SIEMENS

SINUMERIK

SINUMERIK 840D sl
Safety Integrated plus

Commissioning Manual

Preface

Fundamental safety instructions 1

Introduction 2

Fundamentals 3

Safety program of the F-PLC 4

Safety functions integrated in the drive 5

Controlling safety functions integrated in the drive 6

Commissioning and configuring 7

Diagnostics 8

Acceptance test with SINUMERIK Operate 9

Component replacement (software/hardware) 10

Data descriptions 11

System features 12

Switchover from Safety Integrated (system-integrated) 13

Appendix A

Valid for:

CNC software V4.92
SINUMERIK STEP 7 Toolbox V15

06/2019
A5E46265018B AB

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
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E46265018B AB
℗ 06/2019 Subject to change

Copyright © Siemens AG 2019.
All rights reserved

Preface

SINUMERIK documentation

The SINUMERIK documentation is organized into the following categories:

- General documentation/catalogs
- User documentation
- Manufacturer/service documentation

Additional information

You can find information on the following topics at the following address (https://support.industry.siemens.com/cs/de/en/view/108464614):

- Ordering documentation/overview of documentation
- Additional links to download documents
- Using documentation online (find and search in manuals/information)

If you have any questions regarding the technical documentation (e.g. suggestions, corrections), please send an e-mail to the following address (mailto:docu.motioncontrol@siemens.com).

mySupport/Documentation

At the following address (https://support.industry.siemens.com/My/ww/en/documentation), you can find information on how to create your own individual documentation based on Siemens' content, and adapt it for your own machine documentation.

Training

At the following address (http://www.siemens.com/sitrain), you can find information about SITRAIN (Siemens training on products, systems and solutions for automation and drives).

FAQs

You can find Frequently Asked Questions in the Service&Support pages under Product Support (https://support.industry.siemens.com/cs/de/en/ps/faq).

SINUMERIK

You can find information about SINUMERIK at the following address (http://www.siemens.com/sinumerik).

Target group

This documentation is intended for commissioning personnel.

Benefits

The intended target group can use the commissioning manual to test and commission the product, system or the plant correctly and safely.

Standard scope

This documentation only describes the functionality of the standard version. Additions or revisions made by the machine manufacturer are documented by the machine manufacturer.

Other functions not described in this documentation might be executable in the control. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For the sake of simplicity, this documentation does not contain all detailed information about all types of the product and cannot cover every conceivable case of installation, operation, or maintenance.

Note regarding the General Data Protection Regulation

Siemens observes standard data protection principles, in particular the principle of privacy by design. That means that

this product does not process / store any personal data, only technical functional data (e.g. time stamps). If a user links this data with other data (e.g. a shift schedule) or stores personal data on the same storage medium (e.g. hard drive) and thus establishes a link to a person or persons, then the user is responsible for ensuring compliance with the relevant data protection regulations.

Technical Support

Country-specific telephone numbers for technical support are provided in the Internet at the following address (https://support.industry.siemens.com/sc/ww/en/sc/2090) in the "Contact" area.

Benefits

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

Notation

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-relevant part of the user program is called "Standard user program".

Term: Control Unit

Note

Term "Control Unit" in this documentation

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

Notation 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):

- MD13370 Machine data 13370
- $MN_SAFE_MODE 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

Table of contents

Preface 3

1 Fundamental safety instructions 15

1.1 General safety instructions 15

1.2 Warranty and liability for application examples 16

1.3 Industrial security 17

2 Introduction 19

2.1 Purpose of this documentation 19

3 Fundamentals 21

3.1 Introduction 21

3.2 Safety functions of the F-PLC 22

3.3 Safety functions integrated in the drive 23

3.4 Approvals 25

3.5 Safety-relevant processing using NCU components 26

3.6 Hardware components 29
3.6.1 Configuration diagram 29
3.6.2 F-I/O for PROFIBUS DP 30
3.6.3 F-I/O for PROFINET IO 30
3.6.4 Drive components 31
3.6.4.1 Interconnecting DRIVE-CLiQ components 31
3.6.4.2 Drive monitoring with or without encoder 31
3.6.4.3 Induction motors and synchronous motors 33
3.6.4.4 SINAMICS HLA 33

3.7 Safety components and licensing 36
3.7.1 Software components required 36
3.7.2 Licensing axes/spindles and F-PLC 36

3.8 Representation of safety-related resources in the TIA Portal 38

4 Safety program of the F-PLC 41

4.1 Overview 41

4.2 Structure of the safety program 43

4.3 Fail-Safe Blocks 46

4.4 Safety Administration Editor 47

4.5 Restrictions in the programming languages FBD/LAD 48

4.6 Instructions for the safety program 54

4.7 F-runtime groups 56
4.7.1 Rules for F-Runtime Groups of the Safety Program 56

4.7.2 Procedure when specifying an F-runtime group 56
4.7.3 F-global DB 61

4.8 Creating F-blocks 62

4.9 Using libraries 64

4.10 Safety-relevant communication 65

4.11 Access to SI-drives and F-I/O 66

4.12 Programming startup protection 68

4.13 Implementing a user acknowledgment 69

4.14 Data exchange between the standard user program and safety program 70
4.14.1 Comparison between standard user program and safety program 70
4.14.2 Data Transfer from the Safety Program to the Standard User Program 71
4.14.3 Data Transfer from Standard User Program to Safety Program 72

5 Safety functions integrated in the drive 75

5.1 SS1 Basic: 76
5.1.1 Details and parameterization 77
5.1.1.1 SS1 with OFF3 77
5.1.1.2 SS1 with external stop (SS1E) 78
5.1.1.3 Function diagrams and parameters 79

5.2 SS1 80
5.2.1 Details and parameterization 82
5.2.1.1 Safe Stop 1 (SS1, time and acceleration controlled) 82
5.2.1.2 Safe Stop 1 without encoder 83
5.2.1.3 SS1 (Extended Functions) with external stop 85
5.2.1.4 Function diagrams and parameters 86

5.3 STO (Basic/Extended) 87
5.3.1 Details and parameterization 87

5.4 SBC (Basic/Extended) 93
5.4.1 Hardware required 94
5.4.2 Details and parameterization 95
5.4.2.1 SBC for Motor Modules in the chassis format 97
5.4.2.2 Function diagrams and parameters 98

5.5 SS2 100
5.5.1 Details and parameterization 102
5.5.1.1 SS2 with external stop (SS2E) 103
5.5.1.2 Dynamic response adaptation for SS2E 105
5.5.1.3 Safe Stop 2 Extended Stop and Retract (SS2ESR) 107

5.6 SOS 110
5.6.1 Safe Operating Stop (SOS) 110
5.6.2 Details and parameterization 111
5.6.2.1 Function diagrams and parameters 112

5.7 SLS 113
5.7.1 Details and parameterization 118
5.7.1.1 Connection to motion control in the NC 119
5.7.1.2 Safely Limited Speed (SLS) 119
5.7.1.3 Safely Limited Speed without encoder 122

5.7.1.4 Safely-Limited Speed without selection 124
5.7.1.5 Function diagrams and parameters 125
5.7.1.6 EPOS and safety-relevant setpoint velocity limiting 125

5.8 SSM 127
5.8.1 Details and parameterization 127
5.8.1.1 Signal characteristic (with encoder) 129
5.8.1.2 Differences in operation without encoder 129
5.8.1.3 Signal characteristic (without encoder) 130
5.8.1.4 Function diagrams and parameters 131

5.9 SAM 133

5.10 SBR 135
5.10.1 Overview of important parameters 137

5.11 SDI 138
5.11.1 Details and parameterization 140
5.11.1.1 Safe Direction with encoder 140
5.11.1.2 Safe Direction without encoder 141
5.11.1.3 Safe Direction without selection 143
5.11.1.4 Function diagrams and parameters 144

5.12 SLP 146
5.12.1 Safely-Limited Position (SLP) 146
5.12.2 Details and parameterization 146
5.12.2.1 Retraction 149
5.12.2.2 Function diagrams and parameters 150

5.13 SP 151
5.13.1 Details and parameterization 151
5.13.1.1 Function diagrams and parameters 154

5.14 SBT (diagnostic function) 156
5.14.1 Features 156
5.14.2 Connection to NC and PLC programs 157
5.14.3 Details and parameterization 157
5.14.3.1 Requirements 157
5.14.3.2 Handling overview 158
5.14.3.3 Enabling the function 159
5.14.3.4 Selection 162
5.14.3.5 Start of the Safe Brake Test sequence 162
5.14.3.6 Sequence 163
5.14.3.7 Cancellation/deselection and acknowledgment (SBT) 164
5.14.3.8 Communication via SIC/SCC 165
5.14.3.9 Function diagrams and parameters 167

5.15 SCA 168
5.15.1 Details and parameterization 168
5.15.1.1 Function diagrams and parameters 170

5.16 SLA 171
5.16.1 Details and parameterization 172
5.16.1.1 Function diagrams and parameters 172
5.16.1.2 Transmission via PROFIsafe or SIC 174

5.17 Safe referencing 175

5.17.1 User agreement 176
5.17.2 Function diagrams and parameters 178

5.18 Safe actual value acquisition....179
5.18.1 Overview of important parameters 185

5.19 Safe gearbox stage switchover 186
5.19.1 Overview of important parameters 190

5.20 Forced checking procedure....191
5.20.1 Examples for when the forced checking procedure is carried out....191
5.20.2 Options and control 191

6 Controlling safety functions integrated in the drive 193

6.1 Control possibilities 193

6.2 Overview of telegrams 194

6.3 Overview: Process data in telegrams....195

6.4 Controlling via PROFIsafe....197
6.4.1 Enabling PROFIsafe control....197
6.4.2 Selecting the PROFIsafe telegram....197
6.4.3 ESR response in the event of a communication error....198
6.4.4 Parameters and function diagrams 199

6.5 Safety Info Channel and Safety Control Channel (SIC/SCC) 201
6.5.1 Introduction 201
6.5.2 Safety Info Channel (SIC) 201
6.5.3 Safety Control Channel (SCC) 201
6.5.4 SIC/SCC communication using telegram 701....201
6.5.5 PLC user interface (DB3x) 202
6.5.6 Overview of important parameters 202

6.6 Control signals via terminals on the NCU and motor/power module....203
6.6.1 Features 203
6.6.2 Terminals for STO, SS1 (time-controlled), SBC....204
6.6.3 Grouping drives....205
6.6.4 Simultaneity and tolerance time of the two monitoring channels 206
6.6.5 Bit pattern test 207

7 Commissioning and configuring 209

7.1 Handling overview....209

7.2 Configuring safety-relevant components....210
7.2.1 Handling overview for configuring 210
7.2.2 Activating Safety Integrated plus....210
7.2.3 Configuring additional safety-related components 212
7.2.4 Loading the configuration into the controller 212
7.2.5 Allocating and assigning a PROFINET device name....213
7.2.6 Assigning F-destination addresses, address type 1....215
7.2.7 Assigning F-destination addresses, address type 2....215
7.2.8 Checking the PROFIsafe address....217

7.3 Generating a safety program 219
7.3.1 Overview 219
7.3.2 Create receive/send data as PLC tags 219

7.3.3 Adapting the settings of the F-runtime group (optional) 221
7.3.4 Setting up access protection 222
7.3.5 Parameterizing EMERGENCY STOP 223
7.3.6 Implementing user acknowledgment for global reintegration 224
7.3.7 Acknowledging messages related to safety functions integrated in the drive 226
7.3.8 Deselecting safety functions integrated in the drive 229
7.3.9 Initiate a forced checking procedure (test stop) 231
7.3.10 Programming the wiring test 231

7.4 Loading the configuration 232
7.4.1 Loading the configuration to the NCU 232
7.4.2 Transferring the safety mode from the configuration 233

7.5 Configuring NC and drive-specific safety settings 235
7.5.1 Overview 235
7.5.2 Setting software options 236
7.5.3 Activating the safety commissioning mode 236
7.5.4 Selecting the safety functional scope 238
7.5.5 Parameterizing the setpoint speed limiting 239
7.5.6 Parameterizing reaction of the stop response 241
7.5.7 Parameterizing an encoder 242
7.5.8 Configuring encoderless operation 246
7.5.9 Configuring telegrams 251

7.6 Configuring safety functions integrated in the drive 254
7.6.1 Overview 254
7.6.2 STO/SS1 Basic 255
7.6.3 STO Extended 256
7.6.4 SBC 258
7.6.5 SS1 Extended 259
7.6.6 SS2/SOS 261
7.6.7 SS2E 263
7.6.8 SAM 265
7.6.9 SBR 268
7.6.10 SLS 269
7.6.11 SSM 272
7.6.12 SDI 274
7.6.13 SCA 276
7.6.14 SLP/SP 278
7.6.15 SBT 281
7.6.16 Safe referencing 284
7.6.17 Further safety functions 286

7.7 Finalizing commissioning 287
7.7.1 Confirming settings 287
7.7.2 Assigning a Safety Integrated password 288

7.8 Series commissioning 289
7.8.1 General information about series commissioning 289
7.8.2 Series commissioning with third-party motor 289

8 Diagnostics 291

8.1 Diagnostics guide 292

8.2 System alarms and diagnostic screens for F-PLC and F-I/O. 294

8.3 Diagnostic functions in SINUMERIK Operate 296
8.3.1 Safety Integrated diagnostics overview 296
8.3.2 SI drives status 297
8.3.3 SI telegrams overview 299
8.3.4 SI telegrams PROFIsafe 300
8.3.5 PROFIdrive SI telegrams 301
8.3.6 SI checksums 302
8.3.7 SI alarms 304
8.3.8 SI Safe Cams 305
8.3.9 SI integrated F-PLC 306
8.3.10 SI I/O 307

8.4 General information about displaying and evaluating diagnostic information 309

8.5 Checksums 310
8.5.1 Calculating the global checksums/master checksums 310
8.5.2 SINAMICS checksums 312

8.6 Stop responses 313
8.6.1 Overview 313
8.6.2 Basic Functions 313
8.6.3 Extended Functions 315
8.6.4 Connection and effects in the NC 317
8.6.5 Priorities 318

8.7 Using the fault buffer and safety message buffer 320

8.8 Configuring the message buffer and alarm buffer 321
8.8.1 Configuring the standard alarm buffer 321
8.8.2 Configuring the safety alarm buffer 321

8.9 Acknowledgment 323
8.9.1 Overview 323
8.9.2 Acknowledgment via PROFIsafe 324
8.9.3 Additional acknowledgment via PROFIdrive RESET 324
8.9.4 Acknowledgment using POWER ON 325
8.9.5 Extended acknowledgment (deselecting STO/SS1) 325
8.9.6 Additional acknowledgment when the safety message buffer is inactive 325

9 Acceptance test with SINUMERIK Operate 327

9.1 Purpose and requirements 327

10 Component replacement (software/hardware) 329

10.1 Safety instructions 329

10.2 Software, F-CPU, F-I/O 330

10.3 Motors, CU (SINAMICS Safety Integrated) 332

10.4 Parameters and function diagrams - notes regarding replacing components 334

10.5 Messages when components are replaced after Safety Integrated has been commissioned 335

11 Data descriptions 337

11.1 Machine data 337

11.2 NC tags 339
11.2.1 Overview 339

11.3 System variables 340
11.3.1 Overview 340
11.3.2 $VA_STOPSI - actual STOP 340
11.3.3 $A_STOPESI - actual STOP E 340

11.4 Standard telegram start addresses 341

11.5 Telegram structure and data 344
11.5.1 SIEMENS telegram 701 344
11.5.2 SIEMENS telegram 903 344
11.5.3 SIEMENS telegram 902 345
11.5.4 SIEMENS telegram 901 345
11.5.5 PROFIsafe telegram 30 346
11.5.6 PROFIsafe telegram 31 346

11.6 Process data 347
11.6.1 Overview: Process data in telegrams 347
11.6.2 PROFIsafe process data 348
11.6.2.1 S_STW1: Safety control word 1 348
11.6.2.2 S_ZSW1: Safety status word 1 350
11.6.2.3 S_STW2: Safety control word 2 352
11.6.2.4 S_ZSW2: Safety status word 2 354
11.6.2.5 S_SLS_LIMIT_A: SLS limit value input 357
11.6.2.6 S_SLS_LIMIT_A_ACTIVE: Active SLS limit value 357
11.6.2.7 S_CYCLE_COUNT: Counter for the safety cycle 358
11.6.2.8 S_XIST16: Current actual position value (16 bits) 358
11.6.2.9 S_XIST32: Current actual position value (32 bits) 358
11.6.2.10 S_ZSW_CAM1 359
11.6.3 SIC/SCC (PROFIdrive) process data 361
11.6.3.1 S_STW1B: Safety Control Channel control word 1 361
11.6.3.2 S_ZSW1B: SI Motion / Safety Info Channel status word 361
11.6.3.3 S_ZSW2B: Safety Info Channel status word 2 362
11.6.3.4 S_STW3B: Safety Control Channel control word 3 363
11.6.3.5 S_ZSW3B: Safety Info Channel status word 3 363
11.6.3.6 S_V_LIMIT_B: Safety Info Channel setpoint velocity limiting 364

11.7 Interface signals: Axis/spindle signals 365

12 System features 367

12.1 Latest information 367

12.2 Response times 369
12.2.1 Controlling Basic Functions via terminals on the Control Unit and Motor Module 369
12.2.2 Controlling the Basic Functions via PROFIsafe 370
12.2.3 Controlling the Extended Functions via PROFIsafe 370

13 Switchover from Safety Integrated (system-integrated) 373

13.1 Overview 373

13.2 Comparison of the safety functions 374
13.2.1 Overview 374
13.2.2 STOP E 375

13.2.3 SG override 376
13.2.4 Safe Cams 377
13.2.5 Parameterizing EMERGENCY STOP 377

13.3 Additional differences when commissioning 379
13.3.1 Overview 379
13.3.2 Commissioning the F-I/O 380
13.3.3 Parameterizing the safety functions 383
13.3.4 Fault response and acknowledgment for F-I/O faults 386
13.3.5 Accessing status/control information 388

13.4 Procedure when switching over between systems 389

A Appendix 391

A.1 Abbreviations 391

A.2 Documentation overview SINUMERIK 840D sl 394

Index 395

Fundamental safety instructions 1

1.1 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.

1.2 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.

1.3 Industrial security

Note

Industrial security

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. Products and solutions from Siemens 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. using firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that can be implemented, please visit:

Industrial security (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 become available, and that only 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 at:

Industrial security (https://www.siemens.com/industrialsecurity)

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.
- Protect the drive against unauthorized changes by activating the "Know-how protection" converter function.

Introduction 2

2.1 Purpose of this documentation

This documentation provides a description of functions and data about the SINUMERIK Safety Integrated plus (F-PLC) 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 NCU or PLC-controlled NC axes - or external drives, which are assigned to an NC axis.

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

You can find information about the SINUMERIK Safety Integrated (system-integrated) mode in separate documentation:

- Function Manual SINUMERIK Safety Integrated (FBSIsl) (http://support.automation.siemens.com/WW/view/en/28368678/133300)

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 NCU, being part of plants and systems, requires that special standards and regulations are 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).

Note

Information for those switching over from "Safety Integrated (SPL)" to Safety Integrated plus (F-PLC).

Additional information, which is relevant for users that previously worked with Safety Integrated (system-integrated) is provided in the index under keyword "Information for people switching over from a different system".

Fundamentals 3

3.1 Introduction

Safety solution SINUMERIK Safety Integrated plus (F-PLC) combines various safety functions in the SINUMERIK 840D sl:

- F-I/O are connected via the F-capable PLC of the SINUMERIK 840D sl
  - 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 via the Safety Administration Editor (Page 47)
- Control of the safety functions integrated in the drive (via SINAMICS Safety Integrated)
  - Safety Integrated Basic Functions
  - Safety Integrated Extended Functions

3.2 Safety functions of the F-PLC

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 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 users 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.

3.3 Safety functions integrated in the drive

SINUMERIK Safety Integrated plus supports, through SINAMICS Integrated (as subcomponent of the NCU), the SINAMICS Safety Integrated Functions (Page 75). These safety functions integrated in the drive can communicate with the process via safety-relevant 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 36). Extended Functions with encoder require a safety-relevant encoder concept (Page 179).

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)	Extended	Safe Torque Off is a safety function that prevents the drive from re-starting 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 Extended (Page 256)
	Basic		STO/SS1 Basic (Page 255)
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 imple-mented.	
Safe Stop 1 (SS1, time and accelera-tion controlled)	Extended		SS1 Extended (Page 259)
Safe Brake Control (SBC)	Basic Extended	Safe Brake Control is used to safely control a holding brake.[1) 2)]	SBC (Page 258)
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)] The "Safe Brake Test" (SBT) diagnostic function is suitable for safety functions up to Category 2 according to ISO 13849-1.	SBT (Page 281)

Safety Function	Scope	Brief description	Configuration via
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/SOS (Page 261)
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.	

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 269)
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 272)
Safe Direction (SDI)	Extended	Safe Direction is used to safely monitor the direction of motion.	SDI (Page 274)

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

Safety Function	Scope	Brief description	Configuration via
Safely-Limited Position (SLP)	Extended[1]	Safely-Limited Position ensures that a freely definable traversing range is not left.	SLP/SP (Page 278)
Transferring safe position values (SP)	Extended[1]	The "Transfer safe position values (SP)" function enables you to transfer a safe position to the higher-level control via PROFIsafe.	
Safe cams (SCA)	Extended[1]	Safe electronic cams enable a secure, axis-specific range detection or a work zone / protection zone delimitation.	SCA (Page 276)

1) For SINAMICS, these Safety Functions are called "Advanced".

3.4 Approvals

The classification of the functional safety always refers to the overall safety system. The maximum safety requirements that can be achieved for an overall system are obtained from the lowest achievable safety requirement of the individual safety-relevant components.

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

- SIL2 - safety class (Safety Integrity Level) according to IEC 61508
- PL d - Performance Level according to DIN EN ISO 13849-1
- Category 3 according to DIN EN ISO 13849-1

In addition, most of the safety functions of the SINAMICS S have been certified by independent institutes. An up-to-date list of certified components is available on request from your local Siemens office.

Note

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

It is only permissible to use SIMATIC Safety 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-relevant 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)

3.5 Safety-relevant processing using NCU components

In the SINUMERIK Safety Integrated plus (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 Safety Integrated (DRIVE) for this purpose.

Status and control information are transferred using SIC/SCC (Safety Info Channel / Safety Control Channel) between the integrated subcomponents of the NCU (PLC, NC and SINAMICS Safety Integrated).

PROFIsafe communication via NCU subcomponents

PROFIsafe communication is only possible between F-components. As a consequence, for the SINUMERIK NCU, PROFIsafe communication is established between the following components:

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

Details on internal processing of safety-related communication

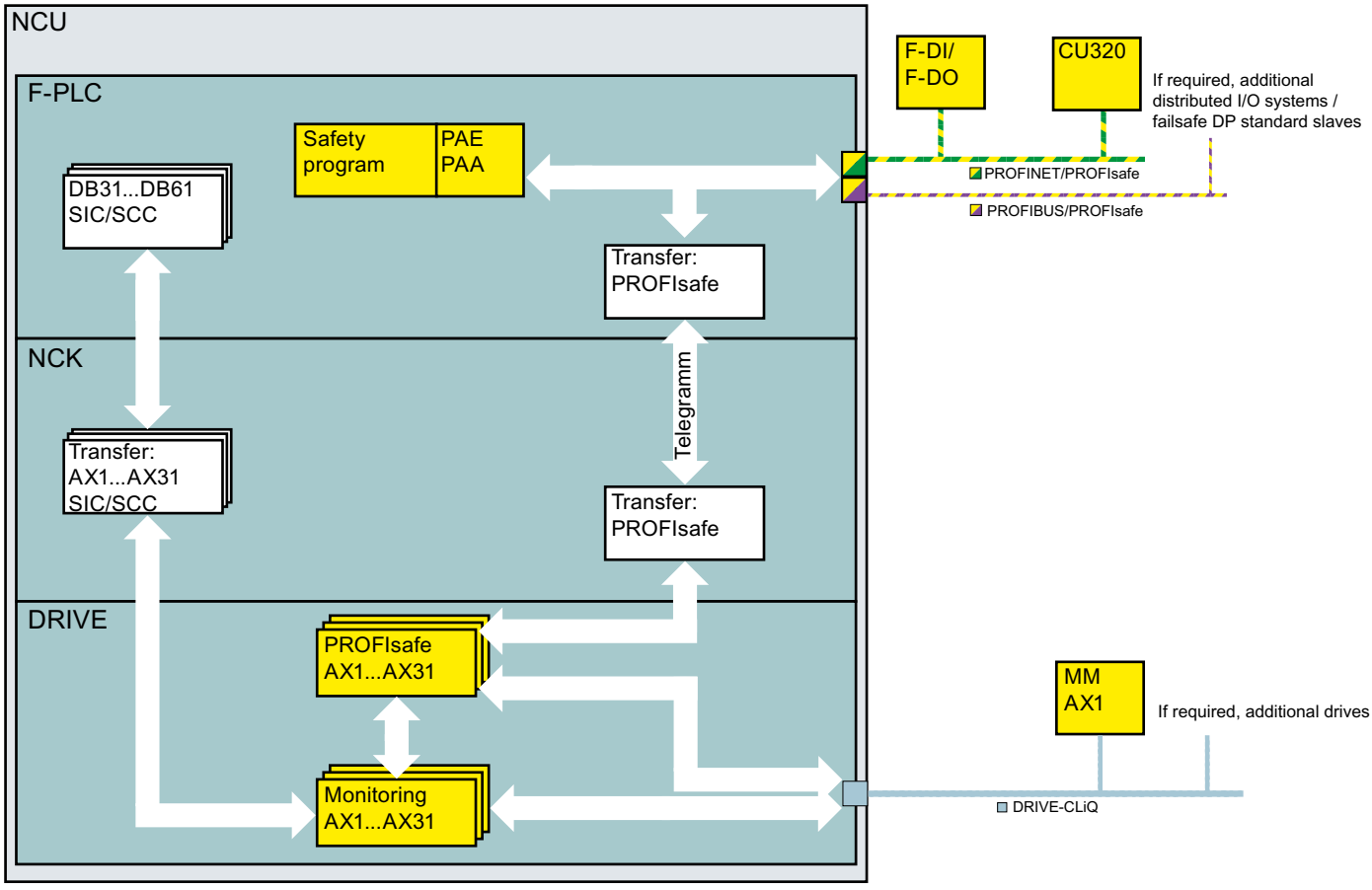


Figure 3-1 Component diagram for processing safety-relevant information and data

Table 3-4 Subcomponents of the NCU

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 41) • Processing status and control signals (SIC/SCC) via the corresponding axis DB (axis1 [DB31] ... axis 31 [DB61]) See: PLC user interface (DB3x) (Page 202), SIC/SCC (Page 201)
NC	• Transfers status and control information (SIC/SCC, axis DB) between the F-PLC and DRIVE • Transfers PROFIsafe telegrams (safety program, PAE/PAA) between F-PLC and DRIVE • Reads-in safety-relevant messages/signals from the message buffers of SINAMICS Safety Integrated into the NC alarm buffer

HMI	• Displays safety-relevant messages/alarms from the NCK alarm buffer • Reading out and displaying additional safety-relevant diagnostics information directly from the drive • Displays a safety delete symbol for active safety messages See: Diagnostics (Page 291)
DRIVE (SINAMICS Safety 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 75) • 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 41), F-I/O for PROFIBUS DP (Page 30), F-I/O for PROFINET IO (Page 30)
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 75), Drive components (Page 31)

3.6 Hardware components

Overview

The SINUMERIK Safety Integrated plus (F-PLC) 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 30) or PROFINET IO (Page 30) - as known from SIMATIC Safety.

The drive system that you can use (Page 31) depends on whether a safety-relevant encoder is used - and which axis type is to be used.

3.6.1 Configuration diagram

Hardware components

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

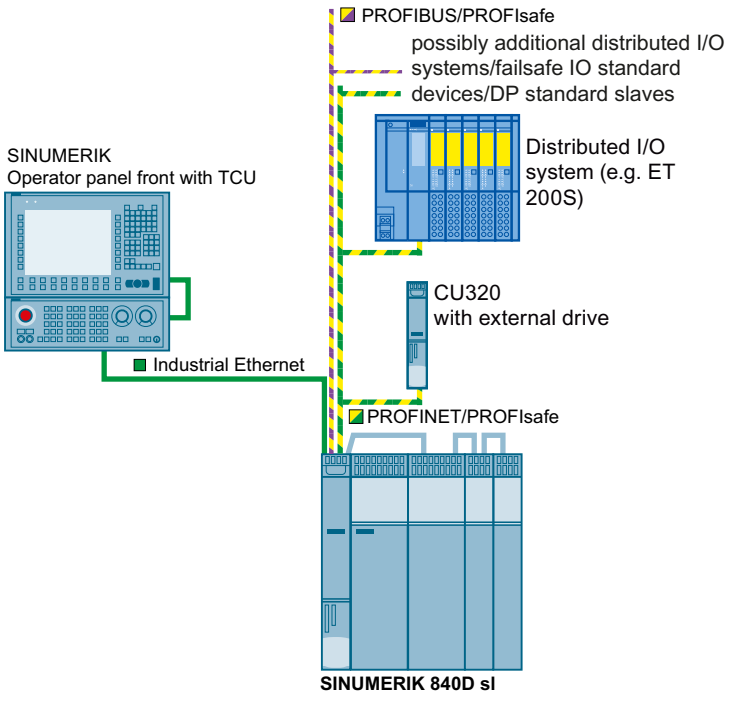


Figure 3-2 Configuration diagram: Hardware structure with SINUMERIK Safety Integrated plus

3.6.2 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:
  - S7-300 failsafe signal modules in ET 200M
  - ET 200MP failsafe modules
  - ET 200SP failsafe modules
  - ET 200S failsafe modules
  - ET 200pro failsafe modules
  - 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.

3.6.3 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:
  - S7-300 failsafe signal modules in ET 200M
  - ET 200MP failsafe modules
  - ET 200SP failsafe modules
  - ET 200S failsafe modules
  - ET 200pro failsafe modules
  - ET 200iSP failsafe modules
  - Failsafe GSD based I/O devices (light grid, laser scanner, etc.)

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

3.6.4 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 33) or SINAMICS HLA (Page 33).

3.6.4.1 Interconnecting DRIVE-CLiQ components

The maximum number of drives connected to a DRIVE-CLiQ line is limited to 4 drives as a result of the increased communication traffic for Safety Integrated plus. If you wish to operate more drives, then distribute these over various DRIVE-CLiQ lines.

3.6.4.2 Drive monitoring with or without encoder

In the SINUMERIK Safety Integrated plus system, safety operation without using an encoder is only supported for spindles equipped 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 commissioning area of SINUMERIK Operate (Page 254).

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 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	-	x[3]	x	x[1]	Safe Torque Off / Safe Stop according to Stop Category 1 of DIN EN 60204-1.
STO Extended Safe Torque Off	-	x	x[3]	x	x[1]	Safe Torque Off
SBC Safe Brake Control	x	x	-	x	x[1]	Safe brake control
SS1 Extended Safe Stop 1	-	x	x[3]	x	x[1]	Safe Stop according to Stop Category 1 of DIN EN 60204-1.
SS2/SOS Safe Stop 2 / Safe Operating Stop	-	x	x[3]	x	-	Safe Stop according to Stop Category 2 of DIN EN 60204-1 / Safe Operating Stop
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
SBT Safe Brake Test	-	x	-	x	-	Safe Brake Test
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 Supported axis types as a function of the drive type and the use of a safety-relevant encoder (Page 31).

[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 33).

3.6.4.3 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).

3.6.4.4 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 plus 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.
- 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 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 license (Page 36).

3.7 Safety components and licensing

3.7.1 Software components required

To configure Safety Integrated plus (F-PLC), in addition to SIMATIC STEP 7 Professional (TIA Portal) with option package SINUMERIK STEP 7 Toolbox, you also require the licensed STEP 7 Safety Advanced option package.

When installing STEP 7 Safety Advanced, the Safety Integrated plus functionality of the SINUMERIK Toolbox is also enabled in the TIA Portal.

Engineering system:

- SIMATIC STEP 7 Professional V15
- SIMATIC STEP 7 Safety Advanced V15
- SINUMERIK STEP 7 Toolbox V15

NCU:

- Firmware version 4.91
- HMI software SINUMERIK Operate 4.91

3.7.2 Licensing axes/spindles and F-PLC

To use Safety Integrated plus (F-PLC), 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 for the use of Safety Integrated plus (F-PLC)

Software option	Article No.	Purpose
SINUMERIK 840D sl Safety Integrated plus /SI logic	6FC5800-0AS60-0YB0	Activate the F-PLC in SINUMERIK 840D sl in order to process the failsafe sensors and actuators in an F-program.
SINUMERIK 840D sl Safety Integrated plus / SI axis/spindle	6FC5800-0AK00-0YB0	Use the motion control functions of the SINAMICS Safety Integrated in the SINUMERIK Safety Integrated plus (F-PLC) mode. License for one axis/spindle, multiple licensing in order to be able to use further axes/spindles.
SINUMERIK 840D sl Safety Integrated plus / SI multi-axis package	6FC5800-0AS61-0YB0	Use the motion control functions of the SINAMICS Safety Integrated in the SINUMERIK Safety Integrated plus (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 plus /SI-Logic basic option
- MD19121 $MN_NUM_DRIVEBASED_SAFE_AXES: Number of axes/spindles in Safety Integrated plus (F-PLC) mode

See also:

Collection of documents SINUMERIK 840D sl Base Software and Operating Software, Commissioning Manual SINUMERIK Operate (IM9)

3.8 Representation of safety-related resources in the TIA Portal

Overview

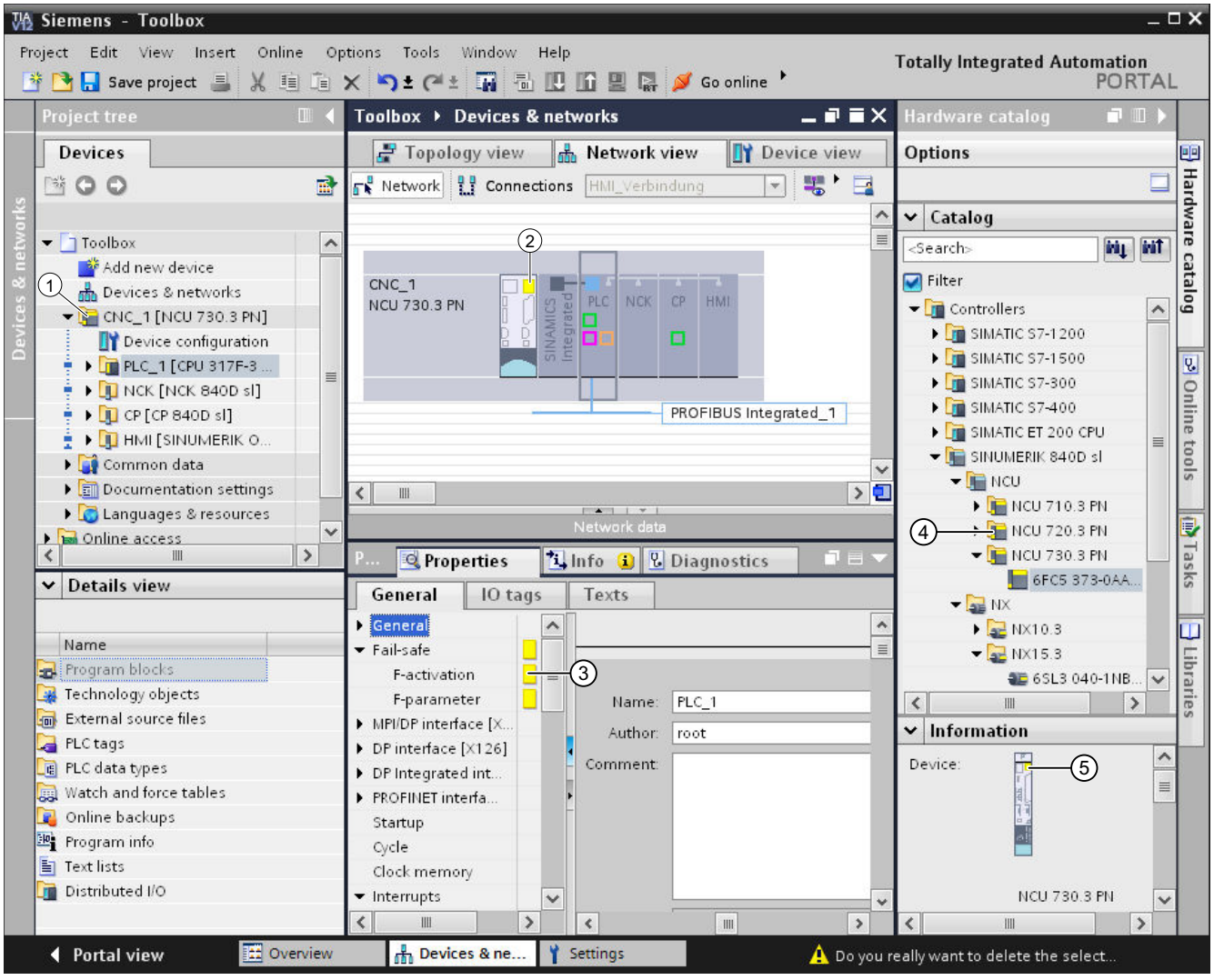
All safety-relevant resources are marked yellow in the TIA Portal, e.g. in the following views:

- 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 PLC and SINAMICS subcomponents support Safety Integrated Functions, the higher-level NCU is marked as related resource.
- Integrated PLC
- Integrated SINAMICS Safety 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 SINUMERIK 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 plus (F-PLC)

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

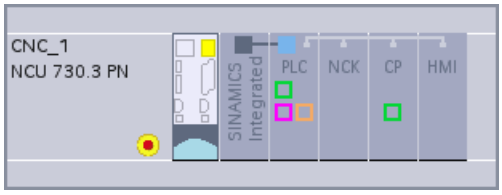


Figure 3-4 NCU with EMERGENCY STOP button symbol

Safety program of the F-PLC 4

4.1 Overview

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-relevant 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 ensure the safe processing of field information (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 can be provided through a user safety function or a fault reaction 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 210) Safety Integrated plus in the properties of the NCU, then also 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 create 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-relevant 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.

4.2 Structure of the safety program

Representation of program structure

The structure of a safety program (or an F-runtime group) of the PLC of a SINUMERIK 840D sl (F-PLC S7-300) is schematically shown in the following diagram.

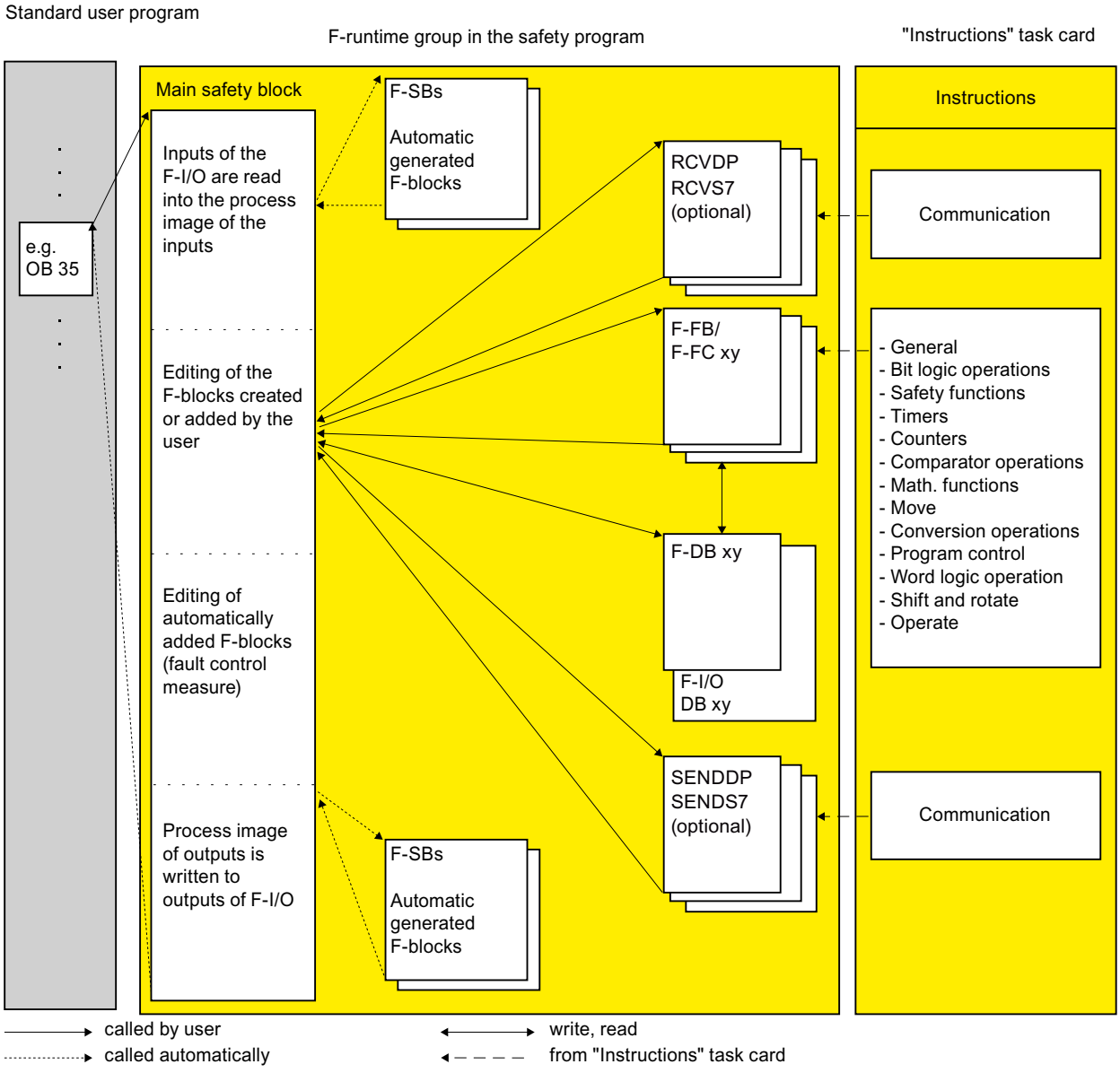


Figure 4-1 Schematic structure of a safety program

Main safety block

The main safety block is the first F-block of the safety program that you program yourself. During compiling, it is supplemented by additional invisible calls of F-system blocks.

You must assign the main safety block to an F-runtime group (Page 56).

The main safety block is called in an F-CPU S7-300 from any block belonging to the standard user program. We recommend a call from an OB 3x.

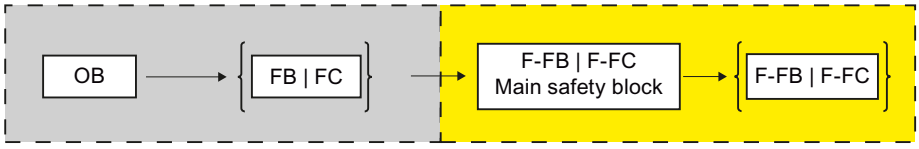


Figure 4-2 Calling the main safety block

F-runtime group

To improve handling, a safety program comprises one F-runtime group. An F-runtime group is a logical arrangement comprising several contiguous F-blocks, which are internally formed by the F-system.

An F-runtime group is made up of the following components:

- Main safety block (F-FB/F-FC, which you assign to the calling OB)
- F-blocks that you generated yourself - or that you inserted:
  - F-blocks from the project library or from global libraries
  - Possibly other F-FBs/F-FCs, which you program with FBD/LAD - and that you call from the main safety block
  - Possibly one or several F-DBs
- Automatically added F-blocks:
  - F-I/O DBs
  - F-system blocks (F-SB)
  - Automatically generated F-blocks

Block types and number ranges of the safety program

An F-runtime group is automatically created - together with the associated blocks - when you activate the Safety Integrated plus (F-PLC) mode.

- Calling block: CYC_INT5_RTG1 [OB35]
- Main safety block: Main_Safety_RTG1 [FB1010]
- I-DB for the main safety block: Main_safety_RTG1_DB [DB1010]

Number range reserved for SINUMERIK

In order to avoid assigning block addresses or numbers twice, the F blocks are automatically assigned a free number within a certain number range reserved for SINUMERIK. You can also

subsequently change the numbers of F blocks in the block properties. However, only use the number range that has been reserved:

- Number range reserved for F-FB, F-FC and F-DB of F execution groups
  - F-FB 1010..1019
  - F-FC 1010..1019
  - F-DB 1010..1019
- Additional number range for F blocks (e.g. generated F system blocks)
  - F-FB 3999..7999
  - F-FC 3999..7999
  - F-DB 8000..16000

If you configure F I/O, then automatically an F I/O DB is created within this number range. You can change the number of an F I/O DB in the properties of the associated F I/O.

4.3 Fail-Safe Blocks

Main safety block

For the integrated PLC of the SINUMERIK 840D sl (PLC 317F-3 PN/DP or PLC 319F-3 PN/DP), the main safety block is a F-FC or F-FB (with instance DB), which is called by a standard block (recommendation: OB 35) from the standard user program.

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 tags of the F-I/O DB in conjunction with F-I/O accesses.

F-shared DB

The F-shared DB is a failsafe data block that contains all of the shared data of the safety program and additional information needed by the F-system.

Note

It is not permissible that you add, change or delete blocks in the "System blocks" folder. If this is not complied with, then this can result in compilation errors or the F-PLC stopping.

Note

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

Additional information

Detailed information about the safety program blocks can be found at Procedure when specifying an F-runtime group (Page 56).

4.4 Safety Administration Editor

The "Safety Administration Editor" is available in the Safety Integrated plus (F-PLC) mode - in the project navigation.

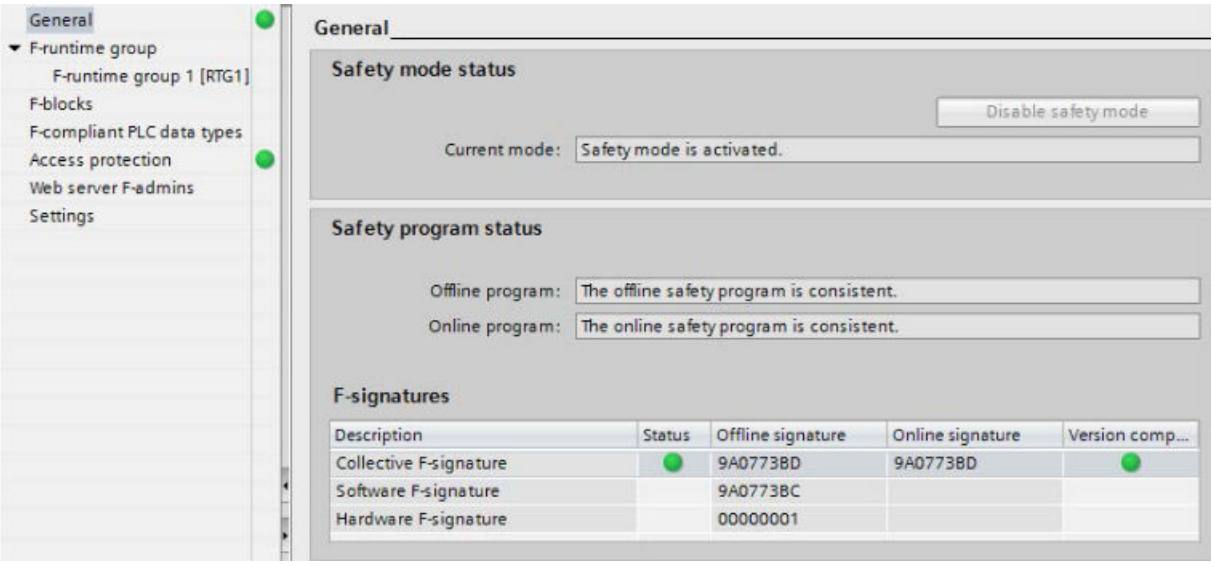


Figure 4-3 Safety Administration Editor

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

- Display of the safety program status
- Display of the collective signature
- Display of the safety mode status
- Creation/organization of F-runtime groups
- Display of information on the F-blocks
- Definition/change of the access protection
- Definition/change of the general settings for the safety program

The Safety Administration Editor is divided into the following sections:

- General
- F-runtime groups (Page 56)
- F-blocks
- Access protection
- Settings

Further information

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

4.5 Restrictions in the programming languages FBD/LAD

LAD and FBD programming languages

Generally, the user program in the F-PLC comprises a standard application 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.

Supported instructions

The instructions available depend on the F-PLC being used. SINUMERIK 840D sl supports all F-CPU S7-300 instructions.

Note

Preconnection of enable input EN or evaluation of enable output ENO is not possible.

Supported data types and parameter types

Only the following data types are supported:

- BOOL
- INT
- WORD
- DINT
- DWORD
- TIME

Note

If the result of an operation lies outside the range permissible for the specific data type, then the F-PLC can go into STOP. The cause of the diagnostic result is entered in the diagnostics buffer of the F-PLC.
Additional information regarding the cause is available in the online help for the diagnostics message. You must therefore ensure that the permitted range for the data type is observed when creating the program or select a matching data type.

Non-permitted data and parameter types

The following types are **not** permitted:

- All types not listed in the section "Supported data types and parameters types" (e.g. BYTE, REAL)
- structured data types (e.g. STRING, ARRAY, STRUCT, PLC data type)
- Parameter types (e.g., BLOCK_FB, BLOCK_DB, ANY)

Supported operand areas

The system memory of an F-PLC is structured in the same operand area as that of a standard PLC. You can access the operand areas listed in the table below from within the safety program.

Note that you can access data in the safety program only via the declared data type for the tag/element of an F-compliant PLC data type:

- For the BOOL data type only bit by bit
- For the INT data type only word by word
- For the WORD data type only word by word
- For the DINT data type only double word by double word
- For the DWORD data type, only double word by double word
- For the TIME data type only double word by double word

Example: You can only access input channels, data type BOOL in the process image of the inputs of F I/O via unit "Input (bit)".

Byte access to eight consecutive input channels of the BOOL data type is not allowed.

For reasons of clarity, you should always access operand areas in a safety program using symbolic names.

Table 4-1 Supported operand areas

Operand area	Access via units of the following size:	S7 Notation	Description
Process image of the inputs			
• Of F-I/O	Input (bit) Input word Input double-word	I IW ID	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 before the start of the main safety block.
• Of standard I/O	Input (bit) Input word Input double-word	I IW ID	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.

Operand area	Access via units of the following size:	S7 Notation	Description
Process image of the outputs			
• Of F-I/O	Output (bit) Output word Output double-word	Q QW QD	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 calculated 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 (bit) Output word Output double-word	Q QW QD	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	Bit memory (bit) Memory word Memory double word	M MW MD	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-accessed 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	Access via units of the following size:	S7 Notation	Description
• F-DB	Data bit Data word Data double word	DBX DBW DBD	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	Data bit Data word Data double word	DBX DBW DBD	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.

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 (Page 46) and in the F global DB (Page 46).
- I/O area: Inputs
- I/O area: Outputs

Boolean constants "0" or "FALSE" and "1" or "TRUE" (S7-300, S7-400)

If you require Boolean constants "0" or "FALSE" and "1" or "TRUE" in your safety program to assign parameters during block calls, you can access the tags "VKE0" and "VKE1" in the F-shared DB using fully qualified DB access ("F_GLOBDB".VKE0 or "F_GLOBDB".VKE1).

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 the initialization of the local data element is **not** skipped over by JMP, JMPN. or RET instructions (branching).

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.

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. You can find additional information on the cause in the online help for diagnostic messages.

"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.

For F-PLCs S7-300/400, only the first access must be realized as "fully qualified DB access" Alternatively, you can use the instruction "OPN".

Example of "fully qualified DB access":

Assign a name for the F-DB, e.g. "F_Data_1". Use the names assigned in the declaration of the F-DB instead of the absolute addresses.

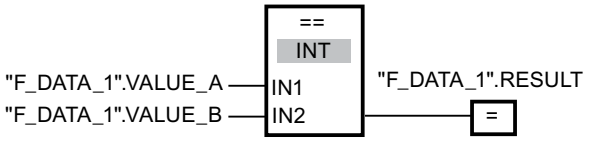


Figure 4-4 Example with fully qualified access and symbolic names

Example of "not fully qualified DB access":

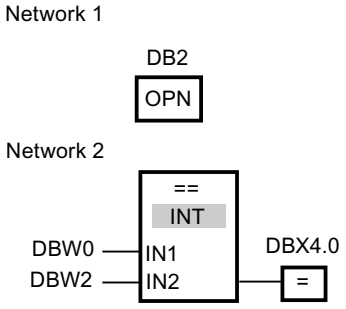


Figure 4-5 Example without fully qualified access and symbolic names

Access to instance DBs

Please note that when accessing instance DBs of F-FBs, which are not called in the safety program, can result in the F-PLC going into STOP.

Additional information is provided in the SIMATIC Safety Programming and Operating Manual.

4.6 Instructions for the safety program

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

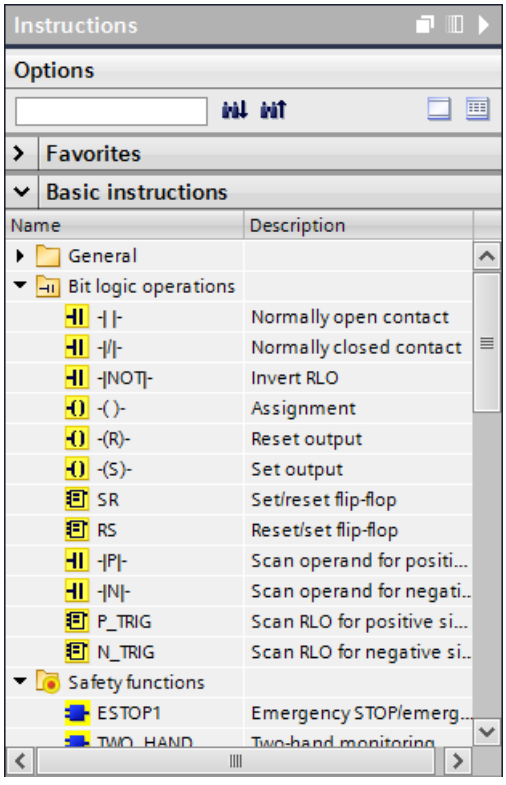


Figure 4-6 Task Card "Instructions"

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 operation.

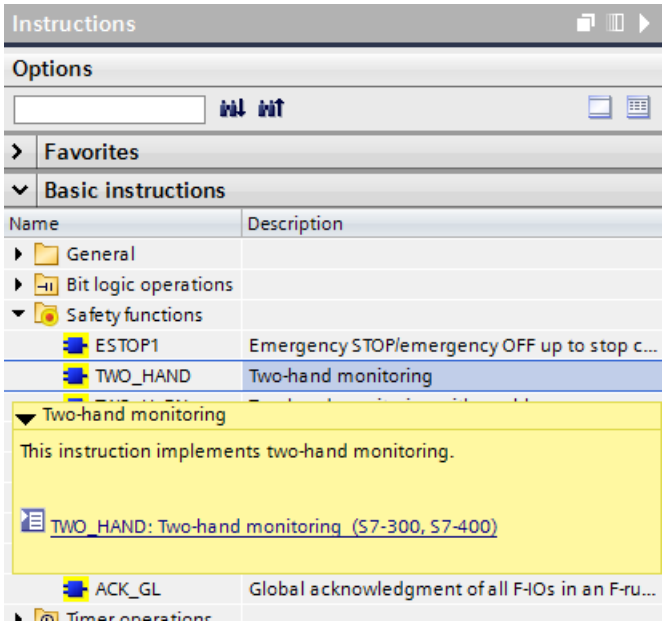


Figure 4-7 Tooltip of an instruction

4.7 F-runtime groups

4.7.1 Rules for F-Runtime Groups of the Safety Program

General rules relating to the safety program

Carefully comply with the following general rules when programming with F-blocks and F-runtime groups:

- 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).
- Individual tags of F-DBs (except the F-shared DB) can only be used in one F-runtime group (however, an F-DB can be used in more than one F-runtime group).
- The process image of inputs and outputs of standard I/O, bit memories and tags of the DB of the standard user program may be accessed, either reading or writing, from several F-runtime groups. (see also Data exchange between the standard user program and safety program (Page 70))

You can find additional specific rules at Procedure when specifying an F-runtime group (Page 56).

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 distributing your program between a standard user program and safety program, you should note that you can change the standard user program more simply and load to the F-PLC. In general, changes in the standard user program do not require an acceptance.

4.7.2 Procedure when specifying an F-runtime group

An F-runtime group comprises a block (cyclic interrupt (OB3x), FB or FC), which calls the main safety block (FB or FC).

Automatically creating the safety program

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

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

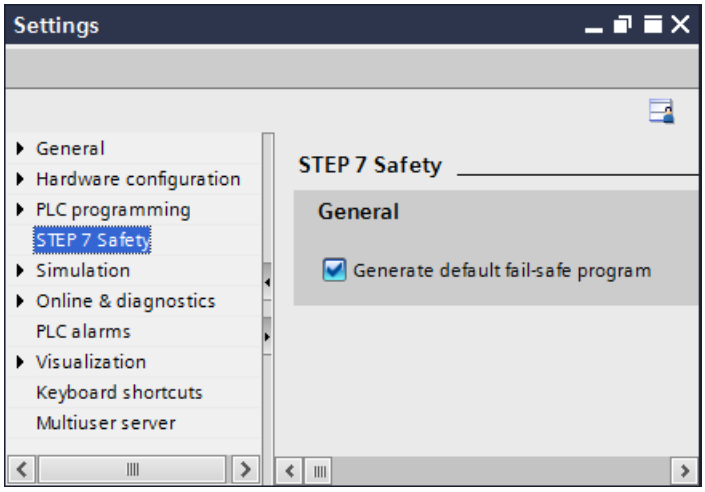


Figure 4-8 Settings for STEP 7 Safety

Archiving the F blocks

The automatically created F-blocks of the F-runtime group are in folder "Program blocks": CYC_INT5_RTG1 [OB35], Main-Safety_RTG1 [FB1010] and Main-Safety_RTG1_DB [DB1010].

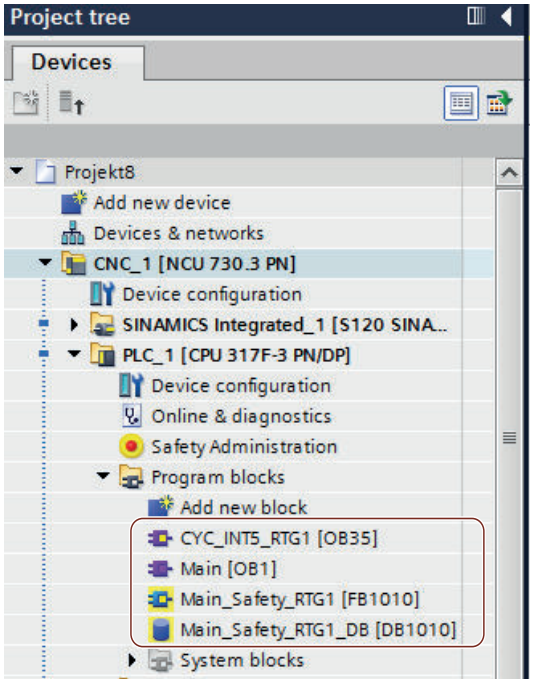


Figure 4-9 F runtime group blocks in the project navigator

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.

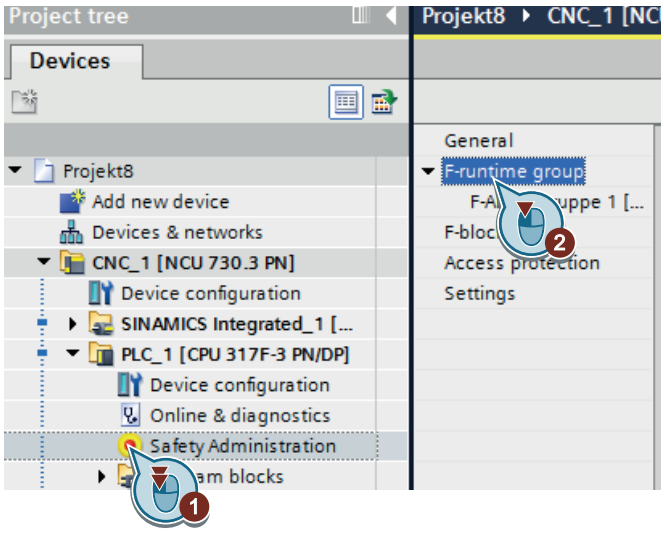
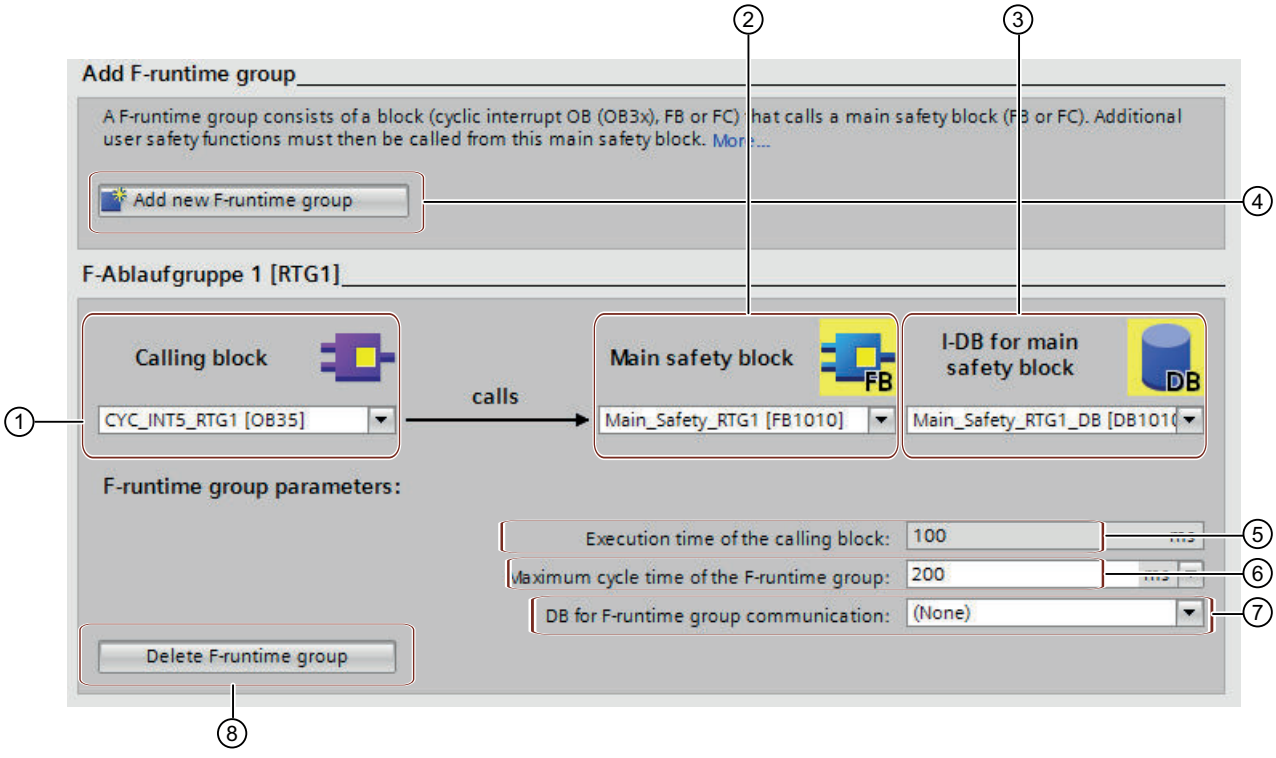


Figure 4-10 Displaying the "F runtime group" work cell

"F runtime group" work cell



① Calling block
② Main safety block
③ I-DB for the main safety block
④ Create a new F-runtime group
⑤ Execution time of the calling block
⑥ Maximum cycle time of the F-runtime group
⑦ DB for F-runtime group communication
⑧ Delete F-runtime group

Figure 4-11 Safety Administration Editor, "F runtime group" work cell

Calling block

The default value is "CYC_INT5_RTG1 [OB35]", a cyclic interrupt OB.

The advantage of using cyclic interrupt OBs is that they interrupt the cyclic program execution in OB 1 of the standard user program at fixed time intervals; that is, the safety program is called and executed at fixed time intervals in a cyclic interrupt OB.

Programming language

In the drop-down list "Calling block", you can only select blocks that were generated in the programming languages LAD, FBD or STL.

If you want to call the main safety block in a block that was created in another programming language, you must program this call itself. The text box is then inactive (grayed out), and you cannot change the call in the Safety Administration Editor, but only in the calling block.

Rules:

- The main safety block may only be called once from a standard block. Calling the block a multiple number of times can result in the F-PLC going into a STOP.
- To optimally utilize the temporary local data, you must call the F runtime group (the main safety block) directly in an OB (if at all possible, a cyclic interrupt OB); in this cyclic interrupt OB you should not declare any additional temporary local data.
- Within a cyclic interrupt OB, the F runtime group should be executed **before** the standard user program, i.e. should be located right at the beginning of the OB so that the F runtime group is always called at fixed intervals in time, independent of how long it takes to process the standard user program.
  This is also the reason that the cyclic interrupt OB should not be interrupted by higher-priority alarms.

Main safety block

In the "Number" text field, enter a free block number reserved for SINUMERIK Safety Integrated: 1010..1019.

Rules:

- F-FBs can be used in several F-runtime groups; however, they must be called with different instance DBs.
- F-FCs can always be called in several F-runtime groups.

I-DB for the main safety block

In the "Number" text field, enter a free block number reserved for SINUMERIK Safety Integrated: 1010..1019.

Rules:

- Instance DBs may only be accessed from the F-runtime group in which the associated F-FB is called

Create a new F-runtime group

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

Execution time of the calling block

You can adapt the cyclic execution time of the calling block under "Alarms > Cyclic interrupts" in the PLC properties.

Maximum cycle time of the F-runtime group

In the the F-runtime group, the F-PLC monitors the F-cycle time For "Maximum cycle time of the F-runtime group", select the maximum time that can elapse between two calls of this F-runtime group.

The F-runtime group call interval is monitored for the maximum value; i.e. monitoring is performed to determine whether the call is executed often enough, but not whether it is executed too often. Therefore, failsafe times must be implemented using instructions TP, TON or TOF from the task card "Instructions" and not using a counter (OB calls). *(S007)*

DB for F-runtime group communication

If one F-runtime group is to provide tags for evaluation to another F-runtime group of the safety program, assign a DB for F-runtime group communication. Select an F-DB for "DB for F-runtime group communication".

Rules:

- It is only permissible to access an F-communication DB from an F-runtime group.
- A DB for F-runtime group communication may read and write to the F-runtime group, for which you set up a DB; the "receiving" F-runtime group may only read this F-DB.
- Individual tags of the F-runtime group DB may only be used in their own F-runtime group.

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.

4.7.3 F-global DB

Function

The F-shared DB is a fail-safe data block that contains all of the shared data of the safety program and additional information needed by the F-system. The F-shared DB is automatically inserted when the hardware configuration is compiled.

Using its name F_GLOBDB, you can evaluate certain data elements of the safety program in the standard user program.

Reading an F-shared DB in the standard user program

You can read out the following information in the F-shared DB in the standard user program or on an operator control and monitoring system:

- Operating mode: safety mode or disabled safety mode ("MODE" tag)
- Error information "Error occurred when executing safety program" ("ERROR" tag)
- Collective F-signature ("F_PROG_SIG" tag)
- Compilation date of the safety program ("F_PROG_DAT" tag, DATE_AND_TIME data type)

You use fully qualified access to access these tags (e.g. ""F_GLOBDB".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. Double-click on "Add new block" under "Program blocks" in the project tree.
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 the dialog is confirmed, the F-block is opened in the *Program editor*.

Note the following

Note the following important instructions:

Note

The main safety block must not contain any parameters, as they cannot be provided with actual values when the block is called.

Note

It is not permissible to edit the start values in instance DBs of F-FBs online and offline – and this can result in the F-PLC going into STOP mode.

Note

It is not permitted to access static local data in single instances or multi-instances of other F-FBs.

Note

Outputs of F-FCs must always be initialized.

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. You can find additional information on the cause in the online help for diagnostic messages.

Note

If you wish to assign an operand from the data area (data block) to a formal parameter of an F-FC as an actual parameter, you must use fully qualified DB access.

Note

Note that access to the inputs in an F-FB/F-FC is read-only, while access to the outputs is write-only.

Use an in/out if you wish to have both read and write access.

Note

For greater clarity, assign unique symbolic names to the F-blocks you have created. These symbolic names appear in the project tree and in the block interface. Symbolic names are assigned in the same way as for standard blocks.

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 must not copy blocks from the 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 *STEP 7* help in "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 instruction versions can be found in the help on *STEP 7* in "Basics 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 Safety-relevant communication

Options for safety-related communication

Safety-related communication	On subnet	Additional hardware required
I-slave-slave communication	PROFIBUS DP	—
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	—
I-slave-I-slave communication	PROFIBUS DP	—
IO controller-I-slave communication	PROFINET IO and PROFIBUS DP	IE/PB link
Safety-related communication via S7 connections	Industrial Ethernet	—
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
Safety-related communication to S7 Distributed Safety or S7 F Systems via S7 connections	Industrial Ethernet	—

Additional information

Additional information and configuration graphics are provided in the help for SIMATIC STEP 7 Safety Advanced in Chapter "Safety-relevant communication".

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

Overview

A description is subsequently provided as to how you can access the F-I/O and the safety-relevant drive telegrams; certain issues are also explained, that you must take into account when programming this access.

Access via the process image

You access F-I/O and drive telegrams (just the same as standard I/O and standard drive telegrams) via the **process image** (PAE and PAA).

Access is only permissible via the data type specified for the particular channel.

Example: You can only access input channels, data type BOOL in the process image of the inputs of F I/O via unit "Input (bit)" (E x.y). It is not possible to access 16 consecutive input channels, data type BOOL via unit "Input word" (EW x).

It is not permissible to directly access drive telegrams or F-I/O. Inputs or outputs of the F-I/O or drive telegrams, which you wish to access, must be activated in the hardware configuration. The channel value of an F-I/O or a drive telegram may only be accessed from a joint F-runtime group.

The process image of the inputs is updated at the start of the F-runtime group. The process image of the outputs is updated at the end of the F-runtime group (see Structure of the safety program (Page 43)).

The actual communication between F-PLC (process image) and the F-I/O or drive telegram to update the process image is realized in the background using a special security protocol according to PROFIsafe.

If, between the F-PLC (S7-300) and the F-I/O, you insert an additional component, which copies the safety telegram according to PROFIsafe between the F-PLC (S7-300) and the F-I/O using the user program, then for each change to the user-programmed copy function, you must carefully test all of the safety functions involved with the copy function. *(S049)*

Note

As a result of the special safety protocol, F-I/O and drive telegrams occupy a larger area of the process image than is required by real channels available on the F-I/O or the drive telegram (channel values and value status).

To find the area of the process image where the channels are stored, refer to the relevant *manuals for the F-I/O*. When the process image is accessed in the safety program, only the channels that are actually present may be accessed.

Note that for certain F-I/O (such as ET 200SP failsafe modules or ET 200MP fail-safe modules), a "1oo2 evaluation of the sensors" can be specified. To find out which of the channels combined by the "1oo2 evaluation of the sensors" you can access in the safety program, refer to the relevant manuals for the F-I/O.

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.

4.12 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 starts, all FDBs – just the same as for a cold start – are initialized with values from the load memory. This means that saved error information is lost. The F-system automatically re-integrates 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 signal after process values can be output without incurring any risk, and faults have been removed. *(S031)*

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, you declare a tag of data type BOOL with initial value "TRUE" in an F-DB.

Block the output of process data when this tag has the value "1," for example, by passivating F-I/O using the PASS_ON tag 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

4.13 Implementing a user acknowledgment

After communication, channel or F-I/O errors, the send data must be reintegrated.

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 a F-runtime group

In your safety program you must always provide a user acknowledgment to reintegrate F-I/O. You can implement the user acknowledgment as follows:

- User acknowledgment using an operation and visualization system
- User acknowledgment using an acknowledgment button at an 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 224)
- Additional information and examples are provided in the help for SIMATIC STEP 7 Safety Advanced under keywords "ACK_REI", "ACK_GL" as well as in Chapter "Implementing a user acknowledgment".

4.14 Data exchange between the standard user program and safety program

4.14.1 Comparison between 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

For data exchange between standard user program and safety program, we recommend that you define special data blocks (transfer blocks) in which the data to be exchanged is stored. This action allows you to decouple the blocks of the standard and the safety program. The changes in the standard program do not affect the safety program (and vice versa) provided these data blocks are not modified.

4.14.2 Data Transfer from the Safety Program to the Standard User Program

Description

The standard user program can read all data of the safety program, for example using symbolic (fully qualified) accesses to the following:

- 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

Process image of the inputs and outputs: Access and update

The process image of the inputs of F-I/O is updated not only at the start of the main safety block, but also by the standard operating system.

To find the standard operating system update times, refer to the *Help on STEP 7* under "Process image of the inputs and output". For F-CPUs that support process image partitions, also bear in mind the update times when process image partitions are used. For this reason, when the process image of the inputs of F-I/O is accessed in the standard user program, it is possible to obtain different values than in the safety program. The differing values can occur due to:

- Different update times
- Use of failsafe values in the safety program

To obtain the same values in the standard user program as in the safety program, you must not access the process image of the inputs in the standard program until after execution of an F-runtime group. In this case, you can also evaluate the QBAD or QBAD_I_xx tag in the associated F-I/O DB in the standard user program, in order to find out whether the process image of the inputs is receiving failsafe values (0) or process data. When using process image partitions, also make sure that the process image is not updated by the standard operating system or by the UPDAT_PI instruction between execution of an F-runtime group and evaluation of the process image of the inputs in the standard user program.

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 48)):

Data block/bit memory

In order to write safety program data directly to the standard user program (e.g., DIAG output of the SENDDP instruction), you can write to data blocks of the standard user program from the safety program. 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.

4.14.3 Data Transfer from Standard User Program to Safety Program

Description

As a basic principle, only fail-safe data or fail-safe signals from F-I/O and other safety programs (in other F-CPUs) can be processed in the safety program, as standard tags are unsafe.

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 48)).

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 facilitate checks, all PLC tags from the standard user program that are evaluated in the safety program are included in the safety summary.

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.

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-safety-related tags from the standard user program, for example, using operations "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 out variables that can be changed from the standard user program

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.

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

You must write variables from the standard user program to these bit memories or variables of a standard DB before calling the F-runtime group.

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. You can find additional information on the cause in the online help for diagnostic messages.

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 254).

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

Different grouping of the SLP, SP and SCA Safety Functions for SINAMICS und SINUMERIK

- SINUMERIK: SLP, SP and SCA = Extended Functions
- SINAMICS: SLP, SP and SCA = Advanced Functions

For reasons of uniformity, these functions are called Extended Functions in the complete Manual.

Note

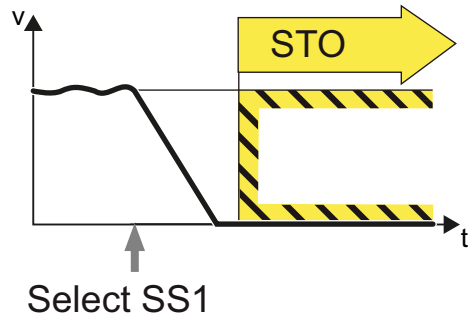
Term "Control Unit" in this documentation

In the Safety Integrated plus 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 function SS1 brakes the motor and trips the function STO after a delay time."



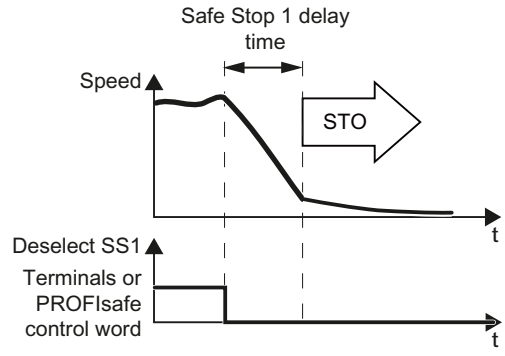
Example of how the function can be used

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" 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 the 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 inverter 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 brake 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 93)".

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 suppression 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

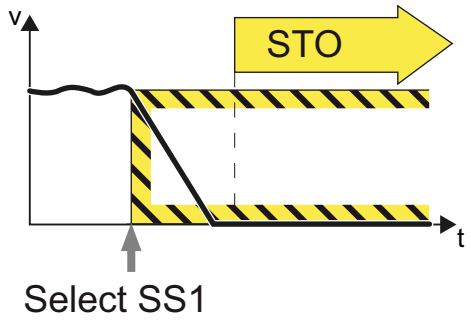
5.2 SS1

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

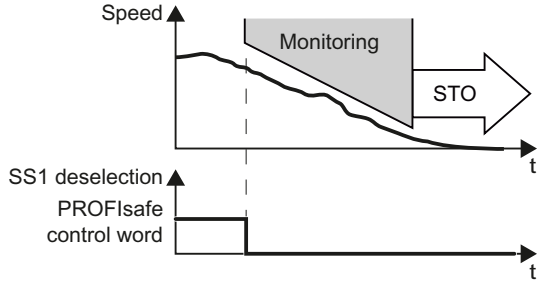
Example	Possible solution
A central Emergency Stop button ensures that several drives are braked as quickly as possible and brought into the STO state.	• Evaluating an Emergency Stop pushbutton in an F-PLC • Select SS1 via PROFIsafe. • SS1 brakes the drives and then brings them into the STO state.

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 .



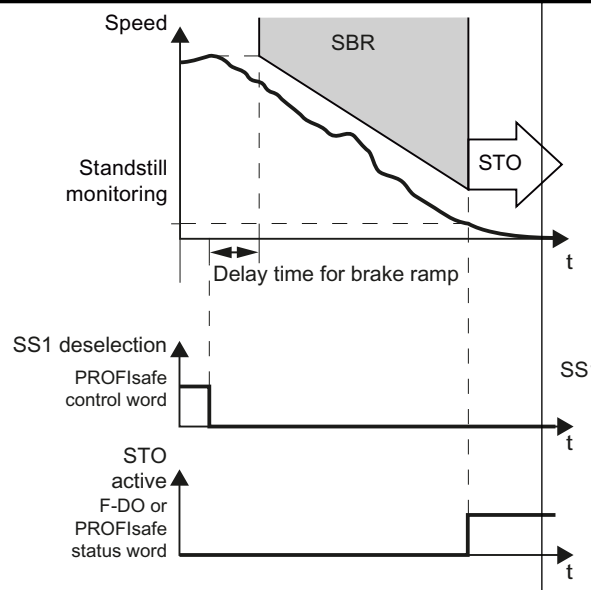
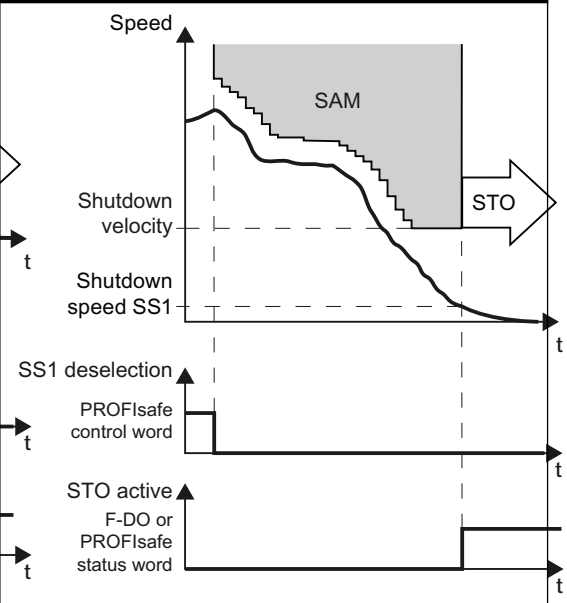
Select SS1

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)

Brake ramp monitoring (with or without encoder)	Acceleration monitoring (with or without encoder)
	
• 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).	• 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.

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 133)").
  In this case, we also talk about "SS1 (time and acceleration controlled)".
- **For p9506 = 2, the following applies:**
  Here, also for SS1, the monitoring function "Safe Brake Ramp" is active (see Chapter "SBR (Page 135)").
  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 suppression (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 82).
  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 135)." In this case, we also talk about "SS1 (speed controlled)".

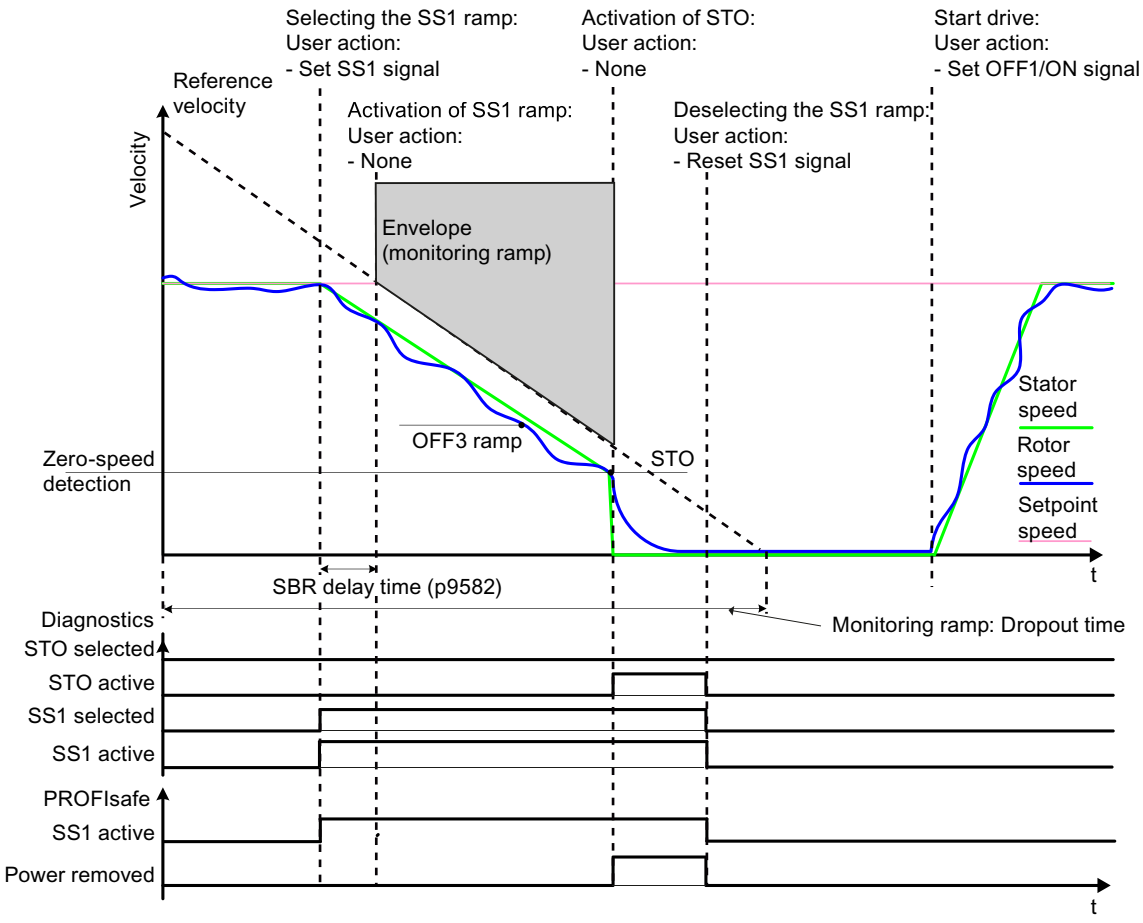


Figure 5-1 Sequence for "Safe Stop 1" without encoder with SBR monitoring (p9506 = 1)

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 315).

Constraint

> **Note**
>
> The function is configurable; however, the brake behavior using SS1E is not supported by the NC (path stop).

See also

SBC (Basic/Extended) (Page 93)

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

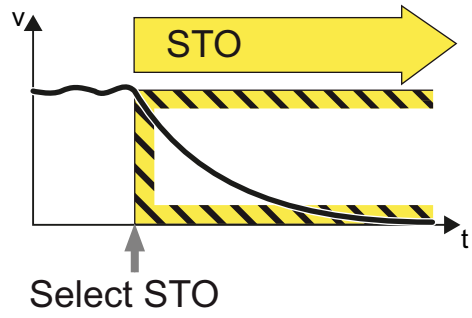
Only for SS1 (Extended Functions) with external stop

- 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."



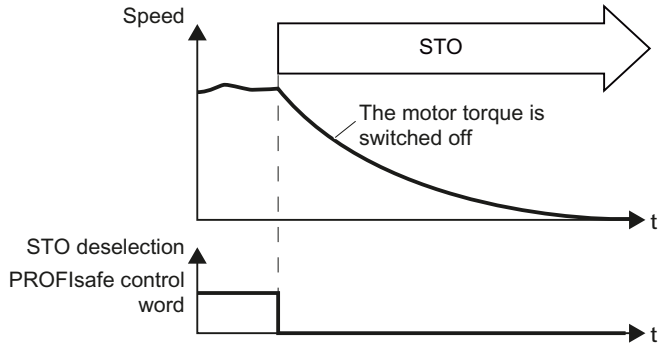
Examples of how the function can be used

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 324), 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 93)".

⚠ 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 93)".

[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 suppression 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 suppression 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.

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 suppression

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
- r9722 CO/BO: SI Motion drive-integrated status signals
- r9772 CO/BO: SI Status (Control Unit)
- r9773 CO/BO: SI Status (Control Unit + Motor Module)
- r9774 CO/BO: SI Status (group STO)

For the HLA module, Safe Torque Off (STO) corresponds to shutting off a safety-relevant 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-relevant output (PROFIsafe feedback signal telegram).

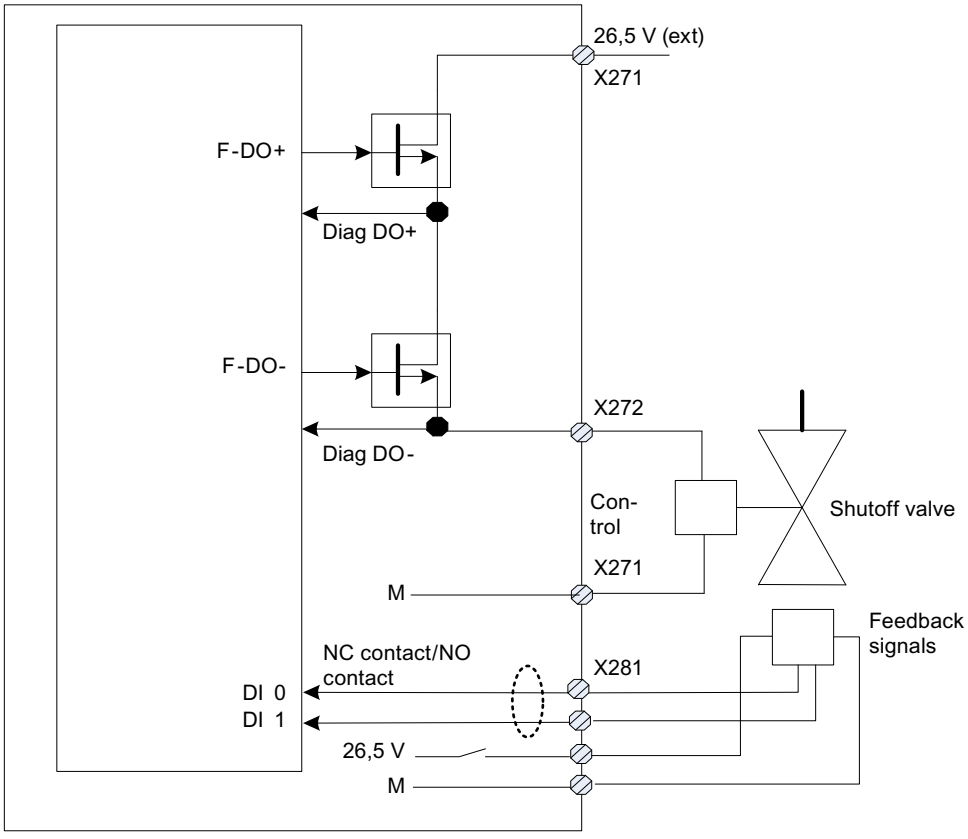


Figure 5-2 Interconnecting the shutoff valve (for an axis)

- 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.

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 suppression

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

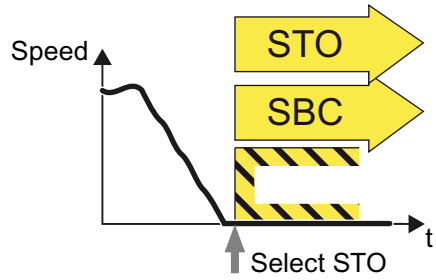
- p9625[0...1] SI HLA shutoff valve wait time (CU)
- p9626 SI HLA shutoff valve feedback contacts configuration (CU)
- r9773 CO/BO: SI Status (Control Unit + Motor Module)

- 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

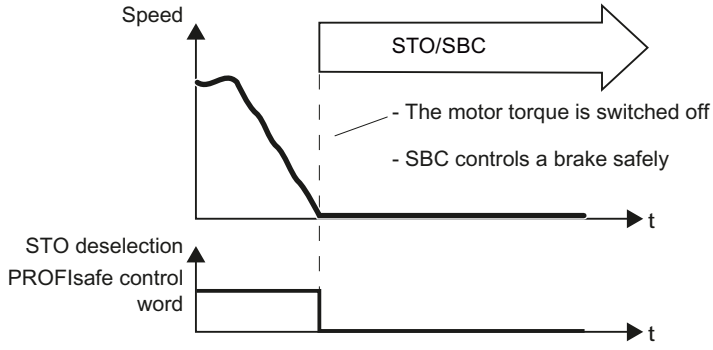
Example	Possible solution
The safe control of a motor holding brake must be guaranteed in order to guarantee the motor is at a standstill.	SBC is (if configured) initiated together with STO. The Motor Module / Safe Brake Relay / Safe Brake Adapter then carries out the action and safely controls the outputs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

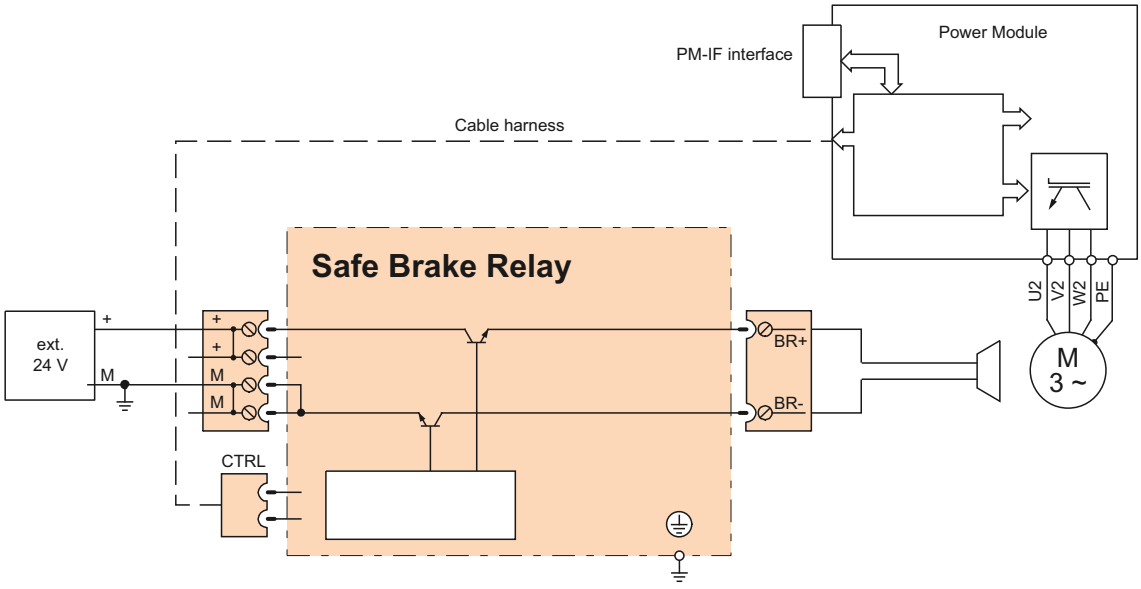


Figure 5-3 Interconnecting the Safe Brake Relay using Blocksize as an example

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.

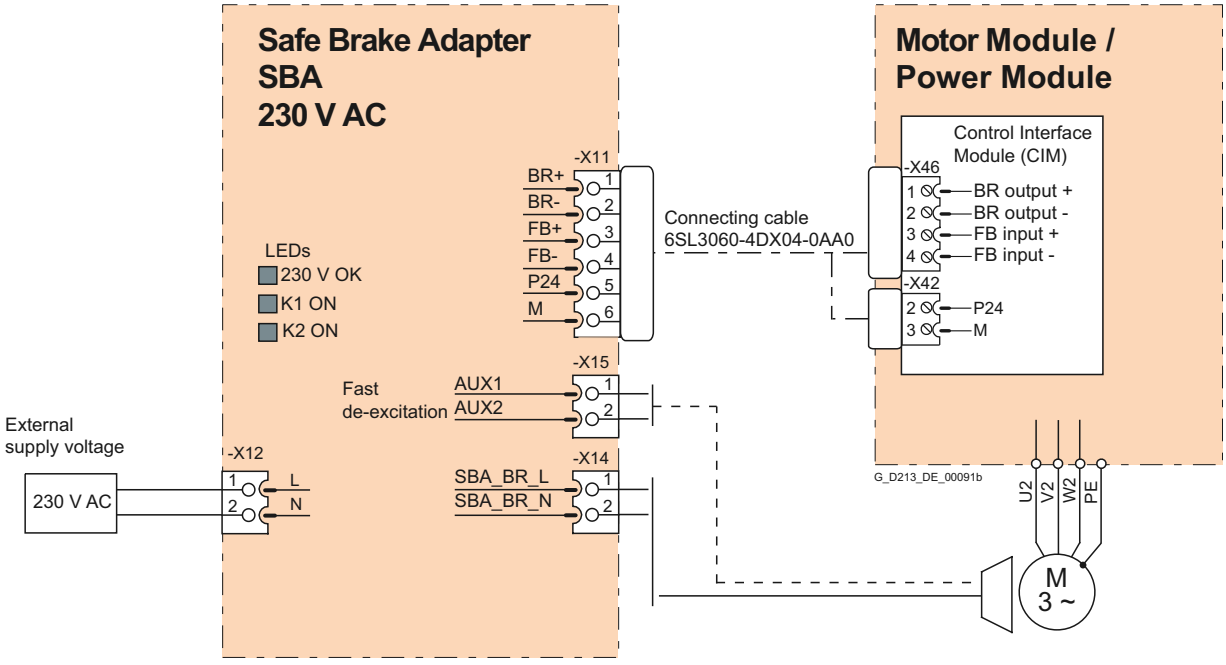


Figure 5-4 Interconnecting the Safe Brake Adapter

5.4.2 Details and parameterization

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

No SBC for SINAMICS HLA

SINAMICS HLA does not support Safe Brake Control.

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 SINAMICS S120M, an interrupted cable is only detected when the brake is opened. 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 159)").

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. The selection of SBC alone is not possible.

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.

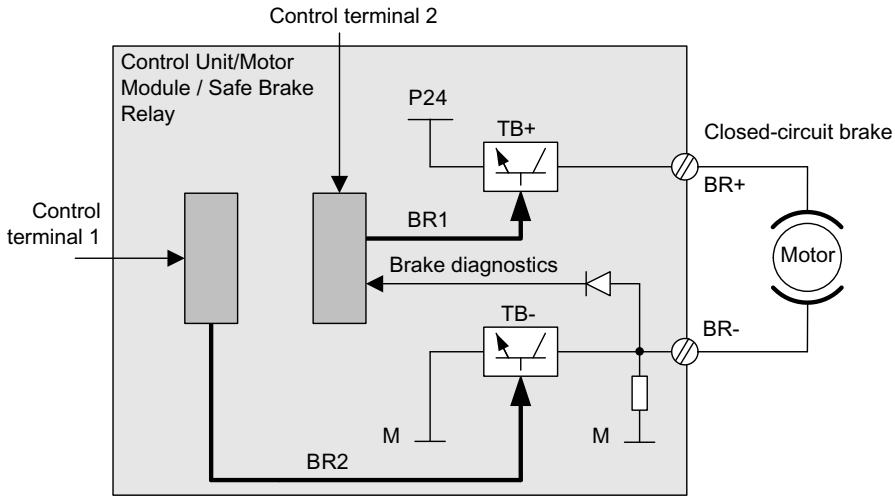


Figure 5-5 Two-channel brake control, blocksize (example)

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)

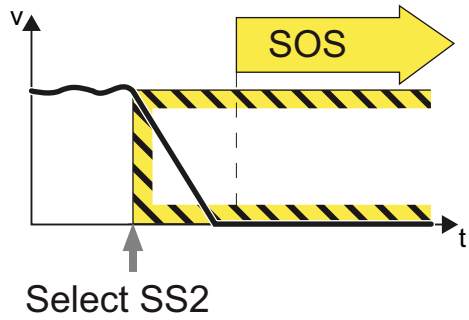
5.5 SS2

Definition according to EN 61800-5-2:

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

- SS1-a with acceleration monitoring (SAM)
- SS1-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.

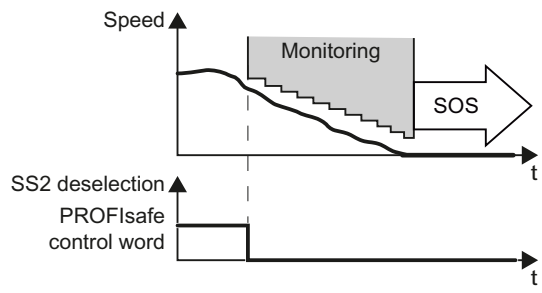


Example of how the function can be used

Example	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 the Safe Operating Stop function (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 the Safe Operating Stop function (SOS). This function monitors the safe standstill of the drive.

Braking behavior

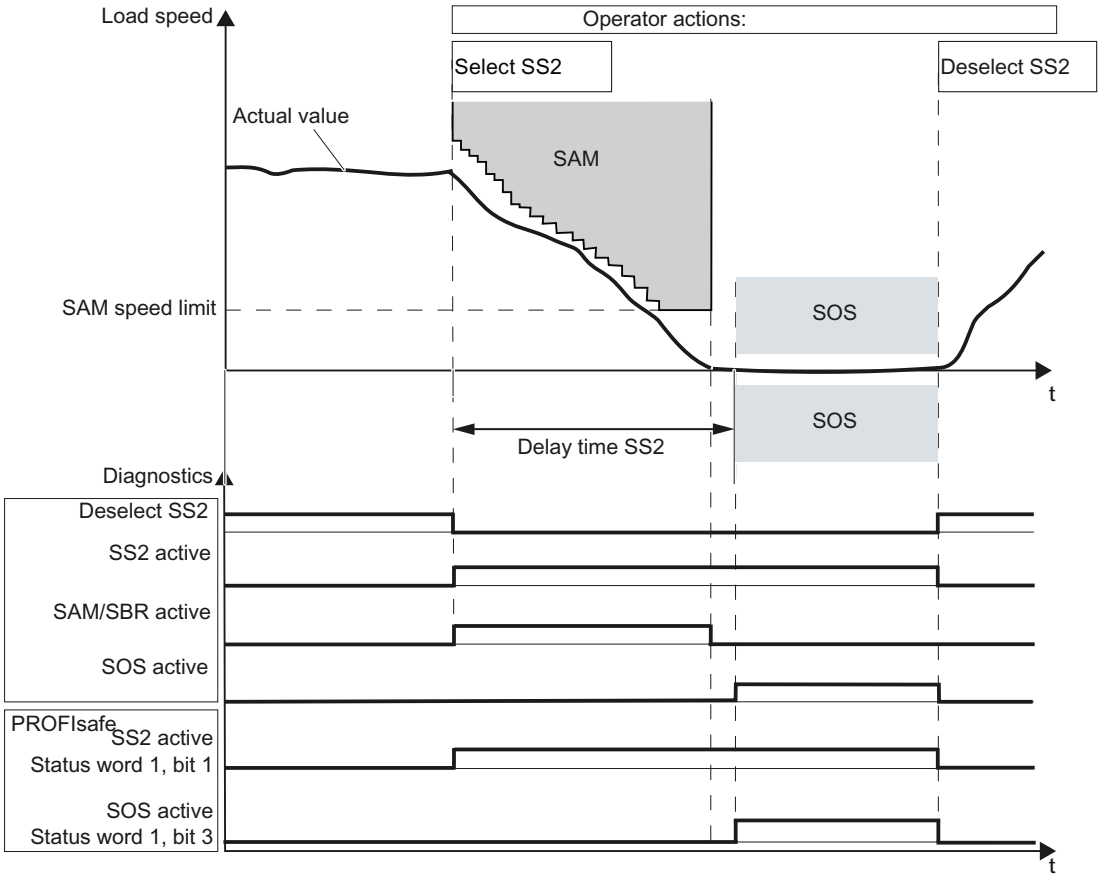


Figure 5-6 Braking behavior and diagnostics (example for SS2 with SAM)

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 "Safe Operating Stop") 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 133)").
- **For p9506 = 2, the following applies:**
  Here, also for SS1, the monitoring function "Safe Brake Ramp" is active (see Chapter "SBR (Page 135)").

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

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)

- 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)]
- r9722.0...15 CO/BO: SI Motion drive-integrated status signals

[1)] STOP C corresponds to SS2.

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.

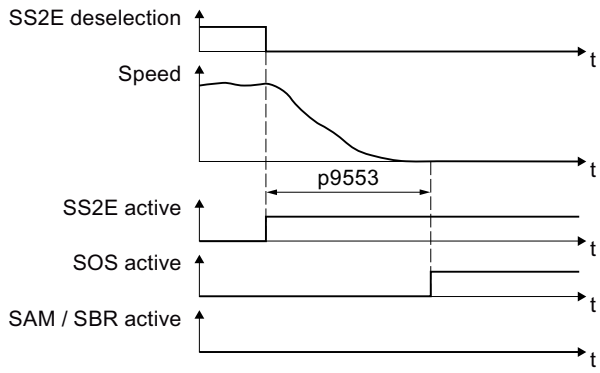


Figure 5-7 Selecting function SS2E

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

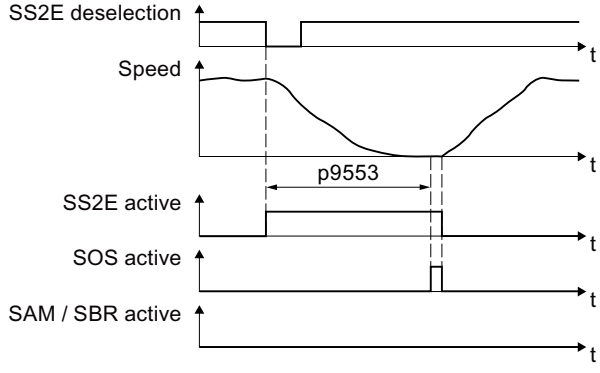


Figure 5-8 Deselecting function SS2E while SS2E is active

After the function has been selected, the delay time starts to expire - 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, the drive may accelerate the motor back to the speed setpoint.

Interruption of the active SS2E function by functions SS1 and SS2

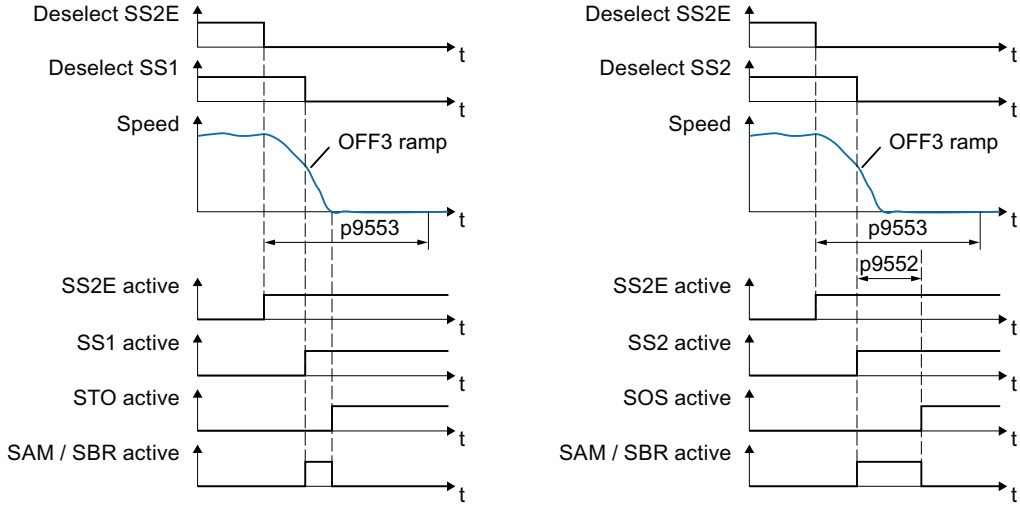


Figure 5-9 Interruption of function SS2E by functions SS1 (shown at the left) and SS2 (shown at the right)

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

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.

When ramping up, for all axes with SIC/SCC connection, the control checks whether the braking time set in p9553 is sufficient for the active acceleration characteristic of the axis. When violated, the suppressible alarm 22001 "Channel %1 Block%2 Axis %3: Braking ramp longer than STOP D time. Reason: %4" 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.

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 ramp longer than STOP D time. Gearbox stage %3. Reason: %4" is output.

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

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.

When Alarm 22001/22002 is output, the following formulas are applied:

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_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	Program command
MAX_AX_ACCEL	MAX_AX_ACCEL	ACC
MAX_AX_JERK	JOG_AND_POS_MAX_JERK	JERKLIM

Comment regarding INCH-METRIC switchover:

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.

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

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

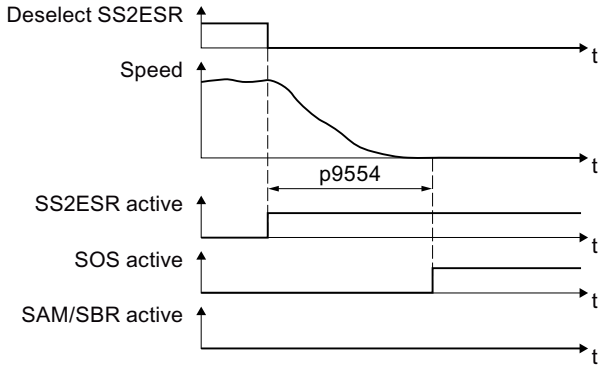


Figure 5-10 Selecting function SS2ESR

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 the 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

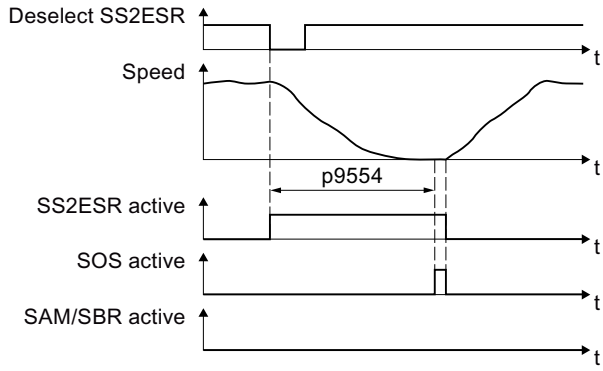


Figure 5-11 Deselecting SS2ESR while SS2ESR is active

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

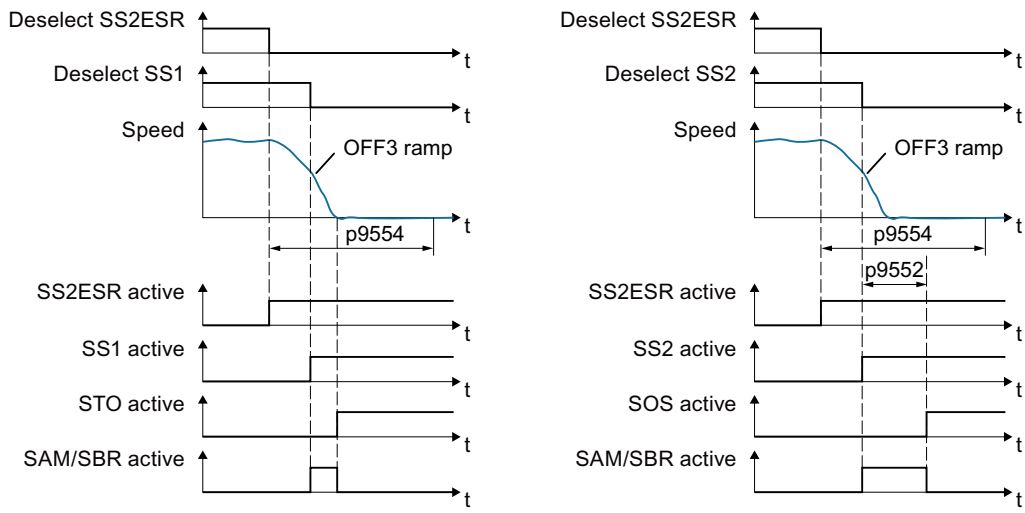


Figure 5-12 Interrupting function SS2ESR by functions SS1 (shown at the left) and SS2 (shown at the right)

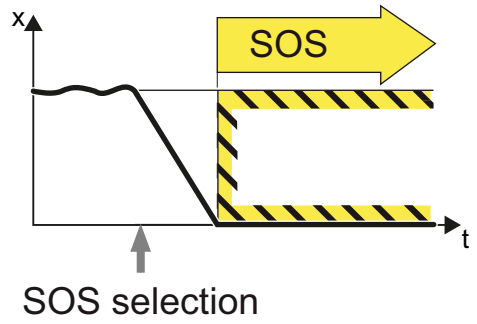
When selecting SS1, the drive brakes the motor along the OFF3 ramp and monitors the speed using function SAM/SBR. Function STO becomes active when the motor is at a standstill.

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.

5.6 SOS

Definition according to EN 61800-5-2:

"This SOS function is used for safe monitoring of 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.

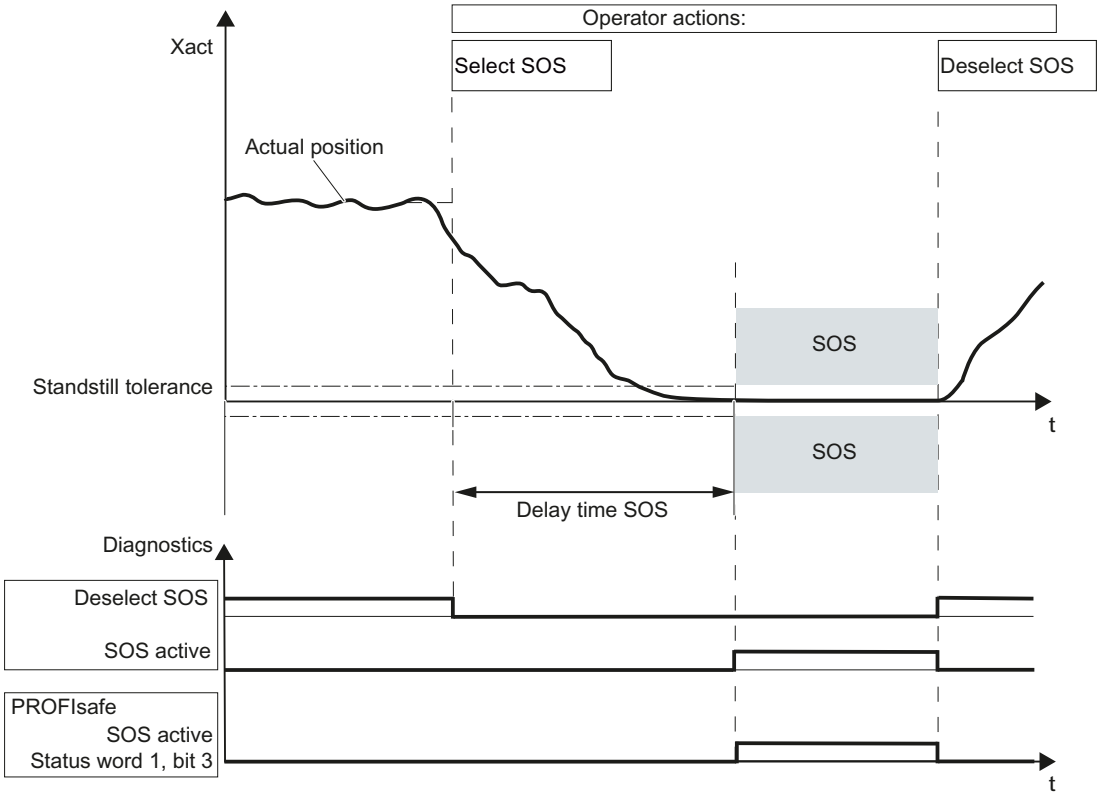


Figure 5-13 Standstill tolerance

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 93)).

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 comes into effect 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
- 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

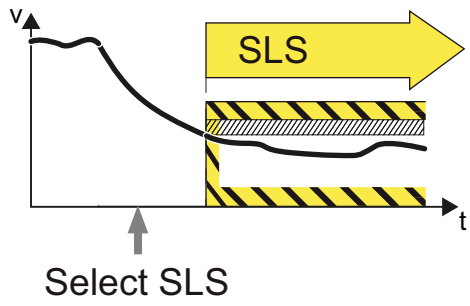
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9501 SI Motion enable safety functions (Control Unit)
- p9530 SI Motion standstill tolerance (Control Unit)
- p9551 SI Motion SLS(SG) switchover/SOS(SBH) delay time (CU)
- 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 specified speed limit."



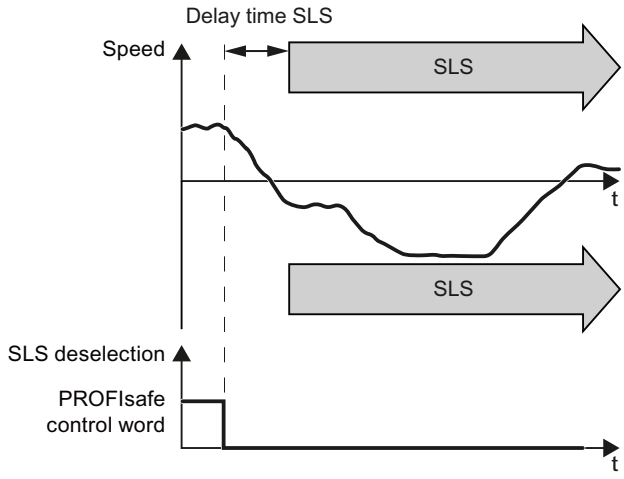
Examples of how the function can be used

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 via a fail-safe 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

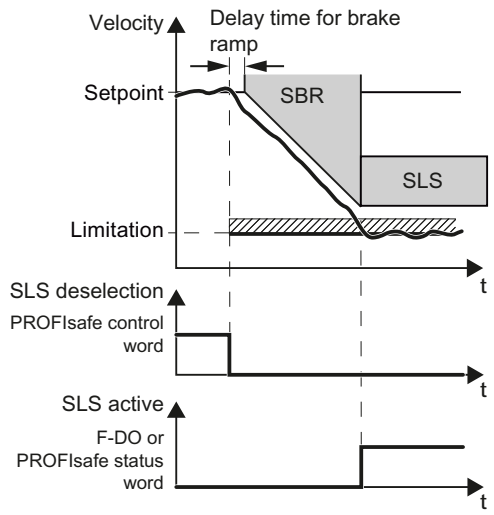
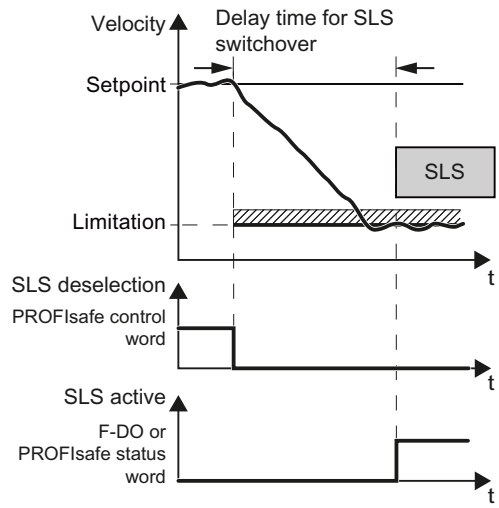
SLS without selection

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 124)".

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 the converter monitors motor braking using the function SBR (Safe Brake Ramp) or SAM (Safe Acceleration Monitor) – or not. For SLS with encoder, the SBR function cannot be selected.

With braking ramp monitoring[1] (only without encoder)	Without braking ramp monitoring (with or without encoder)
	
• 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.	• The converter monitors the load velocity after the "delay time for SLS switchover" has expired.
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.	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.

[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:

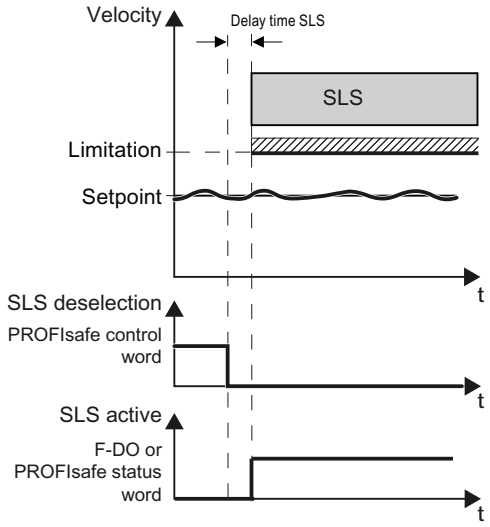


Figure 5-14 Selecting SLS at low velocities

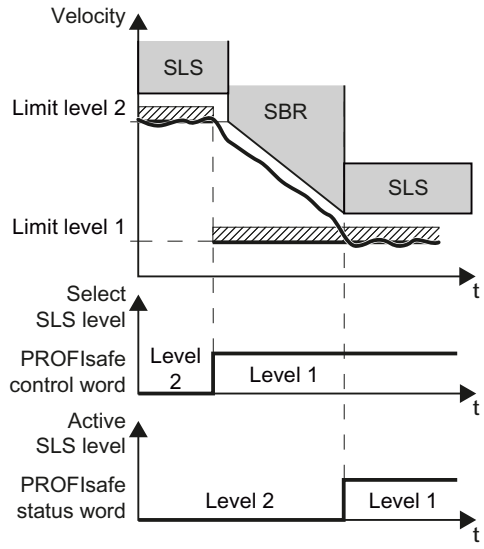
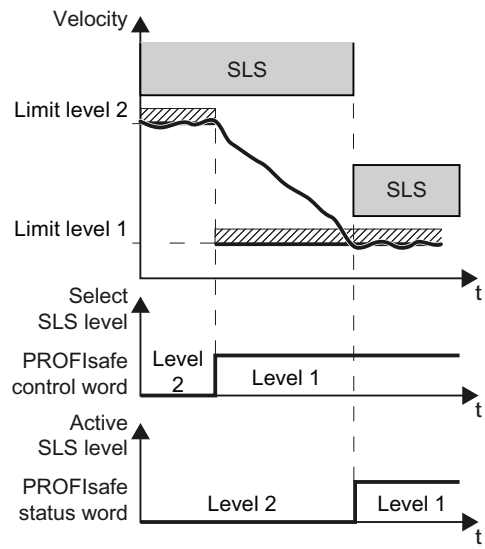
Deselecting SLS

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

With braking ramp monitoring[1] (only without encoder)	Without braking ramp monitoring (with or without encoder)
	
• 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.	• 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).

[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.

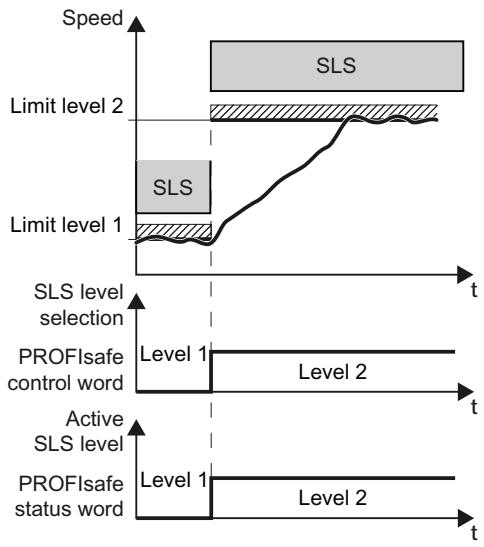


Figure 5-15 Switching to a higher speed level

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 information 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 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 361)
  - 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 361)

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, SV_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.
- If the actual speed of the drive is higher than the new Safely-Limited Speed limit after the delay time has elapsed, 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 the PROFIsafe telegrams 901 and 902 (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 unacknowledged discrepancy errors. 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 messages C01711

Transferring the first limit value using SIEMENS telegram 902

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 135)".

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 triggered 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:

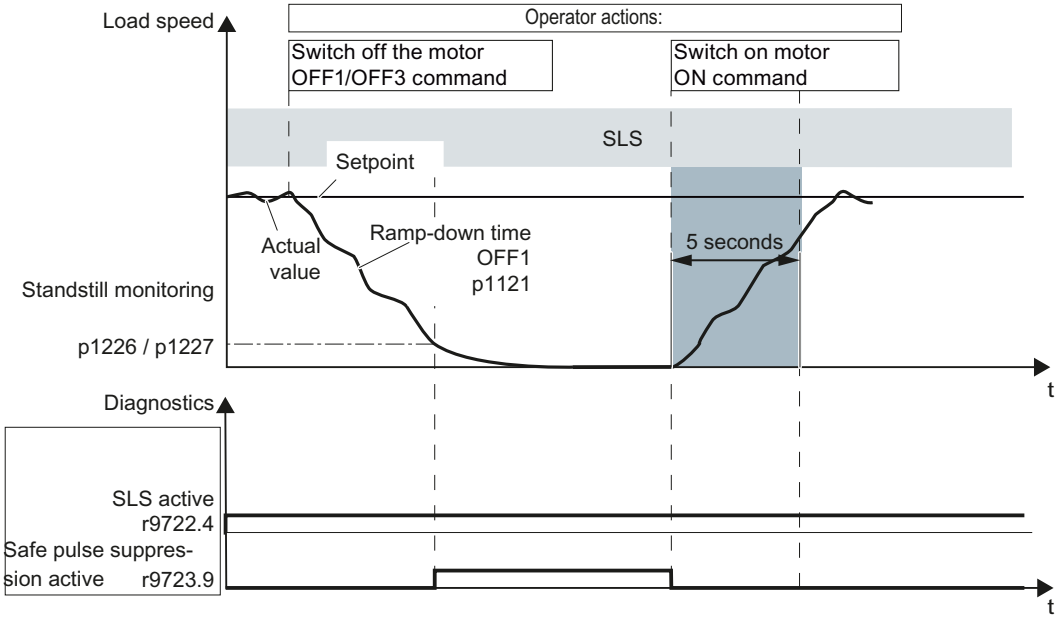


Figure 5-16 Time response of SLS without selection (example: Switching the motor on and off (without encoder))

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

- After switch-off, the motor behaves in accordance with the removed 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)

5.7.1.6 EPOS and safety-relevant setpoint velocity limiting

If safe speed monitoring (SLS) or the safe direction motion monitoring (SDI) is also to be used at the same time as the EPOS positioning function, EPOS must be informed about the activated monitoring limits. Otherwise these speed monitoring limits can be violated by the EPOS setpoint input. By monitoring the limit value, if violated, the drive is stopped therefore exiting the intended motion sequence. In this case, the relevant safety faults are output first, and then the sequential faults created by EPOS.

Using parameter r9733, the safety functions offer EPOS setpoint limiting values, which when taken into account, prevent the safety limit value being violated.

In order to prevent a safety limit violation by the EPOS setpoint specification, you must transfer the setpoint limit value (r9733) as follows to the maximum speed setpoint of EPOS (p2594):

- r9733[0] = p2594[1]
- r9733[1] = p2594[2]

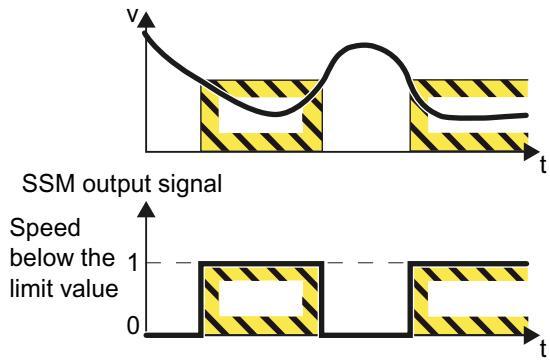
In this regard you must set the delay time for SLS/SOS (p9551), so that the relevant safety monitoring function only becomes active after the maximum required time for the speed to be reduced below the limit. This required braking time is determined by the current speed, the jerk limit in p2574 and the maximum delay in p2573.

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

- p2573 EPOS maximum delay
- p2574 EPOS jerk limitation
- p2593 CI: EPOS LU/revolution LU/mm
- p2594[0...2] CI: EPOS maximum speed, externally limited
- p9551 SI Motion SLS(SG) switchover/SOS(SBH) delay time (CU)
- r9733[0...2] CO: SI Motion speed setpoint limit active

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

- Safety-relevant 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 201711. 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.

- SSM is only considered to be an active monitoring function if "SSM with hysteresis" has been activated.

How does SSMfunction 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.

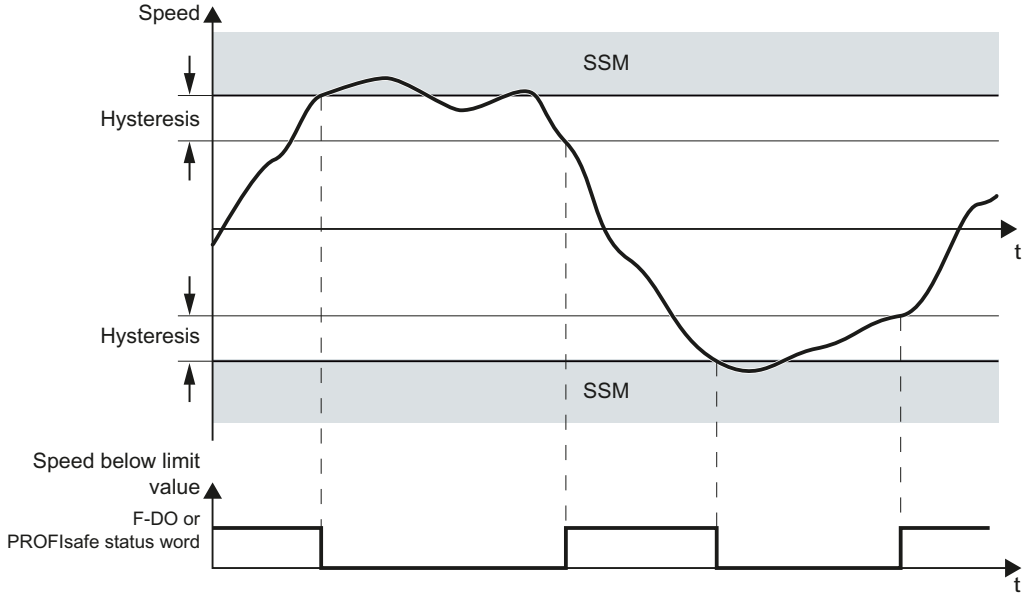


Figure 5-17 Time response of the safety function SSM (Safe Speed Monitor)

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:

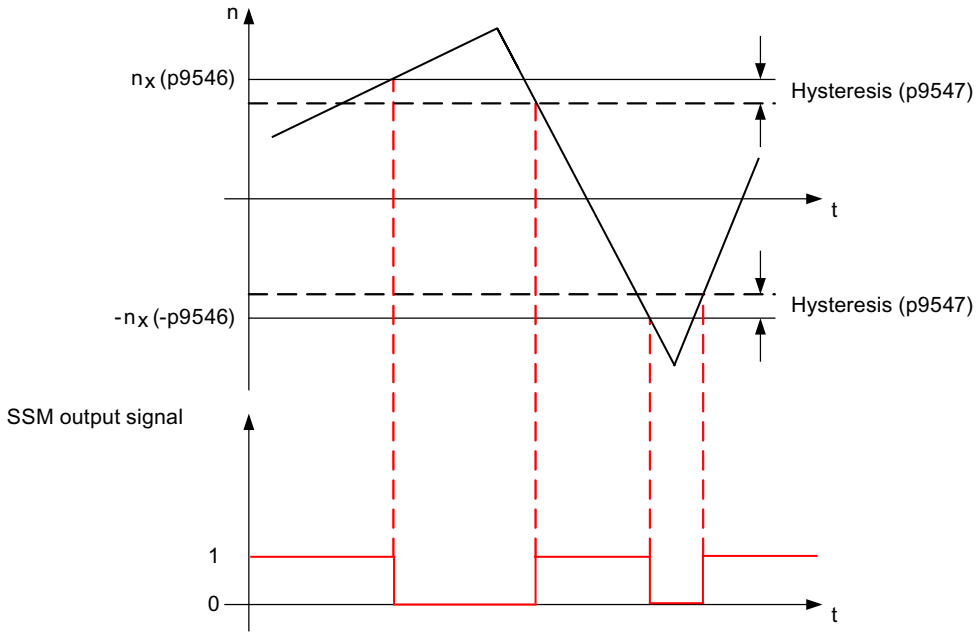


Figure 5-18 Safe output signal for SSM with hysteresis

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 the property "Feedback signal SSM for pulse inhibit"is activated. (p9509.0 = 0)

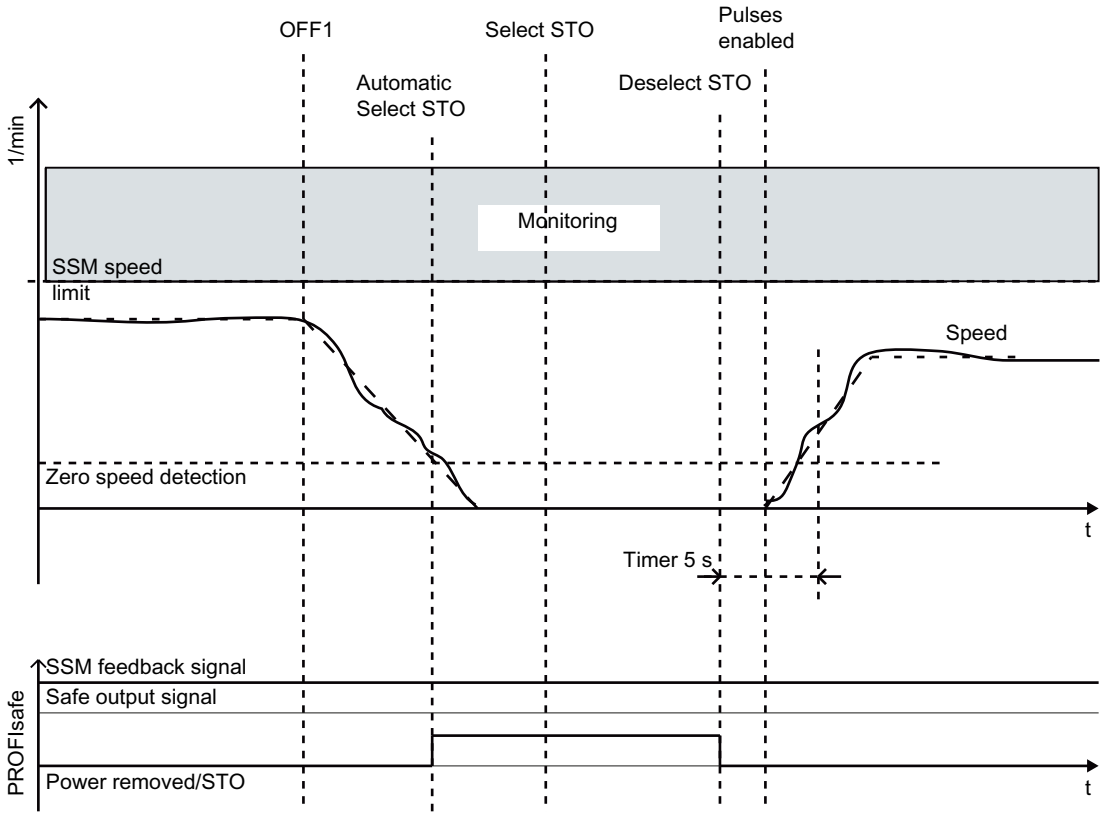


Figure 5-19 Flow chart: SSM without encoder with feedback signal SSM for pulse inhibit (p9509.0 = 0)

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

When the property "Feedback signal SSM for pulse inhibit" is de-activated (p9509.0 = 1), then SSM the monitoring is exited after the pulses have been canceled. 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

The following parameters are relevant for the SSM safety function:

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

You can parameterize parameters that are marked in column "Designation in function-specific screen form" using these.

Parameters not designated there are either part of the general NC and drive-specific settings (Page 235) - or can only be configured using the expert list. The expert list can be reached 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 safe method for monitoring the brake ramp. The Safe Brake Ramp function is used to monitor braking for functions "SS1 with/without encoder," "SLS without encoder" - as well as for STOP B / STOP C (for Safety 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.

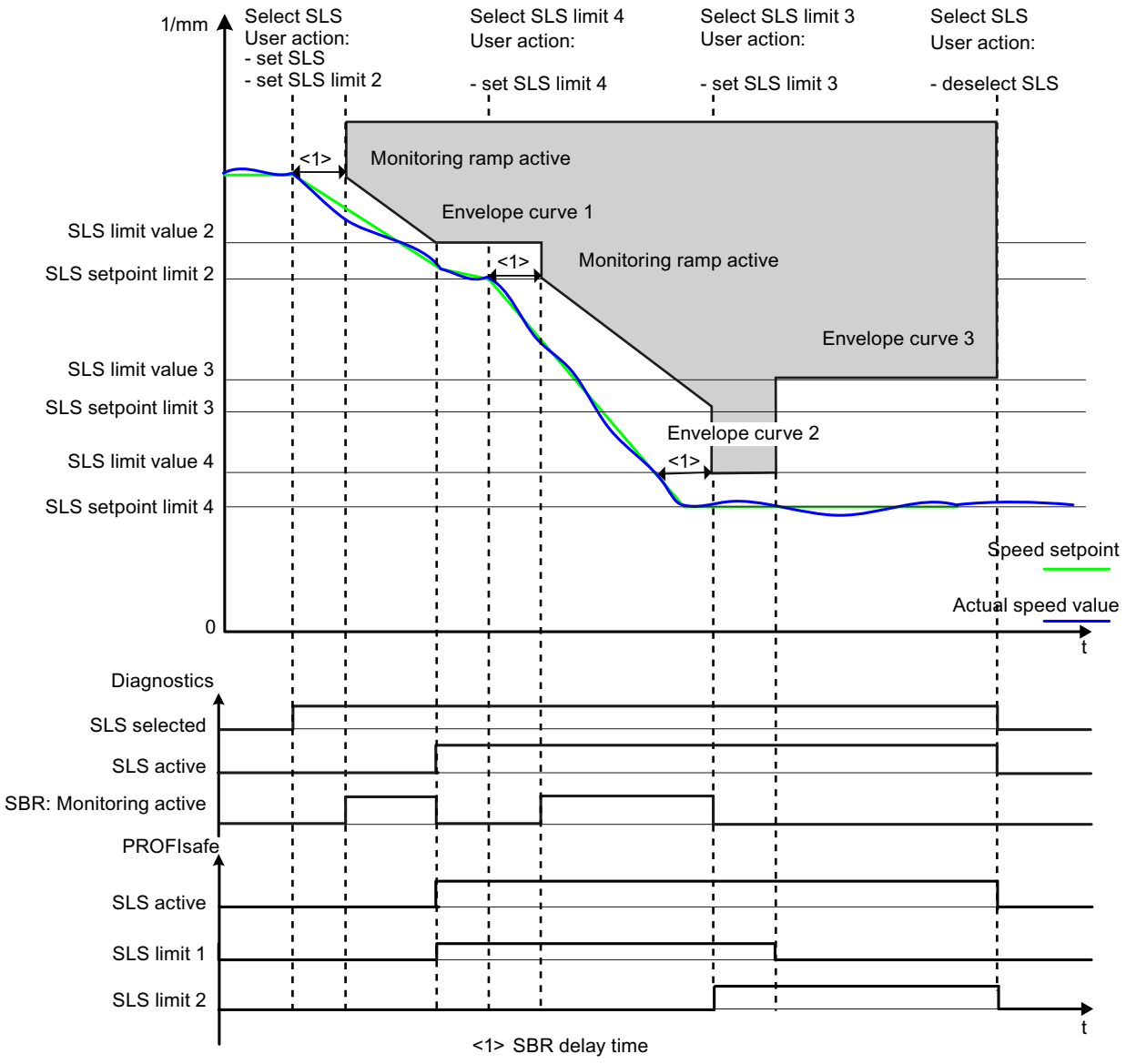


Figure 5-20 Safe Brake Ramp without encoder (for SLS)

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 stop response, Category 0 or 1 (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

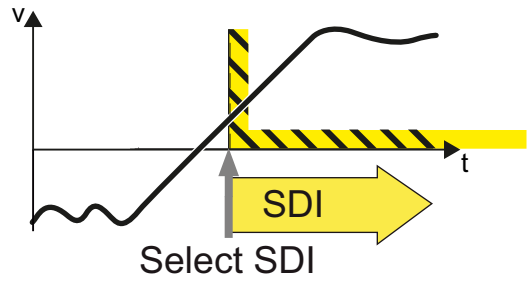
5.10.1 Overview of important parameters

- 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 the motor shaft moving in the wrong direction."



Examples of how the function can be used

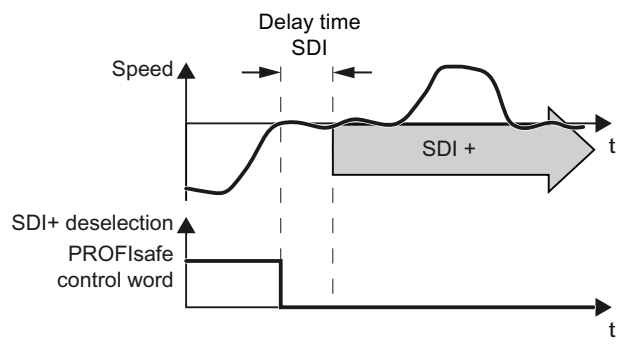
Example	Possible solution
A protective door must only be opened if a drive moves in the safe direction (away from the operator).	• Select SDI in the converter using a fail-safe input or PROFIsafe . • Enable the locking mechanism of the protective doors via the PROFIsafe status bit of the converter.
When 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 fail-safe 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.

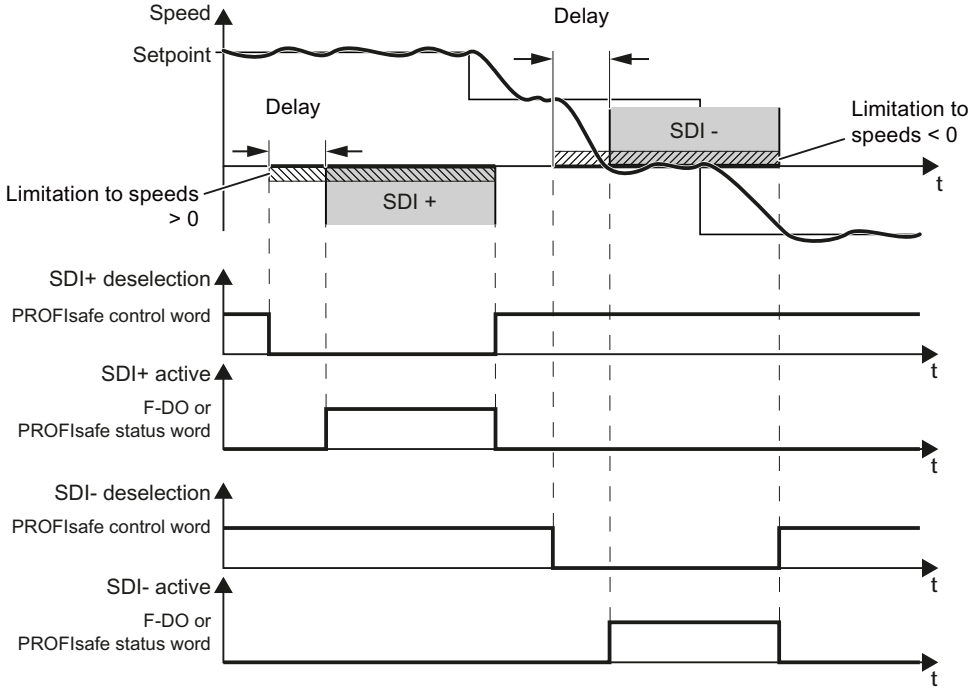


Figure 5-21 Time response of the safety function SDI (Safe Direction)

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 143)".

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 function (SDI) allows reliable monitoring of the direction of motion 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 function is active and the direction of motion is monitored.

If the drive now moves more than the configured tolerance (p9564) in the blocked 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 324) 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 the Safe Direction function

The "Safe Direction" function is enabled with p9501.17 = 1.

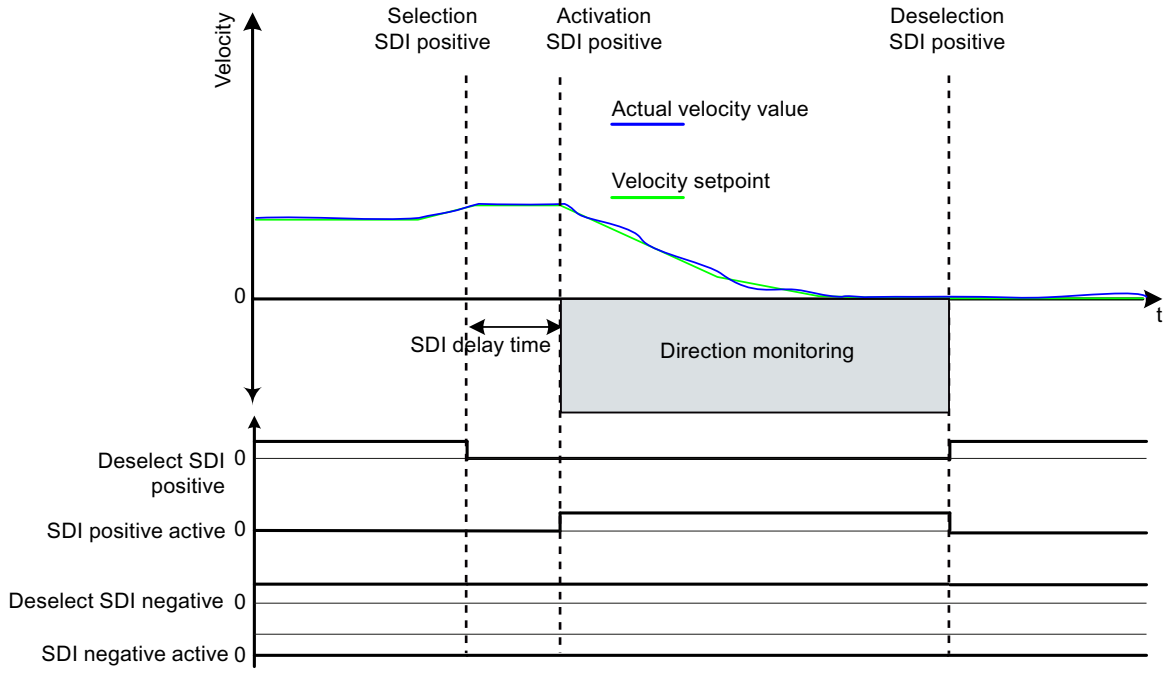


Figure 5-22 Functional principle SDI with encoder

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 238).

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:

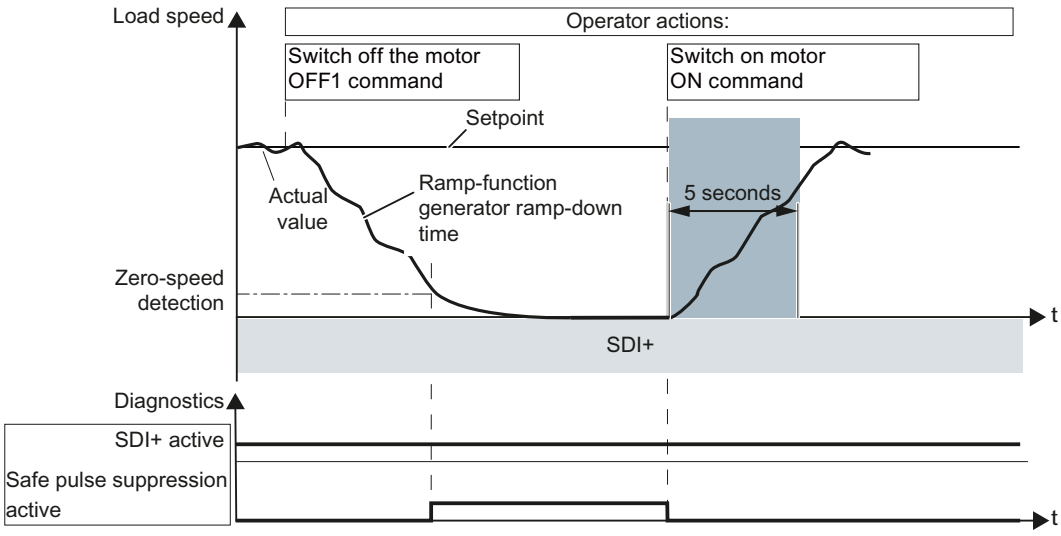


Figure 5-23 Time response of SDI without selection (example: Switching the motor on and off (without encoder))

"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

The following parameters are relevant for the SSM safety function:

- p1820[0...n] Reverse the output phase sequence
- p1821[0...n] Direction of rotation

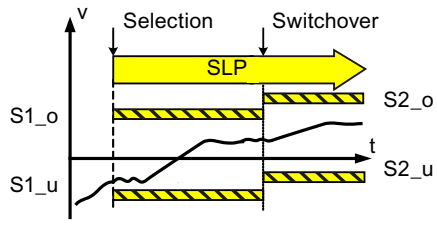
- p9501.17 SI Motion enable safety functions (Control Unit): Enable SDI
- p9506 SI Motion function specification (Control Unit)
- p9509 SI Motion behavior during pulse suppression (Control Unit)
- p9564 SI Motion SDI tolerance (Control Unit)
- p9565 SI Motion SDI delay time (Control Unit)
- p9566 SI 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

5.12.1 Safely-Limited Position (SLP)

Definition according to EN 61800-5-2:

"The SLP function 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.

The Safely-Limited Position function (SLP) is used to safely monitor the limits of two traversing and/or positioning ranges, which are toggled between using a safe 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 149)").

5.12.2 Details and parameterization

The Safely-Limited Position function (SLP) is used to safely monitor the limits of two traversing or positioning ranges which can be switched over by a safe signal.

Requirements

For the Safely-Limited Position function, the following requirements must be met:

- The use of one or two suitable encoders for the extended safety functions with encoder (see also Section "Safe actual value acquisition (Page 179)").

- 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 Section "AUTOHOTSPOT".

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 initiated and the messages C01715 are 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-relevant fashion using the "Retract" function (see Chapter "Retraction (Page 149)").

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 the Safely-Limited Position function

- The "Safety-Limited Position" function 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 the SLP function 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 the Safely-Limited Position function 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 the 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).

5.12.2.1 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

You will find a description of how retraction can be implemented via a failsafe control and PROFIsafe communication in the Internet at:
http://support.automation.siemens.com/WW/view/de/65128501

5.12.2.2 Function diagrams and parameters

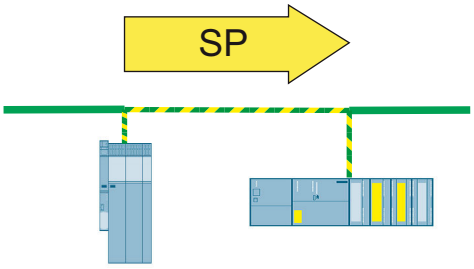
Function diagrams (see SINAMICS S120/S150 List Manual)

- 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



The "Safe Position (SP)" function enables you to transfer safe position values to the F-CPU 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 195)

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

The function "Transfer safe position values (SP)" enables you to transfer a safe position (i.e. absolute or relative position) to the F-PLC via PROFIsafe. Transfer of the safe relative position (Safe Position SP) can be used to calculate the safe speed 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 the "Transfer safe position values" function:

- 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 for an overflow of the range that can be represented. As a consequence, p9505 may only be parameterizing 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 the "Transfer safe position values" function, but the function that was implemented with the aid of SP must be accepted in the higher-level controller.

5.13.1.1 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2840 Extended Functions, control word and status word

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

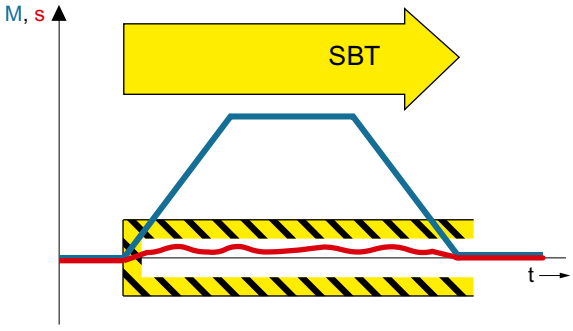
- p9501 SI Motion enable safety functions (Control Unit)
- p9505 SI Motion SP modulo value (Control Unit)
- p9542 SI Motion actual value comparison tolerance (crosswise) (Control Unit)
- p9601 SI enable functions integrated in the drive (Control Unit)

- 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)

The diagnostic function "Safe Brake Test" function (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.



The "Safe Brake Test" function allows a safe test of up to two brakes:

- 1 motor holding brake and 1 external brake
- 2 external brakes
- 1 motor holding brake
- 1 external brake

The Safe Brake Test (SBT) diagnostic function is suitable for safety functions up to Category 2 according to ISO 13849-1.

5.14.1 Features

The Safe Brake Test function has the following properties:

- The parameters of the SBT function 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
- The Safe Brake Test (SBT) diagnostic function is suitable for safety functions up to Category 2 according to ISO 13849-1.

See also

Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 201)

5.14.2 Connection to NC and PLC programs

The SBT function integrated in the drive does not require a setpoint from the PLC or NC - but only an enable signal from the NC, and control via PLC user program. The relevant signals when executing the brake test (SBT) are communicated between the PLC and drive via the Safety Info Channel and the Safety Control Channel (SIC/SCC).

- SIC/SCC communication is realized using telegram 701 (Page 201). Telegram 701 is automatically inserted in the TIA Portal configuration if you activate the Safety Integrated plus mode (F-PLC).
- 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 365).

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. The SI_BrakeTest [FB11] block - known from the Safety Integrated mode (SPL) - is no longer used in the Safety Integrated plus (F-PLC) mode.

See also

PLC user interface (DB3x) (Page 202)

5.14.3 Details and parameterization

5.14.3.1 Requirements

NC

The following conditions must be met 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 requirements must be satisfied when using the "Safe Brake Test" function with DRV:

- 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 179)".

Note

SBT only with encoder

The "Safe Brake Test" (SBT) safety 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

The "Safe Brake Test" (SBT) function is not available for SINAMICS HLA.

5.14.3.2 Handling overview

Selecting SBT

1. In the associated axis DB, set bit "Start brake test" DBX11.0 = 1.
   The NC checks that the appropriate conditions exist for the test to be performed:
   – 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.
2. 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 157) are satisfied, and start again with step 1.
3. Select SBT via SCC by setting bit 0 "SELECTION_SBT" to 1 in STW3 (signal edge 0 => 1).
   See also: Selection (Page 162)
   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 163)

Deselecting SBT

1. Select SBT via SCC by setting bit 0 "SELECTION_SBT" to 0 in STW3 (signal edge 1 => 0).
   See also: Selection (Page 162)
   DRV initiates the de-selection process, and then in ZSW3 bit 1 "SETPOINT_SETTING_DRIVE" is set to 0. The setpoint chain 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 again.
   See also: Sequence (Page 163)
2. In the associated axis DB, set bit "Start brake test" DBX11.0 = 0.
   The "Brake test active" bit is set by the NC to 0 (DBX71.0 = 0).

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 164)

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.

See also

Enabling the function (Page 159)

5.14.3.3 Enabling the function

To enable the Safe Brake Test function, proceed as follows:

- Enable the Safe Brake Control (SBC) function when using an internal motor holding brake (MHB): p9602 = 1.
- Select the SBT selection type:

p10203	**Selects SBT**
= 0	Via SCC
= 1	Via BICO
= 2	For test stop / forced checking procedure

- 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 201)".
- 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 EPOS

If EPOS is activated, you must activate "follow-up mode" (r2683.0) before you perform the brake test so that the position monitoring does not react during the brake test.

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 201), SBT: Communication via SIC/SCC (Page 165)
- **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 Safety 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:

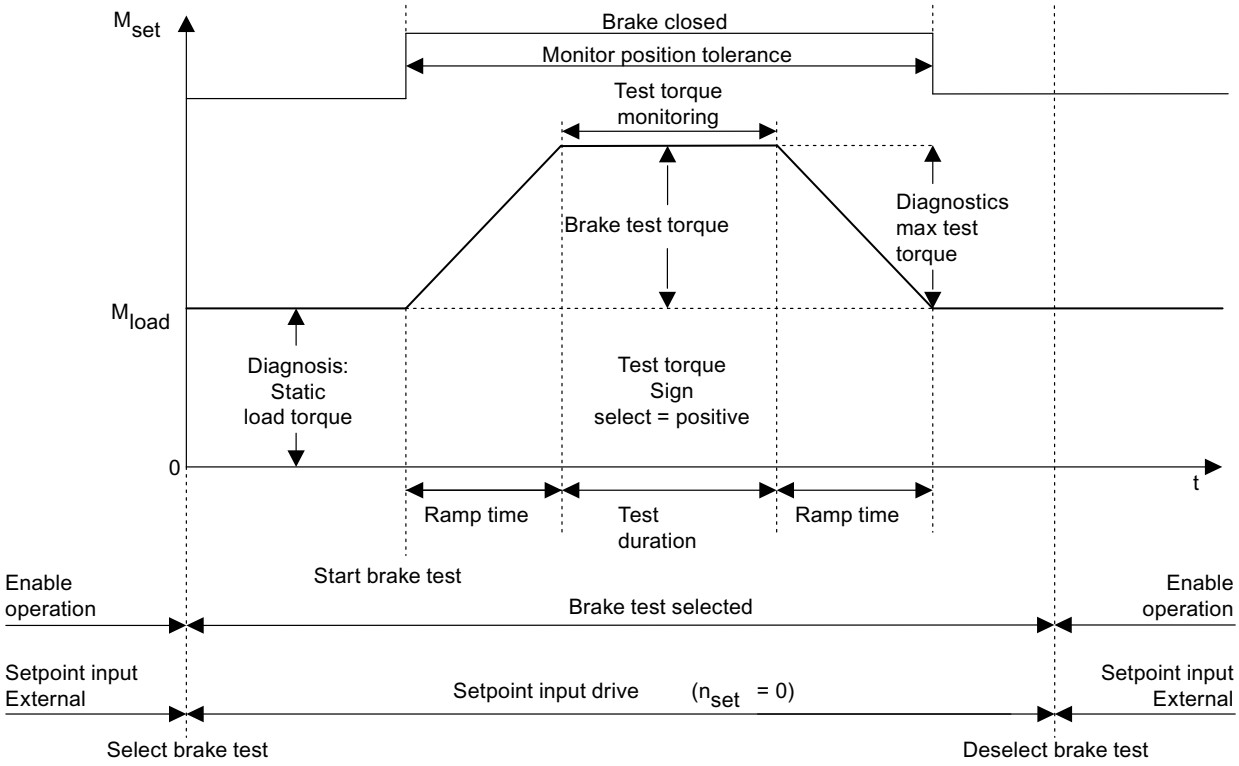


Figure 5-24 SBT: Time sequence

- 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

Testing a motor holding brake

The following figure shows the communication via SIC and SCC during the test of a motor holding brake:

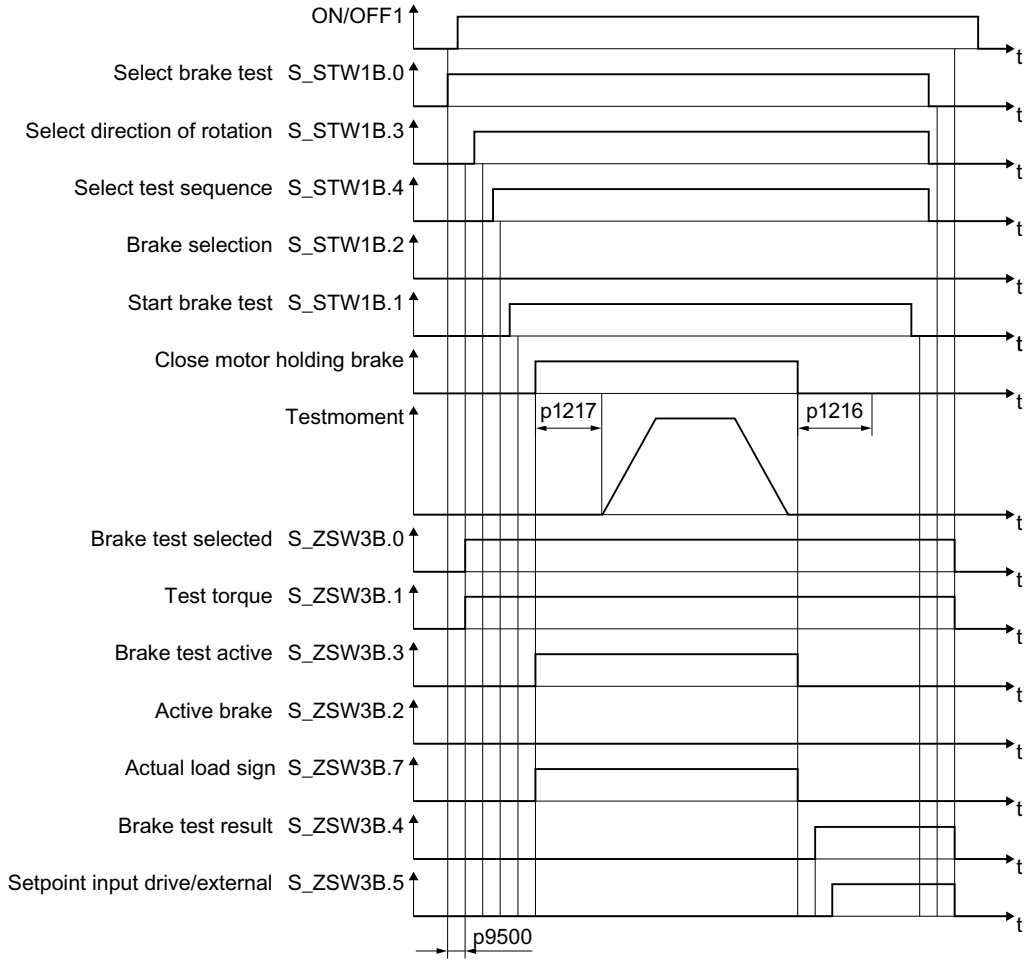


Figure 5-25 Testing a motor holding brake

Test of an external brake

The following figure shows the communication via SIC and SCC during the test of an external brake:

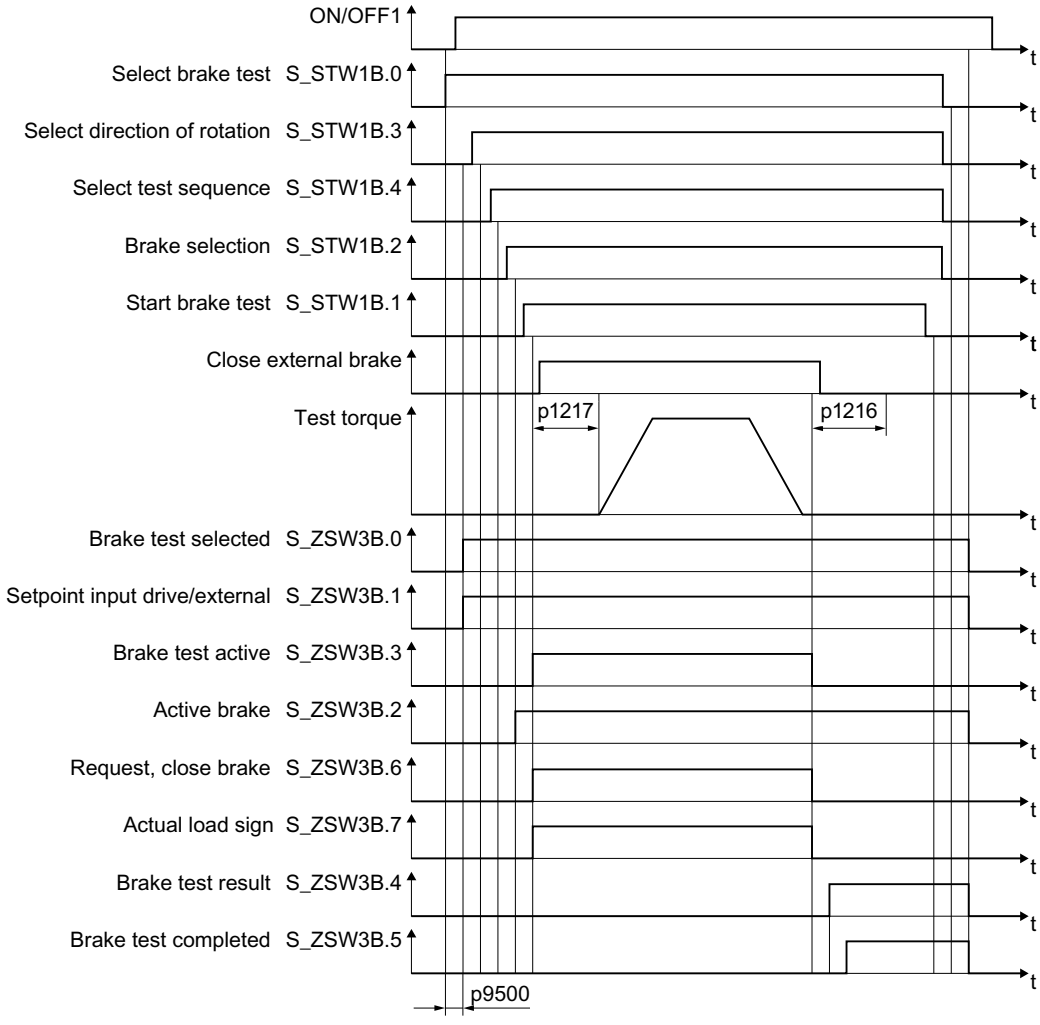


Figure 5-26 Testing an external brake

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

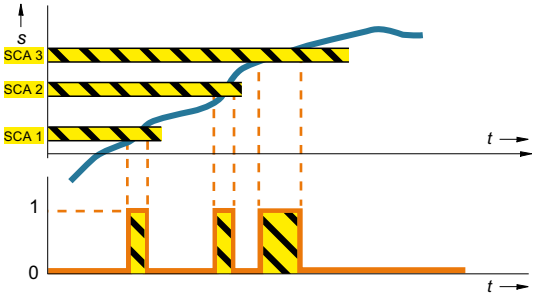
Overview of important parameters (see SINAMICS S120/S150 List Manual)

- 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:

The function "Safe Cam" (SCA) safe supplies a safety-related output signal to indicate whether the motor shaft position is within a defined range.



The "Safe Cam" function outputs a safe 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

With the "Safe Cam" function (SCA), you implement safe electronic cams, safe zone sensing, or a working area limitation/protection zone delimitation for a specific axis, to replace a hardware-based solution. You parameterize up to 30 output cams for each axis. You enable each output cam individually.

Note

The "Safe Cam" (SCA) safety function 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:

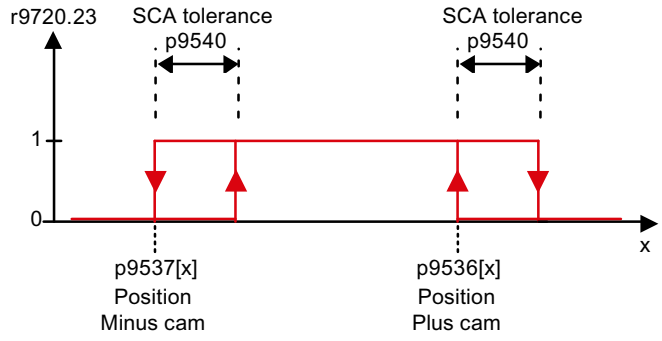


Figure 5-27 Parameterize output cam and tolerance

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 175)" function.

Enable SCA

- You enable the SCA function 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 (homed)

The enabled cam signals are immediately output after POWER ON. However, the output is only safety-related after safety-related referencing (safety-related homing) 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 175)" function.

Select SCA

Select the SCA function using the 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 output cam status word via PROFIsafe to the F host, the output 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 359)").

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:
"The SLA function prevents the motor from exceeding the defined 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.

Function "Safely-Limited Acceleration" (SLA) monitors that the motor does not violate the defined acceleration limit (e.g. in the 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 Operate parameter list

Contrary to other Safety Integrated Functions, there is no Operate configuration screen form for SLA. Therefore, parameterize this function in Operate in the parameter list.

Enabling SLA

- You enable the SLA function with p9501.20 = 1.

Selecting SLA

Select the SLA function using the 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.

5.16.1 Details and parameterization

5.16.1.1 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

Principle of operation

The following diagram shows the principle of operation of SLA:

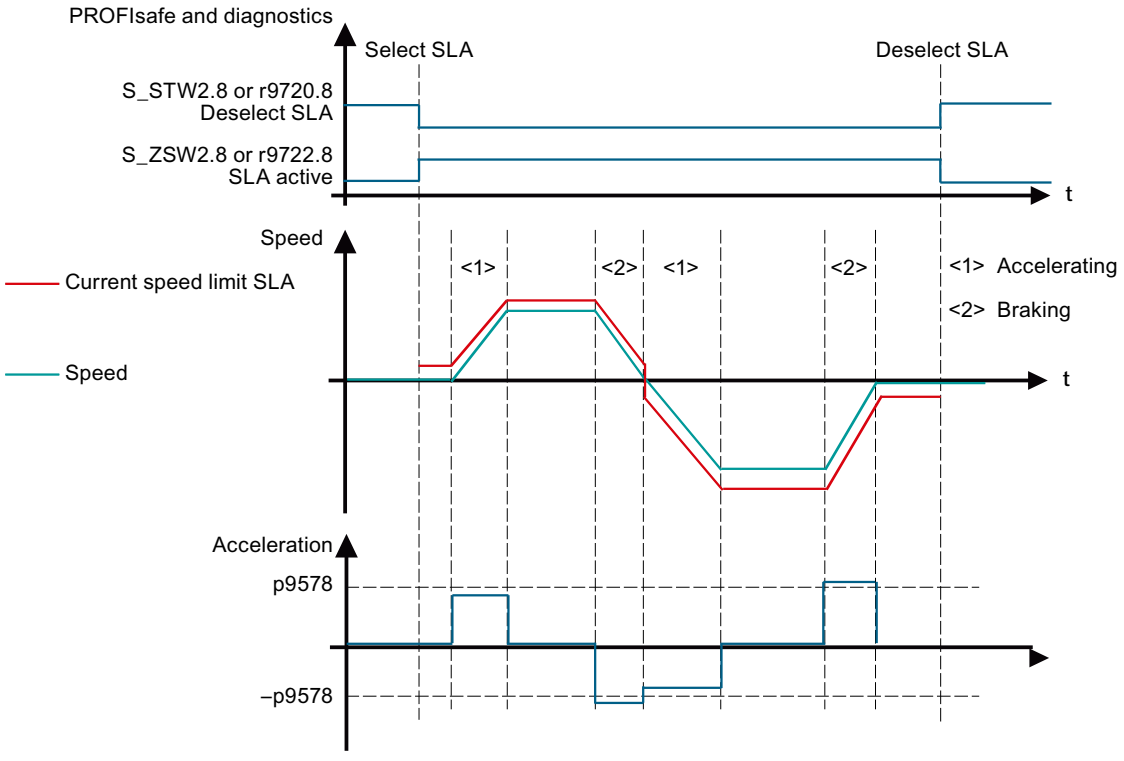


Figure 5-28 Safely-Limited Acceleration (SLA): Principle

5.16.1.2 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.

5.17 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 146)
- SP (Page 151)
- SCA (Page 168)

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, 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.

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2821 SI Extended Functions - Safe referencing

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

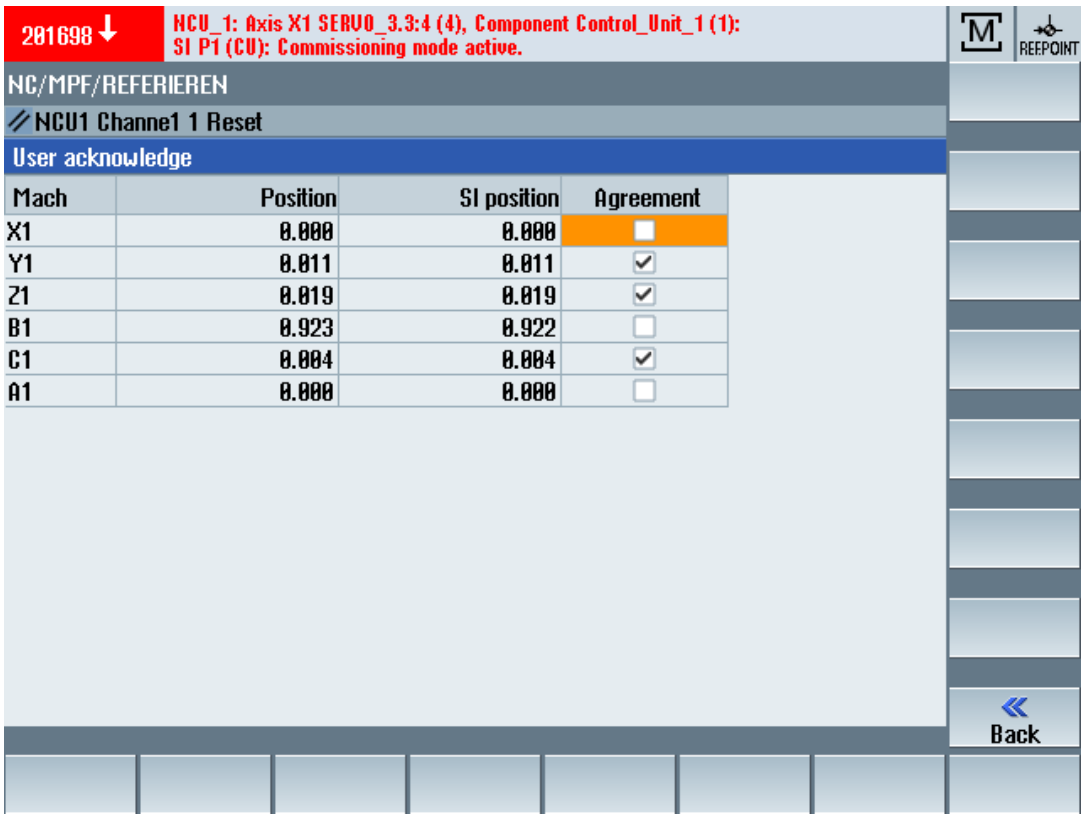


Figure 5-29 User agreement

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.

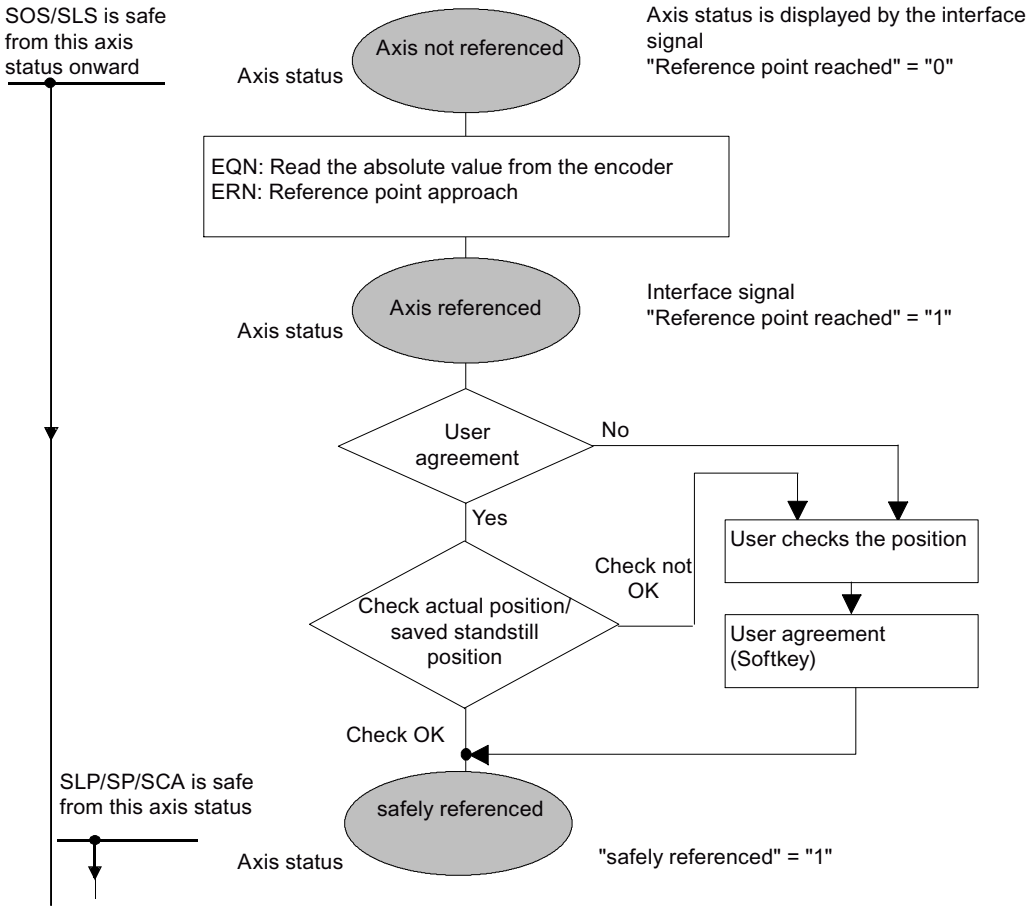


Figure 5-30 Axis states when referencing

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

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-relevant 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-relevant 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.

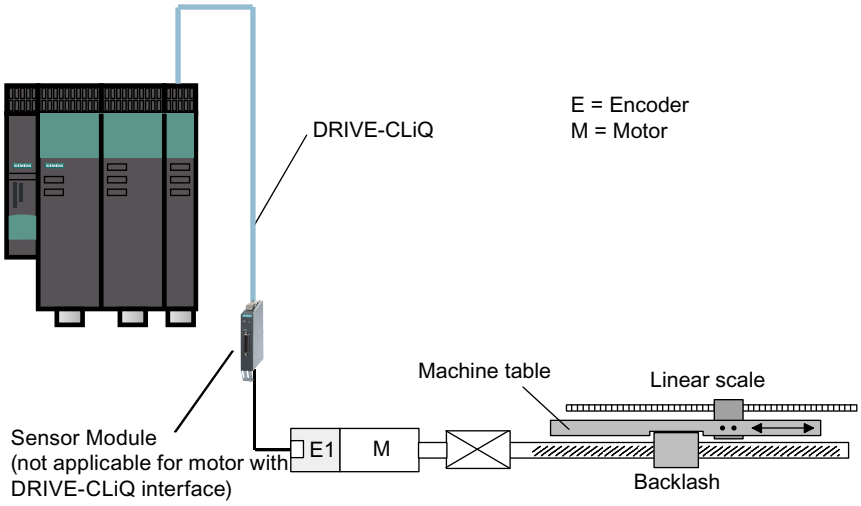


Figure 5-31 Example of a single-encoder system

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).

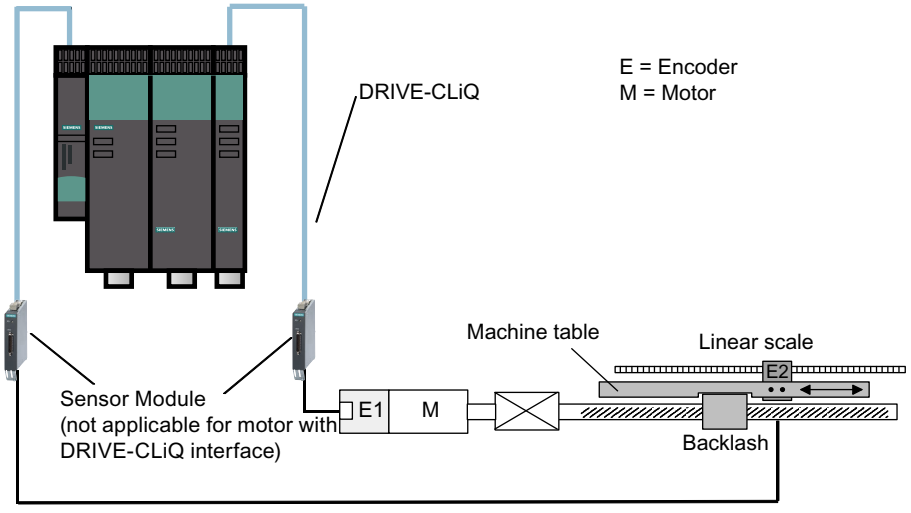


Figure 5-32 Example of a 2-encoder system on a linear axis via a ball screw

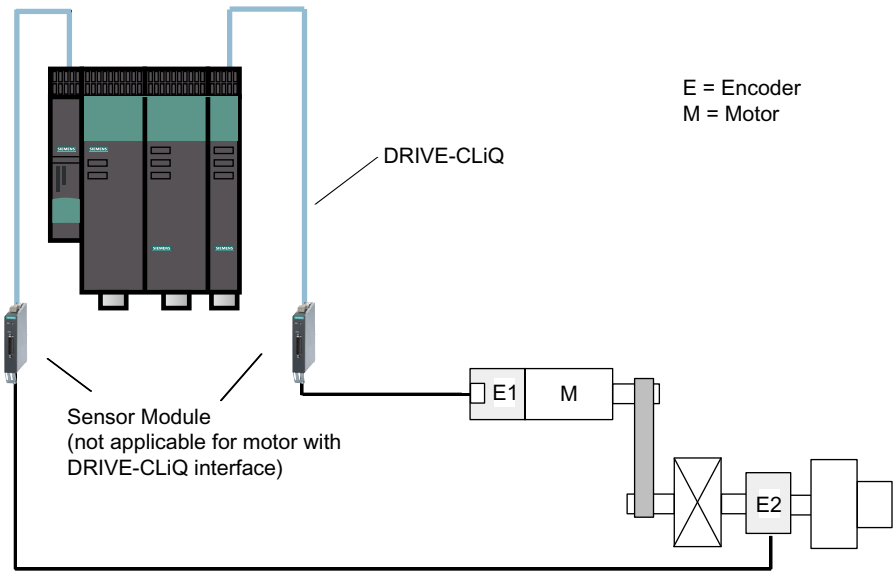


Figure 5-33 Example of a 2-encoder system on a rotary axis

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 5-4 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.

Siemens motors with and without DRIVE-CLiQ connection, which can be used for Safety Integrated Functions, are listed under:

http://support.automation.siemens.com/WW/view/en/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.

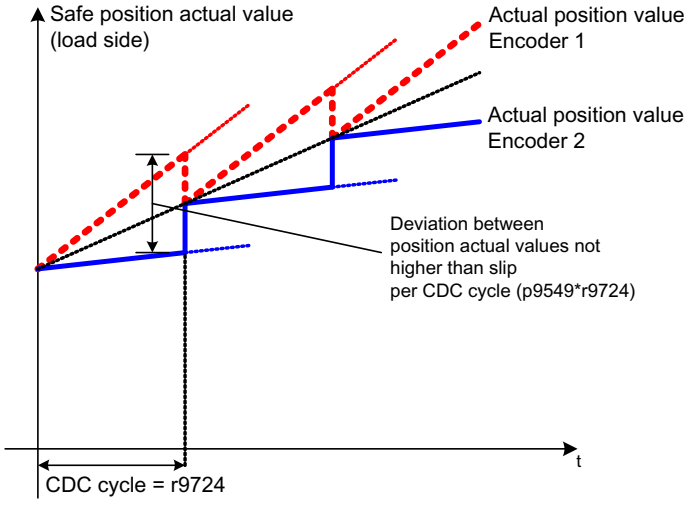
Note

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-relevant 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.
  For SINAMICS S120M, only the values 2 and 0 ms are allowed for the actual value acquisition cycle clock (p9511). In both cases, the frequency converter calculates with an actual value acquisition cycle clock of 2 ms regardless of the PROFIBUS DP/PN clock cycle.
- 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 Overview of 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 PROFIBUS (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:

- 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.

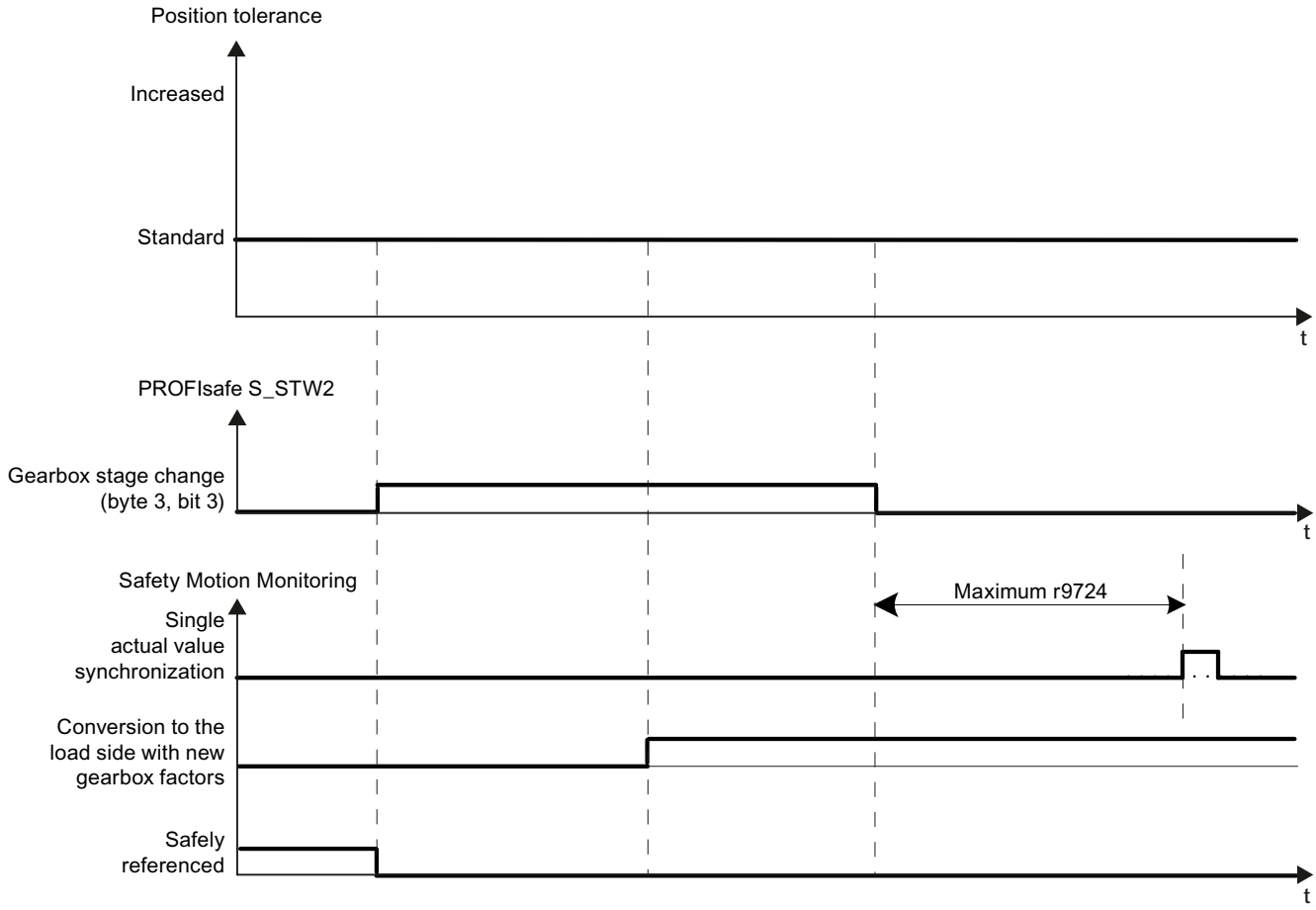


Figure 5-35 Gearbox switchover from stage "0" to "1" without increased position tolerance

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).

- Set the increased position tolerance using bit 3 (= 1) in byte 3 of S_STW2.
- Set the new gearbox stage using bits 0 to 2 in byte 3 of S_STW2.
- 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.

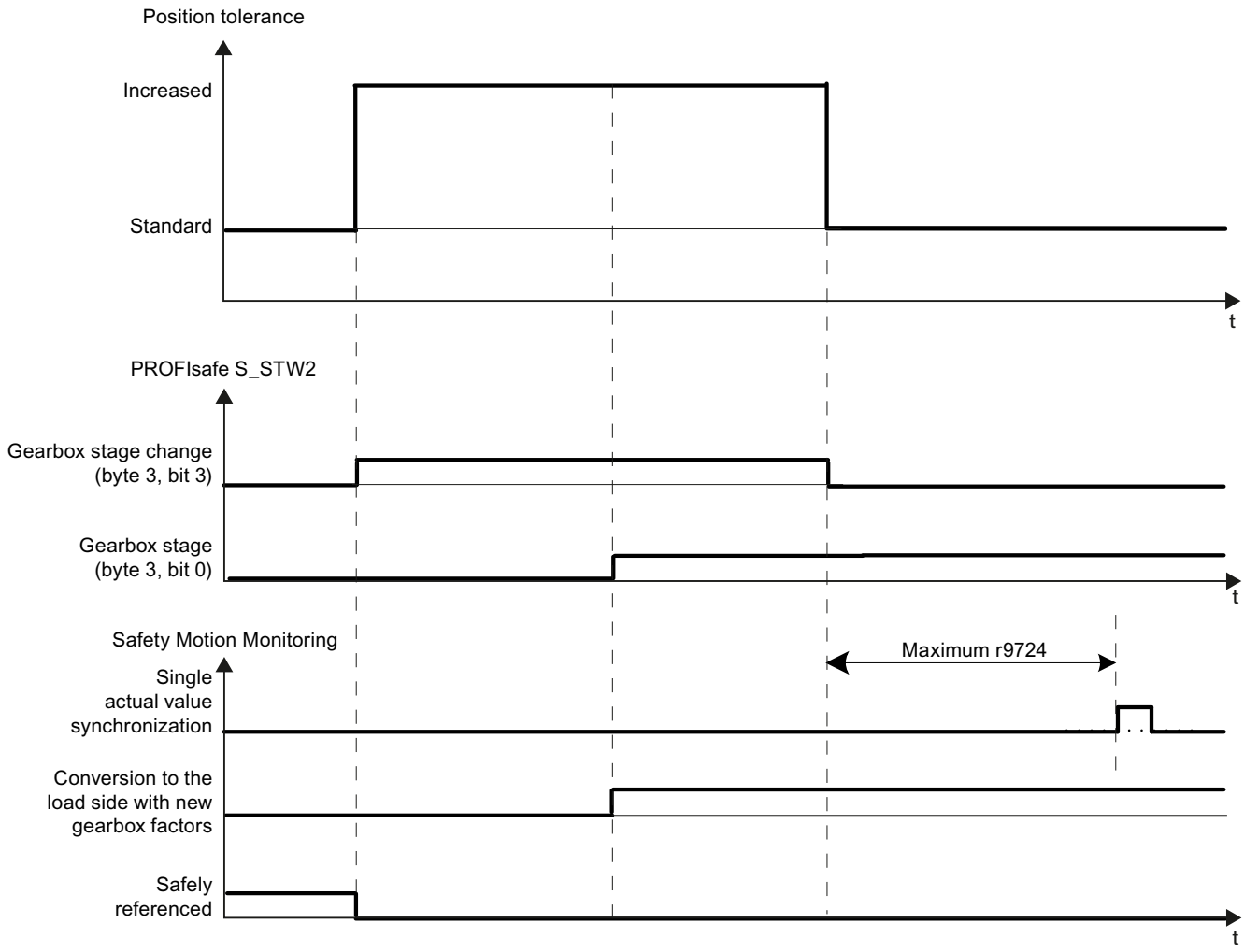


Figure 5-36 Gearbox switchover with increased position tolerance

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 175)).

5.19.1 Overview of important parameters

- 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. On expiration of the parameterized timer (also after POWER ON / warm restart), the 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 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 201)
  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 194) • Controlling via PROFIsafe (Page 197) • SIC/SCC (Page 201)	Yes	Yes
Controlling via terminals (on the Control Unit and on the Motor/Power Module) See: Control signals via terminals on the NCU and motor/power module (Page 203)	Yes	No

Note

Term "Control Unit" in this documentation

In the Safety Integrated plus 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 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.
- SIEMENS telegram 701
  Manufacturer-specific telegram for SIC/SCC communication. With SINUMERIK, SIC/SCC communication only takes place via telegram 701.

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	903	902	901	31	30
Safety control word 1 S_STW1 (Page 348)	–	–	–	–	PZD1
Safety status word 1 S_ZSW1 (Page 350)	–	–	–	–	PZD1
Safety control word 2 S_STW2 (Page 352)	PZD1…2	PZD1…2	PZD1…2	PZD1…2	–
Safety status word 2 S_ZSW2 (Page 354)	PZD1…2	PZD1…2	PZD1…2	PZD1…2	–
SLS limit value input S_SLS_LIMIT_A (Page 357)	PZD3	PZD3	PZD3	–	–
Active SLS limit value S_SLS_LIMIT_A_ACTIVE (Page 357)	PZD5	PZD3	PZD3	–	–
Counter for the safety cycle S_CYCLE_COUNT (Page 358)	–	PZD4	PZD4	–	–
Actual position value (16 bits) S_XIST16 (Page 358)	–	–	PZD5	–	–
Actual position value (32 bits) S_XIST32 (Page 358)	–	PZD5…6	–	–	–
Safe Cam status word S_ZSW_CAM1 (Page 359)	PZD3…4	–	–	–	–

Table 6-3 Process data from SIEMENS telegram 701 (SIC/SCC)

Telegram Process data	701
Safety Control Channel control word 1 S_STW1B (Page 361)	PZD1
SI Motion Safety Info Channel status word S_ZSW1B (Page 361)	PZD1
Safety Info Channel status word 2 S_ZSW2B (Page 362)	PZD2
Safety Control Channel control word 3 S_STW3B (Page 363)	PZD2
SLS setpoint speed limiting (32 bit) S_V_LIMIT_B (Page 364)	PZD3…4
Safety Info Channel status word 3 S_ZSW3B	PZD5

See also

S_ZSW3B: Safety Info Channel status word 3 (Page 363)

6.4 Controlling via PROFIsafe

6.4.1 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 6-4 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

6.4.2 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 6-5 Parameter to select the PROFIsafe telegram

Parameter/name	Setting	Meaning
p60022 PROFIsafe telegram selection / Ps telegr_sel p9611 SI PROFIsafe telegram selection (Control 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 • Structure of telegram 903 (Page 344)
	902	• PROFIsafe SIEMENS telegram 902, PZD-3/6 • Extended PROFIsafe telegram with 32-bit position value • Structure of telegram 902 (Page 345)
	901	• PROFIsafe SIEMENS telegram 901, PZD-3/5 • Extended PROFIsafe telegram with 16-bit position value • Structure of telegram 901 (Page 345)
	31	• PROFIsafe standard telegram 31, PZD-2/2 • Extended standard PROFIsafe telegram • Structure of telegram 31 (Page 346)
	30	• PROFIsafe standard telegram 30, PZD-1/1 • Standard PROFIsafe telegram • Structure of telegram 30 (Page 346)

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.

6.4.3 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 Parameters and function diagrams

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2840 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)

6.5.1 Introduction

In the Safety Integrated plus (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)" diagnostic 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 automatically responds to the drive STOP response 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 (DB3x) (Page 202), Interface signals: Axis/spindle signals (Page 365)

Note

SIC and SCC must always be jointly configured and/or parameterized.

6.5.2 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).

6.5.3 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).

6.5.4 SIC/SCC communication using telegram 701

SIC/SCC communication can always be transferred using the predefined PROFIdrive telegrams 700 or 701. However, for SINUMERIK only telegram 701 (Page 344)is used.

If another telegram is configured for SIC/SCC, then cyclic SIC/SCC communication is inhibited, and Alarm 27811 is output.

6.5.5 PLC user interface (DB3x)

In the Safety Integrated plus (F-PLC) mode, additional axis-specific data from the axis DB (axis 1 [DB31] ... axis 31 [DB61]) are relevant, which are mapped 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 365).
- See also: SBT: Connection to NC and PLC programs (Page 157)

6.5.6 Overview of important parameters

The following parameters are relevant for the SSM safety function:

- r9733[0...2] CO: SI Motion setpoint speed limit effective
- 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 signals via terminals on the NCU and motor/power module

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.

- 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
- 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 206), otherwise a fault is output.

Example: Terminals for STO

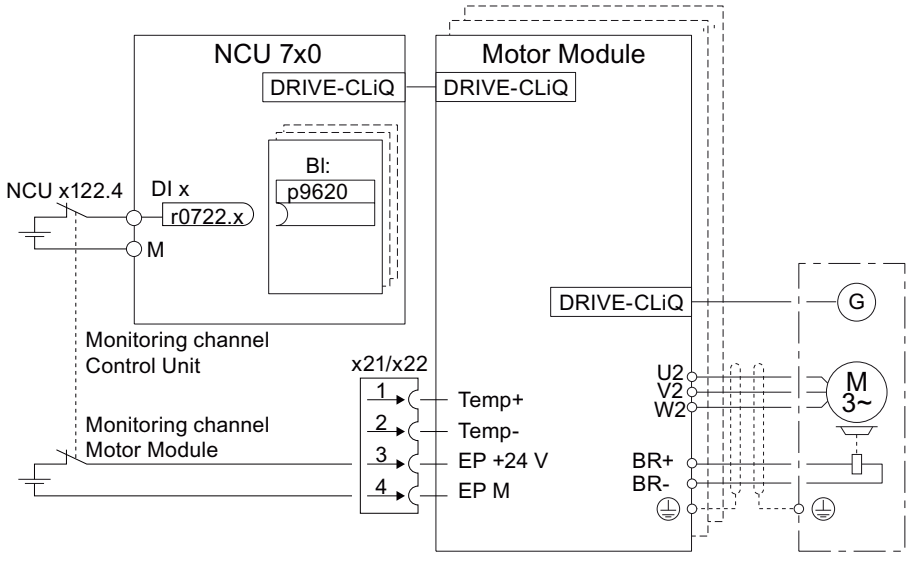


Figure 6-1 Example: Terminals for STO for an NCU7x0 and a Motor Module, booksize format

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.

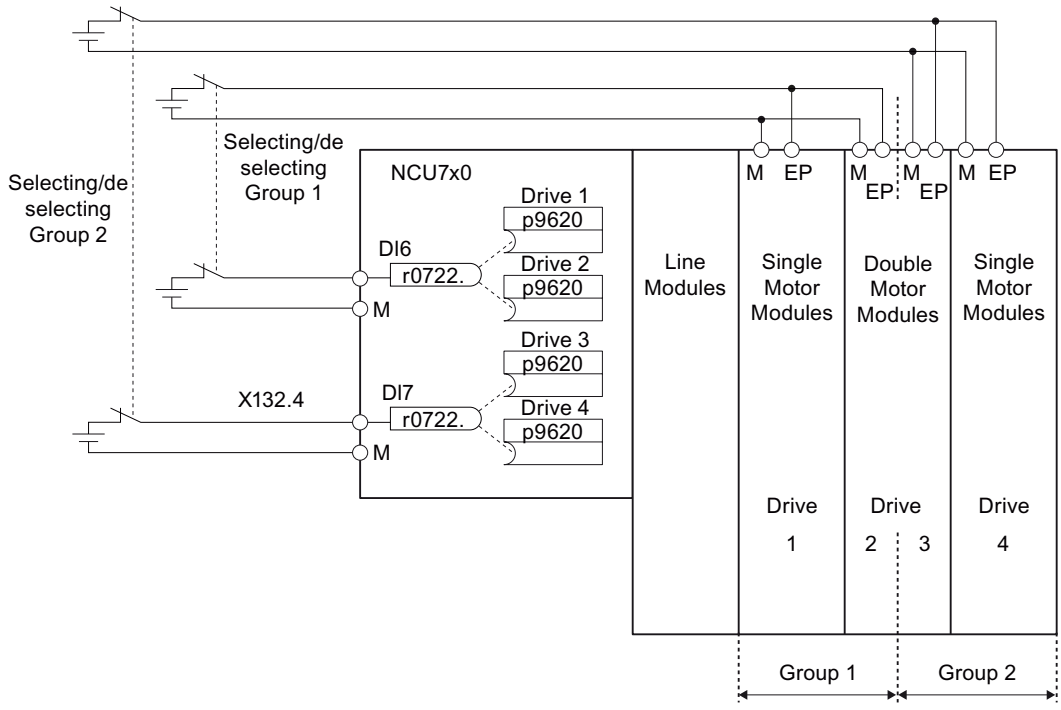


Figure 6-2 Example: Grouping the terminals for Motor Modules, booksize format

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.

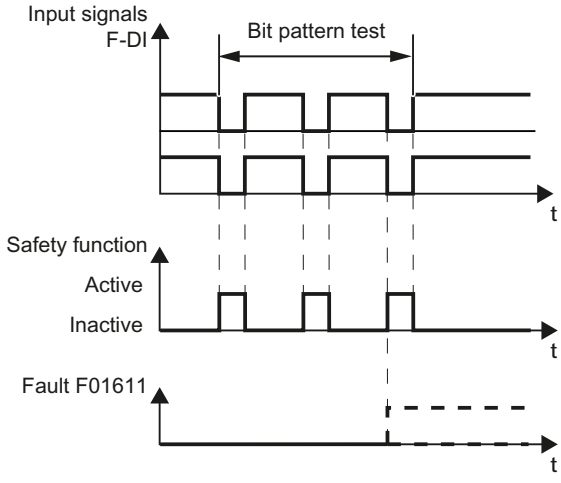


Figure 6-3 Converter response to a bit pattern test

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 (see SINAMICS S120/S150 List Manual)

- p9651 SI STO/SBC/SS1 debounce time (Control Unit)

Commissioning and configuring 7

7.1 Handling overview

Safety Integrated plus is partially commissioned in the TIA Portal - and partially in SINUMERIK Operate. Commissioning can be roughly subdivided into the following steps:

- Configuring safety-relevant components (Page 210)
- Generating a safety program (Page 219)
- Loading the configuration (Page 232)
- Configuring NC and drive-specific safety settings (Page 235)
- Configuring safety functions integrated in the drive (Page 254)
- Finalizing commissioning (Page 287)

Detailed action overviews can found in the linked sections.

7.2 Configuring safety-relevant components

7.2.1 Handling overview for configuring

The following handling overview (as example) and the associated descriptions illustrate the features when configuring Safety Integrated plus (F-PLC) with a SINUMERIK NCU compared to a CPU S7-300. Consequently, the overview serves only as an introduction to the configuring and programming of STEP 7 Safety Advanced with SINUMERIK.

Requirement

- The following TIA Portal software is installed:
  - SIMATIC STEP 7 Professional
  - SINUMERIK STEP 7 Toolbox
  - SIMATIC STEP 7 Safety Advanced
- The non-safety-relevant components have been configured.
- The NCU (firmware version ≥ 4.8) 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 Safety Integrated plus mode (F-PLC).

Example handling overview

Step	Description
1	Activating Safety Integrated plus (Page 210)
2	Configuring additional safety-related components (Page 212)
3	Loading the configuration into the controller (Page 212)
4	Allocating and assigning a PROFINET device name (Page 213)
5	Assigning F-destination addresses, address type 1 (Page 215) or Assigning F-destination addresses, address type 2 (Page 215)
6	Checking the PROFIsafe address (Page 217)

After completing the configuration, generate the safety program of the F-PLC (Page 219).

7.2.2 Activating Safety Integrated plus

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".

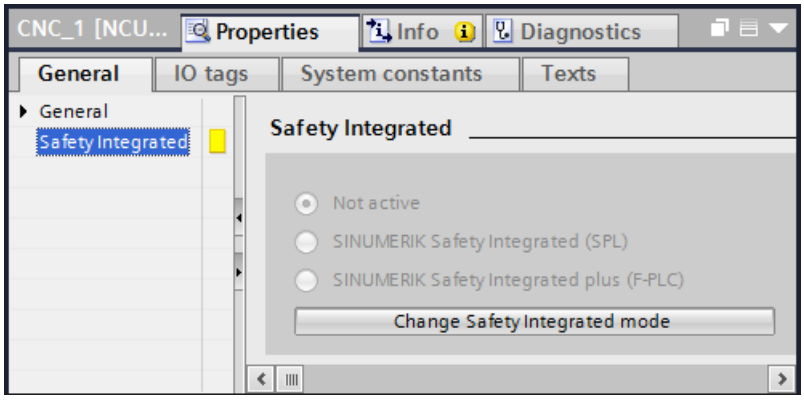


Figure 7-1 Inspection window "Properties" - Safety Integrated

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.

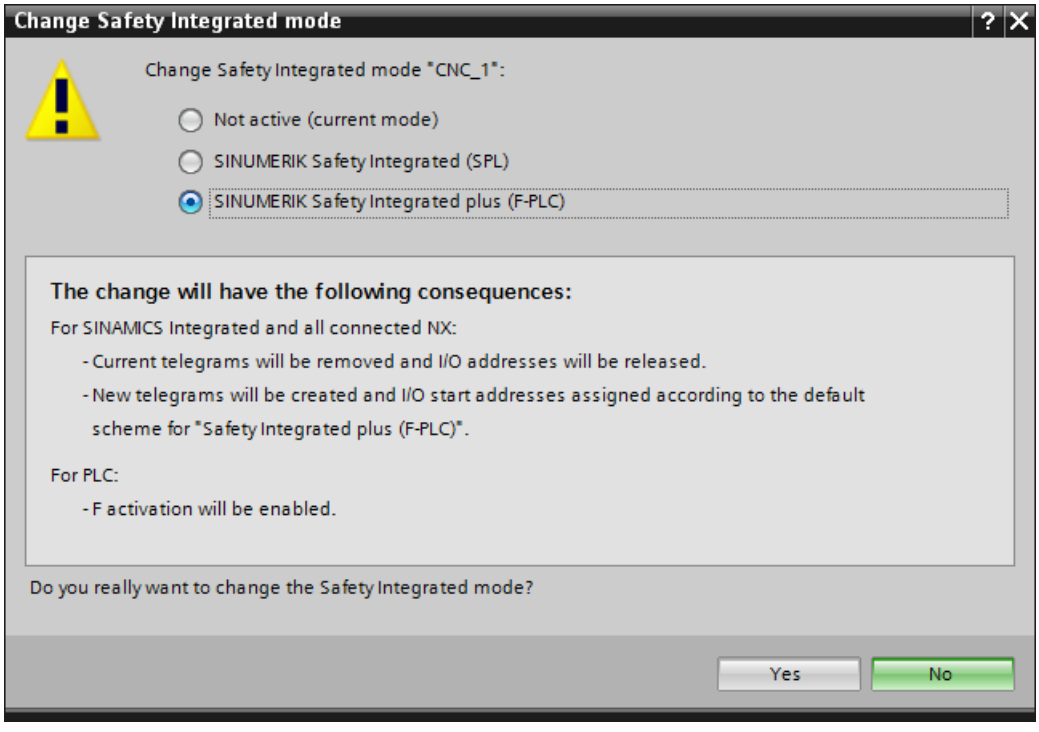


Figure 7-2 "Change Safety Integrated mode" dialog

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 affects the telegram configuration because, in the Safety Integrated plus (F-PLC) mode, different telegrams are used than in the inactivated Safety Integrated or the Safety Integrated modes.

Telegrams that are added or changed are kept, however, as long as they are compatible with the newly selected Safety Integrated mode.

Make sure, if applicable, that any modifications are still present following the change of mode in the telegram configuration (Page 251).

7.2.3 Configuring additional safety-related components

Basic procedure

After you have activated Safety Integrated plus, you can insert and configure optional F-I/Os as well as fail-safe 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.

Precondition

- The NCU is in the STOP operating state.

  Note

  Loading/stopping via TIA Portal only applies to PLC

  Using the TIA Portal, you can stop and then restart the PLC before the loading. However, the other subcomponents of the NCU are not stopped or started.

- A network connection exists between the PG/PC and the NCU.

Procedure

Proceed as follows to load the hardware configuration into the NCU:

1. In the project navigation, right-click on the NCU, and select command "Load to device > Hardware configuration".
2. Make the following settings in the "Extended load" dialog:
   – PG/PC interface: Network card used, e.g. "Intel[R] Ethernet Connection I217-V"
   – Connection with interface/subnet: Directly at slot '2 X120/X130/127'
3. Click "Start search".
   A search is made for the target devices, and they are displayed in the 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".

7.2.5 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.

The assignment of a device name for a PROFINET IO device can be compared with setting the PROFIBUS address of a DP slave.

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. Enter the required device name in the device properties in the field "Name".
2. Click in the network view, right-click on the device and select command "Assign name".

3. Make the following settings in the "Assign PROFINET device name" dialog:
   - 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.

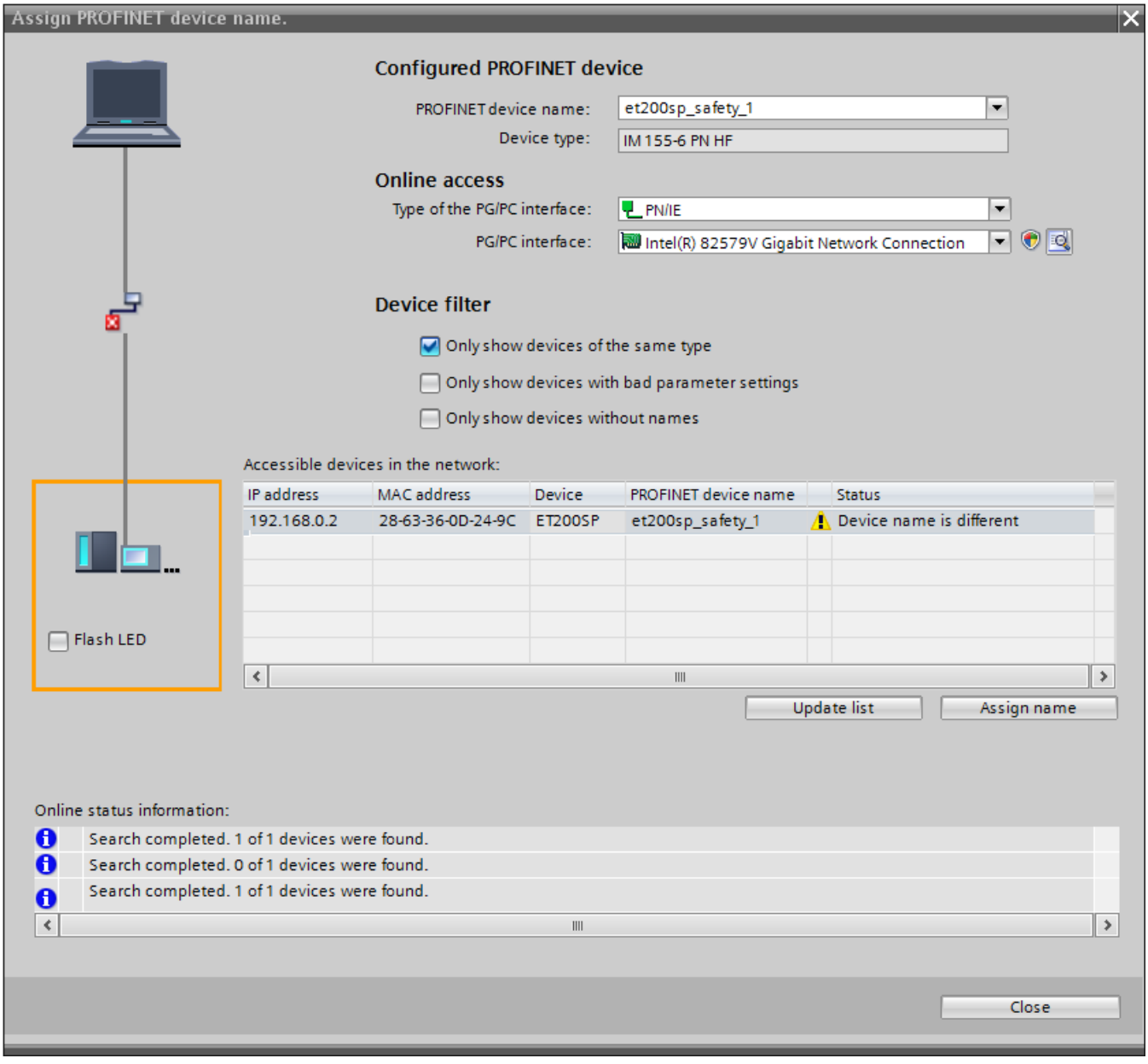


Figure 7-3 Dialog "Assigning a PROFINET device name"

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-destination addresses of the F-I/O of PROFIsafe address type 1 are generally assigned using the DIL switch on the module. 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 217)").

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".

As an alternative to this procedure, you can use the F-IO Connect commissioning software:

SINUMERIK F-IO Connect in SIOS (http://support.industry.siemens.com/cs/document/109744986/)

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

Precondition

- 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:

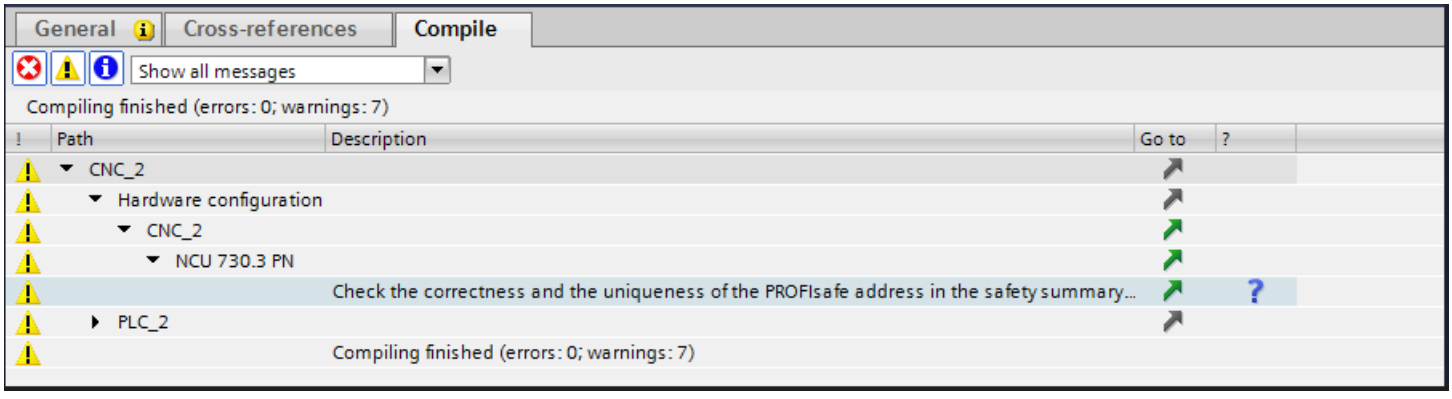


Figure 7-4 Warning when compiling the safety program

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.

Rail - Slot	Module	Start address	F-destination address	F-monitoring time	Parameter signature (w/o addresses)
0	Drive_Axis_1_SIEMENS_telegram_903	1008	1	150 ms	0xEE5 (3813)
0	Drive_Axis_2_SIEMENS_telegram_903	992	2	150 ms	0xEE5 (3813)
0	Drive_Axis_3_SIEMENS_telegram_903	976	3	150 ms	0xEE5 (3813)
0	Drive_Axis_4_SIEMENS_telegram_903	960	4	150 ms	0xEE5 (3813)
0	Drive_Axis_5_SIEMENS_telegram_903	944	5	150 ms	0xEE5 (3813)
0	Drive_Axis_6_SIEMENS_telegram_903	928	6	150 ms	0xEE5 (3813)

   Figure 7-5 F-target addresses of SINAMICS Safety Integrated drive objects in the safety printout (example)

2. Check the PROFIsafe addresses listed in the safety printout:
   - Compare the F-target addresses of the drive objects of SINAMICS Safety Integrated and NX modules with the values of the p9610 drive parameter
   - 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

Precondition

- Safety Integrated plus (F-PLC) is active.
- The F-components have been configured and parameterized.

Example of a handling overview

Step	Description
1	Create receive/send data as PLC tags (Page 219)
2	Adapting the settings of the F-runtime group (optional) (Page 221)
3	Setting up access protection (Page 222)
4	Parameterizing EMERGENCY STOP (Page 223)
5	Implementing user acknowledgment for global reintegration (Page 224)
6	Acknowledging messages related to safety functions integrated in the drive (Page 226)
7	Deselecting safety functions integrated in the drive (Page 229)
8	Initiate a forced checking procedure (test stop) (Page 231)
9	Programming the wiring test (Page 231)

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 tags with the corresponding drive addresses.

You can create all the PLC tags required before you start programming - or you can always add your PLC tags if you wish to access new drive data. If you address the drive data with absolute values instead, tag names are automatically assigned that are subsequently difficult to comprehend.

You can import or export PLC tags in the XLSX, SDF or XML formats. You can copy PLC tag tables as copy templates in global libraries.

Procedure

Proceed as follows to create PLC tag tables with the required drive data.

1. In the project navigation, double-click below "PLC tags " on "Add new tag table", e.g. "CNC_1 > PLC_1 > PLC tags > Add new tag table".
2. Right-click on the new tag table, select "Rename" and assign a name, e.g. "Safety status data" or "Safety control data".

3. Double-click on the new tag table to open it.
4. In the "Name" column, click on "Add" and enter the tag properties:

Property	Meaning
Name	Enter a meaningful name, e.g. <drive name>-<process data>-<where relevant, bit identifier>. Example 1: DR1-S_ZSW2-SP_valid Example 2: DR2-S_SLS_LIMIT_A
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 Safety Integrated. The standard start addresses are also listed in Tables (Page 341). • Refer to the telegram structure (Page 344) 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 347). Example 1: %I1010.6 Example 2: %QW996
Comment	Optionally, you can formulate a user-defined note for each tag that is added - or take this from the manual.

Result

The PLC tags were added.

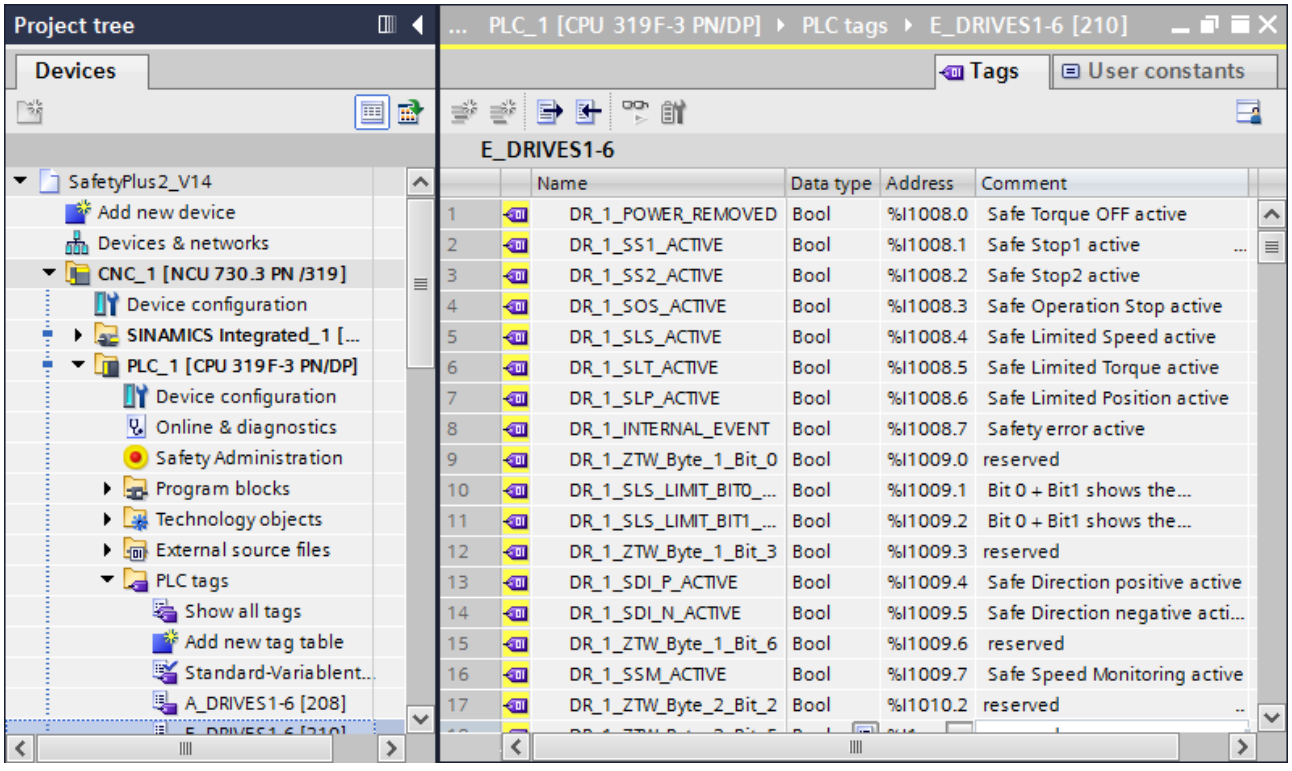


Figure 7-6 Example of a user-defined tag table, with the drive addresses required in the programming

7.3.3 Adapting the settings of the F-runtime group (optional)

An F-runtime group is automatically created when you activate the Safety Integrated plus (F-PLC) mode. The associated F-blocks are provided in folder "Program blocks" - or in the Safety Administration Editor under "F-blocks":

- CYC_INT5 [OB35]
- Main safety [FB1010]
- Main safety_DB [DB1010]

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-relevant program sections that are executed quickly, in their own dedicated F-runtime group.

Precondition

- Safety Integrated plus (F-PLC) 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. If necessary, adapt the following settings.

Setting	Purpose
Calling block	CYC_INT5_RTG1 [OB35] is set as default. 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.
Main safety block	Default setting: Main_Safety_RTG1 [FB1010] In the drop-down list you can select a block other than the previously created F-block. The following main safety block numbers are intended for SINUMERIK Safety Integrated plus: 1010..1019.
I-DB for the main safety block	Default setting: Main_safety_RTG1_DB [DB1010] If the main safety block is an FB, then in the drop-down list you can adapt the associated I-DB. The following I-DB block numbers are intended for SINUMERIK Safety Integrated plus: 1010..1019.
Execution time of the calling block	If, as executing block, you use a cyclic interrupt OB 3x, then the parameterized execution time is displayed here. You can change this execution time in the properties of the PLC under "Alarms > Cyclic interrupts".
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.
DB for F-runtime group communication	If one F-runtime group is to provide tags 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".

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). *(S001)*

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 "Write protection for fail-safe blocks" 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

The operation "ESTOP1" implements an EMERGENCY STOP shutdown with acknowledgment for stop Category 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. Parameterize the inputs and outputs of the instruction.

Parameters	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, however, but instead use the corresponding settings 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.

Further 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 fail-safe 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:

Fault type	Passivation	Reintegration
Communication	All channels of the module	After a communication error, user acknowledgment is always required.
F-I/O or Drive		dependent on the F-I/O DB parameter: • ACK_NEC=1: user acknowledgment required • ACK_NEC=0 automatic reintegration
Channel	Depending on F-parameter "Behavior after channel fault" of the module: • Passivation of the channel • Passivation of the complete module	

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	Procedure
Evaluation of the acknowledgment request	You can evaluate the F-I/O DB tag "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 tags: – QBAD – QBAD_I_xx/QBAD_O_xx – 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 tag "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 tags ACK_NEC = 0 is only permitted, if, from a safety-relevant perspective automatic reintegration is permissible for the process involved. *(S010)*

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).

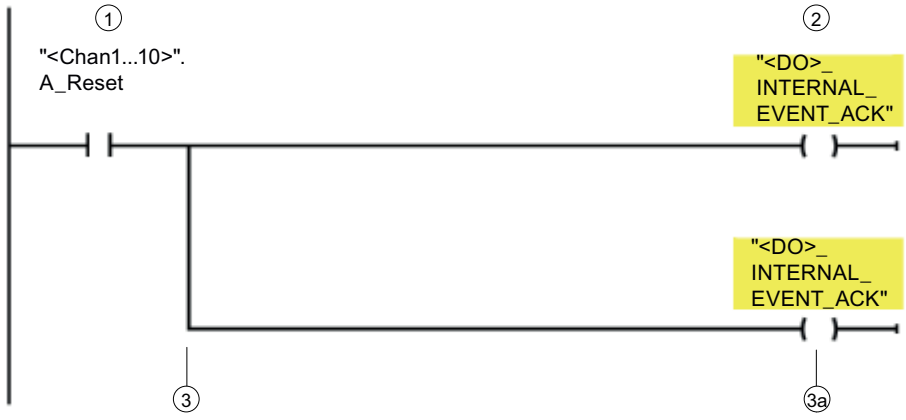
Precondition

- PLC tags for the "Internal Event ACK" signal are added (Page 219) for each drive object.

Procedure

In order to logically combine the reset signal of the machine control panel with the safety-relevant 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 tag> Example: "DR1-S_STW2-INTERNAL_EVENT_ACK"	Assign the logic operation result to the corresponding PLC tag, that you created for the "Internal Event ACK" signal of the appropriate drive.
(3)	Branch	If you are using several safety-relevant drive objects, for each drive object insert a branch together with the operation (see 3a).
(3a)	---( )--- Assignment <PLC tag> Example: "DR2-S_STW2-INTERNAL_EVENT_ACK"	Assign the logic operation result to the corresponding PLC tag.

Figure 7-7 Inserting a new network

Result

The channel reset signal of the channel involved was logically combined with the safety-relevant acknowledgment of faults in the individual drive objects.

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.

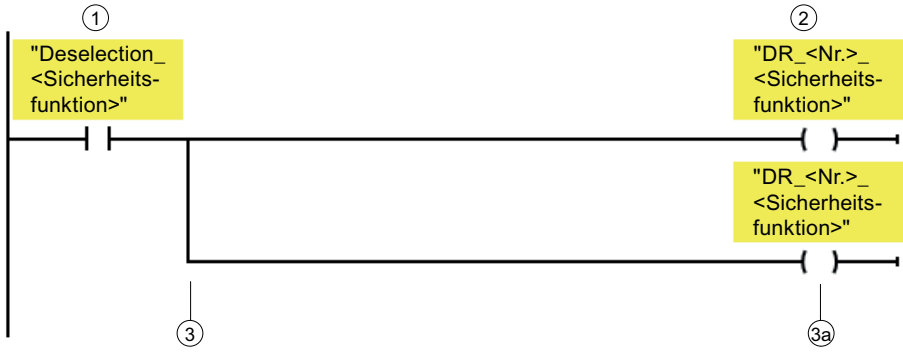
Precondition

- PLC tags for the signals required have been added (Page 219).

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: "Deselection_SS1" or Drive I/O address with ZSW bit	Address the PLC tag "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: "DR_1_SS1" 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: "DR_2_SS1" 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

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

7.4.1 Loading the configuration to the NCU

Precondition

- There is a network connection between the configuring PG/PC and SINUMERIK 840D sl.

Procedure

Proceed as follows to load the hardware and software configuration into the SINUMERIK 840D sl:

1. In the project navigation, right-click the NCU and select the "Load to device > Hardware and software (only changes)" command.
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.

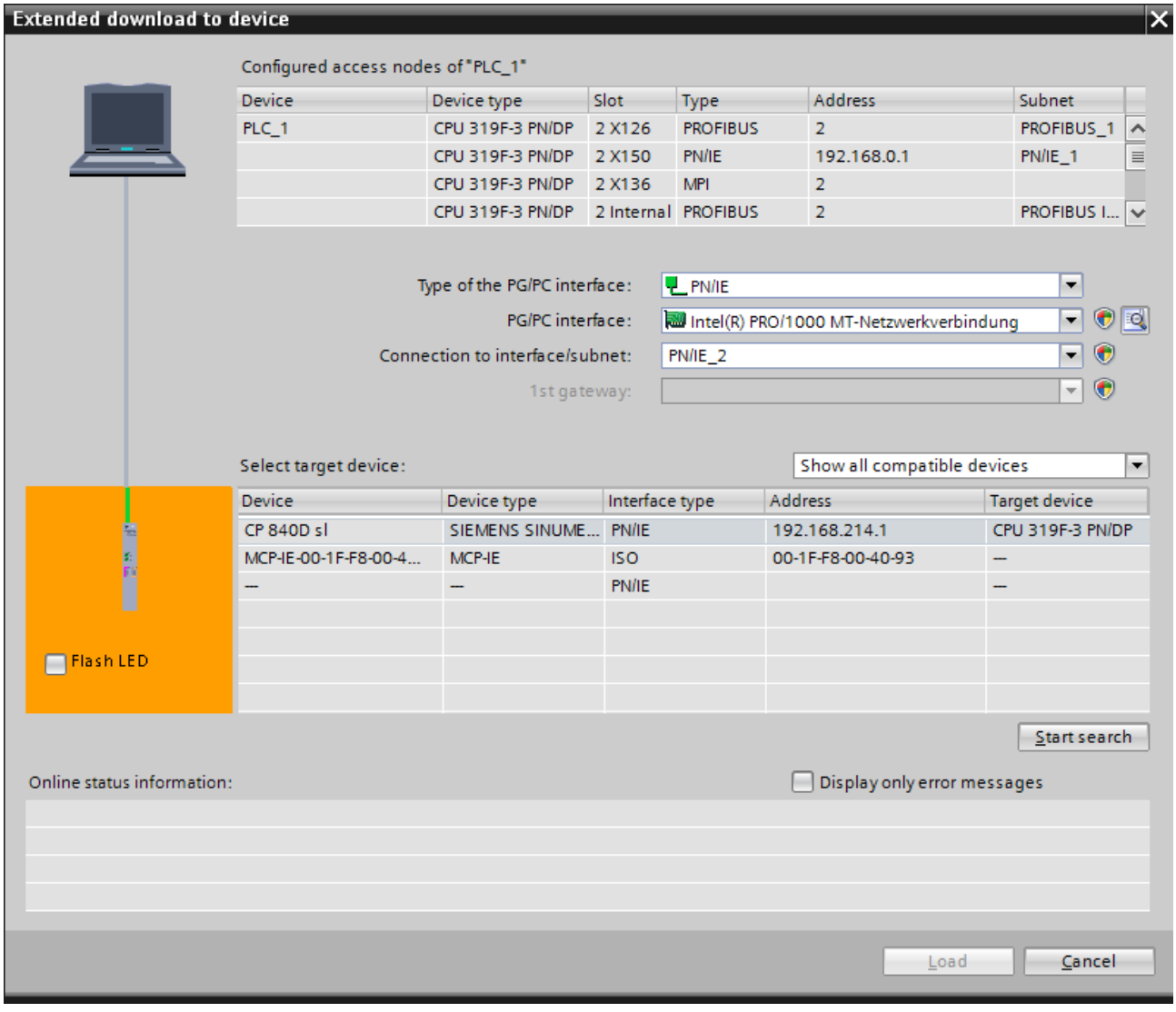


Figure 7-9 "Extended download" dialog

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 the "Results of the load procedure" dialog, select whether the PLC should be restarted, and then confirm with "Complete".

7.4.2 Transferring the safety mode from the configuration

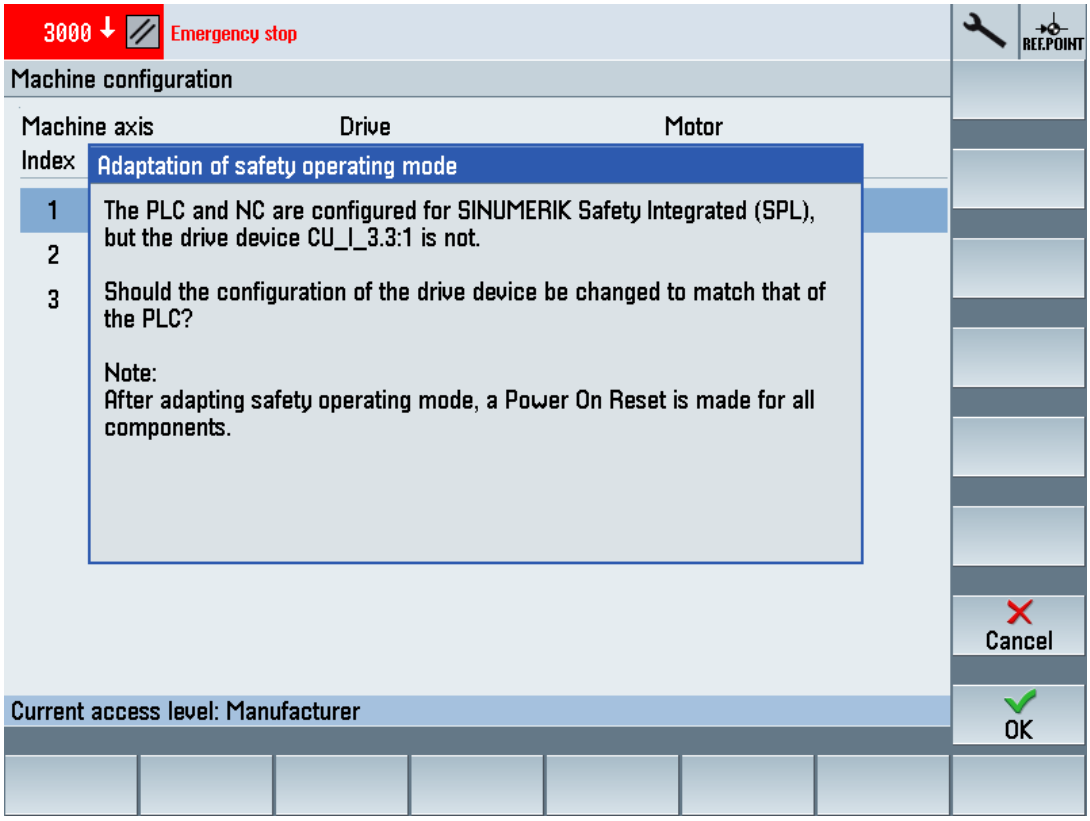
Precondition

- The configuration has been loaded (Page 232).

Procedure

To apply the safety mode in SINUMERIK Operate, proceed as follows:

1. In SINUMERIK Operate, switch to the commissioning area (start-up area) using "MENU SELECT > Commissioning".
2. Press the "Reset (po)" softkey and confirm with "Yes".
   The NCU is restarted, and the "Adaptation of safety operating mode" dialog is then displayed.



3. Confirm the adaption of the safety mode with "OK".

7.5 Configuring NC and drive-specific safety settings

7.5.1 Overview

Higher-level safety settings are described in this chapter, which you specifically configure for each drive.

Requirement

- Access rights of access level 2 (service) are available in SINUMERIK Operate.
- The commissioning of the (non-safety-related) default drive functions has been completed.
- The configuration (hardware and software) is loaded in the NCU (Page 232).
- The transfer of the Safety Integrated mode from the configuration has been completed. (Page 233)

Example handling overview

Step	Description
1	Setting software options (Page 236)
2	Activating the safety commissioning mode (Page 236)
3	Selecting the safety functional scope (Page 238)
4	Parameterizing the setpoint speed limiting (Page 239)
5	Parameterizing reaction of the stop response (Page 241)
6	Parameterizing an encoder (Page 242) or Configuring encoderless operation (Page 246)
7	Configuring telegrams (Page 251)
8	Configuring the message buffer and alarm buffer (Page 321)

7.5.2 Setting software options

Procedure

Proceed as follows to set the software options for Safety Integrated plus:

1. In SINUMERIK Operate switch to licensing via "MENU SELECT > Commissioning > Menu forward key > Licenses".
2. Press softkey "All options".
3. Set the safety software options required for your particular machine configuration:

Software option	Article No.	Purpose
SINUMERIK 840D sl Safety Integrated plus /SI logic	6FC5800-0AS60-0YB 0	Activate the F-PLC in SINUMERIK 840D sl in order to process the failsafe sensors and actuators in an F-program.
SINUMERIK 840D sl Safety Integrated plus / SI axis/spindle	6FC5800-0AK00-0YB 0	Use the motion control functions of the SINAMICS Safety Integrated in the SINUMERIK Safety Integrated plus (F-PLC) mode. License for 1 axis/spindle, multiple licensing in order to be able to use additional axes/spindles.
SINUMERIK 840D sl Safety Integrated plus /SI multi-axis package	6FC5800-0AS61-0YB 0	Use the motion control functions of the SINAMICS Safety Integrated in the SINUMERIK Safety Integrated plus (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.

See also

Licensing axes/spindles and F-PLC (Page 36)

7.5.3 Activating the safety commissioning mode

Changes to the safety-relevant 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-relevant) standard drive functions must have been completed.
- The configuration (hardware and software) has been loaded to the NCU (Page 232).
- Transferring the Safety Integrated mode from the configuration has been completed (Page 233).

Procedure

Proceed as follows to activate the Safety Integrated commissioning mode for all drives:

1. In SINUMERIK Operate, go to "MENU SELECT > Commissioning > Menu forward key > Safety".

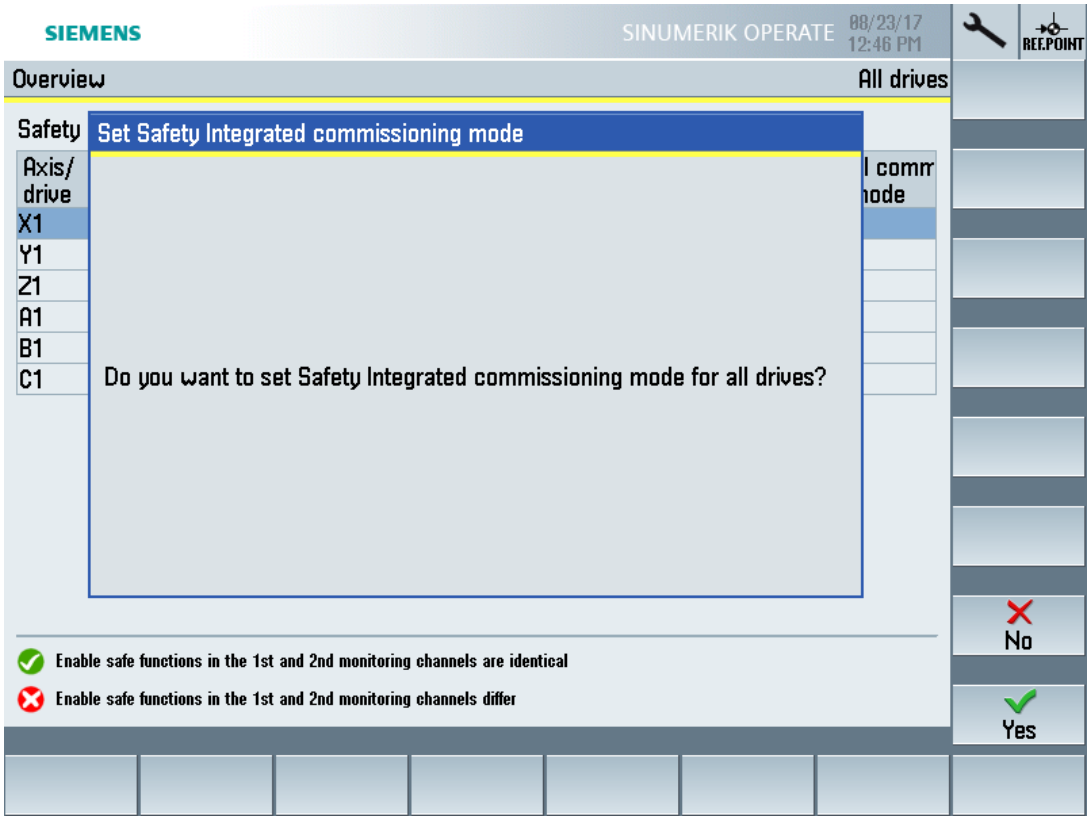


Figure 7-10 Activating the Safety Integrated commissioning mode for individual drives

> **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-relevant 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-relevant) standard drive functions must have been completed.
- The configuration (hardware and software) has been loaded to the NCU (Page 232).
- Transferring the Safety Integrated mode from the configuration has been completed (Page 233).
- The safety commissioning mode is activated for the drive to be configured (Page 236).

Procedure

Proceed as follows to set the safety functional scope for a drive:

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".
3. Under "Select safety function" select the functional scope:
   - 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 31), Overview of safety functions integrated in the drive (Page 23), Control options (Page 193)
5. Press softkey "OK".

Note

When the selected safety function is saved, the enable signal 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.

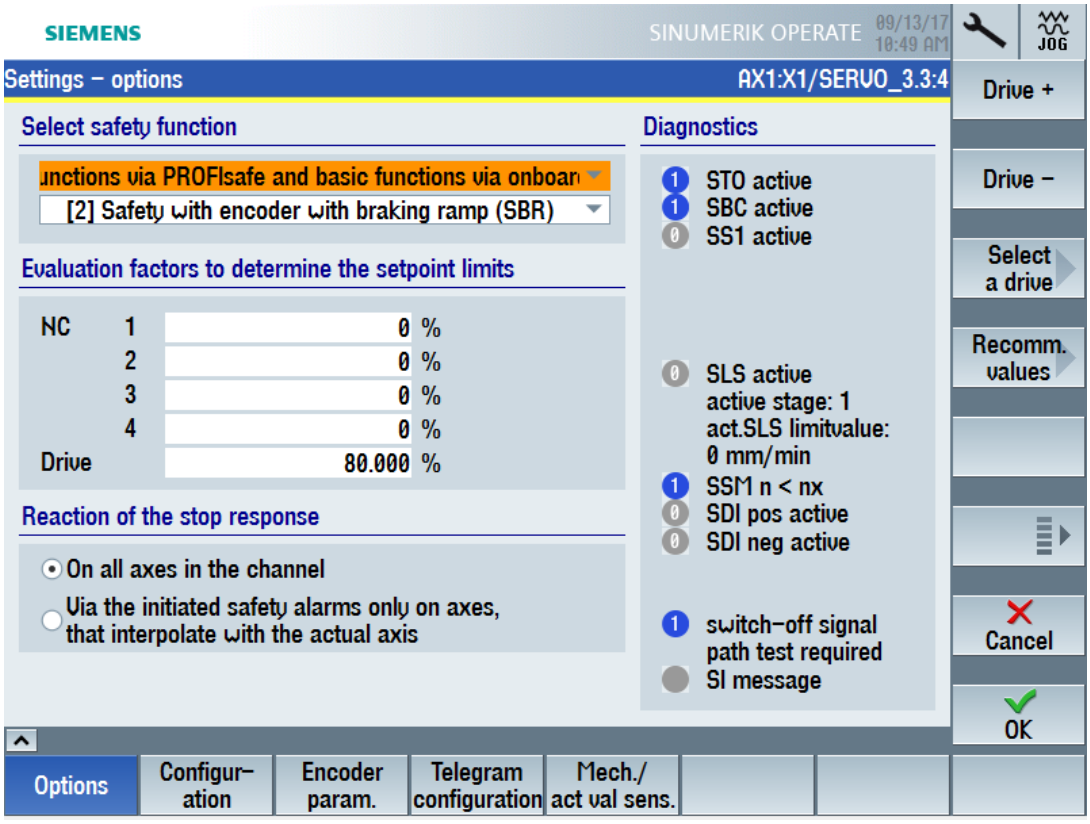
Precondition

- The safety functional scope of the drive has been selected. (Page 238)

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.



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 a power on 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.

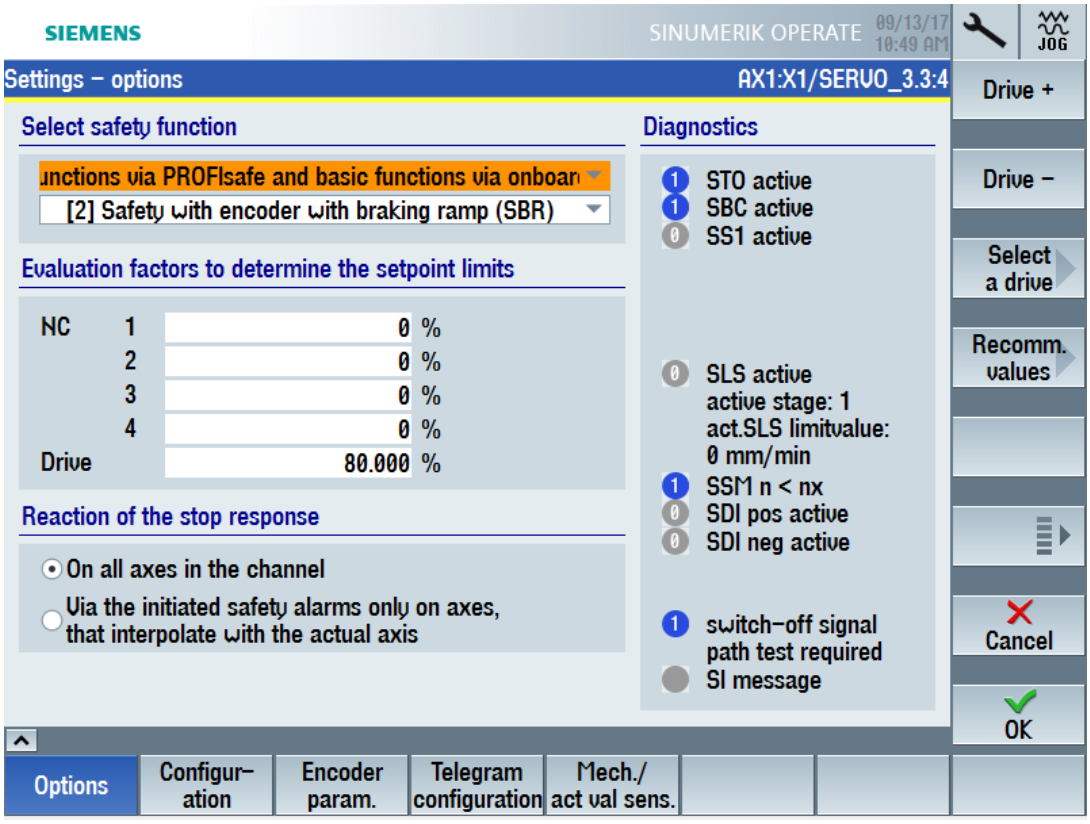
7.5.6 Parameterizing reaction of the stop response

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, go to the safety settings of the drive via "MENU SELECT > Commissioning > Menu forward key > Safety > Settings > Options".
2. Go to the corresponding drive, for example, using the "Select drive" softkey.
   The parameter assignment is displayed for the selected drive.



3. Select one of the following options as desirable 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.

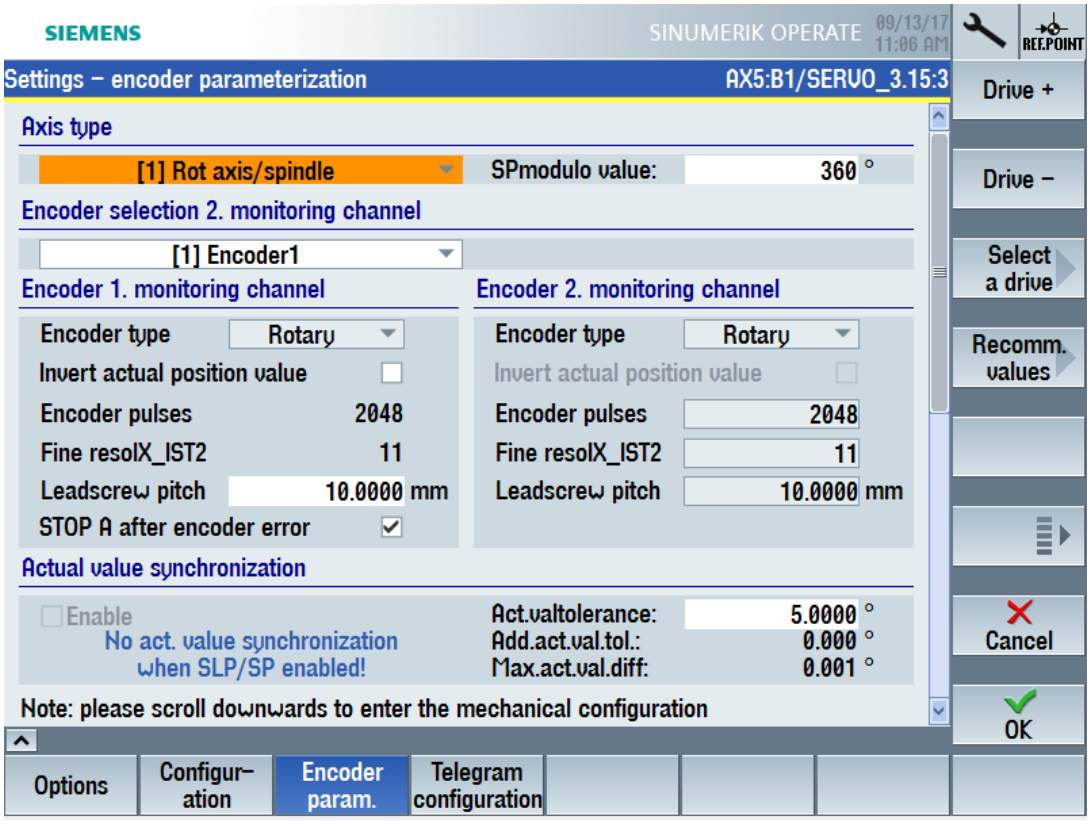
7.5.7 Parameterizing an encoder

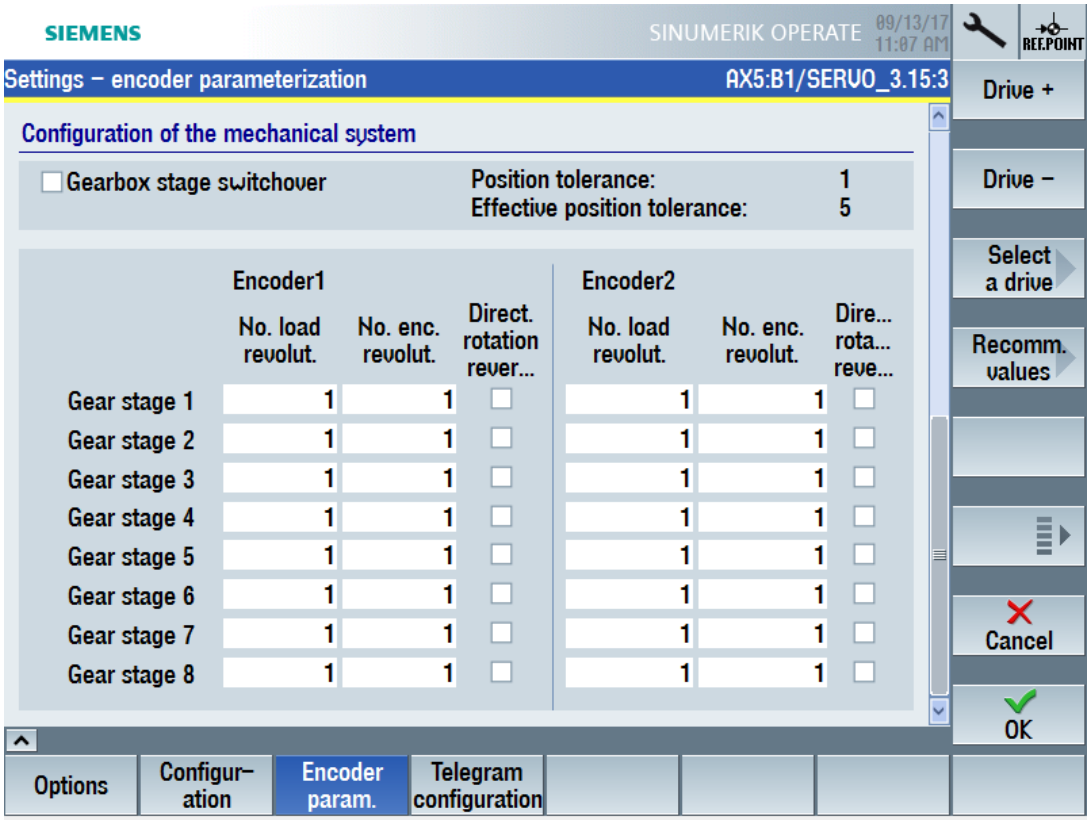
Precondition

- The SI commissioning mode (Page 236) 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





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 enabled. 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-relevant 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.
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.

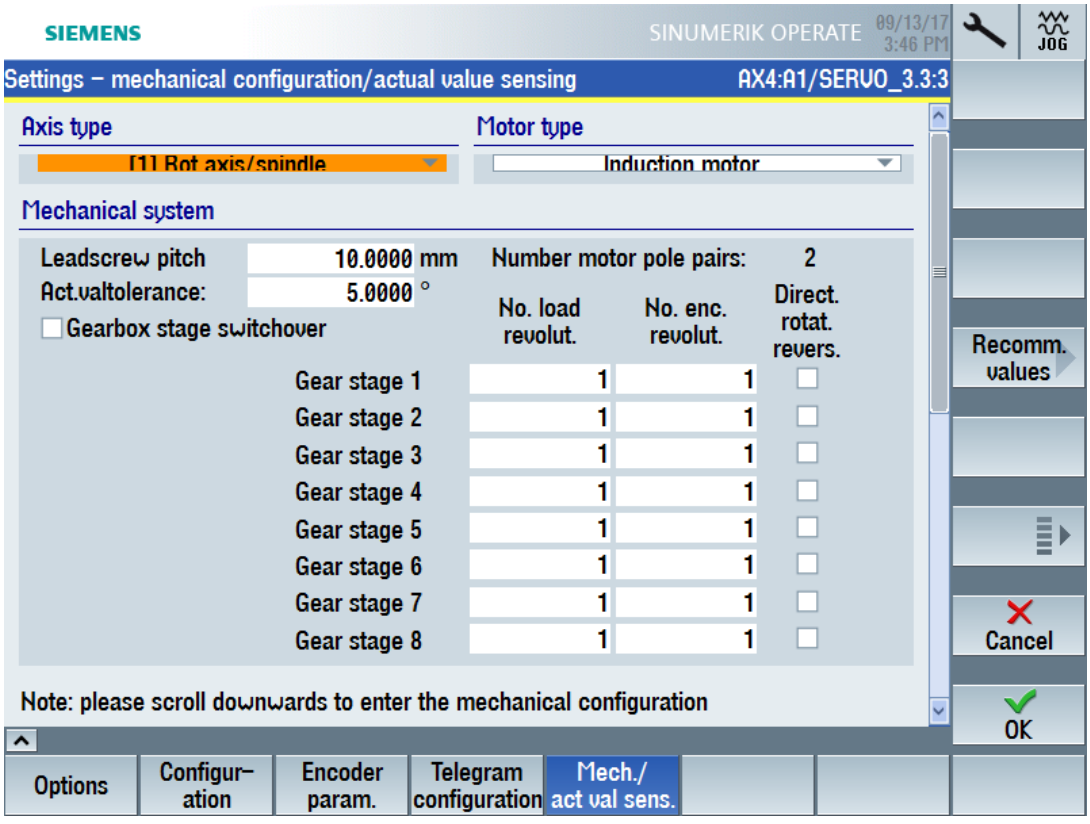
7.5.8 Configuring encoderless operation

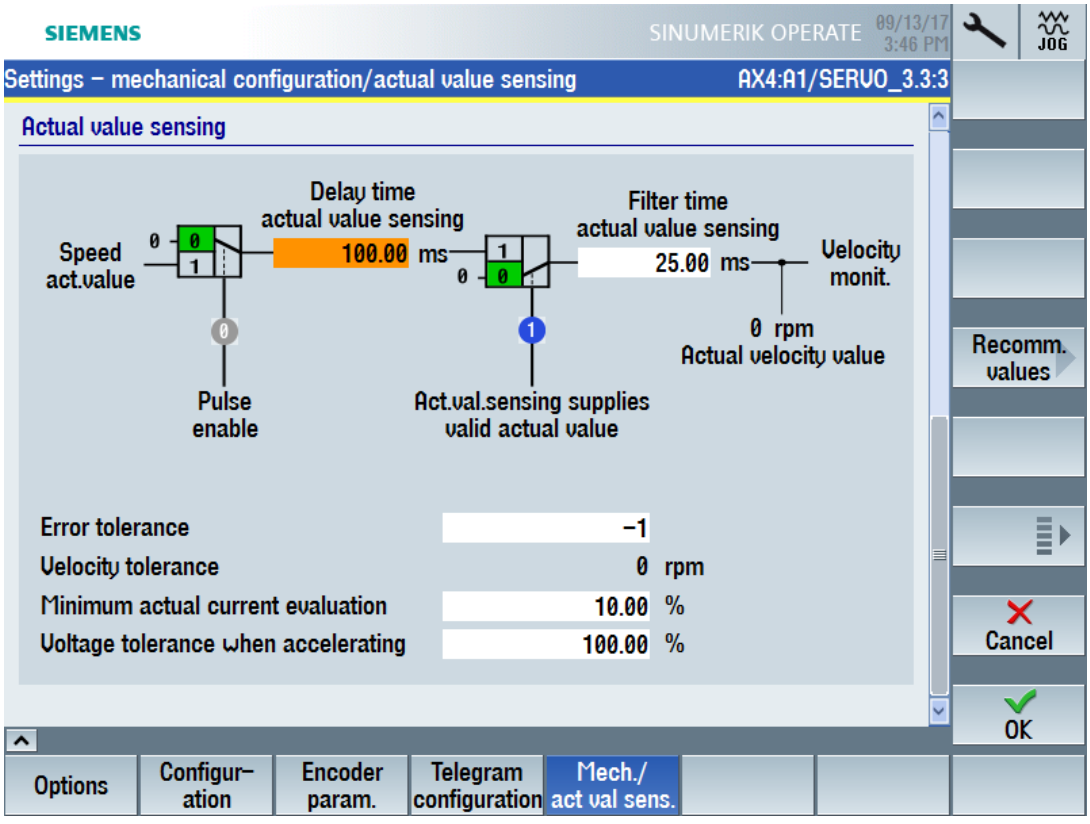
Precondition

- The SI commissioning mode (Page 236) 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





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. 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 between 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-relevant 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).

Setting	Meaning
Minimum actual current evaluation	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
Acceleration voltage tolerance	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

See also

Selecting the safety functional scope (Page 238)

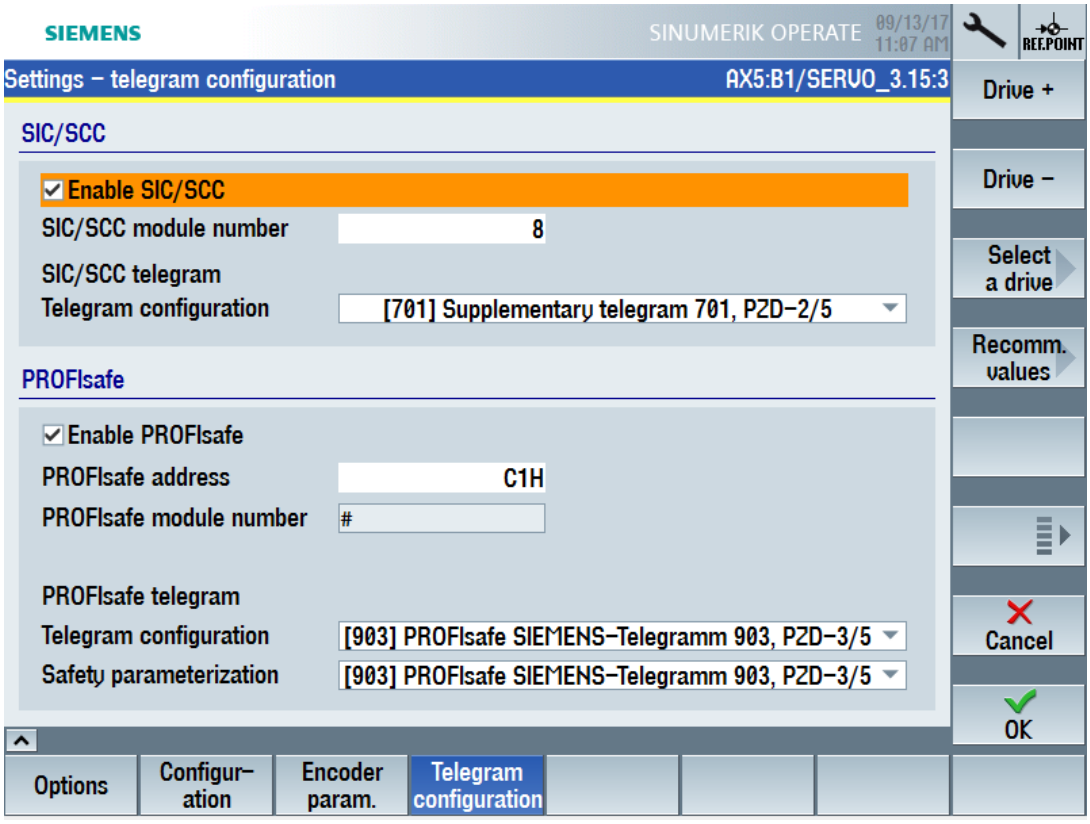
7.5.9 Configuring telegrams

Precondition

- The SI commissioning mode (Page 236) is active for the drive to be configured.
- Extended Functions or Basic Functions via PROFIsafe are set (Page 238) for the drive to be configured.

Call up "Telegram configuration" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > 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.
Telegram configuration	Sets the telegram type for the Safety Info Channel (SIC)/Safety Control Channel (SCC)

Table 7-9 PROFIsafe telegram settings (Settings - telegram configuration)

Setting	Meaning
Enable PROFIsafe	Enables/inhibits PROFIsafe communication between F-PLC and drive
PROFIsafe address	Sets the PROFIsafe address for the Control Unit.
PROFIsafe module number	Sets the PROFIsafe module number.
Telegram configuration	Sets the PROFIsafe telegram type.
Safety parameter assignment	Sets the PROFIsafe telegram type for the Control Unit.

7.6 Configuring safety functions integrated in the drive

7.6.1 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 7-10 Startup screen forms and function descriptions

Startup screen form	Detailed function description
STO/SS1 Basic (Page 255)	Safe Torque Off (Page 87) / Safe Stop 1 (Page 76)
STO Extended (Page 256)	Safe Torque Off (Page 87)
SBC (Page 258)	Safe Brake Control (Page 93)
SS1 Extended (Page 259)	Safe Stop 1 (Page 80)
SS2/SOS (Page 261)	Safe Stop 2 (Page 100) / Safe Operating Stop (Page 110)
SLS (Page 269)	Safely-Limited Speed (Page 113)
SSM (Page 272)	Safe Speed Monitor (Page 127)
SAM (Page 265)	Safe Acceleration Monitor (Page 133)
SBR (Page 268)	Safe Brake Ramp (Page 135)
SDI (Page 274)	Safe Direction (Page 138)
SLP/SP (Page 278)	Safely-Limited Position (Page 146) / Safe Position (Page 151)
SBT (Page 281)	Safe Brake Test (Page 156)
SCA (Page 276)	Safe Cam (Page 168)

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.

7.6.2 STO/SS1 Basic

Precondition

- The SI commissioning mode (Page 236) is active for the drive to be configured.
- One of the basis functions (Page 238) is is selected.

Displaying the "Safe torque off - STO/SS1 Basic" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > STO/SS1 Basic

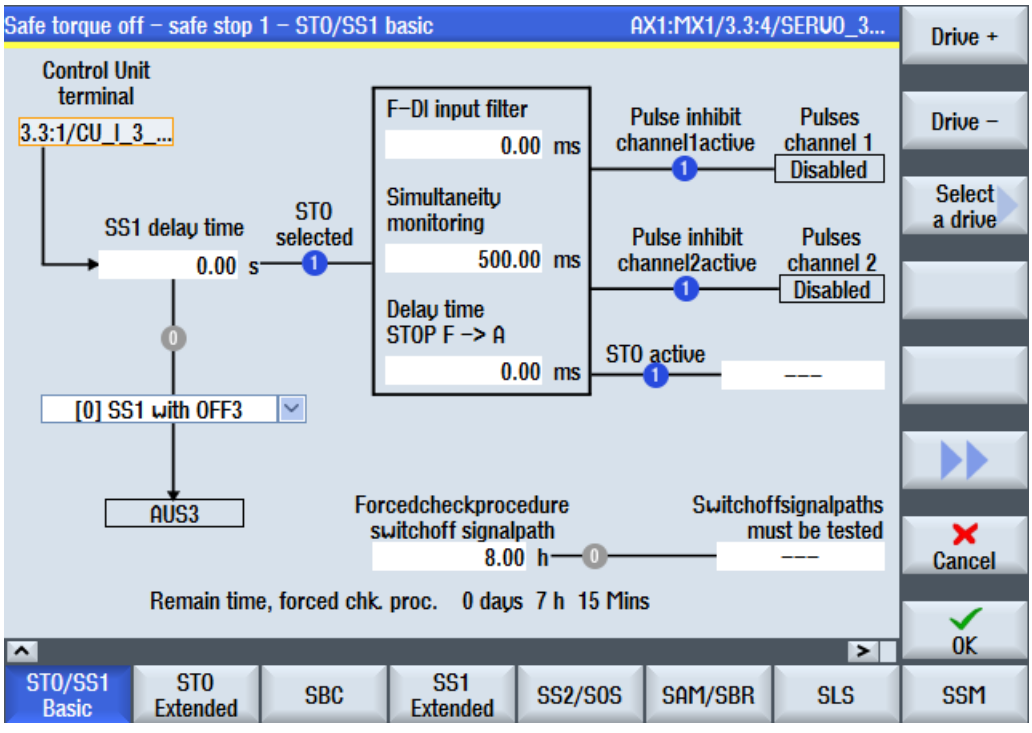


Figure 7-11 Safe Torque Off - Safe Stop 1 - STO/SS1 Basic

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 reaction) (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 paths must be tested (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-relevant inputs (SGE) on the Control Unit.
Delay time STOP F -> STOP A (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 paths must be tested (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.

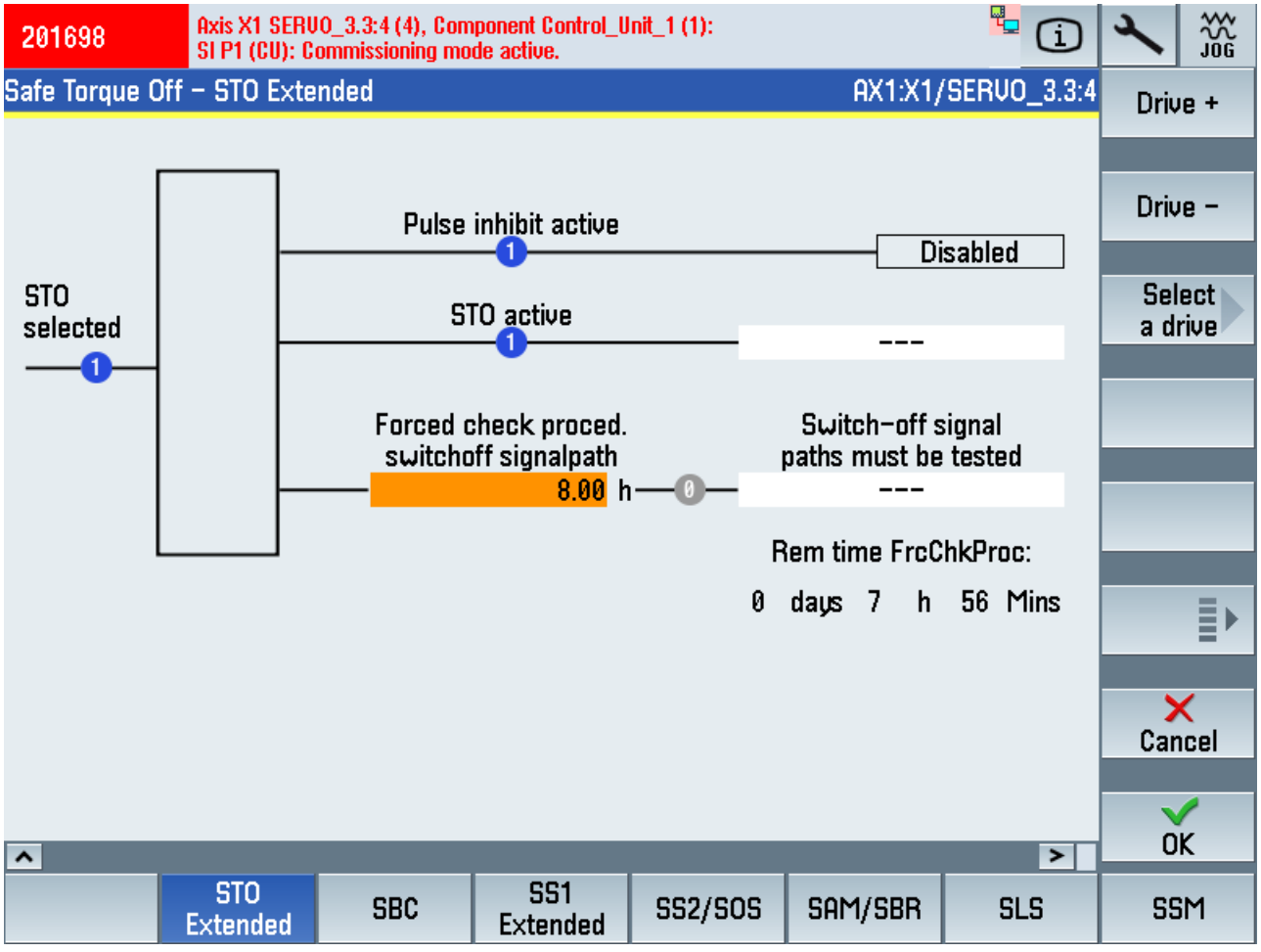
7.6.3 STO Extended

Precondition

- The SI commissioning mode (Page 236) 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



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.

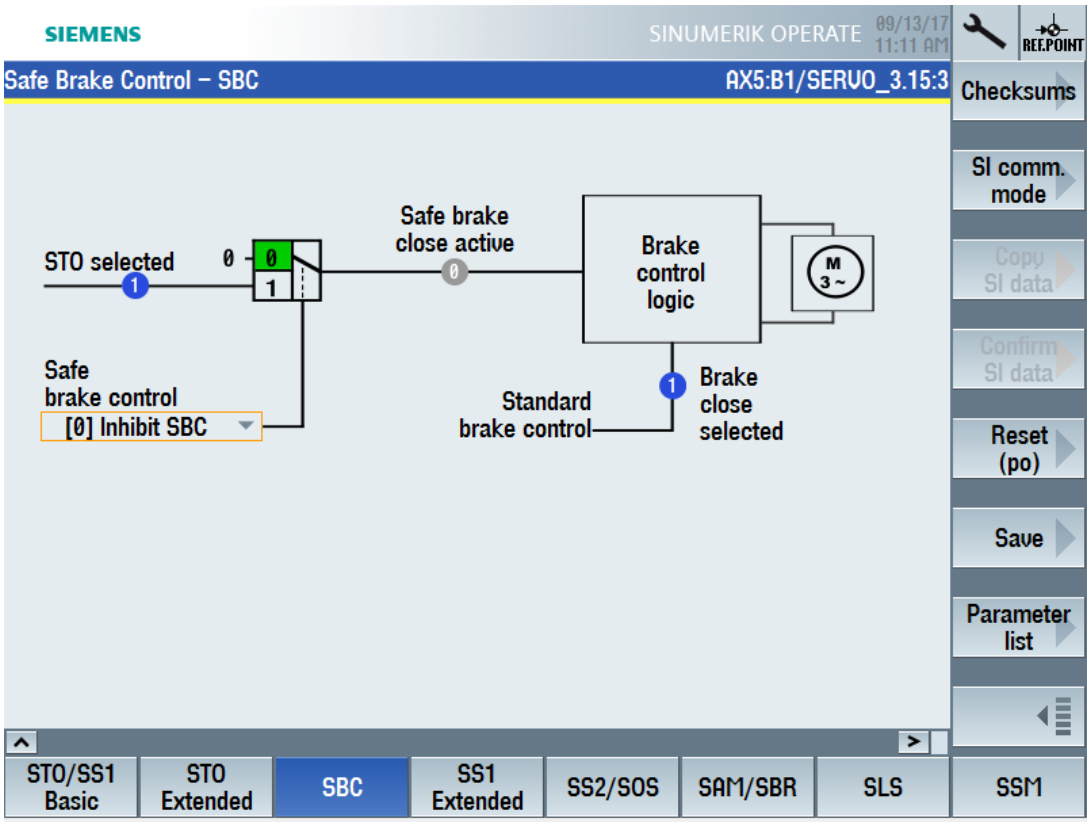
7.6.4 SBC

Precondition

- The SI commissioning mode (Page 236) 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



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
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

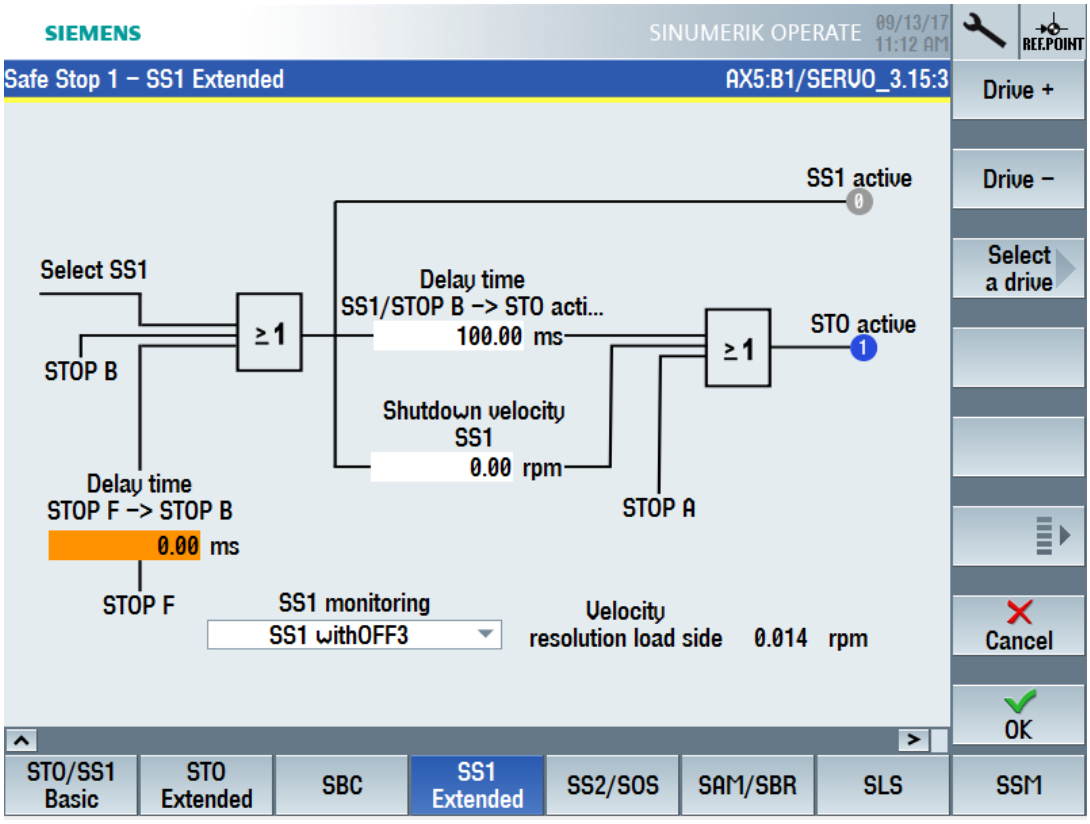
7.6.5 SS1 Extended

Precondition

- The SI commissioning mode (Page 236) 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



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.

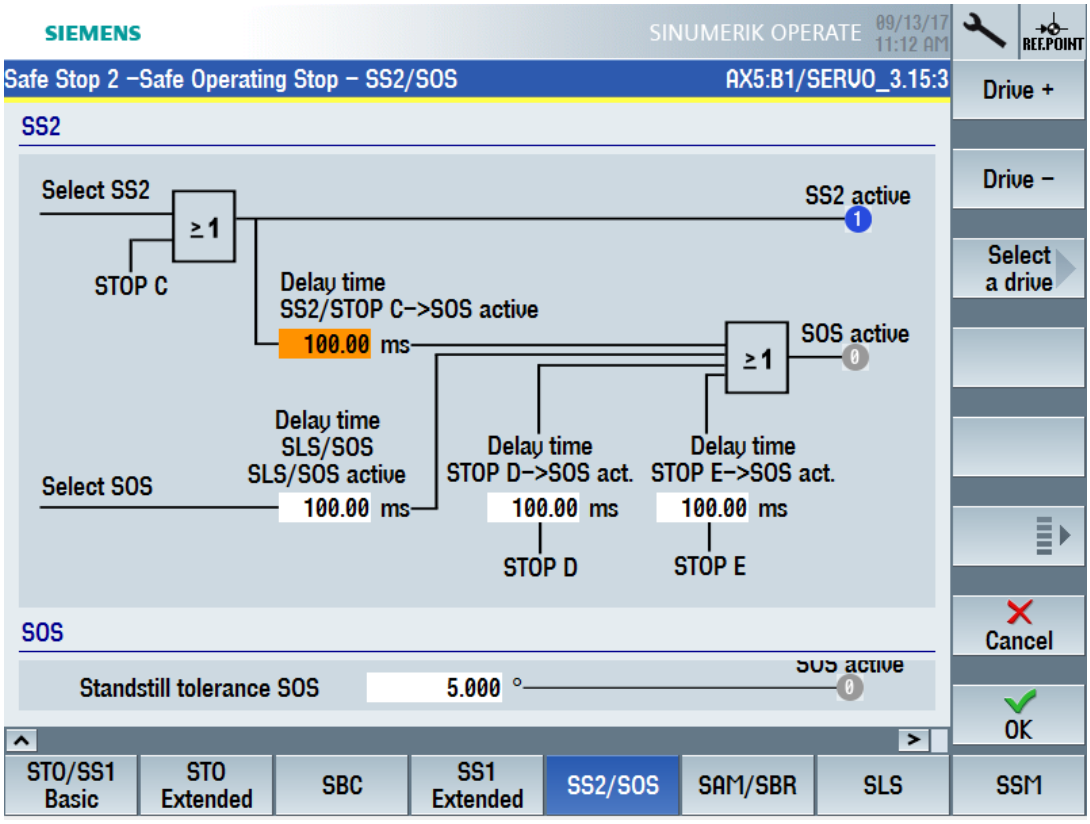
7.6.6 SS2/SOS

Precondition

- The SI commissioning mode (Page 236) 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



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)
Standstill tolerance SOS p9530	Sets the tolerance for the "Safe operating stop" function (SOS).

7.6.7 SS2E

Precondition

- The Safety Integrated commissioning mode 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

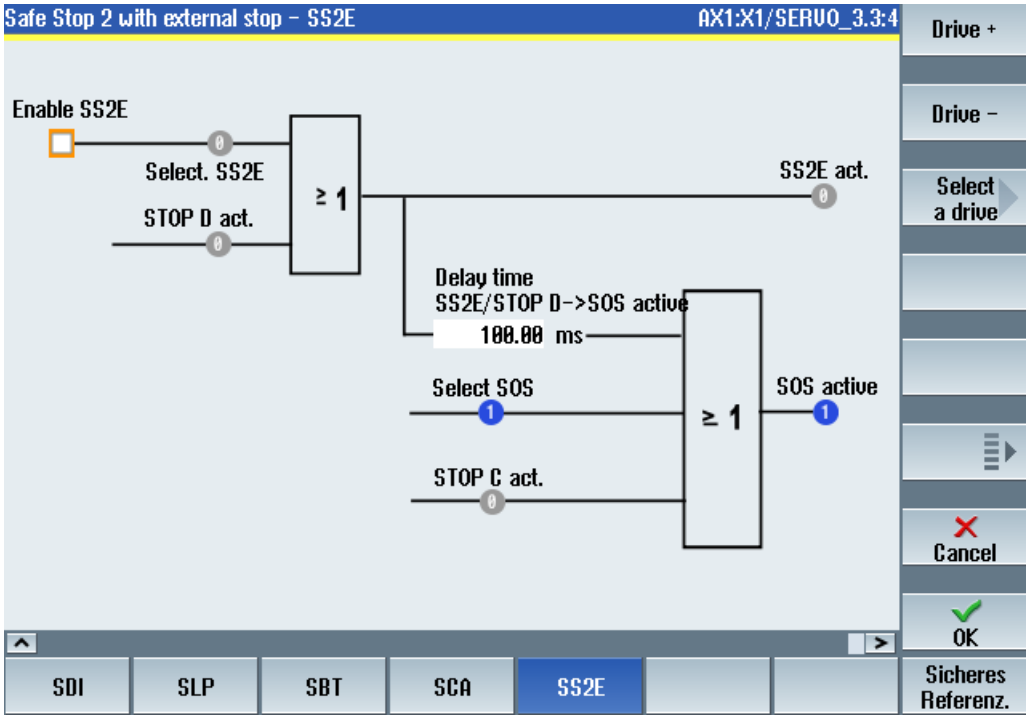


Figure 7-12 Safe Stop 2 with external stop - SS2E

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.

See also

Activating the safety commissioning mode (Page 236)

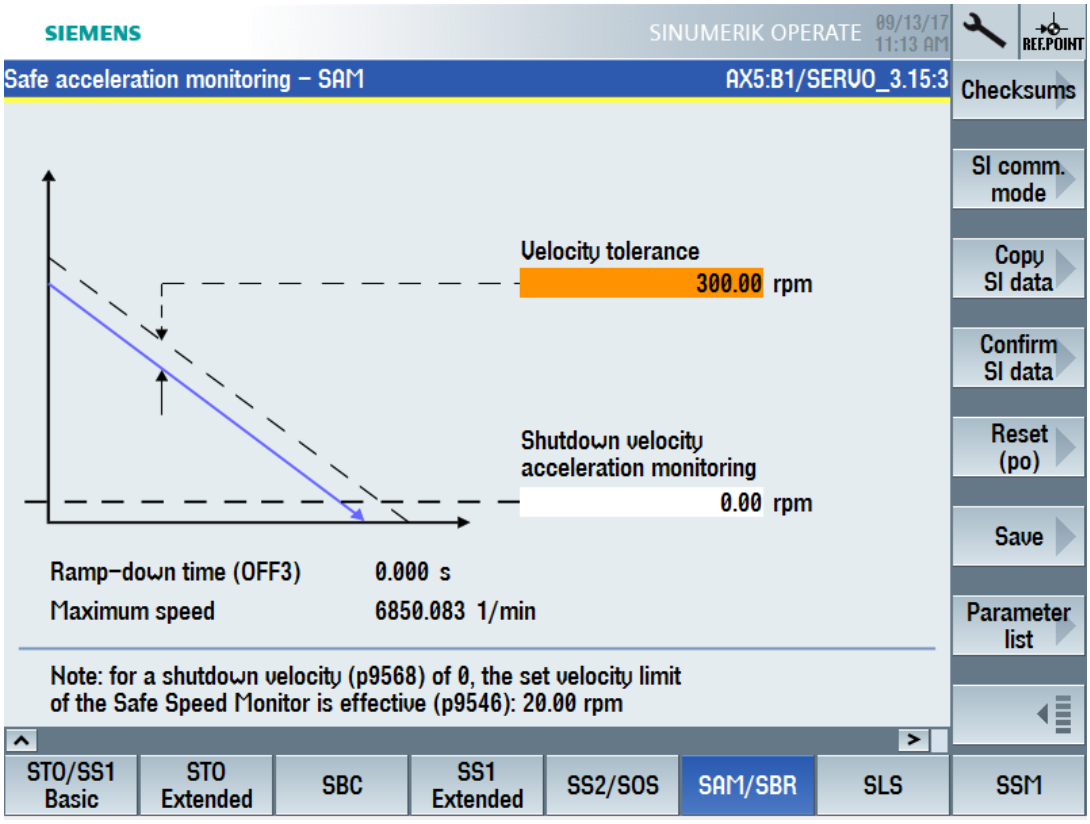
7.6.8 SAM

Precondition

- The SI commissioning mode (Page 236) 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



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/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. • 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.

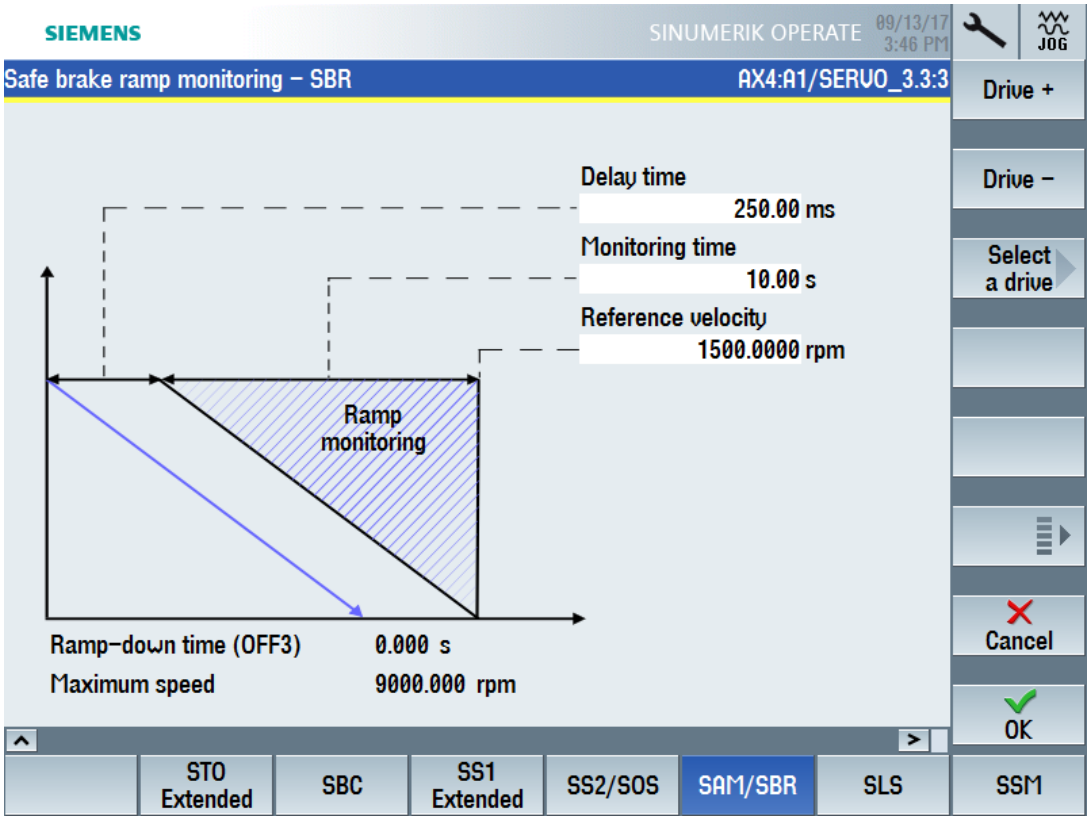
7.6.9 SBR

Precondition

- The SI commissioning mode (Page 236) is active for the drive to be configured.
- The drive is configured for operation without an encoder and Extended Functions.
- 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 > 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.

7.6.10 SLS

Precondition

- The SI commissioning mode (Page 236) is active for the drive to be configured.
- The drive is configured for operation with an encoder and Extended Functions.

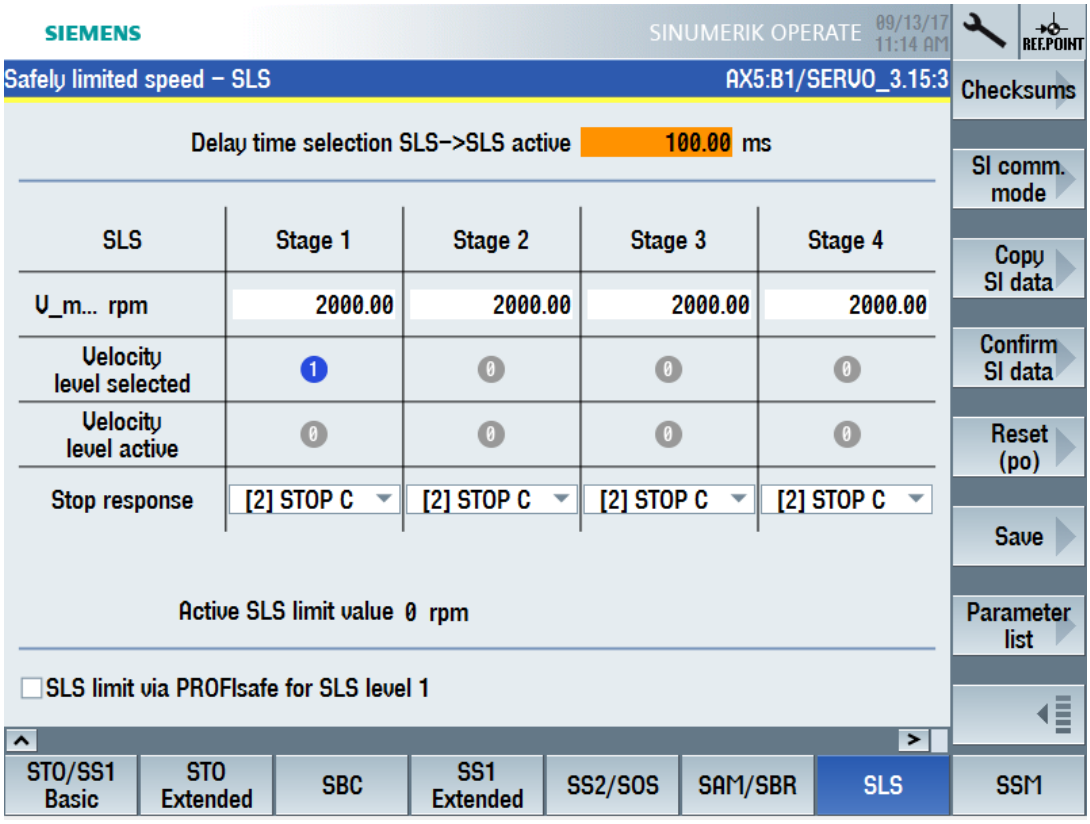
Note

Transmitting process data for SLS in SIEMENS telegram 903

PROFIsafe telegram 903 - set as default setting for SINUMERIK - is optimized for the use of SCA (Safe Cam), and only includes restricted process data for SLS. On the other hand, SIEMENS telegram 902 includes all of the process data for SLS.

Display "Safely Limited Speed - SLS" commissioning screen

MENU SELECT > Commissioning > Menu forward key > Safety > Functions > 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, when switching over the "Delay time, selecting SLS -> SLS active" is active (see above). Switchover between these 4 values The value of a selected maximum velocity level 1 is transferred via PROFIsafe if check box "SLS limit via PROFIsafe for SLS level 1" is active.
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 velocity level 1 via PROFIsafe can also be used to parameterize (fixed) maximum velocity levels 2, 3 and 4. When activated, the value is transferred using PROFIsafe in control word S_SLS_LIMIT_A (Page 357), 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 velocity level 1" If an incorrect SLS limit value is transferred, then the converter responds with the parameterized "Stop response level 1".

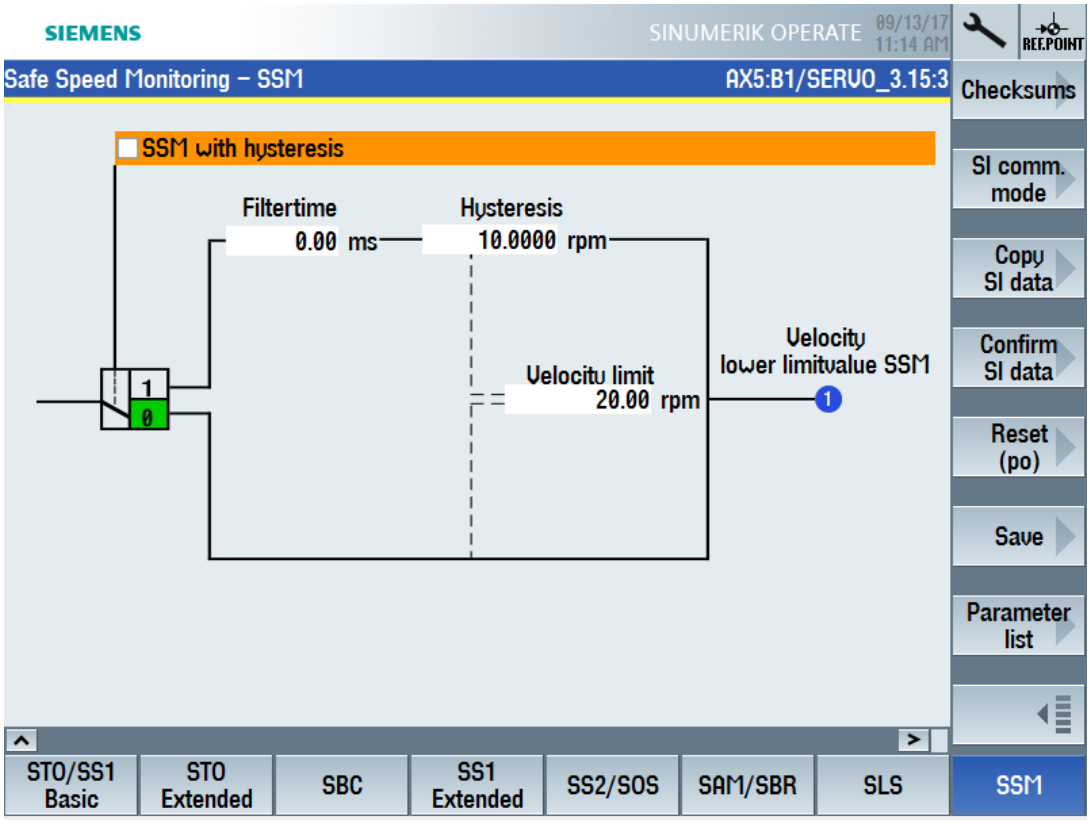
7.6.11 SSM

Precondition

- The SI commissioning mode (Page 236) 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



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.

Setting	Meaning
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 242)), then you must also comply with the following rule: • "SI Motion slip velocity tolerance" (p9549) ≤ hysteresis
Velocity 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 suppression 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 130)

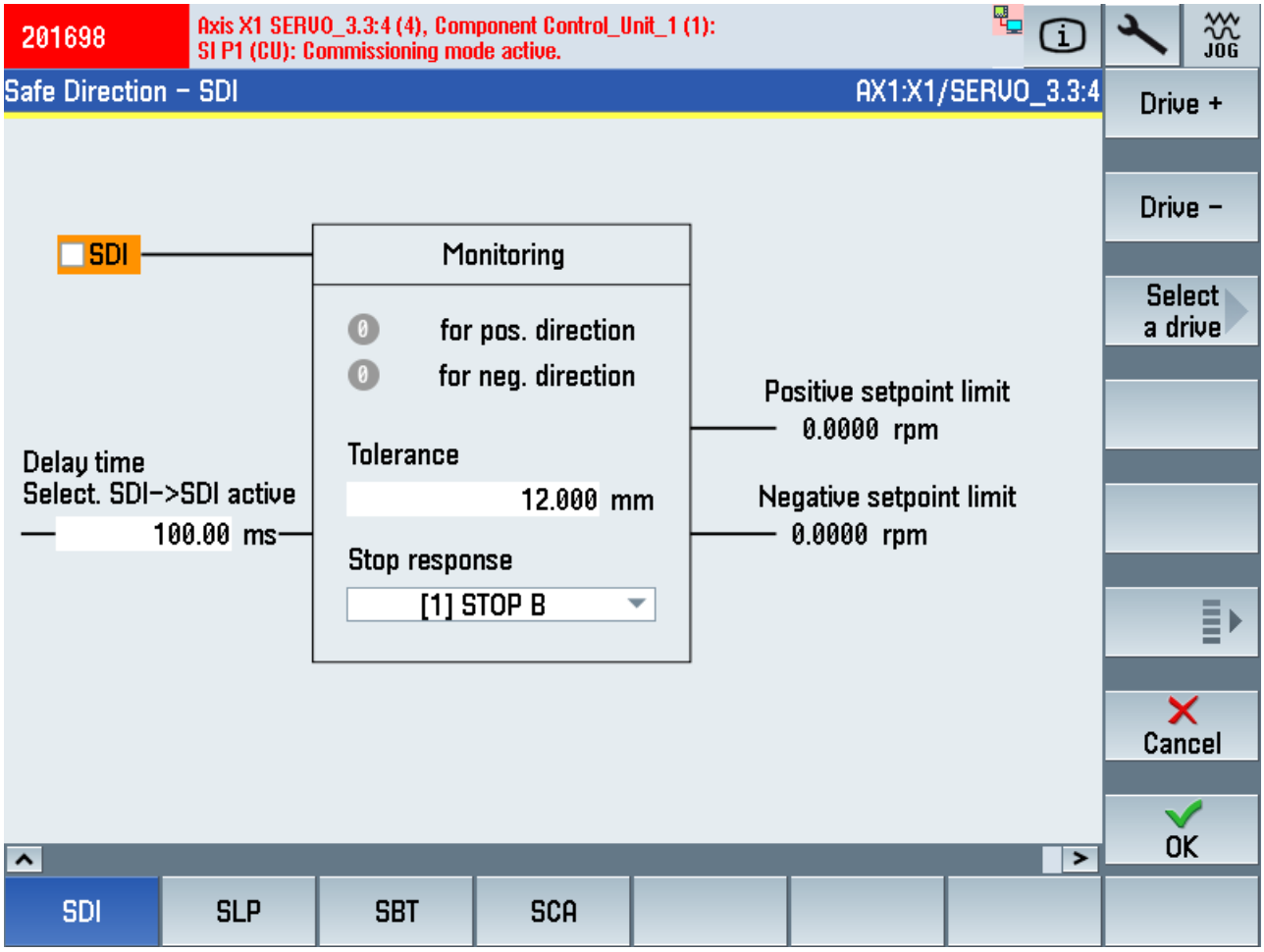
7.6.12 SDI

Precondition

- The SI commissioning mode (Page 236) 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



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.
Feedback signal SDI active for pulse inhibit p9509.8 (only in encoderless operation)	Activates/deactivates SDI during pulse cancellation in encoderless operation.

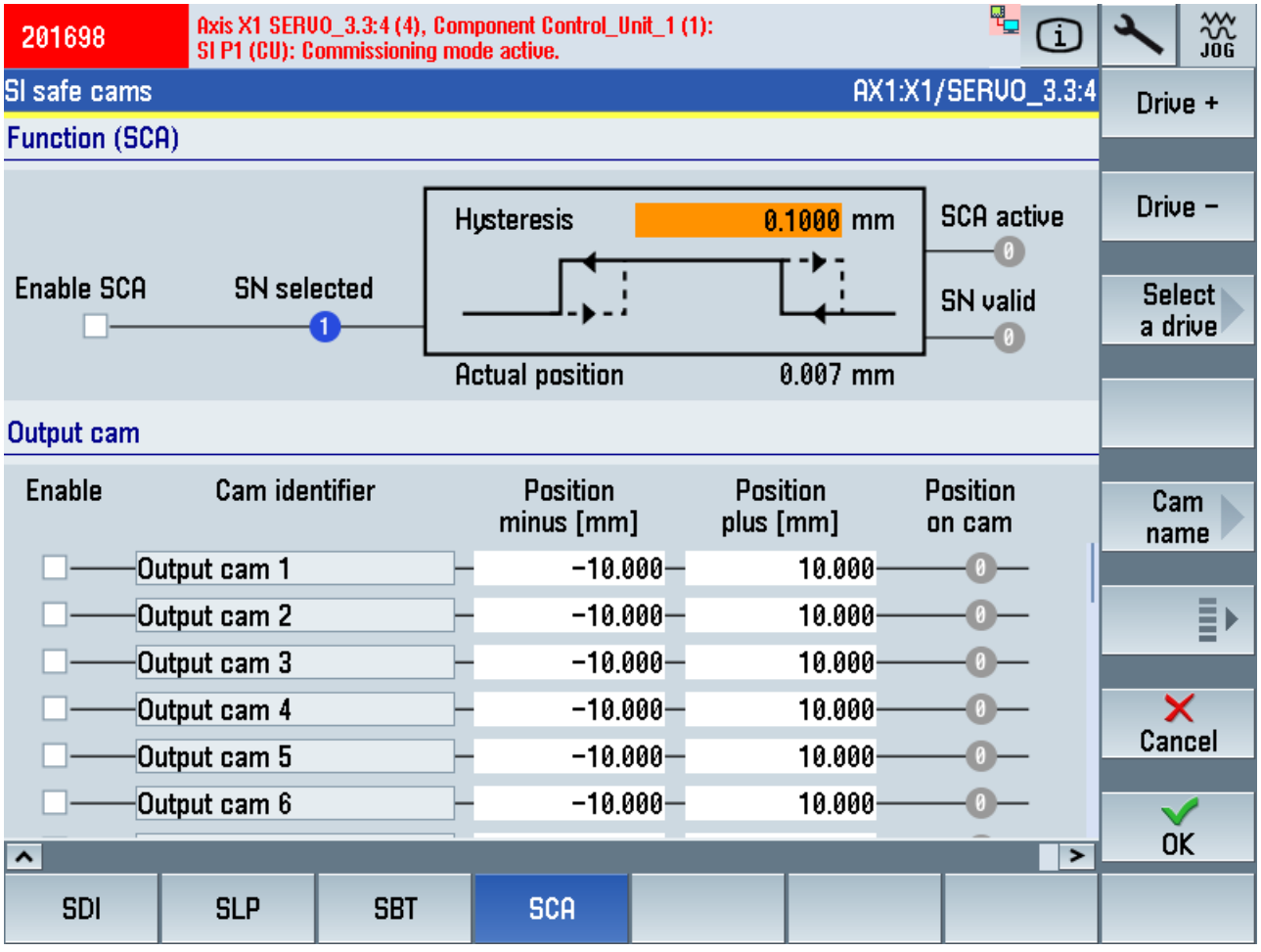
7.6.13 SCA

Precondition

- The SI commissioning mode (Page 236) 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



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.
SCA function	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.

Setting	Meaning
<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 cams 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.

7.6.14 SLP/SP

Precondition

- The SI commissioning mode (Page 236) 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

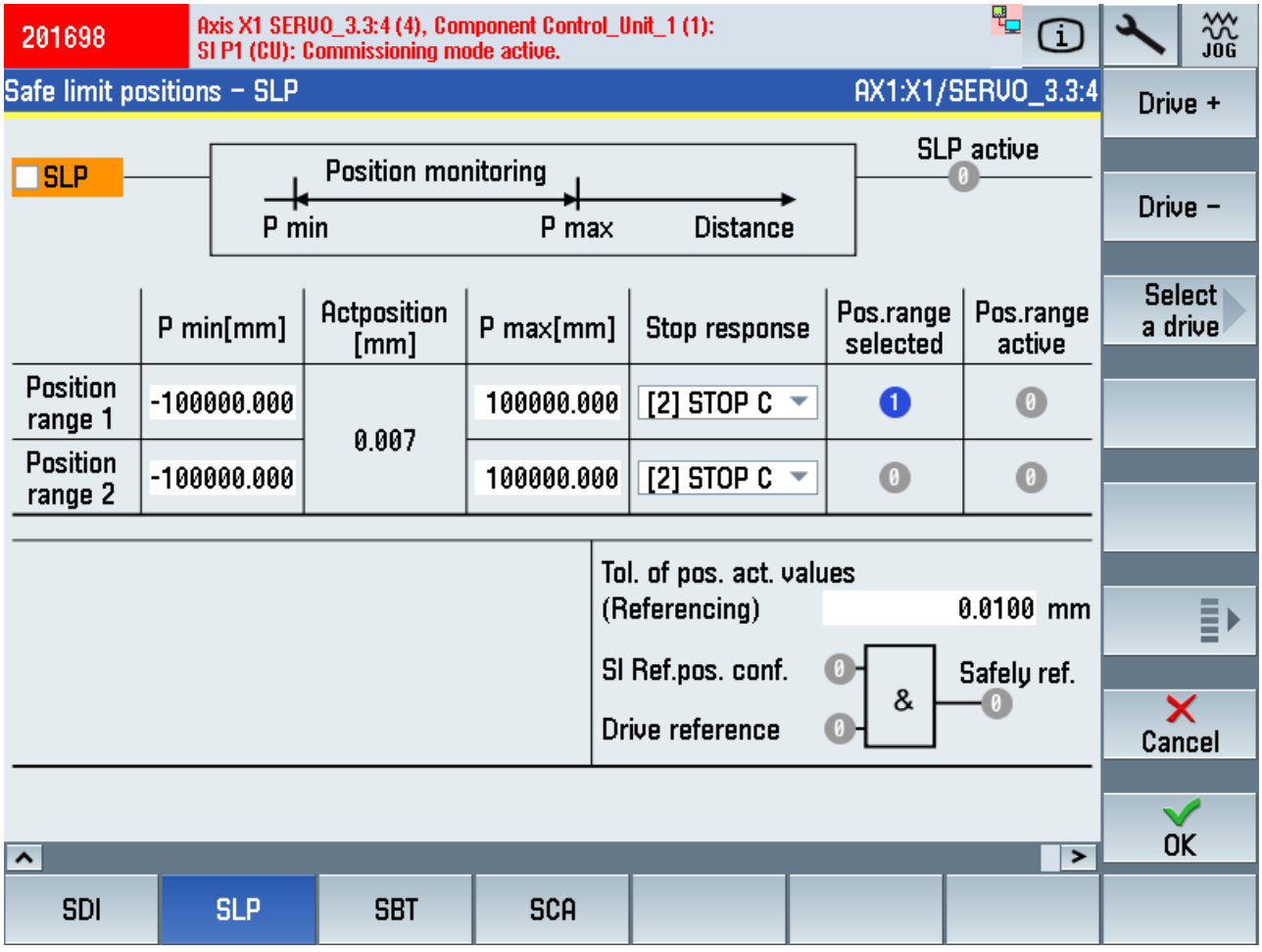


Figure 7-13 Example of the "SLP" commissioning screen, that is, with telegram 903 being set

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.

Status	Meaning
Actual position value r9708[4] (only PROFIsafe)	Displays the actual load-side actual value via PROFIsafe.
Safety-relevant 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]	
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

Setting	Meaning
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 358). 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.
Tolerance of the position actual values (referencing) p9544 (only for telegram 902)	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.

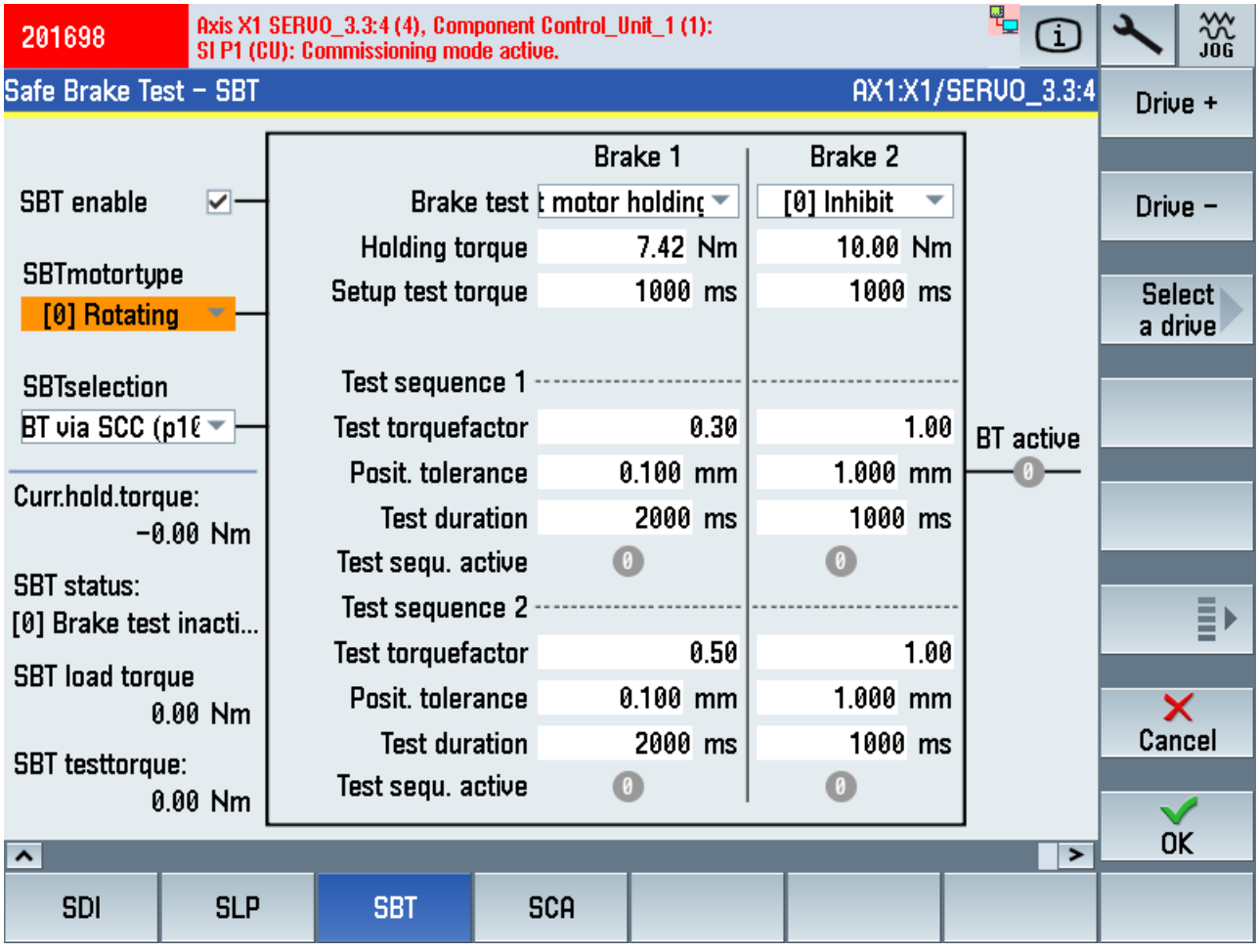
7.6.15 SBT

Precondition

- The SI commissioning mode (Page 236) 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



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.

7.6.16 Safe referencing

Precondition

- The Safety Integrated commissioning mode is active for the drive to be configured.
- Access rights of access level 2 (service) are available in SINUMERIK Commissioning.
- 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

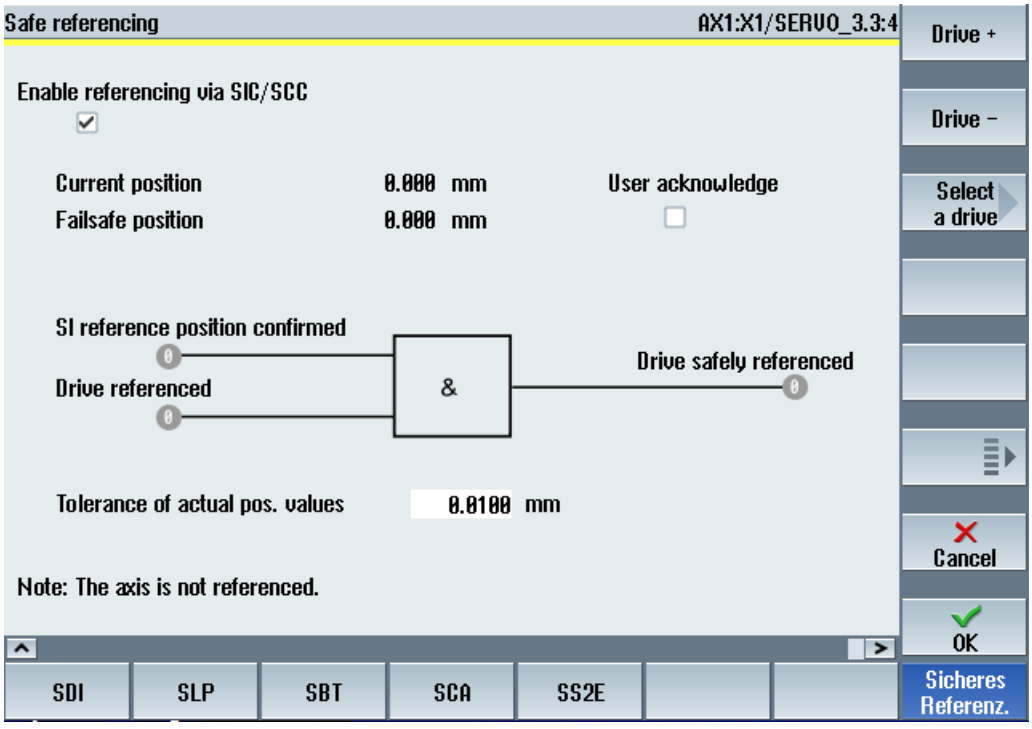


Figure 7-14 Safe referencing

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.

See also

Activating the safety commissioning mode (Page 236)

7.6.17 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 103)
- Homing via SIC/SCC (Page 175)
- Cancellation of the stop transition times
- Automatic SLS (Page 113)/SOS (Page 110) deselection when STO active

7.7 Finalizing commissioning

7.7.1 Confirming settings

After parameterization, the Safety Integrated commissioning mode must be deactivated and the actual checksums must be transferred into the reference checksums.

Precondition

- The NC and drive-specific settings have been correctly configured for all safety-relevant drives and for all F-I/O devices.
- The safety functions integrated in the drive are configured.
- The safety commissioning mode is activated (Page 236).

Procedure

Proceed as follows to confirm the NC and 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".

7.7.2 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

The SINAMICS safety password must be used for SINUMERIK Safety Integrated

The assigning of the Safety Integrated password using the SINUMERIK operate screen is supported as of V4.8 SP2 HF1.

Alternatively, assign the password as follows via the expert list as in SINAMICS Safety Integrated:

- 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. Press softkey "SI password".
3. Select the check box for the all "axes/drives".
4. Assign a password and confirm by clicking on "OK".

7.8 Series commissioning

7.8.1 General information about series commissioning

A project that has been loaded and commissioned, can be loaded to another NCU, keeping the safety parameterization. However, observe the following information:

- Different component checksums as a result of series commissioning with Safety Integrated functionality (Page 335)
- Safety message for series commissioning with third-party motor (Page 289)

For series commissioning, for each NCU, you must carry out an acceptance test (Page 327).

7.8.2 Series commissioning with third-party motor

If you are using third-party motors with absolute encoders, then a safety message can block commissioning.

Possible cause:

A different serial number of the absolute encoder is saved on the memory card other that in the Control Unit that is to be commissioned.

Remedy:

Correct the serial number of the absolute encoder (e.g. with SINUMERIK Operate) before you acknowledge the safety messages. Then continue with commissioning.

Diagnostics 8

If you are looking for a description of the diagnostic functionality, then in this Chapter you can find a Diagnostics guide (Page 292) and descriptions relating to the safety diagnostic functionality (Page 296) with SINUMERIK Operate.

These diagnostic functions are possible in the following software depending on the particular component:

Table 8-1 Diagnostic functionality depending on the components

Component	SINUMERIK Operate	TIA Portal
F-PLC	Operating area "Diagnostics"	See the help for SIMATIC Safety
F-I/O	Operating area "Diagnostics"	See the help for SIMATIC Safety
Safety program (F-program)	-	See the help for SIMATIC Safety
Checksums	Master checksums and SINAMICS checksums in operating area "Diagnostics"	Signatures of F-I/O, the safety program and checksums of the F-PLC. 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:

- General information about displaying and evaluating diagnostic information (Page 309)
- Checksums (Page 310)
- Stop responses (Page 313)
- Using the fault buffer and safety message buffer (Page 320)
- Acknowledgment (Page 323)

Information about replacing components (software or hardware components) is provided in a separate chapter (Page 329).

8.1 Diagnostics guide

Table 8-2 Steps for evaluating diagnostic capabilities

Step	Procedure	Reference
1	**Evaluate LEDs on the hardware (F-CPU, F-I/O):** • BUSF LED on the F-CPU: Flashes when a communication error occurs on PROFIBUS DP/PROFINET IO; On if a programming error occurs when OB85 and OB121 are programmed (e.g. instance DB is not loaded) • STOP LED on the F-CPU: illuminates when the F-CPU is in STOP mode • Fault LEDs on the F-I/O: e.g. SF-LED (group error LED) on if any fault occurs in the individual F-I/O	*Manuals for F-CPU and F-I/O*
2	**Evaluate diagnostic buffer of the modules:** You read the diagnostic buffer of a module (F-CPU, F-I/O, CP) in its online and diagnostic view in the "Diagnostic buffer" group under the "Online & Diagnostics folder.	*Help on STEP 7 and manuals for the F-CPU and F-I/O*
3	**Evaluate stacks of the F-CPU:** when the F-CPU is in STOP mode, read the following successively: • Block stack: Check whether STOP mode of the F-CPU was triggered by an F-block of the safety program • Interruption stack • Local data stack	*Help on STEP 7*
4	**Evaluate diagnostic tag of the F-I/O DB using testing and commissioning functions, by means of an operator control and monitoring system, or in the standard user program:** Evaluate the DIAG tag in the F-I/O DB	F-I/O access (Page 66) or help relating to SIMATIC Safety
5	**Evaluate diagnostic outputs of the instance DBs of instructions using testing and commissioning functions, using an operator control and monitoring system, or in the standard user program:** • For MUTING, EV1oo2DI, TWO_H_EN, MUT_P, ESTOP1, FDBBACK, SFDOOR, evaluate in the assigned instance: – Output DIAG • Evaluate the following for SENDDP or RCVDP in the assigned instance DB: – Output RET_DPRD/RET_DPWR – Output DIAG • Evaluate the following for SENDS7 or RCVS7 in the assigned instance DB: – Output STAT_RCV – Output STAT_SND – Output DIAG	Operations (Page 54) or help relating to SIMATIC Safety

Tip on RET_DPRD/RET_DPWR

The diagnostic information of the RET_DPRD/RET_DPWR parameters correspond to the diagnostic information of the RETVAL parameter of the "DPRD_DAT" and "DPWR_DAT" instructions. You can find the description in the help on *STEP 7* for the "DPRD_DAT" and "DPWR_DAT" instructions.

Tip: STAT_RCV and STAT_SND

The diagnostic information of the parameter STAT_RCV corresponds to the diagnostic information of the parameter STATUS of the instruction "URCV". The diagnostic information of the parameter STAT_SND corresponds to the diagnostic information of the parameter STATUS of the instruction "USEND". You can find the description in the help on *STEP 7* for the instruction "UCRV" or "USEND" .

8.2 System alarms and diagnostic screens for F-PLC and F-I/O.

The diagnosis of faults of F-I/O or F-PLC is supported in SINUMERIK Operate via specific system alarms (number ranges 4300XX and 43100X) as well as own diagnostics screens (Page 296).

To use this functionality, the configuration must be properly completed and loaded:

- The configured NCU must have firmware version ≥V4.8 and Safety Integrated plus (F-PLC) must be activated.
- Hardware and software must be consistently compiled and loaded.

With such a correct configuration, SI_DiagDB [DB1009] is automatically generated during the compilation and transferred to the NCU during loading.

Details on internal processing of the F-PLC / F-I/O system alarms

The system alarms for the diagnostics of the F-PLC and F-I/O are formed based on the status information of the safety program and collected and processed by the basic PLC program. Information required for processing is stored in the SI_DiagDB [DB1009] (for example, design of the safety program and assignment of the F-I/O DBs and F-global DBs). SI_DiagDB [DB1009] is automatically generated during compilation and transferred to the NCU during loading, if Safety Integrated plus (F-PLC) is activated and the NCU device version is correctly configured (≥V4.8). The association between the SI_DiagDB [DB1009] and the safety program is secured by a checksum (see also Alarm 430000).

Depending on this status information, the corresponding system alarms are triggered and displayed in SINUMERIK Operate.

Meaning of the "F-PLC/F-I/O system alarms

Note

No simultaneous display of different system alarms with the same alarm number.

If the same error occurs for multiple modules, the respective system alarms are not displayed at the same time but instead successively. This means that the alarm for the next module is only displayed if the error has been corrected and/or the first module has been reintegrated.

Table 8-3 General

Meaning	Alarm No.
F-diagnostics: PLC project is inconsistent The F-diagnostics is not possible because the PLC project is inconsistent (safety program and SI_DiagDB [DB1009] do not match) or the configured firmware version is not supported. The configured NCU firmware version (TIA Portal) must be at least V4.8. Compile and re-load hardware and software consistently.	430000

Table 8-4 F-PLC system alarms

Meaning	Alarm No.
Safety mode disabled The safety mode of the F-PLC has been disabled by the user, fault control measures are partly deactivated. Safety mode is reactivated at the next startup of the PLC.	431001
Error detected by fail-safe system A serious problem was detected in safety mode (group signal); STEP 7 is required for exact analysis. Carrying out diagnostics on the diagnostics buffer of the CPU using STEP 7.	431003

Table 8-5 F-I/O system alarms

Meaning	Alarm No.
F-module %1: Timeout detected by F-I/O The F-I/O has detected a timeout in the PROFIsafe communication. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430001
F-module %1: Channel fault detected by F-I/O The F-I/O has detected a channel fault. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430002
F-module %1: CRC error / sequence number error detected by F-I/O The F-I/O has detected a CRC error / sequence number error. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430003
F-module %1: Timeout detected by F-system The F-system has detected a timeout. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430005
F-module %1: Sequence number error detected by F-system The F-system has detected a sequence number error. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430006
F-module %1: CRC error detected by F-system The F-system has detected a CRC error. Correct the displayed cause of the error and, if necessary, reintegrate the module.	430007
F-module %1: Reintegration necessary The F-module is passivated and has to be reintegrated for further use. Reintegrate the F-module using the ACK_REI signal.	430010

8.3 Diagnostic functions in SINUMERIK Operate

You can find the SI-diagnostics overview and more specific diagnostic screens under "MENU SELECT > Diagnostics > Menu forward key > Safety".

Note

A properly completed and loaded configuration is a requirement for diagnostics functionality.

- The configured NCU must have firmware version ≥V4.8 and Safety Integrated plus (F-PLC) must be activated.
- Hardware and software must be consistently compiled and loaded.

With such a correct configuration, SI_DiagDB [DB1009] is automatically generated during the compilation and transferred to the NCU during loading.

8.3.1 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 referencing (homing).

Call

MENU SELECT > Diagnostics > Menu forward key > Safety

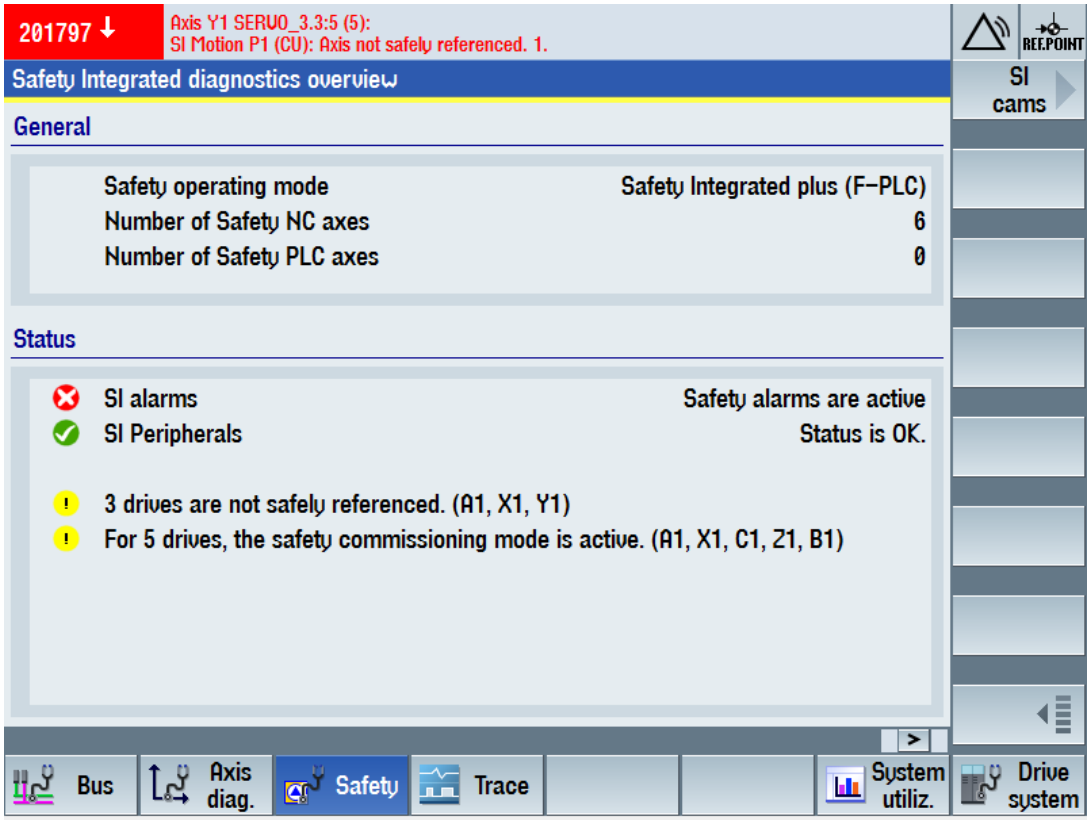


Figure 8-1 Safety Integrated diagnostics overview

This screen is simultaneously used as entry to the following diagnostic screens:

- SI drives (Page 297)
- SI telegrams (Page 300)
- SI checksum (Page 302)
- SI alarms (Page 304)
- SI Safe Cams (Page 305) (via menu forward key)
- SI integrated F-PLC (Page 306)
- SI I/O (Page 307)

8.3.2 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

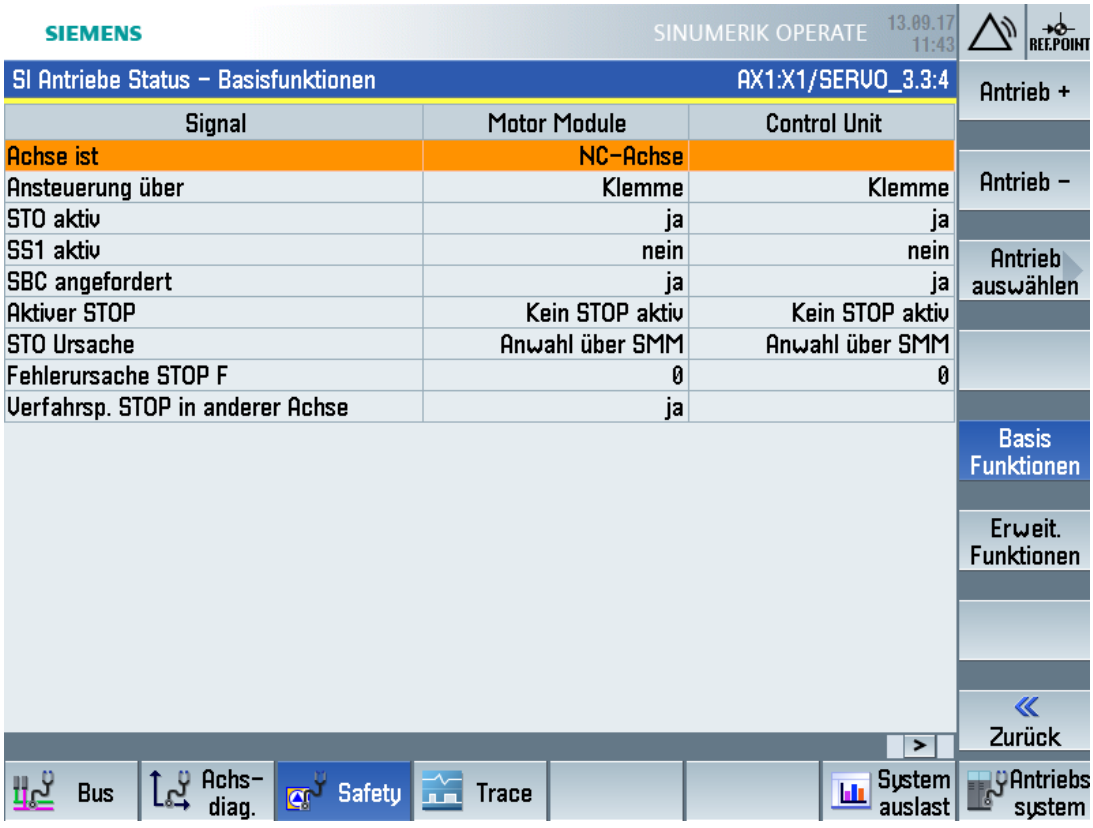


Figure 8-2 Diagnostic screen "SI drive status - Basic functions" (sample screenshot)

Call "SI drive status - Extended functions"

MENU SELECT > Diagnostics > Menu forward key > Safety > SI drives > Extended Functions

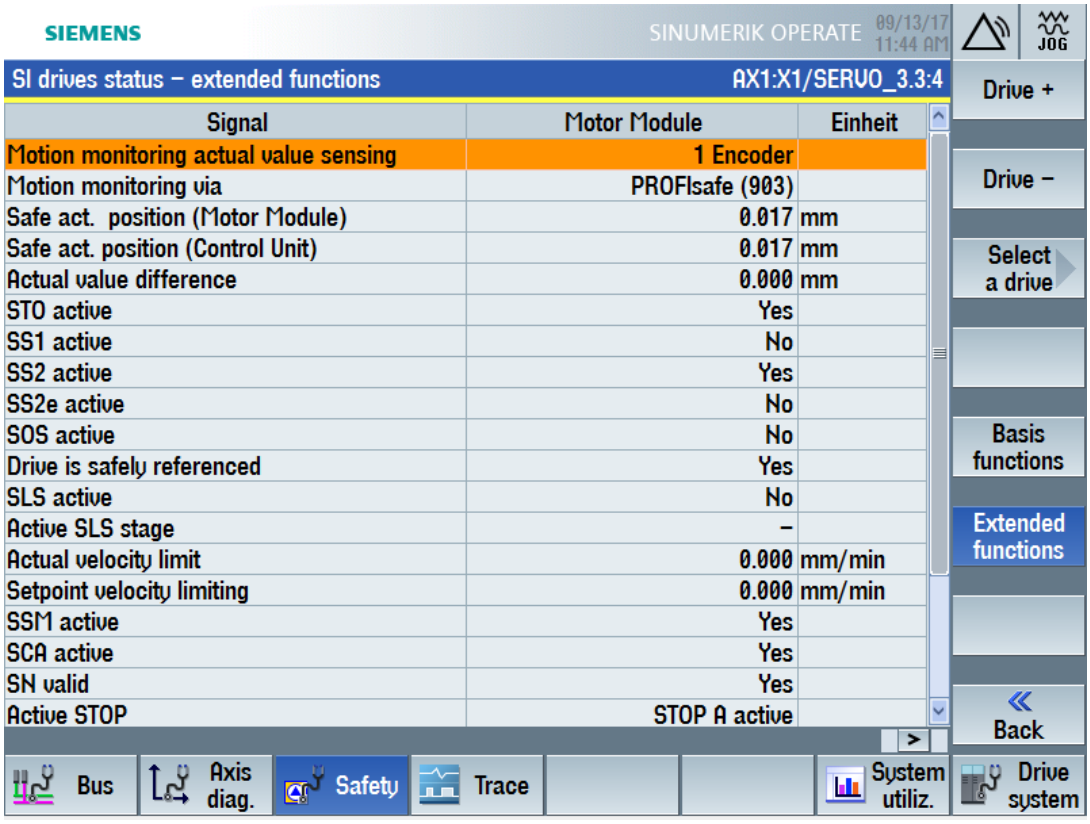


Figure 8-3 "SI drive status - Extended functions" diagnostic screen (sample screenshot)

8.3.3 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

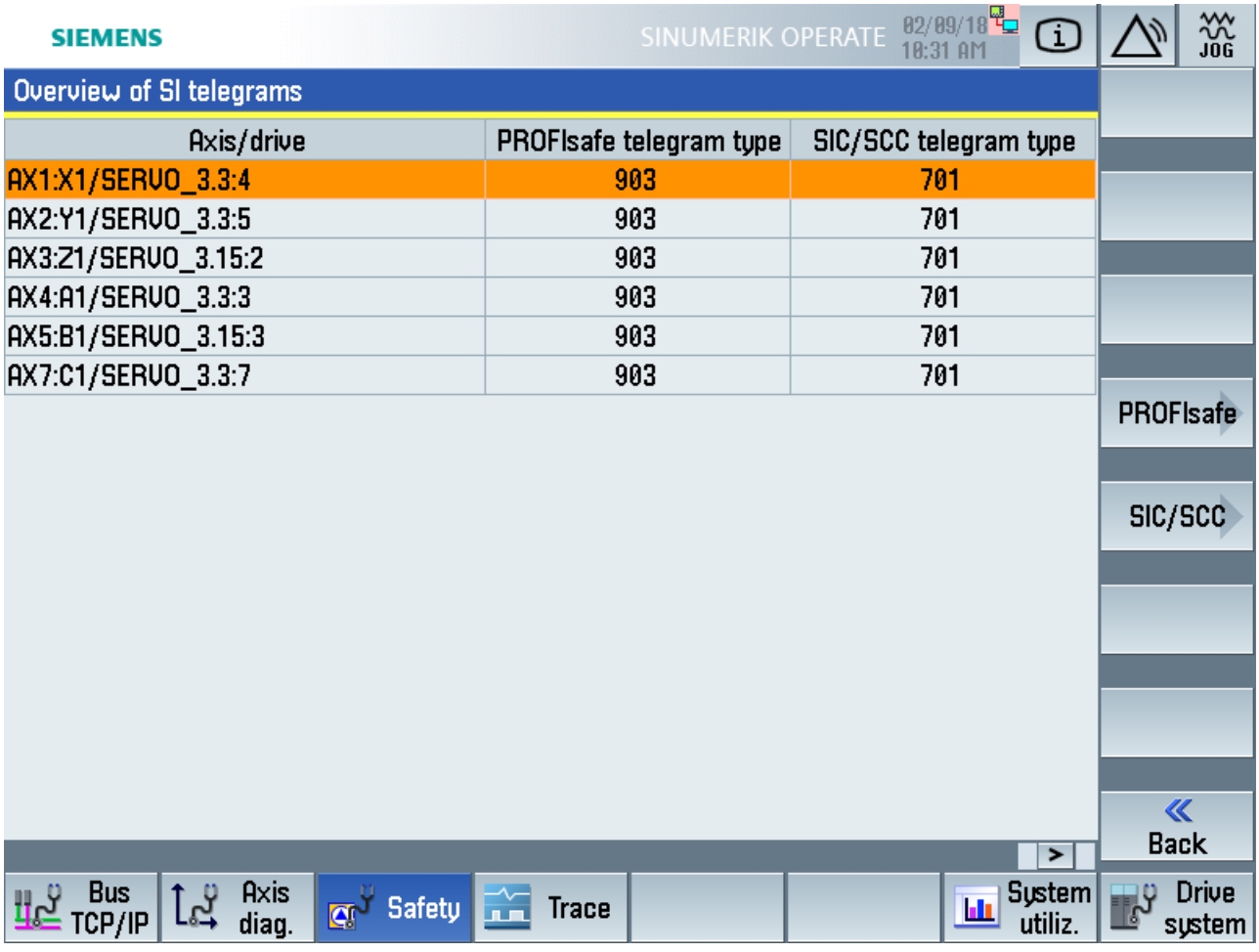


Figure 8-4 "SI telegrams overview" diagnostic screen

This screen is simultaneously used as entry to the following diagnostic screens:

- SI telegrams PROFIsafe (Page 300)
- PROFIdrive SI telegrams (Page 301)

Additional information

- You will find general information on safety-relevant telegrams in Chapter Controlling safety functions integrated in the drive (Page 193).

8.3.4 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

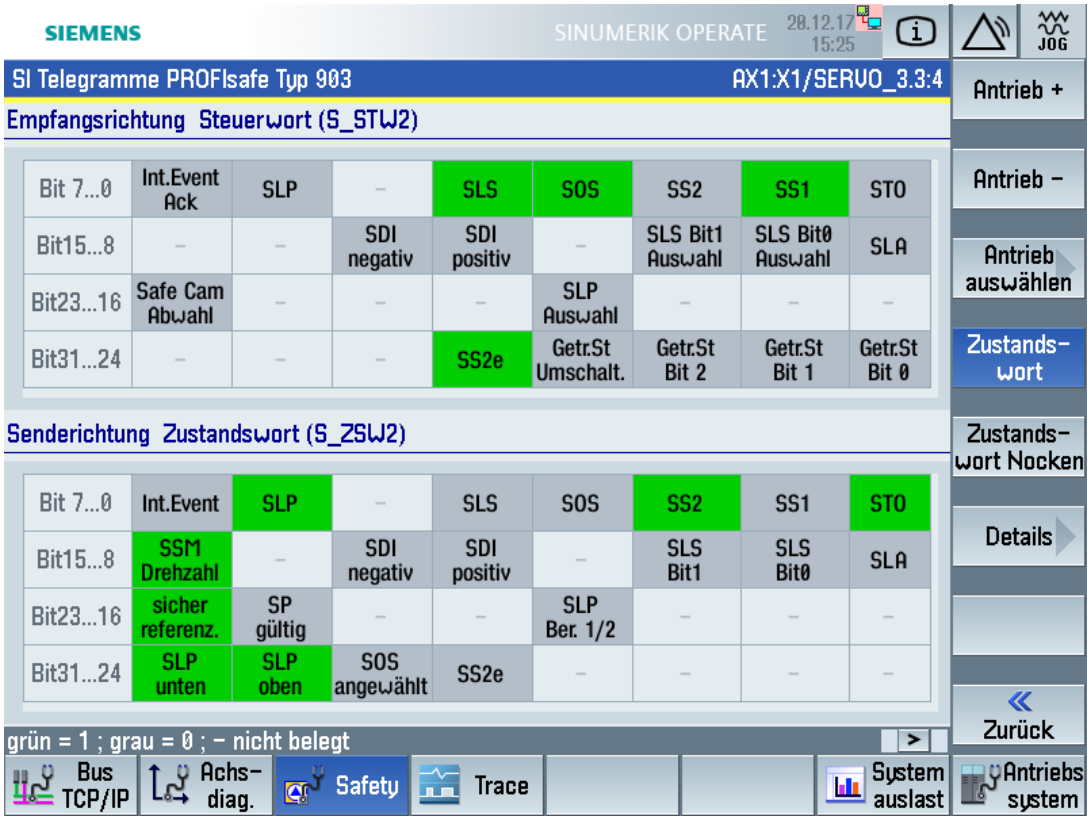


Figure 8-5 "PROFIsafe SI telegrams" diagnostic screen

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 197).

8.3.5 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

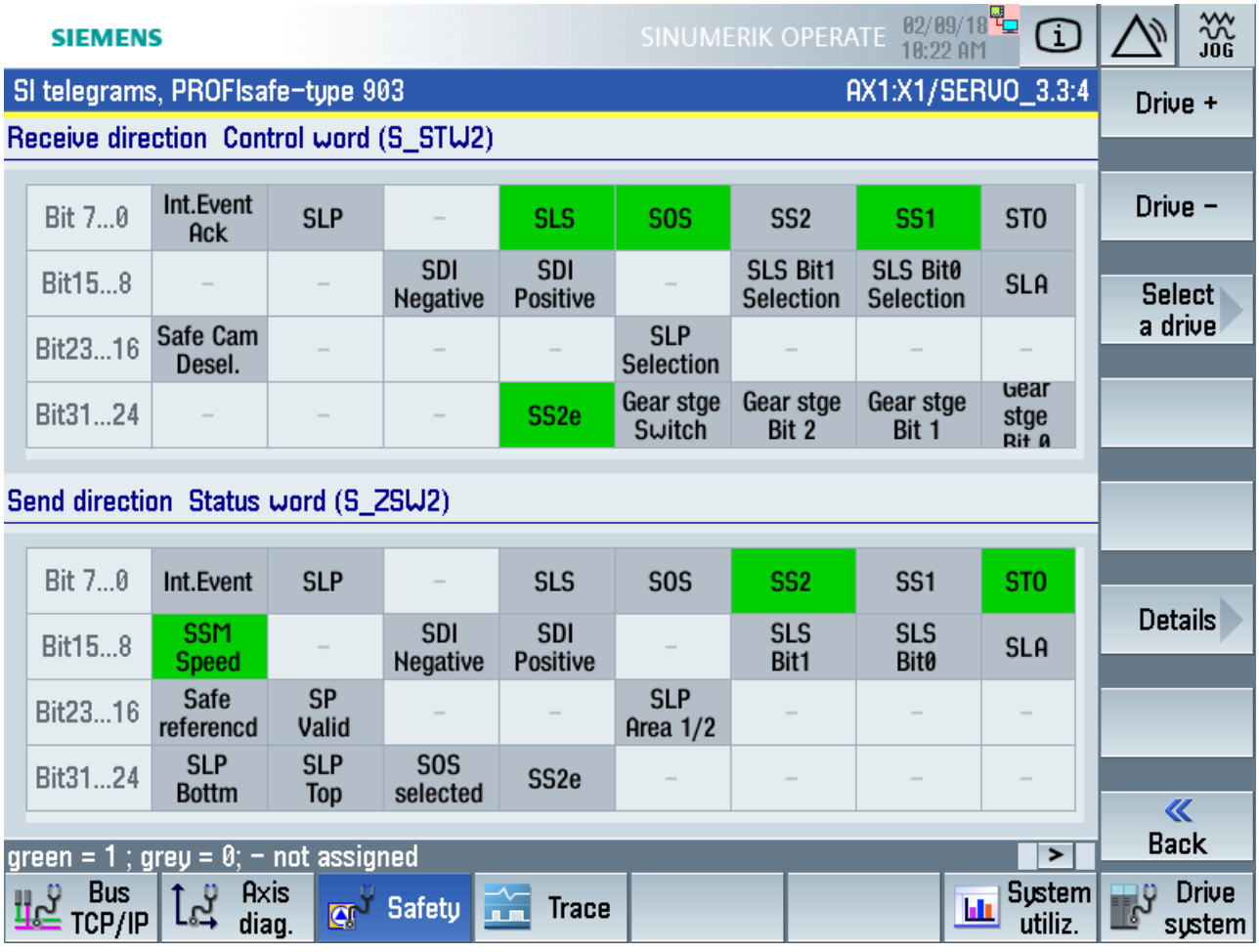


Figure 8-6 "SI telegrams PROFIdrive" diagnostic screen

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 SIC/SCC telegrams in Chapter Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 201).

8.3.6 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 checksum

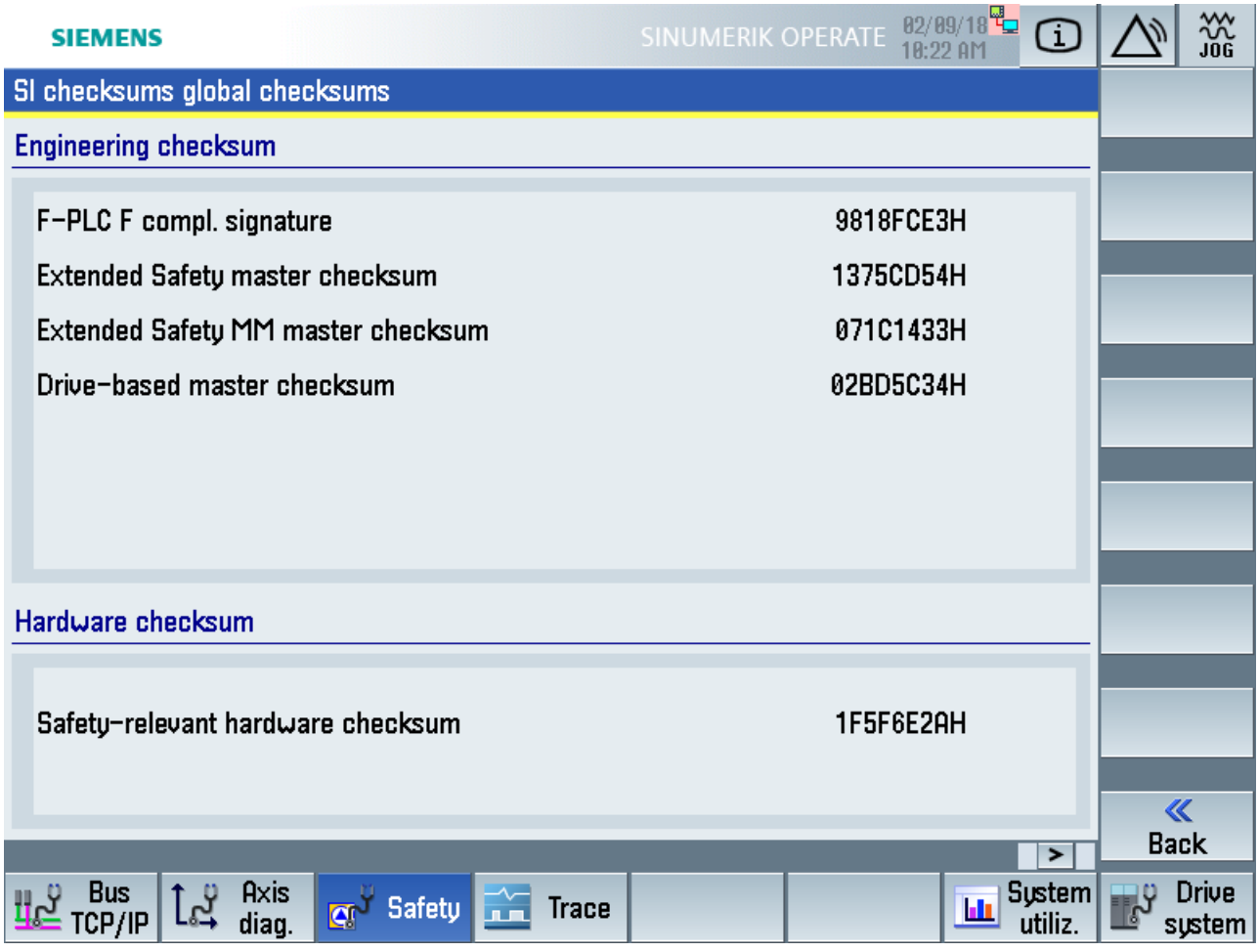


Figure 8-7 "SI checksums overview" diagnostics screen

Higher-level actual checksums that are calculated from the master checksums (Page 310) 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

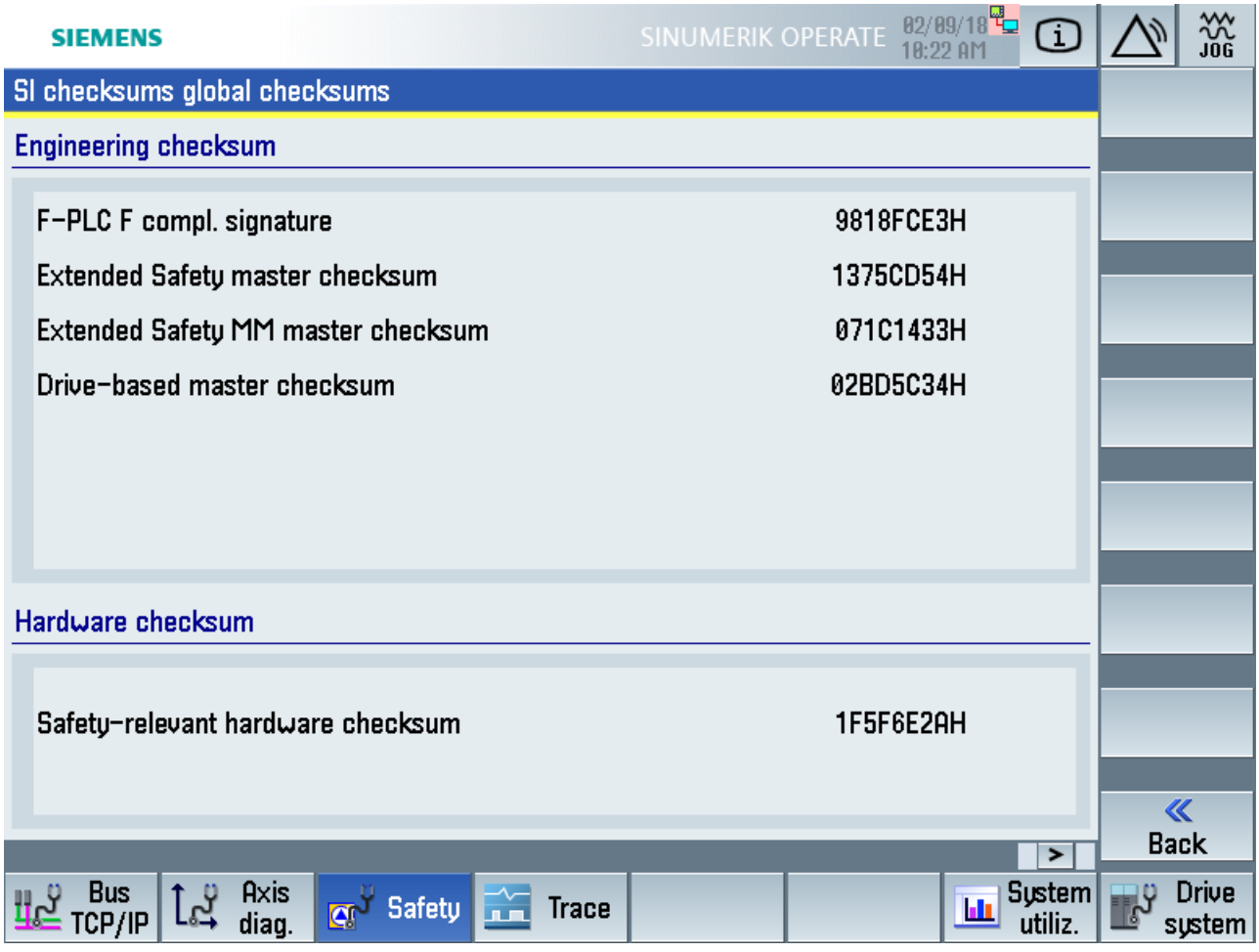


Figure 8-8 "SI checksums global checksums" diagnostic screen

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.

8.3.7 SI alarms

Active safety-relevant alarms are displayed in diagnostics screen "SI-alarms".

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI alarms

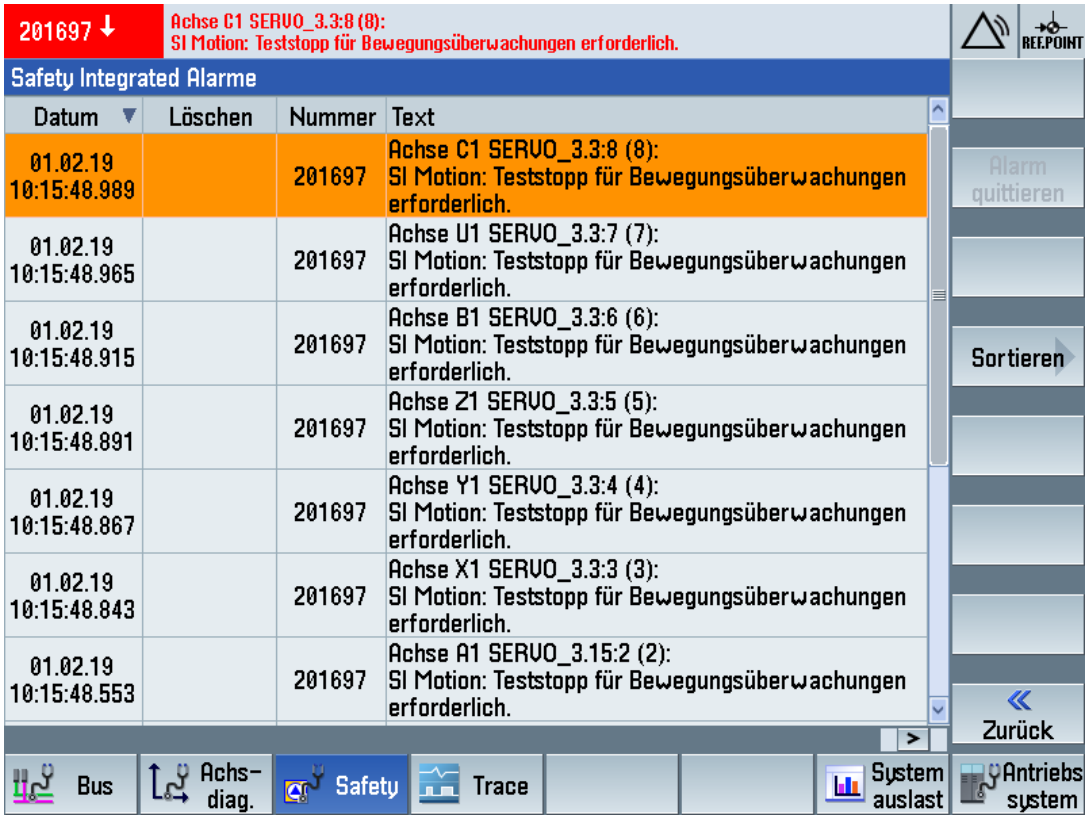


Figure 8-9 "Safety Integrated alarms" diagnostic screen

8.3.8 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

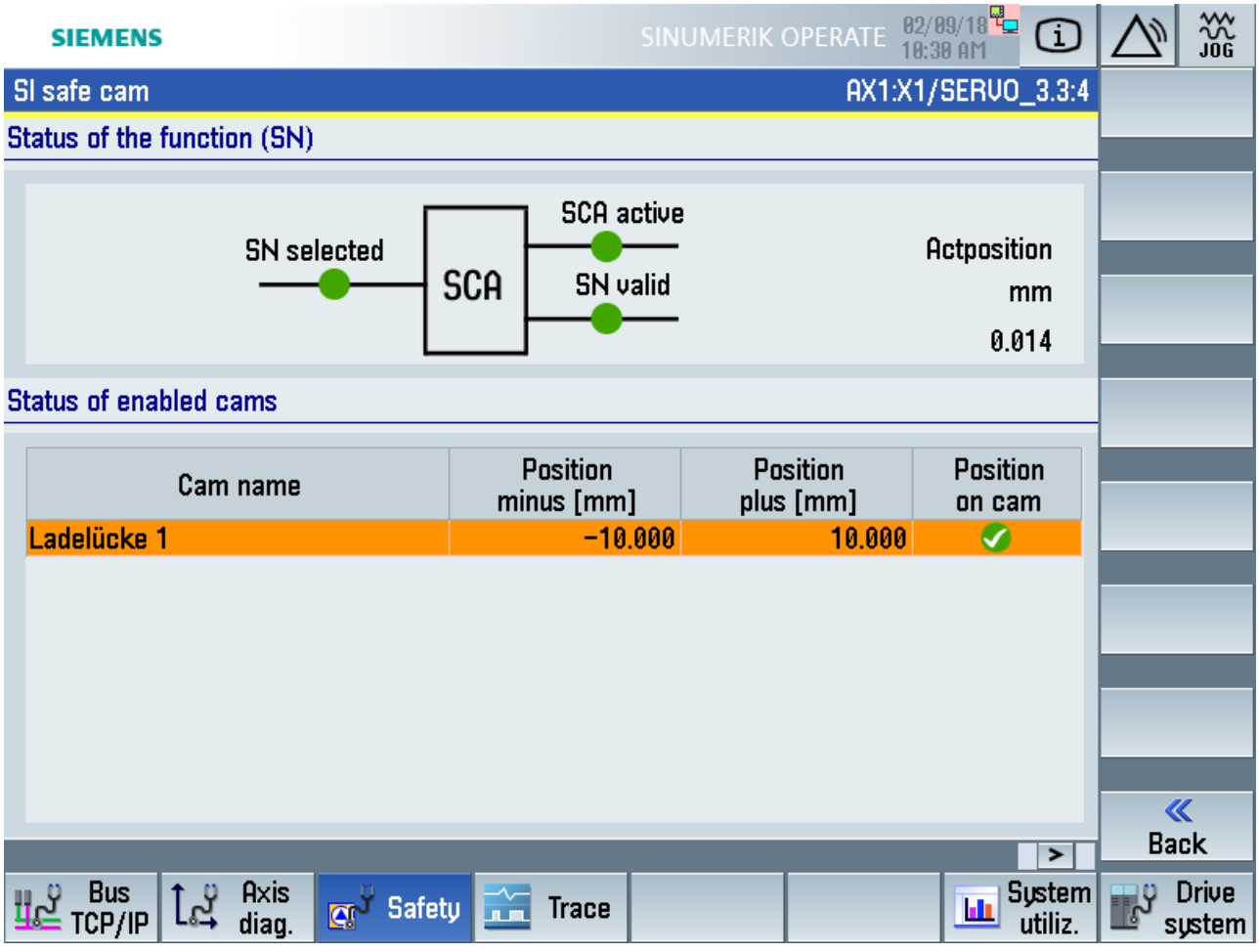


Figure 8-10 "SI safe cams" diagnostics screen

8.3.9 SI integrated F-PLC

The configured safety-related status and diagnostic information of the integrated F-PLC of the SINUMERIK NCU is displayed in the "SI Integrated F-PLC" diagnostic screen.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI Integrated F-PLC

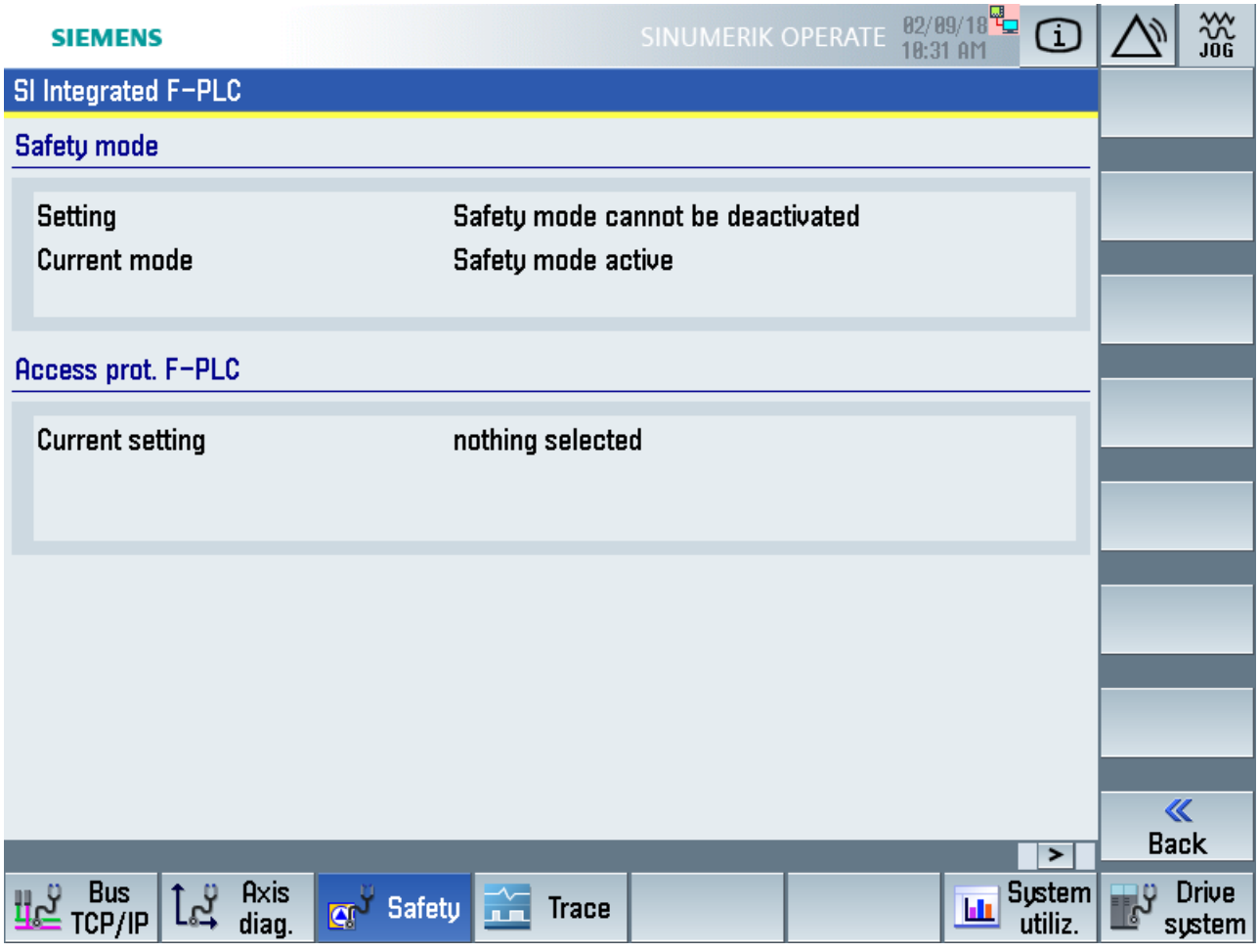


Figure 8-11 "SI Integrated F-PLC" diagnostic screen (screenshot as example)

8.3.10 SI I/O

The configured F-I/O is displayed in the "SI I/O overview F-modules " diagnostic screen.

Call

MENU SELECT > Diagnostics > Menu forward key > Safety > SI I/O

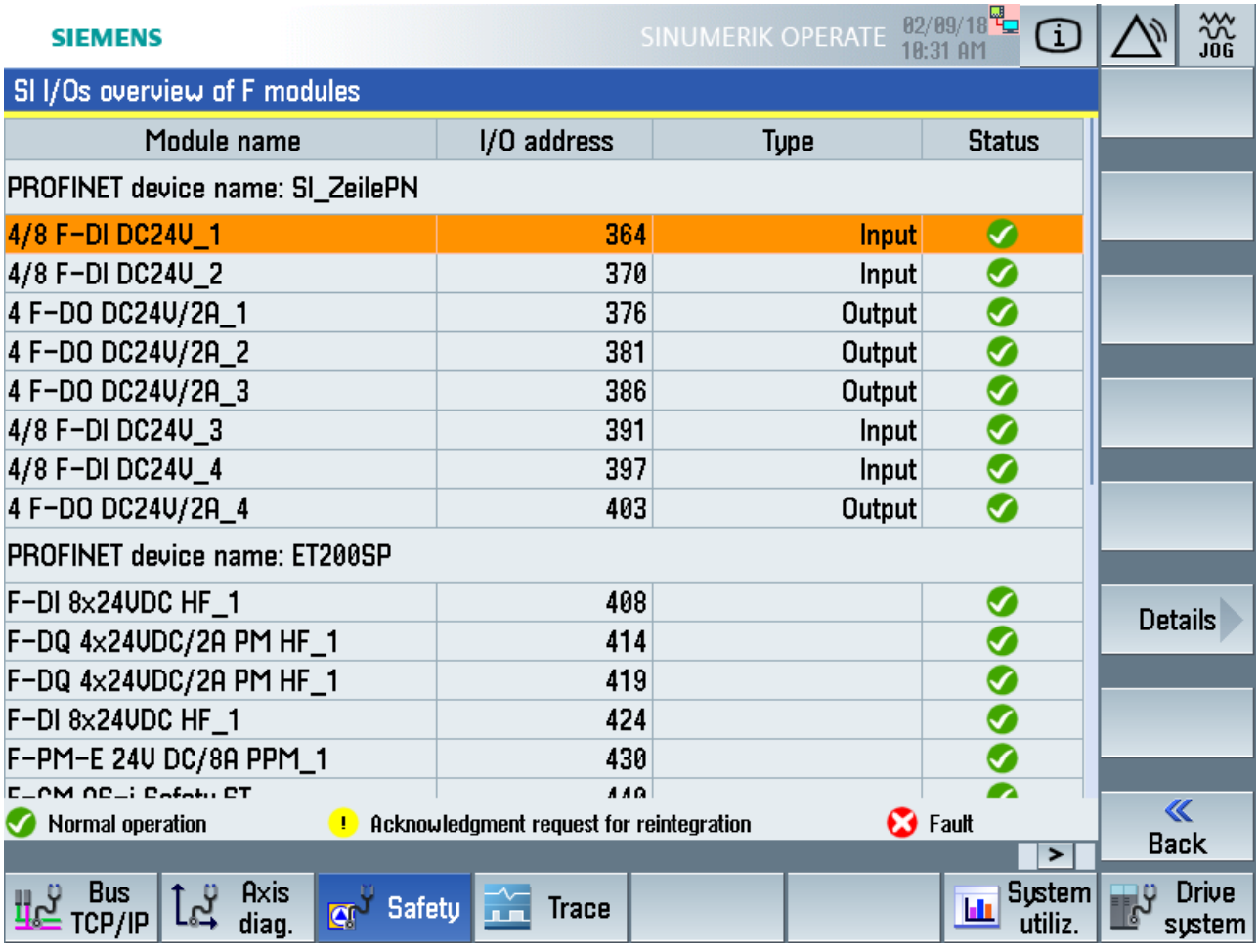


Figure 8-12 "SI I/O overview F-modules" diagnostics screen (sample screenshot).

With the "Details" softkey, you can display additional information about the selected module.

8.4 General information about displaying and evaluating diagnostic information

In operating mode Safety Integrated plus, safety-relevant monitoring functions are executed in the drive itself. Diagnostic information is communicated and evaluated as follows:

- The status and control information (SIC/SCC) (Page 201) of the drive is communicated between the integrated subcomponents of the NCU:
  - As a consequence, the motion control in the NC is also linked (Page 317) 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 339).
- SINAMICS Safety Integrated messages and alarms can be displayed as follows:
  - Safety messages of the drive are displayed in SINUMERIK Operate in the alarm lists.

    Note

    Information for those switching over from a different system: Evaluating alarms using the NC

    As Safety Integrated plus uses the safety functions integrated in the drive, the NC does not suppress alarms, prioritize alarms or check alarm numbers of safety messages of the drive (contrary to the Safety Integrated operating mode).

  - The standard alarm of a drive can also include safety-relevant diagnostic information. In order that these are displayed in SINUMERIK Operate, you must activate the alarm buffer (Page 321).
  - Display and acknowledgment (Page 323) of messages depend on the scope of the Safety Integrated Functions (Page 23) used - and the use of the safety message buffer (Page 320).

8.5 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 302).

- The individual F-blocks have signatures, and the safety program has an overall F-signature. These checksums for the safety program are displayed in the TIA Portal as well as in the safety printout.
- The F-PLC has a hardware checksum.
- There are SINAMICS parameters with reference checksums (defined when commissioning) - and actual checksums for CU, MM and motion monitoring functions, which are checked by SINAMICS Safety Integrated when the system runs up. SINAMICS alarms 201650/230650 and/or 201680/230680 are output if the checksums differ.
  See: SINAMICS checksums (Page 312)
- 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 310)
  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 302)

8.5.1 Calculating the global checksums/master checksums

In addition to the checksums or signatures of the subcomponents SINAMICS Safety Integrated and F-PLC, in SINUMERIK Operate global checksums and master checksums are displayed, which are calculated from various actual checksums from the F-PLC and SINAMICS Safety 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 8-6 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 Modules) / 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 8-7 Calculating 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 Modules) / SI Mtn act CRC MM

8.5.2 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.

- 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)

- 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.

8.6 Stop responses

8.6.1 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 313)
- Stop responses that can be initiated for faults involving Safety Integrated Extended Functions (Page 315)

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 318).
- For stop responses and Safety Integrated Extended Functions, there are some dependencies regarding the priority (Page 318).

The motion control in the NC is linked (Page 317) to the safety functions integrated in the drive and the associated stop responses, which means that no unnecessary follow-on responses are initiated in the NC.

8.6.2 Basic Functions

When faults associated with Safety Integrated Basic Functions occur, the following stop responses can be initiated:

Table 8-8 Stop responses for Safety Integrated Basic Functions

Stop response	Triggered ...	Action	Effect
STOP A cannot be acknowl-edged	For all Safety faults with pulse suppression that cannot be ac-knowledged.	Trigger safe pulse suppression via the switch-off signal path for the relevant monitoring channel. During operation with SBC: Apply motor holding brake.	The motor coasts to a standstill or is braked by the holding brake.
STOP A	For all acknowledgeable Safety faults As a follow-up reaction of STOP F		
	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.		

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.

8.6.3 Extended Functions

Faults involving Safety Integrated Extended Functions and violation of limits can trigger the following stop responses:

Table 8-9 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 suppression • Subsequent response of STOP B • Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP	Immediate pulse suppression **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	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 Section SS1 (Extended Functions) with external stop (Page 85))	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	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]	• Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP	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]	• Configurable subsequent stop p9563 for SLS • Configurable subsequent stop p9566 for SDI • Configurable subsequent stop p9562 for SLP	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 cross-wise 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.

Note

Delayed pulse cancellation when the bus fails

For SLS and SDI, the stop responses are also available with delayed pulse cancellation when the bus fails (in order that the drive does not immediately respond 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 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 (p9566[0...3] ≥ 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_{F1}: p9658
- t_{F2}: p9555
- $n_{shutdown}$: p9560

8.6.4 Connection and effects in the NC

The motion control in the NC is linked to the safety 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 response 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.

See also

Safety Info Channel and Safety Control Channel (SIC/SCC) (Page 201)

8.6.5 Priorities

Table 8-10 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 8-11 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 parameterizable time. 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 follow-up stop B. SS2 remains active.

Examples for illustrating the information in the table:

1. Safety function SS1 has just been selected. STOP A remains selected.
2. 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.
3. 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.
4. 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.

8.7 Using the fault buffer and safety message buffer

In addition to the standard fault buffer and the standard alarm buffer, SINAMICS Safety Integrated has its own safety message buffer for safety-related messages for 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 323) is required.
    - In SINUMERIK Operate, in the "Safety Integrated diagnostics overview", reference is made to active safety-relevant alarms (in addition to the standard alarm list).
    - A safety delete symbol makes reference to active alarms that require a safety-relevant acknowledgment.
  - To acknowledge messages in the safety message buffer, safety-relevant acknowledgment is required - and possibly also acknowledgment with PROFIdrive RESET (Page 324).
- 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 321).
  - 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.
    In SINUMERIK Operate, safety-relevant alarms are displayed in the standardalarm 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 an acknowledgment via PROFIdrive (Page 325).

8.8 Configuring the message buffer and alarm buffer

8.8.1 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.

8.8.2 Configuring the safety alarm buffer

The safety message buffer is activated in the factory setting, and is used for issuing safety-relevant messages from Extended Functions.

In certain situations it can make sense to also deactivate the safety message buffer for Extended Functions. This means that messages associated with Basic Functions and Extended Functions can be saved in the fault and/or alarm buffer (e.g. if you are predominantly using Basic Functions).

The setting to activate/deactivate the safety message buffer is a CU parameter (p3117). This cannot be set for specific drives or axes - it is always applicable for all drives 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)".

8.9 Acknowledgment

8.9.1 Overview

Most safety messages require safety-relevant acknowledgment.

Safety-relevant acknowledgment involves deleting safety-relevant messages of the drive-integrated monitoring functions via safety-relevant communication. With the safety-related acknowledgment, the fault case in the drive is marked as having been resolved (gone).

Safety-relevant 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-relevant acknowledgment are possible:

Table 8-12 Permissible acknowledgment types for various drive types

Drive type	Permissible acknowledgment
Integrated drives (CU_I, CU_NX)	• Safety-relevant acknowledgment using PROFIsafe signal "IEACK" (Page 324) • Acknowledgment by switching-off/switching-on (Page 325)
External NC drives	• Safety-relevant acknowledgment using PROFIsafe signal "IEACK" (Page 324) • Acknowledgment by deselecting STO or SS1 (Page 325) • Acknowledgment by switching-off/switching-on (Page 325)
External SINAMICS drives without any assignment to an NC axis	The safety message buffer is not supported and must be deactivated (Page 321). 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 325) all safety messages that are saved in the standard fault buffer using a PROFIdrive RESET.
- In addition to a safety-relevant acknowledgment, various fault situations also require an acknowledgment using a PROFIdrive RESET (Page 324).

⚠ 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).

8.9.2 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.

8.9.3 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 Safety 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

If, in the case of a fault, the safety-relevant acknowledgment is realized without PROFIdrive RESET, then although the part program remains in the stop state, the spindle continues to operate.

A configuration such as this is not in conformance with standard IEC 61800-5-2. According to the standard, a restart inhibit is mandatory for all STOP functions, and it is only permissible that the spindle starts again after a RESET.

1. Therefore, in the safety program logically combine safe acknowledgment (PROFIsafe IEACK) with a RESET at the machine control panel (PROFIdrive RESET).
2. 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.

8.9.4 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.

8.9.5 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.

8.9.6 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 safety messages are saved in the standard fault buffer or in the standard alarm buffer. These messages require a safety-relevant acknowledgment, even when the safety message buffer is deactivated.

The safety messages in the standard fault buffer require, in addition to safety-relevant acknowledgment, also 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 025201.

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 8-13 Saving safety-relevant messages in the the fault buffer (when the safety message buffer is deactivated)

Alarm number	Alarm text
201689	SI Motion: Axis re-configured
201700	SI Motion P1 (CU): STOP A initiated
201701	SI Motion P1 (CU): STOP B initiated
201708	SI Motion P1 (CU): STOP C initiated
201770	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.

Acceptance test with SINUMERIK Operate 9

9.1 Purpose and requirements

An acceptance test has the objective to check that the parameterization and principle of operation of the safety functions are correct, identify potential configuring errors and 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 safety functions that have been accepted can result in faults and undesirable motion - and in turn in death or severe injury.
>
> - 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

This chapter provides recommendations for the content and scope of an 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/109761095)).

Component replacement (software/hardware) 10

10.1 Safety instructions

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.
  You can find more detailed information in the chapters "AUTOHOTSPOT" and "Acceptance test with SINUMERIK Operate (Page 327)".

10.2 Software, F-CPU, F-I/O

Replacement of software components

When replacing software components on your programming device or PC (e.g. with a new version of *STEP 7)*, you must adhere to the information regarding upward and downward compatibility in the documentation and readme files for 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:

If you have selected the "Activate firmware after update" option for the firmware update (see *Help on STEP 7*, "Online & Diagnostics"), the IM will be automatically reset following a successful download operation and will then run on 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

A complete list of the probability of failure values (PFD, PFH values) for F-CPUs is provided in the Siemens web page Industry Online Support at the following address (https://support.industry.siemens.com/cs/ww/en/view/109481784/80883060875):

There you can find a list for the following probability of failure values:

- PFD, PFH values for F-CPUs S7-300/400 - and the proof test intervals for components that can be used in SIMATIC Safety
- PFD, PFH values for F-CPUs S7-1200/1500 for a usage time of 20 years and for a repair time of 100 hours. Excerpt:

Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode 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-relevant communication. Excerpt:

Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h^{-1}]
< 1E-05	< 1E-09*

*** Note on S7-300/400 F-CPUs:** The value is valid under the assumption that a maximum of 100 F-I/Os are involved in a safety function. If more than 100 F-I/Os are used, you need to add 4E-12 for each F-I/O for this safety function.

10.3 Motors, CU (SINAMICS Safety Integrated)

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 replacements, see "Example of component replacements" 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 by setting p0977 = 1.
  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.

See also

Acceptance test with SINUMERIK Operate (Page 327)

10.4 Parameters and function diagrams - notes regarding replacing components

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

- r9670 SI module identifier Control Unit
- r9671[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 SI diagnostics
- r9793[0...9] SI diagnostics component replacement

10.5 Messages when components are replaced after Safety Integrated has been commissioned

Safety-relevant 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.

Basic procedure

⚠ 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 hazardous area - and before resuming operation - perform a simplified function test for the drive affected by the component replacement (see Chapter "Acceptance test (Page 327)").

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

Data descriptions 11

11.1 Machine data

Overview

Table 11-1 Machine data with settings for the Safety Integrated plus mode

Number	Symbolic name	Purpose
MD13370	$MN_SAFE_MODE	Different safety operating modes
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 and PROFIsafe enable
MD37952	$MA_PROFISAFE_MODULE_NR	Number to select a logical basis address from MD13372
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
MD13372	$MN_PS_DRIVE_LOGIC_ ADDR[0..30]	I/O start address of SIEMENS telegrams 903 and 902 (PROFIsafe) of the corresponding drive object
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
MD37950	$MA_SAFE_INFO_ENABLE	Activation / deactivation of safety-related telegrams
MD37952	$MA_PROFISAFE_MODULE_NR	Number to select a logical basis address from MD13372 $MN_SAFE_PS_DRIVE_LOGIC_ADDR.
MD37954	$MA_SAFE_INFO_MODULE_NR	Number to select a logical basis address from MD13374

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 List Manual "SINUMERIK 840D sl, SINAMICS S120 Machine Data and Parameters" - or in the online help for SINUMERIK Operate

11.2 NC tags

11.2.1 Overview

Safety-relevant NC variables (OPI) are available in the Safety Integrated plus operating mode; to a large extent, these are mapped using SIC signals.

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-relevant NC variables are specific to an operating mode - and are not supplied in the two operating modes.

Table 11-4 Safety-relevant 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	Selected safety-relevant setpoint velocity limit in the drive.
SEMA	277	safeAxisType	Type of axis-specific safety monitoring functions (safety axis operating mode).
S	358	safeMode	Configured Safety Integrated operating mode.

Further information

List Manual "SINUMERIK 840D sl, NC Variables and Interface Signals".

11.3 System variables

11.3.1 Overview

Safety-relevant system variables are available in the Safety Integrated plus operating mode, which are mapped using SIC signals (interface NC/PLC-DRIVE):

- $VA_STOPSI (Page 340)
- $A_STOPESI (Page 340)

Note

Information for those switching over from a different system: System variables available in the Safety Integrated plus operating 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 Safety Integrated operating mode are not supplied in the Safety Integrated plus operating mode.

11.3.2 $VA_STOPSI - actual STOP

System variable $VA_STOPSI

Axis-specific system variable that contains the present stop. For a value of 4, a STOP E is active for this axis.

11.3.3 $A_STOPESI - actual STOP E

System variable $A_STOPESI

Global system variable that with a value not equal to 0 indicates that a STOP E is active for a particular axis.

11.4 Standard telegram start addresses

Table 11-5 SINAMICS Integrated: I/O addresses of PROFIsafe/PROFIdrive telegrams

Drive	Telegram type	I/O start address		Machine data
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	5800	15756	13374[0]
	SIEMENS telegram 903	1008		13372[0]
Drive_Axis_2	SIEMENS telegram 701	5816	15676	13374[1]
	SIEMENS telegram 903	992		13372[1]
Drive_Axis_3	SIEMENS telegram 701	5832	15596	13374[2]
	SIEMENS telegram 903	976		13372[2]
Drive_Axis_4	SIEMENS telegram 701	5848	15516	13374[3]
	SIEMENS telegram 903	960		13372[3]
Drive_Axis_5	SIEMENS telegram 701	5864	15436	13374[4]
	SIEMENS telegram 903	944		13372[4]
Drive_Axis_6	SIEMENS telegram 701	5880	15356	13374[5]
	SIEMENS telegram 903	928		13372[5]

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
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	5896	15206	13374[6]
	SIEMENS telegram 903	912		13372[6]
Drive_Axis_2	SIEMENS telegram 701	5912	15126	13374[7]
	SIEMENS telegram 903	896		13372[7]
Drive_Axis_3	SIEMENS telegram 701	5928	15046	13374[8]
	SIEMENS telegram 903	880		13372[8]
Drive_Axis_4	SIEMENS telegram 701	5944	14966	13374[9]
	SIEMENS telegram 903	864		13372[9]
Drive_Axis_5	SIEMENS telegram 701	5960	14886	13374[10]
	SIEMENS telegram 903	848		13372[10]
Drive_Axis_6	SIEMENS telegram 701	5976	14806	13374[11]
	SIEMENS telegram 903	832		13372[11]

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	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	5992	14656	13374[12]
	SIEMENS telegram 903	816		13372[12]

Drive	Telegram type	I/O start address		Machine data
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_2	SIEMENS telegram 701	6008	14576	13374[13]
	SIEMENS telegram 903	800		13372[13]
Drive_Axis_3	SIEMENS telegram 701	6024	14496	13374[14]
	SIEMENS telegram 903	784		13372[14]
Drive_Axis_4	SIEMENS telegram 701	6040	14416	13374[15]
	SIEMENS telegram 903	768		13372[15]
Drive_Axis_5	SIEMENS telegram 701	6056	14336	13374[16]
	SIEMENS telegram 903	752		13372[16]
Drive_Axis_6	SIEMENS telegram 701	6072	14256	13374[17]
	SIEMENS telegram 903	736		13372[17]

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
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	6088	14106	13374[18]
	SIEMENS telegram 903	720		13372[18]
Drive_Axis_2	SIEMENS telegram 701	6104	14026	13374[19]
	SIEMENS telegram 903	704		13372[19]
Drive_Axis_3	SIEMENS telegram 701	6120	13946	13374[20]
	SIEMENS telegram 903	688		13372[20]
Drive_Axis_4	SIEMENS telegram 701	6136	13866	13374[21]
	SIEMENS telegram 903	672		13372[21]
Drive_Axis_5	SIEMENS telegram 701	6152	13786	13374[22]
	SIEMENS telegram 903	656		13372[22]
Drive_Axis_6	SIEMENS telegram 701	6168	13706	13374[23]
	SIEMENS telegram 903	640		13372[23]

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
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	6184	13556	13374[24]
	SIEMENS telegram 903	624		13372[24]
Drive_Axis_2	SIEMENS telegram 701	6200	13476	13374[25]
	SIEMENS telegram 903	608		13372[25]
Drive_Axis_3	SIEMENS telegram 701	6216	13396	13374[26]
	SIEMENS telegram 903	592		13372[26]
Drive_Axis_4	SIEMENS telegram 701	6232	13316	13374[27]
	SIEMENS telegram 903	576		13372[27]

Drive	Telegram type	I/O start address		Machine data
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_5	SIEMENS telegram 701	6248	13236	13374[28]
	SIEMENS telegram 903	560		13372[28]
Drive_Axis_6	SIEMENS telegram 701	6264	13156	13374[29]
	SIEMENS telegram 903	544		13372[29]

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
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	6280	13006	13374[30]
	SIEMENS telegram 903	528		13372[30]
Drive_Axis_2	SIEMENS telegram 701	6296	12926	13374[31]
	SIEMENS telegram 903	512		13372[31]
Drive_Axis_3	SIEMENS telegram 701	6312	12846	13374[32]
	SIEMENS telegram 903	496		13372[32]
Drive_Axis_4	SIEMENS telegram 701	6328	12766	13374[33]
	SIEMENS telegram 903	480		13372[33]
Drive_Axis_5	SIEMENS telegram 701	6344	12686	13374[34]
	SIEMENS telegram 903	464		13372[34]
Drive_Axis_6	SIEMENS telegram 701	6360	12606	13374[35]
	SIEMENS telegram 903	448		13372[35]

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
		Standard addressing schematic	Optimized addressing schematic	
Drive_Axis_1	SIEMENS telegram 701	6376	12456	13374[36]
	SIEMENS telegram 903	432		13372[36]
Drive_Axis_2	SIEMENS telegram 701	6392	12376	13374[37]
	SIEMENS telegram 903	416		13372[37]
Drive_Axis_3	SIEMENS telegram 701	6408	12296	13374[38]
	SIEMENS telegram 903	400		13372[38]
Drive_Axis_4	SIEMENS telegram 701	6424	12216	13374[39]
	SIEMENS telegram 903	384		13372[39]
Drive_Axis_5	SIEMENS telegram 701	6440	12136	13374[40]
	SIEMENS telegram 903	368		13372[40]
Drive_Axis_6	SIEMENS telegram 701	6456	12056	13374[41]
	SIEMENS telegram 903	352		13372[41]

11.5 Telegram structure and data

11.5.1 SIEMENS telegram 701

Telegram 701

The predefined PROFIdrive telegram 701 is available for the transfer of the SIC and the SCC:

Table 11-12 SIEMENS telegram 701 (telegram structure)

	Receive data	Parameter	Send data	Parameter
PZD1	S_STW1B (Page 361)	p10250	S_ZSW1B (Page 361)	r9734
PZD2	S_STW3B (Page 363)	p10235	S_ZSW2B (Page 362)	r9743
PZD3	–	–	S_V_LIMIT_B (Page 364)	r9733[2]
PZD4	–	–		
PZD5	–	–	S_ZSW3B (Page 363)	r10234

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

You can find further information on communication via PROFIdrive in the Manual "SINAMICS S120 Drive Functions Function Manual", Chapter "Communication according to PROFIdrive".

11.5.2 SIEMENS telegram 903

Structure of telegram 903

Telegram 903 transmits the following user data: S_STW2, S_SLS_LIMIT_A, S_ZSW2, S_ZSW_CAM1 and S_SLS_LIMIT_A_ACTIVE.

Telegram 903 is the default setting for internal NC drives.

	Output data	Input data
PZD1	S_STW2 (Page 352)	S_ZSW2 (Page 354)
PZD2		

	Output data	Input data
PZD3	S_SLS_LIMIT_A (Page 357)	S_ZSW_CAM1 (Page 359)
PZD4	–	
PZD5	–	S_SLS_LIMIT_A_ACTIVE (Page 357)

11.5.3 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 11-13 SIEMENS telegram 902 (telegram structure)

	Output data	Input data
PZD1	S_STW2 (Page 352)	S_ZSW2 (Page 354)
PZD2		
PZD3	S_SLS_LIMIT_A (Page 357)	S_SLS_LIMIT_A_ACTIVE (Page 357)
PZD4	–	S_CYCLE_COUNT (Page 358)
PZD5	–	S_XIST32 (Page 358)
PZD6		

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 11-14 SIEMENS telegram 901 (telegram structure)

	Output data	Input data
PZD1	S_STW2 (Page 352)	S_ZSW2 (Page 354)
PZD2		
PZD3	S_SLS_LIMIT_A (Page 357)	S_SLS_LIMIT_A_ACTIVE (Page 357)
PZD4	–	S_CYCLE_COUNT (Page 358)
PZD5	–	S_XIST16 (Page 358)

11.5.5 PROFIsafe telegram 30

Telegram 30 transfers as user data safety control word 1 (S_STW1) and safety status word 1 (S_ZSW1).

Table 11-15 PROFIsafe telegram 30 (telegram structure)

	Output data	Input data
PZD1	S_STW1 (Page 348)	S_ZSW1 (Page 350)

11.5.6 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 11-16 PROFIsafe telegram 31 (telegram structure)

	Output data	Input data
PZD1	S_STW2 (Page 352)	S_ZSW2 (Page 354)
PZD2		

11.6 Process data

11.6.1 Overview: Process data in telegrams

Table 11-17 Process data from PROFIsafe telegrams

Telegram Process data	903	902	901	31	30
Safety control word 1 S_STW1 (Page 348)	–	–	–	–	PZD1
Safety status word 1 S_ZSW1 (Page 350)	–	–	–	–	PZD1
Safety control word 2 S_STW2 (Page 352)	PZD1…2	PZD1…2	PZD1…2	PZD1…2	–
Safety status word 2 S_ZSW2 (Page 354)	PZD1…2	PZD1…2	PZD1…2	PZD1…2	–
SLS limit value input S_SLS_LIMIT_A (Page 357)	PZD3	PZD3	PZD3	–	–
Active SLS limit value S_SLS_LIMIT_A_ACTIVE (Page 357)	PZD5	PZD3	PZD3	–	–
Counter for the safety cycle S_CYCLE_COUNT (Page 358)	–	PZD4	PZD4	–	–
Actual position value (16 bits) S_XIST16 (Page 358)	–	–	PZD5	–	–
Actual position value (32 bits) S_XIST32 (Page 358)	–	PZD5…6	–	–	–
Safe Cam status word S_ZSW_CAM1 (Page 359)	PZD3…4	–	–	–	–

Table 11-18 Process data from SIEMENS telegram 701 (SIC/SCC)

Telegram Process data	701
Safety Control Channel control word 1 S_STW1B (Page 361)	PZD1
SI Motion Safety Info Channel status word S_ZSW1B (Page 361)	PZD1
Safety Info Channel status word 2 S_ZSW2B (Page 362)	PZD2
Safety Control Channel control word 3 S_STW3B (Page 363)	PZD2

Telegram Process data	701
SLS setpoint speed limiting (32 bit) S_V_LIMIT_B (Page 364)	PZD3…4
Safety Info Channel status word 3 S_ZSW3B (Page 363)	PZD5

See also

S_ZSW3B: Safety Info Channel status word 3 (Page 363)

11.6.2 PROFIsafe process data

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 11-19 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

Byte	Bit	Meaning	Remarks	
1	0	Reserved	–	–
	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 11-20 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	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	Reserved	–	–
	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	–	–

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 11-21 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	Reserved	–	–
	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 11-22 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	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	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	Reserved	–	–
	1	Active SLS level bit 0	–	Display of the velocity 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)

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 11-23 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	Reserved	–	–
	7	SSM	0	–[1)]
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, 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 11-24 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	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	Reserved	–	–
	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	Select SLP area 2 (SLP2)
			0	Select SLP area 1 (SLP1)
	4 ... 7	Reserved	–	–

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 SSE
			0	Select SSE
	5 ... 7	Reserved	–	–

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 11-25 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
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)]

Byte	Bit	Meaning	Remarks	
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	Reserved	–	–
	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 11-26 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	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

Byte	Bit	Meaning	Remarks	
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)
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	Reserved	–	–
	4	SS2E active	1	SS2E active
			0	SS2E not active
	5	SOS selected	1	SOS selected
			0	SOS deselected
	6	SLP high limit maintained[1]	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 low limit maintained[1]	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 telegrams 901 and 902, 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 telegrams 901 and 902, 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 11-27 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
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

Byte	Bit	Meaning	Remarks	
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
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 11-28 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...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 11-29 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	Reserved	–	–	–

Bit	Meaning	Remarks		Parameter
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 11-30 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 11-31 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	
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 11-32 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	

Bit	Meaning	Remarks		Parameter
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...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 11-33 Description S_V_LIMIT_B

Parameter	Meaning
r9733[2]	SLS speed limit
p2000	Scaling of the SLS velocity 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 201) in the axis DB (Page 202):

- DB31 … DB61, Safety Info Channel (SIC)
- DB31 … DB61, Safety Control Channel (SCC)

This means, for example, that you can perform the brake test via the PLC user program.

Additional information

List Manual "SINUMERIK 840D sl, NC Variables and Interface Signals".

System features 12

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 Newsletter

1. Go to the following Internet address in your browser:
   All Newsletters (https://www.industry.siemens.com/newsletter/public/AllNewsletters.aspx)
2. Select the desired language for the Web page.
3. You have to register and log in if you want to subscribe to any newsletters. Please proceed as follows if you have still not registered:
   - Click on "Login / registration".
   - Login with your access data. If you do not yet have a login and password, select "Yes, I would like to register now".
     You can subscribe to the individual newsletters in the following window.
4. Activate the "All Newsletters" tab.

5. In the list, open the "Products and solutions" topic.
   You will now be shown which newsletter is available for this particular subject area or topic. You can subscribe to the appropriate newsletter by clicking on the "Subscribe" entry. If you require more detailed information on the newsletters, then please use the supplementary function on the website.

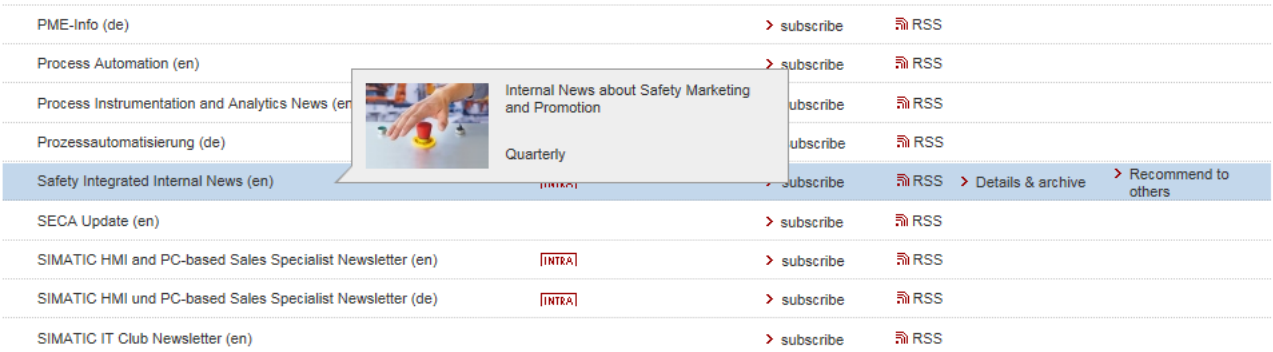


Figure 12-1 Ordering the newsletter

6. Subscribe to the "Safety Integrated Internal News" Newsletter.

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.

Switchover from Safety Integrated (system-integrated) 13

13.1 Overview

If you previously worked with SINUMERIK Safety Integrated (SPL), the information provided in this chapter can make it easier for you to switch over to Safety Integrated plus:

- Comparison of the safety functions (Page 374)
- Additional differences when commissioning (Page 379)
- Procedure when switching over between systems (Page 389)

13.2 Comparison of the safety functions

13.2.1 Overview

The safety functions of SINUMERIK Safety Integrated - integrated in the system - use, in some instances, their own function names. The names of the safety functions of Safety Integrated plus, integrated in the system, correspond to the SINAMICS safety functions, and are therefore orientated to DIN EN 60204-1.

These names are compared in this chapter.

For Safety Integrated plus, the drive-integrated safety functions available with Safety Integrated (STO, SBC, SS1), belong to the Basic Functions - and are available with the same function names. These are not listed here.

Table 13-1 Comparison of the system-integrated safety functions (Safety Integrated) and Extended Functions integrated in the drive (Safety Integrated plus)

Safety Integrated		Safety Integrated plus		Additional information
External STOP A	Stop A/SH	Safe Torque Off (Safe Torque Off)	STO	
		Safe Stop 1 (Safe stop in accordance with stop Category 1)	SS1	
Ext. STOP C	STOP C	Safe Stop 2 (Safe stop in accordance with stop Category 2)	SS2	
Ext. STOP D	STOP D	Safe Stop 2e	SS2e	
Ext. STOP E	STOP E	--*	--*	*Available as stop response when SLS/SLP is exceeded (Page 375)
Safe operating stop	SBH	Safe Operating Stop (Safe operating stop)	SOS	
Safely-Limited Speed	SG	Safely Limited Speed (Safely-Limited Speed)	SLS	
SG override (32 SG levels can be selected via SPL)	Override for SG	SLS override		Enters the correction factor in the safety program via PROFIsafe (Page 376)
Safe Acceleration Monitoring	SBR	Safe Acceleration Monitor (Safe Acceleration Monitoring)	SAM	
--	--	Safe Brake Ramp (Safe brake ramp monitoring)	SBR	
Safety-relevant output signal n<nx	n<nx	Safe Speed Monitor (Safe Speed Monitor)	SSM	
--	--	Safe Direction (Safe motion direction)	SDI	
Safe end positions	SE	Safely-Limited Position (Safely-Limited Position)	SLP	

Safety Integrated		Safety Integrated plus		Additional information
Safe Brake Test (SI_BrakeTest [FB11])	SBT	--	--	
Safe Brake Test (SIC/SCC)	SBT	Safe Brake Test (Safe Brake Test)	SBT	
Safe Cams/cam track	SN	Safe Position (Safe position)	SP	Safe Cams (Page 377)
		Safe Cam (Safe Cams)	SCA	
Internal SOS deselection	--	Internal SOS deselection	--	
Dyn. Stop D	--	--	--	
--	--	Additional operations for the safety program of the F-PLC	--	See also: Instructions for the safety program (Page 54)

See also

Parameterizing EMERGENCY STOP (Page 377)

13.2.2 STOP E

Safety Integrated

Safety Integrated allows STOP E to be initiated with a transition into SBH. To achieve this, the initiation of ESR must be programmed, taking into account system tags $AC_ESR_TRIGGER=1 and $VA_STOPSI or $VA_STOPESI. The timer can be parameterized in p9554 "SI Motion transition time from STOP E to SBH" (drive monitoring channel) and in the MD36954 $MA_SAFE_STOP_SWITCH_TIME_E (NC monitoring channel).

The initiation of STOP E - as a result of a fault - can be realized using PLC-SPL-CDC, FSEND-FRECV communication or F-I/O fault (Page 386). The acknowledgment or the deselection can be realized, either using a NC RESET or e.g. in the PLC program using SGE "Deselect ext. STOP E" in "<axis DB>.DBX32.5".

Safety Integrated plus

Safety Integrated plus only supports STOP E as parameterizable fault response of safety functions SLS and SLP. All safety functions can be parameterized in dedicated SINUMERIK Operate screen forms. In the screen forms you can also set the fault response and the delay time.

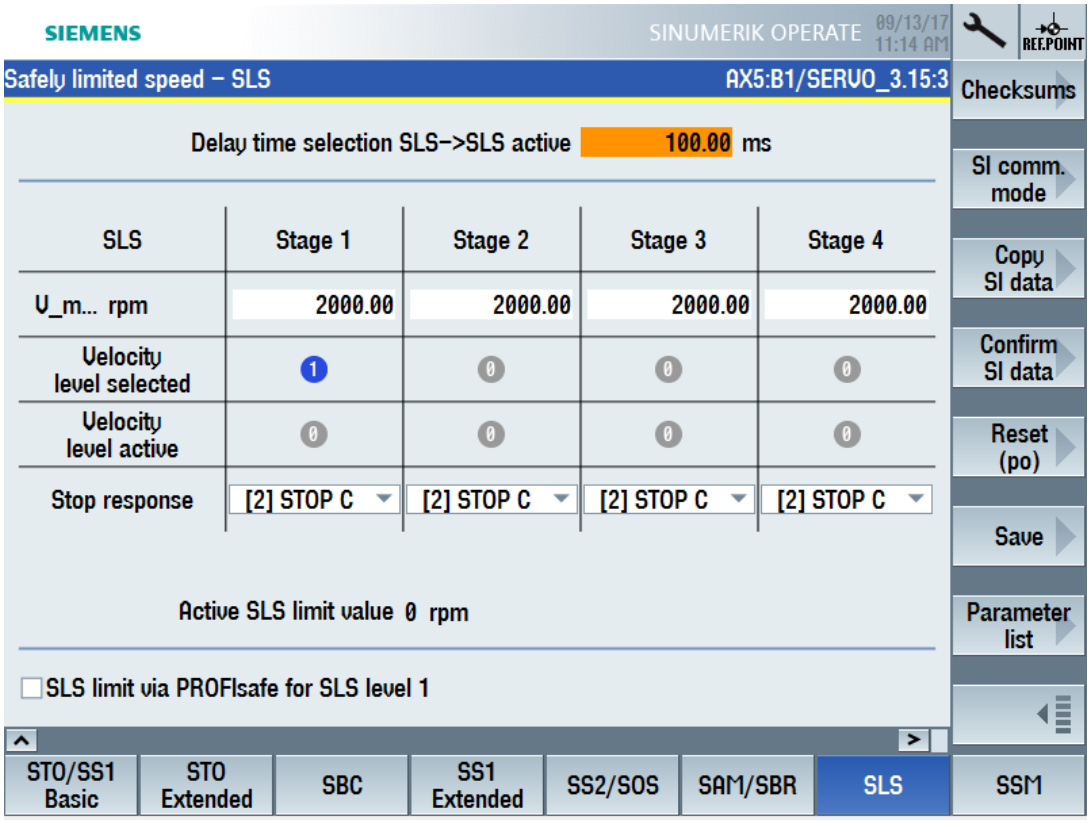


Figure 13-1 Selecting STOP E as stop response for SLS

SLS is acknowledged or deselected with STOP E in the safety program of the F-PLC by resetting the corresponding bits in the drive addresses (via PROFIsafe telegram) - and additional safety-relevant acknowledgment (PROFIsafe IEACK) along with a PROFIdrive reset.

See also: Acknowledgment (Page 323), Deselecting safety functions integrated in the drive (Page 229).

For Safety Integrated plus, system tags $VA_STOPSI and $VA_STOPESI are also supplied.

13.2.3 SG override

Safety Integrated

Safety Integrated allows up to 4 safety-relevant velocity values to be used. Safety-relevant velocities SG2 and SG4 can also be assigned 16 different percentage values, so that 34 different velocity values are available for each axis.

Safety Integrated plus

4 safety-relevant velocity values are also available for Safety Integrated plus. You can set these 4 values in the function-specific SINUMERIK Operate screen form.

In addition, the 1st safety-relevant velocity level can be assigned percentage values between 0 and 100% - to achieve a high level of granularity. To do this, in the associated screen form, activate option "SLS limit via PROFIsafe for SLS level 1" - and in the safety program, access the corresponding bit using the PROFIsafe telegram.

This means that theoretically more than a 32,000 values can be defined.

13.2.4 Safe Cams

Safety Integrated

With Safety Integrated, depending on the particular application, you use the "Safe Software Cams" or "Safe Cam Track" safety function.

- With "Safe software cams", up to 4 cam pairs are available for each axis. Here, the precondition is that the axes involved are safely referenced.
- Alternatively, the "Safe Cam Track" function can be used, which can be used to evaluate a total of 30 cams. Here, up to 4 cam tracks - with a maximum of 15 cams per cam track - are available.

In both cases, you must configure the cams using the appropriate machine data or drive parameters. SGA with information about the cams can be evaluated using Safe Programmable Logic (SPL).

Safety Integrated plus

Safety Integrated plus allows safety-relevant cams to be implemented using two different safety functions:

- Safety function SCA (Safe Cam) allows up to 30 safety-relevant cams per axis to be directly configured in a function-specific SINUMERIK Operate screen form. To use this safety function, you require process data S_ZSW_CAM1, which is only available in SIEMENS telegram 903.
- SP (Safe Position) allows safety-relevant position values to be transferred (process data S_XIST32) in SIEMENS telegram 902. The safety-relevant position values can be evaluated in the F-PLC safety program to implement safety-relevant cams.

13.2.5 Parameterizing EMERGENCY STOP

For EMERGENCY STOP shutdowns, for Safety Integrated, the PLC basic program block "SI_relay [FB10]" was used in conjunction with the corresponding NC SPL syntax for SI relay.

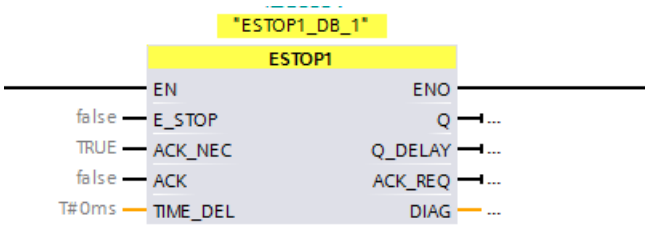
For example, when actuating an EMERGENCY STOP pushbutton, a STOP C or STOP D can be initiated with delayed STOP A. The same EMERGENCY STOP shutdown operations can also be implemented when using Safety Integrated plus:

Table 13-2 Examples of EMERGENCY STOP shutdown operations in Safety Integrated and Safety Integrated plus that can be parameterized

Safety Integrated	Safety Integrated plus
Ext. Stop C → Δt → STOP A	SS1
Ext. Stop D → Δt → STOP A	SS2e → Δt → STO

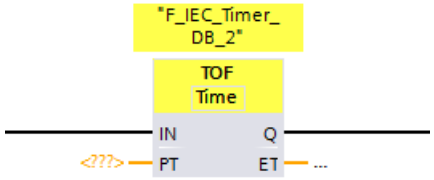
Further, for Safety Integrated, external I/O devices can be shut down in a safety-relevant way using an SI-relay.

Instead of this function, for Safety Integrated Plus, the certified ESTOP1 operation is available. Instruction ESTOP1 can be used to control the required stopping requirements in SINAMICS Safety Integrated as well as the F-I/O.



The following differences exist when parameterizing the switch-off delay time of the EMERGENCY STOP signal:

Table 13-3 Parameterizing the delay time of the EMERGENCY STOP signal

Delay time	Safety Integrated	Safety Integrated plus
Drive components	The safety relay block has 3 timers for different delay times.	Parameterize the switch-off delay time directly in the SINUMERIK Operate screen form for the corresponding safety function.
F-I/O		You can specify 1 time in parameter Q_DELAY of the ESTOP1 operation. You can use the TOF operation for each additional delay time that is required. 

13.3 Additional differences when commissioning

13.3.1 Overview

Several commissioning steps and functions of Safety Integrated plus and the corresponding functions of Safety Integrated are compared in the following.

Commissioning step	Safety Integrated (SPL)	Safety Integrated plus (F-PLC)
Maximum number of axes that are supported	31 axes per NCU, of which, a maximum of 6 can be connected to one DRIVE CLiQ line.	31 axes per NCU, of which, a maximum of 4 can be connected to one DRIVE CLiQ line. See also: Interconnecting DRIVE-CLiQ components (Page 31)
Commissioning the F-I/O	Configuring in STEP 7 and parameterizing - partially redundantly - in STEP 7 and in SINUMERIK Operate using machine data.	Configuring and parameterizing the F-I/O in STEP 7 (TIA Portal). See: Commissioning the F-I/O (Page 380)
Commissioning the safety functions	Commissioning in SINUMERIK Operate using machine data that can be filtered and in some instances using function-specific screen forms.	SI drives and drive-integrated safety functions are commissioned using function-specific screen forms in SINUMERIK Operate See: Parameterizing the safety functions (Page 383)
Programming the safety logic	Redundant programming as NC-SPL program (SAFE.SPF) and PLC-SPL program.	The complete safety program is programmed in the TIA Portal using the operating concepts known from standard PLC user programs. LAD and FBD programming languages are used with a scope of operations adapted to F-blocks.
	F-I/O are accessed using system tags or data block "SPL [DB18]"; safety functions of the drives are accessed (axis-specific SGE/SGA) via system tags or axis-DBs	F-I/O and drive telegrams are accessed via the process image in the safety program and PLC user program. Some system tags are also used. See: Accessing status/control information (Page 388)
Accessing status/control signals	Access is mainly realized via axis/channel DB, SPL [DB18] and NC/system tags.	Access to process data of the telegrams, the process image and F-I/O DB. See: Accessing status/control information (Page 388)
Fault response to F-I/O faults	A fault message is displayed followed by a stop response for all axes	A fault message is displayed, the stop response has to be configured depending on the specific situation.
Configuring a fault response to communication faults/errors	Passivation, provision of substitute values for FSEND/FRECV, system-related STOP D/E response can be parameterized, additional response can be configured.	Passivation of the F-I/O or drive components involved, provision of substitute values (FSEND/FRECV), additional response can be configured. See: Fault response and acknowledgment for F-I/O faults (Page 386)

Commissioning step	Safety Integrated (SPL)	Safety Integrated plus (F-PLC)
Acknowledging after a communication faults/errors	User acknowledgment using interface signal DB18.FRDP_ACK_REI - and via a channel_1 reset.	User acknowledgment by configuring an acknowledgment button with assignment to the corresponding F-I/O DB tag ("ACK_GL" or "ACK_GLOB") and channel_1 reset (PROFIdrive reset). See: Fault response and acknowledgment for F-I/O faults (Page 386) See also: Implementing user acknowledgment for global reintegration (Page 224).
Evaluating alarms using the NC	The NC checks safety alarms, and if necessary suppresses an alarm, prioritizes an alarm - or checks alarm numbers. See also: General information about displaying and evaluating diagnostic information (Page 309)	As Safety Integrated plus uses the safety functions integrated in the drive, the NC does not suppress alarms, prioritize alarms or check alarm numbers of safety messages of the drive.

13.3.2 Commissioning the F-I/O

Safety Integrated

Initially, you configure and parameterize the F-I/O in STEP 7. You then load the configuration to the NCU, and also enter some settings in the machine data:

- F-source addresses (PROFIsafe addresses of the F-master)
- F-destination addresses (PROFIsafe addresses of the F-DI-/F-DO modules)
- Allocate symbolic names for F-modules (optional)
- Distribution of the computational load on the NC side
- Select F-user data signals to be transferred in the SPL (F-user data filter)
- Assign F-user data signals to be transferred to the SPL-SGE/SGA

Safety Integrated plus

You configure and parameterize the F-I/O completely in STEP 7 (TIA Portal).

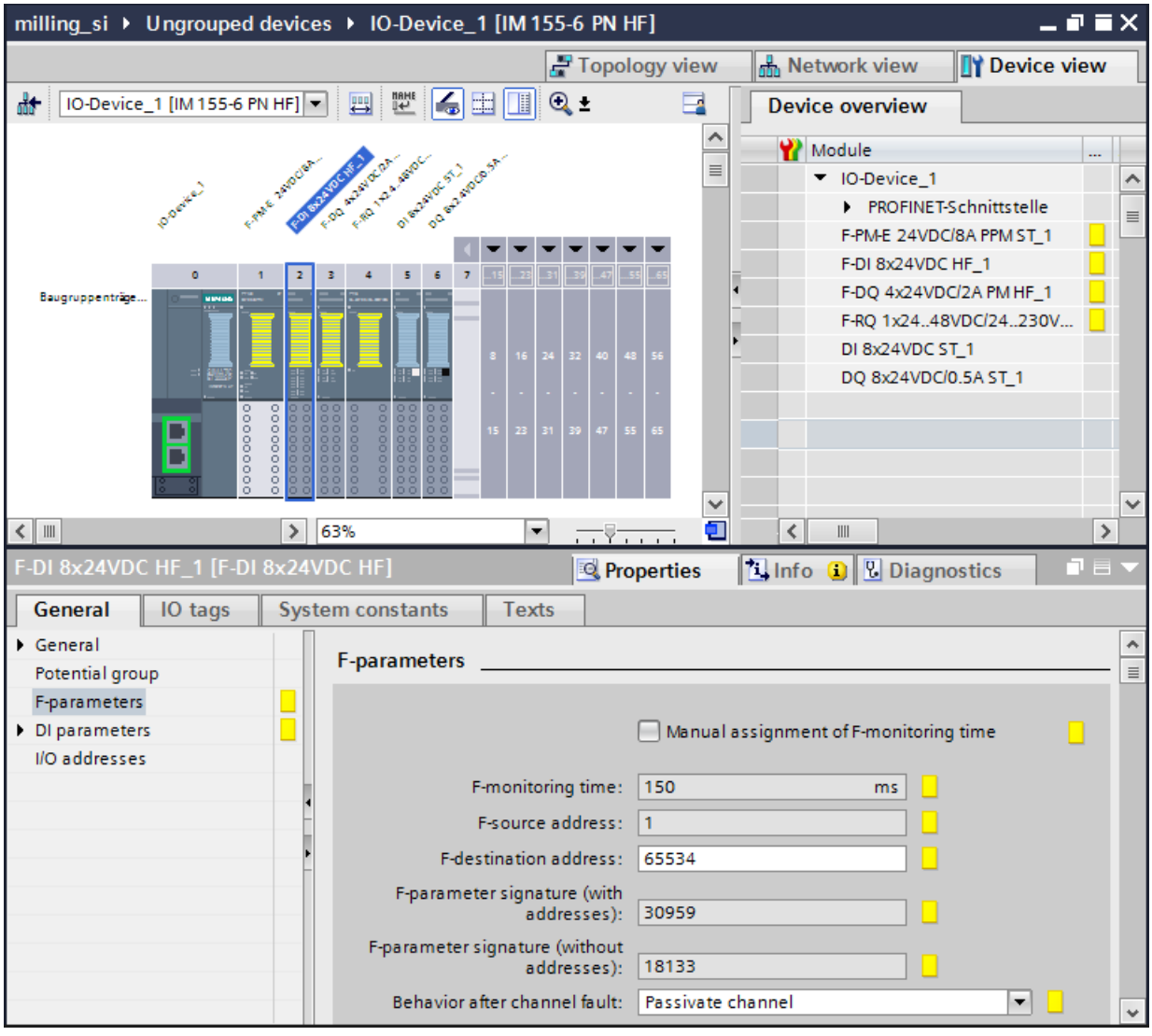
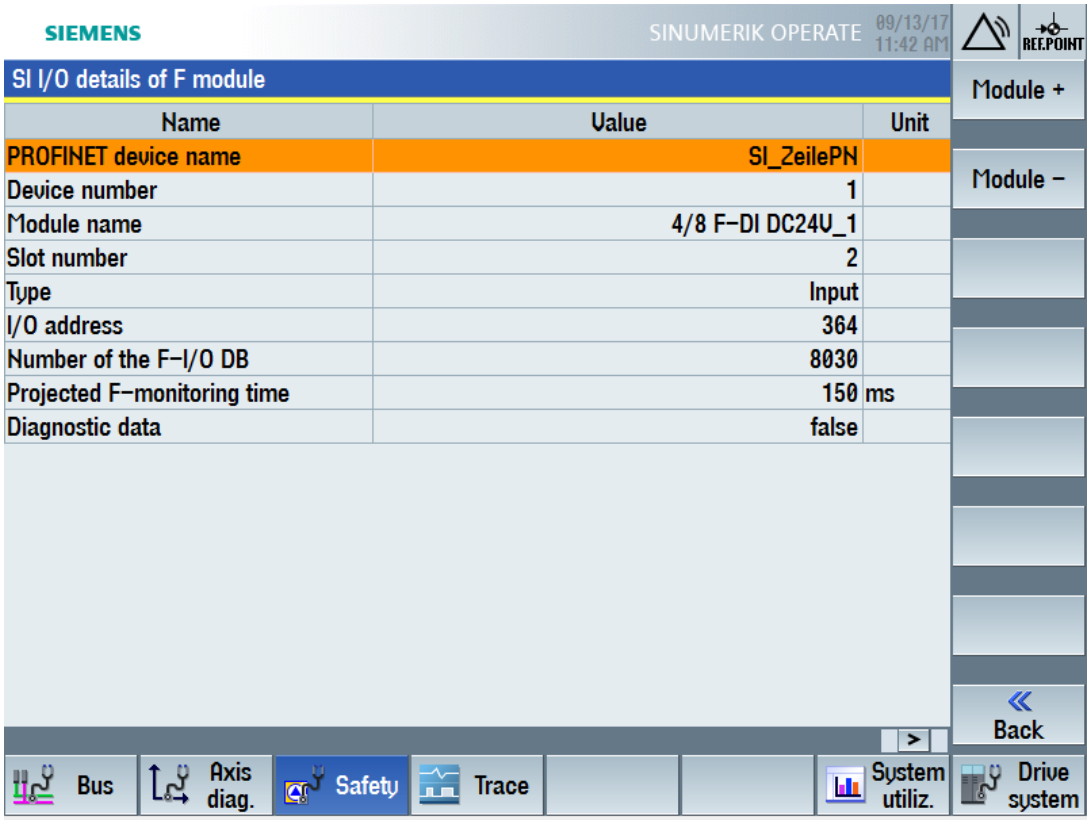


Figure 13-2 F-parameters of an F-DI

After you have loaded the configuration to the NCU, the F-I/O parameterization is automatically accepted, and you can, for example, display detailed and diagnostic information relating to the F-I/O directly in SINUMERIK Operate.



Name	Value	Unit
PROFINET device name	SI_ZeilePN	
Device number	1	
Module name	4/8 F-DI DC24V_1	
Slot number	2	
Type	Input	
I/O address	364	
Number of the F-I/O DB	8030	
Projected F-monitoring time	150	ms
Diagnostic data	false	

Figure 13-3 Parameterization of an F-module taken from the TIA Portal configuration

13.3.3 Parameterizing the safety functions

Safety Integrated

SINUMERIK Operate has function-specific (generally tabular) screen forms to enter some general safety-relevant settings - as well as for the safety functions SBR, SBH/SG, SBC, safety-relevant end positions and safety-relevant cams.

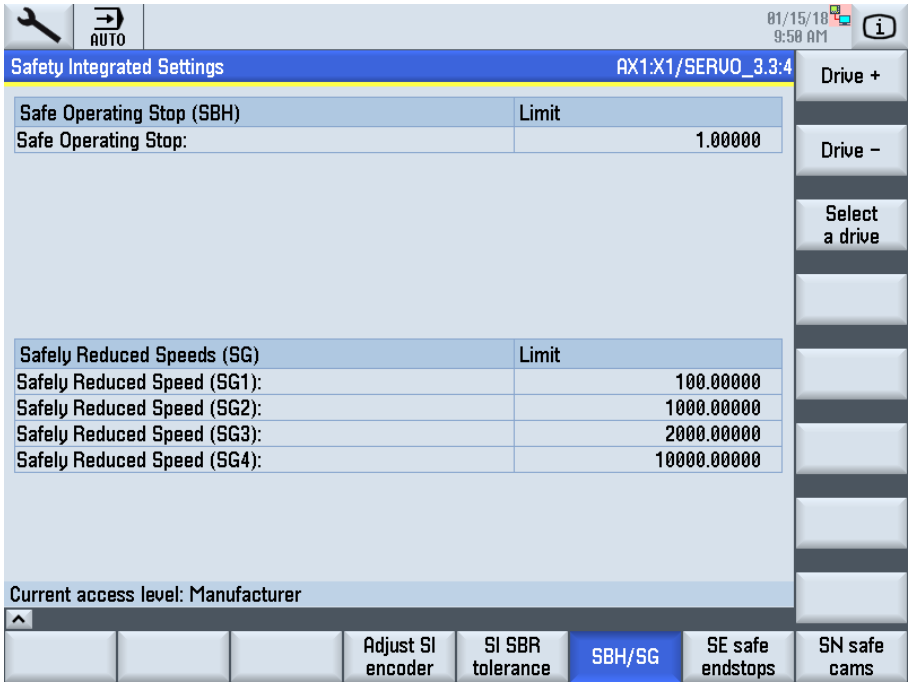


Figure 13-4 Parameterizing a safety function (SBH/SG)

Additional settings and safety functions should be configured in SINUMERIK Operate using machine data and drive parameters that can be filtered.

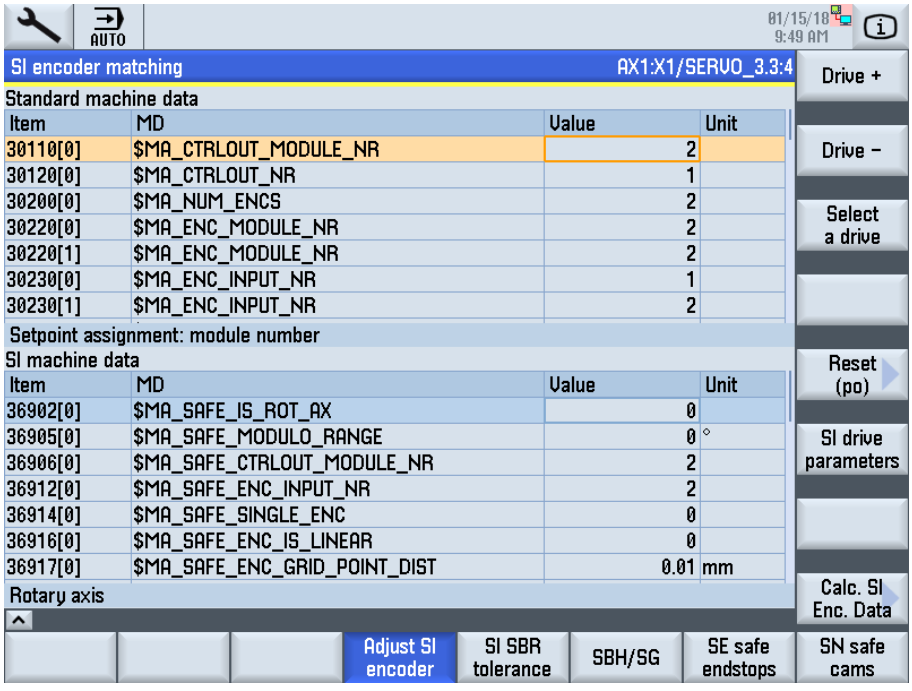


Figure 13-5 Parameterizing using machine data (SI encoder adaptation)

Safety Integrated plus

All of the drive-integrated safety functions as well as higher-level or general settings can be configured using function-specific graphic SINUMERIK Operate screen forms.

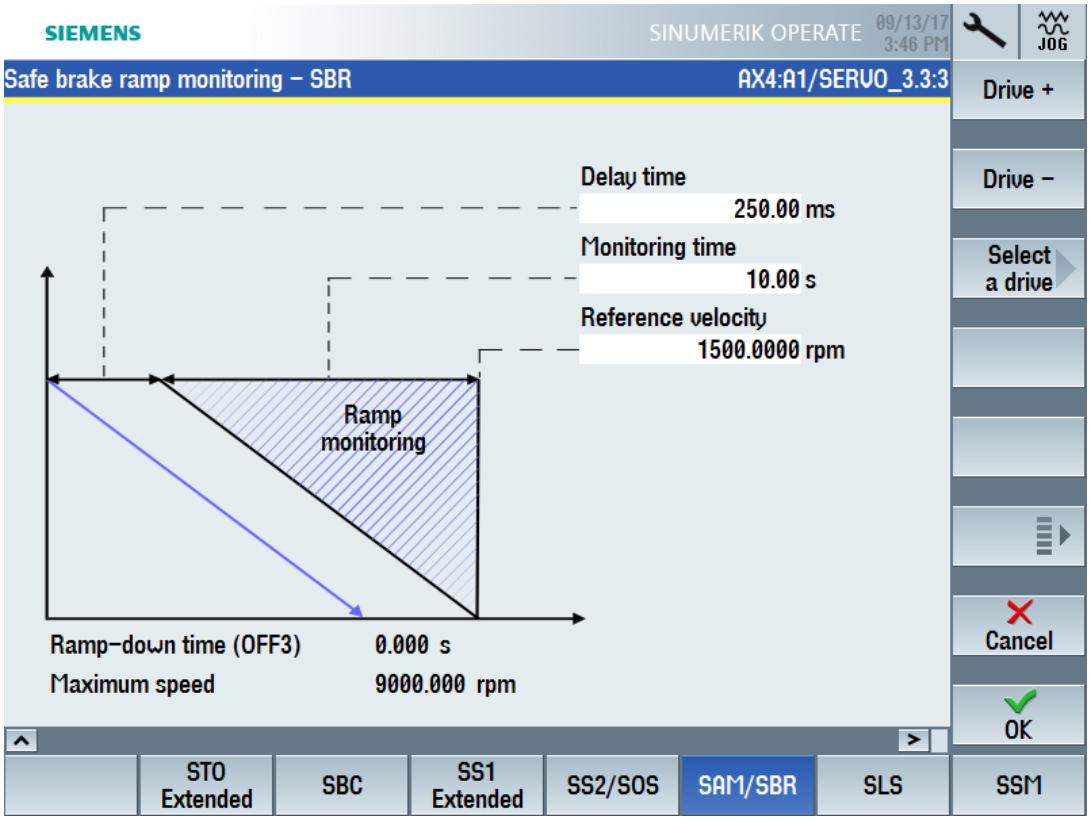


Figure 13-6 Parameterizing a safety function (SBR)

The "Recommended values" softkey is available as supplementary function; this allows recommended values to be automatically calculated and entered. The basis for the calculated recommended values is the corresponding equations to be taken into account for manual parameterization.

Alternatively, all safety-relevant settings can be made in tabular expert lists ("Parameter list" softkey), in which all parameters are listed which involve the corresponding safety function

13.3.4 Fault response and acknowledgment for F-I/O faults

Safety Integrated

In the context of Safety Integrated, F-I/O faults are identified by evaluating the PROFIsafe status of F-I/O devices. A system response is initiated if such a fault occurs:

Error detected by	System response
Drive/NC-CDC	STOP F
SPL-CDC	STOP D/E (Redundant configuration of the stop response to be initiated in the machine data and in data block SPL [DB18].)
Communication CDC	The SGE/SGA involved are brought into a failsafe state (substitute values are provided). Substitute values can be specified. Additional system-specific responses can be configured by reading out DB18.DBX119.5.

Generally, the system response can involve passivation of all of the F-I/O modules - or only those of the channel involved. The cause of the fault must be removed and acknowledged in order to remove the fault and to reset the system response.

Safety Integrated plus

Safety Integrated plus responds to F-I/O faults by providing substitute values, i.e. *passivation* is realized.

The following options exist to adapt and supplement the response:

- Passivate all of the F-I/O modules - or only those of the channel involved.
- Reintegration (depassivation) of the F-I/O automatically, depending on the configuration, with a user acknowledgment.
- In addition, each F-I/O has its own F-I/O DB. This means that you can access status information and program user-specific system responses.

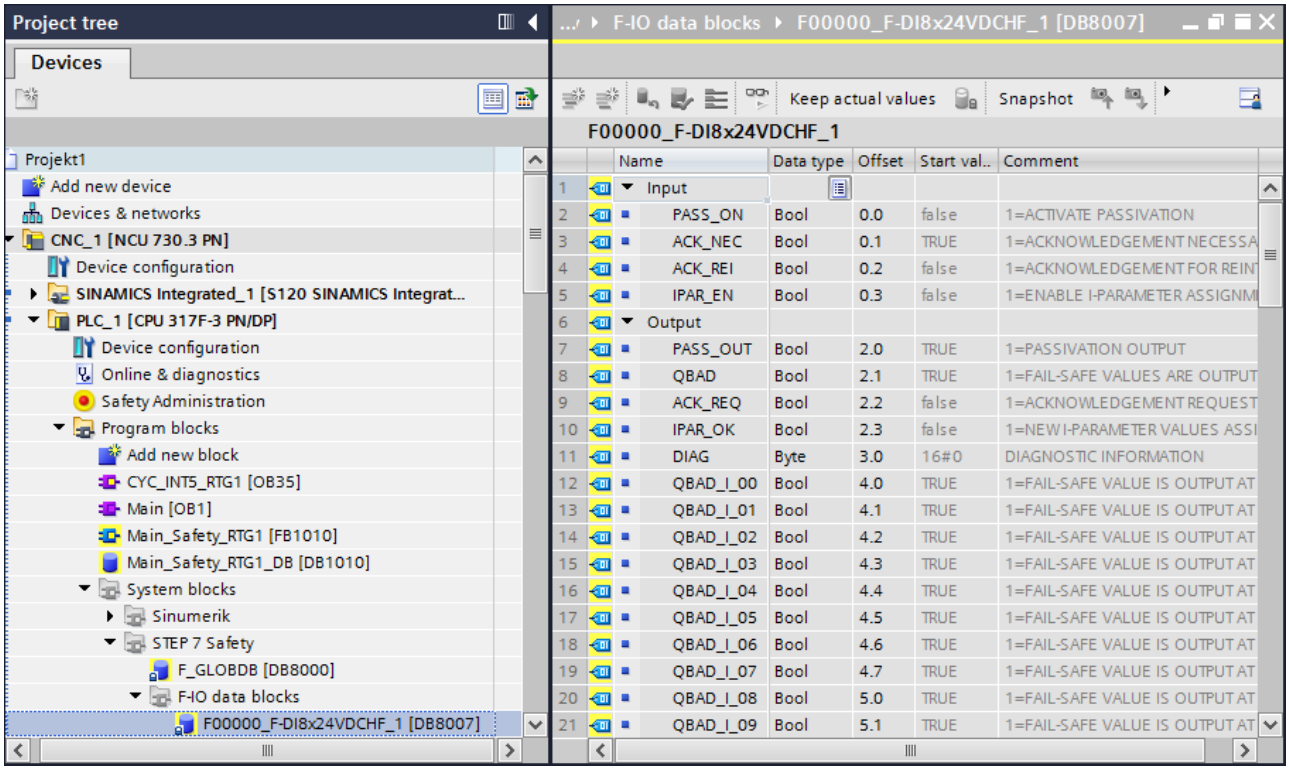


Figure 13-7 Example of an F-I/O DB

Additional information

- Implementing user acknowledgment for global reintegration (Page 224)
- System alarms and diagnostic screens for F-PLC and F-I/O. (Page 294)

13.3.5 Accessing status/control information

As the safety functions of the two safety operating modes are implemented using different subcomponents, there are some fundamental differences regarding the control options:

Access from → to	Safety Integrated	Safety Integrated plus
PLC program → F-I/O PLC program → drive	SPL [DB18]	Process image
PLC program → safety function PLC program → safety-relevant setting	Axis-specific signals for the system-integrated safety functions in <axis DB>.DB22 … <axis DB>.DB125.	Process data in telegrams (PROFIsafe, SIC/SCC)
	Axis-specific signals for drive-integrated safety functions in <axis DB>.DB140 … <axis DB>.DB187 (mapped from SIC).	
	Control via terminals for drive-integrated safety functions (Basic Functions)	
	~ 20 NC variables	5 NC variables (mapped from SIC)
NC part program → safety function NC part program → safety-relevant setting	~ 50 system variables	2 system variables (mapped from SIC)

Safety Integrated

For Safety Integrated, the basic PLC program automatically connects the I/O (F-user data) of an F-module to the SPL interface in data block SPL [DB18]. It is not possible to connect them in a PLC user program.

The safety functions are accessed on an axis-for-axis basis.

Safety Integrated plus

For Safety Integrated plus, F-I/O and safety-relevant drive telegrams are accessed via the process image, as is the case for the standard I/O. The PLC user program can access this status/control information, therefore allowing functional expansions to be made.

Safety functions are accessed on an axis-for-axis basis.

13.4 Procedure when switching over between systems

It is not possible to automatically migrate the safety functions from Safety Integrated to Safety Integrated plus.

- The safety-relevant program code used in the two safety modes differs significantly. This relates to the programming language and operations - as well as the positions and/or blocks from where the safety program can be called.
- Instead of the safety functions of Safety Integrated integrated in the system, for Safety Integrated plus, the drive-based safety functions of SINAMICS Safety Integrated are used; although they are functionally comparable, they use different parameters and values however.

However, the existing risk analysis and the safety concept can be used to create a new safety program on this basis - and to configure the drive-integrated safety functions.

Fundamental approach when switching over

The procedure can be roughly split-up into the following steps:

1. Migrating a STEP 7 V5.x project to the TIA Portal
   Safety Integrated plus is supported from SINUMERIK STEP 7 toolbox V14 (TIA Portal). Information about migrating the standard components of a STEP 7 5.x project into the TIA Portal is provided in the TIA Portal online help, search terms "Migrating SINUMERIK PLC projects" and "Migrating PLC project".
2. Deleting components of the Safety Integrated (SPL) program from the TIA Portal project:
   – Remove the access operations to SPL function blocks or functions - and to SPL data blocks signals from your PLC user program.
     (you can use the following commands to find these locations: "Cross-references" in the shortcut menu of an SPL block, "Browse project" in the shortcut menu of the program block folder)
   – Delete the Safety Integrated (SPL) blocks used in the project:
     SI_relay [FB10]
     SI_BrakeTest [FB11]
     SPL [DB18]
     Additional blocks (e.g. test stop blocks "SI Pulse Teststop SL [FC264]", "SI External Stop SL [FC265]")
3. Adapting the configuration (Page 210)
4. Setting the safety program (Page 219)
5. Commissioning safety functions integrated in the drive
   – Comparison of the functions (Page 374)
   – Configuring NC and drive-specific safety settings (Page 235)
   – Safety functions integrated in the drive (Page 75)

Appendix A

A.1 Abbreviations

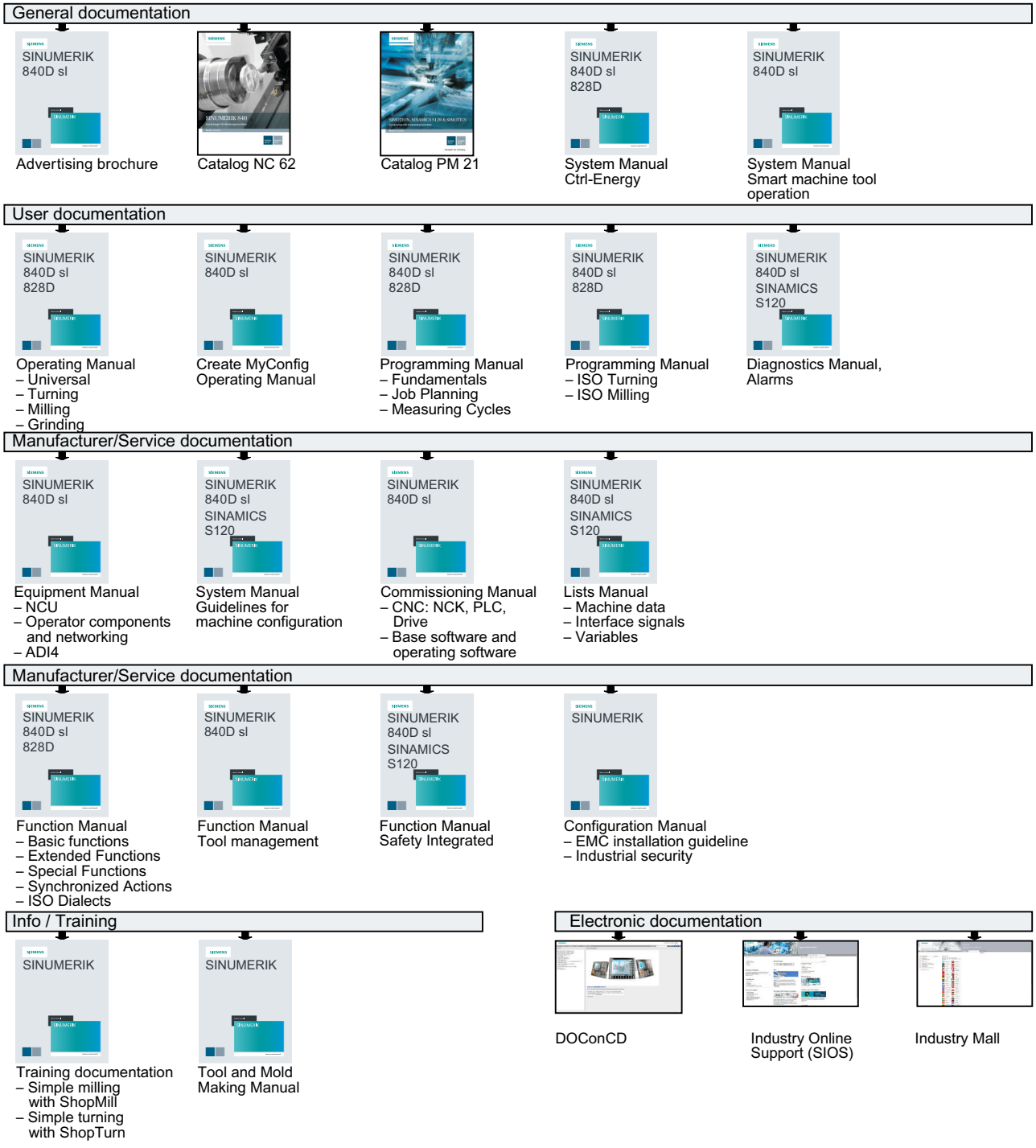
The following list of abbreviations includes all of the relevant abbreviations for SINUMERIK Safety Integrated Functions.

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
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
HLA	Hydraulic Linear Actuator	Hydraulic linear actuator
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
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 motion 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.
STW	Steuerwort	Control word
TM54F	Terminal Module 54 F	Terminal expansion module 54 F
UL	Underwriteres 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 Documentation overview SINUMERIK 840D sl



Index

2

2-encoder system, 179

A

Acknowledgment
    Extended, 325
    Extended alarm acknowledgment, 325
Actual value acquisition, 179
Actual value acquisition clock cycle
    S120M, 184
Actual value synchronization
    Encoder, 184
Advanced Functions, 75
Alarm
    Extended alarm acknowledgment, 325
Alarm buffer, (Buffer)

B

Basic Functions
    SBC, 93, 95
    SS1, 76, 77, 80
    STO, 87
    STO for HLA, 90
Bit memory, 71
Block
    DB1010, 221
    DB1010..1019, 44
    DB31..DB61, 157
    DB8000..16000, 44
    FB1010, 221
    FB1010..1019, 44
    FB11, 157
    FB3999..7999, 44
    F-block, 44
    FC1010..1019, 44
    OB35, 221
Buffer
    Standard alarm buffer, 321

C

Checksum, (Checksum)
    Global checksum, 310
    Master checksum, 310
Communication
    Standard user program and safety program, 71, 72
Communication failure, 198
    ESR, 198
Component replacement
    After Safety Integrated has been commissioned, 335
    Effects, 332
    POWER ON and acceptance test, 329
    Required measures, 332
constants
    Boolean, 51
CRC, (Checksum)

D

Data block, 71
Data transfer
    From safety program to standard user program, 71
    From standard user program to safety program, 72
Data types
    For safety program, 48
DB access, fully qualified, 52
Debounce time, 203
Delay time
    SBR, 81
    SS1, 82
Drive type
    Drive without NC axis assignment, 19
    External drive with NC axis assignment, 19
    Integrated drive, 19
    PLC-controlled NC axis, 19
    Third-party motor with absolute encoder, 289

E

Emergency Stop button, 76
EN, 48
EN 61800-5-2, 87

Encoder
Actual value synchronization, 184
Types for HLA, 183
Encoder systems, 179
Encoder types, 179
Encoders with sin/cos 1 Vpp signals, 182
ENO, 48
ESR
Communication failure, 198
Extended alarm acknowledgment, 325

F

F system block
Number range, 44
F01611
Fault value 1000, 198, 207
Fault reaction function, 41
Fault response, 315
F-block
Copying, 63
F-DB, 46
Creating, 62
F-shared DB, 61
F-FB, 46, 62
F-FC, 46, 62
F-I/O
Removing and inserting during operation, 330
F-I/O access, 66
Via the process image, 66
F-I/O DB
Number range, 44
F-I/O DB, 46
Filter
On/off test, 207
Filter time, (Debounce time)
Firmware update, 330
POWER ON and acceptance test, 329
F-OB, 46
Forced checking procedure, 191
Extended Functions, 191
F-runtime group, 43, 46, 221
F-shared DB, 61, 71
Fully qualified DB access, 52
Function test, 191

H

Hardware components, 29
HLA
Permissible encoder types, 33
Supported Extended Functions, 34
HTL/TTL encoders, 182

I

Increased position tolerance, 187
Information for those switching over from a different system
Comparison of stop responses, 315, 318
Differences between Safety Integrated and Safety Integrated plus, 309
Migration overview, 389
SBT, 157
Using variables, 339, 340
Instance DB, 53, 62
Internal armature short-circuit, 90

L

Limit value violation, 315
Local data, 52

M

Main safety block, 46, 62

O

Operand area
For safety program, 49
Operating system update, 330
Operations
for the safety program., 54

P

Parameter types, 48
Position tolerance, 187
Increased, 187
Process data
S_CYCLE_COUNT, 358
S_SLS_LIMIT_A, 357
S_SLS_LIMIT_A_ACTIVE, 357
S_XIST16, 358
S_XIST32, 358
Process data, control words
S_STW1 (Basic Functions), 348
S_STW1 (Extended Functions), 349

S_STW2 (Basic Functions), 352
S_STW2 (Extended Functions), 353
Process data, status words
S_ZSW_CAM1 (Extended Functions), 359
S_ZSW1 (Basic Functions), 350
S_ZSW1 (Extended Functions), 351
S_ZSW2 (Basic Functions), 354
S_ZSW2 (Extended/Advanced Functions), 355
Process image, 66, 71
PROFIBUS DP, 29
PROFINET IO, 29
PROFIsafe
Enable control via PROFIsafe, 197
SLS limit value, 120
Programming
Startup protection, 68
Validity checks, 72
Proof test, 330

R

Replacing
Software components, 330
Response times, 369
Basic Functions via PROFIsafe, 370
Basic Functions via terminals on the Control Unit and the Motor Module, 369
Extended Functions via PROFIsafe, 370
Restart protection, 68

S

S_CYCLE_COUNT, 358
S_SLS_LIMIT_A, 357
S_SLS_LIMIT_A_ACTIVE, 357
S_STW1
Basic Functions, 348
Extended Functions, 349
S_STW1B, 361
S_STW2
Basic Functions, 352
Extended Functions, 353
S_STW3B, 363
S_V_LIMIT_B, 364
S_XIST16, 358
S_XIST32, 358
S_ZSW_CAM1
Extended Functions, 359
S_ZSW1
Basic Functions, 350
Extended Functions, 351
S_ZSW1B, 361
S_ZSW2
Basic Functions, 354
Extended/Advanced Functions, 355
S_ZSW2B, 362
S_ZSW3B, 363
S120M
Actual value acquisition clock cycle, 184
Safe Acceleration Monitor, 133
Safe actual value acquisition, 179
Safe Brake Adapter
Chassis format, 97
Safe Brake Control
Chassis format, 97
SBC, 95
Safe Brake Ramp
SBR, 82, 135
Safe Cam, 168, (SCA)
Safe Direction, 138, 140
With encoder, 140
Without selection, 143
Safe gearbox stage switchover, 186
Safe motion direction, 140
Safe motion monitoring, 184
Safe Operating Stop, 110
SOS, 111
Safe referencing, 175
Safe Speed Monitor
General, 127
Restart, 131
SSM, 127
With encoder, 129
Safe Stop 1
Basic Functions, 77
Extended Functions, 82
Speed controlled, 83
SS1, 77, 82
Time and acceleration controlled, 82
Time-controlled, 77
With encoder, 82
With external stop (Extended Functions), 85
With OFF3 (Basic Functions), 77
With OFF3 (Extended Functions), 82
Without encoder, 83
Safe Stop 2, 100, 102
Extended Stop and Retract, 107
SS2, 102
with external stop, 104
Safe Torque Off, 87
Basic Functions, 87
STO, 87

Safe Torque Off for HLA
Basic Functions, 90
Safely Limited Speed, 113, 118
Safely-Limited Acceleration, 171
Safely-Limited Position, 146
Safely-Limited Speed
With encoder, 119
Without selection, 124
Safety Control Channel, 201
Safety function, 41
Example, 41
Safety Info Channel, 201
Safety Integrated Basic Functions
Stop responses, 313
Safety Integrated plus (F-PLC), 221
Safety program, 29
Operations, 54
Signature, 310
Structuring, 43
SAM
For SS1, 81
For SS2, 101
SAM (Safe Acceleration Monitor), 133
SBA, 97
SBC
Basic Functions, 93, 95
Safe Brake Control, 93, 95
Select, 93
SBR
Delay time, 81
For SLS, 117
For SS1, 81
For SS2, 101
SCA, 168
Description, 168
Enable, 169
Overview, 168
Referencing, 169
S_ZSW_CAM1, 359
Tolerance, 169
SCC
See Safety Control Channel, 201
SDI, 140
Crane trolley, 138
General, 138
Pressure cylinder, 138
Protection against jamming, 138
Rolling shutter gate, 138
Safe Direction, 138
Time response, 138
With encoder, 140
Without encoder, 141
Without selection, 143
Series commissioning
Confirming the hardware CRC, 335
General procedure, 289
With third-party motor, 289
SIC
see Safety Info Channel, 201
SIMATIC Safety
Configuring and programming software, 29
Hardware and software components, 29
Safety program, 29
STEP 7 Safety optional package, 29
Single-encoder system, 179
SLA, 171
Description, 171
Enable, 171
Safely-Limited Acceleration, 171
Setup mode:, 171
SLP, 146
General, 146
Safely-Limited Position, 146
SLS
Deselect, 115
Horizontal conveyors, 113
Level, 116
Limit value via PROFIsafe, 120, 121
Monitoring threshold, 117
Safely Limited Speed, 113
Select, 115
Speed limit values, 120
Spindle drive, 113
Switching over the monitoring threshold, 116
Time response, 113, 115
With encoder, 119
Without encoder, 122
Without selection, 124
Software components, 29, 330
SOS, 110
Protective door, 110
Safe Operating Stop, 111
SS1
Basic Functions, 76, 77, 80
Brake ramp monitoring, 83
Braking behavior, 81
Delay, 117
Delay time, 81, 82
Delay time SBR, 81
Enable, 81
Monitoring mode, 81
Principle of operation, 76, 80
Protective door, 87

Safe Stop 1, 76, 77, 80, 82
Safe Stop 1 (Basic Functions), 77
Safe Stop 1 (Extended Functions), 82
SBR, 83
Shutdown speed, 81
Speed controlled, 83
Time and acceleration controlled, 83
Time response, 76, 80, 81
Tolerance, 81
With encoder, 82
With external stop (Basic Functions), 78
With external stop (Extended Functions), 85
With OFF3 (Basic Functions), 77
With OFF3 (Extended Functions), 82
Without encoder, 83
SS1E, 78
SS1 with external stop (Basic Functions), 78
SS2, 100
Braking behavior, 101
Diagnostics, 101
Enable, 101
Principle of operation, 100
Protective door, 100
Safe Stop 2, 100, 102
Select, 101
Speed, 100
Time response, 100, 101
with external stop, 104
SS2E, 104
SS2ESR, 107
SSM
Centrifuge, 127
Restart, 131
Safe Speed Monitor, 127
Time response, 129
With encoder, 129
Standstill monitoring, 81
Startup, 68
Startup protection, 68
STEP 7 Safety, 29
STO
Basic Functions, 87
Internal armature short-circuit, 90
Safe Torque Off, 87
Safe Torque Off (Basic Functions), 87
Select, 87
STO for HLA
Basic Functions, 90
STOP A, 313, 315
STOP B, 315
STOP C, 315
STOP D, 315
STOP E, 315
STOP F, 314, 315
Stop response, 315
Priorities compared to Extended Functions, 318
Priority classes, 318
STOP A, 313
STOP F, 314
Structure of the safety program, 43
Switching operation
Timing, 198, 207
Switching over
SLS level, 116
Switching over the gear ratio
Safe, 186
System variable, (Variable)

T

Telegram
30, 346
31, 346
701, 344
901, 345
902, 345
903, 344
Test stop
Extended Functions, 191
Time and acceleration controlled, 83
Two-channel brake control, 96

U

User safety function, 41

V

Validity check, 72
Variable
$A_STOPESI, 340
$VA_STOPSI, 340