following sequence:

1. Correct the incorrect setpoint input.
2. Deselect SDI.
   While the safety STOP is active, this ensures that the motor cannot travel in the direction that has not been enabled while the SDI function is deselected.
3. Select SDI again.
   The SDI limits are then set again.
4. Cancel the safety STOP as a result of "safe acknowledgment".

5.11.1.3 Safe Direction without selection

Differences between Safe Direction with and without selection

- As an alternative to controlling via terminals and/or PROFIsafe, there is also the option of parameterizing SDI without selection. In this case, SDI will be permanently active after POWER ON (with encoder) or will be active after switch-on (without encoder).
- The "SDI without selection" function is activated as follows:
  - p9512.12 = 1 (SDI positive static active)
  - p9512.13 = 1 (SDI negative static active)
- The stop response is parameterized with p9566[0].

Switching the motor on and off (without encoder)

The time response and diagnostic options are as follows in this SDI version:

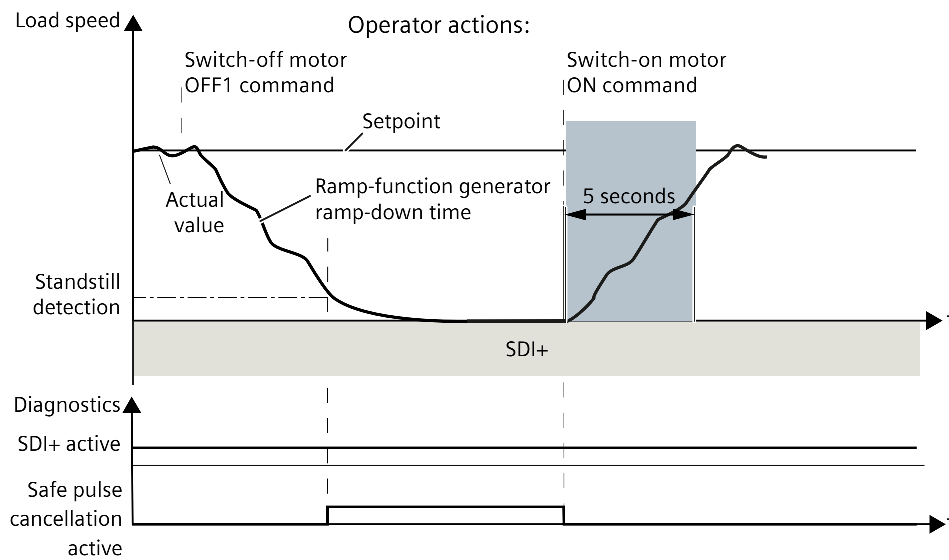


Figure 5-23 Time response of SDI without selection (example: Switching the motor on and off (without encoder))

"SDI without selection" behaves as follows when switching off and switching on again:

- After switch-off, the motor behaves in accordance with the canceled signal (OFF1, OFF2 or OFF3).
- STO (≙ safe pulse cancellation) becomes active after the standstill limit is undershot.
- After the ON command, the converter cancels the "safe pulse suppression" state and the start procedure is initiated.
- If the minimum current has not been reached after 5 seconds, the converter returns to the "safe pulse suppression" state and initiates the safety message C01711(1041).

5.11.1.4 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2824 SI Extended Functions - SDI (Safe Direction)
- 2840 SI Extended Functions - SI Motion drive-integrated control signals/status signals

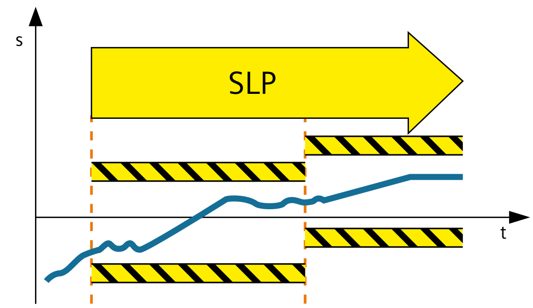
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p1820[0...n] Reverse the output phase sequence
- p1821[0...n] Direction of rotation
- p9501.17 SI Motion enable safety functions (Control Unit): Enable SDI
- p9506 SI Motion function specification (Control Unit)
- p9509 SI Motion behavior during pulse suppression (Control Unit)
- p9564 SI Motion SDI tolerance (Control Unit)
- p9565 SI Motion SDI delay time (Control Unit)
- p9566 SI Motion SDI stop response (Control Unit)
- p9580 SI Motion pulse suppression delay bus failure (Control Unit)
- r9720.0...27 CO/BO: SI Motion drive-integrated control signals
- r9722.0...31 CO/BO: SI Motion drive-integrated status signals (Control Unit)
- r9733[0...2] CO: SI Motion speed setpoint limit active
- p10017 SI Motion digital inputs debounce time (processor 1)
- p10030[0...3] SI Motion SDI positive input terminal (processor 1)
- p10031[0...3] SI Motion SDI negative input terminal (processor 1)
- p10039[0...3] SI Motion safe state signal selection (processor 1)
- p10042[0...5] SI Motion F-DO signal sources (processor 1)
- p10043[0...5] SI F-DO 1 signal sources
- p10044[0...5] SI F-DO 2 signal sources
- p10045[0...5] SI F-DO 3 signal sources

5.12 SLP

Definition according to EN 61800-5-2:

Function "Safely-Limited Position (SLP)" prevents the motor shaft from exceeding the specified position limit(s).



Examples of how the function can be used

Example	Possible solution
It is not permissible that the drive exits the specified position ranges.	• Select SLP in the converter; inhibit the range that is not permitted. • After the enabled range has been exited, a parameterizable stop response is initiated.

Function "Safely-Limited Position (SLP)" is used to safely monitor the limits of two traversing and/or positioning ranges, which can be switched over using a safety-related signal.

Features

- Selection via terminals or PROFIsafe
- 2 position ranges, each defined by a limit switch pair
- Safe switchover between the two position ranges
- Adjustable stop response
- To move the motor out of the unauthorized range, you must execute a special sequence (see "Retraction (Page 179)").

5.12.1 Details and parameterization

Function "Safely-Limited Position (SLP)" is used to safely monitor the limits of two traversing or positioning ranges, which can be switched over using a safety-related signal.

Requirements

For function "Safely-Limited Position (SLP)", the following requirements must be met:

- The use of one or two suitable encoders for the extended safety functions with encoder (see also Chapter "Safe actual value sensing with encoder system (Page 208)")

- Determining the absolute position of the drive by referencing during commissioning and after all actions after which a safe absolute reference can no longer be guaranteed (POWER ON, parking)

A description of safe referencing is provided in Chapter "Safe referencing (Page 204)".

Principle of operation

As soon as SLP is active, maintaining the limits of the active positioning range is safely monitored. With a safety signal you can switch between 2 position ranges. Each position range is limited by its previously defined limit switch pair. When passing the position of one of the two limit switches, a parameterizable stop response (STOP A, STOP B, STOP C, STOP D or STOP E) is triggered and safety message C01715 is output.

To acknowledge this fault, you can either switch over to a range whose limits have not been violated, or you can deselect the SLP function. After acknowledgment, the drive can then be traversed again in the permissible range.

Traversing in the permissible range can be realized in a safety-related fashion using the "Retract" function (see Chapter "Retracting (Page 179)").

Features

- Selection via safe terminals (onboard F-DI) or PROFIsafe
- Definition of the position range using 2 limit switch pairs (p9534 and p9535)
- Safe switchover between 2 different position ranges (not available for PROFIsafe telegram 30)
- Adjustable stop response (p9562)

Enabling function "Safely-Limited Position (SLP)"

- Function "Safely-Limited Position (SLP)" is enabled with p9501.1 = 1.
- After the enable, POWER ON at the converter.

Note

No actual value synchronization for SLP

It is not permissible to simultaneously enable function "SLP" and the actual value synchronization (p9501.3 = 1). In this case, the drive outputs fault F01688.

Control and status signals from the SLP

Selecting SLP and switching over between the position ranges is performed via a PROFIsafe control bit. SLP selection can be checked using parameter r9720.6. The selected position range can be checked using parameter r9720.19. Status bit r9722.6 is set if SLP is active. The active position range is displayed by r9722.19. Maintaining the upper or lower active SLP limit can be checked using r9722.30 and r9722.31.

Note

Jumps in the display

There is no hysteresis available for r9722.30 and r9722.31. Small fluctuations in the area around the range limit can result in the display jumping back and forth.

Controlling the Safely-Limited Position function

You have 2 options to select/deselect function "Safely-Limited Position (SLP)" and to switch over the range limits:

- PROFIsafe
  - SLP is selected/deselected using control words S_STW1.6 or S_STW2.6.
  - Switchover between the two limit switch pairs using control word S_STW2.19.
  - S_ZSW2.23 indicates whether the actual position is "safe"; for instance, the bit is only set after the axis was "safely referenced".
  - Whether SLP is active is indicated in bit 6 of the status words S_ZSW1.6 or S_ZSW2.6. The bit is not set until SLP is selected and the axis is in the "safely referenced" state.
  - Which SLP limit switch pair is active is indicated in status word S_ZSW2.19. This indication is only valid if SLP is itself active.
  - S_ZSW2.30 and S_ZSW2.31 indicate whether the upper or lower limit of the active position range is maintained.

Note

Extended Functions via PROFIsafe

The status signal "SLP active" (S_ZSW1.6 or S_ZSW2.6) is not the same as the diagnostic signal "SLP active" (r9722.6), but is the AND logic operation of "SLP active" (r9722.6) and "safely referenced" (r9722.23).

The other SLP status signals S_ZSW2.19 "SLP active position range", S_ZSW2.30 "upper SLP limit maintained" and S_ZSW2.31 "lower SLP limit maintained" match the corresponding bits in r9722.

Note

Restrictions for PROFIsafe telegram 30

The use of PROFIsafe telegram 30 (with 16-bit words S_STW1 and S_ZSW1) has the following restrictions:

- Only position range 1 is available.
- A switchover to position range 2 is not possible.
- The status feedback signals "safely referenced", "active position range", "upper SLP limit maintained" and "lower SLP limit maintained" are not available.

Note

Response to bus failure

If p9580 ≠ 0 and SLP is active, in the event of communication failure the parameterized ESR reaction is only realized if, as an SLP response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9562[0...1] ≥ 10).

5.12.1.1 Retraction

After a limit of the active traversing range has been exceeded, the drive must be brought back to the permissible range. A safety acknowledgment would, in this case, only retrigger the safety messages; the drive would be prevented from moving. If a switchover to the other traversing range doesn't come into question, then the only thing that remains is to deselect SLP. However, this would have the disadvantage that it is not monitored as to whether the drive is moving in the direction of the permissible traversing range.

Therefore, it is recommended that a retract function is implemented as follows:

Safety commissioning

1. Completely parameterize SLP.
2. Completely parameterize SDI.
3. Perform an acceptance test for both functions.

The next steps differ depending on the control type:

Control via PROFIsafe

- Implement a user program in your F-CPU with the following steps to implement a retract function:
  - Select SDI positive in the case that the lower SLP limit is violated, or SDI negative if the upper SLP limit is violated
  - Wait until the selected SDI is active, then deselect SLP
  - Safe acknowledgment of the limit violation
  - Movement of the drive with suitable setpoint inputs in the range that has been enabled
  - Select SLP
  - Wait until SLP is active, then deselect SDI

Note

FAQ retraction

A description of how retraction can be implemented via a failsafe control and PROFIsafe communication is provided in the Internet at:
FAQ retraction (https://support.industry.siemens.com/cs/ww/en/view/65128501)

5.12.1.2 Function diagrams and parameters

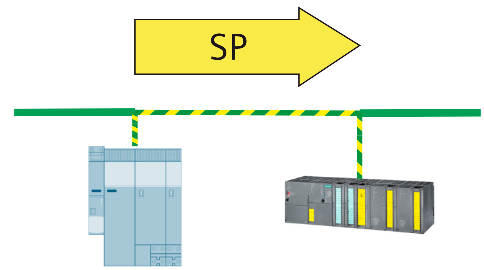
Function diagrams (see SINAMICS S120/S150 List Manual)

- 2822 SI Extended Functions - SLP (Safely-Limited Position)
- 2840 SI Extended Functions - SI Motion drive-integrated control signals/status signals

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9534[0...1] SI Motion SLP (SE) upper limit values (Control Unit)
- p9535[0...1] SI Motion SLP (SE) lower limit values (Control Unit)
- p9544 SI Motion actual value comparison tolerance (referencing) (CU)
- p9562[0...1] SI Motion SLP (SE) stop response (Control Unit)

5.13 SP



Function "Safe Position (SP)" allows safe position values to be transferred to the F-PLC via PROFIsafe (telegram 901 or 902).

From the position change over a specific time, the F-PLC can also calculate the actual velocity. In telegram 902, the values are transferred in 32-bit format, in telegram 901, in 16-bit format.

The position actual value is not transferred in PROFIsafe telegram 903, which is preset for SINUMERIK.

See also: Overview of process data telegrams (Page 225)

After parameter assignment, release and POWER ON, the function is automatically selected and the values transferred. Please observe the following:

- For use as the safe absolute position, the "Absolute position" must also be enabled and then safely referenced.
- In order that the transferred position can be used, the actual position value must be valid.

Using the time stamp that is also transferred, you can also calculate the velocity from the position values. If you only want to calculate the velocity, it is sufficient to enable the "Transfer of safe position values" without the "Absolute position."

5.13.1 Details and parameterization

Function "Safe Position (SP)" allows a safe position (i.e. absolute or relative position) to be transferred to the F-PLC via PROFIsafe. Transferring a safe relative position can be used to calculate the safe speed/velocity in the F-PLC. Its use for safe position monitoring is only permissible if the reference to the absolute position was established at the control level. In this case, the "safely referenced" bit of SINAMICS S120 (r9722.23) cannot be used.

Enabling the "Transfer safe position values" function

The following steps are required to enable function "Safe Position (SP)":

- Enable the Safety Integrated Extended Functions
  - p9601 = 12 = C hex (≙ Extended Functions via PROFIsafe)
    or
  - p9601 = 13 = D hex (≙ Extended Functions via PROFIsafe and Basic Functions via onboard terminals)
- Enable "Transfer the safe absolute position with the possibility of calculating the velocity by the controller"
  - Select one of the PROFIsafe telegrams 901 or 902 (p60022, p9611, p9811)
  - p9501.2 = 1 (≙ enable absolute position)
  - p9501.25 = 1 (≙ enable transfer of safe position via PROFIsafe)

Note

No actual value synchronization when SP is enabled

If the transfer safe position value function is used, it is not permissible to enable actual value synchronization (p9501.3 = 1): In this case, the drive outputs fault F01688.

- Enable the "Transfer safe relative position" only to calculate the speed by the controller
  - Select one of the PROFIsafe telegrams 901 or 902
  - p9501.25 = 1
- After the enable, POWER ON the converter.

Principle of operation

After parameter assignment, release and POWER ON, the function is automatically selected and the values transferred. Please observe the following:

- Transfer of safe absolute position values
  - If the transfer of the safe relative position has been enabled through p9501.25 = 1 and p9501.2 = 0, the validity of the safe relative position is displayed by the set bit S_ZSW2.22.
  - If the transfer of the safe absolute position has been enabled using p9501.25 = 1 and p9501.2 = 1, S_ZSW2.22 is only set when the drive has also been safely referenced.
- Transfer of safe relative position values (e.g. for calculating the velocity)
  - Only S_ZSW2.22 (r9722.22, actual position value valid) must be set to calculate the speed.

Setting the modulo value for rotary axes

- p9505 is used to define the modulo range of a safety rotary axis (p9502 = 1) when the transfer of a safe absolute position (p9501.2 = 1 and p9501.25 = 1) is enabled. Parameterizing the modulo value can result in a jump in the position actual value if the range that can be represented overflows. p9505 must therefore only be parameterized in steps of $2^n \times 360°$ (n = 1, 2, 3, ...). In all other cases, the converter issues alarm A01794. This alarm can be hidden in the case that the possible jump in the position actual value can be tolerated in the particular application – or this does not present a problem.
- The modulo function is deactivated if p9505 = 0. This parameter has no relevance for a safety linear axis (p9502 = 0) or when the transfer of a safe relative position (p9501.2 = 0 and p9501.25 = 1) is enabled.
- If SLP is also enabled (p9501.1 = 1), the modulo function must be deactivated (p9505 = 0).

Transfer formats and value range

- 32-bit
  The values are transferred in telegram 902 as 32-bit values with the following value ranges:

Table 5-2 Value range and resolution (32 bits)

	Linear axis	Rotary axis
Position values	±737280000	±737280000
Unit	1 µm	0.001 °
Comment	Monitoring ±737.280 m with an accuracy of 1 µm	≙ 2048 revolutions

- 16-bit
  To transfer the position values in telegram 901 in the 16-bit format, you must scale the values using p9574. In this case, you must select the scaling factor so that the value of the actual position value does not exceed the 16-bit format. If the actual position value exceeds the range that can be displayed with 16 bits (±32767), a STOP F is initiated and message C01711 is output with fault value 7001. Depending on the scaling factor, this means that ranges with different sizes can be monitored with varying accuracy. Example:
  - Scaling factor: 1000
  - Unit: 1 µm (linear axis)
  - Position value: ±32767 mm

  It may therefore be precisely monitored in a range of ±32.767 m to an accuracy of 1 mm.

Note

Scaling to 16 bits

The scaling is performed by dividing the mean value of r9708[0] and r9708[1] with this scaling factor.

Example: For a position of -29.999 mm signaled in r9708[0] and r9708[1] and a scaling factor of p9574 = 1000, a numerical value of -29 is signaled to the controller.

Value range r9708

The diagnostics information in parameter r9708 is displayed with the following properties:

Table 5-3 Value range and resolution (32 bits)

	Linear axis	Rotary axis
Position values	±737280000	±737280000
Unit	1 µm	0.001 °
Comment	Monitoring ±737.280 m with an accuracy of 1 µm	≙ 2048 revolutions

What is shown in parameter r9713 is identical to the values of r9708; however, in SINAMICS-internal calculation units.

Speed calculation

The control must calculate the speed from the position change:

- `Pos diff = Pos new - Pos old`
- `Cycle diff = cycle counter new - cycle counter old`
- `Timediff = Cyclediff × Safetycycle`
  (If `Cyclediff` = 0, the speed that was last calculated must be used.)
- `v = Pos diff/time diff`
- `Format v`

Acceptance test

An acceptance test is not required for function "Safe Position (SP)", but the function that was implemented using SP must be accepted in the higher-level control system.

5.13.1.1 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

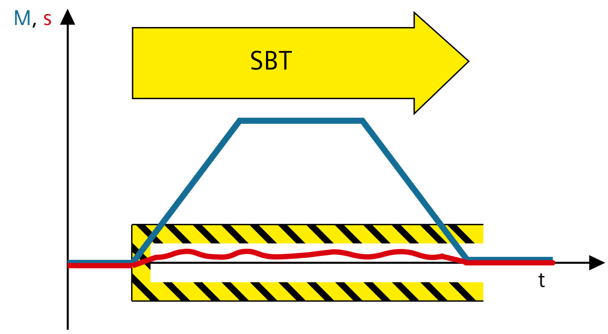
- 2840 SI Extended Functions - SI Motion drive-integrated control signals/status signals

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9505 SI Motion SP modulo value (Control Unit)
- p9542 SI Motion actual value comparison tolerance (crosswise) (Control Unit)
- p9601 SI enable functions integrated in the drive (Control Unit)
- r9708[0...5] SI Motion diagnostics safe position
- r9713[0...5] CO: SI Motion diagnostics actual position value load side

5.14 SBT

Diagnostic function "Safe Brake Test (SBT)" checks the required holding torque of a brake (operating or holding brake).



You can test linear and rotary brakes. The drive purposely generates a force/torque against the applied brake. If the brake is operating correctly, the axis motion remains within a parameterized tolerance. If, however, a larger axis motion is detected, it must be assumed that the braking force/torque has deteriorated and maintenance is required.

Diagnostic function "Safe Brake Test" allows a safe test of up to 2 brakes:

- 1 motor holding brake and 1 external brake
- 2 external brakes
- 1 motor holding brake
- 1 external brake

Diagnostic function "Safe Brake Test" (SBT) function meets the requirements for Category 2 according to EN ISO 13849-1.

5.14.1 Features

Diagnostic function "Safe Brake Test" has the following properties:

- The parameters of diagnostic function "Safe Brake Test" are protected by the Safety password, and can only be changed in the Safety commissioning mode.
- Using this function, brakes can be tested that are directly connected to SINAMICS S120 (integrated brake control), but also externally controlled brakes (e.g. via a PLC).
- A maximum of 2 brakes can be tested:
  - A motor holding brake, controlled by the integrated brake control of the SINAMICS, and in addition, an externally controlled brake.
  - Two externally controlled brakes
  - A motor holding brake, controlled by the integrated brake control of the SINAMICS.
  - One externally controlled brake
- Diagnostic function "Safe Brake Test" complies with SIL 1 according to IEC 61508 or PL d/Cat. 2 according to EN ISO 13894-1.

5.14.2 Connection to NC and PLC programs

Diagnostic function "Safe Brake Test" integrated in the drive does not require a setpoint input from the PLC or NC, but only enable signals from the NC and control via the PLC user program. The relevant signals when executing the brake test (SBT) are communicated between the PLC and drive via the Safety Info Channel (SIC) and the Safety Control Channel (SCC).

- SIC/SCC communication is realized using telegram 701 (Page 232). In the TIA Portal configuration, telegram 701 is automatically inserted when you activate the "SINUMERIK Safety Integrated (F-PLC)" mode.
- The SIC/SCC signals (to control SBT) are mapped in the axis DB (axis 1 [DB31] ... axis 31 [DB61]). Bits (DBX11.0 and DBX71.0) in the relevant axis DB are used to control SBT. As a consequence, you can execute the SBT via PLC user program.
  See: Interface signals: Axis/spindle signals (Page 419).

Note

Information for those switching over from a different system: Block required for SBT (Safe Brake Test)

The relevant axis DB is used to control SBT. Block SI_BrakeTest [FB11], known from the "SINUMERIK Safety Integrated mode (system-integrated)" mode, is no longer used in the "SINUMERIK Safety Integrated (F-PLC)" mode.

5.14.3 Details and parameterization

5.14.3.1 Requirements

NC

The following preconditions must be complied with before the brake test is enabled by the NC:

- The axis must be at a standstill, and be in a safe axis position.
- The NC must have issued the controller enable and pulse enable.

DRV

The following preconditions must be satisfied for the DRV to use diagnostic function "Safe Brake Test":

- The Safety Integrated Extended Functions must be enabled; also available for the Safety Integrated Extended Functions without selection.
- Safe Brake Control must be enabled when testing a brake controlled by SINAMICS (motor holding brake).

- Safety Integrated Extended Functions with encoder have been enabled.
  You can find information about possible encoder concepts in Chapter "Safe actual value acquisition (Page 208)".

  Note

  SBT only with encoder

  The "Safe Brake Test" (SBT) diagnostic function can only be used with an encoder.

- Speed control with encoder (p1300 = 21).
  SBT is not possible with encoderless speed control (e.g. vector V/f control) and torque control. In this case, alarm A01784 is output.
- The pulses must be enabled when SBT is selected. The actual speed value must not exceed 1 % of the maximum speed (p1082) when SBT is selected and over the complete time that SBT is active.
- The brake(s) must be open

Note

SBT and HLA

Diagnostic function "Safe Brake Test" is not available for SINAMICS HLA.

5.14.3.2 Handling overview

Table 5-4 Selecting SBT

Step	Procedure
1st	In the associated axis DB, set bit "Start brake test" DBX11.0 = 1.
→	The NC checks that the appropriate conditions are satisfied: • If the conditions are satisfied, then the "Brake test active" bit is set to 1 (DBX71.0 = 1). • Alarm 27830 is output if the conditions are not satisfied.
2nd	Check whether the "Brake test active" bit (DBX71.0) is set to 1. It this is not the case, then it is not permissible that you perform the SBT In this case, ensure that the requirements (Page 186) are satisfied, and start again with step 1.
3rd	Select SBT via SCC by setting bit 0 "SELECTION_SBT" to 1 in STW3 (signal edge 0 => 1). See also: Selection (Page 191)
→	In ZSW3, bit 1 "SETPOINT_SETTING_DRIVE" is set to 1 - which in the SIC signals that the NC no longer enters the setpoint, but instead, DRV. The monitoring functions are deactivated in the NC, and the setpoint is set the same as the actual value. The brake test sequence is executed. See also: Sequence (Page 192)

Table 5-5 Deselecting SBT

Step	Procedure
1st	Select SBT via SCC by setting bit 0 "SELECTION_SBT" to 0 in STW3 (signal edge 1 => 0). See also: Selection (Page 191)
→	DRV initiates the de-selection process, and then in ZSW3 bit 1 "SETPOINT_SETTING_DRIVE" is set to 0. The setpoint circuit from the NC is synchronized to the actual values (setpoint position = actual position), the position is aligned and the contour and standstill monitoring are reactivated. See also: Sequence (Page 192)
2nd	In the associated axis DB, set bit "Start brake test" DBX11.0 = 0.
→	The "Brake test active" bit is set to 0 (DBX71.0 = 0) by the NC.

Canceling the brake test sequence (SBT)

If the brake test sequence (SBT) is canceled due to errors, then you can carry out the evaluation and implement the resulting measures via the corresponding PLC interface signals.

See also: Cancellation/deselection and acknowledgment (SBT) (Page 193)

Note

Using MD36968.2 to select the parameter assignment behavior at the end of SBT

You can parameterize the positioning behavior after the brake test via the expert list using MD36968.2 $MA_SAFE_BRAKETEST_CONTROL, bit 2:

- 0: Positioning at the actual axis position
  To conclude the brake test, the actual axis position for the next path motion is used. (MD36968 $MA_SAFE_BRAKETEST_CONTROL bit 2 = 0). This results in motion to the last programmed axis position on the path.
- 1: Positioning to the last programmed axis position
  Acceptance of the actual axis position is not carried out. After the axis has been pressed against the brake, the closed-loop position controller withdraws the axis to the last programmed position.
  Vertical axes can thus be prevented from sagging as a result of a repeated brake test. It is also possible to briefly exceed the software limit switch while pressing against the brake without initiating an alarm.

5.14.3.3 Enabling the function

Proceed as follows to enable diagnostic function "Safe Brake Test":

1. Enable function "Safe Brake Control (SBC)" when using an internal motor holding brake (MHB): p9602 = 1.
2. Select the SBT selection type:

p10203	Selects SBT
= 0	Via SCC
= 1	Via BICO
= 2	For test stop / forced checking procedure

3. Check the motor type; the following must apply: p10204 = r0108.12

For testing brake 1 [index 0] or 2 [index 1], initially, those values must be entered, which apply to both test sequences:

- Brake type

p10202[0,1]	SI Motion SBT brake selection
= 0	Inhibit This must be set if one of the brakes is either not available or is not to be tested.
= 1	Testing the motor holding brake Here, in addition p1215 must be set to = 1
= 2	Setting an external brake

- You define the holding torque of brakes using p10209.
- Test torque ramp time p10208[0,1]
  Within this time, before starting the test sequence, the test torque is ramped up – and at the end of the sequence, is ramped down again.

Note

When testing an external brake, whose mechanical design exhibits backlash (e.g. if there is a gearbox located between the motor and external brake), it can make sense to extend the ramp time (p10208) when ramping up and ramping down the test torque.

- The interconnection of the parameters for the telegram extension, relevant for SCC/SIC, can be performed automatically by setting p60122 = 701. However, the telegram extension must have been previously created. More detailed information on this can be found in Chapter "Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 231)".
- The following parameters must also be set if you control the brake test using BICO signals (p10203 = 1):

p10230.0	Signal for selecting the brake test
p10230.1	Signal for starting the test sequence
p10230.2	Signal for selecting the brake to be tested (= 0: Brake 1; = 1: Brake 2)

p10230.3	Signal for selecting the sign of the test torque (= 0: positive; = 1: negative)
p10230.4	Signal to select the test sequence (= 0: sequence 1; = 1: sequence 2)
p10230.5	Feedback signal for the state of the external brake (= 0: external brake open; = 1: external brake closed)

You can parameterize 2 test sequences for each brake. Each test sequence is characterized by the following setting values:

- Brake test sequence 1

p10210[0,1]	Test torque to be generated in % of the brake holding torque
p10211[0,1]	Test duration in ms
p10212[0,1]	Positional deviation to be tolerated in mm/degrees during the test

- Brake test sequence 2

p10220[0,1]	Test torque to be generated in % of the brake holding torque
p10221[0,1]	Test duration in ms
p10222[0,1]	Positional deviation to be tolerated in mm/degrees during the test

- Perform a POWER ON after commissioning

Note

SBT and DSC

If SBT is used with DSC, parameter r10234 (S_ZSW3B) must be evaluated and Safety Control Channel control word 3B (S_STW3B) must be activated. In the PLC, r10234.1 specifies that no position monitoring may be active during the brake test (the same applies of course for traversing).

5.14.3.4 Selection

You have the following options for the selection of the Safe Brake Test:

- **Safety Control Channel (SCC) via PROFIBUS or PROFINET (integrated drives, external drives)**
  Using SCC, the SBT function can be directly controlled from a higher-level control system.
  Select the brake test sequence with a 0/1 edge in S_STW3B bit 0
  See also: Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 231), SBT: Communication via SIC/SCC (Page 194)
- **Selection via BICO (only external drives)**
  BICO interconnection; here, digital signals (e.g. DIs) are used to operate the SBT function.
  You cannot select SBT for integrated drives of the NCU (SINAMICS Integrated, NX modules) via BICO, but only via SCC.
  Selected using 0/1 edge at DI for p10230[0]
- **Selected using test stop/forced checking procedure of the Extended Functions**
  Automatic execution when selecting the test stop/forced checking procedure; restricted test options; however, no additional signals are required for the control.
  Selected using a 0/1 edge in the S_STW1B bit 8 (integrated drives, external drives) or at the DI for p9705 (only external drives).
  After selection, initially SBT is automatically performed, followed by the test stop/forced checking procedure.

Note

Only brake 1 when selecting using test stop/forced checking procedure

When selecting using test stop/forced checking procedure, only the internal motor holding brake parameterized as brake 1 is tested with test sequence 1 in the direction parameterized in p10218.

5.14.3.5 Start of the Safe Brake Test sequence

- Make the following decisions before starting the brake test sequence:
  - The brake to be tested using DI for p10230[2] or S_STW3B bit 2
  - Positive or negative direction of the test torque using DI for p10230[3] or S_STW3B bit 3
  - Brake test sequence 1 or 2 using DI for p10230[4] or S_STW3B bit 4.
- Start the brake test sequence using a 0/1 edge at the DI for p10230[1] or in S_STW3B bit 1.

5.14.3.6 Sequence

SBT has the following basic sequence:

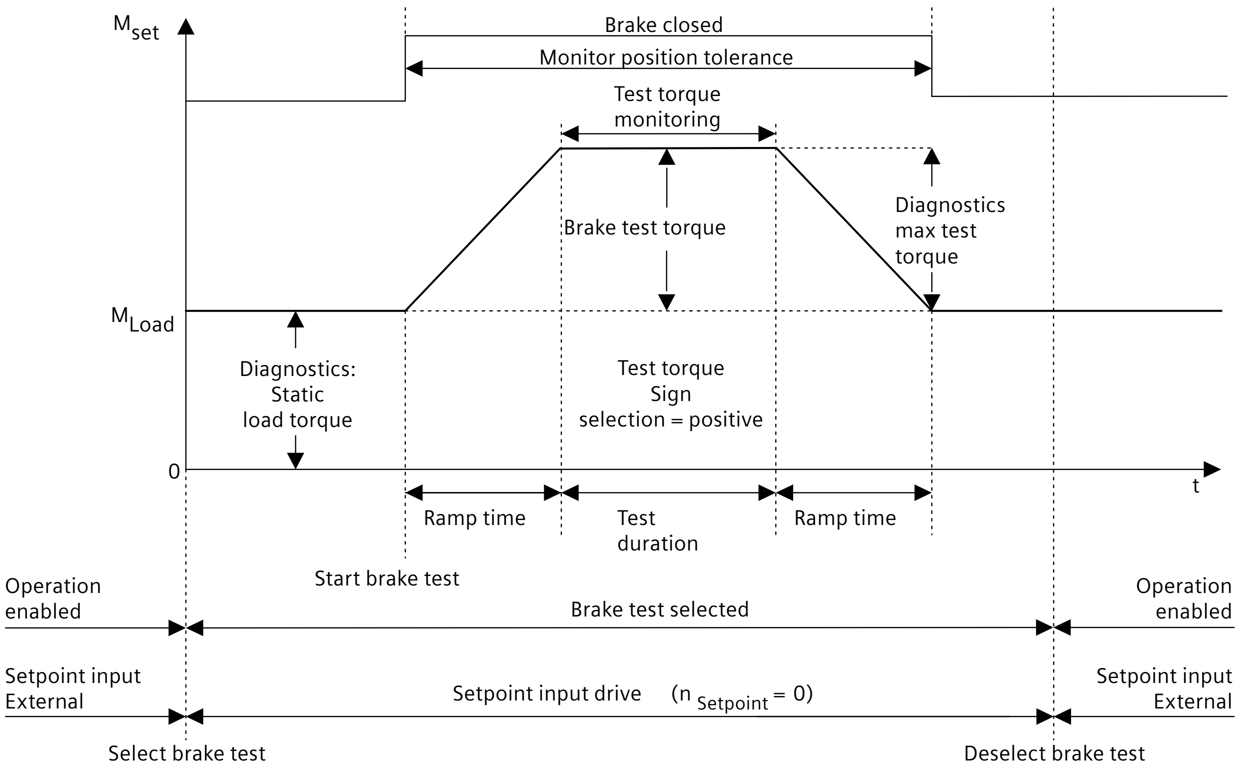


Figure 5-24 SBT: Time sequence

- After the user selects the brake test (0/1 edge in r10231.0), the static hanging load is determined. For this reason, all brakes must be open and the pulses enabled when the brake test is selected.
  - When testing a motor holding brake, which is directly controlled from SINAMICS, the brake is automatically opened when the pulses are enabled and p1215=1.
  - When testing an external brake, via p10234.6 or for SIC/SCC, via S_ZSW3B.6, a value of 0 indicates that the external brake must be opened. This must occur within 11 seconds, otherwise the test is canceled and a fault is output.
- The brake, the test sequence and the test direction are then selected by the user.
- When the brake test is active after the start of the brake test / brake test sequence by the user (0/1 edge in r10231.1), the holding brake (MHB) is closed or there is a prompt to close the external brake. The request to close the brake is again indicated with p10234.6 = 1 or S_ZSW3B.6 = 1. Also in this case, only a maximum of 11 seconds must elapse, otherwise a fault is issued.
- The test torque (test torque ± load torque for a vertical axis) is specified during the SBT. When n = 0 is entered, the controller builds up an appropriate test torque against the closed brake. The test torque is built up along a ramp. The ramp is defined by the time of p10208.
- At the end of the test sequence, the brake is opened or there is a prompt to open the brake.

- After deselection of the test sequence (test sequence is switched off), another test sequence can be started, e.g. with a different brake in a different direction, assuming that the brake test is still selected.
- When the test sequence is active, the brake that is not being tested must remain open.
- After deselection of the SBT, the original speed setpoint takes effect again.

5.14.3.7 Cancellation/deselection and acknowledgment (SBT)

An active brake test is cancelled through deselection of the test sequence or deselection of the brake test. Alarm A01782 is output.

Acknowledging alarms

The alarms relevant for the brake test can only be safely acknowledged (failsafe acknowledge), and under certain circumstances only acknowledged, when the brake test is deselected. For "motion monitoring without selection", a POWER ON is required – or STO/SS1 must be selected/deselected (for a configured extended alarm acknowledgment).

5.14.3.8 Communication via SIC/SCC

Test of a motor holding brake

The following figure shows the communication via SIC and SCC during the test of a motor holding brake:

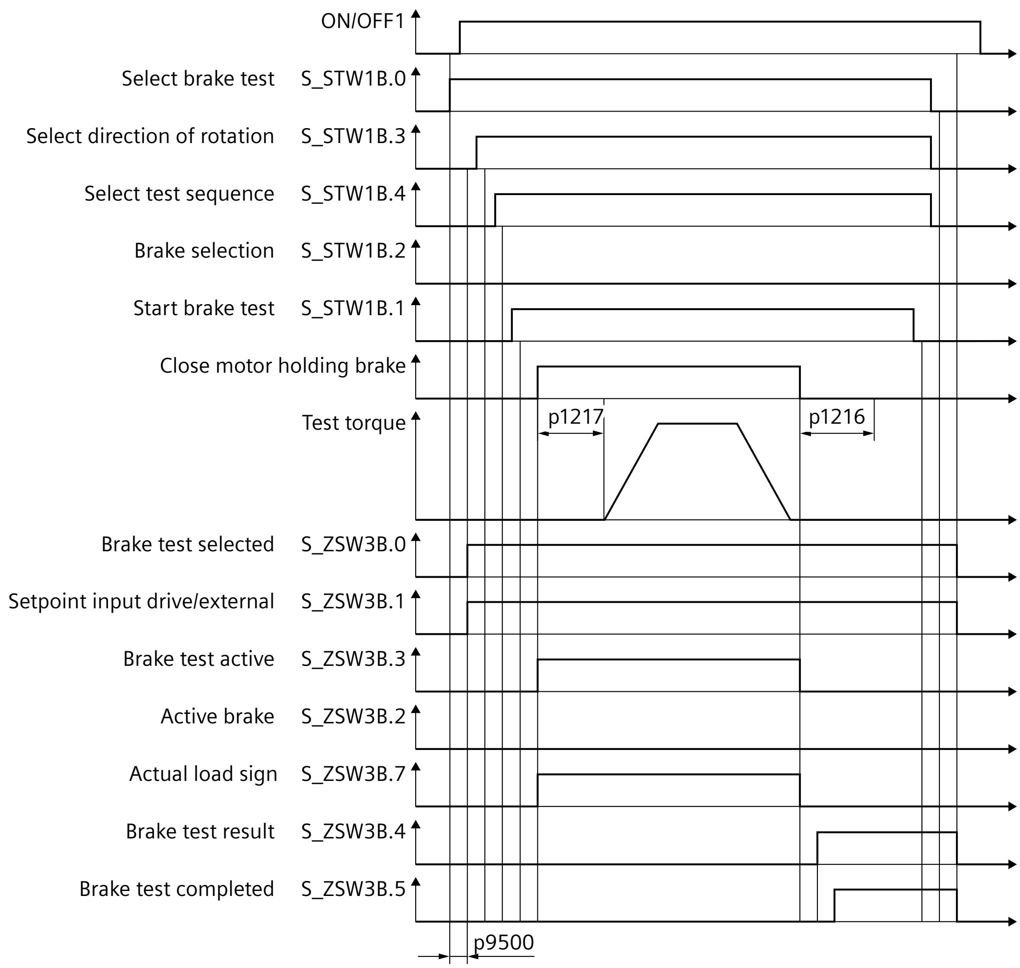


Figure 5-25 Testing a motor holding brake

Test of an external brake

The following figure shows the communication via SIC and SCC during the test of an external brake:

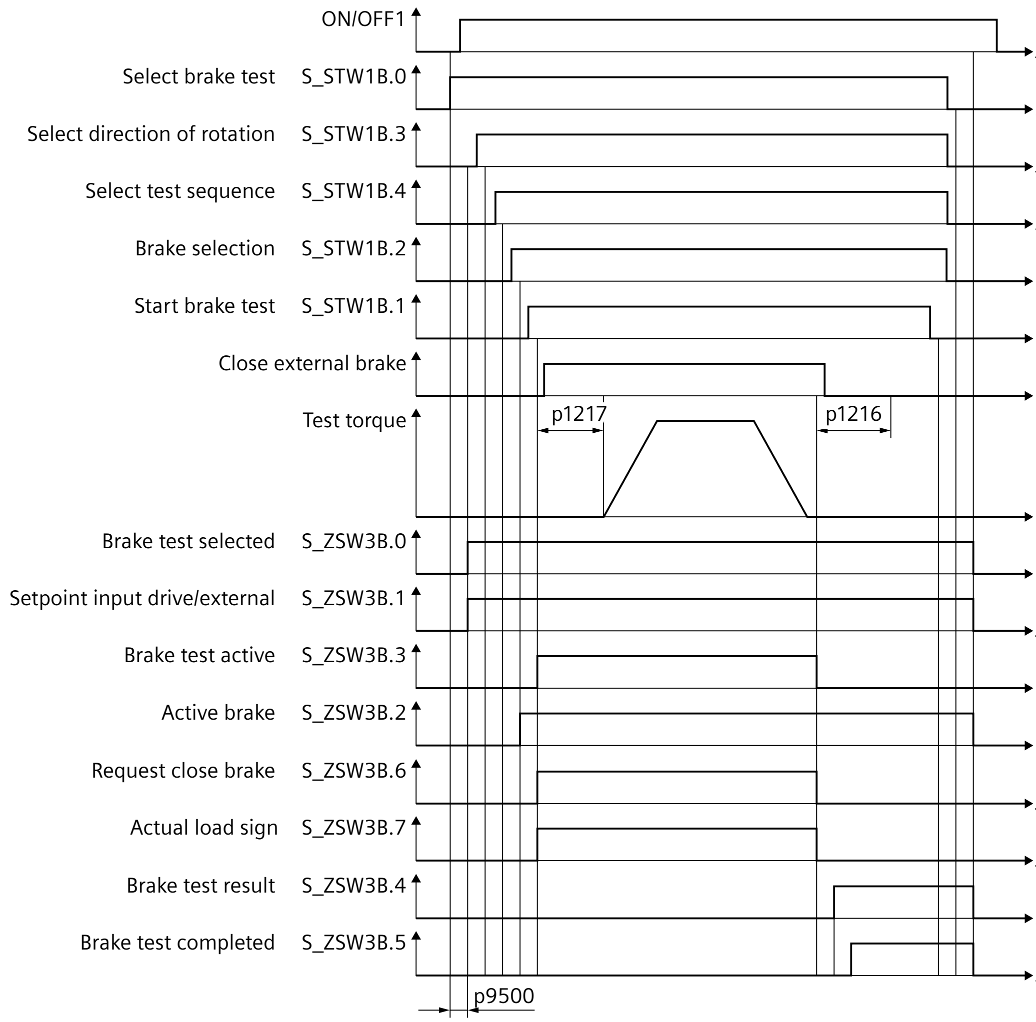


Figure 5-26 Testing an external brake

5.14.3.9 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2836 SI Extended Functions - SBT (Safe Brake Test)
- 2837 SI Extended Functions – selection of active control word

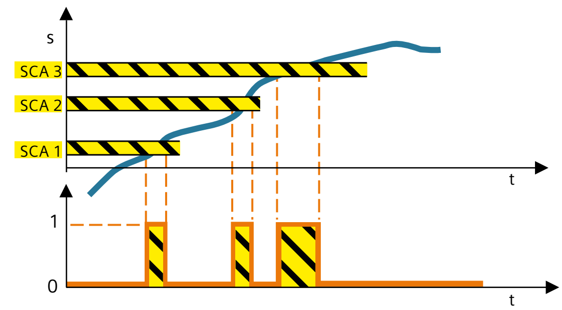
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p1215 Motor holding brake configuration
- p1216 Motor holding brake opening time
- p1217 Motor holding brake closing time
- p9501 SI Motion enable safety functions (Control Unit)
- p9601 SI enable functions integrated in the drive (Control Unit)
- p9602 SI enable safe brake control (Control Unit)
- p10201 SI Motion SBT enable
- p10202[0...1] SI Motion SBT brake selection
- p10203 SI Motion SBT control selection
- p10204 SI Motion SBT motor type
- p10208[0...1] SI Motion SBT test torque ramp time
- p10209[0...1] SI Motion SBT brake holding torque
- p10210[0...1] SI Motion SBT test torque factor sequence 1
- p10211[0...1] SI Motion SBT test duration sequence 1
- p10212[0...1] SI Motion SBT position tolerance sequence 1
- p10218 SI Motion SBT test torque sign
- p10220[0...1] SI Motion SBT test torque factor sequence 2
- p10221[0...1] SI Motion SBT test duration sequence 2
- p10222[0...1] SI Motion SBT position tolerance sequence 2
- p10230[0...5] BI: SI Motion SBT control word
- r10231 SI Motion SBT control word diagnostics
- r10234.0...15 CO/BO: SI Safety Info Channel status word S_ZSW3B
- p10235 CI: Safety Control Channel control word S_STW3B
- r10240 SI Motion SBT test torque diagnostics
- r10241 SI Motion SBT load torque diagnostics
- p60122 IF1 PROFIdrive SIC/SCC telegram selection

5.15 SCA

Definition according to EN 61800-5-2:

Function "Safe Cam (SCA)" supplies a safety-related output signal to indicate whether the motor shaft position is within a defined range.



Function "Safe Cam" outputs a safety-related signal if the drive is within a specified position range. It facilitates the realization of safe range detection for each individual axis.

5.15.1 Details and parameterization

Using function "Safe Cam (SCA)", you can implement safe electronic cams, safe zone sensing or a working area limitation/protection zone delimitation for a specific axis, therefore replacing a hardware-based solution. You parameterize up to 30 output cams for each axis. You enable each output cam individually.

Note

Safety function "Safe Cam (SCA)" can only be used with an encoder.

Defining the output cam positions

- You define the output cam positions to be monitored using the parameters p9536[x] and p9537[x] (where x = 0 ... 29).
  Note that the defined output cams must have a certain minimum length: p9536[x] - p9537[x] ≥ p9540 + p9542
  If you violate this rule, the drive will output the message F01686 ("SI Motion: Output cam position parameterization not permissible").
- Owing to variations in the cycle and signal propagation times, the output cam signals of the two monitoring channels do not switch simultaneously and not precisely at the same position. For this reason, enter a tolerance band for all output cam types via parameter p9540. Within this tolerance band, the monitoring channels can have different signal states for the same output cam:

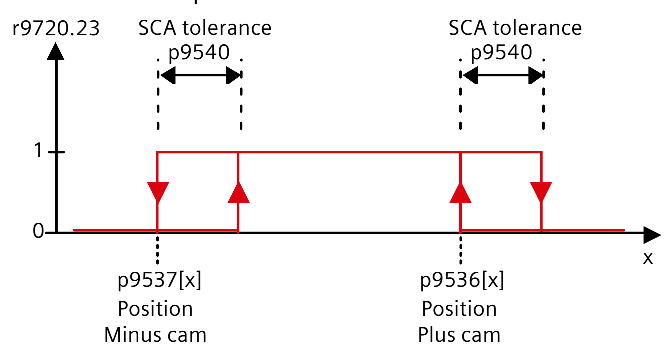


Figure 5-27 Parameterize output cam and tolerance

Note

The smallest possible tolerance band should be selected for the SCA function (<5 ... 10 mm). It makes sense to parameterize the output cam tolerance to be greater than or equal to the actual value tolerance.

- Reference the axis using the "Safe referencing (Page 204)" function.

Enable SCA

- Enable function "Safe Cam (SCA)" with p9501.28 = 1.
- You enable each output cam individually with p9503.x = 1 (where x = 0 ... 29).

WARNING

Unexpected speed of the machine component as the axis was not referenced

The enabled cam signals are immediately output after POWER ON. However, the output is only safety-related after safety-related referencing People can be put into a dangerous situation or material damage can result if the axis is not referenced in a safety-related way.

- Reference the axis using the "Safe referencing (Page 204)" function.

Select SCA

Select function "Safe Cam (SCA)" using PROFIsafe control word S_STW2.23. For SCA, you must use telegram 903, in which control word S_STW2 and status word S_ZSW_CAM1 are available for SCA.

Cam synchronization

For transmission of the cam status word via PROFIsafe to the F host, the cam signals of the two monitoring channels are synchronized. Monitoring is also performed as to whether a different output cam signal from the second channel is plausible. If the drive detects an error, it outputs the message C01711 with the fault value 1014.

As the position tolerance for monitoring the output cam positions, the tolerance for the cross-check of the actual position between the two monitoring channels in p9542 ("Actual value comparison tolerance") is used.

Transmission via PROFIsafe

After SCA has been parameterized and selected, the monitoring results are transmitted in status word S_ZSW_CAM1 (see Chapter "S_ZSW_CAM1 (Page 412)").

5.15.1.1 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2826 SCA (Safe Cam)
- 2844 S_ZSW_CAM1 Safety status word Safe Cam 1

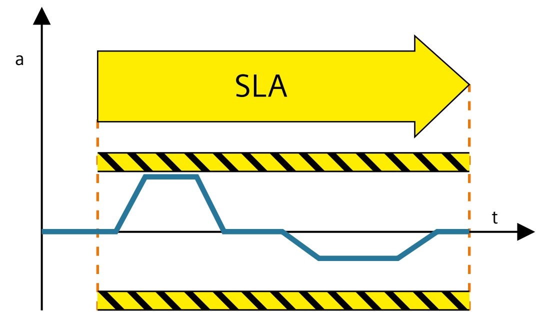
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9503 SI Motion SCA (SN) enable (Control Unit)
- p9505 SI Motion SP modulo value (Control Unit)
- p9536[0...29] SI Motion SCA (SN) plus cam position (Control Unit)
- p9537[0...29] SI Motion SCA (SN) minus cam position (Control Unit)
- p9540 SI Motion SCA (SN) tolerance (Control Unit)
- p9542 SI Motion actual value comparison tolerance (crosswise) (Control Unit)
- r9703.0...31 CO/BO: SI Motion SCA status signal (Control Unit)
- r9708[0...5] SI Motion diagnostics safe position
- r9720.23 CO/BO: SI Motion drive-integrated control signals: Deselect SCA
- r9727 SI Motion user agreement inside the drive
- r9771.22 SI shared functions: SCA supported

5.16 SLA

Definition according to EN 61800-5-2:

Function "Safely-Limited Acceleration (SLA)" prevents the motor from exceeding the specified acceleration limit.



Examples of how the function can be used

Example	Possible solution
In the setup mode, it is not permissible that the drive exceeds the permissible acceleration.	• Select SLA in the converter via PROFIsafe. • The converter limits and monitors the acceleration of the machine.

5.16.1 Description

Function "Safely-Limited Acceleration (SLA)" monitors that the motor does not exceed the defined acceleration limit (e.g. in setup mode). SLA detects early on whether the speed is increasing at an inadmissible rate (the drive accelerates uncontrollably) and initiates the stop response.

SLA is effective when accelerating, however, not when braking.

Note

Safety function "Safely-Limited Acceleration (SLA)" can only be used with an encoder.

Note

Safety function "Safely-Limited Acceleration (SLA)" can only be used for 1-encoder systems.

Note

Configuration only possible in the parameter list

Contrary to other Safety Integrated Functions, there is no configuration screen form in SINUMERIK Operate for SLA. Therefore, parameterize this function in the parameter list.

Enabling SLA

- Enable function "Safely-Limited Acceleration (SLA)" with p9501.20 = 1.

Selecting SLA

Select function "Safely-Limited Acceleration (SLA)" using PROFIsafe control word S_STW1.8 or S_STW2.8. Which control word you use depends on the PROFIsafe telegram that you configured.

Once selected, the SLA function becomes immediately active without any delay.

You can use telegrams 30, 31, 901, 902 and 903 for SLA. These telegrams contain the control words S_STW1.8 and S_STW2.8 and status words S_ZSW1.8 and S_ZSW2.8 for SLA.

Acceleration limit

- You define the acceleration limit to be monitored using parameter p9578. This limit value is applicable for both the positive and negative directions of rotation.
- When setting p9578, the following rule must be complied with:
  – p9578 ≥ 10 · r9790[1]
- The possible acceleration resolution is shown by the drive in r9790:
  – r9790[0] = resolution, coarse
  – r9790[1] = resolution, fine

  The actual accuracy of the acceleration detection depends on the type of actual value acquisition, the gear ratios as well as the quality of the encoder being used.
- The drive indicates the velocity limit corresponding to the actual acceleration in r9714[3].
- r9789 allows the finer resolution acceleration monitoring to be diagnosed. Index 0 indicates the actual acceleration determined. Index 1 and 2 indicate the current limit values of the SLA monitoring.

Filter time

If the determination of the acceleration leads to very noisy signals, the drive cannot reasonably monitor the acceleration.

Remedy

- In this case, increase the "SLA filter time" (p9576).
  Note that SLA reacts with a delay when you increase the filter time.

Stop response

If the SLA subsequently detects violation of the acceleration limit, the drive initiates the stop response configured using p9579.

5.16.2 Details and parameterization

Principle of operation

The following diagram shows the principle of operation of SLA:

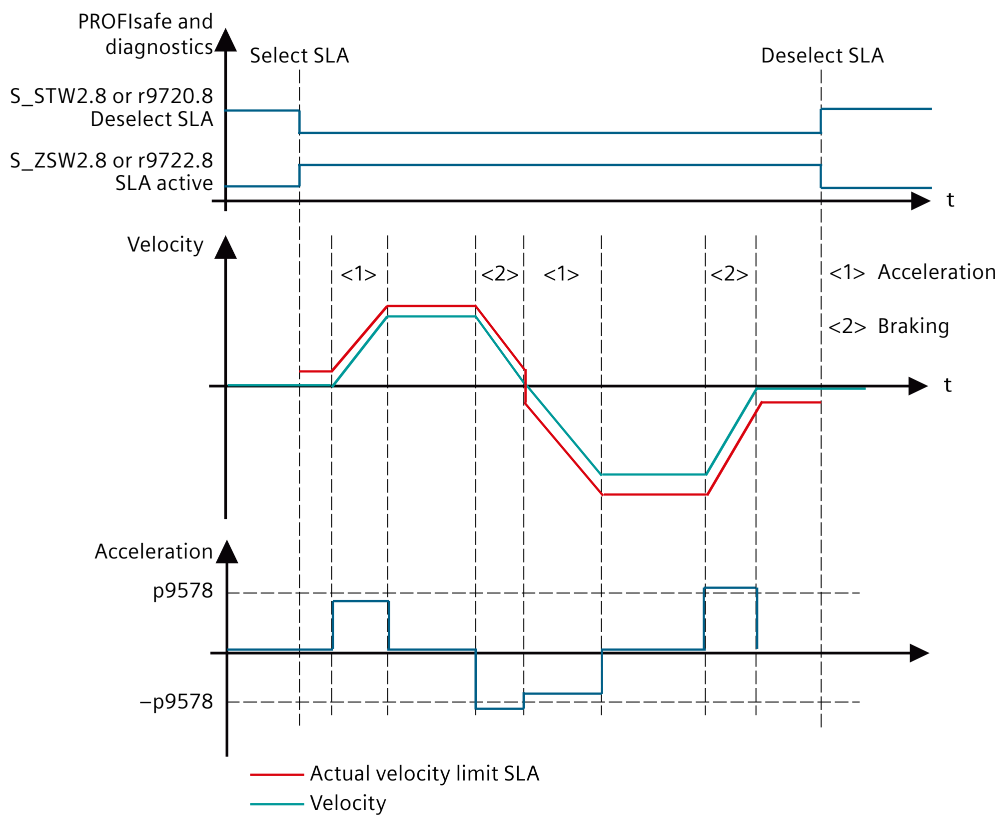


Figure 5-28 Safely-Limited Acceleration (SLA): Principle

5.16.2.1 Transmission via PROFIsafe or SIC

Transmission via PROFIsafe

Once SLA has been parameterized and selected, the monitoring results are transmitted in status words S_ZSW1.8 or S_ZSW2.8.

Note

Response to bus failure

If p9580 ≠ 0 and SLA is active, in the event of a communication failure, the parameterized ESR reaction only occurs if a STOP with delayed pulse suppression when the bus fails has been parameterized as the SLA response (p9579 ≥ 10).

Transfer via SIC

Once SLA has been parameterized and selected, the monitoring results are also transmitted in SIC in status word S_ZSW1B.8. You will find this status word in telegrams 700 and 701.

5.16.2.2 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2838 SLA (Safely-Limited Acceleration)

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9576 SI Motion SLA filter time (CU)
- p9578 SI Motion SLA acceleration limit (CU)
- p9579 SI Motion SLA stop response (Control Unit)
- r9714[3] CO: SI Motion diagnostics velocity: Actual SLA velocity limit on the Control Unit
- r9719.17 CO/BO: SI Motion control signals 2: Deselect SLA
- r9720.8 CO/BO: SI Motion drive-integrated control signals: Deselect SLA
- r9721.11 CO/BO: SI Motion status signals (Control Unit): SLA active
- r9722.8 CO/BO: SI Motion drive-integrated status signals (Control Unit): SLA active
- r9789 CO: SI Motion SLA acceleration acceleration diagnostics
- r9790 SI Motion acceleration resolution

5.17 Safe referencing

The "safe referencing" function allows a safe absolute position to be defined. This safe position is used for the following functions:

- SLP (Page 176)
- SP (Page 181)
- SCA (Page 197)

General description

Referencing to an absolute position is performed by the motion control of the NC. The functionality SIC/SCC is used for this.

For SINUMERIK Safety Integrated or SINUMERIK Safety Integrated plus, the current absolute NC actual position (also in motion) is transferred to the drive as the "reference position" for the safe actual value system. This process is carried out on the system side for each referencing of the NC actual position system. This requires the enabling of SIC/SCC and the "Reference via SCC" function (p9501.27). The "safely referenced" state is reached when user agreement has been set.

Referencing methods

SINAMICS distinguishes between 2 types of referencing:

- Initial referencing
  For initial safe referencing, or in the event of a fault during a subsequent referencing, the following steps are necessary:
  - Perform referencing by the NC
  - Setting user agreement
- Subsequent referencing
  Subsequent referencing involves referencing with a safety-relevant history (i.e. with an internally buffered user agreement) after a POWER ON or after deselecting "parking axis".
  - After the drive has been referenced, Safety Integrated automatically performs a plausibility check.
  - If the deviation between the current absolute position and the previous position saved by Safety Integrated is within the tolerance of p9544, then the drive goes into the "safely referenced" state.

5.17.1 User agreement

Description

With a user agreement, an appropriately authorized person confirms that the currently displayed SI actual position of an axis corresponds to the actual position at the machine.

You can check this by traversing the axis to a known position (e.g. a visual mark) or adjusting/calibrating the axis and then comparing the SI actual position with the "user agreement" screen.

An axis/spindle with integrated safety functions can have the following status:

- User agreement = yes, or
- User agreement = no

All safety axes that require user agreement to be set are listed in the HMI display "user agreement".

The following data are displayed:

- Machine axis name
- Position
- SI position
- User agreement

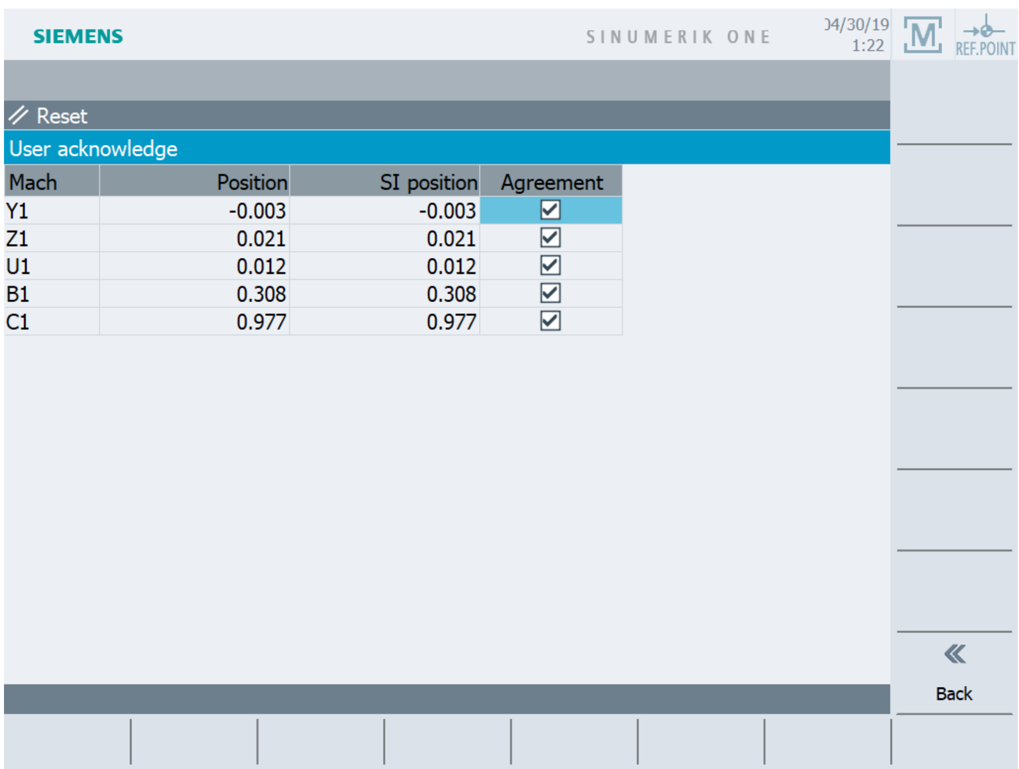


Figure 5-29 User agreement

The user agreement can only be set by an authorized user.

User agreement can be canceled in the following ways:

- By the user
- By selecting a function (e.g. a new gear stage)
- By a fault state (e.g. user acceptance inconsistency in the monitoring channels)

When user agreement is canceled, the "safely referenced" state is always reset.

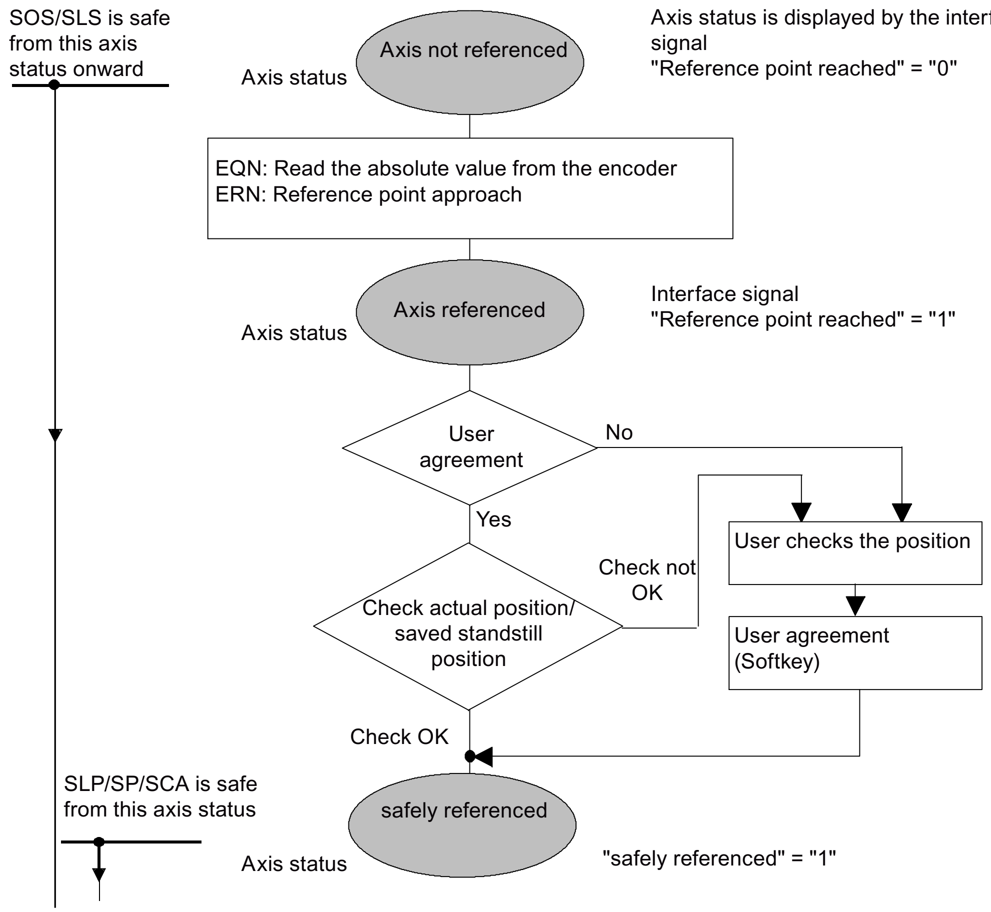


Figure 5-30 Axis states when referencing

Interlocking the user agreement

Before a user agreement can be issued, the interlock must first be canceled:

- Keyswitch: In position 3 → User agreement can be issued

After user agreement has been issued, you must reactivate the interlock (e.g. keyswitch position 3 must be left and the key withdrawn).

5.17.2 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2821 SI Extended Functions - Safe referencing

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9572 SI Motion reference position (Control Unit)
- p9573 Accept SI Motion reference position (Control Unit)
- r9708[0...5] SI Motion diagnostics safe position
- r9713[0...5] CO: SI Motion diagnostics actual position value load side
- r9722.0...31 CO/BO: SI Motion drive-integrated status signals (Control Unit)
- r9723.0...17 CO/BO: SI Motion diagnostics signals integrated in the drive
- p9726 SI motion, user agreement, select/deselect
- p9740 SI motion, user agreement, select/deselect MM

5.18 Safe actual value acquisition

Supported encoder systems

The following encoder systems can in principle be used for safety-related speed/position acquisition:

- Single-encoder systems
  or
- 2-encoder systems

Note

Rules for connecting an encoder

Note when connecting an encoder the valid rules: See SINAMICS S120 Drive Functions Function Manual.

Single-encoder system

In a single-encoder system, only the motor encoder is used to safely acquire the drive actual values. This motor encoder must be appropriately suitable (see encoder types). The actual values are generated in a safety-related fashion either directly in the encoder or in the Sensor Module and are transferred to the Control Unit via DRIVE-CLiQ.

For motors without a DRIVE-CLiQ interface, the connection is made using additional Sensor Modules.

Even if the drive is operating in the closed-loop torque controlled mode, motion monitoring functions may be selected as long as it is guaranteed that the encoder signals can be evaluated.

Note

No "Safe Acceleration Monitoring" for encoder faults in a 1-encoder system

For an encoder fault in a 1-encoder system, the "Safe Acceleration Monitoring" function (p9506 = 3) is not active.

A stop response of category 0 or 1 (EN 60204-1) can be set with parameter p9516.4.

Special feature in the case of linear motors

The motor encoder (linear scale) of linear motors also acts as load measuring system. Only one measuring system is required for this reason. The system is connected by means of a Sensor Module or directly via DRIVE-CLiQ.

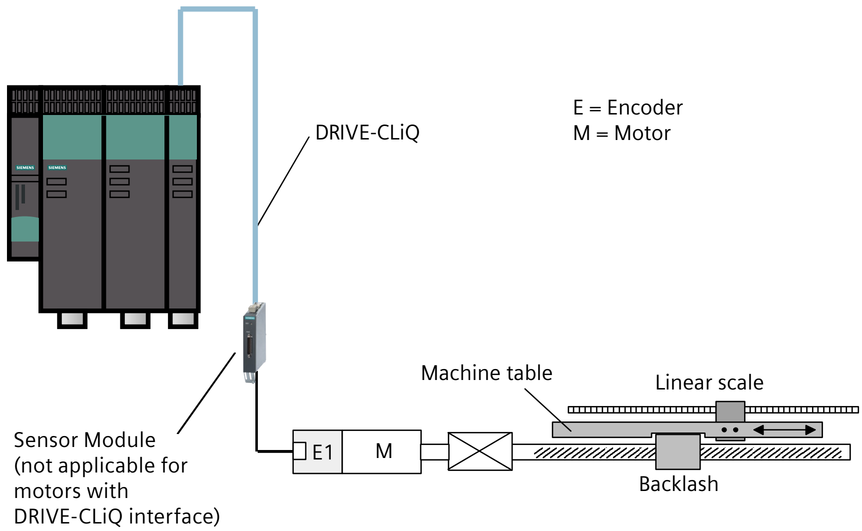


Figure 5-31 Example of a single-encoder system

2-encoder system

The failsafe actual values for a drive are provided by 2 separate encoders. The actual values are transferred to the Control Unit via DRIVE-CLiQ.

For motors without a DRIVE-CLiQ interface, the connection is made using additional Sensor Modules (see encoder types).

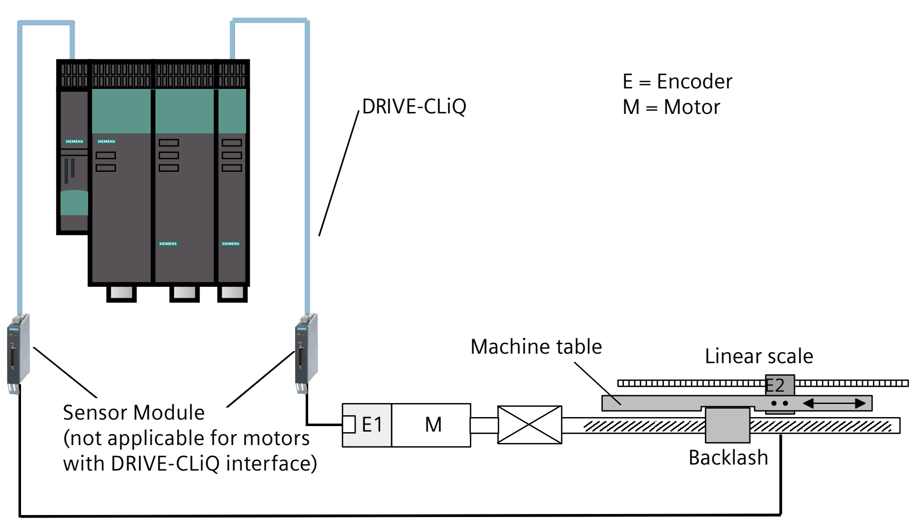


Figure 5-32 Example of a 2-encoder system on a linear axis via a ball screw

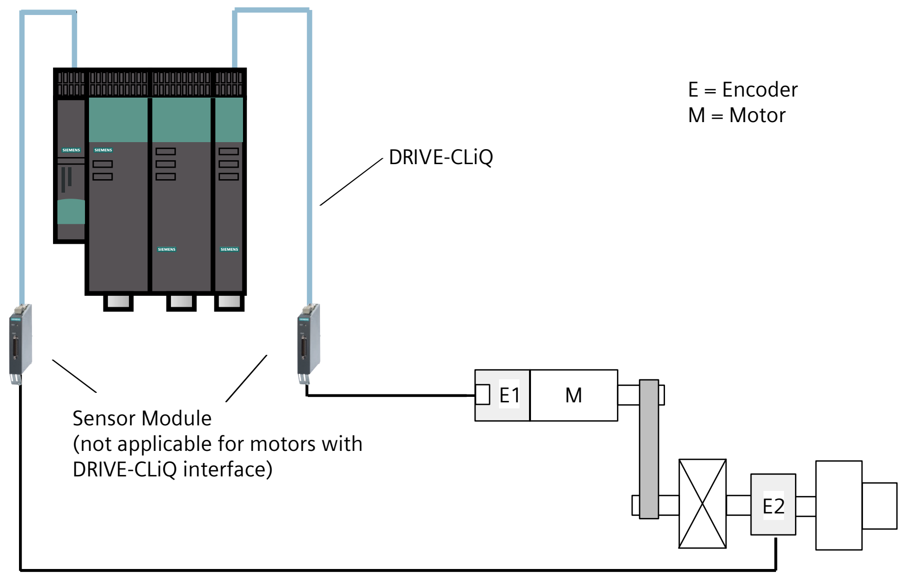


Figure 5-33 Example of a 2-encoder system on a rotary axis

When parameterizing a 2-encoder system with Safety Integrated, you must align parameters p9315 to p9329 with parameters r0401 to r0474.

Note

Assignment of the encoder parameters

Parameters p95xx are assigned to the 1st encoder; parameters p93xx to the 2nd encoder.

Note

Transfer of the values from the encoder commissioning

To accept the values from the parameters filled during the encoder commissioning to the safety parameterization, set parameter p9700 = 46 (2E hex). This copy function is only possible if you are connected online with the drive unit.

Table 5-6 Encoder parameters and corresponding safety parameters for 2-encoder systems

Safety parameters	Designation	Encoder parameters
p9315/p9515 SI Motion coarse position value configuration		
p9315.0/p9515.0	Up-counter	r0474[x].0
p9315.1/p9515.1	Encoder CRC, least significant byte first	r0474[x].1
p9315.2/p9515.2	Redundant coarse position value, most significant bit left-justified	r0474[x].2
p9315.16/p9515.16	DRIVE-CLiQ encoder	p0404[x].10
p9316/p9516 SI Motion encoder configuration, safety functions		
p9316.0/p9516.0	Motor encoder, rotary/linear	p0404[x].0
p9316.1/p9516.1	Actual position value, sign change	p0410[x]
p9317/p9517	SI Motion linear scale grid division	p0407
p9318/p9518	SI Motion encoder pulses per revolution	p0408

Safety parameters	Designation	Encoder parameters
p9319/p9519	SI Motion fine resolution G1_XIST1	p0418
p9320/p9520	SI Motion leadscrew pitch	Encoder parameterizing screen form
p9321/p9521	SI Motion gearbox encoder	Encoder parameterizing screen form
p9322/p9522	SI Motion gearbox encoder	Encoder parameterizing screen form
p9323/p9523	Redundant coarse position value valid bits	r0470
p9324/p9524	Redundant coarse position value fine resolution bits	r0471
p9325/p9525	Redundant coarse position value relevant bits	r0472
p9326/p9526	SI Motion encoder assignment	Encoder parameterizing screen form
p9328/p9528	SI Motion Sensor Module node identifier	
p9329/p9529	Gx_XIST1 coarse position safety most significant bit	p0415 = r0470 – r0471

Encoder types for single and 2-encoder systems

Incremental encoders or absolute encoders can be used for safe acquisition of the position values on a drive.

The absolute position values can be transferred via the serial EnDat interface or an SSI interface to the controller. However, these are not evaluated by the safety functions.

In systems with encoders with SINAMICS Safety Integrated (single and 2-encoder systems), the following encoders are permitted for safe actual value acquisition:

- Encoders with sin/cos 1 Vpp signals
  - Single and 2-encoder systems
  - Connected to the SINAMICS SME20/25, SME120/125 and SMC20 Sensor Modules
  - The encoders must contain purely analog signal processing and creation. This is necessary to be able to prevent the A/B track signals with valid levels from becoming static ("freezing").
- HTL/TTL encoders
  - Can only be used for 2-encoder systems. In this case, one encoder must be an HTL/TTL encoder. The other encoder can be a sin/cos encoder or an HTL/TTL encoder.
  - Connected to an SMC30 Sensor Module Cabinet or to SINAMICS HLA or SINAMICS S120 Combi.
  - An HTL/TTL encoder connected to SINAMICS HLA or SINAMICS S120 Combi must not be operated as first encoder.
  - Note the lowest possible velocity resolution (r9732[1]) for an HTL/TTL encoder system.

Note

Encoders with integrated DRIVE-CLiQ interface

These encoders must be certified at least according to IEC 61800-5-2 (SIL2) or ISO 13849-1 (Performance Level d / Category 3).

A fault mode effect analysis (FMEA) for securing the encoder on the motor shaft or on the linear drive must be performed. The result must be that the risk of the encoder mounting loosening is defined as a fault that can be ruled out (see DIN EN 61800-5-2, 2008, Table D.16). The encoder would no longer correctly map the motion if its mounting were to become loose.

It should be noted that the machine manufacturer has sole responsibility for the fulfillment of the above-described requirements. Information on the internal realization of the encoder must come from the encoder manufacturer. The FMEA must be created by the machine manufacturer.

Information about Siemens motors with and without DRIVE-CLiQ connection, which can be used for Safety Integrated Functions, is available in the SIOS Portal:

Suitable motors and encoders (https://support.industry.siemens.com/cs/ww/en/view/33512621)

For these motors, the encoder mounting on the motor shaft can be considered to be safety relevant, and faults associated with an encoder becoming loose ruled out.

Note

Basic absolute encoders with EnDat interface and additional sin/cos tracks

Basic absolute encoders (e.g. EQI) that offer an EnDat interface with additional sin/cos tracks, but operate according to an inductive measuring principle internally, are not permitted for SINAMICS Safety Integrated.

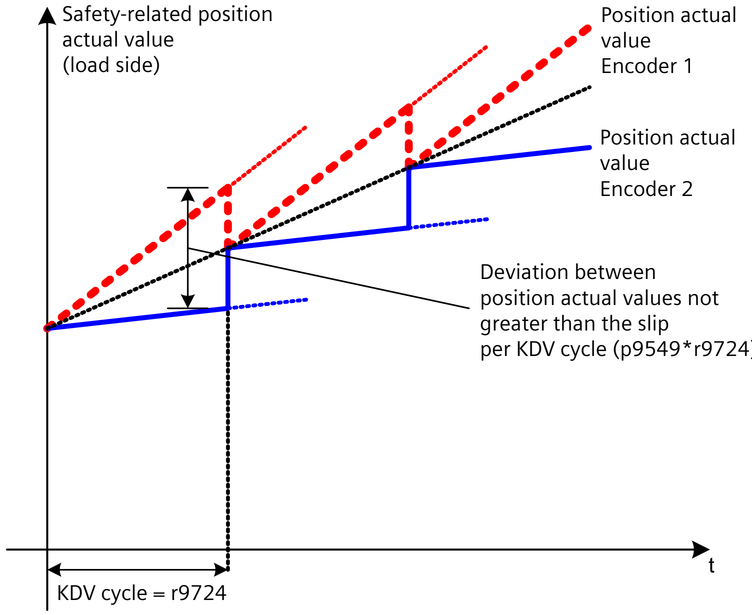
Note

Encoder types for SINAMICS HLA

The following encoder types are permissible for SINAMICS HLA:

- Single-encoder systems
  - DRIVE-CLiQ encoder with safety capability
  - sin/cos encoder connected via SME20/25, SME120/125 or SMC20 (1Vpp, pure analog signal processing)
- 2-encoder systems
  - Encoders with DRIVE-CLiQ connection
  - sin/cos encoder connected via SME20/25, SME120/125 or SMC20 (1Vpp, pure analog signal processing)
  - HTL/TTL encoder connected via SMC30 (not in connection with SINUMERIK)
  - TTL encoder connected via the onboard interface of the HLA module (not in connection with SINUMERIK)

Actual value synchronization



1) This deviation cannot be larger than the position difference that can occur at maximum slip (p9549) during a cross-check cycle (r9724).

Figure 5-34 Example diagram of actual value synchronization

The mean value of the actual values of both channels is calculated cyclically after actual value synchronization (p9301.3 = 1) has been activated, for example, for systems or machines with slip. The maximum slip defined in p9549 is monitored in the cross-check cycle (r9724). If "actual value synchronization" is not enabled, the value parameterized in p9542 is used as tolerance value for the crosswise comparison.

Safe motion monitoring

The properties of the actual value acquisition determine not only the encoders used, but also the values for safe motion monitoring that can be achieved in the best case.

- Safe maximum speed (r9730)
  The maximum speed (load side) that is permissible due to the acquisition of actual values for safe motion monitoring functions is indicated in r9730. This parameter shows up to which load velocity the safety-related encoder actual values (redundant coarse encoder position) can still be correctly sensed as a result of the particular encoder parameterization.
  The actual value acquisition clock (p9511) determines the frequency at which the actual values are acquired. The longer the clock cycle, the higher the "safe maximum velocity." On the other hand, a longer actual value acquisition clock cycle places a greater load on the Control Unit. You must consider this when setting the optimum for your particular application.
- Safe positioning accuracy (r9731)
  This positioning accuracy can be achieved in the best case by acquiring the actual values. If a 2-encoder system is used, the accuracy of the poorer encoder is indicated based on the number of encoder pulses.

5.18.1 Important parameters

Overview of important parameters - with encoder system (see SINAMICS S120/S150 List Manual)

• p9501.3	SI Motion enable safety functions (Control Unit), enable actual value synchronization
• p9502	SI Motion axis type (Control Unit)
• p9511	SI Motion actual value acquisition clock (Control Unit)
• p9515	SI Motion encoder coarse position value configuration (Control Unit)
• p9516	SI Motion encoder configuration safety functions (Control Unit)
• p9517	SI Motion linear encoder grid division (Control Unit)
• p9518	SI Motion encoder pulses per revolution (Control Unit)
• p9519	SI Motion fine resolution G1_XIST1 (Control Unit)
• p9520	SI Motion leadscrew pitch (Control Unit)
• p9521[0...7]	SI Motion gearbox encoder (motor)/load denominator (Control Unit)
• p9522[0...7]	SI Motion gearbox encoder (motor)/load numerator (Control Unit)
• p9523	SI Motion redundant coarse position value valid bits (Control Unit)
• p9524	SI Motion redundant coarse position value, fine resolution (Control Unit)
• p9525	SI Motion redundant coarse position relevant bits (Control Unit)
• p9526	SI Motion encoder assignment second channel
• p9542	SI Motion actual value comparison tolerance (crosswise) (Control Unit)
• p9549	SI Motion slip velocity tolerance (Control Unit)
• p9700	SI Motion copy function
• r9713[0...5]	SI Motion diagnostics actual position value load side
• r9714[0...2]	SI Motion diagnostics velocity
• r9724	SI Motion, cross-check cycle
• r9730	SI Motion safe maximum speed
• r9731	SI Motion safe positioning accuracy
• r9732[0...1]	SI Motion velocity resolution

Overview of important parameters - without encoder system

• p9585	SI Motion actual value acquisition without encoder fault tolerance (CU)
• p9586	SI Motion actual value acquisition without encoder delay time (CU)
• p9587	SI Motion actual value acquisition without encoder filter time (CU)
• p9588	SI Motion actual value acquisition without encoder minimum current (CU)
• p9589	SI Motion actual value acquisition without encoder acceleration limit (CU)
• p9700	SI Motion copy function
• r9732[0...1]	SI Motion velocity resolution

5.19 Safe gearbox stage switchover

"Safe gearbox switchover" allows you to switch between 8 gearbox ratios in operation. Switchover between gearbox ratios is only possible via PROFIsafe (p9601.3 = 1).

Parameterization

Before you can use "Safe gearbox switchover", you must parameterize the following values:

- Gear ratios
  You can set up to 8 different gearbox ratios using parameter p9521 (denominator) and p9522 (numerator).
- Direction reversal
  Using parameter p9539, you can set as to whether a direction of rotation reversal is involved for the particular gearbox.
- Position tolerance
  As a result of the motion that can possibly occur when switching over the gearbox, it may be necessary to increase the tolerance threshold for the duration of the switchover operation. Using parameter p9539, you set how the tolerance is calculated when switching over the gearbox:
  - Without actual value synchronization: p9542 × p9543
  - With actual value synchronization: p9549 × p9543

Selection

Proceed as follows to enable the "Safe gearbox switchover" function:

1. Set p9501.26 = 1
   - If control via PROFIsafe is not parameterized, then the converter outputs fault F01681 with the appropriate fault value.
   - If you activate the "Safe gearbox switchover" function on a converter, which does not support the function, then the converter outputs fault F01682 with fault value 39.
2. Switch off the drive unit and then on again (POWER ON).

Gearbox switchover without increased position tolerance

In order to switch over the gearbox stage, where no increased tolerance is required for the crosswise comparison of the actual positions, proceed as follows:

1. Set the new gearbox stage using bits 0 to 2 in byte 3 of S_STW2.
   - The actual values are then synchronized once automatically. This synchronization is used to compensate any possible difference that occurs between the position actual values of the two monitoring channels as a result of the switchover operation.
   - The new gearbox stage is then active.

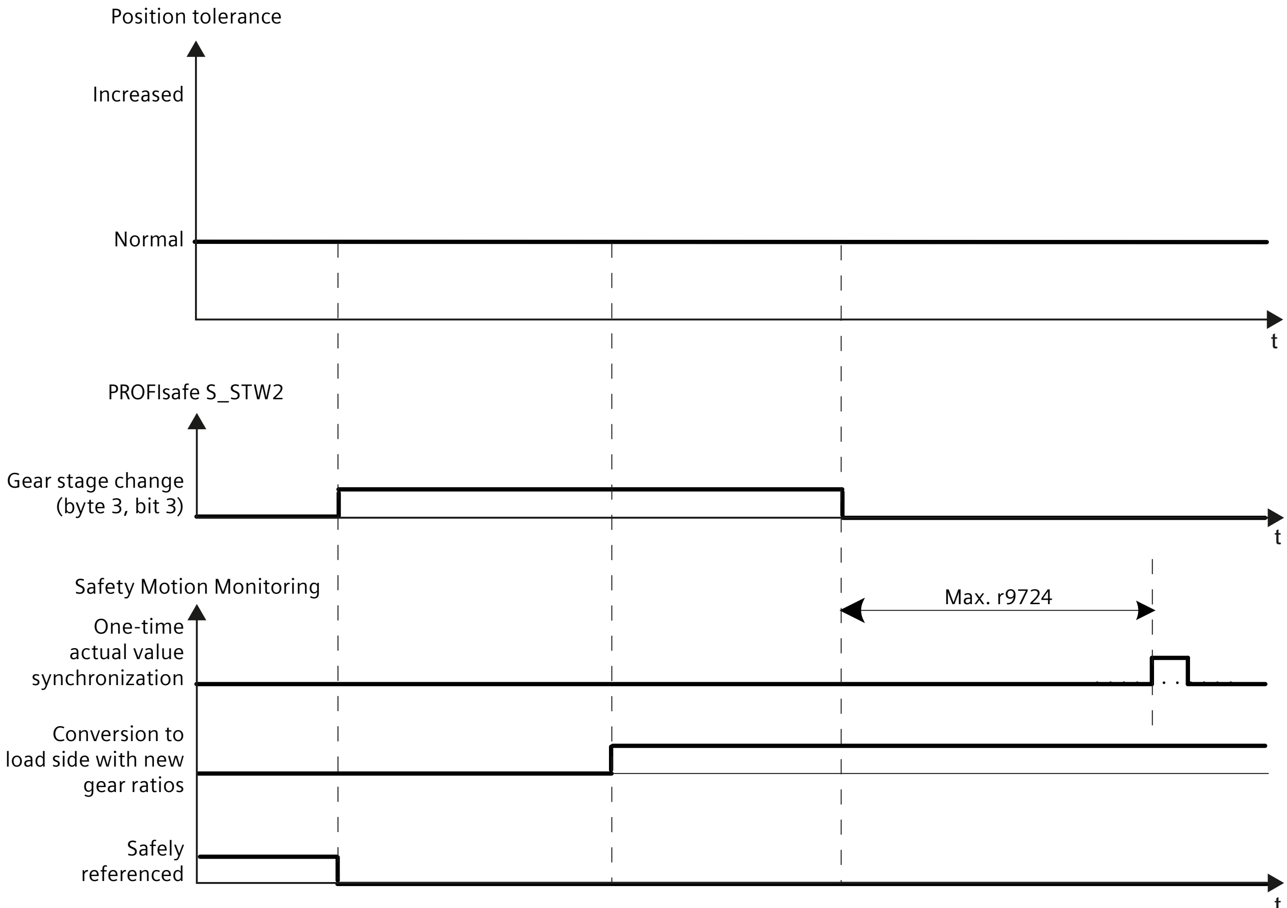


Figure 5-35 Gearbox switchover from stage "0" to "1" without increased position tolerance

Gearbox switchover with increased position tolerance

In order to switch over the gearbox stage, where increased tolerance is required for the crosswise comparison of the actual positions, proceed as follows:

Note

Maximum duration of the increased position tolerance

It is not permissible that the increased position tolerance is set for longer than 2 min. If this time is exceeded, then the converter outputs alarm C01711 with fault value 1015 (≙ STOP F).

1. Set the increased position tolerance using bit 3 (= 1) in byte 3 of S_STW2.
2. Set the new gearbox stage using bits 0 to 2 in byte 3 of S_STW2.
3. Set the position tolerance back to the normal value using bit 3 (= 0) in byte 3 of S_STW2.
   – The actual values are then synchronized once automatically. This synchronization is used to compensate any possible difference that occurs between the position actual values of the two monitoring channels as a result of the switchover operation.
   – The new gearbox stage is then active.

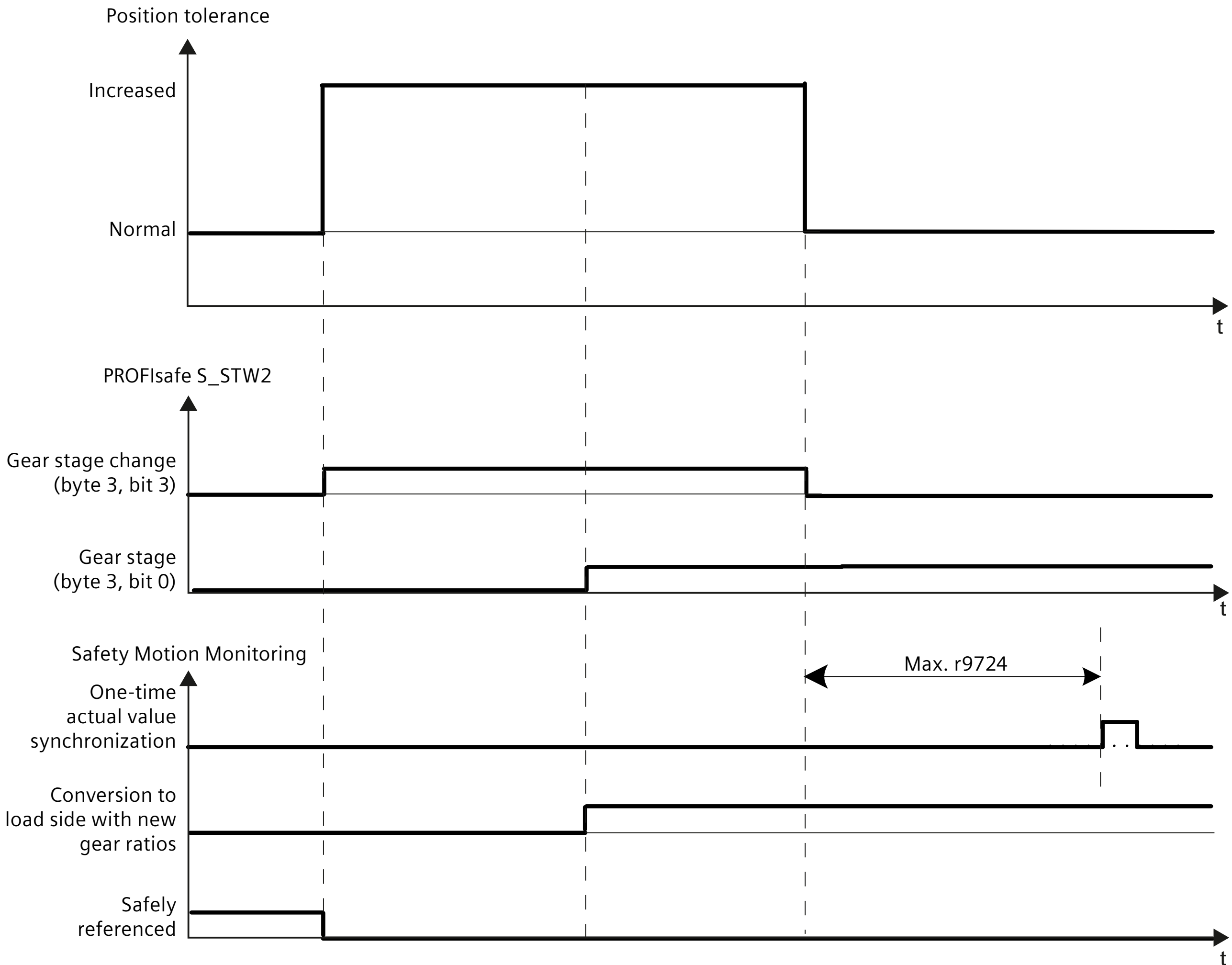


Figure 5-36 Gearbox switchover with increased position tolerance

Diagnostics

The selected gearbox stage is displayed for diagnostic purposes in parameter r9720, bits 24 to 26.

The selected gearbox stage is displayed for diagnostic purposes in parameter r9720, bit 27.

Safe gearbox switchover and referencing

The gearbox stage switchover means that the reference position and the user agreement are lost. This means that after a gearbox switchover, initial referencing is required, in order to return to the "safely referenced" state (see Chapter Safe referencing (Page 204)).

5.19.1 Important parameters

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501.26 SI Motion enable safety functions (Control Unit): Enable reliable gearbox switchover
- p9521[0...7] SI Motion gearbox encoder (motor)/load denominator (Control Unit)
- p9522[0...7] SI Motion gearbox encoder (motor)/load numerator (Control Unit)
- p9539[0...7] SI Motion gearbox direction of rotation reversal (Control Unit)
- p9542 SI Motion actual value comparison tolerance (crosswise) (Control Unit)
- p9543 SI Motion gearbox switching position tolerance factor (CU)
- p9549 SI Motion slip velocity tolerance (Control Unit)
- r9720.0...27 CO/BO: SI Motion drive-integrated control signals

5.20 Forced checking procedure

The functions and switch-off signal paths must be tested at least once within a defined period to establish whether they are working properly in order to meet the requirements of EN ISO 13849-1 and IEC 61508 in terms of timely error detection.

The maximum permissible interval for a test stop/forced checking procedure for Basic and Extended Functions is 8760 hours; i.e. the forced checking procedure must be performed at least once per year.

This functionality must be implemented by initiating a test stop/forced checking procedure either in the cyclic manual mode or as part of an automated process.

The test stop cycle is monitored. When the parameterized timer expires (also after POWER ON / warm restart), alarm A01697: "SI Motion: Test of motion monitoring required" is generated and a status bit is set which can be transferred to an output or to a PZD bit via BICO. This alarm does not affect machine operation.

5.20.1 Examples for when the forced checking procedure is carried out

When the appropriate safety devices are implemented (e.g. protective doors), it can be assumed that running machinery will not pose any risk to personnel. For this reason, an alarm is only output to inform the user that a forced checking procedure run is due and to request that this be carried out at the next available opportunity.

Examples of when to carry out forced checking procedure:

- When the drives are at a standstill after the system has been switched on (POWER ON).
- Before the protective door is opened.
- At defined intervals (e.g. every eight hours).
- In automatic mode (time and event dependent).

5.20.2 Options and control

Note

Requirements

STO is triggered when a test stop is carried out for the Safety Integrated Functions. It is not permissible that STO is selected before selecting the test stop.

When blocksize Power Modules are used, the test stop must be triggered under controlled standstill conditions (speed setpoint setting 0, current is flowing through the motor).

The forced checking procedure (test stop) can be triggered at any time by an application. The parameter assignment and control are performed as follows:

- **Controlled via SCC (integrated drives, external drives), programmed in the application**
  You can perform the test stop via SCC, programmed in the application itself. The following parameters are relevant:
  - p9559 SI Motion Forced checking procedure timer (Control Unit)
  - p9705 BI: SI Motion Test stop signal source
  - r9723.0 CO/BO: SI Motion diagnostics signals integrated in the drive

  See: Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 231)
  If the test stop is executed as described, the action does not require a POWER ON. The acknowledgment is set by canceling the test stop request.

Controlling safety functions integrated in the drive 6

6.1 Control possibilities

The following options are available for controlling safety functions integrated in the drive:

Table 6-1 Controlling the Safety Integrated Functions

Scope **Control type**	**Basic Functions**	**Extended Functions**
Telegrams to control process data via PROFIsafe and SIC/SCC (PROFIdrive) See: • Overview of telegram/process data (Page 224) • Controlling via PROFIsafe (Page 227) • SIC/SCC (Page 231)	Yes	Yes
Controlling via terminals (on the Control Unit and on the Motor/Power Module) See: Control via terminals on the Control Unit (Page 233)	Yes	No

Note

Term "Control Unit" in this documentation

In the Safety Integrated environment and in this documentation the term "Control Unit" designates the SINUMERIK NCU.

6.2 Overview of telegrams

You can use the following safety-oriented telegrams.

- PROFIsafe telegram 30
  PROFIsafe standard telegram
- PROFIsafe telegram 31
  Extended PROFIsafe standard telegram
- SIEMENS telegram 701
  Manufacturer-specific telegram for SIC/SCC communication. With SINUMERIK, SIC/SCC communication only takes place via telegram 701.
- SIEMENS telegram 901
  Extended manufacturer-specific telegram with 16-bit position value.
- SIEMENS telegram 902
  Extended manufacturer-specific telegram with 32-bit position value.
- SIEMENS telegram 903
  Extended manufacturer-specific telegram with 32-bit Safe Cam (S_ZSW_CAM1). Default setting for internal NC drives.

The following overview shows which process data is transferred in which telegram types.

6.3 Overview: Process data in telegrams

Table 6-2 Process data from PROFIsafe telegrams

Telegram Process data	30	31	901	902	903
Safety control word 1 S_STW1	PZD1	–	–	–	–
Safety status word 1 S_ZSW1	PZD1	–	–	–	–
Safety control word 2 S_STW2	–	PZD1...2	PZD1...2	PZD1...2	PZD1...2
Safety status word 2 S_ZSW2	–	PZD1...2	PZD1...2	PZD1...2	PZD1...2
SLS limit value input S_SLS_LIMIT_A	–	–	PZD3	PZD3	PZD3
Active SLS limit value S_SLS_LIMIT_A_ACTIVE	–	–	PZD3	PZD3	PZD5
Counter for the safety cycle S_CYCLE_COUNT	–	–	PZD4	PZD4	–
Actual position value (16 bits) S_XIST16	–	–	PZD5	–	–
Actual position value (32 bits) S_XIST32	–	–	–	PZD5...6	–
Safe Cam status word S_ZSW_CAM1	–	–	–	–	PZD3...4

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

Table 6-3 Process data from SIEMENS telegram 701 (SIC/SCC)

Telegram Process data	701
Safety Control Channel control word 1 S_STW1B	PZD1
SI Motion Safety Info Channel status word S_ZSW1B	PZD1
Safety Info Channel status word 2 S_ZSW2B	PZD2
Safety Control Channel control word 3 S_STW3B	PZD2
SLS setpoint speed limiting (32 bit) S_V_LIMIT_B	PZD3...4
Safety Info Channel status word 3 S_ZSW3B	PZD5

Detailed information about the process data of telegram 701 is provided in Chapter "SIC/SCC (PROFIdrive) process data (Page 414)".

6.4 Controlling via PROFIsafe

6.4.1 Selecting the PROFIsafe telegram

You can use telegrams 903, 902, 901, 31 or 30 for PROFIsafe communication via PROFIBUS and PROFINET. SIEMENS telegram 903 is the default setting for internal NC drives.

You make the settings for the F-PLC (F-host) in the TIA Portal; the settings for the individual drives (F-slaves or F-devices), in SINUMERIK Operate (p60022, p9611, p9811).

Table 6-4 Parameter to select the PROFIsafe telegram

Parameter/name	Setting	Meaning
p60022 PROFIsafe telegram selection / Ps tel-egr_sel p9611 SI PROFIsafe telegram selection (Con-trol Unit) / SI Ps telegr CU p9811 SI PROFIsafe telegram selection (Motor Module) / SI Ps telegram MM	903	• PROFIsafe SIEMENS telegram 903 • Extended manufacturer-specific telegram with 32-bit Safe Cam • Default setting for internal NC drives
	902	• PROFIsafe SIEMENS telegram 902, PZD-3/6 • Extended PROFIsafe telegram with 32-bit position value
	901	• PROFIsafe SIEMENS telegram 901, PZD-3/5 • Extended PROFIsafe telegram with 16-bit position value
	31	• PROFIsafe standard telegram 31, PZD-2/2 • Extended standard PROFIsafe telegram
	30	• PROFIsafe standard telegram 30, PZD-1/1 • Standard PROFIsafe telegram

Detailed information about the structure of the telegrams is provided in Chapter "Telegram structure and data (Page 395)".

The PROFIsafe telegram received at the Control Unit is indicated in r9768, and the PROFIsafe telegram to be sent, in parameter r9769.

Note

Timing between the switching operations

Message F01611 with fault value 1000 indicates that the switching operations occur too frequently.

- STO is being permanently initiated via PROFIsafe (also as subsequent response).

Within the time 5 × p9650, there must be at least two switching operations via PROFIsafe with a minimum time between them of p9650.

6.4.2 Enabling PROFIsafe control

Control via PROFIsafe is available for both Safety Integrated Basic Functions and Safety Integrated Extended Functions, and must be enabled in p9601

Table 6-5 Parameter to enable the PROFIsafe control

Parameters	Name	Setting	Meaning
p9601	SI enable functions integrated in the drive (Control Unit) / SI enable fct CU	0008 hex	Basic Functions are enabled via PROFIsafe (permissible for r9771.6 = 1).
		0009 hex	Basic Functions are enabled via PROFIsafe and onboard terminals (permissible for r9771.6 = 1).
		000C hex	Extended Functions are enabled via PROFIsafe (permissible for r9771.4 = 1).
		000D hex	Extended Functions are enabled via PROFIsafe - and Basic Functions via onboard terminals (permissible for r9771.4 = 1).
		p9601.0 = 1	Enable STO (SH) via terminals (CU) **Comment:** Safety Integrated Basic Functions via PROFIsafe and via terminals Control of the Basic Functions via terminals on the Control Unit and on the Motor/Power Module (parameters p9601.0 = 1) may be enabled in parallel. In order to be able to select SS1, an SS1 delay time p9652 > 0 must be configured. With PROFIsafe, both SS1 and STO can be selected. Only SS1 is available for control via terminal. STO takes priority over SS1, i.e. STO becomes active if SS1 and STO are simultaneously selected.
r9771	SI common functions (Control Unit) / SI common fct CU	r9771.4 = 1	Extended Functions, PROFIsafe supported
		r9771.6 = 1	Basic Functions, PROFIsafe supported

6.4.3 ESR response in the event of a communication error

The response of the SINAMICS S drive in the case of a communication error when the "Extended stop and retract (ESR)" function module is simultaneously enabled is described in the following.

Requirement

- The Safety Integrated Extended Functions are controlled via PROFIsafe
- The function module "Extended stop and retract" is activated and enabled

Communication failure

Under communication failure in this context, we understand one of the following possibilities:

- Interruption/fault of the PROFIBUS or PROFINET connection for control via PROFIsafe
- STOP response of the F-PLC

Drive response

In the event of a communication failure, SINAMICS S makes a distinction between the following responses:

- If p9580 ≠ 0 and ESR has been enabled, in the event of a communication failure, the parameterized ESR response is realized.
- If p9580 ≠ 0 and SLS is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SLS response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9563[0...3] ≥ 10).
- If p9580 ≠ 0 and SDI is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SDI response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9566[0...3] ≥ 10).
- If p9580 ≠ 0 and SLP is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SLP response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9562[0...1] ≥ 10).

Note

Maximum response time for interruption in communication

When a safety-relevant communication is interrupted, Safety Integrated only permits a response time (p9580) of max. 800 ms. The drive changes into the "fail safe state" once this time expires. In this case, S_STW1/2 is assumed to be 0. This means that all safety functions are selected. STO has in this case the highest priority, i.e. the pulses are safely canceled.

6.4.4 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2840 SI Extended Functions - SI Motion drive-integrated control signals/status signals
- 2858 SI Extended Functions - control via PROFIsafe (p9601.2 = p9601.3 = 1)

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9563[0...3] SI Motion SLS (SG)-specific stop response (Control Unit)
- p9566 SI Motion SDI stop response (Control Unit)
- p9580 SI Motion STO delay bus failure (Control Unit)
- p9601 SI enable functions integrated in the drive (Control Unit)
- p9610 SI PROFIsafe address (Control Unit)
- p9611 SI PROFIsafe telegram selection (Control Unit)
- p60022 Selecting a PROFIsafe telegram

6.5 Safety Info Channel and Safety Control Channel (SIC/SCC)

Note

Precondition for the function of the Safety Info Channel (SIC)/Safety Control Channel (SCC).

Precondition for the function of the Safety Info Channel (SIC)/Safety Control Channel (SCC) is that option "SINUMERIK ONE Safety Integrated - F-PLC" is set.

In the "SINUMERIK Safety Integrated (F-PLC)" mode, status and control signals of the drive-based motion monitoring functions are connected to the PLC and NC:

- Via the Safety Control Channel (SCC), control signals are sent from the PLC and NC to the drive (e.g. to start the "Safe Brake Test (SBT)" function in the drive - and to influence it).
- Via the Safety Info Channel (SIC), status signals of the drive are sent to the PLC (e.g. for the brake test).
- For a STOP response of the drive, status signals are transferred to the NC as well as to the PLC. The motion control in the NC therefore responds automatically to the drive STOP responses by no longer issuing additional setpoints for the path, for example. As a consequence, alarms to be acknowledged are avoided, such as "Contour monitoring" or "Positioning monitoring".

You can parameterize SIC/SCC as follows, and access the signals:

- You activate SIC/SCC while commissioning the drive in SINUMERIK Operate.
- The SIC/SCC signals are mapped in the PLC user interface, and can therefore be accessed via axis DBs.
  See: PLC user interface of the axis/spindle signals (Page 232), Interface signals: Axis/spindle signals (Page 419)

Note

SIC and SCC must always be jointly configured and/or parameterized.

6.5.1 Safety Info Channel (SIC)

Status information of the Safety Integrated functionality of the drive (S_ZSW1B, S_ZSW2B, S_ZSW3B and S_V_LIMIT_B) can be transferred to the F-PLC and NC using the Safety Info Channel (SIC).

6.5.2 Safety Control Channel (SCC)

Control information (S_STW1B and S_STW3B) can be transferred from the F-PLC and the NC to the safety functions of the drive using the Safety Control Channel (SCC).

6.5.3 SIC/SCC communication using telegram 701

SIC/SCC communication can always be transferred using the predefined PROFIdrive telegrams 700 or 701. For SINUMERIK, only telegram 701 (Page 395) is used.

If another telegram is configured for SIC/SCC, then cyclic SIC/SCC communication is inhibited, and Alarm 27811 is output.

6.5.4 PLC user interface of the axis/spindle signals

In the Safety Integrated mode, additional axis-specific data from the axis DB (LBP_Axis1 ... LBP_Axis31) are relevant, which are formed from the SIC/SCC.

Additional information

- You can find the significance of the individual axis DB signals and the precise addresses at Interface signals: Axis/spindle signals (Page 419).
- See also: SBT: Connection to NC and PLC programs

6.5.5 Important parameters

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- r9733[0...2] CO: SI Motion speed setpoint limit active
- r9734.0...15 CO/BO: SI Safety Info Channel status word S_ZSW1B
- r9743.4...15 CO/BO: SI Safety Info Channel status word S_ZSW2B
- r10231 SI Motion SBT control word diagnostics
- r10234.0...15 CO/BO: SI Safety Info Channel status word S_ZSW3B
- p10235 CI: SI Safety Control Channel control word S_STW3B
- p10250 CI: SI Safety Control Channel control word S_STW1B
- r10251.8...12 CO/BO: SI Safety Control Channel control word S_STW1B diagnostics
- p60122 IF1 PROFIdrive SIC/SCC telegram selection

6.6 Control via terminals on the Control Unit

6.6.1 Features

- Control via terminals is only available for Basic Functions.
- Dual-channel structure via 2 digital inputs (Control Unit/power unit)
- In order to prevent nuisance trips as a result of signal disturbances or non-symmetrical test signals, the signals can be debounced at the terminals of the connected components (pushbuttons, switches etc.).
  You can specify these debounce times in the following parameters:
  - p9651 SI STO/SBC/SS1 debounce time (Control Unit) / SI STO t_debou CU
  - p9851 SI STO/SBC/SS1 debounce time (Motor Module) / SI STO t_debou MM
- Different terminal blocks depending on the format.
- Automatic ANDing of up to 8 digital inputs (p9620[0...7]) on the Control Unit with parallel configuration of power units in the chassis format is not supported.

The various SINUMERIK components and SINAMICS power unit formats have different terminal designations for the inputs used for the safety functions. These are shown in the following table.

Table 6-6 Inputs for safety functions

Component	**1st switch-off signal path (p9620[0])**	**2nd switch-off signal path (EP terminals)**
NCU	Selected using BICO interconnection (BI: p9620[0]): Digital input DI 0...7	
NX module	Selected using BICO interconnection (BI: p9620[0]): Digital input DI 0...3	
Single Motor Module Booksize/Booksize Compact	X122.1....6/X132.1...6DI 0...7/16/17/20/21	EP terminals X21.3 and X21.4 (on the Motor Module)
Single Motor Module/ Power Module Chassis	X122.1....6/X132.1...6DI 0...7/16/17/20/21	EP terminals X41.1 and X41.2
Double Motor Module Booksize/Booksize Compact	X122.1....6/X132.1...6DI 0...7/16/17/20/21	EP terminals on the Motor Module: X21.3 and X21.4 (motor connection X1) X22.3 and X22.4 (motor connection X2)
Power Module Blocksize with CUA31/CUA32	X122.1....6/X132.1...6DI 0...7/16/17/20/21	X210.3 and X210.4 (on the CUA31/ CUA32)
Control Unit CU320-2	X122.1....6/X132.1...6DI 0...7/16/17/20/21	

For further information about the terminals, see the Equipment Manuals.

6.6.2 Terminals for STO, SS1 (time-controlled), SBC

Safety functions STO, SS1 (time-controlled) and SBC are selected/deselected separately for each drive using 2 terminals.

Basic procedure

The functions are separately selected/deselected for each drive using two terminals.

1. Switch-off signal path, Control Unit:
   - Input terminal for Safe Torque Off (STO):
     Selected using BICO interconnection (BI: p9620[0]).
   - Possible signal sources:
     NCU: Digital input DI 0...7
     NX modules: Digital input DI 0...3
2. Motor Module switch-off signal path:
   The input terminal is the "EP" terminal ("Enable Pulses").
   The EP terminal is periodically interrogated with a sampling time, which is rounded off to an integer multiple of the current controller cycle; however, it is a minimum of 1 ms. (Example: t_i = 400 µs, t_{EP} => 3x, t_i = 1.2 ms)

Both terminals must be energized within the tolerance time p9650/p9850 (Page 236), otherwise a fault is output.

Example: Terminals for STO

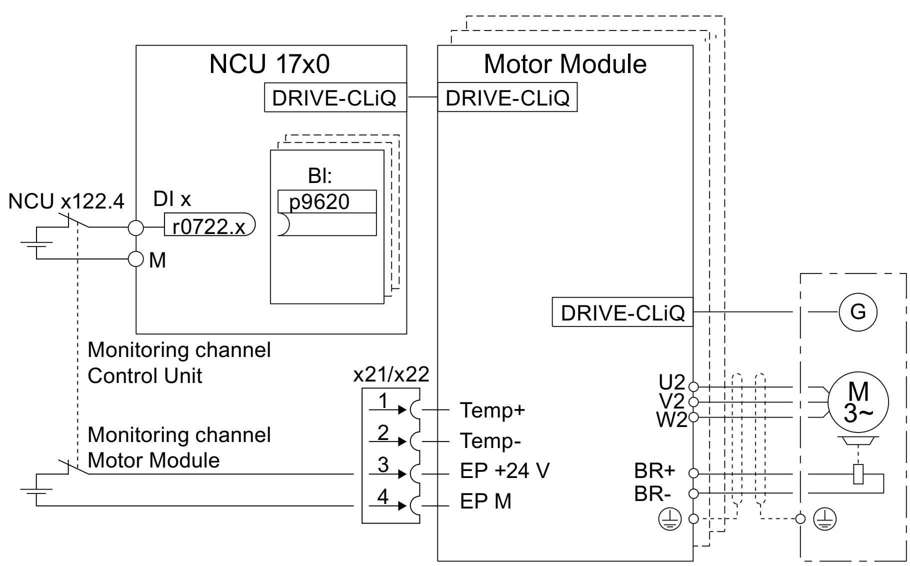


Figure 6-1 Example: Terminals for STO for an NCU 17x0 and a Motor Module in the booksize format

6.6.3 Grouping drives

To ensure that the safety function for several drives can be initiated simultaneously, you must group the terminals for the corresponding drives.

Note

Response of the "STO" safety function when grouping

If a fault in a drive results in a "Safe Torque Off" (STO), this does not automatically mean that the other drives in the same group also switch to "Safe Torque Off" (STO).

Basic procedure

Proceed as follows to group the corresponding drives:

1. Switch-off signal path, Control Unit
   Group by appropriately interconnecting the binector input to the common input terminal for the drives belonging to a group.
2. Motor Module switch-off signal path
   Group by appropriately connecting terminal "EP" for the individual Motor Modules belonging to a group.

Note

Parameterization of the grouping

The grouping must be set the same in both monitoring channels.

The assignment is checked during the test for the switch-off signal paths. The operator selects the STO safety function for each group. The check is drive-specific.

Example: Terminal groups

It must be possible to select/deselect safety function STO separately for group 1 (drives 1 and 2) and group 2 (drives 3 and 4).

For this purpose, the same grouping for STO must be realized both for the Control Unit and the Motor Modules.

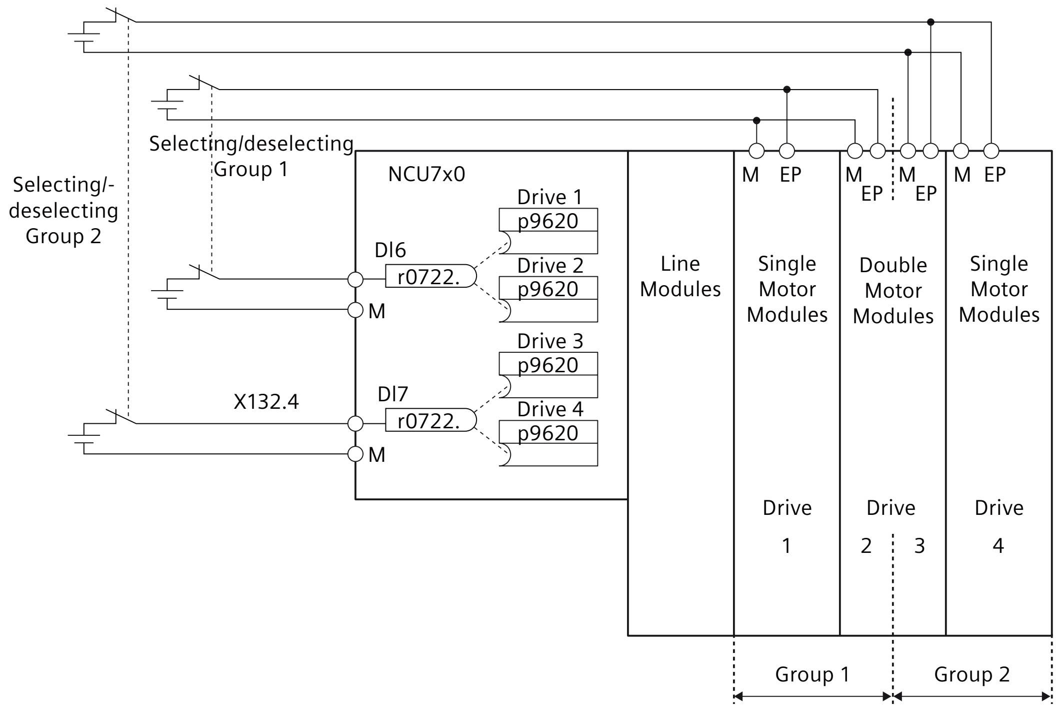


Figure 6-2 Example: Grouping the terminals for Motor Modules, booksize format

6.6.4 Simultaneity and tolerance time of the two monitoring channels

The "Safe Torque Off" (STO) safety function must be selected/deselected **simultaneously** in both monitoring channels using the input terminals, and is only effective for the associated drive.

- 1 signal: Deselecting the function
- 0 signal: Selecting the function

Parameterization of the tolerance time

Even when simultaneously selecting/deselecting, a certain time delay cannot be avoided, e.g. as a result of mechanical switching operations. Therefore, in the following parameters, define the tolerance times, within which selection/deselection in both monitoring channels is considered to be simultaneously valid.

- p9650 SI SGE switchover tolerance time (Control Unit)
- p9850 SI SGE switchover tolerance time (Motor Module)

In order to avoid that faults are incorrectly initiated, at these inputs the tolerance time must always be set shorter than the shortest time between two switching events (ON/OFF, OFF/ON).

Fault F01611

If the "Safe Torque Off" function is not selected/deselected within the tolerance time, this is detected by the cross-comparison, and fault F01611 (STOP F) is output. In this case, the pulses have already been canceled as a result of the selection of "Safe Torque Off" on one channel.

Note

Timing between the switching operations

Message F01611 with fault value 1000 indicates that the switching operations occur too frequently.

- STO is being permanently initiated via PROFIsafe (also as subsequent response).

Within the time 5 × p9650, there must be at least two switching operations via PROFIsafe with a minimum time between them of p9650.

Additional notes regarding setting the discrepancy time are included in the "SINAMICS S120/S150 List Manual" for the C01770 and F01611 safety messages.

6.6.5 Bit pattern test

Bit pattern test of failsafe outputs

The converter normally responds immediately to signal changes in its failsafe inputs. This is not desired in the following case: Several control modules test their failsafe outputs using bit pattern tests (on/off tests), in order to identify faults due to either short-circuit or cross-circuit faults. When you interconnect a failsafe input of the converter with a failsafe output of a control module, the converter responds to these test signals.

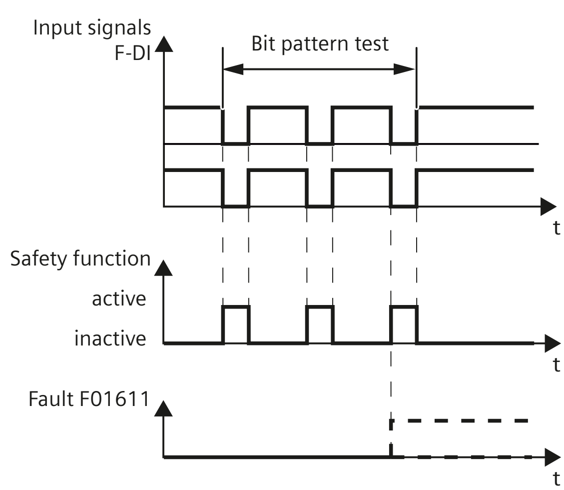


Figure 6-3 Converter response to a bit pattern test

Note

Debounce time for unwanted triggering of Safety Integrated Functions

If the test pulses cause an unwanted triggering of the Safety Integrated Functions, these test pulses can be suppressed with the aid of the F-DI input filter (p9651). To do this, a value must be entered in p9651 that is greater than the duration of a test pulse.

Overview of important parameters

- p9651 SI STO/SBC/SS1 debounce time (Control Unit)

Commissioning and configuring 7

7.1 Commissioning sequence

Safety Integrated is partially commissioned in the TIA Portal - and partially in SINUMERIK Operate. Commissioning can be roughly subdivided into the following steps:

1. Configuring safety-related components (Page 240)
2. Creating a safety program (Page 249)
3. Creating SafeUserData instances in the TIA Portal (Page 81)
4. Loading the configuration to the control (Page 263)
5. Configuring NC and drive-specific safety settings (Page 265)
6. Configuring SafeUserData in SINUMERIK Operate (Page 283)
7. Configuring safety functions integrated in the drive (Page 299)
8. Completing commissioning (Page 337)

Detailed action overviews can be found in the linked chapters.

7.2 Configuring safety-relevant components

7.2.1 Overview

The following handling overview (as example) and the associated descriptions illustrate the special issues when configuring Safety Integrated with a SINUMERIK NCU compared to a CPU S7-1500. Consequently, the overview serves only as an introduction to the configuring and programming of STEP 7 Safety Advanced with SINUMERIK.

Preconditions

- The following TIA Portal software is installed and licensed:
  - SIMATIC STEP 7 Professional V17
    SIMATIC STEP 7 Safety Advanced V17
  - SINUMERIK ONE STEP 7 Toolbox V17
- The non-safety-related components have been configured.
- The NCU is inserted
- SINUMERIK PLC basic program and standard PLC user program exist in a project.
- The devices are networked with one another using the specified interfaces (PROFINET or PROFIBUS).
  You can also connect devices at the interfaces of both types (PROFINET and PROFIBUS) - and then operate them in the "SINUMERIK Safety Integrated (F-PLC)" mode.

Workflow:

Step	Description
1	Activating Safety Integrated (Page 240)
2	Configuring additional safety-related components (Page 242)
3	Loading the configuration into the controller (Page 242)
4	Allocating and assigning a PROFINET device name (Page 243)
5	Assigning F-destination addresses, address type 1 (Page 245) or Assigning F-destination addresses, address type 2 (Page 245)
6	Checking the PROFIsafe address (Page 247)

After completing the configuration, generate the safety program of the F-PLC (Page 249).

7.2.2 Activating Safety Integrated

Precondition

- The "SIMATIC STEP 7 Safety Advanced" option package has been installed.

Procedure

To change the Safety Integrated mode, proceed as follows:

1. Click the NCU in the network or device view and select the "Safety Integrated" entry in the "Properties" inspector window at "General".

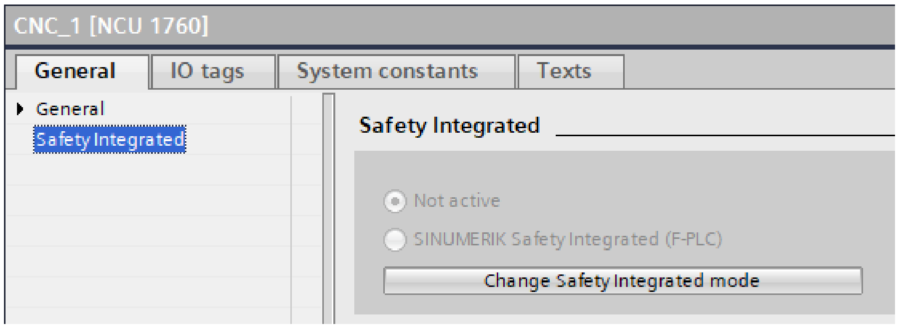


Figure 7-1 Inspection window "Properties" - Safety Integrated

2. Click the "Change Safety Integrated mode" button.
   The "Change Safety Integrated mode" dialog opens. If you select an option, the effects of the mode change are performed here.

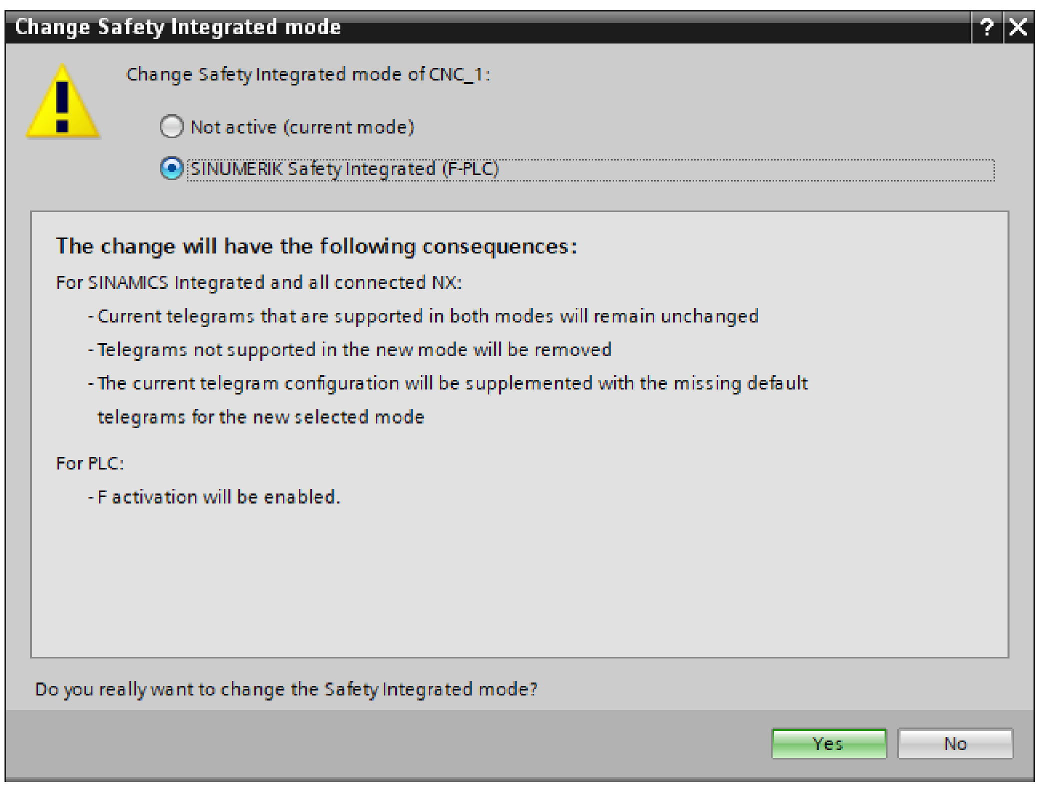


Figure 7-2 "Change Safety Integrated mode" dialog

3. Select the required Safety Integrated mode and confirm the reconfiguration with "Yes".

Result

The Safety Integrated mode has been changed.

If problems occur during the changeover, you can find further information in the "Info" inspector window at "General".

Note

Effects on telegram configuration

The Safety Integrated mode used influences the telegram configuration because, in the "SINUMERIK Safety Integrated (F-PLC)" mode, different telegrams are used than for the inactive Safety Integrated mode or for SINUMERIK Safety Integrated (system-integrated).

Telegrams that are added or changed are kept, however, as long as they are compatible with the newly selected Safety Integrated mode.

Ensure, if applicable, that any adaptations are still available following the change of mode in the telegram configuration.

7.2.3 Configuring additional safety-related components

Basic procedure

After you have activated Safety Integrated, you can insert and configure optional F-I/Os as well as failsafe modules/submodules and telegrams.

You can find further information in the documentation for SIMATIC Safety.

7.2.4 Loading the configuration into the controller

If you have changed an existing hardware configuration, then you must first load the actual configuration to the device. This ensures that the same configuration is set on the PG/PC and the physical device itself.

Requirements

- The PLC is in the STOP operating state.
  Using the TIA Portal, you can stop and then restart the PLC before the loading. However, the other subcomponents of the control system are not stopped or started.
- There is a network connection between the PG/PC and the control system.

Procedure

Proceed as follows to load the hardware configuration into the control system:

1. Select the PLC in the project navigation and call shortcut menu "Load to device > Hardware configuration".
   The "Extended download" dialog opens.
2. Select the PG/PC interface type (the network card being used), e.g. "Intel[R] Ethernet Connection I217-V".

3. Select the slot for the connection with interface/subnet, e.g. "Directly at slot '2 X120'
4. Click "Start search".
   A search is made for the target devices, and they are displayed in the dialog.
5. Select the appropriate target device, e.g. based on the IP address, and confirm with "Load".
   If several F-CPUs can be accessed from a PG/PC via a network, then carefully observe the notes in Manual SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/products?search=SIMATIC%20Safety&dtp=Manual&pnid=24471&lc=en-WW).
6. Check the information in the "Load preview" dialog and confirm with "Load".
7. In the "Results of the load procedure" dialog, select whether the PLC should be restarted, and then confirm with "Complete".

7.2.5 Allocating and assigning a PROFINET device name

Before a PROFINET IO device can be addressed by an I/O controller, it must have a device name.

Additional general information about PROFINET device names is provided in the TIA Portal online help.

Precondition

- The PROFINET IO device can be accessed in the network.

Procedure

In order to assign a device name to a PROFINET IO device, proceed as follows:

1. In the device properties, in field "Name", enter the required device name.
2. Click in the network view, right-click on the device and select command "Assign name".

3. Make the following settings in dialog "Assign PROFINET device name":
   – PG/PC interface type: PN/IE
   – PG/PC interface: Network card used, e.g. "Intel(R) 82579V Gigabit Network Connection"

   The list of accessible nodes is updated in the dialog.

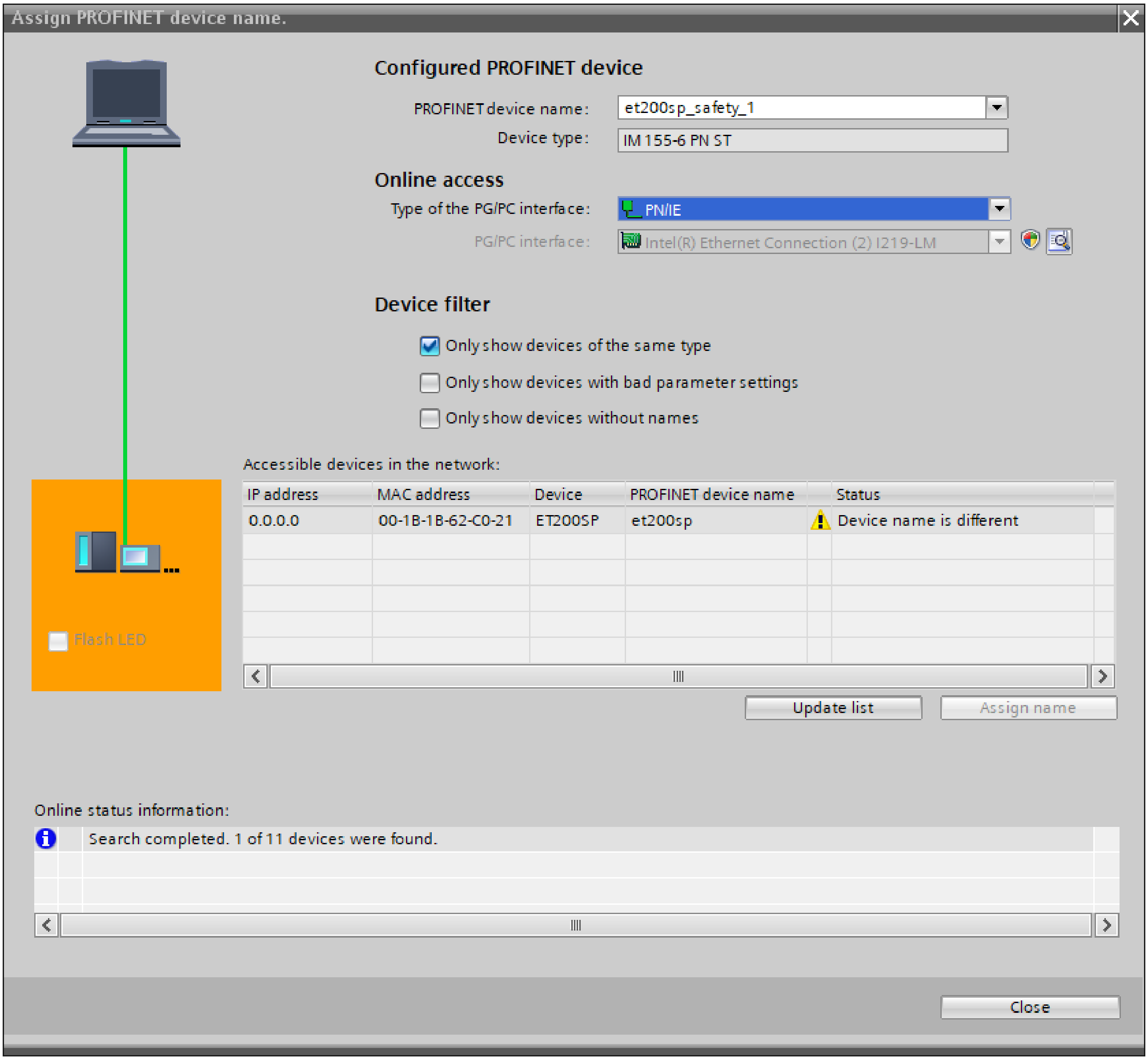


Figure 7-3 Dialog "Assigning a PROFINET device name"

4. Select the appropriate target device, e.g. based on the device type and IP address, and confirm with "Name".

7.2.6 Assigning F-destination addresses, address type 1

The F-target addresses of the F-I/O from PROFIsafe address type 1 are assigned to the module using a DIL switch or via drive parameters (for SINAMICS).

Information on how you can set the F-destination address for F-I/O using DIL switches is provided in the documentation for the F-I/O.

Unique PROFIsafe addresses

To ensure safe communication, unique PROFIsafe addresses are required throughout the CPU and the network.

The failsafe I/O of PROFIsafe address type 1 is uniquely addressed by its failsafe destination address (e.g. using the position of the address switch) (see Chapter "Checking the PROFIsafe address (Page 247)").

The F-destination address (and therefore also the setting at the address switch) of the F-I/O must be unique **for the entire** F-I/O throughout the network and the CPU (system-wide). The F-I/O of PROFIsafe address type 2 should be taken into account.

See the help for SIMATIC Safety at:

- DIL switch setting
- Special considerations when configuring the F-system
- Recommendation for allocating PROFIsafe addresses
- PROFIsafe addresses for F-I/O of PROFIsafe address type 1
- Configurations supported by the SIMATIC Safety F-safety
- Completeness and correctness of the hardware configuration

7.2.7 Assigning F-destination addresses, address type 2

For the F-I/O of PROFIsafe address type 2, you can adapt the F-destination address in the module properties - and then use command "Assign F-destination address".

Unique PROFIsafe addresses

To ensure safe communication, unique PROFIsafe addresses are required throughout the CPU and the network.

F-I/O of PROFIsafe address type 2 is uniquely addressed using a combination of F-source address ("Basis for PROFIsafe addresses of the assigned F-CPU" parameter) and F-destination address.

The combination of F-source address and F-destination address for each F-I/O must be unique throughout the network and CPU (system-wide). In addition, the F-destination address must not be occupied by F-I/O of PROFIsafe address type 1.

To ensure that addresses are unique across F-CPUs for supported configurations, you must ensure that the parameter "Basis for PROFIsafe addresses" is unique for all F-CPUs in the network*. This is achieved by having different settings for the "Basis for PROFIsafe addresses" parameter of the F-CPUs.

See the help for SIMATIC Safety at:

- Special considerations when configuring the F-system
- Recommendation for allocating PROFIsafe addresses
- PROFIsafe addresses for F-I/O, PROFIsafe address type 2
- Configurations supported by the SIMATIC Safety F-safety
- Completeness and correctness of the hardware configuration

Requirements

- The F-I/O device can be accessed in the network.
- A device name has been assigned to the F-I/O.
- The hardware configuration has been loaded to the device.

Procedure

Proceed as follows, to assign the configured F-destination address to F-I/O, PROFIsafe address type 2:

1. Click in the network view, right-click on the F-I/O device and click on "Assign F-destination address".
2. Make the following settings in the "Extended load" dialog:
   - PG/PC interface type: PN/IE
   - PG/PC interface: Network card used, e.g. "Intel[R] Ethernet Connection I217-V"
   - Connection with interface/subnet: Directly at slot '1 X150'
3. Under "Identification" select how you wish to identify the F-modules:
   - "By flashing the LEDs"
     This is the default setting. During identification, the STATUS LEDs of the F-modules to be identified flash.
   - "Using the serial number"
     If you cannot see the F-modules clearly, you can identify them by the serial number of the interface module.

   Note

   The displayed serial number may have a year number added to it compared with the serial number printed on the interface module. The serial numbers are nevertheless identical.
4. In column "Assign" select all F-modules where you wish to assign an F-destination address.
5. Click the "Identification" button.
   - If you have selected LED flashing for the identification type, then check whether the status LEDs of that F-module flash green whose F-destination address you wish to assign.
   - If you have selected the serial number for the identification type, compare the displayed serial number with the serial number of the module.

6. Confirm successfully identified F-modules in the "Confirm" column of the table.
7. Using button "Assign F-destination address" assign the configured F-destination addresses to the F-modules, and confirm dialog "Acknowledge assignment" (within 60 seconds).
8. Close the dialog.

7.2.8 Checking the PROFIsafe address

To ensure safe communication, unique PROFIsafe addresses are required throughout the CPU and the network. For this reason, it is also necessary that you check the settings of the PROFIsafe addresses carefully.

WARNING

Incorrect assignment of the safety functions of an axis

An incorrect assignment of a (valid) F-address results in an incorrect assignment of the safety functions to the corresponding axis. The system does not identify this incorrect assignment (in the CPU and in the network). As a consequence, the safety functions can act in a way that was not intended, which in turn can result in death and serious injury.

- Uniquely address the F-destination address of the F-I/O of PROFIsafe address type 1.
- Ensure that the F-destination address of the F-I/O (the drive units in this case) is unique for the entire failsafe I/O throughout the network and the CPU (system-wide). When doing this, also take into account the F-I/O of PROFIsafe address type 2, e.g. modules of the ET 200SP type.
- Note also the corresponding documentation in the TIA Portal online help in the section "SIMATIC Safety - Configuration and programming".

During compilation of the safety program, a warning indicates the importance of unique PROFIsafe addresses:

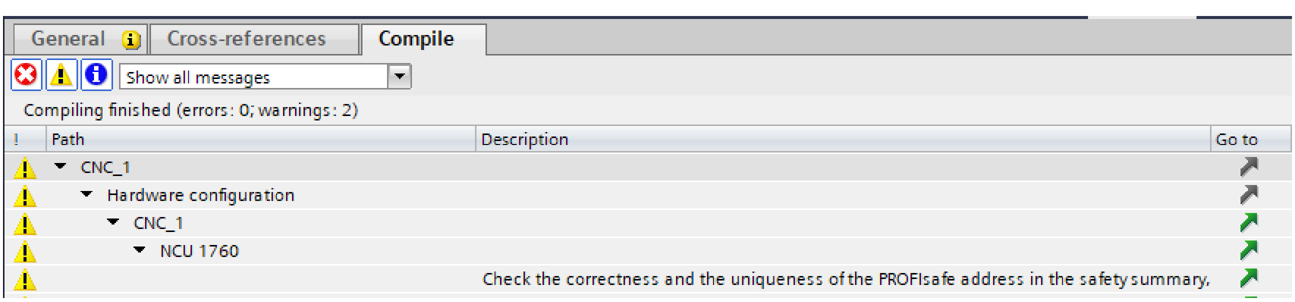


Figure 7-4 Warning when compiling the safety program

Precondition

- F-destination addresses have been configured and assigned.
- Hardware and software have been compiled.

Procedure

Proceed as follows to check PROFIsafe addresses:

1. Right-click on "Safety Administration > Print", select a printer or a PDF application and confirm with "OK".
   The safety printout is generated.

SINAMICS Integrated_1					
Rail - Slot	Module	Start address	F-destination address	F-monitoring time	Parameter signature (w/o ad-dresses)
0	DriveAxis01FIODB	6700	1	150 ms	0xEE5 (3813)
0	DriveAxis02FIODB	6716	2	150 ms	0xEE5 (3813)
0	DriveAxis03FIODB	6732	3	150 ms	0xEE5 (3813)
0	DriveAxis04FIODB	6748	4	150 ms	0xEE5 (3813)
0	DriveAxis05FIODB	6764	5	150 ms	0xEE5 (3813)
0	DriveAxis06FIODB	6780	6	150 ms	0xEE5 (3813)

Figure 7-5 F-destination addresses of drive objects of SINAMICS Integrated in the safety printout (example)

2. Check the PROFIsafe addresses listed in the safety printout:
   - Compare the F-destination addresses of the drive objects from SINAMICS Integrated and NX modules with the values of drive parameter p9610.
   - In the safety printout compare the F-destination addresses of the individual modules with those of all other modules or participants, and ensure that the addresses are unique.

7.3 Generating a safety program

7.3.1 Overview

Preconditions

- Safety Integrated is active
- The F-components have been configured and parameterized.

Workflow:

Step	Description
1	Create receive/send data as PLC tags (Page 249)
2	Adapting the settings of the F-runtime group (optional) (Page 251)
3	Setting up access protection (Page 254)
4	Parameterizing EMERGENCY STOP (Page 255)
5	Implementing user acknowledgment for global reintegration (Page 256)
6	Acknowledging messages related to safety functions integrated in the drive (Page 257)
7	Deselecting safety functions integrated in the drive (Page 260)
8	Initiate a forced checking procedure (test stop) (Page 262)
9	Programming the wiring test (Page 262)

7.3.2 Create receive/send data as PLC tags

In order that you can access the required drive data symbolically in the safety program, in the TIA Portal create PLC variables with the corresponding drive addresses.

You can create all the PLC variables required before you start programming - or you can always add your PLC variables if you wish to access new drive data. If you address the drive data with absolute values instead, variable names are automatically assigned that are subsequently difficult to comprehend.

You can import or export PLC variables in the XLSX, SDF or XML formats. You can copy PLC variable tables as copy templates in global libraries.

Procedure

Proceed as follows to create PLC variable tables with the required drive data.

1. In the project navigation, double-click below "PLC variables " on "Add new variable table", e.g. "CNC_1 > PLC_1 > PLC variables > Add new variable table".
2. Right-click on the new variable table, select "Rename" and assign a name, e.g. "Safety status data" or "Safety control data".

3. Double-click on the new variable table to open it.
4. In the "Name" column, click on "Add" and enter the variable properties:

Property	Meaning
Name	Enter a meaningful name, e.g. <drive name>-<process data>-<where relevant, bit identifier>. Example 1: drive1SpValid Example 2: drive2SlsLimitA
Data type	Specify with which data type the process data is addressed. • Bool: S_STW1, S_ZSW1, S_STW2, S_ZSW2, S_ZSW_CAM1 • Int: S_SLS_LIMIT_A, S_SLS_LIMIT_A_ACTIVE, S_CYCLE_COUNT, S_XIST16 • DInt: S_XIST32 Example 1: Bool Example 2: Int
Address	In the "Address" column, click on the drop-down list symbol - and enter the properties: **Address identifier** Status/input data: I Control/output data: Q **Address** Enter the I/O address to which the specific process data is transferred. This is obtained from the telegram start address and the PZD range within the telegram, where the process data starts. • You can see the start address for a specific drive telegram in the telegram configuring of SINAMICS Integrated. The standard start addresses are also listed in Tables (Page 392). • Refer to the telegram structure (Page 395) to identify in which PZD range (1 PZD = 1 word = 2 byte) within the telegram the required drive data is contained. **Bit number** For data type "Bool" - or if you address a bit - then in addition, specify the bit number that you take from the process data description (Page 398). Example 1: %I6702.6 Example 2: %QW6704
Comment	Optionally, you can formulate a user-defined note for each variable that is added - or take this from the manual.

Result

The PLC variables were added.

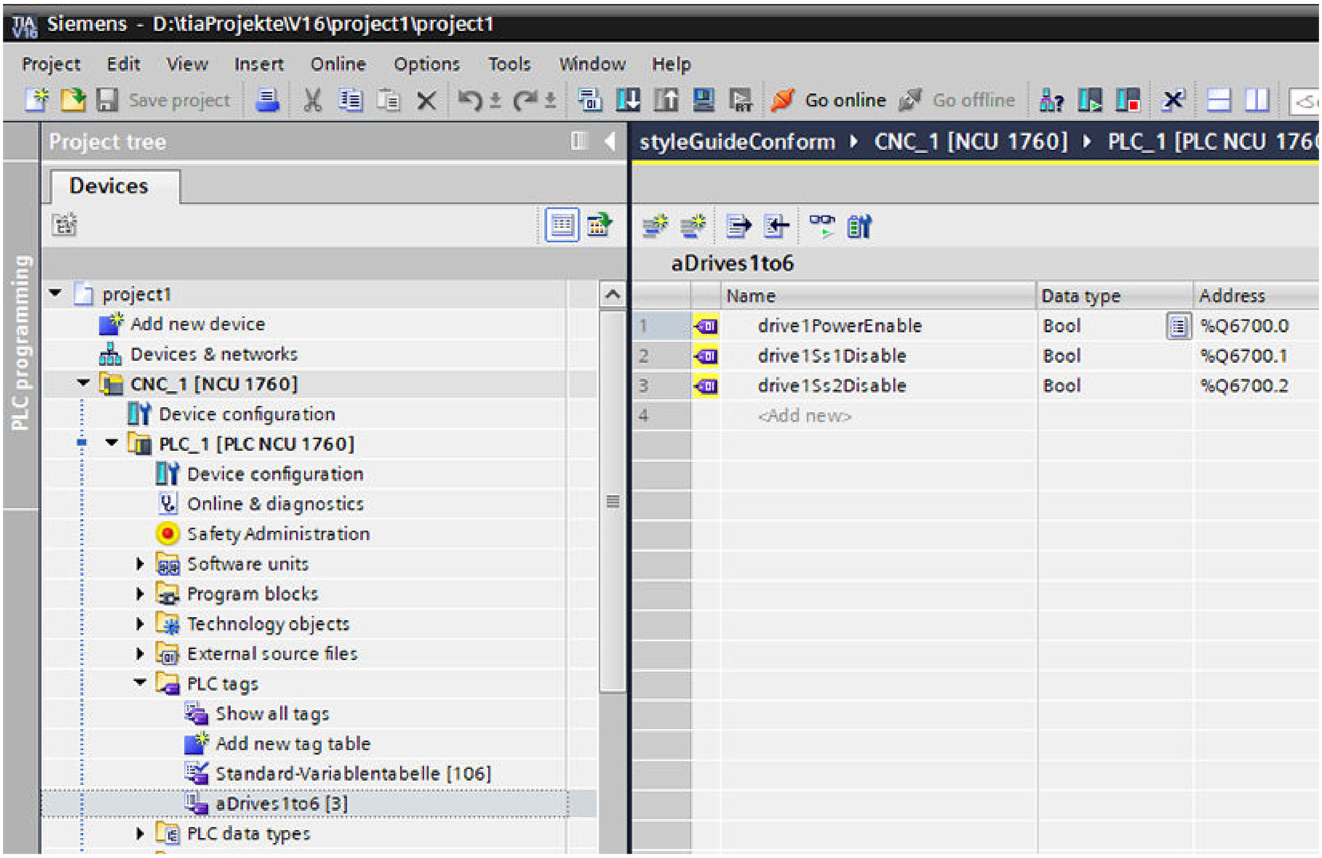


Figure 7-6 Example of a user-defined variable table, with the drive addresses required in the programming

7.3.3 Adapting the settings of the F-runtime group (optional)

An F-runtime group is automatically created when you activate the "SINUMERIK Safety Integrated (F-PLC)" mode. The associated F-blocks are provided in folder "Program blocks" - or in the Safety Administration Editor under "F-blocks":

- FOB_RTG1[OB123]
- Main_Safety_RTG1[FB...]
- Main_Safety_RTG1_DB[DB...]

You can adapt the default settings of the F-runtime group and the associated blocks, as described here.

Optionally, you can also create a second F-runtime group; for example, to organize safety-related program sections that are executed quickly, in their own dedicated F-runtime group.

Precondition

- Safety Integrated is active

Procedure

Proceed as follows to view the settings of an F-runtime group - or to adapt them:

1. In the project navigation, double-click below the PLC involved on "Safety Administration", e.g. "CNC_1 > PLC_1 > Safety Administration".
2. In the Safety Administration Editor switch to "F-runtime group".
3. You can also adapt the following settings:

Setting	Purpose
Calling block	FOB_RTG1[OB123] is the default setting. This block is a cyclic interrupt OB, which means that within an execution time, the safety program is called at fixed intervals in time. In the drop-down list you can define a block other than the calling block: • If you select an LAD, FBD or STL block, then the call in the block is automatically updated. • If you select a block in another programming language, then you must adapt the call yourself. Setting options: • Name: Names for the F-OB • Event class (only when creating): For an F-OB, you can select between event classes "Program cycle", "Cyclic interrupt" and "Synchronous cycle". • Number: If necessary, you can manually change the F-OB number that the system suggests. When doing this, observe the number ranges permissible for the particular event class. • Cycle time: Select a cycle time that is less than the "Maximum cycle time of the F-runtime group" and less than the "Warning limit cycle time of the F-runtime group". The cycle time replaces the execution time. • Phase offset: Select a phase offset that is less than the cycle time. • Priority: If possible, select a priority that is higher than the priority of all other OBs.
Main safety block	Default setting: Main_Safety_RTG1[FB...] In the drop-down list you can select a block other than the previously created F-block.
I-DB for the main safety block	Default setting: Main_Safety_RTG1_DB[DB...] If the main safety block is an FB, then in the drop-down list you can adapt the associated I-DB.
Maximum cycle time of the F-runtime group	The F-CPU monitors the F-cycle time in the F-runtime group. For "Maximum cycle time of the F-runtime group", select the maximum time that may elapse between two calls of this F-runtime group.
Warning limit, cycle time of the F-runtime group	You must parameterize the "Warning limit cycle time of the F-runtime group" lower or the same as the "Maximum cycle time of the F-runtime group".

Setting	Purpose
DB for F-runtime group communication	If one F-runtime group is to provide variables for evaluation to another F-runtime group of the safety program, assign a DB for F-runtime group communication. Additional information is provided in the help for SIMATIC Safety under "Safety-related communication between the F-runtime groups".
F-runtime group information DB	Under "F-runtime group information DB" assign a name for the F-runtime group information DB. Default setting: "RTG1SysInfo"

7.3.4 Setting up access protection

In productive operation, it is absolutely crucial that an F-system is provided with access protection.

For test purposes, commissioning etc. initially access protection is not required; this means that you can execute all offline and online actions without access protection, i.e. without a password prompt.

In the safety mode, when changing the standard user program it is not permissible that access authorization exists based on the CPU password – as in this case, the safety program can also be changed. To rule this out, you must configure protection level "Write protection for failsafe blocks" - and a password for the F-CPU. If only one person is authorized to change both the standard user program and the safety program, then the protection level "Write protection" or "Read/write protection" should be configured so that other persons are only given a restricted or no access to the complete user program (standard and safety program).

For additional information, refer to the "Access protection" chapter in the SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/products?search=SIMATIC%20Safety&dtp=Manual&pnid=24471) Manual.

Procedure

To set up access protection for productive operation, follow these steps:

1. In the project navigation, double-click below the PLC involved on "Safety Administration", e.g. "CNC_1 > PLC_1 > Safety Administration".
2. In the Safety Administration Editor switch to "Access protection".
3. Assign passwords for the two access protection types:
   - Under "Offline safety program protection", click on "Setup", assign a password and confirm with OK.
   - Under "F-CPU access protection", click the link "Go to the "Protection" area of the F-CPU". Select the setting "Full access (no protection)" in the called properties and assign the "Password for write/read access".
4. Load the hardware and software to the device.

Result

Two different access protection types are setup:

- Protection of the safety program
- Protection of the F-CPU

7.3.5 Parameterizing EMERGENCY STOP

Instruction "ESTOP1" implements an EMERGENCY STOP shutdown with acknowledgment for stop Categories 0 and 1.

Procedure

Proceed as follows to program an EMERGENCY STOP shutdown:

1. Open the F-block involved.
2. From the task card "Instructions", insert operation "Basic instructions > Safety functions > ESTOP1".
3. Supply the inputs and outputs of the operation.

Parameter	Declaration	Description
E_STOP	Input	EMERGENCY STOP/EMERGENCY OFF
ACK_NEC		1= acknowledgment required
ACK		1=acknowledgment
TIME_DEL		Delay time
Q	Output	1=enable
Q_DELAY		Enabling of the OFF delay for F-I/O The enabling signal Q_DELAY is reset to 0 after the delay time has been set at the TIME_DEL input. Do not use Q_DELAY for drive components; instead use the corresponding setting of the relevant drive-integrated safety function.
ACK_REQ		1= acknowledgment required
DIAG		Non failsafe service information

4. Link the F-DOs for the I/O shutdown or the safety function in the specific drive with the outputs.

Additional information

You can find more information about the instruction in the online help for the instruction or in the manual for SIMATIC Safety.

7.3.6 Implementing user acknowledgment for global reintegration

If an F-I/O error is detected by the failsafe system, the affected F-I/O and/or drive components are passivated.

With the **passivation** of a failsafe component, for the components involved, substitute values are provided or are transferred instead of the active process values or output values.

After resolving the cause of the fault, the component involved must be **reintegrated**, i.e. a switchover from substitute values to process values or output values.

Depending on the fault type or the component, in which the fault occurs, you can set passivation and reintegration differently:

<table>
<tr><th>Fault type</th><th>Passivation</th><th>Reintegration</th></tr>
<tr><td>Communication</td><td rowspan="2">All channels of the module</td><td>After a communication error, user acknowledgment is always required.</td></tr>
<tr><td>F-I/O
or Drive</td><td rowspan="2">dependent on the F-I/O DB parameter:
• ACK_NEC=1:
user acknowledgment required
• ACK_NEC=0
automatic reintegration</td></tr>
<tr><td>Channel</td><td>Depending on F-parameter "Behavior after channel fault" of the module:
• Passivation of the channel
• Passivation of the complete module</td></tr>
</table>

You implement reintegration after user acknowledgment by interconnecting the signal, generated by the operator action, with one of the following parameters:

- F-I/O DB parameter "ACK_REI": Reintegration of the corresponding module (all channels)
- Operation "ACK_GL" (parameter "ACK_GLOB"): Reintegration of all modules of a F-runtime group

Procedure

Proceed as follows to implement a user acknowledgment for global reintegration:

1. Insert operation "ACK_GL" in that F-runtime group, whose F-I/O should be globally acknowledged by the user acknowledgment.
2. In operation "ACK_GL", assign input "ACK_GLOB" to the input of the acknowledgment button.
3. If necessary, carry out the optional steps:

Setting	Description
Evaluation of the acknowledgment request	You can evaluate the F-I/O DB variable "ACK_REQ" in the standard user program or on an operation and monitoring system, to interrogate as to whether a user acknowledgment is required. • ACK_REQ = 0: No acknowledgment request • ACK_REQ = 1: Acknowledgment request for reintegration (this is set by the F-system after the fault has been resolved)
Controlling a signal light or output of a signal	In the case of a fault, you can control a signal light and/or output messages/signals in the standard user program, by evaluating the following: • F-I/O DB variables: – QBAD – DIAG • Diagnostics buffer of the F-PLC
Automatic or manual reintegration for F-I/O/channel faults	You can parameterize the F-I/O DB variable "ACK_NEC" if, after an F-I/O/channel fault, automatic reintegration should take place without user acknowledgment. • ACK_NEC = 1 (start value): User acknowledgment required • ACK_NEC = 0: Automatic reintegration A user acknowledgment is always required after a communication error.

Parameterizing variables ACK_NEC = 0 is only permitted, if, from a safety-related perspective, automatic reintegration is permissible for the process involved.

7.3.7 Acknowledging messages related to safety functions integrated in the drive

You program PROFIsafe acknowledgment in the safety program of the F-PLC by setting the "Internal Event ACK" signal - separately for each drive object - via the PROFIsafe telegram (S_STW1/S_STW2 bit 7).

Safety messages cannot be acknowledged collectively by the F-PLC, but instead have to be individually acknowledged for each drive object. A falling edge of the "Internal Event ACK" signal resets the status "Internal Event" in the particular drive, and thus acknowledges the fault.

In the safety program, logically combine all channel reset signals of channels that contain drive objects with safety functions, with the "Internal Event ACK" signal for each drive object involved.

> **WARNING**
>
> **Unexpected restart for safety-related acknowledgment without MCP reset!**
>
> If a STOP response is acknowledged in a safety-related fashion by the machine operator, but without PROFIdrive RESET acknowledgment, then the part program is not canceled and is continued with the acknowledgment. When the machine restarts unexpectedly, this can put people in dangerous situations or cause material damage.
>
> - In the safety program logically combine safe acknowledgment (PROFIsafe IEACK) with a RESET at the machine control panel (PROFIdrive RESET).

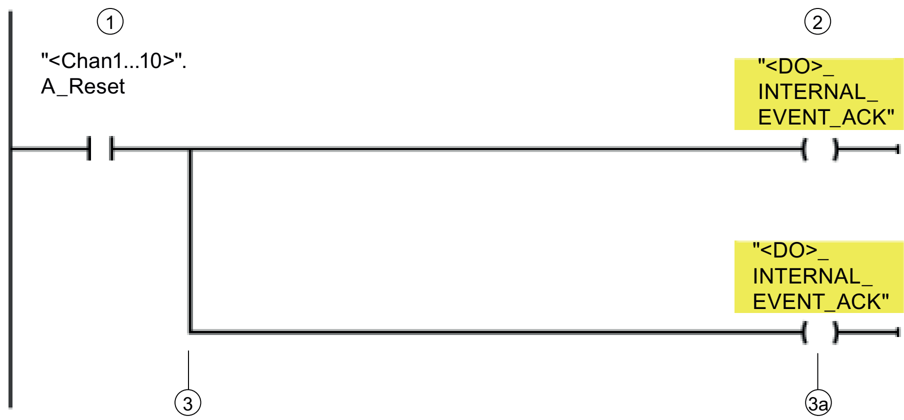
Precondition

- PLC variables for the "Internal Event ACK" signal are added for each drive object.

Procedure

In order to logically combine the reset signal of the machine control panel with the safety-related acknowledgment in the safety program for a channel, proceed as follows:

1. Open the corresponding F-runtime group, e.g. Main_Safety_RTG1 [FB1010].
2. Insert a new network, in which you logically combine the signals:



No.	Instruction/variable	Purpose/procedure
(1)	---| |---NO contact: "<Channel DB name>".A_Reset	The channel reset must be active, i.e. the interface signal in the corresponding channel DB must be 1.
(2)	---( )--- Assignment <PLC variable> Example: "drive1InternalEventAck"	Assign the logic operation result to the corresponding PLC variable, that you created for the "Internal Event ACK" signal of the appropriate drive.
(3)	Branch	If you are using several safety-related drive objects, for each drive object insert a branch together with the operation (see 3a).
(3a)	---( )--- Assignment <PLC variable> Example: "drive2InternalEventAck"	Assign the logic operation result to the corresponding PLC variable.

Figure 7-7 Inserting a new network

Result

The channel reset signal of the channel involved was logically combined with the safety-related acknowledgment of faults in the individual drive objects.

See also

Create receive/send data as PLC tags (Page 249)

7.3.8 Deselecting safety functions integrated in the drive

You deselect safety functions integrated in the drive by accessing the corresponding drive addresses in the safety program and then set/reset the relevant bits.

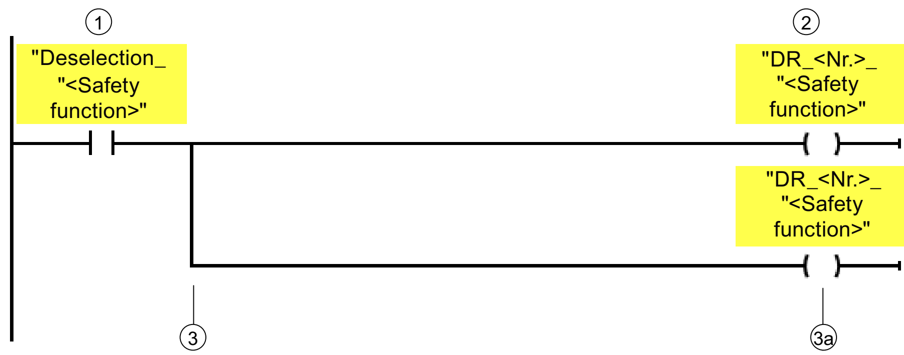
Precondition

- PLC variables for the signals required have been added.

Procedure

Proceed as follows to select or deselect a safety function integrated in the drive in the safety program:

1. Open the F-block, e.g. Main_Safety_RTG1 [FB1010].
2. Insert a new network, and in the network, link (logically combine) the signals:



No.	Instruction/variable	Purpose/procedure
(1)	---| |---NO contact: "Deselection_<safety function>" Example: "deselectionSs1" or Drive I/O address with ZSW bit	Address the PLC variable "Deselection_<safety function>" or the drive I/O address, which transfers the associated bit of the safety control word.
(2)	---( )--- Assignment: "DR_<drive number>_<safety function>" Example: "drive1Ss1Disable" or Drive I/O address with STW bit	Assign the logic operation result to the safety function in the drive involved.
(3)	Branch	If you deselect the safety function involved for several drives, insert a branch and operation for each drive (see 3a).
(3a)	---( )--- Assignment: "DR_<drive number>_<safety function>" Example: "drive2Ss1Disable" or Drive I/O address with ZSW bit	Assign the logic operation result to the safety function in the drive involved.

Figure 7-8 Inserting a new network

See also

Create receive/send data as PLC tags (Page 249)

7.3.9 Initiate a forced checking procedure (test stop)

Basic procedure

Functions and switch-off signal paths must be regularly tested using the forced checking procedure (test stop). The forced checking procedure should be performed each time that the control system runs up and must, however, be performed at least once a year.

The forced checking procedure is not performed in the safety program but in the standard PLC program. This means that you insert the affected program code in your PLC user program in order to trigger the forced check procedure during run-up of the controller.

7.3.10 Programming the wiring test

Basic procedure

You must program a wiring test in order that your F-I/O devices can be correctly addressed. For the wiring test, use a tag QBAD of the F-I/O DB of the corresponding F-I/O. You can perform a wiring test jointly for all F-I/O modules of an F-runtime group.

Therefore, configure the F-I/O in such a way that the modules themselves perform the test.

Further information

Further information may be found in the SIMATIC Safety manual.

7.4 Loading the configuration to the control system

Precondition

- There is a network connection between the configuring PG/PC and the SINUMERIK control system.

Procedure

Proceed as follows to load the hardware and software configurations into the SINUMERIK control system:

1. In the project navigation, right-click the NCU and select the "Load to device > Hardware and software (only changes)" shortcut menu.
2. Make the following settings in the "Extended load" dialog:
   – PG/PC interface: Network card used, e.g. "Intel(R) 82579V Gigabit Network Connection"
   – Connection with interface/subnet: "PN/IE_2"

3. Click "Start search".
   A search is made for the target devices, and they are displayed in the dialog.

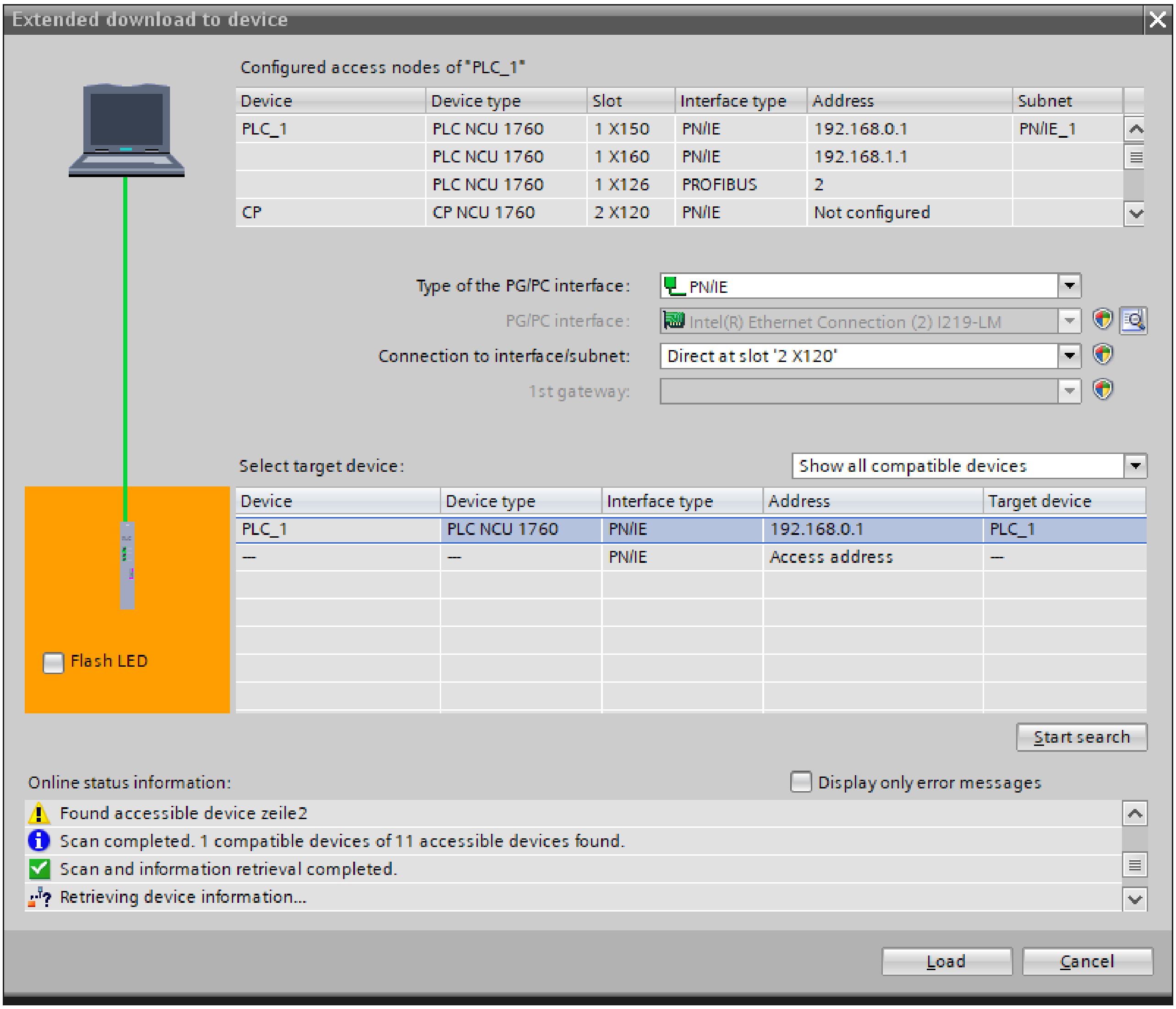


Figure 7-9 "Extended download" dialog

4. Select the appropriate target device, e.g. based on the IP address, and confirm with "Load".
5. Check the information in the "Load preview" dialog and confirm with "Load".
6. In dialog "Load results" select whether the PLC should be restarted, and then confirm with "Complete".

7.5 Configuring NC and drive-specific safety settings

7.5.1 Overview

This chapter describes higher-level safety settings that you specifically configure for each drive.

Requirements

- Access rights of access level 2 (service) are available in SINUMERIK Operate.
- The commissioning of the (non-safety-related) standard drive functions has been completed.
- The configuration (hardware and software) has been loaded (Page 263).
- The transfer of the Safety Integrated mode from the configuration has been completed.

Procedure

Step	Description
1	Setting software options (Page 266)
2	Activating Safety Integrated commissioning mode (Page 266)
3	Selecting the safety functional scope (Page 267)
4	Parameterizing the setpoint speed limiting (Page 269)
5	Parameterizing reaction of the stop response (Page 271)
6	Parameterizing an encoder (Page 272) or Configuring encoderless operation (Page 276)
7	Configuring telegrams (Page 280)
8	Using the fault buffer, message buffer and alarm buffer (Page 373)

7.5.2 Setting software options

Procedure

To set the software options for Safety Integrated, proceed as follows:

1. In SINUMERIK Operate switch to licensing via "MENU SELECT > Commissioning > Menu forward key > Licenses".
2. Press the "All options" softkey.
3. Set the safety software options required for your particular machine configuration:

Software option	Article No.	Purpose
Safety Integrated – F-PLC	6FC5800-0BS60-0YB0	Activate the F-PLC in the SINUMERIK control system to process the failsafe sensors and actuators in an F-program.
Safety Integrated - axis/spindle	6FC5800-0BK00-0YB0	Use the motion control functions of the SINAMICS Integrated in the "SINUMERIK Safety Integrated (F-PLC)" mode. License for 1 axis/spindle, multiple licensing in order to be able to use additional axes/spindles.
Safety Integrated – multi-axis package;	6FC5800-0BS61-0YB0	Use the motion control functions of the SINAMICS Integrated in the "SINUMERIK Safety Integrated (F-PLC)" mode. License for any number of axes/spindles.

Result

The software options were set.

The individual software options to be licensed for the machine can be displayed using softkey "Missing licenses/options", which you can then order, e.g. through the Siemens Industry Mall.

7.5.3 Activating Safety Integrated commissioning mode

Changes to the safety-related drive parameterization are only possible if the corresponding drive is in the Safety Integrated commissioning mode. After parameterization, the Safety Integrated commissioning mode must be deactivated and the actual checksums must be transferred into the reference checksums.

Precondition

- The commissioning of the (non-safety-related) standard drive functions has been completed.
- The configuration (hardware and software) has been loaded (Page 263).
- The transfer of the Safety Integrated mode from the configuration has been completed.

Procedure

Proceed as follows to activate the Safety Integrated commissioning mode for all drives:

1. In SINUMERIK Operate, switch to "MENU SELECT > Commissioning > Menu forward key > Safety".

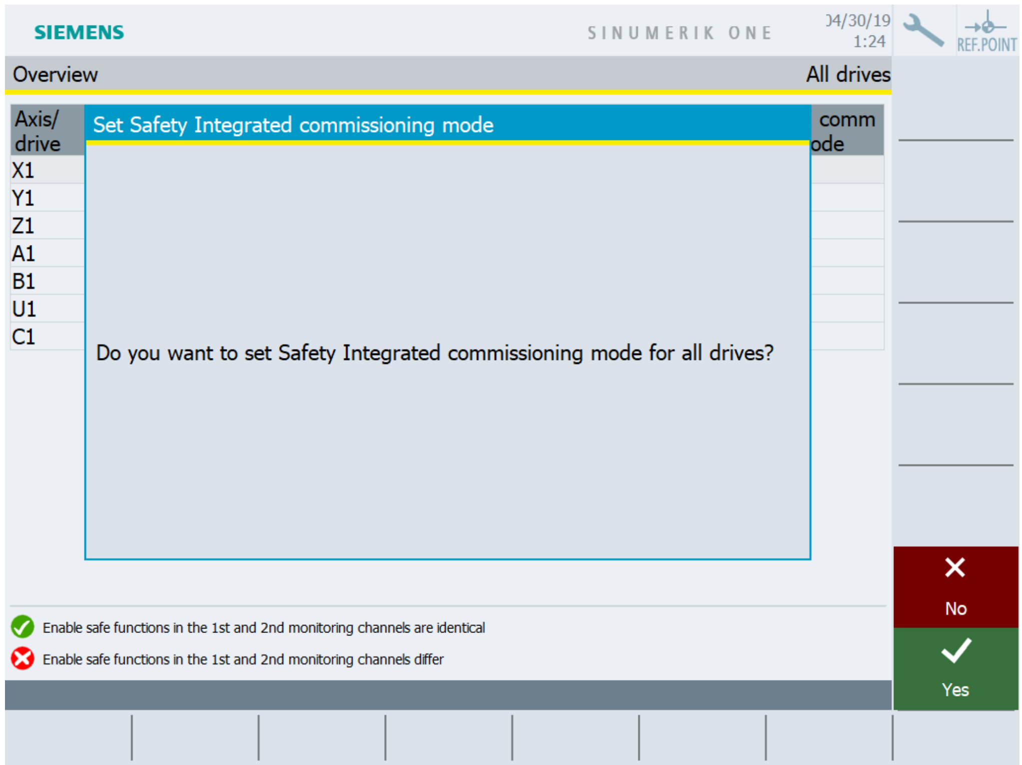


Figure 7-10 Activating the Safety Integrated commissioning mode for individual drives

---

Note

Activating the Safety Integrated commissioning mode for individual drives

To activate the mode for an individual drive only, instead, switch to "MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Options".

---

2. Select the softkey "Set SI Commissioning", then "Activate/deactivate drive commissioning" and confirm with "Yes".

7.5.4 Selecting the safety functional scope

Before you parameterize the various safety functions of the drive, make the following basic settings for the corresponding drives:

- Scope of the safety functions used (Basic or Extended)
- Control (PROFIsafe, terminals, without selection)
- Use of a safety-related encoder

You must make these settings one after the other for each drive where you wish to use the drive-integrated safety functions.

Precondition

- The commissioning of the (non-safety-related) standard drive functions has been completed.
- The configuration (hardware and software) has been loaded (Page 263).
- The transfer of the Safety Integrated mode from the configuration has been completed.
- The safety commissioning mode is activated for the drive to be configured (Page 266).

Procedure

Proceed as follows to set the safety functional scope for a drive:

1. In SINUMERIK Operate, go to the safety settings of the drive via "MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Options".
2. Switch to the corresponding drive, e.g. using softkey "Select a drive".
3. Select the functional scope under "Select safety function":
   - Basic Functions via onboard terminals
   - Basic Functions via PROFIsafe
   - Basic Functions via PROFIsafe and onboard terminals
   - Extended Functions via PROFIsafe
   - Extended Functions via PROFIsafe and Basic Functions via onboard terminals
   - Extended Functions without selection
   - Extended Functions without selection and Basic Functions via onboard terminals
4. Make additional settings, when using the extended functional scope:
   - Safety with encoder and acceleration monitoring (SAM)
   - Safety without encoder with braking ramp (SBR) - can only be set for induction motors
   - Safety without encoder with acceleration monitoring (SAMR) - can only be set for induction motors

   See also: Supported axis types (Page 39), Overview of safety functions integrated in the drive (Page 30), Control options (Page 223)
5. Press softkey "OK".

Note

When the selected safety function is saved, the enable for referencing via SIC/SCC (p9501.27) is automatically set via SINUMERIK Operate.

7.5.5 Parameterizing the setpoint speed limiting

During the runtime, the setpoint speed limiting of the drive (p9533) is evaluated with the selected evaluation factor of the NC, and issued to the interpolator as setpoint limit.

Precondition

- The safety functional scope of the drive has been selected. (Page 267)

Procedure

Proceed as follows, to parameterize the evaluation factors of the NC to define the setpoint limits:

1. In SINUMERIK Operate, switch to the safety settings of the drive via "MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Options".
2. Switch to the corresponding drive, e.g. using softkey "Select a drive".
   The parameterization is displayed for the selected drive.

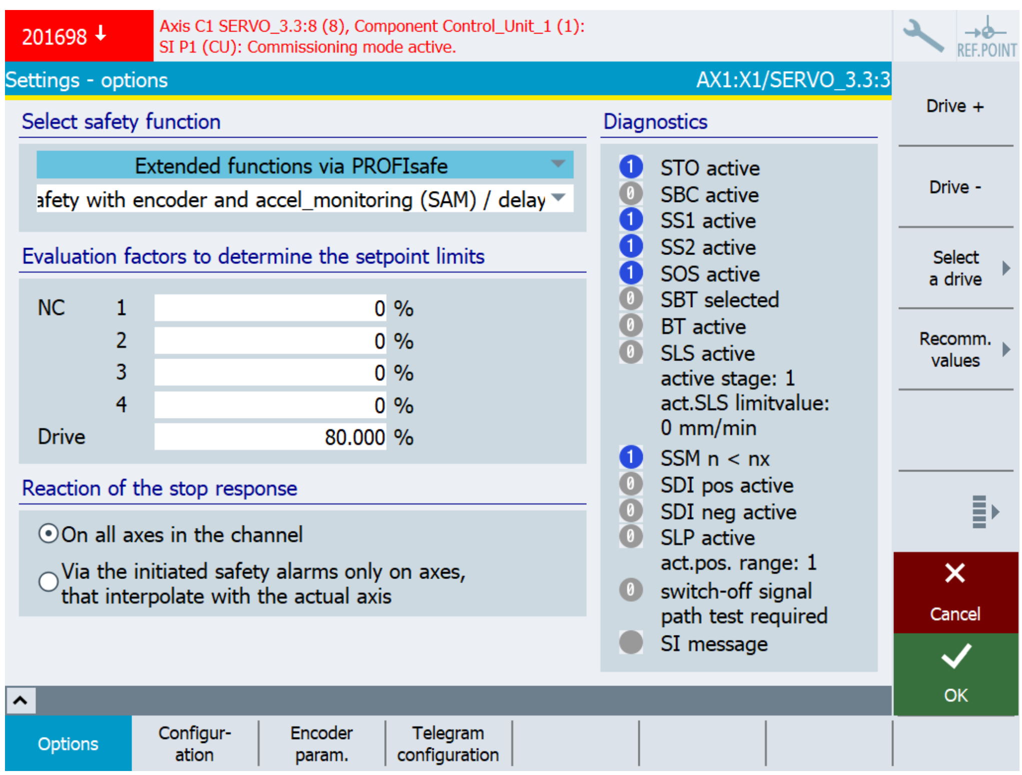


Figure 7-11 Settings - options

3. Parameterize 4 evaluation factors for defining the setpoint limits
   MD36933 $MA_SAFE_DES_VELO_LIMIT includes 4 values (indices 0...3). Using the axis-specific PLC user interface, in the PLC program you can select which of these values is active (DBX34.0...DBX34.1 in axis1 [DB31]...axis31[DB61]).

Bit 0	Bit 1	active setpoint limiting factor
= 0	= 0	SAFE_DES_VELO_LIMIT[0]
= 1	= 0	SAFE_DES_VELO_LIMIT[1]
= 1	= 1	SAFE_DES_VELO_LIMIT[2]
= 1	= 1	SAFE_DES_VELO_LIMIT[3]

   Select the active setpoint limiting factor using DBX34.0..DBX34.1 in axis1 [DB31]...axis31[DB61]

4. Enter the 4 required evaluation factors.
   To optimally set this MD, it is possible that several changes must be made in order to take into account the dynamic response of the drives.
   You can use 80% as recommended value, for example.

Result

The evaluation factors of the NC were parameterized, and are active after an operator panel reset.

During the runtime, the setpoint speed limiting of the drive (p9533) is evaluated with the selected (in the PLC user program) evaluation factor of the NC, and issued to the interpolator as setpoint limit.

The value in MD36933[0] becomes active if a specific value is not selected in the PLC user program.

7.5.6 Parameterizing reaction of the stop response

If a stop response is initiated, then this has effects on all of the other axes in the channel. The effect on the other axes in the channel can be influenced using MD36964 $MA_SAFE_IPO_STOP_GROUP. This allows, for example, the pulses of the spindle to be safely cancelled. This means that the spindle can be manually rotated and the axes can still be safely monitored while it is moving.

Procedure

Proceed as follows to assign parameters for the reaction of the stop response:

1. In SINUMERIK Operate, switch to the safety settings of the drive via "MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Options".
2. Switch to the corresponding drive, e.g. using softkey "Select a drive".
   The parameterization is displayed for the selected drive.

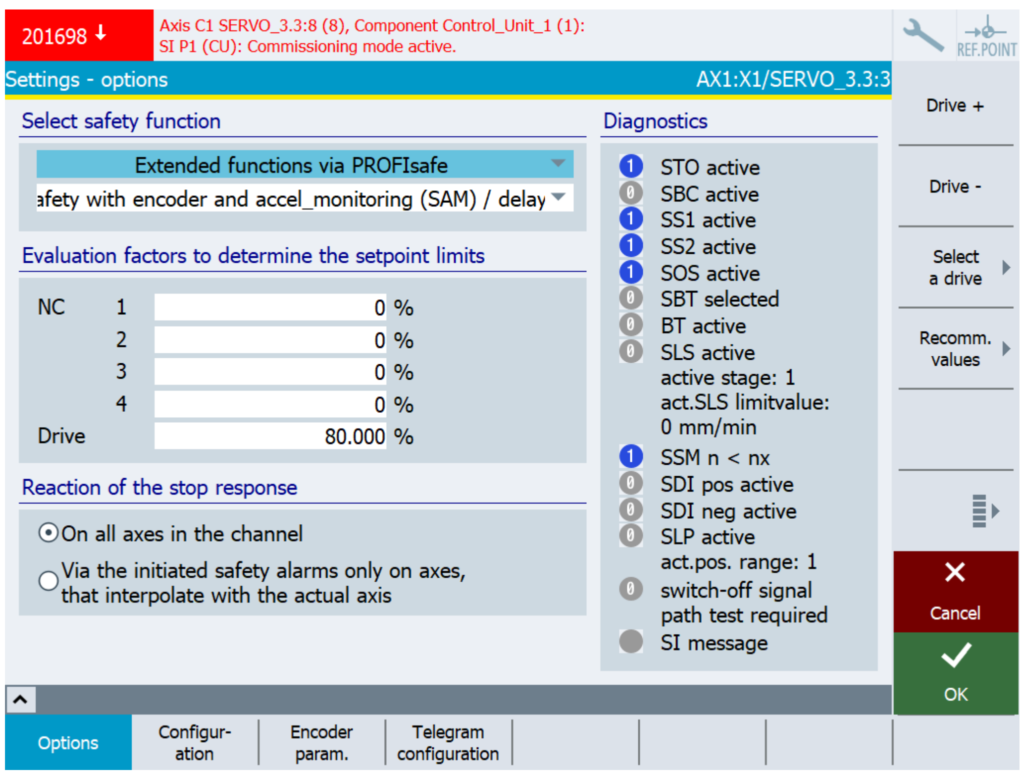


Figure 7-12 Settings - options

3. Select the reaction to the stop response
   – On all axes in the channel
   – Via the triggered safety alarms only on axes that interpolate with the current axis.

   The reaction to the stop response is saved in MD36964 $MA_SAFE_IPO_STOP_GROUP.

7.5.7 Parameterizing an encoder

Requirements

- The SI commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder.

Call the "Encoder parameterization" startup screen form

MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Encoder parameterization

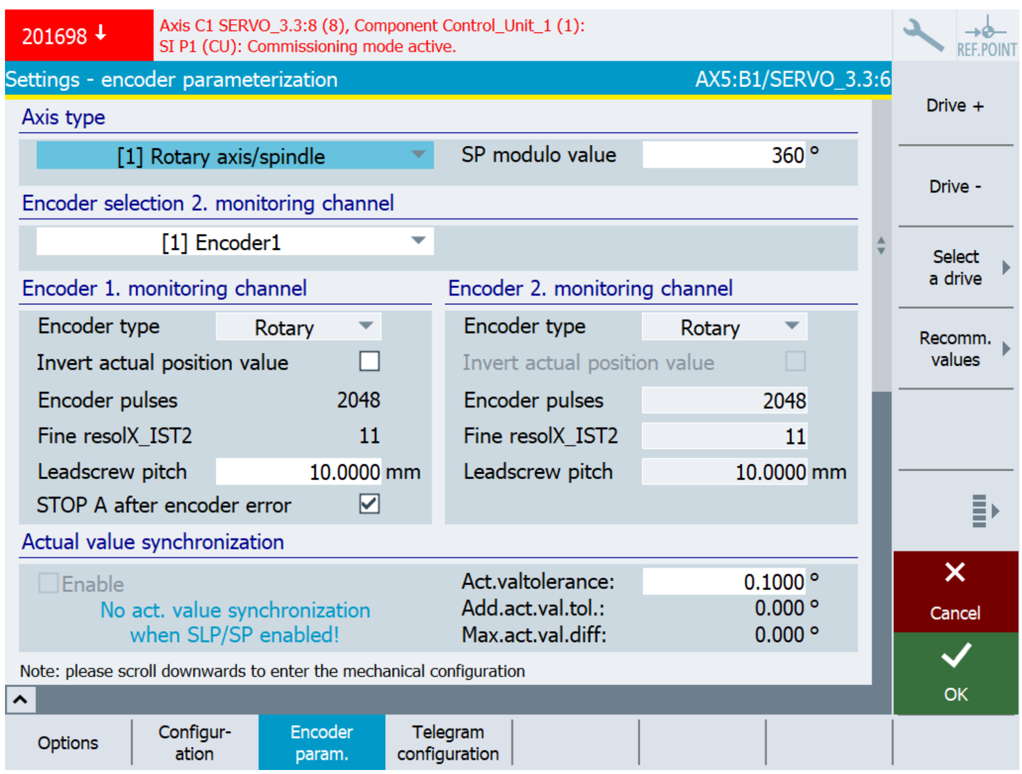


Figure 7-13 Settings - encoder parameterization

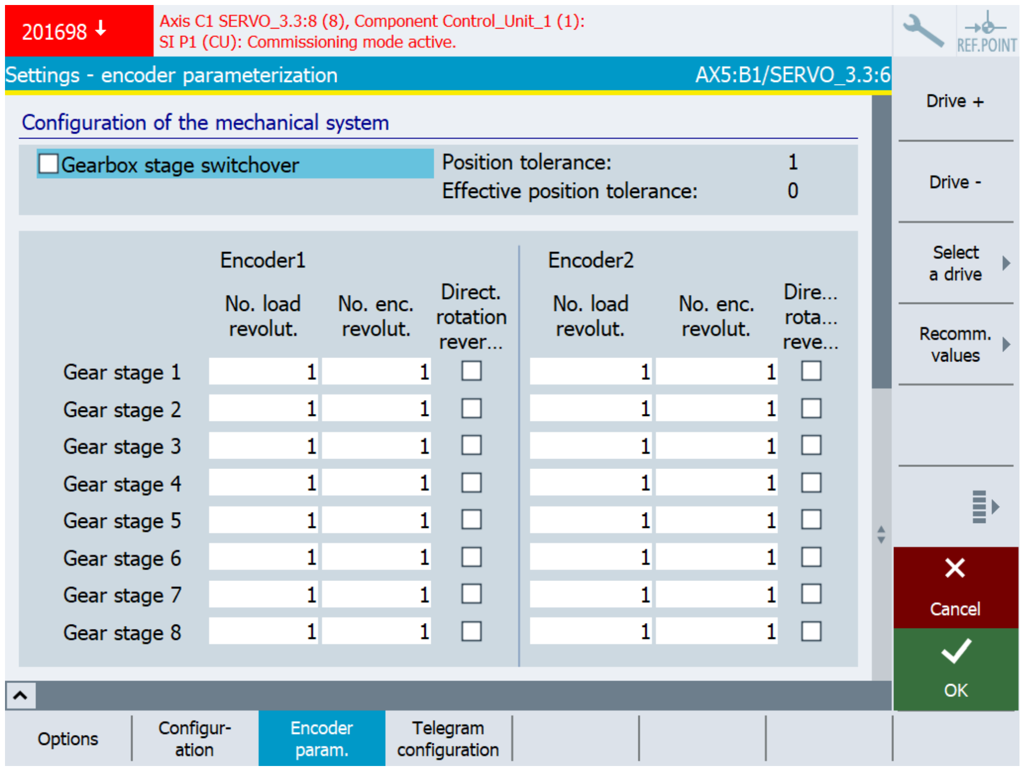


Figure 7-14 Settings - encoder parameterization Mechanical system configuration

Softkey	Purpose
Drive +	The settings are specific to a certain drive. Switch to the corresponding drive using the appropriate softkey before configuring.
Drive -	
Select a drive	
Recommended val- ues	You can automatically assign defaults to the encoder settings of the specific drive using the "Recommended values" softkey. Check the individual suggested values.

Making the settings

Table 7-1 Parameterizing an encoder (setting - encoder parameterization)

Setting	Meaning
Axis type	Sets the axis type (linear axis or rotary axis/spindle).
SP modulo value	Sets the modulo value in degrees for rotary axes for the "Safe position" function. This modulo value is taken into account for safe referencing and for the transfer of the safe position via PROFIsafe when absolute position is ena- bled. The value should be set so that it lies precisely at 2^n revolutions, so that when the range that can be represented overflows (+/-2048), then the position actual value does not exhibit a step (jump). The modulo function is deactivated for a value = 0.
Encoder selection 2nd monitoring channel	Selects a configured encoder as the encoder that is used by the second channel (control, Motor Module) for safe motion monitoring.

Table 7-2 Encoder-monitoring channel (settings - encoder parameterization)

Setting	Meaning
Encoder type	Sets the motor encoder as either rotary or linear encoder.
Invert position actual value	Activates/deactivates the inversion of the position actual value (sign change).
Encoder pulses	Displays the number of encoder pulses per revolution for rotary encoders.
Fine resolution X_IST2	Displays the fine resolution for G1_XIST1 in bits.
Leadscrew pitch	Sets the ratio between the encoder and load in mm/revolutions for a linear axis with rotary encoder.

Table 7-3 Actual value synchronization (settings - encoder parameterization)

Setting	Meaning
Enable	Enables/inhibits actual value synchronization. It is not permissible to enable actual value synchronization and SLP/SP for the same drive.
Actual value tolerance	Sets the tolerance for the crosswise comparison of the actual position between the two monitoring channels.
Additional actual value tolerance	Displays the maximum additional difference between the load-side actual position value on the Control Unit and the load-side actual position value on the second channel, which can occur due to the delay of the actual value acquisition in the EnDat 2.2 converter.
Maximum actual value tolerance	Displays the maximum difference between the load-side position actual value on the Control Unit and the load-side position actual value on the second channel.

Table 7-4 Mechanical configuration (settings - encoder parameterization)

Setting	
Gearbox stage switchover	Enables/inhibits safety-related gearbox stage switchover. When enabled, you can parameterize up to 8 ratios, and switchover the active gearbox stage via PROFIsafe.
Position tolerance	Sets the factor to increase the tolerance for the crosswise data comparison of the actual position between the two monitoring channels while the gearbox stage is being switched over. This factor is active when actual value synchronization is both activated as well as also deactivated. It is obtained, depending on the following tolerance: • Actual value synchronization activated: p9549 * position tolerance • Actual value synchronization deactivated: Actual value tolerance * position tolerance
Active position tolerance	Displays the active position tolerance. (product from the position tolerance and actual value tolerance or velocity tolerance)
Number of load revolutions	Sets the denominator for the gearbox between the encoder and load.

Setting	
Number of encoder revolutions	Sets the numerator for the gearbox between the encoder and load.
Direction reversal	Activates/deactivates the direction of reversal for the gearbox.

7.5.8 Configuring encoderless operation

Requirements

- The SI commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation without an encoder.

Call the startup screen form "Configuration mechanical/actual value sensing"

MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Mechanical /actual value sensing

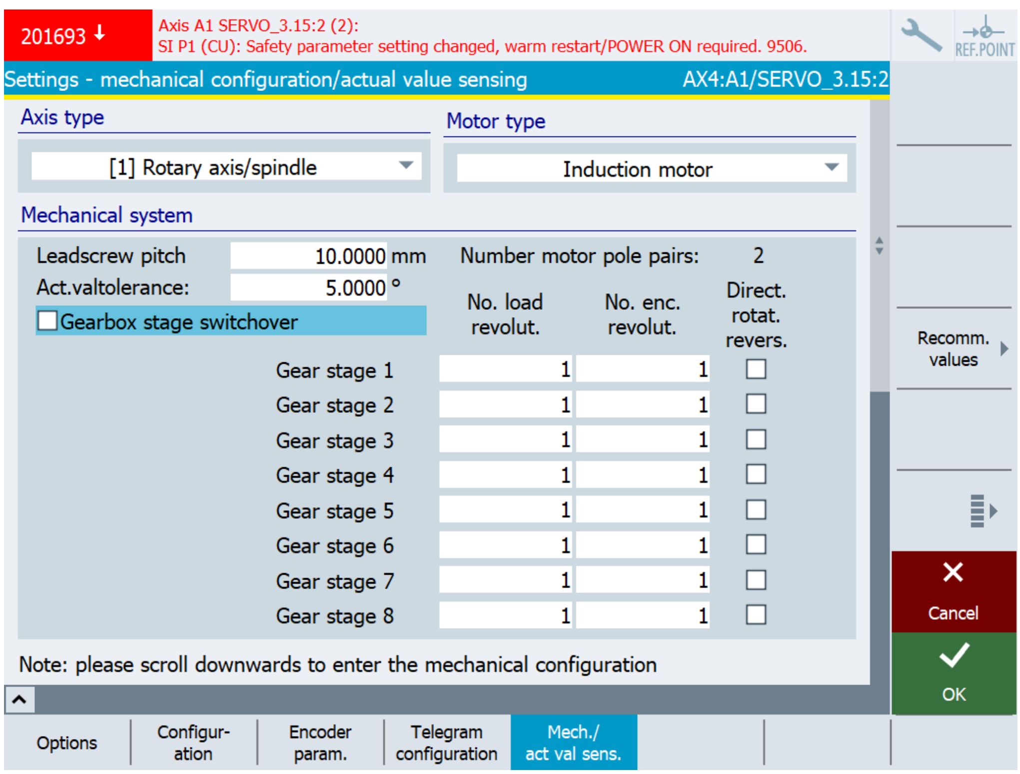


Figure 7-15 Settings – mechanical configuration/actual value sensing: Mechanical system

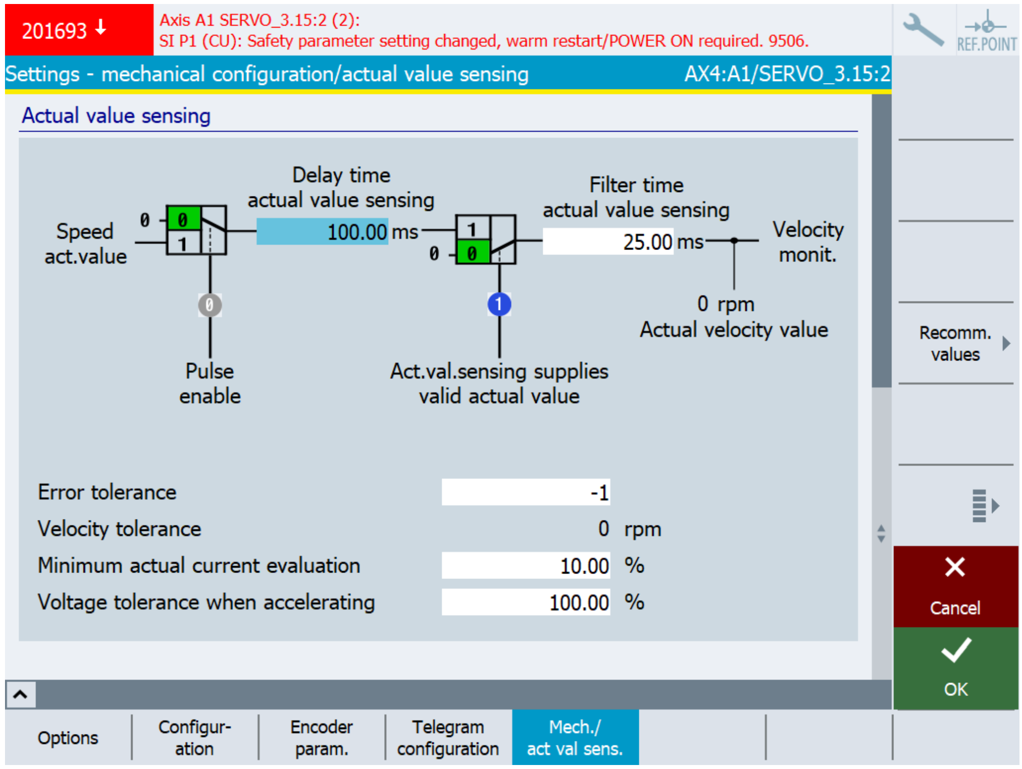


Figure 7-16 Settings – mechanical configuration/actual value sensing: Actual value acquisition

Softkey	Purpose
Drive +	The settings are specific to a certain drive. Switch to the corresponding drive using the appropriate softkey before configuring.
Drive -	
Select a drive	
Recommended val-ues	Using softkey "Recommended values", you can automatically preassign the val-ues of the particular startup screen form. Check the individual suggested values.

Adapting settings

Table 7-5 (Settings – mechanical configuration/actual value sensing)

Setting	Meaning
Leadscrew pitch	Sets the ratio between the encoder and load in mm/revolutions for a linear axis with rotary encoder.
Actual value tolerance	Sets the tolerance for the crosswise comparison of the actual position be-tween the two monitoring channels. The tolerance must be set higher (e.g. 12 degrees rotary and 1 mm linear) for encoderless motion monitoring functions.

Table 7-6 Gearbox stages switchover (Settings - mechanical configuration/actual value sensing)

Setting	Meaning
Gearbox stage switchover	Enables/inhibits safety-related gearbox stage switchover. When enabled, you can parameterize up to 8 ratios, and switchover the active gearbox stage via PROFIsafe.
Number of load revolutions	Sets the denominator for the gearbox between the motor and load. The active gearbox stage can be switched over via PROFIsafe.
Number of encoder revolutions	Sets the denominator for the gearbox between the motor and load. The active gearbox stage can be switched over via PROFIsafe. For encoderless monitoring functions, the numerator of the gear ratio must be multiplied by the number of pole pairs (see below). Example: Gearbox ratio 1:4, number of pole pairs = 2 Number of load revolutions = 1, number of encoder revolutions = 8 (4 x 2)
Direction reversal	Activates/deactivates the direction of reversal for the gearbox.
Motor pole pair number	Displays the number of motor pole pairs.

Table 7-7 Actual value sensing (Settings – mechanical configuration/actual value sensing)

Setting	Meaning
Delay time actual value sensing	Sets the delay time for evaluating the encoderless actual value sensing after the pulses have been enabled. The value should be greater than or equal to the magnetization time of the motor (p0346). The set time is internally rounded off to an integer multiple of the monitoring clock cycle. Caution: The safety functions are not fully effective until this time has elapsed. Notice: Reducing this value can have a negative impact on the actual value acquisition and plausibility check - and result in safety message C01711 with message value 1041 or 1042. Dependencies: C01711
Filter time actual value sensing	Sets the filter time for the actual value smoothing for actual value acquisition without encoder. Notice: A higher filter time results in a longer response time. The smoothing is realized using a 1st order lowpass filter. For a minimum value, the filter is deactivated. The set time is internally rounded off to an integer multiple of the monitoring clock cycle.
Pulse enable	Display: Enable power
Actual value sensing supplies valid actual value	Display: Actual value sensing supplies valid actual value
Actual speed value	Displays actual speed values for motion monitoring on the Control Unit. Index [0] = load side actual speed value on the Control Unit

Setting	Meaning
Fault tolerance	Setting of the plausibility monitoring tolerance for the current and the voltage angle. A higher value makes the drive more stable when it is reversing at low speeds - or when the load changes abruptly in the field-weakening range. An increase brings advantages when the current or voltage at the motor becomes small. Increasing the value results in a longer evaluation delay - and to a higher speed tolerance (see below). Notice: Reducing this value can have a negative impact on the actual value acquisition and the plausibility check. For synchronous motors, the value must be set to 4. For value = -1: - for synchronous motors, the calculation automatically uses a value of 4 - for induction motors, the calculation automatically uses a value of 0 (if the code number of the power unit p0201[0] is < 14000, otherwise a value of 2 is used). Dependencies: F01681, C01711
Speed tolerance	Displays the actual speed deviation for encoderless actual value acquisition. This value is calculated when setting the error tolerance (see above).

<table>
<tr><th>Setting</th><th>Meaning</th></tr>
<tr><td>Minimum actual current sensing</td><td>Sets the minimum current for encoderless actual value acquisition referred to 1 A (i.e. 1 % = 10 mA).
• The value must be increased if C01711 is output with message value 1042.
• The value must be decreased if C01711 is output with message value 1041.
For synchronous motors, the following condition must be satisfied:
|p0305 x p9783| >= minimum current actual value acquisition x 1.2
Recommendation: If necessary, to determine the correct value, the minimum motor current must be measured.
Notice: An excessive reduction of this percentage value can result in a safety message and in an inaccurate actual value.
Dependencies: r9785, C01711</td></tr>
<tr><td>Acceleration voltage tolerance</td><td>Sets the acceleration limit to filter discontinuities in the speed/velocity. The filter is deactivated when setting the maximum value.
An increase in this percentage value means that velocity peaks can occur when accelerating, which do not reflect the real velocity characteristic.
A decrease in this value dampens velocity peaks when accelerating.
• The value must be increased if message C01711 is output with the value 1043.
• The value must be decreased if acceleration has resulted in an excessive safety actual velocity.
Recommendation: This parameter setting depends on the motor and closed-loop control, and must be redetermined for each configuration.
To do this, a measurement must be made while the actual value is changing (step function/jump), and the limit should be set so low in r9785[0] via p9589 that it is not exceeded more than four times per second by the value set in r9785[1]. At this point in time, the actual value correction filter intervenes. The step is no longer so drastic.
Dependencies: r9784, C01711</td></tr>
</table>

See also

Selecting the safety functional scope (Page 267)

7.5.9 Configuring telegrams

Requirements

- The Safety Integrated commissioning mode has been activated for the drive to be configured.
- Extended Functions or Basic Functions via PROFIsafe are set for the drive to be configured.

Call up "Telegram configuration" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Telegram configuration

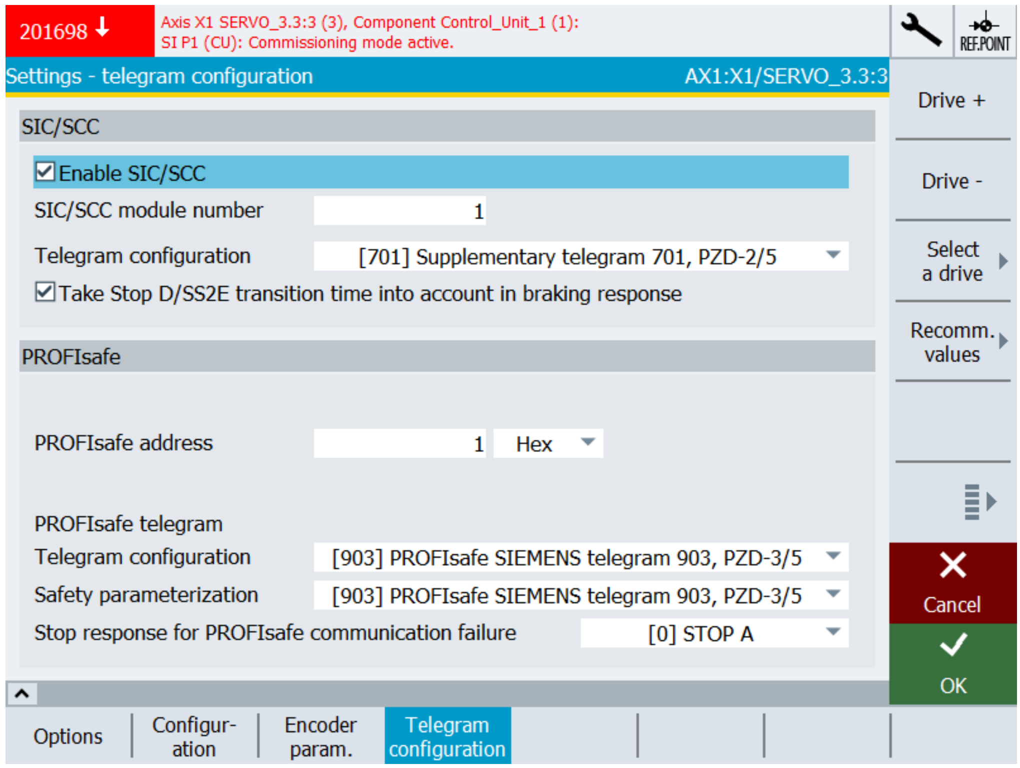


Figure 7-17 Settings - telegram configuration

Softkey	Purpose
Drive +	The settings are specific to a certain drive. Switch to the corresponding drive using the appropriate softkey before configuring.
Drive -	
Select a drive	
Recommended values	Using softkey "Recommended values", you can automatically preassign the values of the particular startup screen form. For example, in the startup screen form "Telegram configuration", the telegram types from the configuration belong to the settings that can be assigned as default. Check the individual suggested values.

Making the settings

Table 7-8 SIC/SCC telegram settings (Settings - telegram configuration)

Setting	Meaning
Enable SIC/SCC	Enables/inhibits the evaluation of the Safety Info Channel / Safety Control Channel (SCC/SIC).
SIC/SCC module number	Sets the SIC/SCC module number.

Setting	Meaning
Telegram configuration	Sets the telegram type for the Safety Info Channel (SIC)/Safety Control Channel (SCC)
Takes into account the stop D/SS2E transition time in the braking response	Activates the adaptation of the braking ramp for stop D/SS2E

Table 7-9 PROFIsafe telegram settings (Settings - telegram configuration)

Setting	Meaning
PROFIsafe address	Sets the PROFIsafe address for the Control Unit.
Telegram configuration	Sets the PROFIsafe telegram type.
Safety parameter assignment	Sets the PROFIsafe telegram type for the Control Unit.
Stop response for PROFIsafe communication failure	Setting the stop response in case of failure of the PROFIsafe communication

See also

Activating Safety Integrated commissioning mode (Page 266)

7.6 Configuring SafeUserData in the SINUMERIK Commissioning Tool

7.6.1 Overview

The screen forms to use SafeUserData are provided in SINUMERIK Operate (or in the SINUMERIK ONE Commissioning Tool) in operating area "Commissioning".

Precondition

- Softkey "SafeUserData" is only visible if you configure the SafeUserData blocks in the PLC project, and have set the "Machine manufacturer" password.

Call

MENU SELECT > Commissioning > Menu forward key > Safety > Overview

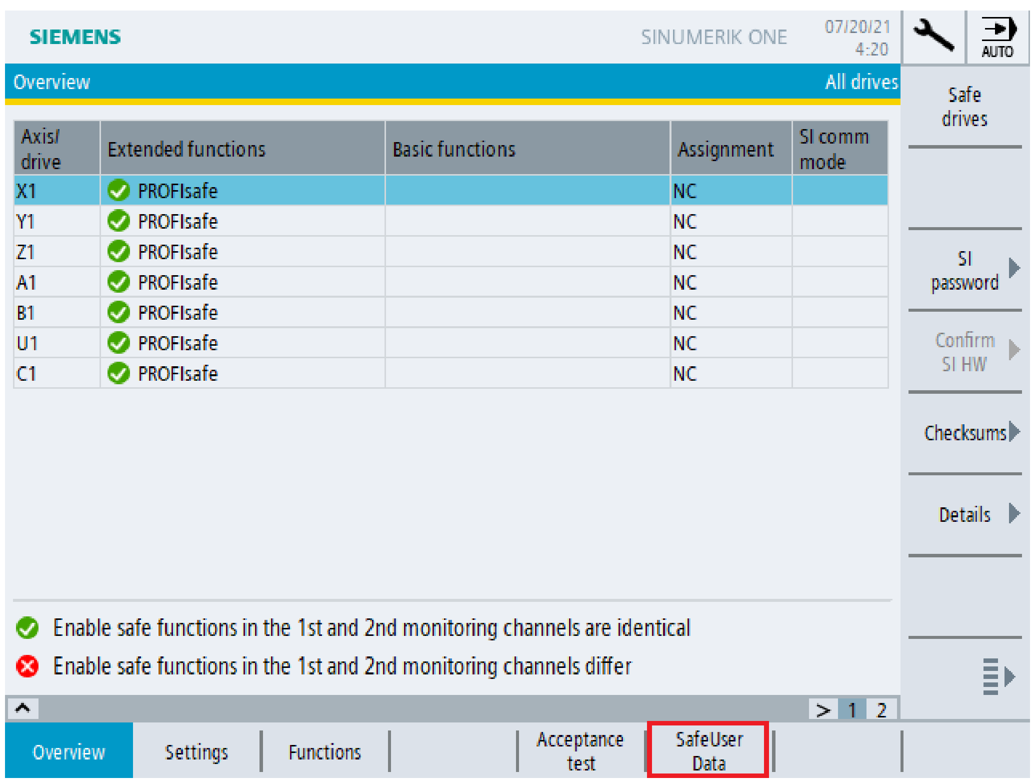


Figure 7-18 Safety overview with softkey "SafeUserData"

7.6.2 SafeUserData - Block overview

All of the SafeUserData instances that have been created are listed in screen form "SafeUserData - Overview".

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData

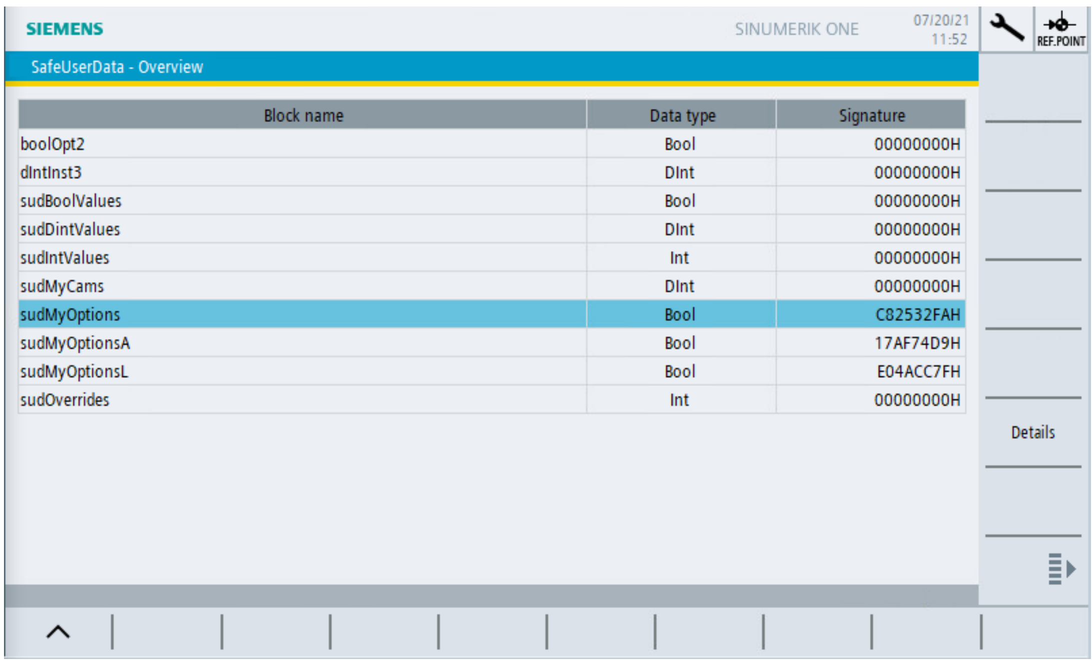


Figure 7-19 SINUMERIK ONE example: SafeUserData - Block overview

Table 7-10 Information

Name	Description
Block name	The "User interfaces DB" of SafeUserData are listed in this column.
Type	The data type of the "User interfaces DB" is displayed in this column.
Signature	The actual signature of the SafeUserData instance is displayed in this column.

Table 7-11 Vertical softkeys

Name	Description
Details	Using this softkey, you switch to screen form "SafeUserData - Details".

7.6.3 SafeUserData - Details

All elements with the active values of the selected "User interfaces block" are displayed in screen form "SafeUserData - Overview - Details".

If changing the values has not been released, then the vertical softkey "Change" is grayed out.

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details

Figure 7-20 SINUMERIK ONE example: SafeUserData - Details

Table 7-12 Information

Name	Description
Signature	The current signature is displayed above the table.
Element name	The names of all block elements are listed in this column.
Format	The display format is displayed in this column (B = bool, +/-D = Int/DInt).
Active value	The values active in the PLC are displayed in this column.

Table 7-13 Vertical softkeys

Name	Description
Block+	If several blocks exist, you can select the next block with block+. This softkey is not displayed if there is only one block.
Block-	If several blocks exist, you can select the previous block with block. This soft-key is not displayed if there is only one block.

Name	Description
Select block >	A selection box is displayed using this softkey. It includes a list of all of the blocks. You can select a block from this list. This softkey is not displayed if there is only one block.
Change	Using this softkey, you switch to screen form "SafeUserData - Change".
<< Back	Using this softkey you switch back to the block overview.

7.6.4 Configure SafeUserData

7.6.4.1 SafeUserData - Change active values

You can change the values in screen form "SafeUserData - Change". Softkey "Accept" is grayed out as long as nothing has been changed. The changed values are saved in the internal SINUMERIK Operate memory (or in the SINUMERIK ONE Commissioning Tool). To transfer the changed values, softkey "Accept" must be pressed (see "Accepting activated values (Page 288)").

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details > Change

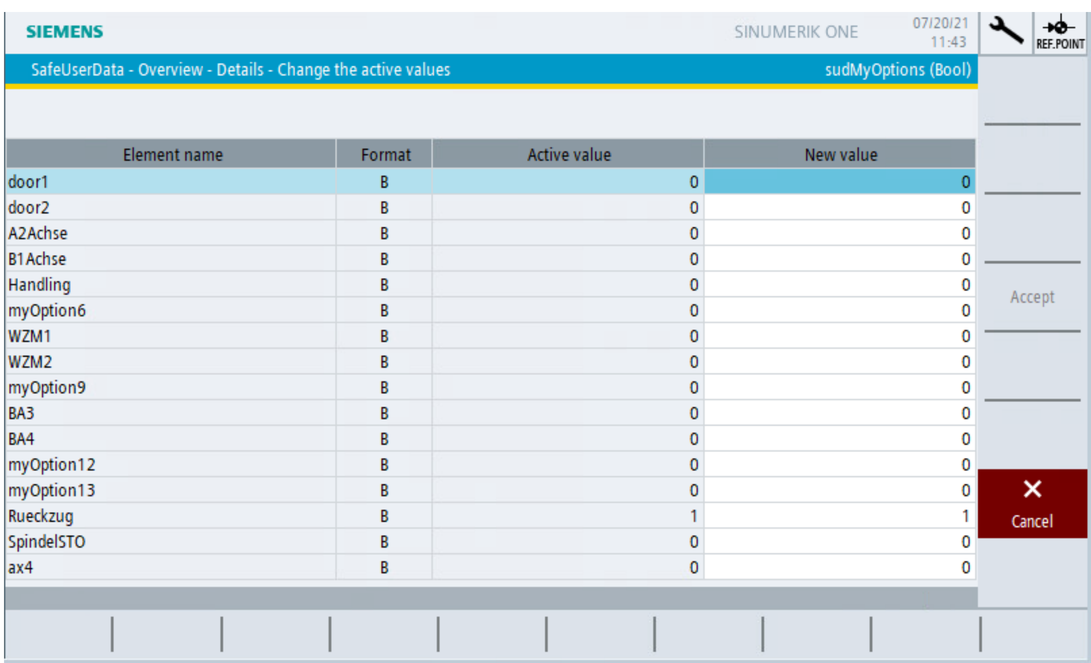


Figure 7-21 SINUMERIK ONE example: SafeUserData - Change

Table 7-14 Information

Name	Description
Element name	The names of all block elements are listed in this column.
Format	The display format is displayed in this column (B = bool, +/-D = Int/DInt).

Name	Description
Active value	The values active in the PLC are displayed in this column.
New value	You can make changes in this column (fields that have been changed are assigned a yellow background).

Table 7-15 Vertical softkeys

Name	Description
Accept	Softkey "Accept" is grayed out as long as you have made no modification in this block. The changed values are accepted using this softkey.
Cancel	You cancel the change using this softkey.

7.6.4.2 SafeUserData - Accept activated values

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details > Change > Transfer

Softkey "Accept" is active after individual values have been modified. Modified values are assigned a "yellow" background.

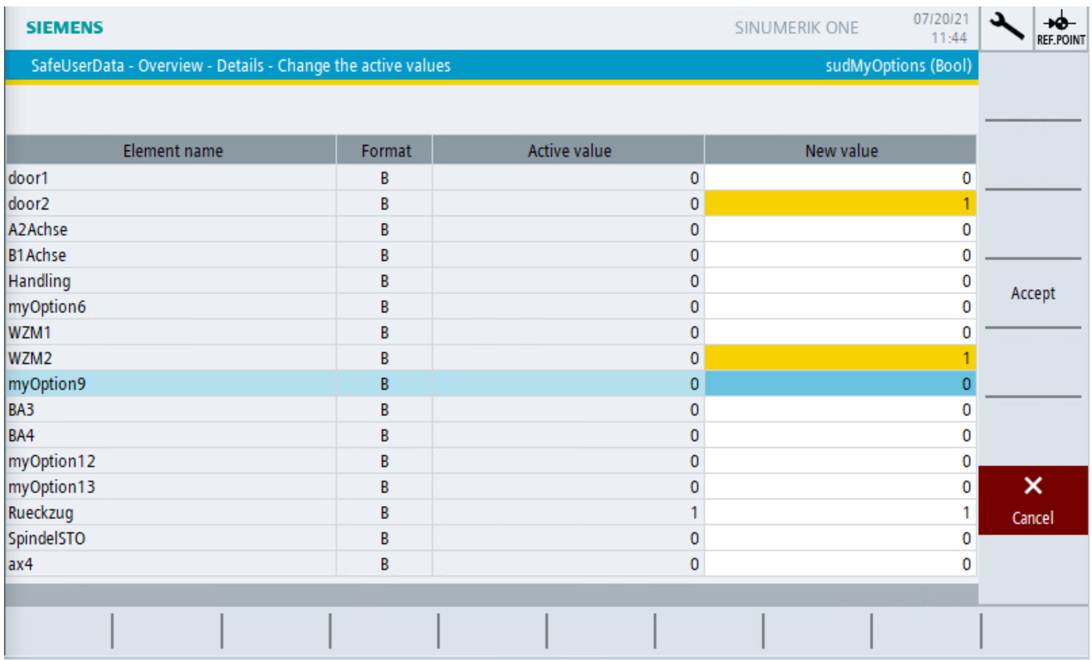


Figure 7-22 SINUMERIK ONE example: SafeUserData - Accepting active values

Table 7-16 Information

Name	Description
Element name	The names of all block elements are listed in this column.
Format	The display format is displayed in this column (B = bool, +/-D = Int/DInt).
Active value	The values active in the PLC are displayed in this column.
New value	You can make changes in this column (fields that have been changed are assigned a yellow background).

Table 7-17 Vertical softkeys

Name	Description
Accept	The values are transferred to the PLC after pressing softkey "Accept". It is checked there, and for a positive result, is output at the user interfaces block. You are then requested to check/test the newly activated values, and to exit the change sequence by pressing softkey "Confirm/Save" (see "Check newly activated values (Page 290)").
Cancel	You cancel the change sequence using this softkey.

7.6.4.3 SafeUserData - Check newly activated values

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details > Change > Accept

After the modified values have been accepted, you must compare the values in column "Newly activated value" with the values in "Entered value". After the check, start the confirmation sequence using softkey "Confirm/Save".

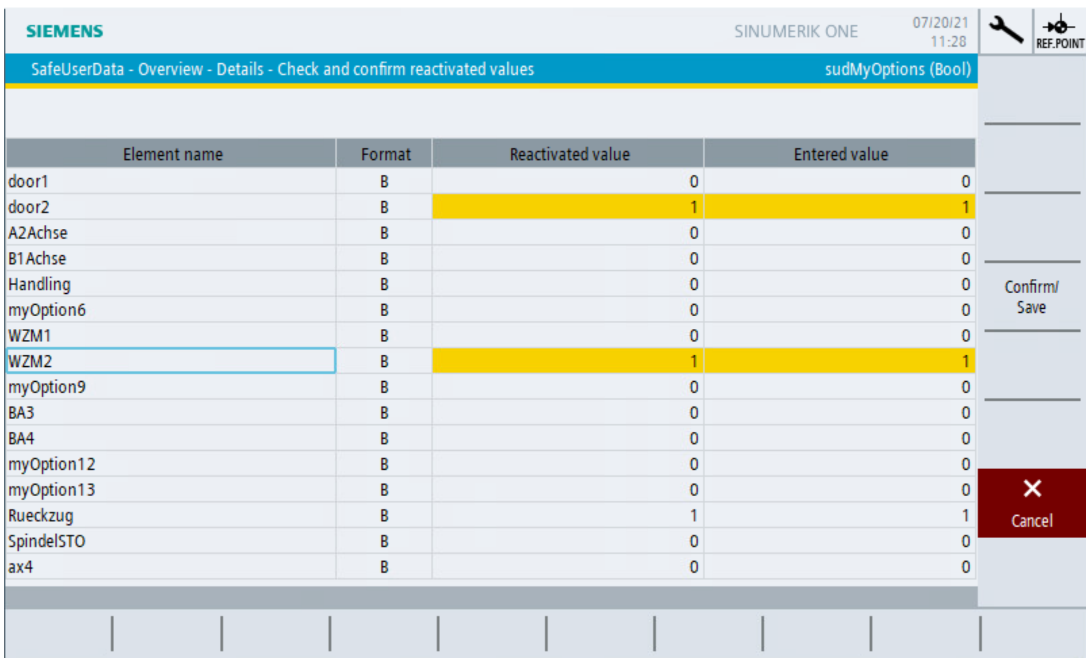


Figure 7-23 SINUMERIK ONE example: SafeUserData - Checking newly activated values

Table 7-18 Information

Name	Description
Element name	The names of all block elements are listed in this column.
Format	The display format is displayed in this column (B = bool, +/-D = Int/DInt).
Newly activated value	The values active in the PLC are displayed in this column.
Entered value	The newly entered value is displayed in this column.

Table 7-19 Vertical softkeys

Name	Description
Confirm/save	You start the confirmation sequence at the PLC using this softkey. The PLC confirms the values, the block signature is updated and saved.
Cancel	You cancel the change sequence using this softkey. The activated values are reset, and the previously valid values are again active. The confirmation sequence with the PLC is not started. After cancellation, screen form "SafeUserData - Changing the active values" is displayed.

7.6.4.4 SafeUserData - Confirm/save changed values

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details > Change > Accept > Confirm/Save

The following screen form is displayed if the PLC confirms the changed values:

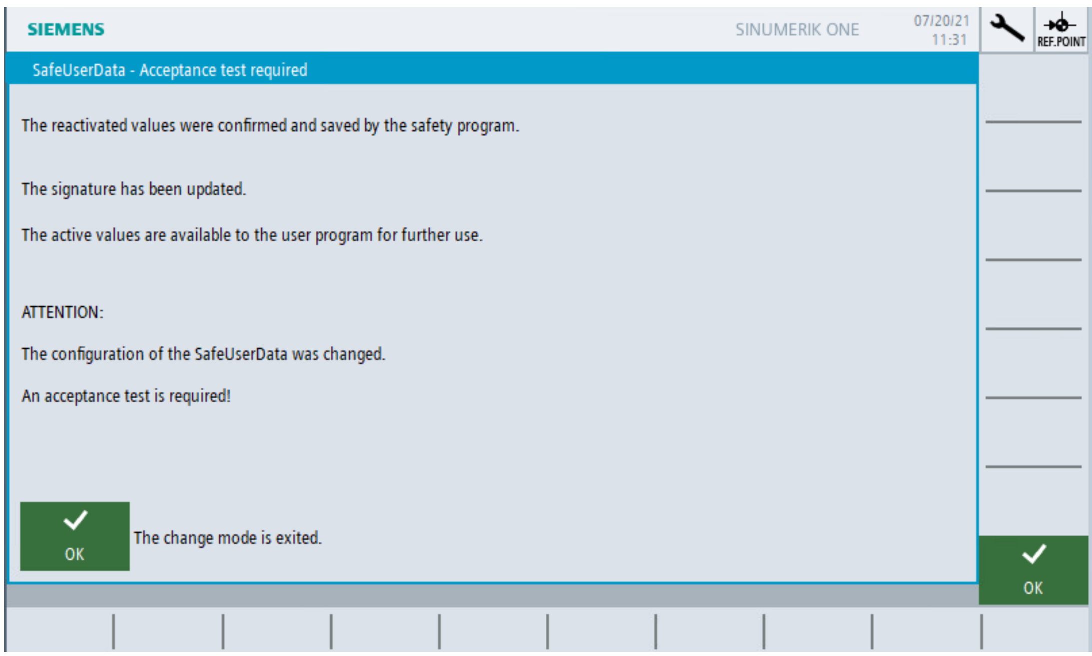


Figure 7-24 SINUMERIK ONE example: SafeUserData - Confirming/saving changed values

Table 7-20 Vertical softkey

Name	Description
OK	You exit the change mode using the softkey. You return to screen form "SafeUserData - Overview - Details".

Result

The SafeUserData has now been configured. The data was saved and is available at the user interface. The block signature was updated.

- **Important**: At the end, carry out an acceptance test in SINUMERIK Operate (or in the SINUMERIK ONE Commissioning Tool).

7.6.5 SafeUserData - Default values

7.6.5.1 SafeUserData - Default value details

Overview

To reduce the data entry time, for data changes default values can be saved in a data block. If a data block with the default values for the selected user interfaces block exists, then softkey "Default values" in screen form "SafeUserData – Details" and in screen form "SafeUserData – Changing the active values" is active and can be used.

In the change mode, the default values can then be transferred as complete data set into the internal memory of SINUMERIK Operate (or in the SINUMERIK ONE Commissioning Tool); they are then visible in column "New values". It is not possible to partially transfer the default values.

Information is subsequently provided as to how you can execute the change sequence with default values.

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details

All elements with the active values of the selected "User interfaces block" are displayed in screen form "Details". The default values can be displayed as read-only values using softkey "Default values". To activate the default values you must first press softkey "Change".

Figure 7-25 SINUMERIK ONE example: SafeUserData - Displaying default values

7.6.5.2 SafeUserData - Accept default values

Call

MENU SELECT > Commissioning > Menu forward key > Safety > SafeUserData > Details > Change > Default values

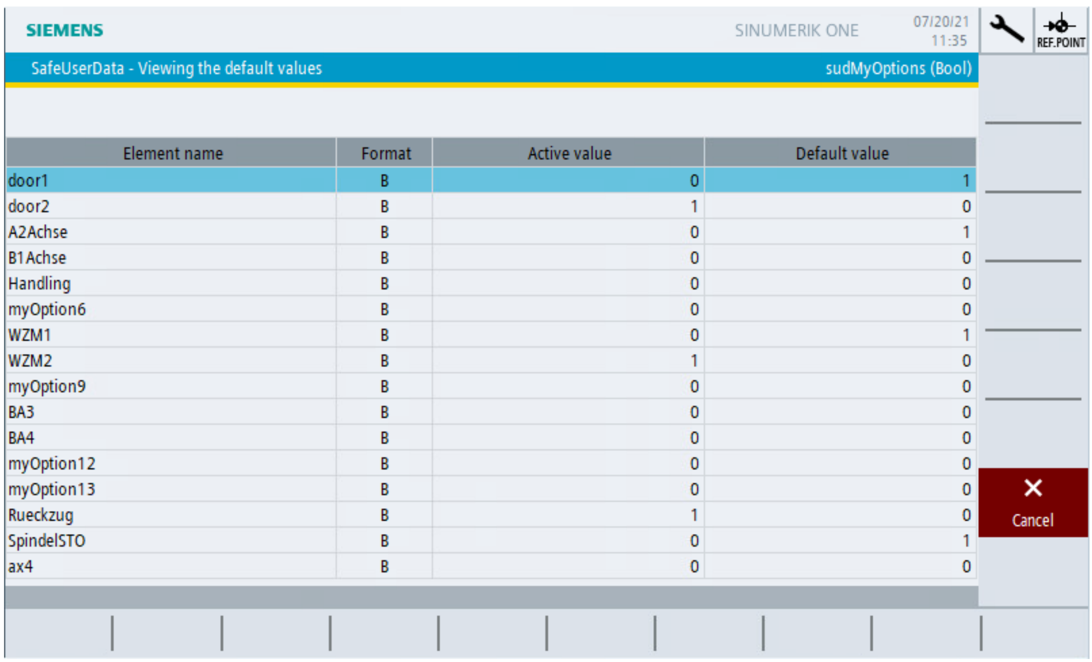


Figure 7-26 SINUMERIK ONE example: SafeUserData - Accepting default values

The default values are now displayed in the column to the right of "Active value".

Table 7-21 Information

Name	Description
Element name	The names of all block elements are listed in this column.
Format	The display format is displayed in this column (B = bool, +/-D = Int/DInt).
Active value	The values active in the PLC are displayed in this column.
Default value	The default values stored in a data block are displayed in this column.

Table 7-22 Vertical softkeys

Name	Description
OK	You accept all default values as "New value" in the internal memory of SINUMERIK Operate (or the SINUMERIK ONE Commissioning Tool). Screen form "SafeUserData - Changing the active values" (see "Change activated values (Page 286)") is redisplayed. The fields that have been changed have a yellow background.
Cancel	You cancel the acceptance of the default values using this softkey. After cancellation, screen form "SafeUserData - Changing the active values" is displayed.

7.6.6 SafeUserData - Comments for blocks and block elements

7.6.6.1 SafeUserData - Create template for comments

The SUD blocks and SUD block element comments can be displayed as tooltip via SINUMERIK Operate (or the SINUMERIK ONE Commissioning Tool).

Procedure

1. In SINUMERIK Operate, create a template file for the comment text.
2. Open screen form "SafeUserData - Overview".
3. Press softkey "Generate comments" to create a template for all blocks.
   When doing this, file "oem_sud_tooltip_eng.ts" is created under directory "/HMI data/Safety Integrated/SafeUserData/Tooltip template".
   You can enter your own comments in this template, which are then used as basis for additional languages.

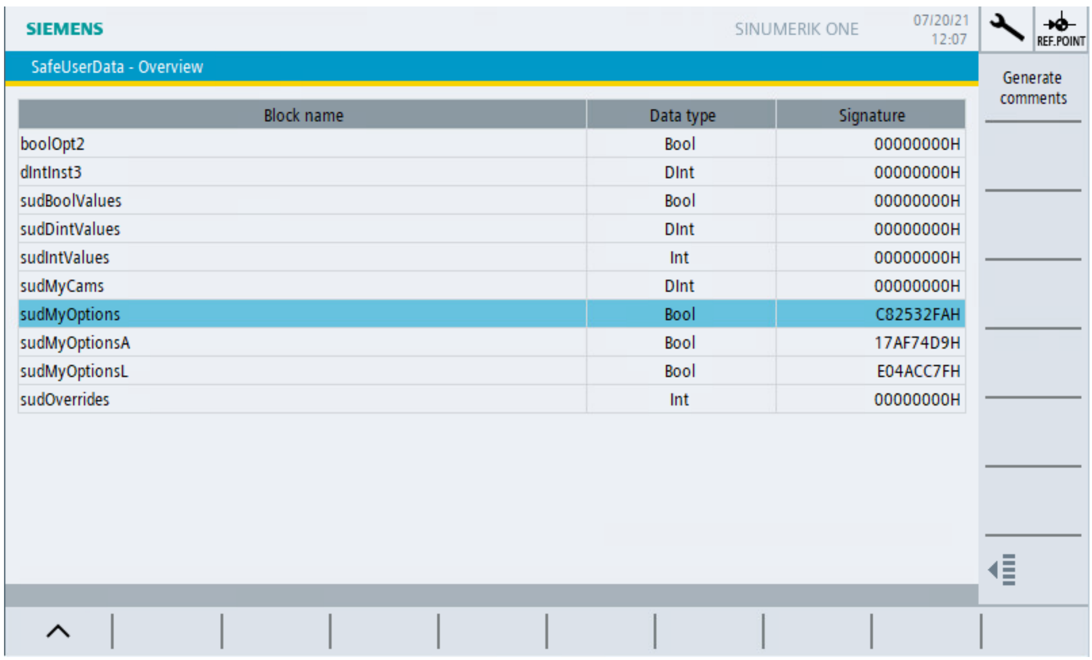


Figure 7-27 SafeUserData - Generating overview with softkey comments

7.6.6.2 SafeUserData - Edit template for comments

Tag "context" includes the description of a user interfaces block. Text "Tooltip text" can be replaced by your own comment text in tag "translation" for each block/each block element.

After editing, the file must be copied to the control to directory "/HMI data/Text/Manufacturer". The comments are available after SINUMERIK Operate (or the SINUMERIK ONE Commissioning Tool) restarts. This must be performed for each language setting required.

Example of an excerpt from a processed "*.ts file":

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE TS>
<TS>
    <context>
        <name>sudMyOptions</name>
        <message>
            <source>TT_sudMyOptions</source>
            <translation>SafeUserData options</translation>
        </message>
        <message>
            <source>TT_WZM2</source>
            <translation> tool magazine2 available</translation>
        </message>
    </context>
</TS>
```

Display of user comments at SINUMERIK Operate:

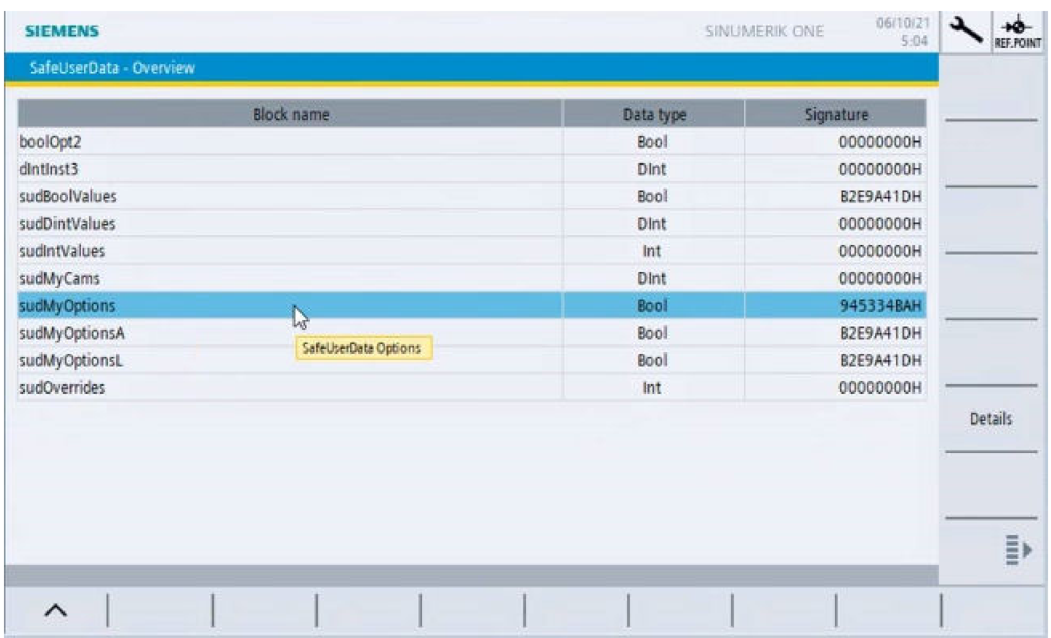


Figure 7-28 SafeUserData - Overview, with comment for block

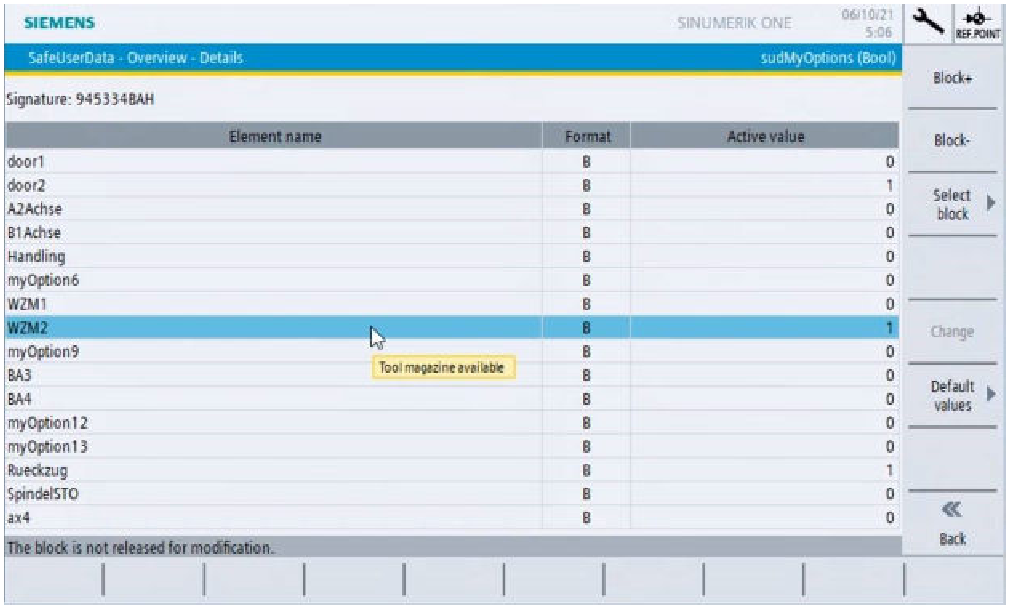


Figure 7-29 SafeUserData - Details, with comment for block element

7.7 Configuring safety functions integrated in the drive

7.7.1 Overview

SINUMERIK Operate screen forms and settings to commission the various safety functions are described in this chapter.

Basic procedure

Call the appropriate startup screen forms in SINUMERIK Operate and configure the safety functions for the individual drives.

Table 7-23 Startup screen forms and function descriptions

Startup screen form	**Detailed function description**
STO (Page 115)/ SS1 Basic (Page 104)	Safe Torque Off (Page 115) / Safe Stop 1 (Page 104)
STO Extended (Page 303)	Safe Torque Off (Page 115)
SBC (Page 305)	Safe Brake Control (Page 121)
SS1 Extended (Page 307)	Safe Stop 1 (Page 108)
SS2/SOS (Page 309)	Safe Stop 2 (Page 128) / Safe Operating Stop (Page 139)
SLS (Page 315)	Safely-Limited Speed (Page 143)
SSM (Page 319)	Safe Speed Monitor (Page 156)
SAM (Page 311)	Safe Acceleration Monitor (Page 162)
SBR (Page 313)	Safe Brake Ramp (Page 164)
SDI (Page 321)	Safe Direction (Page 168)
SLP/SP (Page 323)	Safely-Limited Position (Page 176) / Safe Position (Page 181)
SBT (Page 326)	Safe Brake Test (Page 185)
SCA (Page 329)	Safe Cam (Page 197)

Startup screen form	Detailed function description
Can only be parameterized via the parameter list	Safely-Limited Acceleration (Page 200)
SS2E (Page 331)	Safe Stop 2 with external stop (Page 131)
SS2ESR (Page 333)	Safe Stop 2 extended stop and retract (Page 135)
Safe referencing (Page 335)	Safe referencing (Page 204)

You can find additional information on the function sequence of parameterization in the Function Description.

In many cases, using the "Recommended values" softkey, you can automatically preassign the values of the particular startup screen form.

Alternative to the commissioning screen forms, you can switch to "Parameter list", where all of the parameters are listed in tabular form that are relevant for the particular safety function.

7.7.2 STO/SS1 Basic

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- One of the basic functions is selected.

Displaying the "Safe torque off - STO/SS1 Basic" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > STO/SS1 Basic

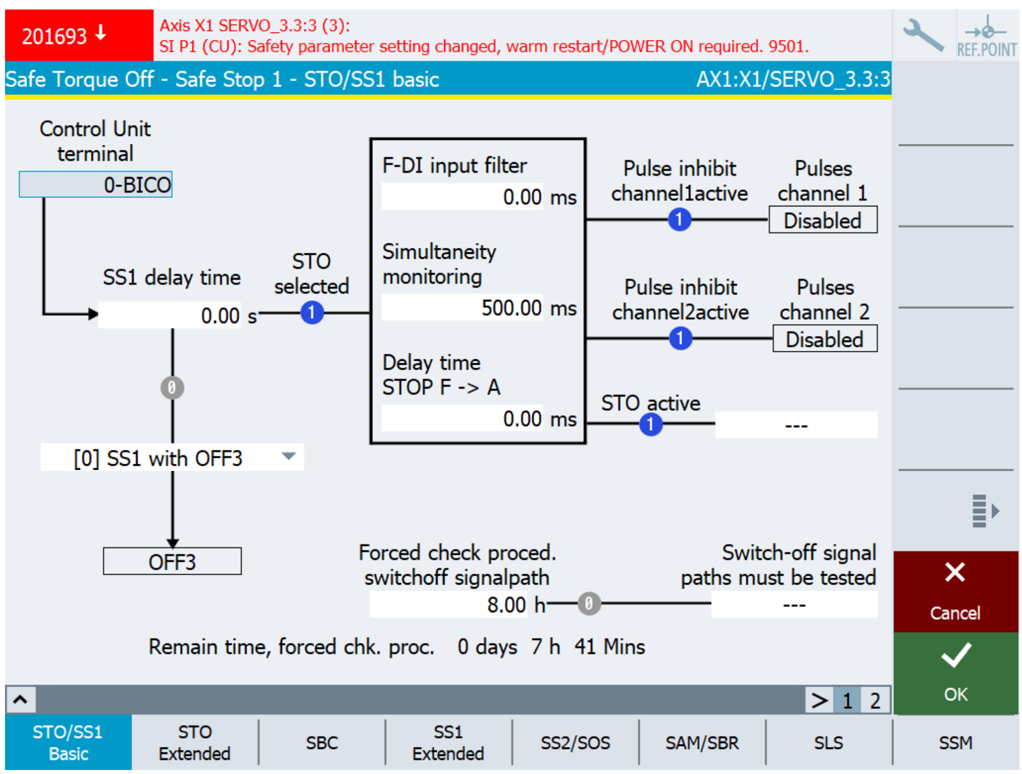


Figure 7-30 Safe Torque Off - Safe Stop 1 - STO/SS1 Basic

Status information

For the following parameters, the status symbols indicate the actual state (blue = active; gray = inactive):

Status	Meaning
STO selected r9772.0	"STO selected in the drive" setting
no text (brake response) r9773.2	Setting "SS1 Delay time active in the drive"

Status	Meaning
Pulse inhibit channel 1 active r9772.1	Setting "STO or safe pulse cancellation active on the CU"
Pulse inhibit channel 2 active r9872.1	Setting "STO on Motor Module active"
STO active r9773.1	Setting "STO active in the drive"
Switch-off signal path test required r9773.31	Setting "Switch-off signal paths must be tested"

Settings

Setting	Meaning
Control unit terminal p9620[0]	Sets the signal source for the STO, SBC and SS1 functions of the Control Unit. This is only relevant if a basic function via terminal is set in the options. Otherwise, the input field is deactivated.
SS1 delay time p9652	Sets the delay time of the pulse cancellation in seconds for the function "Safe Stop 1" (SS1) on the Control Unit to brake along the OFF3 down ramp (p1135).
Braking response for SS1 p9653	Select a predefined braking response below the input field "SS1 delay time". Parameter p9653 is preassigned depending on the selected braking response.
F-DI input filter p9651	Setting the debounce time in ms for the Failsafe Digital Inputs to control STO/SBC/SS1.
Simultaneity monitoring p9650	Sets the discrepancy time in ms for the switchover of the safety-related inputs (SGE) on the Control Unit.
STOP F -> STOP A delay time p9658	Sets the transition time from STOP F to STOP A in ms on the Control Unit.
Forced checking procedure of the switch-off signal paths p9659	Sets the time interval in hours for carrying out the forced checking procedure and testing the switch-off signal paths.
Switch-off signal path test required r9773.31	To evaluate whether the switch-off signal paths must be tested, the status of r9773.31 "Switch-off signal path must be tested" can be interconnected with a parameter via the BICO editor.

7.7.3 STO Extended

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display commissioning screen "Safe torque off - STO Extended"

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > STO Extended

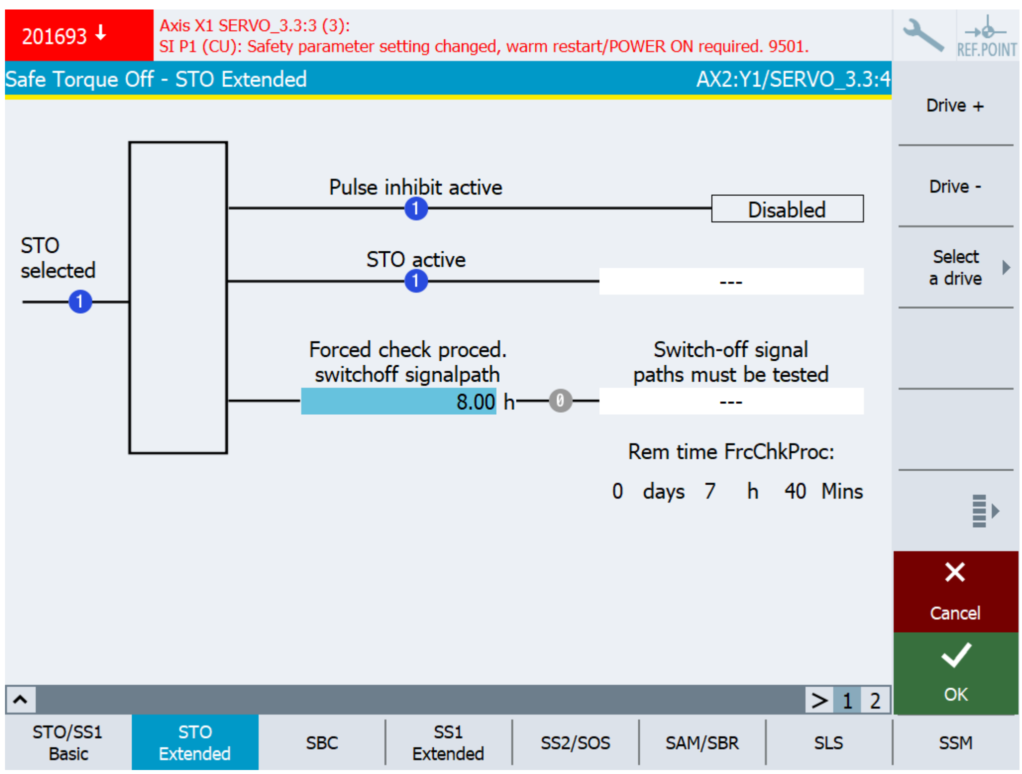


Figure 7-31 Safe torque off - STO Extended

Status information

Status	Meaning
STO active r9773.1	Safety Integrated status of the drive (Control Unit and MM).
Test stop required r9773.31	

Settings

Setting	Meaning
Forced checking procedure of the switch-off signal paths p9659	Sets the time interval for performing the forced checking procedure and testing the safety switch-off signal paths. Within the parameterized time, STO must have been deselected at least once. The monitoring time is reset at every STO deselection.

7.7.4 SBC

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- At least one safety monitoring function is enabled for the drive.
- A motor holding brake has been configured for the drive.

Display "Safe brake control - SBC" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SBC

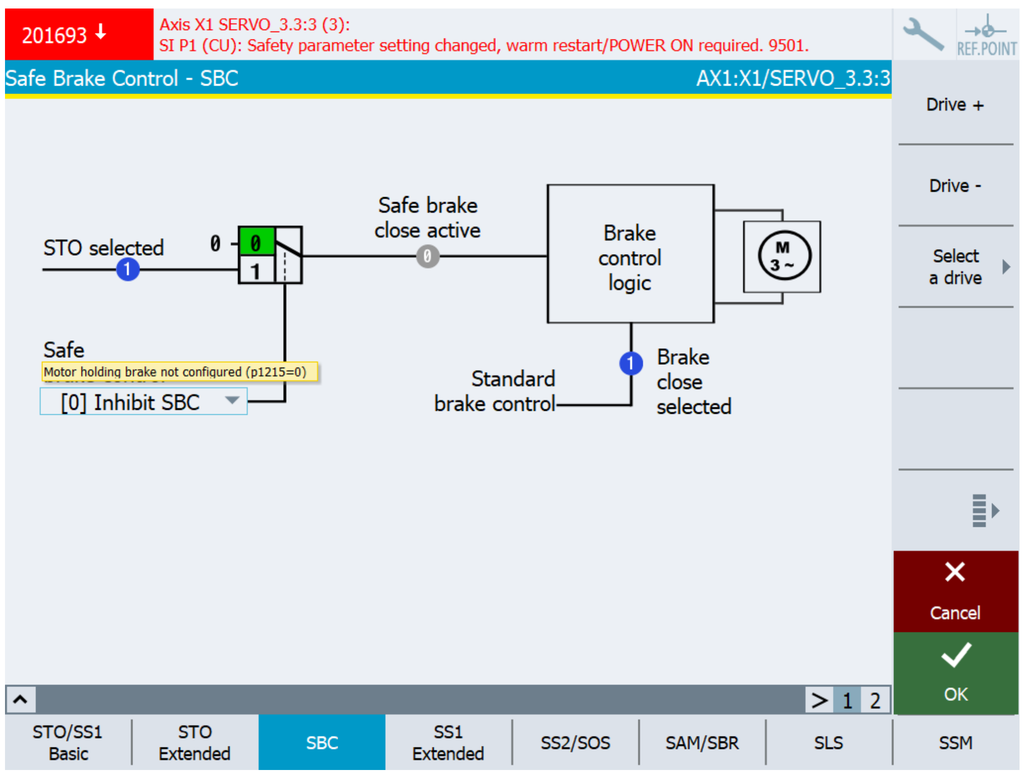


Figure 7-32 Safe brake control - SBC

Status information

Status	Meaning
STO selected r9773.0	Display and BICO output for the status of Safety Integrated on the drive (Control Unit + Motor Module): STO selected in the drive
Switching element	See "Safe brake control" setting

Status	Meaning
Safe brake close active r9773.4	Display and BICO output for the status of Safety Integrated on the drive (Control Unit + Motor Module): SBC requested
Close brake selected r0899.13	Display and BICO output for the status word of the sequence control: Command, close holding brake

Settings

Setting	Meaning
Safe brake control p9602	Sets the enable signal for the "Safe brake control" (SBC) function on the Control Unit. • [0] Inhibit SBC • [1] Enable SBC

7.7.5 SS1 Extended

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display "Safe Stop 1 - SS1 Extended" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SS1 Extended

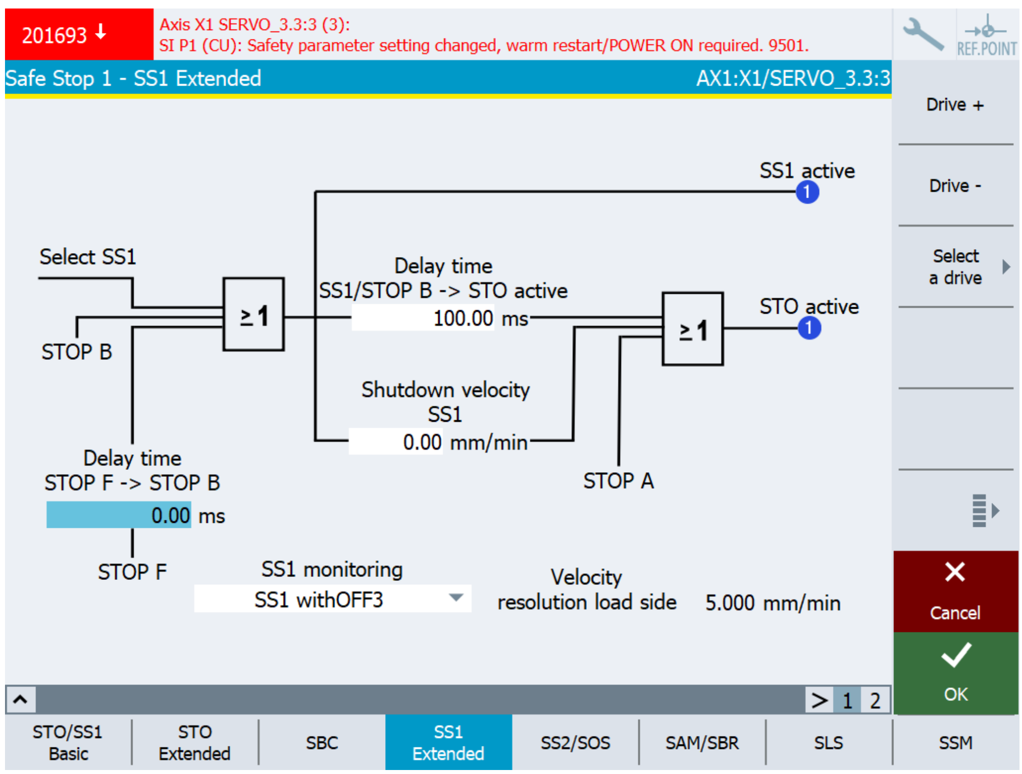


Figure 7-33 Safe Stop 1 - SS1 Extended

Status information

Status	Meaning
SS1 active r9722.1	Status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1.
STO active r9722.0	
Velocity resolution Load side r9732[0]	Displays the safe velocity resolution (load side). Velocity limits that are specified - or parameter changes for velocities below this threshold - have no effect.

Settings

Setting	Meaning
Delay time STOP F -> STOP B p9555	Sets the transition time from STOP F to STOP B The set time is internally rounded off to an integer multiple of the monitoring clock cycle.
SS1 monitoring p9507.3=0	Selects the stop response, which is initiated when selecting function SS1 or activating a STOP B. • SS1 with OFF3 SS1 with OFF3 braking response integrated in the drive • SS1E external stop Stop to be externally initiated. Braking monitoring (SBR, SAM) is deactivated.
Delay time SS1/STOP B -> STO active p9556	Sets the delay time for STOP A to STOP B. The set time is internally rounded off to an integer multiple of the monitoring clock cycle.
Shutdown speed SS1 p9560 (only for SS1 with OFF3)	Sets the shutdown velocity for activating STO. "Standstill" is assumed below this velocity, and for STOP B / SS1, an STO is selected. In the case of encoderless motion monitoring functions, this parameter must be > 0 (10 is recommended). Note: The shutdown velocity has no effect for a value = 0.

7.7.6 SS2/SOS

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display "Safe Stop 2 - Safe Operating Stop - SS2/SOS" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SS2/SOS

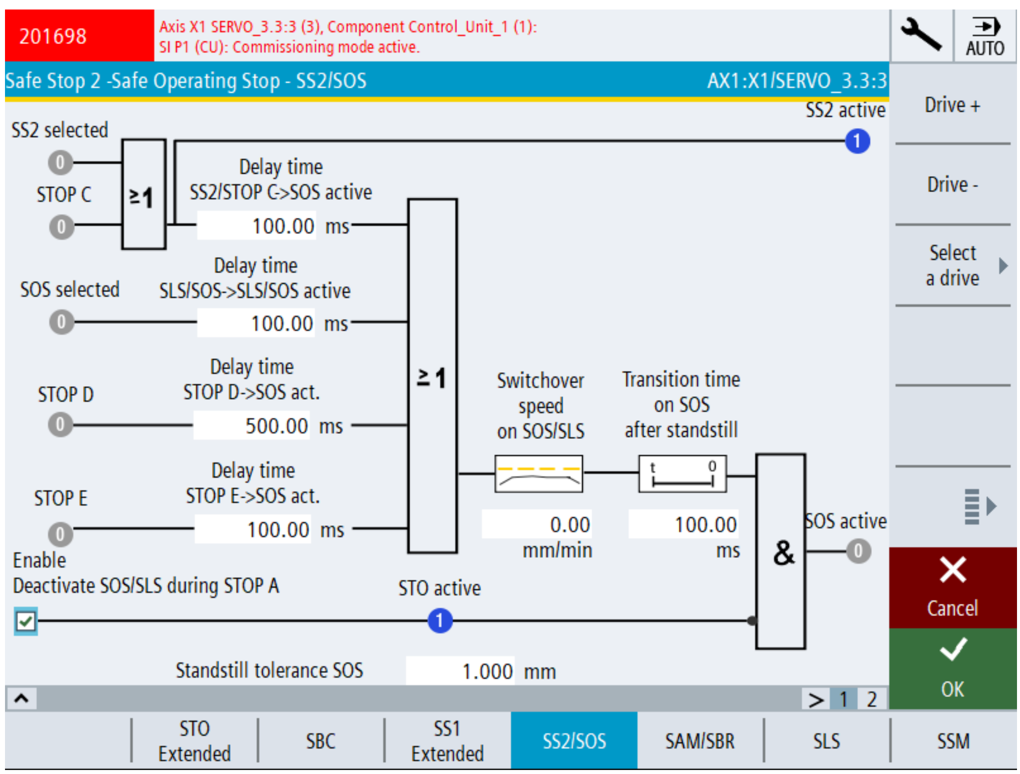


Figure 7-34 Safe Stop 2 - safe operating stop - SS2/SOS

Status information

Status	Meaning
SS2 active r9722.2	Status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1.
SOS active r9722.3	

Settings

Setting	Meaning
Delay time for SS2/STOP C -> SOS active p9552	Sets the transition time from STOP C to "Safe Operating Stop" (SOS).
Delay time, SLS/SOS - SLS/SOS active p9551	Sets the delay time for the SLS changeover and for the activation of SOS for the functions "Safely-Limited Speed" (SLS) and "Safe Operating Stop" (SOS). When transitioning from a higher to a lower Safely-Limited Speed stage and when activating a Safe Operating Stop (SOS), the "old" speed stage remains active for this delay time. A delay is also occurred when activating SLS from the "SOS and SLS inactive" state - and when activating SOS from the "SOS inactive" state.
Delay time, STOP D -> SOS active p9553	Sets the transition time from STOP D to "Safe Operating Stop" (SOS)
Delay time, STOP E -> SOS active p9554	Sets the transition time from STOP E to "Safe Operating Stop" (SOS)
Switchover speed to SOS/SLS p9567	Sets the switchover speed to SOS/SLS in mm/min.
Transition time to SOS after standstill p9569	Sets the transition time to SOS after standstill in ms.
Enable deactivation SOS/SLS during an external STOP A p9501.23	Using the checkbox, "Enable deactivation SOS/SLS during an external STOP A" can be activated.
Standstill tolerance SOS p9530	Sets the tolerance for the "Safe operating stop" function (SOS).

7.7.7 SAM

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display "Safe Acceleration Monitoring - SAM" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SAM/SBR

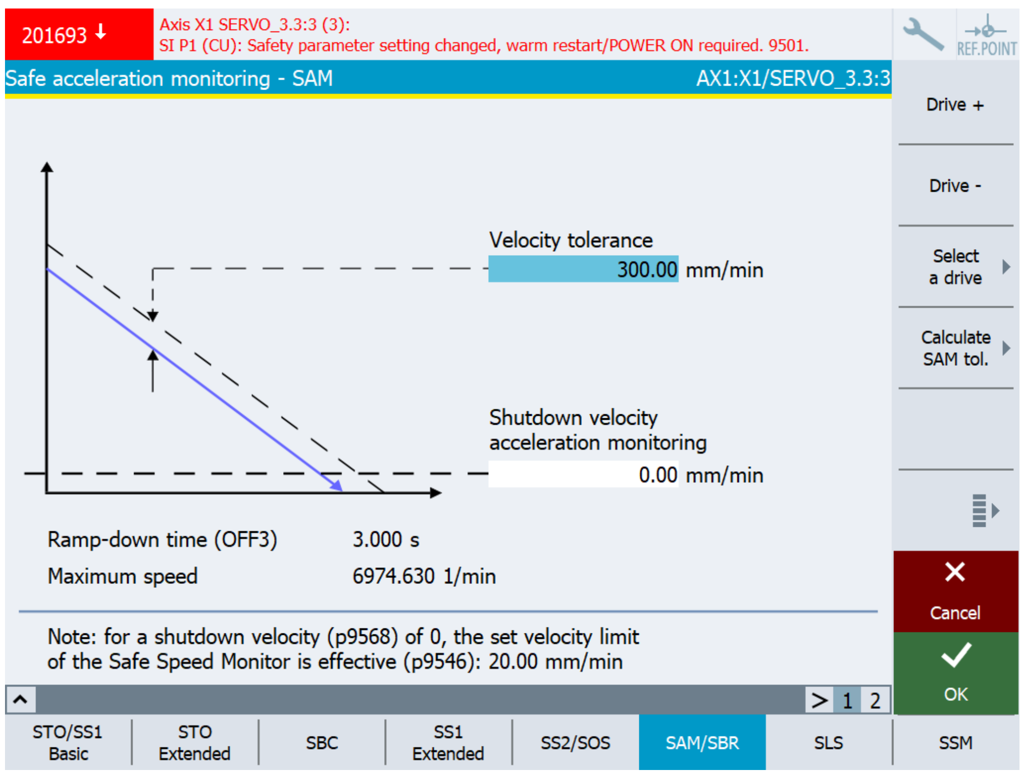


Figure 7-35 Safe acceleration monitoring - SAM

Settings

Setting	Meaning
Velocity tolerance p9548	During the down ramp, the converter continually adds the speed tolerance to the actual speed. The converter reduces the monitoring threshold until the "Shutdown speed" has been reached. • If the speed temporarily increases, the monitoring threshold remains at the last value. • If the drive accelerates by the velocity tolerance, then SAM identifies this, and a STOP A is initiated. **Calculation** • The following applies when parameterizing the SAM tolerance: – The maximum speed increase after SS1 or SS2 is triggered results from the effective acceleration (a) and the duration of the acceleration phase. – The duration of the acceleration phase is equivalent to one monitoring clock cycle (delay from detecting an SS1/SS2 until $n_{set} = 0$): • Calculating the velocity tolerance: Actual speed for SAM = acceleration × acceleration duration The following setting rule is obtained: – For linear axes: SAM tolerance [mm/min] = a [m/s²] x MC [s] x 1000 [mm/m] x 60 [s/min] – For rotary axes: SAM tolerance [rpm] = a [rev/s²] x MC [s] x 60 [s/min] • Recommendation The SAM tolerance value entered should be approx. 20 % higher than the calculated value. • With the tolerance, the "overshoot", which is automatically obtained when reaching standstill when braking along the OFF3 ramp, must be tolerated. However, it cannot be calculated as to just how high this is.
Shutdown speed acceleration monitoring p9568	Sets the speed limit for the "SAM" and "SBR" functions. SAM is deactivated once the set velocity limit has been fallen below. SBR is deactivated if the safe braking ramp falls below the set speed limit.
Ramp-down time (OFF3) p1135[0]	Sets the ramp down time from the maximum velocity or maximum speed to standstill for the OFF3 command. This time can be exceeded if the maximum the DC link voltage is reached.
Maximum velocity or maximum speed (linear axis or rotary axis/spindle) p1082[0]	Sets the highest possible velocity or speed.

7.7.8 SBR

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- Safety function SS1 with stop response OFF3 is configured for the drive.

Displaying the "Safe brake ramp - SBR" startup screen form

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SAM/SBR

Figure 7-36 Safe Brake Ramp - SBR

Settings

Setting	Meaning
Delay time p9582	Set the delay time for monitoring the braking ramp. Time that lapses after initiating SS1, selecting SLS or SLS level changeover and the start of brake ramp monitoring. The delay time has a minimum value of 2 safety monitoring clock cycles. (if the parameterized delay time is less than 2 safety monitoring clock cycles, then internally, a delay time of 2x monitoring clock cycles is used.)
Monitoring time p9583	Sets the monitoring time to determine the braking ramp. The gradient of the braking ramp depends on the reference velocity (reference value) and the monitoring time.
Reference velocity p9581	Sets the reference value to determine the braking ramp. The gradient of the braking ramp depends on the reference velocity (reference value) and the monitoring time.
Ramp-down time (OFF3) p1135[0]	Sets the ramp down time from the maximum velocity or maximum speed to standstill for the OFF3 command. This time can be exceeded if the maximum the DC link voltage is reached.
Maximum velocity or maximum speed (linear axis or rotary axis/spindle) p1082[0]	Sets the highest possible velocity or speed.

7.7.9 SLS

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Note

Transferring process data for SLS in PROFIsafe telegrams

PROFIsafe telegram 901, 902 or 903 can be used to transfer process data. The default setting is telegram 903.

Display "Safely-Limited Speed - SLS" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SLS

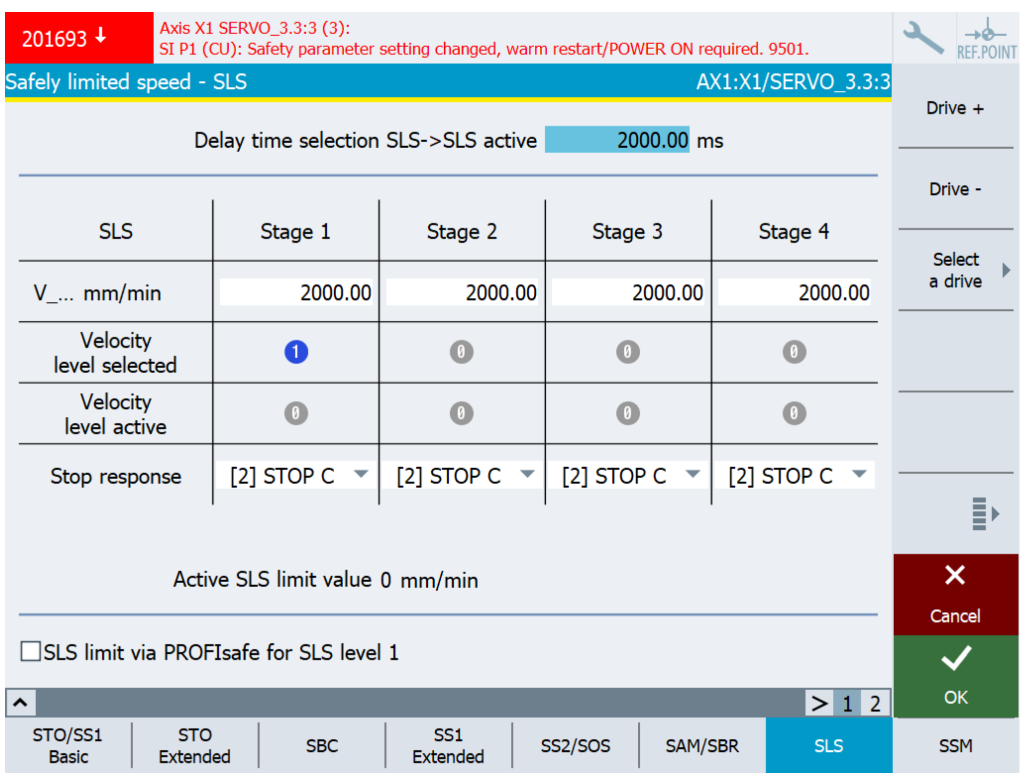


Figure 7-37 Safely-Limited Speed - SLS

Status information

Status	Meaning
Velocity level selected Level 1: r9720.9=0 and r9720.10=0 Level 2: r9720.9=1 and r9720.10=0 Level 3: r9720.9=0 and r9720.10=1 Level 4: r9720.9=1 and r9720.10=1	Indicates which parameterized velocity level is currently selected.
Velocity level active Level 1: r9722.9=0 and r9722.10=0 Level 2: r9722.9=1 and r9722.10=0 Level 3: r9722.9=0 and r9722.10=1 Level 4: r9722.9=1 and r9722.10=1	If one of the velocity levels is currently active, then this is displayed in the corresponding column.
Active SLS limit value r9714.0	Displays the load-side velocity actual value of the CU. The display is updated in the safety monitoring cycle clock.

Settings

Setting	Meaning
Delay time when selecting SLS -> SLS active p9551	Sets the delay time for SLS switchover. This delay time is active in the following cases: • Selecting SLS: Monitoring only becomes active after the configurable delay time has elapsed. Within this time, the actual velocity must be below the (selected) limit. • This delay time is also incurred when activating SLS from the "SOS and SLS in active" state. • Reducing the 1st limit value via PROFIsafe - or switching over to a lower maximum velocity level: The actual velocity of the drive must have dropped below the new limit within the delay time. The existing limit remains active during the delay time. The lower limit value becomes active after the delay time has expired. The delay time is not active in the following cases: • Deselecting SLS • Switching over to a higher limit value: The higher limit value immediately becomes active. In operation, the parameterized delay time cannot be changed. If you require various delay times in your application, then you must realize this using a time-delayed transfer of the SLS limit value using the F-PLC.
Maximum velocity (V_max) level 1 p9531[0]	Up to 4 parameterizable SLS velocity limit values must be specified based on the results of the risk analysis. Also when SLS is activated, these limit values can be toggled between. Depending on the particular situation, the "Delay time, select SLS -> SLS active" acts for switchover (see above). Switchover between these 4 values The value of a selected maximum speed stage 1 is transferred via PROFIsafe if the "SLS limit via PROFIsafe for SLS level 1" checkbox is activated.
Maximum velocity (V_max) level 2 p9531[1]	
Maximum velocity (V_max) level 3 p9531[2]	
Maximum velocity (V_max) level 4 p9531[3]	

Setting	Meaning
Stop response level 1 p9563[0]	Sets the specific stop response for the appropriate maximum velocity level: • STOP A • STOP B • STOP C • STOP D • STOP E • STOP A with delayed STO when the bus fails • STOP B with delayed STO when the bus fails • STOP C with delayed STO when the bus fails • STOP D with delayed STO when the bus fails • STOP E with delayed STO when the bus fails Using the settings without delayed STO, when the bus fails, protection for persons can be implemented - with delayed STO, when the bus fails, protection for machinery can be implemented. Here, in a wider sense, bus failure should be understood as a communication error relating to the signals that are used to control the safety functions (e.g. via PROFIsafe).
Stop response level 2 p9563[1]	
Stop response level 3 p9563[2]	
Stop response level 4 p9563[3]	
SLS limit value via PROFIsafe for SLS level 1	Setting to transfer the maximum velocity level 1 via PROFIsafe. The transfer of maximum speed level 1 via PROFIsafe can also be used to parameterize (fixed) maximum speed levels 2, 3 and 4. When activated, the value is transferred using PROFIsafe in control word S_SLS_LIMIT_A (Page 410), assuming that level 1 is currently selected. S_SLS_LIMIT_A has the value range 1 ... 32767; where the following applies: • 32767 ≙ 100 % of the 1st SLS level • The actually monitored limit value is calculated as follows: SLS limit value = (S_SLS_LIMIT_A/32767) × "maximum speed level 1" If an incorrect SLS limit value is transferred, then the converter responds with the parameterized "Stop response level 1".

7.7.10 SSM

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with Extended Functions.

Display "Safe Speed Monitoring - SSM" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SSM

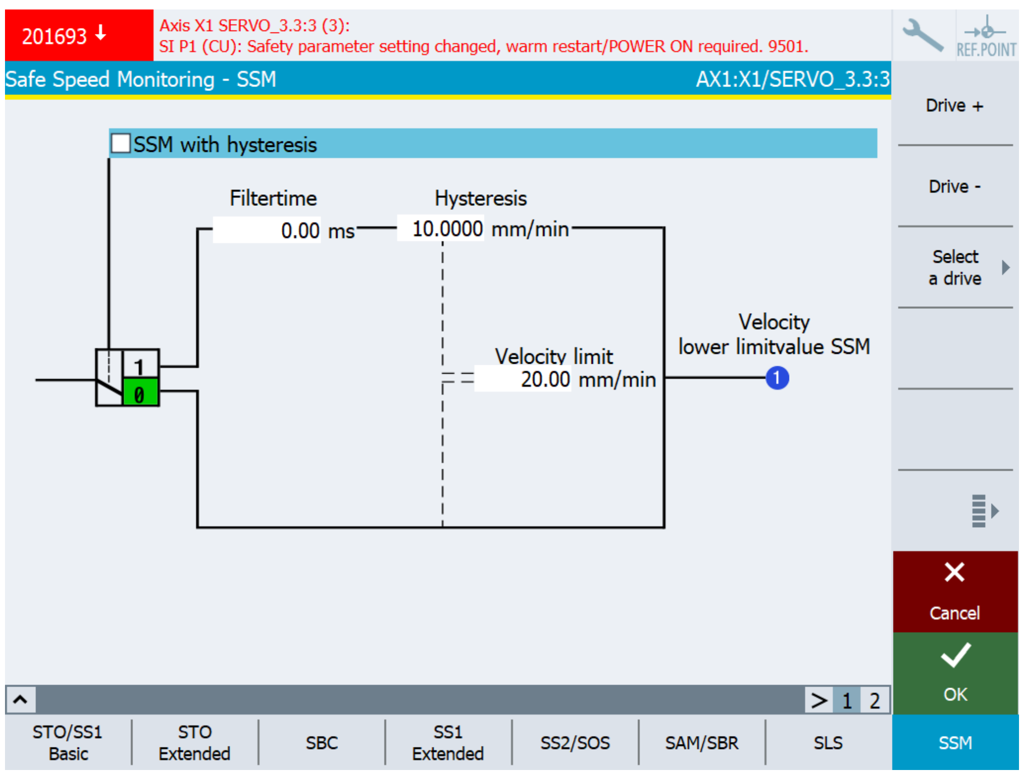


Figure 7-38 Safe Speed Monitor - SSM

Status information

Status	Meaning
Switching element (SSM with hysteresis) p9501.16	Indicates whether the "Hysteresis" and "Filter time" functions are active.
Speed below SSM limit value r9722.15	Indicates whether the current velocity is below the parameterized velocity limit.

Settings

Setting	Meaning
SSM with hysteresis p9501.16	Activates the "Hysteresis" and "Filter time" functions for SSM. If the "SSM with hysteresis" function is enabled, the SSM function is evaluated as an active monitoring function, and after a STOP F, also results in a subsequent STOP B / STOP A response.
Filter time p9545	Sets a filter time (PT1 filter) to smooth the output signal for SSM. As filtering characteristic, for output signal SSM, a time-delayed SSM feedback signal occurs for the axes.
Hysteresis p9547	Parameterizing hysteresis for SSM In this way, a more stable SSM signal characteristic can be achieved at velocities close to the "Velocity limit" (monitoring threshold). The velocity (or speed) determined by both channels may differ as a maximum by the difference between "Velocity/speed limit" and "Hysteresis". Otherwise, it would be theoretically possible that for SSM one channel returns a HIGH signal and the other a LOW signal. Take into account the following rule when parameterizing: • Hysteresis p9547 ≤ 0.75 · velocity limit p9546 If actual value synchronization is enabled (Settings - encoder parameterization (Page 272)), then you must also comply with the following rule: • "SI Motion slip speed tolerance" (p9549) ≤ hysteresis
Speed limit p9546	Sets the velocity limit for the SSM feedback signal to detect standstill (n < nx). If the velocity limit is fallen below, then the signal "Safe Speed Monitor feedback signal active" (SGA n < n_x) is set. The abbreviation SGA n < nx stands for the safety function required for determining an output signal when a parameterizable velocity limit has been undershot. This value is also active for safety function SAM as "Shutdown velocity acceleration monitoring" - assuming that this shutdown velocity is parameterized with "0". In this case, the effects of Safe Acceleration Monitoring are therefore restricted if a relatively high SSM velocity limit is set when using the SS1 and SS2 stop functions.
Feedback signal SSM active for pulse inhibit (only in encoderless operation) p9509.0	Sets the response during pulse cancellation in encoderless operation. For Safe Speed Monitor without encoder, after pulse cancellation the drive is unable to determine the current velocity. 2 responses can be selected for this operating state: • The status signal (SSM feedback signal) indicates "0" (factory setting). • The status signal (SSM feedback signal) is frozen. "Safe Torque Off" (STO) is selected internally. See also: Signal characteristic for setting "Feedback signal SSM for pulse inhibit " (Page 159)

7.7.11 SDI

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with Extended Functions.

Display "Safe Direction - SDI" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > SDI

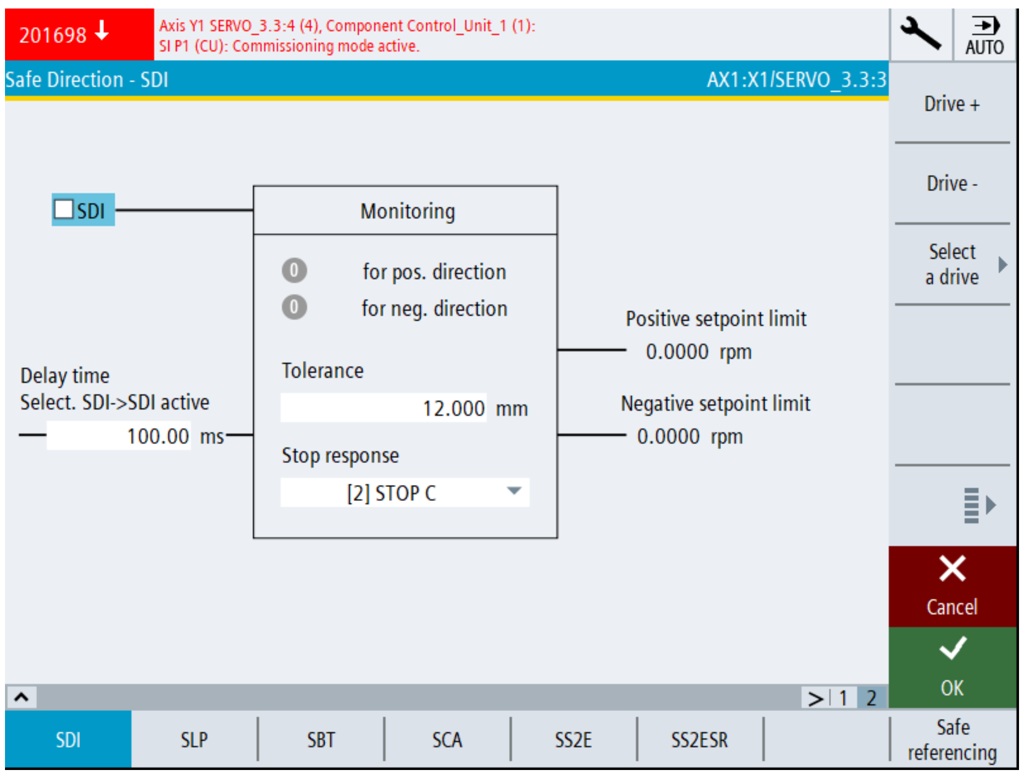


Figure 7-39 Safe Direction - SDI

Status information

Status	Meaning
for positive direction r9722.12	Status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1.
for negative direction r9722.13	

Settings

Setting	Meaning
SDI p9501.17	Activating/deactivating (enable) SDI.
Delay time, selection SDI -> SDI active p9565	Sets the delay time. After selecting function SDI, motion in the monitored direction is permissible, as a maximum for this time. Therefore, this time can be used to brake active motion.
Tolerance p9564	Sets the tolerance. This motion is still permissible in the monitored direction before safety message C01716 is initiated.
Stop response p9566	Sets the stop response. This setting applies to both directions of motion. • [0] STOP A • [1] STOP B • [2] STOP C • [3] STOP D • [4] STOP E • [10] STOP A with delayed stop response when the bus fails • [11] STOP B with delayed stop response when the bus fails • [12] STOP C with delayed stop response when the bus fails • [13] STOP D with delayed stop response when the bus fails • [14] STOP E with delayed stop response when the bus fails In encoderless operation, only settings "[0] STOP A" and "[1] STOP B" can be selected.
SDI active feedback for pulse inhibit p9509.8 (only in encoderless operation)	Activates/deactivates SDI during pulse cancellation in encoderless operation.

7.7.12 SLP/SP

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.
- Telegram 902 (using SLP/SP) or telegram 903 (using only SLP) is set
- Actual value synchronization is not enabled (p9501.3 = 0).

Display "Safe Limit Positions - Safe Position - SLP/SP" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > SLP/SP

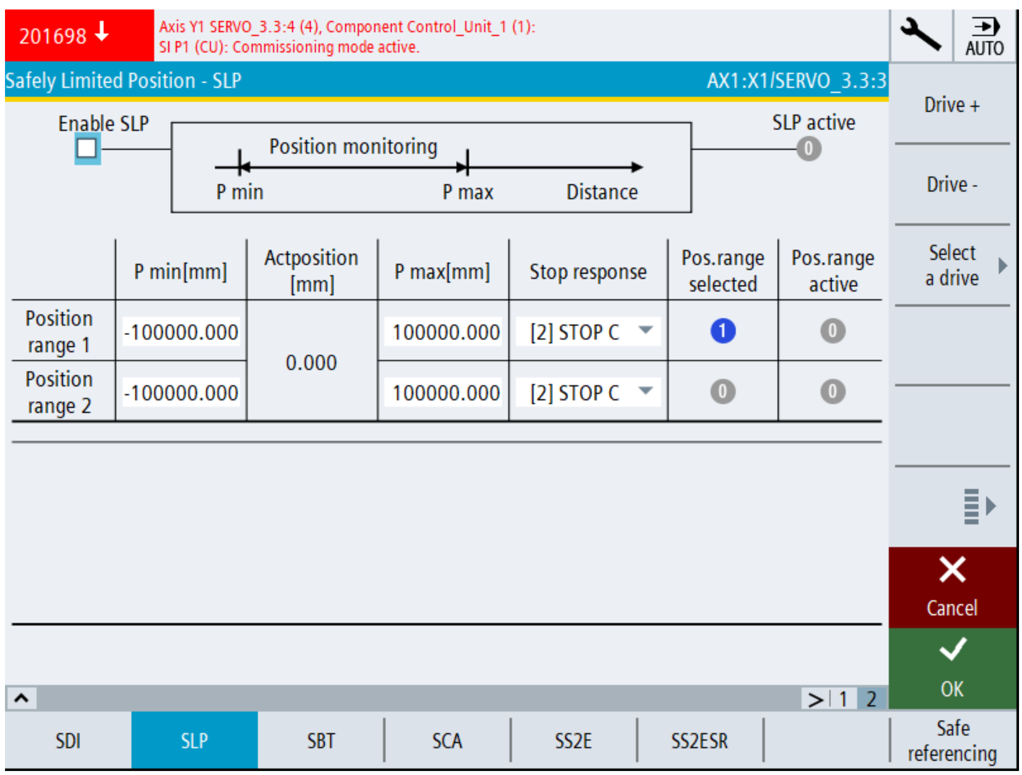


Figure 7-40 Example of the "SLP" commissioning screen, i.e. with telegram 903 set

Status information

Status	Meaning
Positioning range selected Range 1: r9720.19=0 & r9720.6=0 Range 2: r9720.19=1 & r9720.6=0	Displays whether positioning range 1 or 2 is currently selected.
Positioning range active Range 1: r9722.19=0 & r9722.6=1 Range 2: r9722.19=1 & r9722.6=1	Displays whether positioning range 1 or 2 is currently active.
Actual position value r9708[4] (only PROFIsafe)	Displays the actual load-side actual value via PROFIsafe.
Safety-related position valid r9722.22	Status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1. SP valid
Safety reference position confirmed r9727	Displays the internal status of the user agreement
Drive reference. r9723.17	Display: Position referenced
Safely ref. r9722.23	Display: SP valid

Settings

Setting	Meaning
SLP p9501.1	Enable/inhibit SLP.
P min [mm] Range 1: p9535[0] Range 2: p9535[1]	Sets the lower and upper limit values for position range 1 or 2 of the SLP function. For the setting, these limit values apply: • P max > P min • The limit values must lie in the valid traversing range (-737280 ... 737280). See also: C01715
P min [mm] Range 1: p9534[0] Range 2: p9534[1]	

Setting	Meaning
Stop response Range 1: p9562[0] Range 2: p9562[1]	Sets the stop response for position range 1 or 2 of the SLP function. • [0] STOP A • [1] STOP B • [2] STOP C • [3] STOP D • [4] STOP E • [10] STOP A with delayed stop response when the bus fails • [11] STOP B with delayed stop response when the bus fails • [12] STOP C with delayed stop response when the bus fails • [13] STOP D with delayed stop response when the bus fails • [14] STOP E with delayed stop response when the bus fails
Safe position p9501.25 (only for telegram 902) (only for PROFIsafe)	Enables/inhibits the transfer of the safe position via PROFIsafe
Safe absolute position p9501.27 (only for telegram 902) (only for PROFIsafe)	Enables/inhibits the safe absolute position.
SP scaling p9574 (only for telegram 902) (only for PROFIsafe)	Sets the scaling factor to transfer the safe position via PROFIsafe in the 16-bit format. The parameter is only active when PROFIsafe telegram 901 is selected, see S_XIST16: Current actual position value (16 bits) (Page 411). Scaling is realized by dividing the 32-bit position actual value r9713[0] with this scaling factor. If, during operation, a position actual value is determined that cannot be scaled, then this results in message C0711 with value 7001 - as well as STOP F.

7.7.13 SBT

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with Extended Functions.

Display "Safe Brake Test - SBT" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > SBT

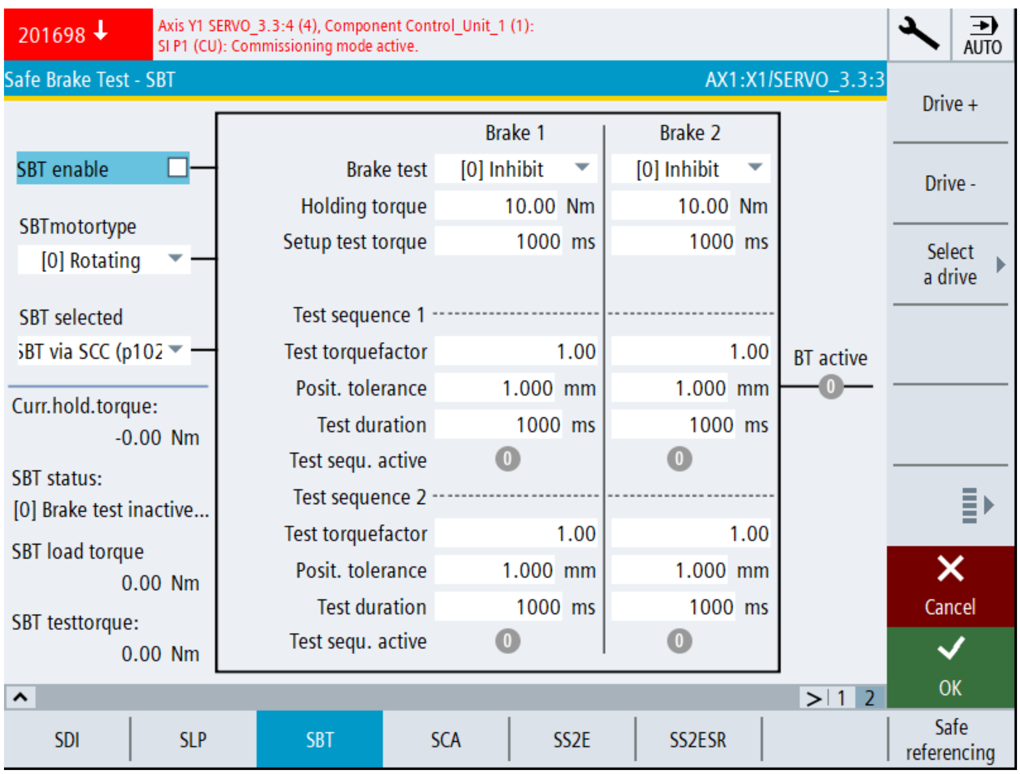


Figure 7-41 Safe Brake Test - SBT

Note

Additional commissioning support

The following SINUMERIK Operate screen forms are available to commission SBT:

- "Graphic" softkey: Displays a torque-time diagram or a force-time diagram
- "Trace" softkey: Starts a drive trace session with various options.

Status information

Status	Meaning
Actual holding torque or force r0080	Displays the torque actual value or force actual value (unsmoothed).
SBT state r10242	Displays the current status of the Safe Brake Test.
SBT load torque or force r10241	Displays the load torque or the load force for the Safe Brake Test. This load torque or this load force is available at the drive when initializing the brake test. The displayed value is kept until the brake test is deselected.
SBT test torque or force r10240	Displays the maximum test force or the maximum test torque available on the motor side. The displayed value remains until the start of the next test sequence.

Settings

Setting	Meaning
SBT enable p10201.0	Enables/inhibits SBT.
SBT motor type p10204	Selects the motor type for the Safe Brake Test. • 0: Rotary • 1: Linear
SBT selection p10203	Selects the control type • 0: SBT via SCC (p10235) • 1: SBT via BICO (p10230) • 2: SBT for test stop selection (p9705/p10250.8) For integrated drives (CU_I, CU_NX), only "SBT via SCC" is permissible.
Brake test Brake 1: p10202[0] Brake 2: p10202[1]	Selects the brakes to be tested. • 0: Inhibit • 1: Test motor holding brake • 2: Test external brake It is not possible to test two motor holding brakes.
Actual holding torque or force Brake 1: p10209[0] Brake 2: p10209[1]	Sets the effective holding torque or holding force of the brakes to be tested on the motor side.
Establish the test torque or test force Brake 1: p10208[0] Brake 2: p10208[1]	Sets the time during which the test torque or the test force is ramped up against the closed brake. After the Safe Brake Test, the test torque or the test force is ramped-down again.
Test torque factor or test force factor Test sequence 1, brake 1: p10210[0] Test sequence 1, brake 2: p10210[1] Test sequence 2, brake 1: p10220[0] Test sequence 2, brake 2: p10220[1]	Sets the factor for the test torque or the test force of test sequence 1 or 2 for the Safe Brake Test. The factor is referred to the brake holding torque or the brake holding force (see above, p10209).

Setting	Meaning
Position tolerance Test sequence 1, brake 1: p10212[0] Test sequence 1, brake 2: p10212[1] Test sequence 2, brake 1: p10222[0] Test sequence 2, brake 2: p10222[1]	Sets the tolerated position deviation for test sequence 1 or 2 for the Safe Brake Test.
Test duration Test sequence 1, brake 1: p10211[0] Test sequence 1, brake 2: p10211[1] Test sequence 2, brake 1: p10221[0] Test sequence 2, brake 2: p10221[1]	Sets the test duration for test sequence 1 or 2 for the Safe Brake Test. The test torque or the test force is applied to the closed brake for this time.

Note

Using MD36968.2 to select the parameter assignment behavior at the end of SBT

You can parameterize the positioning behavior after the brake test via the expert list using MD36968.2 $MA_SAFE_BRAKETEST_CONTROL, bit 2:

- 0: Positioning at the actual axis position
  To conclude the brake test, the actual axis position for the next path motion is used. (MD36968 $MA_SAFE_BRAKETEST_CONTROL bit 2 = 0). This results in motion to the last programmed axis position on the path.
- 1: Positioning to the last programmed axis position
  Acceptance of the actual axis position is not carried out. After the axis has been pressed against the brake, the closed-loop position controller withdraws the axis to the last programmed position.
  Vertical axes can thus be prevented from sagging as a result of a repeated brake test. It is also possible to briefly exceed the software limit switch while pressing against the brake without initiating an alarm.

7.7.14 SCA

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display "SI Safe Cams" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > SCA

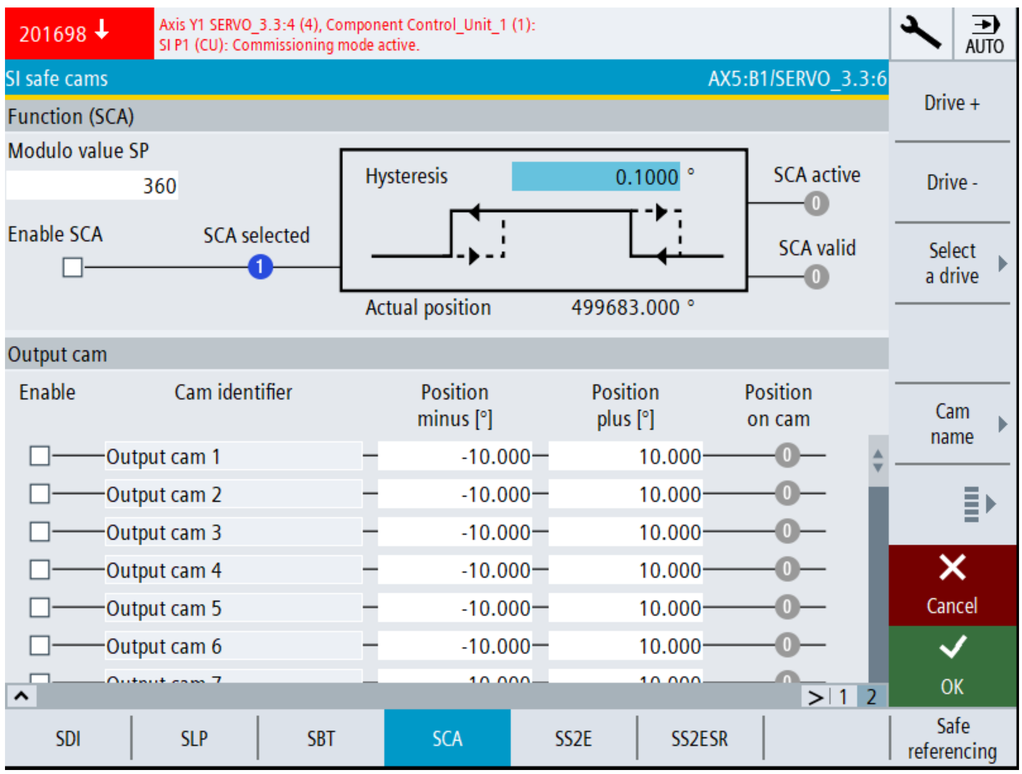


Figure 7-42 SI safe cams

Status information

Status	Meaning
SCA selected r9720.23	SI Motion control signals integrated in the drive: Deselect SCA
SCA active r9703.30	SI Motion SCA status signal (Control Unit)

Status	Meaning
SCA valid r9703.31	SI Motion SCA status signal (Control Unit)
Position at cam r9703.0	SI Motion SCA status signal (Control Unit)

Settings

Setting	Meaning
Modulo value SP p9505	Sets the modulo value in degrees for rotary axes for the "Safe position" function. This modulo value is taken into account for safe referencing and for the transfer of the safe position via PROFIsafe when absolute position is enabled.
Enable SCA	Inhibits or enables the SCA function throughout.
Hysteresis	Specifies the hysteresis value.
<Inhibit or enable> 9503.0 ... 29	Inhibits/enable individual Safe Cams of the SCA function.
<Cam identifier>	Displays the cam identifier. Default setting, "Cam 1" ... "Cam 30". The cam identifiers are defined in the associated TS files depending on the language, and can be freely defined by copying and adapting the files: • Template for the TS file: /card/siemens/sinumerik/hmi/template/lng/oem_scam_names_deu.ts • Archive path for user-defined TS file: /card/oem/sinumerik/hmi/lng/oem_scam_names_<Sprachkennung>.ts
Minus cam position p9537[0...29]	Sets the minus cam position in ° or mm.
Plus cam position p9536[0...29]	Sets the plus cam position in ° or mm.

7.7.15 SS2E

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display commissioning screen "Safe Stop 2 with external stop - SS2E"

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > SS2E

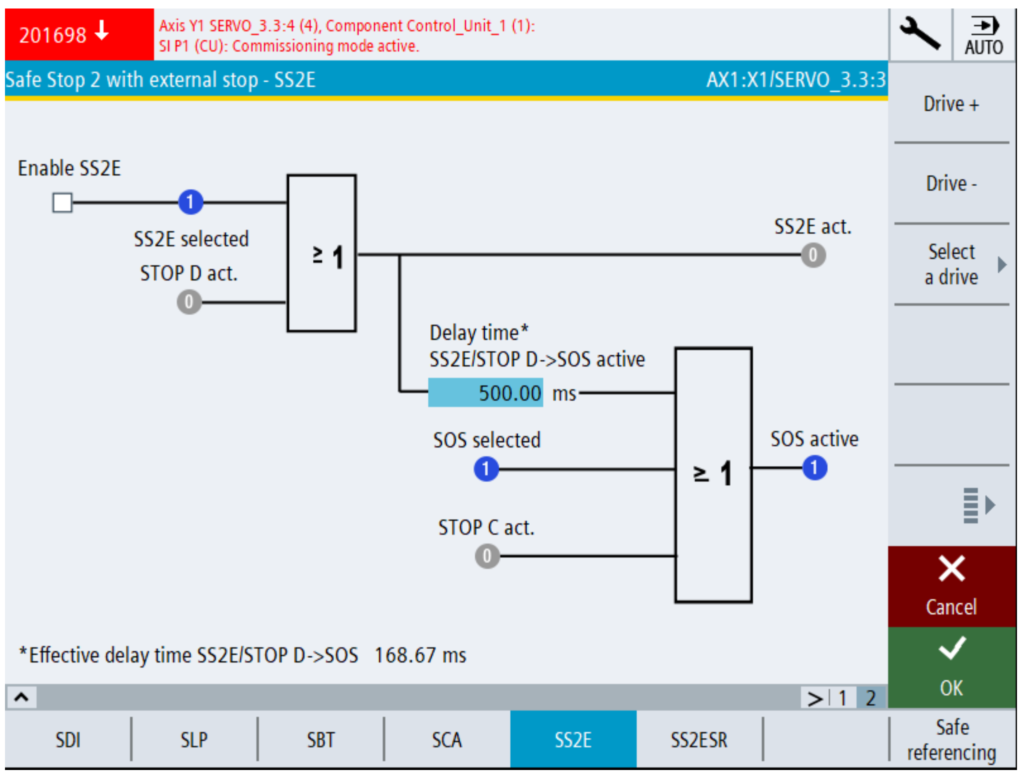


Figure 7-43 Safe Stop 2 with external stop - SS2E

Status information

Status	Meaning
Status control signals:	Status - control and status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1.
Select SS2E r9720.28	
Select SOS r9720.3	
Status signals:	
SS2E active r9722.28	
SOS active r9722.3	
STOP C active r9721.13	
STOP D active r9721.14	

Settings

Setting	Meaning
Enable SS2E p9501.18	SS2E enable is activated via the parameter.
Delay time, STOP D -> SOS active p9553	Sets the transition time from STOP D to "Safe Operating Stop" (SOS) in ms.

7.7.16 SS2ESR

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

Display commissioning screen "Safe Stop 2 Extended Stop and Retract (SS2ESR)"

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > SS2ESR

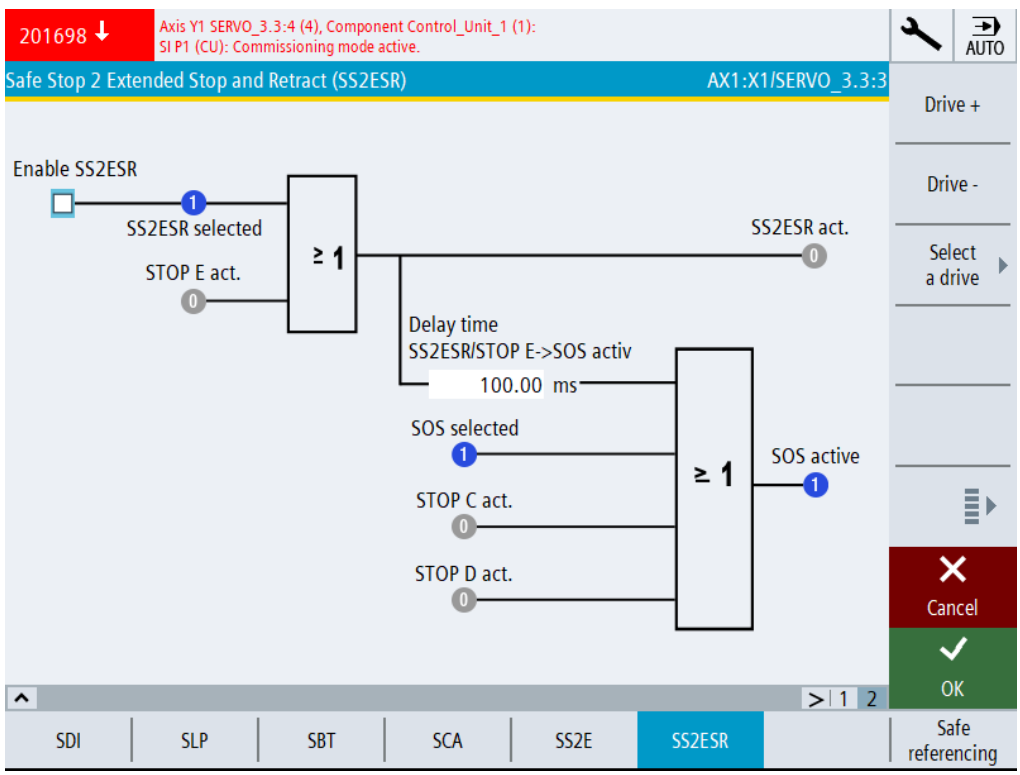


Figure 7-44 Safe Stop2 Extended Stop and Retract (SS2ESR)

Status information

Status	Meaning
Status control signals:	Status - control and status signals for the safety motion monitoring functions integrated in the drive on monitoring channel 1.
Select SS2ESR r9720.29	
Select SOS r9720.3	
Status signals:	
SS2ESR active r9722.27	
STOP E active r9721.15	
STOP C active r9721.13	
STOP D active r9721.14	

Settings

Setting	Meaning
Enable SS2ESR p9501.04	SS2ESR enable is activated via the parameter.
Delay time SS2ESR/STOP E -> SOS active p9554	Sets the transition time from STOP D to "Safe Operating Stop" (SOS) in ms.

7.7.17 Safe referencing

Requirements

- The Safety Integrated commissioning mode (Page 266) is active for the drive to be configured.
- Access rights of access level 2 (service) are available in SINUMERIK Operate.
- The drive is configured for operation with an encoder and Extended Functions.

Display "Safe referencing" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > Menu forward key > Safe referencing

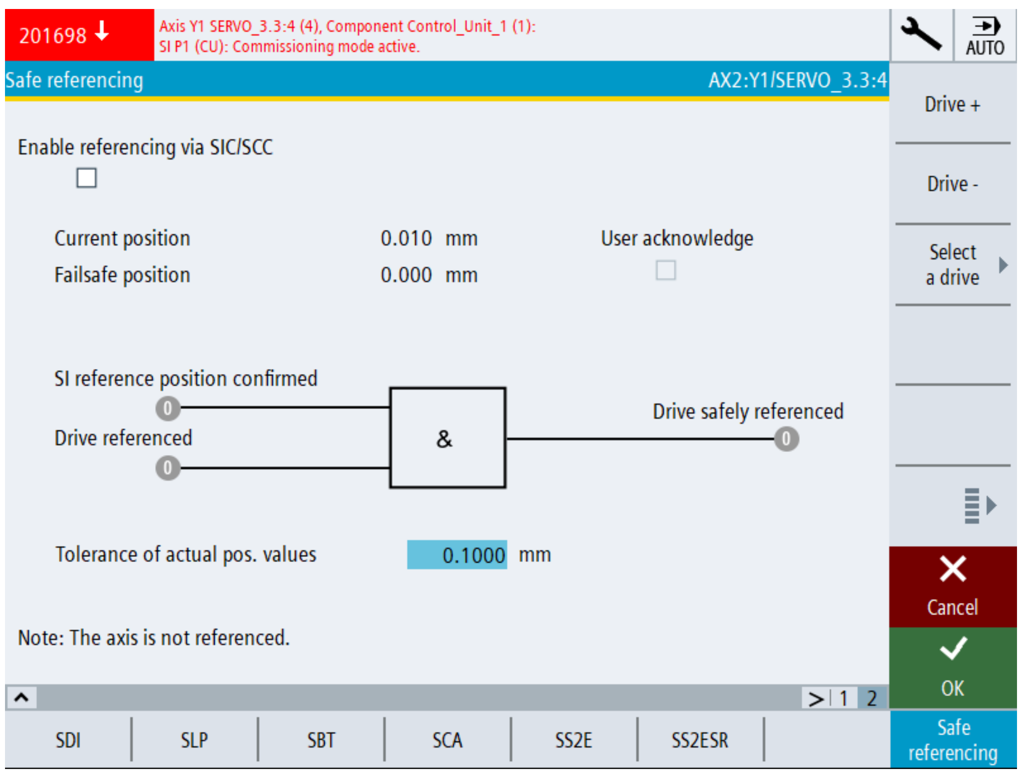


Figure 7-45 Safe referencing

Status information

Status	Meaning
Safety reference position confirmed r9727	Displays the internal status of the user agreement
Drive reference. r9723.17	Display: Position referenced
Safely ref. r9722.23	Display: Safely referenced

Settings

Setting	Meaning
Enable referencing via SCC p9501.27	Sets the enable signals for the safety-related motion monitoring functions.
SI Motion, user agreement, select/deselect p9726	User agreement Safe Position (is only displayed if functions with Safe Position evaluation are activated)
Tolerance of the position actual values (referencing) p9544	Sets the tolerance for checking the actual values. For an incremental encoder, the actual values are checked after referencing, for an absolute encoder, when switching on.

7.7.18 Further safety functions

In addition to the described safety functions that are configured using commissioning screens, the following drive-integrated safety functions can be configured in the expert list, that is, by directly entering the parameters:

- SS2e - SS2 with external stop (Page 131)
- Homing via SIC/SCC (Page 204)
- Cancellation of the stop transition times
- Automatic SLS (Page 143)/SOS (Page 139) deselection when STO active

7.8 Finalizing commissioning

7.8.1 Confirming settings

After parameterization, the Safety Integrated commissioning mode must be deactivated and the actual checksums must be transferred into the reference checksums.

Requirements

- The NC and drive-specific settings have been correctly configured for all safety-related drives and for all F-I/O devices.
- The safety functions integrated in the drive are configured.
- The safety commissioning mode is activated (Page 266).

Procedure

Proceed as follows to confirm the drive-specific safety settings that have been made:

1. In SINUMERIK Operate, switch to "MENU SELECT > Commissioning > Menu forward key > Safety".
2. Using the menu forward key, switch to the 2nd Level of the vertical softkey bar.
3. Press softkey "Copy SI data" and confirm with "OK".
   The safety settings are copied from the 1st into the 2nd monitoring channel.
4. Press softkey "Confirm SI data" and confirm with "OK".
5. Press softkey "Save all drive objects" and confirm with "OK".

7.8.2 Assigning a Safety Integrated password

In SINUMERIK Operate, commissioning data is generally stored in various access levels. You protect the safety-related drive parameterization additionally with the Safety Integrated password. This password is stored in the drive data so that it can be changed only by authorized persons who know the password.

Note

SINAMICS Safety password must be used for SINUMERIK Safety

You can assign the SINAMICS safety password via the SINUMERIK Operate screen form (access level "Manufacturer"). SINUMERIK Operate automatically sets the assigned SINAMICS safety password for all axes/drives as soon as you select "Safety" in the Commissioning operating area. The precondition to do this is an active "Service" or "Manufacturer" access level.

Alternatively, assign the password as follows via the expert list as in SINAMICS Safety:

- p0010 = 95 Commissioning mode
- p9761 = enter "Old safety password". Default setting for p9761 = 0.
- p9762 = enter "new password".
- p9763 = confirm "new password"
- p0977 = 1; "Copy from RAM to ROM"

The new and confirmed safety password is valid immediately.

Procedure

To assign the Safety Integrated password for all axes/drives, proceed as follows:

1. IN SINUMERIK Operate, go to "MENU SELECT > Commissioning > Menu forward key > Safety".
2. Select softkey "SI password".
3. Select the check box for the all "axes/drives".
4. Assign a password and confirm by clicking on "OK".

7.9 Series commissioning

A loaded project that has been commissioned can be loaded to another SINUMERIK control system, while still keeping the safety parameterization. However, observe the following information:

- Different component checksums as a result of series commissioning with Safety Integrated functionality (Page 386)
- Safety message for series commissioning with third-party motor (Page 339)

For series commissioning, you must perform an acceptance test (Page 345) for each SINUMERIK control system.

Safety message for series commissioning with third-party motors under Safety Integrated Extended Functions

If third-party motors with absolute encoders are being used, a situation may arise where a Safety message prevents commissioning.
One reason for this may be that a different serial number of the absolute encoder is saved on the memory card than that in the Control Unit which is to be commissioned. The safety message can only be acknowledged once the serial number for the absolute encoder has first been manually corrected. You can then proceed with the commissioning.

7.10 Interaction with other functions

7.10.1 Gantry axes

Note

In a gantry group, you must configure Safety Integrated or SINUMERIK Safety Integrated plus in the leading as well as the following axis.

Otherwise, for a gantry group it is not ensured, that a STOP at the leading axis is automatically transferred to the following axis, for example. The gantry coupling could be opened. As a consequence, an axis would have no monitoring.

Note

STOP A, B, C stop responses

If a stop response is only initiated on one axis in the coupled group (STOP A, B, C), then this is taken into account on all axes of the coupled group, and an n_{set}=0 is initiated. If this results in different axis braking responses, then you can use drive function FASTBRK. If this results in an offset that is not acceptable, then you should configure an SS2E stop response (STOP D).

Note

Braking response when selecting SS1/SS2

If a stop response (SS1, SS2) is simultaneously initiated at several axes, then the braking response of the drives is not synchronized.

Especially for coupled axes, the time offset can result in position differences. To keep position differences low, we recommend that safety clock cycles are parameterized as short as possible.

Alternatively, the use of an SS2 with internal stop (SS2E) as stop request can be tested/checked.

7.10.2 Leading/following axis

For a leading/following axis group, on both axes you must configure Safety Integrated or SINUMERIK Safety Integrated plus, assuming that there is no fixed mechanical coupling.

If a fixed mechanical coupling exists, then you must only configure SINUMERIK Safety Integrated or SINUMERIK Safety Integrated plus in the leading axis.

Based on a risk assessment, the machine manufacturer must evaluate as to whether the fixed mechanical coupling is sufficiently stable, so that it is adequate that Safety Integrated or SINUMERIK Safety Integrated plus is only configured in the leading axis.

7.10.3 Brake tests for axis groups

For a gantry or leading/following axis group, the machinery manufacturer (OEM) must decide on a case-for-case basis whether a defective brake could result in mechanical damage. The brake test should not be performed if mechanical damage could occur.

7.10.4 SERVCOUP special solution

In the SERVO control mode, SERVCOUP allows motors to be operated, which as a result of their size and/or type of construction, cannot be operated from a single SINAMICS power unit. These motors are subdivided into several drive objects, each of which can be operated on a Motor Module, and can be coupled with one another. As a consequence, the individual drive objects can be considered as partial motors with their own winding and terminals.

- When using the SERVO coupling, similar motors must be mechanically coupled very rigidly with one another.
- OA applications (generally) have no influence on Safety Integrated or SINUMERIK Safety Integrated plus.
- For SERVCOUP, for the leading axis, Safety Integrated Extended Functions are used to monitor the drive. The following axes only have Safety Integrated Basic Functions.
- In the case of a leading axis fault, the following axes are stopped via STO. You must implement this as part of your application engineering (see Function Manual SERVCOUP (https://support.industry.siemens.com/cs/ww/en/view/109779937), Chapter "Function Description/SINAMICS Safety Integrated/SINUMERIK Safety Integrated").
- If, for instance, the monitoring speed of the Safely-Limited Speed (SLS) is violated at the leading drive object, then the parameterized safety STOP response is initiated at the leading drive object. The complete drive line-up is then shut down.

7.10.5 Closing the internal motor brake using SCC

In conjunction with the safety monitoring functions and with SCC activated, you can control the internal brake using signal SCC.CW1.CloseBrake (DB3x, ...DBX140.5) "Close internal brake".

Note

BICO interconnection

When upgrading from software release < V6.14, you might have to change the BICO interconnection of p858 to r10251.13.

7.10.6 Limiting the setpoint velocity on the NC side

Fundamentals

The source for calculating the NC-side setpoint velocity limitation is transferred from the safety monitoring function in the drive via the Safety Info Channel (SIC).

The drive enters the active velocity limit value on the motor side in the Safety Info Channel (S_V_LIMIT_B). Drive parameter p2000 is used as reference value. With active SLS monitoring, the NC converts the limit value on the motor side supplied by the drive to the load side, takes into account the NC-side evaluation factor, and passes on the calculated setpoint velocity limitation to the motion control of the NC.

Ensure that the safety parameter assignment in the drive and the standard parameter assignment in the NC match (encoder values, gear stages).

The NC-side evaluation factor for limiting the setpoint velocity is parameterized in MD36933 $MA_SAFE_DES_VELO_LIMIT[...]. This is independent of the SLS setpoint velocity limitation parameterized in drive parameter p9533:

- MD36933 = 0%:
  NC-side influencing of the setpoint limitation inactive.
- MD36933 > 0%:
  NC-side setpoint limitation = drive-side setpoint limitation multiplied by the MD value.

If SLS or SOS monitoring is not selected or if the acceptance test mode is active, "Setpoint velocity limitation inactive" is signaled to the motion control.

If the drive supplies the value "0" as the setpoint velocity limitation, this value is passed on 1:1 to the motion control.

The effective setpoint velocity limitation is made available to the user in the OPI tag safeDesVeloLimit.

Effect of the function in the NC interpolator:

- This function influences both axes and spindles.
- The position control loop should be set so that it does not overshoot. Thus a sudden setpoint change does not cause the SLS monitoring function to respond on the actual value side.

Example: spindle with gear stage change

Gear changing on the drive side changes the motor-side setpoint velocity limit entered by the drive in the SIC. If other gear stages are parameterized in the NC or if another gear stage is active, then the setpoint velocity limit active in the NC changes. This can result in the setpoint velocity limit being greater than the parameterized SLS limit.

This response must be avoided by correctly parameterizing the safety-related encoder and gear settings in the drive as well as the standard data in the NC, and by simultaneously changing the gear in the drive and the NC.

Example: parameter assignment

Parameter assignment in the drive: (gear stage 1 faulty, gear stage 2 correct)

Active SLS limit value	p9531 = 280 rpm
SLS (Safely-Limited Speed)	p9533 = 100%
Gear motor/load denominator	p9521[0,1] = 28, 28
Gear motor/load numerator	p9522[0,1] = 3088, 3088

Example of a parameter assignment in the NC:

Setpoint velocity limiting	MD 36933 = 90%
Denominator load gearbox	MD 31050[1,2] = 1, 28
Numerator load gearbox	MD 31060[1,2] = 1, 3088

Scenario 1: SLS active, gear stage 1 (NC/drive) > Different parameterization of gearboxes

- Motor-side setpoint velocity limitation: (corresponds to S_V_LIMIT_B in SIC):
  r9733 = 280 rpm * 3088/28 * 1.0 = 30880 rpm
- NC-side setpoint velocity limitation:
  OPI safeDesVeloLimit = 30880 rpm* 1/1 * 0.9 = 27792 rpm
  – The active setpoint velocity limitation is greater than the SLS limit.

Scenario 2: SLS active, gear stage 2 (NC/drive) > Identical parameterization of gearboxes

- Motor-side setpoint velocity limitation (corresponds to S_V_LIMIT_B in SIC):
  r9733 = 280 rpm * 3088/28 * 1.0 = 30880 rpm
- NC-side setpoint velocity limitation:
  OPI safeDesVeloLimit = 30880 rpm* 28/3088 * 0.9 = 252 rpm
  – The active setpoint velocity limit corresponds to 90% of the SLS limit.

Acceptance test 8

8.1 Purpose and requirements

The objective of the acceptance test is to check the correct parameterization and mode of operation of the safety functions and to detect potential configuration errors or to document the correctness of the configuration.

With the acceptance test, the limit values entered for all activated safety functions must be exceeded (violated). This allows the correct execution of the function to be checked and verified.

WARNING

Unwanted motion due to incorrect parameter changes

Changes to accepted safety functions may lead to faults or to unwanted motion and thus to serious injuries or death.

- Perform a new acceptance test as soon as changes have been made to any of the safety functions.
- Also create an appropriate acceptance report.

Responsibility for the acceptance test

The machine manufacturer is responsible for carrying out and documenting an acceptance test.

It is not permissible to use the results of the acceptance test for other purposes!

The measured values obtained when executing the acceptance test (e.g. distance or time) and the system response identified (e.g. initiation of a specific stop) are used to check the plausibility of the configured safety functions. The values that are measured are typical and are not worst-case values. They represent the behavior of the machine at the time of measurement. These measurements cannot be used to derive real values (e.g. maximum distances for over-travel distances).

Acceptance test in SINUMERIK Operate

A detailed description of the acceptance test in SINUMERIK Operate is provided in Function Manual "SINUMERIK Operate Acceptance Test" (download (https://support.industry.siemens.com/cs/ww/en/view/109783228)).

Diagnostics 9

If you are looking for a description of the diagnostic functionality, then in this Chapter you can find a Diagnostics guide (Page 348) and descriptions relating to the safety diagnostic functionality (Page 352) with SINUMERIK Operate.

These diagnostic functions are possible in the following software depending on the particular component:

Table 9-1 Diagnostic functionality depending on the components

Component	SINUMERIK Operate	TIA Portal
F-PLC	-	See the help for SIMATIC Safety
F-I/O	-	See the help for SIMATIC Safety
Safety program (F-program)	-	See the help for SIMATIC Safety
Checksums	SINAMICS checksums in operating area "Diagnostics"	F-runtime group signature and F-signature of the software and hardware. See the help for SIMATIC Safety
Status of safety-relevant drives	Operating area "Diagnostics"	-
Telegram diagnostics	Operating area "Diagnostics"	-
SCA diagnostics	Operating area "Diagnostics"	-
Status and diagnostic information about specific safety functions	Operating area "Startup" (without activating the commissioning mode)	-

You will also find general descriptions and background information about diagnostics using SINUMERIK Operate in this chapter:

- For the display and evaluation of diagnostic information (Page 362)
- Checksums (Page 363)
- Stop responses (Page 366)
- Use of the fault buffer and safety message buffer (Page 373)
- Acknowledgment (Page 376)

Information about replacing components (software or hardware components) is provided in a separate chapter (Page 381).

9.1 Pathfinder to S7-1500 diagnostics

Detailed information about F-CPU S7-1500 diagnostics is available in the Function Manual Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926).

Note

The description in the Function Manual Diagnostics is not specifically intended for SINUMERIK Safety Integrated.

Tip on RET_DPRD/RET_DPWR

RET_DPRD:

Non failsafe error code RET_VAL of instruction DPRD_DAT.

The description of the error code is provided in STEP 7 help for instruction DPRD_DAT (Extended instructions > Distributed I/O > Additional).

RET_DPWR:

Non failsafe error code RET_VAL of instruction DPWR_DAT.

The description of the error code is provided in STEP 7 help for instruction DPWR_DAT (Extended instructions > Distributed I/O > Additional).

9.2 System alarms

Display diagnostic screen "Messages"

MENU SELECT > Diagnostics > Menu extension > Messages

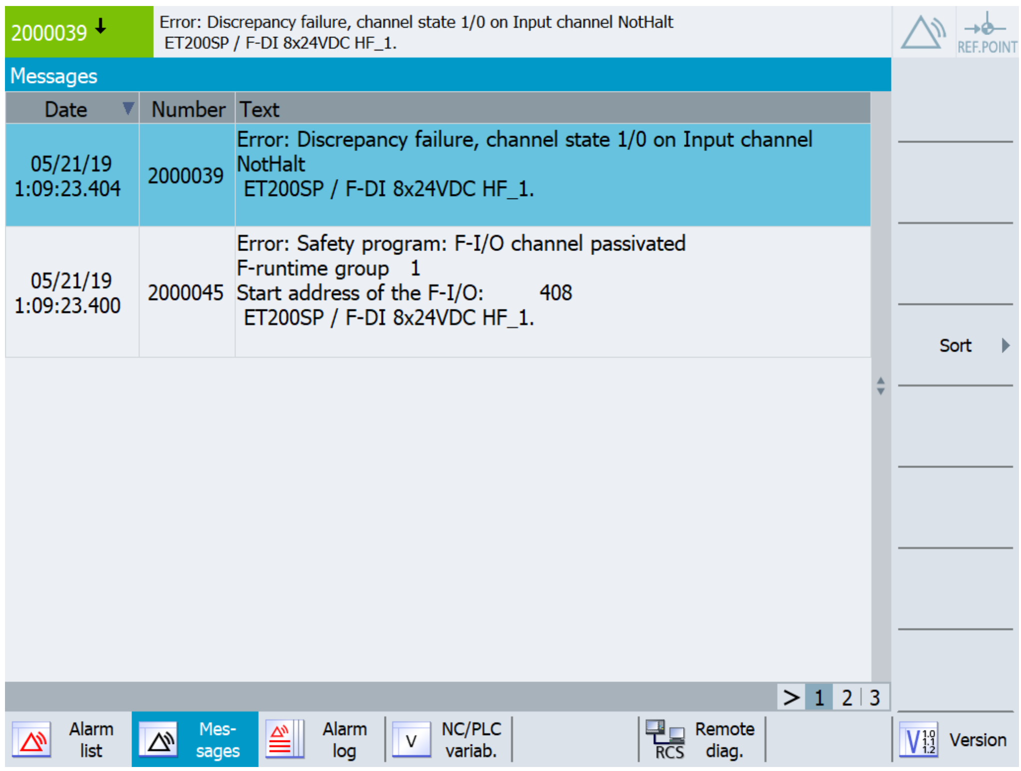


Figure 9-1 Messages - system alarms

Exporting alarm texts from the TIA Portal

You must export alarm texts from the TIA Portal in order that alarm texts from the TIA Portal can be displayed in SINUMERIK Operate in the diagnostic screen "Messages".

Proceed as described below:

1. Open the project in the TIA Portal.
2. In the project navigator, click on the SINUMERIK control and select shortcut menu "Export alarms and texts for SINUMERIK Operate ...".

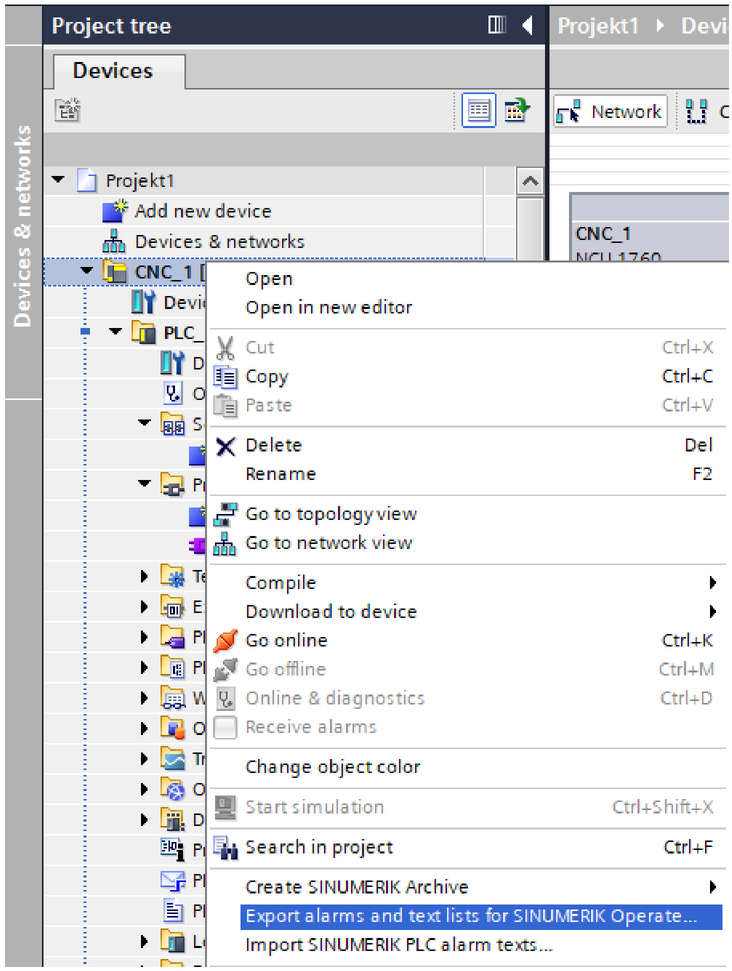


Figure 9-2 Exporting alarms from the TIA Portal

3. In the following dialog, select the memory path for the export files.

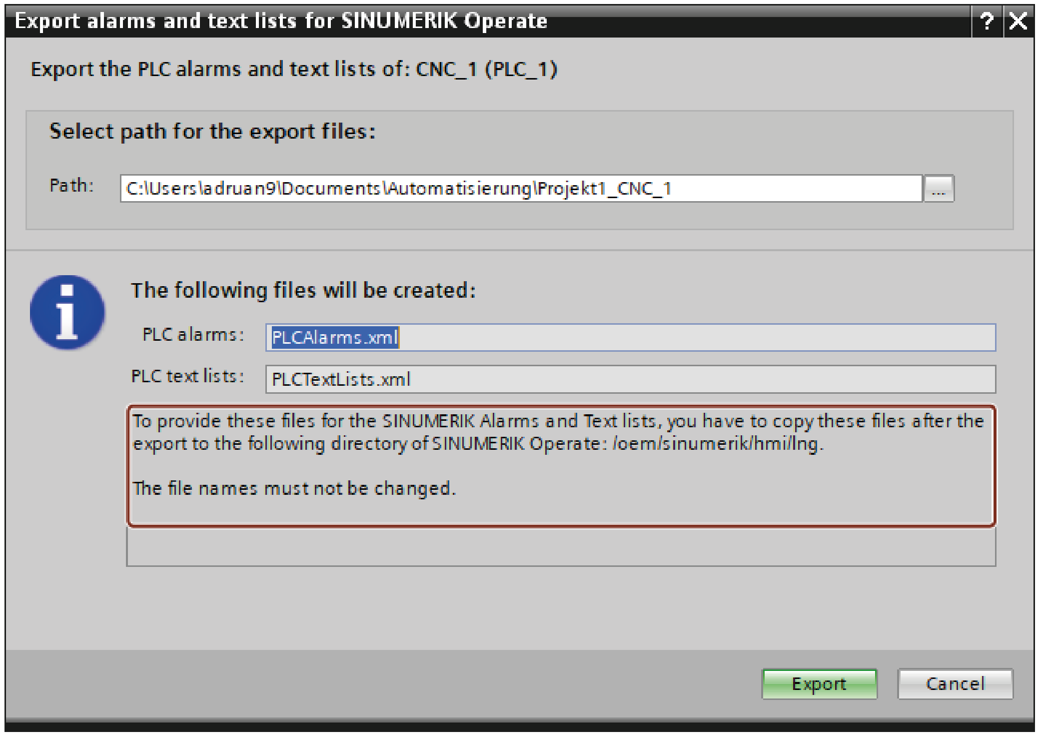


Figure 9-3 Export dialog

4. Then click on "Export".
   The export files for Operate are saved to the specified directory.
5. From there, copy the files to be exported to directory **/oem/sinumerik/hmi/lng**.

9.3 Diagnostic functions in SINUMERIK Operate

9.3.1 Safety Integrated diagnostics overview

The diagnostics overview includes general information about the operating mode used, the number and type of axes used - as well as status information about the pending alarms and safe homing.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety

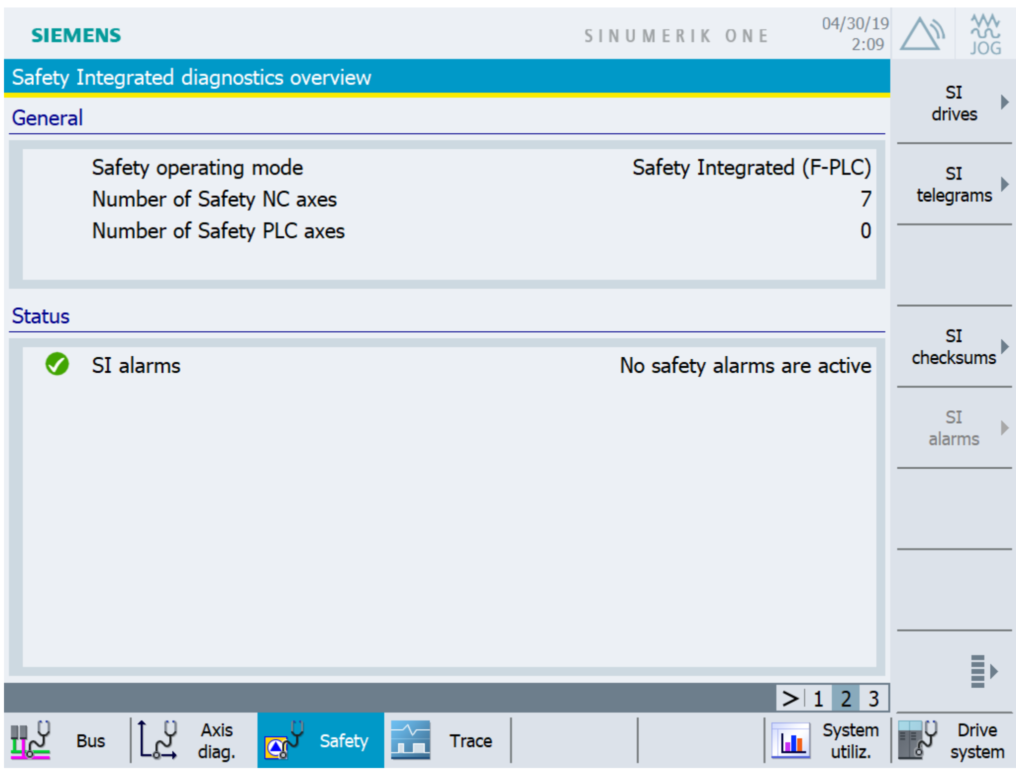


Figure 9-4 Safety Integrated diagnostics overview

This screen is simultaneously used as entry to the following diagnostic screens:

- SI drives (Page 353)
- SI telegrams (Page 356)
- SI checksum (Page 358)
- SI alarms (Page 360)
- SI Safe Cams (Page 361) (via menu forward key)

9.3.2 SI drives status

The configured safety-relevant status and diagnostic information of the selected drive are displayed in the "SI drive status" diagnostic screen.

Functions, which are not configured for the selected drive, are not displayed on the screen.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI drives

The diagnostic screen "SI drive status" is available for basic functions and for extended functions.

Call "SI drive status - Basic functions"

MENU SELECT > Diagnostics > Menu forward key > Safety > SI drives > Basic functions

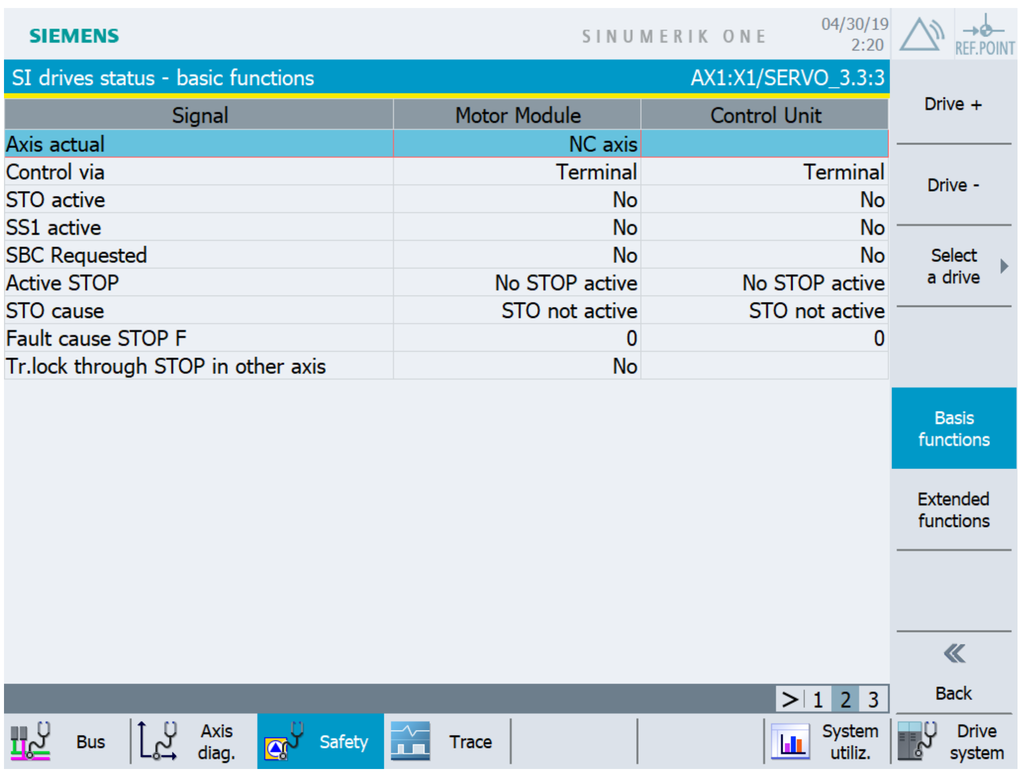


Figure 9-5 Diagnostic screen "SI drive status - Basic functions"

Call "SI drive status - Extended functions"

MENU SELECT > Diagnostics > Menu forward key > Safety > SI drives > Extended functions

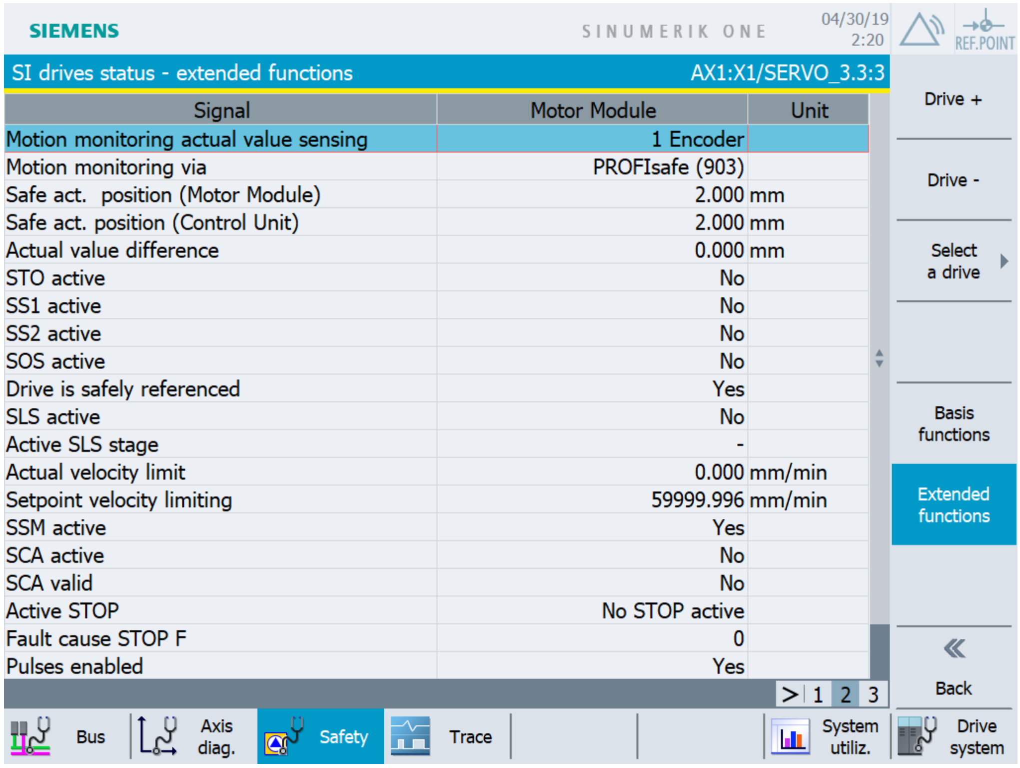


Figure 9-6 "SI drive status - Extended functions" diagnostic screen (sample screenshot)

9.3.3 SI telegrams overview

The telegram types for PROFIsafe and SIC/SCC for the respective drives/axes are displayed in the "SI telegrams overview" diagnostic screen.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI telegrams

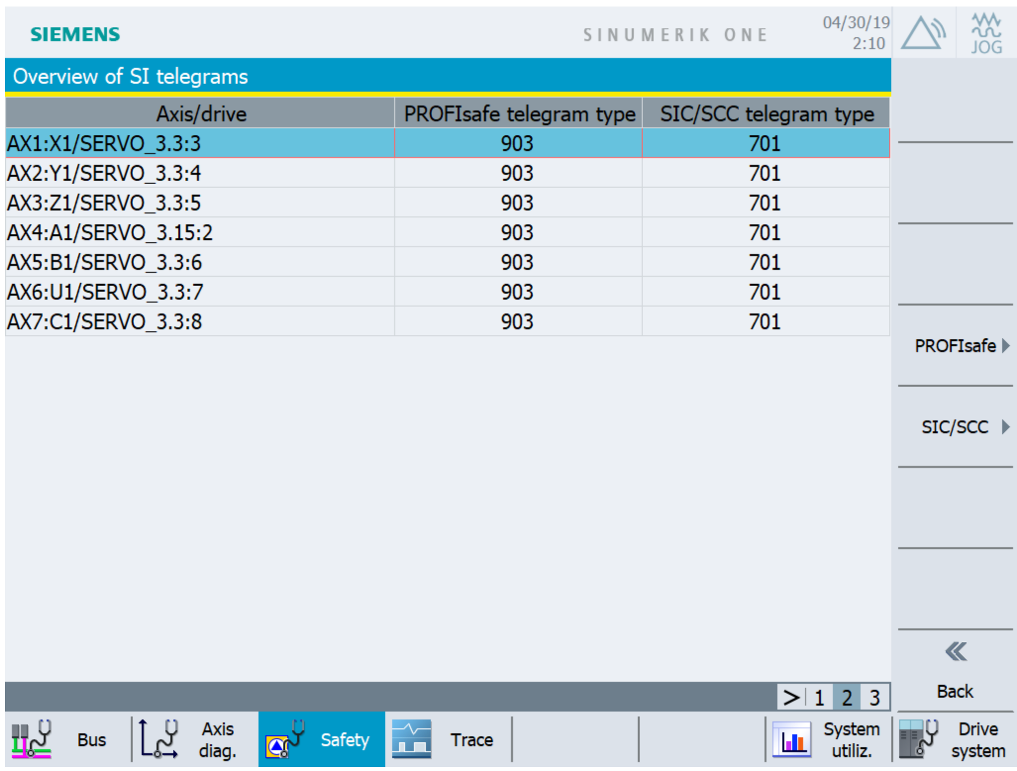


Figure 9-7 "SI telegrams overview" diagnostic screen

This screen is simultaneously used as entry to the following diagnostic screens:

- SI telegrams PROFIsafe (Page 356)
- PROFIdrive SI telegrams (Page 357)

Additional information

- You will find general information on safety-relevant telegrams in Chapter Controlling safety functions integrated in the drive (Page 223).

9.3.4 SI telegrams PROFIsafe

The meanings and statuses of the individual bits in the control word and status word are shown in the "PROFIsafe SI telegrams" diagnostic screen. You can switch between the following views:

- Status word
- Status word cam (**Note:** only when the cam function is enabled in SINAMICS)

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI telegrams > PROFIsafe

Figure 9-8 "PROFIsafe SI telegrams" diagnostic screen

The view of all user data of the control word and status word is displayed using the "Details" softkey.

Additional information

- You can obtain general information about PROFIsafe telegrams in Chapter Controlling via PROFIsafe (Page 227).

9.3.5 PROFIdrive SI telegrams

The meanings and statuses of the individual bits in the control word and status word are shown in the "PROFIdrive SI telegrams" diagnostic screen.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI telegrams > SIC/SCC

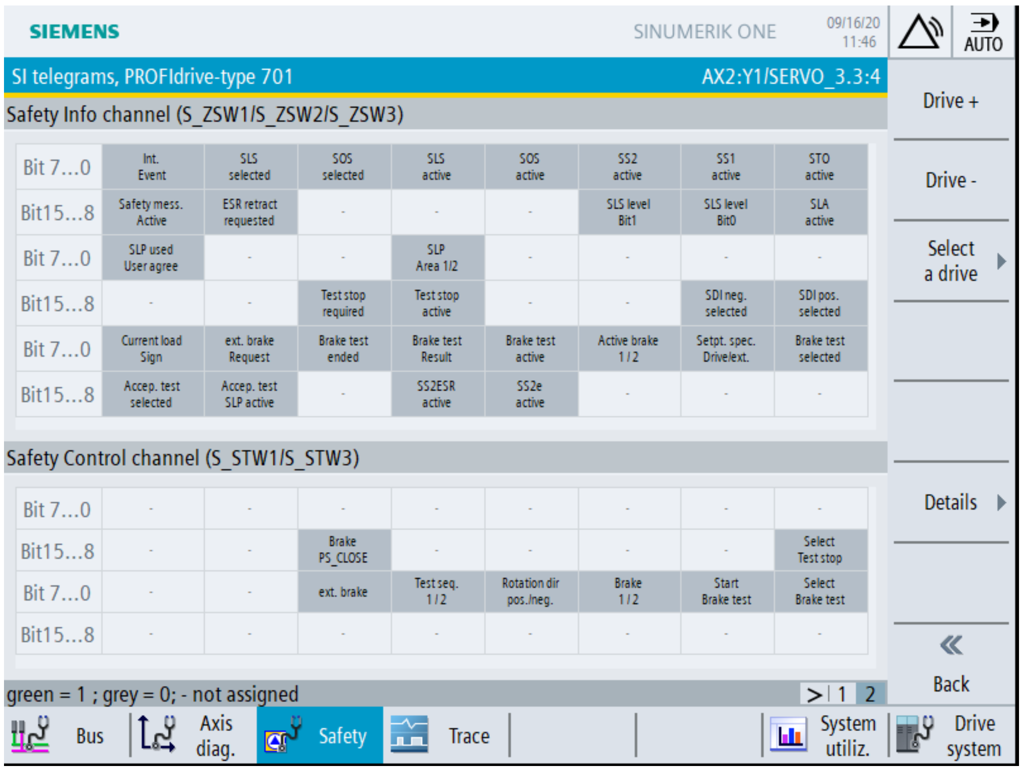


Figure 9-9 PROFIdrive SI telegrams

The view of all user data of the control word and status word is displayed using the "Details" softkey.

Additional information

- You can obtain general information about SIC/SCC telegrams in Chapter Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 231).

9.3.6 SI checksums

In the "SI checksums overview" diagnostic screen, all of the safety reference and actual checksums are displayed for the axes and drives. Status symbols are used to flag differences between reference and actual checksums

Calling checksums

MENU SELECT > Diagnostics > Menu forward key > Safety > SI checksums

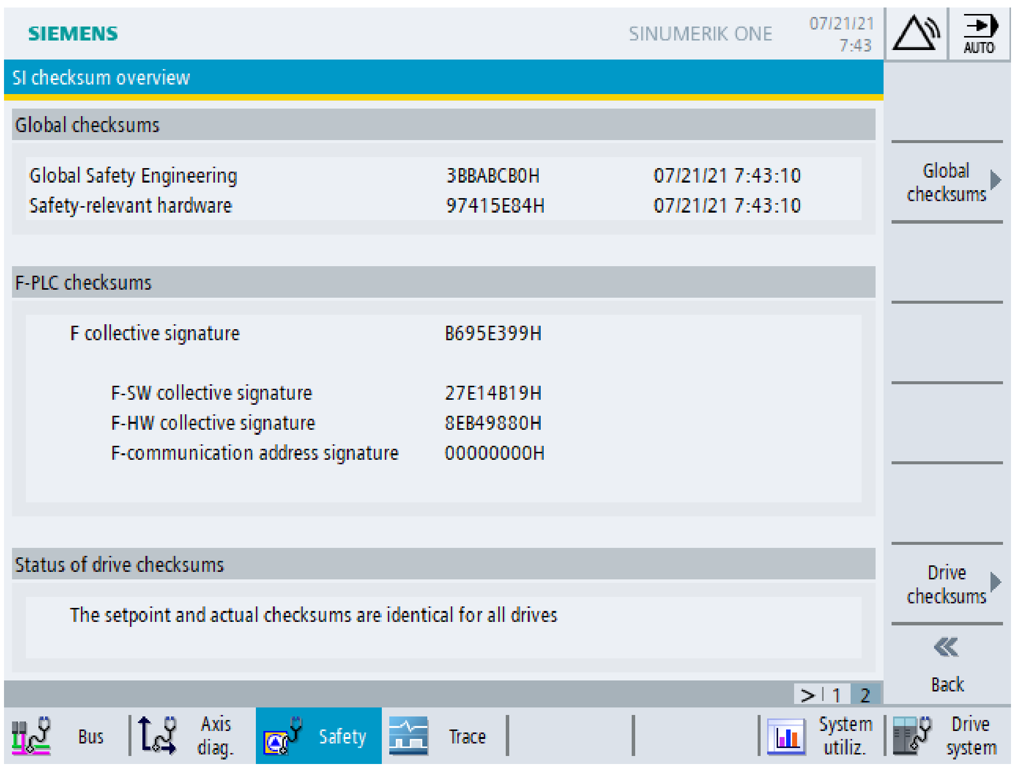


Figure 9-10 "SI checksums overview" diagnostics screen

Higher-level actual checksums that are calculated from the master checksums (Page 363) are displayed in the "SI checksums global checksums" diagnostic screen. If you call the diagnostics screen, then the calculation of the global checksums is started - and after completion, these actual checksums, along with the calculation date, are displayed.

Calling global checksums

MENU SELECT > Diagnostics > Menu forward key > Safety > SI checksum > Global checksums

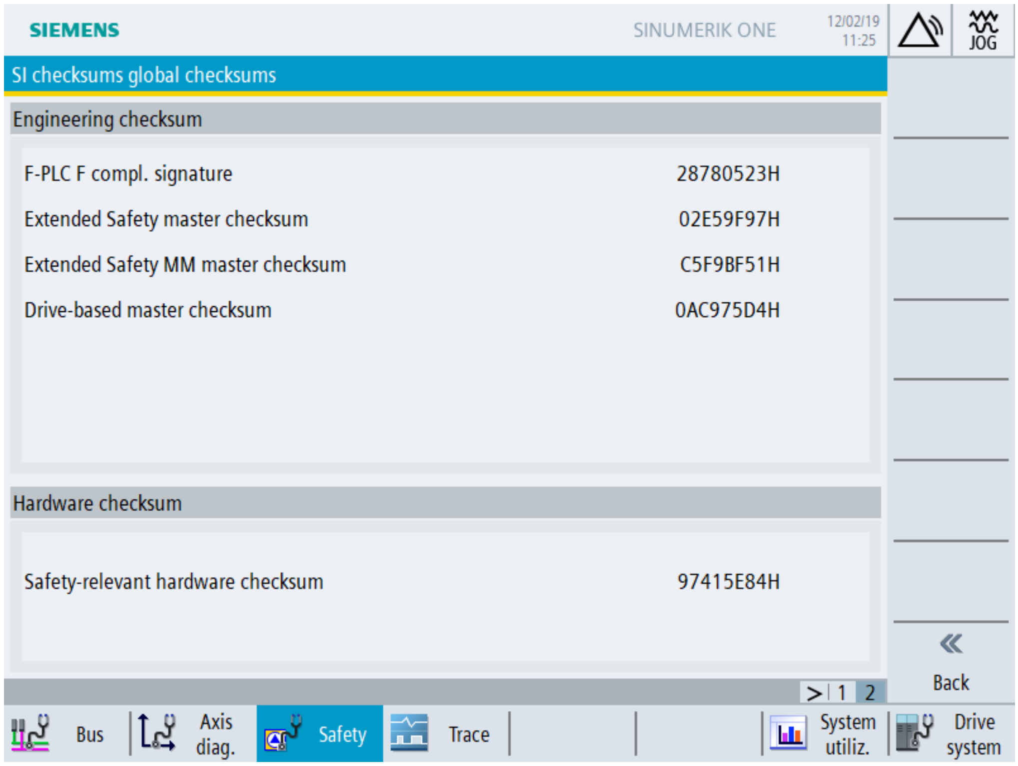


Figure 9-11 "SI checksums global checksums" diagnostic screen

If, based on these global checksums, you identify some changes in the safety configuration, then you can switch from diagnostics screen "Global checksums" to the individual axis/drive checksums in order to identify specific differences.

9.3.7 SI alarms

Active safety-relevant alarms are displayed in diagnostics screen "SI-alarms".

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI alarms

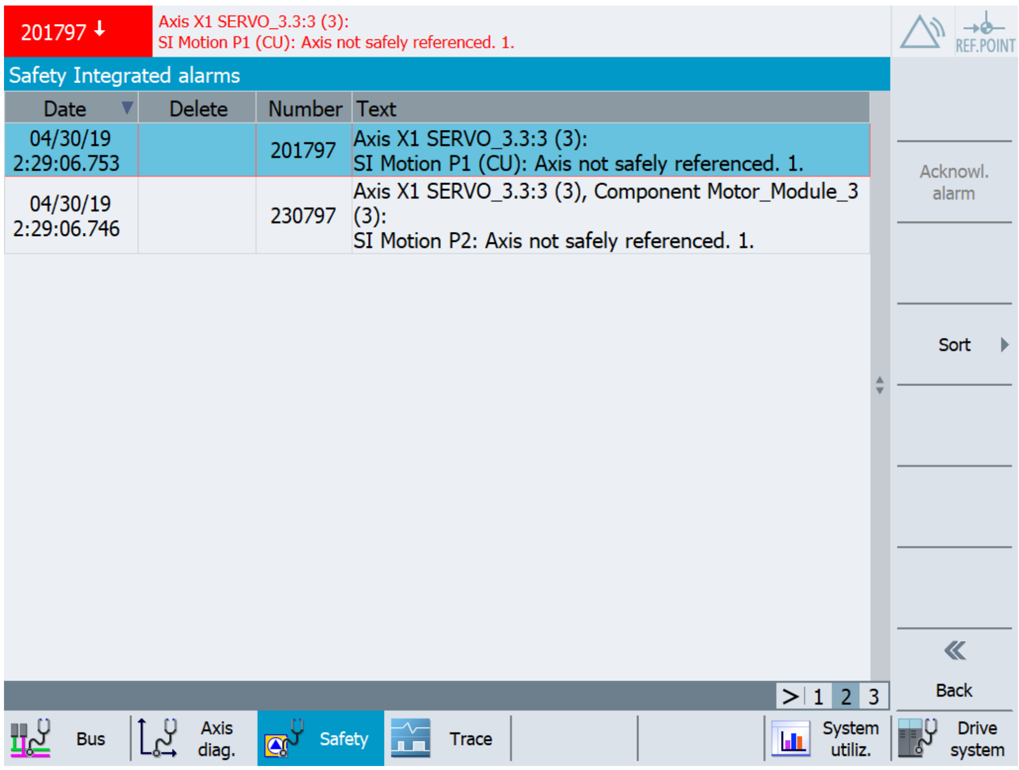


Figure 9-12 "Safety Integrated alarms" diagnostic screen

9.3.8 SI Safe Cams

In the "SI safe cams" diagnostic screen, the following information about the Safe Cam (SCA) safety function of the selected drive is displayed:

Status of the function (SCA)	For the selected drive, indicates whether the Safe Cam (SCA) safety function has been selected, is active and is valid. The actual position is also displayed (actual value on the load side on the CU).	
		Inactive
		Active
		Invalid. Safe referencing was not carried out.
Status of the enabled cams	For each configured and enabled cam, displays the identifier, the minus and plus positions - as well as the validity of the cam position.	
		Cam position is reached and the cam is invalid.
		Cam position is reached and the cam is valid. Safe referencing was carried out.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > Menu forward key >SI cams

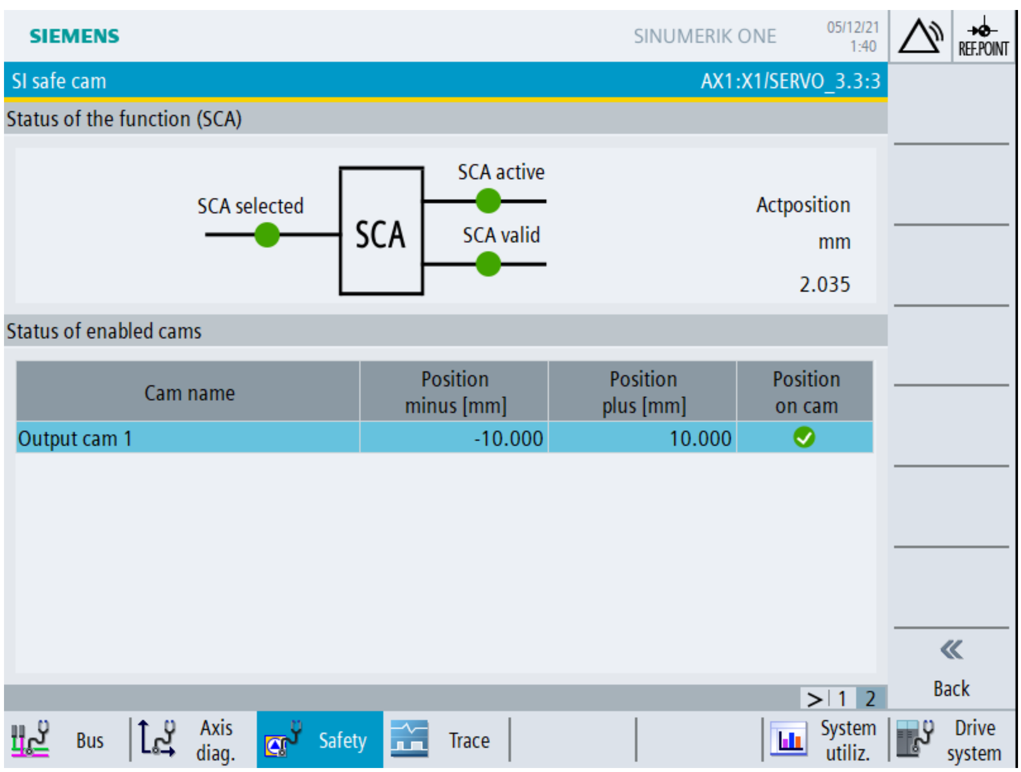


Figure 9-13 "SI safe cams" diagnostics screen

9.4 Display and evaluation of diagnostic information

In the "SINUMERIK Safety Integrated (F-PLC)" mode, safety-related monitoring functions are integrated in the drive. Diagnostic information is communicated and evaluated as follows:

- The status and control information (SIC/SCC) (Page 231) of the drive is transferred between the integrated subcomponents of the SINUMERIK ONE:
  - As a consequence, the motion control in the NC is also linked (Page 371) to the safety functions integrated in the drive, therefore avoiding unnecessary follow-on responses in the NC.
  - Some SIC status information is also saved to NC variables (OPI) (Page 390).
- SINAMICS Integrated messages and alarms can be displayed as follows:
  - Safety messages of the drive are displayed in SINUMERIK Operate in the alarm lists.
  - The standard alarm of a drive can also include safety-related diagnostic information. In order that these are displayed in SINUMERIK Operate, you must activate the alarm buffer (Page 374).
  - Display and acknowledgment (Page 376) of messages depend on the scope of the Safety Integrated Functions (Page 30) used - and the use of the safety message buffer (Page 374).

9.5 Checksums

Based on Safety Integrated checksums and signatures, you can compare the actual state of the machine with the original state when delivered, which is documented in the acceptance report. The checksums are displayed in SINUMERIK Operate in the Diagnostics area (Page 358).

- The individual F-blocks have signatures, and the safety program has an F-collective signature. These checksums for the safety program are displayed in the TIA Portal as well as in the safety printout.
- The F-PLC has an F-collective signature. The hardware F-signature and the software F-signature are output in the TIA Portal or in the safety summary (printout).
- There are SINAMICS parameters with reference checksums (defined when commissioning) and actual checksums for the CU, MM and motion monitoring functions; these are checked by SINAMICS Integrated when they power up. SINAMICS alarms F01650/F30650 and/or F01680/F30680 are output if the checksums differ.
  See: SINAMICS checksums (Page 365)
- In SINUMERIK Operate, additional master checksums and global checksums are displayed, which are calculated from the actual checksums listed above. The NCU does not compare these higher-level checksums with reference checksums - and it does not save them.
  See: Calculating the global checksums/master checksums (Page 363)
  The global checksums/master checksums are displayed in the diagnostics area of SINUMERIK Operate, which means that it is easy to identify differences between the actual and reference states.
  See: SI checksums (Page 358)

9.5.1 Calculating the global checksums/master checksums

In addition to the checksums or signatures of the SINAMICS Integrated and F-PLC subcomponents, in SINUMERIK Operate, global checksums and master checksums are displayed, which are calculated from various actual checksums of the F-PLC and SINAMICS Integrated. The NCU does not compare these higher-level actual checksums with reference checksums - and it does not save them.

By displaying these higher-level actual checksums, differences between the actual and reference states can be easily and transparently identified.

The global checksums/master checksums are calculated as follows:

- The global checksum is the sum of the associated master checksums (see table).
- The master checksums comprise the sums of the values/parameters with actual checksums for the calculation (see table).
  If SINAMICS parameters are involved for the values being used as basis, then when making the calculation, the sum over the following drives is generated:
  - Drives, which do not have an assigned NC axis, and where the safety functions are enabled in p9601: p9601 SI enable functions integrated in the drive (Control Unit) / SI enable fct CU ! = 0

Table 9-2 Calculating the global checksum and the associated master checksums

Global checksum	Master checksum	Values/parameters used for the calculation
Global safety engineering checksum (sum of all master checksums)	F-CPU master checksum	• Signature of the safety program • Hardware checksum of the F-PLC
	Extended Safety master checksum	• r9728[0] SI Motion actual checksum SI parameters / SI Mtn act CRC • r9728[1] SI Motion actual checksum SI parameters / SI Mtn act CRC
	Extended Safety MM master checksum	• r9398[0] SI Motion actual checksum SI parameters (Motor Module) / SI Mtn act CRC MM
	Drive-based master checksum	• r9798 SI actual checksum SI parameters (Control Unit) / SI act_checksum CU • r9898 SI actual checksum SI parameters (Motor Module) / SI act_checksum MM

Table 9-3 Calculation of the master checksum "Safety-relevant hardware checksum"

Master checksum	Parameters used for the calculation
Safety-relevant hardware checksum	• r9728[2] SI Motion actual checksum SI parameters / SI Mtn act CRC • r9398[1] SI Motion actual checksum SI parameters (Motor Module) / SI Mtn act CRC MM

9.5.2 SINAMICS checksums

For each monitoring channel, the safety parameters include 2 parameters for the reference and actual checksum.

During commissioning, the actual checksum must be transferred to the corresponding parameter for the reference checksum. This can be done for all checksums of a drive object at the same time using parameter p9701 - or using the corresponding SINUMERIK Operate functionality.

Table 9-4 Basic Functions

• r9798	SI actual checksum SI parameters (Control Unit)
• p9799	SI reference checksum SI parameters (Control Unit)
• r9898	SI actual checksum SI parameters (Motor Module)
• p9899	SI reference checksum SI parameters (Motor Module)

Table 9-5 Extended Functions (contain also the following checksum parameters)

• r9398[0...1]	SI Motion actual checksum SI parameters (Motor Module)
• p9399[0...1]	SI Motion reference checksum SI parameters (Motor Module)
• r9728[0...2]	SI Motion actual checksum SI parameters
• p9729[0...2]	SI Motion reference checksum SI parameters

During each ramp-up procedure, the actual checksum is calculated via the Safety parameters and then compared with the reference checksum.

If the actual and reference checksums are different, fault F01650/F30650 or F01680/F30680 is output.

9.6 Stop responses

9.6.1 Overview

The stop responses that can be initiated depend on the scope of the Safety Integrated Functions used:

- Stop responses that can be initiated for faults involving Safety Integrated Basic Functions (Page 366)
- Stop responses that can be initiated for faults involving Safety Integrated Extended Functions (Page 368)

Stop responses and safety functions can be dependent on a priority that has been assigned:

- No overall priority is assigned to individual safety functions.
- The various stop responses each have a certain priority (Page 371).
- For stop responses and Safety Integrated Extended Functions, there are some dependencies regarding the priority (Page 371).

The motion control in the NC is linked (Page 371) to the Safety Integrated Functions integrated in the drive and the associated stop responses, which means that no unnecessary follow-on responses are initiated in the NC.

9.6.2 Basic Functions

When faults associated with Safety Integrated Basic Functions occur, the following stop responses can be initiated:

Table 9-6 Stop responses for Safety Integrated Basic Functions

<table>
<tr><th>Stop response</th><th>Triggered ...</th><th>Action</th><th>Effect</th></tr>
<tr><td>STOP A cannot be acknowledged</td><td>For all Safety faults with pulse suppression that cannot be acknowledged.</td><td rowspan="2">Trigger safe pulse suppression via the switch-off signal path for the relevant monitoring channel. During operation with SBC: Apply motor holding brake.</td><td rowspan="2">The motor coasts to a standstill or is braked by the holding brake.</td></tr>
<tr><td rowspan="2">STOP A</td><td>For all acknowledgeable Safety faults
As a follow-up reaction of STOP F</td></tr>
<tr><td colspan="3">STOP A corresponds to Stop Category 0 in accordance with EN 60204-1.
With STOP A, the motor is switched directly to zero torque via the "Safe Torque Off (STO)" function.
A motor at standstill cannot be started again accidentally.
A moving motor coasts to standstill. This can be prevented by using external braking mechanisms, e.g. holding or operating brake.
When STOP A is present, "Safe Torque Off" (STO) is active.</td></tr>
</table>

Stop response	Triggered ...	Action	Effect
STOP F	If an error occurs in the cross-wise data comparison.	Transition to STOP A.	Follow-up response STOP A with adjustable delay (factory setting without delay) if one of the safety functions is selected
	STOP F is permanently assigned to the crosswise data comparison (CDC). In this way, errors are detected in the monitoring channels. After STOP F, STOP A is triggered. When STOP A is present, "Safe Torque Off" (STO) is active.		

WARNING

Uncontrolled axis motion when a STOP A/F is initiated

With a vertical axis or pulling load, there is a risk of uncontrolled axis movements when STOP A/F is triggered. If present in the hazardous area, this can result in death or severe injury.

- Use the "Safe Brake Control (SBC)" and a holding brake (not a safety-relevant brake!) with sufficient holding force to prevent these movements.

9.6.3 Extended Functions

Faults involving Safety Integrated Extended Functions and violation of limits can trigger the following stop responses:

Table 9-7 Stop responses for Safety Integrated Extended Functions

Stop response	Triggered ...	Response of the initiating axis or DRV response	Response of other axes or NC response
STOP A[1)] (corresponds to STO[2)])	• For all acknowledgeable safety faults with pulse cancellation • Subsequent response of STOP B • Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP • Configurable subsequent stop p9579 for SLA	Immediate pulse cancellation **Effect:** Drive coasts down	All path axes: IPO rapid stop All axes, with the exception of the path axes and the initiating axis: Braking along a ramp (acceleration limit)
STOP B[1)] (corresponds to SS1[3)])	Examples: • Standstill tolerance violated in p9530 (SOS) • Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP • Subsequent response of STOP F • Configurable subsequent stop p9579 for SLA	Immediate input of speed setpoint = 0 and start of timer t_B. Once t_B or $n_{act} < n_{shutdown}$ has expired, STOP A is triggered. **Effect:** STOP B with subsequent STOP A. The drive decelerates along the OFF3 ramp and then switches to STOP A. **Note:** For "SS1 with external stop" (SS1E), braking is **not** along the OFF3 ramp (see Chapter SS1 (Extended Functions) with external stop (Page 113))	All path axes: IPO rapid stop All axes, with the exception of the path axes and the initiating axis: Braking along a ramp (acceleration limit)
STOP C[1)] (corresponds to SS2[4)])	• Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP Configurable subsequent stop p9579 for SLA	Immediate input of speed setpoint = 0 and start of timer t_C. Once t_C has elapsed, SOS is selected. **Effect:** The drive decelerates along the OFF3 ramp; SOS is then selected.	All path axes: IPO rapid stop All axes, with the exception of the path axes and the initiating axis: Braking along a ramp (acceleration limit)

Stop response	Triggered ...	Response of the initiating axis or DRV response	Response of other axes or NC response
STOP D[1), 5)]	• Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP • Configurable subsequent stop p9579 for SLA	Timer t_D is started. No drive-integrated response, but an NC response (see right). Once t_D has elapsed, SOS is selected. An automatic response is only triggered if the standstill tolerance window is violated in SOS.	Braking along the path (interpolatory braking)
STOP E[1), 5)]	• Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP • Configurable subsequent stop p9579 for SLA	SOS triggered after the expiry of p9554 **Effect:** Controlling the drive-integrated ESR functionality	Fast retraction (ESR), which allows the controlled axes to be retracted
STOP F[1)]	If an error occurs in the crosswise data comparison. Follow-up response STOP B or STOP A	Timer t_{F1} (Basic Functions) or t_{F2} (Extended Functions) No drive response **Effect:** If a safety function (SOS, SLS) has been selected or if SSM with hysteresis has been enabled, transition to STOP A after t_{F1} (Basic Functions) has elapsed or STOP B after t_{F2} (Extended Functions) has elapsed.	NC start/traversing interlock

1) See also the following note "delayed pulse cancellation when the bus fails".

2) The behavior of the drive after STOP A is triggered corresponds (apart from the safety messages) to the behavior after STO is triggered. Note that the parameterization of STO applies equally for STOP A.

3) The behavior of the drive after STOP B is triggered corresponds (apart from the safety messages) to the behavior after SS1 is triggered. Monitoring with the aid of SAM or SBR, for example, works in exactly the same way. Note that the parameterization of SS1 applies equally for STOP B.

4) The behavior of the drive after STOP C is triggered corresponds (apart from the safety messages) to the behavior after SS2 is triggered. Monitoring with the aid of SAM, for example, works in exactly the same way. Note that the parameterization of SS2 applies equally for STOP C.

5) The behavior of the drive after STOP D (E) is initiated corresponds (apart from the safety messages) to the behavior after SS2E (SS2ESR) is initiated.

Note

Delayed pulse cancellation when the bus fails

For SLS, SDI, SLP and SLA, the stop responses are also available with delayed pulse cancellation when the bus fails (to prevent the drive from immediately responding with pulse cancellation when a communication error occurs):

- If p9580 ≠ 0 and SLS is active, in the event of communication failure, the parameterized ESR reaction is only realized if, as SLS response, a STOP with delayed pulse cancellation when the bus fails has been parameterized (p9563[0...3] ≥ 10).
- If p9580 ≠ 0 and SDI is active, in the event of a communication failure, the parameterized ESR reaction only occurs if a STOP with delayed pulse cancellation when the bus fails has been parameterized as the SDI response (p9566 ≥ 10).
- If p9580 ≠ 0 and SLP is active, the parameterized ESR reaction only takes place for a communication failure if a STOP with delayed pulse cancellation in the event of bus failure is parameterized as the SLP response (p9562[0...1] ≥ 10).
- If p9580 ≠ 0 and SLA is active, the parameterized ESR response is only triggered in the event of a communication failure if a STOP with delayed pulse cancellation when the bus fails has been parameterized as the SLA response (p9579 ≥ 10).

The delay time (p9580) must not exceed 800 ms.

Note

Delay time between STOP F and STOP B

A delay time between STOP F and STOP B should only be set if an additional response is initiated during this time when the "Internal Event" (r9722.7) message signal is evaluated.

Further, when using the delay time, a monitoring function should always be selected (e.g. SLS with a high limit speed) or the hysteresis of SSM should be configured.

When hysteresis is activated for SSM, then this should be considered to be an activated monitoring function.

On delays at the transition of the stop responses

- t_B: p9556
- t_C: p9552
- $t_{D:}$ p9553
- t_E: p9554
- t_{F1}: p9658
- t_{F2}: p9555
- $n_{shutdown}$: p9560

9.6.4 Definitions and effects in the NC

The motion control in the NC is linked to the Safety Integrated Functions in the drive via the SIC status signals. This avoids that subsequent responses are initiated in the NC as a result of safety stops in the drive.

Example: The motion control in the NC responds to the drive STOP responses by no longer issuing additional setpoints for the path, for example. As a consequence, alarms to be acknowledged are avoided, such as "Contour monitoring" or "Positioning monitoring".

The corresponding status bits from S_ZSW1 (or S_ZSW1B) are used to emulate the safety stop responses in the NC.

9.6.5 Priorities

Table 9-8 Priorities of the stop responses

Priority classes	Stop response
Highest priority	STOP A
.....	STOP B
...	STOP C
..	STOP D
..	STOP E
Lowest priority	STOP F

Priorities between stop responses and Extended Functions

The following table lists which stop response or safety function is set if a STOP is initiated when a safety function is active.

Table 9-9 Priorities between stop responses and Extended Functions

Stop response/ Extended Function		Highest priority	...	...	...	...	Lowest priority
		STOP A	**STOP B**	**STOP C**	**STOP D**	**STOP E**	**STOP F**
Highest priority	**STO**	STOP A / STO	STO	STO	STO	STO	STO
.....	**SS1**	STOP A	STOP B / SS1	SS1	SS1	SS1	SS1
...	**SS2**	STOP A	STOP B	STOP C / SS2	SS2	SS2	SS2 / STOP B[2)]

..	**SOS**	STOP A[1)]	STOP B[1)]	SOS	SOS	STOP E/SOS	STOP B[2)]
Lowest priority	**SLS**	STOP A[3)]	STOP B[3)]	STOP C[4)]	STOP D[4)]	STOP E[4)]	STOP B[2)]

1) The SOS monitoring function remains active, although the fault response in the event of a fault can no longer be triggered because it is already present.

2) STOP B is the subsequent stop of STOP F, which is activated after a time that can be parameterized. STOP F alone does not have any effect; the active safety function is still present.

3) The SLS monitoring function remains active, although the fault response in the event of a fault can no longer be triggered because it is already present.

4) SLS remains active during the braking phase, after which the system switches to SOS.

Explanation of the table

No overall priority is assigned in the individual safety functions. SOS remains active, for example, even if STO is requested.

- The safety functions that cause the drive to decelerate (SS1, SS2) are specified from top to bottom in descending order of priority.
- The stop responses arranged here from left to right in descending order of priority (STOP A-F).

If a field contains two entries, the stop responses and safety functions have the same priority.

- STOP A corresponds to selecting STO
- STOP B corresponds to selecting SS1
- STOP C corresponds to selecting SS2
- STOP D corresponds to selecting SOS
- STOP E corresponds to selecting SOS (for additional activation of the standard "Extended stop and retract (ESR)" function)
- When the SS2 function is active, STOP F results in subsequent stop STOP B. SS2 remains active.

Examples for illustrating the information in the table:

- Safety function SS1 has just been selected. STOP A remains selected.
- By selecting a STOP with a higher priority, STOPs that are present with a lower priority will be replaced. This means that when SS1 is selected (≙ STOP B), any STOPs C-F that are present will be replaced.
- The SLS safety function is selected. This selection does not modify the function of STOP A-D. A STOP F now triggers a STOP B because a safety function has been activated.
- Stop response, STOP C is selected. If the STO or SS1 safety functions are active, this does not have any effect. If SS2 is active, this brake ramp is retained. If SOS is active, SOS remains effective, which is also the end status of STOP C. When SLS is selected, the drive is decelerated with STOP C.

9.7 Using the fault buffer, message buffer and alarm buffer

In addition to the standard fault buffer and the standard alarm buffer, SINAMICS Integrated has several safety message buffers for safety-relevant messages involving Safety Integrated Extended Functions:

- Messages for Extended Functions are displayed in the safety message buffer.
  - You must enable SIC/SCC for the appropriate axes in MD39750.
  - For all messages in the safety message buffer, a specific reference is made in the HMI to the fact that safety-relevant acknowledgment (Page 376) is required.
    - Reference is made to active safety-relevant alarms in SINUMERIK Operate in the "Safety Integrated diagnostics overview "(in addition to the standard alarm list).
    - Reference is made to active alarms that require a safety-relevant acknowledgment using a safety delete symbol.
  - To acknowledge messages in the safety message buffer, safety-relevant acknowledgment is required - and possibly also acknowledgment with PROFIdrive RESET (Page 377).
- Messages for Basic Functions or for external drives without an NC axis assignment, cannot be saved to the safety message buffer.
  - When using external drives without NC axis assignment, then you must deactivate the safety message buffer (Page 374).
  - The response when saving safety-relevant messages relating to Basic Functions corresponds to the response for a deactivated safety message buffer (see below).
- If the safety message buffer is deactivated, then safety-relevant messages are saved in the standard fault and/or alarm buffer.
  - For safety-related messages in the fault and alarm buffer, in SINUMERIK Operate, specific reference is not made to the safety-relevant acknowledgment required.
    Safety-relevant alarms are displayed in SINUMERIK Operate in the standard alarm list ("MENU SELECT > Diagnostics > Alarms"); however, they require safety-relevant acknowledgment.
  - The messages require additional acknowledgment: For an entry in the fault buffer, in addition alarm 25201 ("Drive fault") is output, and the drive message requires a safety-relevant acknowledgment as well as also the acknowledgment via PROFIdrive (Page 378).

9.7.1 Configuring the standard alarm buffer

The standard alarm buffer is automatically activated when you configure the safety mode.

This alarm buffer is required for safety-related standard warnings (Axxxx).

The display of safety-related standard warnings cannot be activated independently of the display of other standard warnings.

The activation is entered in the following machine data:

- MD13150 $MN_SINAMICS_ALARM_MASK
  - "bit 2: output faults of the drive controls"
  - "bit 10: output alarms of the drive controls"

  Alarms/warnings have to be evaluated.
  Optionally, you can set additional bits in order to output faults or alarms of other DO groups.

9.7.2 Configuring the safety message buffer

The safety message buffer is activated in the factory setting, and is used for safety-related messages from Extended Functions.

Under certain circumstances it can also make sense to deactivate the safety message buffer for Extended Functions so that the messages of Basic Functions as well as those of Extended Functions are saved to the fault and/or alarm buffer (for example, if you are predominantly using Basic Functions).

The setting to activate/deactivate the safety message buffer is a CU parameter (p3117). It cannot be set on a drive-specific or axes-specific basis, but is always applicable for all drives and/or axes of this CU.

The following drive parameter is relevant:

- p3117 change safety message type/ Ch. SI mess type
  Setting to re-parameterize all safety messages to faults and alarms.

Precondition

- Settings for drive parameters are protected with access level 2 (service).

Procedure

Proceed as follows to deactivate or activate the safety message buffer:

1. In SINUMERIK Operate, call the drive parameters using "MENU SELECT > Commissioning > Machine data > Control Unit parameters".
2. Activate the CU commissioning state "Device configuration" with "p0009 = 1".

3. Set the required value in drive parameter p3117 Change safety message type / Ch. SI mess type:
   - p3117 = 0: Safety messages of this CU are not reparameterized; this means that messages associated with Extended Functions are entered in the safety message buffer.
   - p3117 = 1: All safety messages of this CU are reparameterized, and entered in the standard fault or alarm buffer.
4. Deactivate the CU commissioning state "Device configuration" with "p0009 = 0".
5. Confirm the setting with "Save/reset> Menu forward key> Reset (po)".

9.8 Acknowledgment

9.8.1 Overview

Most safety messages require safety-related acknowledgment.

Safety-related acknowledgment involves deleting safety-related messages of the drive-integrated monitoring functions via safety-related communication. With the safety-related acknowledgment, the fault case in the drive is marked as having been resolved (gone).

Safety-related acknowledgment is independent of the scope of the Safety Functions used (Basic or Extended) - and is required in addition to actually removing the cause of the fault.

Depending on the drive type, different types of acknowledgment and/or safety-related acknowledgment are possible:

Table 9-10 Permissible acknowledgment types for various drive types

Drive type	Permissible acknowledgment
Integrated drives (CU_I, CU_NX)	• Safety-related acknowledgment using PROFIsafe signal "IEACK" (Page 377) • Acknowledgment by switching-off/switching-on (Page 378)
External NC drives	• Safety-related acknowledgment using PROFIsafe signal "IEACK" (Page 377) • Acknowledgment by deselecting STO or SS1 (Page 378) • Acknowledgment by switching-off/switching-on (Page 378)
External SINAMICS drives without any assignment to an NC axis	The safety message buffer is not supported and must be deactivated (Page 374). The acknowledgment options correspond to those of external NC drives (see above).

Depending on what has been configured, additional acknowledgments may be necessary:

- If you are using Basic Functions, or the safety message buffer is deactivated (p3117 = 1), then you must additionally acknowledge (Page 378) all safety messages that are saved in the standard fault buffer using a PROFIdrive RESET.
- In addition to a safety-related acknowledgment, various fault situations also require an acknowledgment using a PROFIdrive RESET (Page 377).

⚠ **WARNING**

Unexpected restart for safety-related acknowledgment without MCP reset!

If a STOP response is acknowledged in a safety-related fashion by the machine operator, but without PROFIdrive RESET acknowledgment, then the part program is not canceled and is continued with the acknowledgment. When the machine restarts unexpectedly, this can put people in dangerous situations or cause material damage.

- In the safety program logically combine safe acknowledgment (PROFIsafe IEACK) with a RESET at the machine control panel (PROFIdrive RESET).

9.8.2 Acknowledgment via PROFIsafe

You program a PROFIsafe acknowledgment in the safety program of the F-PLC by setting signal "Internal Event ACK" separately for each drive object using the PROFIsafe telegram (STW bit 7).

Faults in the drive objects (DOs) cannot be acknowledged by the F-PLC in the line-up, but must instead be acknowledged separately for each individual drive object. A falling edge of the "Internal Event ACK" signal resets the status "Internal Event" in the particular drive, and thus acknowledges the fault.

9.8.3 Additional acknowledgment via PROFIdrive RESET

⚠ WARNING

Unexpected restart for safety-related acknowledgment without MCP reset!

If a STOP response is acknowledged in a safety-related fashion by the machine operator, but without PROFIdrive RESET acknowledgment, then the part program is not canceled and is continued with the acknowledgment. When the machine restarts unexpectedly, this can put people in dangerous situations or cause material damage.

- In the safety program logically combine safe acknowledgment (PROFIsafe IEACK) with a RESET at the machine control panel (PROFIdrive RESET).

In addition to a safety-relevant acknowledgment, various fault situations also require an acknowledgment using a PROFIdrive RESET.

This applies to the following STOP responses or safety functions:

- Extended Functions:
  - All fault situations - or safety functions and STOP responses
- Basic Functions or inactive safety message buffer:
  - Parameterizing SLS with STOP D or STOP E

In the case of a fault, if safety-relevant acknowledgment is realized without a PROFIdrive RESET, even though the part program remains in the stop state, the spindle starts again.

A configuration such as this is not in conformance with standard IEC 61800-5-2. According to the standard, a restart inhibit is required for all STOP functions, and it is only permissible that the spindle restarts after a RESET.

Therefore, in the safety program logically combine safety-relevant acknowledgment (PROFIsafe IEACK) with a RESET at the machine control panel (PROFIdrive RESET).

This means that you should configure the machine control panel RESET (MCP reset or channel/ MODE GROUP RESET) so that when actuated, a PROFIdrive RESET as well as a safety-relevant acknowledgment (e.g. PROFIsafe IEACK) are initiated.

9.8.4 Acknowledgment using POWER ON

Safety faults can also be acknowledged (as with all other faults) by switching the drive unit off and then on again (POWER ON).
If this action has not eliminated the fault cause, the fault is displayed again immediately after power-up.

9.8.5 Extended acknowledgment (deselecting STO/SS1)

For external drives, the extended alarm acknowledgment can be used as alternative to safety-relevant acknowledgment. To do this, the extended alarm acknowledgment must be activated in the safety configuration of the drive.

Extended alarm acknowledgment is not supported for integrated drives.

Basic procedure

If STO or SS1 is selected/deselected - and if p9507.0 is set = 1 - then the safety messages are automatically withdrawn.

- Remove the cause of the fault.
- Deselect "Safe Torque Off" (STO) or "Safe Stop 1" (SS1).
- Acknowledge the fault.

If, in addition to the "Basic Functions via terminals", the "Extended Functions" are also enabled, then acknowledgment is also possible by selecting/deselecting STO via PROFIsafe.

If the safety commissioning mode is exited when the safety functions are switched off (p0010 ≠ 95 when p9601 = 0), then all safety faults can be acknowledged.

Once safety commissioning mode has been selected again (p0010 = 95), all the faults that were previously present reappear.

9.8.6 Additional acknowledgment when the safety message buffer is inactive

If you are using Basic Functions or the safety message buffer is deactivated (p3117 = 1), then the safety messages are saved to the standard fault buffer or to the standard alarm buffer. These messages require a safety-relevant acknowledgment, even when the safety message buffer is deactivated.

In addition to safety-relevant acknowledgment, safety messages in the standard fault buffer require acknowledgment using PROFIdrive signal "Acknowledge faults" (PROFIdrive RESET). For NC axes, a PROFIdrive RESET corresponds to a machine control panel RESET.

The required PROFIdrive RESET is displayed in SINUMERIK Operate with NC alarm 25201.

When the safety message buffer is deactivated, the following safety messages are saved in the fault buffer, and therefore also additionally required a PROFIdrive RESET:

Table 9-11 Saving safety-relevant messages in the the fault buffer (when the safety message buffer is deactivated)

Alarm number (SINAMICS)	Alarm text
F01689	SI Motion: Axis re-configured
C01700	SI Motion P1 (CU): STOP A initiated
C01701	SI Motion P1 (CU): STOP B initiated
C01708	SI Motion P1 (CU): STOP C initiated
C01770	SI Motion P1 (CU): Discrepancy error of the failsafe digital inputs/outputs

When the safety message buffer is deactivated, all of the safety messages listed in the table are saved in the standard alarm buffer.

Component replacement (software/hardware) 10

⚠ WARNING

Unsafe operating state after POWER ON

After a firmware update, the system generally requests a POWER ON. After a POWER ON, an unsafe operating state can occur - and if persons are in the hazardous area, this can result in death or severe injury.

- After each POWER ON, perform an acceptance test and create an acceptance report.
- Do not enter the danger zone of the motor until the acceptance test has been successfully completed.

⚠ WARNING

Unwanted motion if components are replaced without a function test

After a component replacement, connections or functions can be defective so that death or serious injury can result if a person enters the danger zone of the motors.

- Perform a POWER ON before resuming operation.
- After component replacement, always run a simplified function test.
  More detailed information can be found in Chapter "Acceptance test (Page 345)".

10.1 Software, F-CPU, F-I/O

Replacement of software components

When replacing software components on your PG/PC, e.g. when installing a new version of STEP 7, you must carefully observe the notes regarding upward and downward compatibility in the documentation and in the readme files provided with these products.

Replacement of hardware components

Hardware components for SIMATIC Safety (F-CPU, F-I/O, batteries, etc.) are replaced in the same way as in standard automation systems.

Removing and inserting F-I/O during operation

It is possible to remove and insert F-I/O during operation, as with standard F-I/O. However, be aware that replacing an F-I/O module during operation can cause a communication error in the F-CPU.

You must acknowledge communication errors in your safety program at variables ACK_REI of the F-I/O DB - or alternatively, using instruction "ACK_GL". Without an acknowledgment, the F-I/O will remain passivated.

CPU firmware update

Check of the CPU operating system for F-approval: When using a new CPU operating system (firmware update), you must check to see if the CPU operating system you are using is approved for use in an F-system.

The minimum CPU operating system versions with guaranteed F-capability are specified in the appendix of the Certificate. This information and any notes on the new CPU operating system must be taken into account.

Firmware update for interface module

When using a new operating system for an interface module, e.g. IM 151-1 HIGH FEATURE ET 200S (firmware update), you must observe the following:

When updating the firmware (see help for STEP 7 "Online & Diagnostics"), if you selected option "Activate firmware after update", then after the firmware has been successfully loaded, the IM is automatically reset, and then runs with the new operating system. Note that the firmware update for interface modules during operation generates a communication error in the F-CPU.

You must acknowledge communication errors in your safety program at variables ACK_REI of the F-I/O DBs - or alternatively, using instruction "ACK_GL". Without an acknowledgment, the F-I/O will remain passivated.

Preventive maintenance (proof test)

The probability values for the certified F-system components guarantee a proof-test interval of 20 years for ordinary configurations.

Proof test for complex electronic components generally means replacement with unused components.

PFD, PFH values for F-CPU S7-1500

Probability of failure values (PFD_{avg}-, PFH values) for F-CPU S7-1500 for a usage time of 20 years and for a repair time of 100 hours are subsequently listed:

Low demand mode of operation **low demand mode** **According to IEC 61508:2010:** **PFD_{avg} = Average probability of a dangerous failure on demand**	**High demand or continuous mode of operation** **high demand/continuous mode** **According to IEC 61508:2010:** **PFH = Average frequency of a dangerous failure [h^{-1}]**
< 2E-05	< 1E-09

PFD, PFH values for safety-related communication

Below you will find the failure probability values (PFD_{avg}, PFH values) for safety-related communication:

Low demand mode of operation **low demand mode** **According to IEC 61508:2010:** **PFD_{avg} = Average probability of a dangerous failure on demand**	**High demand or continuous mode of operation** **high demand/continuous mode** **According to IEC 61508:2010:** **PFH = Average frequency of a dangerous failure [h^{-1}]**
< 1E-05	< 1E-09

10.2 SINAMICS components

Note

Note additional safety instructions

Observe the instructions with regard to changing or replacing software components in Section "Safety instructions (Page 381)"!

Overview

The faulty component was replaced according to safety regulations. The information relevant from the perspective of Safety Integrated is provided in the following. For information about component replacement, see "Component replacement" in the SINAMICS S120 Function Manual Drive Functions.

- Based on the NodeID and the saved CRC of the particular hardware component, the drive identifies that a component has been replaced. You can take the responses of the drive and the actions that have to be carried out from the following table:

	Replaced component	Control type	Drive response (fault)	User action			Diagnostic parameters
				Fault acknowledgment required[1)]	Acknowledgment is required that the component has been replaced[2)]	Save[3)]	
Basic Functions	Control Unit	All	F01641.0 = 1	Yes	No	Yes	r9776.2 = 1
	Motor Module	All	F01641.1 = 1	Yes	No	Yes	r9776.2 = 1
	Power Module	All	F01641.2 = 1	Yes	No	Yes	r9776.2 = 1

	Replaced component	Control type	Drive response (fault)	User action			Diagnostic parameters
				Fault acknowledgment required[1)]	Acknowledgment is required that the component has been replaced[2)]	Save[3)]	
Extended Functions	Control Unit	All	F01641.0 = 1	Yes	No	Yes	r9776.2 = 1
	Motor Module	PROFIsafe, OnBoard F-DI, without selection	F01641.1 = 1	Yes	No	Yes	r9776.2 = 1
	Power Module	All	F01641.2 = 1	Yes	No	Yes	r9776.2 = 1
	Sensor Module (CPU 1)	All	F01641.3 = 1	Yes	No	Yes	r9776.2 = 1
	Sensor Module (CPU 2)	All	F01640.4 = 1	Yes	Yes	Yes	r9776.2 = 1 r9776.3 = 1
	Encoder[4)]	All	F01641.5 = 1 F01641.6 = 1	Yes	No	Yes	r9776.2 = 1

1) The fault must be acknowledged each time a component is replaced using a standard acknowledgment (e.g. using a 0/1 signal at p2103). However, even without acknowledgment the drive can still be operated.

2) The replacement of the components listed in the table must be acknowledged in order to ensure the new internal device communications to be established. When replacing other components, acknowledgment is not required, as the new communications to be established are automatically ensured.
To acknowledge a component replacement, perform the following sequence on all of the drive objects involved:
- Check whether the following preconditions are fulfilled:
  - p0010 = 0
  - It is not permissible for a firmware update to be active on the drive object.
- Set p9702 = 29 (= 1D hex)

3) The modified data must be saved after a component has been replaced:
- It is not permissible for a firmware update to be active on the drive object.
- Copy from RAM to ROM.
If the data is not saved, the fault is output again after the next POWER ON.

4) Only for encoders with serial number (e.g. EnDat)

Replacing motors for safety without encoder

When using safety functions without encoder, the motor pole pair number plays a decisive role. If a motor is replaced, then the behavior depends on the pole pair number: If a motor with a higher pole pair number is used (other than that configured), the mechanical speed is less than that calculated by Safety Integrated. If a motor with a lower pole pair number is used (e.g. when a motor is replaced), the mechanical speed is higher than that calculated by Safety Integrated.

- After a replacement such as this, perform a test by comparing the safe actual speed (r9714) with the normal speed (r0063 or the output frequency), and if required, correct the configured pole pair number.

10.3 Messages when components are replaced after Safety Integrated has been commissioned

> ⚠ **WARNING**
>
> **Unsafe states after a component has been replaced**
>
> Non-safe states are possible after a component has been replaced. If persons are in the danger zone, accidents causing death or severe injury can occur.
>
> - Before re-entering the danger zone - and before resuming operation - perform a simplified function test for the drive affected by the component replacement (see Chapter "Acceptance test (Page 345)").

Safety-related components are assigned a CRC checksum, which can be used to identify if the hardware was changed:

- Replacing certain drive components after Safety Integrated has been commissioned.
- Different checksums as a result of series commissioning with Safety Integrated functionality

The appropriate messages are displayed, depending on the components involved and the control type:

Control type	Alarm
Extended Functions via PROFIsafe	F01650 SI P1 (CU): Acceptance test required Fault value 2005 Indicates that the Control Unit has been replaced.
	A01695 SI Motion: Sensor Module has been replaced Indicates that the Sensor Module has been replaced.
	C30711 SI Motion P2: Defect in a monitoring channel Fault value 1031 Stop response STOP F As a consequence of A01695, a defect is signaled in a monitoring channel.

Procedure

Use the following function in SINUMERIK Operate to acknowledge a CRC checksum that differs for one of the reasons listed above:

- Commissioning > Safety Integrated > Overview > Confirm SI hardware

10.4 Important parameters

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9670 SI module identifier Control Unit
- p9671[0...n] SI module identifier, Motor Module
- p9672 SI module identifier, Power Module
- p9673 SI module identifier, Sensor Module channel 1
- p9674 SI module identifier, Sensor Module channel 2
- p9675 SI module identification sensor channel 1
- p9676 SI module identification sensor channel 2
- p9702 Acknowledge SI component replacement
- r9776 BO: SI diagnostics
- r9793[0...9] SI diagnostics component replacement

11 Data descriptions

11.1 Machine data

Table 11-1 Machine data with settings for the Safety Integrated mode

Number	Symbolic name	Purpose
MD36933	$MA_SAFE_DES_VELO_LIMIT	Evaluation factors to define the setpoint limits
MD36964	$MA_SAFE_IPO_STOP_GROUP	Channel-wide IPO response distribution
MD36968.2	$MA_SAFE_BRAKETEST_CONTROL, bit 2	Positioning behavior after completion of SBT
MD37950	$MA_SAFE_INFO_ENABLE	SIC/SCC enable
MD37954	$MA_SAFE_INFO_MODULE_NR	Number to select a logical basis address from MD13374

Table 11-2 Machine data with I/O addresses of safety-relevant telegrams

Number	Symbolic name	Purpose
MD13374	$MN_SAFE_INFO_DRIVE_LOGIC_ ADDR[0..30]	I/O start address of SIEMENS telegrams 701 (SIC/SCC) of the corresponding drive object
MD13376	$MN_SAFE_INFO_TELEGRAM_ TYPE[0..30]	Telegram type that is used for SIC/SCC communication. The default value (701) corresponds to the default in the TIA Portal configuration

Table 11-3 Machine data with safety-relevant settings for alarms/messages

Number	Symbolic name	Purpose
MD13140	$MN_PROFIBUS_ALARM_ACCESS	Alarm response of the PROFIBUS/PROFINET drives during run-up
MD13150	$MN_SINAMICS_ALARM_MASK	Activation/deactivation of interference and alarm buffer output of specific DO groups (for not NC-controlled axes)

Additional information

- More detailed information on parameterizing, searching and filtering machine data in SINUMERIK Operate can be found in documents SINUMERIK 840D sl Basic Software and Operating Software, Commissioning Manual SINUMERIK Operate (IM9), Chapter Machine and setting data.
- General information on all of the machine data is provided in the SINUMERIK 840D sl List Manual, Detailed Description of the Machine Data (AMDsl) - or in the online help for SINUMERIK Operate.

11.2 NC variables

Note

Information for those switching over from a different system: Different use of NC variables (OPI)

Only variables "vaStopSi", "aStopesi" and "safeDesVeloLimit" are used in the two Safety Integrated operating modes. All other safety-related NC variables are specific to an operating mode - and are not supplied in the two operating modes.

Safety-related NC variables (OPI) are available in the "Safety Integrated" mode; to a large extent, these are mapped using SIC signals.

Table 11-4 Safety-related NC variables available

Block	index	Name	Meaning
S	183	aStopesi	Actual Safety Integrated Stop E for any axis.
SEMA	214	vaStopSi	Safety Integrated stop.
SEMA	119	safeDesVeloLimit	Effective speed setpoint limit in the NC. This is obtained from a speed setpoint limit in the drive and a (possibly) active speed setpoint limit in the NC.
SEMA	277	safeAxisType	Type of axis-specific safety monitoring functions (safety axis operating mode).
SEMA	306	diagSlopeTime	Expected braking time of the axis/spindle that has been determined
S	358	safeMode	Configured Safety Integrated operating mode.

More information

You can find additional information about SINUMERIK NC variables in the:

(840D sl) List Manual NC Variables (https://support.industry.siemens.com/cs/ww/en/view/109769139)

11.3 System variables

Note

Information for those switching over from a different system: System variables available in the "Safety Integrated" mode

Only variables "$VA_STOPSI" and "$A_STOPESI" listed here are used in both Safety Integrated operating modes. All of the other system variables known from the "SINUMERIK Safety Integrated mode (SPL)" are not supplied in the "Safety Integrated" mode.

Safety-related system variables are available in the "Safety Integrated" mode, which are mapped using SIC signals (interface, NC/PLC-DRIVE):

- $VA_STOPSI
- $A_STOPESI
- $VA_SAFE_TYPE

$VA_STOPSI - actual STOP

Axis-specific system variable that includes the present stop. For a value of 4, a STOP E is active for this axis.

$V_STOPESI - actual STOP E

Global system variable that with a value not equal to 0 indicates that a STOP E is active for one particular axis.

$VA_SAFE_TYPE - axial Safety Integrated operating mode

Global system variable. It indicates whether Safety Integrated motion monitoring is active for the active axis; if yes, whether it involves motion monitoring integrated in the NC or drive-based motion monitoring.

Additional information

Additional information about SINUMERIK system variables is available in the:

(840D sl) List Manual System Variables (https://support.industry.siemens.com/cs/ww/en/view/109769180)

11.4 Standard telegram start addresses

Table 11-5 I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	5800	13374[0]
	SIEMENS telegram 902/903	6700	
DriveAxis02	SIEMENS telegram 701	5816	13374[1]
	SIEMENS telegram 902/903	6716	
DriveAxis03	SIEMENS telegram 701	5832	13374[2]
	SIEMENS telegram 902/903	6732	
DriveAxis04	SIEMENS telegram 701	5848	13374[3]
	SIEMENS telegram 902/903	6748	
DriveAxis05	SIEMENS telegram 701	5864	13374[4]
	SIEMENS telegram 902/903	6764	
DriveAxis06	SIEMENS telegram 701	5880	13374[5]
	SIEMENS telegram 902/903	6780	

Table 11-6 NX on DRIVE-CLiQ socket X105; DP address 15: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	5896	13374[6]
	SIEMENS telegram 902/903	6796	
DriveAxis02	SIEMENS telegram 701	5912	13374[7]
	SIEMENS telegram 902/903	6812	
DriveAxis03	SIEMENS telegram 701	5928	13374[8]
	SIEMENS telegram 902/903	6828	
DriveAxis04	SIEMENS telegram 701	5944	13374[9]
	SIEMENS telegram 902/903	6844	
DriveAxis05	SIEMENS telegram 701	5960	13374[10]
	SIEMENS telegram 902/903	6860	
DriveAxis06	SIEMENS telegram 701	5976	13374[11]
	SIEMENS telegram 902/903	6876	

Table 11-7 NX on DRIVE-CLiQ socket X104; DP address 14: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
		Standard addressing schematic	
DriveAxis01	SIEMENS telegram 701	5992	13374[12]
	SIEMENS telegram 902/903	6892	
DriveAxis02	SIEMENS telegram 701	6008	13374[13]
	SIEMENS telegram 902/903	6908	
DriveAxis03	SIEMENS telegram 701	6024	13374[14]
	SIEMENS telegram 902/903	6924	

Drive	Telegram type	I/O start address	Machine data
		Standard addressing schematic	
DriveAxis04	SIEMENS telegram 701	6040	13374[15]
	SIEMENS telegram 902/903	6940	
DriveAxis05	SIEMENS telegram 701	6056	13374[16]
	SIEMENS telegram 902/903	6956	
DriveAxis06	SIEMENS telegram 701	6072	13374[17]
	SIEMENS telegram 902/903	6972	

Table 11-8 NX on DRIVE-CLiQ socket X103; DP address 13: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	6088	13374[18]
	SIEMENS telegram 902/903	6988	
DriveAxis02	SIEMENS telegram 701	6104	13374[19]
	SIEMENS telegram 902/903	7004	
DriveAxis03	SIEMENS telegram 701	6120	13374[20]
	SIEMENS telegram 902/903	7020	
DriveAxis04	SIEMENS telegram 701	6136	13374[21]
	SIEMENS telegram 902/903	7036	
DriveAxis05	SIEMENS telegram 701	6152	13374[22]
	SIEMENS telegram 902/903	7052	
DriveAxis06	SIEMENS telegram 701	6168	13374[23]
	SIEMENS telegram 902/903	7068	

Table 11-9 NX on DRIVE-CLiQ socket X102; DP address 12: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	6184	13374[24]
	SIEMENS telegram 902/903	7084	
DriveAxis02	SIEMENS telegram 701	6200	13374[25]
	SIEMENS telegram 902/903	7100	
DriveAxis03	SIEMENS telegram 701	6216	13374[26]
	SIEMENS telegram 902/903	7116	
DriveAxis04	SIEMENS telegram 701	6232	13374[27]
	SIEMENS telegram 902/903	7132	
DriveAxis05	SIEMENS telegram 701	6248	13374[28]
	SIEMENS telegram 902/903	7148	
DriveAxis06	SIEMENS telegram 701	6264	13374[29]
	SIEMENS telegram 902/903	7164	

Table 11-10 NX on DRIVE-CLiQ socket X101; DP address 11: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	6280	13374[30]
	SIEMENS telegram 902/903	7180	
DriveAxis02	SIEMENS telegram 701	6296	13374[31]
	SIEMENS telegram 902/903	7196	
DriveAxis03	SIEMENS telegram 701	6312	13374[32]
	SIEMENS telegram 902/903	7212	
DriveAxis04	SIEMENS telegram 701	6328	13374[33]
	SIEMENS telegram 902/903	7228	
DriveAxis05	SIEMENS telegram 701	6344	13374[34]
	SIEMENS telegram 902/903	7244	
DriveAxis06	SIEMENS telegram 701	6360	13374[35]
	SIEMENS telegram 902/903	7260	

Table 11-11 NX on DRIVE-CLiQ socket X100; DP address 10: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address	Machine data
DriveAxis01	SIEMENS telegram 701	6376	13374[36]
	SIEMENS telegram 902/903	7276	
DriveAxis02	SIEMENS telegram 701	6392	13374[37]
	SIEMENS telegram 902/903	7292	
DriveAxis03	SIEMENS telegram 701	6408	13374[38]
	SIEMENS telegram 902/903	7308	
DriveAxis04	SIEMENS telegram 701	6424	13374[39]
	SIEMENS telegram 902/903	7324	
DriveAxis05	SIEMENS telegram 701	6440	13374[40]
	SIEMENS telegram 902/903	7340	
DriveAxis06	SIEMENS telegram 701	6456	13374[41]
	SIEMENS telegram 902/903	7356	

11.5 Telegram structure and data

11.5.1 PROFIsafe telegram 30

Telegram 30 transfers as user data safety control word 1 (S_STW1) and safety status word 1 (S_ZSW1).

Table 11-12 PROFIsafe telegram 30 (telegram structure)

	Output data	Input data
PZD1	S_STW1	S_ZSW1

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

11.5.2 PROFIsafe telegram 31

Telegram 31 transfers safety control word 2 (S_STW2) and safety status word 2 (S_ZSW2) as user data. It is structured as follows:

Table 11-13 PROFIsafe telegram 31 (telegram structure)

	Output data	Input data
PZD1	S_STW2	S_ZSW2
PZD2		

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

11.5.3 SIEMENS telegram 701

The predefined PROFIdrive telegram 701 is available for transferring SIC and SCC:

Table 11-14 SIEMENS telegram 701 (telegram structure)

	Receive data	Parameter	Send data	Parameter
PZD1	S_STW1B	p10250	S_ZSW1B	r9734
PZD2	S_STW3B	p10235	S_ZSW2B	r9743
PZD3	–	–	S_V_LIMIT_B	r9733[2]
PZD4	–	–		
PZD5	–	–	S_ZSW3B	r10234

Detailed information about the process data of telegram 701 is provided in Chapter "SIC/SCC (PROFIdrive) process data (Page 414)".

Note

Update of the send data

The send data S_ZSW1B, S_ZSW2B, S_ZSW3B and S_V_LIMIT_B is only updated if the Safety Integrated Extended Functions are enabled.

Additional information

Additional information regarding communication via PROFIdrive is available in "Communication according to PROFIdrive" in the

SINAMICS S120 Communication Function Manual

11.5.4 SIEMENS telegram 901

Telegram 901 transfers the S_STW2, the variable SLS limit (S_SLS_LIMIT_A), the S_ZSW2, the active SLS value of level 1 (S_SLS_LIMIT_A_ACTIVE), a counter value (S_CYCLE_COUNT) and the safe position value in 16-bit format (S_XIST16) as user data.

Table 11-15 SIEMENS telegram 901 (telegram structure)

	Output data	Input data
PZD1	S_STW2	S_ZSW2
PZD2		
PZD3	S_SLS_LIMIT_A	S_SLS_LIMIT_A_ACTIVE
PZD4	–	S_CYCLE_COUNT
PZD5	–	S_XIST16

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

11.5.5 SIEMENS telegram 902

Telegram 902 transfers as user data S_STW2, the variable SLS limit (S_SLS_LIMIT_A), the S_ZSW2, the active SLS value of level 1 (S_SLS_LIMIT_A_ACTIVE), a counter value (S_CYCLE_COUNT) and the safe position value in 32-bit format (S_XIST32).

Table 11-16 SIEMENS telegram 902 (telegram structure)

	Output data	Input data
PZD1	S_STW2	S_ZSW2
PZD2		
PZD3	S_SLS_LIMIT_A	S_SLS_LIMIT_A_ACTIVE
PZD4	–	S_CYCLE_COUNT
PZD5	–	S_XIST32
PZD6		

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

11.5.6 SIEMENS telegram 903

Telegram 903 transfers the following user data: S_STW2, S_SLS_LIMIT_A, S_ZSW2, S_ZSW_CAM1 and S_SLS_LIMIT_A_ACTIVE.

Table 11-17 SIEMENS telegram 903 (telegram structure)

	Output data	Input data
PZD1	S_STW2	S_ZSW2
PZD2		
PZD3	S_SLS_LIMIT_A	S_ZSW_CAM1
PZD4	–	
PZD5	–	S_SLS_LIMIT_A_ACTIVE

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

11.6 Process data

11.6.1 Overview: Process data in telegrams

Table 11-18 Process data from PROFIsafe telegrams

Telegram Process data	30	31	901	902	903
Safety control word 1 S_STW1	PZD1	–	–	–	–
Safety status word 1 S_ZSW1	PZD1	–	–	–	–
Safety control word 2 S_STW2	–	PZD1...2	PZD1...2	PZD1...2	PZD1...2
Safety status word 2 S_ZSW2	–	PZD1...2	PZD1...2	PZD1...2	PZD1...2
SLS limit value input S_SLS_LIMIT_A	–	–	PZD3	PZD3	PZD3
Active SLS limit value S_SLS_LIMIT_A_ACTIVE	–	–	PZD3	PZD3	PZD5
Counter for the safety cycle S_CYCLE_COUNT	–	–	PZD4	PZD4	–
Actual position value (16 bits) S_XIST16	–	–	PZD5	–	–
Actual position value (32 bits) S_XIST32	–	–	–	PZD5...6	–
Safe Cam status word S_ZSW_CAM1	–	–	–	–	PZD3...4

Detailed information about the process data of these telegrams is provided in Chapter "PROFIsafe process data (Page 399)".

Table 11-19 Process data from SIEMENS telegram 701 (SIC/SCC)

Telegram Process data	701
Safety Control Channel control word 1 S_STW1B	PZD1
SI Motion Safety Info Channel status word S_ZSW1B	PZD1
Safety Info Channel status word 2 S_ZSW2B	PZD2
Safety Control Channel control word 3 S_STW3B	PZD2

Telegram Process data	701
SLS setpoint speed limiting (32 bit) S_V_LIMIT_B	PZD3...4
Safety Info Channel status word 3 S_ZSW3B	PZD5

Detailed information about the process data of telegram 701 is provided in Chapter "SIC/SCC (PROFIdrive) process data (Page 414)".

11.6.2 PROFIsafe process data

Note

Additional information in the function block diagrams

Generally, for the subsequent descriptions, reference is made to a function block diagram. You can find the function block diagram mentioned in the SINAMICS S120/S150 List Manual.

Note

Reserved control/status bits

A series of control and/or status bits are listed as reserved in the following tables. The reason for this is that various Safety Integrated Functions will only be implemented at a later point in time. The bits are reserved for future functions.

11.6.2.1 S_STW1: Safety control word 1

S_STW1 (Basic Functions)

Safety control word 1 (S_STW1)

S_STW1, output signals
see function chart [2806].

Table 11-20 Description of safety-control word1 (S_STW1)

Byte	Bit	Meaning	Remarks	
0	0	STO	1	Deselect STO
			0	Select STO
	1	SS1	1	Deselect SS1
			0	Select SS1
	2	SS2	0	–[1)]
	3	SOS	0	–[1)]
	4	SLS	0	–[1)]
	5	Reserved	–	–
	6	SLP	0	–[1)]
	7	Internal Event ACK	1/0	Acknowledgment
			0	No acknowledgment
1	0	SLA	0	–[1)]
	1	Select SLS bit 0	0	–[1)]
	2	Select SLS bit 1	0	
	3	Reserved	–	–
	4	SDI positive	0	–[1)]
	5	SDI negative	0	
	6, 7	Reserved	–	–

1) Signals not relevant for Basic Functions: Should be set to "0".

S_STW1 (Extended Functions)

Safety control word 1 (S_STW1)

S_STW1, output signals
see function chart [2842].

Table 11-21 Description of safety-control word1 (S_STW1)

Byte	Bit	Meaning	Remarks	
0	0	STO	1	Deselect STO
			0	Select STO
	1	SS1	1	Deselect SS1
			0	Select SS1
	2	SS2	1	Deselect SS2
			0	Select SS2
	3	SOS	1	Deselect SOS
			0	Select SOS
	4	SLS	1	Deselect SLS
			0	Select SLS
	5	Reserved	–	–
	6	SLP[1)]	1	Deselect SLP
			0	Select SLP
	7	Internal Event ACK	1/0	Acknowledgment
			0	No acknowledgment
1	0	SLA	1	Deselect SLA
			0	Select SLA
	1	Select SLS bit 0	–	Selection of the speed limit for SLS (2 bits)
	2	Select SLS bit 1	–	
	3	Reserved	–	–
	4	SDI positive	1	Deselect SDI positive
			0	Select SDI positive
	5	SDI negative	1	Deselect SDI negative
			0	Select SDI negative
	6, 7	Reserved	–	–

1) Signals not relevant for Extended Functions: Must not be evaluated.

11.6.2.2 S_ZSW1: Safety status word 1

S_ZSW1 (Basic Functions)

Safety status word 1 (S_ZSW1)

S_ZSW1, input signals
see function diagram [2806].

Table 11-22 Description of safety status word 1 (S_ZSW1)

Byte	Bit	Meaning	Remarks	
0	0	STO active	1	STO active
			0	STO not active
	1	SS1 active	1	SS1 active
			0	SS1 not active
	2	SS2 active	0	–[1]
	3	SOS active	0	–[1]
	4	SLS active	0	–[1]
	5	Reserved	–	–
	6	SLP active	0	–[1]
	7	Internal Event	1	Internal event
			0	No internal event
1	0	SLA active	0	–[1]
	1	Active SLS level bit 0	0	–[1]
	2	Active SLS level bit 1	0	
	3	SOS selected	0	–[1]
	4	SDI positive active	0	–[1]
	5	SDI negative active	0	–[1]
	6	Reserved	–	–
	7	SSM (speed below limit value)	0	–[1]

[1] Signals not relevant for Basic Functions: Must not be evaluated.

S_ZSW1 (Extended Functions)

Safety status word 1 (S_ZSW1)

S_ZSW1, input signals
see function diagram [2842].

Table 11-23 Description of safety status word 1 (S_ZSW1)

Byte	Bit	Meaning	Remarks	
0	0	STO active	1	STO active
			0	STO not active
	1	SS1 active	1	SS1 active
			0	SS1 not active
	2	SS2 active	1	SS2 active
			0	SS2 not active
	3	SOS active	1	SOS active
			0	SOS not active
	4	SLS active	1	SLS active
			0	SLS not active
	5	Reserved	–	–
	6	SLP active[1)]	1	SLP active
			0	SLP not active
			–	The status signal "SLP active" is not the same as the diagnostic signal "SLP active" (r9722.6), but is the AND logic operation of "SLP active" (r9722.6) and "safely referenced" (r9722.23).
	7	Internal Event	1	Internal event
			0	No internal event
1	0	SLA active	1	SLA active
			0	SLA not active
	1	Active SLS level bit 0	–	Display of the speed limit for SLS (2 bits)
	2	Active SLS level bit 1	–	
	3	SOS selected	1	SOS selected
			0	SOS deselected
	4	SDI positive active	1	SDI positive active
			0	SDI positive not active
	5	SDI negative active	1	SDI negative active
			0	SDI negative not active
	6	Reserved	–	–
	7	SSM (speed)	1	SSM (speed below limit value)
			0	SSM (speed higher than/equal to limit)

1) Signals not relevant for Extended Functions: Must not be evaluated.

11.6.2.3 S_STW2: Safety control word 2

S_STW2 (Basic Functions)

Safety control word 2 (S_STW2)

S_STW2, output signals
see function diagram [2806].

Table 11-24 Description of safety-control word 2 (S_STW2)

Byte	Bit	Meaning	Remarks	
0	0	STO	1	Deselect STO
			0	Select STO
	1	SS1	1	Deselect SS1
			0	Select SS1
	2	SS2	0	–[1)]
	3	SOS	0	–[1)]
	4	SLS	0	–[1)]
	5	Reserved	–	–
	6	SLP	0	–[1)]
	7	Internal Event ACK	1/0	Acknowledgment
			0	No acknowledgment
1	0	SLA active	0	–[1)]
	1	Select SLS bit 0	0	–[1)]
	2	Select SLS bit 1	0	
	3	Reserved	–	–
	4	SDI positive	0	–[1)]
	5	SDI negative	0	–[1)]
	6, 7	Reserved	–	–
2	0 ... 2	Reserved	–	–
	3	Select SLP position range	0	–[1)]
	4 ... 6	Reserved	–	–
	7	SCA	0	–[1)]
3	0	Select gearbox stage, bit 0	0	–[1)]
	1	Select gearbox stage, bit 1	0	–[1)]
	2	Select gearbox stage, bit 2	0	–[1)]
	3	Gearbox stage switchover	0	–[1)]
	4	SS2E	0	–[1)]
	5	SS2ESR	0	–[1)]
	6, 7	Reserved	–	–

1) Signals not relevant to Basic Functions should be set to "0".

S_STW2 (Extended Functions)

Safety control word 2 (S_STW2)

S_STW2, output signals
see function diagram [2843].

Table 11-25 Description of safety-control word 2 (S_STW2)

Byte	Bit	Meaning	Remarks	
0	0	STO	1	Deselect STO
			0	Select STO
	1	SS1	1	Deselect SS1
			0	Select SS1
	2	SS2	1	Deselect SS2
			0	Select SS2
	3	SOS	1	Deselect SOS
			0	Select SOS
	4	SLS	1	Deselect SLS
			0	Select SLS
	5	Reserved	–	–
	6	SLP	1	Deselect SLP
			0	Select SLP
	7	Internal Event ACK	1/0	Acknowledgment
			0	No acknowledgment
1	0	SLA	1	Deselect SLA
			0	Select SLA
	1	Select SLS bit 0	–	Selection of the speed limit for SLS (2 bits)
	2	Select SLS bit 1	–	
	3	Reserved	–	–
	4	SDI positive	1	Deselect SDI positive
			0	Select SDI positive
	5	SDI negative	1	Deselect SDI negative
			0	Select SDI negative
	6, 7	Reserved	–	–
2	0 … 2	Reserved	–	–
	3	Select SLP position range[1)]	1	Select SLP area 2 (SLP2)
			0	Select SLP area 1 (SLP1)
	4 … 6	Reserved	–	–
	7	SCA	1	Deselect SCA
			0	Select SCA

Byte	Bit	Meaning	Remarks	
3	0	Select gearbox stage, bit 0	–	Select gearbox stage (3 bits)
	1	Select gearbox stage, bit 1	–	
	2	Select gearbox stage, bit 2	–	
	3	Gearbox stage switchover	1	With increased position tolerance
			0	Without increased position tolerance
	4	SS2E	1	Deselect SS2E
			0	Select SS2E
	5	SS2ESR	1	Deselect SS2ESR
			0	Select SS2ESR
	6, 7	Reserved	–	–

1) Signals not relevant for Extended Functions: Must not be evaluated.

11.6.2.4 S_ZSW2: Safety status word 2

S_ZSW2 (Basic Functions)

Safety status word 2 (S_ZSW2)

S_ZSW2, input signals
see function diagram [2806].

Table 11-26 Description of safety status word 2 (S_ZSW2)

Byte	Bit	Meaning	Remarks	
0	0	STO active	1	STO active
			0	STO not active
	1	SS1 active	1	SS1 active
			0	SS1 not active
	2	SS2 active	0	–[1)]
	3	SOS active	0	–[1)]
	4	SLS active	0	–[1)]
	5	Reserved	–	–
	6	SLP active	0	–[1)]
	7	Internal Event	1	Internal event
			0	No internal event

Byte	Bit	Meaning	Remarks	
1	0	SLA active	0	–[1]
	1	Active SLS level, bit 0	0	–[1]
	2	Active SLS level, bit 1	0	
	3	Reserved	–	–
	4	SDI positive active	0	–[1]
	5	SDI negative active	0	–[1]
	6	Reserved	–	–
	7	SSM (speed)	0	–[1]
2	0 ... 2	Reserved	–	–
	3	SLP active position range	0	–[1]
	4, 5	Reserved	–	–
	6	Safe position valid	0	–[1]
	7	Safely referenced	0	–[1]
3	0 ... 2	F-DI 0 ... 2[2]	0	–[1]
	3	SS2ESR active	0	–[1]
	4	SS2E active	0	–[1]
	5	SOS selected	0	–[1]
	6	SLP upper limit maintained	0	–[1]
	7	SLP lower limit maintained	0	–[1]

[1] Signals not relevant for Basic Functions: Must not be evaluated.

[2] Only valid for CU310-2.

S_ZSW2 (Extended Functions)

Safety status word 2 (S_ZSW2)

S_ZSW2, input signals
see function diagram [2843].

Table 11-27 Description of safety status word 2 (S_ZSW2)

Byte	Bit	Meaning	Remarks	
0	0	STO active	1	STO active
			0	STO not active
	1	SS1 active	1	SS1 active
			0	SS1 not active
	2	SS2 active	1	SS2 active
			0	SS2 not active
	3	SOS active	1	SOS active
			0	SOS not active
	4	SLS active	1	SLS active
			0	SLS not active
	5	Reserved	–	–
	6	SLP active[1]	1	SLP active
			0	SLP not active
			–	The status signal "SLP active" is not the same as the diagnostic signal "SLP active" (r9722.6), but is the AND logic operation of "SLP active" (r9722.6) and "safely referenced" (r9722.23).
	7	Internal Event	1	Internal event
			0	No internal event
1	0	SLA active	1	SLA active
			0	SLA not active
	1	Active SLS level bit 0	–	Display of the speed limit for SLS (2 bits)
	2	Active SLS level bit 1	–	
	3	Reserved	–	–
	4	SDI positive active	1	SDI positive active
			0	SDI positive not active
	5	SDI negative active	1	SDI negative active
			0	SDI negative not active
	6	Reserved	–	–
	7	SSM (speed)	1	SSM (speed below limit value)
			0	SSM (speed higher than/equal to limit)

Byte	Bit	Meaning	Remarks	
2	0 … 2	Reserved	–	–
	3	SLP active position range[1)]	1	SLP area 2 (SLP2) active
			0	SLP area 1 (SLP1) active
			-	The status signal "SLP active position range" always corresponds to the diagnostic signal "SLP active position range" (r9722.19).
	4, 5	Reserved	-	-
	6	Safe position valid	1	Safe position valid
			0	Safe position invalid
	7	Safely referenced	1	Safe position is applicable as "safely referenced"
			0	Safe position is not applicable as "safely referenced"

1) Signals not relevant for Extended Functions: Must not be evaluated.

Byte	Bit	Meaning	Remarks	
3	0	F-DI 0[2)]	1	F-DI 0 inactive
			0	F-DI 0 active
	1	F-DI 1[2)]	1	F-DI 1 inactive
			0	F-DI 1 active
	2	F-DI 2[2)]	1	F-DI 2 inactive
			0	F-DI 2 active
	3	SS2ESR active	1	SS2ESR active
			0	SS2ESR not active
	4	SS2E active	1	SS2E active
			0	SS2E not active
	5	SOS selected	1	SOS selected
			0	SOS deselected
	6	SLP upper limit maintained	1	SLP: Upper limit maintained
			0	SLP: Upper limit not maintained
			–	The status signal "upper SLP limit maintained" always corresponds to the diagnostic signal "upper SLP limit maintained" (r9722.30).
	7	SLP lower limit maintained	1	SLP: Lower limit maintained
			0	SLP: Lower limit not maintained
			–	The status signal "lower SLP limit maintained" always corresponds to the diagnostic signal "lower SLP limit maintained" (r9722.31).

1) Signals not relevant for Extended Functions: Must not be evaluated.

2) Only valid for CU310-2.

11.6.2.5 S_SLS_LIMIT_A: SLS limit value input

S_SLS_LIMIT_A

- PZD3 in telegram 901, 902, 903, output signals
- SLS limit value input
- Value range 1 ... 32767; 32767 ≙ 100% of the 1st SLS level

11.6.2.6 S_SLS_LIMIT_A_ACTIVE: Active SLS limit value

S_SLS_LIMIT_A_ACTIVE

- PZD3 in telegram 901, 902, 903, input signals
- Active SLS limit value

- Value range 1 ... 32767; 32767 ≙ 100%
- Must only be evaluated if SLS 1 active and p9501.24 = 1.

11.6.2.7 S_CYCLE_COUNT: Counter for the safety cycle

S_CYCLE_COUNT

- PZD4 in telegrams 901 and 902, input signals
- Counter for the safety cycle
- Value range -32768 ... +32767
- May only be evaluated if the transfer of safe position values is active (p9501.25 = 1) and the position value is valid (r9722.22 = r9722.23 = 1).

11.6.2.8 S_XIST16: Current actual position value (16 bits)

S_XIST16

- PZD5 in telegram 901, input signals
- Current actual position value (16 bits)
- Value range ±32767
- Scaling using p9574

Note

Scaling

It is not permissible that the position value transferred in S_XIST16 exceeds the value range that can be represented. This is the reason that the safe position value of the drive (r9713[0]) can be allocated a scaling factor. The position value is divided by this factor before transfer. As a consequence, a wider value range can be transferred with a reduced accuracy.

Example: For a position of -29.999 mm signaled in r9708[0] and r9708[1] and a scaling factor of p9x74 = 1000, a numerical value of -29 is signaled to the controller.

- May only be evaluated if the transfer of safe position values is active (p9501.25 = 1) and the position value is valid (r9722.22 = r9722.23 = 1).

11.6.2.9 S_XIST32: Current actual position value (32 bits)

S_XIST32

- PZD5 and PZD6 in telegram 902, input signals
- Current actual position value (32 bits)
- Value range ±737280000

- Unit: 1 μm (linear axis), 0.001 ° (rotary axis)
- May only be evaluated if the transfer of safe position values is active (p9501.25 = 1) and the position value is valid (r9722.22 = r9722.23 = 1).

11.6.2.10 S_ZSW_CAM1

S_ZSW_CAM1

S_ZSW_CAM1, Safe Cam
see function diagram [2844].

Table 11-28 Description of Safety status word Safe Cam (S_ZSW_CAM1)

Byte	Bit	Meaning	Remarks	
0	0	Position at cam 1	1	Position is at cam 1
			0	Position is not at cam 1
	1	Position at cam 2	1	Position is at cam 2
			0	Position is not at cam 2
	2	Position at cam 3	1	Position is at cam 3
			0	Position is not at cam 3
	3	Position at cam 4	1	Position is at cam 4
			0	Position is not at cam 4
	4	Position at cam 5	1	Position is at cam 5
			0	Position is not at cam 5
	5	Position at cam 6	1	Position is at cam 6
			0	Position is not at cam 6
	6	Position at cam 7	1	Position is at cam 7
			0	Position is not at cam 7
	7	Position at cam 8	1	Position is at cam 8
			0	Position is not at cam 8

Byte	Bit	Meaning	Remarks	
1	0	Position at cam 9	1	Position is at cam 9
			0	Position is not at cam 9
	1	Position at cam 10	1	Position is at cam 10
			0	Position is not at cam 10
	2	Position at cam 11	1	Position is at cam 11
			0	Position is not at cam 11
	3	Position at cam 12	1	Position is at cam 12
			0	Position is not at cam 12
	4	Position at cam 13	1	Position is at cam 13
			0	Position is not at cam 13
	5	Position at cam 14	1	Position is at cam 14
			0	Position is not at cam 14
	6	Position at cam 15	1	Position is at cam 15
			0	Position is not at cam 15
	7	Position at cam 16	1	Position is at cam 16
			0	Position is not at cam 16
2	0	Position at cam 17	1	Position is at cam 17
			0	Position is not at cam 17
	1	Position at cam 18	1	Position is at cam 18
			0	Position is not at cam 18
	2	Position at cam 19	1	Position is at cam 19
			0	Position is not at cam 19
	3	Position at cam 20	1	Position is at cam 20
			0	Position is not at cam 20
	4	Position at cam 21	1	Position is at cam 21
			0	Position is not at cam 21
	5	Position at cam 22	1	Position is at cam 22
			0	Position is not at cam 22
	6	Position at cam 23	1	Position is at cam 23
			0	Position is not at cam 23
	7	Position at cam 24	1	Position is at cam 24
			0	Position is not at cam 24

Byte	Bit	Meaning	Remarks	
3	0	Position at cam 25	1	Position is at cam 25
			0	Position is not at cam 25
	1	Position at cam 26	1	Position is at cam 26
			0	Position is not at cam 26
	2	Position at cam 27	1	Position is at cam 27
			0	Position is not at cam 27
	3	Position at cam 28	1	Position is at cam 28
			0	Position is not at cam 28
	4	Position at cam 29	1	Position is at cam 29
			0	Position is not at cam 29
	5	Position at cam 30	1	Position is at cam 30
			0	Position is not at cam 30
	6	Safe Cam active	1	Safe Cam is active
			0	Safe Cam is not active
	7	Validity of the values of Safe Cam	1	Values of Safe Cam apply
			0	Values of Safe Cam do not apply

11.6.3 SIC/SCC (PROFIdrive) process data

11.6.3.1 S_STW1B: Safety Control Channel control word 1

S_STW1B

Safety Control Channel control word 1

Table 11-29 Description of S_STW1B

Bit	Meaning	Remarks		Parameter
0...7	Reserved	–	–	–
8	Extended Functions test stop/forced checking procedure	1	Extended Functions test stop/forced checking procedure selected	r10251.8
		0	Extended Functions test stop/forced checking procedure deselected	
9...12	Reserved	–	–	–
13	Close brake from control	1	"Close brake from control" selected	r10251.13
		0	"Close brake from control" deselected	
14, 15	Reserved	–	–	–

11.6.3.2 S_ZSW1B: SI Motion / Safety Info Channel status word

S_ZSW1B

SI Motion Safety Info Channel status word

Table 11-30 Description S_ZSW1B

Bit	Meaning	Remarks		Parameter
0	STO active	1	STO active	r9734.0
		0	STO not active	
1	SS1 active	1	SS1 active	r9734.1
		0	SS1 not active	
2	SS2 active	1	SS2 active	r9734.2
		0	SS2 not active	
3	SOS active	1	SOS active	r9734.3
		0	SOS not active	
4	SLS active	1	SLS active	r9734.4
		0	SLS not active	
5	SOS selected	1	SOS selected	r9734.5
		0	SOS deselected	
6	SLS selected	1	SLS selected	r9734.6
		0	SLS deselected	
7	Internal event	1	Internal event	r9734.7
		0	No internal event	
8	SLA selected	1	SLA selected	r9734.8
		0	SLA deselected	
9	Active SLS level bit 0	–	Display of the velocity limit for SLS (2 bits)	r9734.9
10	Active SLS level bit 1	–		r9734.10
11	Reserved	–	–	–
12	SDI positive selected	1	SDI positive selected	r9734.12
		0	SDI positive deselected	
13	SDI negative selected	1	SDI negative selected	r9734.13
		0	SDI negative deselected	
14	ESR retract requested	1	ESR retract requested	r9734.14
		0	ESR retract not requested	
15	Safety message effective	1	Safety message effective	r9734.15
		0	No Safety message effective	

11.6.3.3 S_ZSW2B: Safety Info Channel status word 2

S_ZSW2B

Safety Info Channel status word 2

Table 11-31 Description of S_ZSW2B

Bit	Meaning	Remarks		Parameter
0...3	Reserved	–	–	–
4	SLP selected position range	1	SLP area 2 selected	r9743.4
		0	SLP area 1 selected	
5, 6	Reserved	–	–	–
7	SLP selected and user agreement	1	SLP selected and user agreement set	r9743.7
		0	SLP selected or user agreement not set	
8	SDI positive	1	SDI positive selected	r9743.8
		0	SDI positive deselected	
9	SDI negative	1	SDI negative selected	r9743.9
		0	SDI negative deselected	
10, 11	Reserved	–	–	–
12	Test stop active	1	Test stop active	r9743.12
		0	Test stop not active	
13	Test stop required	1	Test stop required	r0743.13
		0	Test stop not required	
14, 15	Reserved	–	–	–

11.6.3.4 S_STW3B: Safety Control Channel control word 3

S_STW3B

Safety Control Channel control word 3

Table 11-32 Description of S_STW3B

Bit	Meaning	Remarks		Parameter
0	Select brake test	1	Brake test selected	r10231.0
		0	Brake test deselected	
1	Start brake test	1	Start brake test requested	r10231.1
		0	Start brake test not requested	
2	Brake selection	1	Test brake 2 selected	r10231.2
		0	Test brake 1 selected	
3	Select direction of rotation	1	Negative direction selected	r10231.3
		0	Positive direction selected	

Bit	Meaning	Remarks		Parameter
4	Select test sequence	1	Test sequence 2 selected	r10231.4
		0	Test sequence 1 selected	
5	Status of external brake	1	External brake closed	r10231.5
		0	External brake open	
6...15	Reserved	–	–	–

11.6.3.5 S_ZSW3B: Safety Info Channel status word 3

S_ZSW3B

Safety Info Channel status word 3

Table 11-33 Description of S_ZSW3B

Bit	Meaning	Remarks		Parameter
0	Brake test	1	Brake test selected	r10234.0
		0	Brake test deselected	
1	Setpoint input, drive/external[1)]	1	Setpoint specification for the drive	r10234.1
		0	Setpoint specification, external (controller)	
2	Active brake	1	Test brake 2 active	r10234.2
		0	Test brake 1 active	
3	Brake test active	1	Test active	r10234.3
		0	Test inactive	
4	Brake test result	1	Test successful	r10234.4
		0	Test error	
5	Brake test completed	1	Test run	r10234.5
		0	Test incomplete	
6	External brake request	1	Close brake	r10234.6
		0	Open brake	
7	Current load sign	1	Negative sign	r10234.7
		0	Positive sign	
8...10	Reserved	–	–	–
11	SS2E active	1	SS2E active	r10234.11
		0	SS2E inactive	
12	SS2ESR active	1	SS2ESR active	r10234.12
		0	SS2ESR inactive	
13	Reserved	–	–	–
14	Acceptance test SLP (SE) selected	1	Acceptance test SLP (SE) selected	r10234.14
		0	Acceptance test SLP (SE) deselected	
15	Acceptance test mode selected	1	Acceptance test mode selected	r10234.15
		0	Acceptance test mode deselected	

1) Setpoint input for the drive: The speed setpoint is entered by the function SBT.
External setpoint input (open-loop control): The "normal" speed setpoint is effective.

11.6.3.6 S_V_LIMIT_B: Safety Info Channel setpoint velocity limiting

S_V_LIMIT_B

SLS speed limit with a 32-bit resolution with sign bit.

Table 11-34 Description S_V_LIMIT_B

Parameter	Meaning
r9733[2]	SLS speed limit
p2000	Scaling of the SLS speed limit S_V_LIMIT_B = 4000 0000 hex ≙ speed in p2000

11.7 Interface signals: Axis/spindle signals

As PLC user interface, certain axis-specific signals are mapped from the SIC/SCC (Page 231) in the axis DB (Page 232):

- DB31 ... DB61, Safety Info Channel (SIC)
- DB31 ... DB61, Safety Control Channel (SCC)

This means, for example, that you can perform the brake test (Page 326) via the PLC user program.

Further information

Further information on the PLC user interface can be found in the SINUMERIK ONE PLC Function Manual.

12 System features

12.1 Latest information

Important note for maintaining the operational safety of your system:

Note

Requirements for operational safety

Systems with safety-related characteristics are subject to special operational safety requirements on the part of the operating company. The supplier is also obliged to comply with special product monitoring measures. For this reason, we publish a special newsletter containing information on product developments and features that are (or could be) relevant when operating safety-related systems.

- You should subscribe to the corresponding newsletter in order to obtain the latest information and to allow you to modify your equipment accordingly.

Subscribing to the Safety Integrated Newsletter

1. Go to the following Internet address in your browser:
   Safety Integrated Newsletter (https://new.siemens.com/global/de/produkte/automatisierung/themenfelder/safety-integrated/fertigungsautomatisierung/newsletter.html)
2. Select the desired language for the Web page.
3. Enter your address data on the Newsletter page.
4. Select your areas of interest in the Safety Integrated domain.
5. Activate the consent.
6. Click on "Send".

12.2 Response times

The Basic Functions are executed in the monitoring cycle (p9780). PROFIsafe telegrams are evaluated in the PROFIsafe scan cycle, which corresponds to twice the monitoring clock cycle (PROFIsafe scan cycle = 2 · r9780).

Note for understanding the tables

The drive system is the component that provides the safety functions. The designation "fault-free drive system" means that the component that provides the safety functions does not have a defect itself:

- Worst case for a fault-free drive system
  For faults outside the drive system, such as e.g. faulty setpoint input from a control system, limit value violations as a result of the behavior of the motor, closed-loop control, load, etc., the "Worst case for a fault-free drive system" response time is guaranteed.
- Worst case when a fault exists
  For a single fault within the drive system, such as a defect in a switch-off signal path of the power unit, a defect in an encoder actual value measurement, a defect in a microprocessor (Control Unit or Motor Module) etc., the "Worst case when a fault exists" response time is guaranteed.

12.2.1 Controlling Basic Functions via terminals on the Control Unit and Motor Module

The following table lists the response times from the control via terminals until the response actually occurs.

Table 12-1 Response times for control via terminals on the Control Unit and the Motor Module.

Function	**Worst case for**	
	Drive system has no fault	**A fault is present**
STO	2 · r9780 + t_E[1)]	3 · r9780 + t_E[1)]
SBC	4 · r9780 + t_E[1)]	8 · r9780 + t_E[1)]
SS1/SS1E (time-controlled) Selection until STO is initiated	2 · r9780 + p9652 + t_E[1)]	3 · r9780 + p9652 + t_E[1)]
SS1/SS1E (time-controlled) Selection until SBC is initiated	4 · r9780 + p9652 + t_E[1)]	8 · r9780 + p9652 + t_E[1)]
SS1 (time-controlled) Selection until braking is initiated	3 · r9780 + 2 ms + t_E[1)]	4 · r9780 + 2 ms + t_E[1)]

[1)] The following applies for t_E (debounce time of the digital input being used):

p9651 = 0	t_E = 2 · p0799 (default = 4 ms)
p9651 ≠ 0	t_E = p9651 + p0799 + 1 ms

The minimum time for t_E is t_E_min = 2 ms.

12.2.2 Controlling the Basic Functions via PROFIsafe

The following table lists the response times[1)] from receiving the PROFIsafe Telegram in the drive up to initiating the particular response.

Table 12-2 Response times when controlling via PROFIsafe

Function	Worst case for	
	Drive system has no fault	**A fault is present**
STO	5 · r9780 + t_E[2)]	5 · r9780 + t_E[2)]
SBC	6 · r9780 + t_E[2)]	10 · r9780 + t_E[2)]
SS1/SS1E (time-controlled) Selection until STO is initiated	5 · r9780 + p9652 + t_K[2)]	5 · r9780 + p9652 + t_K[2)]
SS1/SS1E (time-controlled) Selection until SBC is initiated	6 · r9780 + p9652 + t_K[2)]	10 · r9780 + p9652 + t_K[2)]
SS1 (time-controlled) Selection until braking is initiated	5 · r9780 + 2 ms + t_K[2)]	5 · r9780 + 2 ms + t_K[2)]

1) The specified response times involve internal SINAMICS response times. Program run times in the F-host and the transmission time via PROFIBUS or PROFINET are not taken into account. When calculating the response times between the F-CPU and the converter, you must take into account that faults in the communication can result in a safety function only being selected after the PROFIsafe monitoring time (F_WD_Time) has expired. The PROFIsafe monitoring time (F_WD_Time) must also be included in the calculation when an error occurs.

2) t_K is the time for internal communication within the SINAMICS module; t_K can be determined as follows:
t_K = To (for To, see parameter r2064[4])

12.2.3 Controlling the Extended Functions via PROFIsafe

The following table lists the response times[1) 2)] from receiving the PROFIsafe Telegram in the drive up to initiating the particular response.

Table 12-3 Response times when controlling via PROFIsafe

Function	Worst case for	
	Drive system has no fault	**A fault is present**
STO	5 · p9500[8)] + r9780 + t_K[6)]	5 · p9500[8)] + 2 · r9780 + t_K[6)]
SBC	5 · p9500[8)] + 2 · r9780 + t_K[6)]	5 · p9500[8)] + 6 · r9780 + t_K[6)]
SS1 (time controlled), SS1E, SS2E: Time from selecting up to starting the safe timer SS1 (acceleration controlled), SS2: Time from selecting up to initiating braking SOS: Time from selecting up to starting standstill monitoring	5 · p9500[8)] + 2 ms + t_K[6)]	5 · p9500[8)] + 2 ms + t_K[6)]
SBR or SAM (limit value violation until STO active)	2 · p9500 + r9780	2.5 · p9500 + r9780 + t_ACT[5)]
SOS standstill tolerance window violated	1.5 · p9500 + 2 ms	3 · p9500 + 2 ms + t_ACT[5)]
SLS speed limit violated [3)]	2 · p9500 + 2 ms	3.5 · p9500 + 2 ms + t_ACT[5)]
SSM[4)]	4 · p9500	4.5 · p9500 + t_ACT[5)]
SDI (limit value violation until braking is initiated)	1.5 · p9500 + 2 ms	3 · p9500 + 2 ms + t_ACT[5)]

Function	Worst case for	
	Drive system has no fault	A fault is present
SLA [9]: Selection or deselection	5 · p9500[8] + t_K	5 · p9500[8] + t_K
SLA: Limit value violation	3 · p9500 + 2 ms	4 · p9500 + 2 ms + t_act
SLP (limit value violation until a response is initiated)	1.5 · p9500 + 2 ms	3 · p9500 + 2 ms + t_ACT[5]
SCA: Time between violation of a cam start or end position and output of the feedback message in S_ZSW_CAM1	3.5 · p9500	4 · p9500 + t_ACT[5]
SP[7] with isochronous PROFIsafe telegram	3 · p9500	3 · p9500 + t_ACT[5]

1) The specified response times are valid for Extended Functions with and without selection.

2) The specified response times involve internal SINAMICS response times. Program run times in the F-host and the transmission time via PROFIBUS or PROFINET are not taken into account. When calculating the response times between the F-CPU and the converter, you must take into account that faults in the communication can result in a safety function only being selected after the PROFIsafe monitoring time (F_WD_Time) has expired. The PROFIsafe monitoring time (F_WD_Time) must also be included in the calculation when an error occurs.

3) SLS: Specification of the response time required to initiate a braking response in the drive - or for the output of the "SOS selected" message to the motion control system.

4) SSM: The data corresponds to the times between the limit value being undershot up to sending the information via PROFIsafe.

5) t_ACT:

For p9511 ≠ 0	t_ACT = p9511
For p9511 = 0	t_ACT = PROFIBUS cycle

6) t_K is the time for internal communication within the SINAMICS module; t_K can be determined as follows:
t_K = To (for To, see parameter r2064[4])

7) SP: The data corresponds to the times between acquisition of the safe position and transfer of the safe position via PROFIsafe.

8) For the best possible execution (relating to time) on the F-CPU this component is reduced from 5 · p9500 to 3 · p9500.

9) In SINUMERIK Operate, the settings for SLA can only be made via the parameter list.

Safety Integrated with SINUMERIK ONE Create MyVirtual Machine 13

13.1 System-related properties

The SINUMERIK ONE control system is available as a real "SINUMERIK ONE" control system and as a digital twin "SINUMERIK ONE Create MyVirtual Machine". As a result of the hardware modeling, the virtual system has system-related attributes and restrictions, which differ with respect to the real system. The restrictions relating to Safety Integrated are explained in the following Chapter.

13.2 Overview of the functions

Functions and restrictions overview table

Only those safety functions listed in the following overview table are supported.

Function group / function		Short designation	Actual Sinumerik	Virtual SINUMERIK
Safety Integrated motion control features				
	Safe Torque Off	STO	X	X
	Safe Stop 1	SS1	X	X
	Safe Stop 2	SS2	X	X
	Safe Stop 2e	SS2e	X	X
	Safe Stop 2 ESR	SS2ESR	X	X* (*only in conjunction with an NC-controlled retraction, when SS2ESR is externally selected)
	Safe Operating Stop	SOS	X	X
	Safely-Limited Speed	SLS	X	X
	SLS Override (Specification of the correction factor in the F-program via PROFIsafe)	SLS Override	X	X
	Safe Acceleration Monitoring	SAM	X	--
	Safe Brake Ramp	SBR	X	--
	Safe Speed Monitoring	SSM	X	X
	Safe Direction	SDI	X	X
	Safe Limit Positions	SLP	X	X
	Safe Brake Test (only telegram 701 SIC/SCC)	SBT	X	X
	Safe Cams (Can be used only with PROFIsafe telegram 903, not together with the SP function, only for linear axes; modulo axes are not supported)	SCA	X	X
	Transfer of safe position values (only with PROFIsafe telegram 901/902, cannot be used together with the SCA function)	SP	X	X* (* only PROFIsafe telegram 902)
	Safely-Limited Acceleration (SLA)	SLA	X	X
	Internal SOS/SLS deselection		X	X
	Switchover speed to SOS (Abort the stop transition times at SOS for SOS, SS2, SS2e, SLS selection)		X	X

Function group / function		Short designation	Actual Sinumerik	Virtual SINUMERIK
	Safe User Data		--	--
	Safety Integrated change of view to dbSI mode		X	X
NCK				
	Dynamic Stop D		X	X
	SIC/SCC		X	X
	Homing via SIC/SCC		X	X
SINUMERIK Operate diagnostic support				
	Diagnostics overview		X	X
	SI drives		X	X
	SI telegrams		X	X
	Integrated F-CPU		--	--
	SI checksums - global checksum		X	--
	SI checksums - F-signature		X	X
	SI checksums - drive checksum		X	--
	SI alarms		X	--
	SI peripherals		--	--
	SCA		X	X
SINUMERIK Operate commissioning support (Safety Integrated)				
	Overview (PROFIsafe is activated only in one channel)		X	X
	Setting options		X	X
	Settings - configuration		X	X
	Settings - telegram configuration (PROFIsafe enable and input of the PROFIsafe module number is not relevant for the Create MyVirtual Machine)		X	X
	Proposed values for encoder parameterization Automatic presetting of the encoder parameterization by means of the "Default" softkey		X	--
	STO/SS1 (Basic)		X	X* (* via PROFI-safe)
	STO Extended		X	X
	SBC		X	--
	SS1 Extended		X	X
	SS2/SOS/SS2e		X	X
	SAM/SBR		X	--
	SLS		X	X
	SSM		X	X
	SDI		X	X
	SLP/SP		X	X
	SBT		X	X
	SCA		X	X
	SS2 E		X	X

Function group / function		Short designation	Actual Sinumerik	Virtual SINUMERIK
	SI Ref		X	X
Acceptance test				
	SINUMERIK Safety Integrated features		X	--
	F-PLC		X	--
F-PLC				
	F-programming		X	X
	F-I/O		X	X

13.3 Safety Integrated restrictions

The following functions are currently not permitted or are not available in SINUMERIK ONE Create MyVirtual Machine for hardware-related reasons.

Commissioning the F-PLC and programming the safety program

You configure and program the F-PLC in the TIA Portal just like a real PLC S7-1500 - taking into account the restrictions and supplementary conditions listed in this manual as well as in the manuals for SINUMERIK Safety Integrated, SIMATIC Safety Advanced and SIMATIC S7-PLCSIM Advanced.

- **Controlling safety functions integrated in the drive**
  Control via terminals is not supported. Use the control via PROFIsafe/PROFIdrive. Only PROFIsafe/PROFIdrive telegrams 902/903 are supported.
- **Monitoring channels**
  - The 2nd monitoring channel (p93xx) is not functionally supported.
  - However, the parameters for the 2nd channel are used to calculate the current load-side actual values of the second monitoring channel and the difference between the two monitoring channels.
  - A data comparison with the output of a safety message is output only for the parameters p9326 and p9526.
- **Alarms and messages**
  Safety messages are not output.
- **Safety Integrated commissioning**
  In the real system, the Safety Integrated commissioning must be activated to change Safety Integrated-relevant data. In SINUMERIK ONE Create MyVirtual Machine, the Safety Integrated data can be changed without Safety Integrated commissioning mode (p0010=95)
- **SI drive alarms**
  If safety functions respond or are initiated, then at least one alarm or a message is output for each safety function.
- **SI encoder system**
  Only a 2-encoder safety system is supported in SINUMERIK ONE Create MyVirtual Machine.
- **Forced dormant error detection (test stop pulse cancellation)**
  Forced dormant error detection can only be configured using SIC/SCC.
- **Encoder preassignment**
  An encoder preassignment created in SINUMERIK ONE Create MyVirtual Machine may differ from the encoder preassignment on a real machine.
  In SINUMERIK ONE Create MyVirtual Machine, for example, a direction reversal or the fine resolution X_IST2 cannot be determined.

- **Scope of the usable safety functions and stop responses**
  - Only the safety functions listed in the SINUMERIK ONE Safety Integrated Commissioning Manual in the "Overview table of functions and restrictions (Page 426)" are supported.
  - SAM cannot be activated by triggering a stop response by SS1 or SS2.
- **Safety Info Channel (SIC)/Safety Control Channel (SCC)**
  - A prerequisite for the function of the Safety Info Channel (SIC)/Safety Control Channel (SCC) is that the option SINUMERIK ONE Safety Integrated - F-PLC is set.
  - With SINUMERIK ONE Create MyVirtual Machine, alarm 27813 "Option F logic not set" is not output if the option is not set.

Appendix A

A.1 Abbreviations

The following list of abbreviations includes all of the relevant abbreviations for SINUMERIK Safety Integrated Functions.

Abbreviation	Source of abbreviation	Meaning
AIM	Active Interface Module	Active Interface Module
ALM	Active Line Module	Active Line Module
ASM	Asynchronmotor	Induction motor
BERO	---	Contactless proximity switch
BI	Binector Input	Binector input
BICO	Binector Connector Technology	Binector connector technology Remark: BICO is not used for S210 drives.
BLM	Basic Line Module	Basic Line Module
BO	Binector Output	Binector output
CI	Connector Input	Connector input
CNC	Computerized Numerical Control	Computer-supported numerical control
CO	Connector Output	Connector output
CoL	Certificate of License	Licensing certificate
CP	Communication Processor	Communications processor
CPU	Central Processing Unit	Central processing unit
CU	Contol Unit	Control Unit
DI	Digital Input	Digital input
DO	Digital Output	Digital output
DO	Drive Object	Drive object
DRAM	Dynamic Random Access Memory	Dynamic Random Access Memory
DRIVE-CLiQ	Drive Component Link with IQ	Drive Component Link with IQ
DSC	Dynamic Servo Control	Dynamic Servo Control
EGB	Elektronisch gefährdete Baugruppen	Electrostatic Sensitive Device
EMV	Elektromagnetische Verträglichkeit	Electromagnetic compatibility
EN	Europäische Norm	European Standard
EPOS	Einfachpositionierer	Basic positioner
F-DI	Failsafe Digital Input	Failsafe Digital Input
F-DO	Failsafe Digital Output	Failsafe Digital Output
GC	Global Control	Global Control telegram
GSD	Gerätestammdatei	Generic Station Description: Describes the features of a PROFIBUS slave
GUID	Global Unique Identifier	Globally Unique Identifier
IPO	Interpolator	Interpolator
JOG	Jogging	JOG mode: Jogging

Abbreviation	Source of abbreviation	Meaning
LED	Light-Emitting Diode	Light emitting diode
MC	Motion Control	Motion control
MM	Motor Module	Motor Module
NC	Numerical Control	Numerical control
NSR	Netzstromrichter	Line side converter
p...	-	Setting parameters
PCU	PC Unit	Computer unit
PELV	Protective Extra Low Voltage	Safe extra low voltage
PG	Programmiergerät	Programming device
PLC	Programmable Logic Control	Programmable logic controller
PN	PROFINET (Process Field network)	Open Ethernet standard for automation
PPU	Panel Processing Unit	Compact control unit
PZD	Prozessdaten	Process data
r...	-	Display parameters (read only)
RAM	Random Access Memory	Memory for reading and writing
SAM	Safe Acceleration Monitor	Safe acceleration monitoring
SBC	Safe Brake Control	Safe brake activation
SBR	Safe Brake Ramp	Safe Brake Ramp
SBT	Safe Brake Test	Safe Brake Test (pure diagnostics function)
SCA	Safe Cam	Safe Cam
SCC	Safety Control Channel	Safety Control Channel
SDI	Safe Direction	Safe Direction
SH	Sicherer Halt	Safe standstill
SI	Safety Integrated	Safety Integrated
SIC	Safety Info Channel	Safety Info Channel
SIL	Safety Integrity Level	Safety Integrity Level
SLA	Safely Limited Acceleration	Safely-Limited Acceleration
SLM	Smart Line Module	Smart Line Module
SLP	Safe Limited Position	Safely-Limited Position
SLS	Safely Limited Speed	Safely-Limited Speed
SM	Sensor Module	Sensor Module
SMC	Sensor Module Cabinet	Sensor Module Cabinet
SME	Sensor Module External	Sensor Module External
SMI	Sensor Module Integrated	Sensor Module Integrated
SOS	Safe Operating Stop	Safe Operating Stop
SP	Safe Position	Safe Position
SS1	Safe Stop 1	Safe Stop 1 (time-monitored, ramp-monitored)
SS1E	Safe Stop 1 with external Stop	Safe Stop 1 with external stop
SS2	Safe Stop 2	Safe Stop 2
SS2E	Safe Stop 2 with external Stop	Safe Stop 2 with external stop
SS2ESR	Safe Stop 2 with extended Stop and Retract	Safe Stop 2 with extended stop and retraction
SSM	Safe Speed Monitor	Safe feedback from speed monitor
STO	Safe Torque Off	Safe Torque Off

Abbreviation	Source of abbreviation	Meaning
STOP A, B, ...	Stop reaction	Stop response In the event of a fault, the system responds corresponding to the configured stop response. Applies to SINAMICS Integrated or SINAMICS S120 drives. Does not apply to S210 drives.
STO, SS1, SS2.... KDV	Fault responses	Fault response: In the event of a fault, the system responds corresponding to the configured fault response. Only applicable for S210 drives.
STW	Steuerwort	Control word
TM54F	Terminal Module 54 F	Terminal expansion module 54 F
UL	Underwriters Laboratories Inc.	Underwriters Laboratories Inc.
UPS	Uninterruptible Power Supply	Uninterruptible power supply
ZK	Zwischenkreis	DC link
ZM	Zero Mark	Zero mark
ZSW	Zustandswort	Status Word

A.2 Additional information on safety topics

A.2.1 Information sheets issued by the Employer's Liability Insurance Association

Safety-related measures to be implemented cannot always be derived from directives, standards, or regulations. In this case, supplementary information and explanations are required.

Some regulatory bodies issue publications on an extremely wide range of subjects.

Note

These publications are in German. In some instances, they are also available in English and French.

Information sheets covering the following areas are available, for example:

- Process monitoring in production environments
- Axes subject to gravitational force
- Roller pressing machines
- Lathes and turning centers - purchasing/selling

These information sheets issued by specialist committees can be obtained by all interested parties (e.g. to provide support in factories, or when regulations or safety-related measures for plants and machines are defined). These information sheets provide support for the fields of machinery construction, production systems, and steel construction.

You can download the information sheets from the Internet address (https://www.bghm.de):

1. First select the area "Arbeitsschützer", followed by the menu item "Praxishilfen" and finally "DGUV-Informationen".

A.2.2 Further information

You can find additional information on Safety Integrated in the:

- System Manual Safety Integrated - the safety program for the industries of the world (https://support.industry.siemens.com/cs/ww/en/view/28813929)

Index

E

F

G

H

I

L

M

O

P

R

S

T

U

V

W