SIEMENS

SIMATIC
Fail-safe function blocks for storage and retrieval machines

TIA Safety Advanced with S7-1500F

Manual

Edition 04/2016
Version v2.0

Safety notes

This manual contains information which you should observe in order to ensure your own personal safety, as well as to avoid material damage. These notices are highlighted in the manual by a warning triangle and marked as follows according to the level of danger:

Safety notes and instructions
is important information, which is of significance for the acceptance and the safety-related use of the product.

Warning
indicates that death, severe injury or substantial property damage can result if proper precautions are not taken.

Caution
indicates that minor personal injury or property damage may result if proper precautions are not taken.

Note
is important information about the product, the way to handle the product or the respective part of the documentation and we wish to especially bring this to your notice.

Qualified personnel

Commissioning and operation of a device are to be carried out by qualified personnel only. Qualified personnel under the terms of the safety instructions contained in this manual are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Proper and intended use

Please observe the following:

Warning
The product may only be used for the applications specified in the catalog and technical description, and only in conjunction with third-party equipment and components if these have been specifically recommended or approved by Siemens.

This product can function correctly and reliably only if it is transported, stored, assembled, and installed correctly, and operated and maintained as recommended.

Trademarks

SIMATIC® is a registered trademark of Siemens AG.
Other designations used in this document may be registered trademarks; the owner's rights may be violated if they are used by third parties for their own purposes.

Siemens AG
Digital Factory
D-Erlangen

Warranty and liability regarding the application examples

The application examples of the software library "ASRM_Failsafe_TS1500_V20" (following “application example”) of Siemens AG are a free of charge service for our customers. The application examples are to be understood as non-binding and they could be incomplete concerning configuration and equipment. The application examples shall not constitute customized solutions, but rather simply provide support for typical questions. Every customer is responsible for appropriate conditions and operations of the products within the valid regulations and has to control the results of the application examples and adapt them individually to its system.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Transfer and reproduction of these application examples or extracts of them are forbidden if not explicit allowed by the Siemens AG.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Contents

List of diagrams

List of tables

1 Storage and retrieval machines and safety functions

This chapter provides a schematic overview of the application conditions of fail-safe function blocks for storage and retrieval machines and the supported hardware platforms.

1.1 General design and structure for safe position sensing

The following components are essentially required for the use of fail-safe blocks (known as RBG blocks in the following) for storage and retrieval machines, depending on the expansion stage and the functions that are used.

- Fail-safe SIMATIC S7 control – STEP7 Safety Advanced
- SINAMICS S120 converters with CU320-2 (from firmware release 4.6), known as SINAMICS S120 in the following, with encoder, e.g. connected to
  - SMC20/SMC30
  - or connected via DRIVE-CLiQ.
- PROFIBUS/PROFINET data transfer between SINAMICS and F-CPU
- F-DQ module to control the brakes
- External mechanical brake and/or motor holding brake
- Signal source for load measurement for overload/slack cable detection, e.g. via F_AI with qualified encoder or two encoders, which mutually check signal plausibility (e.g. weighing cell and motor torque)

A typical hardware configuration looks like this:

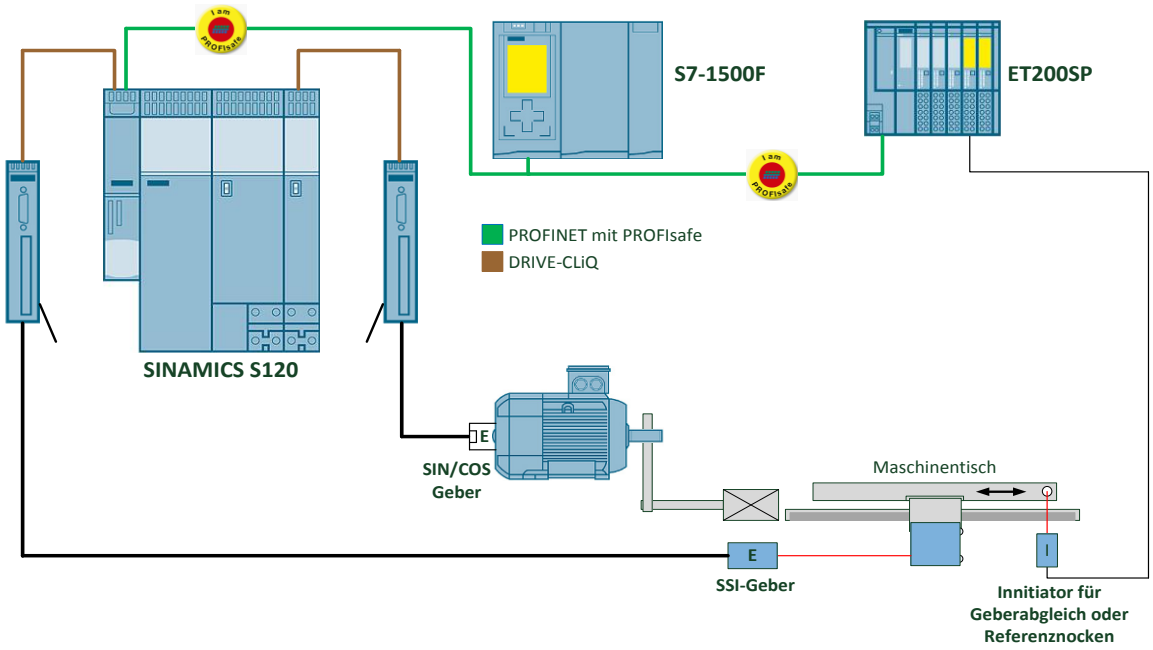


Fig. 1 : Hardware configuration

The package of blocks covers several versions of encoder combinations, also see Table 1. As a consequence, the following scenarios are obtained regarding the required components. These can differ depending on the specific application, however, they must be comparable from a safety-related perspective.

1.2 Encoder combinations and configuration versions that are supported

An overview of the encoder combinations, supported by the storage and retrieval machine blocks, is provided in the following.

1.2.1 Safety-related motor encoder with directly connected, positive locking mechanical system

Sensing:

- Safety-related SIN/COS motor encoder, mounted in a safety-related way and connected via PROFIsafe telegram 902 from SINAMICS S120.
- The absolute position is transferred to the F-CPU, e.g. via a standard telegram from the SINAMICS S120.

In order to achieve a two channel architecture for transferring data to the F-CPU, for example, the EPOS position actual value is transferred via standard telegram. SI additionally determines the motor encoder position actual value - and this is sent to the F-CPU via a safety-related telegram. A safety-related encoder must be used for the motor encoder (safety-related motor encoder, mounted in a safety-related fashion).

As a consequence, the signal flow of the safety function looks like this:

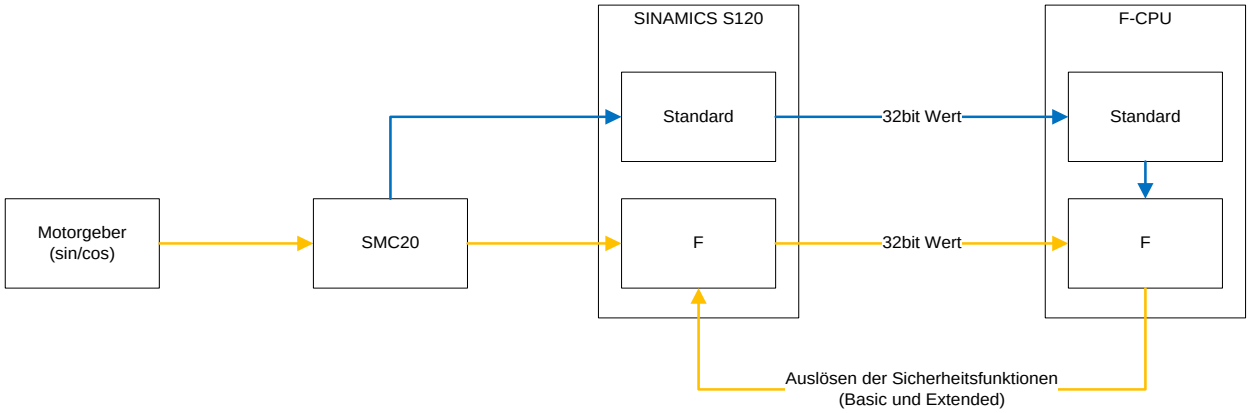


Fig. 2: Version 1: Safety-related motor encoder with directly connected, positive locking mechanical system

Safety note
To identify communication errors, the PROFIsafe monitoring time of the PROFIsafe telegram 902 of the converter being used must be set to the minimum possible for the application; this means that for a communication failure between the control system and converter, the system can be brought into a safe state. If the F-CPU controls external brakes, these can be closed in advance using the QBAD signal of PROFIsafe telegram 902.

1.2.2 Two-encoder system with connection via SINAMICS S120

Sensing:

- The SIN/COS motor encoder is, for example, connected via an SMC20 or a DRIVE-CLiQ interface (SMI) to the SINAMICS S120; the direct measuring system (SSI), e.g. via an SMC30. The EPOS position control system is realized using the direct measuring system.
-

In order to achieve a two channel architecture for transferring data to the F-CPU, for example, the position actual value of EPOS (basic positioner, drive function) is transferred using a standard telegram. SI determines the motor encoder position actual value - and this is sent to the F-CPU via a safety-related telegram. The motor encoder must comply with the requirements of SINAMICS Safety Integrated. Safety-related mounting is not required, as in this case possible errors can be monitored using the crosswise comparison with the second encoder.

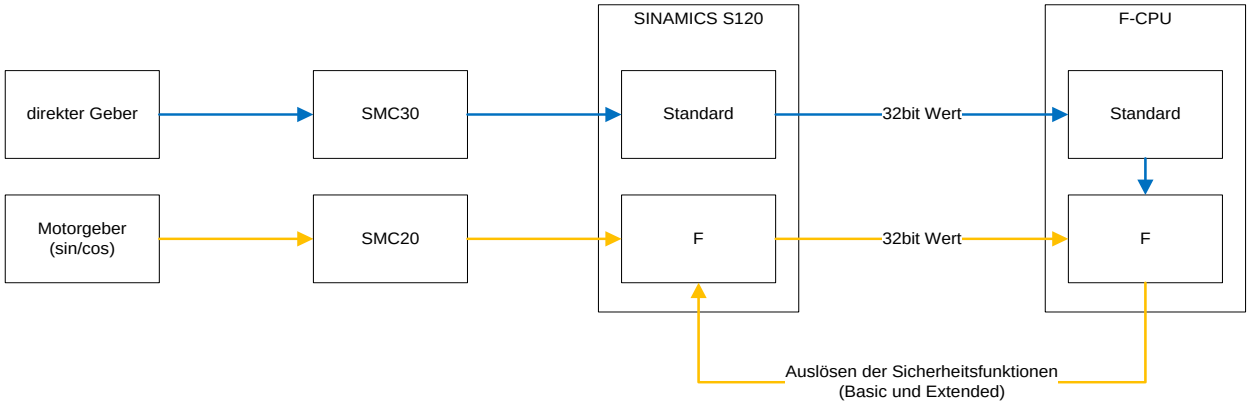


Fig. 3: Version 2: Two-encoder system with connection via SINAMICS S120

1.2.3 Two-encoder system with connection via distributed I/O

Sensing:

a) SIN/COS motor encoder (safety-related mounting is not required) corresponding to the requirements of SINAMICS Safety Integrated (e.g. via SMC20 or DQI/SMI) via PROFIsafe telegram from SINAMICS S120, direct measuring system via standard telegram from SSI module (e.g. TM PosInput 2) to the F-CPU.

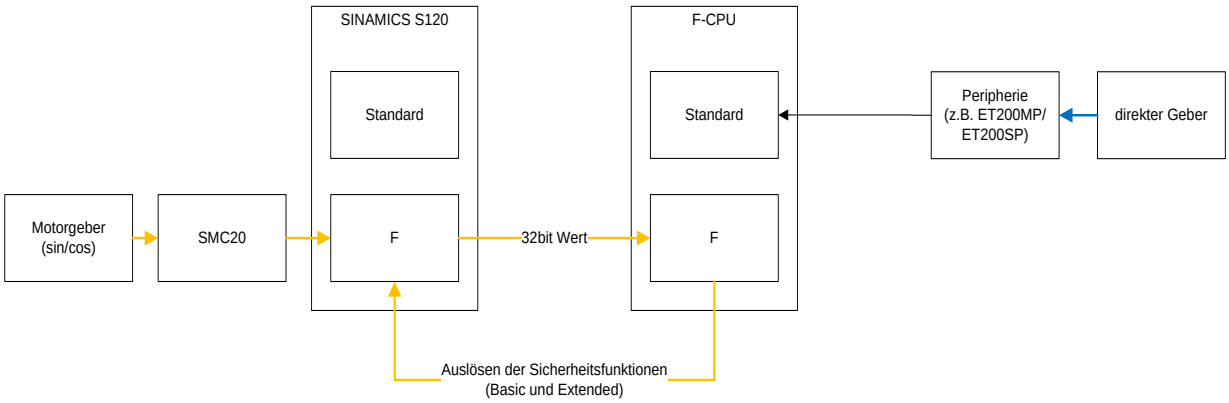


Fig. 4: Version 3 a): Two-encoder system, connection via distributed I/O

b) SIN/COS motor encoder (safety-related mounting is not required) corresponding to the requirements of SINAMICS Safety Integrated (e.g. via SMC20 or DQI/SMI) via PROFIsafe telegram from SINAMICS S120, direct encoder via standard telegram PROFIBUS/PROFINET-capable encoder.

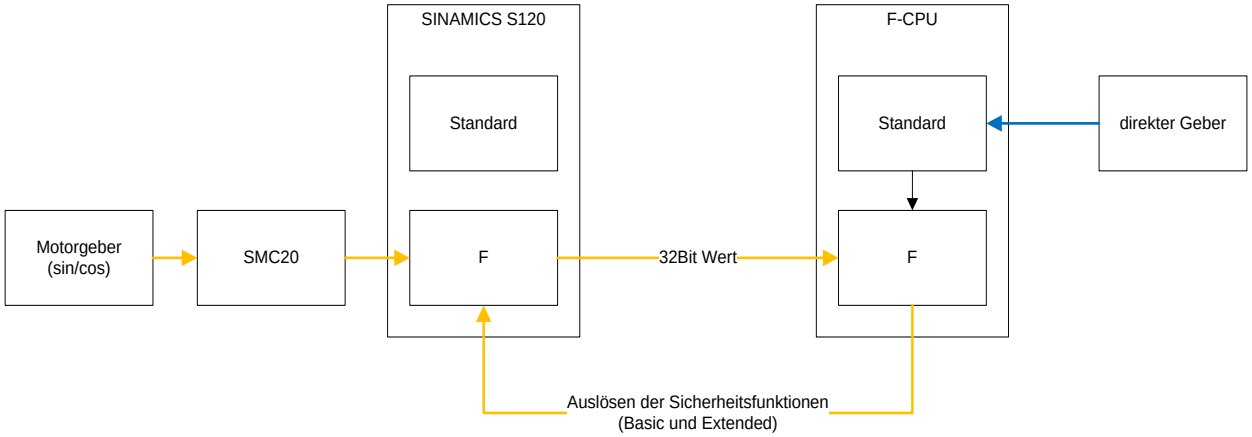


Fig. 5: Version 3 b): Two-encoder system, connection via direct encoder

1.2.4 Three-encoder system

Sensing:

a) SIN/COS motor encoder (safety-related mounting is not required) corresponding to the requirements of SINAMICS Safety Integrated (e.g. via SMC20 or DQI/SMI) via PROFIsafe telegram from SINAMICS S120.
Two direct measuring systems via standard telegram (Fig. 6):

- Position 1 via SINAMICS S120
- Position 2 from the distributed I/O, with secure communication via an F module

Alternatively:

- Position 1 via SINAMICS S120 with secure communication via the PROFIsafe telegram of the converter
- Position 2 from the distributed I/O

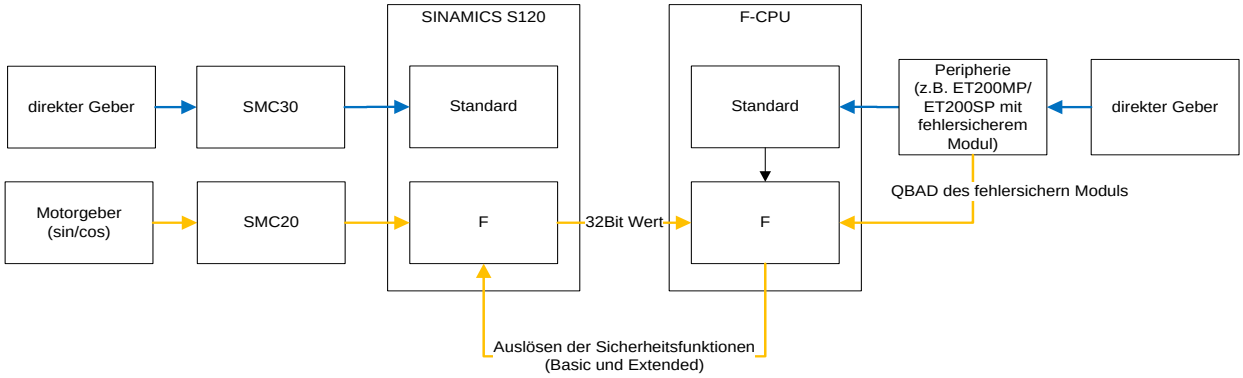


Fig. 6: Version 4 a): Three-encoder system, position encoder via SINAMCS 120 and distributed PLC I/O, secure communication via F module

b) SIN/COS motor encoder corresponding to the requirements of SINAMICS Safety Integrated via PROFIsafe telegram from SINAMICS S120.
Two direct measuring systems via standard telegram:

- Positions 1 and 2 via distributed I/O. One channel with secure communication via an F module

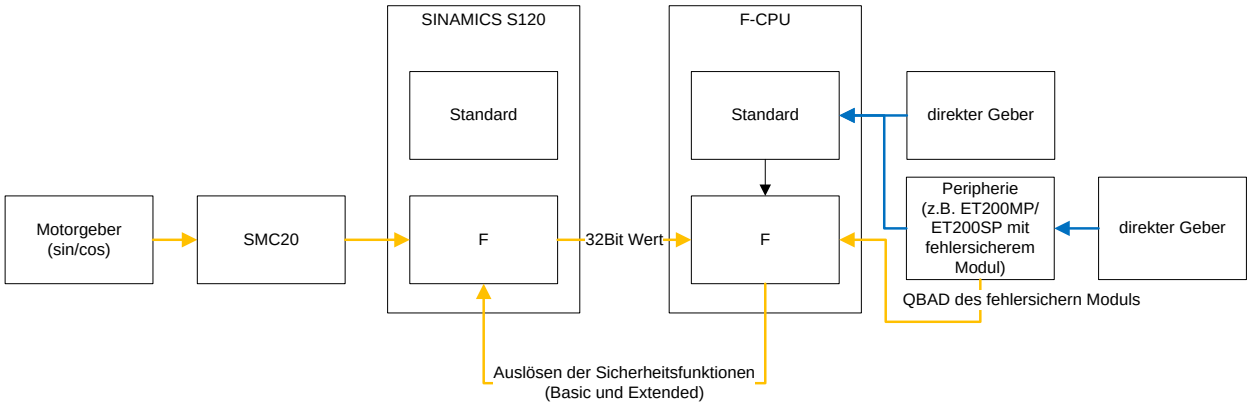


Fig. 7: Version 4 b): Three-encoder system, position encoder via distributed PLC I/O, secure communication via F module

Three-encoder systems are used if a high degree of slip is to be expected, which in turn means that the position cannot be made plausible using the motor encoder. Instead, the position is made plausible by a making a cross comparison between the two direct measuring systems.

Safety note
In order to identify a bus driver that has frozen, i.e. communication between the measuring system and CPU is no longer operational, a fail-safe module is inserted in at least one channel in the station, via which the direct measuring system is

read in. If the communication runs too slowly or completely fails, then the associated F module signals a communication error. This is then evaluated in the safety program and must be used to initiate a stop response.

Safety note
Both direct measuring systems must be installed opposing one another in order to achieve the specified diagnostics coverage.

1.2.5 Summary of the encoder versions

The following table summarizes the encoder combinations that are possible in principle - and their ability to be implemented. POS1, POS2 as well as POS_SI are referenced to the interconnection at the "F_SAFE_POS" block described in more detail in Chapter 3.2. See below for the legend.

A motor encoder (MSSI or MNSI) is always necessary to sense the safety-related position and velocity; this is sensed via the SI part of the drive.

The following encoder combinations should be used depending on the application scenario:

	POS1	POS2	POS_SI
Version 1: Safety-related motor encoder with directly connected, positive locking mechanical system	LM-ST-NS	-	MNSI[1] / MSSI
Version 2: Two-encoder system: Connected via SINAMICS S120.	LM-SMx-NS	-	MNSI / MSSI
Versions 3 a) and b): Two-encoder system: Connected via distributed I/O.	LD-DP-NS	-	MNSI / MSSI
Version 4 a): Three-encoder system. Position encoder via SINAMCS 120 and distributed PLC I/O. Secure communication via an F module.	LM-SMx-NS[2]	LD-DP-KS[2]	MNSI / MSSI
Version 4 b): Three-encoder system. Position encoder via distributed PLC I/O. Secure communication via an F module.	LD-DP-NS[2]	LD-DP-KS[2]	MNSI / MSSI

Table 1: Overview of possible encoder combinations

[1] Not permissible for a single-channel encoder connection to the motor shaft; permissible, if two independent encoders are used, for example, for a double-axis drive. LM-ST-NS via motor encoder 1 and MNSI via motor encoder 2.

[2] Overwriting the process image must be detected using counter-rotating encoders

Legend:
MSSI: Motor encoder, safety-related mounting, via SI F telegram
MNSI: Motor encoder, no safety-related mounting, via SI F telegram
LM-ST-NS: Position actual value from motor encoder via standard 32-bit telegram (from Epos), not safety-related
LD-SMx-NS: Position actual value Epos from direct measuring system via SMC/SMI via standard 32 bit telegram, not safety-related
LD-DP-NS: Position actual value from the direct measuring system via distributed I/O, non safety-related communication (e.g. PROFINET encoder, TM PosInput 2).
LD-DP-KS: Position actual value from the direct measuring system via distributed I/O, safety-related communication using F module on the backplane bus.

To be able to use the safety functions integrated in the drive, for the subsequently described software architecture, it is assumed that a SIN/COS encoder is always used as a motor encoder, and this is a read in using a fail-safe telegram from the safety program. A second encoder is used to check the plausibility, with the design versions described above.

1.2.6 Safety-related parameters of the encoder versions

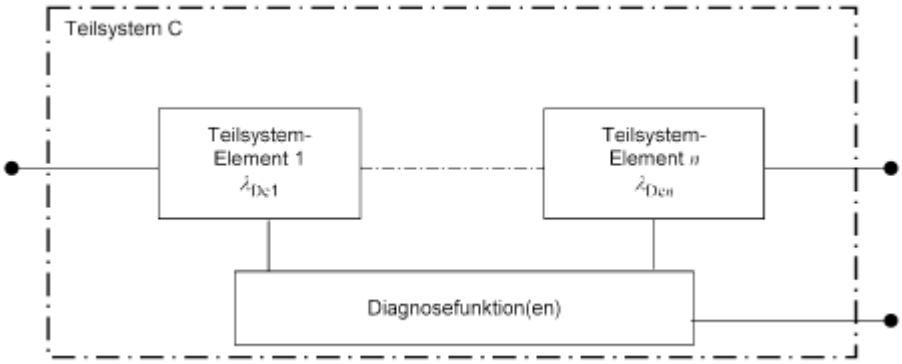
Chapter 1.2.5describes the various encoder versions. The particular version used depends on the application; for the safety-related use of the subsequently described software solution, it is always mandatory to use one of the versions described

As a result of the different encoder versions - and therefore the resulting wide range of hardware versions that can be used - users must determine the safety integrity level achieved of the safety function. To comply with EN 528, as a minimum this must correspond to SIL2/PL_r d over the entire safety function (sense -> evaluate -> respond).

To be able to verify this, in this section, parameters are described which are directly influenced by the software solution for calculating the safety integrity level based on DIN EN 62061. Only the "Sense" block is discussed here. The "Evaluate" block corresponds to a SIMATIC F-CPU with STEP7 Safety Advanced, certified to SIL3/PL e, the "Respond" block corresponds to a SINAMICS S120, certified to SIL2/PL d. The precise parameters of the "Evaluate" and "Respond" blocks should be taken from the corresponding data sheets.

While versions 2, 3a), 3b), 4a) and 4b) satisfy the requirements according to subsystem D, version 1 satisfies the requirements according to subsystem C, as shown in the following:

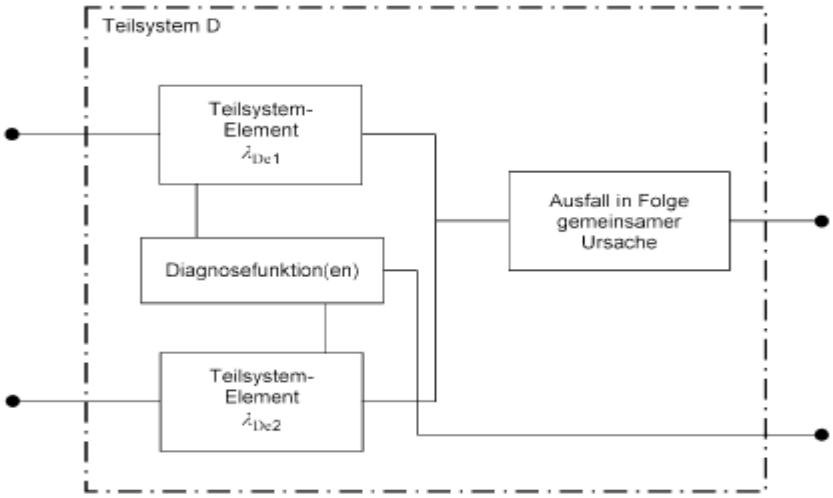
1.2.6.1 Subsystem C according to DIN EN 62061 (Chapter 6.7.8.2.4):



$$\lambda_{DssC} = \lambda_{De1} \cdot (1 - DC_1) + \ldots + \lambda_{Den} \cdot (1 - DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1\,h$$

1.2.6.2 Subsystem D according to DIN EN 62061 (Chapter 6.7.8.2.5):



$$\lambda_{DssD} = (1-\beta)^2 \left\{ \left[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \right] \times T_2/2 + \left[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \right] \times T_1/2 \right\} + \beta \times (\lambda_{De1} \times \lambda_{De2})/2$$

$$PFH_{DssD} = \lambda_{DssD} \times 1\,h$$

	Subsys-tem (SFF/HFT)	SIL CL limit	λ_{Ds1}	λ_{Ds2}	DC_1	DC_2	β	T1	T2
Version 1: Safety-related motor encoder with directly connected, positive locking mechanical system	C ((≥0.99[1]/ 0)	Internal safety function of the SINAMICS S120, certified according to SIL2/PLd							
Version 2: Two-encoder system: Connected via SINAMICS S120.	D (≥0.99[1]/ 1[2])	3[3]	Dependent on the hardware	Dependent on the hardware	99% of the diagnostics implemented in the RBG block library	Corresponding to DC1	0.02 acc. to Table 3: Evaluating common cause faults according to DIN EN 62061 Annex F.1	Dependent on the hardware	Corresponding to the call interval of the safety program
Version 3: Two-encoder system: Connected via distributed I/O.									
Version 4 a): Three-encoder system. Position encoder via SINAMCS 120 and distributed PLC I/O. Secure communication via an F module.									
Version 4 b): Three-encoder system. Position encoder via distributed PLC I/O. Secure communication via an F module.									

Table 2: Parameters according to DIN EN 62061

Comments regarding Table 2: Parameters according to DIN EN 62061:

1) As the diagnostics implemented in the RBG block library identify all hazardous faults, it follows: $\lambda_{DU} \rightarrow 0$. When calculating SFF ($SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$) immediately SFF ≥ 0.99 is obtained.
2) The failure of a subsystem element does not result in the loss of the SRCF, as these faults are detected through a comparison value, as well as through a plausibility check (based on the redundant configuration). This means that HFT = 1 is directly obtained.
3) According to DIN EN 62061 Table 5, it follows that for HFT = 1 and SFF = 1, a SIL CL of 3 is obtained.

Evaluating common cause faults according to DIN EN 62061 Annex F.1 is shown in the following table. In some instances, measures against common cause faults are provided through the solution implemented in the RBG block library - in some instances, users must apply these measures themselves. Measures that users must always apply themselves are appropriately marked in the subsequent table. If additional measures are to be taken, which are shown in gray in the table, then these can improve the CCF factor or β value, on the other hand, measures that are not taken reduce the CCF factor or β value.

Feature	Reference	Points	Reason
Disconnection/isolation			
Are SRECS signal cables for the individual channels separately routed away from other channels at all locations - or adequately protected?	1a	5	
Is the detection of signal transfer errors adequate when using information coding/decoding?	1b	**10**	Provided by the solution implemented in the RBG block library
Are SRECS signal cables and electric power cables routed separately - or adequately protected?	2	5	
Are subsystem elements accommodated in physically separate housings/enclosures if they can contribute to a CCF?	3	**5**	Requirements placed on users when installing sensors
Diversity/redundancy			
Are various electrical/electronic technologies used in the subsystems, for example, in some instances electronics or programmable electronics - and in some instances electromechanical relays?	4	8	
Are elements used in the subsystems that employee different physical principles (for example, sensing elements at a protective door that use mechanical and magnetic sensing techniques).	5	10	
Are elements used in the subsystems with different time responses with reference to functional operation and/or failure types?	6	**10**	Provided by the solution implemented in the RBG block library
Do the subsystem elements have a diagnostics test interval of ≤ 1 min?	7	**10**	Provided by the solution implemented in the RBG block library **Note:** The safety program must be called/run in less than 1 min intervals!
Complexity/design/application			
Are cross connections between channels of the subsystem prevented - with the exception of cross connections that are used for diagnostics?	8	**2**	Provided by the solution implemented in the RBG block library
Assessment/analysis			
Have the results of the failure types and effect analysis been evaluated in order to identify sources of common cause failures - and have these types of sources that have been previously determined been eliminated through an appropriate design?	9	**9**	Provided by the solution implemented in the RBG block library
Are field failures analyzed and incorporated in the design process?	10	9	
Competence/training			
Do the engineers developing the subsystems know the reasons for and the effects of failures originating from a common cause?	11	**4**	Requirements placed on users

Monitoring ambient conditions			
Is it probable that the subsystem elements always operate - without externally monitoring the ambient conditions - within the temperature, humidity, corrosion, dust and vibration range in which they have been tested?	12	**9**	Users must appropriately select the sensors for the application
Is the subsystem immune with respect to the negative influence of electromagnetic fields - up to and including the limits defined in Annex E?	13	**9**	Users must appropriately select the sensors for the application
Result		**68**	**acc. to DIN EN 62061 Table F.2: β = 0.02**

Table 3: Evaluating common cause faults according to DIN EN 62061 Annex F.1

Total number of points	**Factor of the failures resulting from a common cause (β)**
< 35	10 % (0.1)
35 to 65	5 % (0.05)
65 to 85	2 % (0.02)
85 to 100	1 % (0.01)

Table 4: DIN EN 62061 Annex F.2

2 System and software requirements

2.1 General

The fail-safe function blocks for storage and retrieval machines described in the following chapters can be used in conjunction with fail-safe Siemens automation systems

- CPU 1516F-3 PN/DP
- CPU 1517F-3 PN/DP
- CPU 1518F-4 PN/DP

Initially, the safety aspects when creating fail-safe function blocks are discussed before the properties and attributes are explained in detail.

Fail-safe function blocks for storage and retrieval machines have been developed based on individual subfunctions to ensure that these blocks can be used in a modular way.

2.2 Safety requirements

S7-1500F automation systems can satisfy the following safety requirements:

Safety Integrity Levels SIL1 to SIL3 according to
IEC 61508 2nd Edition

2.3 Software

The following *Siemens SIMATIC* software must be installed on the PC/PG for using fail-safe function blocks for storage and retrieval machines:

- SIMATIC STEP 7 Professional V13 SP1 or higher
- SIMATIC STEP 7 Safety Advanced V13 SP1 or higher

as well as for the drive parameterization

- SINAMICS MICROMASTER STARTER V4.4 or higher

The current version - as well as all predecessor versions of the SINAMICS MICROMASTER STARTER - can be downloaded at the following link:

https://support.industry.siemens.com/cs/ww/de/view/26233208

2.4 Safety aspects when creating blocks

The blocks for the safety-related control of storage and retrieval machines were created using certified, fail-safe function blocks in F-FBD and F-LAD. The compiler of the development tool generates coded, fail-safe blocks. These can then be transferred into libraries and called in any arbitrary F-FBs and F-FCs.

Regarding the internal implementation and the software development process employed, the fail-safe function blocks for storage and retrieval machines comply with the requirements according to PLd/SIL2. However, it must be additionally proven that the function blocks from the storage and retrieval machine block library used in the user software are in compliance with the relevant standards regarding their behavior/response and their principle of operation. Generally, this proof can be provided in the form of a function test.
Also due to restrictions regarding the hardware components that can be used, specifically converters/inverters, the safety integrity level that can be achieved using the fail-safe function blocks for storage and retrieval machines is restricted to PLd/SIL2.

The safety-related parameters, required to verify the hardware components, can be taken from Chapter 1.2.6.

2.5 Standards complied with

The RBG block package was developed according to the following standards:

DIN EN 528 (see Chapter 2.5.1)
DIN EN ISO 13849-1
DIN EN ISO 13849-2
DIN EN 62061

2.5.1 Demarcation of DIN EN 528 with respect to the RBG block library

Requirements according to EN528:2008 Table C.2			Covered by the RBG block library
No.	Safety function	Section	
1	Function to monitor access through doors	5.3.3 5.3.4 5.10.3.3 5.10.3.6	No User interconnection required (e.g. Safety Advanced Bibliothek)
2	Stop function	5.3.7	No User interconnection required (e.g. Safety Advanced Bibliothek)
3	Emergency Stop function	5.3.8 5.3.8.1 5.3.8.3	No User interconnection required (e.g. Safety Advanced Bibliothek)
4	Function to stop hoisting motion at the end stops and when the power fails	5.4.1.1 5.4.2 a), b), c)	Yes
5	Function to stop travel motion at the end of the travel section (e.g. the end of the aisle), when the power fails, when collisions occur, if more than one machine is traveling on the same rail system	5.5.1.1 5.5.1.2 5.5.3	Yes
6	Additional brake and velocity reduction function if curved sections must be traveled along with reduced velocity	5.5.1.2 a) 5.5.2	Yes
7	Function of the additional brake and velocity reduction function if the end stops have not been designed so that the machine can approach them with at least 70% of its rated velocity	5.5.1.2 b) 5.5.2	Yes
8	Function to prevent the load and the load handling device from colliding with the rack itself	5.4.6.6 5.6.2 5.6.3 5.6.5 5.6.7 5.6.8.2 5.10.7.1	Yes
9	Load handling device - interlocks	5.6.5 a), b)	Yes
10	Load handling device - interlocks	5.6.5 c)	Yes
11	Load handling device - storage location assigned	5.6.5 d)	No User interconnection required (e.g. Safety Advanced Bibliothek)

Requirements according to EN528:2008 Table C.2			Covered by the RBG block library
No.	Safety function	Section	
12	Load handling device - load position monitoring	5.6.7	No User interconnection required (e.g. Safety Advanced Bibliothek)
13	Function of control devices for dangerous motion (manual control)	5.7.6	No User interconnection required (e.g. Safety Advanced Bibliothek)
14	Interlocking function with transfer equipment	5.8.2 5.8.3 5.8.4	No User interconnection required (e.g. Safety Advanced Bibliothek)
15	Function, which only permits slow velocity, if a person is located on the emergency control station	5.3.7 5.9.4	No User interconnection required (e.g. SLS in the converter)
16	Function to stop the unit if access is required through emergency exits and covers	5.10.3.2 c) 5.10.3.2 e) 5.10.3.4 5.10.6.4	No User interconnection required (e.g. Safety Advanced Bibliothek)
17	Area around equipment - to secure against inadvertent load movement Storage location (rack compartment) sensor	5.10.7.1 a)	No User interconnection required (e.g. Safety Advanced Bibliothek)
18	Area around equipment - to secure against inadvertent load movement Backstop to prevent goods sliding through	5.10.7.1 b)	No User interconnection required (e.g. Safety Advanced Bibliothek)
19	Area around equipment - to secure against inadvertent load movement Backstop to prevent goods sliding through	5.10.7.1 c)	No User interconnection required (e.g. Safety Advanced Bibliothek)

Other sections of EN528:2008 covered by the RBG block library:

- 5.4.3.1 – overload protection
- 5.4.3.2 - slack cable protection

3 Fail-safe function blocks for storage and retrieval machines

3.1 Overview

3.1.1 Safety note

As shown in Chapter 2.5 the fail-safe function blocks for storage and retrieval machines comply with the requirements of EN528:2008.

The safety integrity of the particular safety function is only given with the correct interconnection. This is the reason that the correct interconnection of every fail-safe function block in this library - and the complete functionality of the safety function with the particular application-specific hardware and software - must be validated using the appropriate positive and negative tests.

Initially, these tests should be made in an area of the system that has sufficient clearance to fixed endstops. When tests are being conducted it must be ensured that the system can be safely stopped if an emergency arises.

The tests should be documented, for example, using traces so that limit value violations, shutdown conditions and stopping distances can be clearly identified, and in turn a statement can be made about the correct function of each individual safety function.

3.1.2 Fail-safe blocks

Library "ASRM_Failsafe_TS1500_V20.zal13" includes the following blocks:

F_SAFE_POS	Function block to generate a safety-related position and velocity actual value
F_SLP_MONITOR	Function block for safe position monitoring
F_ENDZONE	Function block to monitor the velocity at the end of the traversing range
F_BRAKE_TEST	Function block to execute a safe brake test in conjunction with drive function *SBT*
F_LOAD_MONITOR	Function block for overload and slack cable detection - with the possibility of testing the measuring equipment
F_SBR_MONITOR	Function block for brake ramp monitoring
F_MIN_MAX	Function for minimum/maximum value selection
F_INTERPOLATION	function to calculate the envelope curve for function block F_ENDZONE
LFAddDInt	Envelope block to intercept an overflow in the double integer counting range for an addition
LFSubDInt	Envelope block to intercept an overflow in the double integer counting range for a subtraction
LFMulDInt	Envelope block to intercept an overflow in the double integer counting range for a multiplication
LFDivDInt	Envelope block to intercept an overflow in the double integer counting range for a division

The following fail-safe blocks of the STEP7 Safety Advanced library are additionally required:

F_TP	Generates a pulse with a specific duration
F_W_BO	Converts a value into the WORD format in 16 data, bool data type
F_BO_W	Converts 16 data, BOOL data type into WORD data type

These blocks are contained under Statements -> Simple statements.

Note
The library blocks listed under SIMATIC STEP 7 Safety Advanced must be set to Version 1.3 before integrating the RBG library. Further, in the Safety Administration, the elements of the system library used must be set to Version 1.3. Otherwise, error messages can be generated when compiling the safety program.

3.1.3 Optional standard blocks

SAFE_REF	Function to safely reference an axis in SINAMICS

3.1.4 Block connections

With fail-safe blocks, a few special characteristics must be taken into account regarding the block connections

Note
Although the EN and ENO connections appear in the FBD/LAD editor, they are neither evaluated nor supplied from the program code of the F-block - and it is not permissible that you interconnect or parameterize them.

3.1.5 Block numbers and signatures

Block number	***Block name***	**SIMATIC STEP 7 Safety Advanced**
		Block signature
FB200	F_SAFE_POS	0xB1AF374D
FB201	F_SLP_MONITOR	0x4306B514
FB202	F_ENDZONE	0x7784F9C7
FB203	F_BRAKE_TEST	0xACB3FBA5
FB204	F_LOAD_MONITOR	0xEE56B413
FB207	F_SBR_MONITOR	0x94B95126
FC206	F_MIN_MAX	0x088D67F5
FC200	F_INTERPOLATION	0x21D8E5C4
FC211	LFAddDInt	0x68F88786
FC212	LFSubDInt	0xA2E3FC8A
FC213	LFMulDInt	0xB06B3E93
FC214	LFDivDInt	0x0302D921

Table 5: Block signatures

In the following chapter, FB/FC numbers are assigned for the blocks to be implemented. When required, these can be adapted to the requirements of the specific machine - i.e. the blocks can be freely renumbered, however it is not permissible that they are renamed.

Note
In the following chapter, FB/FC numbers are assigned for the blocks provided in this library. When required, these can be adapted to the requirements of the specific machine - i.e. the blocks can be freely renumbered. However, it is **not** permissible that the blocks are renamed, as otherwise it is possible that the safety program signature changes.

3.1.6 Integration in cyclic interrupts - F-OB

Safety note
The specific configuration of the cycle time of the safety program is orientated to the requirements arising from the risk assessment for the machine where the blocks are to be used. The user is responsible for correctly carrying out the risk assessment and appropriately configuring the times.

3.1.7 Using instance data blocks/multi-instances

Note
The RBG blocks can be called as multi-instance without any restrictions.

3.1.8 Response times

The response times required can be taken from the risk assessment. This involves a block package that can be universally used. As a consequence, specific response times for the individual safety functions cannot be specified.

Safety note
Depending on the required response time, parameter T_SAMPLE (and therefore the interval in which the safety program is called) as well as POS_SI_T_SAMPLE should be parameterized in the RBG blocks so that they are always less than the maximum permitted response time. It should be taken into account that the hardware components used influence the response time. Using the s7safety_rttplus table it is possible to calculate the response time that is achieved from the sensor to the actuator.

3.1.9 Runtimes

The runtime (execution) values of the fail-safe RBG blocks on the supported F-CPUs, required to calculate the response times, can be taken from Table in Attachment I).

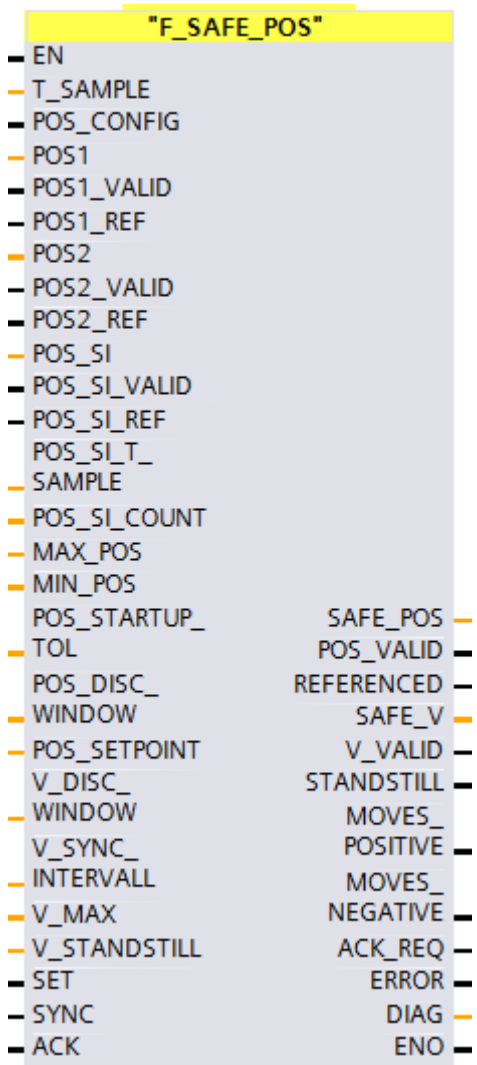
Safety note
It is the users responsibility to interconnect and parameterize the RBG blocks in compliance with the applicable standards. This especially applies to the brake test rates and the overload/slack cable detection - as well as all load and velocity limits.

Safety note
All position limits must be selected so that when violated, the axis can come to a standstill before the end of the traversing range. The value to be parameterized is also dependent on the maximum velocity expected for a specific application - as well as the maximum possible and permitted deceleration.

3.2 F_SAFE_POS

3.2.1 Introduction

The fail-safe function block F_SAFE_POS generates a safety-related position actual value by comparing the discrepancy from two encoders. A velocity is calculated from the motor encoder value, and verified by comparing the position discrepancy using an absolute encoder. Within a time that can be parameterized, the positions between the motor encoder and the second encoder, used to check the plausibility, must not deviate from one another by more than the slip tolerance so that the velocity value can be considered to be safety-related.
The safety-related position and velocity form the basis for other blocks described in this document.
Redundant position sensing is always required if the position cannot be uniquely identified using the Safety Integrated (SI) motor encoder in the drive. This can be the case if the encoder cannot be mounted in a safety-related fashion - or the mechanical system has slip or is subject to elongation (e.g. travel gear with a wheel-rail system or hoisting gear with a cable winch). As a consequence, the position-referred safety functions cannot be used in the SI of the drive. A direct measuring system to monitor the position must then be used. This is realized in the F-CPU via this block. The motor measuring system can then only be used to check the plausibility of the direct position actual value.
For applications where a high slip can be expected, and therefore the motor encoder cannot be used to check the plausibility of the position, then the block provides the possibility of deriving the safety-related position by comparing the discrepancy between two direct measuring systems.



Note

When using this block, then block **F_BO_W (FC 176)** must be available in the block folder. It is not permissible to renumber these! Blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)**, **LFMulDInt (FC 213)** and **LFDivDInt (FC 214)** are also required from this library. These may be renumbered, but not renamed.

3.2.2 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0 and all word variables with W#16#0.

3.2.2.1 Inputs

Name	Data type	Description
T_SAMPLE	DInt	**Block sampling time [ms]** Interval in which the safety program is called
POS_CONFIG	Bool	**Configuration word for encoder interconnection** 1: two direct measuring systems + motor encoder 0: one direct measuring systems + motor encoder
POS1	DInt	**1st direct measuring system - measured value [mm]** Value from the process image
POS1_VALID	Bool	**1st direct measuring system - encoder signal status** 1: Encoder signal valid 0: Encoder fault
POS1_REF	Bool	**1st direct measuring system - encoder referencing status** 1: Encoder referenced 0: Encoder not referenced
POS2	DInt	**2nd direct measuring system - measured value [mm]** Value from the process image
POS2_VALID	Bool	**2nd direct measuring system - encoder signal status** 1: Encoder signal valid 0: Encoder fault
POS2_REF	Bool	**2nd direct measuring system - encoder referencing status** 1: Encoder referenced 0: Encoder not referenced
POS_SI	DInt	**Motor encoder Safety Integrated - measured value [µm]** Value from the process image
POS_SI_VALID	Bool	**Motor encoder Safety Integrated - encoder signal status** 1: Encoder signal valid 0: Encoder fault
POS_SI_REF	Bool	**Motor encoder Safety Integrated - encoder referencing status** 1: Encoder referenced 0: Encoder not referenced
POS_SI_T_SAMPLE	DInt	**SINAMICS Safety Integrated - sampling time [ms]** Sampling time of SI configured in the drive
POS_SI_COUNT	DInt	**SINAMICS Safety Integrated - cycle counter [ms]** Cyclic counter value of telegram 902
MAX_POS	DInt	**Max. permitted position [mm]**
MIN_POS	DInt	**Min permitted position [mm]**

POS_STARTUP_TOL	DInt	**Max. permissible deviation when starting [mm]** When starting, the value of the second encoder, used to check the plausibility (POS_SI or POS2, dependent on POS_CONFIG), may not deviate by more than this value from encoder 1 (POS1)
POS_DISC_WINDOW	DInt	**Max. permissible encoder deviation in operation [mm]** In operation, the value of the second encoder, used to check the plausibility (POS_SI or POS2, dependent on POS_CONFIG), may not deviate by more than this value from encoder 1 (POS1)
POS_SETPOINT	DInt	**Reference position [mm]** With a positive edge at SET, POS1 and the redundant encoder (POS_SI or POS2, depending on POS_CONFIG) are synchronized at this position
V_DISC_WINDOW	DInt	**Tolerance window velocity monitoring [mm]** Max. permissible increase in the encoder deviation [mm] within V_SYNC_INTERVALL for velocity monitoring
V_SYNC_INTERVALL	DInt	**Tracking interval velocity monitoring [ms]**
V_MAX	DInt	**Max. permissible velocity for checking the plausibility [mm/min]**
V_STANDSTILL	DInt	**Velocity limit for standstill detection [mm/min]**
SET	Bool	**Referencing** 0 -> 1: Determine the encoder offset regarding POS_SETPOINT
SYNC	Bool	**Synchronizing** 0 -> 1: The encoder used to check the plausibility (POS_SI or POS2, depending on POS_CONFIG) is synchronized with encoder 1 (POS1)
ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted. Acknowledgment is realized with a positive edge at ACK, and in normal operation has no effect.

3.2.2.2 Outputs

Name	Data type	Description
SAFE_POS	DInt	**Safe position actual value [mm]** Safe position (for all additional blocks in this block package)
POS_VALID	Bool	**Status, position actual value** 1: SAFE_POS was generated in a safety-related fashion
REFERENCED	Bool	**Referencing status** 1: Both encoders are referenced, and the discrepancy between both encoders is within the tolerance window
SAFE_V	DInt	**Safe velocity actual value [mm/min]** Safe velocity (for all additional blocks in this block package)
V_VALID	Bool	**Status, velocity actual value** 1: SAFE_V was generated in a safety-related fashion
STANDSTILL	Bool	**Standstill detection** 1: Actual velocity less than V_STANDSTILL
MOVES_POSITIVE	Bool	**Motion in the positive direction**
MOVES_NEGATIVE	Bool	**Motion in the negative direction**
ACK_REQ	Bool	**Acknowledgment request**

		1: Faults that are no longer active can be acknowledged 0: No acknowledgment requested
ERROR	Bool	**Error** 1: At least one error has been identified 0: No error active
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.2.2.3 Structure of DIAG

Bit	Description	Reset condition
0	Value range violation of input variables	1 <= POS_SI_T_SAMPLE <= 1023
		V_SYNC_INTERVALL > 0
		0 < T_SAMPLE <= 2 * POS_SI_T_SAMPLE
		V_DISC_WINDOW >= 0
		POS_DISC_WINDOW >= 0
		POS_STARTUP_TOL >= 0
1	Ratio between the input variables cannot be represented as integer number	V_SYNC_INTERVAL / T_SAMPLE is an integer number
2	Incorrect reference of the input variables to one another	V_MAX >= V_STANDSTILL
		MAX_POS >= MIN_POS
3	Position when starting not plausible, safety-related referencing required	Reference point approach until positive edge at SET
4	Max. permitted position discrepancy exceeded	Pos. edge at SYNC or SET
5	Minimum one encoder not referenced, safe referencing required	Reference point approach until positive edge at SET
6	Actual position > MAX_POS	Actual position <= MAX_POS and positive edge at ACK
7	Actual position < MIN_POS	Actual position>= MIN_POS and positive edge at ACK
8	Actual velocity > V_MAX	Actual velocity <= V_MAX and positive edge at ACK
9	Max. permissible velocity discrepancy exceeded	Velocity discrepancy <= V_DISC_WINDOW and positive edge at ACK
10	Invalid encoder raw values	POS1 and POS_SI/POS2 supply valid values (VALID = 1) and positive edge at ACK
11	Error for internal calculation	Pos. edge at ACK, if the fault is no longer active
12	Reserved	---
13	Reserved	---
14	Reserved	---
15	Reserved	---

3.2.3 Interrelationship between the assignment of the block inputs and the drive configuration

The safe absolute position actual value from the drive is transferred via PROFIsafe telegram 902 as a 32-bit value with unit µm. To do this, in the converter, the "Extended functions via PROFIsafe" should be set and the safety functions enabled.

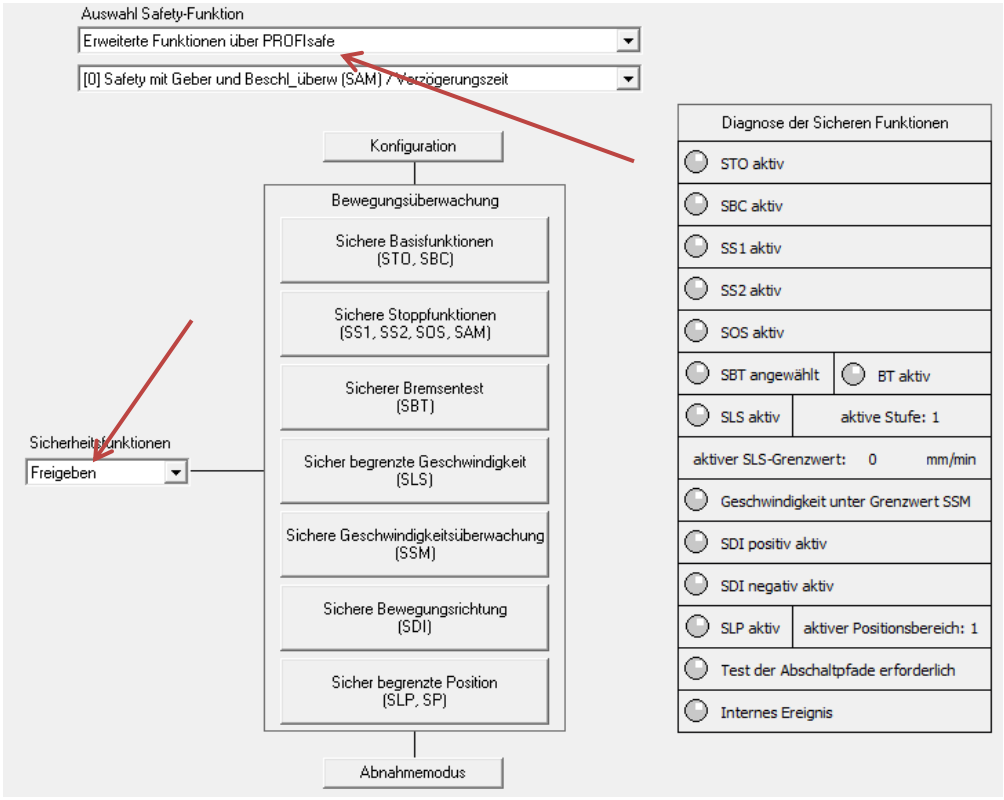


Fig. 8: Setting Safety Integrated in the converter

The drive type must then be set to linear axis; the monitoring clock cycle is subsequently important when parameterizing the block.

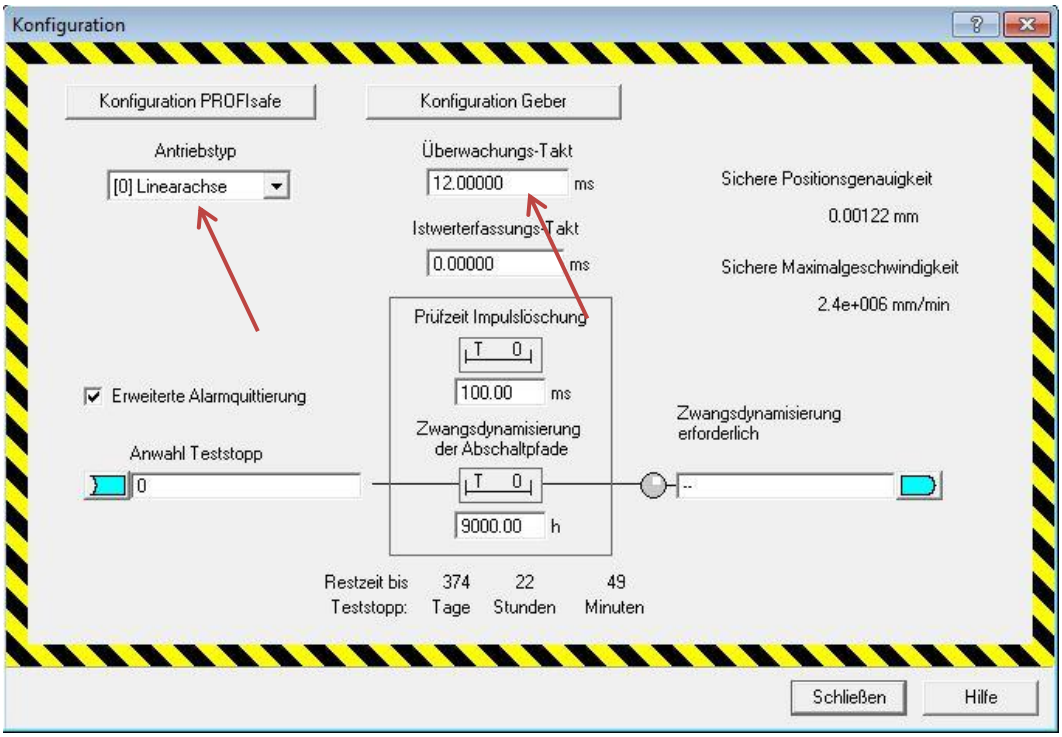


Fig. 9: Configuring Safety Integrated

The encoder parameterization opens by selecting "Encoder configuration". Here, the leadscrew pitch as well as the gearbox stage should be set so that they match the physical mechanical arrangement.

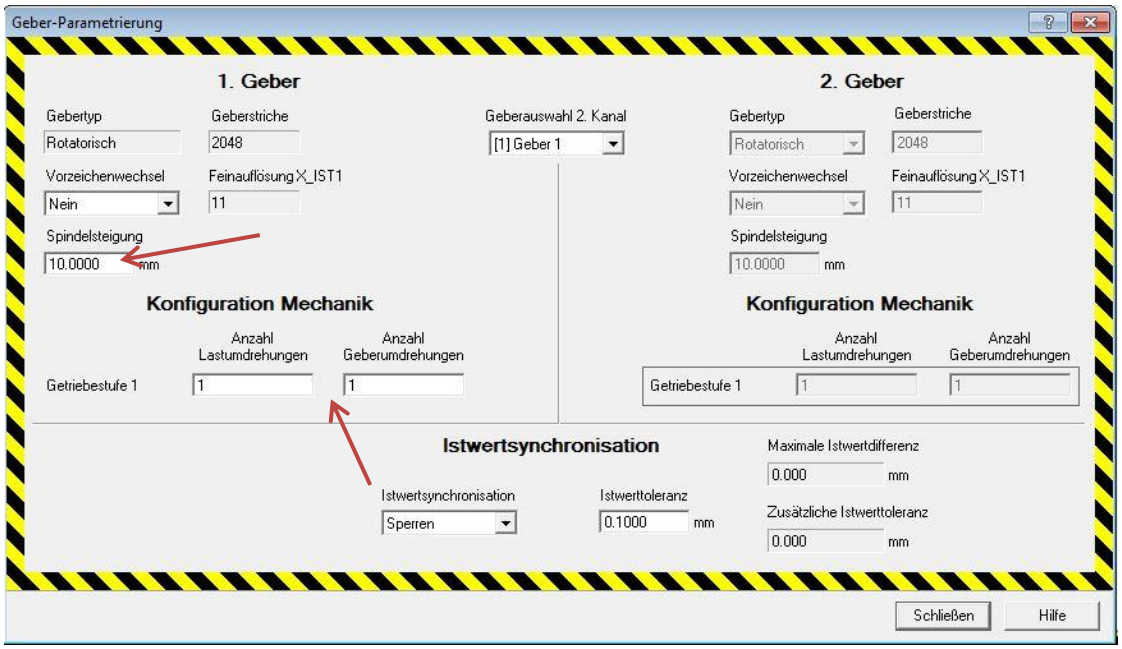


Fig. 10: Encoder parameterization

Now, in the "Safety limited position" safety function, the safe position as well as the safe absolute position must be enabled. The safe position value must be valid - and the axis must be safely referenced. It is not permissible that the SLP function is activated in the drive; block F_SLP_MONITOR in this library is used for monitoring.

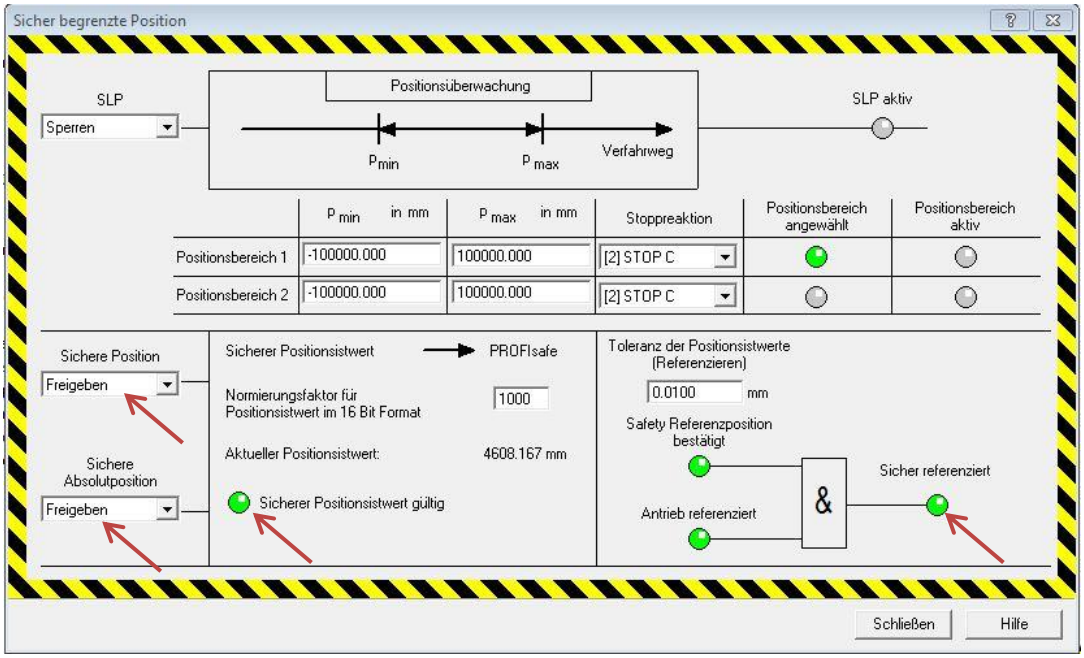


Fig. 11: Safe position transfer

Configuring the encoder at the block

The safe absolute position actual value from the drive is transferred via PROFIsafe telegram as a 32-bit value with unit [µm]. The encoder value of the first direct encoder is interconnected in [mm] at POS1 - or, if a second direct encoder is available, its encoder value is interconnected at POS2 in [mm] - and POS_CONFIG is a parameterized to 1.

The plausibility of the calculated velocity from POS_SI is always checked using the encoder interconnected at POS1. For POS_CONFIG = 0, the plausibility of the position from POS1 is checked using the encoder interconnected at POS_SI; for POS_CONFIG = 1, the plausibility of POS1 with respect to POS2 is checked.

Note
POS1 and POS2 expect opposing values!

Note
The encoder values at POS_SI, POS1 and POS2 must always be positive

Safety note
Encoder value POS_SI moves in the range -737280mm up to +737280mm, for block F_SAFE_POS, only the value range 0 mm - +737280mm is permissible. POS_SI can, using block SAFE_REF (Chapter3.11), be safely referenced to a defined position value. If POS_SI assumes values higher than +737280mm, then a rollover occurs. As a result of the high value change and the resulting discrepancy, enable signals are reset - and the system initiates the shutdown response interconnected by the user. This is the reason that POS_SI should be monitored for excessively high values.

Safety note
The signals interconnected at POS1 and POS2 must come from two independent sources. If a signal source is connected at both inputs, then for example, unplausible values of this channel cannot be detected. As a consequence, the safety integrity of the block is no longer guaranteed.

3.2.4 Principle of operation

3.2.4.1 Parameterization

1. The position-defining encoder in [mm] is interconnected to POS1.
2. At input POS1_VALID, users have the option of interconnecting possibly available additional validity queries of the position value (e.g. error bit from the module). The input must be permanently set to TRUE if no information of this type is available.
3. The information "Position actual value referenced" is interconnected by the user at input POS1_REF.
4. The sampling time of the block, e.g. the configured call interval of F-OB, which calls the safety program, is parameterized at input T_SAMPLE.
5. The sampling time of SI in the drive is parameterized at POS_SI_T_SAMPLE - and POS_SI_COUNT must be interconnected with the counter value from telegram 902.
6. T_SAMPLE is relevant for the calculations carried out in the block.
7. The safe absolute position actual value of the motor encoder from telegram 902 is interconnected at input POS_SI.
8. For applications with a high slip, users have the option of interconnecting a second direct encoder in [mm] at POS2.
9. Using POS_CONFIG, users also have the option of switching over between operation with one and two direct encoders. If the input is set, then the block is in the mode for two direct encoders, otherwise it is in the mode for one direct encoder
10. The significance of inputs POS2_VALID and POS2_ REF or POS_SI_REF and POS_SI _VALID, is equivalent to the corresponding inputs for POS1.

When parameterizing, it must be ensured that the following relationships can be represented as integer multiples:

V_SYNC_INTERVALL / T_SAMPLE

Further, the following relationship between the input variables must apply:

V_MAX >= V_STANDSTILL

MAX_POS >= MIN_POS

Sampling rates

To calculate the velocity, as time base, the clock cycle of the F_SAFE_POS block on the CPU (T_SAMPLE, normally the interval in which the safety program is called) is not used, but the SI clock cycle in the drive (POS_SI_T_SAMPLE). In order to avoid an inadmissibly high subsampling, the relationship T_SAMPLE <= 2x POS_SI_T_SAMPLE must be guaranteed.

The permissible value ranges of the individual inputs should be taken from the table describing the inputs.

If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Note

The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, it is not possible to reparameterize the system while it is in operation. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.2.4.2 Starting behavior

11. After a CPU restart, outputs V_VALID, POS_VALID and REFERENCED initially output a 0 signal.
12. V_VALID is set to 1 after acknowledging using a positive edge at ACK.
13. In order to execute a reference point approach, POS_VALID must be set to 1, by calibrating/synchronizing both encoders using a positive edge at SYNC. The position value as such is now valid, and can be used to make relative position statements; however, it is still not permissible to make a safe absolute evaluation of the position as long as REFERENCED outputs a 0 signal.
14. If the axis is at the reference point defined using input POS_SETPOINT, then using a positive edge at SET, the block is referenced - and REFERENCED changes to 1. The position value output at SAFE_POS can now be used as absolute position.

3.2.4.3 Position actual value

15. When all of the relevant encoders return (POS_x_VALID), if the calculated position value from POS1 deviates by more than POS_STARTUP_TOL from the internally saved reference value (which was saved when POS_x_VALID went to zero), then REFERENCED is reset to 0, ERROR issues a 1 signal and DIAG bit 3 is set.
16. If, in operation, the positions calculated from POS1 and POS_SI differ by more than the value parameterized at input POS_DISC_WINDOW - and if POS_CONFIG is not set, then POS_VALID is set to 0, ERROR issues a 1 signal and DIAG bit 4 is set.
17. If POS_CONFIG =1, and if in operation the positions calculated from POS1 and POS_2I differ by more than the value parameterized at input POS_DISC_WINDOW, then POS_VALID is set to 0, ERROR issues a 1 signal and DIAG bit 4 is set.
18. If none of these errors occurs, and at POS1_VALID and at POS_SI_VALID a 1 signal is available - or for POS_CONFIG = 1, POS2_VALID has a 1 signal, then the block supplies a 1 signal at output POS_VALID to indicate that SAFE_POS is valid.
19. If SAFE_POS exceeds the value of MAX_POS, then ERROR and DIAG bit 6 are set. POS_VALID is withdrawn.
20. If SAFE_POS falls below the value of MIN_POS, then ERROR and DIAG bit 7 are set. POS_VALID is withdrawn.
21. The block itself does not provide any retraction logic; using a suitable logic interconnection, the user must externally ensure that for REFERENCED = 0 the axis can only be traversed with safely reduced speed.

Warning

As long as REFERENCED supplies a 0 signal, the position can only be used for relative position information, an absolute evaluation is only permissible when REFERENCED = 1.

For REFERENCED = 0, axes should only traverse with a safely reduced speed in applications.

Warning

As long as POS_VALID supplies a 0 signal, the position actual value is not generated as safety-related value. For a falling edge, a stop response should be initiated in the application.

3.2.4.4 Velocity actual value

22. The safe velocity, calculated by the block from the absolute position actual value of the motor encoder interconnected at POS_SI, is output at SAFE_V.
23. If SAFE_V falls below the value parameterized at V_STANDSTILL, then at output STANDSTILL, standstill is signaled using a 1 signal.
24. If SAFE_V is greater than/equal to V_STANDSTILL, then a 1 signal is output at MOVES_POSITIVE if SAFE_POS assumes higher values over time - or a 1 signal is output at MOVE_NEGATIVE if SAFE_POS assumes lower values over time.
25. If SAFE_V exceeds the value parameterized at V_MAX, then ERROR is set to 1 and DIAG bit 8 is set. V_VALID is reset to 0.
26. At input V_DISC_WINDOW it is parameterized to what extent (specified in mm) the values of POS1 and POS_SI can, within V_SYNC_INTERVALL, drift apart without resulting in a velocity error.
27. After the time parameterized at V_SYNC_INTERVALL, the discrepancy between the relative positions POS1 and POS_SI for the velocity monitoring, which has accumulated in the block, is eliminated in order to permit tolerance for slip.
    If the drift between POS1 and POS_SI exceeds the value parameterized at V_DISC_WINDOW, then ERROR and DIAG bit 9 are set. V_VALID is reset to 0.

Warning

As long as V_VALID supplies a 0 signal, the velocity actual value is not generated as safety-related value.

3.2.4.5 Referencing

28. With a positive edge at SET, inside the block, a safe adjustment is carried out where, for both raw position values, a separate position offset relative to the value specified at input POS_SETPOINT is determined and saved. Output REFERENCED is set if referencing was successful.
29. For successful referencing, both encoder actual values must be valid and referenced (POS1_VALID/REF & POS_SI_VALID/REF = 1 (for POS_CONFIG = 0) or POS1_VALID/REF & POS2_VALID/REF = 1 (for POS_CONFIG = 1)
30. REFERENCED is then set with a rising edge at input SET and the offsets internally saved.
31. REFERENCED is withdrawn soon as the position tolerance window POS_DISC_WINDOW is violated, or as soon as an encoder is not referenced.
32. ERROR as well as DIAG bit 5 are set to 1 if the conditions listed above are not satisfied.

After an encoder fault, the block is in a position to reproduce SAFE_POS without requiring a reference point approach. If POS1_VALID and POS_SI_VALID or POS2_VALID (depending on POS_CONFIG = 0) have a rising edge, then inside the block, the position is reproduced according to the following schematic:

33. A check is made as to whether POS1, taking into account the POS_STARTUP_TOL, corresponds to reference value X_{REF}. Reference value X_{REF} was previously saved with a falling edge at POS_VALID and in the safely referenced mode (REFERENCED was at this instant in time, set). The fact that when POS1 is reactivated it corresponds to the internally saved reference value X_{REF} confirms and verifies the adjustment. The relative encoder is then automatically synchronized.

34. REFERENCED is withdrawn if one of the encoders is not referenced, or the position tolerance is violated.
35. If POS_STARTUP_TOL was exceeded, in order to set REFERENCED back to 1, a reference point approach must be carried out as described under Point 28.

Note
An encoder fault must always lead to input signal POS1_VALID or POS_SI_VALID/POS2_VALID being withdrawn. As a consequence, the safe actual value is immediately declared as being invalid, and the position tolerance monitoring hidden. As a consequence, an encoder fault does not immediately lead to the loss of the safe reference, and the safe position can be reproduced after the encoder returns.

3.2.4.6 Synchronizing the encoders

36. Both encoders are synchronized with a positive edge at SYNC, i.e. the discrepancy that has accumulated between the two encoders is brought to 0. To do this, both encoder actual values must be valid.

Warning
Cyclic synchronization means that the two-channel structure is bypassed for the position actual value processing, and is therefore not permissible. Whether synchronization is permissible, depends on the specific application - and the user is responsible in ensuring that the appropriate correct logic interconnection is used.

3.2.4.7 Acknowledging errors

37. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors. As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.

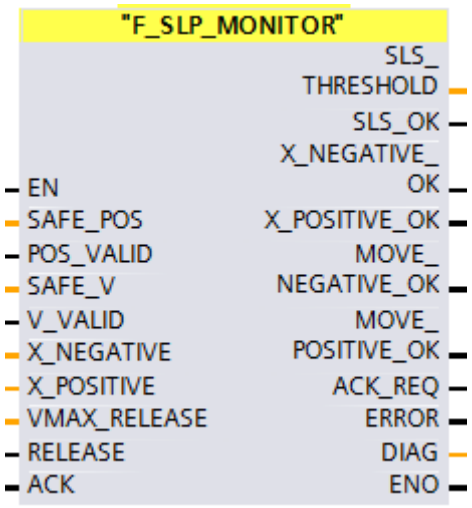
3.2.5 Additional diagnostic options

To optimize the system response, the currently active position and velocity discrepancy from the instance DB of the block can be read out for diagnostic purposes.
For the position discrepancy, static variable "pos_delta" - for the velocity discrepancy, static variable "v_discrepancy_abs".

3.3 F_SLP_MONITOR

3.3.1 Introduction

The fail-safe function block F_SLP_MONITOR is used to safely monitor the end stops of a travel range. The block signals if the defined traversing range is exited. Depending on the user interconnection, a stop response can be initiated.
The block has retraction logic, so that the storage and retrieval machine can be returned to the permitted travel range. With this function, the machine can be moved away from the end stop with a safe velocity parameterized at the block. The block provides two signals to control the SDI function in the drive, so that traversing back towards the end stop is inhibited.



Note

When using this block, then block **F_BO_W (FC 176)** must be available in the block folder. It is not permissible to renumber this!

3.3.2 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0 and all word variables with W#16#0.

3.3.2.1 Inputs

Name	Data type	Description
SAFE_POS	DInt	**Safe position actual value [mm]** is supplied from block F_SAFE_POS.
POS_VALID	Bool	**Actual position valid** is supplied from block F_SAFE_POS. 1: Position is plausible 0: Position is not plausible, i.e. the discrepancy between the two encoders is outside the tolerance window. If a 0 signal is available here, then DIAG bit No. 5 is set.
SAFE_V	DInt	**Safe velocity actual value [mm/min]** is supplied from block F_SAFE_POS.
V_VALID	Bool	**Actual velocity valid** is supplied from block F_SAFE_POS. 1: Velocity is plausible 0: Velocity is not plausible, i.e. the increase of the deviation between the two encoders over time is outside the tolerance window. If a 0 signal is available here, and the block is in the retraction mode, then DIAG bit No. 6 is set.
X_NEGATIVE	DInt	**Minimum permitted position [mm]**

		If the value at input SAFE_POS falls below this limit value, then output X_NEGATIVE_OK is reset
X_POSITIVE	DInt	**Maximum permitted position [mm]** If the value at input SAFE_POS exceeds this limit value, then output X_POSITIVE_OK is reset
VMAX_RELEASE	DInt	**Retraction velocity [mm/min]** If the block is in the retraction mode, then this value is output at SLS_THRESHOLD. VMAX_RELEASE must be parameterized in the range 1-2147483647. Otherwise, DIAG bit No. 4 is set
RELEASE	Bool	**Retracting** If the permissible position range was exited, then the machine can be traversed back to the permissible position range using this input with the velocity parameterized at VMAX_RELEASE. Retraction motion is immediately stopped as soon as this input has a 0 signal.
ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted. Acknowledgment is only realized with a positive edge at ACK - and in fault-free (normal) operation it has no effect.

3.3.2.2 Outputs

Name	Data type	Description
SLS_THRESHOLD	DInt	**SLS limit [mm/min]** The presently maximum permissible traversing velocity is output here. This is 2147483647 in normal operation; if the user is retracting the machine, then VMAX_RELEASE is output here. If VMAX_RELEASE has been parameterized <= 0, then an equivalent value of 1 is output here.
SLS_OK	Bool	**SLS limit status** 1: SAFE_V is less than/equal to SLS_THRESHOLD 0: SAFE_V has exceeded the value of SLS_THRESHOLD. If this output changes to 0, then a stop response should be initiated.
X_NEGATIVE_OK	Bool	**Status minimum position** 1: SAFE_POS is greater than/equal to X_NEGATIVE 0: SAFE_POS has fallen below the value of X_NEGATIVE. If this output changes to 0, then a stop response should be initiated.
X_POSITIVE_OK	Bool	**Status maximum position** 1: SAFE_POS is less than/equal to X_POSITIVE 0: SAFE_POS has exceeded the value of X_POSITIVE. If this output changes to 0, then a stop response should be initiated.
MOVE_NEGATIVE_OK	Bool	**Negative motion permitted** If a 0 signal is available at this output, then it is not permissible that the machine continues to move in the negative direction. The output is then set to 0 as soon as SAFE_POS assumes values lower than X_NEGATIVE. If SAFE_POS again lies above X_NEGATIVE, then after acknowledgment, the output is set again.
MOVE_POSITIVE_OK	Bool	**Positive motion permitted** If a 0 signal is available at this output, then it is not permissible that the machine continues to move in the positive direction. The output is then set to 0 as soon as SAFE_POS assumes values higher than X_POSITIVE. If SAFE_POS again lies below X_POSITIVE, then after acknowledgment, the output is set again.
ACK_REQ	Bool	**Acknowledgment request** If a fault has occurred, however it is no longer active, and

		can therefore be acknowledged, then the block indicates this using a 1 signal at ACK_REQ.
ERROR	Bool	**Error** This output is set if the block has been incorrectly parameterized, or if the block in operation detects a potentially dangerous combination of input signals. The output remains set until an error is no longer active and has been acknowledged.
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.3.2.3 Structure of DIAG

Bit No.	Description	Reset condition
0	Lower end stop was fallen below	While retracting, SAFE_POS >= X_NEGATIVE and positive edge at ACK
1	Upper end stop was exceeded	While retracting, SAFE_POS <= X_POSITIVE and positive edge at ACK
2	Actual velocity higher than the retraction velocity	SAFE_V <= SLS_THRESHOLD and positive edge at ACK
3	Reserved	---
4	Parameterizing error, retraction velocity	0 < VMAX_RELEASE <= 2147483647 parameterized
5	Actual position invalid	Actual position valid again
6	Actual velocity invalid	Actual velocity valid again
7	Reserved	---
8	Reserved	---
9	Reserved	---
10	Reserved	---
11	Reserved	---
12	Reserved	---
13	Reserved	---
14	Reserved	---
15	Reserved	---

3.3.3 Principle of operation

3.3.3.1 Parameterization

1. At input SAFE_POS, the user must interconnect the safe position actual value of the system to be monitored - and at input POS_VALID its validity AND'ed with the valid reference (REFERENCED). Block "F_SAFE_POS" (Chapter 3.2) provides the three signals as output.
2. The same applies to inputs SAFE_V and V_VALID, which refer to the safe actual velocity.
3. The permitted travel range is parameterized by specifying the upper and lower limits at inputs X_POSITIVE and X_NEGATIVE.
4. VMAX_RELEASE must lie in the range 1 – 2147483647. The block identifies if values less than 1 or values higher than 2147483647 are parameterized and DIAG bit 4 is set. ERROR changes to 1.

If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Note
The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, it is not possible to reparameterize the system while it is in operation. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.3.3.2 Position monitoring

5. As long as the position actual value is valid, and is in the permitted range, the block does not signal an error; this means that outputs ERROR and DIAG supply a 0 signal.
6. If, although the position actual value is in the permitted range, but via POS_VALID = 0 is declared invalid, then an error code is also output to DIAG. Until acknowledged, ERROR remains in the actual state - assuming that no additional faults occur as a result of another active monitoring function. All other outputs maintain their actual state until acknowledgment or RELEASE is deselected. In this case, DIAG bit No. 5 is set
7. As soon as POS_VALID changes back to 1, DIAG bit No. 5 again has a 0 signal.
8. As soon as SAFE_POS is outside the parameterized travel range, depending on the direction in which this was exited, either X_POSITIVE_OK or X_NEGATIVE_OK is set to 0. A stop response should then be initiated in the drive by the user interconnection.
9. In addition, DIAG bit No. 0 for falling below the lower end stop - or DIAG bit No. 1 for exceeding the upper end stop is set. ERROR is set to 1.

Safety note
Block F_SAFE_POS provides a 0 signal at POS_VALID via output ERROR = 1. However, when POS_VALID goes to zero, a stop response must be initiated in the drive via a user interconnection. All other blocks indicate the status using an error code; however in order to avoid being confronted by a flood of messages/signals, in this case ERROR is not again set to a 1 signal. This means that the end stops are no longer monitored. Active faults for the end position monitoring can be immediately acknowledged X_NEGATIVE_OK, X_POSITIVE_OK and SLS_OK are set again.
If a 1 signal is again available at POS_VALID, then the associated DIAG bit 5 is reset, and end position monitoring is resumed.

3.3.3.3 Retracting

10. To traverse from the end stop back into the permitted travel range, the retraction function of the block can be activated using a positive edge at RELEASE. The velocity parameterized at VMAX_RELEASE is then output at SLS_THRESHOLD, and depending on the direction of travel when the end zone was violated, either MOVE_POSITIVE_OK or MOVE_NEGATIVE_OK is set to 0 in order to prevent further motion towards this end zone.

MOVE_POSITIVE_OK = 0 inhibits motion in the positive direction, MOVE_NEGATIVE_OK = 0 inhibits motion in the negative direction.

Note
The signal for RELEASE must be generated in a safety-related fashion, e.g. by using a key-operated switch or similar device.

11. In order to facilitate retraction, when RELEASE is selected, X_POSITIVE_OK or X_NEGATIVE_OK is reset to 1; the stop response of the drive should be deselected using a suitable user interconnection.
12. If, during retraction, the value of SAFE_V exceeds the value of VMAX_RELEASE, then SLS_OK changes to 0 and DIAG bit 2 is set.
13. A velocity fault can always be acknowledged if the actual velocity SAFE_V is again below SLS_THRESHOLD.
14. As soon as SAFE_POS is back in the parameterized permissible range, after acknowledgment, the machine can again be traversed with the full velocity, i.e. SLS_THRESHOLD is reset to maximum velocity (maximum possible DINT value = 2147483647).
15. If, when retracting, the removal and storage machine should traverse to the opposite end stop, then the block behaves in just the same way as the corresponding end range violation in normal operation. This means that it again changes X_POSITIVE_OK or X_NEGATIVE_OK to 0, which means motion is only possible in the direction away from the end stop.
16. If V_VALID = 0 while SAFE_POS lies outside the parameterized travel range, then the retraction velocity can no longer be monitored in a safely-related way. Therefore, selection using RELEASE = 1 has no effect, and retraction motion is stopped.
17. To exit this state, V_VALID must first be again set to a 1 signal using F_SAFE_POS by acknowledging.
18. Retraction can then be continued. Alternatively, the initial state can be restored by deselecting RELEASE and subsequent acknowledgment. If SAFE_POS still lies outside the parameterized traversing range, then the system responds corresponding to Point 9.

Safety note
Block F_SAFE_POS signals a 0 signal at V_VALID via output ERROR = 1. However, when V_VALID goes to zero, a stop response must be initiated in the drive via a user interconnection. All other blocks indicate the status using an error code; however in order to avoid being confronted by a flood of messages/signals, in this case ERROR is not again set to a 1 signal. This means that the retraction velocity is no longer monitored. Active faults of the retraction monitoring can be immediately acknowledged, SLS_OK is again set. Retraction via RELEASE can be exited normally; MOVE_POSITIVE_OK and MOVE_NEGATIVE_OK are again set. If, at this instant in time, the axis is not in a valid position range, then X_NEGATIVE_OK or X_POSITIVE_OK is withdrawn and ERROR is set.
If a 1 signal is again available at V_VALID, then the associated DIAG bit 6 is reset, and if retraction motion is pending, then this is again monitored.

Safety note
The parameterization of input V_MAX_RELEASE must be adapted according to the permissible safely reduced velocity, derived from the application-specific risk assessment.

Safety note

The interconnection of output MOVE_POSITIVE_OK must match the selection of drive function SDI for a positive direction. For MOVE_POSITIVE_OK = 0, motion in the positive direction must no longer be possible.

The same is true when interconnecting output MOVE_NEGATIVE_OK and inhibiting the negative direction of motion.

It is absolutely crucial that the block outputs are interconnected with the correct signals to control the drive.

Otherwise, inadmissible motion towards the end stops is possible, which cannot be identified internally in the block.

3.3.3.4 Acknowledging errors

19. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors. As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.

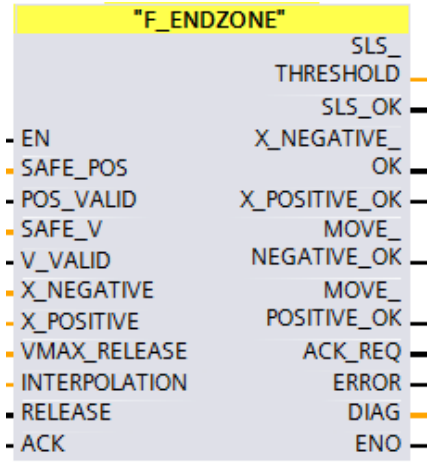
3.4 F_ENDZONE

3.4.1 Introduction

The fail-safe function block F_ENDZONE is used to safely monitor the end stops of a traversing range - or the collision monitoring of two systems. If the system that is being monitored approaches the parameterizable positive or negative end stop, then its maximum permissible velocity, dependent on the actual position, is limited according to a parameterizable curve until standstill is reached. This curve is parameterized using 17 interpolation points; the system linearly interpolates the curve between these points.

If the storage and retrieval machine traverses beyond the end stop, or the maximum permissible velocity is exceeded, then the block signals this situation. Depending on the user interconnection, a stop response can be initiated.

The block has retraction logic, so that the storage and retrieval machine can be returned to the permitted traversing range if it passes and end stop. With this function, the machine can be moved away from the end stop with a low safe velocity parameterized at the block. The block provides two signals to control the SDI function in the drive, so that traversing back towards the end stop is inhibited.



Note

When using this block, then block **F_BO_W (FC 176)** must be available in the block folder. It is not permissible to renumber this! In addition, blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)** and **F_INTERPOLATION (FC 200)** are required from this library. These may be renumbered, but not renamed.

In addition, F-UDT **INTERP** is required from this library.

3.4.2 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0 and all word variables with W#16#0.

3.4.2.1 Inputs

Name	Data type	Description
SAFE_POS	DInt	**Safe position actual value [mm]** is supplied from block F_SAFE_POS.
POS_VALID	Bool	**Actual position valid** is supplied from block F_SAFE_POS. 1: Position is plausible 0: Position is not plausible, i.e. the discrepancy between the two encoders is outside the tolerance window.
SAFE_V	DInt	**Safe velocity actual value [mm/min]**

		is supplied from block F_SAFE_POS.
V_VALID	Bool	**Actual velocity valid** is supplied from block F_SAFE_POS. 1: Velocity is plausible 0: Velocity is not plausible, i.e. the increase of the deviation between the two encoders over time is outside the tolerance window.
X_NEGATIVE	DInt	**Minimum permitted position [mm]** If the value at input SAFE_POS falls below this limit value, then output X_NEGATIVE_OK is reset
X_POSITIVE	DInt	**Maximum permitted position [mm]** If the value at input SAFE_POS exceeds this limit value, then output X_POSITIVE_OK is reset
VMAX_RELEASE	DInt	**Retraction velocity [mm/min]** If the block is in the retraction mode, then this value is output at SLS_THRESHOLD. VMAX_RELEASE must be parameterized in the range 1 <= VMAX_RELEASE <= INTERPOLATION.V16.
INTERPOLATION	F-UDT "INTERP"	**F-UDT with interpolation points to define the end zone according to Chapter 3.4.2.4**
RELEASE	Bool	**Retracting** If the permissible position range was exited, then the machine can be traversed back to the permissible position range by selecting this input with the velocity parameterized at VMAX_RELEASE. Retraction motion is immediately stopped as soon as this input has a 0 signal.
ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted. Acknowledgment is only realized with a positive edge at ACK - and in fault-free (normal) operation it has no effect.

3.4.2.2 Outputs

Name	Data type	Description
SLS_THRESHOLD	DInt	**SLS limit [mm/min]** The presently maximum permissible traversing velocity is output here. This is cyclically calculated in the block itself.
SLS_OK	Bool	**SLS limit status** 1: SAFE_V is less than/equal to SLS_THRESHOLD 0: SAFE_V has exceeded the value of SLS_THRESHOLD. If this output changes to 0, then a stop response should be initiated.
X_NEGATIVE_OK	Bool	**Status minimum position** 1: SAFE_POS ist greater than/ equal X_NEGATIVE 0: SAFE_POS has fallen below the value of X_NEGATIVE. If this output changes to 0, then a stop response should be initiated.
X_POSITIVE_OK	Bool	**Status maximum position** 1: SAFE_POS is less than/equal to X_POSITIVE 0: SAFE_POS has exceeded the value of X_POSITIVE. If this output changes to 0, then a stop response should be initiated.
MOVE_NEGATIVE_OK	Bool	**Negative motion permitted** If a 0 signal is available at this output, then it is not permissible that the machine continues to move in the negative direction. The output is then set to 0 as soon as SAFE_POS assumes values lower than X_NEGATIVE. If SAFE_POS again lies above X_NEGATIVE, then after acknowledgment, the output is set again.
MOVE_POSITIVE_OK	Bool	**Positive motion permitted** If a 0 signal is available at this output, then it is not permis-

		sible that the machine continues to move in the positive direction. The output is then set to 0 as soon as SAFE_POS assumes values higher than X_POSITIVE. If SAFE_POS again lies below X_POSITIVE, then after acknowledgment, the output is set again.
ACK_REQ	Bool	**Acknowledgment request** If a fault has occurred, however it is no longer active, and can therefore be acknowledged, then the block indicates this using a 1 signal at ACK_REQ.
ERROR	Bool	**Error** This output is set if the block has been incorrectly parameterized, or if the block in operation detects a potentially dangerous combination of input signals. The output remains set until an error is no longer active and has been acknowledged.
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.4.2.3 Structure of DIAG

Bit No.	Description	Reset condition
0	Lower end stop was fallen below	While retracting, SAFE_POS >= X_NEGATIVE and positive edge at ACK
1	Upper end stop was exceeded	While retracting, SAFE_POS <= X_POSITIVE and positive edge at ACK
2	Retraction velocity exceeded	SAFE_V <= SLS_THRESHOLD and positive edge at ACK
3	Parameterizing error envelope curve, for remaining distance 0, the velocity is not 0	Envelope curve according to 3.9
4	Parameterizing error, retraction velocity	0 < VMAX_RELEASE <= V_MAX parameterized
5	Actual position invalid	Actual position valid again
6	Actual velocity invalid	Actual velocity valid again
7	Reserved	---
8	Reserved	---
9	Actual velocity too high regarding actual position and direction	SAFE_V <= SLS_THRESHOLD and positive edge at ACK
10	Reserved	---
11	Error for internal calculation	Pos. edge at ACK, if the fault is no longer active
12	Reserved	---
13	Reserved	---
14	Reserved	---
15	Reserved	---

3.4.2.4 F-UDT “INTERP”

Name	Data type	Description
X_0	DInt	Remaining distance point 0 [mm]
X_1	DInt	Remaining distance point 1 [mm]
X_2	DInt	Remaining distance point 2 [mm]
X_3	DInt	Remaining distance point 3 [mm]
X_4	DInt	Remaining distance point 4 [mm]
X_5	DInt	Remaining distance point 5 [mm]
X_6	DInt	Remaining distance point 6 [mm]
X_7	DInt	Remaining distance point 7 [mm]
X_8	DInt	Remaining distance point 8 [mm]
X_9	DInt	Remaining distance point 9 [mm]
X_10	DInt	Remaining distance point 10 [mm]
X_11	DInt	Remaining distance point 11 [mm]

X_12	DInt	Remaining distance point 12 [mm]
X_13	DInt	Remaining distance point 13 [mm]
X_14	DInt	Remaining distance point 14 [mm]
X_15	DInt	Remaining distance point 15 [mm]
X_16	DInt	Remaining distance point 16 [mm]
V_0	DInt	Velocity at remaining distance point 0 [mm/min]
V_1	DInt	Velocity at remaining distance point 1 [mm/min]
V_2	DInt	Velocity at remaining distance point 2 [mm/min]
V_3	DInt	Velocity at remaining distance point 3 [mm/min]
V_4	DInt	Velocity at remaining distance point 4 [mm/min]
V_5	DInt	Velocity at remaining distance point 5 [mm/min]
V_6	DInt	Velocity at remaining distance point 6 [mm/min]
V_7	DInt	Velocity at remaining distance point 7 [mm/min]
V_8	DInt	Velocity at remaining distance point 8 [mm/min]
V_9	DInt	Velocity at remaining distance point 9 [mm/min]
V_10	DInt	Velocity at remaining distance point 10 [mm/min]
V_11	DInt	Velocity at remaining distance point 11 [mm/min]
V_12	DInt	Velocity at remaining distance point 12 [mm/min]
V_13	DInt	Velocity at remaining distance point 13 [mm/min]
V_14	DInt	Velocity at remaining distance point 14 [mm/min]
V_15	DInt	Velocity at remaining distance point 15 [mm/min]
V_16	DInt	Velocity at remaining distance point 16 [mm/min]

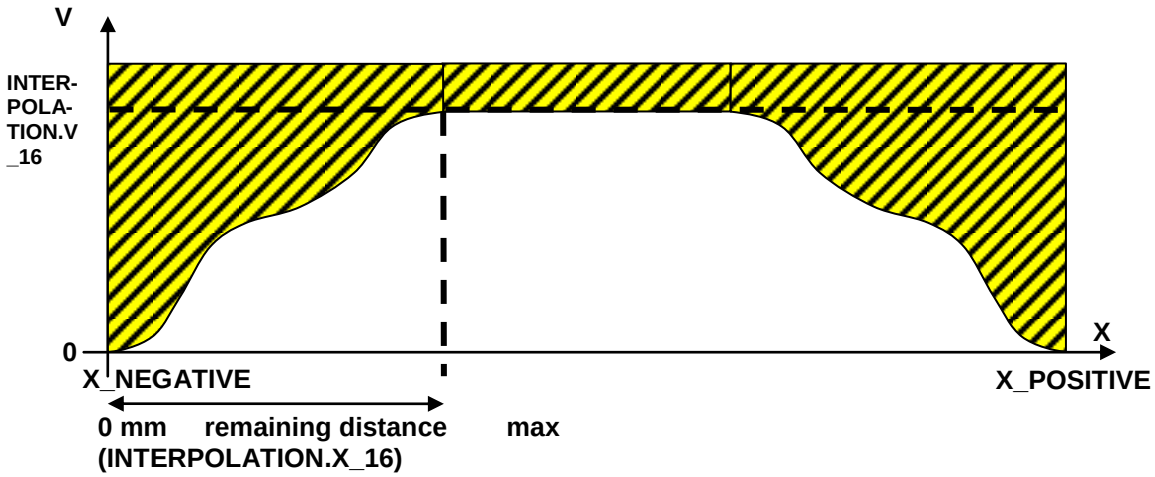
3.4.3 Principle of operation

3.4.3.1 Parameterization

1. At input SAFE_POS, the user must interconnect the safe position actual value of the system to be monitored - and at input POS_VALID its validity AND'ed with the valid reference (REFERENCED). Block "F_SAFE_POS" (Chapter3.2) provides the three signals as output.
2. The same applies to inputs SAFE_V and V_VALID, which refer to the safe actual velocity.
3. The lower end position is parameterized via input X_NEGATIVE, and the upper end position is parameterized via X_POSITIVE.
4. The velocity envelope curve of the end zone to be monitored is parameterized using 17 interpolation points (velocity with respect to distance) using the F-UDT „INTERP", referred to the remaining distance to an end stop. To do this, a fail-safe global data block should be created, in which a variable, type "INTERP" is created. The end zone curve is defined using the start values of the positions and the associated velocities. The intermediate values between the interpolation points is calculated using linear interpolation. The velocity envelope curves are symmetrical for the positive and negative end zones.

   Note
   The deceleration referred to the remaining distance to standstill is defined using a root function. The remaining distance to an end stop is used as basis to determine the velocity limit. Using linear interpolation over 17 interpolation points, this root function must be emulated corresponding to the braking response of the specific application

5. Interpolation point INTERPOLATION.X_0/ INTERPOLATION.V_0 must be parameterized with INTERPOLATION.X_0 := 0 mm and INTERPOLATION.V_0 := 0 mm/min. Velocity values parameterized higher than the interpolation value INTERPOLATION.V_16, are limited to this value.
6. VMAX_RELEASE must lie in the range 1 – INTERPOLATION.V_16. The block identifies if values lower than 1 or higher than INTERPOLATION.V_16 are parameterized, and signals this with DIAG bit 4. ERROR changes to 1.



If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Safety note

The user **must** validate the parameterized envelope curve and the correct functionality by recording traces and carrying out the appropriate tests (see Chapter 3.1.1).

Note

The requirements relating to monotony and gradient of the envelope curve depend on the specific application and the risk assessment.

Note

The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, reparameterization is not possible while the system is in operation, with the exception of X_ NEGATIVE and X_ POSITIVE. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.4.3.2 Position and velocity monitoring

7. As long as the position actual value is valid, and SAFE_V lies below the parameterized velocity envelope curve, the block does not signal an error; this means that outputs ERROR and DIAG supply a 0 signal.
8. At output SLS_THRESHOLD, depending on SAFE_POS, the associated maximum permissible velocity for this position is output.
9. If the value at input SAFE_V lies above this limit, and if the system is moving towards the end stop, then output SLS_OK is set to 0, ERROR changes to 1 and DIAG bit No. 9 is set. Depending on the user interconnection, a stop response must be initiated in the drive.
10. As soon as SAFE_V is again in the permissible range, i.e. lower than SLS_THRESHOLD, then the fault can be acknowledged and ACK_REQ outputs a 1 signal.
11. The fault can be reset with a positive edge at ACK. ERROR and the appropriate DIAG bits then change back to 0, and SLS_OK outputs a 1 signal.
12. If the value at input SAFE_V lies above the permitted velocity, but the system is moving away from the end stop, then the system may traverse with 100% velocity; INTERPOLATION.V16 is output at SLS_THRESHOLD. As a consequence, a fault is not signaled, and ERROR and DIAG remain at 0.
13. If a 0 signal is available at POS_VALID, then DIAG bit 5 is set; until acknowledged, ERROR remains in the actual state - assuming that no additional monitoring functions signals a fault condition. All other outputs maintain their actual state until acknowledgment or RELEASE is deselected.

Safety note
Block F_SAFE_POS provides a 0 signal at POS_VALID via output ERROR = 1. However, when POS_VALID goes to zero, a stop response must be initiated in the drive via a user interconnection. All other blocks indicate the status using an error code; however in order to avoid being confronted by a flood of messages/signals, in this case ERROR is not again set to a 1 signal. This means that the end stops and the envelope curve are no longer monitored. Maximum velocity INTERPOLATION.V16 - as well as the validity of the velocity actual value SAFE_V, are still monitored. Active faults for the end position and envelope curve monitoring can be immediately acknowledged X_NEGATIVE_OK, X_POSITIVE_OK and SLS_OK are set again.
If a 1 signal is again available at POS_VALID, then DIAG bit 5 is reset, and the end position and the envelope curve monitoring are resumed.

14. If a 1 signal is again available at POS_VALID, then the associated DIAG bit 5 is reset.
15. If a 0 signal is available at V_VALID, then DIAG bit 6 is set; until acknowledged, ERROR remains in the actual state - assuming that no additional active monitoring functions signals a fault condition. All other outputs maintain their actual state until acknowledgment or RELEASE is deselected.

Safety note
Block F_SAFE_POS signals a 0 signal at V_VALID via output ERROR = 1. However, when V_VALID goes to zero, a stop response must be initiated in the drive via a user interconnection. All other blocks indicate the status using an error code; however in order to avoid being confronted by a flood of messages/signals, in this case ERROR is not again set to a 1 signal. This means that the maximum velocity and the envelope curve are no longer monitored. Active faults of the maximum velocity and envelope curve monitoring can be immediately acknowledged, SLS_OK is again set. Retraction via RELEASE can be exited normally; MOVE_POSITIVE_OK and MOVE_NEGATIVE_OK are again set. If, at this instant in time, the axis is not in a valid position range, then X_NEGATIVE_OK or X_POSITIVE_OK is withdrawn and ERROR is set.
If a 1 signal is again available at V_VALID, then the associated DIAG bit 6 is reset, and the maximum velocity and the envelope curve monitoring are resumed.

16. If a 1 signal is again available at V_VALID, then the associated DIAG bit 6 is reset.
17. If the permissible traversing range is exited, i.e. SAFE_POS assumes values greater than X_POSITIVE or less than X_NEGATIVE, then the block behaves in a comparable fashion to block "F_SLP_MONITOR" (Chapter 3.3).
    Depending on the direction in which the traversing range was exited, either X_POSITIVE_OK or X_NEGATIVE_OK is set to 0. A stop response should then be initiated in the drive by the user interconnection.

3.4.3.3 Retracting

18. The retraction function of the block can be activated by selecting RELEASE. If the system is within the permissible traversing range, then MOVE_POSITVE_OK and MOVE_NEGATIVE_OK are reset to 1, the velocity parameterized at VMAX_RELEASE is output at SLS_THRESHOLD and internally this value is monitored. The velocity envelope curve is still monitored. If this supplies a more restrictive value for the permitted velocity than VMAX_RELEASE, then the permissible velocity is limited to the more restrictive (lower) value. If the permissible traversing range is exited, then the block responds as described under Point 17.
19. To traverse from the end stop back into the permitted traversing range, the retraction function of the block can be activated by selecting RELEASE. The velocity parameterized at VMAX_RELEASE is then output at SLS_THRESHOLD, and depending on the direction of travel when the end zone was violated, either MOVE_POSITIVE_OK or MOVE_NEGATIVE_OK is set to 0 in order to prevent further motion towards this end zone. MOVE_POSITIVE_OK = 0 inhibits motion in the positive direction, MOVE_NEGATIVE_OK = 0 inhibits motion in the negative direction.

Note
The signal for RELEASE must be generated in a safety-related fashion, e.g. by using a key-operated switch or similar device.

20. In order to facilitate retraction, when RELEASE is selected, X_POSITIVE_OK or X_NEGATIVE_OK is reset to 1; the stop response of the drive should be deselected using a suitable user interconnection.
21. If, during retraction, the value of SAFE_V exceeds the value of VMAX_RELEASE - or the permissible velocity of the opposite end zone, if this is below VMAX_RELEASE, then SLS_OK changes to 0 and DIAG bit 2 is set.
22. A velocity fault can always be acknowledged if the actual velocity SAFE_V is again below SLS_THRESHOLD.
23. As soon as SAFE_POS is back in the parameterized permissible range, after acknowledgment, the machine can again be traversed with full velocity, i.e. the permissible velocity of the envelope curve monitoring is output at SLS_THRESHOLD and monitored.
    ERROR and DIAG change back to 0.
24. If V_VALID = 0 while SAFE_POS lies outside the parameterized traversing range, then the retraction velocity can no longer be monitored in a safely-related way. Therefore, selection using RELEASE = 1 has no effect.
25. To resume retraction, after acknowledgment, at block F_SAFE_POS, V_VALID must be again set to a 1 signal.
26. Retraction can then be continued. Alternatively, the initial state can be restored by deselecting RELEASE and subsequent acknowledgment. If SAFE_POS still lies outside the parameterized traversing range, then the system responds corresponding to Point 17.

Safety note
The parameterization of input VMAX_RELEASE must be adapted according to the permissible safely reduced velocity, derived from the application-specific risk assessment.

Warning
The interconnection of output MOVE_POSITIVE_OK must match the selection of drive function SDI for a positive direction. For MOVE_POSITIVE_OK = 0, motion in the positive direction must no longer be possible.
The same is true when interconnecting output MOVE_NEGATIVE_OK and inhibiting the negative direction of motion.
It is absolutely crucial that the block outputs are interconnected with the correct signals to control the drive.
Otherwise, inadmissible motion towards the end stops is possible, which cannot be identified internally in the block.

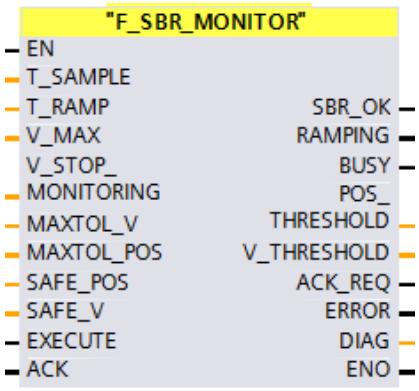
3.4.3.4 Acknowledging errors

DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors. As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.

3.5 F_SBR_MONITOR

3.5.1 Introduction

The fail-safe function block F_SBR_MONITOR monitors that the braking ramp is maintained. If, for example after SS1 has been initiated, the velocity is not reduced in the drive along the parameterized down ramp, the block outputs a signal to initiate STO or to close the brake.



Note

When using this block, then block **F_BO_W (FC 176)** must be available in the block folder. It is not permissible to renumber this! Blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)**, **LFMulDInt (FC 213)** and **LFDivDInt (FC 214)** are also required from this library. These may be renumbered, but not renamed.

3.5.2 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0 and all word variables with W#16#0.

3.5.2.1 Inputs

Name	Data type	Description
T_SAMPLE	DInt	**Sampling time [ms]** Here, the block sampling time, i.e. the interval in which the safety program is called (cyclic interrupt OB interval for the F-OB) is parameterized in ms.
T_RAMP	DInt	**Ramp-down time [ms]** Here, the corresponding value in ms for the ramp-down time from maximum velocity down to standstill is parameterized as in the drive. In conjunction with V_MAX, the gradient of the down ramp is calculated from this value. It must be ensured that T_RAMP/T_SAMPLE is an integer multiple.
V_MAX	DInt	**Max. permissible velocity [mm/min]** Here, the corresponding value for the maximum operating velocity is parameterized, just the same as in the drive, whereby the conversion from rpm to mm/min must be observed. From this value, in conjunction with T_RAMP, the down ramp gradient is calculated. It must be ensured that V_MAX/(T_RAMP/T_SAMPLE) is an integer multiple.
V_STOP_MONITORING	DInt	**Shutdown threshold for monitoring [mm/min]** As soon as the actual velocity falls below this threshold, after the brake ramp monitoring has been initiated, the block can be acknowledged.
MAXTOL_V	DInt	**Velocity tolerance [mm/min]** Max. permissible value that SAFE_V can exceed the configured braking ramp
MAXTOL_POS	DInt	**Position tolerance [mm]** Max. value that SAFE_POS can exceed the position limit according to the configured braking ramp
SAFE_POS	DInt	**Safe position actual value [mm]** is supplied from block F_SAFE_POS. The block derives the velocity from the rate that this value changes (with respect to time). If, after SS1 is initiated, the block identifies that the drive does not brake

		along the configured ramp, then at SBR_OK the block sets a 0 signal - and as a consequence, for example STO is initiated or a mechanical brake can be closed.
SAFE_V	DInt	**Safe velocity actual value [mm/min]** This is supplied from the F_SAFE_POS block; the motor encoder is the signal source, which is read-in via the SI part of the drive. If, after SS1 is initiated, the block identifies that the drive does not brake along the configured ramp, then at SBR_OK the block sets a 0 signal - and as a consequence, for example STO is initiated or a mechanical brake can be closed.
EXECUTE	Bool	**Starting monitoring...** The block becomes active with a rising edge at this input, i.e. braking ramp monitoring is started (e.g. interconnection with a bit "SS1 active" from the PROFIsafe telegram 902)
ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted.

3.5.2.2 Outputs

Name	Data type	Description
SBR_OK	Bool	**Status of the braking ramp monitoring** 1: The braking ramp is maintained - or monitoring is not active. 0: The drive brakes but not to achieve the minimum configured down ramp If this output changes to 0, then STO should be initiated or a mechanical brake closed.
RAMPING	Bool	**Braking ramp status** 1: Braking active
BUSY	Bool	**Status of the ramp monitoring** 1: Position and velocity limit monitoring active
POS_THRESHOLD	DInt	**Position limit value [mm]** Effective limit for the ramp monitoring regarding the position change
V_THRESHOLD	DInt	**Velocity limit value [mm/min]** Effective limit for the ramp monitoring regarding the velocity
ACK_REQ	Bool	**Acknowledgment request** If a fault has occurred, however it is no longer active, and can therefore be acknowledged, then the block indicates this using a 1 signal at ACK_REQ.
ERROR	Bool	**Error** This output is set if the block has been incorrectly parameterized, or if the block in operation detects that the SS1 braking ramp has been violated. The output remains set until an error is no longer active and has been acknowledged.
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.5.2.3 Structure of DIAG

Bit No.	Description	Reset condition
0	SS1 braking ramp is not maintained	SAFE_V falls below V_STOP_MONITORING and a positive edge at ACK
1	Parameterizing error T_RAMP: Not a multiple integral of T_SAMPLE	The ratio between T_RAMP and T_SAMPLE is an integer multiple

2	Reserved	---
3	Parameterizing error V_MAX: V_MAX / (T_RAMP / T_SAMPLE) cannot be represented as integer multiple	The ratio between V_MAX and the number of cycles, given by T_RAMP and T_SAMPLE for the braking ramp, is an integer multiple.
4	T_SAMPLE <= 0	T_SAMPLE parameterized > 0
5	MAXTOL_V > V_MAX	MAXTOL_V parameterized <= V_MAX
6	T_RAMP < 0	T_RAMP parameterized >= 0
7	Reserved	---
8	Reserved	---
9	Reserved	---
10	Reserved	---
11	Error for internal calculation	Pos. edge at ACK, if the fault is no longer active
12	Reserved	---
13	Reserved	---
14	Reserved	---

3.5.3 Principle of operation

3.5.3.1 Parameterization

1. The actual velocity calculated by block F_SAFE_POS is interconnected to the SAFE_V input.
2. The braking ramp gradient is determined in the block using T_RAMP and V_MAX. Using T_SAMPLE and T_RAMP, the number of cycles are determined that are required to brake from V_MAX down to standstill. In each cycle, the maximum permissible velocity internally calculated in the block is then appropriately reduced.

When parameterizing, it must be ensured that the following relationships can be represented as integer multiples:

T_RAMP / T_SAMPLE

V_MAX / (T_RAMP/T_SAMPLE)

Further, the following relationship between the input variables must apply:

MAXTOL_V <= V_MAX

The permissible value ranges of the individual inputs should be taken from the table describing the inputs.

If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Safety note
The parameterization of V_MAX and T_RAMP must be selected so that when it is identified that the permissible traversing range has been exited (with the associated stop response), when an STO is initiated, the axis can be braked to standstill before the physical end of the traversing range is reached.

Note
The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, it is not possible to reparameterize the system while it is in operation. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.5.3.2 Ramp monitoring

3. Braking ramp monitoring is activated with a rising edge at EXECUTE.
4. If SAFE_V exceeds the internally calculated maximum permissible value, then output SBR_OK changes to 0, ERROR to 1 and DIAG bit 0 is set.
5. SBR_OK is also set to 0, if, in each cycle, SAFE_POS changes by more than the maximum position change per cycle internally calculated by the block. This establishes a two channel ramp monitoring configuration.
6. In this case, ERROR also changes to 1 - and DIAG bit 0 is set.
7. Monitoring is exited as soon as EXECUTE is reset to 0, and the internally calculated velocity ramp has reached a value of 0.
8. A tolerance value for the velocity and positioning monitoring can be parameterized via inputs MAXTOL_V and MAXTOL_POS. SBR_OK is then set to 0 if SAFE_V exceeds the internally calculated ramp + MAXTOL_V - or if the position increase with respect to the position at the instant of the selection is greater than the internally calculated maximum value + MAXTOL_POS.

Warning
For a 0 signal at SBR_OK, STO must be immediately initiated or the mechanical brake(s) closed.

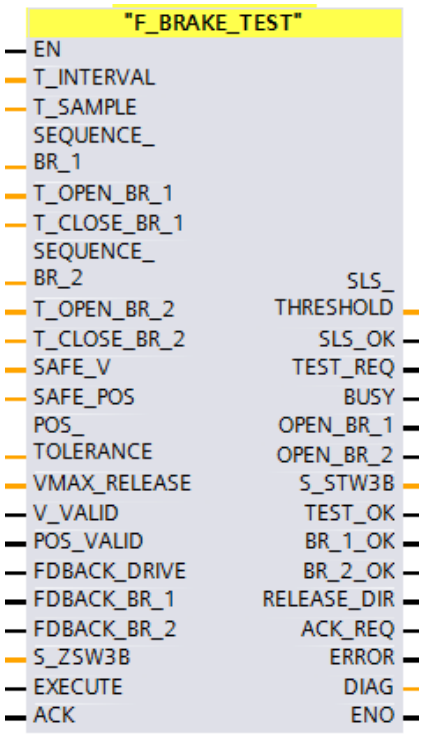
3.5.3.3 Acknowledging errors

9. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors.
   As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.
10. After SBR_OK has changed to a 0 signal, i.e. the braking ramp was not maintained, the block can only be acknowledged if the actual velocity at SAFE_V falls below the value at V_STOP_MONITORING. ACK_REQ then changes to a 1 signal.

3.6 F_BRAKE_TEST

3.6.1 Introduction

The fail-safe function block F_BRAKE_TEST is used to control the drive function SBT to test a motor holding brake or an external brake.
The torque setpoint and the test profiles are saved in the SI section of the drive in the Safe Brake Test (SBT). When requested, the block automatically coordinates the parameterized test sequences.
The functions of two independent brakes are then consecutively tested by establishing a torque against the closed brake.
If the brake test was unsuccessful, the block supports retraction logic with SDI and SLS. This means that only traversing/travel motion with reduced velocity, and for example for a hoisting gear application, only in the downward direction.



Note

When using this block, blocks **F_BO_W (FC 176), F_W_BO (FC 177)** and **F_TP (FB 184)** must be available in the block folder. It is not permissible to renumber these! Blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)**, **LFMulDInt (FC 213)** and **LFDivDInt (FC 214)** are also required from this library. These may be renumbered, but not renamed.

3.6.1 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0, all TIME variables with T#0ms and all word variables with W#16#0.

3.6.1.1 Inputs

Name	Data type	Description
T_INTERVAL	Time	**Test interval** After this time has elapsed, the block requests that a brake test is performed. This is signaled at output TEST_REQ using a 1 signal.
T_SAMPLE	DInt	**Sampling time [ms]** Here, the block sampling time, i.e. the interval in which the safety program is called (cyclic interrupt OB interval for the F-OB) is

		parameterized in ms.
SEQUENCE_BR_1	Word	**Configuration parameters** The test pattern to be executed and the brake type for brake 1 are defined according to the following schematic via this input: Bit 0: Test with test sequence 1 positive Bit 1: Test with test sequence 1 negative Bit 2: Test with test sequence 2 positive Bit 3: Test with test sequence 2 negative Bit 4: 0: external brake; 1: motor holding brake
T_OPEN_BR_1	DInt	**Opening time brake 1 [ms]** Within this time, the brake must completely open; otherwise a read back error is identified - and the test is exited as having not been successfully completed. In this case, DIAG bit 0 is also set.
T_CLOSE_BR_1	DInt	**Closing time brake 1 [ms]** Within this time, the brake must completely close; otherwise a read back error is identified - and the test is exited as having not been successfully completed. In this case, DIAG bit 0 is also set.
SEQUENCE_BR_2	Word	**Configuration parameters** The test pattern to be executed and the brake type for brake 2 are defined according to the following schematic via this input: Bit 0: Test with test sequence 1 positive Bit 1: Test with test sequence 1 negative Bit 2: Test with test sequence 2 positive Bit 3: Test with test sequence 2 negative Bit 4: 0: external brake; 1: motor holding brake
T_OPEN_BR_2	DInt	**Opening time brake 2 [ms]** Within this time, the brake must completely open; otherwise a read back error is identified - and the test is exited as having not been successfully completed. In this case, DIAG bit 1 is also set.
T_CLOSE_BR_2	DInt	**Closing time brake 2 [ms]** Within this time, the brake must completely close; otherwise a read back error is identified - and the test is exited as having not been successfully completed. In this case, DIAG bit 1 is also set.
SAFE_V	DInt	**Safe velocity actual value [mm/min]** is supplied from block F_SAFE_POS. If, for a brake test that has not been successfully completed, the actual velocity is greater than the upper limit parameterized at VMAX_RELEASE then output SLS_OK is reset and the machine is stopped. In this case, DIAG bit 2 is also set.
SAFE_POS	DInt	**Safe position actual value [mm]** is supplied from block F_SAFE_POS. This is required to monitor standstill during the brake test. If the axis moves by more than the value parameterized at POS_TOLERANCE, then the test is considered to have not been successfully completed, and is exited. In this case, DIAG bit 3 is also set.
POS_TOLERANCE	DInt	**Threshold for standstill detection [mm]** If the axis moves by more than this absolute value, then the test is considered to have not been successfully completed, and is exited. In this case, DIAG bit 3 is also set.
VMAX_RELEASE	DInt	**Retraction velocity [mm/min]** If the test was not successfully completed, then this value is output at SLS_THRESHOLD until a brake test has been successfully performed. VMAX_RELEASE must be parameterized in the range 1-2147483647. Otherwise, DIAG bit No. 4 is set

V_VALID	Bool	**Actual velocity valid** is supplied from block F_SAFE_POS. 1: Velocity is plausible 0: Velocity is not plausible, i.e. the increase of the deviation between the two encoders over time is outside the tolerance window. If a 0 signal is available here, then DIAG bit No. 6 is set.
POS_VALID	Bool	**Actual position valid** is supplied from block F_SAFE_POS. 1: Position is plausible 0: Position is not plausible, i.e. the discrepancy between the two encoders is outside the tolerance window. If a 0 signal is available here, then DIAG bit No. 5 is set.
FDBACK_DRIVE	Bool	**Brake control normal operation** 0: Close brake 1: Open brake
FDBACK_BR_1	Bool	**Feedback signal brake 1** 0: open 1: closed
FDBACK_BR_2	Bool	**Feedback signal brake 2** 0: open 1: closed
S_ZSW3B	WORD	**S120 Safety Info Channel – status word 3 (r10234)** **Bit 00: SBT_SELECTED** **Feedback signal drive – select SBT** 1: SBT selected 0: function not selected **Bit 02: SBT_ACTIVE_BR** **Feedback signal drive – active brake** Here, the drive signals the number of the brake currently being tested: 0: brake 1 1: brake 2 **Bit 03: SBT_ACTIVE** **Feedback signal drive – status SBT** 1: test running; drive establishes a torque against the closed brake 0: test not active; drive passive **Bit 04: SBT_RESULT** **Feedback signal drive – test result** 0: Brake faulty 1: Brake successfully tested **Bit 05: SBT_FINISHED** **Feedback signal drive – status test sequence** 0: Test running 1: Test completed **Bit 06: SBT_CLOSE_BR** **Brake control SBT for external brake** The drive issues the command to open/close external brakes via this input. 0: open ext. brake 1: close ext. brake **Bit 07: SBT_FDBACK_DIR** **Feedback signal drive – direction of torque buildup** Here, the drive signals the direction of the currently established torque: 0: positive 1: negative
EXECUTE	Bool	**Start brake test** The brake test is started via a positive edge at this input. After the test has been successfully completed, the time for the test interval is restarted and output TEST_OK is set again.

ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted. Acknowledgment is only realized with a positive edge at ACK; in fault-free (normal) operation has no effect.

3.6.1.2 Outputs

Name	Data type	Description
SLS_THRESHOLD	DInt	**SLS limit [mm/min]** The presently maximum permissible traversing velocity is output here. This is 2147483647 in normal operation; if the brake test has not been successfully completed, then VMAX_RELEASE is output here. If VMAX_RELEASE has been parameterized <= 0, then an equivalent value of 1 is output here.
SLS_OK	Bool	**SLS limit status** 1: SAFE_V is less than/equal to SLS_THRESHOLD 0: SAFE_V has exceeded the value of SLS_THRESHOLD. If this output changes to 0, then a stop response should be initiated.
TEST_REQ	Bool	**Request brake test** 1: brake test requested 0: no brake test requested
BUSY	Bool	**Test status** 1: Test running 0: Test not selected
OPEN_BR_1	Bool	**Control signal, external brake 1** 1: Open brake 0: Close brake
OPEN_BR_2	Bool	**Control signal, external brake 2** 1: Open brake 0: Close brake
S_STW3B	Word	**S120 Safety Control Channel – control word 3 (r10235)** **Bit 00: SBT_SELECT** **Drive communication: Brake test selected** Same conditions as BUSY output **Bit 01: SBT_START** **Drive communication: Start** 1: Start test sequence **Bit 02: SBT_BR_SELECT** **Drive communication: Brake selection** 0: brake 1 1: brake 2 **Bit 03: SBT_TORQUE_DIR** **Drive communication: Torque preselection** 0: positive 1: negative **Bit 04: SBT_SEQUENCE** **Drive communication: Select test sequence** 0: sequence 1 1: sequence 2 **Bit 05: SBT_FDBACK_DIR** **Drive communication: Status ext. brake** 0: open 1: closed
TEST_OK	Bool	**Test result status** 0: Test unsuccessful 1: Test successfully completed
BR_1_OK	Bool	**Status brake 1** 0: faulty or test still not performed 1: OK

BR_2_OK	Bool	**Status brake 2** 0: faulty or test still not performed 1: OK
RELEASE_DIR	Bool	**Status motion direction** is FALSE for a test that has not been successfully completed;
ACK_REQ	Bool	**Acknowledgment request** If a fault has occurred, however it is no longer active, and can therefore be acknowledged, then the block indicates this using a 1 signal at ACK_REQ.
ERROR	Bool	**Error** This output is set if the block has been incorrectly parameterized, or if the block in operation detects a potentially dangerous combination of input signals. The output remains set until an error is no longer active and has been acknowledged.
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.6.1.3 Structure of DIAG

Bit No.	Description	Reset condition
0	Runtime error T_OPEN/T_CLOSE_BR_1 not maintained	Pos. edge at ACK, restart test, reset is realized if the test was successful
1	Runtime error T_OPEN/T_CLOSE_BR_2 not maintained	Pos. edge at ACK, restart test, reset is realized if the test was successful
2	SLS monitoring triggered SAFE_V exceeds V_MAX_RELEASE or V_VALID == 0 while the axis moves for an unsuccessful test	SAFE_V <= VMAX_RELEASE and V_VALID == 1 and pos. edge at ACK
3	no standstill during the test SAFE_POS changes during the test by more than POS_TOLERANCE	Pos. edge at ACK, restart test, reset is realized if the test was successful
4	Parameterizing error, value range	T_SAMPLE >= 1 and T_OPEN_BR_1 >= 1 and T_CLOSE_BR_1 >= 1 and T_OPEN_BR_2 >= 1 and T_CLOSE_BR_2 >= 1 and POS_TOLERANCE >= 0 and V_MAX_RELEASE >= 1
5	parameterizing error integer multiple	T_OPEN_BR_1 / T_SAMPLE can be represented as integer multiple and T_CLOSE_BR_1 / T_SAMPLE can be represented as integer multiple T_OPEN_BR_2 / T_SAMPLE can be represented as integer multiple and T_CLOSE_BR_2 / T_SAMPLE can be represented as integer multiple
6	Non-plausible feedback signal from SBT:	Pos. edge at ACK, restart test, reset is realized if the test was successful
7	Drive enable missing for active brake test	Pos. edge at ACK, restart test, reset is realized if the test was successful
8	No safe position available for active brake test	Pos. edge at ACK, restart test, reset is realized if the test was successful
9	Monitoring time: no feedback signal SBT_SELECTED within the monitoring time after selecting SBT	Pos. edge at ACK, restart test, reset is realized if the test was successful
10	Monitoring time external brake request initiated by SBT	Pos. edge at ACK, restart test, reset is realized if the test was successful
11	Error for internal calculation	Pos. edge at ACK, if the fault is no longer active
12	Reserved	---

13	Reserved	---
14	Warning: not a safe position, SBT not possible	POS_VALID = 1
15	Warning: not a safe velocity, SBT not possible	V_VALID = 1

3.6.2 Principle of operation

3.6.2.1 Parameterization

When parameterizing, it must be ensured that the following relationships can be represented as integer multiples:

T_OPEN_BR_1 / T_SAMPLE

T_CLOSE_BR_1 / T_SAMPLE

T_OPEN_BR_2 / T_SAMPLE

T_CLOSE_BR_2 / T_SAMPLE

The permissible value ranges of the individual inputs should be taken from the table describing the inputs.

If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Note
The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, it is not possible to reparameterize the system while it is in operation. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.6.2.2 Interface to SINAMICS S120

The interface between F_BRAKE_TEST and SINAMICS S120 is described in the following. Communication runs in the standard telegram using status/control word S_ZSW3B(Safety Info Channel status word 3)/S_STW3B (Safety Control Channel control word 3). SBT selection should be interconnected to "SBT via SCC (p10235)". The signals are interconnected to the block directly via the control/status word; the assignment can be taken from the following tables and the interface description of this block.

3.6.2.2.1 Communication direction, F_BRAKE_TEST -> SINAMICS S120

Bit	Meaning	Remarks		Parameter
0	Select brake test	1	Brake test selected	r10235.0
		0	Brake test deselected	
1	Start brake test	1	Start brake test requested	r10235.1
		0	Start brake test not requested	
2	Brake selection	1	Test brake 2 selected	r10235.2
		0	Test brake 1 selected	
3	Select direction of rotation	1	Negative direction selected	r10235.3
		0	Positive direction selected	
4	Select test sequence	1	Test sequence 2 selected	r10235.4
		0	Test sequence 1 selected	
5	Status external brake	1	External brake closed	r10235.5
		0	External brake open	
6…15	Reserved	--	--	--

3.6.2.2.2 Communication direction, SINAMICS S120 -> F_BRAKE_TEST

Bit	Meaning	Remarks	Parameter

0	Brake test	1	Brake test selected	r10234.0
		0	Brake test deselected	
1	Setpoint input drive/external	1	Setpoint input for drive	r10234.1
		0	Setpoint input external (control)	
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 successfully completed	r10234.4
		0	Test unsuccessful	
5	Brake test exited	1	Test performed	r10234.5
		0	Test incomplete	
6	External brake request	1	Close brake	r10234.6
		0	Open brake	
7	Actual load sign	1	Sign negative	r10234.7
		0	Sign positive	
8…13	Reserved	--	--	--
14	Acceptance test SLP(SE) deselected	1	Acceptance test SLP(SE) deselected	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	

3.6.2.2.3 Setting the safe brake test in the converter

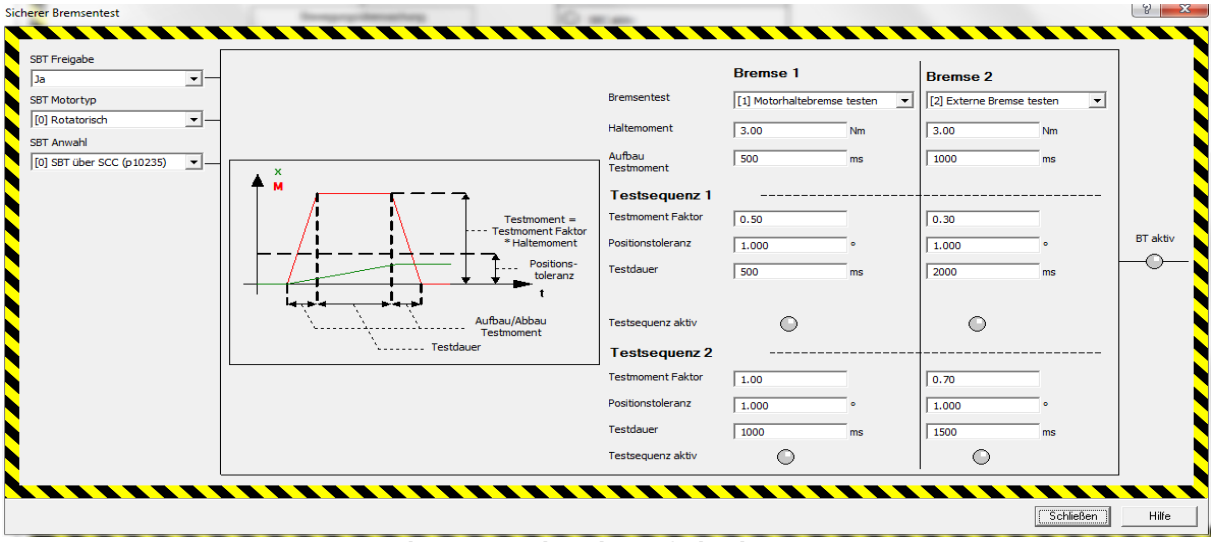


Fig. 12: Setting the safe brake test

The sequence in which the brakes should be tested must match the configuration in SINAMICS S120 and that at F_BRAKE_TEST. Otherwise, the block and SINAMICS S120 will output an error when performing the tests.

The parameters of the test sequences are set in SINAMICS S120; the selection as to which test sequences are to be performed and how are specified at F_BRAKE_TEST.

3.6.2.3 Test sequence and error handling

1. After the time parameterized at T_INTERVALL elapses, the block is requested to perform a brake test via output TEST_REQ.
   This is started using a rising edge at EXECUTE, BUSY is set to 1.
2. The test sequence for the particular brake is parameterized using input SEQUENCE_BR_1 or SEQUENCE_BR_2.

   SEQUENCE_BR_1/2 is specified, bit coded:
   - Bit 0: Test with test sequence 1 positive
   - Bit 1: Test with test sequence 1 negative

Bit 2: Test with test sequence 2 positive
Bit 3: Test with test sequence 2 negative
Bit 4: 0: external brake; 1: motor holding brake

Brake 1 is always tested first, followed by brake 2

3. The test is canceled when the first error/fault occurs ERROR changes to 1, BUSY is reset to 0.
4. At BR_1_OK or BR_2_OK, a 0 signal indicates that the test for this brake was not successful; output TEST_OK is set to 0.
5. These signals are only set to 1 after the test has been successfully completed.
6. As long as the test was not successfully completed, the velocity parameterized at input VMAX_RELEASE is output at SLS_THRESHOLD - and TEST_OK outputs a 0 signal.
7. RELEASE_DIR is set to 0 for an unsuccessful test. By appropriately controlling the SDI safety function on the drive side, it is possible to only allow traversing in the safe direction, i.e. for a hoisting gear slowly downwards. RELEASE_DIR outputs a 1 signal again as soon as the test has been successfully completed.
8. If SAFE_V exceeds the value of SLS_THRESHOLD, then SLS_OK changes to 0 and DIAG bit 2 is set.
9. If the test for both brakes was successfully completed, then the maximum value (maximum DINT value = 2147483647) is again output at SLS_THRESHOLD.
10. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors.
11. As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.
12. If a brake test was unsuccessful, a new brake test can only be started after acknowledgment using a positive edge at ACK. EXECUTE must again be selected to start.
13. DIAG bit 15 is set if a 0 signal is present at V_VALID.
14. Further, ERROR changes to 1 and SLS_OK to 0 if the block is presently in the retraction mode.
15. To exit this state, V_VALID must first be again set to a 1 signal using F_SAFE_POS by acknowledging.

16. If the test is started using EXECUTE = 1, then the block initially signals this at the BUSY output. The SCC/SIC (Safety Control Channel/Safety Information Channel) is interconnected directly to the relevant input or output of the block as word. The internal signal processing in the block takes the appropriate bits for the brake test from the SIC (in the text, this are symbolically designated to make it easy to understand) - and processes them. The corresponding control signals for the brake test are then output, combined via word SCC. To ensure a good understanding of the situation, the internal signals from SCC or SIC words are designated with SBT_... in the following.
17. In the block, depending on the parameterized test sequence, outputs SBT_BR_SELECT, SBT_TORQUE_DIR and SBT_SEQUENCE are switched.
18. If the test has been started, then an appropriate feedback signal from the drive must be available at SBT_SELECTED. The user must also establish this signal interconnection.
19. The drive provides feedback about the brake presently being tested at input SBT_ACTIVE_BR. This feedback is used to check the plausibility. The block sets ERROR and DIAG bit 6 if the control signals contradict one another.

Warning
For RELEASE_DIR = 0, it is not permissible that any potentially hazardous motion is executed. For hoisting gear, this would be motion upwards - for travel gear, motion in the positive or negative direction. For hoisting gear, drive function SDI is predominantly used to inhibit a specific traversing direction; for travel gear, the SOS drive function is used to inhibit any direction.

It is absolutely crucial that, depending on the application, the block output is interconnected with the correct signal to control the drive.

Otherwise, inadmissible motion is possible, which cannot be identified internally in the block.

Safety note
The parameterization of input V_MAX_RELEASE must be adapted according to

the permissible safely reduced velocity, derived from the application-specific risk assessment.

Safety note
Parameter "T_INTERVAL" defines in which cyclic intervals a brake test is required. The value, which must be configured here, depends on the specific application - and is also dependent on the specific risk assessment and the actual hardware architecture of the safety function.

Note
A brake test is requested at each stop-start transition of the CPU.

Note
Block F_SAFE_POS provides a 0 signal at POS_VALID via output ERROR = 1. All other blocks, i.e. also F_BRAKE_TEST, indicate the status using an error code; however in order to avoid being confronted by a flood of messages, in this case ERROR is not again set to a 1 signal, assuming that the block is not performing a brake test at this instant in time. ERROR is also set to 1 if a brake test is active, and a 0 signal is available at input POS_VALID.

3.6.2.4 Testing an external brake

If a 0 signal is available at SEQUENCE_BR_1/2.BIT4, then an external brake is tested according to the following schematic:

20. If a 1 signal is available at SBT_CLOSE_BR, depending on the state of SBT_ACTIVE_BR, the block either switches OPEN_BR_1 or OPEN_BR_2 inactive, i.e. the brake presently being tested is closed. A 1 signal must be available at feedback channel FDBACK_BR_1/ FDBACK_BR_2 within the time parameterized at T_CLOSE_BR_1/T_CLOSE_BR_2.
21. If this is not the case, then the test is canceled as described above. ERROR and DIAG bit 0/1 (depending on the brake presently being tested) change to 1.
22. After T_CLOSE_BR_1/T_CLOSE_BR_2 expires - and if there is a 1 signal at FDBACK_BR_1/ FDBACK_BR_2 - the drive is signaled that the brake is closed via SBT_FDBACK_BR = 1; the drive then executes the test profile.
23. During the test the system monitors as to whether the value at input SAFE_POS changes by more than the value parameterized at POS_TOLERANCE. The test is canceled as described above if this change is higher. ERROR and DIAG bit 3 change to a 1 signal.
24. Once the drive completes the test, the command to open the brake is given at the block input via SBT_CLOSE_BR using a 0 signal.
25. A 1 signal is again available at output OPEN_BR_1/ OPEN_BR_2.
26. A 0 signal must be available at feedback channel FDBACK_BR_1/ FDBACK_BR_2 after the time parameterized at input T_OPEN_BR_1/ T_OPEN_BR_2.
27. If this is not the case, then the test is canceled as described above. ERROR and DIAG bit 0/1 (depending on the brake presently being tested) change to 1.
28. After T_OPEN_BR_1/ T_OPEN_BR_2 expires - and if there is a 0 signal at FDBACK_BR_1/ FDBACK_BR_2 - then drive is signaled that the brake is open via SBT_FDBACK_BR = 0.
29. If the brake was successfully tested, then the drive signals this using SBT_FINISHED = 1.
30. When a test has been successfully completed, a 1 signal is available at SBT_RESULT.
31. If necessary, this test pattern is repeated for the second brake - or depending on SEQUENCE_BR_2.BIT4 for the second brake - the following test pattern is applied:

3.6.2.5 Testing a motor holding brake

If a 1 signal is available at SEQUENCE_BR_1/2.BIT4, then a motor holding brake is tested according to the following procedure at the drive:

32. In this operating mode, the drive directly controls the brake. This means that the drive independently executes its test profile; the block ignores SBT_CLOSE_BR.
33. During the test the system monitors as to whether the value at input SAFE_POS changes by a maximum of POS_TOLERANCE. The test is canceled as described above if this change is higher. If the brake was successfully tested, then the drive signals this using SBT_FINISHED = 1.

34. When a test has been successfully completed, a 1 signal is available at SBT_RESULT.

3.6.2.6 Test completed

35. If the test is still running for brake 2, however, the configured sequences for brake 1 have been executed already without any errors, then BR_1_OK has a 1 signal, while BR_2_OK and TEST_OK still have a 0 signal.
36. If the test was successfully completed for all of the configured test sequences, then this is signaled at output TEST_OK with a 1 signal, BR_2_OK then also has a 1 signal.
37. The time monitoring for when the next test is due (T_INTERVAL) is restarted, and then the block sets output BUSY back to 0.

3.6.2.7 Acknowledging errors

38. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors.
    As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ. After a positive edge at ACK, ACK_REQ is reset to 0.
39. If a brake test was unsuccessful, then this must first be acknowledged using a positive edge at ACK - before a new test can be started using EXECUTE.

3.6.3 Application example for safely controlling external brakes

In the following function example, the external brakes at F-DO channel A20.0 ("BRAKE1") and A20.1 ("BRAKE2") are to be controlled from F_BRAKE_TEST for the brake test - and safety function STO triggered.
The signal for STO (designated here as “STO_select") is low active; i.e. 1 means that STO is not active; 0 means that at least one safety function requests an STO.
The brake feedback signals are wired to the two standard inputs E1.0 ("FDBACK_BRAKE1") and E1.1 ("FDBACK_BRAKE2"); a 1 signal means that the brake is closed, while a 0 signal means that the particular brake is open.
In this particular example, 100ms is used as the monitoring time for opening and closing the brakes. This time also depends on the response time for your safety functions specified from the risk assessment.

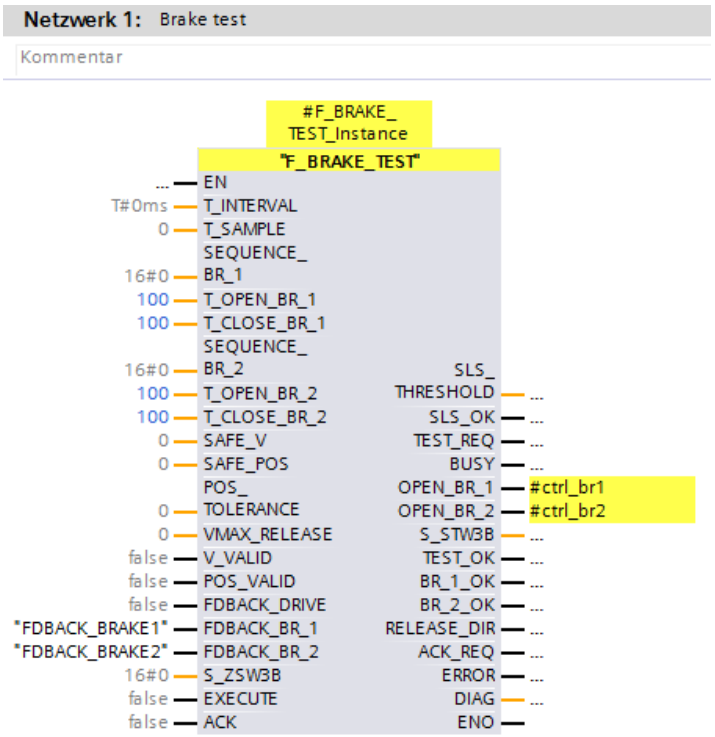
Safety note
The parameterization of inputs T_OPEN_BR_x and T_CLOSE_BR_x - as well as FDB_TIME - used in this example - must be adapted to address the required response time of the safety functions for the specific application.

It is not permissible that the monitoring time exceeds the required response time.

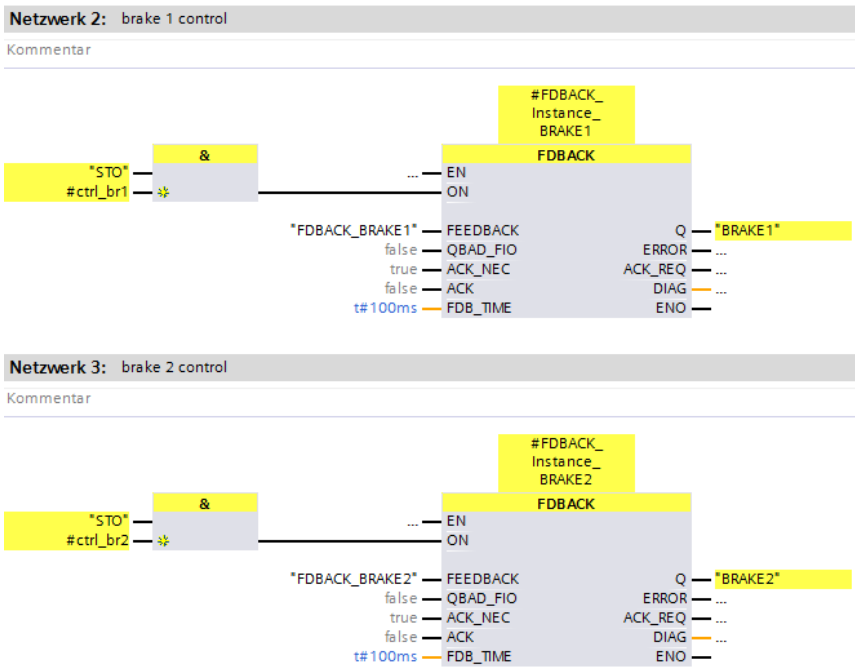
In the following code example, only the relevant interconnections have been made for the above description of the application for reasons of transparency.
In order that a program is created that can actually run, block F_BRAKE_TEST must be parameterized according to the description in Chapter 3.6.2.

The example is subdivided into three networks.

Block F_BRAKE_TEST is called in the first network. This does not directly control the brakes, but transfers the control commands via temporary variables #ctrl_br1 and #ctrl_br to networks 2 and 3.



In the 2nd and 3rd networks these signals, together with signal “STO_select", are connected to a F_FDBACK function block. Block F_FDBACK is included in the STEP7 Safety Advanced library under number FB216, and is used to monitor the feedback circuit.
You can find additional information on this block in the online help in the TIA Portal.
Assuming that there is no feedback circuit fault for the brake, and the logic operation at the ON input of the F_FDBACK has a 1 signal, the brakes at output A20.0 ("BRAKE1") and A20.1 ("BRAKE2") are opened.



3.7 F_LOAD_MONITOR

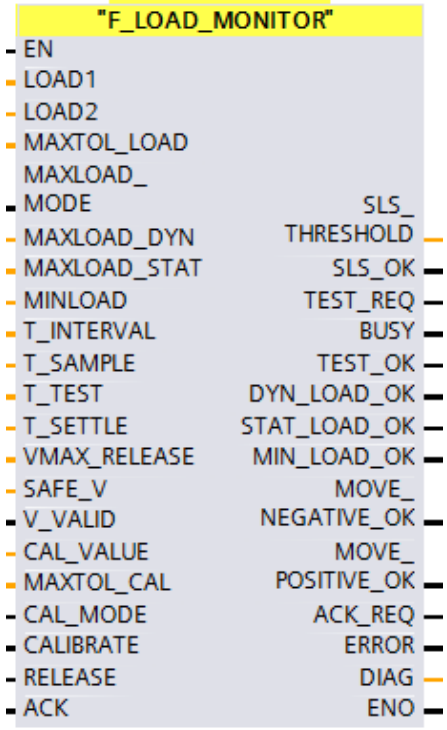
3.7.1 Introduction

The fail-safe function block F_LOAD_MONITOR has the function to guarantee safety-related overload and slack cable detection.
The block allows various versions of the actual load value to be read in, e.g.:

1. Qualified (safe) measurement source - as well as safe evaluation (e.g. F-AI module)
2. Two diverse (non safety-related) measurement sources (e.g. motor torque via SINAMICS and weighing cell via AI module) - the plausibility of the encoder values is checked using this block.

Safety note
The encoder and evaluation units used must be evaluated in accordance with the specific application.

A retraction logic becomes available if slack cable or overload is detected during operation. When a slack cable is detected, retraction is monitored so that upward retraction is only permissible with reduced velocity. For overload, retraction is only permissible downward.
The block provides the option of making a distinction between static and dynamic loads, for example that can occur when quickly lifting loads.
To check the correct functioning of the measurement equipment, after a parameterizable interval expires, the system requests that the block is calibrated.



Note

When using this block, block **F_BO_W (FC 176)** and block **F_TP (FB 184)** must be available in the block folder. It is not permissible to renumber these! Blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)**, **LFMulDInt (FC 213)** and **LFDivDInt (FC 214)** are also required from this library. These may be renumbered, but not renamed.

3.7.1 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0, all TIME variables with T#0ms and all word variables with W#16#0.

3.7.1.1 Inputs

Name	Data type	Description
LOAD1	DInt	**Load channel 1 [%]** 10000 = 100.00%
LOAD2	DInt	**Load channel 2 [%]** 10000 = 100.00%
MAXTOL_LOAD	DInt	**Tolerance window load monitoring [%]** 10000 = 100.00%
MAXLOAD_MODE	Bool	**Monitoring mode** 0: Monitoring for static load 1: Monitoring for dynamic load
MAXLOAD_DYN	DInt	**Max. dynamic load [%]** 10000 = 100.00%
MAXLOAD_STAT	DInt	**Max. static load [%]** 10000 = 100.00%
MINLOAD	DInt	**Min. load** 10000 = 100.00%
T_INTERVAL	Time	**Test interval** After this time has elapsed, the block requests that the measurement equipment is tested. This is signaled at output TEST_REQ using a 1 signal.
T_SAMPLE	DInt	**Sampling time [ms]** Here, the block sampling time, i.e. the interval in which the safety program is called (cyclic interrupt OB interval of the F-OB) is parameterized in ms.
F_TEST:	DInt	**Test duration [ms]**
T_SETTLE	DInt	**Settling time [ms]**
VMAX_RELEASE	DInt	**Retraction velocity [mm/min]** For an overload/underload condition, this value is output at SLS_THRESHOLD
SAFE_V	DInt	**Safe velocity actual value [mm/min]** is supplied from block F_SAFE_POS.
V_VALID	Bool	**Actual velocity valid** is supplied from block F_SAFE_POS. 1: Velocity is plausible 0: Velocity is not plausible, i.e. the increase of the deviation between the two encoders over time is outside the tolerance window.
CAL_VALUE	DInt	**Calibration value (%)** 10000 = 100.00% Relevant for testing the measurement equipment
MAXTOL_CAL	DInt	**Calibration tolerance [%]** 10000 = 100.00%
CAL_MODE	Bool	**Test mode** 0: Test with constant load value 1: Test with defined load step
CALIBRATE	Bool	**Starting the measurement equipment test** The calibration test is started using a positive edge at this input. After the test has been successfully completed, the time for the test interval is restarted.
RELEASE	Bool	**Retracting** If the block detects an overload/underload condition, by selecting this input, the axis can be moved with the velocity parameterized at VMAX_RELEASE in the direction enabled by the block using MOVE_POSITIVE_OK/MOVE_NEGATIVE_OK. Retraction motion is immediately stopped as soon as this input has a 0 signal.

ACK	Bool	**Acknowledging** If a fault occurs in normal operation, then this must be reset using ACK before the system can be restarted. Acknowledgment is only realized with a positive edge at ACK; in fault-free (normal) operation has no effect.

3.7.1.2 Outputs

Name	Data type	Description
SLS_THRESHOLD	DInt	**SLS limit [mm/min]** The presently maximum permissible traversing velocity is output here. This is 2147483647 in normal operation; when overload/underload is detected, VMAX_RELEASE is output here. If VMAX_RELEASE has been parameterized <= 0, then an equivalent value of 1 is output here.
SLS_OK	Bool	**SLS limit status** 1: SAFE_V is less than/equal to SLS_THRESHOLD 0: SAFE_V has exceeded the value of SLS_THRESHOLD. If this output changes to 0, then a stop response should be initiated.
TEST_REQ	Bool	**Request to test the measuring equipment** 1: T_INTERVAL expired 0: Test not necessary
BUSY	Bool	**Test status** 1: Test running 0: Test not selected
TEST_OK	Bool	**Test result status** 0: Test faulty or test still not performed 1: Test successfully completed
DYN_LOAD_OK	Bool	**Status dyn overload** 0: Overload detected 1: Load OK
STAT_LOAD_OK	Bool	**Status stat. overload** 0: Overload detected 1: Load OK
MIN_LOAD_OK	Bool	**Underload status** 0: Slack cable detected 1: Load OK
MOVE_NEGATIVE_OK	Bool	**Negative motion permitted** If a 0 signal is available at this output, then it is not permissible that the machine continues to move in the negative direction. The output is set to 0 as soon as the block detects a slack cable condition.
MOVE_POSITIVE_OK	Bool	**Positive motion permitted** If a 0 signal is available at this output, then it is not permissible that the machine continues to move in the positive direction. The output is set to 0 as soon as the block detects a slack cable condition.
ACK_REQ	Bool	**Acknowledgment request** If a fault has occurred, however it is no longer active, and can therefore be acknowledged, then the block indicates this using a 1 signal at ACK_REQ.
ERROR	Bool	**Error** This output is set if the block has been incorrectly parameterized, or if the block in operation detects a potentially dangerous combination of input signals. The output remains set until an error is no longer active and has been acknowledged.
DIAG	Word	**Diagnostics word** Information about the function status and errors of the block are output here.

3.7.1.3 Structure of DIAG

Bit No.	Description	Reset condition
0	Discrepancy error load monitoring	LOAD1 and LOAD2 within MAXTOL_LOAD and positive edge at ACK
1	Overload detected	LOAD1 and LOAD2 less than MAXLOAD_STAT or MAXLOAD_DYN (depending on MAXLOAD_MODE) – MAXTOL_LOAD and positive edge at ACK
2	Slack cable detected	LOAD1 and LOAD2 greater than MINLOAD + MAXTOL_LOAD and positive edge at ACK
3	Parameterizing error, load limits	MINLOAD < MAXLOAD_STAT <= MAXLOAD_DYN
4	Settling process, calibration inadmissibly long	Restart test
5	Inadmissibly high load fluctuation during calibration	Restart test
6	Parameter error test times	T_TEST > T_SETTLE > 0 and both times integer multiple of T_SAMPLE
7	Retraction velocity exceeded	SAFE_V <= SLS_THRESHOLD and positive edge at ACK
8	Parameterizing error, value range	0 < VMAX_RELEASE <= 2147483647 and 0<= MAXLOAD_DYN / MAXLOAD_STAT / MINLOAD / CAL_VALUE / MAXTOL_LOAD / MAXTOL_CAL <= 10000 parameterized
9	Actual velocity invalid	Active velocity again valid and positive edge at ACK
10	Invalid value range input variables	LOAD1, LOAD2 in the range 0 to 10000 and positive edge at ACK
11	Error for internal calculation	Pos. edge at ACK, if the fault is no longer active
12	Reserved	---
13	Reserved	---
14	Reserved	---
15	Reserved	---

3.7.2 Scaling the input variables

The block expects that load limits or load actual values are entered as percentage to two decimal places, i.e. a value of 10000 corresponds to 100%. The user must carry out the scaling corresponding to the reference variable of the module used.
For example, for F-AI modules the reference variable is 27648. STEP7 Safety Advanced provides block "F_SCALE" specifically for this purpose.
If hardware is used with other reference variables, then the user is responsible for programming the scaling himself.

Safety note
Users must correctly calculate the load limit values in compliance with the requirements laid down in EN528. Users must appropriately interconnect the calculated limit values at the block.

3.7.3 Principle of operation

3.7.3.1 Parameterization

When parameterizing, it must be ensured that the following relationships can be represented as integer multiples:

T_TEST / T_SAMPLE

T_SETTLE / T_SAMPLE

Further, the following relationship between the input variables must apply:

MINLOAD < MAXLOAD_STAT <= MAXLOAD_DYN

T_TEST > T_SETTLE > 0

The permissible value ranges of the individual inputs should be taken from the table describing the inputs.

If not all of the specified preconditions are satisfied, then the block identifies this, and signals a parameterizing error with the appropriately set DIAG bits.

Note
The block only checks the parameterization when it is called for the 1st time. This increases the performance for further block operation.

As a consequence, it is not possible to reparameterize the system while it is in operation. The safety program must be regenerated and loaded each time that the block operating parameters are changed.

3.7.3.2 Load monitoring

1. If two independent sources are used for measuring the force, then after scaling these should be interconnected to inputs LOAD1 or LOAD2. If one measurement source is sufficient, then this is interconnected to both inputs.
2. If the difference between the two inputs is greater than the value parameterized at MAXTOL_LOAD, then ERROR = 1 and an error code is output at DIAG.
3. In addition, the velocity parameterized at VMAX_RELEASE is output at SLS_THRESHOLD.
4. If both values again lie within the parameterizable window using MAXTOL_LOAD, then output ERROR and DIAG can be set to 0 with a positive edge at ACK.
5. Using input MAXLOAD_MODE, a distinction can be made between monitoring for static overload (MAXLOAD_MODE = 0) and dynamic overload (MAXLOAD_MODE = 1).
6. For MAXLOAD_MODE =0, as soon as the value at LOAD1 or LOAD2 exceeds the value parameterized at MAXLOAD_STAT, this error is signaled to STAT_LOAD_OK using a 0 signal.
7. In addition, ERROR is set to 1 and an error code is output at DIAG.
8. For MAXLOAD_MODE =1, as soon as the value at LOAD1 or LOAD2 exceeds the value parameterized at MAXLOAD_DYN, this error is signaled to STAT_LOAD_OK using a 0 signal.
9. In addition, ERROR is set to 1 and an error code is output at DIAG.
10. As long as one of these errors is active, then the velocity parameterized at VMAX_RELEASE is output at SLS_THRESHOLD.
11. The response when MINLOAD is fallen below is essentially the same.

3.7.3.3 Retracting

12. The retraction function of the block can be activated using a 1 signal at input RELEASE. Further traversing in the positive direction is no longer permissible; the block signals this with a 0 signal at MOVE_POSITIVE_OK. Through an appropriate interconnection with the drive, users must ensure that in this case retraction is only possible downwards.
13. To facilitate retraction, DYN_LOAD_OK or STAT_LOAD_OK is reset to 1 with a rising edge at RELEASE; the drive stop response should be selected using a suitable user interconnection.
14. If, during retraction, the value of SAFE_V exceeds the value of SLS_THRESHOLD, then SLS_OK changes to 0.
15. If, in both cases LOAD1 and LOAD2 are again less than the active limit - MAXTOL_LOAD, then ERROR and DIAG bit 1 can be reset to 0 with a positive edge at ACK.
16. The maximum velocity is again output at SLS_THRESHOLD. (Maximum DINT value = 2147483647)
17. VMAX_RELEASE must lie in the range 1 – 2147483647; if values less than 1 are parameterized, the block detects this and signals it with DIAG bit No. 8. ERROR changes to 1. 1 is then output for the retraction velocity as equivalent value.
18. If, during retraction V_VALID = 0, then the retraction velocity can no longer be monitored in a safely-related way. Therefore, selection using RELEASE = 1 has no effect, and retraction motion is stopped. DIAG bit 9 and ERROR change to 1, SLS_OK has a 0 signal.

19. To exit this state, V_VALID must first be again set to a 1 signal using F_SAFE_POS by acknowledging.

Safety note
The signal for RELEASE must be generated in a safety-related fashion, e.g. by using a key-operated switch or similar device.

Safety note
The parameterization of input V_MAX_RELEASE must be adapted according to the permissible safely reduced velocity, derived from the application-specific risk assessment.

Warning
The interconnection of output MOVE_POSITIVE_OK must match the selection of drive function SDI for a positive direction. For MOVE_POSITIVE_OK = 0, motion in the positive direction must no longer be possible.
The same is true when interconnecting output MOVE_NEGATIVE_OK and inhibiting the negative direction of motion.
It is absolutely crucial that the block outputs are interconnected with the correct signals to control the drive.
Otherwise, inadmissible motion towards the end stops is possible, which cannot be identified internally in the block.

3.7.3.4 Testing the measuring equipment

20. After the time that can be parameterized at T_INTERVALL has elapsed, the force sensor must be tested; the block flags this using a 1 signal at TEST_REQ.
21. The test is started using a positive edge at CALIBRATE, and output BUSY changes to 1.
22. Depending on input CAL_MODE, as test variable, a constant load or a defined load step is expected.

Safety note
Parameter "T_INTERVAL" defines in which cyclic intervals the measuring equipment must be tested. The value, which must be configured here, depends on the specific application - and is also dependent on the specific risk assessment and the actual hardware architecture of the safety function.

3.7.3.4.1 Case a): Test with constant load

23. If a 0 signal is available at input CAL_MODE, then within T_SETTLE, the measured load at LOAD1 and LOAD2 must assume the calibration value that can be parameterized at CAL_VALUE - taking into account the tolerance parameterized at MAXTOL_CAL.
24. If this is not the case, then ERROR changes to a 1 signal and at DIAG bit 4 is set.
25. The measured load value at LOAD1 and LOAD2 must not deviate from CAL_VALUE by more than MAXTOL_CAL for the time parameterized at T_TEST.
26. If this is not the case, then ERROR changes to a 1 signal and at DIAG bit 5 is set.
27. After T_TEST expires - and there is a valid load value - BUSY is reset to 0, and output TEST_OK is set to a 1 signal.
28. If T_TEST is parameterized to be <= T_SETTLE, then DIAG bit 5 and ERROR are set to 1.

3.7.3.4.2 Case b): Test with defined load step

29. The load value must execute a defined load stroke if a 1 signal is available at input CAL_MODE. In so doing, the signal at LOAD1 and LOAD2 must assume the expected stroke of CAL_VALUE within T_SETTLE.
30. If this is not the case, then ERROR changes to a 1 signal and at DIAG bit 4 is set.
31. For the duration of T_TEST, the measured range (stroke) must not deviate by more than MAXTOL_CAL from the expected range that can be parameterized at CAL_VALUE.

32. If this is not the case, then ERROR changes to a 1 signal and at DIAG bit 5 is set to 1.
33. If, after T_SETTLE expires, the signal level measured at LOAD1 and LOAD2 is not higher than the initial value (before the test stroke was started) by the value CAL_VALUE (taking into account MAXTOL_CAL), then ERROR is set to 1 and DIAG bit 4 is set.
34. After T_TEST expires - and there is a valid value for the load step - BUSY is reset to 0, and output TEST_OK is set to a 1 signal.
35. If T_TEST is parameterized to be <= T_SETTLE, then at DIAG bit 6 and ERROR are set to 1.
36. A successful test is signaled at block output TEST_OK using a 1 signal. BUSY is reset to 0. TEST_OK remains set to 1 until the next time that TEST_REQ changes to 1, or a new test is started.

Note
A brake test is requested at each stop-start transition of the CPU.

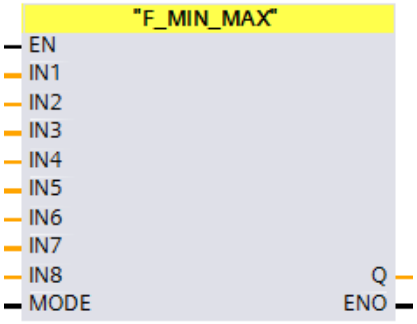
3.7.3.5 Acknowledging errors:

37. DIAG and ERROR are reset to 0 using a positive edge at ACK, assuming that there are no active errors.
38. As soon as the block can be acknowledged, it indicates this using a 1 signal at output ACK_REQ.
39. After a positive edge at ACK, ACK_REQ is reset to 0.

3.8 F_MIN_MAX

3.8.1 Introduction

The fail-safe F_MIN_MAX function executes a minimum/maximum value evaluation from up to 8 DINT values. The function can be used, for example, to select the presently most restrictive active SLS limit.



3.8.2 Connections

3.8.2.1 Inputs

Name	Data type	Description
IN1	DInt	Operand 1 for evaluation
IN2	DInt	Operand 2 for evaluation
IN3	DInt	Operand 3 for evaluation
IN4	DInt	Operand 4 for evaluation
IN5	DInt	Operand 5 for evaluation
IN6	DInt	Operand 6 for evaluation
IN7	DInt	Operand 7 for evaluation
IN8	DInt	Operand 8 for evaluation
MODE	Bool	Selects minimum/maximum evaluation 0: Minimum evaluation 1: Maximum evaluation

3.8.2.2 Outputs

Name	Data type	Description
Q	DInt	Depending on the particular MODE, minimum or maximum value of the 8 inputs

3.8.3 Principle of operation

3.8.3.1 Parameterization

1. The block is realized as function. This means that when called, all inputs must be interconnected. If a minimum/maximum value evaluation is to be carried out for less than 8 signals, then the signal sources should be interconnected a multiple number of times so that all of the inputs are occupied at the block.

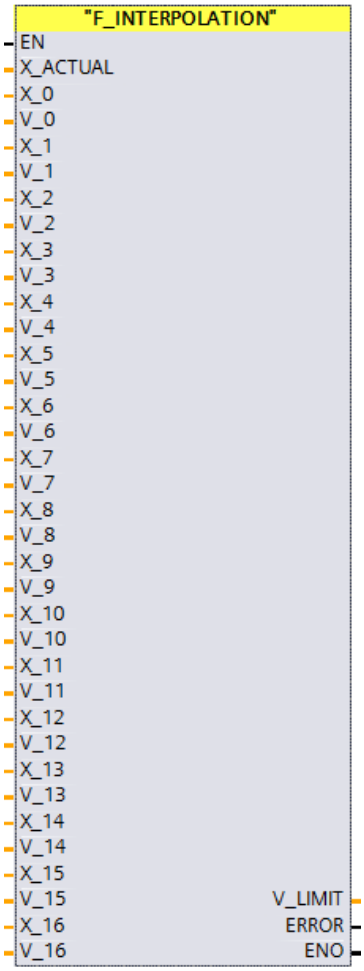
3.8.3.2 Evaluating the minimum/maximum value

2. If, at input MODE, there is a 1 signal, then the block carries out a maximum evaluation from the 8 inputs IN1-IN8. The highest of these up to 8 DINT values are made available at output Q.
3. If, at input MODE, there is a 0 signal, then the block carries out a minimum evaluation; this means the lowest of these 8 DINT values is output at Q.

3.9 F_INTERPOLATION

3.9.1 Introduction

The fail-safe F_INTERPOLATION function implements a linear interpolation across 17 interpolation points. It is used as subordinate function of block F_ENDZONE (Chapter3.4) to map the envelope curve.



Note

When using this block, blocks **LFAddDInt (FC 211)**, **LFSubDInt (FC 212)**, **LFMulDInt (FC 213)** and **LFDivDInt (FC 214)** are also required from this library. These may be renumbered, but not renamed.

3.9.2 Connections

3.9.2.1 Inputs

Name	Data type	Description
X_ACTUAL	DInt	Actual position [mm]
X_0	DInt	Position 0 [mm]
V_0	DInt	Velocity at position 0 [mm/min]
X_1	DInt	Position 1 [mm]
V_1	DInt	Velocity at position 1 [mm/min]
X_2	DInt	Position 2 [mm]
V_2	DInt	Velocity at position 2 [mm/min]
X_3	DInt	Position 3 [mm]
V_3	DInt	Velocity at position 3 [mm/min]
X_4	DInt	Position 4 [mm]

V_4	DInt	Velocity at position 4 [mm/min]
X_5	DInt	Position 5 [mm]
V_5	DInt	Velocity at position 5 [mm/min]
X_6	DInt	Position 6 [mm]
V_6	DInt	Velocity at position 6 [mm/min]
X_7	DInt	Position 7 [mm]
V_7	DInt	Velocity at position 7 [mm/min]
X_8	DInt	Position 8 [mm]
V_8	DInt	Velocity at position 8 [mm/min]
X_9	DInt	Position 9 [mm]
V_9	DInt	Velocity at position 9 [mm/min]
X_10	DInt	Position 10 [mm]
V_10	DInt	Velocity at position 10 [mm/min]
X_11	DInt	Position 11 [mm]
V_11	DInt	Velocity at position 11 [mm/min]
X_12	DInt	Position 12 [mm]
V_12	DInt	Velocity at position 12 [mm/min]
X_13	DInt	Position 13 [mm]
V_13	DInt	Velocity at position 13 [mm/min]
X_14	DInt	Position 14 [mm]
V_14	DInt	Velocity at position 14 [mm/min]
X_15	DInt	Position 15 [mm]
V_15	DInt	Velocity at position 15 [mm/min]
X_16	DInt	Position 16 [mm]
V_16	DInt	Velocity at position 16 [mm/min]

3.9.2.2 Outputs

Name	Data type	Description
V_LIMIT	DInt	Actual velocity limit [mm/min]
ERROR	Bool	Fault is active

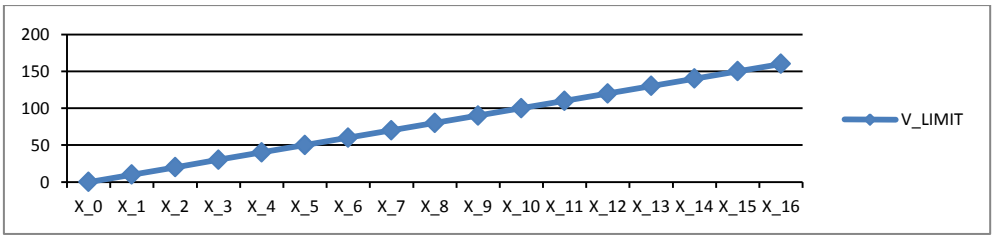
3.9.3 Principle of operation

3.9.3.1 Parameterization

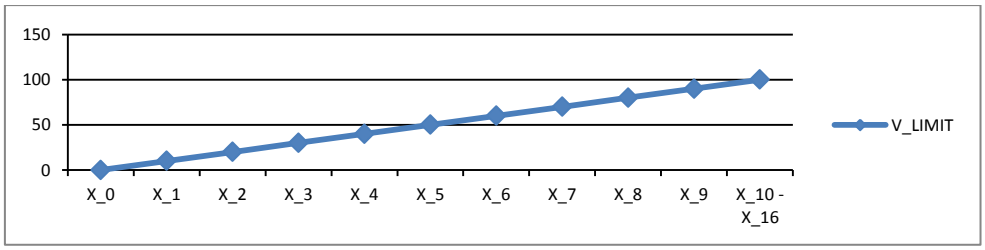
1. To start, the block checks the parameterization by checking that the X values of the interpolation points are valid. The X value of the subsequent interpolation point may not be less than the X value of the previous interpolation point.

3.9.3.2 Interpolation

2. If X_ACTUAL is identical to an X value of an interpolation point, then the associated V value of the interpolation point is directly output at V_LIMIT.
3. If X_ACTUAL lies between two interpolation points, then the value is calculated using linear interpolation and output at V_LIMIT. This is shown in the following diagram.



4. Is less than 17 interpolation points are required, all interpolation points above the last required point must be parameterized with its value. 11 interpolation points are required in the following diagram. As a consequence, interpolation points X_10/V_10 – X_16/V_16 have the same value.

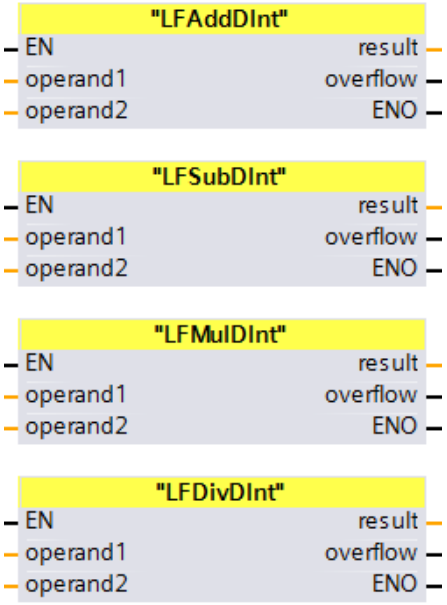


5. If an error occurs when parameterizing - or for an internal calculation, then this is output using ERROR = 1; the user program must then appropriately respond to this.

3.10 LFAddDInt/LFSubDInt/LFMulDInt/LFDivDInt

3.10.1 Introduction

For addition, subtraction, multiplication and division mathematical operations, the four fail-safe blocks check whether the result has exceeded the permissible value range of data type double integer (DINT). The functions are used within the blocks described in this library to execute and check mathematical calculations.



3.10.2 Connections

3.10.2.1 Inputs

Name	Data type	Description
operand1	DInt	Operand 1 for evaluation
operand2	DInt	Operand 2 for evaluation

3.10.2.2 Outputs

Name	Data type	Description
result	DInt	Result ("0" for overflow)
overflow	Bool	1: Overflow 0: No overflow

3.10.3 Principle of operation

3.10.3.1 LFAddDInt

1. The block adds operand1 and operand2. If the result lies in the valid value range, the result is output at result - and output overflow is set to false.
   If the valid value range after the mathematical operation is violated, at output result, a 0 is output and output overflow is set to true.

   result := operand1 + operand2

3.10.3.2 LFSubDInt

2. The block subtracts operand2 from operand1. If the result lies in the valid value range, the result is output at result - and output overflow is set to false.
   If the valid value range after the mathematical operation is violated, at output result, a 0 is output and output overflow is set to true.

result = operand1 - operand2

3.10.3.3 LFMulDInt

3. The block multiplies operand1 with operand2. If the result lies in the valid value range, the result is output at result - and output overflow is set to false.
   If the valid value range after the mathematical operation is violated, at output result, a 0 is output and output overflow is set to true.

   result = operand1 * operand2

3.10.3.4 LFDivDInt

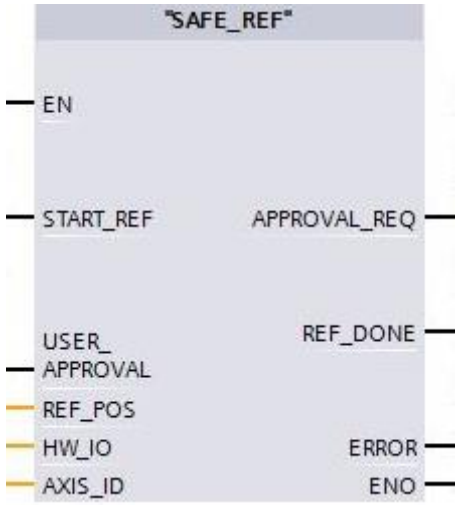
4. The block divides operand1 by operand2. If the result lies in the valid value range, the result is output at result - and output overflow is set to false.
   If the valid value range after the mathematical operation is violated, at output result, a 0 is output and output overflow is set to true.

   result = operand1 / operand2

3.11 SAFE_REF

3.11.1 Introduction

Function block SAFE_REF is used to reference the safety-related encoder signal in the SINAMICS drive. Referencing the safety-related encoder signal for SINAMICS drives must be performed in a defined sequence, in consecutive steps. This block is intended to simplify this sequence. The steps required for referencing are automatically activated one after the other and/or the parameter values are transferred to the drive corresponding to the connections that have been made at the block input.



Note

When using this block, block **SINA_PARA_S (FB287)**, from library "DriveLib_S71500_V13 -> Copy templates-> 02_EPOS_SINAMICS", must be available in the block folder. This cannot be renumbered, however, it can be renamed.

3.11.2 Connections

All bool type variables listed in the following table are preassigned FALSE, all integer variables with 0, HW_IO variables with 16#0 - and real variables with 0.0.

3.11.2.1 Inputs

Name	Data type	Description
EN	Bool	Block enable
START_REF	Bool	Start referencing
USER_APPROVAL	Bool	User agreement (approval) safe position
REF_POS	Real	Referencing position
HW_IO	HW_IO	Hardware ID of the actual value telegram slot - or the diagnostics address of the axis or drive
AXIS_ID	Int	Drive object number as parameterized in STARTER

3.11.2.2 Outputs

Name	Data type	Description
APPROVAL_REQ	Bool	User agreement (approval) expected
REF_DONE	Bool	Referencing completed
ERROR	Bool	The time until user agreement (approval) must have been given was exceeded.
ENO	Bool	Block was successfully executed

3.11.3 Safe referencing sequence

After setting an absolute reference position in the SINAMICS drive, the sequence described in the following must be complied with. The block handles the execution timing of these steps. The following sequence must be executed to safely reference in the drive.

Safety note

The user must ensure the correct mechanical position when initiating referencing.
The user must check the reference position transferred into the converter

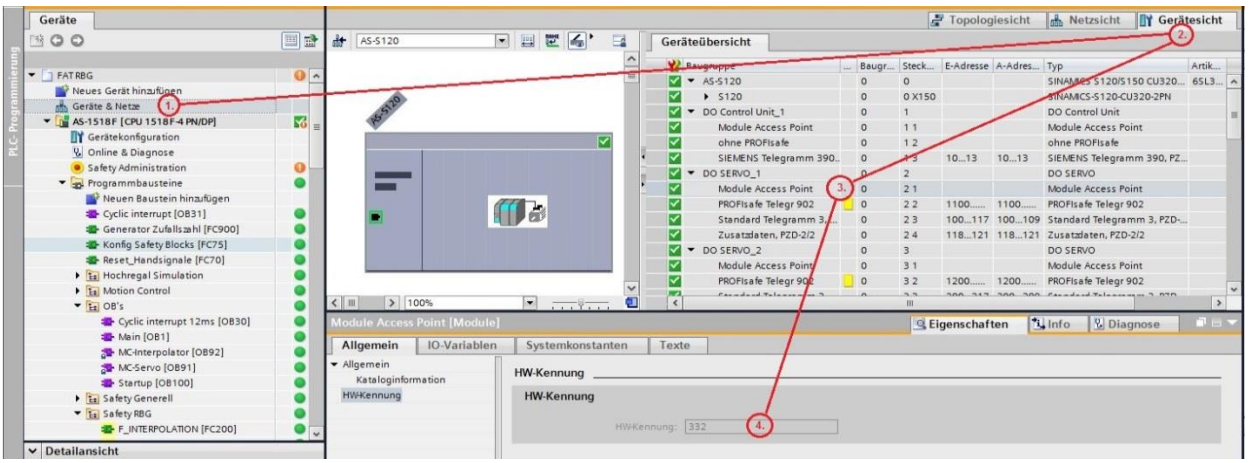
1. Deselect SI motion user agreement (p9726)
2. Deselect SI motion user agreement MM (p9740)
3. Set the SI motion reference position to a defined value (p9572)
4. Accept SI motion reference position (p9573)
5. Select SI motion user agreement (p9726)
6. Select SI motion user agreement MM (p9740)

Steps 5 and 6 must be selected within two seconds after accepting the reference position (p9573).

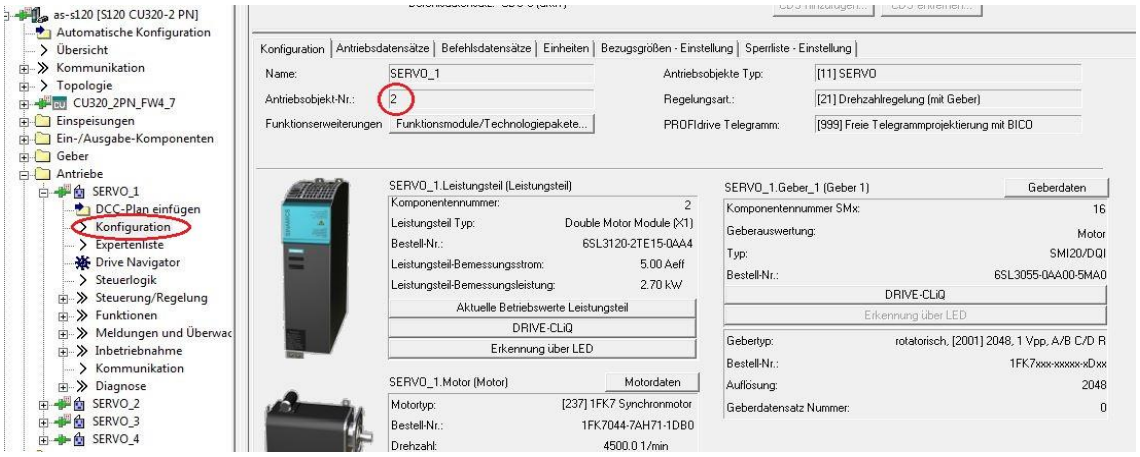
3.11.4 Principle of operation

3.11.4.1 Parameterization

1. When parameterizing it must be observed that the time in which the user agreement must be issued after activating the reference position, cannot be parameterized. In SINAMICS converters and at the described block, this is preassigned with two seconds.
2. The hardware ID of the axis must be specified at input HW_IO. Refer to the following diagram to understand at which location the hardware identification can be taken from in the TIA Portal.



3. The parameterized drive object number should be parameterized at input AXIS_ID; this is specified when configuring the drive in STARTER - and must be taken from the following location.



3.11.4.2 Safe position referencing

4. With a rising edge at input START_REF, the internal block signals are initialized - and the execution of the sequence for safe referencing initiated.

5. To start, the user agreement (p9726) and user agreement MM (p9740) are deselected
6. The position input parameterized at input REF_POS is transferred to the drive and then activated.
7. After activating the position input, within two seconds, the drive expects that the two user agreements are selected. The block signals this at output APPROVAL_REQ.
8. If, while output APPROVAL_REQ has a 1 signal, a 1 signal is detected at input USER_APPROVAL, then the user agreements are selected in the drive. And the block signals successful referencing at output REF_DONE.
9. If, after the time of two seconds expires, a 1 signal is not detected at input USER_APPROVAL, then the block resets output APPROVAL_REQ - and signals at output ERROR that referencing was not successfully completed.
10. Referencing can be restarted with a rising edge at input START_REF.

4 Interaction between the blocks

4.1 Overview

This chapter explains significant points, which must be taken into account when using fail-safe function blocks for storage and retrieval machines. The necessary block interconnection options are also shown as example.

The block package has a modular structure, and can be individually configured to address the particular application.
The blocks execute an autonomous subfunction. Depending on the specific machine in which they used, not all of the blocks are always required from the library.

If additional functions are required to specifically control an application, then users must realize this by adding additional fail-safe functions themselves. The signals of these functions are then interconnected with the RBG blocks.

Safety note

The safety-related times must be parameterized and the inputs and outputs interconnected corresponding to all of the directives applicable for the specific system. Further, they must be carefully checked at the system to ensure that they are in full compliance with the specific requirements.

4.2 Signal flow between components

The signal flow between the block interfaces, which can directly interact with one another, is shown in the following overview. For reasons of transparency, the additional inputs that are not connected are parameterized according to the above description, but are not interconnected in the following overview. This is because they do not exchange any information or data between the blocks, but are individually parameterized for each block.

4.2.1 Automation task

The signal flow between the block interfaces, which can directly interact with one another, is shown in the following overview. For reasons of transparency, the additional inputs that are not connected are parameterized according to the above specification, but are not interconnected in the following overview. This is because they do not exchange any information or data between the blocks, but are individually parameterized for each block.
In the following overview, the block interconnection monitors a hoisting gear so that it only traverses within a defined range. To achieve this, either block F_SLP_MONITOR or block F_ENDZONE is used. When F_ENDZONE is used, there is also the option that the machine may only approach the end zones with a reduced velocity.
The safe position and velocity required for the blocks mentioned above are supplied from block F_SAFE_POS.
Further, the hoisting gear is monitored for overload and slack cable using F_LOAD_MONITOR.
A block F_BRAKE_TEST is responsible for testing the correct functioning of the hoisting gear brakes.
If F_LOAD_MONITOR, F_BRAKE_TEST or F_SLP_MONITOR/F_ENDZONE identifies that a limit value has been violated, then the SLS threshold is also set to the value parameterized at the block.
Block F_SBR_MONITOR monitors as to whether the drive brakes along the configured down ramp after it selects an SS1. If this is not the case, then the signal to initiate STO is generated.
By ANDing all of the relevant enable signals of the blocks, the signal to initiate a stop response (e.g. SS1) can be formed for the drive.
For the retraction function of blocks F_ENDZONE, F_LOAD_MONITOR and F_SLP_MONITOR, using an AND logic operation of the corresponding MOVE_POSITIVE_OK/MOVE_NEGATIVE_OK signals, only that direction is permitted that allows the storage and retrieval machine to move away from the end zone.

If the brake test was unsuccessful, using block F_BRAKE_TEST, via output RELEASE_DIR, the hoisting gear can be prevented from moving upwards.

4.3 Response in the case of an error

If, when parameterizing the block, or as a result of an invalid input assignment, as a result of the process, a error occurs at a block, then each block in the library, with the exception of F_MIN_MAX, signals this using output ERROR = 1.
With the exception of F_MIN_MAX, the blocks in the library have a DIAG output; this allows more precise diagnostics based on the error code that is output.

4.4 Block interconnection

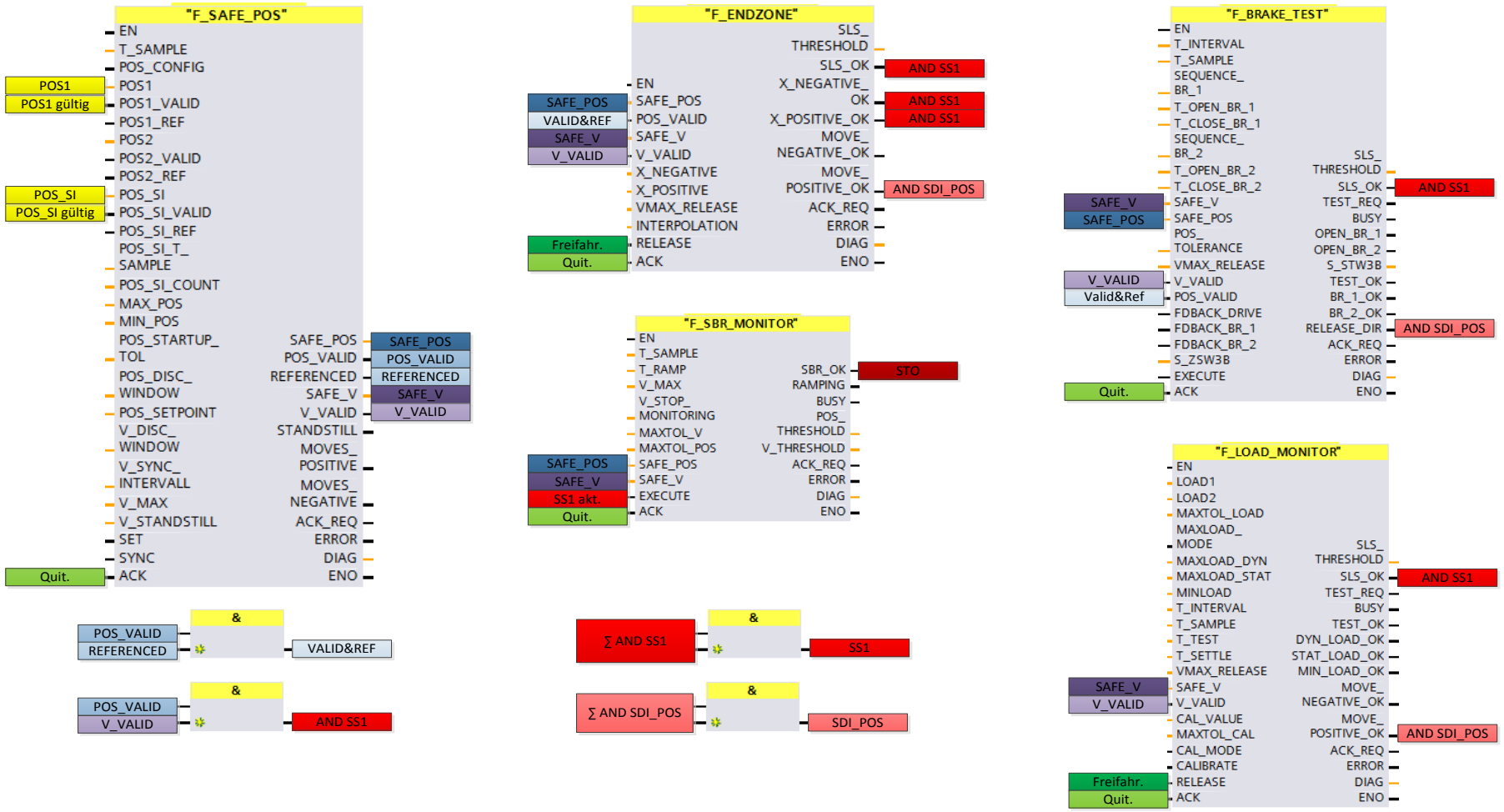


Fig. 13: Block interconnection

4.4.4 Additionally required blocks

The following blocks in the STEP7 Safety Advanced library are called in the fail-safe function blocks - and must therefore be available in the block folder:

See Chapter 3.1.2

4.4.5 Additional information

Information about configuring and parameterizing the hardware - as well as a description of handling STEP7 and the graphic editor (F-FBD or F-LAD) of SIMATIC safety - are described in the manuals listed:

- SIMATIC Safety - Configuring and Programming
  https://support.industry.siemens.com/cs/ww/de/view/54110126
- SINAMICS S120 Function Manual Safety Integrated
  https://support.industry.siemens.com/cs/ww/de/view/99668646

5 Abbreviations

CPU	Central Processing Unit
CU	Control Unit
DB	Data block
DINT	Double integer; 32 bit data type
DQ	Digital output
EPOS	Basic positioner; drive function
F-AI	Fail-safe analog module
F-CPU	Fail-safe central processing unit
FMEA	Failure mode and effects analysis
HTL	Type of incremental encoder
HW	Hardware
I-DB	Instance data block
INT	Integer; 16 bit data type
PL	Performance level
SBT	Safe Brake Test
SDI	Safe Direction
SI	Safety Integrated
SIL	Safe Integrity Level
SIN/COS	Sine-cosine; type of incremental encoder
SLS	Safely Limited Speed
SLU	Safe Length Unit
SOS	Safe Operating Stop
SRS	Safety Requirements Specification
SS1	Safe Stop 1
SS2	Safe Stop 2
SSI	Synchronous serial interface; type of absolute encoder
STARTER	Drive engineering tool
STO	Safe Torque Off

6 Support

Application Center

If you have any questions about the use of products described in this manual that have not been answered, then contact the Application Center in D-91056 Erlangen

mailto:tech.team.motioncontrol@siemens.com

or your local Siemens contact in the local office and business location.

http://www.automation.siemens.com/partner/

Training center

We offer courses to help you get started with the S7 automation system. Please contact your regional Training Center, or the central Training Center in D-90327 Nuremberg.

Phone: +49 (0)911 895–3200

http://www.sitrain.com/

***SIMATIC* documentation in the Internet/ Siemens Intranet**

• Documentation is available at no charge in the Internet at:

https://support.industry.siemens.com/

Contact the Knowledge Manager listed there to quickly locate the documentation that you require.

7 Appendix

7.1 Block runtimes

	CPU 1516F-3 PN/DP	*CPU 1517F-3 PN/DP*	*CPU 1518F-4 PN/DP*
F_SAFE_POS	1.150 µs	147 µs	71 µs
F_SLP_MONITOR	95 µs	16 µs	9 µs
F_ENDZONE	910 µs	105 µs	54 µs
F_BRAKE_TEST	500 µs	76 µs	39 µs
F_SBR_MONITOR	521 µs	58 µs	29 µs
F_LOAD_MONITOR	760 µs	86 µs	46 µs
Total, without F_SLP_MONITOR	**3841 µs**	**472 µs**	**239 µs**
Total, without F_ENDZONE	**3026 µs**	**383 µs**	**194 µs**

8 Notes