Product Manual

FSM 2.0 - MOV

for the ARS 2000 FS series servo drives

Metronix Meßgeräte und Elektronik GmbH
Kocherstraße 3
38120 Braunschweig
Germany

Telephone: +49 (0) 531-8668-0
Fax: +49 (0) 531-8668-555
E-mail: vertrieb@metronix.de
http://www.metronix.de

Translation of the original instructions

Revision Information	
Author:	Metronix Meßgeräte und Elektronik GmbH
Manual title:	Product Manual "FSM 2.0 - MOV"
File name:	P-HB_FSM_MOV_ARS2000_1p0_EN.docx
Version 1.0	July 2016

Identification of hazards and instructions on how to prevent them:

Warning

Hazards that can cause death or serious injuries.

Caution

Hazards that can cause minor injuries or serious material damage.

Other symbols:

Note

Material damage or loss of function.

Recommendations, tips, references to other documentation.

Essential or useful accessories.

Information on environmentally sound usage.

Text designations:

❖ Activities that may be carried out in any order.

1. Activities that should be carried out in the order stated.

– General lists.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Notes on this documentation

This documentation is intended to help you safely work with the safety functions

- STO – Safe Torque Off
- SS1 – Safe Stop 1
- SS2 – Safe Stop 2
- SOS – Safe Operating Stop
- SLS – Safely-Limited Speed
- SSR – Safe Speed Range
- SSM – Safe Speed Monitor
- SBC – Safe Brake Control

in accordance with EN 61800-5-2 through the usage of the safety module FSM 2.0 – MOV for the servo drive ARS 2000 FS.

❖ In addition, always observe the "Safety instructions for electrical drives and controllers" for the ARS 2000 FS servo drives.

The "Safety instructions for electrical drives and controllers" for the ARS 2000 FS servo drives can be found the product manuals that are listed in Table 2.

Observe the information regarding safety and on the requirements for product use in section 1.2.

Product identification

This documentation refers to the following versions:

- Safety module FSM 2.0 - MOV, from revision 1.1.
- Servo drive ARS 2000 FS with firmware from version 4.1.0.1.1 and the following hardware versions:
  - ARS 2102 FS: version 6.0 or higher
  - ARS 2105 FS: version 6.0 or higher
  - ARS 2108 FS: version 2.4 or higher
  - ARS 2302 FS: version 4.1 or higher
  - ARS 2305 FS: version 4.1 or higher
  - ARS 2310 FS: version 4.1 or higher
- Metronix ServoCommander® (MSC) parameterisation software version 4.1.0.1.1 or higher with SafetyTool version 1.0.2.1 or higher.

These are the first available of supported versions. In the case of more versions or the replacement of the safety module, check whether the versions are compatible ➔ see documentation of the appropriate version used.

Type key

The functional safety modules are available in different versions in terms of the integrated functional safety. Example (FSM 2.0 – MOV):

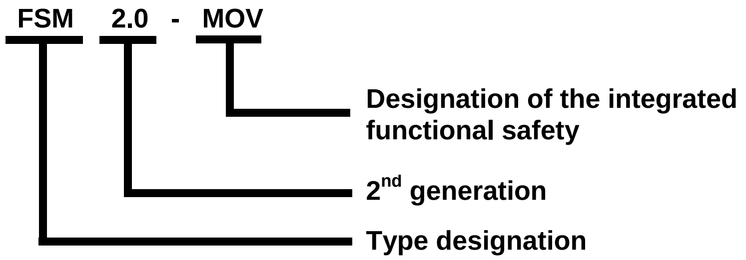


Figure 1: Type key example (FSM 2.0 – MOV)

Support

Please consult your sales partner if you have any technical queries.

Issue status of the specified standards

Standard: issue status	
EN 50178:1997	EN ISO 13849-1:2008
EN 61326-3-1:2008	EN ISO 13849-2:2012
EN 61800-3:2004 + A1:2012	EN 62061:2005
EN 61800-5-1:2007	EN 61508-1 to -7:2010
EN 61800-5-2:2007	

Table 1: Issue statuses of the specified standards

Documentation

You will find information on the servo drives in the following documentation:

User documentation on the ARS 2000 FS servo drives	
Name, type	**Content**
Product manual "Servo Drive ARS 2100 FS"	Description of the technical data and device functionality plus notes concerning the installation and operation of ARS 2102 FS, ARS 2105 FS, and ARS 2108 FS servo drives.
Product manual "Servo Drive ARS 2302 FS – ARS 2310 FS"	Description of the technical data and device functionality plus notes concerning the installation and operation of ARS 2302 FS, ARS 2305 FS, and ARS 2310 FS servo drives.
Product manual "FSM 2.0 - STO"	Description of the functional safety technology for the ARS 2000 FS servo drives with the safety function STO.
Product manual "FSM 2.0 - MOV"	Description of the functional safety technology for the ARS 2000 FS servo drives with the safety function MOV (this product manual).
Software manual "Servo drives ARS 2000 FS"	Description of the device functionality and software functions of the firmware, including the RS232 communication. Description of the Metronix ServoCommander® parameterisation software with instructions concerning the start-up of the ARS 2000 FS servo drives.
Mounting instructions "Servo drives ARS 2102 FS, 2105 FS, and 2108 FS"	Instructions concerning the commissioning of the servo drives ARS 2102 FS, 2105 FS, and 2108 FS.
Mounting instructions "Servo drives ARS 2302 FS, 2305 FS, and 2310 FS"	Instructions concerning the commissioning of the servo drives ARS 2302 FS, ARS 2305 FS, and ARS 2310 FS.
Help concerning the SafetyTool	User interface and functions of the SafetyTool for the parameterisation of the FSM 2.0 – MOV safety module.
Online help of the parameterisation program Metronix ServoCommander®	User interface and functions of the Metronix ServoCommander®
Other fieldbus manuals for the ARS 2000 servo drives	Description of the implemented fieldbus protocols

Table 2: Documentation on the ARS 2000 FS servo drives

ℹ You can find all of these documents on our homepage for download: http://www.metronix.de.

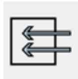
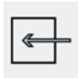
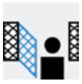
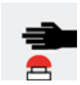
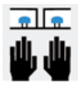
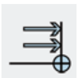
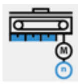
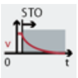
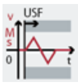
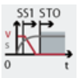
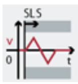
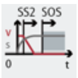
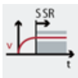
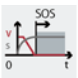
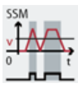
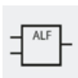
Safety engineering system symbols used			
Inputs and outputs			
	Input, two-channel		Output, two-channel
	Input, single-channel		Relay output
Sensor types			
	Mode selector switch		Start button
	Holding brake		Exit safety function (restart)
	Light curtain		Door lock/safety guard
	Emergency stop switches		Enabling buttons
	Acknowledgement		Two-hand control device
	Reliable reference switch		Position encoder
Safety functions			
	STO – Safe Torque Off		USF – Universal Safety Function
	SS1 – Safe Stop 1		SLS – Safely-Limited Speed
	SS2 – Safe Stop 2		SSR – Safe Speed Range
	SOS – Safe Operating Stop		SSM – Safe Speed Monitor
	SBC – Safe Brake Control		ALF – Advanced Logic Function, not a safety function

Table 3: Safety engineering system symbols

1 Safety and requirements for product use

1.1 Safety

1.1.1 General safety information

❖ In addition, always observe the "Safety instructions for electrical drives and controllers" for the ARS 2000 FS servo drives.

The "Safety instructions for electrical drives and controllers" for the ARS 2000 FS servo drives can be found the product manuals that are listed in Table 2 on page 23.

Note

Failure of the safety function.

The safety functions might fail if you do not comply with the parameters and conditions required for the surroundings and connections.

❖ In particular, you must provide input voltages within the specified tolerances ➔ Technical data, appendix 7.1.

Note

Incorrect handling can damage the safety module or servo drive.

❖ Switch off the supply voltage before mounting and installation work. Switch on the supply voltage only when mounting and installation work are completely finished.

❖ Never unplug the safety module from, or plug it into the servo drive when powered!

❖ Observe the specifications for handling electrostatically sensitive devices.

1.1.2 Intended use

The safety module FSM 2.0 – MOV serves as an expansion of the servo drives ARS 2000 FS to implement the safety function:

- STO – Safe Torque Off
- SS1 – Safe Stop 1
- SS2 – Safe Stop 2
- SOS – Safe Operating Stop
- SLS – Safely-Limited Speed
- SSR – Safe Speed Range
- SSM – Safe Speed Monitor
- SBC – Safe Brake Control

When suitable position transmitters are used and with suitable activation of the safety module, the requirements are fulfilled in accordance with EN 61800-5-2 up to and including SIL3 and in accordance with EN ISO 13849-1 up to and including Category 4 / PL e.

Depending on the encoders used for position recording, it is possible that only SIL2 is implemented ➔ Section 1.1.4.

The servo drive ARS 2000 FS with the safety module FSM 2.0 – MOV is a product with safety-relevant functions and is intended for installation in machines or automation systems. Use it only:

- in excellent technical condition,
- in its original state without unauthorised modifications,
- within the product's limits as defined by the technical data ➔ appendix 7.1,
- in an industrial environment.

The functional safety modules of the FSM 2.0 series can be operated in all servo drives of the ARS 2000 FS series. They have a slot for functional safety modules ("FSM slot"). The safety modules cannot be plugged into one of the extension slots for technology modules (TECH1 or TECH2).

➔ **Note**

In the event of damage caused by unauthorised manipulation or improper use, the guarantee is invalidated and the manufacturer is not liable for damages.

1.1.3 Foreseeable misuse

The following misuses are among those not approved as intended use:

- use in a device other than the ARS 2000 FS servo drive,
- use outdoors,
- use in non-industrial areas (residential areas),
- use outside the limits of the product defined in the technical data,
- unauthorised modifications.

➔ **Note**

- The STO function must not be used as the sole safety function for drives subject to permanent torque (e.g. suspended loads). Take this into account through the use of suitable measures, e. g. a clamping unit.
- Bypassing of safety equipment is no allowed.
- Repairs to the safety module are not allowed! A professional replacement of the safety module is permissible.

i The STO (Safe Torque Off) function does not provide protection from electric shock, only from hazardous movements! The drive is not disconnected from the power supply as is required for electrical safety.

➔ Product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS

1.1.4 Achievable safety level, safety function in accordance with EN ISO 13849-1/EN 61800-5-2

The safety module fulfils the basic test requirements

- Category 4, PL e in accordance with EN ISO 13849-1,
- SIL CL 3 in accordance with EN 62061,

and can be used in applications up to cat. 4 / PL e in accordance with EN ISO 13849-1 and up to SIL 3 in accordance with EN 62061 / IEC 61508.

The achievable safety level depends on the other components used to implement a safety function.

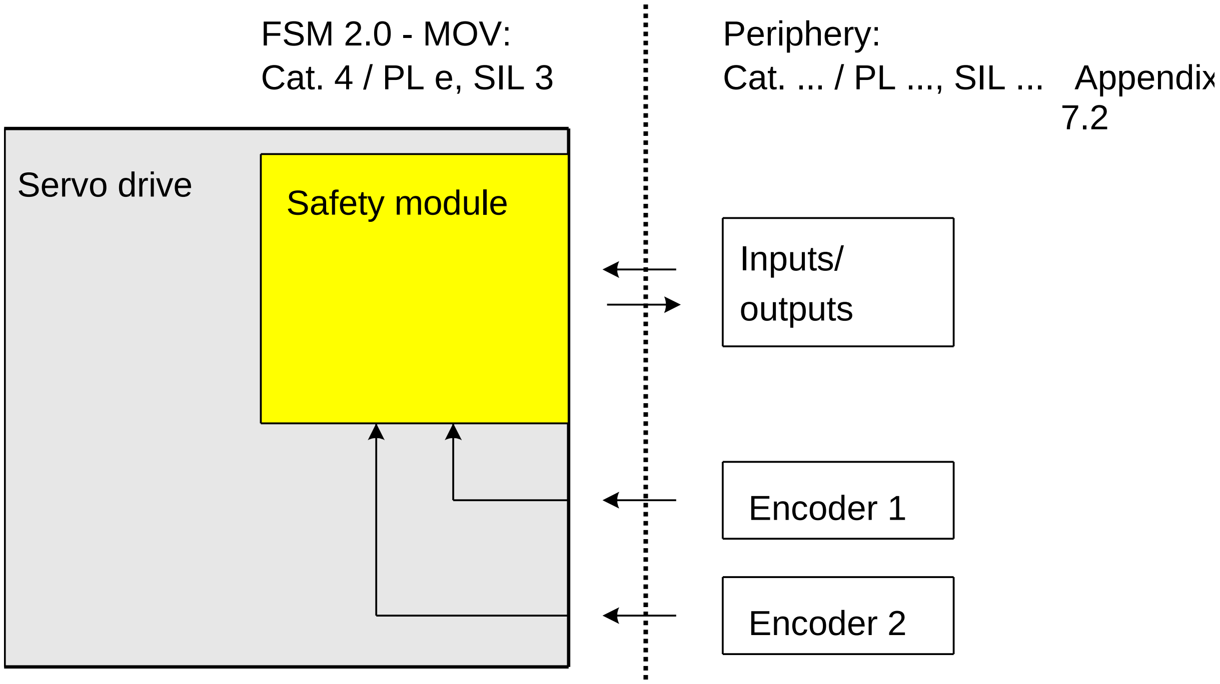


Figure 2: Safety level FSM 2.0 – MOV and complete system

Take into account the approved combinations of position encoders along with the corresponding notes ➔ Section 2.2.5, Table 10.

You can find information on the characteristic safety values, which can be implemented with the corresponding peripherals, for the different safety functions in ➔ appendix 7.1.

1.2 Requirements for product use

- ❖ Make the complete documentation available to the design engineer, installation technician and personnel responsible for commissioning the machine or system in which this product is used.
- ❖ Make sure that the specifications of the documentation are always complied with. When so doing, also take into account the documentation for the other components and modules (e. g. servo drives, circuits etc.).
- ❖ Take into consideration the legal regulations applicable at the installation site, as well as:
  - – regulations and standards,
  - – regulations of the testing organisations and insurers,
  - – national specifications.
- ❖ The safety module fulfils the requirements of the EN 61800-5-2. Additional regulations, standards and directives apply to the other safety devices used in the machine and their use, and must also be taken into account.
- ❖ For emergency stop applications, protection from automatic restart corresponding to the required category must be planned. This can be achieved, for example, with an external safety switching device or suitable parameterisation of the safety module FSM 2.0 – MOV ➔ Section 2.7.

1.2.1 Technical prerequisites

General information for the correct and safe use of the product, which must be observed at all times:

- ❖ Comply with the connection and environmental conditions of the safety module (➔ appendix 7.1), servo drive, and all connected components.
  The product can only be operated in compliance with the relevant safety regulations if you comply with the limit values and load limits.
- ❖ Observe the instructions and warnings in this documentation.

1.2.2 Qualification of the specialised personnel (personnel requirements)

The device may only be set into operation by a qualified electrical technician who is familiar with:

- – how to install and operate electrical control systems,
- – the applicable regulations for operating safety-engineered systems,
- – the applicable regulations for accident protection and operational reliability, and
- – the documentation for the product.

1.2.3 Diagnostic coverage (DC)

Diagnostic coverage depends on the integration of the servo drive with safety module into the control loop system, the motors/position encoders used, as well as the implemented diagnostic measures.

If a malfunction is detected during the diagnostics, appropriate measures must be taken to maintain the safety level.

➔ **Note**

The reaction of the safety module to detected faults can be parameterised accordingly, e.g. activate the safety functions SS1 and SBC if there is a cross-circuit of safe input signals.

➔ **Note**

Check whether cross-circuit detection of the input circle and the connection wiring is required in your application.

If needed, use a safety switching device with cross-circuit detection to activate the safety module or use the safe outputs of the safety module for the supply of passive switching devices together with the corresponding monitoring functions of the safe inputs.

1.2.4 Range of application and certifications

The servo drive with built-in safety module is a safety device in accordance with the EC Machinery Directive 2006/42/EC; the servo drive has the CE logo.

Safety-oriented standards and test values, which the product must comply with and fulfil, can be found in the section "Technical data" ➔ Appendix 7.1. The product-relevant EC directives and standards can be found in the declaration of conformity.

i Certificates and declarations of conformity on this product can be found at http://www.metronix.de.

2 Product description of the safety module FSM 2.0 – MOV

2.1 Product overview

2.1.1 Purpose

As processes become increasingly automated, protecting people from potentially hazardous movements is gaining in importance. Functional safety refers to measures required of electrical or electronic equipment to reduce or eliminate malfunction-induced dangers. In normal operation, protective devices prevent human access to hazardous areas. In certain operating modes, during set-up, for example, people need to be in hazardous areas. In such situations, the machine operator must be protected by drive and internal control measures.

The functional safety engineering integrated with the safety module FSM 2.0 – MOV in the ARS 2000 FS servo drives meets the requirements of the controller and drive for optimised implementation of protective functions. Planning and installation complexity are reduced. The use of integrated functional safety engineering produces extended machine functionality and better availability over the levels achieved by conventional safety engineering.

The servo drives of the ARS 2000 FS series can be equipped with plug-in modules for integrated functional safety technology. The following modules are available.

Type	**Description**
FSM 2.0 – FBA	Fieldbus activation module with DIP switches, **no safety function**.
FSM 2.0 – STO	Safety module with DIP switches and STO function.
FSM 2.0 - MOV	Safety module with the STO, SS1, SS2, SOS, SBC, SLS, SSR, SSM functions and DIP switches.

Table 4: Overview of the safety and fieldbus activation modules for the ARS 2000 FS

2.1.2 Performance characteristics

The safety module FSM 2.0 – MOV has the following performance characteristics:

- Implementation of one or more of the safety functions:
  - STO – Safe Torque Off
  - SS1 – Safe Stop 1
  - SS2 – Safe Stop 2
  - SOS – Safe Operating Stop
  - SLS – Safely-Limited Speed
  - SSR – Safe Speed Range
  - SSM – Safe Speed Monitor
  - SBC – Safe Brake Control
- Two-channel and single-channel inputs to request the safety function.
- Two-channel safe outputs to control additional safety elements and functions.
- Potential-free acknowledgement contact for the operating status.
- Design as a module that can be plugged in from the outside thus enabling retrofits.

This functional safety engineering integrated in the servo drive allows:

- Shortest reaction times through more rapid detection of possibly hazardous statuses.
- Comprehensive detection of hazards through rapid, direct access to a wide range of signals and measured variables in the servo drive.
- Analysis of a wide range of position transmitters, such as resolvers, SIN/COS encoders, HIPERFACE encoders, and also the analysis of position transmitters with purely serial protocols (EnDat 2.2, BISS).
- If necessary, rapid, direct manipulation of the setpoints / control system of the drive controller. An axle can also be safety and precisely brought to idle without action by the functional controller / PLC or braked to a limited speed.
- Direct interaction between the sequence control in the servo drive and the safety module. In this way, for example, the clamping unit or holding brake, after a request of the SBC safety function and the subsequent restart, is only opened when the servo drive is actively controlling the position. This avoids "dropping" of vertical axles and there is no need to program a sequence in the function controller.

2.1.3 Supported devices

The safety module FSM 2.0 – MOV can only be used in servo drives in conformity with section 1.1.2.

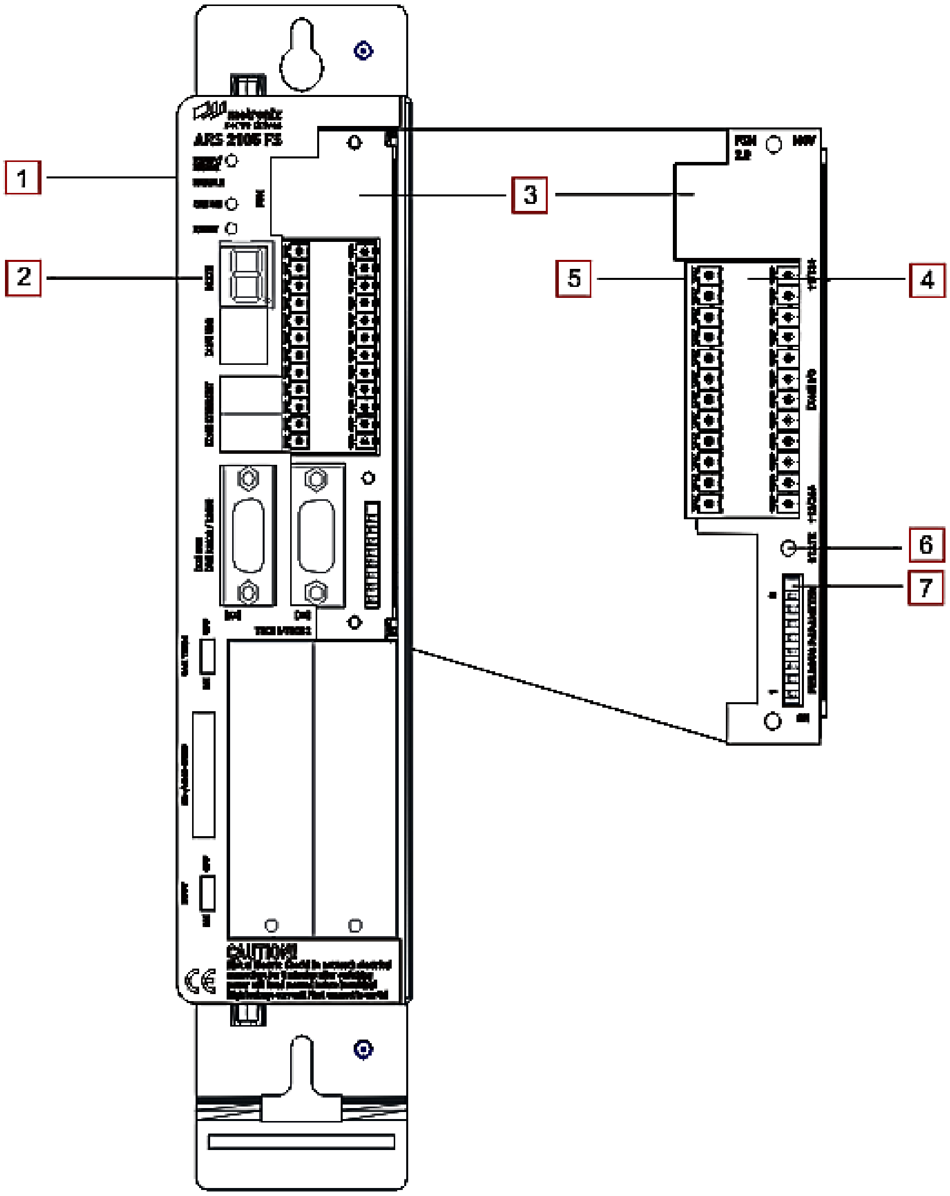
The servo drives of the ARS 2000 FS series are delivered with the FSM 2.0 – FBA module without any integrated functional safety.

The use of safety module FSM 2.0 – MOV enables the safety functions described in this documentation for the integrated functional safety of safety-relevant motion monitoring and motion control to be expanded.

If no safety functions are required, the module FSM 2.0 – FBA must be inserted in the FSM slot for safety modules.

2.1.4 Operating elements and connections

The safety module FSM 2.0 – MOV has the following control sections, connections and display components:



1 Servo drive ARS 2000 FS with a slot for functional safety modules

2 7-segment display of the servo drive to display the active safety function or error messages of the safety module

3 Safety module FSM 2.0 – MOV

4 I/O interface [X40A] and [X40B] to control the safety functions

5 Pin 1 of the interface [X40]

6 LED for display of the operating status (status of functional safety)

7 DIP switch (activation/configuration of the fieldbus communication in the servo drive)

Figure 3: Control section an connections FSM 2.0 – MOV

2.1.5 Scope of delivery

1x	**Safety module FSM 2.0 – MOV**	
	Type	FSM 2.0 – MOV for the safety functions STO, SS1, SS2, SOS, SLS, SSR, SSM, SBC
	Metronix order number	9200-0152-00
	Auxiliary equipment	
	1x	Mounting accessories (2 screws with spring washer)
	1x	2 plug for I/O interface [X40A], [X40B] PHOENIX Mini-Combicon MC1.5_12-ST-3.81-BK
	1x	Brief description with mounting instructions in German/English

Table 5: Scope of delivery FSM 2.0 – MOV

2.2 Function and application

2.2.1 System overview

The following figure shows a typical drive system with integrated functional safety design, comprising the following components:

– servo drive ARS 2000 FS,
– safety module FSM 2.0 – MOV,
– synchronous servo motor,
– linear axle with second measuring system,
– reliable clamping unit.

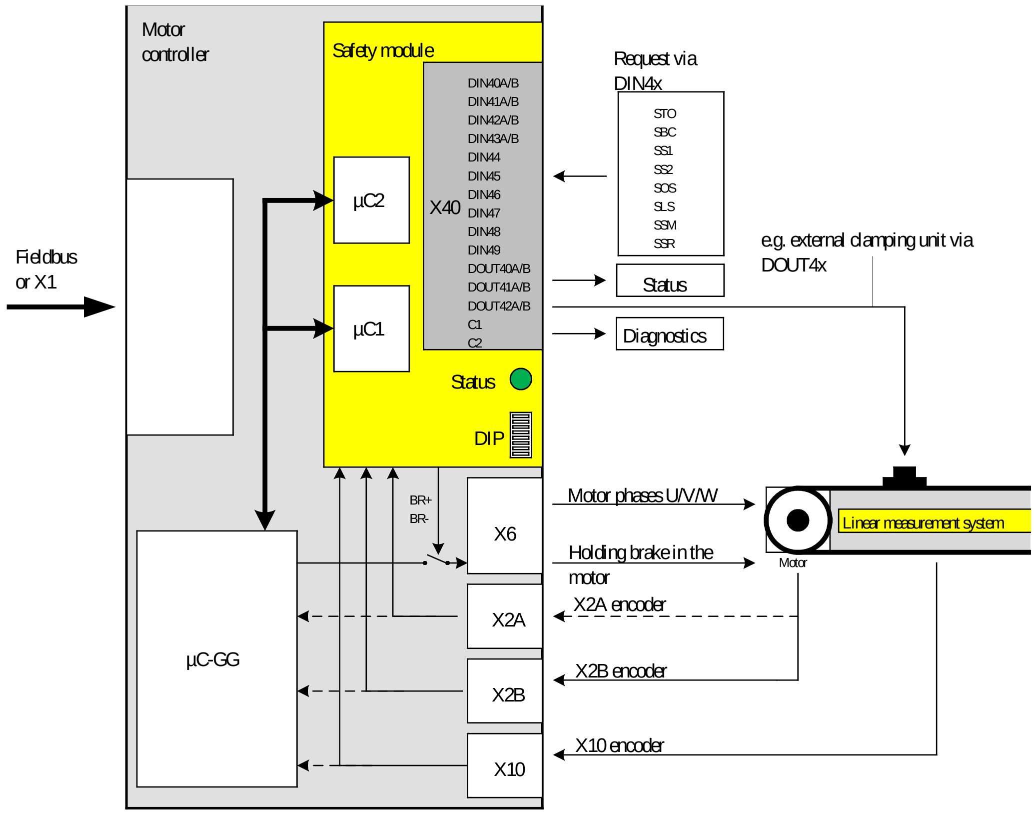


Figure 4: Safety module functional principle

The actual drive control and function control of the axle of motion takes place a usual via the servo drive ARS 2000 FS and the assigned control interfaces, e. g. [X1] or a fieldbus.

The safety module monitors the function of drive controller of the servo drive. For this, the safety-relevant variables of the motor movement are recorded and monitored according to the selected safety functions. If the safety limits are exceeded (e.g. a maximum permissible speed), then the safety module can, for example, safely switch off the driver supply for the output semi-conductors, thus preventing the power output stage from supplying the energy required by the motor.

Note

Technical failure or failure of the power supply will lead to a switch-off of the power output stage of the servo drive. Safety limitations could be the result, depending on the application.

The safety module monitors the safety of the axle as follows:

– In the FSM 2.0 – MOV, there are two microcontrollers in a redundant structure. During operation, they continuously compare all the relevant input and output signals as well as the data of the position encoders.
– The safety functions in the FSM 2.0 – MOV are requested or activated via the digital safe inputs on the safety module, by other safety functions or as an error response. Logic operations can be used to set which digital inputs in which signal combination request a safety function.
– As soon as a safety function is active, safe monitoring of the status of the basic unit and axle takes place.
– For this, the safety module detects the movement of the axle (position, speed) via the position encoder in the motor and, depending on the system structure, via a second measuring system.
– For this, the position sensors are connected to [X2A], [X2B] and [X10] on the basic unit, as usual. The signals are forwarded internally to the safety module.

Important: The second measuring system on the axle may be essential, depending on the requested safety classification and the axle configuration.

– If the axle is in the safe status, the safety function signals the status SSR, "Safe State Reached", and, when the safety conditions are violated, the safety function signals the status SCV "Safety Condition Violated".
– The safety module has safe digital outputs, in order to signal the safety status to the outside, e.g. to an external safety controller or an additional FSM 2.0 – MOV or to supply digital inputs with test pulses.
– The safety module uses an internal device path to control the brake control output at the motor connection [X6], thus allowing the safety function SBC in combination with an appropriately-certified clamping unit.
– An external clamping unit can also be activated via a safe digital output and an external safe switching device.

Important: To use the safety function SBC, a clamping unit with corresponding safety classification must be used. For all types of holding brakes or clamping units without certification, a risk analysis must be carried out and the suitability determined for the appropriate safety application. Otherwise, these may not be used.

The holding brake in motors is not usually qualified and is thus not suitable.

- A potential-free signal contact is available for diagnostic purposes.
- The operating status of the safety module is displayed by a status LED and the 7-segment display of the basic unit.

Data is exchanged between the safety module and the basic unit via an internal communication interface.

- This means that the basic unit is always aware of the current operating status of the safety module, e.g. whether a safety function is requested and executed, or whether a violation of a safety condition is detected.
- This means that the operating status of the safety design can be signalled to the functional controller via the different fieldbus interfaces.
- The safety module can actively manipulate the controller of the basic unit, without having to go through the function controller. For example, the drive can actively be decelerated to the zero speed when the safety function SS2 is requested.

Important: This function is primarily beneficial when individual axles are moved. By contrast, if the axle is moved in an interpolating operating mode (e.g. CAN interpolated position mode), then this function makes less sense.

Additional functions of the firmware in the safety module:

- Safe switch-off of the servo drive in case of error, variable reaction to various errors.
- Analysis of the signals of the safe inputs, monitoring of the correct function of the hardware (test pulses).
- Control of the safe outputs, monitoring of the correct function of the hardware.
- Safe monitoring of the correct function of the microcontrollers: Cyclical test of the memory (RAM, Flash) and the CPU.
- Monitoring of the supply voltages.
- Cross-monitoring of the two involved microcontrollers.
- Management of the parameter sets, implementation of a safe parameterisation, secured with check sums and a password.

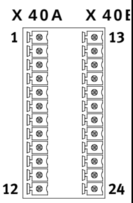
2.2.2 Circuitry of the safety module [X40]

To connect the safety functions, the safety module has a 24-pin interface [X40A/B] with the following connections:

- 4 digital, two-channel sensor inputs with configurable allocation (SIL3 inputs),
- 6 digital, single-channel inputs with configurable allocation (max. SIL2 inputs), e.g. as
  - 1 digital, 3-pole mode selector switch
  - 1 input for error acknowledgement
  - 1 input to control the restart after a safety function was requested
  - 1 input for a feedback signal of an external clamping unit
- 3 digital, two-channel outputs (SIL3) with configurable allocation, optionally useable as clock output,
- 1 acknowledgement contact (relay contact) for diagnostic purposes,
- reference potential for all inputs and outputs,
- a 24 V auxiliary current supply for connected sensors.

Table 6 shows the connections, arranged by function. You can find the pin allocation arranged by pin numbers in ➔ Section 3.2, Electrical installation.

Designation	Description (factory setting[1])	Pin, plug
Digital inputs		
DIN40A	Digital input 40, two-channel (factory setting: emergency stop switching device, STO and SBC request)	X40A.1
DIN40B		X40A.2
DIN41A	Digital input 41, two-channel	X40B.13
DIN41B		X40B.14
DIN42A	Digital input 42, two-channel	X40A.3
DIN42B		X40A.4
DIN43A	Digital input 43, two-channel	X40B.15
DIN43B		X40B.16
DIN44	Digital input 44 (factory setting: brake activation feedback)	X40A.7
DIN45	Digital inputs 45, 46, 47 (factory setting: mode selector switch)	X40A.8
DIN46		X40A.9
DIN47		X40A.10
DIN48	Digital input 48 (factory setting: error acknowledgement)	X40A.11
DIN49	Digital input 49 (factory setting: terminate safety function on rising edge)	X40A.12
Digital outputs and signal contacts		
DOUT40A	Digital output 40, two-channel	X40A.5
DOUT40B		X40A.6
DOUT41A	Digital output 41, two-channel	X40B.17
DOUT41B		X40B.18
DOUT42A	Digital output 42, two-channel	X40B.19
DOUT42B		X40B.20
C1	Signal contact, relay contacts (factory setting: safe state reached, no safety condition violated) – Open: "Safety function not active" – Closed: "Safety function active"	X40B.21
C2		X40B.22
Reference potential and auxiliary supply		
GND24	0 V, reference potential for DINx / DOUTx / +24 V	X40B.23
+24 V	24 V output, auxiliary supply, e.g. for safety peripherals (24 V DC logic supply of the servo drive)	X40B.24



1) Function in the delivery status or after resetting to factory settings (advance parameterisation)

Table 6: Digital inputs and outputs, signal contact, reference potential and auxiliary supply [X40]

2.2.3 Overview of the supported safety functions

The safety module supports the following safe stop and safe movement functions:

Function	Number	Comment	
STO	1	Uncontrolled stopping, safe restart interlock ➔ Section 2.5.3	
SS1	1	Controlled stopping with subsequent STO ➔ Section 2.5.5	
SS2	1	Controlled stopping with subsequent SOS ➔ Section 2.5.6	
SOS	1	Safe stop (with "fine rotational speed limit"1)) ➔ Section 2.5.7	
USF	4	"Universal Safety Function", combined safety functions. In the "Safe Speed Function" (SSF) version, the following safety functions can be implemented with appropriate parameterisation:	
		SLS	Safely limited speed ➔ Section 2.5.10
		SSR	Safe speed range ➔ Section 2.5.11
		SSM	Safely monitored speed ➔ Section 2.5.12
SBC	1	Safe brake control ➔ Section 2.5.4	
1) A slow movement within the monitored position window can be permissible			

Table 7: Equipment of the safety module

2.2.4 Functional diagram of the safety module

The functions of the safety module are explained using the following functional diagram:

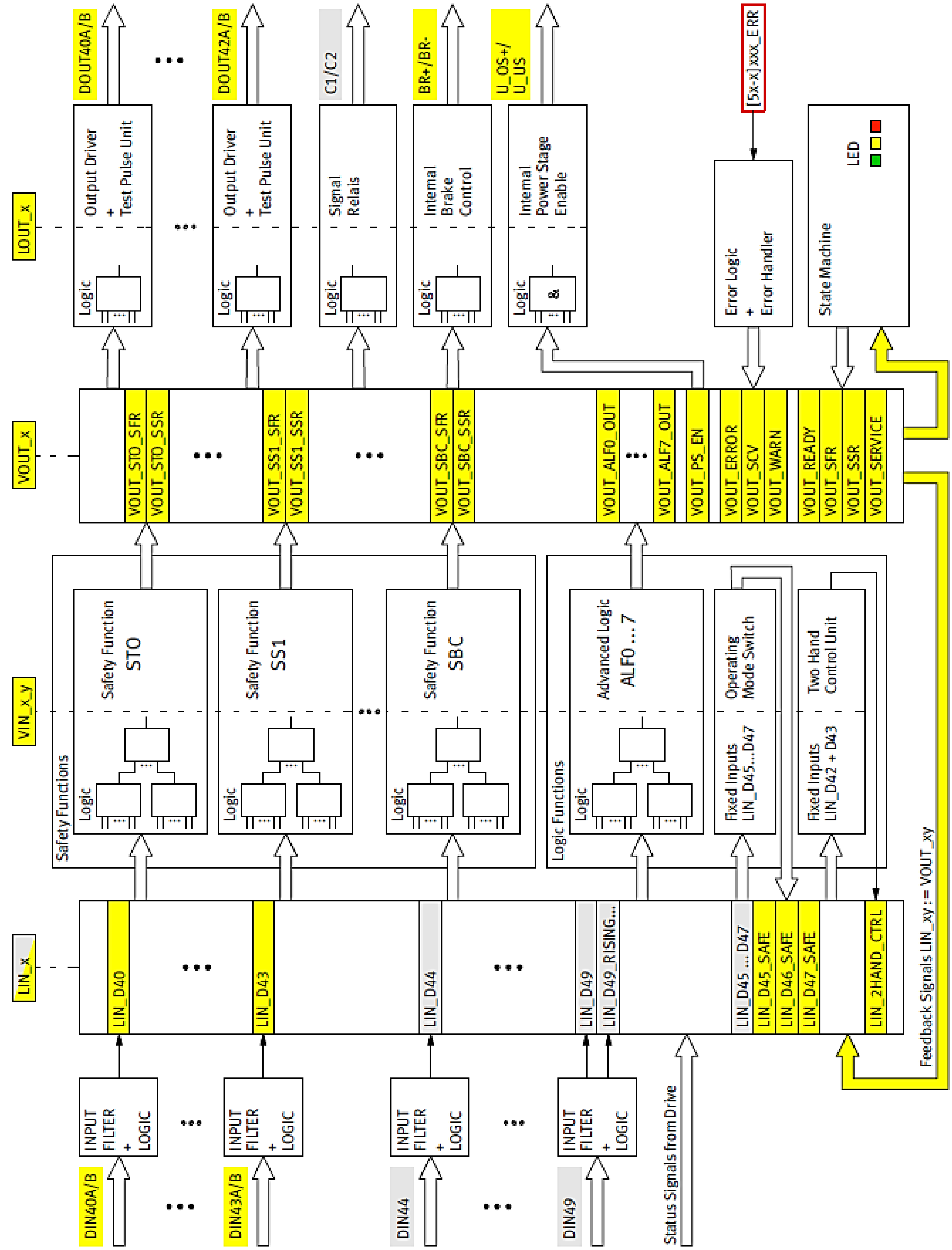


Figure 5: Functional diagram, safety module (legend ➔ Table 8)

Term/abbreviation	Explanation
DIN40A/B ... DIN43A/B	Two-channel digital inputs
DIN44 ... DIN49	Single-channel digital inputs
INPUT FILTER + LOGIC	Input filter and input logic
Status signals from drive	Status signals from drive
LIN_x	Logical inputs
VIN_x_y	Virtual inputs
Safety functions	Safety functions
Logic	Logic, configurable for the safety functions using product terms
Safety function STO, SS1, ...	Safety function STO, SS1, ...
Logic functions	Logic functions
Advanced logic ALF...	Advanced logic functions ALF...
Fixed inputs LIN_...	Permanently assigned logical inputs LIN_...
Operating mode switch	Mode selector switch
Two-hand control unit	Two-hand control unit
VOUT_x	Virtual outputs
LOUT_x	Logical outputs
Output driver + test pulse unit	Output driver and test pulse generation
DOUT40A/B ... DOUT42A/B	Two-channel digital outputs
Signal relay	Signal contact
C1/C2	Pins C1/C2 of the signal contact
Internal brake control	Internal brake control
BR+/BR-	Pins BR+/BR- of the internal brake control
Internal power stage enable	Internal output stage enable
U_OS+/U_OS-	Pins U_OS+/U_OS- of the internal output stage enable
Error logic + error handler	Error logic and error handling
[5x-x] xxx_ERR	Internal error signal, error 5x-x
State machine	State machine
Feedback signals LIN_xy := VOUT_xy	Feedback of the signals LIN_xy := VOUT_xy

Table 8: Legend for Figure 5

The digital inputs of the interface [X40] are shown on the very left of the block diagram and the digital outputs on the very right. Between them is a structure with logic blocks and the safety functions.

In the functional diagrams and other block diagrams, all the safe signals have a yellow background and potentially unsafe signals have a grey background.

2.2.4.1 Input filters and logical inputs

The digital input signals at [X40] are first filtered in the "Input Filter + Logic" function block. The block also checks whether test pulses exist on the input signals and whether they are plausible. In the case of two-channel inputs, a test is carried as to whether the input level corresponds to the configured input type (equivalent / antivalent switching) and whether the signals switch at the same time.
As a result of these tests, the logical statuses of the input signals are mapped, shown in the block diagram as LIN_x "Logic Inputs". For example, the signal LIN_D40 maps the logical switching status of the two-channel input DIN40.
List of logical inputs ➔ Section 8.1.1, Table 150.

2.2.4.2 Safety functions

The safety functions have some standardised features:
Configurable logic functions are used to define which logical input signals, LINs, are switched to the safety function for

- requesting the safety function,
- terminating the request,
- selecting additional control signals, if required.

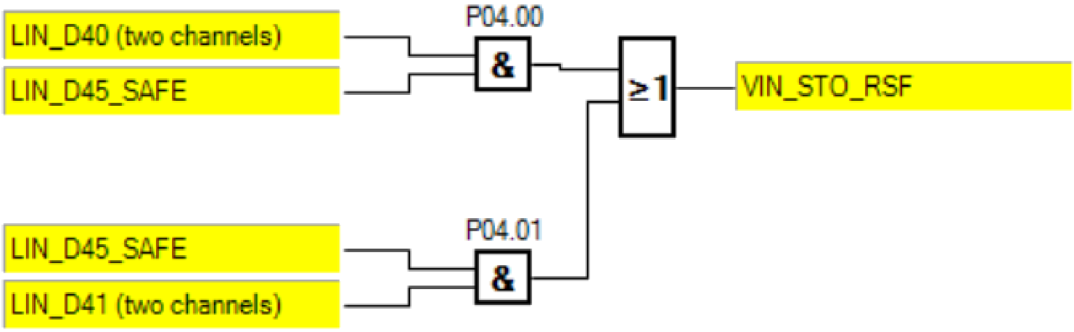
These internal control signals for the safety functions are termed VIN_x_y "Virtual Inputs", e.g. VIN_SS1_RSF is the term for the input for requesting (Request Safety Function) the safety function SS1. The switching status of these signals can be read out and displayed. List of virtual outputs ➔ Section 8.1.2, Table 153.

A total of 32 product terms are available for the configuration of the switching conditions and are comparable to a programmable logic module (PLD). The product terms can be distributed flexibly to the desired functions.

A maximum of 4 of OR-linked product terms with a maximum of 7 inputs with/without inversion can be used for each VIN_x_y control signal for safety and logic functions, but also for the configuration of the VOUT_x outputs.

Virtual inputs, to which no product term has been assigned, have the logical status "0".

The following example uses two of the 32 product terms to request the STO function:



The product terms are managed automatically using the SafetyTool (a special software, integrated in the MSC) and are scarcely visible to the user.

The safety function itself contains logic and sequence functions which can be parameterised. The safety function takes the current status of the drive (position, speed) into account and monitors the drive. Each safety function makes the following output signals available:

- the status signal that the safety function has been requested,
- the status signal that the safe state has been reached,
- an error message in the case of violation of the safety condition.

In addition, some safety functions make yet more control signals available for the direct control of functions in the drive controller. These status messages are shown as a group in the block diagram and are indicated with VOUT_x "Virtual Output Signals". List of virtual outputs ➔ Section 8.1.2, Table 153.

2.2.4.3 Logic functions for the inputs

Special logical control signals are required for some applications, and are made up of a combination of multiple input signals. The safety module supports these applications by making predefined logic functions available for:

- the mode selector switch,
- the two-handed control device

The output signals of these logic blocks are mapped directly in LIN_x, as they also serve to control safety functions.

However, you can configure your own additional logic blocks. The so-called ALF "Advanced Logic Functions" ALF0 to ALF7 are available for this. Their output signals are available as VOUT_x "Virtual Output Signals". List of virtual outputs ➔ Section 8.1.2, Table 153.

2.2.4.4 Logical outputs and output drivers

The safety module has configurable blocks with power drivers for:

- activating the digital outputs with the generation of test pulses,
- activating the relay output,
- activating the basic unit, e.g. the output for brake activation and to switch off the driver supply for STO.

A configurable logic function is used to define which VOUT signals are switched to the appropriate output driver as LOUT "Logic Output Signal".

The logic function consists of a product term with a maximum of seven inputs as well as input and output inversion. List of virtual outputs ➔ Section 8.1.4, Table 155.

The status of the logical output (one bit) is converted by the output driver to the physical output signals (frequently two signals, configurable as antivalent / equivalent / test pulses).

2.2.4.5 Feedback

The safety module has an internal feedback path, as it is desirable in some applications to execute safety functions according to the status of another safety or logic function:

The most important VOUT signals are therefore guided back to logical inputs LIN and are available to logical operations.
List of logical inputs ➔ Section 8.1.1, Table 150.

2.2.4.6 State machine

The operating status of the safety module is controlled using a finite state machine. The operating status is displayed using a multi-coloured LED and also mapped in VOUT.
An exact description of the operating statuses can be found in ➔ Section 2.10.

2.2.4.7 Error management

The error management controls how the safety module reacts when errors occur. The most important error reaction is to immediately switch-off the power output stage in the basic unit (Safe Torque Off, STO) as well as to switch off all safe outputs. The error responses can be configured ➔ Section 2.8.

2.2.5 Overview of supported position encoders

Position-detection sensors are required, in order to safely monitor the speed (e.g. for SLS) and position (e.g. for SOS).

The ARS 2000 FS servo drive supports many different shaft encoders for position and speed detection via the device interfaces X2A, X2B and X10. The signals of the position encoders are forwarded internally from the servo drive to the safety module (➔ Figure 3). Most shaft encoders can also be analysed directly by the safety module, as the signals are available to the safety module. The position and speed are detected via the shaft encoders.

The following shaft encoders are supported by the safety module:

- resolvers via X2A
- SIN/COS incremental encoders via X2B
- SICK HIPERFACE shaft encoders via X2B (only process data channel)
- Heidenhain EnDat encoders via X2B
- incremental encoders with digital A/B signals via X2B
- BISS position transmitters for linear motors via X2B
- incremental encoders with digital A/B signals via X10

The position and speed are detected via the shaft encoders.

i The safety functions supported by the safety module do not require knowledge of the absolute position. For this reason, safe analysis of the absolute position of the encoders or safe homing is not intended.

Each microcontroller on the safety module can analyse up to two position transmitters:

Encoder analysis

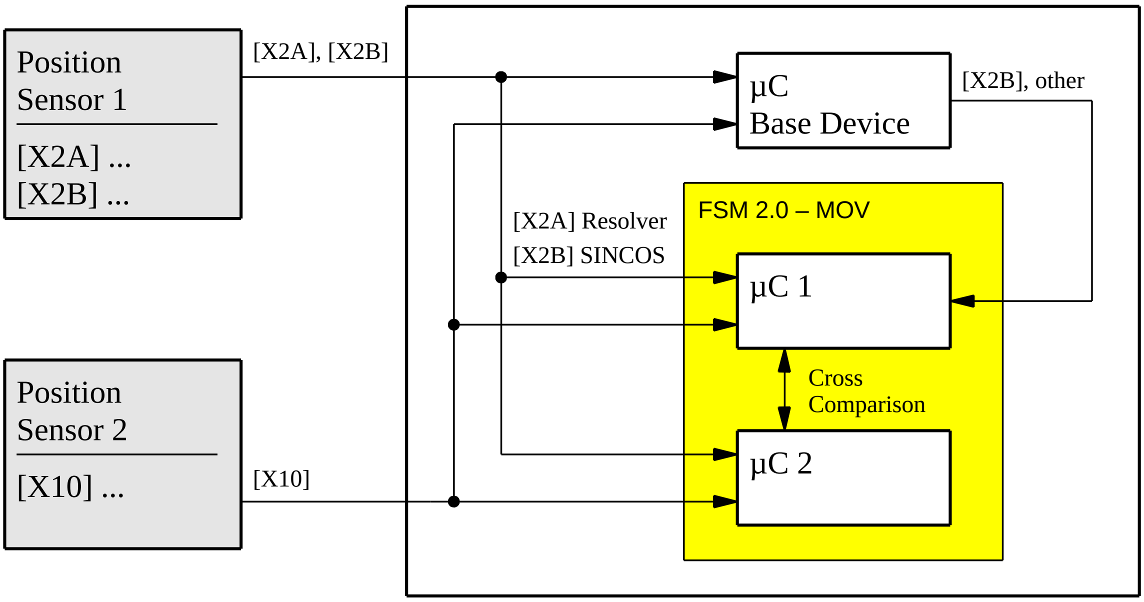


Figure 6: Analysis of the position sensors on the safety module

Term/abbreviation	Explanation
Position Sensor 1/2	Position encoder 1/2
µC Base Device	Microcontroller basic unit
Cross Comparison	Cross-comparison

Table 9: Legend for Figure 6

– If two position transmitters are used, each microcontroller analyses both sensors. Each microcontroller compares the position and speed values of both sensors and triggers an error message if there are impermissible deviations.
– If only one position sensor with SIL classification is used, then this is also analysed by both microcontrollers on the safety module.
– If a position transmitter is used, which can be analysed by the basic unit (µC GG) but is not directly supported by the safety module, the standardised angle information can be sent from the basic unit to the safety module. In combination with a second position transmitter, which is analysed directly by the safety module, it is possible to configure a safe system (up to SIL2). In Table 10, the variant is indicated as "X2B other encoder".
– In all cases, there is a continuous cross-comparison of the position data between microcontroller 1 and microcontroller 2, with error triggering in the case of impermissible deviations.
– In each configuration, the two microcontrollers, 1 and 2, use various position and speed values to monitor the axle. In addition, acceleration monitoring can also be configured for a plausibility check.

The manufacturers of SIL-certified shaft encoders publish instructions for the use of these shaft encoders in safety applications.

The FSM 2.0 – MOV takes the following manufacturer specifications into account when evaluating the encoder signals:

- Specification of the E/E/PES safety requirements for EnDat-Master dated 19/10/2009 (D533095 - 04 - G - 01) ➔ www.heidenhain.de (in preparation)
- Implementation Manual HIPERFACE® Safety dated 21/12/2010 (8014120/2010-12-21) ➔ www.sick.com

Please check these documents with regard to necessary measures for the attachment of the shaft encoders and required fault exclusions.

2.2.5.1 Permissible combinations of position encoders

Table 10 shows the permissible encoder combinations. Other combinations cannot be parameterised in the safety module.
The characteristic safety values which can be achieved with the combinations can be found in ➔ Section 7.2.3.

First encoder	**Second encoder**	**Note**
[X2A] Resolver	[X2B] Other encoder	–
[X2A] Resolver	[X10] Incremental encoder	–
[X2A] Resolver	None	Note the following instructions!
[X2B] SIN-/COS incremental encoder	None	Requires SIL classification of the encoder.
[X2B] SIN-/COS incremental encoder	[X10] Incremental encoder	Note the following instructions!
[X2B] HIPERFACE incremental encoder	[X10] Incremental encoder	Note the following instructions!
[X2B] HIPERFACE incremental encoder	None	Requires SIL classification of the encoder.
[X2B] EnDat encoder	[X10] Incremental encoder	Setting, encoder 1: "[X2B] Other encoder". Note the following instructions!
[X2B] EnDat encoder	None	In preparation. Requires SIL classification of the encoder.
[X2B] Other encoder	[X10] Incremental encoder	–

Table 10: Permissible combinations of position encoders

Note

Please analyse whether your selected position encoder is sufficiently accurate to fulfil the monitoring task, in particular the SOS safety function. Refer to the information on system accuracy in ➔ Appendix 7.3.

➔ **Note**

In applications with only one shaft encoder / position encoder, it must have the SIL classification required in accordance with the risk analysis. In most cases, the classification requires additional requirements or fault exclusions in the mechanical system. Please check carefully that these requirements are fulfilled in your application and that the appropriate fault exclusions can be performed. In this regard, always observe the implementation information and the required fault exclusions, required by the manufacturer of the position encoder.

➔ **Note**

In applications with only one shaft encoder / position encoder with analogue signal interface (Resolver, SIN-/COS, HIPERFACE, etc.), the restrictions regarding diagnostic cover and possible accuracy of rest and speed monitoring must be taken into account ➔ Appendix 7.3.5 and 7.3.6.

➔ **Note**

When using two functional encoders without SIL classification, the suitability of the encoder combination for use in safe systems up to SIL3 must be proven separately (for example, the following are required: diversity of the encoder systems with regard to CCF, MTTFd, etc., suitability of the encoders for the operating and ambient conditions, EMC, etc.).

i Recommendation: If necessary, use sample solutions created by the manufacturer with defined combinations of axles, motors and encoders.

2.2.6 Data exchange and control of the servo drive

The safety module can manipulate the power output stage of the servo drive using digital control signals. The servo drive uses further digital control signals to indicate its operating status. In addition, it is connected to the microcontroller in the basic unit via an internal communication interface (➔ Section 2.2.1, Figure 4, Safety module functional principle).

i The safety module can control the servo drive ("Master control"). It controls:

– switching off the power output stage,
– manipulation of the brake control,
– the setpoint values for the controller,
– error acknowledgement.

The digital control signals are used as follows:

a) Switching off the driver supply in the servo drive:

The power output stage of the servo drive can be switched off using two independent channels. One channel controls power connected to the top switch and the other the power connected to the bottom switch. The channels are controlled diversely by the safety module and are continuously monitored using test pulses during operation. These units are activated exclusively by means of the STO safety functions ➔ Section 2.5.3.

b) Manipulation of the brake control (connection [X6]):

The brake control is switched off redundantly in the safety module using the appropriate control signals to the basic unit. The brake control is also monitored continuously during operation using test pulses. Thus, the safe brake output of the basic unit can also be used to activate clamping units. These units are activated exclusively by means of the SBC safety functions ➔ Section 2.5.4.
By contrast, the holding brake is only vented when the basic unit signals to the safety module via another control cable that it also wishes to enable the holding brake function. This logic operation allows a simple restart of the axle after SBC.

In the case of system errors on the safety module, dynamically-activated hardware circuits ensure that the control cables for the driver supply and for brake control are switched off quickly and safely.

c) Triggering a quick stop in the basic unit:

The safety module can trigger a quick stop in the basic unit via an internal control cable. The reaction time of the basic unit is very short (< 2 ms).
When the signal is activated, in rotational speed control and positioning modes, the basic unit brakes at the Quick Stop ramp down to a speed of zero. After this, depending on the operating mode, the rotational speed is regulated to 0 rpm or the position to the current position.

This function is used to implement the safety function SS1 or SS2 type b) ➔ Section 2.5.5 and 2.5.6.

The internal communication interface between the safety module and the basic unit is used for the following tasks:

- Setting up the outward communication connection between the safety module and the PC for parameterisation and diagnostics.
- Additional active manipulations by the safety module in the control system of the servo drive.
- Exchange of status messages and operating statuses.
- Providing debug information for troubleshooting/analysis.
- Bi-directional transmission of secure data telegrams to external safety controllers (in preparation).

d) Interface for parameterisation:

The safety module is parameterised using the SafetyTool (➔ Sections 2.2.7 and 4.5). The SafetyTool is opened via the Metronix ServoCommander® (MSC). Secure communication between the SafetyTool and the safety module is optionally ensure via one of the interfaces of the servo drive (Ethernet [X18], USB [X19] or, if included, via RS232 [X5]). The servo drive forwards the telegrams from and to the safety module without changing them.

e) Active limitation of the rotational speed/speed in the basic unit:

The safety module can use the internal communication connection to manipulate the drive control of the basic unit directly, by actively limiting the speed setpoint in the basic unit. The basic unit is braked at the ramp parameterised in the safety module. This limiting is possible in the following operating modes of the basic unit:

– rotational speed/speed control
– positioning (set or direct operation)

This function is used to implement the safety function SS1 or SS2 type a) ➔ Section 2.5.5 and 2.5.6. It can also be used in conjunction with safe speed functions, such as SLS, as the axle can be braked autonomously, even without manipulation by the controller.

If multiple safety functions are active simultaneously on the safety module and specify different speed limits, then the minimum is formed from the limit values of all the safety functions and transmitted to the basic unit.
In all interpolating operating modes, in which the basic unit is run directly via the controller, the rotational speed should not be actively limited.

f) Status signals:

The operating status of the safety module and the status of the safety functions (e.g. Safety Function Requested (SFR), Safe State Reached (SSR)) are transmitted at regular intervals to the basic unit via the internal communication interface.
The basic unit can

– output and display this status via the digital outputs,
– transmit this status to the higher-order controller via the appropriately active fieldbus interface,
– output this status via the 7-segment display.

You can find the description of the available status signals in ➔ Section 2.10.

You can find the status information available via the CANopen communication protocol in ➔ Section 7.4.

g) Error analysis/debugging:

The basic unit also receives the error status of the safety module via the communication interface and it has access to internal status variables, such as the measured safe speed or the monitoring limits for speed.
The basic unit uses this data:

– to display the operating status and any error messages on the 7-segment display,
– to detect all signals in a permanent event memory for later diagnostics,
– to analyse the status variables of the safety module via the oscilloscope function. For example, the monitored speed limits and the current speed can be recorded to test why the safety module has detected a violation of a safety condition.

2.2.7 Configuration of the safety functions with the SafetyTool

In contrast to a safety controller, the safety module is not freely-programmable.

It has a defined function range, which can be activated and parameterised by the user. To be able to adapt the functions in the safety module flexibly to different applications, the actual safety functions and the outputs have a configurable logic section to specify the switching conditions.

The selection of the safety functions, the assignment of the I/Os and the request of the safety functions via inputs and other conditions are configured using the SafetyTool.

The SafetyTool is a software module for safe commissioning of the safety module and is started from the Metronix ServoCommander®.

The parameterisation defines the following settings, amongst other things:

- The inputs are activated when a function is allocated to them, such as a sensor type ➔ Example, Section 4.6.7.
- The individual safety functions are activated and parameterised, e.g. by specifying limit speeds, etc.
- The request of a safety function is parameterised as a logical operation, e.g. via the request through an input ➔ Example, Section 4.6.8.
- To signal an active safety function, the internal status can, for example, be linked to an output.
- The behaviour in case of error (the error response) can be configured.

You can find the description of the procedure for parameterising the safety module with the SafetyTool in ➔ Section 4.5.

Important:

The SafetyTool supports automatic data transfer from the basic unit. The shaft encoder, gear unit, feed constants, etc. are configured only once during basic unit commissioning. After the commissioning of the basic unit, this data is read by the SafetyTool and transmitted to the safety module, guided by dialogs.

- Fully parameterise the basic unit in the first step and functionally optimise the application.
- In the second step, please parameterise the safety engineering.

➔ **Note**

Safety functions in the commissioning phase.

As measures to ensure the required functional safety are required during the commissioning phase of a system, note that:

❖ The safety module must be fully configured and the application must be fully validated before it can provide any protection.

i

The safety module is delivered "preconfigured" ex works ➔ Section 4.4.1.

- The safety functions STO and SBC are requested via DIN40.
- Restart takes place via DIN49.
- Error acknowledgement takes place via DIN48.

The delivery status can also be recognised without MSC/SafetyTool by the green-red flashing LED of the safety module (if DIN40 was switched on and no safety function is requested ➔ Section 2.10).

2.3 Data transfer from the servo drive

For safe motion monitoring, the safety module must know which sensors are connected for position detection, which resolution they have, how they are designed mechanically, what type of feed, gear unit, etc. is used and in which units the user wishes to parameterise the application. The user interface of the SafetyTool will show you how to take this data from the servo drive (basic unit). This simplifies parameterisation and helps you avoid making mistakes when entering the data.

Ideally, proceed as follows when creating new projects:

Use a safety module in the delivery status or reset it to the factory settings ➔ Section 4.4.2 and 4.4.1.

Firstly, completely parameterise the basic unit using MSC and commission it (if possible).

Only then should you start the safe parameterisation using the SafetyTool and transfer the set data from the basic unit to the SafetyTool automatically using the "Copy" buttons ➔ Section 4.5.1 and 4.6.2.

Note

Data transfer from the basic unit is also required if you wish to use a safety module which has already been used in another application with a different mechanical design or if you have set a safety module manually to the factory settings.

In this case too, the configuration of the basic unit "leads" and the appropriate data on the display units, the mechanical design and the encoder configuration must be transferred from the basic unit.

If previously-configured safe motion functions exist in the safety module, then the limit values set in the safety module are transferred to the SafetyTool as setpoints. They must be transmitted to the safety module again, so that the limit values remain unchanged.

Example:

In the safety module, an SLS function with a limit value of +/- 200 mm/s was originally configured. It was operational on a toothed belt axle with a feed of 100 mm/rev.

The safety module is now used in another application, and the feed in this application is now 150 mm/rev.

After transfer of the changed feed, the SafetyTool now displays a discrepancy between the setpoint and actual value in the SLS function:

Setpoint: 200 mm/s
Actual value: 300 mm/s

For this reason, the setpoint must be written to the safety module again and validated.

2.3.1 Basic information

The basic information contains the selected display units for (➔ Table 11):

- path (P06.3E and P06.41),
- speed (P06.42 to P06.45),
- acceleration (P06.46 to P06.49),

as well as a description of the mechanical translation using:

- gear ratio (numerator and denominator) between motor and downforce (P06.4A and P06.4B),
- feed constant (numerator and denominator) for rotational -> translational conversion (P06.3F and P06.40).

This information is used for the conversion between display and device values (position, speed, acceleration).

➔ **Note**

These parameters must be transferred to the safety module and checked and validated. Only then can it be guaranteed that the safety module will perform calculations in the same units as the basic unit!

2.3.1.1 Parameters for basic information:

Basic information		
No.	**Name**	**Description**
P06.3E	Unit to be displayed for positions.	Unit to be displayed for positions. Selecting "UserDefined" in the SafetyTool means that no unit is displayed for position values.
P06.3F	Numerator, feed constant for the axle in position units	Numerator of the feed constant of the axle in position units per motor revolution (without gear ratios).
P06.40	Denominator, feed constant for the axle in position units	Denominator of the feed constant of the axle in position units per motor revolution (without gear ratios).
P06.41	Number of digits displayed after the decimal point for positions.	Number of digits displayed after the decimal point for position values.
P06.42	Unit to be displayed for speeds.	Unit to be displayed for speeds. Selecting "UserDefined" means that no unit is displayed. If the position is UserDefined, then the speed must be too.
P06.43	Numerator, altered time base for speeds of type UserDefined.	Numerator, altered time base for speeds of type "UserDefined".
P06.44	Denominator, altered time base for speeds of type UserDefined.	Denominator, altered time base for speeds of type "UserDefined".
P06.45	Number of displayed post-decimal positions for speeds.	Number of displayed post-decimal positions for speeds.
P06.46	Unit to be displayed for accelerations.	Unit to be displayed for accelerations. Selecting UserDefined means that no unit is displayed. If the position is "UserDefined", then the acceleration must be too.
P06.47	Numerator, altered time base for accelerations of type UserDefined.	Numerator, altered time base for accelerations of type "UserDefined".
P06.48	Denominator, altered time base for accelerations of type UserDefined.	Denominator, altered time base for accelerations of type "UserDefined".
P06.49	Number of displayed post-decimal positions for accelerations.	Number of displayed post-decimal positions for accelerations.
P06.4A	Numerator, total gear ratio between motor and axle.	Numerator, total gear ratio between motor and axle.
P06.4B	Denominator, total gear ratio between motor and axle.	Denominator, total gear ratio between motor and axle.

Table 11: Parameters for basic information

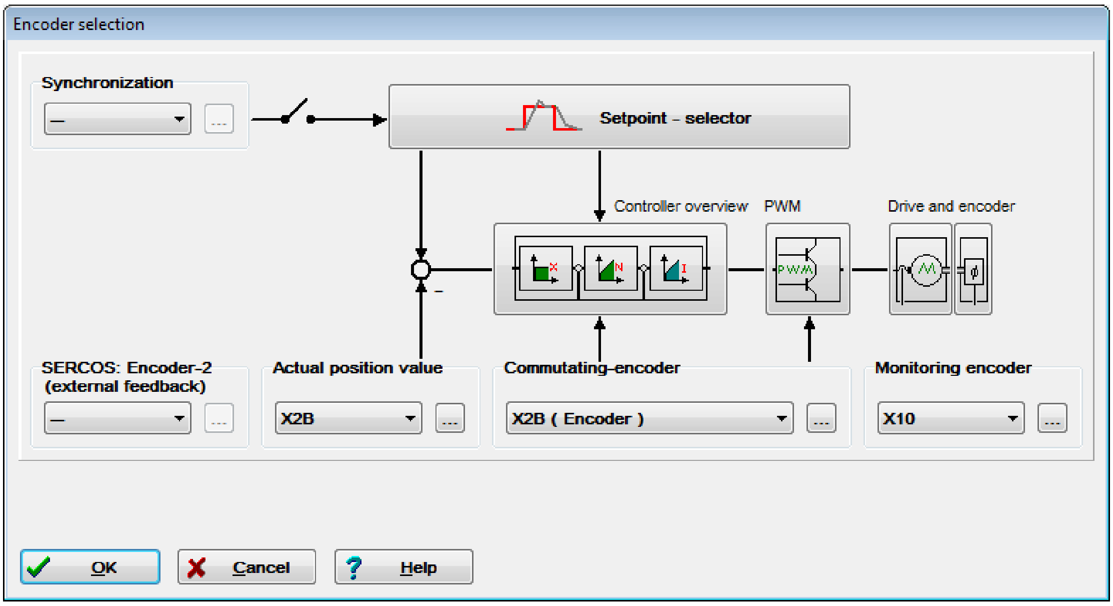
2.3.2 Configuration of the encoders

The selection and setting of the shaft encoder for measuring position, setting the angle/position counting direction, resolution of the position encoder and the setting of the gear ratios of the position encoder are also taken automatically from the configuration of the basic unit.

Important:

Frequently, in the basic unit, only one position encoder (on the motor) is used for control, but, in many cases, for functional safety (➔ Table 10) a further position encoder is planned, e.g. at the downforce.

Please ensure that you have already configured the position encoder(s) in the basic unit via MSC, as the following example for 2 encoders shows:



Otherwise data transfer cannot take place fully.

Note

These parameters must be transferred to the safety module and checked and validated. Only then can it be guaranteed that the safety module will perform calculations in the same units as the basic unit!

The configuration of the position encoder is relatively involved, because the safety module supports many different encoder types and configurations. For this reason, the configuration is divided up into the following tabs in the SafetyTool:

- standard parameters (selection of the encoder interfaces and encoder types),
- parameters for position encoder at [X2B],
- parameters for position encoder at [X10],
- expert parameters for cross-comparison of the position data,
- expert parameters for configuration of the safe rotational speed recording and idle detection,
- expert parameters for the signal monitoring of safe encoders with analogue signals (resolver, SIN/COS encoder).

2.3.2.1 Standard parameters

Here, a selection is made of which encoder interface and which encoder type in the safety module is used as position encoder 1 and as position encoder 2. Gear units between motor and axle are mapped via the gear ratio. Via negative gear factors, a rotational direction reversal is taken into account.

Data transfer/setting of the leading position encoder 1 (first encoder):

– resolver [X2A],
– SIN/COS or HIPERFACE encoder [X2B],
– other encoder [X2B], e.g. EnDat, BISS.

In addition, a gear ratio for position encoder 1 between the encoder and motor can be set.

In addition, the data transfer/setting of the position encoder 2 (second encoder) is made:

– other encoder [X2B], e.g. SIN/COS, EnDat, BISS,
– incremental encoder [X10],
– none (only if position encoder 1 is a certified position encoder).

In addition, you can set a gear ratio for position encoder 2 between the encoder and motor.

Important: The SafetyTool will warn you of impermissible encoder combinations.

Send	ID	Name	Unit	Nominal value
	P06.00	Selection of leading position sensor 1		SINCOS / Hiperface (X2B) = [2]
	P06.0B	Gear ratio enumerator for position sensor 1		-1
	P06.0C	Gear ratio denumerator for position sensor		1
	P06.01	Selection of redundant position sensor 1		Other encoder (X2B) = [4]
	P06.0D	Gear ratio enumerator for position sensor 2		1
	P06.0E	Gear ratio denumerator for position sensor		1

For the permissible encoder combinations and the corresponding safety classification, refer to ➔ Section 2.2.5 (Table 10).

Note

Should a cross-comparison error between encoder 1/2 occur despite successful data transfer:

❖ In this case, check the gear ratio of encoder 2, as this is only monitored by the safety module and is not integrated into the control in MSC.

2.3.3 Parameters for the position encoder

2.3.3.1 Parameter for position encoder at [X2A]

The connection is intended for resolvers [X2A]. The analogue, amplitude-modulated tracking signals of the resolver are sampled behind the input differential amplifier in the ARS 2000 FS, run internally to the safety module and then analysed safely and via two channels there by both microcontrollers.

Parameterised/data transfer from the basic unit is not required.

2.3.3.2 Parameter for position encoder at [X2B]

The connection [X2B] is intended for encoders with analogue tracking signals, such as:

- incremental encoders with SIN/COS tracking signals,
- HIPERFACE encoders with SIN/COS tracking signals.

The tracking signals of the SIN/COS encoders and HIPERFACE encoders are sampled behind the input differential amplifier in the ARS 2000 FS, run internally to the safety module and then analysed safely and via two channels there by both microcontrollers. This is always the case if, in the Standard parameters tab, "2SIN/COS encoder/HIPERFACE encoder (X2B) = [2]" was selected.

During data transfer/parameterisation, the number of digital angular counting steps is set (corresponding to 4 x division marks per motor revolution or, for linear motors, per $2\tau_p$).

➔ **Note**

When the axle is idling, SIN/COS encoders supply static signals. If no second angle encoder is used, Stuck-At errors (values not updated due the output signal remaining unchanged or changed too little) cannot be detected. For this reason, the axle must be moved regularly when safety functions are requested.

If a SIN/COS or HIPERFACE encoder is used as the sole encoder, then the error 55-2 is triggered when a safety function is requested after the axle is idle for more than 24 hours. If the safety function SS2/SOS is requested continually for longer than 24 hours, this will trigger the error 54-7.

➔ **Note**

In applications with only one shaft encoder / position encoder with analogue signal interface (Resolver, SIN-/COS, HIPERFACE, etc.), the restrictions regarding diagnostic cover and possible accuracy of rest and speed monitoring must be taken into account ➔ Appendix 7.3.5 and 7.3.6.

In addition, the connection [X2B] is also intended for encoders with digital interfaces, such as

- digital incremental encoders with A/B/N square wave signals,
- EnDat-2.1 and 2.2 encoders with digital interface,
- serial encoders with digital interface, e.g. BISS.

These encoders are not analysed for safety in the basic unit ARS 2000 FS.

The safety module polls standardised digital angle information at regular intervals from the basic unit via the internal data interface. This is always the case if, in the Standard parameters tab, "Other encoder (X2B) = [4]" was selected.

1455The angle information of any encoder connected to X2B on the servo drive can be used as a channel of the two-channel safe angle detection.

It is possible to parameterise an allowable error time, when the safety module detects faulty data telegrams. The default value of 1 ms should not be changed without a significant reason, as the value acts as an additional filter on the reaction time of the safety module.

Note

The use of encoders with purely digital data transmission in safety systems in only permissible in conjunction with a second encoder, e.g. at [X10].

It is not yet possible to use a safe EnDat encoder (in preparation).

Formally, "Angle encoder 1 = EnDat" is parameterised when a safe EnDat encoder is used. Only one incremental encoder at [X10] can be additionally analysed as angle encoder 2.

Note

During homing of drives with EnDat multiturn encoders, which save the zero point shift in the encoder, a jump in the actual position occurs during saving. This jump causes acceleration monitoring in the safety module to respond, leading to an error of the safety module.

This homing need only be carried out once during machine setup.

2.3.3.3 Parameter for position encoder at [X10]

The [X10] connection is intended for digital incremental encoders with A/B/N square wave signals. The position is detected using quadrature counter inputs of the microcontroller of the safety module.

The incremental encoder [X10] is ideally used as the second position measurement system. This is always the case if, in the Standard parameters tab, "Incremental encoder (X10) = [5]" was selected.

During data transfer/parameterisation, the number of digital angular counting steps is set (corresponding to 4 x division marks per motor revolution or, for linear motors, per $2\tau_p$).

2.3.4 Parameter for encoder monitoring and rotational speed measuring

Figure 7 shows the structure of encoder analysis and monitoring:

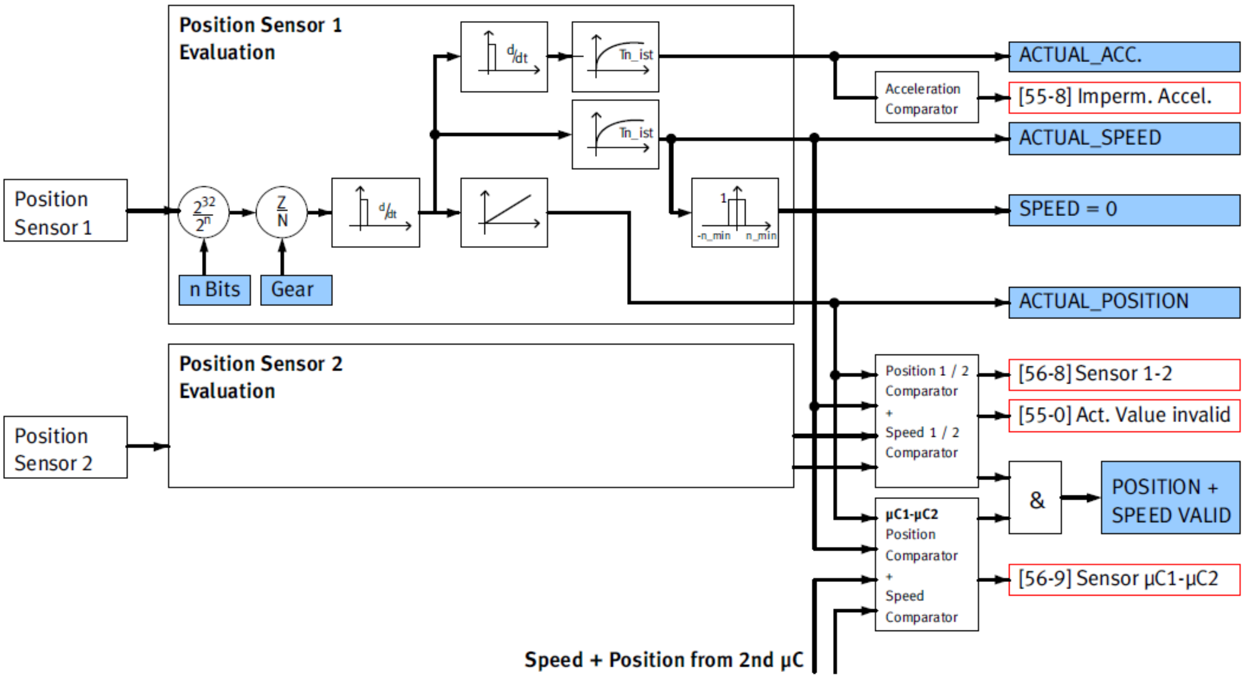


Figure 7: Calculation of the speed and acceleration

Term/abbreviation	Explanation
Position of sensor 1/2	Analysis of position encoder 1/2
Evaluation	Evaluation
Gear	Gear units
Acceleration Comparator	Comparison of acceleration 1/2
Position 1/2 Comparator + Speed 1/2 Comparator	Comparison of position 1/2 and comparison of speed 1/2
ACTUAL_ACC.	Internal signal: Current acceleration
ACTUAL_SPEED	Internal signal: Current speed
SPEED = 0	Internal signal: Speed = 0
ACTUAL_POSITION	Internal signal: Current position
POSITION + SPEED VALID	Internal signal: Position and speed valid
[5x-x] xxx_ERR	Internal error signal, error 5x-x 55-0 Invalid actual value 55-8 Impermissible acceleration 56-8 Deviation of angle encoders 1/2 56-9 Deviation of µC values 1/2

Table 12: Legend for Figure 7

Description

- The block position Sensor Evaluation exists twice in each microcontroller, separately for position encoder 1 and position encoder 2.
- The position information of encoder 1 and encoder 2 is first standardised to 2^{32}. Then, a gear ratio is taken into account, which can be used to map a counting direction switch.
- Thus the block supplies a standardised position and uses it to calculate the current speed and the acceleration.
- The data of position encoder 1 are used to monitor the status variables.
- The acceleration is monitored and checked for plausibility - this can be parameterised.
- Each microcontroller carries out a continuous comparison of the position values and speed values of encoder 1 with those of encoder 2.
- The tolerances for this encoder comparison can be parameterised.
- In addition, each microcontroller performs a cross-comparison to compare its own position and speed data with that of the other microcontroller. Limit values can be parameterised for this.
- The microcontroller will generate various error messages if deviations or limit value violations are detected.

➔ **Note**

The factory settings of the parameters for encoder analysis are adapted to the resolution of the position encoders and to the electronic analysis unit in the safety module.

They should only be changed when required, as they influence the reaction time of the safety module when dangerous movements are detected or during error detection. They are so-called "Expert parameters".

2.3.4.1 Expert parameters for configuration of the safe rotational speed recording and idle detection

Both microcontrollers use the recorded position data to calculate the safe speed and the acceleration. The following parameters are available for rotational speed recording and for idle detection:

- Acceleration monitoring is used to check the plausibility of the position measurement. An acceleration has been parameterised which the motor surely cannot reach on account of its design. If the rotational speed ramp exceeds a limit defined by the maximum acceleration, then an error 55-8 is triggered ➔ Section 5.6.
- The filter for the rotational speed/speed measurement reduces the noise in the speed signal, in particular when encoders with analogue signals or a coarse resolution are used.
- The threshold value and the filter time for the idle detection. The idle detection is used, for example, for the SOS safety function.

2.3.4.2 Expert parameters for cross-comparison of the position data

This tab contains parameters for the plausibility check of the position and speed data.

- The tolerance window and allowable time for the comparison of the position data of encoder 1/encoder 2 by the appropriate microcontroller in the safety module.
- The tolerance window and allowable time for the comparison of the speed data of encoder 1/encoder 2 by the appropriate microcontroller in the safety module.
- The tolerance window and allowable time for the cross-comparison of the position data between microcontroller 1 and microcontroller 2 on the safety module.
- The tolerance window for the cross-comparison of the speed data between microcontroller 1 and microcontroller 2 on the safety module.

If the safety module detects a deviation in the position or speed data and/or their value exceeds the parameterised value continuously for the parameterisable time, then an error is triggered and the actual values are invalid.

2.3.4.3 Expert parameters for the signal monitoring of safe encoders with analogue signals

This tab contains parameters for monitoring the analogue encoder signals of SIN/COS encoders and resolvers.

- Amplitude and vector length monitoring for the resolver signals, as well as an allowable time for monitoring.
- Parameterisable observer filter for the resolver analysis.
- The amplitude and vector length monitoring for the SIN/COS and HIPERFACE encoder analysis, as well as an allowable time for monitoring.

2.3.4.4 Influence of the parameters for the encoder configuration on the runtime performance

Some configuration parameters for detecting safe rotational speed influence the reaction time, with which changes in the movement are detected.

The following parameters have an influence:

Parameters for movement detection and error detection, which influence the runtime performance				
Parameter		**Min.**	**Max.**	**Factory setting**
P06.08	Filter time constant for measuring rotational speed	0.4 ms	1000 ms	8.0 ms
P06.0A	Filter time for rest detection	0.0 ms	1000 ms	10.0 ms
P06.04	Allowable time for position difference 1-2	0.0 ms	1000 ms	10.0 ms
P06.06	Allowable time for speed difference 1-2	0.0 ms	1000 ms	10.0 ms
P06.15	Resolver observer filter - filter time	0.0 ms	3 ms	1.0 ms
P06.13	Resolver signal monitoring, allowable time	0.0 ms	10 ms	1.0 ms
P06.1E	SIN/COS signal monitoring, allowable time	0.0 ms	10 ms	1.0 ms

Table 13: Parameters for error detection in the position transmitter system, which influence the runtime performance

If you do not change the factory settings, you can use the following for simplified reaction times:

Detection of speed and position: T_I < 10 ms

Detection of errors in position detection: T_F < 10 ms

2.3.5 List of all parameters for encoder configuration

Encoder configuration		
No.	**Name**	**Description**
Standard parameters		
P06.00	Selection of the leading position encoder 1	Used encoder 1 for angles
P06.0B	Gear ratio numerator for position encoder 1	Gear ratio / pole pair number numerator
P06.0C	Gear ratio denominator for position encoder 1	Gear ratio / pole pair number denominator
P06.01	Selection of the redundant position encoder 2	Used encoder 2 for angles
P06.0D	Gear ratio numerator for position encoder 2	Gear ratio / pole pair number numerator
P06.0E	Gear ratio denominator for position encoder 2	Gear ratio / pole pair number denominator
X2B		
P06.19	Number of incr./rev. of the incremental encoder at X2B	Number of increments / revolution of the incremental encoder at X2B
Expert parameter		
P06.28	Allowable time for faulty encoder communication	Allowable time for faulty encoder communication
X10		
P06.18	Number of incr./rev. of the incremental encoder at X10	Number of increments / revolution of the incremental encoder at X10
Rotational speed detection		
Expert parameter		
P06.07	Maximum acceleration for encoder monitoring	Maximum acceleration which the drive never reaches --> Error limit for the angle plausibility check
P06.08	Filter time constant for measuring rotational speed	Filter time constant, actual rotational speed value filter
P06.09	Speed threshold value for idle detection	Max. rotational speed for idle detection
P06.0A	Filter time for rest detection	Time window for $n < n_{min}$ for idle detection
Comparison, encoder 1-2		
P06.03	Tolerance window for position offset, encoder 1-2	Approved position offset between angle encoder 1 and 2
P06.04	Allowable time for position difference	Time, for which the position difference may be outside the limit
P06.05	Tolerance window, speed deviation, encoder 1-2	Approved rotational speed offset between angle encoder 1 and 2
P06.06	Allowable time for speed difference	Time, for which the rotational speed difference may be outside the limit
Expert parameter		
P1D.04	Tolerance window for position - cross-comparison µC1 - µC2	Approved angle offset between this processor and the partner
P1D.05	Allowable time for position - cross-comparison µC1 - µC2	Time, for which the cross-comparison values may be outside the limit
P1D.06	Tolerance window for speed - cross-comparison µC1 - µC2	Approved rotational speed difference between this processor and the partner

Encoder configuration		
No.	**Name**	**Description**
Signal monitoring		
Expert parameter		
P06.11	Resolver signal amplitude - lower error limit	Min. input voltage, sine or cosine signal
P06.12	Resolver signal amplitude - upper error limit	Max. input voltage, sine or cosine signal
P06.0F	Resolver - vector length lower limit	Min. input voltage U = root(sin^2 + cos^2)
P06.10	Resolver - vector length upper limit	Max. input voltage U = root(sin^2 + cos^2)
P06.13	Resolver signal monitoring, allowable time	Maximum time during which a resolver signal may be outside the signal monitoring limits, before an error is triggered.
P06.15	Filter time, resolver analysis	Filter time for the observer filter
P06.1C	SIN/COS signal amplitude - lower error limit	Min. input voltage, sine or cosine signal
P06.1D	SIN/COS signal amplitude - upper error limit	Max. input voltage, sine or cosine signal
P06.1A	SIN/COS - vector length lower limit	Vector length root(sin^2 + cos^2) min.
P06.1B	SIN/COS - vector length upper limit	Vector length root(sin^2 + cos^2) max.
P06.1E	Allowable time, signal amplitude monitoring	Maximum time during which a signal may be outside the limit, before an error is triggered.

Table 14: Encoder configuration

2.4 Digital inputs

2.4.1 Overview

The safety module has numerous digital inputs and outputs for the connection of passive and active sensors. Safety functions are requested via two-channel, safe inputs.

For the following descriptions, it is necessary to define some terms:

Term	Meaning
Discrepancy time	Maximum time, during which the two channels of a safe input may be in antivalent statuses, without the safety engineering triggering an error response.
Input filter time	Time during which the interfering pulses and test pulses, such as those from connected active sensors, are not detected.
Safety function in OFF status	The function of the inputs can be freely configured in broad ranges. During configuration, the user must ensure that the safe status is achieved on de-energised inputs (comply with idle current principle!).
Control function in ON status	The function of the inputs can be freely configured in broad ranges. Control functions require active actuation / switching of the control input with 24 V, in order to trigger the desired reaction (example: error acknowledgement, restart, mode selection switch). The idle current principle would not be safe for this!
Equivalent input signals	A safe input consists of two control cables, which both switch HIGH or LOW simultaneously (equally-switching inputs).
Antivalent input signals	A safe input consists of two control cables, which both switch HIGH or LOW against one another. At any time (with the exception of the discrepancy time) only one input is simultaneously HIGH or LOW (unequally-switching inputs).

Table 15: Terms

2.4.1.1 Passive sensors (two-channel)

Passive sensors are two-channel, contact-based switching elements. The connecting cables and the function of the sensors must be monitored.

The contacts can switch antivalently and equivalently (according to the standard for the appropriate switching element). Irrespective of this, safety functions are triggered as soon as at least one channel is switched.

Examples of passive sensors:

- emergency stop switching devices (always equivalent)
- door contact switches (both antivalent and also equivalent)
- enabling buttons (both antivalent and also equivalent)
- two-handed control devices
- mode selector switches (1-of-n selection)

The following errors are detected by the safety module in the case of passive sensors:

– antivalent or equivalent input signals after the discrepancy time has elapsed, depending on the sensor type and parameterisation
– If power is supplied via a safe output of the safety module:
  Cross-circuits and shorts to +24 V and 0 V through the lack of the test pulses.

Passive sensors, which trigger an emergency stop of the system (STO, SBC, SS1), must, according to EN 60204-1, have "forced opening" and be parameterised as equivalent inputs.

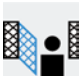
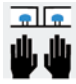
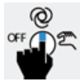
Sensor types					
Function	Emergency stop switching device	Door contact switch	Enabling buttons	Two-handed operator unit	Mode selector switch
Symbol					
Input	DIN40A/B … DIN43A/B	DIN40A/B … DIN43A/B	DIN40A/B … DIN43A/B	DIN40A/B … DIN43A/B	DIN45, DIN46, DIN47
Output	DOUT40A/B … DOUT42A/B (cycle A/B)				+24V[1)]
1) Can also be supplied with test pulses from DOUT40 … 42.					

Table 16: Allocation of the sensors to the inputs and outputs (examples)

2.4.1.1.1 Emergency stop switching device

The emergency stop switching device is usually used to trigger an emergency stop. In most cases, the safety function STO or SS1 is activated.

2.4.1.1.2 Door contact switch

This monitors whether a safety door, a light curtain, or similar is opened/passed through.

2.4.1.1.3 Enabling button

The enabling button is usually used during a setting operation.

Example: During the setting operation, machine travel is allowed when the safety door is open through the use of the SLS function as soon as the enabling button is actuated. In so doing, the enabling button temporarily cancels a safety function, which is briefly replaced by another safety function. The function of the enabling button is implemented through corresponding parameterisation of the logic (request, terminate request) of the safety function.

The following logic functions are permanently allocated to specific inputs:

2.4.1.1.4 Two-handed control device (DIN42A/B and DIN43A/B)

The two-handed control device is used in applications in which the operator must release the movement with both hands as soon as he has left the danger zone. The two-handed control device receives input from two safe input pairs. Here too, a safety function, e.g. SS1, can be overwritten by another function, e.g. SLS. The function of the two-handed control device (monitoring of the two inputs) is implemented in the safety module as a fixed logic function. The safety functions are switched by parameterising the logic (request, terminate request) of the safety functions.

2.4.1.1.5 Mode selector switch (DIN45, DIN46, DIN47)

This is used to select the operating mode. The following operating modes are supported:

- normal operation / operating mode 1
- setting operation / operating mode 2
- special operation / operating mode 3

Note: The operating modes are named according to C standards for the corresponding machines. The function of the mode selector switch is implemented in the safety module as a fixed logic function. The safety functions are switched by parameterising the logic (request, terminate request) of the safety functions.

2.4.1.1.6 Restart

The Restart input can be used to reset those safety functions, which are not required at the time the input is actuated. DIN49 is intended for the restart, but any other input can be parameterised as the restart input.

Example:

- SS1 was requested via Emergency Stop, SS2 via the door contact switch.
- Now, Emergency Stop is cancelled and the door remains open.

=> When the Restart button is actuated, the system remains idling with the SS2 safety function active and can restart immediately when the safety door is closed.

2.4.1.2 Active sensors (two-channel)

Active sensors are units with two-channel semi-conductor outputs (OSSD outputs). The safety module supports active sensors with equivalent / antivalent output signals as well as with / without test pulse outputs. Through the integrated safety design of the ARS 2000 FS series, test pulses to monitor the outputs and cables are approved. Sensors switching plus/minus switch the plus and minus cable or signal and earth cable of a sensor signal.

The outputs must switch simultaneously. Irrespective of this, safety functions are triggered as soon as at least one channel is switched.

Examples of active sensors:

- light curtains
- laser scanners
- controllers

These errors are detected by active sensors:

- antivalent or equivalent input signals after the discrepancy time has elapsed, depending on the sensor type and parameterisation

2.4.1.3 Passive and active sensors (single-channel)

Single-channel sensors are used for sequence control and for feedback and diagnostics.

Examples of passive sensors:

- acknowledgement contact of an external clamping unit,
- pushbutton to acknowledge pending errors,
- pushbutton for restart.

Combinations of single-channel sensors can also be used to control safety functions, for example:

- mode selector switches (1-of-n selection).

These errors are detected by single-channel passive sensors:

- If power is supplied via a safe output of the safety module:
  Cross-circuits and shorts to +24 V and 0 V through the lack of the test pulses.

2.4.1.4 Approved sensor types

Table 17 shows an overview of the approved sensor types at the digital inputs.

Approved sensor type	**DIN...**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**
		Two-channel				**Single-channel**					
1: General two-channel input		X	X	X	X						
2: Emergency stop switching device		**X**[1)]	X	X	X						
3: Enabling buttons		X	X	X	X						
4: Two-handed control device[2)]		X	X	**X**	**X**						
5: Start button		X	X	X	X						
6: Door lock		X	X	X	X						
7: Reliable reference switch		X	X	X	X						
8: Light curtain		X	X	X	X						
9: Brake activation feedback		X	X	X	X	**X**[1)]	X	X	X		
10: General single-channel input						X	X	X	X		
11: Mode selector switch[2)]		X	X	X	X		**X**[1)]	**X**[1)]	**X**[1)]		
12: Acknowledge error		X	X	X	X					**X**[1)]	
13: Restart		X	X	X	X						**X**[1)]

1) Factory setting (information on the factory setting and delivery status → Section 4.4.1 and 4.4.2)

2) On activating the logic function in the SafetyTool, the corresponding inputs must be configured accordingly.

Table 17: Overview of approved sensor types at the digital inputs

2.4.2 Two-channel safe inputs DIN40 … DIN43 [X40]

2.4.2.1 Use

The digital inputs DIN40..DIN43 have two channels (DIN40A/B … DIN43A/B). They serve the requirement of the safety functions up to Cat. 4 / PL e or SIL3 and thus have an 1oo2 architecture.
To request safety functions, the allocated internal logical inputs are linked with the corresponding safety function.

2.4.2.2 Function

Figure 8 shows the block diagram of an input. The function is explained below for DIN40. The inputs DIN40 to DIN43 have an identical structure.

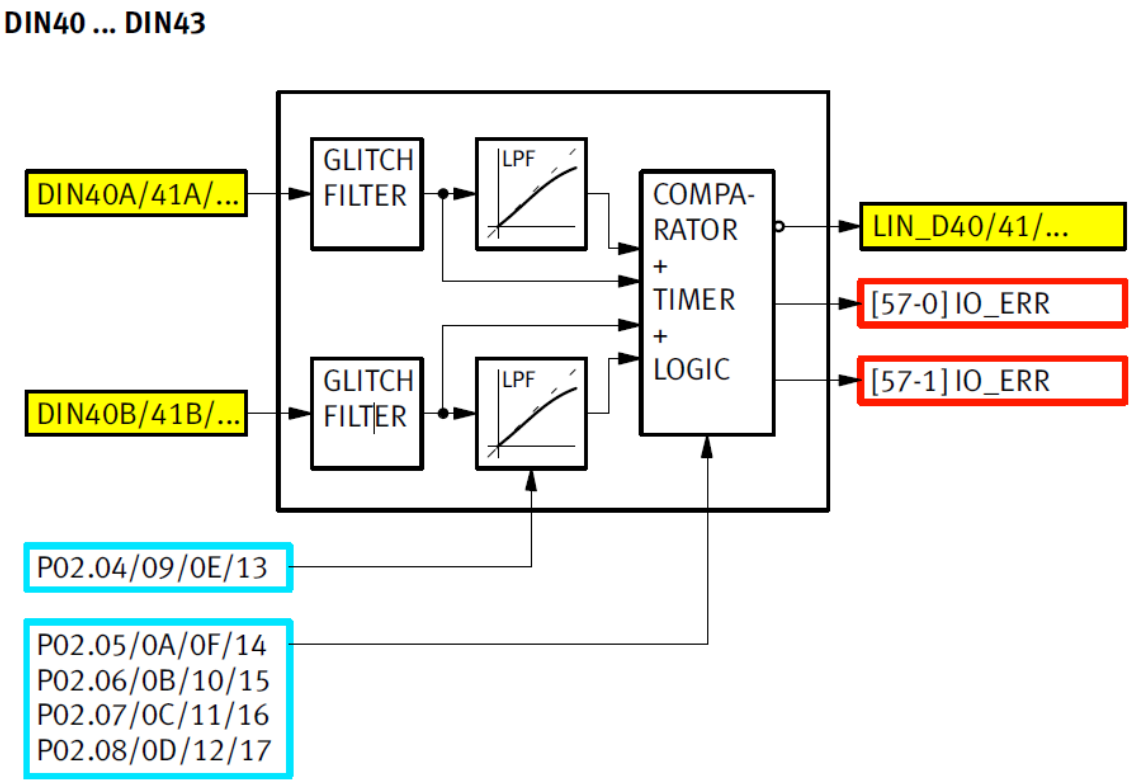


Figure 8: Block diagram of the two-channel safe inputs

Term/abbreviation	Explanation
DIN40A/..., DIN40B/...	Two-channel digital inputs DIN40A/DIN40B ...
GLITCH FILTER	Filter for interference
LPF	Low-pass filter
COMPARATOR + TIMER + LOGIC	Comparator, timer and logic
LIN_x	Logical inputs ...
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Table 18: Legend for Figure 8

The signal levels at the inputs DIN40A and DIN40B are first dejammed in a preliminary EMC filter ("Glitch Filter"). The filter time constant is 500 µs and cannot be parameterised.

After this first filter, a second "LPF" low-pass filter, which can be parameterised using the parameter "Filter time constant" (P02.04/...), follows for each input signal, and is designed as a programmable Mono-Flop. It is used for the following purposes:

- filtering out of external test pulses, e. g. of an active sensor with OSSD outputs.
- filtering out of the test pulses of DOUT4x in the case of passive sensors.
- filtering out of contact bounces.

In a downstream logic operation with comparator, the two input signals A and B are used to form the logical control signal LIN_D40. In this section, the test pulses at the input are also analysed. To request safety functions, the logical input is linked with the corresponding safety function (LIN_D40 = 1 means that the safety function has been requested).

A sensor type can be selected using the parameter "Sensor type" (P02.24/…).

The inputs can be used in three different operating modes through the use of the "Operating mode" parameter (P02.06/...):

- Operating mode = "Unused" (P02.06/... = 0), input is not used. The logical input signal LIN_D40 is continually 0.
- Operating mode = "Equivalent" (P02.06 = 1), input switching equivalently: The inputs A and B of a channel must show the same signal levels. The logical input signal LIN_D40 is inverse to the signal level to DIN40, as Table 19 shows.

Input DIN40/ … /43 equivalent	**Idle state**	**Safety function requested**
DIN40A / … / 43A	24 V	0 V
DIN40B / … / 43B	24 V	0 V
Status LIN_D40 / … /43	0	1

Table 19: Inputs switching equivalently

The inversion of the logical status corresponds to the idle current principle. Only use the inputs according to the idle current principle and request the safe status through 0 V at the input.

- Operating mode = "Antivalent" (P02.06 = 2), input switching antivalently: The inputs A and B must show contrasting signal levels. The logical input signal LIN_D40 is inverse to the signal level to DIN40A, as Table 20 shows.

Input DIN40/ … /43 antivalent	**Idle state**	**Safety function requested**
DIN40A / … / 43A	24 V	0 V
DIN40B / … / 43B	0 V	24 V
Status LIN_D40 / … /43	0	1

Table 20: Inputs switching antivalently

Passive sensors, which trigger an emergency stop of the system (STO, SBC, SS1), must, according to EN 60204-1, have "forced opening" and be parameterised as equivalent inputs.

2.4.2.3 Error detection

The level of the inputs A and B may deviate from the statuses such in Table 19 and Table 20 for a parameterisable time ("Discrepancy time", P02.05/...). If the deviation persists for a longer time, then the error "[57-1] Digital inputs - Signal level error" (discrepancy error) is generated.

The inputs A and B can be monitored using test pulses. The test pulse source is selected using the parameter "Source for test pulse" (P02.07/...). If a test pulse is missing or the input logic detects a short circuit or cross circuit, then the error "[57-0] Self test I/O (internal/external)" is generated.

In cases of error, the logical input LIN_D40 switches to 1 (Safety function requested).

Note

A detected error is forwarded to the error management using the error signals shown in the block diagram. The reaction to the error can be set (only warning, STO, SS1, SS2, etc.). In this case, for further processing, the logical input LIN_D40 assumes the status 1.

The user must ensure that an error (error management) leads to the safe status for the overall system.

2.4.2.4 Timing diagrams

Figure 9, Figure 10, Figure 11 and Figure 12 show the corresponding timing diagrams of a two-channel input, both for equivalent and antivalent parameterisation.

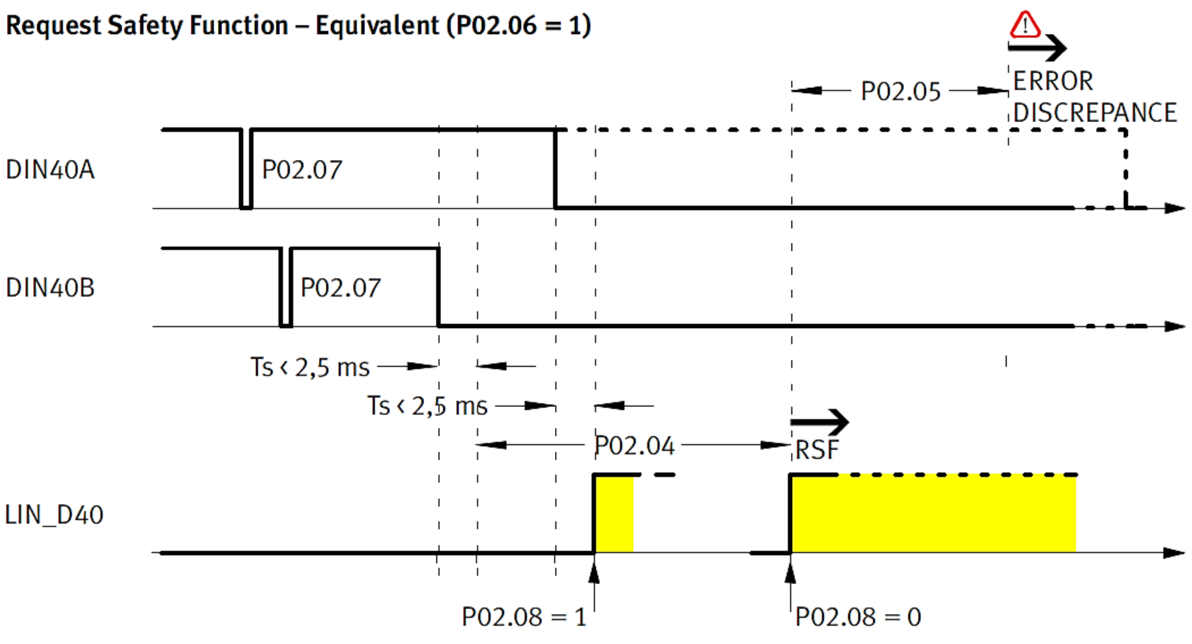


Figure 9: Timing diagram of two-channel equivalent safe input – Start request (DIN40)

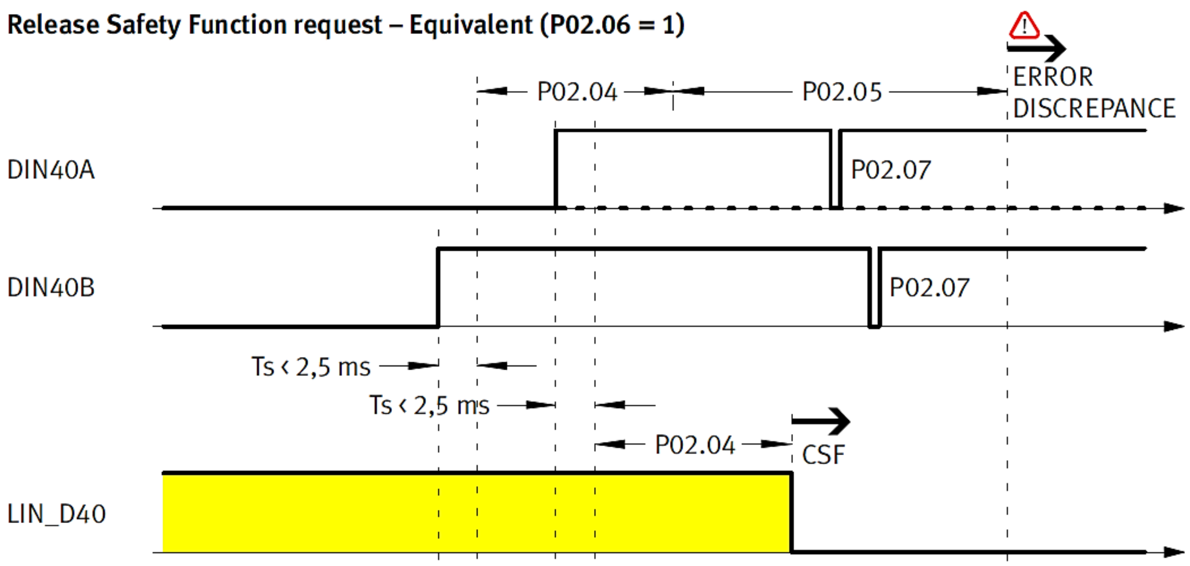


Figure 10: Timing diagram of two-channel equivalent safe input – Terminate request (DIN40)

Term/abbreviation	Explanation
RSF: Request Safety Function	Request safety function
CSF: Release Safety Function request	Terminate the safety function request
Error Discrepancy	Discrepancy error

Table 21: Legend for Figure 9 and Figure 10

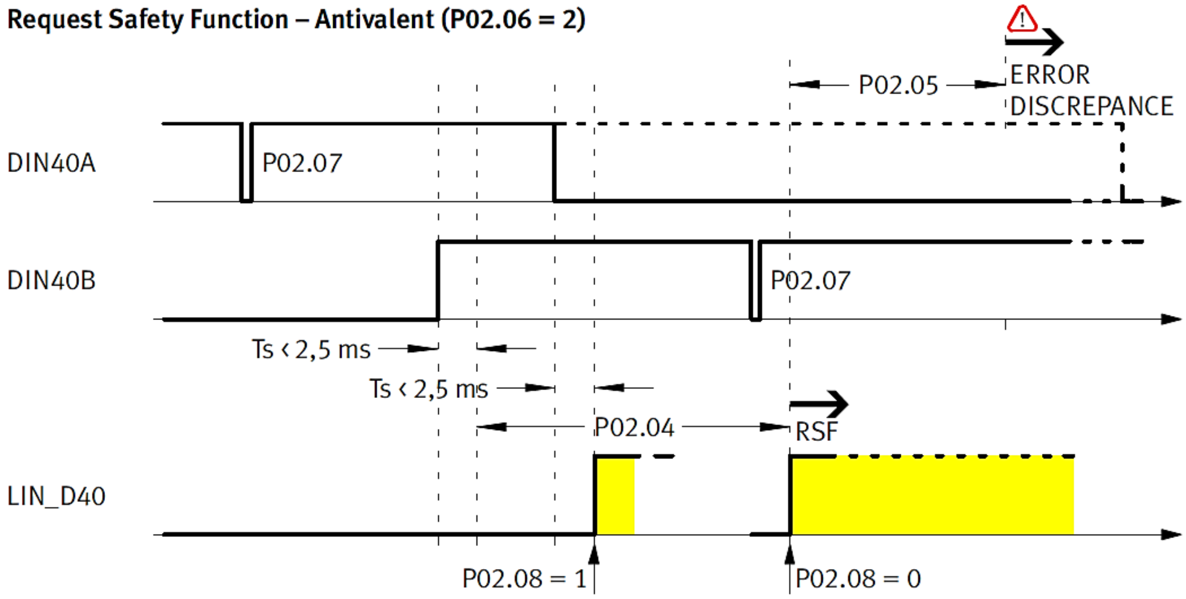


Figure 11: Timing diagram of two-channel antivalent safe input – Start request (DIN40)

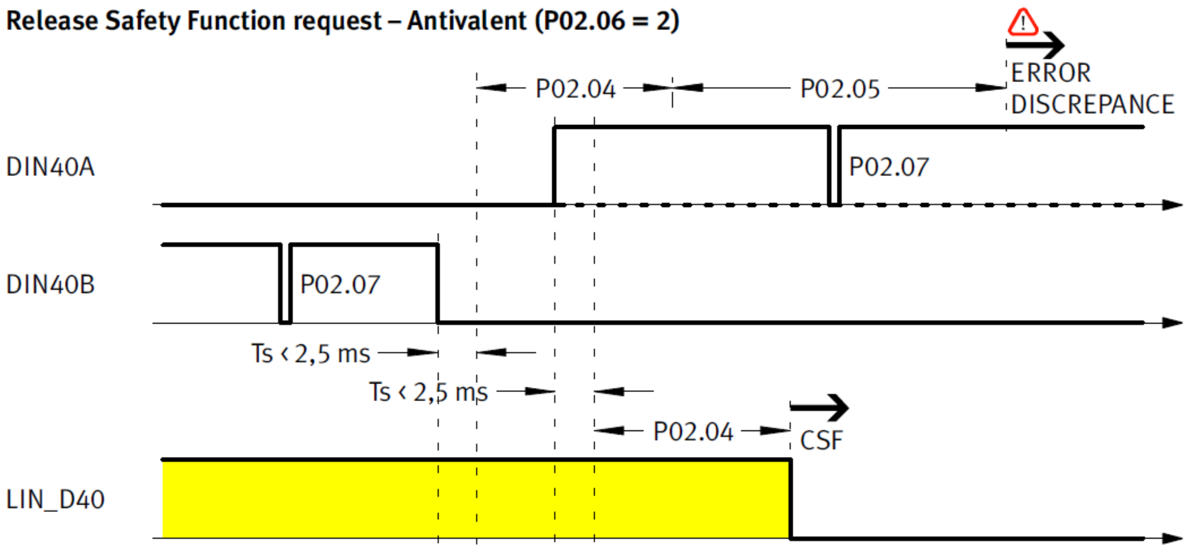


Figure 12: Timing diagram of two-channel antivalent safe input – Terminate request (DIN40)

Term/abbreviation	Explanation
RSF: Request Safety Function	Request safety function
CSF: Release Safety Function request	Terminate the safety function request
Error Discrepancy	Discrepancy error

Table 22: Legend for Figure 11 and Figure 12

The rapid detection of a safety requirement can be activated using the "Quick detection request" parameter (P02.08/...). If both inputs, DIN40A and DIN40B, change level simultaneously, then the switching status is forwarded to the logical signal LIN_D40, by-passing the "LPF" filter. This means that very rapid detection of a safety function request is possible, even in the case of relatively long test pulses and thus large time constant of the filter.

After the request of a safety function via DIN40 ... DIN43, the following times elapse until the logical input LIN_D... and thus the safety function request is activated:

Time delays from the level change	**Minimum**	**Maximum**	**Typical**
Ts	0.5 ms	2.5 ms	1.5 ms
"Filter time constant" (P02.04/09/0E/13)	1.0 ms	1000.0 ms	3.0 ms
Reaction time for "Quick detection request" = 0 (P02.08/P02.0D/P02.12/P02.17 = 0)	1.5 ms	12.5 ms	4.5 ms
Reaction time for "Quick detection request" = 1 (P02.08/P02.0D/P02.12/P02.17 = 1)	0.5 ms	2.5 ms	1.5 ms

Table 23: Time delays DIN40 … DIN43

2.4.2.5 Parameters for the two-channel digital inputs

Parameter no. for input ...				**Name**	**Description**
DIN40	**DIN41**	**DIN42**	**DIN43**		
P02.24	P02.25	P02.26	P02.27	Sensor type	Identifier of the sensor connected to DIN4x.
P02.06	P02.0B	P02.10	P02.15	Operating mode	Mode: 0 = Unused, 1 = Equivalent, 2 = Antivalent
P02.05	P02.0A	P02.0F	P02.14	Discrepancy time	Discrepancy time
P02.07	P02.0C	P02.11	P02.16	Source for test pulse	Selection of the output supplying the test pulses.
Expert parameter					
P02.04	P02.09	P02.0E	P02.13	Filter time constant	Filter time constant.
P02.08	P02.0D	P02.12	P02.17	Quick detection request	Use quick switch-off on Low level at DIN4xA and DIN4xB.

Table 24: Parameters, two-channel digital inputs

Table 119 ➔ in Appendix 7.1 describes the technical data for the control ports within the specified operating range of the logic voltages in accordance with EN 61131-1.

2.4.3 Single-channel (partially-safe) digital inputs DIN44 … DIN49 [X40]

2.4.3.1 Use

The digital inputs DIN44..DIN49 have one channel. They can be used to connect passive switches and active sensors.

Use the single-channel inputs as diagnostic inputs, for control functions which only require a single-channel input or in a combination of multiple inputs in order to request safety functions.

If active two-wire sensors are used without self-diagnostics:

If the active two-wire sensor is not actuated, then not all the required tests are carried out by the safety module. For this reason, regular actuation is required for a function test. We recommended actuating every 8 hours or once per shift, but at least once every 24 hours (➔ 7.1.4, Table 119).

To request and deactivate safety functions, only the two-channel inputs DIN40 … DIN43 or suitable logical combinations of single-channel inputs may be used.

2.4.3.2 Function

Figure 13 shows the block diagram of the single-channel inputs. The function is explained below for DIN44. The inputs DIN44 to DIN49 have an identical structure.

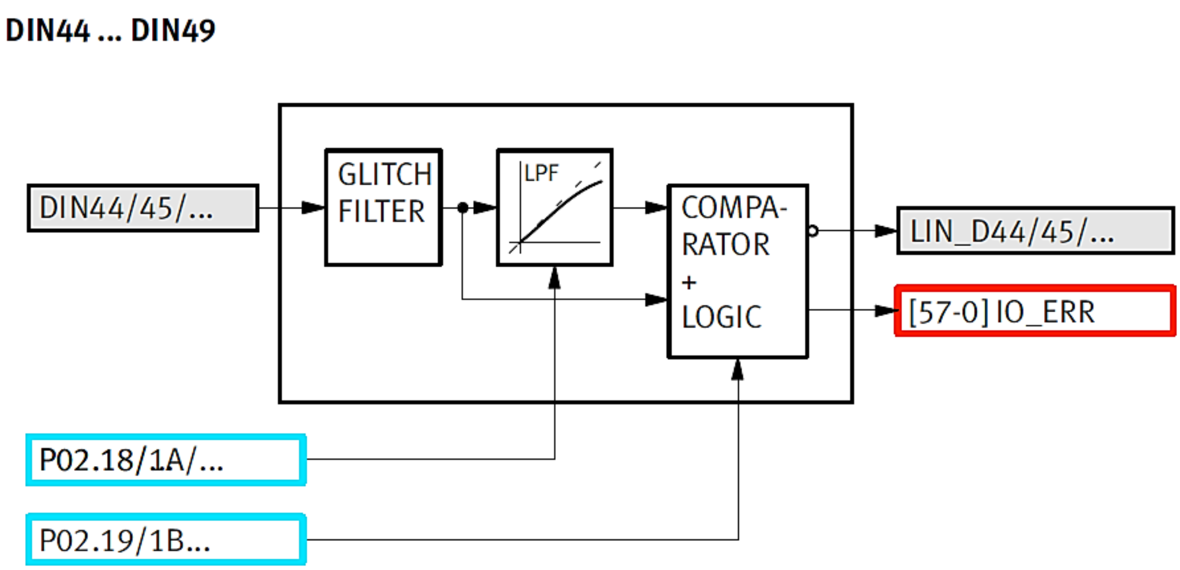


Figure 13: Block diagram of the single-channel inputs

Term/abbreviation	Explanation
DIN40A/..., DIN40B/...	Two-channel digital inputs DIN40A/DIN40B ...
GLITCH FILTER	Filter for interference
LPF	Low-pass filter
COMPARATOR + LOGIC	Comparator and logic
LIN_x	Logical inputs ...
[5x-x] xxx_ERR	Internal error signal, error 5x-x

Table 25: Legend for Figure 13

The signal levels at the inputs DIN44 to DIN49 are first dejammed in a preliminary EMC filter, the "Glitch Filter". The filter time constant is 500 µs and cannot be parameterised.

After this first filter, a second "LPF" filter, which can be parameterised using the parameter "Filter time constant" (P02.18), follows for each input signal, and is designed as a programmable Mono-Flop. It is used for the following purposes:

- filtering out of external test pulses, e. g. of an active sensor with OSSD outputs.
- filtering out of the test pulses of DOUT4x in the case of passive sensors.
- filtering out of contact bounces.

In a downstream logic operation with comparator, the two input signals are used to form the logical control signal LIN_D44/.../49 (LIN_D44/.../49 = 1 equates to Control function requested). In this section, the test pulses at the input are also analysed.

The sensor type can be selected using the parameter "Sensor type" (P02.28 ... P02.2D).

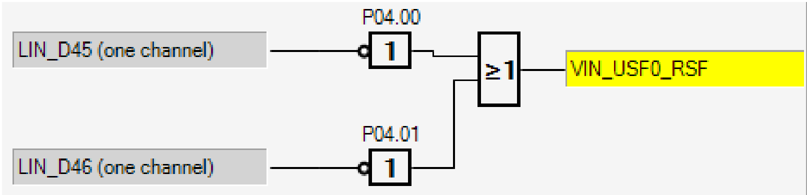
Input DIN44/ … /49	Idle state	Control function requested
DIN44 / … / 49	0 V	24 V
Status LIN_D44 / … /49	0	1

Table 26: Inputs switching antivalently

The logical status directly represents the voltage level at the input - in contrast to the two-channel inputs DIN40...DIN43, which follow the idle current principle. This means that the inputs are designed for control functions, such as the mode selector switch, which require positive logic.

If you wish to use the single-channel inputs or their combination to request safety functions, the idle current principle should be observed:

Then, use the inverted logic signal to request the safety function, e. g. Example:



2.4.3.3 Error detection

The inputs can be monitored using test pulses. The test pulse source (DOUT40 to DOUT42) is selected using the parameter "Source for test pulse" (P02.19/...). If a test pulse is missing or the input logic detects a short circuit or cross circuit, then the error "[57-0] Self test I/O (internal/external)" is generated.

In cases of error, the logical input LIN_D44 switches to 1 (Control function requested).

Note

A detected error is forwarded to the error management using the error signals shown in the block diagram. The reaction to the error can be set (only warning, STO, SS1, SS2, etc.). In this case, for further processing, the logical input LIN_D44 assumes the status 1.

The user must ensure that an error (error management) leads to the safe status for the overall system.

2.4.3.4 Parameters for the single-channel digital inputs

Parameter no. for input ...						**Name**	**Description**
DIN44	**DIN45**	**DIN46**	**DIN47**	**DIN48**	**DIN49**		
P02.28	P02.29	P02.2A	P02.2B	P02.2C	P02.2D	Sensor type	Identifier of the sensor connected to DIN4x.
P02.19	P02.1B	P02.1D	P02.1F	P02.21	P02.23	Source for test pulse	Selection of the output supplying the test pulses.
Expert parameter							
P02.18	P02.1A	P02.1C	P02.1E	P02.20	P02.22	Filter time constant	Filter time constant

Table 27: Digital inputs

2.4.3.5 Timing diagram

Figure 14 shows the corresponding timing diagram of a single-channel input:

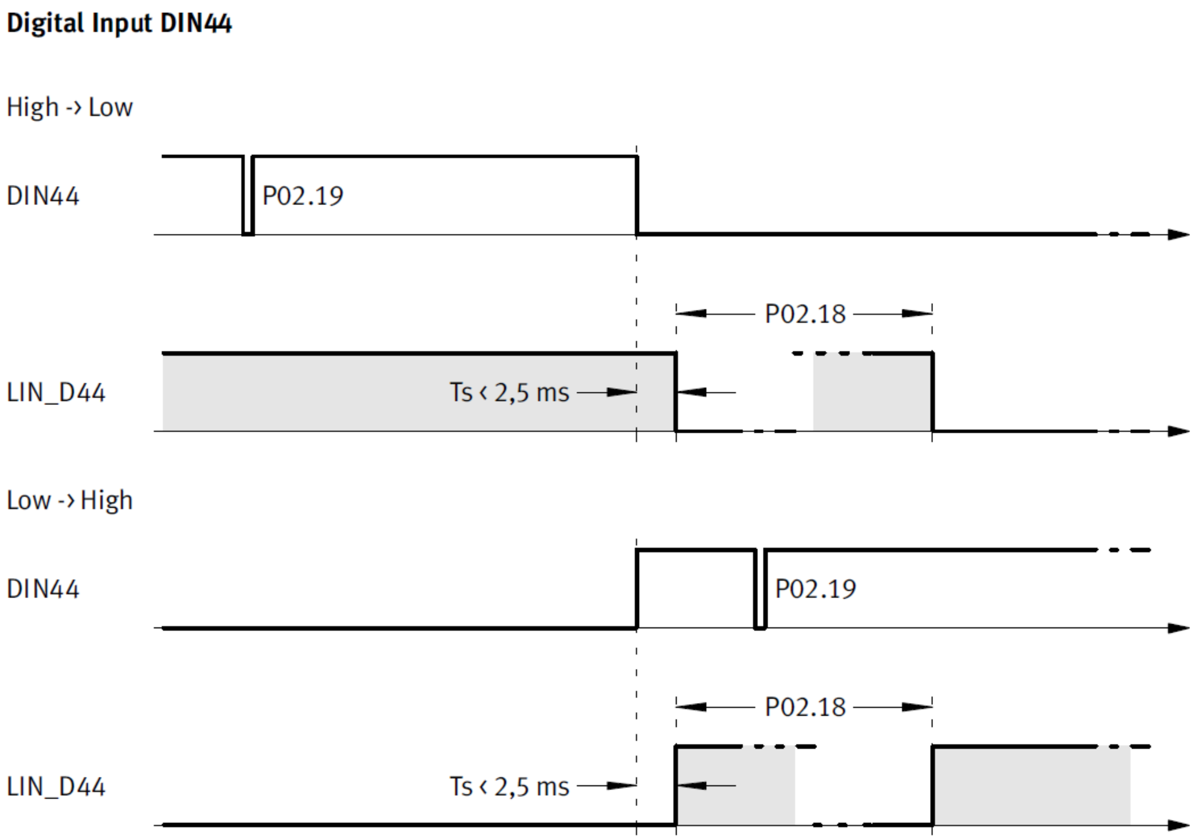


Figure 14: Timing diagram of single-channel input (example DIN44)

After the request of a control function via DIN44 ... DIN49, the following times elapse until the logical input LIN_D... is switched to active:

Time delays from the level change	Minimum	Maximum	Typical
Ts	0.5 ms	2.5 ms	1.5 ms
Filter time constant (P02.18/1A/1C/1E/20/22)	1.0 ms	10.0 ms	3.0 ms
Reaction time	1.5 ms	12.5 ms	4.5 ms

Table 28: Time delays DIN44 … DIN49

Table 119 ➔ in Appendix 7.1 describes the technical data for the control ports within the specified operating range of the logic voltages in accordance with EN 61131-1.

2.5 Safety functions

The safety functions have a two-part structure, which can be seen in all the functions:

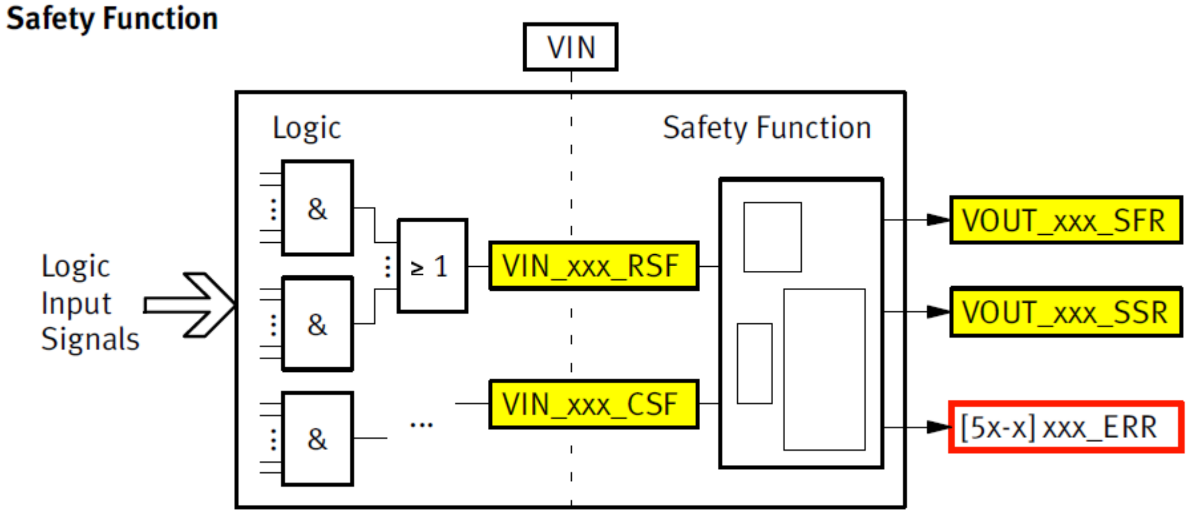


Figure 15: Block diagram, general structure of the safety functions

Term/abbreviation	Explanation
Logic Input Signals	Logical input signals
Logic	Logic, configurable for the safety functions using product terms
Safety Function	Safety function
VIN_xxx_RSF	Virtual input: Request safety function xxx (Request Safety Function)
VIN_xxx_CSF	Virtual input: Terminate safety function xxx request (Clear Safety Function request)
VOUT_xxx_SFR	Virtual output: Safety function xxx requested (Safety Function requested)
VOUT_xxx_SSR	Virtual output: Safety function xxx Safe state reached (Safe State Reached)
[5x-x] xxx_ERR	Internal error signal: Error 5x-x

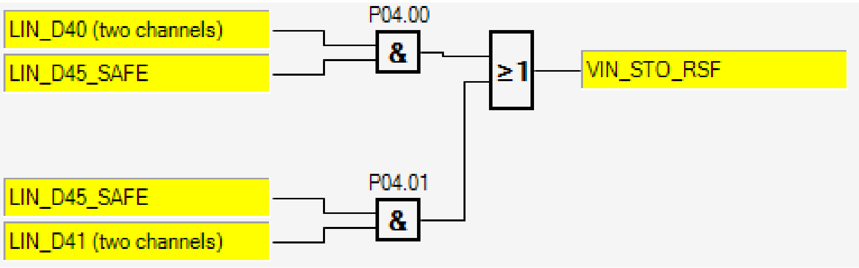
Table 29: Legend for Figure 15

2.5.1 Logic section (left part)

A configurable logic function (AND, OR gate in disjunctive standard format) is used to define which input signals (LIN_x) are switched to the safety function for:

– requesting the safety function, VIN_xxx_RSF signal (Request Safety Function)
– terminating the request of the safety function, VIN_xxx_CSF signal (Clear Safety Function)
– selecting additional feedback signals (e. g. for SBC)

The input logic for the STO function could look as followings in the "Request" tab in the SafetyTool:



The STO function is requested via DIN40, if the mode switch DIN45 is active or via DIN41, if the mode switch DIN45 is not active.

For each VIN... input, there is an OR gate with four inputs and upstream AND gates with seven inputs. All the signals can be inverted.

Each request of the safety function has priority over termination of the request.

This means: As long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

2.5.2 Safety function (right-hand section)

For as long as the safety function is requested, it safely monitors the status variables of the drive. It contains the required logic and sequence functions for this, which can be parameterised.

The logic and sequence function are initialised on the rising edge of the request. For example, the start values for slowdown ramps are calculated in this manner.

The safety function takes the current status of the drive (position, speed) into account and generates various status signals and control signals. The most important functions are described in brief below:

- A parameter is used to define whether an automatic restart should occur after cancelling the request, or not.
- The stop functions have an additional control input to request the safety function. This input, ERR_xxx_RSF, is supplied directly from the error management, as the stop function and error response can be requested by the error management.
- Some safety functions can also be requested directly from other safety functions. For example, STO is automatically activated at the end of the slowdown ramp of an SS1 function, but is also terminated with it as well.

Each safety function provides at least the following output signals:

- the status message VOUT_xxx_SFR, safety function xxx requested,
- the status signal VOUT_xxx_SSR, safe state xxx reached,
- at least one error message xxx_ERR if the safety condition is violated.

In addition, some safety functions provide additional control signals, e.g.

- for direct activation of the hardware, e.g. the driver supply or holding brake output for the safe brake control,
- for the request of downstream safety functions, e.g. STO_SBC_RSF.

These output signals can be transmitted to the function controller as a status signal. They can be used to activate external safety switching devices via safe outputs. For example, an external clamping unit can be activated.

Safety functions for motion monitoring also use the safely-detected speed (ACTUAL_SPEED) or a safely-detected position (ACTAL_POSITION) for monitoring. They control the approved speed in the functional section of the servo drive via a speed limit (SPEED_LIMIT).

The safety functions are configured using a series of parameters. The following can be set:

- speed ramps,
- monitoring limits for speed and position,
- time delays.

Additional settable options are:

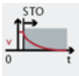
- the behaviour for restart.
- the way in which the safety module manipulates operation of the basic unit:
  - it does not manipulate actively and only monitors.
  - it activates the quick stop in the basic unit and causes the basic unit to perform a quick stop whilst monitoring the braking operation.
  - it actively regulates the speed in the basic unit downwards and, at the same time, monitors compliance with the limit values.

EN 61800-5-2 defines the various safety functions for drive controllers. It also defines three methods for monitoring braking. Through the above configuration, the safety module can support all the methods listed in the standard.

The safety module supports the safe stop and movement functions described in the following sections, in accordance with ➔ Section 2.2.3, Table 44.

2.5.3 STO – Safe Torque Off

2.5.3.1 Application



The function described here implements the safety function STO according to EN 61800-5-2 (stop category 0 from EN 60204-1).

Use the “Safe torque off” function (STO) whenever you have to reliably disconnect the energy supply to the motor in your particular application but there are no additional requests for targeted stopping of the drive.

The STO function is activated by the factory setting (advance parameterisation).

As the function is used by other functions (request through SS1 or error reaction on violation of other requested safety functions), it cannot be deselected.

2.5.3.2 Function

The function "Safe torque off" switches off the driver supply for the power semiconductors, thus preventing the power end stage from supplying the energy required by the motor.

When the "Safe Torque Off" (STO) function is active, the energy supply to the drive is interrupted in a safe manner. The drive cannot generate any torque and, thereby, neither any dangerous movements. With suspended loads or other external forces, additional measures must be taken to ensure that the load does not drop (e.g. mechanical clamping units). In the STO “Safe torque off” status, the idle position is not monitored.

The machine must be stopped and locked in a safe manner. This especially applies to vertical axles without automatic locking mechanisms, clamping units or counterbalancing.

➔ **Note**

There is a risk that the drive will advance if there are multiple errors in the ARS 2000 FS.

Failure of the servo drive output phase during STO status (simultaneous short circuit of 2 power semiconductors in different phases) may result in a limited detent movement of the rotor. The rotation angle / path corresponds to a pole pitch. Examples:

– Rotary axle, synchronous machine, 8-pin ➔ movement < 45° at the motor shaft.
– Linear motor, pole pitch 20 mm ➔ movement < 20 mm at the moving part.

The STO (Safe Torque Off) function does not provide protection from electric shock, only from hazardous movements! The drive is not disconnected from the power supply as is required for electrical safety ➔ product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS.

The logic to request the STO safety function is shown in the following block diagram:

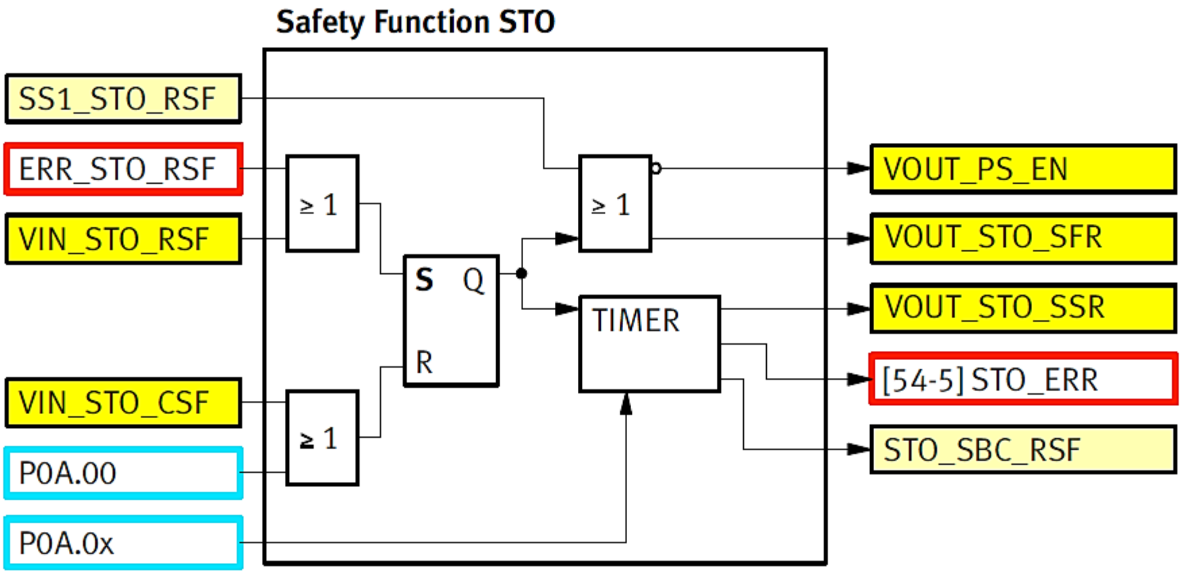


Figure 16: Block diagram STO

Term/abbreviation	Explanation
Safety Function STO	STO safety function
SS1_STO_RSF	Internal signal: Request STO by SS1
ERR_STO_RSF	Internal signal: Request STO through error reaction
VIN_STO_RSF	Virtual input: Request STO
VIN_STO_CSF	Virtual input: Terminate STO request
TIMER	Timer
VOUT_PS_EN	Virtual output: Output stage enable approved
VOUT_STO_SFR	Virtual output: STO requested
VOUT_STO_SSR	Virtual output: Safe state STO reached
[54-5] STO_ERR	Internal error signal: Error 54-5
STO_SBC_RSF	Internal signal: Request SBC by STO

Table 30: Legend for Figure 16

The safety function is requested as follows:

- by the user via any combination of input signals LIN_D... on the signal VIN_STO_RSF.
- as an error reaction, controlled via the error management system, signal ERR_STO_RSF.
- via the safety function SS1, signal SS1_STO_RSF.

A request for the safety function STO is cancelled as follows:

- by the user via a combination of different inputs on the signal VIN_STO_CSF.
- setting the parameter "Automatic restart allowed" (P0A.00) performs an automatic restart when the request is cancelled.

Each request of the safety function has priority over termination of the request.

This means: As long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

The safety function controls the switch-off of the driver supply via the VOUT_PS_EN signal.

If necessary, the safety function SBC can also be requested automatically with the signal STO_SBC_RSF. In addition, it generates the status messages:

- VOUT_STO_SFR, safety function STO requested.
- VOUT_STO_SSR, safe state STO reached.

2.5.3.3 Error detection

The supply of energy to the drive is reliably and immediately disconnected via the active safety function STO "Safe Torque Off". This is ensured by a two-channel design of the switch-off circuit, which is checked continuously during operation. If a switch-off channel fails, an error message is generated. The drive is switched off by the remaining channel.

The error message [54-5] STO_ERR "Safety condition STO violated" is output in the case of an error in the STO function.

2.5.3.4 Process

The sequence of the STO safety function is shown in the following diagram:

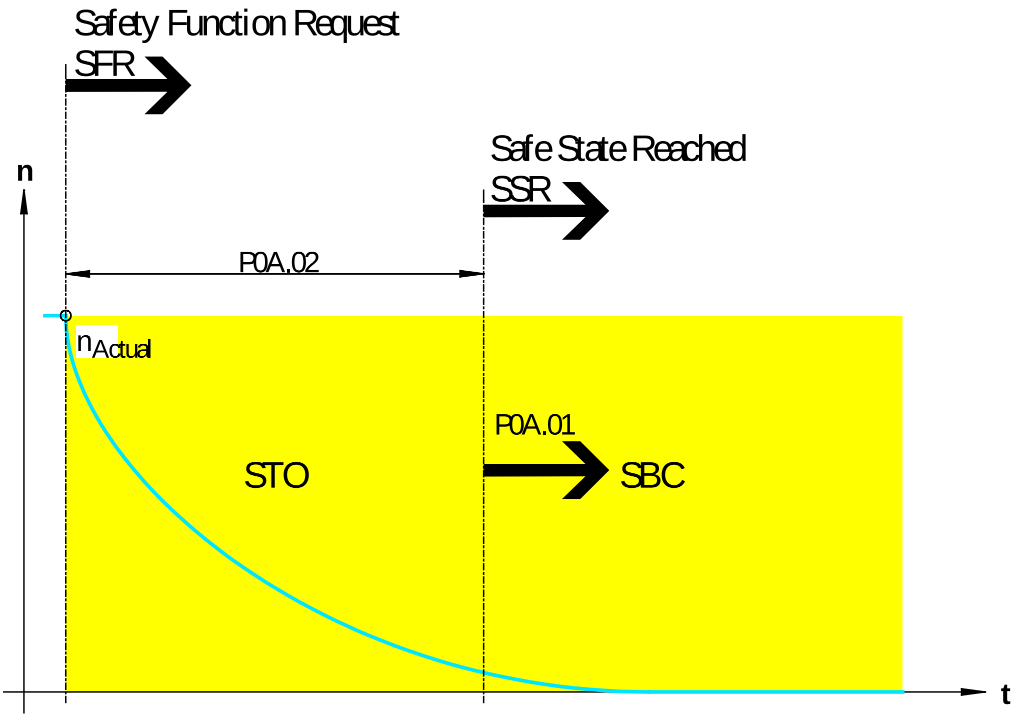


Figure 17: Sequence diagram STO

Term/abbreviation	**Explanation**
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
n_{act}	Actual speed

Table 31: Legend for Figure 17

When the safety function STO is requested, the driver supply is switched off immediately and without any significant delay on two channels.
After a configurable delay time "Delay time to "STO" signal" (P0A.02), the internal status VOUT_STO_SSR "Safe state reached" becomes active.
After the request of the safety function STO, the following times elapse until the safety function is activated:

Time delays from VIN_STO_RSF	**Minimum**	**Maximum**	**Typical**
VOUT_STO_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_STO_SSR	2.0 ms + P0A.02	2.1 ms + P0A.02	2.0 ms + P0A.02
Reaction time until switch-off of drive supply of basic unit and output stage OFF	2.5 ms	4.5 ms	3.5 ms

Table 32: STO time delays

2.5.3.5 Parameters for STO

STO: Safe Torque Off		
No.	**Name**	**Description**
P0A.02	Time delay until "STO" signal	Delay time until the "Safe state reached" output becomes active.
P0A.00	Automatic restart permitted	If set: Cancellation of the request (restart) if an inactive request arrives
P0A.01	Automatic activation of SBC	If set: Safe brake control is activated when the safe state is reached (after the delay time has expired).

Table 33: STO: Safe Torque Off

2.5.4 SBC – Safe Brake Control

2.5.4.1 Application

The function described here implements the safety function SBC according to EN 61800-5-2.

Use the "Safe Brake Control" (SBC) function to activate a clamping unit or holding brake, in order to mechanically brake the axle in a controlled manner or to hold it securely.

The clamping unit or holding brake can be activated via:

- the safe brake output [X6] in the servo drive,
- a safe output of the safety module and an external brake switching device.

Important: To use the safety function SBC, a clamping unit or holding brake with appropriate safety classification must be used. It is always the case that, for all types of clamping units without certification, a risk analysis must be carried out and the suitability determined for the appropriate safety application. Otherwise, these may not be used.

The holding brake in motors is not usually appropriately qualified.

The SBC function is activated by the factory setting (advance parameterisation).

As long as the function is used by other functions (request through STO, by other parameterisations or an error when other requested safety functions are violated), it cannot be deselected.

2.5.4.2 Function

The "Safe Brake Control" function immediately switches off the voltages for the connected clamping unit or holding brake. The clamping unit or holding brake takes effect and brakes the motor or the axle. Dangerous movements are thus prevented mechanically. The braking time is dependent on how quickly the brake engages and how high the energy level is in the system.

→ **Note**

If there are suspended loads, they usually drop if SBC is requested simultaneously with STO. This can be traced back to the mechanical inertia of the clamping unit or holding brake and is thus unavoidable.

The safety module also makes the safety function SS1 available in combination with SBC or the safety function SS2. Please check whether you can or may use these safety functions in your application with SBC instead of STO.

Safe brake control can only be used with clamping units or holding brakes, which engage in the de-energised state. The clamping unit or holding brake is then opened by supplying energy.

When using the brake output of the basic unit, ensure that the cables are routed so that they are protected. If the load capacity of the safe outputs of the safety module is sufficient, then cross-circuit detection with test pulses is possible.

The logic to request the SBC safety function is shown in the following block diagram:

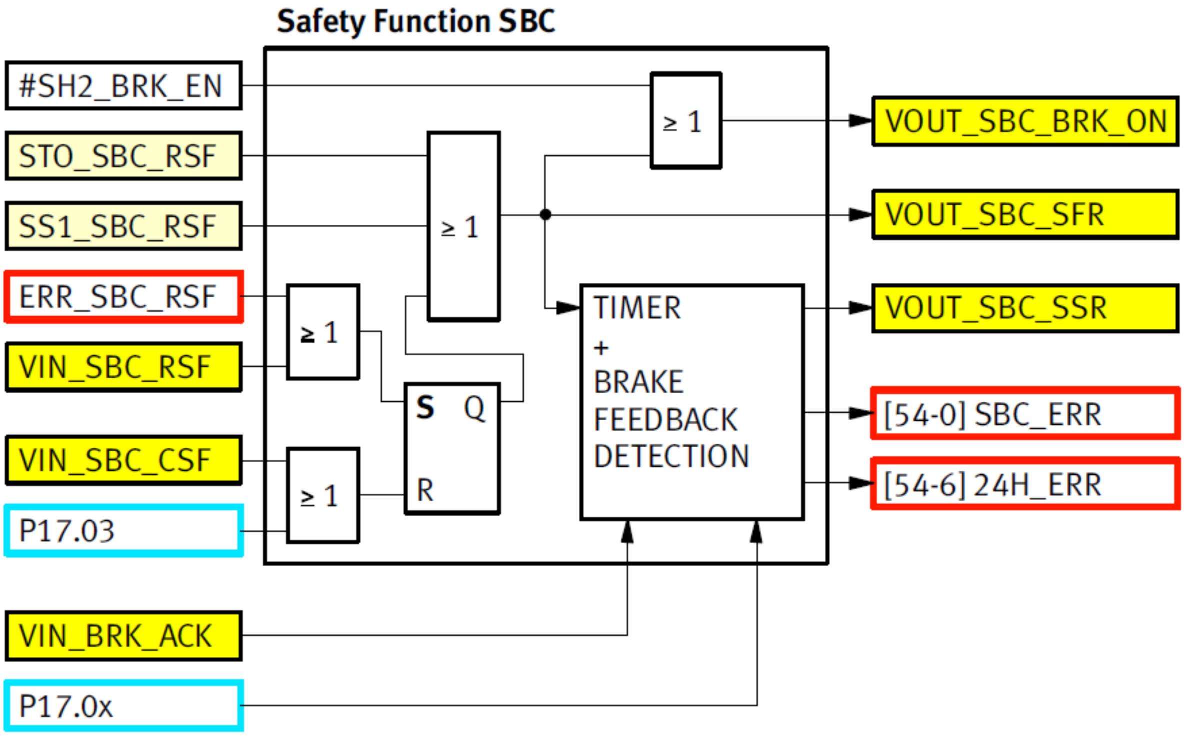


Figure 18: Block diagram SBC

Term/abbreviation	**Explanation**
Safety Function SBC	Safety function SBC
#SH2_BRK_EN	Basic unit enables safe brake control
STO_SBC_RSF	Internal signal: Request SBC by STO
SS1_SBC_RSF	Internal signal: Request SBC by SS1
ERR_SBC_RSF	Internal signal: Request SBC through error reaction
VIN_STO_RSF	Virtual input: Request SBC
VIN_STO_CSF	Virtual input: Terminate SBC request
VIN_BRK_ACK	Virtual input: Analysis of feedback signal, safe brake control
TIMER + BRAKE FEEDBACK DETECTION	Timer and analysis of feedback, safe brake control
VOUT_SBC_BRK_ON	Virtual output: Switch brake output
VOUT_SBC_SFR	Virtual output: SBC requested
VOUT_SBC_SSR	Virtual output: Safe state SBC reached
[54-0] SBC_ERR	Internal error signal, error 54-0
[54-6] 24H_ERR	Internal error signal, error 54-6

Table 34: Legend for Figure 18

The safety function SBC is requested as follows:

- by the user via any combination of input signals LIN_D... on the signal VIN_SBC_RSF.
- as an error reaction, controlled via the error management system, signal ERR_SBC_RSF.
- via the safety function STO, signal STO_SBC_RSF.
- via the safety function SS1, signal SS1_SBC_RSF.

The request for the safety function SBC is cancelled as follows:

- by the user via a combination of different inputs on the signal VIN_SBC_CSF.
- by setting the parameter P17.03, an automatic restart is performed when the request is cancelled.

Each request of the safety function has priority over termination of the request.

This means: As long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

The safety function controls the switch-off of the safe brake control via the VOUT_SBC_BRK_ON signal. If the safety function is requested, VOUT_SBC_BRK_ON = 1.

VOUT_SBC_BRK_ON is internally linked to a control signal of the basic unit which forwards the switching status of the brake activation in the basic unit. Safe brake control is only energised when no SBC has been requested and the basic unit enables the brake (#SH2_BRK_EN is Low).

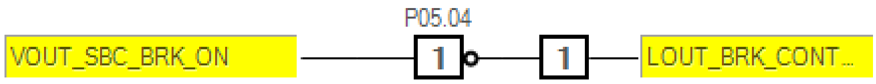
After a request of SBC and subsequent cancellation, the safe brake control is only energised when the basic unit enables the holding brake.

This ensures that z axles with a suspended load can be restarted without the load dropping.

The control signal VOUT_SBC_BRK_ON must either be switched to the internal brake activation of the servo drive (control signal LOUT_BRAKE_CTRL, ➔ Section 8.1.4) or to a digital output for control of an external clamping unit (LOUT_D4x, ➔ Section 8.1.4).

To use the brake activation of the basic unit at [X6] in conjunction with SBC, configure the output "Internal brake" of the safety module:

Request:



Standard parameter:

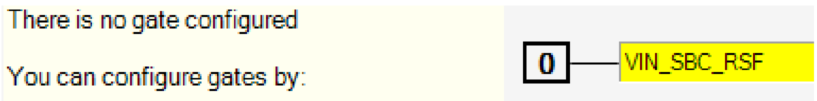
P02.36	Operating mode		Equivalent = [1]
P02.37	Test pulse length	ms	1,0

The brake control of the basic unit is now additionally monitored using test pulses.

The servo drive detects a switch-off of the safe brake control from outside. If necessary, it performs a Quick Stop and switches the output stage off. On the microcontroller side, brake activation can also be switched on continuously (use of the parameters from the holding brake activation in the servo drive), so that control only takes place via the safety module.

To use the brake activation of the basic unit [X6] independently of SBC and to use SBC in combination with DOUT4x, configure the "Internal brake" output of the safety module to Continuous ON:

Request:

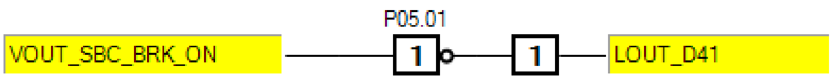


Standard parameter:

P02.36	Operating mode		Static High = [2
P02.37	Test pulse length	ms	1,0

In addition, configure an output, e.g. DOUT41, as an output of the control signal for the safe brake control:

Request:



Standard parameter:

P02.36	Operating mode		Equivalent = [1
P02.37	Test pulse length	ms	1,0

If the SBC function activates an external clamping unit or holding brake via a digital output, then the control signals for the internal safe brake control in the basic unit can be configured in such a way that SBC no longer has an effect on them. The brake output of the basic unit is then available for other functions (=> control signals FSM_BR+_EN and FSM_BR-_EN can be parameterised to high).

Information concerning the behaviour of the basic unit can be requested from Metronix.

The activation of a clamping unit with its increased current consumption (typically 8 A or more) requires an external circuit via two intermediate contactors with forced feedback contacts. In this case, feedback must be wired separately. In this case, it is run to the safety module via a digital input, usually DIN44.

In addition, the SBC function generates the status messages:

– VOUT_SBC_SFR, safety function SBC requested.
– VOUT_SBC_SSR, safe state SSBC reached (delay settable using P17.01).

SBC output signals	**Idle state**	**Safety function requested/achieved**
VOUT_SBC_BRK_ON	0	1
VOUT_SBC_SFR	0	1
VOUT_SBC_SSR	0	1 (delayed P17.01)

Table 35: SBC output signals

2.5.4.3 Error detection

The safety function can analyse an external feedback signal, thus checking that the clamping unit or holding brake has actually engaged. Analysis takes place via the VIN_BRK_ACK input, if this function is activated via the parameter P17.02.

A time delay for feedback can be parameterised using the parameter P17.00.

The feedback signal is analysed after the delay has elapsed. If there is no feedback, then the error message [54-0] SBC_ERR.

→ **Note**

If the brake output at [X6] is used, then the feedback input VIN_BRK_ACK can be switched to the feedback input of the basic unit (signal LIN_BRAKE_X6_FB). This signal maps the switching status of the safe braking output at the basic unit.

If there is a motor cable at the brake output [X6], but no clamping unit or holding brake is connected, then interference is possible in the open brake cable, leading to incorrect feedback (error [54-0]).

❖ In this case, deactivate the acknowledgement input.

→ **Note**

When an external clamping unit is used, the acknowledgement input VIN_BRK_ACK must be mapped to a safe digital input.

Only the status "Brake fallen in" (level monitoring of VIN_BRK_ACR) is monitored. The feedback is not monitored when there is an "energised brake".

In addition, the SBC function has integrated time monitoring:

The SBC function may be requested for a maximum of 24 hours. The clamping unit or holding brake must therefore be switched (vented) at least once within 24 hrs, as the circuit breakers can only be tested with test pulses when switched on.

If the time limit is exceeded, the error [54-6] 24H_ERR is generated.

The time restriction becomes invalid if the SBC function is used in connection with a safe output (DOUT40 … DOUT42) or the holding brake is not used for safety purposes. The 24 hr. monitoring can then be deactivated by the expert parameter P17.04.

➔ **Note**

In the delivery status of the safety module, the SBC function is always configured in conjunction with the output [X6], even if you do not wish to use the SBC function. In applications in which the brake control lines are run in the motor cable, if no holding brake is connected on the motor side, interference can be coupled into the open brake lines. The safety module then generates the error 57-0.

❖ In these cases, please disconnect the brake control lines from X6 and connect them to PE.

2.5.4.4 Process

The sequence of the SBC safety function is shown in the following diagram:

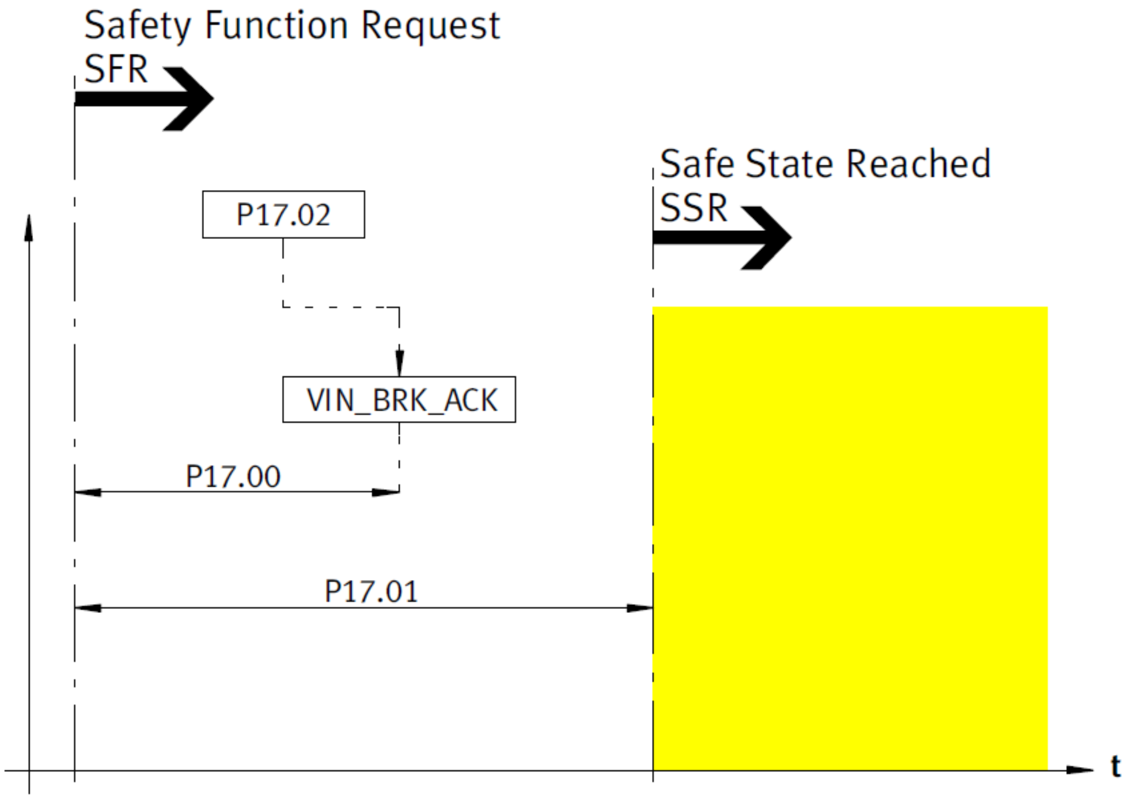


Figure 19: SBC sequence diagram

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
VIN_BRK_ACK	Virtual input: Analysis of feedback signal, holding brake

Table 36: Legend for Figure 19

If the safety function SBC is requested, then the following times elapse for the switch-off of the clamping unit or holding brake (VOUT_SBC_BRK_ON) and the feedback of the safety function:

Time delays from VIN_SBC_RSF	Minimum	Maximum	Typical
VOUT_SBC_BRK_ON	2.0 ms	2.1 ms	2.0 ms
VOUT_SBC_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SBC_SSR	2.0 ms + P17.01	2.1 ms + P17.01	2.0 ms + P17.01
Error response time for missing feedback VIN_BRK_ACK	2.0 ms + P17.00	2.1 ms + P17.00	2.0 ms + P17.00

Table 37: SBC time delays

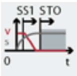
2.5.4.5 Parameters for SBC

SBC: Safe Brake Control		
No.	**Name**	**Description**
P17.00	Time delay, analysis of brake feedback	Time from the request of the safety function, by which the feedback must have come from the holding brake.
P17.01	Time delay until "Brake engaged" signal	Time delay after request of the safety function until the "Safe state reached" output becomes active
P17.02	Analyse holding brake feedback	If 1: Analyse the feedback of the holding brake.
P17.03	Automatic restart permitted	If 1: Cancellation of the request (restart) if an inactive request arrives
Expert parameter		
P17.04	Cyclical test/deactivate 24 hr. monitoring	If 1: The cyclical test of brake activation and 24 hr. monitoring for actuation of the holding brake by the basic unit is deactivated. The safe brake output of the basic unit can be used as a "normal" DOUT with a high acceptable current load.

Table 38: SBC: Safe Brake Control

2.5.5 SS1 – Safe Stop 1

2.5.5.1 Application



The function described here implements the safety function SS1 according to EN 61800-5-2.

Use the "Safe Stop 1" function (SS1) whenever you have to brake the motor and then reliably disconnect the energy supply to the motor in your particular application but there are no additional requests for targeted stopping of the drive (cf. stop category 1 in EN 60204-1).

The three characteristics described in the standard are supported:

a) Triggering and controlling the rate of motor deceleration within specified limits and triggering the STO function when the motor speed falls below a specified limit value.
➔ The drive is taken through a slowdown ramp until it is detected as idling (P06.09), then the output stage is switched off.

b) Triggering and monitoring the motor deceleration variable within specified limits and triggering the STO function when the motor speed falls below a specified limit value.
➔ The safety module activates a fast stop in the basic device, the slowdown ramp is monitored, after which the output stage is switched off.

c) Triggering the motor deceleration and after an application-specific time delay, triggering the STO function.
➔ The safety module delivers a status signal, the basic unit must be braked by the functional controller, after a waiting time the output stage is switched off.

The SS1 function is activated by the factory setting (advance parameterisation).

As long as the function is used by other functions (error response on violation of other requested safety functions), it cannot be deselected.

2.5.5.2 Function

When requesting the SS1 safety function, this checks that the drive is braked to idle within a defined time using a defined slowdown ramp. After the defined time has elapsed, STO is triggered and the power output stage is switched off safely.

Note

If there are suspended loads, they usually drop if STO is requested immediately after the slowdown ramp has elapsed.

For this reason, the SS1 can also trigger through SBC, meaning that an existing clamping unit or holding brake engages, avoiding dropping of an axle. SBC then triggers STO (linkage of the safety functions SS1 → SBC → STO).

The logic to request the SS1 safety function is shown in the following block diagram:

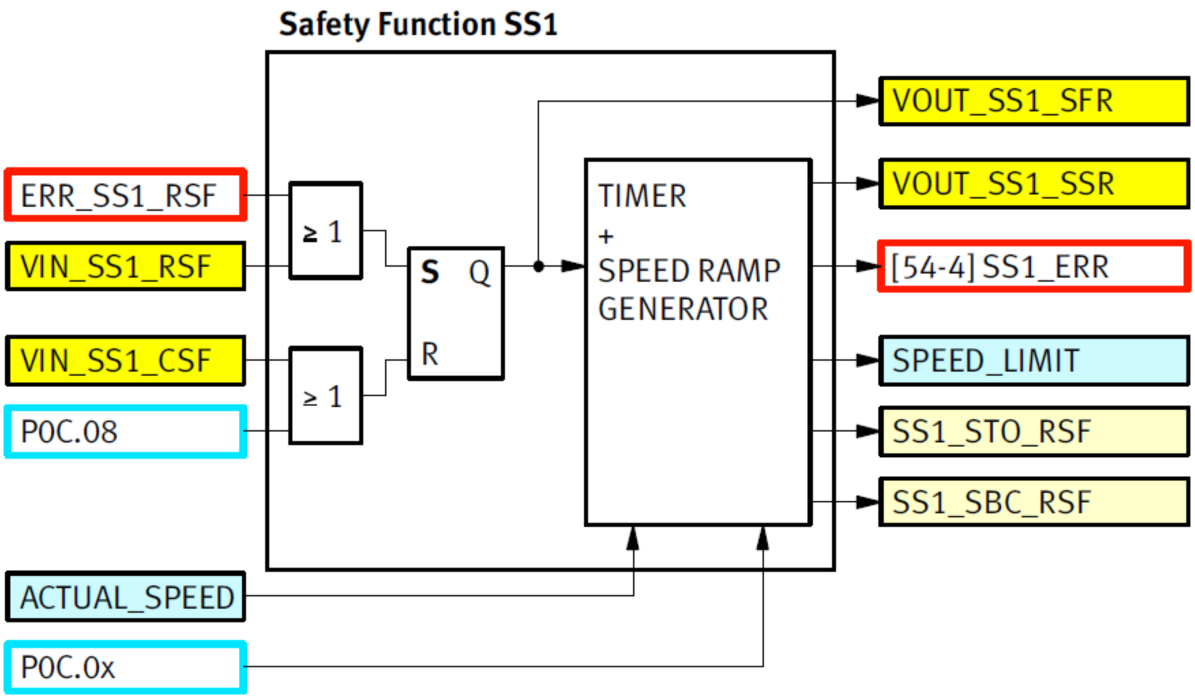


Figure 20: Block diagram SS1

Term/abbreviation	Explanation
Safety Function SS1	Safety function SS1
ERR_SS1_RSF	Internal signal: Request SS1 through error reaction
VIN_SS1_RSF	Virtual input: Request SS1
VIN_SS1_CSF	Virtual input: End SS1 request
ACTUAL SPEED	Internal signal: current speed
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_SS1_SFR	Virtual output: SS1 requested
VOUT_SS1_SSR	Virtual output: Safe state SS1 reached
[54-4] SS1_ERR	Internal error signal: Error 54-4
SPEED_LIMIT	Internal signal: Speed limit in basic unit
SS1_STO_RSF	Internal signal: Request STO by SS1
SS1_SBC_RSF	Internal signal: Request SBC by SS1

Table 39: Legend for Figure 20

The safety function SS1 is requested as follows:

- by the user via any combination of input signals LIN_D... on the signal VIN_SS1_RSF.
- as an error reaction, controlled via the error management system, signal ERR_SS1_RSF.

The request for the safety function SS1 is cancelled as follows:

- by the user via a combination of different inputs on the signal VIN_SS1_CSF.
- by setting the parameter "Automatic restart allowed" (P0C.08), an automatic restart is performed when the request is removed.

Each request of the safety function has priority over termination of the request.

This means: As long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

The safety function directly activates the following safety functions:

- STO via the signal SS1_STO_SFR.
- SBC via the signal SS1_SBC_SFR.

When the request for the SS1 function is terminated, the safety functions which follow directly are also terminated automatically.

In addition, the SS1 function also supplies some control signals for activation of the basic unit:

- limits for speed in the basic unit, SPEED_LIMIT.
- a control signal to trigger the quick stop ramp in the basic unit (not shown in the block diagram).

In addition, the SS1 function generates the status signals:

- VOUT_SS1_SFR, safety function SS1 requested.
- VOUT_SS1_SSR, safe state SS1 reached.

SS1 output signals	**Idle state**	**Safety function requested/achieved**
VOUT_SS1_SFR	0	1
VOUT_SS1_SSR	0	1 (delayed via P0C.01 + P0C.0C + P0C.0B)

Table 40: SS1 output signals

2.5.5.3 Error detection

The safety function at regular intervals compares the current speed (ACTUAL_SPEED) with the calculated speed ramp. If the current speed is outside the permitted speed range for a parameterisable time "Allowable time for limit violation" (P0C.02), then the error [54-4] SS1_ERR is triggered.

The status "Safety condition violated" is not taken back by SS1, if the drive is back in the permitted range after a temporary violation.

If the safety condition is violated, EN 61800-5-2 requires "STO" as an error response. However, in some applications, other error responses may be preferable, e. g. "STO + SBC" ➔ Section 2.8.2.

2.5.5.4 Process

The sequence of the SS1 safety function is shown in the following diagram:

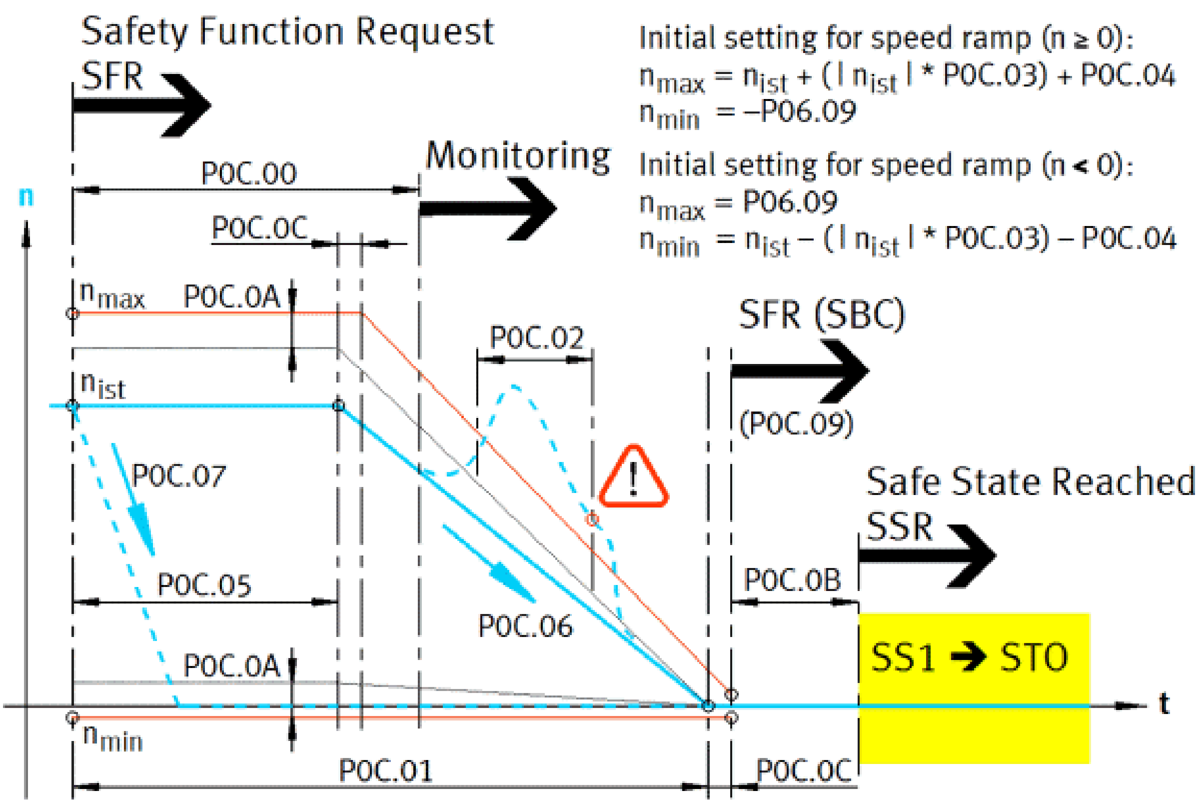


Figure 21: SS1 flow diagram

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
SFR (SBC)	SBC request
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed
n_{max}, n_{min}	Maximum and minimum values for the speed ramp

Table 41: Legend for Figure 21

The flow diagram and the following description apply for a positive speed n_{act}. This applies in a corresponding manner for a negative speed, in which case n_{act} is delayed to zero by a negative speed.

After the request from SS1, the safety module starts a slowdown ramp to monitor the braking operation:

- a time delay is defined using "Time delay until monitoring starts" (P0C.00). Only after this time is compliance with the current speed limit values monitored.
- The length of the slowdown ramp is specified using "Time for slowdown ramp" (P0C.01).
- If "Automatic activation SBC" (P0C.09) was activated, then the safety function SBC is triggered after the "Time for slowdown ramp" (P0C.01) has elapsed, otherwise STO is triggered.
- Only on triggering of SBC (P0C.09 = 1):
  The mechanical delay time of the clamping unit or holding brake can be taken into account using "Delay after expiry of P0C.01 until STO is triggered" (P0C.0B). After the time P0C.01 + P0C.0B expires, STO is triggered and the message VOUT_SS1_SSR is set.
  The time P0C.0b must always elapse, even if P0C.01 = 0.
- The starting value of the monitoring slowdown ramp, n_{max}, is calculated according to the equation in the diagram and can be parameterised via "Slowdown ramp - Starting value factor" (P0C.03) and "Slowdown ramp - Starting value offset" (P0C.04). The ramp ends at speed = 0 (tolerance is specified by the limit value "Speed threshold value for standstill detection" (P06.09)).
- A time delay for the start of the slowdown ramp can be parameterised using "Slowdown ramp - time delay to start" (P0C.05).

i

If the braking operation at SS1 is not to be controlled by the safety module but by the functional controller, then P0C.05 can be used to parameterise a delay to the ramp, in order to compensate for the reaction time of the controller.

Active limiting of the speed in the basic unit is switched on using the parameter "Actively limit speed in the basic unit" (P0C.06):

- Current speed values are transmitted at regular intervals to the basic unit. The speed limits must have a safety distance to the monitoring limits, which is set using the parameter "Speed offset for limiting in the basic unit" (P0C.0A).
- At the end of the monitoring slowdown ramp, the speed limit = 0.
- The basic unit actively limits the speed setpoint and, depending on the parameterisation, also the travel speed of running positioning operations.

The quick stop is activated in the basic unit using the "Activate quick stop ramp in the basic unit" parameter (P0C.07):

- When SS1 is requested, the quick stop ramp in the basic unit is activated automatically and the drive brakes to zero using the quick stop ramp.

→ **Note**

To avoid a violation of the safety condition when braking via the quick stop ramp of the basic unit, please ensure that the ramp time parameterised via "Time for slowdown ramp" (P0C.01) is greater than the braking time of the basic unit from maximum speed at the quick stop ramp.

The SafetyTool will indicate a possible conflict during parameterisation.

After termination of the request of the SS1 function, the internal control signals for the quick stop and the speed limiting in the basic unit are reset.

2.5.5.5 Notes on parameterisation mode a), b) and c) in accordance with EN 61800-5-2

Mode	Parameterisation
Mode a)	Set "Actively limit speed in basic unit" (P0C.06). The safety module controls the slowdown ramp in the basic unit using the parameters set in the safety module for the ramp.
Mode b)	Set "Activate quick stop ramp in the basic unit" (P0C.07). The safety module causes the basic unit to brake with the quick stop ramp and also simultaneously monitors the slowdown ramp set in the safety module.
Mode c)	Do not parameterise slowdown ramp: The functional controller must brake the axle for which the signal VOUT_SS1_SFR or the common message VOUT_SFR must be indicated to the functional controller, Section 8.1.5. Using "Time delay until monitoring starts" (P0C.00), set the desired time until the axle idles and SS1 monitoring should intervene, and always ensure that this is at least 4 ms. No slowdown ramp is monitored prior to this. Set "Time for slowdown ramp" (P0C.01), "Rotational speed ramp - time delay monitoring" (P0C.0C) and "Time delay after reaching n = 0 until STO is triggered" (PC.0B) to the minimum value (2 ms each).

Table 42: Parameterisation mode a), b) and c) in accordance with EN 61800-5-2

After the request of the safety function SS1, the following times elapse until the safety function is activated and errors are detected:

Time delays from VIN_SS1_RSF	Minimum	Maximum	Typical
VOUT_SS1_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SS1_SSR	2.0 ms + P0C.01 + P0C.0B + P0C.0C	2.1 ms + P0C.01 + P0C.0B + P0C.0C	2.0 ms + P0C.01 + P0C.0B + P0C.0C
Detection of a violation of the safety condition after VOUT_SBC_SFR	2.0 ms + P0C.00 + P0C.02	2.1 ms + P0C.00 + P0C.02	2.0 ms + P0C.00 + P0C.02

Table 43: SS1 time delays

Parameterise P0C.00 so that it is smaller than the slowdown ramp to STO (P0C.01 + P0C.0B + P0C.0C).
If the "Time delay until monitoring starts" (P0C.00) is parameterised greater than the total slowdown ramp to STO (P0C.01 + P0C.0B + P0C.0C), then STO and thus the signal SS1_SSR are also only reached after 2.1 ms + P0C.00.

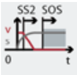
2.5.5.6 Parameters for SS1

SS1: Safe Stop 1		
No.	**Name**	**Description**
P0C.00	Time delay until monitoring starts	Time from the safety function request during which no rotational speed monitoring takes place
P0C.01	Time for slowdown ramp	Time from the safety function request, after which the rotational speed ramps are stopped and the safe status is reached.
P0C.02	Allowable time for limit value overrun	Time interval, during which the actual rotational speed value may be outside the limits, before the "Safety condition violated" status is reached.
P0C.06	Actively limit speed in basic unit	If set: Control the rotational speed of the basic unit
P0C.07	Activate quick stop ramp in the basic unit	If set: When the safety function is requested, the quick stop command (pilot line) is applied to the basic unit
P0C.08	Automatic restart permitted	If set: Cancellation of the request (restart) if an inactive request arrives
P0C.09	Automatic activation of SBC	If set: Safe brake control is activated when idle is reached or after the time delay has expired.
Expert parameter		
P0C.0C	Speed ramp - Monitoring time delay	Time delay between the rotational speed ramp, written to the basic unit, and the start of monitoring by the safety module.
P0C.0B	Delay after expiry of P0C.01 until STO is triggered	Time after which STO is triggered at the end of the braking operation.
P0C.05	Slowdown ramp - time delay to start	Time delay after which the ramps start.
P0C.03	Slowdown ramp - Starting value factor	Factor for calculating the starting value of the rotational speed ramps.
P0C.04	Slowdown ramp - Starting value offset	Offset for calculating the starting value of the rotational speed ramps.
P0C.0A	Speed offset for the limitation in the basic unit	Offset for rotational speed limits to control the basic device.

Table 44: SS1: Safe Stop 1

2.5.6 SS2 – Safe Stop 2

2.5.6.1 Application



The function described here implements the safety function SS2 according to EN 61800-5-2.

Use the "Safe Stop 2" function (SS2) if you brake the motor in your application and must then ensure that the motor will not deviate from the holding position by more than a specified amount (cf. stop category 2 in EN 60204-1).

The three characteristics described in the standard are supported:

a) Triggering and controlling the rate of motor deceleration within specified limits and triggering the SOS function when the motor speed falls below a specified limit value.
➔ The drive is taken through a slowdown ramp until it is detected as idling (P06.09), after which a safe operating stop is executed.

b) Triggering and monitoring the motor deceleration variable within specified limits and triggering the SOS function when the motor speed falls below a specified limit value.
➔ The safety module activates a fast stop in the basic device, the slowdown ramp is monitored, after which a safe operating stop is executed.

c) Triggering the motor deceleration and after an application-specific time delay, triggering the SOS function.
➔ The safety module delivers a status signal, the basic device must be braked by the functional controller. After a waiting time, the safety function SOS is activated.

The SS2 function can also be used as an error response (when other requested safety functions are violated). For this, it must be activated and parameterised.

2.5.6.2 Function

When requesting the SS2 safety function, this checks that the drive is braked to idle within a defined time using a defined slowdown ramp. After the defined time has elapsed, SOS is triggered and thus a safe operating stop executed.

The logic to request the SS2 safety function is shown in the following block diagram:

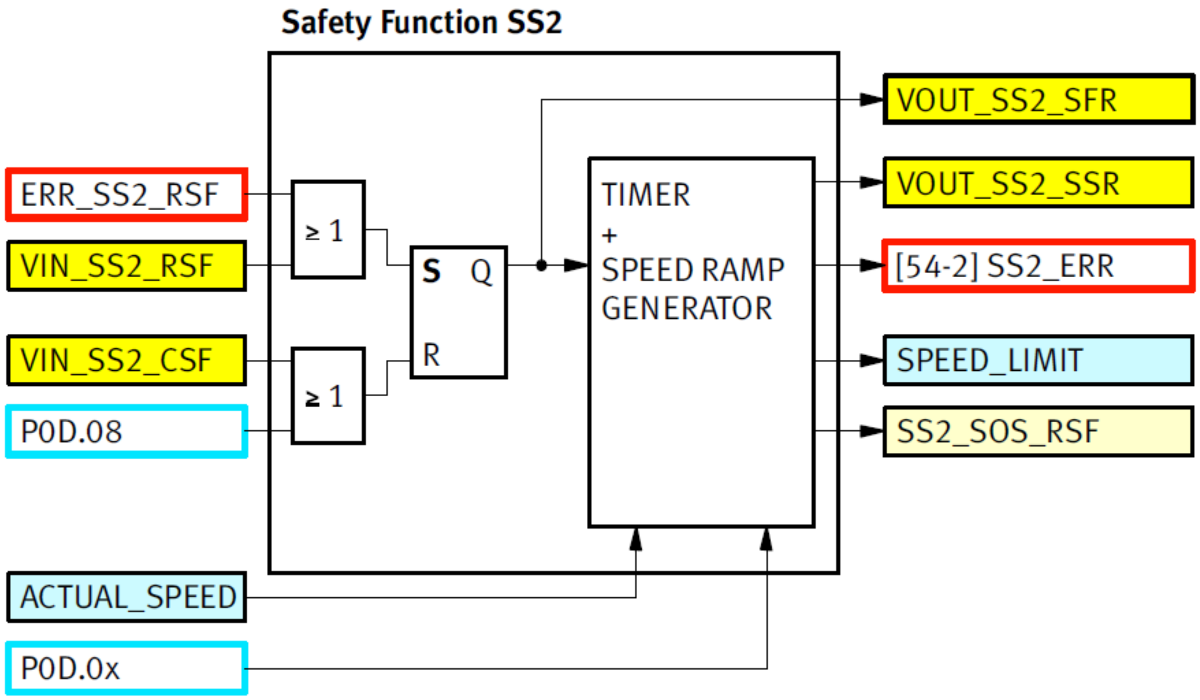


Figure 22: Block diagram SS2

Term/abbreviation	Explanation
Safety Function SS2	Safety function SS2
ERR_SS2_RSF	Internal signal: Request SS2 through error response
VIN_SS2_RSF	Virtual input: Request SS2
VIN_SS2_CSF	Virtual input: End SS2 request
ACTUAL SPEED	Internal signal: current speed
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_SS2_SFR	Virtual output: SS2 requested
VOUT_SS2_SSR	Virtual output: Safe state SS2 reached
[54-2] SS2_ERR	Internal error signal: Error 54-2
SPEED_LIMIT	Internal signal: Speed limit in basic unit
SS2_SOS_RSF	Internal signal: Request SOS by SS2

Table 45: Legend for Figure 22

The safety function SS2 is requested as follows:

- by the user via any combination of input signals LIN_D... on the signal VIN_SS2_RSF.
- as an error reaction, controlled via the error management system, signal ERR_SS2_RSF.

The request for the safety function SS2 is cancelled as follows:

- by the user via a combination of different inputs, run on the signal VIN_SS2_CSF.
- by setting the parameter "Automatic restart allowed" (P0D.08), an automatic restart is performed when the request is cancelled.

Each request of the safety function has priority over termination of the request.

This means: As long as one of the xxx_RSF (Request Safety Function) signals is pending, the safety function cannot be terminated by an xxx_CSF (Clear Safety Function) signal.

The safety function directly activates the following safety functions:

- SOS via the signal SS2_SOS_SFR.

When the request of the SS2 function is terminated, the safety functions which follow directly are also terminated automatically.

In addition, the SS2 function also provides some control signals for activation of the basic unit:

- limits for speed in the basic unit, SPEED_LIMIT.
- a control signal to trigger the quick stop ramp in the basic unit (not shown in the block diagram).

In addition, the SS2 function generates the status messages:

- VOUT_SS2_SFR, safety function SS2 requested.
- VOUT_SS2_SSR, safe state SS2 reached.

SS2 output signals	**Idle state**	**Safety function requested/achieved**
VOUT_SS2_SFR	0	1
VOUT_SS2_SSR	0	1 (delayed via P0D.01 + P0D.0A)

Table 46: SS2 output signals

2.5.6.3 Error detection

The safety function at regular intervals compares the current speed (ACTUAL_SPEED) with the calculated speed ramp. If the current speed is outside the permitted speed range for a parameterisable time "Allowable time for limit violation" (P0D.02), then the error [54-2] SS2_ERR is triggered.

The status "Safety condition violated" is not retracted by SS2, if the drive is back in the permitted range after a temporary violation.

As soon as the drive has been braked to idle, the safety function SOS is requested, which has its own error detection (position monitoring).

If the safety condition is violated, EN 61800-5-2 requires "STO" as an error response. However, in some applications, other error responses may be preferable, e. g. "STO + SBC" ➔ Section 2.8.2.

2.5.6.4 Process

The sequence of the SS2 safety function is shown in the following diagram:

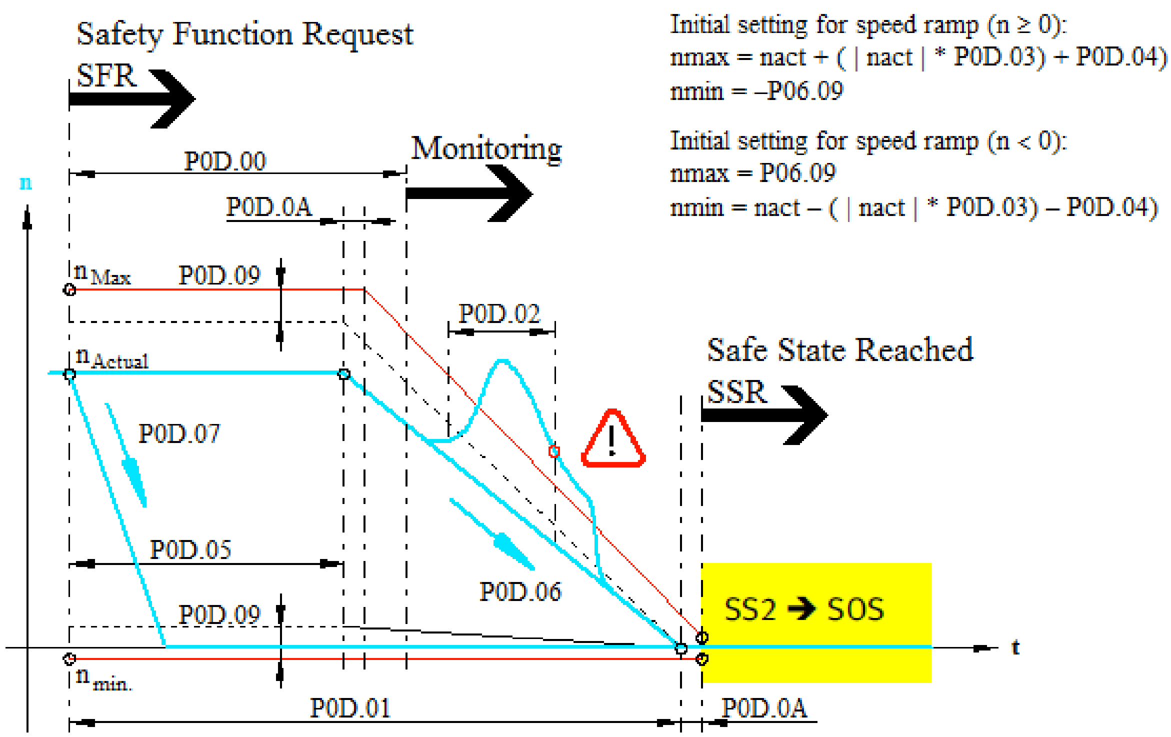


Figure 23: SS2 flow diagram

Term/abbreviation	**Explanation**
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed

Table 47: Legend for Figure 23

The flow diagram and the following description apply for a positive speed n_{act}. For a negative speed, the chart mirrored on the time axle applies.

After the request from SS2, the safety module starts a slowdown ramp:

– A time delay is defined using "Time delay until monitoring starts" (P0D.00). Only after this time is compliance with the current speed limit values monitored.
– The length of the slowdown ramp is specified using "Time for slowdown ramp" (P0D.01).
– The starting value of the monitoring slowdown ramp, n_{max}, is calculated according to the equation in the diagram and can be parameterised via "Slowdown ramp - Starting value factor" (P0D.03) and "Slowdown ramp - Starting value offset" (P0D.04). The ramp ends at speed = 0 (tolerance is specified by the limit value for idle detection "Speed threshold value for idle detection" (P06.09)).
– A time delay for the start of the slowdown ramp can be parameterised using "Slowdown ramp - time delay to start" (P0D.05).

If braking at SS2 is not to be controlled by the safety module but by the functional controller, then P0D.05 can be used to parameterise a delay to the ramp, in order to compensate for the reaction time of the controller.

Active limiting of the speed in the basic unit is switched on using the parameter "Actively limit speed in the basic unit" (P0D.06):

– Current speed values are transmitted at regular intervals to the basic unit. The speed limits must have a safety distance to the monitoring limits, which is set using the parameter "Speed offset for limiting in the basic unit" (P0D.09).
– At the end of the monitoring slowdown ramp, the speed limit = 0.
– The basic unit actively limits the speed setpoint and, depending on the parameterisation, also the travel speed of running positioning operations.

The quick stop is activated in the basic unit using the "Activate quick stop ramp in the basic unit" parameter (P0D.07):

– When SS2 is requested, the quick stop ramp in the basic unit is activated automatically and the drive brakes to zero using the quick stop ramp.

Note

To avoid a violation of the safety condition when braking via the quick stop ramp of the basic unit, please ensure that the ramp time parameterised via P0D.01 is greater than the braking time of the basic unit from maximum speed at the quick stop ramp.

The SafetyTool will indicate a possible conflict during parameterisation.

After termination of the request of the SS2 function, the internal control signals for the quick stop and speed limiting in the basic unit are reset.

2.5.6.5 Notes on parameterisation mode a), b) and c) in accordance with EN 61800-5-2

Mode	Parameterisation
Mode a)	Set "Actively limit speed in basic unit" (P0D.06). The safety module controls the slowdown ramp in the basic unit using the parameters set in the safety module for the ramp.
Mode b)	Set "Activate quick stop ramp in the basic unit" (P0D.07). The safety module causes the basic unit to brake with the quick stop ramp and also simultaneously monitors the slowdown ramp set in the safety module.
Mode c)	Do not parameterise slowdown ramp: The functional controller must brake the axle, for which the signal VOUT_SS2_SFR or the common message VOUT_SFR must be indicated to the function controller, Section 8.1.5. Using "Time delay until monitoring starts" (P0D.00), set the desired time until the axle is idling and SS2 monitoring should intervene, and always ensure that this is at least 4 ms. No slowdown ramp is monitored prior to this. Set "Time for slowdown ramp" (P0D.01), "Rotational speed ramp - time delay monitoring" (P0D.0A) to the minimum value (2 ms each).

Table 48: Parameterisation mode a), b) and c) in accordance with EN 61800-5-2

After the safety function SS2 is requested, the following times elapse until the safety function is activated and errors are detected:

Time delays from VIN_SS2_RSF	Minimum	Maximum	Typical
VOUT_SS2_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SS2_SSR	2.0 ms + P0D.01 + P0D.0A	2.1 ms + P0D.01 + P0D.0A	2.0 ms + P0D.01 + P0D.0A
Detection of a violation of the safety condition after VOUT_SS2_SFR	2.0 ms + P0D.00 + P0D.02	2.0 ms + P0D.00 + P0D.02	2.0 ms + P0D.00 + P0D.02

Table 49: SS2 time delays

Parameterise P0D.00 so that it is smaller than the slowdown ramp to SOS (P0D.01 + P0D.0A).

If the "Time delay until monitoring starts" (P0D.00) is parameterised greater than the total slowdown ramp to SOS (P0D.01 + P0D.0A), then SOS and thus the signal SS2_SSR are accordingly only reached after 2.1 ms + P0D.00.

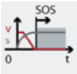
2.5.6.6 Parameters for SS2

SS2: Safe Stop 2		
No.	**Name**	**Description**
P0D.00	Time delay until monitoring starts	Time from the safety function request during which no rotational speed monitoring takes place The monitoring limits of the SOS function are used for SS2.
P0D.01	Time for slowdown ramp	Time from the safety function request, after which the rotational speed ramps are stopped and the safe status is reached.
P0D.02	Allowable time for limit value overrun	Time interval, during which the actual rotational speed value may be outside the limits, before the "Safety condition violated" status is reached.
P0D.06	Actively limit speed in basic unit	If set: Control the rotational speed of the basic unit
P0D.07	Activate quick stop ramp in the basic unit	If set: When the safety function is requested, the quick stop command (pilot line) is applied to the basic unit
P0D.08	Automatic restart permitted	If set: Cancellation of the request (restart) if an inactive request arrives
Expert parameter		
P0D.0A	Speed ramp - Monitoring time delay	Time delay between the start of the rotational speed ramp, written to the basic unit, and the start of monitoring by the safety module.
P0D.05	Slowdown ramp - time delay to start	Time delay after which the ramps start.
P0D.03	Slowdown ramp - Starting value factor	Factor for calculating the starting value of the rotational speed ramps
P0D.04	Slowdown ramp - Starting value offset	Offset for calculating the starting value of the rotational speed ramps
P0D.09	Speed offset for the limitation in the basic unit	Offset for rotational speed limits to control the basic device.

Table 50: SS2: Safe Stop 2

2.5.7 SOS – Safe Operating Stop

2.5.7.1 Application



The function described here implements the safety function SOS according to EN 61800-5-2.

Use the "Safe Operating Stop" (SOS) function if you must ensure in your application that the motor position or the axle position is kept active and is monitored safely.

The SOS function is also triggered by the SS2 function and can also be used as an error response (when other requested safety functions are violated). In this case, it is activated via the factory setting and cannot then be deselected.

2.5.7.2 Function

When requesting the SOS safety function, after a defined time this monitors that the drive is regulated within a specified position tolerance. If necessary, a quick stop can be requested in the basic unit in advance, using which the drive is braked to idle. Even if the SOS safety function has been requested, energy will continue to be supplied to the motor so that it can withstand an attack by exterior forces. In the basic unit, the speed is regulated to zero.

Note

As the signals of the position encoder can be static when idling, e.g. in the case of SIN/COS tracking signals, the SOS function cannot be continuously requested without limits. An axle movement is required in the meantime.
If SOS is requested for > 24 hours, the error 54-7 is triggered.

This means that the maximum idle time in the SOS function is limited to 24 hrs.

The logic to request the SOS safety function is shown in the following block diagram:

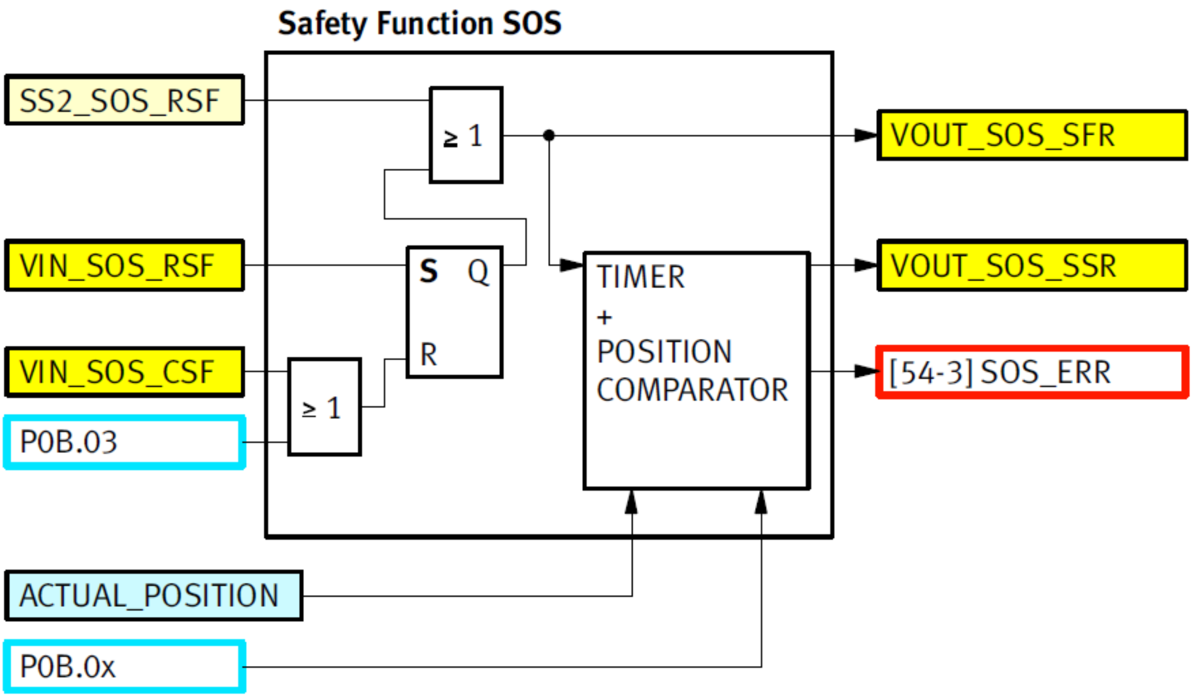


Figure 24: Block diagram SOS

Term/abbreviation	**Explanation**
Safety Function SOS	Safety function SOS
VIN_SOS_RSF	Virtual input: Request SOS
VIN_SOS_CSF	Virtual input: Terminate SOS request
ACTUAL POSITION	Internal signal: Current position
TIMER + POSITION COMPARATOR	Timer and position comparator
VOUT_SOS_SFR	Virtual output: SOS requested
VOUT_SOS_SSR	Virtual output: Safe state SOS reached
[54-3] SOS_ERR	Internal error signal: Error 54-3

Table 51: Legend for Figure 24

The safety function SOS is requested as follows:

– by the user via any combination of input signals LIN_D... on the signal VIN_SOS_RSF.
– via the safety function SS2, signal SS2_SOS_RSF.

The request of the safety function SOS is cancelled as follows:

– by the user via a combination of different inputs, run on the signal VIN_SOS_CSF.
– by setting the parameter "Automatic restart allowed" (P0D.03), an automatic restart is performed when the request is removed.

Each request of the safety function has priority over termination of the request.

This means: This means: As long as one of the xxx_RSF signals is pending, the safety function cannot be terminated by an xxx_CSF signal.

2.5.7.3 Error detection

The safety condition is considered as violated when the drive moves by more than the "Position monitoring tolerance window" distance (±P0B.01) after P0B.00 has elapsed, or if an axle movement is detected by the speed measuring device.

➔ **Note**

In applications with only one shaft encoder / position encoder with analogue signal interface (Resolver, SIN-/COS, HIPERFACE, etc.), the restrictions regarding diagnostic cover and possible accuracy of rest and speed monitoring must be taken into account ➔ Appendix 7.3.5 and 7.3.6.

The safety function is also considered as having been violated when the actual position value assumes the status "invalid" whilst the safety function is requested (e.g. when a position encoder fails).
If the safety condition is violated, an error is triggered. The "SOS" function is implemented in accordance with EN 61800-5-2 when the error reaction to "STO" is parameterised.
The safety function can be executed independently of whether the axle is referenced or not.

2.5.7.4 Process

The sequence of the SOS safety function is shown in the following diagram:

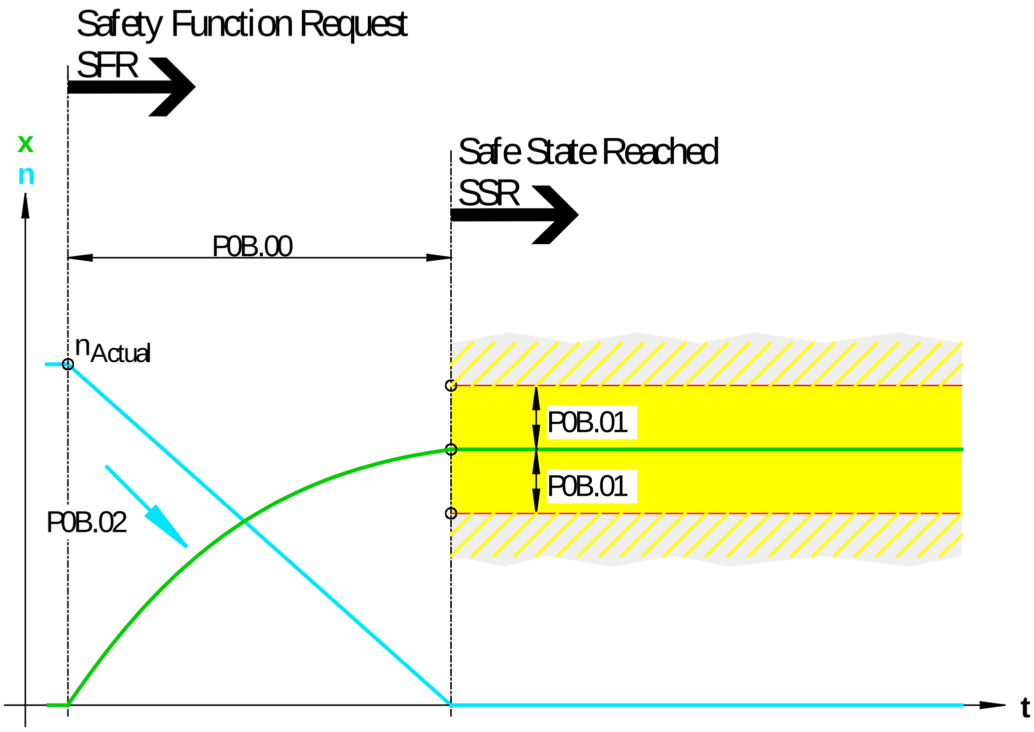


Figure 25: SOS flow diagram

Term/abbreviation	**Explanation**
Safety Function Request SFR	Safety function request
Safe State Reached SSR	Safe state reached
n_{act}	Actual speed

Table 52: Legend for Figure 25

If parameterised appropriately with "Activate quick stop ramp in basic unit" (P0B.02), the servo drive is instructed via the "Quick stop" cable to stop the drive.

After the time "Time delay until monitoring starts" (P0B.00) has elapsed, the drive is monitored to check it is idling. At this time, the output "Safe state reached" becomes active if the safety condition is not violated.

Whilst the time P0B.00 elapses, position monitoring is not yet active. After P0B.00 has elapsed, the current position is saved and is used as the setpoint for the position to be monitored. The position is monitored by comparing the current position value at regular intervals with the saved value.

After the request of the safety function SOS, the following times elapse until the safety function is activated and errors are detected:

Time delays from VIN_SOS_RSF	Minimum	Maximum	Typical
VOUT_SOS_SFR	2.0 ms	2.1 ms	2.0 ms
VOUT_SOS_SSR	2.0 ms + P0B.00	2.1 ms + P0B.00	2.0 ms + P0B.00
Detection of a violation of the safety condition[1)] after P0B.00 within	0.0 ms	2.1 ms	2.0 ms
1) The safety condition is considered as violated when... a) the monitoring window is exited +/- P0B.01 or b) an axle movement is detected via idling detection within the position window			

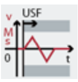
Table 53: SOS time delays

2.5.7.5 Parameters for SOS

SOS: Safe Operating Stop		
No.	**Name**	**Description**
P0B.00	Time delay until monitoring starts	Time delay after request of the function up to the start of monitoring
P0B.01	Tolerance window, position monitoring	Limit value for movement after idle status is reached
P0B.03	Automatic restart permitted	If set: Cancellation of the request (restart) if an inactive request arrives
Expert parameter		
P0B.02	Activate quick stop ramp in the basic unit	Send brake command to the basic unit (Signal SS1) Yes / No

Table 54: SOS: Safe Operating Stop

2.5.8 USF – Universal safety functions



The "Universal Safety Functions" (USF) serve to monitor the status variables (path, speed and force / torque) of the motor / the axle.

Currently available:

– The "Safe Speed Function" (SSF)

The USF function also summarises the product terms for "Request", "Terminate request", the logical and virtual inputs and outputs (LIN_USFx..., VOUT_USFx...), as well as the error management parameters.

4 USF functions (USF0 … USF3) are available.

2.5.9 SSF – Safe speed functions

2.5.9.1 Application

The "Safe Speed Function" (SSF) can be characterised via the parameterisation as one of the following safety functions:

– SLS – Safely Limited Speed ➔ Section 2.5.10,
– SSR – Safe Speed Range ➔ Section 2.5.11,
– SSM – Safe Speed Monitoring ➔ Section 2.5.12.

The specific function is then specified by a specific parameterisation of the SSF, as can be seen in the following sections.

Each of the 4 USF functions contains an SSF function for this (SSF0 … SSF3). This means that up to 4 of the safety functions can be implemented and executed in parallel.

2.5.9.2 Function

The SSFs in the SLS / SSR / SSM versions monitor the speed of the drive using minimum and maximum limits. If the speed of the motor exceeds the limit value, then the error "Safety condition violated" is triggered.

The speed limits for monitoring are not specified statically. The SSF can calculate dynamic speed ramps and also monitor that the drive is is performing in the desired safe speed range from any speed.

In addition, speed limiting of the servo drive can be controlled in such a way that the safety condition is not violated.

The logic to request the SSF0 safety function is shown in the following block diagram:

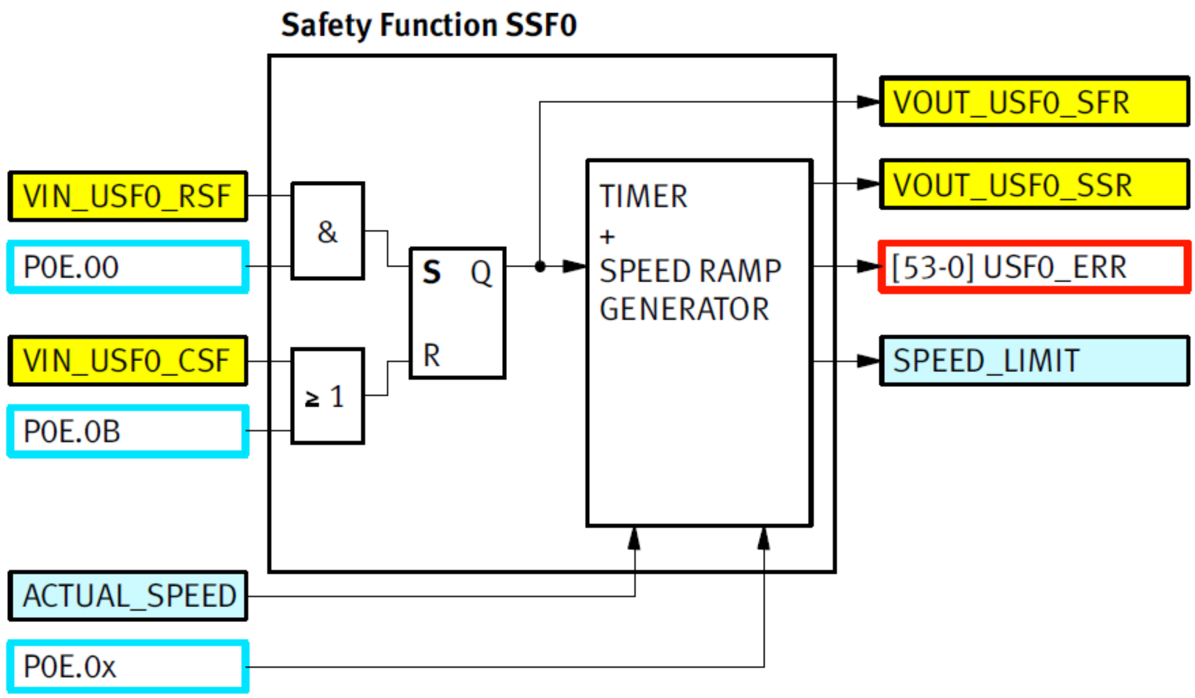


Figure 26: Block diagram SSF0

Term/abbreviation	Explanation
Safety Function SFF0	Safety function SFF0
VIN_USF0_RSF	Virtual input: Request USF0
VIN_USF0_CSF	Virtual input: End USF0 request
ACTUAL SPEED	Internal signal: Current speed
TIMER + SPEED RAMP GENERATOR	Timer and calculation of speed ramps
VOUT_USF0_SFR	Virtual output: USF0 requested
VOUT_USF0_SSR	Virtual output: Safe state USF0 reached
[53-0] USF0_ERR	Internal error signal: Error 53-0
SPEED_LIMIT	Internal signal: Speed limit in basic unit

Table 55: Legend for Figure 26

The safety function SSF0 is requested as follows:

- by the user via any combination of input signals LIN_D... on the signal VIN_USF0_RSF, if the SSF function was activated using the parameter "Activate SSF" (P0E.00/...).

The request of the safety function SSF0 is cancelled as follows:

- by the user via a combination of different inputs, run on the signal VIN_USF0_CSF.
- by setting the parameter "Automatic restart allowed" (P0E.0B/...), an automatic restart is performed when the request is cancelled.

The SSF0 function provides the following control signals for activation of the basic unit:

- Time-dependent limits for speed in the basic unit, SPEED_LIMIT.

In addition, the SSF0 function generates the status messages:

- VOUT_USF0_SFR, safety function USF0 requested.
- VOUT_USF0_SSR, safe state USF0 reached.

USF0 output signals	Idle state	Safety function requested/achieved
VOUT_USF0_SFR	0	1
VOUT_USF0_SSR	0	1 (delayed, see runtime performance)

Table 56: SSF0 status signals

Each request of the safety function has priority over termination of the request. This means: This means: As long as one of the xxx_RSF signals is pending, the safety function cannot be terminated by an xxx_CSF signal.

2.5.9.3 Error detection

The safety condition is considered violated when the rotational speed is continuously outside the permitted range for the time "Allowable time for limit value violation" (P0E.03/...). The violation is considered as cancelled when the rotational speed is continuously within the permitted range for the time "Allowable time for limit value violation".

➔ **Note**

In applications with only one shaft encoder / position encoder with analogue signal interface (Resolver, SIN-/COS, HIPERFACE, etc.), the restrictions regarding diagnostic cover and possible accuracy of rest and speed monitoring must be taken into account ➔ Appendix 7.3.5 and 7.3.6.

If the safety condition is violated, an error is triggered, which results in an error response which can be parameterised.

The error "Safety condition violated" is also generated when a position encoder fails and thus no reliable speed information is available.

2.5.9.4 Process

The sequence of the SSF0 safety function is shown in the following diagram:

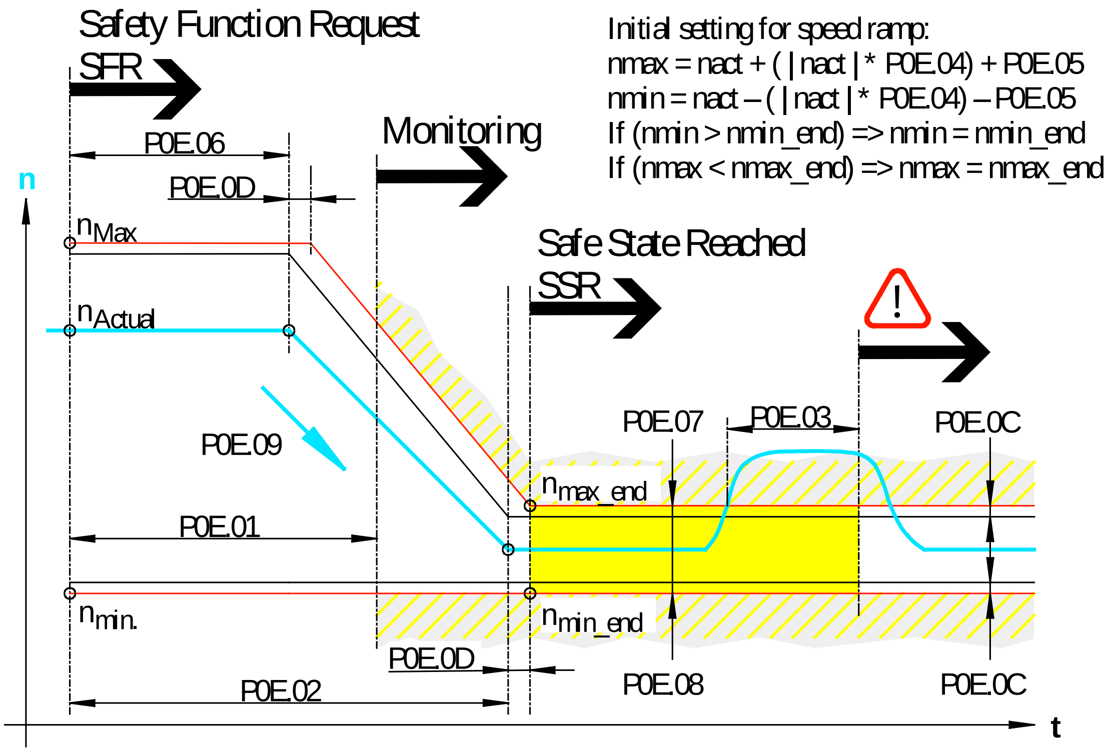


Figure 27: Flow diagram SSF0

Term/abbreviation	Explanation
Safety Function Request SFR	Safety function request
Monitoring	Monitoring
Safe State Reached SSR	Safe state reached
Initial setting for speed ramp	Initial values for the speed ramp
n_{act}	Actual speed

Table 57: Legend for Figure 27

The safety function SSF0 monitors the speed of the drive in the stationary state. The permitted speed corridor is defined using the parameters "Safe speed - upper limit" (P0E.07/..., n_{max_end}) and "Safe speed - lower limit" (P0E.08/..., n_{min_end}) (➔ Figure 27, right-hand section).

When the actual speed leaves the speed corridor, the error "Safety condition violated" is generated after an allowable time "Allowable time for limit violation" (P0E.03/...).

The SSF safety functions are characterised as SLS, SSR or SSM mostly depending on how the final speed is parameterised:

- "Safely Limited Speed" (SLS) ➔ Section 2.5.10,
- "Safe Speed Range" (SSR) ➔ Section 2.5.11,
- "Safe Speed Monitoring" (SSM) ➔ Section 2.5.12.

When the safety function SSF0 is requested (VOUT_USF0_SFR), a calculation for a speed ramp is carried out, so that the drive will perform within the approved speed corridor, starting at the current speed:

- Calculation of the initial values n_{max} and n_{min} is based on the current speed n_{act} as the starting value. A start window around the current speed is first calculated based on a gain parameter "Slowdown ramp - Starting value factor" (P0E.04/...) and an offset parameter "Slowdown value - starting value offset" (P0E.05/...).
- 1876The position of the start window is set relative to the desired speed corridor and the initial values are adapted as necessary to produce a trapezoidal, tapering speed corridor (see Figure 27).
- The start time of the ramp can be specified using "Slowdown ramp - Time delay to start" (P0E.06/..., minimum value: 6 ms) and the end time of the ramp via "Time for slowdown ramp" (P0E.02). After P0E.02 has elapsed, the stationary speed corridor has been reached and SSF0 issues the signal VOUT_USF0_SSR (when the actual speed is in the approved range!).
- Using "Time delay until monitoring starts" (P0E.01/...), it is possible to specify from when the SSF0 function monitors the speed.

A delay of the ramp via "Slowdown ramp - Time delay to start" (P0E.06/...) is always preferable when the axle is braked by the functional controller and is transferred to the monitored speed corridor. P0E.06 can be used to compensate the reaction time of the functional controller.

The safety module can actively manipulate the controller of the basic unit, thus actively limiting the speed of the axle. The limit values are transferred at regular intervals to the basic unit:

- This function is activated by setting the parameter "Actively limit speed in basic unit" (P0E.09/...).
- There are additional parameters to ensure that the monitored limit values are complied with safely during active limiting of the speed in the basic unit:
  - Using the minimum value of "Slowdown ramp - Time delay to start" (P0E.06, 6 ms) compensates for the time it takes to transfer the new limit values to the basic unit, before the control is manipulated in the basic unit.
  - "Rotational speed ramp - monitoring time delay" (P0E.0D/...) can be used in order to add a speed limit delay in the safety module of several additional milliseconds, to monitor for a targeted delay of the speed limit in the safety module for monitoring. This gives the basic unit additional time, for example, if a jolt-limited travel profile was selected in the basic unit and braking may only take place with jolt limiting.
  - Finally, a speed offset can be parameterised using "Speed limit offset" (P0E.0C/...). The speed limits for the basic unit are then around P0E.0C/..., offset within the speed corridor for

monitoring, meaning that slight deviations of the actual speed do not lead to a response from the monitoring system.

– If the upper and lower speed limits for the basic unit overlap, due to a very narrow corridor and the offset P0E.0C/..., then both limits are set to the average value between the monitored minimum and maximum rotational speed.

The description can be applied in a similar manner to the parameters for the functions SSF1, SSF2 and SSF3.

Thus SSF0 permits adaptation to various applications.

In the SafetyTool, the SSF0 parameters are divided up into:

– standard parameters – these are the simple parameters which are to be adapted individually to the application for each speed monitoring operation.
– expert parameters – these are parameters for optimisation of the function in conjunction with the control functions in the basic unit. These parameters are set appropriately at the factory.

In most applications, you will only need the standard parameters!

After the request of the safety function SSF0, the following times elapse until the safety function is activated and errors are detected:

Time delays from VIN_USF0_RSF	**Min.**	**Max.**	**Typical**
VOUT_USF0_SFR signal	2.0 ms	2.1 ms	2.0 ms
VOUT_USF0_SSR signal	8.0 ms + (P0E.02 + P0E.0D)	8.1 ms + (P0E.02 + P0E.0D)	8.0 ms + (P0E.02 + P0E.0D)
Start of monitoring of the safety condition according to VOUT_USF0_SFR	2.0 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))	2.1 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))	2.0 ms + MAX (P0E.01 OR (P0E.06 + P0E.0D))
Detection of a violation of the safety condition after P0E.01 or (P0E.06 + P0E.0D) within	P0E.03	P0E.03	P0E.03

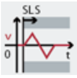
Table 58: SSF0 delay times

2.5.9.5 Parameters for SSF

SSF: Safe speed					
Parameter no. for ...				**Name**	**Description**
SSF0	**SSF1**	**SSF2**	**SSF3**		
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	If 1: Request of the USF triggers request of the SSF
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until monitoring starts	Time from the safety function request during which no rotational speed monitoring takes place
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed - upper limit	Final value of the upper ramp at n_{max_end}
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed - lower limit	Final value of the lower ramp at n_{min_end}
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for slowdown ramp	Time from the safety function request, after which the ramps are stopped and the safe state is reached.
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Time interval, during which the actual speed value may be outside the limits, before the "Safety condition violated" status is reached.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	If set: The speed is transferred to the basic unit and is limited in the basic unit.
P0E.0B	P0E.1F	P0E.33	P0E.47	Automatic restart permitted	If 1: Cancellation of the request (restart) if an inactive request arrives
Expert parameter					
P0E.0D	P0E.21	P0E.35	P0E.49	Speed ramp - Monitoring time delay	The ramp used to monitor the speed in the safety module is also delayed compared to the ramp applied to the basic unit.
P0E.06	P0E.1A	P0E.2E	P0E.42	Slowdown ramp - time delay to start	Time delay, after which the monitoring ramp in the safety module starts.
P0E.04	P0E.18	P0E.2C	P0E.40	Slowdown ramp - Starting value factor	Factor for calculating the starting value of the ramps
P0E.05	P0E.19	P0E.2D	P0E.41	Slowdown ramp - Starting value offset	Offset for calculating the starting value of the ramps
P0E.0C	P0E.20	P0E.34	P0E.48	Speed limit offset	Offset for speed limits for controlling the basic unit.
P0E.0A	P0E.1E	P0E.32	P0E.46	Activate quick stop ramp in the basic unit	If set: When the safety function is requested, the quick stop command (pilot line) is applied to the basic unit

Table 59: SSF: Safe speed

2.5.10 SLS – Safely-Limited Speed



The function described here implements the safety function SLS according to EN 61800-5-2.

Use the "Safely-Limited Speed" (SLS) function when, in your application, you wish to prevent the motor from exceeding a specified speed limit.

The function is indicated by a zero-symmetrical monitoring area for the speed. The limits can be set separately.

The drive can be braked to an approved speed along the slowdown ramp, although the function can be switched off. In the simplest case, monitoring starts after the time "Time delay until monitoring starts" (P0E.01/P0E.15/P0E.29/P0E.3D). The maximum rotational speed is specified using "Safe speed - upper limit" (P0E.07/P0E.1B/P0E.2F/P0E.43).

The following parameterisation means that the Safe Speed Function SSF corresponds to the SLS safety function (with immediate speed monitoring without slowdown ramp):

Parameterise SSF as SLS					
Parameter no. for ...				**Name**	**Setting for SLS safety function**
SSF0	**SSF1**	**SSF2**	**SSF3**		
Standard parameters SSF					
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	= 1, activate
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until monitoring starts	2.0 ms
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed - upper limit	Set positive speed limit for SLS.
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed - lower limit	= -P0E.07/-P0E.1B /-P0E.27 /-P0E.43
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for slowdown ramp	6.2 ms, minimum value
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Default value: 10 ms, can be reduced for rapid error detection.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	Can be set.
SSF expert parameters: No change to factory setting (important!)					
P0E.06	P0E.1A	P0E.2E	P0E.42	Slowdown ramp - time delay to start	= 6 ms (smallest settable value)
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: Safety Condition Violated	Corresponds to the necessary error response of the application.

Table 60: Parameterise SSF as SLS

2.5.11 SSR – Safe Speed Range

The function described here implements the safety function SSR according to EN 61800-5-2.

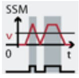
Use the "Safe Speed Range" (SSR) function if you wish to ensure in your application that the motor speed remains within specified limit values.

The following parameterisation means that the Safe Speed Function SSF corresponds to the SSR safety function (with immediate speed monitoring without slowdown ramp):

Parameterise SSF as SSR					
Parameter no. for ...				**Name**	**Setting for SSR safety function**
SSF0	**SSF1**	**SSF2**	**SSF3**		
Standard parameters SSF					
P0E.00	P0E.14	P0E.28	P0E.3C	Activate SSF	= 1, activate
P0E.01	P0E.15	P0E.29	P0E.3D	Time delay until monitoring starts	2.0 ms
P0E.07	P0E.1B	P0E.2F	P0E.43	Safe speed - upper limit	Set upper speed limit for SSR.
P0E.08	P0E.1C	P0E.30	P0E.44	Safe speed - lower limit	Set lower speed limit for SSR.
P0E.02	P0E.16	P0E.2A	P0E.3E	Time for slowdown ramp	6.2 ms, minimum value
P0E.03	P0E.17	P0E.2B	P0E.3F	Allowable time for limit value overrun	Default value: 10 ms, can be reduced for rapid error detection.
P0E.09	P0E.1D	P0E.31	P0E.45	Actively limit speed in basic unit	Can be set.
SSF expert parameters: No change to factory setting (important!)					
P0E.06	P0E.1A	P0E.2E	P0E.42	Slowdown ramp - time delay to start	= 6 ms (smallest settable value)
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: Safety Condition Violated	Corresponds to the necessary error response of the application.

Table 61: Parameterise SSF as SSR

2.5.12 SSM – Safe Speed Monitor



The function described here implements the safety function SSM according to EN 61800-5-2.

Use the "Safe Speed Monitor" (SSM) function if you require a safe output signal in your application to display whether the motor rotational speed is below a specified limit value.

The parameterisation of the SSM corresponds to that for SSR. Only error management must be adapted:

Parameterise SSF as SSM					
Parameter no. for ...				**Name**	**Setting for SSM safety function**
SSF0	**SSF1**	**SSF2**	**SSF3**		
Standard parameters SSF: see SSR, Table 61					
Expert parameters SSF: see SSR, Table 61					
Error management					
P20.00	P20.01	P20.02	P20.03	[53-x] USFx: Safety Condition Violated	Dependent upon application: – none = [0], or – none, only event memory entry = [1] – warning + event memory entry = [2]

Table 62: Parameterise SSF as SSM

2.6 Logic functions

2.6.1 Mode selector switch

2.6.1.1 Use

Use the logic function "Mode selector switch" to switch between various operating modes / monitoring functions of the safety module.

Example:
In the Normal operation switch position, the system travels normally. It stops when there is a change to the system, e.g. via SS1.

In the Setting operation switch position, the SLS safety function is activated. However, a manipulation of the system should not trigger SS1, as setup mode is approved.

The inputs DIN45, DIN46 and DIN47 can be configured as inputs for mode selection. The "Mode selector switch" provides three safe logical control signals, LIN_D45_SAFE, LIN_D46_SAFE and LIN_D47_SAFE, which can be used to switch between various safety functions.

2.6.1.2 Function

The status of the three inputs DIN45, DIN46 and DIN47 is mapped directly to the safe logical signals LIN_D45_SAFE, LIN_D46_SAFE and LIN_D47_SAFE.

If the inputs DIN45 ... DIN47 are configured as mode selector switches, then exactly one input must be High. To achieve this, the logic function executes a 1/N monitoring, with discrepancy time monitoring.

Logical inputs	**System start [1)]**	**Normal operation**	**Error status**
LIN_D45_SAFE	1	= LIN_D45	Last valid status
LIN_D46_SAFE	0	= LIN_D46	
LIN_D47_SAFE	0	= LIN_D47	
1) Status until a valid status is detected or if safe analysis of the mode selector switch is not active.			

Table 63: Logical inputs, mode selector switch

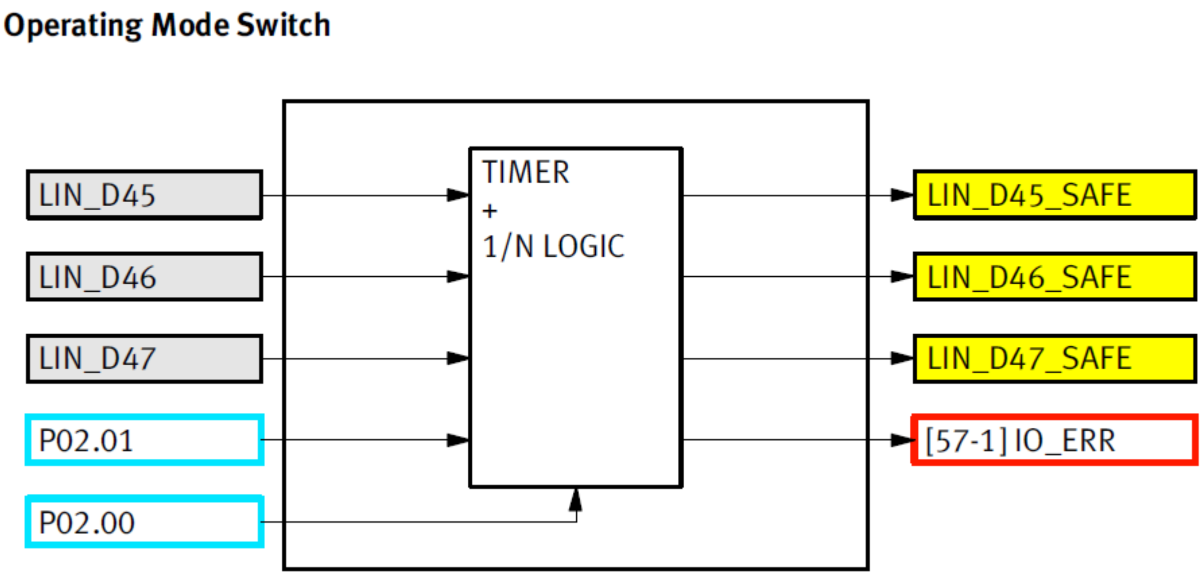


Figure 28: Block diagram of the mode selector switch

Term/abbreviation	Explanation
LIN_...	Logical inputs
TIMER + 1/N LOGIC	Timer and 1-of-n logic
[57-1] IO_ERR	Internal error signal, error 57-1

Table 64: Legend for Figure 28

2.6.1.3 Error detection

If, in the Mode selector switch function, no input or more than one input is High during a parameterisable time, an error is triggered and the input signals are indicated as being invalid.

If the inputs DIN45 … DIN47 have a faulty status, the signals LIN_D45_SAFE, LIN_D46_SAFE and LIN_D47_SAFE retain the most recently detected error-free status.

Time delays from level change LIN_D...	Minimum	Maximum	Typical
LIN_D45/46/47_SAFE	2.0 ms	2.1 ms	2.0 ms
Error reaction time on violation of the 1/N condition	2.0 ms + P02.01	2.1 ms + P02.01	2.0 ms + P02.01

Table 65: Runtime performance of the mode selector switch

2.6.1.4 Parameters of the mode selector switch

Mode selector switch		
No.	**Name**	**Description**
P02.00	Activation	DIN45..DIN47 are used as mode selector switches (1 of 3).
P02.01	Discrepancy time	Time in which no input or more than one input can be High simultaneously.

Table 66: Mode selector switch

2.6.2 Two-handed control device

2.6.2.1 Use

The logic function "Two-handed control device" is used in applications in which the operator must release the movement with both hands as soon as he has left the danger zone (e.g. press applications)

The two-handed control device provides the control signal LIN_2HAND_CTRL = LIN_DIN42 OR LIN_DIN43, with which the safety functions can be switched via logical links.

In addition, it monitors the simultaneous switching of the inputs (discrepancy time monitoring).

The two-handed control device uses the two inputs DIN42 and DIN43 (each with two channels A and B) and can only be activated when "Two-handed control device" is selected as the connected sensor type for the control inputs DIN42 and DIN43.

In the operating mode "Two-handed operator unit", the individual inputs DIN42 and DIN43 continue to have all the "normal" functions (equivalence/antivalence, test signals, cross-comparison with 2nd processor, etc.).

2.6.2.2 Function

The result of the logic operation of the two inputs is transferred to the separate logical input LIN_2HAND_CTRL. LIN_2HAND_CTRL is an OR operation of LIN_D42 and LIN_D43, i.e. it only has the status "0", when both logical inputs have the status "0".
LIN_2HAND_CTRL = LIN_DIN42 OR LIN_DIN43

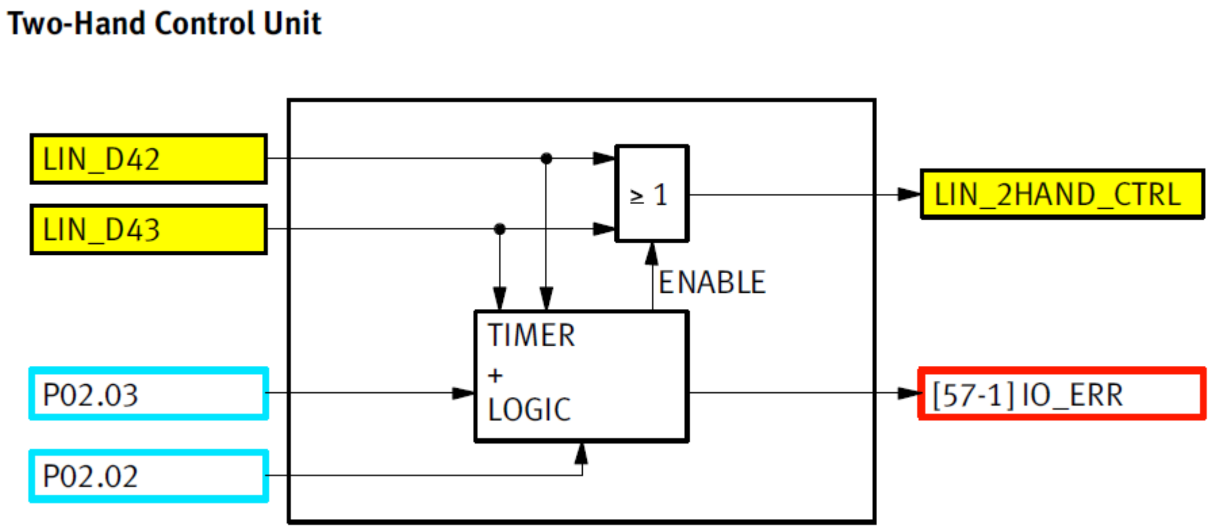


Figure 29: Block diagram of the two-handed control device

Term/abbreviation	Explanation
LIN_...	Logical inputs
TIMER + LOGIC	Timer and logic
ENABLE	Enable signal
[57-1] IO_ERR	Internal error signal, error 57-1

Table 67: Legend for Figure 29

2.6.2.3 Error detection

The logical statuses of the inputs DIN42 and DIN43 must agree. If the logical statuses deviate from one another for longer than a settable discrepancy time, then an error is generated.

The "Discrepancy time" parameter (P02.03) should usually be set as longer than the discrepancy time for the monitoring of the inputs DIN42, DIN43, as this bridges the time the operator needs to press or release both buttons of the two-handed control device.

Time delays from level change LIN_D...	Minimum	Maximum	Typical
LIN_2HAND_CTRL	2.0 ms	2.1 ms	2.0 ms
Error reaction time on violation of the two-handed condition	2.0 ms + P02.03	2.1 ms + P02.03	2.0 ms + P02.03

Table 68: Runtime performance of the two-handed control device

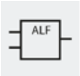
2.6.2.4 Parameters of the two-handed control device

Two-handed control device		
No.	**Name**	**Description**
P02.02	Activation	DIN42 and DIN43 are used as a two-handed terminal
P02.03	Discrepancy time	Time, in which the logical status of DIN42 and DIN43 may deviate from one another.

Table 69: Two-handed control device

2.6.3 Advanced Logic Functions – ALF

2.6.3.1 Use



Use ALF to create more complex operations of logical input signals LIN_x or if, for reasons of clarity in the application, it makes sense to create a specific combination of LIN_x as an internal safe logic signal.

The Advanced Logic Function can be used to link internal inputs and outputs logically. This allows special input combinations to be implemented, for example. ALF is used when more complex logical links are required and the input logic (OR gates with 4 upstream AND gates, each with 7 inputs) of a safety function is insufficient.

2.6.3.2 Function

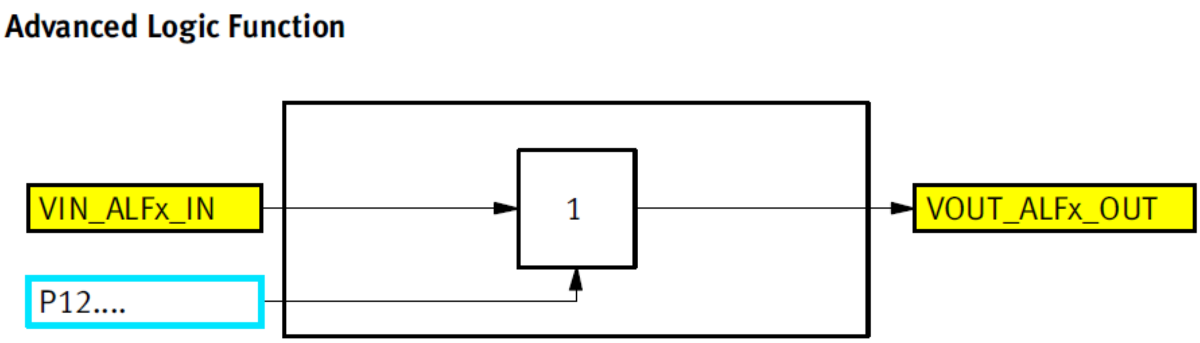


Figure 30: Block diagram, Advanced Logic Function

Term/abbreviation	Explanation
VIN_x_y	Virtual inputs
VOUT_x_y	Virtual outputs

Table 70: Legend for Figure 30

Time delays from VIN_ALFx_IN	Minimum	Maximum	Typical
VOUT_ALFx_OUT	2.0 ms	2.1 ms	2.0 ms

Table 71: Runtime performance of the Advanced Logic Functions

2.6.3.3 Parameters of the Advanced Logic Functions

Advanced Logic Functions			
ALF...	**No.**	**Name**	**Description**
ALF0	P12.00	Transmission function	Selection of the functionality (fixed): Identity (OUT = IN) = [2] With the "Identity" function, the output always has the logical status of the input.
ALF1	P12.03	Transmission function	
ALF2	P12.06	Transmission function	
ALF3	P12.09	Transmission function	
ALF4	P12.0C	Transmission function	
ALF5	P12.0F	Transmission function	
ALF6	P12.12	Transmission function	
ALF7	P12.15	Transmission function	

Table 72: Advanced Logic Functions

2.7 Restart

2.7.1 Function range

One or more safety functions are terminated using the "Restart" function described here, so that the drive can "restart".

In combination with safe movement functions, such as SLS, "Restart" means that the drive is no longer monitored and can travel at full speed again.

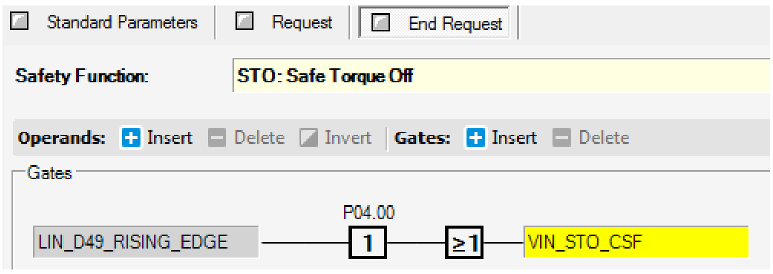
The user can specify separately for each safety function which control signal is to permit the restart. For this, the safety functions have the virtual input VIN_xxx_CSF (Clear Safety Function).

A restart must be defined for each safety function, except if the safety function was parameterised to "Automatic restart". In this case, the restart takes place automatically, as soon as the request for the safety function has been retracted.

A restart is only possible when the request for the safety function was first retracted. A request of a safety function always has a higher priority than the restart.

When the device is delivered, the single-channel input DIN49 is preset to the sensor type "Terminate safety function / Restart" and, as "Restart" is switched to the safety functions "STO" and "SBC".

On each rising edge (0 V -> 24 V) at DIN49, the signal LIN_D49_RISING_EDGE supplies a short switching pulse of a length of 2 ms, via which the safety functions can be reset.



Time delays from LIN_D49_RISING_EDGE	Minimum	Maximum	Typical
VIN_xxx_CSF up to termination of the safety function	0.0 ms	2.1 ms	2.0 ms

Table 73: Runtime performance, restart

➔ **Note**

Please check whether a single channel control input for the restart is permitted in your application and whether it is level-controlled or edge-controlled. Use ...

- LIN_D49, if a level-controlled reset is permitted,
- LIN_D49_RISING_EDGE, if an edge-controlled reset is required,
- in all other cases, use one of the two-channel inputs LIN_D40 to LIN_D43.

➔ **Note**

Please check whether the risk analysis for the machine has created additional requirements for the control of the restart and for the diagnostics of the corresponding control input, e.g. **manual, edge-controlled resetting through accessible protective devices**.

2.7.2 Examples and special notes on implementation

2.7.2.1 Restart after termination of STO

Figure 31 shows the structure for the STO safety function. During operation, STO can be requested via VIN_STO_RSF. The request of the safety function STO causes the driver supply in the servo drive to switch off. To switch the drive back on again after a STO request, the request must have been terminated, as described in ➔ Section 2.7.1.

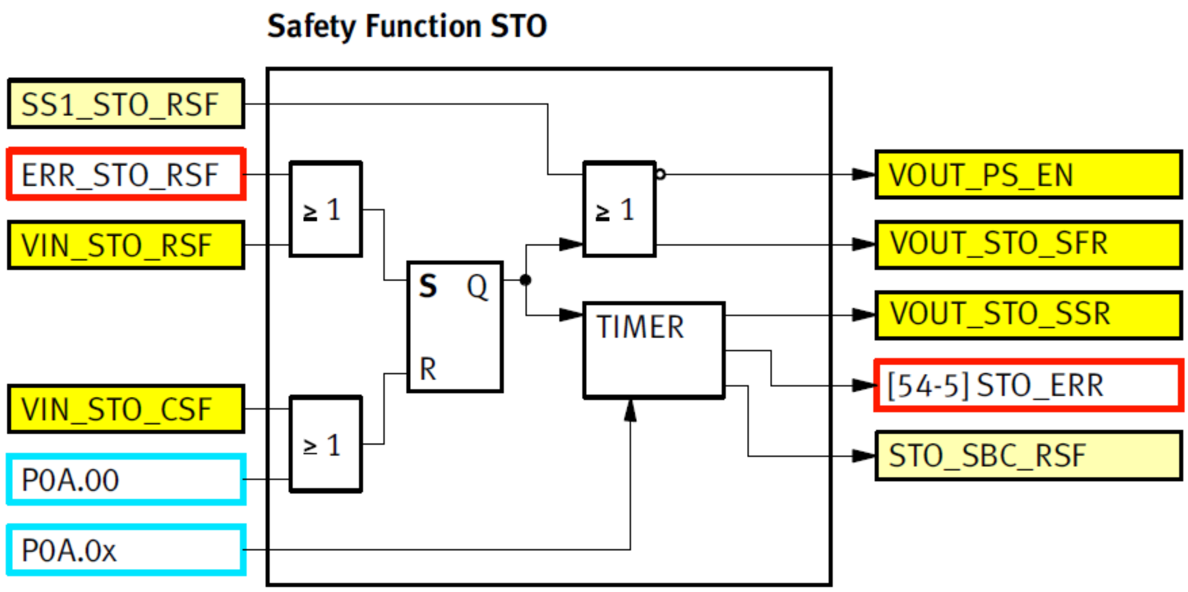


Figure 31: Request of a safety function (example of STO) / Restart

2.7.2.2 Restart after error acknowledgement

The error management can also request the STO function as an error response (via ERR_STO_RSF signal). As shown in Figure 11, the request is fed into the STO function.

For the drive to restart after an acknowledged error, a restart must take place via VIN_STO_CSF or the parameter "Automatic restart permitted" (P0A.00) must be set for an automatic restart. This also applies in a similar manner for the safety functions SS1, SS2 and SBC, which can be configured as an error response.

2.7.2.3 Restart after termination of SS1

The SS1 function requests STO at the end of its sequence via the control input SS1_STO_RSF.
As can be seen in Figure 31, the STO request is automatically deactivated when the request for the SS1 function no longer exists. The request of the STO function does not need to be deactivated separately. This also applies when the SS1 function is requested in case of error: The error must be acknowledged and SS1 deactivated. STO does not need to be deactivated separately.

2.7.2.4 Restart after termination of SBC

The logic for requesting and terminating the SBC function is basically like the logic for requesting STO (➔ Section 2.5.4, Figure 18)
In addition to the standard logic, SBC can also be activated via direct control signals from STO (STO_SBC_RSF) and SS1 (SS1_SBC_RSF). On restarting from STO or SS1, the automatic restart from SBC also takes place.

This means that it is possible to implement different restart conditions, although the same safety functions are being used:

- direct request of SBC, restart, for example, via LIN_D49_RISING_EDGE,
- indirect request, for example via SS1, restart from SBC together with restart from SS1, as soon as its restart condition has been met (e.g. LIN_D40).

2.7.2.5 Restart after termination of SS2

The combination of SS2 and SOS functions in the same way as the combination of SS1 and STO described above.

2.8 Error management and error acknowledgement

2.8.1 Triggering errors and error classes

The safety module executes the required safety functions. It monitors itself, the inputs and outputs and the position encoders 1 and 2. If a safety function is breached or an error is detected, the safety module switches to error state.

In conjunction with the functional safety design and the safety module FSM 2.0 – MOV, there are errors which are triggered by the basic unit and others which are triggered by the safety module. They are divided up into various classes, which can be differentiated using the error number displayed on the seven-segment display of the servo drive.

The number consists of a two-digit main index (range 51 … 59) and a subindex (range 0 … 9):

Error number											
Main index	**Subindex**										**Error type/class**
Basic unit error											
51-x	9	8	7	6	5	4	3	2	1	0	Control signals from the safety module not OK, module type / identifier not OK
52-x	9	8	7	6	5	4	3	2	1	0	Error in activation sequence with the safety module
Error of the safety module											
53-x	9	8	7	6	5	4	3	2	1	0	Violation of a safety function
54-x	9	8	7	6	5	4	3	2	1	0	Violation of a safety function
55-x	9	8	7	6	5	4	3	2	1	0	System error: Actual value recording / position encoder not OK
56-x	9	8	7	6	5	4	3	2	1	0	System error: Position recording / comparison not OK
57-x	9	8	7	6	5	4	3	2	1	0	System error: Inputs and outputs or internal test signals not OK
58-x	9	8	7	6	5	4	3	2	1	0	System error: Communication external / internal not OK
59-x	9	8	7	6	5	4	3	2	1	0	System error of the firmware / hardware error of the safety module

Table 74: Bit field of the error numbers (grey = reserved for future extensions)

You can find a full description of all the errors with possible causes and possible measures for avoiding them in ➔ Section 5.6.

2.8.1.1 Basic unit error

During operation, the basic unit monitors the communication with the safety module and the plausibility of the control signals from the safety module. After switch-on, the basic unit checks whether a module has been replaced and that the correct type of safety module has been mounted. If there are errors, it generates a corresponding error message with parameterisable error response (➔ product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS).

2.8.1.2 Error of the safety module

The safety module executes the required safety functions. It monitors itself, the inputs and outputs and the position encoders 1 and 2. If a safety function is breached or an error is detected, the safety module switches to fault state. For this reason, the safety module distinguishes between

– errors on violation of a safety condition (53-x and 54-x) – LED is permanently red

and

– system errors (55-x to 59-x) – LED flashes red (LED display ➔ Section 2.1.2)

Errors are generated by the various function blocks in the safety module:

For example, the SSF safety function generates an error signal when the drive moves outside the monitored speed range. The error may also be very short, if the drive only leaves the permitted range for a brief interval.

For this reason, both the basic unit and the safety module have an internal error buffer. Each error occurring during operation is firstly entered in this error buffer and then saved.

– The permanent event memory of the basic unit can store more than 8192 entries. When this limit is reached, the oldest entries are overwritten.
– In the case of the safety module, up to 32 errors can occur simultaneously. Errors are immediately transferred to the basic unit where they are stored in the permanent event memory.

i The permanent event memory of the basic unit remains intact, even if there is voltage failure, meaning that an error history is available. Besides errors, other events are also entered in the permanent event memory. You can find a detailed description in ➔ Section 2.11.

In addition, the error number, consisting of the main index and the subindex, is displayed on the 7-segment display of the servo drive. The most recently triggered error of the highest priority (error number) is displayed. Later errors with a lower priority are entered in the error buffer, but are not shown on the 7-segment display.

An error status remains intact until it is acknowledged.

2.8.1.3 Violation of safety conditions

The "Safety condition violated" signals of the individual safety functions are combined into a common error message or a common warning message, depending on the parameterised error response. This can control the signal relay, for example. The common messages themselves do not generate an error response.

The error response is specified individually for each safety function ➔ Sections 4.6.14 and 8.2.

An error is triggered once on the first violation of the safety condition after the request of the safety function. A repeated violation of the safety condition will only generate a new error message after the error has been acknowledged.

The "Safety condition violated" output displays the current status. Example:

1. SLS is requested.
2. Speed outside the approved range → Error message, output active.
3. Speed back in approved range → Output becomes inactive.
4. Speed again outside the approved range ➔ Output active, no new error message.

2.8.1.4 Reaction to faulty status variables

As long as a safety function is not requested, the validity of the input variables (e.g. speed signal, signal of idle detection, etc.) is neither monitored nor checked.

Whilst a safety function is requested or implemented, the validity of the input variables is monitored. If an error is detected, then this generates the corresponding error message "Safety condition violated".

There is a hidden expert parameter, P09.00, which can be used to set a mask to prevent safety functions from generating the statuses VOUT_SSR and VOUT_SCV.

This can be useful if you wish to use safety functions for monitoring, e.g. "Safe Speed Monitor, SSM" and these are to be hidden from the operating status messages.

Please consult your local contact person as necessary.

2.8.2 Parameterisation of the error response of the safety module

For many errors of the groups 53-x to 57-x, the error response can be configured in many ways. For some critical errors, the selection is restricted or prevented completely. Each error triggers the error response assigned to it, irrespective of the temporal sequence in which they occurred. If multiple errors are pending simultaneously, then multiple error responses are activated simultaneously.

If a safety condition is violated, the safety module must stop the axle in a defined way, depending on the stop category requested (STO, SS1, SS2, possibly SBC).

In the case of system errors, the scope of the required error response is dependent on whether the safe function of the safety module can still be guaranteed or not.

The following error reactions (starting with those of the highest priority) are available:

[8] SBC + STO request + and set all digital outputs to "0"
[7] STO + SBC request
[6] STO request
[5] SS1 + SBC request
[4] SS1 request
[3] SS2 request
[2] Generation of a warning (display of the servo drive), no further reaction
[1] No reaction, but logging
[0] No reaction, no logging

➔ **Note**

If there are errors, the drive must be de-energised as quickly as possible (STO). In cases of doubt, the clamping unit or holding brake must take effect (SBC) and all the safe outputs must be switched off, corresponding to error response [8].

This status is the "Safe basic status" of the safety module.

- Energy supply to the motor is now no longer possible.
- A movement is braked via an external clamping unit with emergency braking properties.
- External downstream electronic systems are switched off / switched to the safe status.

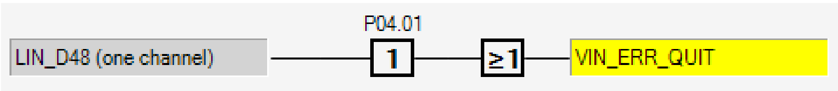
Please check which fault reaction is required in your safety application; when in doubt, select the highest [8].

2.8.3 Logic for error acknowledgement

The "Error acknowledgement" function described here resets errors which have occurred. This is the precondition for a restart after errors.

Errors can be acknowledged via a rising edge of the VIN_ERR_QUIT control signal. For this, the control signal must be connected to a digital input.
Configuration takes place in the same manner as configuration of the request or the restart of a safety function. Please switch a control port to VIN_ERR_QUIT and confirm the input so the safety module exits the error status.

In the delivery status and after a reset to factory settings, the input DIN48 is intended for the "Error acknowledgement" function. Errors are acknowledged with the rising edge (0 V -> 24 V).



An error can only be acknowledged (removed from the temporary error buffer of the safety module) when the error condition no longer exists. Thus, during acknowledgement, the safety module systematically checks all the error conditions and deletes the entries of the errors which have been eliminated. The remaining errors remain intact. After an acknowledgement operation, the safety module writes an "Error acknowledgement" entry to the permanent event memory of the basic unit. After the end of error acknowledgement, any errors which still exist are entered in the error buffer and permanent event memory again.

At the end of error acknowledgement in the safety module, the module sends an "Acknowledge error" command to the basic unit so that pending errors in the basic unit can also be acknowledged.

This means that the safety module has a master function for the acknowledgement of errors.

- Errors acknowledged in the safety module are also acknowledged in the basic unit.
- Error numbers generated by the safety module (53-x to 59-x) can only be acknowledged via the safety module.
- During error acknowledgement, the basic unit can only acknowledge those error numbers via the functional controller or I/O which are also generated by the basic unit.

Errors of the safety module are only acknowledged by the control port configured for this.

Time delays LIN_D48 to ...	**Minimum**	**Maximum**	**Typical**
VIN_ERR_QUIT up to the deletion of the temporary error buffer and change of the operating mode	4.0 ms	20 ms	10 ms
VIN_ERR_QUIT up to the deletion of the errors in the basic unit and ready status of the basic unit	20 ms	500 ms	100 ms

Table 75: Runtime performance of error acknowledgement

Note

When a safety condition is violated, the error can only be acknowledged when the status variables of the drive are once more in the approved range.

Example - Violation of SOS:

After SOS has been requested, the axle is moved outside the tolerance range -> The error [54-3], SOS violation, is generated. The error can only be acknowledged when:

- the axle has been moved back into the permitted range or (alternatively)
- the request of the SOS safety function was terminated (restart).

The result of the SOS violation is that another safety function, in this example SS1, is executed as an error response.

The following sequence is required for a restart after an "SOS violation":

1. Actuation of Restart
   –> Terminates the SOS function, SS1 (from error response) continues to be executed
2. Error acknowledgement
   –> Deletes the error "SOS violation"
3. Restart
   –> Terminates the safety function SS1 –> axle/motor can restart

Errors of the following safety functions can also be acknowledged when a safety function has been requested:
STO, SS1, SBC, USF/SSF in all three versions SLS, SSR, SSM.

2.9 Digital outputs

2.9.1 Two-channel safe outputs DOUT40 … DOUT42 [X40]

2.9.1.1 Use

Use the two-channel safe outputs to:

- transmit safe status messages to external control devices.
- activate safety switching devices.
- when switched on permanently, they can be used as a source for test impulses.

2.9.1.2 Function

The safety module has three safe outputs DOUT40A/B, DOUT41A/B, DOUT42A/B. The outputs are largely freely-configurable and can have various functions (safety function request, safe state reached, errors, etc.) assigned to them. Thus, the operating status of the safety module or an individual safety function can be transferred externally:

- to indicate the safety status to downstream drives,
- to request safety functions in downstream drives with safety module FSM 2.0 – MOV,
- to indicate the safety status to an external safety controller or a function controller,
- to activate external safe actuators, e.g. a clamping unit, a valve vent, a door lock, or similar.

2.9.1.3 Block diagram

DOUT40 ... DOUT42

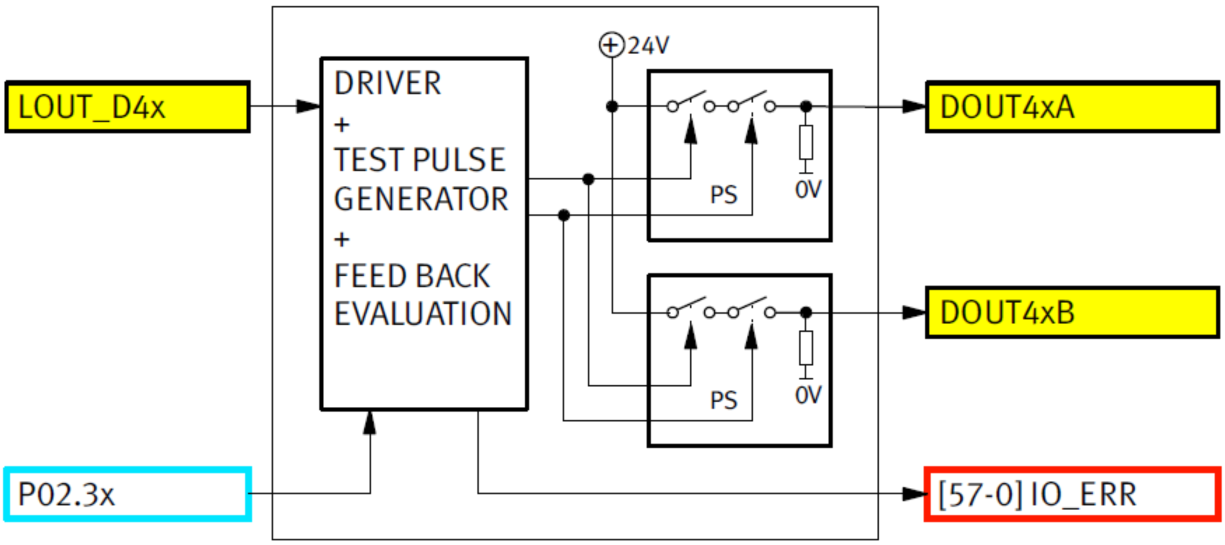


Figure 32: Block diagram of the two-channel safe outputs

Term/abbreviation	Explanation
LOUT_x	Logical outputs
DRIVER + TEST PULSE GENERATOR + FEED BACK EVALUATION	Drivers, generation of test pulses and analysis
DOUT4...A / DOUT4...B	Two-channel digital outputs
[57-0] IO_ERR	Internal error signal, error 57-0

Table 76: Legend for Figure 32

The output is activated by selecting one or more VOUT_x signals, which are applied to LOUT_D4x.

Each safe digital output can be configured as follows (P03.30 for DOUT40):

- permanently OFF (DOUT40A/B = 0 V),
- permanently ON (DOUT40A/B = 24 V),
- equivalent switching,
- antivalent switching.

The test pulse length can be parameterised (P03.31 for DOUT40).

i You can use the outputs to monitor passive sensors using test pulses. To do this, configure one of the outputs to "Permanently on" and use the outputs DOUT4x A/B to supply the switching device ➔ Section 3.3, Sample circuits.

The following tables show the allocation of the logic signal LOUT_D4x to the output level for outputs switching equivalently and antivalently:

Output DOUT40/41/42 Equivalent	Idle state	Safe state requested
LOUT_D40/41/42	1	0
DOUT40A/41A/42A	24 V	0 V
DOUT40B/41B/42B	24 V	0 V

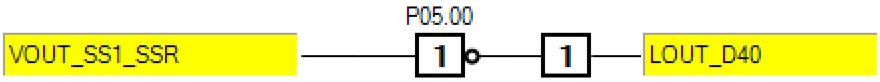
Table 77: Logic signals DOUT40/41/42 equivalent

Output DOUT40/41/42 Antivalent	Idle state	Safe state requested
LOUT_D40/41/42	1	0
DOUT40A/41A/42A	24 V	0 V
DOUT40B/41B/42B	0 V	24 V

Table 78: Logic signals DOUT40/41/42 antivalent

The safe output (including clock output) should always follow the idle current principle, i.e. the Low level is the safe status.

The user must ensure this during configuration by inverting the control signal LOUT_D40 to ensure this principle is implemented.



The user must ensure that a voltage-free output leads to the safe status for the overall system.

Each safe digital output can also be used as a clock output to feed passive sensors. In this case, it is configured as "permanently ON".

2.9.1.4 Error detection

The output drivers have a two-channel, redundant structure. The output levels at DOUT4xA/B are continually read back by both microcontrollers during operation. Both microcontrollers output test pulses to the outputs, which read back and analyses the pulses from their counterpart.

These measures safely detect short circuits to 24 V, 0 V and cross circuits between any outputs. If there is an error, the output switches to the safe status (DOUT4xA/B switched off or 0 V). An error message [57-0] IO-ERR is generated.

If there are serious internal errors and, as a result, one or both microprocessors can no longer control the status of the outputs safely, then all the outputs are switched off jointly. Even in the case of antivalent outputs, both pins A/B are switched to the Low level.

Examples of such errors:

- operating voltage faulty,
- position sensors faulty,
- memory error, stack error,
- program sequence monitoring indicates an error, internal communication fault.

2.9.1.5 Timing diagram

Figure 33 shows an example of the runtime performance when the output DOUT40 is switched off and on again. The test pulses for High level are also shown. They are temporally offset for all the outputs.

Digital Output DOUT40A/B

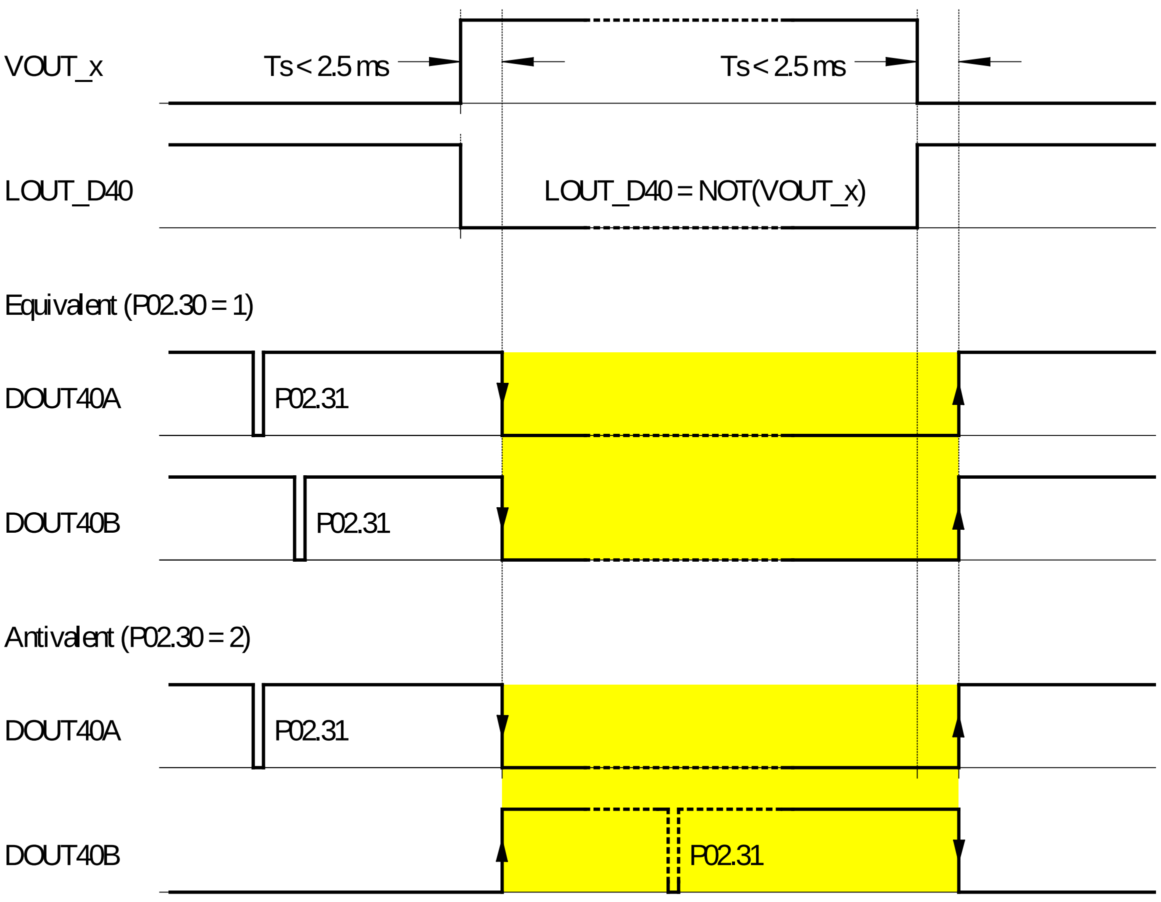


Figure 33: Timing diagram of the two-channel safe outputs

Term/abbreviation	Explanation
VOUT_x	Virtual outputs
LOUT_x	Logical outputs
DOUT40A, DOUT40B	Two-channel digital outputs
Equivalent / Antivalent	Äquivalent / Antivalent

Table 79: Legend for Figure 33

From activation of a safe output, the following times elapse until the output pins are switched over:

Time delays from LOUT_D4x until level change at output	Minimum	Maximum	Typical
Time delay Ts	0.0 ms	2.5 ms	0.5 ms
Length of the test pulses (P02.31, ...)	0.4 ms	10.0 ms	1.0 ms

Table 80: Time delays DOUT40 … DOUT42

2.9.1.6 Parameters for the two-channel digital outputs

Parameter no. for output ...			**Name**	**Description**
DIN40	**DIN41**	**DIN42**		
P02.30	P02.32	P02.34	Operating mode	Mode: Off (0V) / equivalent / antivalent / ON (24 V)
P02.31	P02.33	P02.35	Test pulse length	Length of the test pulse

Table 81: Parameters of two-channel digital outputs

2.9.2 Internal brake control of the servo drive [X6]

2.9.2.1 Use

The servo drive has integrated circuit breakers for safe brake control. Both the +24 V connection and the 0 V connection of the holding brake are switched using separate power transistors.

The holding brake is normally activated functionally via the servo drive. However, the circuit breakers can also be used in combination with the FSM 2.0 – MOV, in order to control a clamping unit or holding brake via the SBC safety function.

The integrated brake control at output [X6] meets the requirements PL d / Cat. 3 according to EN ISO 13849, or SIL 2 according to EN 61800-5-2.

2.9.2.2 Function

The safety module actively controls the high and low-side switches in the servo drive. Control of the safety module is implemented through both microcontrollers via the signals BR+_BASEUNIT and BR-_BASEUNIT. The Low status of the appropriate signal switches off the corresponding power transistor and the holding brake takes effect.

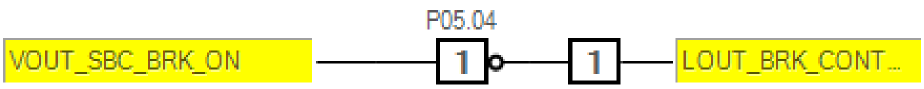
When the device is delivered, the internal brake activation is already configured in such a way that a request by the SBC safety function causes a switch-off of the signals BR+_BASEUNIT and BR-_BASEUNIT.

Observe the polarity of the control signal from the SBC function:

VOUT_SBC_BRK_ON = 1 means that the clamping unit or holding brake should take effect.

For this reason, the control signal must be inverted:

LOUT_BRAKE_CTRL = NOT(VOUT_SBC_BRK_ON)



2.9.2.3 Block diagram

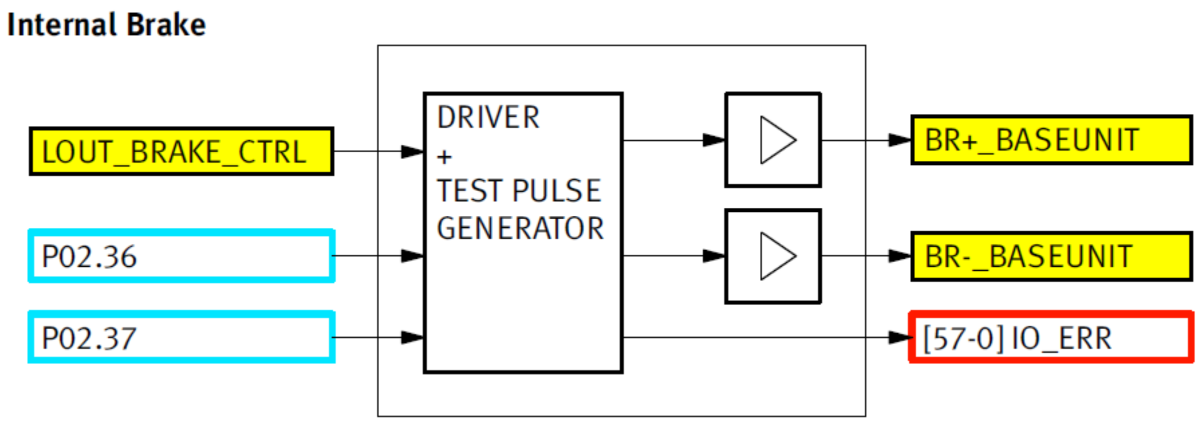


Figure 34: Block diagram of the safe brake control in the basic unit

Term/abbreviation	Explanation
LOUT_BRAKE_CONTROL	Logical output, brake activation
DRIVER + TEST PULSE GENERATOR	Driver and generation of test pulses
BR+_BASEUNIT/BR-_BASEUNIT	Internal signals: Brake activation
[57-0] IO_ERR	Internal error signal, error 57-0

Table 82: Legend for Figure 34

Output control signals BR+ / BR-	Safe brake control not energised	Safe brake control energised
LOUT_BRAKE_CTRL	1	0
BR+_BASEUNIT	0	1
BR-_BASEUNIT	0	1

Table 83: Logic signals BR+_BASEUNIT/BR-_BASEUNIT

2.9.2.4 Error detection

Test pulses check the function of the high-side and low-side switches during operation. The test pulse length can be parameterised (P02.37). When the safe brake control is energised, each circuit breaker in the basic unit is checked separately, using test pulses. The pulse length can be parameterised. An internal feedback signal is used to measure the voltage at the safe brake output of the safety module.

The following faults are recognised:

- short from BR+ to 24 V.
- short from BR- to 0 V.

If there is an error, the error [57-0] IO_ERR is generated.

Internal brake activation at the output [X6] is suitable for clamping units of holding brakes with 24 V and a current consumption of max. 2 A
➔Technical data of the brake output in the product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS.

Alternatively, the clamping unit or holding brake can be activated via a safe digital output (DOUT40 to DOUT42) and an external brake switching device ➔ see the examples in Section 3.3.5 and 3.3.6.

2.9.2.5 Timing diagram

Figure 35 shows an example of the runtime performance when the internal brake output [X6] is switched off and on again. The test pulses for the energised clamping unit or holding brake (vented) are also shown. They are temporally offset.

Internal Brake

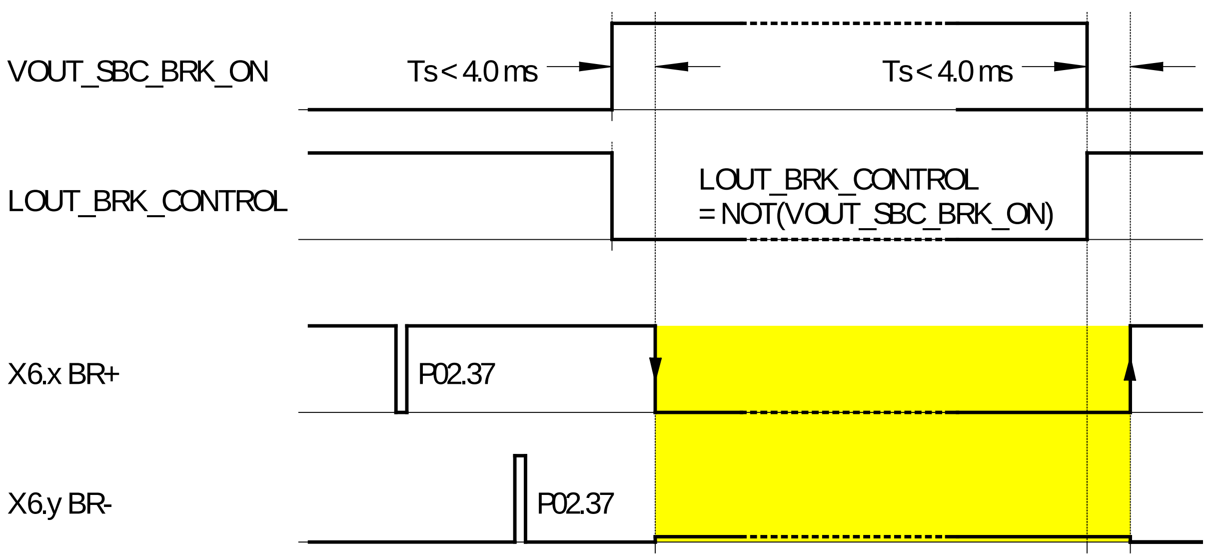


Figure 35: Timing diagram of the integrated brake control in the basic unit

Term/abbreviation	Explanation
VOUT_SBC_BRK_ON	Virtual output, activation of internal brake
LOUT_BRK_CONTROL	Logical output, activation of internal brake
X6.x BR+ / X6.y BR-	Signals at the contacts of the brake output in the basic unit

Table 84: Legend for Figure 35

From activation of the internal brake, the following times elapse until the output pins at [X6] are switched over:

Time delays from LOUT_BRAKE_CTRL until level change of brake output [X6] of the basic unit	Minimum	Maximum	Typical
Time delay Ts	0.0 ms	4.0 ms	2.0 ms
Length of the test pulses (P02.37)	0.4 ms	10.0 ms	1.0 ms

Table 85: Time delays, internal brake

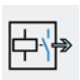
2.9.2.6 Parameters for internal safe brake control

Internal brake		
No.	**Name**	**Description**
P02.37	Test pulse length	Length of the test pulse

Table 86: Parameters of internal brake

2.9.3 Signal contact C1, C2 [X40]

2.9.3.1 Use



The potential-free signal contact is ideally used as a diagnostic output. It can be used to signal the operating status of the safety module to an external safety controller.

2.9.3.2 Function

The signal contact has one channel and may not be used as a part of a safety chain.

The contact does not have forced contacts for safety monitoring of the faulty function. The potential-free signal contact can be configured in the same way as a safe output, although no test pulses to test digital inputs can be output.

The contact is an N/O contact. In the idle / de-energised status, the contact is open, as it is during initialisation and Power off/on of the safety module.

2.9.3.3 Block diagram

Signal relays C1/C2

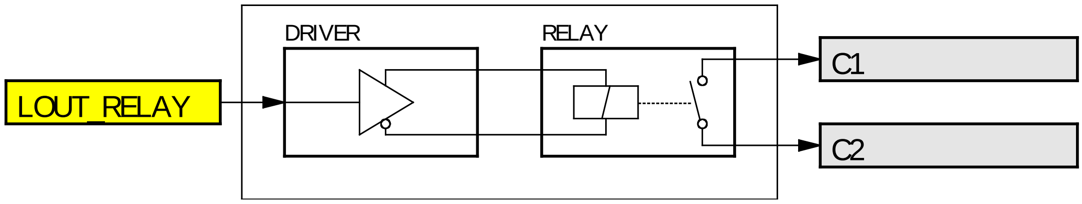


Figure 36: Block diagram of the potential-free relay output

Term/abbreviation	Explanation
LOUT_RELAIS	Logical output, feedback contact
DRIVER	Drivers

Table 87: Legend for Figure 36

Signal contact output	Idle state	Active
LOUT_RELAIS	0	1
Contact C1/C2	Open	Closed

Table 88: Logic signals, signal contact

2.9.3.4 Error detection

The status of the switching contact is not monitored.

When the device is delivered, the signal contact is preconfigured as follows:

Contact closed when no error is pending and all requested safety functions indicate the safe status (common message VOUT_SSR "Safe State Reached").

2.9.3.5 Timing diagram

Figure 37 shows an example of the runtime performance when the signal contact is switched off and on again.

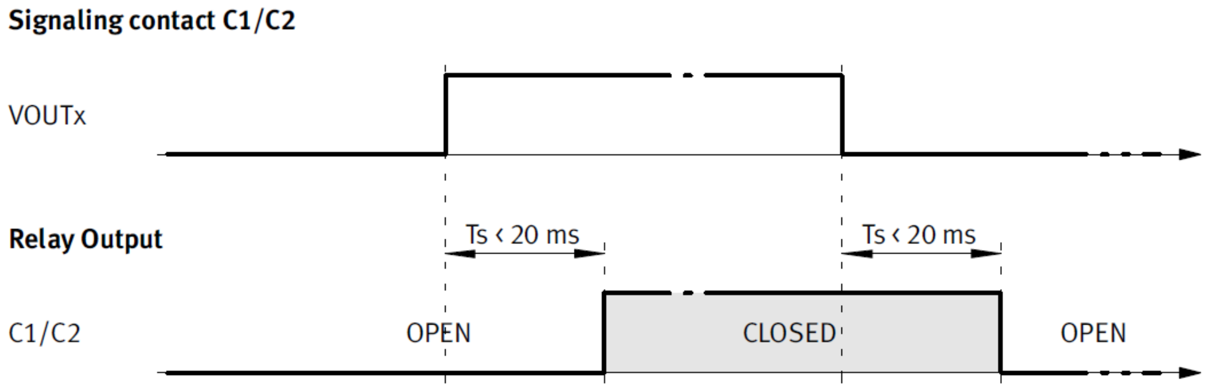


Figure 37: Timing diagram of the potential-free signal contact

Term/abbreviation	Explanation
VOUTx	Virtual output
OPEN / CLOSED	(Relay contact) open / closed

Table 89: Legend for Figure 37

From activation of the relay, the following times elapse until the output pins are switched over:

Time delays from LOUT_RELAIS until relay switches	Minimum	Maximum	Typical
Time delay Ts	0.0 ms	20.0 ms	6.0 ms

Table 90: Time delays, relay output

The signal contact is implemented as a miniature relay.

The service life and switching cycle resistance of the relay is primarily dependent on the level and type of the load on the relay contact.
Table 121 in Appendix 7.1.6 describes the electrical data of the signal contact.

2.9.4 Auxiliary supply +24 V [X40]

The auxiliary supply can be employed when using the acknowledgement contact C1/C2 or to supply external, active sensors.

The safety module provides 24 V DC at the interface X40 with a maximum load capacity of 100 mA.

The output for the 24 V is protected against overloading and short circuits by a PTC.

Table 122 in Appendix 7.1.7 describes the electrical data for the auxiliary supply.

2.10 Operating status and status displays

2.10.1 Statuses of the system / finite state machine

Figure 38 shows the status transitions of the safety modules on starting after Power ON.

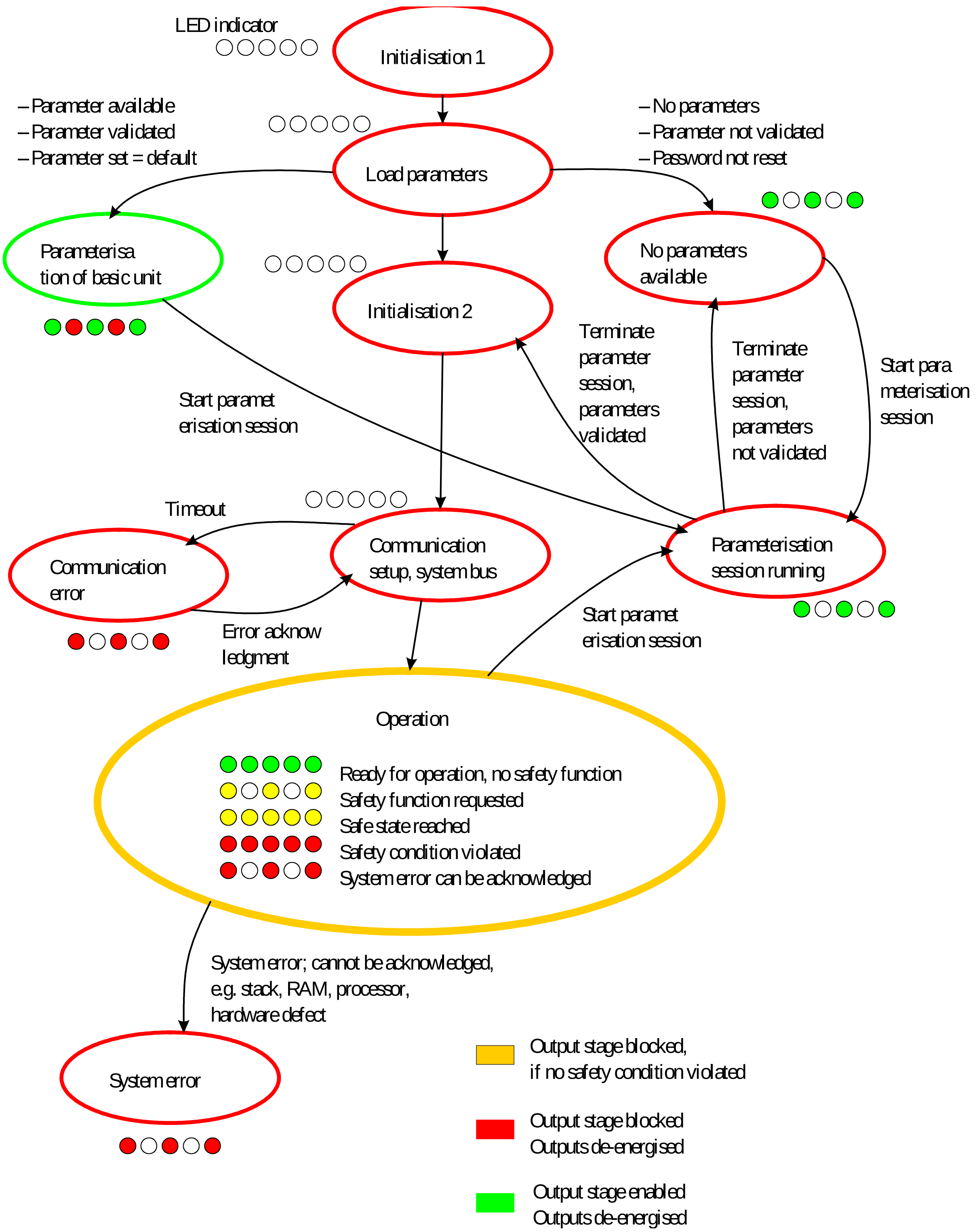


Figure 38: Statuses of the "complete system"

2.10.1.1 Description of the statuses of the "complete system"

- In the Initialisation 1 phase, basic system tests of the hardware and firmware are performed.
- Then, the parameter set is loaded from the FLASH memory of the module and is checked:
  - The safety module checks whether there is a valid safe parameter set in the safety module. A valid safe parameter set exists when all the individual parameters have been validated and the whole parameter set has the identification "validated".
  - It checks whether the safety module is in the delivery status. In the delivery status, all the individual parameters are validated but the whole parameter set has the identification "not validated". In addition, the identifier "Delivery status" is set in the parameter set.

i The basic unit can be commissioned and the motor run in the delivery status. The safety module is pre-configured with the safety functions STO and SBC, which can be requested via DIN40, thus offering minimum protection ➔ Section 4.4.2 and 4.4.1.

- If not all the individual parameters have been validated or the whole parameter set has the identifier "not validated", then the safety module switches to the "Service" status and waits for external parameterisation.

i The motor and the basic unit cannot be commissioned in the "Service" status. The safety module has switched off all the safe outputs and also the internal control signals to enable the output stage and the holding brake.

- When parameterisation is ended, a second initialisation takes place.
- After this, communication is set up with the basic unit.
- If no errors have been found up to that point and the safety module has a valid, safe and fully-validated parameter set, then it switches to the "Operation" status, in which safety functions can be requested and executed. In the "Operation" status, all the modules work according to their specified functionality.
- If system errors are detected, e.g. a defective position encoder, then the safety module switches to the "System error" status, which can only be exited after elimination of the error and subsequent error acknowledgement or a restart of the system.

Figure 39 shows the status transitions of the safety module during "Operation".

- As long as no safety function has been requested, the "Ready for operation" status exists.
- If at least one safety function is requested, the safety module switches to the status "Safety function requested". Monitoring is already active but the safe status has not yet been reached, e.g. because a speed ramp is being travelled.
- The status "Safe state reached" follows, monitoring is active and the drive is in the safe status.
- The status "Safety condition violated" is assumed if there is an error. It can only be exited via error acknowledgement.

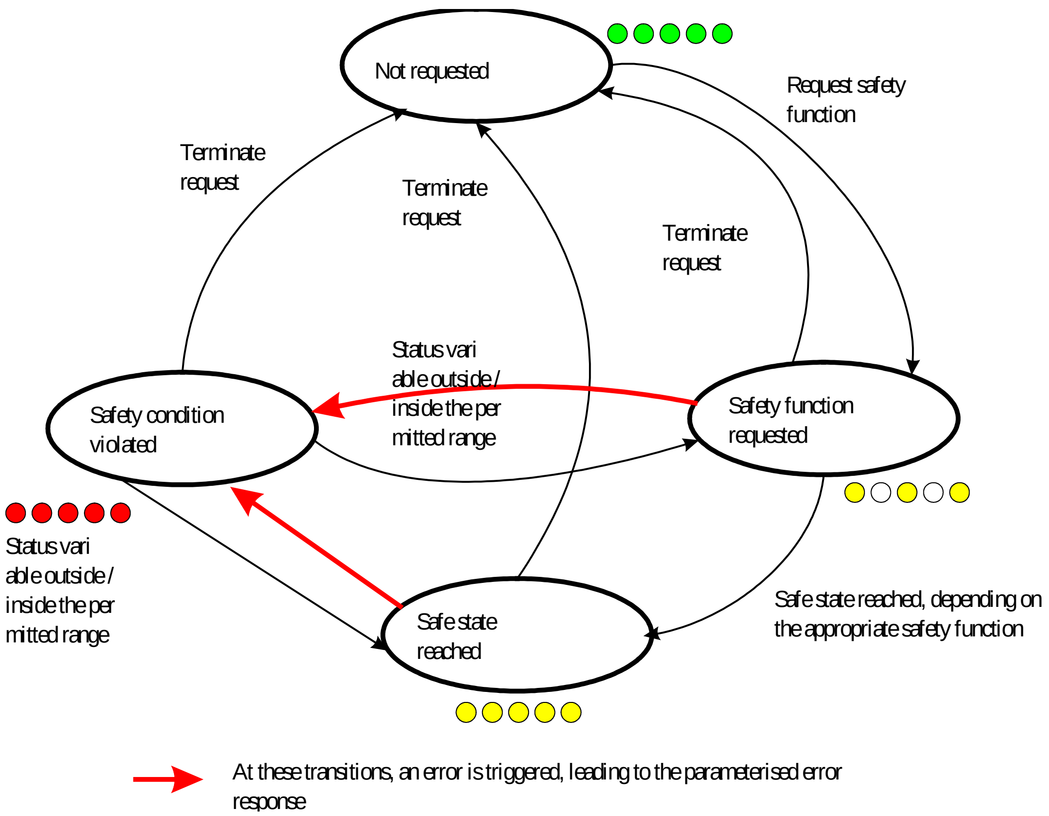


Figure 39: Statuses of the "Operation" safety functions

The safety functions, for their part, have small-scale sequence controls and generate status and error messages (example: Safety function SS1 ➔ Section 2.5.5, Figure 20). Various common status messages are generated from the error or operating statuses of the individual safety and logic functions.

The common messages are formally implemented as virtual outputs. They are fed back as corresponding logical inputs.
This means that outputs (e.g. signal relay) can be activated according to the system status, and safety functions can be activated according to the system status.
The common status messages are described below.

2.10.1.1.1 VOUT_READY: "Ready for operation, no safety function requested"

The "Ready for operation, no safety function requested" signal becomes "1" when no error message is pending whose reaction exceeds a warning and no safety function has been requested.

2.10.1.1.2 VOUT_SERVICE: "Service", the safety module must be parameterised

The "Service" signal becomes "1" when the parameter set of the module is invalid, when a parameterisation session is running or if no parameter set is available. There is an identifier in the parameter set, using which the safety module can detect whether this is a delivery status (= standard parameter set).

→ **Note**

If the checksum of the parameter set is faulty, then this is a serious internal error, which will lead to the "System error" status.

2.10.1.1.3 VOUT_SFR: "Safety Function Requested"

The "Safety function requested" signal becomes "1" when at least one safety function has been requested. It remains active until all the requests have been reset.

2.10.1.1.4 VOUT_SSR: "Safe State Reached"

The "Safe state reached" signal becomes "1" when the "Safe state reached" output is active for **all** the requested safety functions and when at least one safety function has been requested.

2.10.1.1.5 VOUT_ERROR: "System Error"

The "System error" signal becomes "1" when there is at least one error pending whose reaction is parameterised to higher than "Warning". An exception to this is errors of the category "Safety condition violated", which have their own common error message.

Note: This is the case when either an acknowledgeable error of a module is pending or if the entire system is in the "System Error" or "Communication Error" status.

2.10.1.1.6 VOUT_SCV: "Safety Condition Violated"

The "Safety condition violated" signal becomes "1" when at least one error of the category "Safety condition violated" is pending in the error management and when the error response of this error is prioritised as higher than "Warning".

2.10.1.1.7 VOUT_WARN: "Warning"

The "Warning" signal becomes "1" when there is at least one error pending whose reaction is parameterised to "Warning". An exception to this is errors of the category "Safety condition violated".

2.10.1.1.8 VOUT_PS_EN: "Power Stage Enable"

The "Power stage enable" signal directly maps the status of the safe pulse block (STO safety function). It is "1" when the driver supply has been enabled by the safety module and "0" when the driver supply was switched off via the STO safety function.

2.10.2 Status display on the safety module

To display the status of the safety function, the safety module has an LED on its front side ➔ Section 5.4.1.

The status LED displays the operating status of the safety module. The display is exclusively for diagnostics and must not be used in a safety-orientated way.

If multiple statuses are pending simultaneously which result in a display, then the status with the highest priority is displayed. The priorities are shown in Table 91.

The display is a continuous light or flashes at approx. 3 Hz.

LED indicator	**Status signal**	**Prio**	**Status, safety module**	**Internal status**
Flashes red	VOUT_ERROR = 1	7	"System Error"	The entire system is in the "System Error" or "Communication Error" status.
Lights red	VOUT_SCV = 1 VOUT_SFR = 1	6	"Safety Condition Violated", error response initiated	Violation of at least one of the currently required safety functions.
Lights yellow	VOUT_SSR = 1 VOUT_SFR = 1	5	"Safe State Reached", safe status achieved	All requested safety functions are in the status "Safe State Reached".
Flashes yellow	VOUT_SFR = 1	4	"Safety Function Requested"	The signal is active as soon as at least one safety function is requested. It remains active until all the requests have been reset.
Flashes red/green	VOUT_SERVICE = 1 VOUT_PS_EN = 1	3	"Delivery Status"	The delivery status can be distinguished from the "Service status" using VOUT_PS_EN.
Flashes green	VOUT_SERVICE = 1 VOUT_PS_EN = 0	2	"Service" status	No parameters present, parameter invalid or parameterisation session is running.
lights green	VOUT_READY = 1 VOUT_PS_EN = 1	1	"Ready", operational	Operational, no safety function requested, no errors.
Off	VOUT_READY = 0 VOUT_PS_EN = 0	0	"Initialisation Running"	Initialisation 1: Load parameter, Initialisation 2: Establish communication:

Table 91: System statuses and messages

2.10.3 7-segment display of the servo drive

The 7-segment display of the servo drive shows additional information ➔ Section 5.4.2, e.g.:

- display of the active safety function.
- display of error messages of the safety module with unique error numbers. Previously requested stop functions (STO, SS1, SS2, SOS) have a higher display priority than the other safety functions ➔ Section 5.6.
- Display of an active parameterisation session.

2.11 Permanent event memory in the servo drive

The servo drive manages a permanent event memory, which is stored in the non-volatile memory of the device and thus remains intact, even in the case of voltage failure / power-off. The permanent event memory is intended for non-volatile storage of errors and other events.

The permanent event memory consists of two blocks, which can be written to alternately. If one block is full, the other block is deleted. The architecture of the memory means that, during a deletion operation, half of the saved entries are lost.

The permanent event memory is used both by the safety module and by the servo drive. Entries of the servo drive use up the total available memory capacity. There is no reserved memory capacity for the safety module.

Status and error messages are entered chronologically. The oldest entries are deleted when a block is full.

With regard to the safety module, the following events are logged in the permanent event memory:

- starting of a parameterisation session (also attempt to start)
- ending of a parameterisation session
- changing / resetting the password
- storing of the parameter set in the safety module
- errors and warnings
- acknowledging errors
- request of a safety function (can be activated)

A factory setting stipulates that safety functions are not logged. However, safety functions can be logged using the parameter P20.4A.

In the MSC, an entry in the error list looks like this:

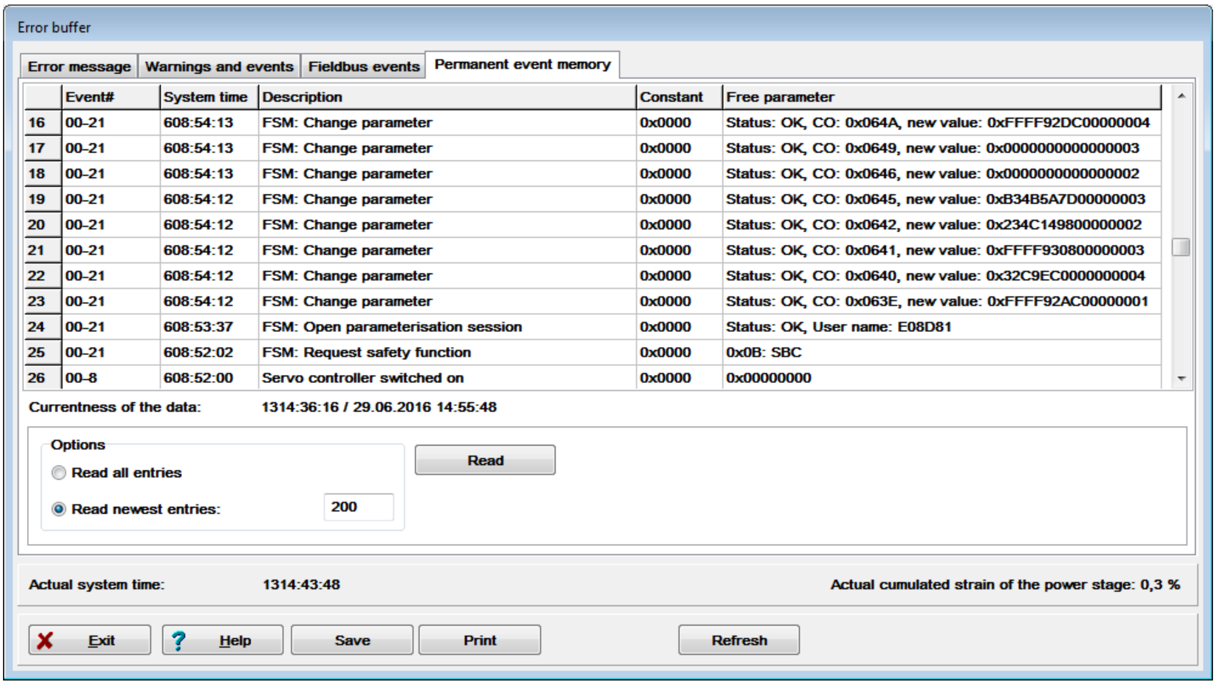


Figure 40: Example of entries in the permanent event memory of the basic unit, with error messages of the safety module

An entry in the permanent event memory contains the following information:

- sequence number
- event number, consisting of the main index and subindex
- system time of the operation hour counter in the servo drive at the time of the event
- description, error or event text
- constant, additional information for the Technical Support
- free parameter, additional information for the Technical Support

If making Support enquiries, please always document the full error information, in particular the diagnostic parameters (constant and free parameter).

The diagnostic parameters contain internal information, for example in which program module and under which conditions the error occurred. This information is intended for the manufacturer and may be of use when solving the problem.

You can read out the entire permanent event memory of the device and export it into a file. The file then contains the entire error history of the device and can be used for troubleshooting and support enquiries.

2.12 Runtime performance

2.12.1 Sampling times

The safety module records the input and output variables at regular intervals.

The variables are recorded at two fixed cycle rates ➔ Table 92.

Cycle	Sampling frequency	Cycle time	Function
TSample	typ. 8 KHz	typ. 125 µs	The cycle is internally synchronised to the control sampling cycle of the basic unit, T_{Sample} range = 100 µs – 200 µs – recording of all inputs and outputs – analysis of the position encoders – filter calculation – generation of the test pulses – internal communication
TLogic	500 Hz	2 ms	Fixed sampling cycle for safety functions – calculation of the safety functions – calculation of the logic functions – finite state machine, error management – signal sequence LIN_x -> VOUT_x

Table 92: Sampling times of the safety module

This means that the recording of the input signals can be affected by a maximum jitter of T_{Logic} + T_{Sample}. Thus an input signal is recorded at best immediately or, at the latest, after 2.125 ms. The start of a safety function can also be affected by this jitter, relative to the input signal. The jitter is taken into account in the specified reaction times of the individual function blocks.

2.12.2 Reaction time on request of a safety function

The reaction time is made up of three components (Figure 41):

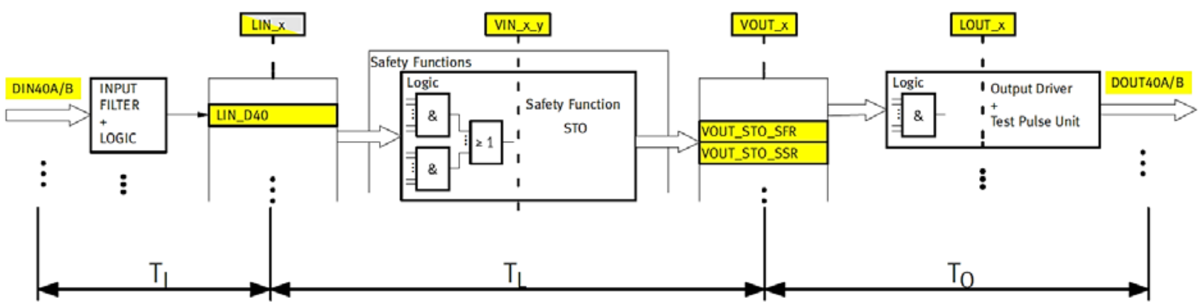


Figure 41: Reaction times of the safety module (schematic diagram, excerpt from Figure 5)

T_I : Time from the signal change at the input to mapping of the input status in the logical input signal LIN_x. The time is dependent upon the settings of the input filters (section 2.4).

T_L : Time for the execution of the safety or logic function of LIN_x to the output of the status in VOUT_x. The time is dependent on the settings of the safety and logic functions, specified in ➔ Section 2.5 and 2.6.

T_O : Time to output the status information VOUT_x to the digital outputs. The time is dependent on the switching delay of the outputs ➔ Section 2.8.

If the output signals VOUT_x lead back to inputs LIN_x, then it should be noted that an additional run-time of T_{Logic} occurs.
Example: Use of the extended logic functions to request a safety function, via the LIN_ALFx_OUT signal.

➔ If possible, safety functions should be requested directly, in order to minimise run-times.

The resulting response time up to the execution of the safety function is made up of:

$$T_{res} = T_I + T_L$$

Example: STO request via DIN40, quick request P02.08 set

Reaction times	**Minimum**	**Maximum**	**Typical**
Specification for T_I for DIN4x from Table 23, Section 2.4.2			
Reaction time for "Quick detection request" = 1 (P02.08/P02.0D/P02.12/P02.17 = 1)	0.5 ms	2.5 ms	1.5 ms
Specification for T_L for STO from Table 32, Section 2.5.3.4			
Reaction time until switch-off of drive supply of basic unit and output stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**3.5 ms**	**7.0 ms**	**5.0 ms**

The time until the status message that the safety function has been requested is calculated from

$$T_{res} = T_I + T_L + T_O$$

Example: SOS request via DIN40, P02.08 =0, P02.04 = 3 ms, P0B.00 = 2 ms

Reaction times	**Minimum**	**Maximum**	**Typical**
Specification for T_I for DIN4x from Table 23, Section 2.4.2			
Reaction time without "Quick detection request" and 3 ms filter time	3.5 ms	5.5 ms	4.5 ms
Specification for T_L for SOS from Table 53, Section 2.5.7			
VOUT_SOS_SSR output with P0B.00 = 2 ms	4.0 ms	4.1 ms	4.0 ms
Specification for T_O via DOUT40 from Table 80, Section 2.9.1.5			
Time delay $T_O = T_s$	0.0 ms	2.5 ms	0.5 ms
Total:	**7.5 ms**	**12.1 ms**	**9.0 ms**

2.12.3 Reaction time on violation of a safety function

The reaction time of the safety module when hazardous movements occur or if a position encoder fails is also made up of three components (Figure 42):

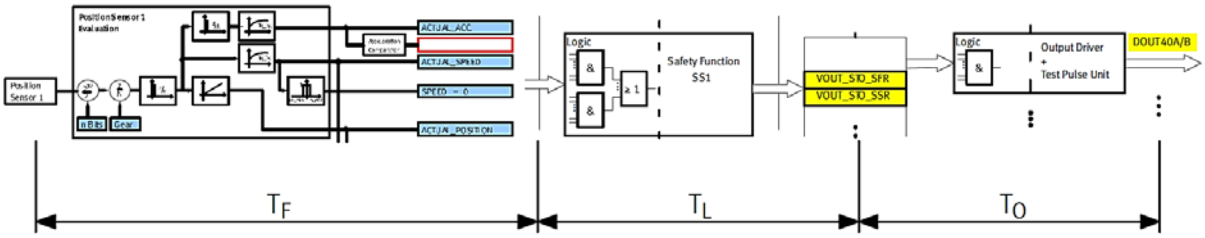


Figure 42: Calculation of the speed and acceleration (schematic diagram, excerpts from Figure 7 and Figure 5)

T_F : Time from the occurrence of the hazardous movement up to mapping in the safety module (filter for speed signals), or time up to the detection of the defective position encoder ➔ Table 13, Section 2.3.4.

T_L : Time for the execution of the safety or logic function of LIN_x, taking into account any allowable times up to the output of the error signal VOUT_xxx_SCV ➔ Section 2.5.

T_O : Time for the output of the status information VOUT_x to the digital outputs. The time is dependent on the switching delay of the outputs ➔ Section 2.8.

Detection of a dangerous movement: The reaction time up to the internal detection of the violation is made up of:

$$T_{res} = T_F + T_L$$

Example: SSF0 safety function, indicated as SLS, allowable time P0E.03 = 4 ms
Encoder configuration with rotational speed filter P06.08 = 8 ms

Reaction times	**Minimum**	**Maximum**	**Typical**
Detection of the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, T_L			
Reaction time, taking the allowable time P0E.03 into account	4.0 ms	6.0 ms	5.0 ms
Total:	**12.0 ms**	**14.1 ms**	**13.0 ms**

Detection of a dangerous movement: The time up to safe output of the status messages indicating that the safety function has been violated is calculated thus

$$T_{res} = T_F + T_L + T_O$$

Example: As above, output via DOUT40

Reaction times	Minimum	Maximum	Typical
Detection of the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, T_L			
Reaction time taking the allowable time P0E.03 = 4 ms into account	4.0 ms	6.0 ms	5.0 ms
Specification for T_O via DOUT40 from Table 80, Section 2.9.1			
Time delay $T_O = T_s$	0.0 ms	2.5 ms	0.5 ms
Total:	**12.0 ms**	**16.6 ms**	**13.5 ms**

Detection of a dangerous movement: The time from the occurrence of a dangerous movement up to the error response (here STO) and up to the safe switch-off of the output stage is calculated thus

$$T_{res} = T_F + T_{L,SSF0} + T_{L,STO}$$

Example: As above, switch-off of the drive via STO error reaction

Reaction times	Minimum	Maximum	Typical
Detection of the dangerous movement T_F			
Signal delay in the rotational speed filter, P06.08	8.0 ms	8.1 ms	8.0 ms
Safety function SS0, TL			
Reaction time taking the allowable time P0E.03 = 4 ms into account	4.0 ms	6.0 ms	5.0 ms
Specification for T_L for STO from Table 32, Section 2.5.1			
Reaction time until switch-off of drive supply of basic unit and output stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**14.5 ms**	**18.6 ms**	**16.5 ms**

Detecting a defective position encoder: The time from the occurrence of an error in the position encoder up to the error response (here STO) and up to the safe switch-off of the output stage is calculated thus

$$T_{res} = T_F + T_{L,STO}$$

Example: Detection of encoder error, switch-off of the drive via STO error reaction

Reaction times	Minimum	Maximum	Typical
Detection of the encoder error T_F			
Error detection in the encoder analysis	10.0 ms	10.1 ms	10.0 ms
Specification for T_L for STO from Table 32, Section 2.5.1			
Reaction time until switch-off of drive supply of basic unit and output stage OFF	2.5 ms	4.5 ms	3.5 ms
Total:	**12.5 ms**	**14.6 ms**	**13.5 ms**

2.12.4 Other times for error detection and communication

Additional time delays / error response times correspond to Table 93.

Description	Time T_F maximum
Safety function is requested, status variables not available Safety condition violated	2 ms
Input: Stuck-At error detected, no test pulse	< 16 s
Output: Stuck-At error detected, no test pulse	< 16 s
Two-channel inputs: Equivalence / antivalence error at the input (discrepancy time)	Parameterisable, typically 100 ms (P02.05, P02.0A, P02.0F, P02.14)
Two-handed control device: Time violation, simultaneity (discrepancy time)	Parameterisable, typically 500 ms (P02.03)
Mode selector switch: Violation 1-of-n (discrepancy time)	Parameterisable, typically 100 ms (P02.01)
RAM error, Flash error, Stack error, CPU error, program sequence error	Depending on error type 2 ms … 8 h
Cross-comparison of data µC1 / µC2 produces errors	< 16 s
Faulty operating voltage: Time between occurrence of error and triggering of the reaction	≤ 2 ms
Digital angle encoders: Communication error, error of 4x cycle (EnDat packets faulty or missing)	≤ 2 ms
Other angle encoder [X2B]: Delay time for transferring the data from the basic unit	≤ 400 µs, typically 250 µs
Determination of the setpoint limits (safety functions control setpoint limits in the servo drive)	≤ 2 ms

Table 93: Other time delays / error response times

2.13 DIP switches

DIP switches are located on the front panel of the safety module. These switches have no safety function. The meaning of the individual switches depends on the technology module used for the fieldbus communication.
The fieldbus communication can be activated/deactivated and a participant address can be set, for example, via the DIP switches.

You can find information on the DIP switch setting in the
➔ product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS.

3 Mounting and installation

3.1 Mounting / removing

The safety module FSM 2.0 – MOV can only be integrated into the servo drives ARS 2000 FS. It cannot be operated apart from the servo drive.

Warning

Danger of electric shock if the safety module is not assembled.

Touching live parts causes severe injuries and can lead to death.

Before touching live parts during maintenance, repair and cleaning work and when there have been long service interruptions:

1. Switch off the power to the electrical equipment via the mains switch and secure it against being switched on again.
2. After switch-off, wait at least 5 minutes for the equipment to discharge before you access the controller.

Note

Incorrect handling can damage the safety module or servo drive.

- Switch off the supply voltage before mounting and installation work. Only switch on the supply voltage when mounting and installation work is completely finished.
- Never unplug the safety module from, or plug it into the servo drive when powered!
- Observe the handling specifications for electrostatically sensitive devices. Do not touch the components and conductive tracks of the printed circuit board or the pins of the manifold rail in the servo drive. Only hold the safety module by the front panel or the edge of the board.

3.1.1 Assembling the safety module

1. Slide the safety module into the guides.
2. Tighten the screws with a torque of 0.4 Nm ± 10%.

Result: The front panel has conducting contact with the housing.

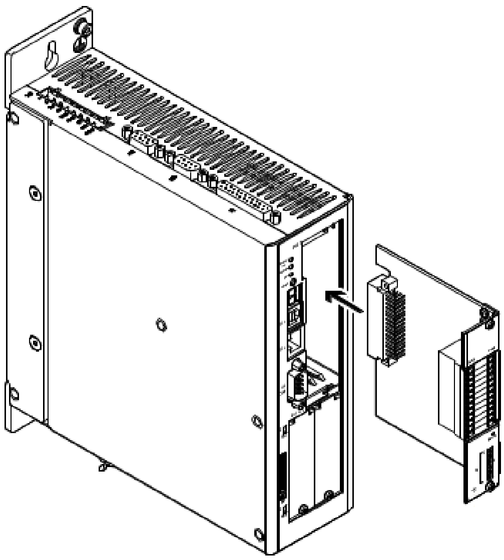


Figure 43: Mounting / removing

3.1.2 Removing the safety module

1. Unscrew the screws.
2. Loosen the safety module by gently prying the front cover or by pulling the mating connector just a few millimetres and pulling it out of the slot.

3.2 Electrical installation

3.2.1 Safety instructions

Warning

Danger of the failure of the safety function!

In mechanical equipment without the impact of external forces, it can always be assumed that a loss of energy will lead to the safety status (idle current principle). This must be shown/confirmed by the danger and risk analysis of the application.

A failure of the safety function can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuator technology.

- ❖ Ensure that your application has a reliable power supply or provide other appropriate measures.

The requirements of EN 60204-1 must be fulfilled during installation. If this is not possible, then fault exclusion can be achieved by using a safety switching device and cross-circuit detection.

Warning

Danger of electric shock from voltage sources without protective measures.

- ❖ For the electric logic supply, use only PELV circuits to EN 60204-1 (Protective Extra-Low Voltage, PELV).
- ❖ Observe the general requirements in accordance with EN 60204-1 for PELV circuits.
- ❖ Use only voltage sources that ensure a reliable electric separation of operating voltage from other active circuits in accordance with EN 60204-1.

Through the use of PELV circuits, protection against electric shock (protection against direct and indirect contact) is ensured in accordance with EN 60204-1. The 24 V power supply unit used in the system must be able to cope with the voltage interruption defined in EN 60204-1.

The cable is connected by means of two plugs. As a result, cables can remain plugged into the sockets when replacing the safety module, for example.

Make sure that no jumpers or the like can be inserted parallel to the safety wiring. For example, use the maximum wire cross section of 1.5 mm or appropriate wire end sleeves with insulating collars.
Use twin wire end sleeves for looping through lines between adjacent equipment.

3.2.2 ESD protection

At unassigned plug connectors, damage can occur to the device or to other system parts as a result of ESD (electrostatic discharge). Earth the system parts before installation and use appropriate ESD equipment (e. g. earthing straps etc.).

3.2.3 Functional earth

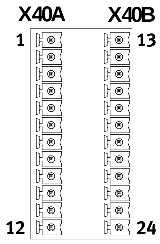
If you are using a screened connecting cable [X40]:
Keep the unscreened part of the cable as short as possible (< 50 mm). For shield connection, use an earthing strip and connect to the earthing screw of the mounting profile (➔ Figure 3 in section 2.1.4).

3.2.4 Connection [X40]

The safety module FSM 2.0 – MOV has a combined interface for control and acknowledgement via the plug connector [X40].

- Design on the device: PHOENIX MINICOMBICON MC 1.5/8-GF-3.81 BK
- Plug (included in scope of delivery): PHOENIX MINICOMBICON MC 1.5/8-STF-3.81 BK

■■■ The mating connector set, consisting of mating connector for X40A and X40B can also be ordered separately.

Plug connector	**Pin**	**Designation**	**Description (factory setting[1])**
	X40A plug connectors		
	1	DIN40A	Digital input 40, two-channel (Factory setting emergency stop switching device, STO and SBC request)
	2	DIN40B	
	3	DIN42A	Digital input 42, two-channel
	4	DIN42B	
	5	DOUT40A	Digital output 40, two-channel
	6	DOUT40B	
	7	DIN44	Digital input 44 (Factory setting brake feedback)
	8	DIN45	Digital inputs 45, 46, 47 (Factory setting mode selector switch)
	9	DIN46	
	10	DIN47	
	11	DIN48	Digital input 48 (Factory setting error acknowledgement)
	12	DIN49	Digital input 49 (Factory setting terminate safety function on rising edge)
	X40B plug connector		
	13	DIN41A	Digital input 41, two-channel
	14	DIN41B	
	15	DIN43A	Digital input 43, two-channel
	16	DIN43B	
	17	DOUT41A	Digital output 41, two-channel
	18	DOUT41B	
	19	DOUT42A	Digital output 42, two-channel
	20	DOUT42B	
	21	C1	Signal contact, relay contacts (Factory setting safe state reached, no safety condition violated) – – Opened: "Safety function not active" – – Closed: "Safety function active"
	22	C2	
	23	GND24	0 V, reference potential for DINx / DOUTx / +24 V
	24	+24 V	24 V output, auxiliary supply, e.g. for safety peripherals (24 V DC logic supply of the servo drive).

1) Function when the device is delivered or after resetting to factory settings (advance parameterisation)

Table 94: Pin allocation [X40]

To ensure the safety functions, the control ports are to be connected in two channels with parallel wiring. For an example, see Figure 44.

3.2.5 Minimum wiring for commissioning [X40]

➔ **Note**

Failure of the safety function!

A failure of the safety function can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuator technology.

❖ Before initial commissioning, clarify which safety functions are required during the commissioning phase, in order to guarantee the safety of the system during this phase as well prior to final delivery.
Usually, at least one safe emergency stop function is required.

i Commissioning according to the EC Machinery Directive is the first intended use of the machine by the end customer. This is the commissioning performed by the manufacturer during mounting of the machine.

If, during the commissioning phase, safety-orientated circuitry is not (yet) required, then the fieldbus activation module FSM 2.0 – FBA can be used. The FSM 2.0 – MOV can only be integrated into the servo drive after the functional commissioning of the axes.

If, during the commissioning phase, only the STO and SBC safety functions are required (emergency stop), then the initial commissioning of the servo drive ARS 2000 FS with the safety module FSM 2.0 – MOV should take place accordingly with minimum wiring in accordance with Figure 44 (➔ Section 3.3.1) with an emergency stop switch (**2**). For this, please use a safety module in the "Delivery status" (it flashes red/green ■ ■ ■ ■ ■), ➔ Section 2.10.2, Table 91). In the delivery status, the STO and SBC safety functions are already prepared.

➔ **Note**

Never bypass safety functions.

Carry out the minimum wiring for initial commissioning in such a way that it must be forcibly removed when the final protection wiring is carried out.

i You can find other wiring examples with a detailed description in the following sections.

3.3 Sample circuits

The following sample circuits each show a single-phase servo drive ARS 2000 FS. For three-phase servo drives, the circuitry of [X9] must be adapted accordingly.

Only one input / switching device is shown. However, all four two-channel inputs can be used to request safety functions.

Note

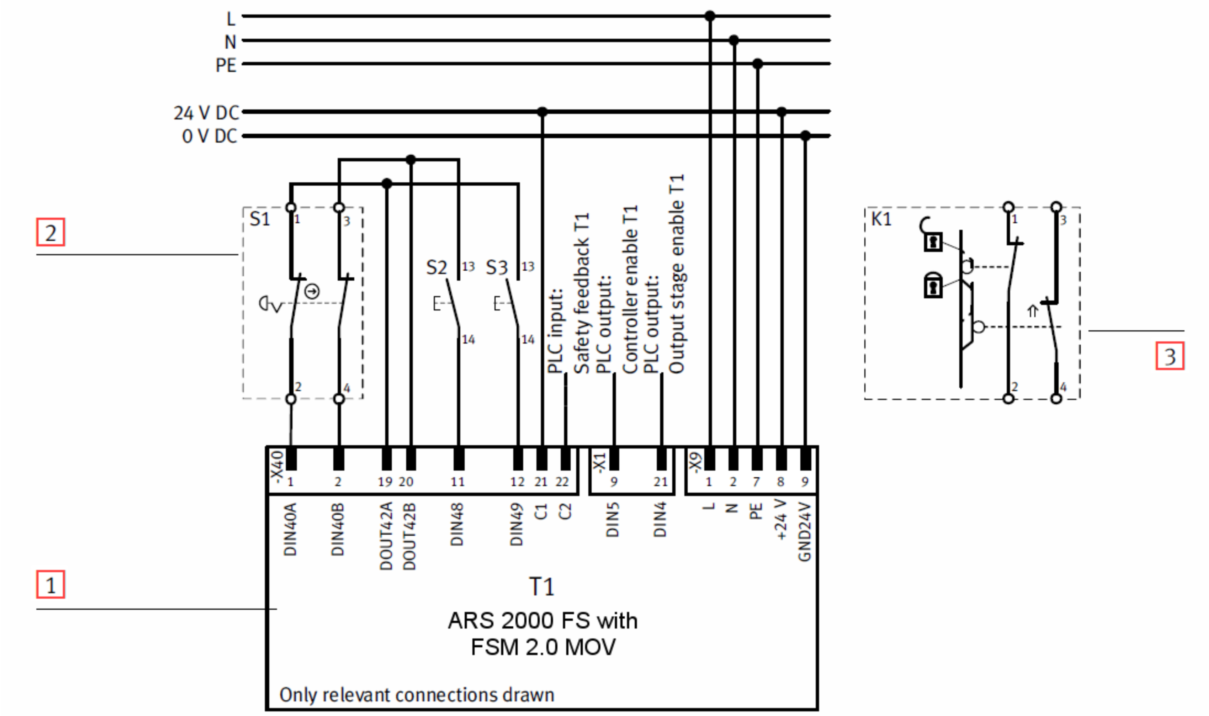
Some of the following sample circuits use passive sensors, such as emergency stop switches, which are monitored using external clock signals. The digital outputs of the safety module should be used as the source for these clock signals. This allows detection of the following errors:

– short circuits between input A and B, in the output circuit (DOUT4x) and in the input circuit (DIN4x)
– shorts of a cable to 0 V or +24 V

Shorts between the input and output of the passive sensor are not detected or only detected on actuation (via discrepancy monitoring). For this reason, preventative measures are required in the system wiring to avoid this error (error exclusion).

3.3.1 Safety request via devices with switch contacts

The safety function (e. g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request. The safety request is sent along 2 channels via the input device S1 and routes to the 2-channel switch-off of the output stage of the servo drive.



1 T1: Servo drive with safety module
(only relevant connections shown)

2 S1: Input device, e.g. emergency stop switch

3 K1: Input device, e.g. safety door

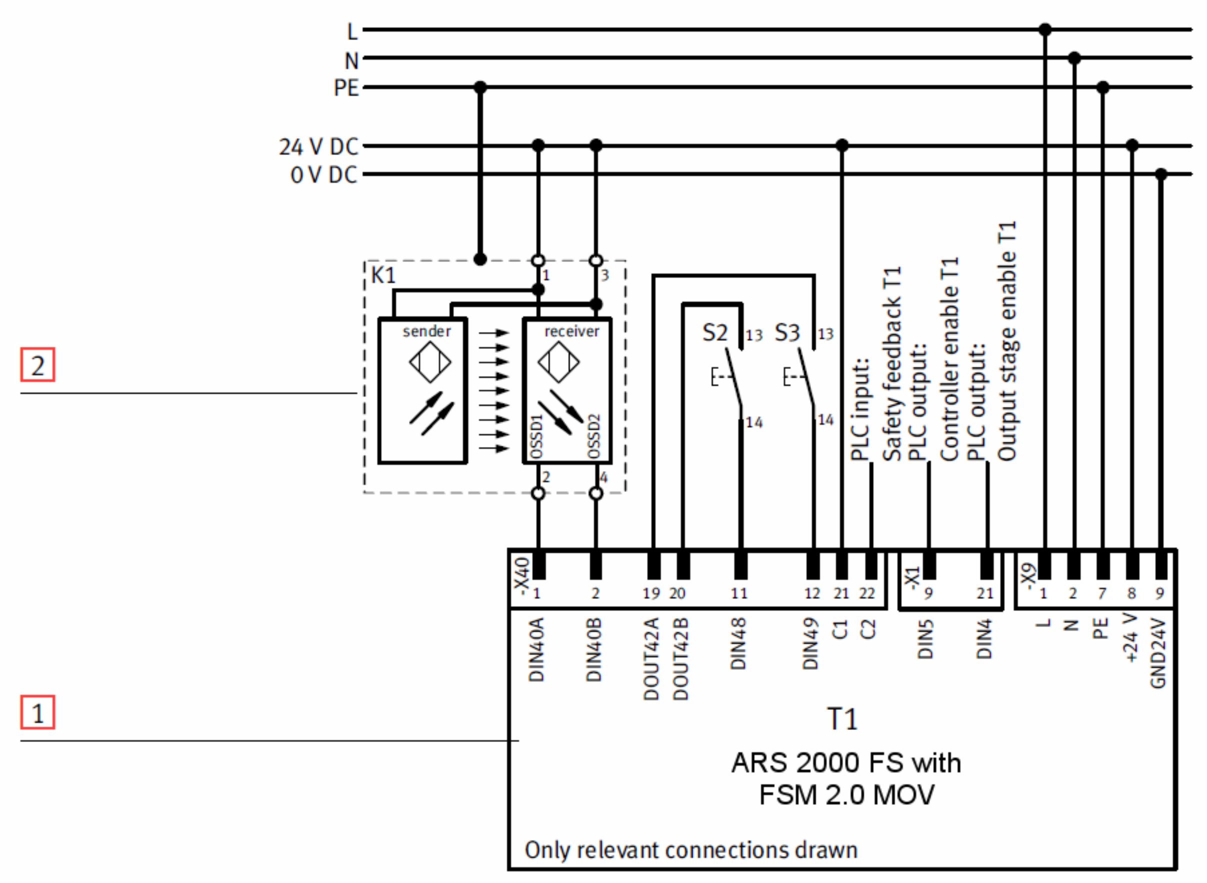
Figure 44: Sample circuit with switch contacts

Notes with regard to the sample circuit:

- In the input circuit for the switches S1 and K1, the safety module FSM 2.0 – MOV detects cross-circuits for the acknowledgement pushbutton S2 and for the Start button S3.
- Actuating the Start button S3 commences the restart.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The acknowledgement contact C1/C2 should be polled via the controller.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required according to the scope of application and the safety concept of the machine.

3.3.2 Safety request via devices with semi-conductor outputs

The safety function can be requested via various devices. Switch 1 can be a light curtain or a safety switching device with semi-conductor outputs. The safety request is sent over 2 channels via switch S1. If the safety function is active, then, in the example, this is output by the potential-free contact C1/C2.



1 T1: Servo drive with safety module (only relevant connections shown)

2 K1: Input device, e.g. light curtain

Figure 45: Sample circuit, device with semi-conductor outputs

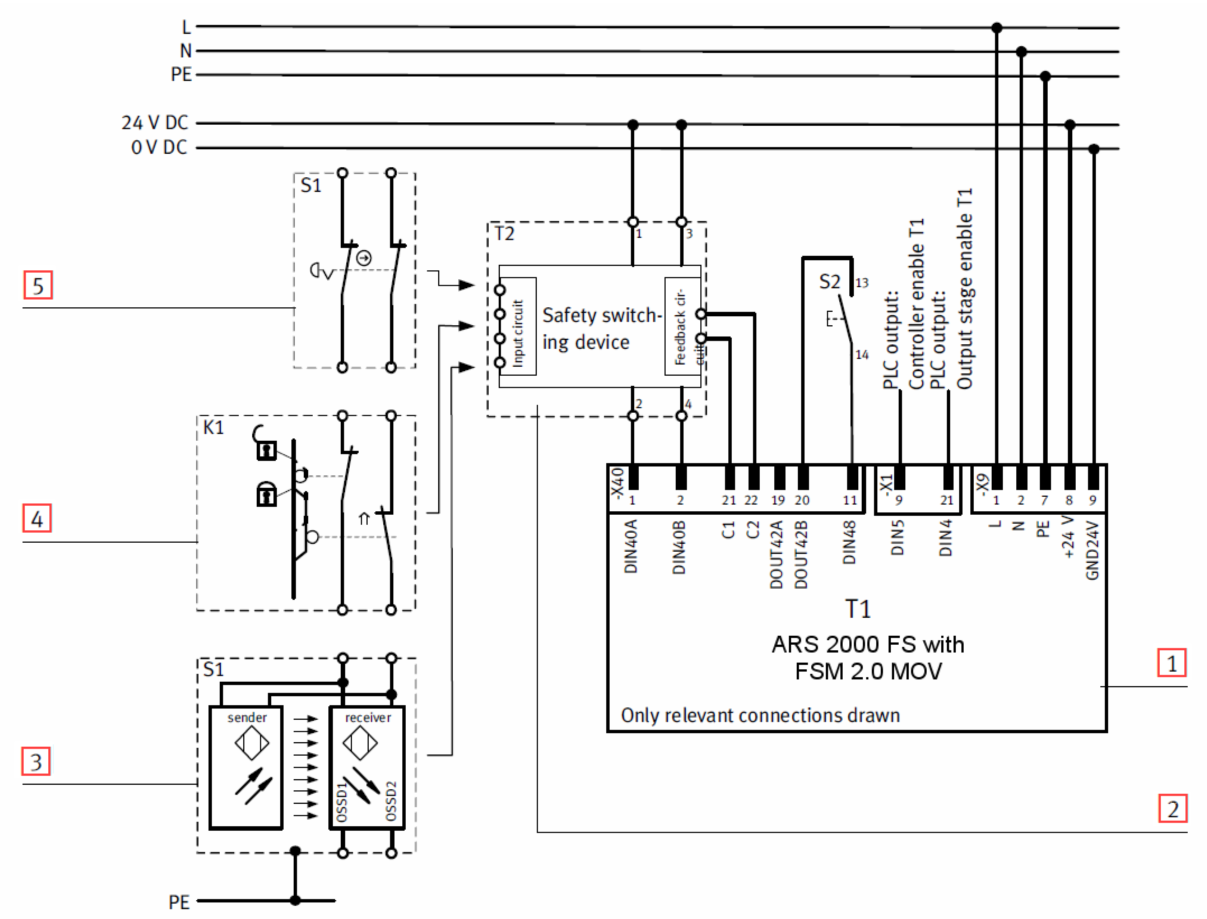
Notes with regard to the sample circuit:

- In the input circuit for the K1 switches, the light curtain K1 detects cross circuits.
- In the input circuit for the Start button S3 and the acknowledgement pushbutton S2, the safety module FSM 2.0 – MOV detects cross-circuits.
- Actuating the Start button S3 and the acknowledgement pushbutton S2 commences the restart.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The acknowledgement contact C1/C2 should be polled via the controller.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required according to the scope of application and the safety concept of the machine.

3.3.3 Safety request via a safety switching device

If more than four safety command devices (S1) are required or if a higher-order safety control is to be used, then the servo drive (T1) can also be activated via other safety command devices.

The safety function can be requested via various devices. The safety request is sent over 2 channels via switch S1 and is analysed by the safety switching device (S2) (safety relay, safety SPS). If the safety function is active, then, in the example, this is output by the potential-free contact C1/C2.



1 T1: Servo drive with safety module (only relevant connections shown)

2 S1: Safety switching device

3 S1: Light curtain

4 K1: Safety door

5 S1: Emergency stop switch

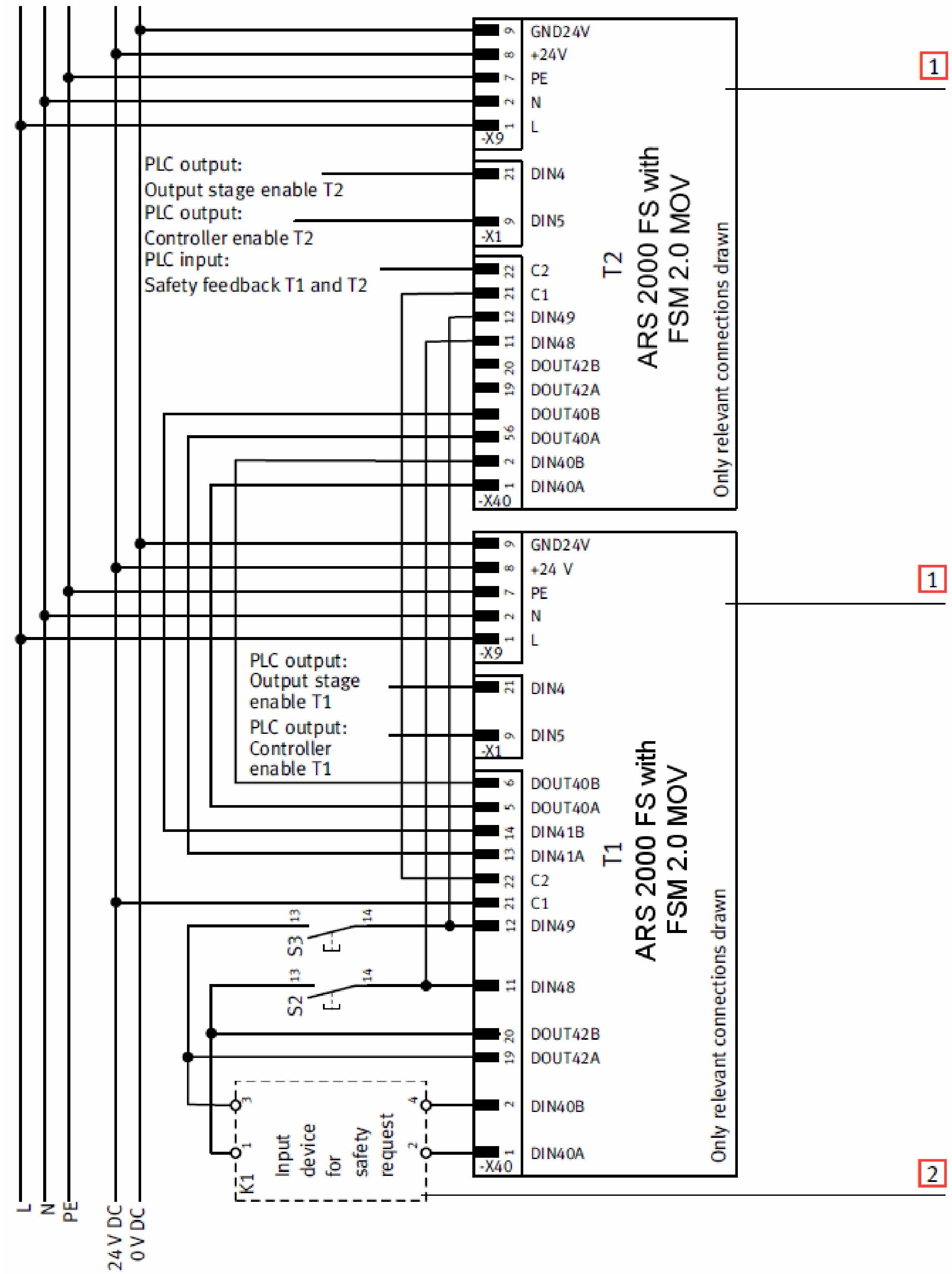
Figure 46: Switching example with safety switching device

Notes with regard to the sample circuit:

- In the input circuit for the S1 switches, the safety switching device T2 detects cross circuits. If a Start button is required for the application, it is also connected to the safety switching device T2. For the acknowledgement pushbutton S2, the safety module FSM 2.0 – MOV detects cross circuits.
- The safety functions in the FSM 2.0 – MOV are parameterised to "Automatic restart after cancellation of request" when an external safety switching device is used.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The acknowledgement contact C1/C2 is included in the return contact of the safety switching device.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required according to the scope of application and the safety concept of the machine.

3.3.4 Linking of multiple ARS 2000 FS with FSM 2.0 – MOV

The safety function is triggered by an input device for the safety request for both servo drives. The safety request is sent along 2 channels via the input device S1 and leads to the 2-channel switch-off of the output stage of the servo drives T1 and T2. If the safe status has been reached in both servo drives, then this is output by the potential-free contact C1-C2 of the servo drives T1 and T2.



1 T1/T2: Servo drive with safety module (only relevant connections shown)

2 S1: Input device for safety request

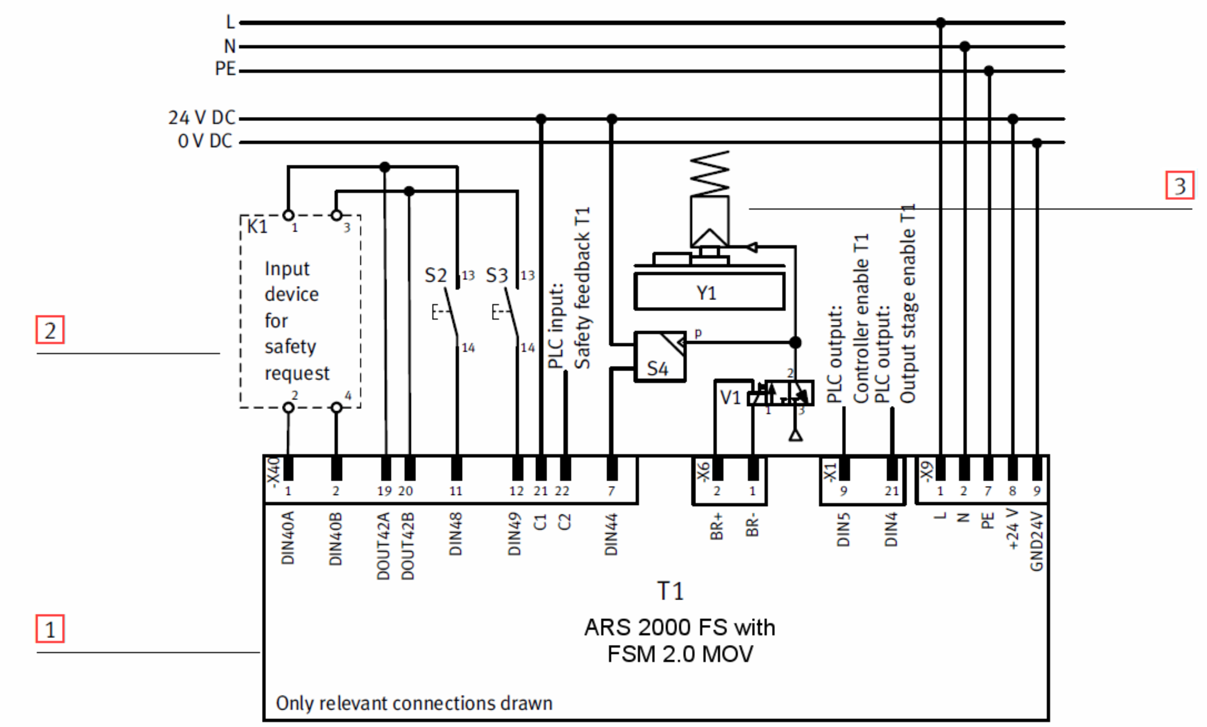
Figure 47: Sample circuit for multiple ARS 2000 FS with FSM 2.0 – MOV

Notes with regard to the sample circuit:

- In the input circuit for the input devices for the safety request S1, the FSM 2.0 – MOV in T1 detects cross-circuits for the acknowledgement pushbutton S2 and for the Start button S3.
- Actuating the Start button S3 commences the restart.
- The servo drive T1 must forward the safety request via DOUT40A/B to the servo drive T2, which then also reacts to the safety request.
- The servo drive T2 must indicate a safety request to the servo drive T1 as feedback.
- The acknowledgement contacts C1, C2 of T1 and T2 are connected in series, and the signal should be polled via the controller. If a safety request has been made, then the controller should react in an appropriate manner (e. g. in the case of SLS, the setpoint values should be reduced, while, in the case of SS1, the servo drive enable should be retracted).
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required according to the scope of application and the safety concept of the machine.

3.3.5 Activating a clamping unit

The safety function (e. g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device that makes the safety request. The safety request is sent along 2 channels via the input device S1 and routes to the 2-channel switch-off of the output stage of the servo drive. At the same time, the clamping unit is activated and monitored.



1 T1: Servo drive with safety module
(only relevant connections shown)

2 K1: Input device for safety request

3 B1: V1/Y1: Valve and clamping unit
S4: Pressure switch to monitor activation of the clamping unit

Figure 48: Sample circuit, clamping unit

Notes with regard to the sample circuit:

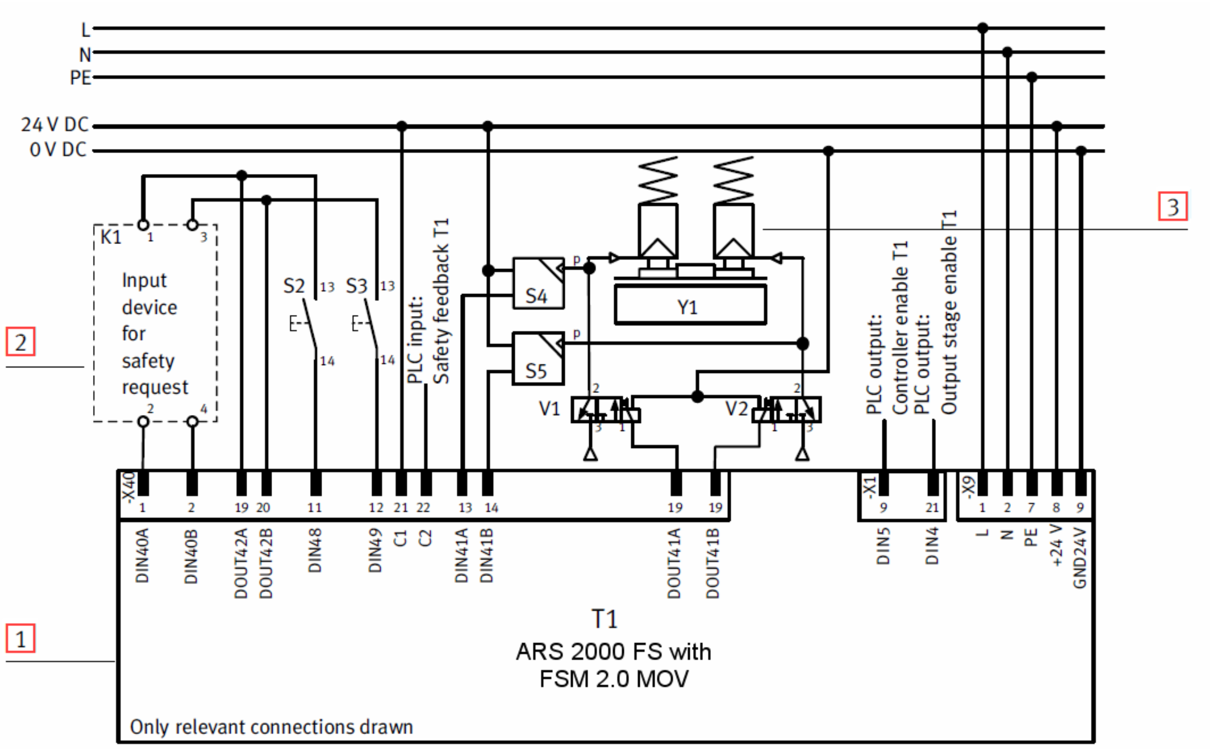
- In the input circuit for the input devices for the safety request K1, the safety module FSM 2.0 – MOV detects cross-circuits for the acknowledgement pushbutton S2 and for the Start button S3.
- Actuating the Start button S3 commences the restart.
- The acknowledgement contact C1, C2 should be polled via the controller. If a safety request has been made, the servo drive enable should be cancelled.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The clamping unit is activated via the BR+/BR- output of the servo drive (T1) and monitored via the switch S4 of the safety module FSM 2.0 – MOV. (Note: Active pressure switches are used for this,

cross-circuit detection with DOUT42 is not possible!). The indirect monitoring shown requires a regular performance test of the clamping unit.

– Monitoring of the clamping unit checks only actuation and not whether the friction value of the clamping unit is high enough for it to still be able to function properly.
– The sample circuit has a single-channel structure in the clamping unit, which is suitable up to category 2 with a performance test of the clamping unit.
– Additional measures are required according to the scope of application and the safety concept of the machine.

3.3.6 Activating a 2-channel clamping unit

The safety function (e. g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request. The safety request is sent along 2 channels via the input device S1 and routes to the 2-channel switch-off of the output stage of the servo drive. At the same time, the clamping units are activated and monitored.



1 T1: Servo drive with safety module
(only relevant connections shown)

2 K1: Input device for safety request

3 V1/V2/Y1: Valves and two-channel clamping unit
S4/S5: Pressure switch to monitor activation of the clamping unit

Figure 49: Sample circuit, 2-channel clamping unit

Notes with regard to the sample circuit:

- In the input circuit for the input devices for the safety request K1, the safety module FSM 2.0 – MOV detects cross-circuits for the acknowledgement pushbutton S2 and for the Start button S3.
- Actuating the Start button S3 commences the restart.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The clamping units are activated via the two-channel output DOUT41A/DOUT41B of the safety module.
- If the valves for the clamping units request more power than DOUT41 can supply, then a suitable relay (with forced contacts and feedback) must be connected between them. Alternatively, it should be checked whether the BR+/BR- output of the servo drive T1 can be used.
- Functioning of the clamping units is monitored by the safety module using the pressure switches S4 and S5 (Note: Active pressure switches are used for this, cross-circuit detection with DOUT41 is not possible!). The indirect monitoring shown requires a regular performance test of the clamping unit.
- Monitoring of the clamping unit checks only actuation and not whether the friction value of the clamping unit is high enough for it to still be able to function properly.
- The sample circuit has a 2-channel structure in the clamping unit, which is suitable up to category 3 with a performance test of the clamping unit.
- Additional measures are required according to the scope of application and the safety concept of the machine.

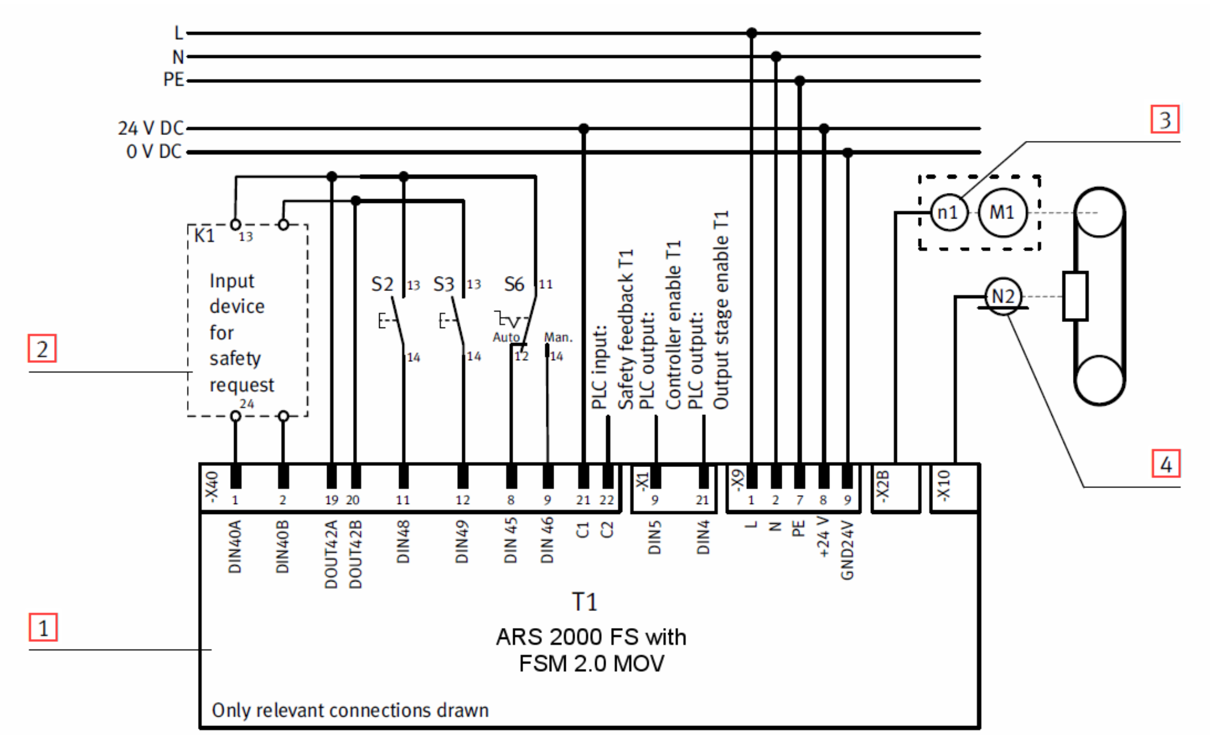
3.3.7 Connection of encoders for dynamic safety functions

The encoder is monitored via the plug connections [X2A], [X2B] and [X10]. Speed and idle monitoring can be carried out, depending on the available incremental or absolute measured values.

In "Automatic" mode, the safety function (e. g. STO – Safe Torque Off or SS1 – Safe Stop 1) is triggered by an input device for the safety request.

The safety function "Safely Limited Speed (SLS)" is requested using the mode selector switch S6 in the "Manual" position.

The safety request is sent along 2 channels via the input device S1 and routes to the 2-channel switch-off of the output stage of the servo drive. Once the output stage has been switched off, it is output by the floating contact C1/C2 of the servo drive.



1 T1: Servo drive with safety module (only relevant connections shown)

2 K1: Input device for safety request

3 n1: Encoder n servo motor to X2B

4 n2: Encoder to X10

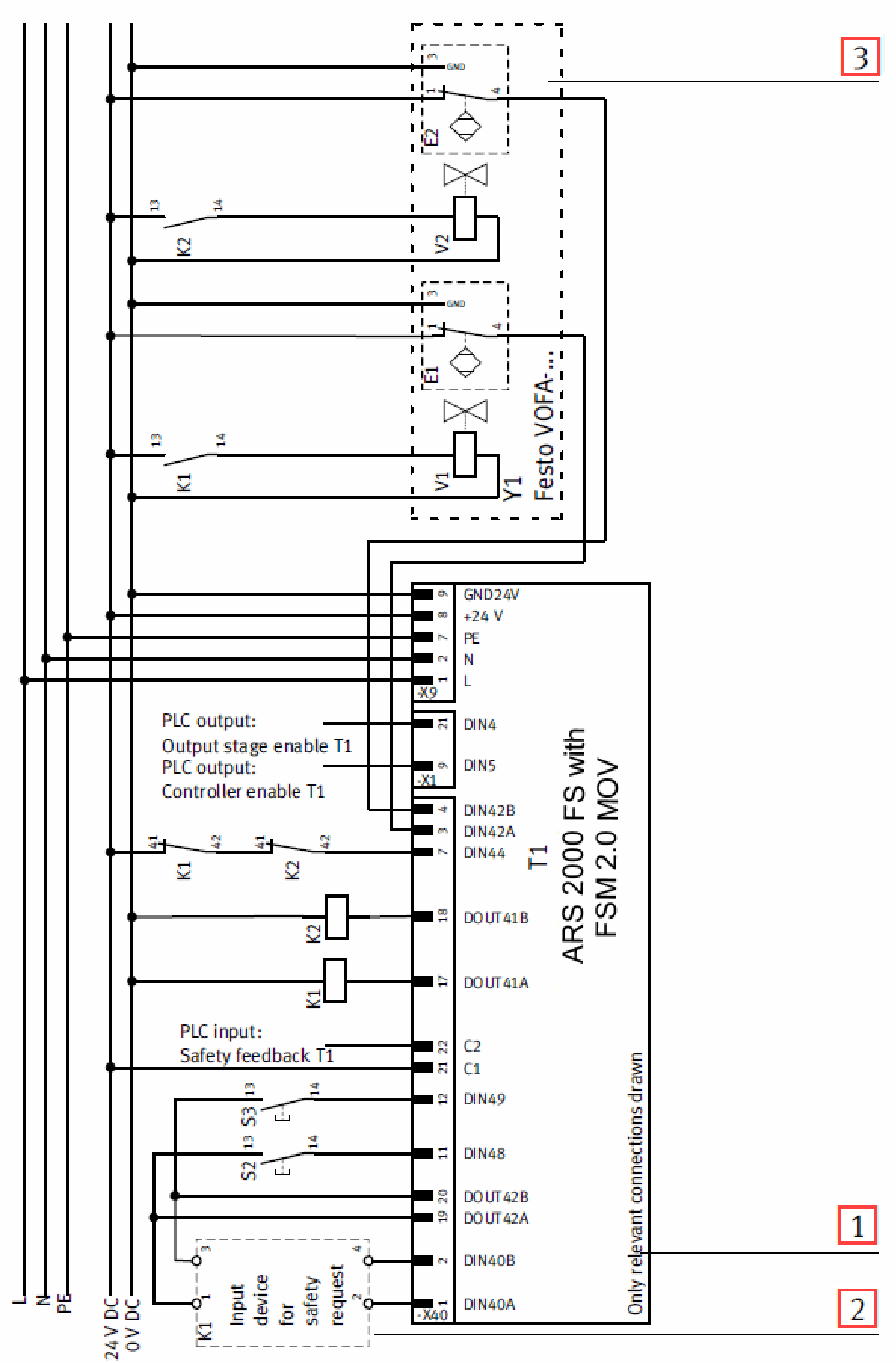
Figure 50: Sample circuit of an encoder for dynamic safety functions

Notes with regard to the sample circuit:

- The encoders must be suitable for safety-orientated applications.
- Encoders with purely incremental signals can be used to safely monitor speed (SLS, SSR, SS1, etc.). Such encoders can also be used for idle-position monitoring with SS2 and SOS.
- In the input circuit for the input devices for the safety request K1, the safety module FSM 2.0 – MOV detects cross-circuits for the acknowledgement pushbutton S2, for the Start button S3 and for the mode selection switch S6.
- Actuating the Start button S3 commences the restart.
- The acknowledgement contact C1, C2 should be polled via the controller. If a safety request has been made, the servo drive enable should be cancelled.

3.3.8 Activation of a 2-channel valve control block with safety functions

The safety function (e. g. for the servo drive STO – Safe Torque Off or SS1 – Safe Stop 1; for the valve control block Safe Venting or Safe Reversing) is triggered by an input device which makes a safety request for the servo drive and the control block with safety function. The safety request is sent along 2 channels via the input device S1 and routes to the 2-channel switch-off of the output stage of the servo drive and the control block.



1 T1: Servo drive with safety module (only relevant connections shown)

2 K1: Input device for safety request

3 Y1: Two-channel control block

Figure 51: Sample circuit of a 2-channel control block with safety functions

Notes with regard to the sample circuit:

- In the input circuit for the K1 contacts, the safety module FSM 2.0 – MOV detects cross-circuits for the acknowledgement pushbutton S2 and for the Start button S3.
- Actuating the Start button S3 commences the restart.
- If the safety module FSM 2.0 – MOV detects a violation of a safety condition or an error is pending, e. g. in the connection wiring, it will indicate a malfunction. The error is acknowledged via the acknowledgement pushbutton S2.
- The inputs DIN42A/B must be configured in such a way that they monitor the switching on and off of the control block V1. Series connection to the protective contacts 41/42 of the contactors K1 and K2 is not possible, as this is not possible with the inductive proximity switches used.
- The acknowledgement contact C1, C2 should be polled via the controller. If a safety request has been made, the servo drive enable should be cancelled.
- The input circuit has a 2-channel structure, which is suitable for category 4.
- Additional measures are required according to the scope of application and the safety concept of the machine.

4 Commissioning

This chapter describes the commissioning of the safety module. You can find information on commissioning the servo drive here:

➔ Product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS

➔ Online help of the parameterisation program Metronix ServoCommander®

Note

Commissioning in the sense of this document does not mean the first intended use by the end customer, but commissioning by the machine manufacturer when setting up the machine.

Note

Failure of the safety function!

Missing safety functions can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuator equipment.

- ❖ Operate the safety module only:
  - if it is installed,
  - after the safety module has been completely parameterised,
  - when all safeguarding, including the safety function, has been installed and checked for functionality.
- ❖ Validate the safety function to complete commissioning ➔ Section 4.8.

Incorrect wiring, use of an incorrect safety module or external components that were not selected according to the category will result in failure of the safety function.

- ❖ Carry out a risk analysis for your application and design the circuitry and components accordingly.
- ❖ Note the examples ➔ Section 3.3.

4.1 Prior to commissioning

Carry out the following steps in preparation for commissioning:

1. Ensure that the safety module is correctly mounted (➔ Section 3.1).
2. Check the electrical installation (connecting cable, pin allocation, ➔ section 3.2). Are all protective conductors connected?

4.2 DIP switch settings

The DIP switches for activating and controlling the bus configuration are located on the safety module. The functionality of the DIP switches is identical for all modules in the FSM slot and is dependent on the bus interface used.

Set the DIP switches as described in the documentation of the servo drives ARS 2000 FS or the corresponding bus-specific documentation, see
Table 2, page 23.

4.3 Parameterisation with the Metronix ServoCommander®

The servo drive must be completely parameterised with the parameterisation software Metronix ServoCommander® (MSC) prior to the parameterisation of the safety module using the SafetyTool.

The following sections provide some information on what to look for when working with the safety module.

You can find additional information on commissioning with the MSC in the online help of the Metronix ServoCommander® or in the ➔ product manual ARS 2100 FS or ARS 2302 – ARS 2310 FS.

Functional safety depends on modifications being traceable. To guarantee this, the specifications for module type, serial number and version are stored in the functional safety module FSM 2.0. These data are stored in the ARS 2000 FS basic unit as comparison values, enabling a modification to the components to be detected.

When a modification is detected, for example a module replacement, a non-acknowledgeable error is triggered. To be able to place the application with the servo drive back in operation, the modification must be "projected". That means, that the modification must be explicitly accepted or confirmed. With the functional safety modules FSM 2.0 – MOV, FSM 2.0 – STO and FSM 2.0 – FBA, these traceable modifications relate to a module replacement.

The project set-up is performed in the **Safety module** window of the Metronix ServoCommander®, see section 4.3.3 "Safety module" window.

The parameterisation software Metronix ServoCommander® (MSC) has been expanded for the operation of the servo drives of the ARS 2000 FS series with a functional safety module.

The main additions are:

- ❖ Indication of the type of the functional safety module FSM 2.0
- ❖ Status indication of the state machine of the firmware of the ARS 2000 FS basic unit
- ❖ Functions for the project set-up of the combination of an FSM 2.0 functional safety module and an ARS 2000 FS servo drive
- ❖ Support of the specified warnings and error messages

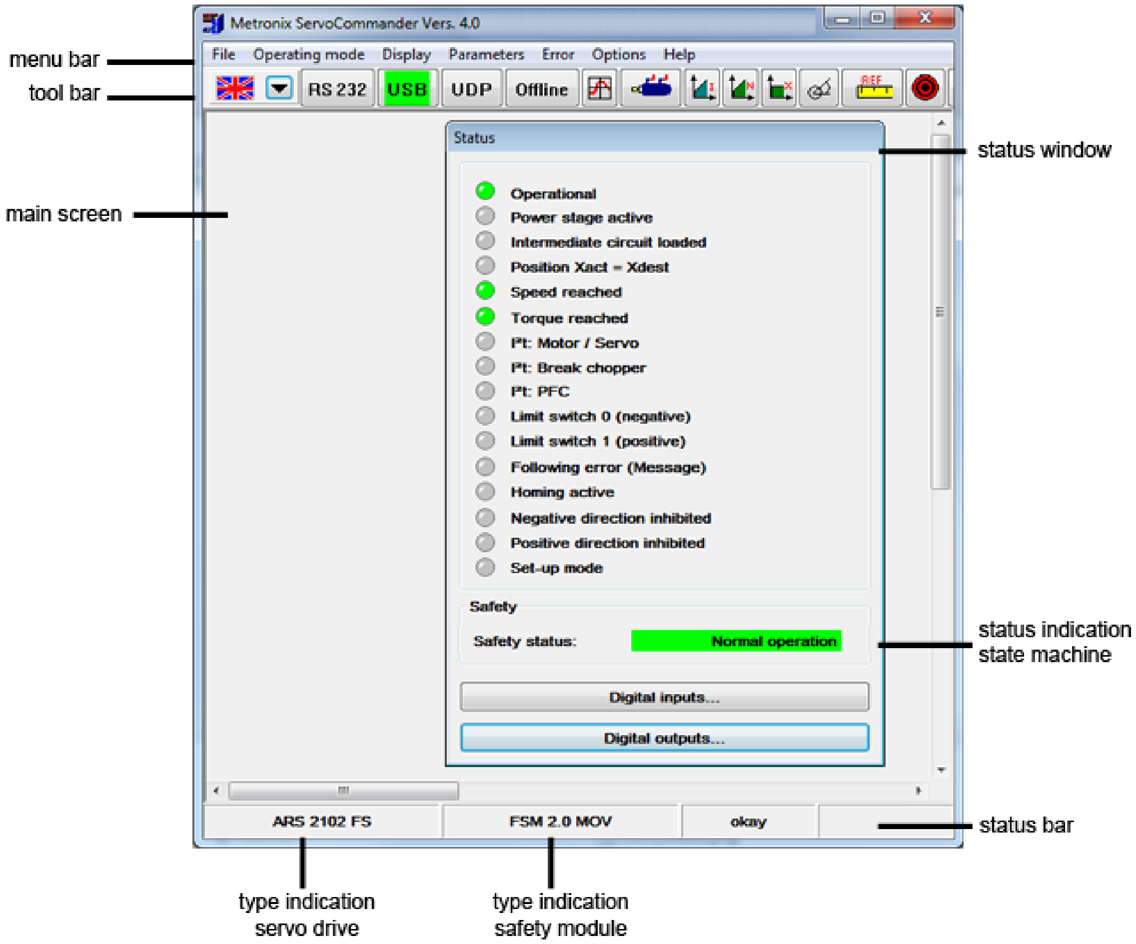


Figure 52: Indication of the type of safety module and extended status window

4.3.1 Indication of the type of servo drive and safety module

At the lower edge of the MSC main screen, there is a **status bar**. It indicates the type of servo drive and functional safety module FSM 2.0, see Figure 52.

In addition, the type, serial number, and revision are displayed in the **Safety module** window, see section 4.3.3.

4.3.2 Status indication of the state machine

The **status window** (i.e. the window that is permanently displayed in the online mode) has been extended by the **status indication of the state machine**. It shows the status of the functional safety in the firmware of the ARS 2000 FS basic unit, see Figure 52.

It is not a representation of the status of the FSM 2.0 – MOV safety module itself. It indicates the status of the state machine in the ARS 2000 FS. Regardless of the indication, the power output stage of the ARS 2000 FS may have already been switched off safely by the functional safety module FSM 2.0 – MOV, see also section 4.3.3.2 Status LEDs.

In addition, the status of the internal state machine is indicated in the **Safety module** window, see section 4.3.3 .

4.3.3 "Safety module" window

For the operation of the ARS 2000 FS servo drives with a functional safety module, the window **Safety module** has been added to the Metronix ServoCommander® parameterisation software.

This window can be opened either via the menu **Parameters – Functional safety – Safety module** or via the **Safety** button in the quick-access toolbar below menu bar, see Figure 53.

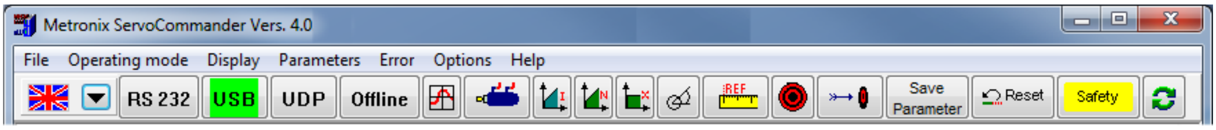


Figure 53: Quick-access toolbar with the "Safety" button

In order to emphasise its importance in view of the functional safety, the **Safety** button is yellow.

The appearance of the **Safety module** window depends on the functional safety module that is connected.

Figure 54 shows this based on the example of the two module types FSM 2.0 – FBA and FSM 2.0 – MOV.

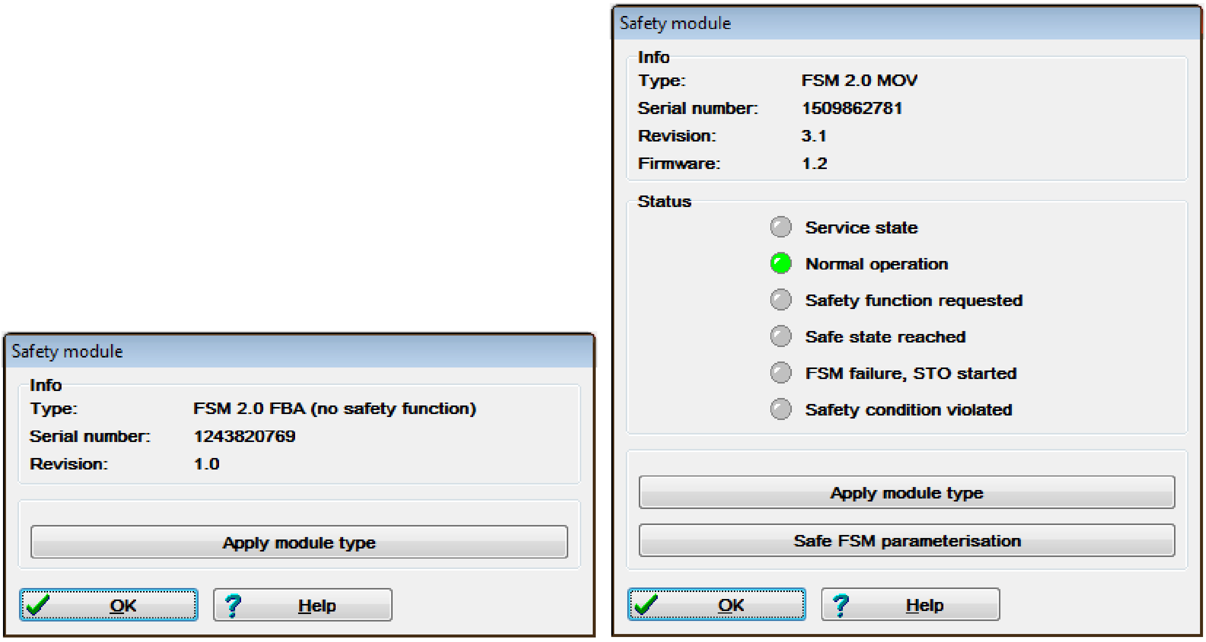


Figure 54: "Safety module" window for FSM 2.0 – FBA (left) and FSM 2.0 – MOV (right)

The "Safety module" window has several areas:

4.3.3.1 Info

This field displays the device data that have been stored in the functional safety module during the commissioning process at the factory.

- **Type:**

  The exact type name, e.g. "FSM 2.0 – MOV".

- **Serial number:**

  The serial number is assigned during production. It is stored on the module. The serial number is unique for a product of the corresponding type.

- **Revision:**

  The revision number of the hardware.

- **Firmware:**

  The version number of the firmware that is currently loaded in the safety module.

A firmware update can only be performed by Metronix!

For further information on the parameterisation program and servo drive, please refer to the window **Help / About**.

4.3.3.2 Status LEDs

The status LEDs indicate the operating status of the FSM 2.0 - MOV in accordance with Table 95. If all of the LEDs are "grey", the functional safety module is not initialised/ready.

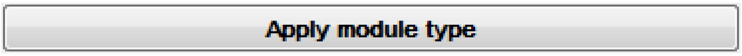
Status display	Meaning	State
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	All LEDs off: The functional safety module is not initialised/ready.	--
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	Die LED **Service state** flashes green: The safety module must be parameterised. The current parameter set of the module is invalid, the module is beeing parameterised, or the module is still in the delivery status.	VOUT_SERVICE
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	The LED **Normal operation** lights green: The functional safety module is initialised in an error-free manner and ready for operation. No safety function has been requested.	VOUT_READY
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	The LED **Safety function requested** flashes yellow: At least one safety function has been requested, but the safe state has not been reached yet.	VOUT_SFR
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	The LED **Safe state reached** lights yellow: At least one safety function has been requested, the "safe state" has been reached for all of the requested safety function, and there is no internal error.	VOUT_SSR
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	The LED **FSM failure, STO started** flashes red: The safety module has detected an internal error.	VOUT_ERROR

Status display	Meaning	State
○ Service state ○ Normal operation ○ Safety function requested ○ Safe state reached ○ FSM failure, STO started ○ Safety condition violated	The LED **Safety condition violated** lights red: At least one safety condition has been violated.	VOUT_SCV
Further information concerning the status of the safety module can be found in ➔ section 2.10.2, Table 91. Further information concerning the status of the safety function can be found in ➔ section 2.5.		

Table 95: Meaning of the LEDs for status indication in the "Safety module" window

4.3.3.3 Button "Apply module type"

In the lower part of the **Safety module** window, there is the button **Apply module type**:



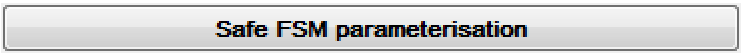
Click this button in order to confirm a module replacement. As a result, the functional safety is parameterised or projected. An existing error message due to a module replacement will not be generated again after Save & Reset.

The following rules apply to a module replacement:

- it is always possible to replace an FSM 2.0 – FBA module with an FSM 2.0 – FBA module.
- a module replacement of FSM 2.0 – STO with another FSM 2.0 – STO does not normally need confirmation.
  Exception: The version check in the basic device shows that the modules are incompatible – error message 51-3 – meaning that the module change must be confirmed.
- when a module type is replaced with another type – error message 51-2 – the module replacement must always be confirmed.
- when an FSM 2.0 – MOV is replaced with an FSM 2.0 – MOV – error message 51-6 – the module replacement must also always be confirmed.

4.3.3.4 Button "Safe FSM parameterisation"

In the lower part of the **Safety module** window, there is the button **Safe FSM parameterisation**:



This button starts the SafetyTool for the parameterisation of the safety module. The selection of the safety functions, the assignment of the I/Os, and the request of the safety functions via inputs and other conditions are configured using the SafetyTool.

Note

- The servo drive must be completely parameterised with the Metronix ServoCommander® (MSC) software prior to the parameterisation of the safety module using the SafetyTool!
- Before starting the SafetyTool, you must load and back up the hardware configuration and any specified display units in the servo drive. This is necessary for data transfer in the SafetyTool.

4.3.4 Setting the encoder configuration

Safe monitoring of speed, e.g. for SLS, and position, e.g. for SOS, requires corresponding sensors for position detection.

Information on the required encoders is provided in section 2.2.5. Refer to Table 10 with the approved encoder combinations.

Specify the first encoder via the menu **Operating mode/Encoder selection**. In this menu, the user can define the angle encoder used to supply the information concerning the commutation position, actual speed value, and actual position value.

Select the interface of the second encoder also via the menu **Operating mode/Encoder selection**.

Then, you must configure the encoder in the appropriate tab of the selected interface in the menu **Parameters/Device parameters/Angle encoder settings**.

4.3.5 Specifying the display units

The display units in the Metronix ServoCommander® software are defined by the following settings:

- selection of the axle – rotatory or translatory application:
  Menu **Parameters/Application parameters/General configuration**
- Specification of the display unit – metric units, number of decimals:
  Menu **Options/Display units**.

4.3.6 Displaying the permanent event memory of the servo drive

To display or save the permanent event memory, activate the menu **Error/Error buffer** in the Metronix ServoCommander®.

Then, select the tab **Permanent event memory**.

The following illustration shows some entries as an example:

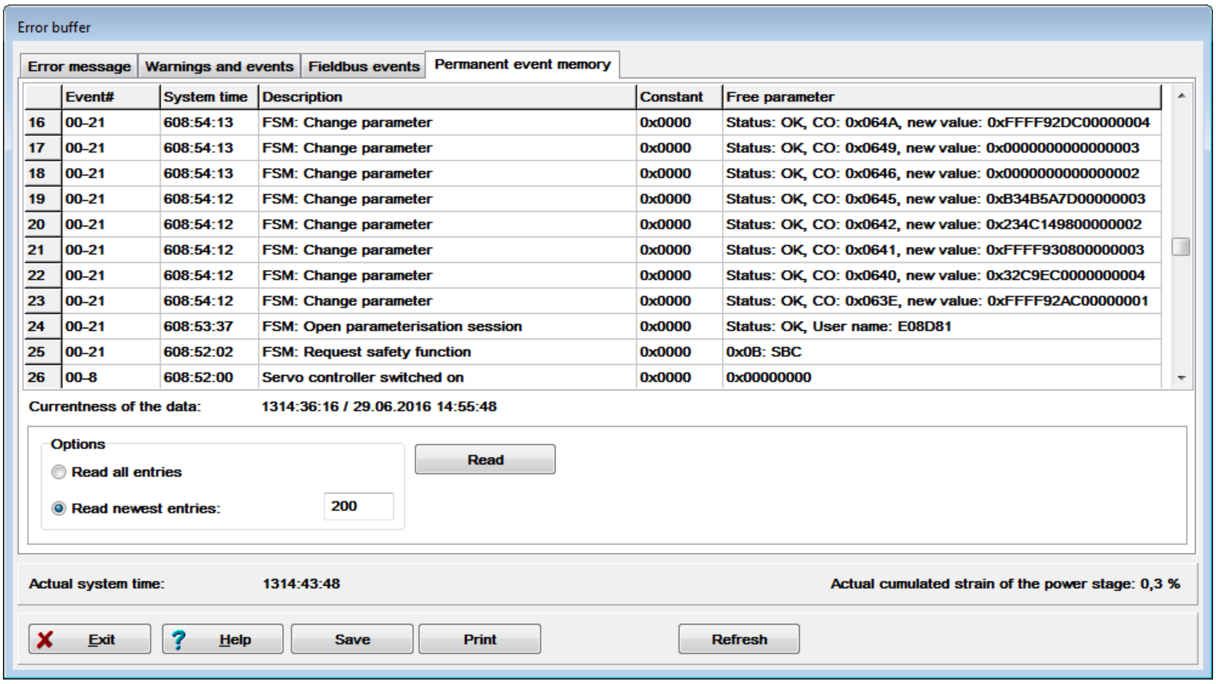


Figure 55: Example of entries in the permanent event memory

To make all entries visible, select the option **Read all entries** and click on the button **Read** to read the entire permanent event memory. This can take a few minutes.

The input field for the number of entries will be updated. The number of the entries actually read may differ because some entries are saved as two entries internally but they are displayed as one entry by the MSC program.

To see just the newest entries, select the option **Read newest entries**, enter the desired number of entries to be displayed into the input field on the right side and then click on the button **Read**. Now, the specified number of entries in the permanent event memory is read and displayed in chronological order, the newest entry first.

The content of the event memory is displayed in tabular form:

Column	Explanation
No.	Consecutive number of the entry.
Event number	Number of the error, warning, or event ➔ see section 5.5.3.
System time	Time of the event in the format <hh>:<mm>:<ss> (operating hours counter, duty cycle of the logic supply).
Description	Name of the entry, error text.
Constant	Additional information for the Technical Support
Free parameter	Additional information for the Technical Support

Table 96: Permanent event memory

Below the table, the field **Currentness of the data** indicates the exact time at which the data has been read from the servo drive (operating hours counter of the servo drive plus date and time of the computer).

On the left-hand side below the options for reading out the entries, you see the **Actual system time**. This is the current value of the operating hours counter of the servo drive. On the right-hand side, you also see the **Actual cumulated strain of the power stage**.

Further information on the entries in the permanent event memory:

- The entries are made chronologically, the topmost entry is the latest entry.
- Minor deviations of the time stamp after Power OFF/ON are possible as the time stamp is saved in a non-volatile manner only once per minute by the servo drive.

Use the button **Save** in order to save the content in the csv format with ';' as the field separator or in the txt format.

Use the button **Print** to print the entries in the form of a table.

The list of errors / events is not refreshed automatically. If required, click the button **Refresh**.

4.4 Basic principles of parameterisation of the safety module

4.4.1 Factory setting

For simplified parameterisation, in the delivery status, or after the factory setting is reset, some functions are activated and standard values are preset.

Table 97 offers an overview of the most important settings.

Page	Factory setting		Allocation
Digital inputs			
DIN40	Sensor type:	Emergency stop switching device	STO and SBC request
	Operating mode:	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN41	Sensor type:	Not defined	Not used
	Operating mode:	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN42	Sensor type:	Not defined	Not used
	Operating mode:	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN43	Sensor type:	Not defined	Not used
	Operating mode:	Equivalent	
	Discrepancy time:	100 ms	
	Source for test pulse:	None	
DIN44	Sensor type:	Brake feedback	Not used
	Source for test pulse:	None	
DIN45	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN46	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN47	Sensor type:	Mode selector switch	Not used
	Source for test pulse:	None	
DIN48	Sensor type:	Fault acknowledgement	Fault acknowledgement request
	Source for test pulse:	None	
DIN49	Sensor type:	Terminate safety function	Rising edge: Terminate STO, SS1 and SBC
	Source for test pulse:	None	
Safety functions			
STO	Request:	DIN40	–
	Automatic restart:	No	
	Automatic activation of SBC:	Yes	
	Terminate request:	DIN49, rising edge	

Page	Factory setting		Allocation
SS1	Request:	No allocation	Not used
	Quick stop ramp:	Yes	
	Automatic restart:	No	
	Automatic activation of SBC:	Yes	
	Terminate request:	DIN49, rising edge	
SS2	Not activated		–
SOS	Not activated		–
USF...	Not activated		–
SBC	Request:	DIN40	–
	Feedback, holding brake:	No	
	Automatic restart:	No	
	Deactivate 24 hr cyclical test:	No	
	Terminate request:	DIN49, rising edge	
Logic functions			
Mode selector switch	Not activated		–
Two-handed operator unit	Not activated		–
ALF...	Not activated		–
Logic error acknowledgement			
Logic error acknowl-edgement	Request:	DIN48	–
Digital outputs			
DOUT40	Request:	No allocation	–
	Operating mode:	Equivalent	–
DOUT41	Request:	No allocation	–
	Operating mode:	Equivalent	–
DOUT42	Request:	No allocation	–
	Operating mode:	Permanently switched on	–
Internal brake	Request:	SBC requested	–
	Operating mode:	Equivalent	–
Signal contact C1/C2	Request:	Safe state reached and no safety condition violated	–
Error management			
Error manage-ment	Safety condition violated: Various other	SBC + STO	Observe and check additional settings.
	Other serious errors:	SBC + STO + outputs = 0	

Table 97: Factory setting

4.4.2 Delivery status

From the factory, you receive the safety module in the so-called "delivery status".

This is indicated by the green and red flashing LED as well as corresponding status messages (➔ Section 2.10.2, Table 91).

Special features of the delivery status in comparison to the factory settings:

– The safety module is "validated as a whole" with the parameterisation of the factory setting and is thus operational. The servo drive can be commissioned, and the output stage and controller enable can be set.
– All error messages due to a different parameterisation of the basic unit and safety module are suppressed.

Hence, you can perform basic commissioning of the servo drive independently of complex safety-related peripherals. For example, the safety module is parameterised to "Resolver" in the delivery status. If other encoders are used, the servo drive could not be commissioned without suppressing the error message of the safety module.

The user cannot restore the delivery status. Only the factory settings can be restored.

4.4.3 Metronix ServoCommander® and SafetyTool

Basic commissioning of the servo drive takes place using the corresponding parameterisation program Metronix ServoCommander® (MSC).

It contains the specification of the hardware configuration, such as the connected motor, the measuring systems, the axis and the technology modules and the safety module installed in the slots.

Parameterisation of the safety module is then performed with special software, the SafetyTool. The SafetyTool is opened via the Metronix ServoCommander®.

➔ **Note**

Before starting the SafetyTool, you must load and back up the hardware configuration and any specified display units in the servo drive ➔ Section 4.3.

This is necessary for data transfer in the SafetyTool.

4.5 Safe parameterisation with the SafetyTool

4.5.1 Starting the program

When the Metronix ServoCommander® is active, start the SafetyTool. There are two ways to do so:

❖ Select the menu **Parameters/Functional safety/Safe FSM parameterisation**.

or

❖ Open the **Safety module** window via the menu **Parameters/Functional safety/Safety module** or by way of the button **Safety** in the toolbar. Then, click **Safe FSM parameterisation**:

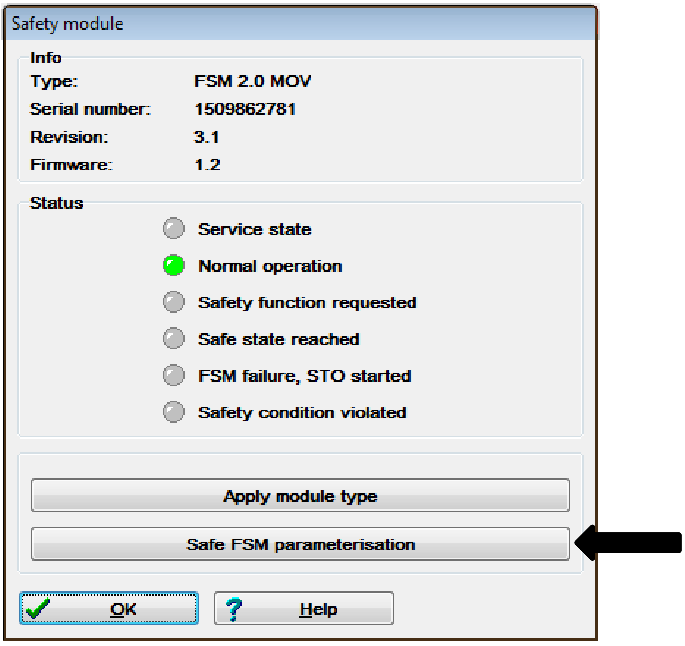


Figure 56: Starting the SafetyTool

4.5.2 Selection of the session types - Configuration wizard

In both session types (online/offline) the SafetyTool is an offline software tool as defined by EN 61508 for installation and commissioning (Phase 12). In addition, the SafetyTool provides support during validation (Phase 13), during which a corresponding protocol can be created using the parameterised functions of the safety module. It is not possible to change parameters during active operation. When an online parameterisation session is started, the safety module switches to the safe status (STO + SBC). It is the duty of the machine manufacturer or machine operator to validate the functions.

The SafetyTool supports 2 session types:

– **Online: Working on the safety module.**

  The SafetyTool communicates with the target system (the safety module).
  You can observe the safety module and read the parameters, you can change individual parameters or transfer a complete safe parameter set.
  Before you change the parameters, the safety module switches to the "Safe basic status". The parameters must be validated before the safety module leaves the "Safe basic status". Changed parameters do not take effect immediately and do not become active until after full validation and restart.

– **Offline: Working on a local file.**

  The SafetyTool **does not** communicate with the target system (the safety module).
  However, you can create and save a preliminary parameterisation for the safety module.

When you start the program, the SafetyTool supports you by displaying the **Configuration Wizard for safe parameterisation**. Select the desired session variant.

Session type	**Session variant**	**Description**
Online ➔ Section 4.5.3	Start new parameterisation	Opens a new project with the standard parameters from the safety module.
	Start new parameterisation with existing project1)	Opens a new project, based on a locally-saved project file.
	Display parameterisation	Displays the parameterisation in the safety module (read-only!).
	Change existing parameterisation	Loads the parameterisation in the safety module for editing.
	Transfer safe parameter set	Transfers a previously-saved safe parameter set to the safe module.
Offline ➔ Section 4.5.4	Create a new project	Opens a new project with the standard settings of the SafetyTool.
	Generate a new project from safe parameter set	Opens a new project, based on a saved safe parameter set.
	Open existing project1)	Opens a locally-saved project file.

1) Only possible if the axis type (linear/rotating) of the SafetyTool project file agrees with the current parameter set of the servo drive.

Table 98: Selection of the session variants - Configuration wizard

4.5.3 Online parameterisation

If the online connection to the servo drive is active in the Metronix ServoCommander®, then the functions for online parameterisation are available in the SafetyTool.

Please ensure that the data in the servo drive have been saved (button **Save Parameter**) before starting the SafetyTool. Otherwise, the basic information after the basic unit is restarted might differ from the basic information that had been used.

The parameters and the parameter set can only be validated during online parameterisation.

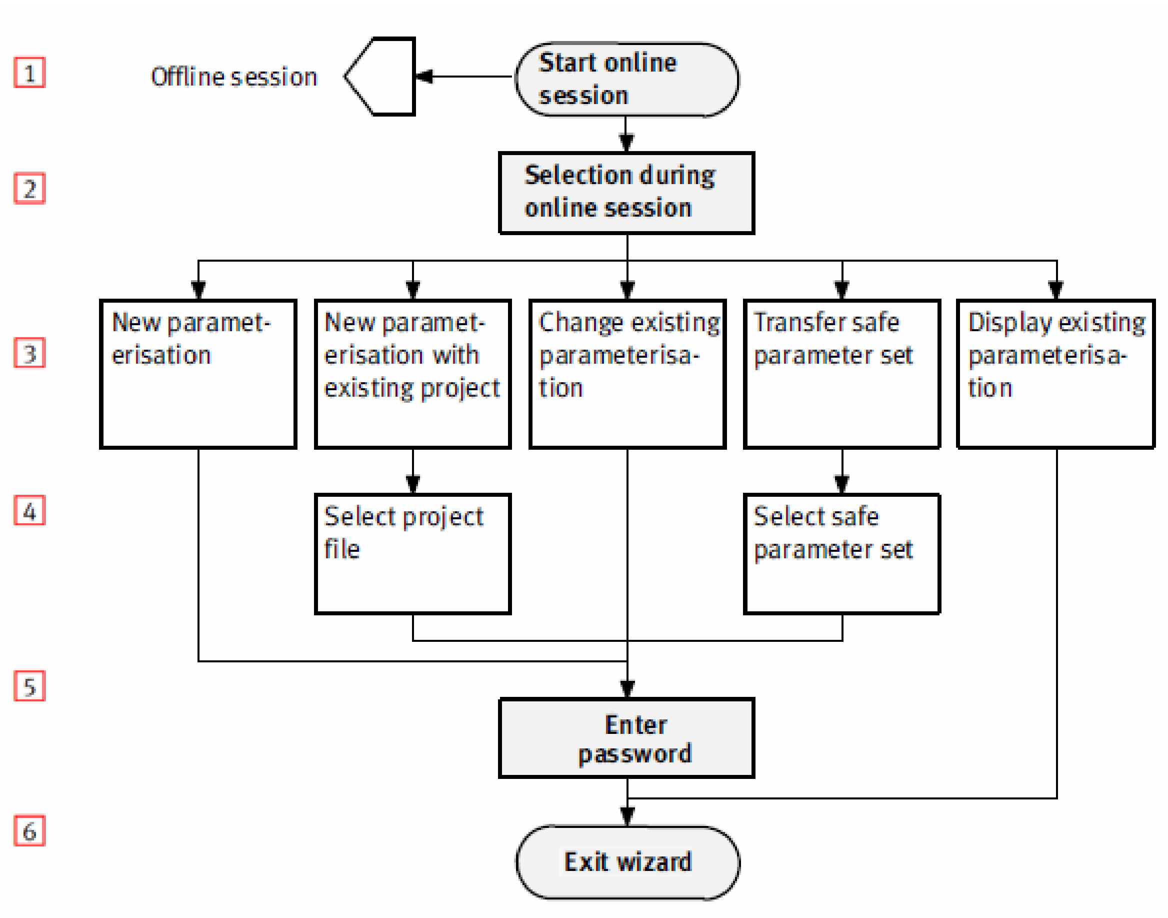
For the online parameterisation functions, it is always necessary to state a user name and to enter a password:

The factory setting for the password is: **SAFETY**

Assign an individual password to your project, in order to protect the safety parameters from unintentional changes (menu **Tools/Change password ➔** Section 4.7.1).

When the SafetyTool starts, the SafetyTool compares its database with the data of the basic unit and with that of the safety module. Depending on the selected session variant, an upload of the parameters from the safety module is required for this.

The operation is indicated by a progress bar. The length of time may vary, depending on the session variant and the speed of the communication connection.



1 Start the Wizard with the option of also selecting Offline mode

2 Selection of the online session variant

3 Note on the appropriate session variant

4 Selection of a project file / a parameter set

5 Personal identification

6 Exit Start wizard

Figure 57: Steps to the selection of the online session variant

A parameterisation session can also be started when the drive is switched on. When the parameterisation session has been started, the drive is switched off by the safety module (no output stage enable).

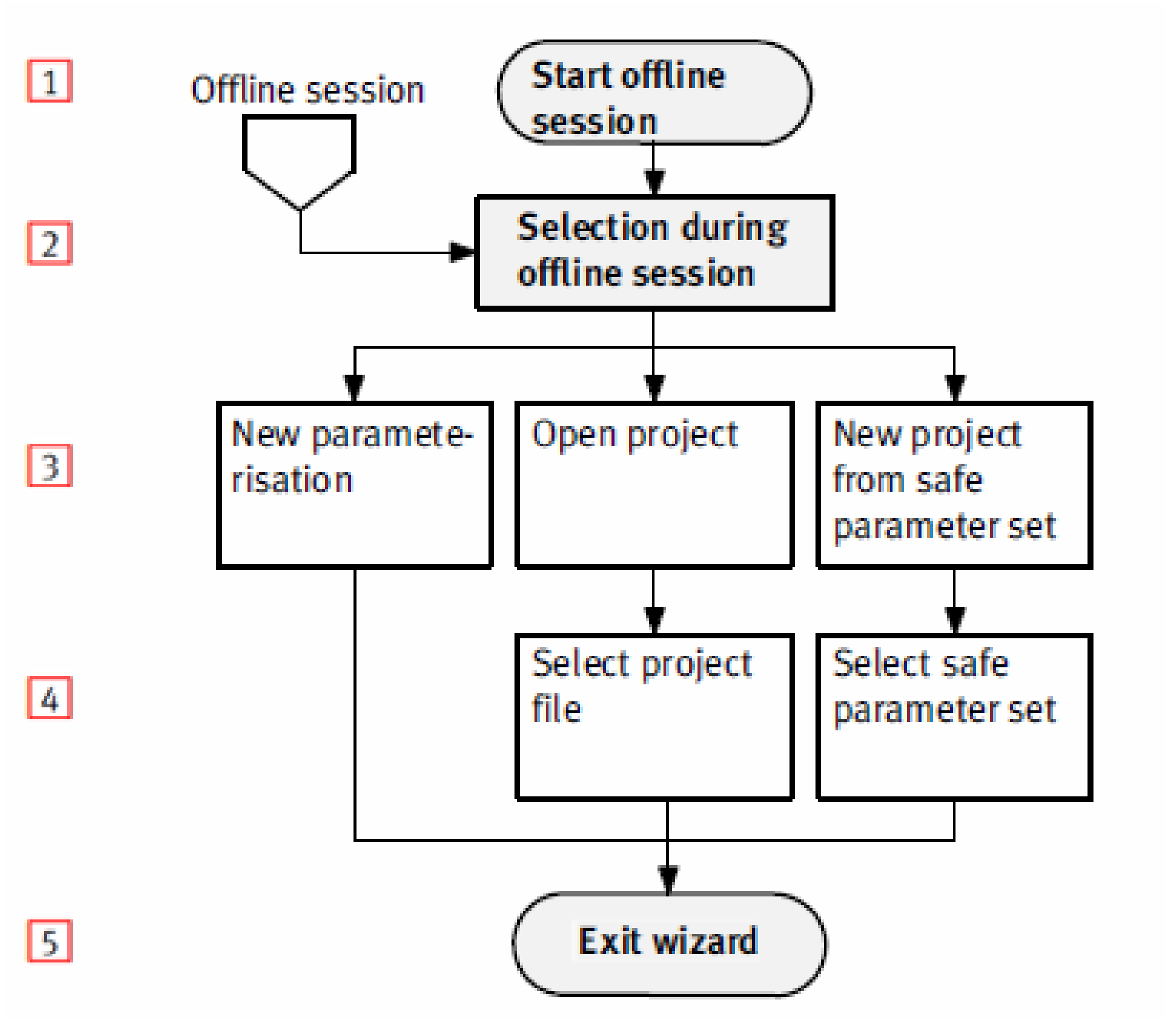
During a running parameterisation session, all the digital outputs are switched off.

The SafetyTool ends the parameterisation session automatically when you exit the wizard. Then, all the parameters must have the status "validated". Otherwise, all the changes are lost and the safety module starts with the most recently saved and validated parameter set.

4.5.4 Offline parameterisation

You can do this completely offline in preparation for parameterisation.

However, to commission the safety module correctly, you must validate the parameters online and transfer the validated parameters to the safety module.



1 Start the Wizard in Offline mode

2 Selection of the offline session variant

3 Information page on the appropriate session variant

4 Selection of a project file / a parameter set

5 Exit Wizard.

Figure 58: Steps to the selection of the offline session variant

4.5.5 Basic rules for parameterisation with the SafetyTool

4.5.5.1 Common properties of the parameterisation operations

Parameterisation always consists of the following steps:

1. Open a parameterisation session.
2. Change individual parameters.
3. Validate individual parameters or the entire parameter sets (generation of a validation code).
4. Permanently save the parameter set in the safety module; entire parameter set is considered validated.

   After further parameter changes, the steps 3. and 4. must be executed again.
5. End a parameterisation session, "activate" the parameter set.
6. Restart the safety module.

4.5.5.2 Opening of a parameterisation session

When a parameter session is opened, the safety module switches to the safe basic status, the drive is switched off (output stage switched off, safe brake control not energised, DOUT4x on the safety module switched off).

During a parameterisation session, the VOUT_SERVICE status is active.

Switch-on / switch-off of the drive is only possible after the parameterisation session is closed and only when the parameter set has been validated.

The opening of a parameterisation session is saved in the permanent event memory.

During the active parameterisation session, the message "FSPArA" is output on the 7-segment display of the servo drive (providing that no error is pending), see ➔ Section 5.4.2. Pressing **Start identification** in the Start Wizard allows you to output the message "HELLO...". The message is there for the identification of the servo drive if multiple servo drives are connected to the parameterisation PC.

Only one parameterisation session can be opened for each safety module at any time.

If a parameterisation session is already opened, the safety module will refuse further requests until the current parameterisation session is closed.

This prevents a safety module from being parameterised simultaneously from multiple PCs using the SafetyTool. The SafetyTool only allows changes to parameters when a parameterising session has been opened.

4.5.5.3 User ID and password

When a parameterisation session is opened, a user ID (user name) and a password must be entered.

The user ID and password both consist of ASCII characters (letters, numbers and umlauts, no special characters) and have a maximum length of 8 characters.

In the delivery status or after a reset to the factory setting, the password is "SAFETY".

The password should be changed immediately after commissioning.
The new password and the password of the factory setting should only be known to the appropriate "Person responsible for functional safety on the machine".

The changed password is saved in the safety module and replaces the previously valid password and applies for all users. The password is not saved in a parameter file. It cannot be read out of the safety module.

4.5.5.4 Data transfer from the servo drive

To compare the relevant parameters in the safety module with those of the servo drive (basic unit), data is first transferred from the basic unit during an online session variant.

When you exit the SafetyTool, any data loaded from the Metronix ServoCommander® to the servo drive could be lost during a restart. To prevent this, you must always make sure that the data is backed up when you start the SafetyTool with an active online connection. This is polled by a dialog.

When transferring data to the SafetyTool, in addition to the display units, the parameters of the connected shaft encoders are also transferred, which are mapped to the safety parameters for encoder 1 and encoder 2.

4.5.5.5 Principle of "Sending and validating"

All the parameters changed in the SafetyTool must be sent to the safety module, checked and validated. This applies to the data transferred from the servo drive (basic unit) as well as to the product terms for requesting safety functions or other mappings.

The sequence is identical on all parameter pages:

Step 1: Enable parameters for editing using the **Enable Edit** button.
Step 2: Manipulate or change parameters. In so doing, the value range is checked.
Step 3: Transmit the changed parameters to the safety module using the **Transmit** button.
Step 4: After this, the transmitted parameters must be validated.

For validation, the setpoints (from the SafetyTool) and the actual values (from the safety module) are displayed. Deviating values are marked by a symbol:

Symbol	Status
	The setpoint and actual value deviate from one another. These parameters must be compared.
	The setpoint and actual value deviate slightly from one another. Certain values, such as times, are rounded to a multiple of the basic unit in the safety module. This is why the setpoint and actual value may differ in the context of this rounding. Such a value can be validated.

Table 99: Display of deviation in setpoint and actual values

For validation after the check, tick the appropriate checkbox in the **Checked** column and validate the selected parameters with the **Validate** button. Only then have the parameters been correctly transferred to the safety module.

The **Valid** column displays whether the actual values of the parameters are valid, i.e. validated.

Symbol	Status
	Parameter not yet validated.
	Parameter is validated.

Table 100: Display of the validity of the parameters

4.5.5.6 Plausibility check

During the parameterisation session, the SafetyTool carries out various plausibility checks.

This ranges from monitoring of the range limits through to logical testing of the rotational speed limits (upper rotational speed limit may not be below the minimum rotational speed, lower limits must be less than the upper limits, etc.). You can also carry out the plausibility check manually ➔ Section 4.7.3.

4.5.5.7 Enabling and permanently saving in the device

After parameters have been changed, they must be saved permanently in the safety module. In addition, consistency of the parameter set is secured through a unique full validation code. The non-volatile saving and calculation of the validation code is implemented using the appropriate button on the **Finish** page.

If a parameterisation session was active in the SafetyTool with write access, then a restart is carried out automatically when the SafetyTool is exited.

4.5.5.8 Save parameterised intermediate states (without full validation):

The function **Parameterisation / Save parameters permanently in the safety module** saves the parameters, although they are not "fully validated". The safety module detects this status on restarting and switches to the safe basic status.

4.5.5.9 Standard and expert parameters

Some of the parameters are indicated as "Expert parameters" or are displayed in their own tab **Expert parameters**.

Note

Expert parameters do not normally need to be changed. Changes are only needed when actually required.

4.5.5.10 Status of the parameter groups

Each page in the SafetyTool contains a so-called parameter group. During an online session, the status of this parameter group is displayed by the LED symbol in the navigation tree:

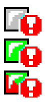
Symbol	Status
	The parameters are not yet validated (all stages of the parameters before validation).
	All the parameters of this page are validated. These parameters are identical to the parameters in the device. Only when all the parameters on all the pages have been validated is full validation and permanent saving of the parameters in the safety module possible.
	At least one parameter deviates from the parameters in the device. The differences must be resolved.
	There is a faulty value in an entry or selection field. The error must be corrected.

Table 101: Display of the status of the parameter groups

4.5.6 Behaviour in case of invalid parameterisation

If there is no valid parameter set in the safety module, then the output stage of the servo drive is blocked and all the digital outputs are de-energised.

The safety module can be parameterised again with the SafetyTool.

4.5.7 Parameter set version

When the revision of the safety module changes, that does not necessarily mean that a new version of the parameter set is needed (change in the firmware version or hardware version leads to a new full revision of the safety module).

The parameter set version monitors the compatibility between the SafetyTool and the safety module.

4.5.7.1 New parameter set in old firmware

Parameter sets are not accepted which are generated with a firmware version which is more recent that in the safety module. An error message "Incompatible parameter set" is generated.

4.5.7.2 Old parameter set in new firmware

The parameters are loaded first. The version number of the parameter set is used to check how to proceed with the parameter set.

If the version of the parameter set is not compatible, then validation via the validation code is refused.

If the version of the parameter set is compatible, then, for example, parameters which the set does not have are set to values which ensure that the safety module behaves in the same way as with an older revision.

A firmware update can only be performed by Metronix.

4.6 Sequence of parameterisation with the SafetyTool (example)

This section describes a complete parameterisation sequence using an example. However, the basic steps can be applied to any other application.

The following is required for the sequence:

- Basic commissioning of the servo drive has taken place with the Metronix ServoCommander® and an online connection to the Metronix ServoCommander® is active.
- The safety module is in the delivery status or has the factory setting (➔ Section 4.7.2).

You can find a complete description of the interface and the functions of the SafetyTool in the SafetyTool help.

You can find information on some of the special functions in ➔ Section 4.7.

Example application:

Machine with

1. Emergency stop switch (DIN40), which, when actuated, should always trigger SS1 type b) and then SBC.
2. Light curtain (DIN41) as protection against manipulation in the machine. In normal operation, SS1 is also triggered, whilst, in Setup mode, SS2 is requested.
3. Enabling button (DIN42), in order to move the axis with SLS in Setup mode.
4. Mode selector switch for normal operation and Setup mode (DIN45, DIN46).
5. Monitoring of the switches with test pulses from DOUT42.
6. Acknowledge error (DIN48).
7. Restart (DIN49) rising edge, restart after SS1 takes place using an external "Restart" control signal.
8. The switch-over between SS2 and SLS takes place on automatic restart.

In the example, the following parameterisation is carried out:

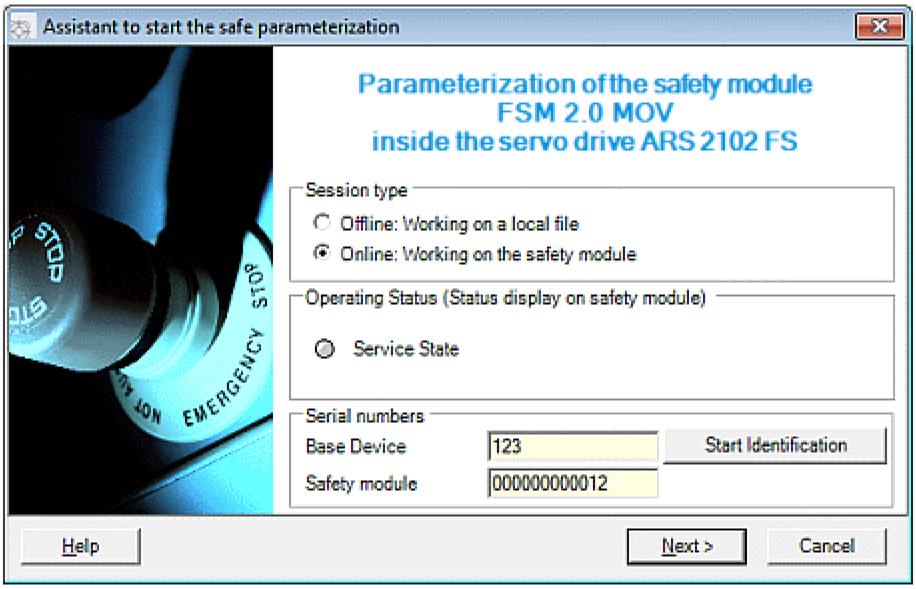
- **After switching on:**
  STO with automatic SBC activation is requested.
- **Normal operation:**
  SS1 is to be triggered after Emergency Stop is actuated or an object enters the light curtain with subsequent SBC, restart only via DIN49.
- **Setup mode:**
  - SLS is always requested when Setup mode is selected.
  - SLS can only be terminated when,
    a) the mode selection switch is set back to normal operation and
    b) the through-beam sensor is no longer interrupted and
    c) restart is actuated.

- SS2 is additionally triggered on entry into the light curtain.
- Restart from SS2 only via DIN49 and when the light curtain has been exited, or via the enabling button DIN42.
- When the enabling button is actuated, there should be a switch from SS2 to SLS.

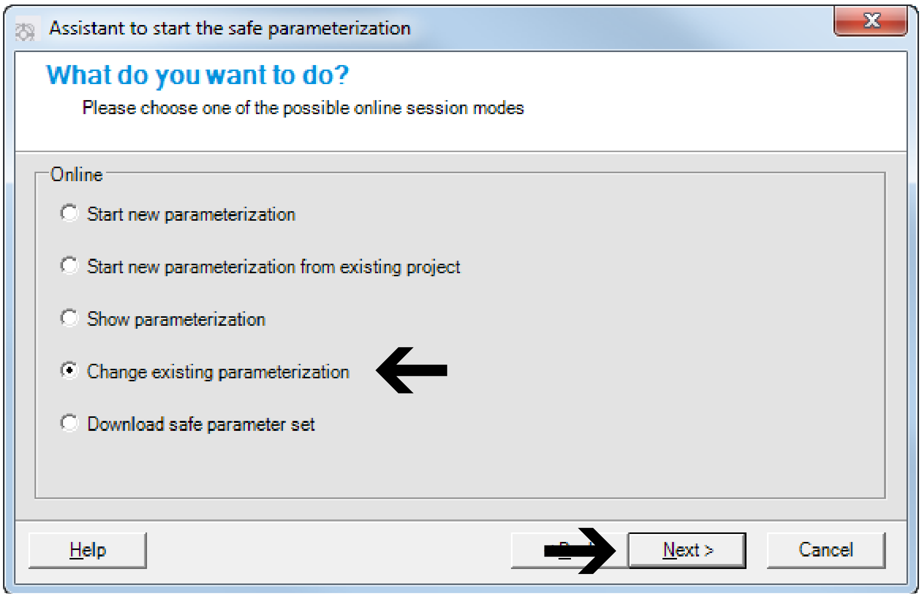
i You must determine the circuitry and parameterisation required for your application as part of your risk analysis.

4.6.1 Selection of the session variant in the Wizard

1. Start the SafetyTool via the menu **Parameters/Functional safety/Safe FSM parameterisation** in the Metronix ServoCommander® ➔ Section 4.5.1.
2. In the **Wizard for starting safe parameterisation**, select the session type **Online ...** and confirm this with **Next**.

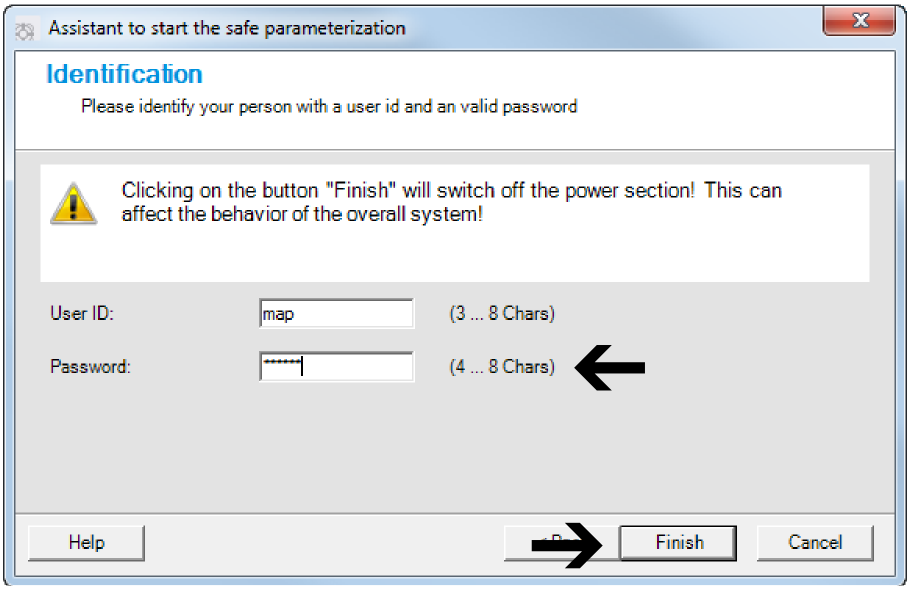


3. Select the session variant **Change existing parameterisation** and confirm this with **Next**.



After this, a note on the session variant is displayed which you should read and then confirm with **Next**.

4. To write parameters, it is necessary to enter a user ID and the password. In the delivery status or after a reset to the factory setting, this is "SAFETY".



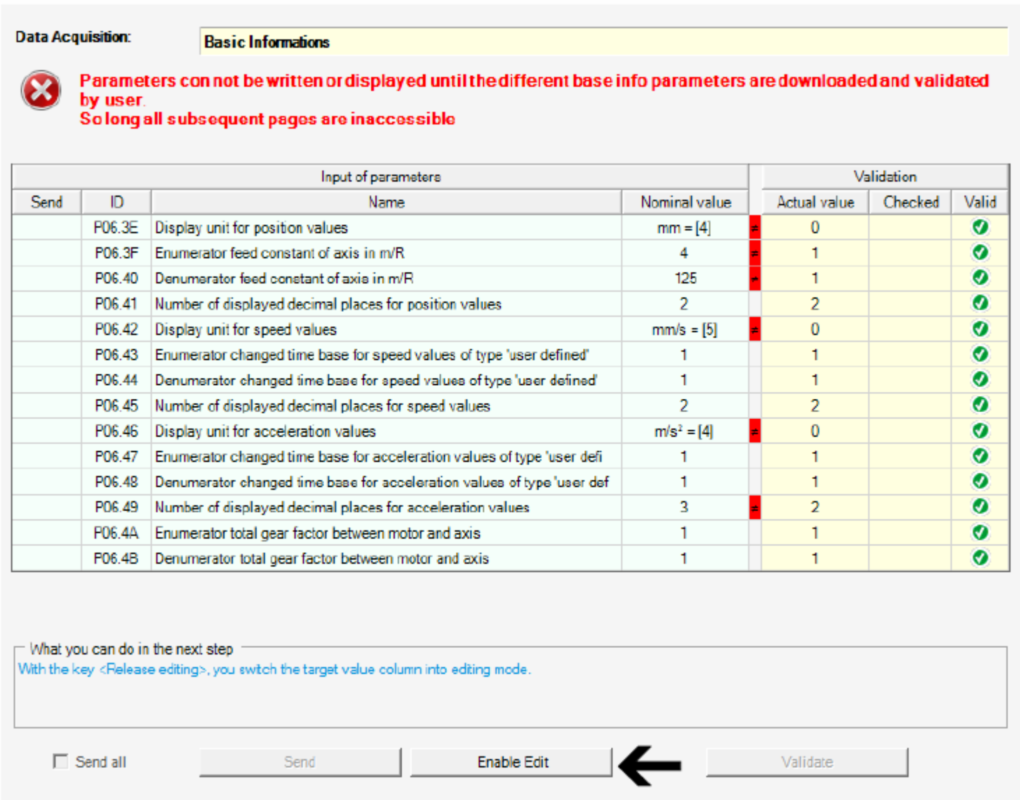
Exit the wizard with **Finish**.

4.6.2 Data transfer and synchronisation

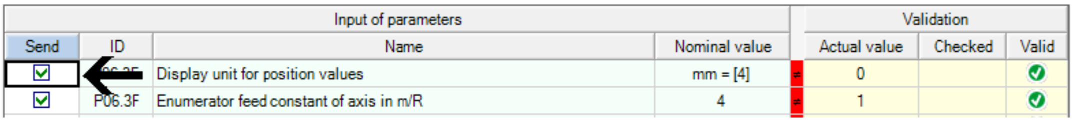
1. Normally, the basic information of the factory setting deviates from the current basic unit parameterisation. This is shown in a dialog, which you should confirm with **OK**.

   If this is not the case, you can continue with item 3.

2. The deviating values are displayed in red on the Basic information page and must first be synchronised.

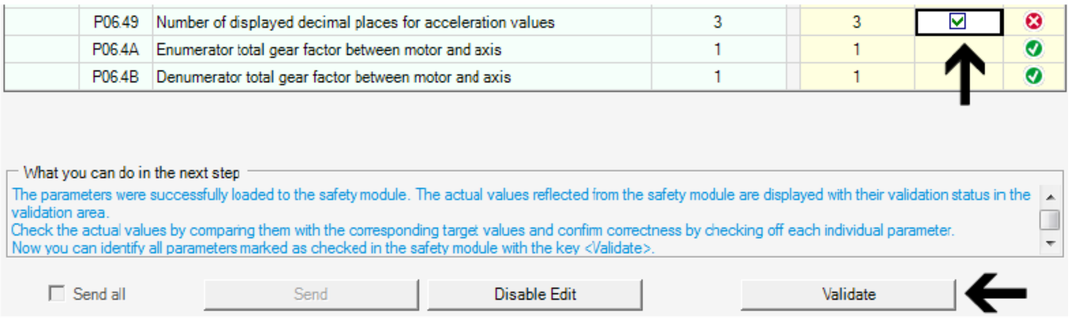


Click **Enable Edit** and tick the checkboxes of the deviating parameters under **Transmit**.

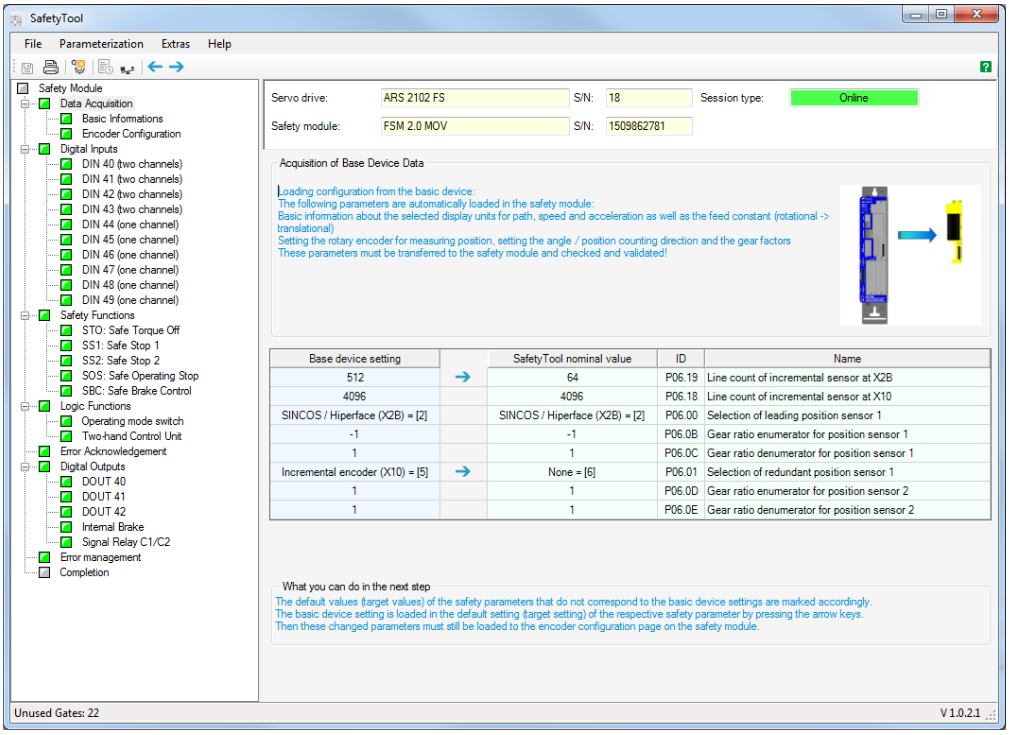


The **Transmit** button loads the selected parameters into the safety module.

This means that the parameters are, for now, invalid. Check the parameters by comparing the values under **Setpoint** and **Actual value**. Confirm the test by ticking the checkbox under **Checked**. Then you should validate them using the **Validate** button.



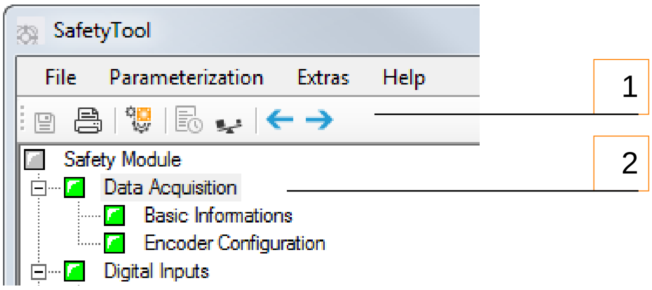
3. If all the parameters of the basic information are identical, then the other parameters are loaded from the safety module and the **Data transfer** page is shown with the comparison of the data transmitted from the basic unit.



4.6.3 Starting parameterisation

Now, the session variant **Change existing parameterisation** is active and you can begin the actual parameterisation.

❖ To do this, use the arrow buttons (**1**) to navigate through **all** the parameter pages and check or change the displayed parameters.



The appropriate parameter page is displayed in the navigation tree (**2**), through which you can also switch directly to another page, e.g. to subsequently review parameters.

For commissioning, we recommend checking or editing each page one after another.

4.6.4 Checking the data transfer

The most important parameters of the encoder configuration are displayed on the first parameter page **Data transfer**.

Base device setting	↓	SafetyTool nominal value	ID	Name
8192		8192	P06.19	Line count of incremental sensor at X2B
4096	→	8192	P06.18	Line count of incremental sensor at X10
Other encoder (X2B) = [4]		Other encoder (X2B) = [4]	P06.00	Selection of leading position sensor 1
1		1	P06.0B	Gear ratio enumerator for position sensor 1
1		1	P06.0C	Gear ratio denumerator for position sensor 1
None = [6]	→	Incremental encoder (X10) = [5]	P06.01	Selection of redundant position sensor 1
1		1	P06.0D	Gear ratio enumerator for position sensor 2
1		1	P06.0E	Gear ratio denumerator for position sensor 2

Any deviations are shown by a blue arrow. Clicking the arrow transfers the basic unit setting as the parameter setpoint. The parameter setpoint must then be transferred to the safety function on the appropriate encoder configuration page and validated.

4.6.5 Basic information

You already processed the basic information in section 4.6.2. For this reason, the values on this page should already be correct.

4.6.6 Encoder configuration

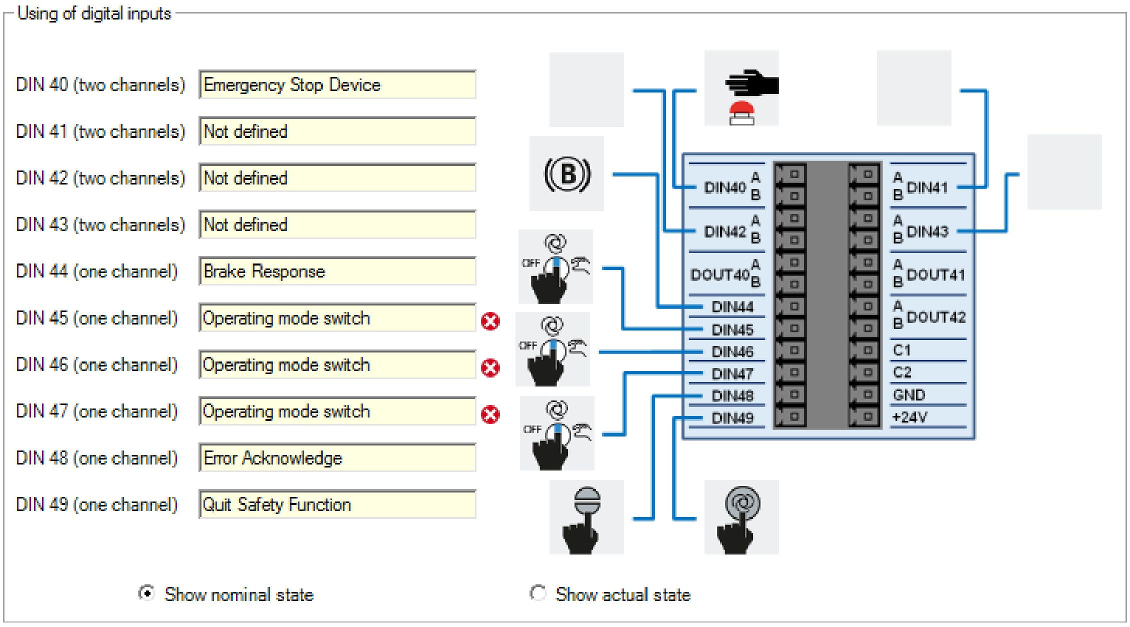
❖ Check or edit each of the parameters of the encoder configuration.

If you have transferred setpoints under Section 4.6.4, then they are already entered in the appropriate parameter. You can then transfer them using **Enable Edit**, **Transmit** and then check and validate them.

Input of parameters						Validation		
Send	ID	Name	Unit	Nominal value		Actual value	Checked	Valid
	P06.18	Line count of incremental sensor at X10		4096	≠	8192		✓

4.6.7 Configuring digital inputs

The allocation of all single-channel and two-channel inputs is displayed on the **Digital inputs** page. Editing then takes place separately for each input on the following pages.



Inconsistencies are indicated by an error symbol. In the example, DIN45, DIN46 and DIN47 are parameterised as the sensor type "Mode selector switch", but the "Activation" parameter of the mode selector switch is not active.

Now, edit the pages of the digital inputs one after another.

DIN40

❖ For the example, DOUT42A/B is set as the source of the test pulse.

Input of parameters						Validation		
Send	ID	Name	Unit	Nominal value		Actual value	Checked	Valid
☐	P02.24	Sensor type		Emergency Stop Device = [2]		2		✓
☐	P02.06	Operating mode		Equivalent = [1]		1		✓
☐	P02.05	Discrepancy time	ms	100,0		100,0		✓
☑	P02.07	Test pulse source		DOUT42A/B = [3]	≠	0		✓

DIN41

❖ For the example, "Light curtain" is set as the sensor type and DOUT42A/B as the source of the test pulse.

Input of parameters						Validation		
Send	ID	Name	Unit	Nominal value		Actual value	Checked	Valid
☑	P02.25	Sensor type		Light Curtain = [8]	≠	0		✓
☐	P02.0B	Operating mode		Equivalent = [1]		1		✓
☐	P02.0A	Discrepancy time	ms	100,0		100,0		✓
☑	P02.0C	Test pulse source		DOUT42A/B = [3]	≠	0		✓

DIN42

❖ For the example, "Enabling button" is set as the sensor type and DOUT42A/B as the source of the test pulse.

Input of parameters						Validation		
Send	ID	Name	Unit	Nominal value		Actual value	Checked	Valid
☑	P02.26	Sensor type		Enable Switch = [3]	≠	0		✓
☐	P02.10	Operating mode		Equivalent = [1]		1		✓
☐	P02.0F	Discrepancy time	ms	100,0		100,0		✓
☑	P02.11	Test pulse source		DOUT42A/B = [3]	≠	0		✓

DIN45 ... DIN47

❖ For the example, DOUT42B is set as the source of the test pulse for DIN45, DIN46 and DIN47.

Input of parameters						Validation		
Send	ID	Name	Unit	Nominal value		Actual value	Checked	Valid
☐	P02.29	Sensor type		Operating mode switch = [11]		11		✓
☑	P02.1B	Test pulse source		DOUT42B = [10]	≠	4		✓

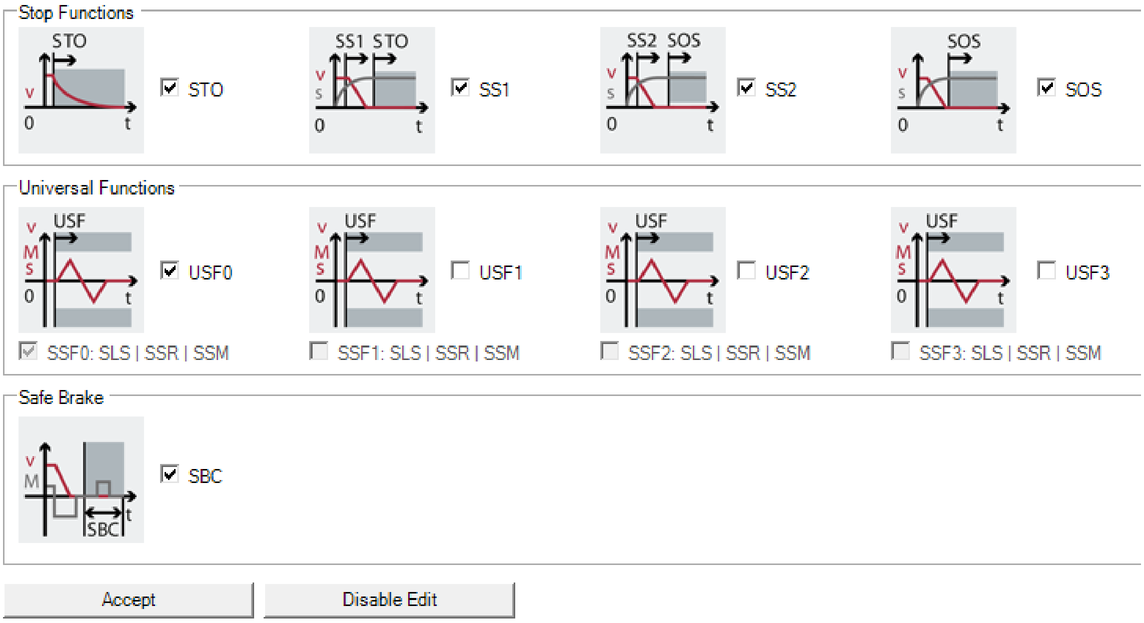
DIN43 and DIN44, DIN48 and DIN49

No changes are required for the example, as all the settings correspond to the factory settings.

4.6.8 Selection and parameterisation of the safety functions

The active functions are displayed on the **Safety functions** page.

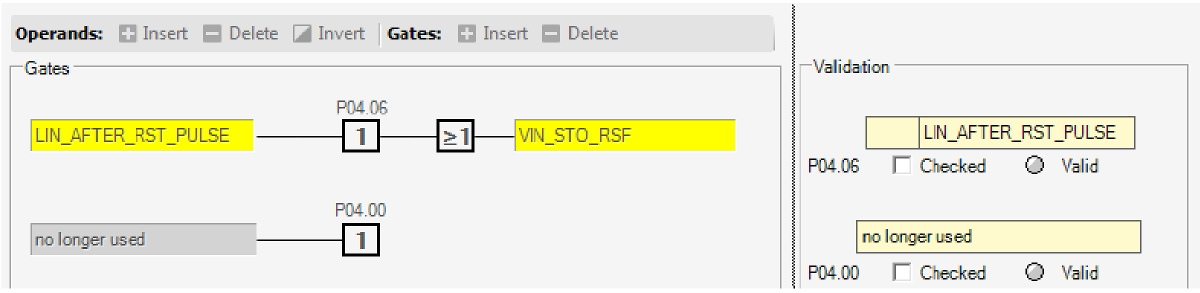
❖ For the example, you should also activate SS2, SOS and USF0. You can parameterise the SLS safety function using USF. No transmission and validation is required to activate safety functions.



4.6.8.1 STO: Safe Torque Off

1. Check, and if necessary, change, the parameters of the STO safety function ➔ Section 2.5.3.
2. In the **Request** tab, delete the request in the factory setting via DIN40. After editing has been enabled, select the logical input LIN_D40 in the gate (highlighted in blue) and remove it using **Operands: Del.**

   As the operand has now been deleted from the product term but the product term (here P04.00) is still assigned, this is still displayed at the bottom.
3. In the right-hand **Operands** frame, select LIN_AFTER_RST_PULSE and apply the entry with **Gate: Ins.**



4. **Transmit** sends the change to the safety module. Then, under **Validation** (in the top right of the above figure), the new assignment and the deletion operation are displayed and can be checked and validated.

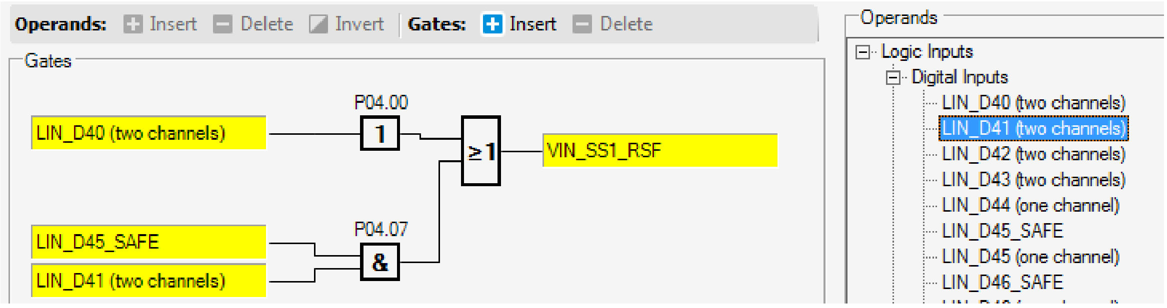
In the example, the setting in the **Terminate request** tab can be left as LIN_D49_RISING_EDGE.

4.6.8.2 SS1: Safe Stop 1

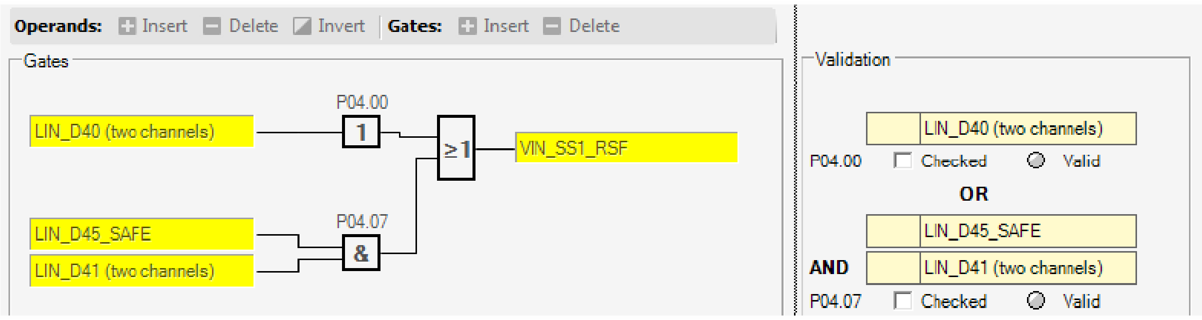
1. In the **Standard Parameter** tab, check the settings and adapt them to your application as necessary ➔ Section 2.5.5.
2. For the example, activate "Automatic Activation SBC" (P0C.09).

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0C.00	Delay time for start of monitoring	ms	2,0	2,0		✓
	P0C.01	Brake ramp time	ms	300,0	300,0		✓
	P0C.02	Tolerance time for limit exceed	ms	10,0	10,0		✓
	P0C.06	Limit speed in base device		☐	0		✓
	P0C.07	Activate quick stop ramp in base device		☑	1		✓
	P0C.08	Automatic restart allowed		☐	0		✓
	P0C.09	Automatic activate SBC		☑	1		✓

For the example, create the following logic in the **Request** tab:



3. In the right-hand **Operands** frame, select LIN_D40 and apply the entry with **Operands: Ins.** Alternatively, you can drag the entry onto the driver link with the mouse (here: Product term P04.00).
4. Then select LIN_D45_SAFE and apply the entry with **Gate: Ins.** Alternatively, you can drag the entry onto the OR gate (≥ 1) with the mouse. This inserts a new gate with the entry LIN_D45_SAFE (in the example: Product term P04.07).
5. Now, under **Gate**, select the LIN_D45_SAFE entry you have just created, in order to highlight the second gate as the target for the insertion of additional operands (here: Product term P04.07).
6. Then, in the right-hand **Operands** frame, select LIN_D41 and apply it with **Operands: Ins.** Alternatively, you can drag the entry onto the driver link with the mouse. The driver automatically turns into an AND operation.
7. After transmission, you must now validate 2 product terms using the OR operation.

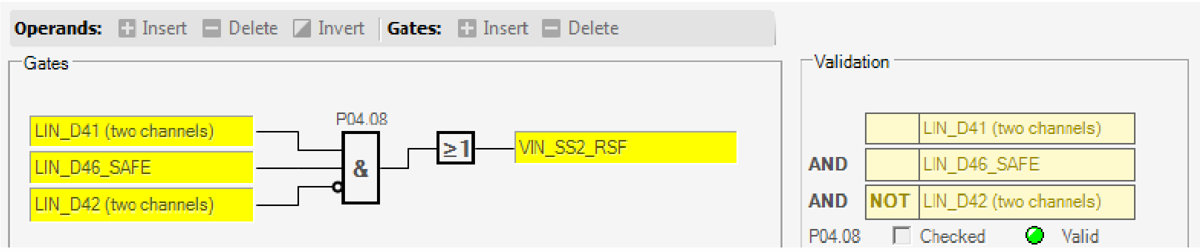


In the example, the setting in the **Terminate request** tab can be left as LIN_D49_RISING_EDGE.

4.6.8.3 SS2: Safe Stop 2

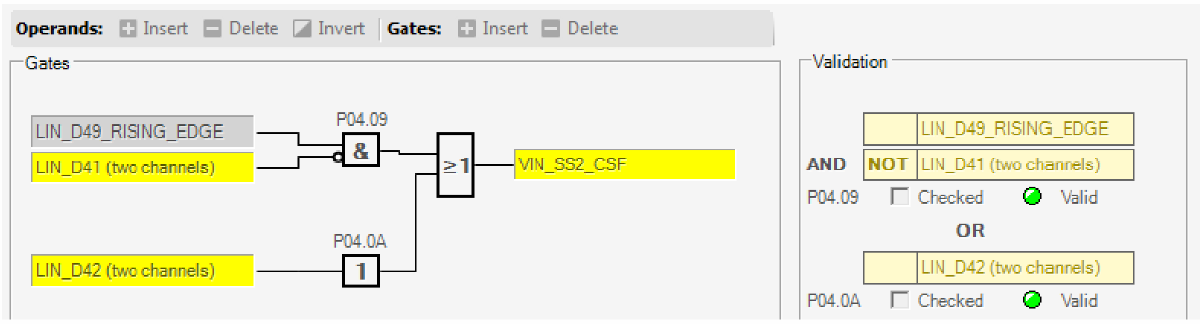
1. In the **Standard Parameter** tab, check the settings and adapt them to your application as necessary ➔ Section 2.5.6.

For the example, create the following logic in the **Request** tab:



2. In the right-hand **Operands** frame, select LIN_D41 and apply the entry with **Operands: Ins.** Alternatively, you can drag the entry onto the driver link with the mouse (here: Product term P04.08).
3. Repeat step 2. with the operands LIN_D46_SAFE and LIN_D42.
4. Invert LIN_D42 with **Operands: Invert.** If you selected another element in the meantime, you may need to select LIN_D42 again in advance.
5. After transmission, you only need to validate one product term.

For the example, create the following logic in the **Terminate request** tab:



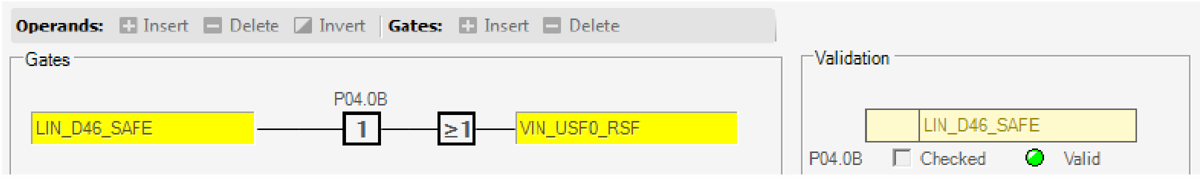
6. In the right-hand **Operands** frame, select LIN_D49_RISING_EDGE and apply the entry with **Operands: Ins.**
7. Repeat step 6. with LIN_D41.
8. Invert LIN_D41 with **Operands: Invert.**
9. Then select LIN_D42 and add as an AND operation using **Gate: Ins.**
10. After transmission, you must now validate 2 product terms using the OR operation.

4.6.8.4 SOS: Safe Operating Stop

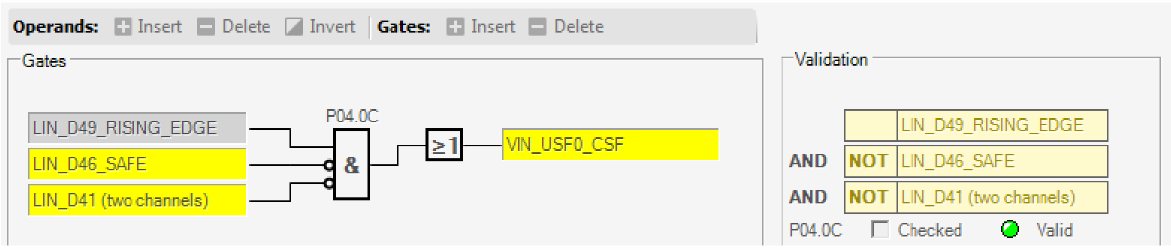
1. Parameterise the safety function SOS according to your application ➔ Section 2.5.7.
2. No logic is required to request SOS, as SOS is only used as an error reaction.
3. For **Terminate request**, insert LIN_D49_RISING_EDGE (as for SS2).

4.6.8.5 USF0: Universal Function

1. To request USF0 in the example, add LIN_DIN46_SAFE.



2. For the example, create the following logic in the **Terminate request** tab:



The basic operating steps are described in the steps listed above.

4.6.8.6 SSF0: Safe speed

❖ For the SLS safety function, parameterise the function SSF0 according to your application ➔ Section 2.5.10.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.00	Activate SSF		☑	1		✓
	P0E.01	Delay time for start of monitoring	ms	2,0	2,0		✓
	P0E.07	Safe speed - upper limit	mm/s	225,00	225,00		✓
	P0E.08	Safe speed - lower limit	mm/s	-225,00	-225,00		✓
	P0E.02	Brake ramp time	ms	300,0	300,0		✓
	P0E.03	Tolerance time for limit exceed	ms	10,0	10,0		✓
	P0E.09	Limit speed in base device		☑	1		✓
	P0E.0B	Automatic restart allowed		☐	0		✓

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.0D	Speed ramp - Delay time monitoring	ms	0,0	0,0		✓
	P0E.06	Brake ramp - start delay	ms	6,0	6,0		✓
	P0E.04	Brake ramp - starting value factor		0,10	0,10		✓
	P0E.05	Brake ramp - starting value offset	mm/s	75,00	75,00		✓
	P0E.0C	Offset speed limit	mm/s	75,00	75,00		✓
	P0E.0A	Activate quick stop ramp in base device		☐	0		✓

4.6.8.7 SBC: Safe Brake Control

1. Parameterise the safety function SBC according to your application ➔ Section 2.5.4.
2. In the example, delete the request by LIN_D40.
3. For **Terminate request**, leave LIN_D49_RISING_EDGE.
4. Depending on your application, logic for the brake feedback may be necessary in the **Feedback** tab.

4.6.9 Logic functions

The Advanced Logic Functions ALFx are not used in the example and therefore do not need to be activated on the **Logic functions** page.

4.6.9.1 Mode selector switch

❖ Activate the mode selector switch on the **Mode selector switch** page.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P02.00	Activation		☑	1		✔
	P02.01	Discrepancy time	ms	500,0	500,0		✔

4.6.9.2 Two-handed control device

The two-handed control device is not used in this example.

4.6.10 Logic error acknowledgement

For the example, the factory setting can be used for logic error acknowledgement.

4.6.11 Digital outputs

4.6.11.1 DOUT40, DOUT41

The digital outputs DOUT40 and DOUT41 are not used for the example.

4.6.11.2 DOUT42

The parameterisation does not need to be changed for the example. In the factory setting, DOUT42 is already parameterised as "Permanently switched on".

DOUT42 must be parameterised as "Permanently switched on" so that it can be used as the test pulse source as is the case in this example.

4.6.12 Internal brake

In the example, the factory setting can be used for parameterisation of the internal brake.

4.6.13 Signal contact

In the example, the factory setting can be used for parameterisation of the signal contact. The relay is closed when all the requested safety functions are active and no safety condition has been violated.

4.6.14 Error management

You must select an adequate error reaction on the **Error management** page for the violation of safety conditions and for errors, for example in the angle encoder analysis.

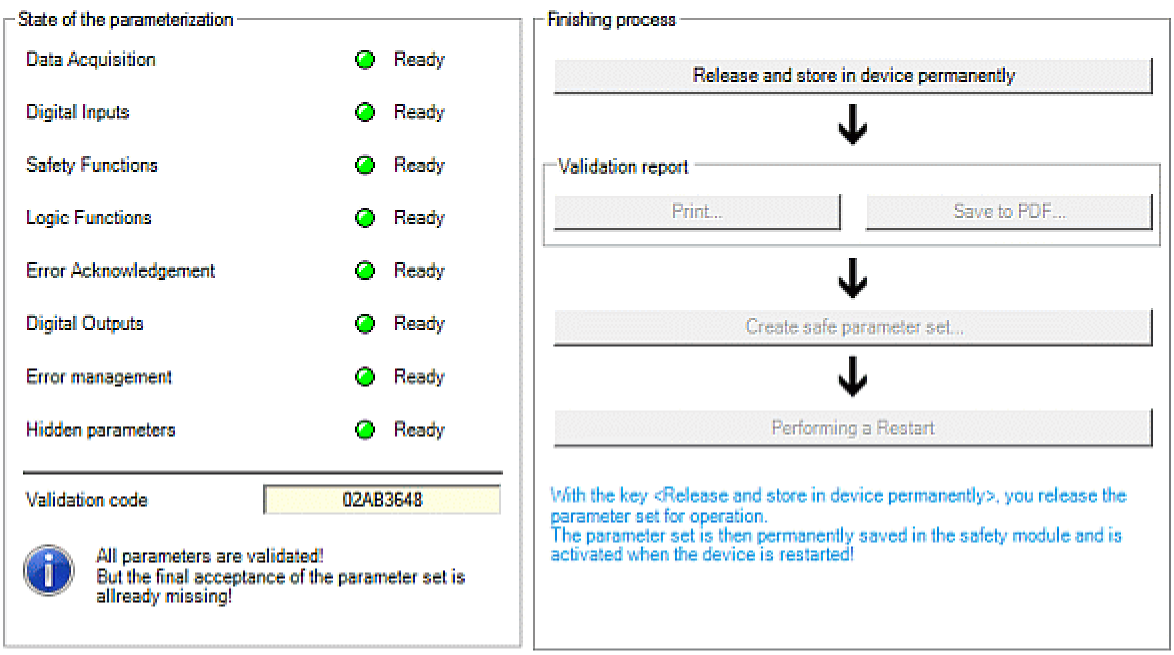
For the example, use the factory settings. If there is an error, STO or SS1 as well as SBC is usually triggered.

4.6.15 Finishing the parameterisation

If the LEDs of the main node are "green", then the parameter set can be validated (full validation). The validation code currently calculated by the safety module is read out and displayed in hexadecimal form in the **Validation code** display field.

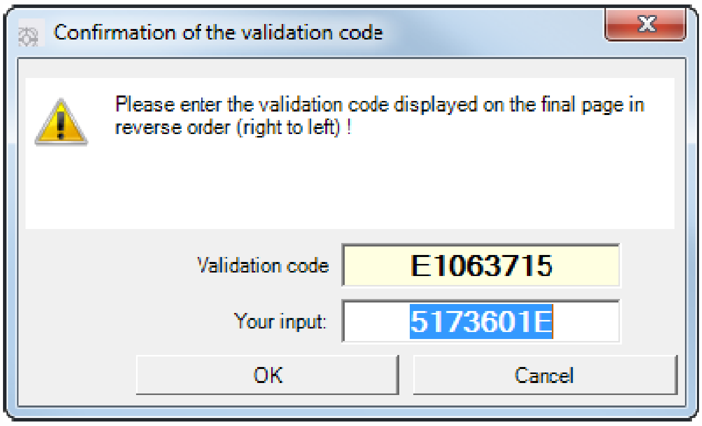
The current status of parameterisation is displayed beneath the **Validation code** field.

To be able to complete validation successfully, the parameters must be backed up in the device.



1. To do this, click **Release and store in device permanently** first.

2. As confirmation, the validation code must be entered **in reverse order** and confirmed with OK.



3. When the validation code has been entered correctly, the safety module saves the parameters permanently in the flash memory and the **Finish** page is now also shown in green in the navigation tree.
4. To create the necessary validation report, you can now either output the summary to a printer using the **Print** option or generate a corresponding PDF document using **Save to PDF**.
5. You can send the validated parameter set to other safety modules that have the same parameters. For this, or to replace the safety module, use **Create safe parameter set**. This saves the file.
6. To finish parameterisation, click **Performing a restart**. This restarts the servo drive and the safety module.

The parameterisation of the example is completed.

4.7 Special functions of the SafetyTool

4.7.1 Changing a password

When parameterisation is active, you can change the password at any time.

1. Open the **Change password** dialog with the menu command **Tools/Change password**.

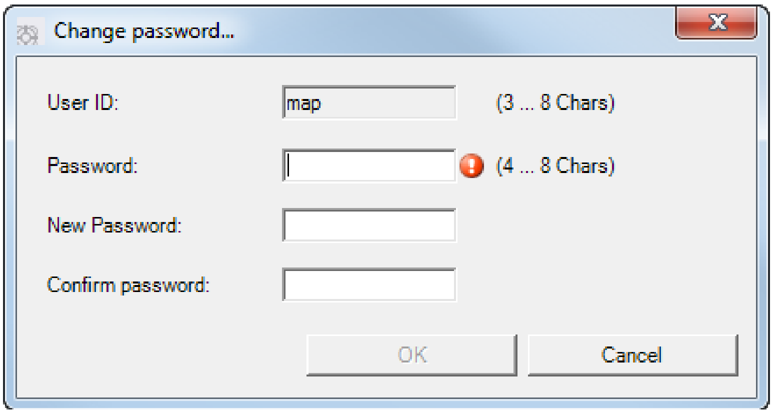


Figure 59: Changing a password

2. Enter the current password under **Password**.
3. Enter the new password twice under **New password** and **Confirm password**.
4. Confirm with **OK**.

The new password is immediately active in the safety module.

4.7.2 Setting the factory settings

To reset the safety module to the factory settings (➔ Section 4.4.1):

1. When the online connection is active, launch the SafetyTool (➔ Section 4.6).
2. Select the online session variant **Display parameterisation** (no password required).
3. It is possible that deviating basic information is then displayed, which you should confirm with OK.
4. The safety module is reset with the menu command **Tools/Set factory settings**. For this, the user name is queried (logged in the permanent event memory).
5. The parameter is then read from the safety module. Confirm again any deviating basic information.
6. Exit the SafetyTool

4.7.3 Plausibility check

The plausibility check can be carried out at any time during a parameterisation session.

❖ Open the **Plausibility check** using the menu command **Tools/Check parameters for plausibility**.

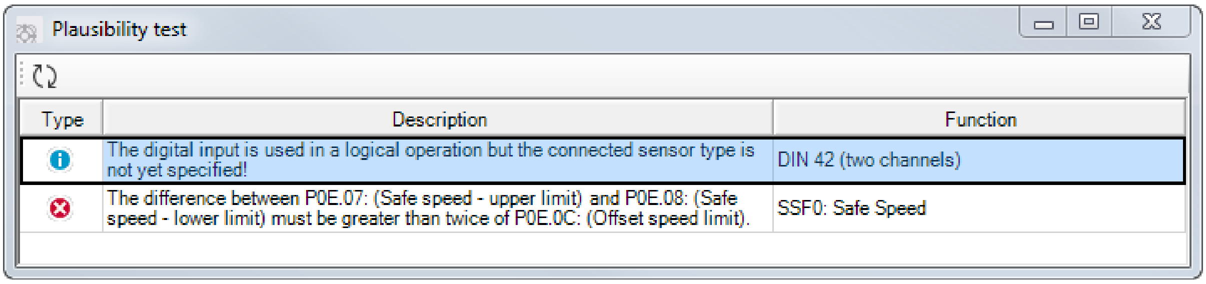


Figure 60: Plausibility check

The points detected during the check are indicated with an icon.

Symbol	Meaning
	Information: Merely information, with no functional meaning.
	Warning: The parameterisation functions, but may not be complete.
	Error: Faulty parameterisation, the safety module will not function properly.

Table 102: Display of the plausibility check

4.7.4 Overview of parameters

For rapid access for experts, the parameters can be displayed and edited in a separate window.

❖ Open the **Parameter overview** using the menu command **Tools/Parameter overview**.

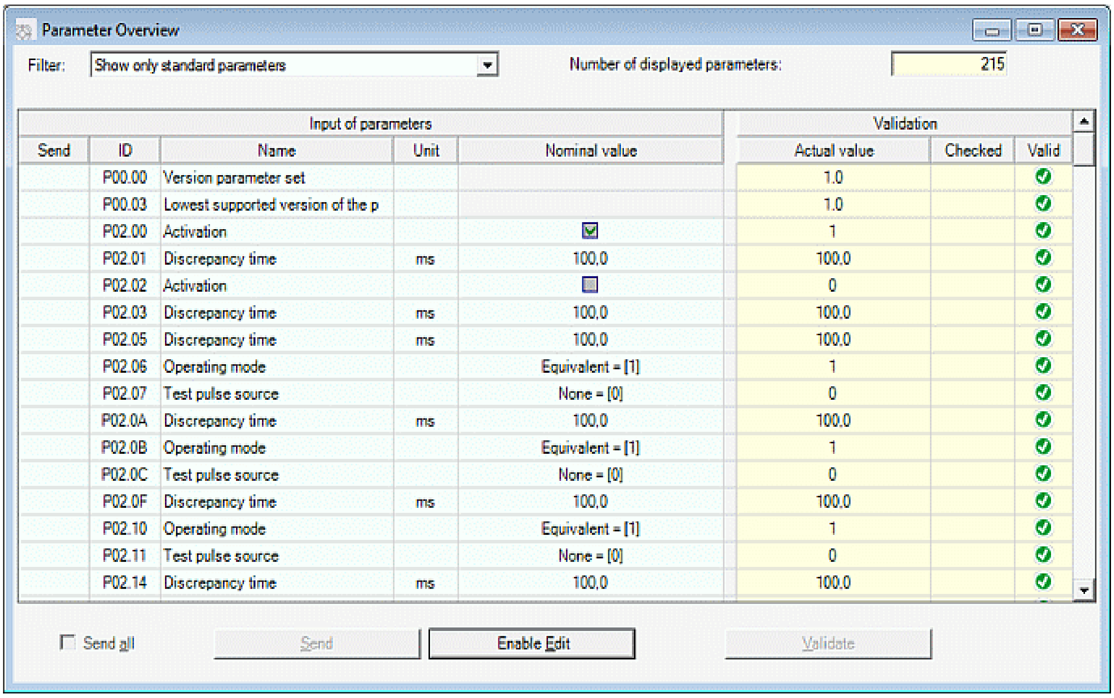


Figure 61: Overview of parameters

4.7.5 Diagnostics window

In the **Extras/Diagnostics** submenu, you will find various commands for the display of different diagnostic windows. You can find additional information in the SafetyTool Help.

The **Digital I/O (logical states)** window shows, for example, the logical state of the inputs and outputs:

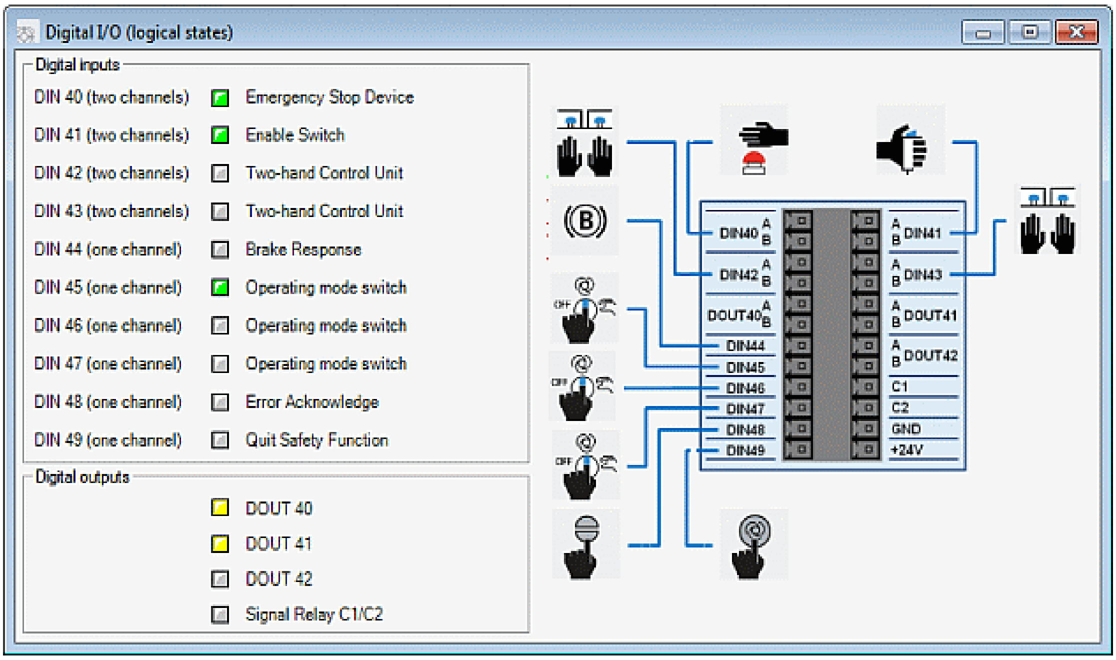


Figure 62: Digital I/O – logical states

The **Error display** window displays the active errors. You can acknowledge them with the **Acknowledge error!** button, if possible here.

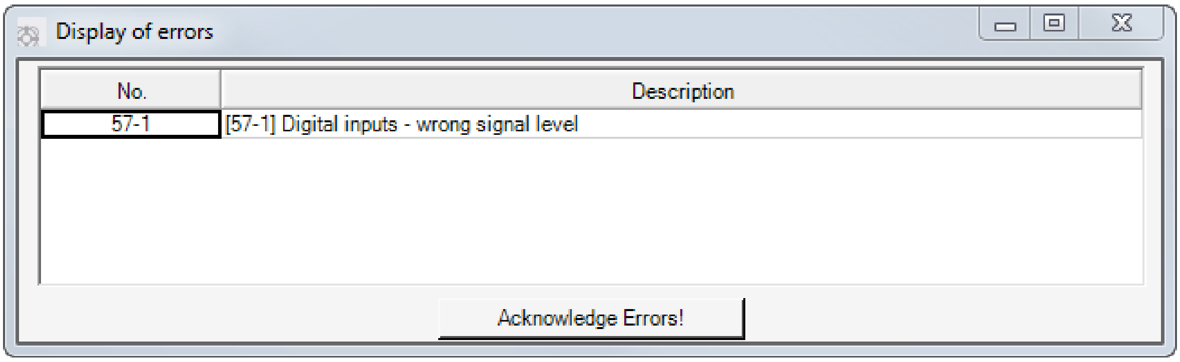


Figure 63: Error display

Open the **Functional circuit diagram** window using the menu command **Tools/Diagnostics/Internal signals**. The window shows an overview of the logical and virtual inputs, as well as the virtual and logical outputs of the safety module.

Clicking one of the blue text links opens an additional window, in which the status of the appropriate signal group is displayed (in the example, this is the logical inputs represented by the physical inputs).

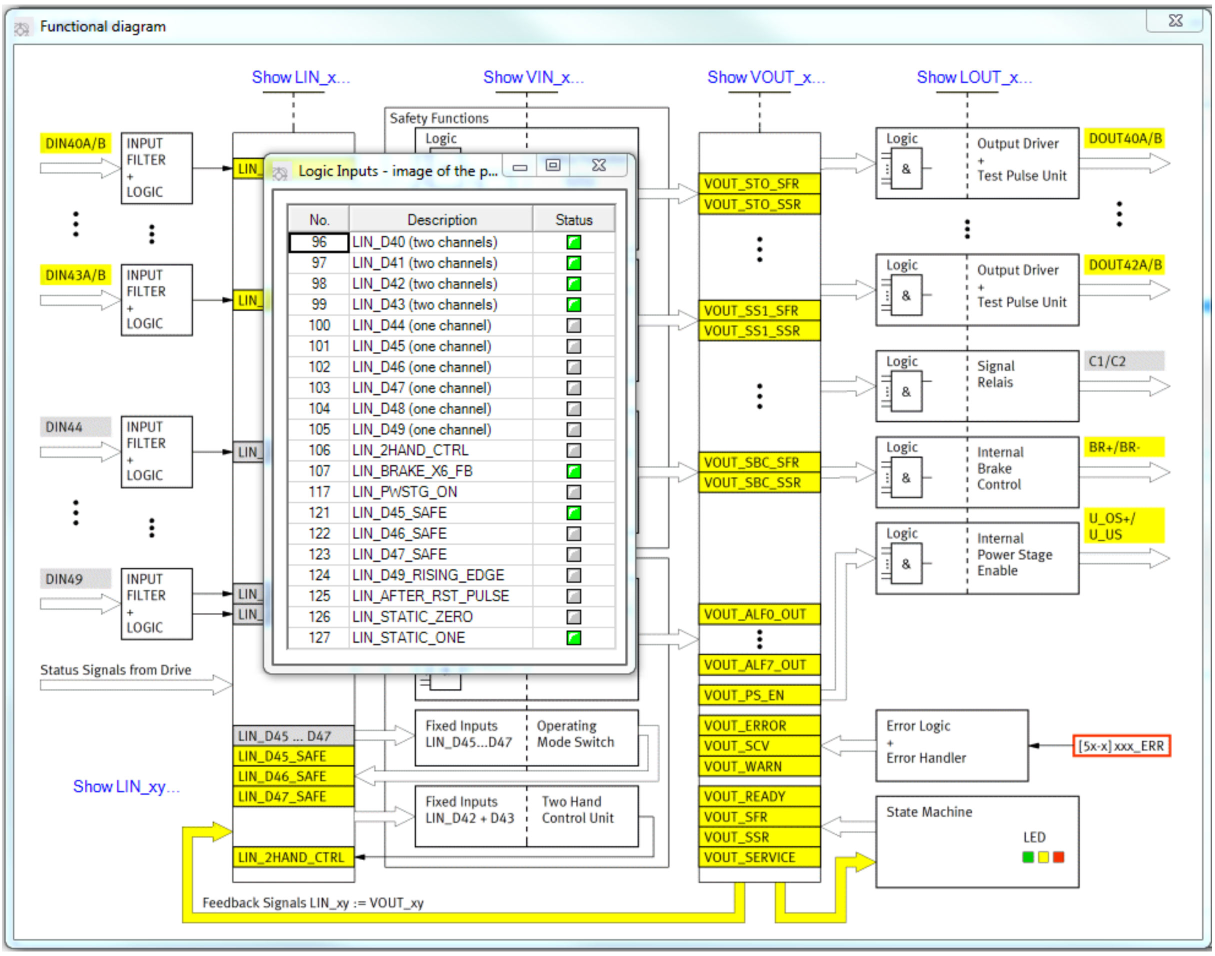


Figure 64: Functional circuit diagram

4.8 Performance test, validation

Note

The safety functions must be validated after installation or after each change to the installation.

This validation must be documented by the person performing the commissioning. To assist you with the commissioning, questions for risk reduction are summarised below in the form of checklists.

The checklists below are no substitute for safety training.
No guarantee can be provided for the completeness of the checklist.

No.	Questions	Applicable		Completed
1.	Were all operating conditions and interventions taken into account?	Yes ☐	No ☐	☐
2.	Has the "3-step method" for risk reduction been applied, i. e.1. Inherently safe engineering design, 2. Technical and possibly additional safeguarding, 3. User information about the residual risk?	Yes ☐	No ☐	☐
3.	Were the hazards eliminated or the hazard risk reduced as far as practically possible?	Yes ☐	No ☐	☐
4.	Can it be guaranteed that the implemented measures will not pose new hazards?	Yes ☐	No ☐	☐
5.	Have the users been adequately informed and warned about the residual risks?	Yes ☐	No ☐	☐
6.	Can it be guaranteed that the operators' working conditions have not deteriorated due to the safeguarding undertaken?	Yes ☐	No ☐	☐
7.	Is the safeguarding mutually compatible?	Yes ☐	No ☐	☐
8.	Was adequate consideration given to the potential consequences of using a machine designed for commercial/industrial purposes in a non-commercial/industrial area?	Yes ☐	No ☐	☐
9.	Can it be guaranteed that the implemented measures will not severely impair the machine's ability to perform its function?	Yes ☐	No ☐	☐

Table 103: Questions for a validation in accordance with EN 12100 (example)

No	Questions	Applicable		Completed
1.	Has a risk assessment been conducted?	Yes ☐	No ☐	☐
2.	Have an error list and a validation plan been drawn up?	Yes ☐	No ☐	☐
3.	Was the validation plan, including analysis and inspection, processed and a validation report compiled? The validation procedure must include the following inspections as a minimum:	Yes ☐	No ☐	☐
	a) Inspection of components: Is the ARS 2000 FS used with the FSM 2.0 – MOV (inspection using the rating plates)?	Yes ☐	No ☐	☐
	b) Is the wiring correct (check the wiring diagram)?	Yes ☐	No ☐	☐
	– Are safety command devices, e. g. emergency stop switch, protective door switch, light curtains, etc. connected to X40?	Yes ☐	No ☐	☐
	– Are the safety command devices suitable for the requirements of the application and wired appropriately?	Yes ☐	No ☐	☐
	c) Testing of the parameterisation:	Yes ☐	No ☐	☐
	– Was the parameterisation of the safety module completed and all the parameters validated?	Yes ☐	No ☐	☐
	– Was the parameter set printed and added to the validation plan?	Yes ☐	No ☐	☐
	d) Functional tests:	Yes ☐	No ☐	☐
	– Actuation of the emergency stop of the system: Is the drive shut down?	Yes ☐	No ☐	☐
	– Actuation of the emergency stop of the system: If only one of the inputs DIN4xA or DIN4xB allocated to the emergency stop is activated - is the allocated safety function executed immediately and the error "Discrepancy time violation" (display 57-1) generated after the discrepancy time in the ARS 2000 FS?	Yes ☐	No ☐	☐
	– Actuation of the additional safety functions of the system – perform separately for each safety function: If only one of the two-channel inputs DIN4xA/B allocated for the safety function request is activated - is the allocated safety function executed immediately and the error “Discrepancy time violation” (display 57-1) generated after the discrepancy time in the ARS 2000 FS?	Yes ☐	No ☐	☐

No	Questions	Applicable		Completed
	– When using safe outputs – perform separately for each output: Do both outputs DOUT4xA/B switch off equivalently when the corresponding switching condition is present and is the safe status implemented in the downstream safety switching device if there is an error (cable break, short circuit, etc.)?	Yes ☐	No ☐	☐
	– Only when using a safety switching device with analysis of the acknowledgement contact C1/C2: In the event of a short circuit from C1 to C2, is the drive shut down no later than when the next safety requirement is issued?	Yes ☐	No ☐	☐
	– Is a restart inhibited? That is, does no movement occur when the emergency stop button is pressed and the enable signals are active unless a start command is first acknowledged by the input "Restart"?	Yes ☐	No ☐	☐

Table 104: Questions for a validation in accordance with EN ISO 13849-2 (example)

5 Operation

5.1 Obligations of the operator

The functionality of the safety module FSM 2.0 – MOV is to be checked at adequate intervals. It is the responsibility of the operator to choose the type of check and time intervals in the specified time period. The check is to be conducted such that flawless functioning of the safety device can be verified in interaction with all components.

Proof test interval ➔ Appendix 7, Table 110.

⚠ **Warning**

Danger of the failure of the safety function!

If there is a voltage failure, the safety functions are no longer guaranteed (exception: Safe Torque Off, STO; Safe Brake Control, SBC).

A failure of the safety function can result in serious, irreversible injuries, e.g. due to uncontrolled movements of the connected actuator equipment.

- ❖ Ensure that your application has a reliable power supply or provide other appropriate measures.

5.2 Maintenance and care

The safety module does not require any maintenance.

5.3 Protective functions

5.3.1 Supply - Overvoltage and reverse polarity protection voltage monitoring

The 24 V power supply comes from the basic unit. The approved operating voltage range is monitored by the safety module.
In addition, the power supply of the safety module is specially protected against

- Surges in accordance with EN 61326-3-1.
- A rise in the 24 V supply to up to 60 V in case of error (specification of the PELV supply).

Reverse polarity protection is provided by the basic unit.

5.3.2 Power supply for the internal electronics

The internal operating voltages are generated from the 24 V supply.

The internal electronic supply voltages are provided redundantly.

This means that the two microcontrollers in the safety module are powered independently.

They alternately monitor all the internal operating voltages.

5.3.3 Fail-safe mode power supply

The core of the activation of the outputs is the so-called "fail-safe mode power supply". Each microcontroller uses a dynamic signal to generate its own (internal) auxiliary power supply (U_FS1, U_FS2) to activate the different (safe) outputs for

- the power supply for driver activation, separately for the top and bottom switches,
- brake activation, separate for the BR+ and BR- circuit breakers,
- the digital outputs DOUT40 – DOUT42, separate for Pin A and Pin B.

U_FS1 affects the outputs activated by microcontroller 2, and, in return, U_FS2 affects the outputs of microcontroller 1. This ensures that, if there is an error, each microcontroller can switch off the outputs of the other microcontroller.

When a microcontroller fails (for whatever reason - hardware error, program crash, etc.), the corresponding "Fail-safe mode" power supply fails and the outputs are switched off.

5.3.4 Protective functions for the digital outputs

The digital outputs are protected against:

- Short circuit to 0 V and 24 V and PE
- Any cross circuits to other outputs
- Voltage surge to 60 V

During operation, active outputs are monitored using test pulses.
If there is an error, the outputs are switched off, possibly all at the same time.

5.3.5 Protective functions for the digital inputs

The digital inputs are protected against:

- Short circuit to 0 V and 24 V and PE
- Any cross circuits to other outputs
- Surge malfunctions
- Voltage surge to 60 V

During operation, the inputs are monitored using internal test pulses.
The connected passive sensors are monitored using external test pulses via DOUT4x.
In the case of multi-channel inputs, a plausibility check takes place for simultaneous switching with discrepancy time monitoring.

5.3.6 Protective functions for the brake activation

The outputs for brake activation are protected against:

- Short circuit to 0 V and 24 V and PE
- Any cross circuits to other outputs
- Voltage surge to 60 V

During operation, active outputs are monitored using test pulses.
If there is an error, the outputs are switched off.

5.3.7 Protective functions of the supply for driver activation

The outputs for driver activation are protected against:

- Short circuit to 0 V and 5 V, as well as external voltage up to 60 V
- Cross circuits between the two supplies
- Voltage surge to 60 V

During operation, active outputs are monitored using test pulses.

If there is an error, the outputs are switched off.

5.3.8 Protective function for the connected position encoder

The function of the position encoder is continuously monitored during operation.

What is monitored depends on the kind of encoder being used, e.g.:

- Monitoring of the analogue tracking signals, amplitudes and vector length monitoring for SIN/COS and HIPERFACE encoders, as well as resolvers
- Monitoring of communication for purely serial encoders
- Additional plausibility check of the position data using acceleration monitoring
- Comparison of the position and speed data of position encoder 1 with those of position encoder 2 in a cross-comparison between the microcontrollers
- Timeout control in case of idling and requested safety function for position encoders without forced dynamisation (24 hr. monitoring).

5.3.9 Internal protective function of the electronics on the safety module

The safety module has countless additional internal monitoring functions, which can be performed by the internal microcontrollers for one another:

- Dynamisation of many internal analogue signals using test pulses
- Factory production control of the microcontroller during operation using memory tests, OP code tests, stack and program sequence monitoring
- Cross-comparison of correct program execution and synchronous program processing between microcontroller 1 and microcontroller 2
- Cross-comparison of all key operating statuses and key status variables between microcontroller 1 and microcontroller 2
- Monitoring of ambient conditions (temperature)
- Monitoring of the internal communication interfaces
- Monitoring of communication to outside
- Monitoring of the data integrity of the safe parameter sets
- Monitoring of the operating statues and changeover
- Monitoring of the parameterisation session (session, password, master control, etc.)
- Monitoring of the error status

5.3.10 Monitoring compliance with the requested safety functions

All the requested safety functions and logic functions are monitored permanently in the safety module. If a safety limit is violated, the corresponding error is triggered. Monitoring primarily comprises:

- Compliance with the set speed limits
- Compliance with the set position limits
- Monitoring of idling
- Compliance with the requested time conditions
- Monitoring of feedback signals (existence, runtime performance)
- 24 hr monitoring (for Safe Operating Stop SOS and Safe Brake Control SBC)

5.4 Diagnostics and fault clearance

5.4.1 LED indicator on the safety module

The operating status is displayed on the two-colour Status LED of the safety module.

➔ Figure 3 in Section 2.1.4.

The following statuses are displayed:

LED indicator	**Operating status**	**Status signal** [1)]
Flashes red	Safety module is in the status "Internal error", error in the safety module.	VOUT_ERROR = 1
Lights red	Safety module is in the status "Safety condition violated", error response started.	VOUT_SCV = 1 VOUT_SFR = 1
Lights yellow	Safety module is in the status "Safe state reached".	VOUT_SSR = 1 VOUT_SFR = 1
Flashes yellow	Safety module is in the status "Safety function requested, not yet reached".	VOUT_SFR = 1
Flashes red/green	Safety module is in the status "Delivery status - parameterisation of servo drive". The drive is disconnected, all digital IOs are de-energised.	VOUT_SERVICE = 1 VOUT_PS_EN = 1
Flashes green	– Safety module is in the status "Service" (basic status). – The parameter set of the safety module has not been validated. – There is no parameter set in the servo drive. – A parameterisation session was opened. – Parameter sets in the servo drive and in the safety module deviate.	VOUT_SERVICE = 1 VOUT_PS_EN = 0
Lights green	Safety module is in the status "Ready for operation, no safety function requested". Safety module has been initialised correctly and is ready for operation.	VOUT_READY = 1 VOUT_PS_EN = 1
Off	Safety module has not been initialised / is not ready for operation.	VOUT_READY = 0 VOUT_PS_EN = 0

1) Component of the "virtual outputs" ➔ Section 8.1.3, Table 154.

Table 105: LED indicator of the safety module

You can find the complete description of the statuses in ➔ Section 2.10.1, Table 91.

5.4.2 7-segment display of the servo drive

→ **Note**

The 7-segment display of the servo drive is a purely diagnostic display. The display of safety-relevant data would require an upstream function test of the display - this is not intended.

Status signals of the servo drive are displayed on the 7-segment display of the servo drive. In addition, the safety module can output status and error messages via the 7-segment display, if the servo drive is not in an error state.

5.4.2.1 Display of strings

The individual characters are displayed in succession. The display goes blank briefly each time the character changes.

The display is repeated at regular intervals. There is a break between the last character of the string and the first character of the repeat and the display goes dark briefly.

Strings can also "flash rapidly". In this case, each character flashes multiple times during the display time.

5.4.2.2 Display of errors

Only errors and warnings are displayed (an error has occurred, whose response was not parameterised as "No reaction, but logging").

Errors of the safety module are displayed in the same way as the errors in the servo drive.

5.4.2.3 A safety function was requested

Functions, which result in a stop of the drive (STO, SOS, SS1, SS2) are given preference, otherwise the most recently displayed safety function is displayed.
If a safety function has been requested, but the safe status has not yet been reached, then the name of the function flashes rapidly.
The requested safety functions are displayed as described in the following table.

Safety function	**Display**	
STO	S t O	
SS1	S S 1	
SS2	S S 2	
SOS	S O S	
USF0 (with SSF0: SLS, SSR, SSM)	U S F 0	
USF1 (with SSF1: SLS, SSR, SSM)	U S F 1	
USF2 (with SSF2: SLS, SSR, SSM)	U S F 2	
USF3 (with SSF3: SLS, SSR, SSM)	U S F 3	
SBC	S b C	

Table 106: Display of the safety functions

5.4.2.4 Other displays

The following table shows other displays connected with the safety module.

Function/status	**Display**	
Active parameterisation session The string is displayed at regular intervals for as long as a parameterisation session occurs.	F S P A r A	
Identify servo drive The string HELLO followed by the serial number[1)] of the basic unit is displayed at regular intervals for as long as the "Identification" function is active (wave function).	H E L L O ...	

1) The serial number of the basic unit is displayed in the info window of the MSC and in the SafetyTool. In addition, you can find the serial number on a little sticker on the side of the device.

Table 107: Other displays

5.5 Error messages and error handling

5.5.1 Error numbers

The error numbers 51 to 59 are reserved for the safety module.

The table below contains an overview of the allocation.

No.	Description
51-x	Servo drive: Hardware error (safety module available, module replacement).
52-x	Servo drive: Safety module error (state machine, discrepancy time, etc.) and servo drive errors, if they affect the safety module.
53-x	Safety module: (Errors of the safety module).
54-x	
55-x	
56-x	
57-x	
58-x	
59-x	

Table 108: Error messages generated by the servo drive and the safety module

5.5.2 Error acknowledgement

Errors 51-x and 52-x generated by the servo drive can be acknowledged via the servo drive
➔ product manual ARS 2100 FS and product manual ARS 2302 – ARS 2310 FS.

Errors 53-x to 59-x are generated by the safety module and can **only** be acknowledged via the safety module.

Acknowledgement takes place using the parameterisable control input on the safety module or in the SafetyTool (on the **Safety module** start page or in the **Error display** window – Menu **Tools/Diagnostics/Errors**. In so doing, all the errors, including the error of the basic unit, are acknowledged as far as possible.

After a restart of the servo drive (Reset button of the basic unit or switch-off/on of the power supply), the errors are also "acknowledged", provided that the cause no longer exists.

For additional information on error acknowledgement in the safety module ➔ Section 2.8.3.

5.5.3 Error messages

If an error occurs, the safety module indicates this using a red or flashing red LED. In addition, the servo drive ARS 2000 FS flashes an error message in the 7-segment display. An error message consists of an E (for Error), a main index and sub-index, e.g.: **E 0 1 0**.

Warnings have the same number as an error message. In contrast to error messages, however, warnings are preceded and followed by hyphens, e.g.: **- 1 7 0 -**.

Section 5.6 lists the messages that are relevant for the functional safety in combination with the safety module.
The complete list of error messages can be found in the product manual of the servo drive that is used.

Table 109 explains the entries in the tables in Section 5.6:

Column	Significance
No.	Main index and sub-index of the error message.
Code	The Code column includes the CANopen error code (Hex).
Message	Message that is displayed in the MSC.
Cause	Possible causes for the message.
Action	Action by the user.
Reaction	The Reaction column includes the error response (default setting, partially configurable): – PS off (switch off output stage), – MCStop (stop with maximum current), – QStop (switch off servor drive enable), – Warn (warning), – Ignore (no message, only entry in buffer), – NoLog (no message and no entry in buffer). The reaction to errors 53-x to 59-x are configured using the SafetyTool: – SBC + STO request + and set all digital outputs to "0" [8] – SBC + STO request [7] – STO request [6] – SBC SS1 request [5] – SS1 request [4] – SS2 request [3] – Generation of a warning, no further reaction [2] – corresponds to "Warn" – No reaction, but logging [1] – corresponds to "Ignore" – No reaction, no logging [0] – corresponds to "NoLog"

Table 109: Explanations of the table "Error messages of the ARS 2000 FS"

If an error message cannot be acknowledged, the cause must first be remedied in accordance with the recommended measures. Then reset the servo drive, and check whether the cause of the error, and the error message, have been eliminated.

5.6 Error messages with instructions for fault clearance

Errors of groups 0 cannot be parameterised. This means that the reaction of the servo drive to the different operating states cannot be influenced.

Error group 0		Information		
No.	**Code**	**Message**		**Reaction**
0-0	-	**Invalid error**		Ignore
		Cause	Information: An invalid error entry (corrupted) was found in the permanent event memory marked with this error number. The system time entry is set to 0.	
		Action	–	
0-1	-	**Invalid error detected and corrected**		Ignore
		Cause	Information: An invalid error entry (corrupted) was found in the permanent event memory and corrected. If necessary, contact the Technical Support.	
		Action	–	
0-2	-	**Error cleared**		Ignore
		Cause	Information: Active errors were acknowledged.	
		Action	–	
0-8	-	**Servo drive switched on**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-9	-	**Servo drive: Change safety parameters**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-10	-	**FSM: Change parameters**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-11	-	**FSM module change (previous type)**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-12	-	**FSM module change (new type)**		Ignore

Error group 0		Information		
No.	**Code**	**Message**		**Reaction**
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-13	-	**FSM: Clear error**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-14	-	**FSM: Request safety function**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-15	-	**FSM: Open parameterisation session**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-16	-	**FSM: Close parameterisation session**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-17	-	**FSM: Change password**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-18	-	**FSM: Reset password**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-19	-	**FSM: Load parameter set**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	
0-20	-	**FSM: Save parameter set**		Ignore
		Cause	Information: ➔ Entry in the permanent event memory.	
		Action	–	

Error group 51		Safety module/function		
No.	**Code**	**Message**		**Reaction**
51-0	8091h	**No/unknown FSM module or driver supply faulty**		PSoff
		Cause	Internal voltage error of the safety module or fieldbus activation module.	
		Action	❖ Module presumably defective. If possible, replace with another module.	
		Cause	No safety module detected or unknown module type.	
		Action	❖ Install a safety module or fieldbus activation module that is suitable for the firmware and hardware. ❖ Load a firmware that is suitable for the safety module or fieldbus activation module; see the type designation on the module.	
51-2	8093h	**FSM: Unequal module type**		PSoff
		Cause	Type or revision of the module does not fit the project planning.	
		Action	❖ Check whether correct module type and correct version are being used. ❖ With module replacement: Module type not yet designed. Accept currently integrated safety module or fieldbus activation module.	
51-3	8094h	**FSM: Unequal module version**		PSoff
		Cause	Type or revision of the module is not supported.	
		Action	❖ Install a safety module or fieldbus activation module that is suitable for the firmware and hardware. ❖ In the basic unit, load a firmware that is suitable for the module; see the type designation on the module.	
		Cause	The module type is correct but the module version is not supported by the basic unit.	
		Action	❖ Check module version; if possible use module of same version after replacement. Install a safety module or fieldbus activation module that is suitable for the firmware and hardware. ❖ If only a module with a more recent version is available: In the basic unit, load a firmware that is suitable for the module; see the type designation on the module.	
51-4	8095h	**FSM: SSIO communication error**		PSoff
		Cause	Fault in the internal communication connection between the basic unit and the safety module.	
		Action	❖ Identify any source of stray radiation in the environment of the servo drive. ❖ Replace the module or basic unit. ❖ Contact the Technical Support.	

Error group 51		**Safety module/function**		
No.	**Code**	**Message**		**Reaction**
51-5	8096h	**FSM: Error in brake activation**		PSoff
		Cause	Internal hardware error (brake activation control signals) of the safety module or fieldbus activation module.	
		Action	❖ Module presumably defective. If possible, replace with another module.	
		Cause	Error in brake driver circuit section in the basic unit.	
		Action	❖ Basic unit presumably defective. If possible, replace with another basic unit.	
51-6	8097h	**FSM: Non-identical module serial number**		PSoff
		Cause	Serial number of currently connected safety module is different from the stored serial number.	
		Action	Error occurs only after replacement of the FSM 2.0 – MOV. ❖ With module replacement: Module type not yet designed. Accept currently integrated FSM 2.0 – MOV. ❖ Check the parameterisation of the FSM 2.0 – MOV in view of the application, since the modules have been replaced.	

Error group 52		Safety function		
No.	**Code**	**Message**		**Reaction**
52-1	8099h	**Safety function: Discrepancy time overrun**		PSoff
		Cause	– Control ports STO-A and STO-B are not actuated simultaneously.	
		Action	❖ Check discrepancy time.	
		Cause	– Control ports STO-A and STO-B are not wired in the same way.	
		Action	❖ Check discrepancy time.	
		Cause	Upper and lower switch supply not simultaneously activated (discrepancy time exceeded) – Error in control / external circuitry of safety module. – Error in safety module.	
		Action	❖ Check circuitry of the safety module – are the inputs STO-A and STO-B switched off on two channels and simultaneously? ❖ Replace safety module if you suspect it is faulty.	
52-2	809Ah	**Safety function: Failure of driver supply with active PWM activation**		PSoff
		Cause	Failure of driver supply with active PWM	
		Action	❖ The safe status was requested with power output stage enabled. Check integration into the safety-orientated interface.	
52-3	809Bh	**FSM: Rotational speed limits in basic unit overlap**		PSoff
		Cause	Basic unit reports error if the currently requested direction of movement is not possible because the safety module has blocked the setpoint value in this direction. Error may occur in connection with the SSFx safe speed functions if an asymmetrical speed window is used where one limit is set to zero. In this case, the error occurs when the basic unit moves in the blocked direction in the Positioning mode.	
		Action	❖ Check application and change if necessary.	

Error group 53		Violation of safety conditions		
No.	**Code**	**Message**		**Reaction**
53-0	80A1h	**USF0: Safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF0 in operation / when USF0 / SSF0 requested.	
		Action	Check when the violation of the safety condition occurs: a) During dynamic braking to safe rotational speed b) After the drive has reached the safe speed. ❖ With a) Critical check of braking ramp – record trace - can the drive follow the ramp? ❖ Change parameters for the slowdown ramp or start time / delay times for monitoring. ❖ With b) Check how far the current speed is from the monitored limit speed; increase distance if necessary (parameter in safety module) or correct speed specified by controller.	
53-1	80A2h	**USF1: Safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF1 in operation / when USF1 / SSF1 requested.	
		Action	❖ See USF0, error 53-0.	
53-2	80A3h	**USF2: Safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF2 in operation / when USF2 / SSF2 requested.	
		Action	❖ See USF0, error 53-0.	
53-3	80A4h	**USF3: Safety condition violated**		configurable
		Cause	– Violation of monitored speed limits of the SSF3 in operation / when USF3 / SSF3 requested.	
		Action	❖ See USF0, error 53-0.	

Error group 54		Violation of safety conditions		
No.	**Code**	**Message**		**Reaction**
54-0	80AAh	**SBC: Safety condition violated**		configurable
		Cause	– Brake should engage; no feedback received within the expected time.	
		Action	❖ Check how the feedback signal is configured – was the correct input selected for the feedback signal? ❖ Does the feedback signal have the correct polarity? ❖ Check whether the feedback signal is actually switching. ❖ Is the parameterised time delay for the analysis of the feedback signal appropriate to the brake used (measure switching time if necessary)?	
54-2	80ACh	**SS2: Safety condition violated**		configurable
		Cause	– Actual speed outside permitted limits for too long.	
		Action	Check when the violation of the safety condition occurs: a) During dynamic braking to zero. b) After the drive has reached zero speed. ❖ With a) Critical check of braking ramp – record trace - can the drive follow the ramp? Change parameters for the slowdown ramp or start time / delay times for monitoring. ❖ With a) If the option "Trigger basic unit quick stop" is activated: Critical check of the basic unit's quick stop ramp. ❖ With b) Check whether the drive continues to oscillate after reaching the zero speed or remains at idle and stable – increase monitoring tolerance time if necessary. ❖ With b) If the actual speed value is very noisy at rest. Check and if necessary adjust expert parameters for speed recording and detection of idling.	
54-3	80ADh	**SOS: Safety condition violated**		configurable
		Cause	– Angle encoder analysis reports "Motor running" (actual speed exceeds limit). – Drive has rotated out of its position since reaching the safe state.	
		Action	❖ Check the position tolerance for the SOS monitoring and increase if necessary, if this is permissible. ❖ If the actual speed value is very noisy when at rest: Check and if necessary adjust expert parameters for speed recording and detection of idling.	

54-4	80AEh	**SS1: Safety condition violated**		configurable
		Cause	– Actual speed outside permitted limits for too long.	
		Action	Check when the violation of the safety condition occurs: a) During dynamic braking to zero. b) After the drive has reached zero speed. ❖ With a) Critical check of braking ramp – record trace - can the drive follow the ramp? Change parameters for the slowdown ramp or start time / delay times for monitoring. ❖ With a) If the option "Trigger basic unit quick stop" is activated: Critical check of the basic unit's quick stop ramp. ❖ With b) Check whether the drive continues to oscillate after reaching the zero speed or remains at idle and stable – increase monitoring tolerance time if necessary. ❖ With b) If the actual speed value is very noisy at rest: Check and if necessary adjust expert parameters for speed recording and detection of idling.	
54-5	80AFh	**STO: Safety condition violated**		configurable
		Cause	– Internal hardware error (voltage error) of the safety module.	
		Action	❖ Module presumably defective. If possible, replace with another module.	
		Cause	– Error in driver circuit section in the basic unit.	
		Action	❖ Basic unit presumably defective. If possible, replace with another basic unit.	
		Cause	– No feedback received from basic unit to indicate that output stage was switched off.	
		Action	❖ Check whether the error can be acknowledged and whether it occurs again upon a new STO request – if yes: Basic unit presumably defective. If possible, replace with another basic unit.	
54-6	80B0h	**SBC: Brake not vented for > 24 hrs**		configurable
		Cause	– Error occurs when SBC is requested and the brake has not been opened by the basic unit in the last 24 hours.	
		Action	❖ If the brake is actuated via the brake driver in the basic unit [X6]: The brake must be energised at least once within 24 hours before the SBC request because the circuit breaker check can only be performed when the brake is switched on (energised). ❖ Only if brake control takes place via DOUT4x and an external brake controller: Deactivate 24 hr monitoring in the SBC parameters if the external brake controller allows this.	

54-7	80B1h	**SOS: SOS requested > 24 hrs**		configurable
		Cause	– If SOS is requested for more than 24 hours, the error is triggered.	
		Action	❖ Terminate SOS and move axle once during this time.	

Error group 55		Measuring of actual value 1		
No.	**Code**	**Message**		**Reaction**
55-0	80C1h	**No actual rotational speed / position value available or idle > 24 hrs**		configurable
		Cause	– Subsequent error when a position encoder fails. – Safety function SSF, SS1, SS2 or SOS requested and actual rotational speed value is not valid.	
		Action	❖ Check the function of the position encoder(s) (see following error).	
55-1	80C2h	**SINCOS encoder [X2B] - Tracking signal error**		configurable
		Cause	– Vector length sin²+cos² is outside the permissible range. – The amplitude of one of the two signals is outside the permissible range. – Offset between analogue and digital signal is greater than 1 quadrant.	
		Action	Error may occur with SIN/COS and HIPERFACE encoders. ❖ Check the position encoder. ❖ Check the connection wiring (broken wire, short between two signals or signal / screening). ❖ Check the supply voltage for the position encoder. ❖ Check the motor cable / screening on motor and drive side – EMC malfunctions may trigger the error.	
55-2	80C3h	**SINCOS encoder [X2B] - Standstill > 24 hrs**		configurable
		Cause	– Input signals of the SinCos encoder have not changed by a minimum amount for 24 hours (when safety function is requested).	
		Action	❖ Terminate SS2 or SOS and move axle once during this time.	
55-3	80C4h	**Resolver [X2A] - Signal error**		configurable
		Cause	– Vector length sin²+cos² is outside the permissible range. – The amplitude of one of the two signals is outside the permissible range. – Input signal is static (same values to right and left of maximum).	
		Measure	❖ Check the resolver. ❖ Check the connection wiring (broken wire, short between two signals or signal / screening). ❖ Check for a failure of the primary radiator signal ❖ Check the motor and encoder cable / screening on motor and drive side. EMC malfunctions can trigger the error.	

55-7	80C6h	**Other encoder [X2B] - Faulty angle information**		configurable
		Cause	– "Angle faulty" message is sent from basic unit when status lasts for longer than the allowed time. – Encoder at X2B is analysed by the basic unit, – Encoder is faulty.	
		Action	❖ Check the position encoder at X2B. ❖ Check the connection wiring (broken wire, short between two signals or signal / screening). ❖ Check the supply voltage for the EnDat encoder. ❖ Check the motor cable / screening on motor and drive side – EMC malfunctions may trigger the error.	
55-8	0x80C7	**Impermissible acceleration detected**		configurable
		Cause	– Error in connected position encoder. – EMC malfunctions affecting the position encoder. – Impermissibly high acceleration rates in the movement profiles. – Acceleration limit parameterised too low. – Angle jump after reference movement in the position data transmitted from the basic unit to the safety module.	
		Action	❖ Check the connected position encoder: If further error messages occur in conjunction with the encoders, then eliminate their cause first. ❖ Check the motor and encoder cable / screening on motor and drive side. EMC malfunctions can trigger the error. ❖ Check the setpoint specifications / movement profiles of the controller: Do they contain impermissibly high accelerations above the limit value for acceleration monitoring (P06.07)? ❖ Check whether the limit value for acceleration monitoring was parameterised correctly - the limit value (P06.07) should be at least 30% ... 50% above the maximum acceleration actually occurring. ❖ In case of an angle jump in the position data transmitted from the basic unit - Acknowledge error once.	

Error group 56		Measuring of actual value 2		
No.	**Code**	**Message**		**Reaction**
56-8	80D1h	**Rotational speed / angle difference, encoder 1 - 2**		configurable
		Cause	– Rotational speed difference between encoders 1 and 2 of one µC outside the permissible range for longer than the allowed time. – Angle difference between encoders 1 and 2 of one µC outside the permissible range for longer than the allowed time.	
		Action	❖ Problem may occur if two position encoders are used in the system and they are not "rigidly coupled". ❖ Check for elasticity or looseness, improve mechanical system. ❖ Adjust the expert parameters for the position comparison if this is acceptable from an application point of view.	
56-9	0x80D2	**Error, cross-comparison of encoder analysis**		configurable
		Cause	Cross-comparison between µC1 and µC2 has detected an angle difference or rotational speed difference or difference in capture times for the position encoders.	
		Action	❖ Timing disrupted. If the error occurs again after a reset, the safety module is presumably faulty.	

Error group 57		**Input/output error**		
No.	**Code**	**Message**		**Reaction**
57-0	80E1h	**Error, I/O self test (internal/external)**		configurable
		Cause	– Internal error of digital inputs DIN40 ... DIN43 (detected via internal test signals). – Error at brake output at X6 (signalling, detected by test pulses). – Internal error of brake output (detected via internal test signals). – Internal error of digital outputs DOUT40 – DOUT42 (detected via internal test signals).	
		Action	❖ Check the connection wiring for the digital outputs DOUT40 ... DOUT42 (short circuit, cross circuit, etc.). ❖ Check the connection wiring for the brake (short circuit, cross circuit, etc.). ❖ Brake connection: The error may occur with long motor cables if: 1. The brake output X6 was configured for the brake (this is the case with factory settings!) and 2. A motor without a holding brake is used and the brake connection lines in the motor cable are terminated at X6. In this case: Disconnect the brake connection lines at X6. ❖ If there is no error in the connection wiring, there may be an internal error in the module (check by swapping the module).	
57-1	80E2h	**Digital inputs - Signal level error**		configurable
		Cause	Exceeding / violation of discrepancy time with multi-channel inputs (DIN40 ... DIN43, two-handed control device, mode selector switch).	
		Action	❖ Check the external active and passive sensors – do they switch on two channels and simultaneously (within the parameterised discrepancy time). ❖ Two-handed control device: Check how the device is operated by the user – are both pushbuttons pressed within the discrepancy time? Give training if necessary. ❖ Check the set discrepancy times – are they sufficient?	
57-2	0x80E3	**Digital inputs - Test pulse error**		configurable
		Cause	– One or more inputs (DIN40 ... DIN49) were configured for the analysis of the test pulses of the outputs (DOUT40 ... DOUT42). The test pulses from DOUTx do not arrive at DIN4x.	
		Action	❖ Check the wiring (shorts after 0 V, 24 V, cross circuits). ❖ Check the assignment – correct output selected / configured for test pulse?	

57-6	0x80E7	**Electronics temperature too high**		configurable
		Cause	– The safety module's temperature monitor has been triggered; the temperature of µC1 or µC2 was below -20° or above +75°C.	
		Action	❖ Check the operating conditions (ambient temperature, control cabinet temperature, installation situation in the control cabinet). ❖ If the servo drive is experiencing high thermal load (high control cabinet temperature, high power consumption / output to motor, large number of occupied slots), a servo drive of the next highest output level should be used.	

Error group 58		**Error during communication / parameterisation**		
No.	**Code**	**Message**		**Reaction**
58-0	80E9h	**Plausibility check of parameters**		configurable
		Cause	The plausibility check in the safety module produced errors, e.g. an invalid angle encoder configuration; the error is triggered when a validation code is requested by the SafetyTool and when parameters are backed up in the safety module.	
		Action	❖ Note instructions for SafetyTool for complete validation; critically check parameterisation.	
58-1	0x80EA	**General error, parameterisation**		configurable
		Cause	Parameter session active for > 8 hrs. The safety module has thus terminated the parameterisation session. The error message is saved in the permanent event memory.	
		Action	❖ Terminate parameterisation session within 8 hrs. If necessary, start a new parameterisation session and continue.	
58-4	80EDh	**Buffer, internal communication**		Fixed [8]
		Cause	– Communication connection faulty. – Timeout / data error / incorrect sequence (packet counter) in data transmission between the basic unit and safety module. – Too much data traffic, new requests are being sent to safety module before old ones have been responded to.	
		Action	❖ Check communication interfaces, wiring, screening, etc. ❖ Check whether other devices have read access to the servo drive and safety module during a parameterisation session - this may overload the communication connection. ❖ Check whether the firmware versions of the safety module and basic unit and the versions of the Metronix ServoCommander® and SafetyTool are compatible.	
58-5	80EEh	**Communication module - basic unit**		Fixed [8]
		Cause	– Packet counter error during transmission µC1 <-➔ µC2. – Checksum error during transmission µC1 <-➔ µC2.	
		Action	❖ Internal malfunction in the servo drive. ❖ Check whether the firmware versions of the safety module and basic unit and the versions of the Metronix ServoCommander® and SafetyTool are compatible.	

58-6	80EFh	**Error in cross-comparison for processors 1 - 2**		Fixed [8]
		Cause	Timeout during cross-comparison (no data) or cross-comparison faulty (data for µC1 and µC2 are different). – Error in cross-comparison for digital I/O. – Error in cross-comparison for analogue input. – Error in cross-comparison for internal operating voltage measurement (5 V, 3.3 V, 24 V) and reference voltage (2.5 V). – Error in cross-comparison for SIN/COS angle encoder analogue values. – Error in cross-comparison for programme sequence monitoring. – Error in cross-comparison for interrupt counter. – Error in cross-comparison for input map. – Error in cross-comparison for violation of safety conditions. – Error in cross-comparison for temperature measurement.	
		Action	This is an internal error in the module that should not occur during operation. ❖ Check the operating conditions (temperature, air humidity, condensation). ❖ Check the EMC wiring as specified and screening design; are there any external interference sources? ❖ Safety module may be faulty – is error eliminated after replacing the module? ❖ Check whether new firmware for the servo drive or a new version of the safety module is available from the manufacturer.	

Error group 59		Internal FSM error		
No.	**Code**	**Message**		**Reaction**
59-1	80F1h	**Fail-safe mode supply/safe pulse inhibitor**		Fixed [8]
		Cause	– Internal error in module in failsafe supply circuit section or in the driver supply for the upper and lower switches.	
		Action	❖ Module faulty, replace.	
59-2	80F2h	**Error external power supply**		Fixed [8]
		Cause	– Reference voltage 2.5 V outside tolerance. – Logic supply overvoltage +24 V detected.	
		Action	❖ Module faulty, replace.	
59-3	80F3h	**Error internal power supply**		Fixed [8]
		Cause	– Voltage (internal 3.3 V, 5 V, ADU reference) outside the permissible range.	
		Action	❖ Module faulty, replace.	
59-4	80F4h	**Error management: Too many errors**		Fixed [8]
		Cause	– Too many errors have occurred simultaneously.	
		Action	❖ Clarify: What is the status of the installed safety module - does it contain a valid parameter set? ❖ Read out and analyse the permanent event memory of the basic unit via Metronix ServoCommander®. ❖ Eliminate causes of error step by step. ❖ Install safety module with "delivery status" and perform commissioning of basic unit. ❖ If this is not available: Set factory settings in the safety module, then copy data from the basic unit and perform complete validation. Check whether the error occurs again.	
59-7	80F7h	**FLASH checksum error**		Fixed [8]
		Cause	– Voltage interruption / power off while parameters were being saved. – FLASH memory in safety module corrupted (e.g. by extreme malfunctions).	
		Action	Check whether the error recurs after a RESET. If it does: ❖ Parameterise the module again and validate the parameter set again. If error persists: ❖ Module faulty, replace.	

59-8	80F8h	**Internal monitoring, processor 1 - 2**		Fixed [8]
		Cause	– Serious internal error in the safety module: Error detected while dynamising internal signals – Disrupted programme sequence, stack error or OP code test failed, processor exception / interrupt.	
		Action	Check whether the error recurs after a RESET. If it does: ❖ Module faulty, replace.	
59-9	80F9h	**Other unexpected error**		Fixed [8]
		Cause	Triggering of internal programme sequence monitoring.	
		Action	❖ Check the firmware version of the basic unit and the version of the safety module – update available? ❖ Safety module faulty; replace.	

6 Service, repair, replacement, disposal

6.1 Service

The safety module includes no parts requiring service.

6.2 Repair

Repair of the safety module is not permissible. If necessary, replace the complete safety module.

- Always replace the safety module in case of an internal defect.
- Send the unchanged defective safety module, including a description of the error and the application, back to Metronix for analysis.
- Please contact your technical consultant to clarify how to return the module.

6.3 Replacement of the safety module

If a safety module fails and has to be replaced, organisational measures must be taken to ensure that an unsafe status is not created. This requires,

- that the safety module is **not** replaced by another module type without safety function (fieldbus activation module).
- that the safety module is **not** replaced by another module type with fewer functions (FSM 2.0 – MOV for FSM 2.0 – STO).
- that the revision status of the new safety module agrees with that of the old safety module or is compatible.
- that the parameterisation of the new safety module agrees with the parameterisation of the defective safety module.

Refer to the rating plate for the type designation of the safety module and the revision status ➔ Figure 1, Page 22.

Observe the required organisational measures to avoid errors in conjunction with the module replacement.

For example, you must always generate a new validation report due to the different serial number of the safety module and the new validation code.

6.3.1 Disassembly and installation

Before a module is replaced, compatibility between the safety module and basic unit must be checked, see also the section "Product identification" at the front of this document.

Information on disassembling and installing the safety module can be found Mounting / removing ➔ Section 3.1.

Tip: If the safety module to be replaced can be contacted from the SafetyTool, we recommend saving a safe parameter set of the validated actual status (start the SafetyTool in Online mode - display the parameterisation - then generate a safe parameter set).

6.3.2 Apply safety module

After replacing the module, you must first accept the new safety module again in the Metronix ServoCommander®.

Accept the serial number of the replaced safety module ➔ Section 4.3.3.3 .

6.3.3 Recommissioning with the SafetyTool

After accepting the replaced safety module, you must transfer the desired parameterisation to the safety module and then validate it.

Basic information can be found in the following sections:

- SafetyTool ➔ Section 4.5
- Parameterisation ➔ Section 4.4
- Performance test and validation ➔ Section 4.8

To do this, you must first start the SafetyTool in the online mode.

You then have the following options, depending on which data is present from the safety module to be replaced:

a) A reliable parameter set of the safety module to be replaced is available:
   - ❖ Open the parameter set in the SafetyTool and load it to the safety module. For this, the basic information of the basic unit must agree with that contained in the parameter set.

b) A stored SafetyTool project that agrees with the current parameterisation is available:
   - ❖ Set the safety module to the factory setting, if it is not in the delivery status.
   - ❖ Then open the SafetyTool project.
   - ❖ The basic information of the basic unit must agree. Otherwise, you must synchronise it.
   - ❖ Then, you can validate the individual parameter pages and load them to the safety module.

c) No stored data of the safety module to be replaced is available:
   - ❖ Set the safety module to the factory setting, if it is not in the delivery status.
   - ❖ Then proceed as for initial commissioning.

Independently of the variant a), b) or c), you must generate a validation report again, with a new validation code and new serial number of the safety module.

6.4 De-commissioning and disposal

Observe the information for dismantling the safety module in section 3.1.

6.4.1 Disposal

Observe the local regulations for environmentally appropriate disposal of electronic modules. The safety module is RoHS-compliant.

The material used in the packaging has been specifically chosen for its recyclability.

7 Technical appendix

7.1 Technical data

7.1.1 Safety engineering

Safety data		
Safety functions in accordance with EN 61800-5-2.	STO	Safe Torque Off
	SS1	Safe Stop 1
	SS2	Safe Stop 2
	SOS	Safe Operating Stop
	SLS	Safely-Limited Speed
	SSR	Safe Speed Range
	SSM	Safe Speed Monitor
	SBC	Safe Brake Control
Values in accordance with EN 61800-5-2		
SIL	SIL 3	Safety Integrity Level
PFH [h^{-1}]	9.5 x 10^{-9}	Probability of dangerous random hardware failure per hour
DC [%]	97.5	Diagnostic coverage
HFT	1	Hardware failure tolerance
SFF [%]	99.5	Safe failure fraction
T [Years]	20	Proof test interval
Values in accordance with EN 62061		
SIL	SIL CL 3	Claim limit, for a subsystem
PFH_D [h^{-1}]	9.5 x 10^{-9}	Probability of dangerous failure per hour
DC [%]	97.5	Diagnostic coverage
HFT	1	Hardware failure tolerance
SFF [%]	99.5	Safe failure fraction
T [Years]	20	Proof test interval
Values in accordance with EN 61508		
SIL	SIL 3	Safety Integrity Level
PFH [h^{-1}]	9.5 x 10^{-9}	Average frequency of dangerous failure
DC [%]	97.5	Diagnostic coverage
HFT	1	Hardware failure tolerance
SFF [%]	99.5	Safe failure fraction
T [Years]	20	Proof test interval
Values in accordance with EN ISO 13849-1		
Category[1)]	4	Category
Performance Level[1)]	PL e	Performance Level
PFH [h^{-1}]	9.5 x 10^{-9}	Average probability of a dangerous failure per hour
DC [%]	97.5	Diagnostic coverage
$MTTF_d$ [Years]	8700	Mean time to dangerous failure
T_M [Years]	20	Mission time
1) Maximum achievable classification, limitations dependent on the safety function ➔ Section 1.1.4, Table 125 as well as the circuitry and the encoders ➔ Appendix 7.2		

Table 110: Technical data: Safety data

Safety information	
Type test	The functional safety design of the product was certified by an independent testing authority in accordance with section 1.1.4, see EC-type examination certificate http://www.metronix.de.
Certificate-issuing authority	TÜV Rheinland, Certification Body of Machinery, NB 0035
Certificate no.	01/205/5058.01/14
Reliable component	Yes

Table 111: Technical data: Safety information

7.1.2 General

Mechanical		
Length / width / height	[mm]	112.2 x 99.1 x 28.7
Weight	[g]	220
Slot		Slot for functional safety modules
Note on materials		RoHS-compliant

Table 112: Technical data: Mechanical

Certifications (safety module FSM 2.0 – MOV for servo drive ARS 2000 FS)	
CE marking (see declaration of conformity at http://www.metronix.de).	According to EC Machinery Directive 2006/42/EC
	To EU EMC Directive
	The device is intended for use in an industrial environment. Additional measures for interference suppression may need to be implemented in residential areas.

Table 113: Technical data: Certifications

7.1.3 Operating and ambient conditions

Transport		
Temperature range	[°C]	-25 … +70
Air humidity	[%]	0 ... 95, at max. 40°C ambient temperature
Maximum transportation duration		Maximum 4 weeks over the entire product lifecycle

Table 114: Technical data: Transport

Storage		
Storage temperature	[°C]	-25 … +55
Air humidity	[%]	5 … 95, non-condensing or protected against condensation
Permissible altitude	[m]	3000 (above sea level)[1)]
1) Note additional limitations, such as the permissible setup altitude for the servo drives (usually < 2000 m above sea level)		

Table 115: Technical data: Storage

Ambient conditions ARS 2000 FS with safety module FSM 2.0 – MOV in FSM slot							
ARS 2000 FS …		2102 FS	2105 FS	2108 FS	2302 FS	2305 FS	2310 FS
Ambient temperature[1)]	[°C]	0 … +35	0 … +40	0 … +40	0 … +40	0 … +40	0 … +40
Ambient temperature with power reduction[1)]	[°C]	+35 … +40	+40 … +50	+40 … +50	+40 … +50	+40 … +50	+40 … +45
		An overtemperature switch-off will take place at a high power output of the basic unit and/or high load of the control section and the I/Os.					
Cooling		By means of ambient atmosphere in the servo drive, no forced ventilation.					
Air humidity	[%]	0 … 90 (non-condensing).					
		No corrosive media permitted near the device.					
Permissible setup altitude above sea level							
with rated output	[m]	1000					
with power reduction	[m]	1000 … 2000					
Degree of protection		IP20 (mounted in the ARS 2000 FS).					
Vibration / shock		Requirements of EN 61800-5-1 and EN 61800-2 are fulfilled.					

The maximum permissible operating temperature is dependent on numerous parameters, including the number of switched inputs and the load of the outputs in the FSM 2.0 – MOV, the equipment of additional modules in TECH 1 and TECH 2 in the ARS 2000 FS, the load of the power output stage in the ARS 2000 FS as well as the airflow conditions in the control cabinet. The specified values apply to a typical device configuration.
The FSM 2.0 – MOV possesses separate temperature monitoring, which switches the safety module and the basic unit off, if the electronics temperature becomes too high ➔ Section 5.6 Error 57-6.

Table 116: Technical data: Ambient conditions

Electrical operating conditions		
Galvanically isolated potential areas		Control voltage of the basic unit.
		24 V control voltage (all inputs and outputs).
		Potential-free signal contact C1/C2.
System voltage	[V]	< 50 (24 V PELV power supply in accordance with EN 60204-1).
		The 24 V power supply unit used in the system must be able to handle the voltage interruption defined in EN 60204-1.
Overvoltage category in accordance with EN 61800-5-1.		3
Degree of contamination in accordance with EN 61800-5-1.		2
		This must always be ensured through appropriate measures, e.g. through installation in a control cabinet.

Table 117: Technical data: Electrical operating conditions

EMC operating conditions	
Resistance to interference	Requirements for "second environment" in accordance with EN 61800-3 (PDS of category C3) Requirements in accordance with EN 61326-3-1
Emitted interference	Requirements for "first environment with restricted availability" in accordance with EN 61800-3 (PDS of category C2)

Table 118: Technical data: EMC operating conditions

7.1.4 Digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40]

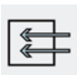
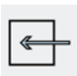
Digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49[1)]		
Input		Type 3 in accordance with IEC 61131-2
Nominal voltage	[V DC]	24
Permissible voltage range	[V]	-3 … 30
Maximum input voltage "HI" $U_{H,max}$	[V]	30
Minimum input voltage "HI" $U_{H,min}$		
Typical	[V]	11
Maximum	[V]	13[3)]
Maximum input voltage "LO" $U_{L,max}$	[V]	5
Minimum input voltage "LO" $U_{L,min}$	[V]	-3
Maximum input current "HI" $I_{H,max}$	[mA]	15
Minimum input current "HI" $I_{H,min}$	[mA]	2
Maximum input current "LO" $I_{L,max}$	[mA]	15
Minimum input current "LO" } "HI" $I_{T,min}$	[mA]	1.5[2)]
Switching delay to port pin (Low-High transition)	[ms]	< 1
Tolerance to test pulses	[ms]	0 ... 10 (can be parameterised ➔ Sections 2.4.2 and 2.4.3)

1) Designations of the data in accordance with IEC 61131-2.

2) The compliance of IT, min cannot be tested in the context of self-diagnostics. If active two-wire sensors are used on DIN40A/B ... DIN43A/B to request safety functions, then cyclical tests are required (every 24 hrs.).

3) Taking all the tolerances in the series into account, the minimum required input voltage UH, min = 13 V, which deviates from the requirement of IEC 61131.

Table 119: Technical data: Digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 [X40]

85The digital inputs DIN40A/B to DIN43A/B and DIN44 to DIN49 conform to the EMC requirements of EN 61326-3-1.

7.1.5 Digital outputs DOUT40A/B to DOUT42A/B [X40]

Digital outputs DOUT40A/B to DIN42A/B		
Output		High-side switch with pull-down
Voltage range	[V DC]	18 … 30
Permissible output current $I_{L,Nom}$ (nominal)	[mA]	< 50
Voltage loss at $I_{L,Nom}$	[V]	≤ 1 V
Residual current with switch OFF[1)]	[µA]	< 100 µA
Pulldown resistance $R_{Pulldown}$	[kΩ]	< 50 (approx. 0.6 mA at 24 V)
Short circuit / overcurrent protection		Short circuit-proof, safe against reverse polarity, overvoltage-resistant up to 60 V
Temperature protection		Switch-off of all the outputs of a group (DOUT40A to DOUT 42A or DOUT40B to DOUT 42B at overtemperature T_J > 150°
Supply port		Protection for inductive loads
Loads		
Ohmic load	[Ω]	> 500
Inductive load	[mH]	< 10
Capacitive load[2)]	[nF]	< 10
Switching delay from port pin	[ms]	< 1
Test pulse output	[ms]	0.4 … 10 (can be parameterised ➔ Section 2.9.1)

1) In specific error cases (e. g. device-internal interruption of the 24 V reference potential), the residual current may still be considerably above 100 µA. If the output is connected to an IEC 61131-compatible Type 3 input, the range of the Low status is not violated, even if there is an error.

2) Requires connection of the output to a Type 3 input and a test pulse length ≥ 400 µs. Longer test pulses may be required for other input types.

Table 120: Technical data: Digital outputs DOUT40A/B to DOUT42A/B [X40]

124The digital outputs DOUT40A/B to DOUT42A/B conform to the EMC requirements in accordance with EN 6132631.

7.1.6 Signal contact C1/C2 [X40]

Signal contact C1/C2		
Version		Relay contact, normally open
Voltage range	[V DC]	18 … 30
Output current $I_{L,Nom}$ (nominal)	[mA]	< 200
Voltage loss at $I_{L,Nom}$	[V]	$\leq$ 1
Residual current with switch OFF	[µA]	< 10
Short circuit / overcurrent protection		Not short circuit-proof, overvoltage-resistant up to 60 V
Switching delay	[ms]	< 20
Service life of acknowledgement contact	[n_{op}]	10 x 10^6 (at 24 V and $I_{Contact}$ = 10 mA, the service life is reduced with higher load currents)

Table 121: Technical data: Signal contact C1/C2 [X40]

7.1.7 24 V auxiliary voltage [X40]

24 V auxiliary voltage		
Version		Logic supply voltage routed over the servo drive (fed in at [X9], not additionally filtered or stabilised). Reverse polarity-protected, overvoltage-proof up to 60 V DC
Nominal voltage	[V]	24
Output current $I_{L,Nom}$ (nominal)	[mA]	100
Voltage loss at $I_{L,Nom}$	[V]	$\leq$ 1
Reverse polarity protection		Via series diode 100 V / 1 A
Short circuit / overcurrent protection		Protective PTC with tripping current, typ. 300 mA, overvoltage-resistant to 60 V

Table 122: Technical data: 24 V auxiliary voltage [X40]

7.1.8 Design of the connecting cable [X40]

Cabling [X40]		
Max. cable length	[m]	< 30
Screening		When wiring outside the control cabinet, use screened cable. Guide screening into the control cabinet / attach to the side of the control cabinet
Cable cross section (flexible conductors, wire end sleeve with insulating collar)		
One conductor	[mm²]	0.25 … 0.5
Two conductors	[mm²]	2 x 0.25 (with twin wire end sleeves)
Tightening torque of mating connector MC1.5_12ST3.81BK – M2	[Nm]	0.22 … 0.25

Table 123: Technical data: Cabling [X40]

7.1.9 Digital output for a holding brake on the basic unit [X6]

Digital output BR+ / BR-		
Output		High-side switch for BR+ Low-side switch for BR-
Voltage range	[V DC]	18 … 30
Permissible output current $I_{L,Nom}$ (nominal)	[mA]	< 2000
Voltage loss at $I_{L,Nom}$	[V]	≤ 1 V
Pulldown resistance $R_{Pulldown}$	[kΩ]	approx. 2.5 (approx. 10 mA at 24 V) between BR+ and BR-
Short circuit / overcurrent protection		Short circuit-proof against 24 V, 0 V and PE
Temperature protection		Switch-off of the power driver in event of over-temperature
Supply port		Protection for inductive loads
Loads		
Ohmic load	[Ω]	> 12
Inductive load	[mH]	< 1000
Capacitive load	[nF]	< 10
Switching delay from port pin	[ms]	< 1
Test pulse output	[ms]	0.4 … 10 (can be parameterised ➔ Section 2.9.2)

Table 124: Technical data: Digital output for a holding brake [X6]

The digital output of the basic unit for holding brake, BR+, BR-, complies with the EMC requirements of EN 61326-3-1.

Note

When the safety module is delivered, the SBC function is always configured in conjunction with the output [X6], even if you do not wish to use the SBC function. In applications in which the brake control lines are run in the motor cable, if no holding brake is connected on the motor side, interference can be coupled into the open brake lines. The safety module then generates the error 57-0.

❖ In these cases, please disconnect the brake control lines from X6 and route them to PE.

7.2 Safety data

7.2.1 Safety functions

7.2.1.1 Assignment of safety function – Classification

Table 125 shows the classification of the safety functions according to EN 61800-5-2

Function	**Cat., PL**[1]	**SIL**[2]	**Note**
STO	Cat. 4, PL e	SIL 3	–
SBC			–
SS2	Cat. 3, PL d or Cat. 4, PL e	SIL 2 or SIL 3	The classification is dependent on the combination of position encoders used. When a single encoder is used with SIL classification, a safe shaft connection is required ➔ Section 7.2.3, Table 128, Table 129, Table 130, Table 131 and Table 132.
SS1			
SLS			
SSR			
SSM			
SOS	Cat. 4, PL e	SIL 3	Depending on the encoder configuration, only Cat. 3, PL d or SIL 2 is achieved ➔ Section 7.2.3, Table 129, Table 130, Table 131 and Table 132. Note that the accuracy of position detection is limited ➔ 'Section 7.3.

1) Classification of category and performance level in accordance with EN ISO 13849-1

2) Classification of Safety Integrity Level in accordance with EN 62061

Table 125: Classification of the safety functions and notes

Some of the information on selected, prequalified encoder combinations is available separately.

Please consult your local contact person as necessary.

For a "safe shaft connection", fault exclusion is achieved using positive-locking and/or appropriately overdimensioned attachment elements.

Take the whole drive train up to the risk point into account.

If the movement of the motor shaft is monitored solely by a single rotary or linear encoder with a two-channel structure, then it must have a certificate of a named office according to the amount of risk reduction.

When using two encoders, the resolution limit for the motion detection for the safety functions is specified by the encoder with the lower resolution limit.

Position encoders used for idle position monitoring, e.g. SOS, and which present static output signals when at idle require dynamisation on the user side, i.e. the drive must be moved once within each 24 hour period.

The safe brake control of the FSM 2.0 – MOV is designed for SIL3 / EN 61800-5-2.
Please check whether the clamping unit you are using achieves a PL e to meet SIL 3. The clamping unit itself usually has a lower classification, meaning that the safety function SBC, in combination with the clamping unit, only achieves the lower classification.

7.2.2 Digital inputs

The relevant standards for command devices which request safety functions must be observed, e.g. EN ISO 13850 for emergency stopping.

Sensor type	**Switch type**	**Classification category, PL[1)]**	**Classification SIL[2)]**
1: General 2-channel input	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
2: Emergency stop switching device	2 N/C contacts	Cat. 4, PL e	SIL 3
3: Enabling button	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
4: Two-handed operator unit	2, consisting of 1 N/C contact, 1 N/O contact	Cat. 4, PL e	SIL 3
5: Start button	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
6: Door lock	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
7: Reliable reference switch	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
8: Light curtain	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
9: Brake feedback	1 N/C contact or 2 N/C contacts	Only as feedback for SBC	
10: General single-channel input	1 N/C contact or 1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Cat. 2, PL d	SIL 2
11: Mode selector switch	1 of n	Cat. 4, PL e	SIL 3
12: Acknowledge error	1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Cat. 2, PL d	SIL 2
13: Restart (terminate safety function)	1 N/O contact	Without allocation of test pulse Cat. 1, PL c	SIL 1
		With allocation of test pulse Cat. 2, PL d	SIL 2

1) To EN ISO 13849-1
2) To EN 61800-5-2

Table 126: Safety reference data for digital inputs

Note

- The following data on measures and DC is based on the data of the standard EN ISO 13849-1.
- The manufacturer's specifications must be used for a safety-related assessment of the sensors.
- The DC values given are only valid when the specified measures and the specified additional conditions are complied with.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

Measure	**DC**	**Comment**	**Use**
Cyclical test pulse created by dynamically changing the input signals.	90	Only effective when allocation of test pulses is active.	Cross-circuit monitoring for 1-channel sensors.
Cross-comparison of input signals with dynamic test if short-circuits cannot be detected (for multiple inputs/outputs).	90	Without allocation of test pulses. Cyclical change of the input signals required, e.g. through the process or regular actuation.	Monitoring of 2-channel sensors.
Cross-comparison of input signals with immediate and intermediate results in the logic (L) and temporal as well as logic program sequence monitoring and detection of static failures and short circuits (for multiple inputs/outputs).	99	Only with allocation of test pulses.	Monitoring of 2-channel sensors.
Plausibility check, e.g. use of normally open and normally closed contacts.	99	Only when using antivalent signals.	Monitoring of 2-channel sensors.

Table 127: Measures for digital inputs

7.2.3 Encoder systems

The relevant standards for the functional safety of electrical drives must always be observed, e.g. EN 61800-5-2. Table 128 shows the approved encoder combinations and the maximum achievable Performance Level and Safety Integrity Level.

P06.00: Selection position encoder 1	**P06.01:' Selection position encoder 2**	**Notes**	**Achievable safety level**	
			EN 61800-5-2	**ISO 13849**
Resolver (X2A)= [1]	Other encoder (X2B) = [4] 1)	–	SIL 3	Cat. 3 / PL d or Cat. 3 / PL e
Resolver (X2A)= [1]	Incremental encoder (X10) = [5]	–	SIL 3	Cat. 4 / PL e
Resolver (X2A)= [1]	None = [6]	Requires a safe shaft connection. Resolver must satisfy the SIL 2 requirements (MTTFd value, etc.)	SIL 2	Cat. 3 / PL d
SINCOS / HIPERFACE (X2B) = [2]	Incremental encoder (X10) = [5]	–	SIL 3	Cat. 4 / PL e
SINCOS / HIPERFACE (X2B) = [2]	None = [6]	Requires a safe shaft connection. Requires a SIL 2-certified encoder	SIL 2	Cat. 3 / PL d
SINCOS / HIPERFACE (X2B) = [2]	None = [6]	Requires a safe shaft connection. Requires a SIL 3-certified encoder	SIL 3	Cat. 3 / PL e
EnDat SIL (X2B) = [3]	Incremental encoder (X10) = [5]	Not a part of PS1	SIL 3	Cat. 4 / PL e
EnDat SIL (X2B) = [3]	None = [6]	Not a part of PS1 Requires a safe shaft connection. Requires a SIL 2-certified encoder	SIL 2	Cat. 3 / PL d
EnDat SIL (X2B) = [3]	None = [6]	Not a part of PS1 Requires a safe shaft connection. Requires a SIL 3-certified encoder	SIL 3	Cat. 4 / PL e
Other encoder (X2B) = [4] 1)	Incremental encoder (X10) = [5]	Please note the following.	SIL 2	Cat. 3 / PL d
Other encoder (X2B) = [4] 1)	None = [6]	Invalid, blocked by FSM 2.0 – MOV and the SafetyTool	–	–

1) Other encoder (X2B) = [4]:
- EnDat encoder without SIL certification
- BISS encoder
- Incremental encoder with A/B/N signals
- Incremental encoder with SINCOS signals
- HIPERFACE encoder without SIL

Table 128: Safety reference data for analysis of encoder systems

➔ **Note**

The actually achievable safety level for the system, consisting of FSM 2.0 – MOV, motor, axis and possibly a second position encoder, must be calculated using the safety reference data of the FSM 2.0 – MOV ➔ Section 7.1.1, and the safety reference data of the remaining components.
Please consult your sales partner if you require precalculated application suggestions.

Note the additional information:

- General information on encoder analysis and the supported position encoders ➔ Section 2.2.5.
- Information on the encoder configuration ➔ Section 2.3.2.
- Example of encoder configuration in the SafetyTool ➔ Section 4.6.4.

➔ **Note**

The suitability of the "Standard encoder" and the "Digital incremental encoder" for use in safe systems up to SIL3 (EN 61800-5-2, EN 61508) as well as PL e (EN ISO 13849) must be proven separately. For example, it must be shown that the encoders meet the requirements for CCF, $MTTF_d$, etc. Additionally, it must be shown that the encoders are suitable for the operating and ambient conditions and meet EMC requirements.

➔ **Note**

- The following data on measures and DC is based on the data of EN 61800-5-2, table in Appendix D.16.
- The manufacturer's specifications must also be used for a safety-related assessment of the position encoder.
- The DC values given for the analysis of the encoder systems in the safety module are only valid when the specified measures and the specified additional conditions are complied with.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

7.2.3.1 SIN/COS encoder / HIPERFACE encoder

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Interruption of any conductor of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Static "0" or "1" signal at the inputs and outputs, individually or simultaneously at multiple inputs/outputs	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Interruption of high-impedance status on a single input/output or multiple inputs/outputs simultaneously	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Reduction or increase of the output amplitude	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Interference vibration on one or more outputs	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)] When a signal oscillates, maximum motor movement in the tolerance window of the amplitude monitoring
Change of phase shift between output signals	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)] e.g. through a soiled code disc
Fastening becomes loose when idling: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Required! According to manufacturer's datasheet for the encoder	Not possible safely! However, monitoring of the period of the SOS request occurs: A switch-off and error message occur after 24 hrs.	Use fault exclusion for the motor - encoder system, or a second measuring system for position comparison!
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)			

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Additional requirements for rotary encoders with sin/cos output signals, analogue signal generation			
Static signal at the inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Change in the signal shape	None	Individual signal monitoring and vector length monitoring[1)]	In accordance with section 7.3; DC > 90%[2)]
Swapping of the sin and cos output signal	Yes	Safety module has sufficiently separated signal processing without multiplexer	–
Supplementary requirements for shaft encoders with incremental and absolute signals			
Simultaneous incorrect position change of incremental and absolute signal	None	None, the safety module only analyses the analogue sin/cos signals	Only for HIPERFACE interface: The basic unit carries out a cyclical plausibility check, using a cross-comparison of the sin/cos signals with the absolute position read via the data interface
Additional requirements for rotary encoders with synthetically-generated output signals			
Any falsification of the output signal	None	Not possible in all cases, if both output signals are falsified simultaneously.	Use fault exclusion for the encoder, or a second measuring system for position comparison!
Additional requirements for linear encoders			
Mounting of read head broken Static offset of the material measure (e.g. visual code strip) Damaged material measure (e.g. visual code strip)	Required! According to manufacturer's datasheet for the encoder	Not possible safely! However, monitoring of the period of the SOS request occurs: A switch-off and error message occur after 24 hrs.	Use fault exclusion for the motor - encoder system, or a second measuring system for position comparison!

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Further requirements for the analysis of SIL position encoders			
Supply voltage monitoring of the encoder	None	Not present. This must be ensured at the encoder	The basic unit contains regulation of the power supply for the encoder. In the case of error (overvoltage, over-current), the encoder supply can be switched off functionally
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of error, the drive can be switched off functionally
1) Sensitivity and DC in accordance with the parameterised fault limits; specification applies to factory setting 2) Position information is "static" if there is a fault => Fixed commutating position, motor at idle / voltage of a channel static => Commutating position changes by max +/-90° of a signal period of an encoder, motor only moves in this range			

Table 129: SIN/COS encoder, HIPERFACE encoder

Classification of the safety mode in conjunction with the SIN/COS encoder, HIPERFACE encoder:

Detection of encoder fault:	DC > 90%
Classification in accordance with EN 61800-5-2 / EN 13849-1:	SIL2 / cat. 3 / PL d (safe positioning, incl. at rest) and SIL2 / cat. 3 / PL e (safe speed and acceleration)

7.2.3.2 Resolver

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Interruption of any conductor of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Static "0" or "1" signal at the inputs and outputs, individually or simultaneously at multiple inputs/outputs	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Interruption of high-impedance status on a single input/output or multiple inputs/outputs simultaneously	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reduction or increase of the output amplitude	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Interference vibration on one or more outputs	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Change of phase shift between output signals	None	Not applicable for resolver	–
Fastening becomes loose when idling: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Required! According to manufacturer's datasheet for the encoder	Not possible safely! However, monitoring of the period of the SOS request occurs: A switch-off and error message occur after 24 hrs.	Use fault exclusion for the motor - encoder system, or a second measuring system for position comparison!
Mounting comes loose during movement: – Sensor housing separates from motor housing Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)	None	Not applicable for resolver	–

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
No light from transmitter diode	None	Not applicable for resolver	–
Supplementary requirements for resolvers with signal processing / reference generator			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
– Central timer fails – No Conversion Start for analogue/digital converter – Sample & Hold occurs at the wrong time	None	Failure monitoring of the SYNC signal	Error is reliably detected (DC_{AV} of the safety module)
Analogue-digital converter generates incorrect values	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Analogue-digital converter does not generate any values	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reference generator does not supply any frequency	None	Failure monitoring of the SYNC signal	Error is reliably detected (DC_{AV} of the safety module)
Reference generator supplies an incorrect frequency	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Reference generator does not supply a periodic reference signal	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Amplification error during signal processing (reference, sin, cos signal), oscillation	None	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Magnetic interference at the installation location	Sufficient screening for the installation location	Individual signal monitoring and vector length monitoring[1)]	Error is reliably detected (DC_{AV} of the safety module)
Further requirements for the analysis of SIL position encoders			
Supply voltage monitoring of the encoder	None	Indirect monitoring of the resolver via vector length monitoring	Error is reliably detected (DC_{AV} of the safety module)

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of error, the drive can be switched off functionally
1) DC = 60% applies to factory setting, DC = 90% for restricted tolerances of the vector length monitoring ➔ Appendix 7.3 2) Position information is "static" if there is a fault => Fixed commutating position, motor at idle / voltage of a channel static => Commutating position changes by max +/-90° of a signal period of an encoder, motor only moves in this range			

Table 130: Resolver

Classification of the safety mode in conjunction with resolver:

Detection of encoder fault:	DC > 90%
Classification in accordance with EN 61800-5-2 / EN 13849-1:	SIL2 / cat. 3 / PL d (safe positioning, incl. at rest) and SIL2 / cat. 3 / PL e (safe speed and acceleration)

7.2.3.3 Combined encoder systems: Encoder 1: Resolver [X2A] or SIN/COS encoder [X2B] Encoder 2: Incremental encoder [X10]

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2)]
Interruption of any conductor of the connecting cable			
Static "0" or "1" signal at the inputs and outputs, individually or simultaneously at multiple inputs/outputs			
Interruption of high-impedance status on a single input/output or multiple inputs/outputs simultaneously			
Reduction or increase of output amplitude Interference vibration on one or more outputs			
Change of phase shift between output signals			
Fastening becomes loose when idling: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2)]
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)			

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
Supplementary requirements for shaft encoders with sin/cos output signals, analogue signal generation			
Static signal at the inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1]	DC "high"[2]
Change in the signal shape			
Swapping of the sin and cos output signal			
Supplementary requirements for shaft encoders with rectangular output signals (encoder 2)			
Interference vibration at the output	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
Output signal terminates			
Zero pulse fails, is too short, too long or occurs multiple times			
Supplementary requirements for shaft encoders with synthetically-generated output signals (encoder 1 or encoder 2)			
Any falsification of the output signal	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
Supplementary requirements for shaft encoders with position determination using a counter (encoder 2)			
Incorrect position value due to faulty count	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
Supplementary requirements for resolvers with signal processing / reference generator			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC "high"[2]
– Central timer fails – No Conversion Start for analogue/digital converter – Sample & Hold occurs at the wrong time	None		
Analogue-digital converter generates incorrect values	None		

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Analogue-digital converter does not generate any values	None		
Reference generator does not supply any frequency	None		
Reference generator supplies an incorrect frequency	None		
Reference generator does not supply a periodic reference signal	None		
Amplification error during signal processing (reference, sin, cos signal), oscillation	None		
Magnetic interference at the installation location	Sufficient screening for the installation location		
Further requirements for the analysis of SIL position encoders			
Supply voltage monitoring of the encoder	None	Separate generation of the supply voltage for: – resolver [X2A] – SIN/COS encoder [X2B] – incremental encoder [X10]	–
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of error, the drive can be switched off functionally

1) Sensitivity and DC in accordance with the parameterised fault limits; specification applies to factory setting

2) Position information is "static" if there is a fault => Fixed commutating position, motor at idle / voltage of a channel static => Commutating position changes by max +/-90° of a signal period of an encoder, motor only moves in this range

Table 131: Combined encoder systems: Encoder 1: Resolver [X2A] or SIN/COS encoder [X2B], Encoder 2: Incremental encoder [X10]

Classification of the safety module in conjunction with the basic unit in the encoder combination, encoder 1: Resolver [X2A] or SIN/COS encoder [X2B], encoder 2: Incremental encoder [X10] (without taking the actual encoder into account):

Detection of encoder fault:	DC > 95%
Classification in accordance with EN 61800-5-2:	SIL3
Classification in accordance with EN ISO 13849:	Cat. 4 / PL e

7.2.3.4 Combined encoder systems: Encoder 1: Resolver [X2A] or incremental encoder [X10] Encoder 2: Other encoder [X2B] (analysis via basic unit)

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Short circuit between any two conductors of the connecting cable	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Interruption of any conductor of the connecting cable			
Static "0" or "1" signal at the inputs and outputs, individually or simultaneously at multiple inputs/outputs			
Interruption of high-impedance status on a single input/output or multiple inputs/outputs simultaneously			
Reduction or increase of the output amplitude			
Interference vibration on one or more outputs			
Change of phase shift between output signals			
Fastening becomes loose when idling: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Mounting comes loose during movement: – Sensor housing separates from motor housing – Sensor shaft separates from motor shaft			
Measuring element is coming loose (e.g. optical encoding disc)			

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
No light from transmitter diode	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Supplementary requirements for shaft encoders with sin/cos output signals, analogue signal generation			
Static signal at the inputs and outputs, individually or on multiple signals, amplitude in the range of the power supply	None	Individual signal monitoring and vector length monitoring[1)] Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2)]
Change in the signal shape			
Swapping of the sin and cos output signal			

Error acceptance	**Fault exclusion**	**Error detection by the safety module**	**Supplementary notes/comments**
Supplementary requirements for resolvers with signal processing / reference generator (encoder 1)			
Crosstalk on the reference frequency	None	Individual signal monitoring and vector length monitoring[1]	DC 1 x "high" (safety module)
– Central timer fails – No Conversion Start for analogue/digital converter – Sample & Hold occurs at the wrong time	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	+ 1 x "low" (basic unit) [2]
Analogue-digital converter generates incorrect values	None		
Analogue-digital converter does not generate any values	None		
Reference generator does not supply any frequency	None		
Reference generator supplies an incorrect frequency	None		
Reference generator does not supply a periodic reference signal	None		
Amplification error during signal processing (reference, sin, cos signal), oscillation	None		
Magnetic interference at the installation location	Sufficient screening for the installation location		
Supplementary requirements for shaft encoders with rectangular output signals (encoder 1)			
Interference vibration at the output	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2]
Output signal terminates			
Zero pulse fails, is too short, too long or occurs multiple times			
Supplementary requirements for shaft encoders with synthetically-generated output signals (encoder 1 or encoder 2)			
Any falsification of the output signal	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) [2]

Error acceptance	Fault exclusion	Error detection by the safety module	Supplementary notes/comments
Additional requirements for rotary encoders with position determination using a counter (encoder 1 or encoder 2)			
Incorrect position value due to faulty count	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)
Additional requirements for linear encoders (encoder 1 or encoder 2)			
Mounting of read head broken	Not required!	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)
Static offset of the material measure (e.g. visual code strip)			
Damaged material measure (e.g. visual code strip)			
Additional requirements for rotary encoders with computer interface (encoder 2)			
Transmission error: – repeat; – loss; – insertion; – incorrect sequence; – message falsification; – delay	None	Cross-comparison of the position data (Encoder 1 - encoder 2)	DC 1 x "high" (safety module) + 1 x "low" (basic unit) 2)
Further requirements for the analysis of SIL position encoders			
Supply voltage monitoring of the encoder	None	Separate generation of the supply voltage for: – resolver [X2A] – SIN/COS encoder [X2B] – incremental encoder [X10]	–
Compliance with the operating and ambient conditions specified for the encoder	None	Not present. This must be ensured at the encoder	The basic unit has an input for monitoring the motor temperature. In the case of error, the drive can be switched off functionally
1) Sensitivity and DC in accordance with the parameterised fault limits; specification applies to factory setting 2) Limitation through DCAV of the module through DC of the basic unit			

Table 132: Combined encoder systems: Encoder 1: Resolver [X2A] or incremental encoder [X10], encoder 2: Other encoder [X2B] (analysis via basic unit)

Classification of the safety module in conjunction with the basic unit in the encoder combination, encoder 1: Resolver [X2A] or incremental encoder [X10], encoder 2: Other encoder [X2B] (without taking the actual encoder into account):

Angle detection of the basic unit:	MTTF of each channel:	> 100 a, "high"
	DC of the channel:	= 50% "low"
Safety module:	MTTF of each channel:	> 100 a, "high"
Detection of encoder fault	DC:	> 95% "high"
System classification (safety module + basic unit):		
Classification in accordance with EN 61800-5-2:	SIL3	
Classification in accordance with EN ISO 13849:	Cat. 3 / PL d	

7.2.4 Digital outputs

The relevant standards for the control of external safety switching devices must always be observed.

Output type	**Switch type**	**Classification category, PL**[1)]	**Classification SIL**[2)]
1: Integrated safe pulse inhibitor	2 N/C contacts	Cat. 4, PL e	SIL 3
2: General 2-channel output DOUT40 ... DOUT42	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
2: General 2-channel output	2 N/C contacts or 1 N/C contact + 1 N/O contact	Cat. 4, PL e	SIL 3
3: Activation of the holding brake via [X6] in the basic unit ARS 2000 FS	2 N/C contacts	Cat. 3, PL d, for directly-connected clamping units, requested via SBC.	SIL 2
	2 N/C contacts	Cat. 1, PL c, for indirectly-connected clamping units (e.g. pneumatically opening), requested via SBC. Depending on the type and safety classification of the connected clamping unit.	SIL 1
	2 N/C contacts	Cat. 3, PL d, for indirectly-connected clamping units (e.g. pneumatically opening), requested via SBC. Depending on the type and safety classification of the connected clamping unit.	SIL 2
10: Potential-free acknowledgment contact (diagnostics)	1 N/O contact	Only as feedback for higher-level safety switching device.	

1) To EN ISO 13849-1

2) To EN 61508, EN 61800-5-2, EN 62061

Table 133: Safety reference data, digital inputs

Note

- The following data on measures and DC is based on the data of the standard EN ISO 13849-1.
- The manufacturer's specifications must be used for a safety-related assessment of the switching devices.
- The DC values given are only valid when the specified measures and the specified additional conditions are complied with.
- Fault exclusions are possible according to the relevant standards, for which the required conditions must be permanently guaranteed.

Measure	DC	Comment	Use
Cyclical test pulse through dynamic change of the output signals.	90	Always effective in the safety module, as the test pulses for the safe pulse block and for DOUT40 ... 42 cannot be switched off.	Cross-circuit monitoring for 2-channel outputs.
Cross-comparison of output signals with dynamic test if short-circuits cannot be detected (for multiple inputs/outputs).	90	Without allocation of test pulses. Cyclical change of the input signals required, e.g. through the process or regular actuation.	Monitoring of 2-channel outputs.
Cross-comparison of output signals with immediate and intermediate results in the logic (L) and temporal as well as logic program sequence monitoring and detection of static failures and short circuits (for multiple inputs/outputs).	99	Always effective in the safety module, as the test pulses for the safe pulse block and for DOUT40 ... 42 cannot be switched off	Monitoring of 2-channel outputs
Plausibility check, e.g. use of outputs switching antivalently.	99	Can only be used for DOUT40 ... 42, in the "antivalent" switching configuration.	Monitoring of 2-channel outputs.

Table 134: Measures for digital outputs

7.3 System precision and reaction time

The following sections view the system precision requirements of functional safety engineering, with regard to safely monitoring movement functions for position and speed.

i

The achievable system accuracy is primarily dependent on the system structure, consisting of: Motor – Gear unit – Axle

It can be increased particularly through the use of a gear unit or through the selection of an axle with a lower feed (➔ Section 7.3.7, Table 144).

The specified accuracies and reaction times of the safety module always represent a compromise between:

- the resolution and the accuracy of the connected position transmitters and the allocated electronic evaluation unit in the safety module,
- the desired high precision for the monitoring of the limit values for position and speed,
- the reaction time until the violation of a condition is detected,
- the system availability during operation in an industrial environment (malfunctions, EMC, etc.).

For this reason, the accuracies and reaction times should be as high as necessary from a safety point of view, but not excessive.

➔ **Note**

The factory settings of the safety module for encoder analysis, speed detection and position monitoring are correct for most applications. They are adapted to the resolution of the position encoders and to the electronic evaluation unit in the safety module.

They should only be changed when there are problems, as they influence the reaction time of the safety module when dangerous movements are detected or during error detection. They are so-called "Expert parameters".

Alternatively, check to see if the mechanical system can be changed (e.g. axle with reduced feed).

Use the data transfer (➔ Section 2.3) to ensure that the safety module has the correct parameters for the feed constant and the gear ratios, before you parameterise safety functions.

7.3.1 Accuracy of position monitoring (SOS) from the point of view of the application

When the SOS safety function is requested, the current position is detected and saved to x_sample.

Monitoring takes place in a position window of:

(x_sample – x_max) ≤ x_act ≤ (x_sample + x_max)

Application-specific requirements for x_max (for SOS) are stated in Section 7.3.7, Table 142.

x_max is set via P0B.01 (➔ Section 2.5.5).

Parameter	Name	Min.	Typical	Max.	Note
x_max	Position tolerances for SOS	–	1 mm	1.8 mm	Section 7.3.7 , Table 142
phi_max	Angle tolerances on the motor shaft for SOS	–	4.0°	7.2°	Sample calculation based on a feed of 90 mm/rev

Table 135: Typical values SOS

The safety module is parameterised as follows for this:

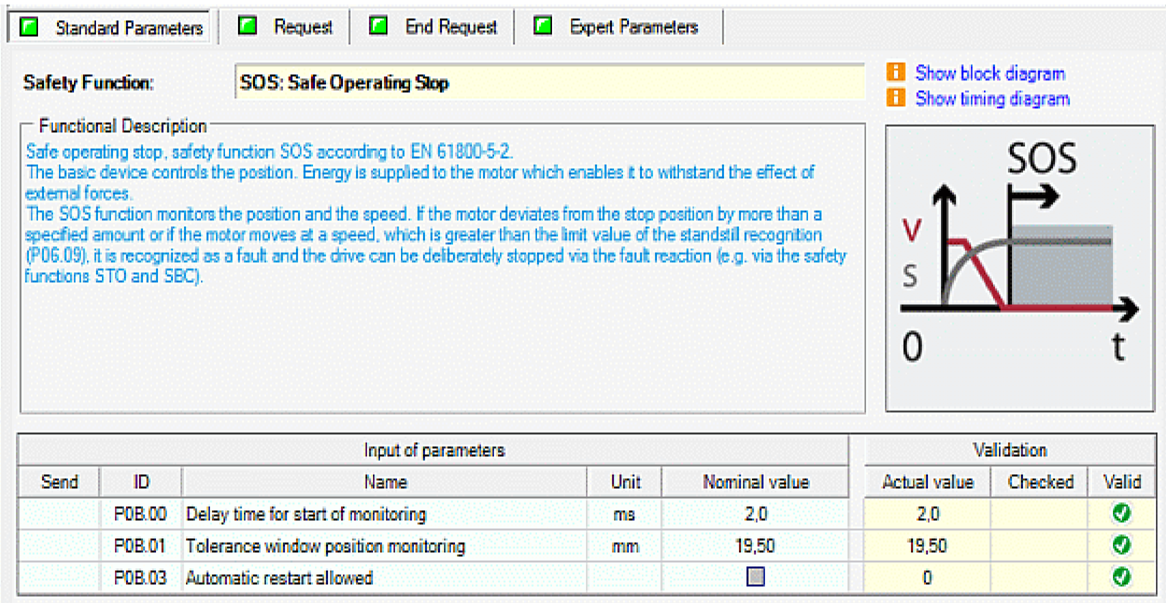


Figure 65: Example: Specification of the relevant parameters for Safe Operation Stop (SOS)

This sample data is converted from translational to rotational variables, based on the following assumptions:

– motor without gear unit,
– axle EGC-80 with a feed of 90 mm/rev.

7.3.2 Accuracy of speed monitoring (SLS, SSR) from the point of view of the application

When the safety function with speed monitoring is requested, e.g. SLS, SSR, the current speed v_act is detected continuously and monitored for compliance with specific limit values.

The limit values can change dynamically, e.g. on requesting SLS, if the system first brakes to the safely-limited speed.

Monitoring takes place in a speed window of:

$v_{min} \le v_{act} \le v_{max}$

Application-specific requirements for v_max (for SLS) are stated in Section 7.3.7, Table 143.

The acceptable filter time constant t_filter_v in the speed monitoring is the result of the quality of the analogue signal processing on the safety module (for position encoders with analogue signals, such as resolvers or HIPERFACE encoders) and the position resolution (number of angle steps for motor revolution).

In addition, on dynamic changes, there is a "swing-in process" until the speed swings into the new setpoint. The length of time depends on the band width of the rotational speed regulation circuit. To ensure a high level of system availability, short swing-in processes in the range of the bandwidth of the rotational speed regulation circuit should not lead to a response of the monitoring system.

An allowable time t_tol_v is provided for that. During the length of time t_tol_v, v_act may move outside the speed window before the violation of the safety condition is triggered.

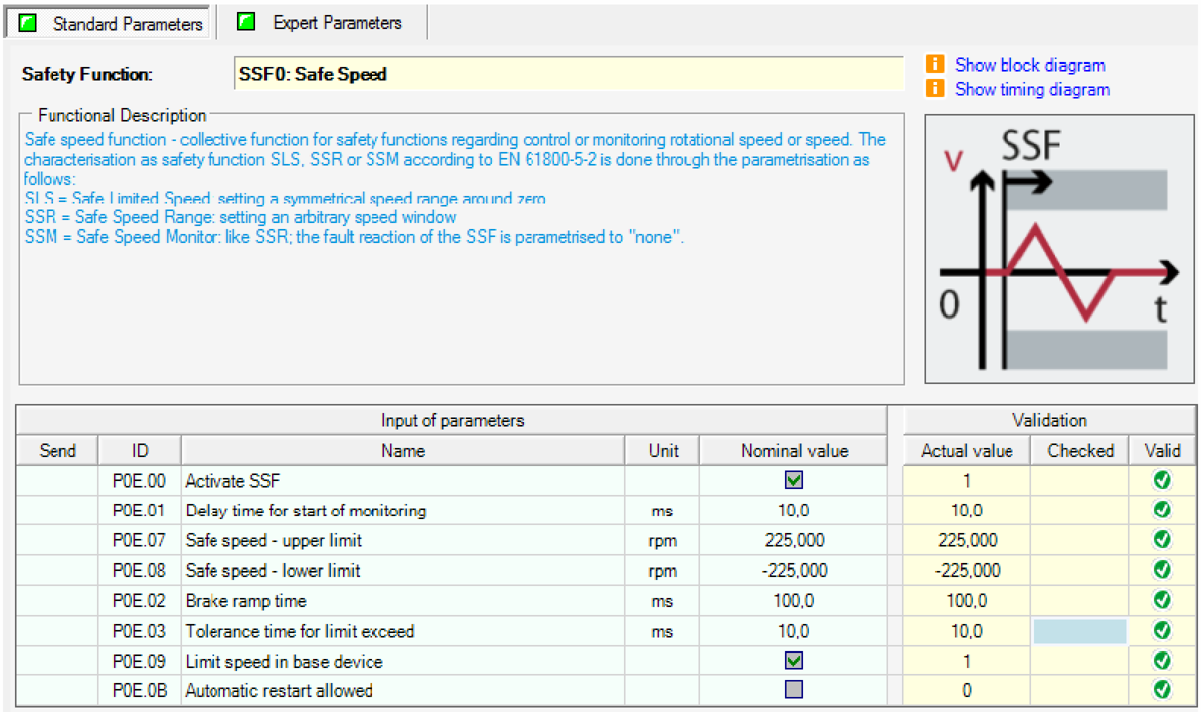
Parameter	Name	Min.	Typical	Max.	Note
v_max	Speed limit for SLS	4 mm/s	250 mm/s	≥ 10 m/s	Section 7.3.7, Table 143
n_max	Minimum speed limit on the motor shaft for SLS	2.1 rpm	167 rpm		Sample calculation based on a feed of 90 mm/rev
t_filter_v	Filter time constant, speed detection	2 ms	8 ms	≥ 100 ms	Section 7.3.7, Table 142
t_tol_v	Allowable time for v_act outside the approved speed range	0 ms	10 ms	≥ 100 ms	Typical bandwidth of the speed control f_gr = 100 Hz

1) The resolution of the speed signal is primarily determined by the quality of the encoders used and the parameterised filter time of the speed filter. Monitoring for n_typ_min should be possible with common shaft encoders, such as resolvers or SIN/COS encoders, if the speed filter is parameterised in the range of 20 ms (the axle moves just 0.08 mm at 4 mm/s for 20 ms).

Table 136: Typical values, SLS

7.3.3 Specification of the relevant parameters for Safe Speed Function (with SLS, SSR)

The safety module is parameterised as follows for the requirements determined in Section 7.3.2:



Standard Parameters | Expert Parameters

Safety Function: SSF0: Safe Speed

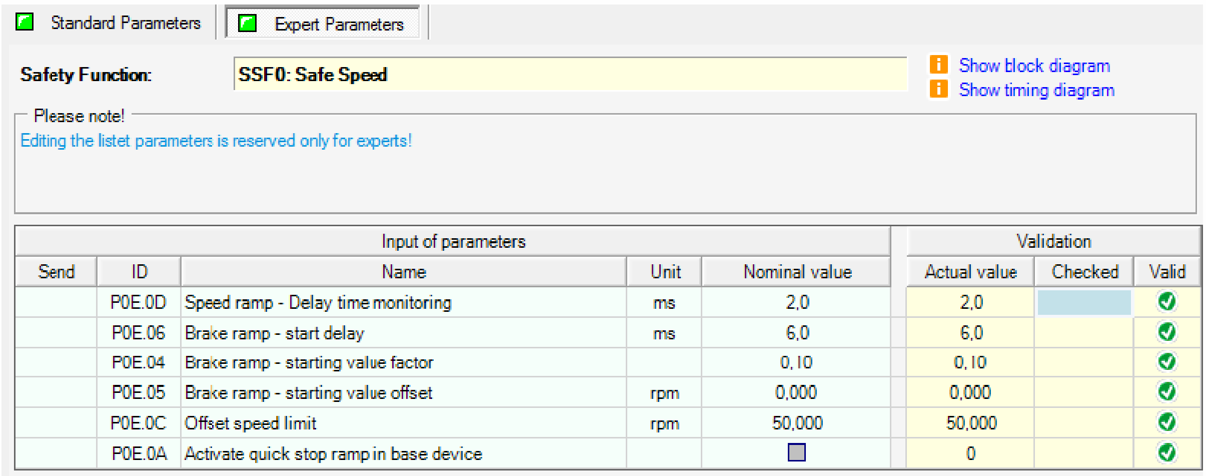
Show block diagram
Show timing diagram

Functional Description

Safe speed function - collective function for safety functions regarding control or monitoring rotational speed or speed. The characterisation as safety function SLS, SSR or SSM according to EN 61800-5-2 is done through the parametrisation as follows:
SLS = Safe Limited Speed: setting a symmetrical speed range around zero
SSR = Safe Speed Range: setting an arbitrary speed window
SSM = Safe Speed Monitor: like SSR; the fault reaction of the SSF is parametrised to "none".

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.00	Activate SSF		☑	1		✔
	P0E.01	Delay time for start of monitoring	ms	10,0	10,0		✔
	P0E.07	Safe speed - upper limit	rpm	225,000	225,000		✔
	P0E.08	Safe speed - lower limit	rpm	-225,000	-225,000		✔
	P0E.02	Brake ramp time	ms	100,0	100,0		✔
	P0E.03	Tolerance time for limit exceed	ms	10,0	10,0		✔
	P0E.09	Limit speed in base device		☑	1		✔
	P0E.0B	Automatic restart allowed		☐	0		✔

Figure 66: Example: Specification of the relevant parameters for Safe Speed Function (SLS, SSR)



Standard Parameters | Expert Parameters

Safety Function: SSF0: Safe Speed

Show block diagram
Show timing diagram

Please note!
Editing the listet parameters is reserved only for experts!

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P0E.0D	Speed ramp - Delay time monitoring	ms	2,0	2,0		✔
	P0E.06	Brake ramp - start delay	ms	6,0	6,0		✔
	P0E.04	Brake ramp - starting value factor		0,10	0,10		✔
	P0E.05	Brake ramp - starting value offset	rpm	0,000	0,000		✔
	P0E.0C	Offset speed limit	rpm	50,000	50,000		✔
	P0E.0A	Activate quick stop ramp in base device		☐	0		✔

Figure 67: Example: Specification of the Expert parameters for Safe Speed Function (SLS, SSR)

7.3.4 Requirements for encoder errors from the point of view of the application

The analysis of the position transmitters on the safety module is based on one of the following basic principles:

a) Two redundant items of position information are available, which are also analysed redundantly and separately by two microcontrollers, i.e. also two independent speed signals.
Example: Motor with EnDat encoder + two incremental position transmitters on the axle.

b) Only one item of position information is “reliably” available. The information is sent along the same cables and via some identical circuit sections (e.g. differential amplifiers for the input signals) and analysed redundantly by two microcontrollers on the safety module.
Example: Resolver (SIL2) or SIN/COS encoder with SIL 2/SIL 3.

Case a) The detection of encoder errors and position deviations between position encoders 1 and 2 is "non-time critical", as monitoring is always guaranteed by the other encoder, even if one of the encoders fails.

Case b) The detection of position deviations between microcontroller 1 and microcontroller 2 is "non-time critical", as the monitoring is always guaranteed by the other microcontroller.
In the transmission channel (e.g. cable) and in the shared circuit sections for encoder analysis, errors must be detected as quickly as possible, within an error response time to be specified.
The detection of the encoder errors is based primarily on the monitoring of analogue signals.
The limits of the signal monitoring have an influence on the resulting accuracy of the monitoring and on the diagnostic coverage ➔ See Section 7.3.2.

Monitoring of the position difference does not need to be more accurate than in other cases of error.

The worst case for an uncontrolled movement of the axle is a fusing of two output semi-conductors in the output stage of the ARS 2000 FS. In the worst case, this error leads to an electrical shift of the axle by up to 180° (== 45° on the shaft with an 8-pin motor).

Note: Of course, the system must be designed in such a way that this error does not lead to an impermissible position difference - e.g. through the selection of a suitably low feed or gear ratio.

➔ **Note**

There is a risk that the drive will advance if there are multiple errors in the ARS 2000 FS.

Failure of the servo drive output phase during STO status (simultaneous short circuit of 2 power semiconductors in different phases) may result in a limited detent movement of the rotor. The rotation angle / path corresponds to a pole pitch. Examples:

- Rotary axle, synchronous machine, 8-pin ➔ movement $\leq$ 45° at the motor shaft.
- Linear motor, pole pitch 20 mm ➔ movement $\leq$ 20 mm at the moving part.

Determination of angle difference (dynamic)	
Detection of signal errors in the "shared" transmission path (resolver, SIN/COS encoder)	≤ 2 ms
Position offset on "fusing" of two output semi-conductors (worst case)	approx. 45° on the shaft (in the case of an 8-pin synchronous machine)
Position offset because microcontroller 1 and microcontroller 2 did not sense the position at the same time	approx. 1° on the shaft
Dynamic position offset on accelerating	typ. 30 ° on the shaft
Length of the compensation operation	typ. ≤ 10 ms
Resulting total position difference	approx. 0.167 revs.

Table 137: Observation of the possible position difference between microcontrollers 1 and 2

Monitoring the speed difference depends on the resolutions in the encoder analysis and the possible time shift in the detection between microcontroller 1 and microcontroller 2 at maximum acceleration. The approved filter time constant is calculated according to Section 7.3.7, Table 142.

Determination of total rotational speed difference (dynamic)	
Resolution of encoder analysis (raw) (important for idling detection, P06.09)	approx. 20 rpm
Rotational speed offset on accelerating	approx. 120 rpm
Time shift	1 basic cycle => ≤ 200 µs
Maximum acceleration	0 > 5000 RPM within 1 ms
Rotational speed offset on accelerating	200 µs x 6000 rpm / 10 ms
Resulting total rotational speed difference	approx. 150 rpm
Filter time constant for speed signals	typ. 8 ms

Table 138: Observation of the possible dynamic rotational speed difference between microcontrollers 1 and 2

Due to the high reliability (PFH) of the circuit, the maximum allowable time for encoder monitoring can be set to 100 ms without any problems.

As a result, the encoder configuration of the safety module is parameterised as follows:

Standard Parameters | X28 | X10 | Speed detection | Comparison encoder 1 - 2 | Signal monitoring

Data Acquisition: **Encoder Configuration** Show block diagram

Functional Description

Parameter for measuring rotational speed:
Parametrising an acceleration monitoring (plausibility check of the position measurement)
Parametrising a filter for measuring rotational speed / speed
Parametrising the threshold value and time tolerance for the standstill recognition (e.g. for SOS)
The parameter presettings should only be changed in justified problem cases.

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.07	Maximum acceleration for sensor monitoring	m/s²	10905,190	10905,190		✓
	P06.08	Filter time constant for revolution speed monitorin	ms	8,0	8,0		✓
	P06.09	Treshold speed for standstill detection	mm/s	26,00	26,00		✓
	P06.0A	Filter time for standstill detection	ms	10,0	10,0		✓

Figure 68: Parameter setting for rotational speed detection

Standard Parameters | X28 | X10 | Speed detection | Comparison encoder 1 - 2 | Signal monitoring

Data Acquisition: **Encoder Configuration** Show block diagram

Functional Description

Parameter for comparing encoder 1 and encoder 2:
Parametrising a tolerance window for comparing postion encoders 1 and 2 (position difference, tolerance time)
Parametrising a tolerance window for the cross-comparison of the safe positions and speeds with tolerance time between µC1 and µC2

Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.03	Tolerance window for position displacem. sensor	mm	13,00	13,00		✓
	P06.04	Tolerance time for position difference	ms	10,0	10,0		✓
	P06.05	Tolerance window for speed deviation sensor 1 -	mm/s	195,00	195,00		✓
	P06.06	Tolerance time for speed difference	ms	10,0	10,0		✓
	P1D.04	Tolerance window for position comparator µC1 - µ	mm	13,00	13,00		✓
	P1D.05	Tolerance time for position comparator µC1 - µC2	ms		100,0		✓
	P1D.06	Tolerance window for speed comparator µC1 - µC	mm/s	195,00	195,00		✓

Figure 69: Parameter settings for comparing encoders 1 - 2

7.3.5 Vector length monitoring of analogue encoder signals (resolver, SIN/COS encoder)

The safety module monitors the analogue encoder signals of a SIN/COS encoder or resolver:

- the tracking signals e_x (corresponds to COS signal of a SINCOS encoder / resolver) and e_y (corresponds to SIN signal of a SINCOS encoder / resolver) are measured.
- each individual signal is monitored (compliance with the approved signal range). Short circuits of individual signals against GND / VCC and impermissibly high signal levels are detected.
- In addition, the vector length is calculated:

$$e=\sqrt{e_x^2+e_y^2}$$

- the currently measured vector length e is checked for compliance with parameterisable limit values:

$$e_{min}<e<e_{max}$$

(parameters P06.0F, P06.10, P06.1A, P06.1B)

- if an individual signal (e_x, e_y) or the vector (e) is outside the permitted range, an encoder error is triggered and the error response is evoked (error of group 55-x).

Vector length monitoring is used to detect various errors of the encoder and for detection of errors in the analogue signal detection ➔ Section 7.2.3:

- failure of a signal through short circuit, interruption, etc.
- amplitude and phase errors
- Stuck-At errors
- drift and oscillation

The maximum error angle up to the response of the vector length monitoring is calculated based on the nominal vector length e_{rated}, taking the limit values into account as follows:

$$\Delta\varepsilon = \mathrm{acos}\left(\frac{e_{min}}{e_{rated}}\right) + \mathrm{acos}\left(\frac{e_{min}}{e_{max}}\right)$$

Diagnostic coverage of vector length monitoring:

The diagnostic coverage can be calculated from the ratio of the voltage surfaces in the x-y coordinate space as follows, assuming a homogeneous distribution list of the voltage errors:

Value	**SIN/COS encoder**	**Resolver**
Voltage range of the encoder signals e_x, e_y	$0.5\ V \le e_x , e_y \le 4.5\ V$	$-6.7\ V \le e_x , e_y \le 6.7\ V$
Total area of the voltage range F_{total}	$F_{total} = (4.50\ V – 0.50\ V)^2$	$F_{total} = (6.7\ V – (-6.7\ V))^2$
Proportion of the "permitted" voltage range F_{valid} F_{valid} = ð($e_{max}^2 – e_{min}^2$)	F_{valid} = ð(0.70 V^2 – 0.21 V^2) 1) F_{valid} = ð(0.60 V^2 – 0.40 V^2) 2)	F_{valid} = ð(2.20 V^2 – 6.40 V^2) 1) F_{valid} = ð(5.20 V^2 – 6.40 V^2) 2)
Diagnostic cover DC_{vl} $DC_{vl} = 1 – F_{valid}/ F_{total}$	DC_{vl} =91% 1) DC_{vl} =95 % 2)	DC_{vl} = 37 % 1) DC_{vl} = 76 % 2)

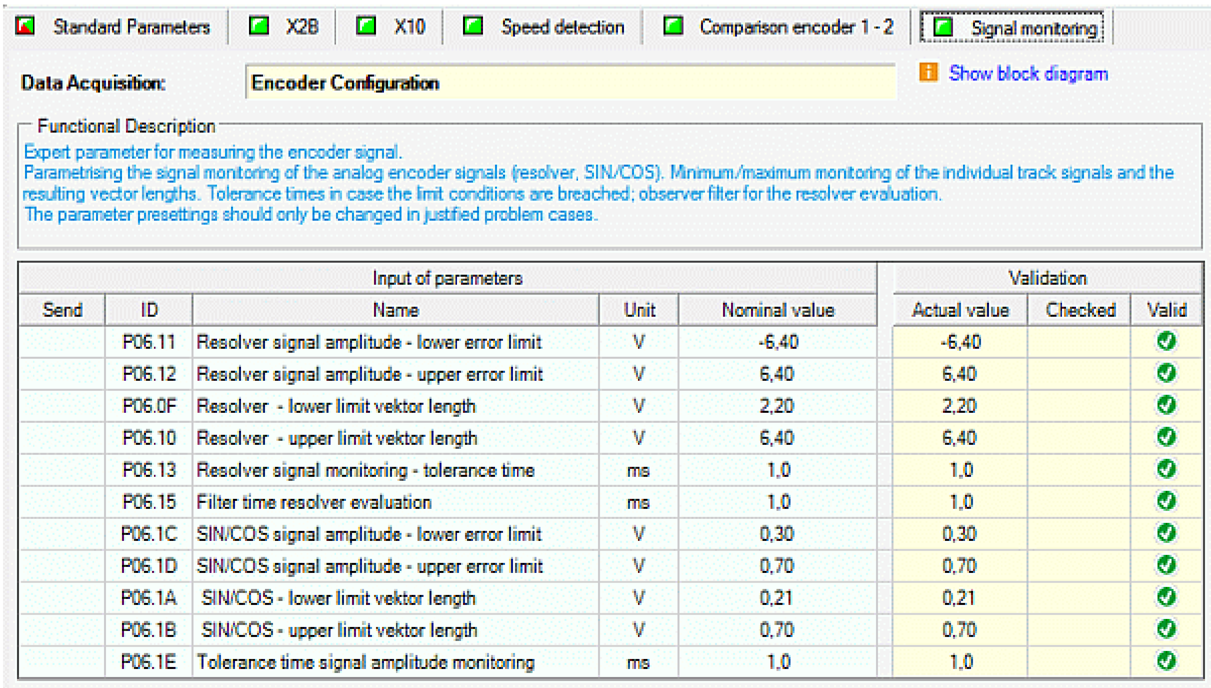
1) Factory setting

2) Setting with reduced tolerance

Table 139: Calculation of diagnostic coverage

The diagnostic coverage of the vector length monitoring DC_{VL} goes through the FMEA of possible encoder errors into the total diagnostic coverage DC_{AV} for the encoder system. DC_{AV} is mostly markedly higher than DC_{VL}.

When the device is delivered, the parameters for vector length are "relatively roughly" parameterised, in order to allow operation with many different encoders and to achieve maximum availability in the case of external interference:



Input of parameters					Validation		
Send	ID	Name	Unit	Nominal value	Actual value	Checked	Valid
	P06.11	Resolver signal amplitude - lower error limit	V	-6,40	-6,40		✓
	P06.12	Resolver signal amplitude - upper error limit	V	6,40	6,40		✓
	P06.0F	Resolver - lower limit vektor length	V	2,20	2,20		✓
	P06.10	Resolver - upper limit vektor length	V	6,40	6,40		✓
	P06.13	Resolver signal monitoring - tolerance time	ms	1,0	1,0		✓
	P06.15	Filter time resolver evaluation	ms	1,0	1,0		✓
	P06.1C	SIN/COS signal amplitude - lower error limit	V	0,30	0,30		✓
	P06.1D	SIN/COS signal amplitude - upper error limit	V	0,70	0,70		✓
	P06.1A	SIN/COS - lower limit vektor length	V	0,21	0,21		✓
	P06.1B	SIN/COS - upper limit vektor length	V	0,70	0,70		✓
	P06.1E	Tolerance time signal amplitude monitoring	ms	1,0	1,0		✓

Figure 70: Parameter setting for analogue signal monitoring and error detection

The following table summarises the additional data of the encoders in commercially available motor series. It specifies the nominal values of the vectors, the frequencies of the encoders, the values for e_{min}, e_{max} (see above), the resulting maximum angle error until error detection responds, DC_{VL} and the resulting total diagnostic coverage DC_{AV} for the motor with encoder system.

Motor	Encoder 1	p_0	e_{min}	e_{rated}	e_{max}	$\Delta\varepsilon_{mech}$	Position error for feed		DC_{VL}	DC_{AV}
							100 mm/rev	20 mm/rev		
Motor with resolver system	Resolver	1	2.20 V	5.80 V	6.40 V	138°	38 mm	7 mm	36 %	91%
Motor with HIPER-FACE encoder system	HIPER-FACE encoder (SIN-/COS encoder)	16	0.21 V	0.50 V	0.70 V	8.6°	2.4 mm	0.5 mm	91%	93%
Servo motor with HIPER-FACE encoder SKS 36 / SKM 36	HIPER-FACE encoder (SIN-/COS encoder)	128	0.21 V	0.50 V	0.70 V	1.1°	0.3 mm	0.06 mm	91%	93%

Table 140: Position error up to response of vector length monitoring, as well as corresponding DC (factory setting)

If the diagnostic coverage is too small, then a restriction is possible by changing e_{min} and e_{max} to the following limit values (possibly at the expense of system availability in an industrial environment with interference):

Motor	Encoder 1	p_0	e_{min}	e_{rated}	e_{max}	$\Delta\varepsilon_{mech}$	Position error for feed		DC_{VL}	DC_{AV}
							100 mm/rev	20 mm/rev		
Motor with resolver system	Resolver	1	5.20 V	5.80 V	6.40 V	62°	17 mm	3.4 mm	75%	91%
Motor with HIPER-FACE encoder system	HIPERFACE encoder (SIN-/COS encoder)	16	0.40 V	0.50 V	0.60 V	5.3°	1.5 mm	0.3 mm	95%	96%
Servo motor with HIPER-FACE encoder SKS 36 / SKM 36	HIPERFACE encoder (SIN-/COS encoder)	128	0.40 V	0.50 V	0.60 V	0.7°	0.2 mm	0.04 mm	95%	96%

Table 141: Position error up to response of the vector length monitoring, as well as corresponding DC (reduced tolerances)

i

The diagnostic coverage of vector length monitoring DC_{VL} is included in the overall diagnostic coverage for operation of the FSM 2.0 – MOV with the appropriate encoder system. But many errors are reliably detected even with "relatively roughly" set vector length monitoring or are detected through other mechanisms for error detection. As a result, the total DC_{AV} is higher than DC_{VL}.

Example: Resolver with factory setting for monitoring → DC_{VL} = 37%, but
DC_{AV} = 91% is achieved in the system.

→ **Note**

Please check your application critically:

❖ What are the requirements for the accuracy of position and idling monitoring?

Take the limitations listed in this chapter into account when selecting your system

7.3.6 Impact of an angle error within the error limits of vector length monitoring on the speed signal

Assume the following case: There is an error in an encoder signal e_x or e_y, which could be an amplitude error, for example. However, the error is small enough for vector length monitoring to not respond.

If the axle moves at a constant speed / the shaft turns at a constant rotational speed, then the error will lead to "fluctuations" in the currently measured speed. However, the speed averaged over an encoder period corresponds to the actual movement speed.

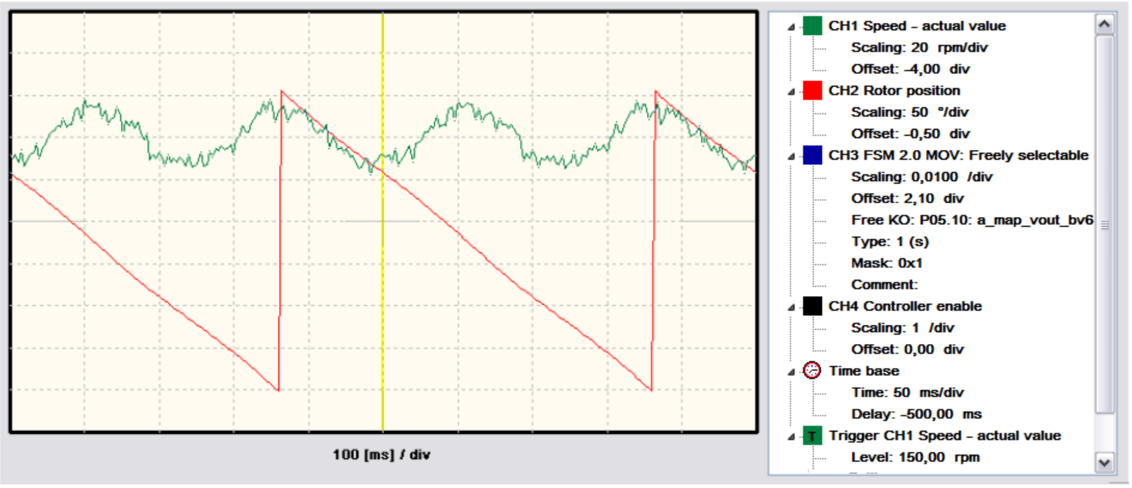


Figure 71: Error curves on the speed signal (CH1) at a reduction of the signal amplitude of e_x by 10%. This also produces a speed ripple of 10%. The measurement took place on an external drive of the shaft with a constant rotational speed.

Normally, position encoder 1 is also analysed in the basic unit and used for rotational speed adjustment. The basic unit now adjusts the current speed to the fluctuations. At low frequencies beneath the critical frequency of the rotational speed control circuit, at least the supposed fluctuation is compensated, the axle does not travel at a constant speed, but the actual rotational speed fluctuates and the angle and speed signal now are "OK"

The option of detection of speed errors in safety functions, such as SLS or SSR, is therefore dependent on multiple factors:

a) If, in addition, a second measuring system is used at the downforce, the fluctuation is detected safely.
The speed fluctuation is detected correctly using the second measuring system, the safety module detects an excessively high current rotational speed and switches to the safe status.

b) Only one encoder system with a high number of periods per revolution is used:
Even at low speeds, there is a relatively high frequency, which is not compensated. The rotational speed fluctuation is detected by the safety module, and it switches to the safe status.

c) Only one encoder system with a low number of periods per revolution is used:
At low speeds, there is a low frequency of rotational speed fluctuation, which is compensated to a great extent.

c1) The safety module is able to detect excessive mean speed safely over an encoder period.

c2) The monitoring limit must be reduced, to ensure that the current rotational speed is also monitored.

Example for C2): Monitoring of the resolver vector length with +/- 20% => The rotational speed must be lowered by the expected amount of the rotational speed fluctuation, i.e. also by 20%
=> If monitoring at v = 200 mm/s is requested, then monitoring is set to v = 160 mm/s.

➔ **Note**

Please check your application critically:

❖ what are the requirements for speed monitoring?

❖ is monitoring of the mean speed of a motor revolution sufficient?

Take the limitations listed in this chapter into account when selecting your system.

7.3.7 Basis for observation of system accuracy

SOS position limits	
Position monitoring	
Example for the maximum tolerance, required value must be specified during risk analysis	1.8 mm is the upper limit for SOS, i.e. the axle may move max. 1.8 mm in the direction of the hazard.
Speed monitoring	
Standard max. filter times	64 ms
Typical default value	Immediate detection with 8 ms monitoring cycle.
Summary	
Typical approved position tolerance	+/ 1 mm
Typical filter time	8 ms filter, 2 ms sampling time.

Table 142: SOS position limits, filter time

SLS speed limits	
DIN EN 12417:2009-07 Safety of machine tools – Machining centres	
Limited speed in special mode	
Opened guards	5m/min = 83.3 mm/s
Limit speed on tool changing, maintenance or setting work	
Only risk of impact	15 m/min = 250 mm/s
Risk of crushing	2 m/min = 33.3 mm/s
DIN EN 23125:2010-10 Safety of machine tools – Turning machines	
Limited speed in manual operation	
For small lathes	6 m/min = 100 mm/s
For large lathes	10 m/min = 166.7 mm/s
Closing speed, jaw chucks	4 mm/s
Axle movement	2 m/min = 33.3 mm/s
Feed motion, spindle sleeve	1.2 m/min = 20 mm/s
EN 10218-1:2012-01 Industrial robots – Safety requirements – Part 1: Robots	
Limited speed	250 mm/s
Summary	
Value range "Limited speed"	
Minimum	4 mm/s
Maximum	250 mm/s
Typical filter time	8 ms filter, 2 ms sampling time.

Table 143: SLS speed limits

Typical data of some commercially available linear axes							
Example 1: Toothed belt axes, with recirculating ball bearing guide							
Size		Type 1	Type 2	Type 3	Type 4	Type 5	
Pitch	[mm]	2	3	3	5	8	
Expansion (max. force)	[%]	0.094	0.08	0.24	0.13	0.29	
Effective diameter	[mm]	18.46	24.83	28.65	39.79	73.85	
Feed constant	[mm/rev]	58	78	90	125	232	
Example 2: Spindle axes, with recirculating ball bearing guide							
Size		Type 1	Type 2	Type 3	Type 4		
Diameter	[mm]	12	15	25	40		
Pitch	[mm/rev]	10	10 20	10 25	40		
Example 3: Toothed belt axle with high speed							
Size		Type 1	Type 2	Type 3	Type 4	Type 5	Type 6
Pitch	[mm]	2	2	2	3	5	8
Expansion (max. force)	[%]	0.04	0.1	0.2	0.11	0.1	0.15
Effective diameter	[mm]	10.18	12.09	16.55	20.05	31.83	56.02
Feed constant	[mm/rev]	32	28	52	63	100	176
Example 4: Toothed belt axle							
Size		Type 1	Type 2	Type 3			
Pitch	[mm]	3	5	5			
Expansion (max. force)	[%]	0.31	0.19	0.23			
Effective diameter	[mm]	28.65	39.79	52.52			
Feed constant	[mm/rev]	90	125	165			
Linear drives, e.g. ELGL-LAS, with air bearings and linear motor							
Typical pole pitches		in the range 20 mm…80 mm == 40 mm…160 mm feed					
Summary							
Value range "Feed"		Z : 20 mm/rev …. 300 mm/rev					

Table 144: Data of some commercially available linear axes - feed constants to be observed

$$\text{Positionsfaktor} = \frac{\text{Getriebeübersetzung} * \text{Inkremente/Umdrehung}}{\text{Vorschubkonstante}}$$

7.4 Status messages, diagnostics via fieldbus

7.4.1 Output of status messages via the digital outputs of the basic unit

The servo drive can output important status signals of the safety module to the digital outputs DOUT0 to DOUT3 via the I/O interface [X1].

The digital outputs are configured using the parameterisation program Metronix ServoCommander® (MSC).

The following common messages are available for output (see Section 2.10.2):

VOUT	Signal	Name	Function
40	VOUT_PS_EN	Output stage enable approved	Status bit specifies whether the servo drive can switch on the output stage.
41	VOUT_WARN	Warning	At least one error with the priority "Warning" has occurred.
42	VOUT_SCV	Safety condition violated	At least one safety condition has been violated.
43	VOUT_ERROR	Error	The safety module has detected an internal error.
44	VOUT_SSR	Safe state reached	Global bit "Safe state reached", all the requested safety functions are indicating a safe status.
45	VOUT_SFR	Safety function requested	Global bit "Safety function requested", at least one safety function is requested. Remains active until all the requests have been reset.
46	VOUT_SERVICE	Service status	"Service" status, no parameters present, parameter invalid or parameterisation session is running.
47	VOUT_READY	Ready for operation	"Ready for operation" status, no safety function requested.

Table 145: Status signal of the safety module for output via DOUTx of the basic unit

The outputs of the basic device must not be used in systems for safety-relevant use!

The status signals of the FSM 2.0 – MOV are compatible with those of the FSM 2.0 – STO (safety module with "Safe Torque Off" safety function).

In applications with mixed use of the safety module, this achieves standardised feedback to the controller.

7.4.2 Status signals via fieldbus – CANopen protocol

The servo drive has all the key information of the safety module (status, modes, errors, IO). The following information is primarily relevant for transfer of data to bus systems, in order to create a detailed map of the system in a function controller:

- Common status messages on the status of the safety module (normal operation, safety function requested, errors, etc. ➔ see Section 2.10.2).
- Status of the individual safety functions (Which have been requested? Which have been implemented?).
- Status of the digital inputs and outputs.

Below, the appropriate CANopen objects are listed, which contain information on the safety module and which the ARS 2000 FS supports.

7.4.2.1 Object 2000h: manufacturer_statuswords

The object group manufacturer_statuswords was introduced, in order to map additional controller statuses which do not need to be present in the status word, which is queried often. The object group manufacturer_statuswords was extended for the safety module.

Index	**2000_h**
Name	**manufacturer_statuswords**
Object Code	RECORD
No. of elements	2

Sub-Index	**00_h**
Description	**manufacturer_statuswords**
Data Type	UINT8
Access	ro
PDO Mapping	no
Units	–
Value Range	–
Default Value	1

Sub-Index	**01_h**
Description	**manufacturer_statusword_1**
Data Type	UINT32
Access	ro
PDO Mapping	yes
Units	–
Value Range	–
Default Value	–

manufacturer_statusword_1		
Bit	**Signal**	**Description**
Bit 0	IS_REFERENCED	Drive is referenced
Bit 1	COMMUTATION_ VALID	Commutation valid
Bit 2	READY_FOR_ENABLE	The bit is set if all conditions to enable the controller are present and only the controller enable itself is lacking. The following conditions must be present: – The drive is error free. – The intermediate circuit is loaded. – Angle encoder analysis is ready. No processes (e.g. serial transmission) are active that prevent enabling. – No blocking process is active (e.g. the automatic motor parameter identification). – STO is not active or a safety function is active, which permits enabling.
Bit 3	IPO_IN_TARGET	Positioning generator has completed the profile.
Bit 4 ... 7	CAM	Reserved and used for the cam.
Bit 8	SAFE_STANDSTILL	"Safe Stop" "H" on the 7-segment display. Use by the safety module FSM 2.0 – STO
Bit 9 ... 11	–	Reserved for extensions
Bit 12	VOUT_PS_EN	Displays that the drive can be switched on (no limitations by safety module).
Bit 13	VOUT_WARN	Corresponds to VOUT_WARN (VOUT41) of the safety module. There is at least one error, whose error response is parameterised as "Warning".
Bit 14	VOUT_SCV	Corresponds to VOUT_SCV (VOUT 42) of the safety module. At least one safety condition has been violated.
Bit 15	VOUT_ERROR	Corresponds to VOUT_ERROR (VOUT 43) of the safety module. An internal fault was ascertained.
Bit 16	VOUT_SAVE_STAT	Corresponds to VOUT_SSR (VOUT 44) of the safety module. The bit is set when a safety function was requested in the safety module and the safe state has been reached.
Bit 17	VOUT_SFR	Corresponds to VOUT_SFR (VOUT 45) of the safety module. The bit is set when at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
Bit 18	VOUT_SERVICE	No parameters present, parameter invalid or parameterisation procedure is running (not supported by FSM 2.0 – STO). Status is assumed when the safety module was replaced with another type.
Bit 19	VOUT_READY	Normal status: VOUT_READY= NOT(VOUT_SFR)
Bit 20 ... 31	–	Reserved.

Table 146: Bit allocation for manufacturer_statusword_1

7.4.2.2 Object 2600h: FSM_VOUT

These objects map the status of the VOUT (0..64).

Index	**2600_h**
Name	**FSM_vout**
Object Code	RECORD
No. of Elements	2

Sub-Index	**01_h**
Description	**FSM_vout_0_31**
Data Type	UINT32
Access	ro
PDO Mapping	yes
Units	–
Value Range	–
Default Value	–

Bits 0..31 = VOUT0..31 of the safety module

Sub-Index	**02_h**
Description	**FSM_vout_32_63**
Data Type	UINT32
Access	ro
PDO Mapping	yes
Units	–
Value Range	–
Default Value	–

Bits 0..31 = VOUT32..63 of the safety module

7.4.2.3 Object 2602h: FSM_IO

Read the level at the inputs of the safety module

Index	**2602_h**
Name	**FSM_io**
Object Code	RECORD
No. of Elements	1

Sub-Index	**01_h**
Description	**FSM_dig_io**
Data Type	UINT32
Access	ro
PDO Mapping	yes
Units	–
Value Range	–
Default Value	–

FSM_dig_io		
Bit	Signal	Description
Bit 0	LOUT48	Logical status DIN40 A/B
Bit 1	LOUT49	Logical status DIN41 A/B
Bit 2	LOUT50	Logical status DIN42 A/B
Bit 3	LOUT51	Logical status DIN43 A/B
Bit 4	LOUT52	Logical status DIN44
Bit 5	LOUT53	Logical status DIN45; mode selector switch (1 of 3)
Bit 6	LOUT54	Logical status DIN46; mode selector switch (1 of 3)
Bit 7	LOUT55	Logical status DIN47; mode selector switch (1 of 3)
Bit 8	LOUT56	Error acknowledgement via DIN48
Bit 9	LOUT57	Restart via DIN49
Bit 10	LOUT58	Logical status, two-handed control device (pair of 2 x DIN4x)
Bit 11	LOUT59	Feedback, holding brake
Bit 12 ... 15	LOUT60 ... 63	Not used
Bit 16	LOUT64	Status of the output DOUT40
Bit 17	LOUT65	Status of the output DOUT41
Bit 18	LOUT66	Status of the output DOUT42
Bit 19	LOUT67	Status of the signal relay
Bit 20	LOUT68	Brake control
Bit 21	LOUT69	Status of the SS1 control signal
Bit 22 ... 31	LOUT70 ...	Not used

Table 147: Bit assignment FSM_dig_io

7.4.3 Status signals via other fieldbus protocols

The servo drive has all the key information of the safety module (status, modes, errors, IO). The following information is primarily relevant for transfer of data to bus systems, in order to create a detailed map of the system in a function controller:

- Common status messages on the status of the safety module (normal operation, safety function requested, errors, ... -> see Section 2.10.2).
- Status of the individual safety functions (Which have been requested? Which have been implemented?).
- Status of the digital inputs and outputs.

At present, the required information can be read out via internal communication objects (COs). This interface is available in all bus systems.

7.5 Recording of measurement data – oscilloscope

7.5.1 Overview

For diagnostic purposes, you can also use the oscilloscope function of the Metronix ServoCommander® (MSC) to record the measurement data of the safety module FSM 2.0 – MOV, in addition to the normal data of the servo drive.

The recorded measurement data is used for troubleshooting. It is not safety-relevant.

The measurement data are parameterised and recorded with the parameterisation program Metronix ServoCommander® (MSC) (➔Section 7.5.2).

You can record up to four items of numeric or digital data in parallel. The following data is available for the safety module:

Data	Description
Numeric data	
Upper limit, speed setpoint value[1)]	Current upper speed limit in the basic unit, limit set by the safety module.
Lower limit, speed setpoint value[1)]	Current lower speed limit in the basic unit, limit set by the safety module.
FSM 2.0 – MOV: Actual speed value	Actual rotational speed value from the safety module.
FSM 2.0 – MOV: Actual position value	Actual position value from the safety module.
FSM 2.0 – MOV: Currently monitored upper speed limit	Current upper speed limit monitored by the safety module.
FSM 2.0 – MOV: Currently monitored lower speed limit	Current lower speed limit monitored by the safety module.
Freely selectable CO ...	This selection can be used to record any number of parameters ➔ Section 7.5.2.
Digital Data	
FSM 2.0 – MOV: ...	Status bits of the safety module
FSM 2.0 – MOV: DIN40A	Physical status of the input DIN40A
...	Physical statuses of the other inputs ...
FSM 2.0 – MOV: DOUT40A	Physical status of the output DOUT40A
...	Physical statuses of the other outputs ...
FSM 2.0 – MOV: C1/C2	Physical status of the signal contact C1/C2
1) Data from basic unit	

Table 148: Measurement data for the safety module

7.5.2 Configure

The recorded data is specified as usual in the Metronix ServoCommander® in the **Oscilloscope - Settings** window. It is opened via the menu **Display/Oscilloscope** and the button **Settings**.

For the safety module, the additional numerical and digital data contained in ➔ Table 148 is available.

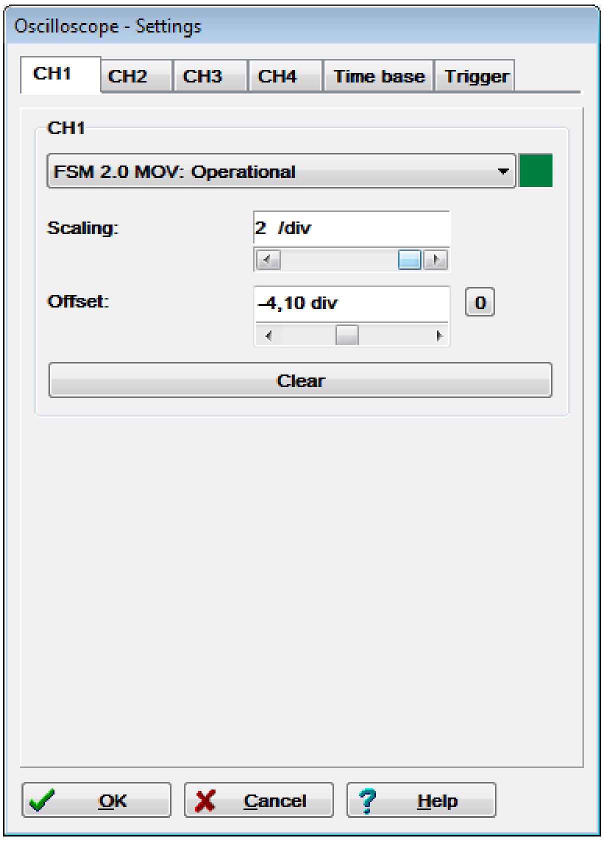


Figure 72: "Oscilloscope - Settings" window

With the exception of **FSM 2p0 MOV: Freely selectable comm. object**, you can set the entries directly.

A special dialog box is opened for the freely-selectable COs (communication objects): Select the option **FSM 2p0 MOV: Freely selectable comm. object** in the scroll box under **CH1..CH4**:

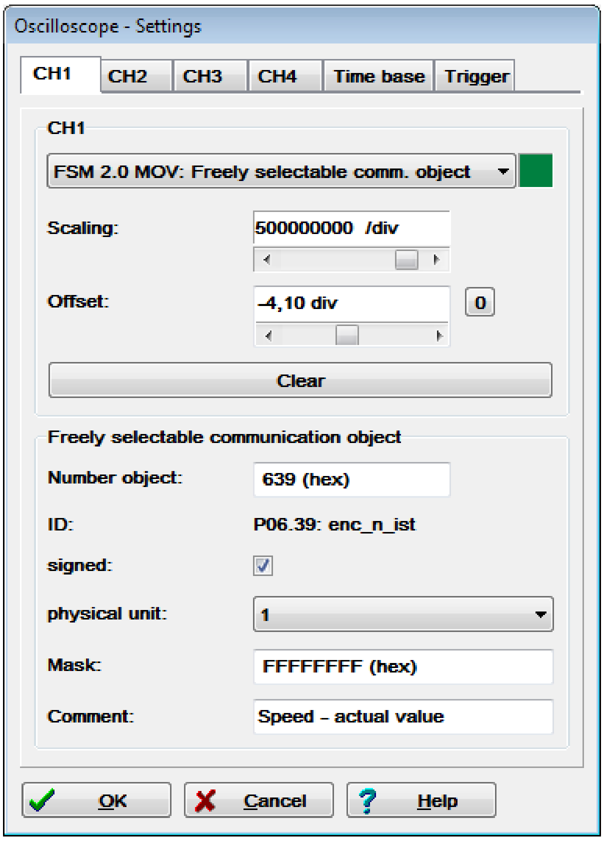


Figure 73: Freely selectable communication object

1. Under **Freely selectable communication object**, enter the number as a hexadecimal value. The number corresponds to the parameter number without "P" and the period. In the example, "639" stands for P06.39 – actual value of the safe speed. The parameter **ID** is displayed below.
   You can find useful parameters, for example, in ➔Section 8.2, Table 158 "Diagnostic parameters".
2. By activating or deactivating the check box **signed**, you can determine whether the value has to be signed or unsigned.
3. In the scroll box **physical unit**, select the correct entry for the measurement quantity so that it will be displayed correctly in the diagram later on.
4. In the field **Mask**, you can specify a mask, for example for bit arrays or other digital data.
5. For a clear identification of the measurement quantity, you can enter any text into the field **Comment** to describe the freely selectable CO. This text will not be saved in the servo drive.
6. Confirm your settings with **OK**.

7.5.3 Starting the oscilloscope

The **RUN / STOP** check box is used to activate or deactivate the oscilloscope. Activate the check box if you want to use the oscilloscope.

The LED indicates the current operating status of the oscilloscope. A green LED means: the oscilloscope is active. An inactive oscilloscope is indicated by a red LED.

7.5.4 Example

Any violation of the safety condition on SS1 should be recorded. DOUT42 is requested as a trigger by VOUT_SCV "Safety Condition Violated".

As shown in Figure 74, the following data is set:

- **CH1** – FSM 2.0 – MOV: Currently monitored upper speed limit
- **CH2** – FSM 2.0 – MOV: Actual speed value
- **CH3** – FSM 2.0 – MOV: Currently monitored lower speed limit
- **CH4** – FSM 2.0 – MOV: DOUT42A

This results, for example, in the following diagram:

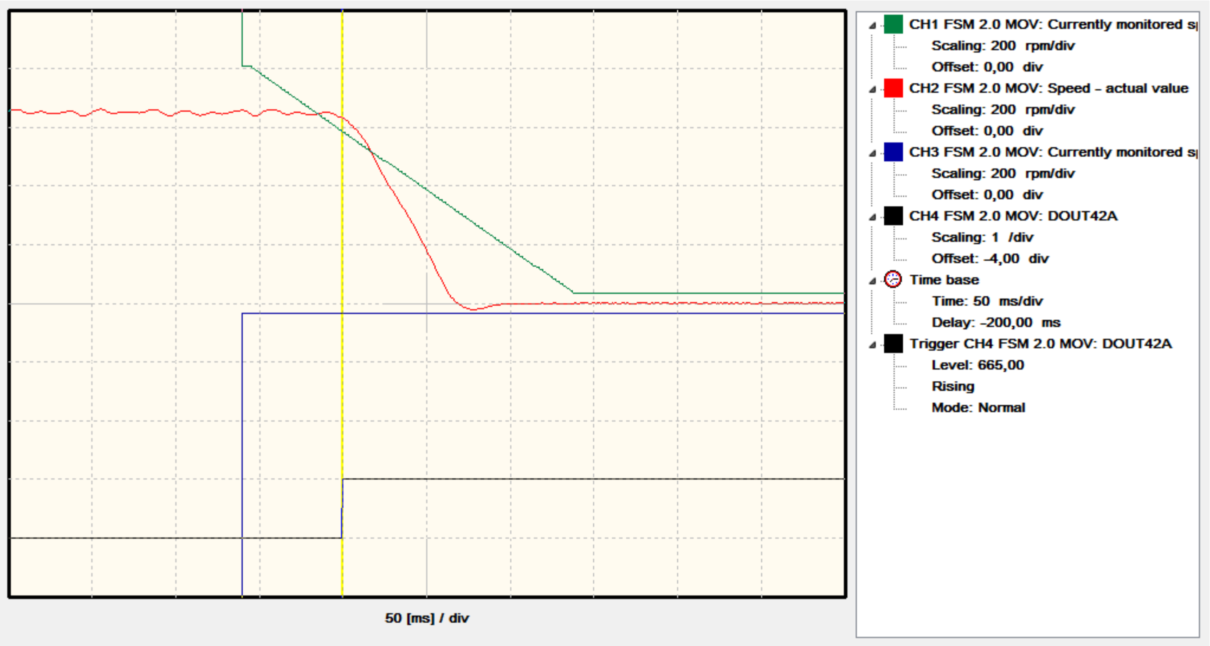


Figure 74: Diagram example

8 Reference list for control signals and parameters

8.1 List of all logic signals

8.1.1 Logical inputs LIN

The logical inputs are combined into a bit vector with a length of 128 bits.

The bit vector has the following structure:

LIN	Name	Function
0	–	Reserved for later expansion of the functionality of the safety module, always zero.
...	...	
63	–	
64	LIN_USF0_SSR	Returned virtual output signals VOUT (status signals of the safety functions, common messages). This means that they can be linked logically with the input signals.
...	...	
95	LIN_READY	
96	LIN_D40	Logical status of the digital inputs DIN40…DIN49, as well as the output signals of the logic functions and some auxiliary statuses.
...	...	
127	LIN_STATIC_ONE	

Table 149: Structure of the bit vector of the logical inputs

The current status of the bit vector LIN can be read via the communication objects:
Bit 00 ... Bit 31: P04.20
Bit 32 ... Bit 63: P04.21
Bit 64 ... Bit 95: P04.22
Bit 66 ... Bit 127: P04.23

8.1.1.1 Mapping of the physical inputs to the logical inputs

The physical inputs are mapped to the logical inputs as follows (the stationary status after filtering, test pulse analysis, etc. is stated):

LIN	Name	Function
96	LIN_D40	Bit LIN_D40 set, if DIN40 A/B = 0 V (idle current principle)[1)]
97	LIN_D41	Bit LIN_D41 set, if DIN41 A/B = 0 V (idle current principle)[1)]
98	LIN_D42	Bit LIN_D42 set, if DIN42 A/B = 0 V (idle current principle)[1)]
99	LIN_D43	Bit LIN_D43 set, if DIN43 A/B = 0 V (idle current principle)[1)]
100	LIN_D44	Bit LIN_D44 set, if DIN44 = 24 V
101	LIN_D45	Bit LIN_D45 set, if DIN47 = 0 V and DIN46 = 0 V and DIN45 = 24 V
102	LIN_D46	Bit LIN_D46 set, if DIN47 = 0 V and DIN46 = 24 V and DIN45 = 0 V
103	LIN_D47	Bit LIN_D47 set, if DIN47 = 24 V and DIN46 = 0 V and DIN45 = 0 V
104	LIN_D48	Bit LIN_D48 set, if DIN48 = 24 V
105	LIN_D49	Bit LIN_D49 set, if DIN49 = 24 V
1) Valid for configuration as equivalent input. Configuration as antivalent input accordingly: LIN_DIN4x set, when D4xA = 0 V and D4xB = 24 V.		

Table 150: Logical inputs, level assignment to the physical inputs

Please note that LIN_D40 ... LIN_D43 have a special assignment to the voltage levels. This means that the logical inputs can be fed to the safety functions (e.g. request STO) without inversion, implementing the idle current principle (input 0 V = STO requested).

8.1.1.2 Logical inputs after preliminary processing and auxiliary functions

Mapping of the physical inputs after preliminary processing (time expectation, 1-of-n etc.)

LIN	Name	Function
96	LIN_D40	Logical status DIN40 A/B
97	LIN_D41	Logical status DIN41 A/B
98	LIN_D42	Logical status DIN42 A/B
99	LIN_D43	Logical status DIN43 A/B
100	LIN_D44	Logical status DIN44
101	LIN_D45	Logical status DIN45; mode selector switch (1 of 3) Logical status DIN45 - 47 (1 of 3) DIN45
102	LIN_D46	Logical status DIN45 - 47 (1 of 3) DIN46
103	LIN_D47	Logical status DIN45 - 47 (1 of 3) DIN47
104	LIN_D48	Logical status DIN48
105	LIN_D49	Logical status DIN49
106	LIN_2HAND_CTRL	Logical status, two-handed control device (pair of 2 x DIN4x)
107	LIN_BRAKE_X6_FB	Feedback, holding brake
117	LIN_PWSTG_ON	Basic unit, output stage active
121	LIN_D45_SAFE	Logical status DIN45 after mode selector switch analysis
122	LIN_D46_SAFE	DIN46 after mode selector switch analysis
123	LIN_D47_SAFE	DIN47 after mode selector switch analysis
124	LIN_D49_RISING_EDGE	Logical "1" pulse with approx. 2 ms – 10 ms length after each rising edge of the signal LIN_D49. Intended for "edge-sensitive restart".
125	LIN_AFTER_RST_PULSE	Logical "1" pulse with approx. 2 ms – 10 ms length after each RESET. Intended for first automatic setting of a safety function request after Power On or after a system RESET.
126	LIN_STATIC_ZERO	Always "0"
127	LIN_STATIC_ONE	Always "1"

Table 151: Logical inputs after preliminary processing

8.1.1.3 Virtual outputs returned as logical outputs

LIN	Name	Function
64	LIN_USF0_SSR	Safe state USF0 reached
65	LIN_USF1_SSR	Safe state USF1 reached
66	LIN_USF2_SSR	Safe state USF2 reached
67	LIN_USF3_SSR	Safe state USF3 reached
75	LIN_SBC_SSR	Safe state SBC reached
76	LIN_SS2_SSR	Safe state SS2 reached
77	LIN_SOS_SSR	Safe state SOS reached
78	LIN_SS1_SSR	Safe state SS1 reached
79	LIN_STO_SSR	Safe state STO reached
80	LIN_ALF0_OUT	"Additional Logic Function" for feedback or own logic
81	LIN_ALF1_OUT	"Additional Logic Function" for feedback or own logic
82	LIN_ALF2_OUT	"Additional Logic Function" for feedback or own logic
83	LIN_ALF3_OUT	"Additional Logic Function" for feedback or own logic
84	LIN_ALF4_OUT	"Additional Logic Function" for feedback or own logic
85	LIN_ALF5_OUT	"Additional Logic Function" for feedback or own logic
86	LIN_ALF6_OUT	"Additional Logic Function" for feedback or own logic
87	LIN_ALF7_OUT	"Additional Logic Function" for feedback or own logic
88	LIN_PS_EN	Status bit specifies whether the servo drive can switch on the output stage
89	LIN_WARN	At least one error with the priority "Warning" has occurred
90	LIN_SCV	At least one of the safety conditions was violated
91	LIN_ERROR	The safety module has detected an internal error
92	LIN_SSR	Global bit "Safe State Reached", when at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
93	LIN_SFR	Global bit "Safety function requested", at least one safety function has been requested but not yet reached.
94	LIN_SERVICE	Service status, no parameters present, parameter invalid or parameterisation session is running.
95	LIN_READY	Ready for operation status, no safety function requested

Table 152: Logical inputs, returned virtual outputs

8.1.2 Virtual inputs VIN

The virtual inputs are the inputs of the safety functions and the additional logic functions (ALF = additional logic function). The following abbreviations apply:

"RSF" = Request Safety Function.

"CSF" = Clear Safety Function, restart after violated safety condition.

The virtual inputs are combined into a bit vector with a length of 64 bits.

The current status of the bit vector VIN can be read via the communication objects:
Bit 00 ... Bit 31: P04.24
Bit 32 ... Bit 63: P04.25

8.1.2.1 Mapping of the virtual inputs

VIN	Name	Function
0	VIN_USF0_RSF	Request safety function USF0
1	VIN_USF1_RSF	Request safety function USF1
2	VIN_USF2_RSF	Request safety function USF2
3	VIN_USF3_RSF	Request safety function USF3
4	–	Reserved, always zero
...	...	
10	–	
11	VIN_SBC_RSF	Request SBC safety function
12	VIN_SS2_RSF	Request SS2 safety function
13	VIN_SOS_RSF	Request SOS safety function
14	VIN_SS1_RSF	Request SS1 safety function
15	VIN_STO_RSF	Request STO safety function
16	VN_USF0_CSF	Terminate USF0 request
17	VIN_USF1_CSF	Terminate USF1 request
18	VIN_USF2_CSF	Terminate USF2 request
19	VIN_USF3_CSF	Terminate USF3 request
27	VIN_SBC_CSF	Terminate SBC request
28	VIN_SS2_CSF	Terminate SS2 request
29	VIN_SOS_CSF	Terminate SOS request
30	VIN_SS1_CSF	Terminate SS1 request
31	VIN_STO_CSF	Terminate STO request
32	VIN_ALF0_IN	Input, additional logic function ALF0
33	VIN_ALF1_IN	Input, additional logic function ALF1

VIN	Name	Function
34	VIN_ALF2_IN	Input, additional logic function ALF2
35	VIN_ALF3_IN	Input, additional logic function ALF3
36	VIN_ALF4_IN	Input, additional logic function ALF4
37	VIN_ALF5_IN	Input, additional logic function ALF5
38	VIN_ALF6_IN	Input, additional logic function ALF6
39	VIN_ALF7_IN	Input, additional logic function ALF7
40	–	Reserved for future extensions of ALF, always zero
...	...	
47	–	
48	–	Reserved for later expansion of the functionality of the safety module, always zero
...	...	
59	–	
60	VIN_ERR_QUIT	Acknowledge error
61	–	Reserved, always zero
62	–	Reserved, always zero
63	VIN_BRK_ACK	Feedback holding brake

Table 153: Virtual inputs

8.1.3 Virtual outputs VOUT

The virtual outputs are the outputs of the safety functions and the additional logic functions. They are defined in terms such as "SS1_Safe_State_Reached". The following abbreviations apply:

SFR = Safety Function Requested

SSR = Safe State Reached

The virtual outputs are combined into a bit vector with a length of 64 bits. Selected virtual output signals are fed back into the processing as logical inputs, see Table 152.

The current status of the bit vector VOUT can be read via the communication objects:
Bit 00 ... Bit 31: P05.10
Bit 32 ... Bit 63: P05.11

VOUT	Name	Function
0	VOUT_USF0_SFR	USF0 safety function requested
1	VOUT_USF1_SFR	USF1 safety function requested
2	VOUT_USF2_SFR	USF2 safety function requested
3	VOUT_USF3_SFR	USF3 safety function requested
4	–	Reserved, always zero
...	...	
10	–	
11	VOUT_SBC_SFR	SBC safety function requested
12	VOUT_SS2_SFR	SS2 safety function requested
13	VOUT_SOS_SFR	SOS safety function requested
14	VOUT_SS1_SFR	SS1 safety function requested
15	VOUT_STO_SFR	STO safety function requested
16	VOUT_USF0_SSR	Safe state USF0 reached
17	VOUT_USF1_SSR	Safe state USF1 reached
18	VOUT_USF2_SSR	Safe state USF2 reached
19	VOUT_USF3_SSR	Safe state USF3 reached
20	–	Reserved, always zero
...	...	
26	–	
27	VOUT_SBC_SSR	Safe state SBC reached
28	VOUT_SS2_SSR	Safe state SS2 reached
29	VOUT_SOS_SSR	Safe state SOS reached
30	VOUT_SS1_SSR	Safe state SS1 reached
31	VOUT_STO_SSR	Safe state STO reached
32	VOUT_ALF0_OUT	Output, additional logic function ALF0
33	VOUT_ALF1_OUT	Output, additional logic function ALF1
34	VOUT_ALF2_OUT	Output, additional logic function ALF2
35	VOUT_ALF3_OUT	Output, additional logic function ALF3
36	VOUT_ALF4_OUT	Output, additional logic function ALF4
37	VOUT_ALF5_OUT	Output, additional logic function ALF5
38	VOUT_ALF6_OUT	Output, additional logic function ALF6
39	VOUT_ALF7_OUT	Output, additional logic function ALF7
40	VOUT_PS_EN	Status bit specifies whether the servo drive can switch on the output stage
41	VOUT_WARN	At least one error with the priority "Warning" has occurred

VOUT	Name	Function
42	VOUT_SCV	At least one safety condition was violated
43	VOUT_ERROR	The safety module has detected an internal error
44	VOUT_SSR	Global bit "Safe state reached", all the requested safety functions are indicating a safe status
45	VOUT_SFR	Global bit "Safety function requested", at least one safety function is requested in the safety module. The bit remains set until all the requests have been reset.
46	VOUT_SERVICE	"Service" status, no parameters present, parameter invalid or parameterisation session is running
47	VOUT_READY	"Ready for operation" status, no safety function requested
48	–	Reserved, always zero
...	...	
62	–	
63	VOUT_SBC_BRK_ON	Engage holding brake

Table 154: Virtual output signals

8.1.4 Logical outputs LOUT

Like the logical inputs, the status of the logical outputs is represented by 1 bit. This also applies for two-channel outputs.

Equivalence / antivalence and test signals are processed into physical outputs during the conversion of the logical outputs.

The logical outputs are combined into a bit vector with a length of 96 bits.

The current status of the bit vector LOUT can be read via the communication objects:
Bit 00 ... Bit 31: P05.12
Bit 32 ... Bit 63: P05.13
Bit 64 ... Bit 95: P05.14

8.1.4.1 Mapping of the logical outputs

LOUT	Name	Function
0	–	Logical outputs for diagnostics via fieldbuses ➔ Section 7.4
...	...	
63	–	
64	LOUT_D40	Status of the output DOUT40
65	LOUT_D41	Status of the output DOUT41
66	LOUT_D42	Status of the output DOUT42
67	LOUT_RELAIS	Status of the signal relay C1/C2
68	LOUT_BRK_CTRL	Brake control
69	LOUT_SS1_RQ	SS1 control signal (fixed wiring)
70	–	Reserved, always zero
...	...	
95	–	

Table 155: Logical outputs, mapping of the physical outputs

The physical outputs are assigned to the logical outputs LOUT64 ... LOUT69.

8.1.5 Status words for the data exchange / diagnostics via fieldbuses

The safety module and the basic unit exchange data on a regular basis. In this way, important data from the safety module is sent and is available for data exchange with a functional controller and for diagnostic functions.

The data of the communication objects in the safety module is "mirrored" in corresponding communication objects in the basic unit.

This data is used for:

- status messages via fieldbuses and digital outputs,
- recording of data using the oscilloscope function of the basic unit.

Table 156 lists the appropriate diagnostic communication objects. This means that the data of the safety module can be read out in the basic unit via the communication objects 0794h to 0797h.

CO basic unit	Name of the CO in the basic unit	CO of safety module	Transmitted value[1)]	Meaning/value sent to the basic unit
0782	ioh_fsm_mov_vout_0_31	P05.10	---	Actual value of the virtual outputs VOUT00…VOUT31
0783	ioh_fsm_mov_vout_32_63	P05.11	---	Actual value of the virtual outputs VOUT32…VOUT63
079B	ioh_fsm_limit_speed_upper			Current upper speed limit in the basic unit
079C	ioh_fsm_limit_speed_lower			Current lower speed limit in the basic unit
0790	ioh_fsm_diag_ch0	---	P06.39	Selection of the CO sent to diagnostic channel 0
0791	ioh_fsm_diag_ch1	---	P04.23	Selection of the CO sent to diagnostic channel 1
0792	ioh_fsm_diag_ch2	---	P05.10	Selection of the CO sent to diagnostic channel 2
0793	ioh_fsm_diag_ch3	---	P05.11	Selection of the CO sent to diagnostic channel 3
0794	ioh_fsm_dat_ch0	P1D.00	P06.39	Safe actual speed of the safety module
0795	ioh_fsm_dat_ch1	P1D.01	P04.23	Status of the logical inputs LIN96…LIN127 ➔ Table 151
0796	ioh_fsm_dat_ch2	P1D.02	P05.10	Status of the virtual outputs VOUT0…VOUT31 ➔ Table 154
0797	ioh_fsm_dat_ch3	P1D.03	P05.11	Status of the virtual outputs VOUT32…VOUT63 ➔ Table 154

1) Default setting

Table 156: List of the diagnostic information for the basic unit

The diagnostic outputs can be revised if needed. For this, use the oscilloscope function of the MSC ➔ Section 7.5. Make the following settings:

1. The COs of the safety module, which are to be recorded, are entered in the basic unit COs nos. 0790h to 0793h.
2. The setting is saved in the basic unit and a restart carried out. The settings are then sent to the safety module.

Example:

CO 0790h → Value: 0639h Transfer of the safe speed
CO 0791h → Value: 0423h Status of LIN96…LIN127 (LIN_D40…LIN_D49, etc.)
CO 0792h → Value: 1D09h Upper speed monitoring limit
CO 0793h → Value: 1D0Ah Lower speed monitoring limit
RESET / Restart:
CO 0794h ← Value: 0639h Transfer of the safe speed
CO 0795h ← Value: 0423h Status of LIN96…LIN127 (LIN_D40…LIN_D49 etc.)
CO 0796h ← Value: 1D09h Upper speed monitoring limit ➔ see list 8.2
CO 0797h ← Value: 1D0Ah Lower speed monitoring limit ➔ see list 8.2
The appropriate data is shown in the basic unit COs 0794h to 0797h (time resolution approx. 2 ms).

8.2 List of additional parameters

The SafetyTool has a menu item called Tools/Parameter overview for experts. It allows you to view or change the parameters of the safety module. Filters can be used to select the parameters which you want to see. This means, for example, that those parameters can be found quickly whose settings are different in the Safety Tool and the safety module.

i

Most parameters are described in the context of the appropriate function:

– basic information ➔ Table 11, page 53
– encoder configuration ➔ Table 14, page 63
– two-channel digital inputs ➔ Table 24, page 74
– single-channel digital inputs ➔ Table 27, page 77
– STO: Safe Torque Off ➔ Table 33, page 86
– SS1: Safe Stop 1 ➔ Table 44, page 102
– SS2: Safe Stop 2 ➔ Table 50, page 109
– SOS: Safe Operating Stop ➔ Table 54, page 114
– SSF: Safe speed ➔ Table 59, page 121
– SBC: Safe Brake Control ➔ Table 38, page 94
– logic functions for mode selector switch ➔ Table 66, page 127
– logic functions for two-handed operator unit ➔ Table 69, page 129
– logic functions for Advanced Logic Functions ➔ Table 72, page 130
– digital outputs panel ➔ Table 81, page 144

The following tables contain a compilation of all the parameters which have not yet been explained above.

Error management		
No.	**Name**	**Description**
P20.00	[53-0] USF0: Safety condition violated	Error response of the error 53-0
P20.01	[53-1] USF1: Safety condition violated	Error response of the error 53-1
P20.02	[53-2] USF2: Safety condition violated	Error response of the error 53-2
P20.03	[53-3] USF3: Safety condition violated	Error response of the error 53-3
P20.0A	[54-0] SBC: Safety condition violated	Error response of the error 54-0
P20.0C	[54-2] SS2: Safety condition violated	Error response of the error 54-2
P20.0D	[54-3] SOS: Safety condition violated	Error response of the error 54-3
P20.0E	[54-4] SS1: Safety condition violated	Error response of the error 54-4
P20.0F	[54-5] STO: Safety condition violated	Error response of the error 54-5
P20.10	[54-6] SBC: Brake not vented for > 24 hrs	Error response of the error 54-6
P20.11	[54-7] SOS: SOS > 24 hr requested	Error response of the error 54-7

Error management		
No.	**Name**	**Description**
P20.14	[55-0] No actual rotational speed / position value available or standstill > 24 hrs	Error response of the error 55-0
P20.15	[55-1] SINCOS encoder [X2B] - Tracking signal error	Error response of the error 55-1
P20.16	[55-2] SINCOS encoder [X2B] - Standstill > 24 hrs	Error response of the error 55-2
P20.17	[55-3] Resolver [X2A] - Signal error	Error response of the error 55-3
P20.18	[55-4] EnDat encoder [X2B] - Sensor error	Error response of the error 55-4
P20.19	[55-5] EnDat encoder [X2B] - Incorrect sensor type	Error response of the error 55-5
P20.1A	[55-6] Incremental encoder [X10] - Tracking signal error	Error response of the error 55-6
P20.1B	[55-7] Other encoder [X2B] - Faulty angle information	Error response of the error 55-7
P20.26	[56-8] Rotational speed / angle difference, encoder 1 - 2	Error response of the error 56-8. The error is triggered when one of the two microcontrollers detects an impermissible position or speed difference between encoder 1 and encoder 2
P20.27	[56-9] Error, cross-comparison of encoder analysis	Error response of the error 56-9. The error is triggered when an impermissible position difference is detected during cross-comparison of the safe position values between microcontroller 1 and microcontroller 2
P20.28	[57-0] Error, I/O self test (internal/external)	Error response of the error 57-0
P20.29	[57-1] Digital inputs - Signal level error	Error response of the error 57-1
P20.2A	[57-2] Digital inputs - Test pulse error	Error response of the error 57-2
P20.2E	[57-6] Electronics temperature too high	Error response of the error 57-6
P20.32	[58-0] Plausibility check of parameters	Error response of the error 58-0
P20.33	[58-1] General error, parameterisation	Error response of the error 58-1
P20.36	[58-4] Buffer, internal communication	Error response of the error 58-4
P20.37	[58-5] Communication module - basic unit	Error response of the error 58-5

Error management		
No.	**Name**	**Description**
P20.38	[58-6] Error in cross-comparison for processors 1 - 2	Error response of the error 58-6. The error is triggered if an impermissible deviation occurs when comparing microcontrollers 1 and 2. Examples: different statuses of the inputs and outputs, or different safe speed values. Error 56-9 is triggered in special cases where position values deviate.
P20.3D	[59-1] Failsafe supply/safe pulse inhibitor	Error response of the error 59-1
P20.3E	[59-2] Error external power supply	Error response of the error 59-2
P20.3F	[59-3] Error internal power supply	Error response of the error 59-3
P20.40	[59-4] Error management: Too many errors	Error response of the error 59-4
P20.41	[59-5] Error writing to permanent event memory	Error response of the error 59-5
P20.42	[59-6] Error on saving parameter set	Error response of the error 59-6
P20.43	[59-7] FLASH checksum error	Error response of the error 59-7
P20.44	[59-8] Internal monitoring, processor 1 - 2	Error response of the error 59-8
P20.45	[59-9] Other unexpected error	Error response of the error 59-9

Table 157: Error management

Diagnostic parameters		
No.	**Name**	**Description**
P00.00	Parameter set version	Parameter set version
P20.46	Error status, group 53 and 54:	Main error number 53 and 54 in the error field
P20.47	Error status, group 55 and 56:	Main error number 55 and 56 in the error field
P20.48	Error status, group 57 and 58:	Main error number 57 and 58 in the error field
P20.49	Error status, group 59:	Main error number 59 in the error field
Expert parameter		
P02.2F	Status of the digital inputs	Status of the digital inputs
P02.38	Status of the digital outputs	Status of the digital outputs
P02.39	Status of the digital outputs B	Status of the digital outputs
P02.3A	Status of the digital inputs B	Status of the digital inputs
P05.10	Status VOUT0…VOUT31	Actual values of VOUT0..VOUT31
P05.11	Status VOUT32…VOUT63	Actual values of VOUT32..VOUT63
P05.12	Status LOUT0…LOUT31	Actual values of LOUT0..LOUT31
P05.13	Status LOUT32…LOUT63	Actual values of LOUT32..LOUT63
P05.14	Status LOUT64…LOUT95	Actual values of LOUT64..LOUT95
P06.39	Actual value of safe speed	Actual rotational speed value
P06.3A	Safe position	Actual position value shortened to 32 bits
P06.3B	Safe acceleration	Acceleration from angle encoder
P06.3C	Angle from encoder 1	Angle from encoder 1 (without gear unit)
P06.3D	Angle from encoder 2	Angle from encoder 2 (without gear unit)
P06.56	Position from encoder 1	Calculated position of encoder 1 (including gear unit conversion)
P06.57	Position from encoder 2	Calculated position of encoder 2 (including gear unit conversion)
P1D.00	CO for diagnostics channel 0	CO for output as diagnostics channel 0
P06.58	Speed from encoder 1	Calculated speed of encoder 1 (including gear unit conversion)
P1D.01	CO for diagnostics channel 1	CO for output as diagnostics channel 1
P06.59	Speed from encoder 2	Calculated speed of encoder 2 (including gear unit conversion)
P1D.02	CO for diagnostics channel 2	CO for output as diagnostics channel 2
P1D.03	CO for diagnostics channel 3	CO for output as diagnostics channel 3
P0E.50	Current upper speed limit	Current upper speed limit in the safety module
P0E.51	Current lower speed limit	Current lower speed limit in the safety module

Table 158: Diagnostic parameters

Mapping		
No.	**Name**	**Description**
P04.00	Product term	Mapping and allocation for product term 0
P04.01	Product term	Mapping and allocation for product term 1
P04.02	Product term	Mapping and allocation for product term 2
P04.03	Product term	Mapping and allocation for product term 3
P04.04	Product term	Mapping and allocation for product term 4
P04.05	Product term	Mapping and allocation for product term 5
P04.06	Product term	Mapping and allocation for product term 6
P04.07	Product term	Mapping and allocation for product term 7
P04.08	Product term	Mapping and allocation for product term 8
P04.09	Product term	Mapping and allocation for product term 9
P04.0A	Product term	Mapping and allocation for product term 10
P04.0B	Product term	Mapping and allocation for product term 11
P04.0C	Product term	Mapping and allocation for product term 12
P04.0D	Product term	Mapping and allocation for product term 13
P04.0E	Product term	Mapping and allocation for product term 14
P04.0F	Product term	Mapping and allocation for product term 15
P04.10	Product term	Mapping and allocation for product term 16
P04.11	Product term	Mapping and allocation for product term 17
P04.12	Product term	Mapping and allocation for product term 18
P04.13	Product term	Mapping and allocation for product term 19
P04.14	Product term	Mapping and allocation for product term 20
P04.15	Product term	Mapping and allocation for product term 21
P04.16	Product term	Mapping and allocation for product term 22
P04.17	Product term	Mapping and allocation for product term 23
P04.18	Product term	Mapping and allocation for product term 24
P04.19	Product term	Mapping and allocation for product term 25
P04.1A	Product term	Mapping and allocation for product term 26
P04.1B	Product term	Mapping and allocation for product term 27
P04.1C	Product term	Mapping and allocation for product term 28
P04.1D	Product term	Mapping and allocation for product term 29
P04.1E	Product term	Mapping and allocation for product term 30
P04.1F	Product term	Mapping and allocation for product term 31
P05.00	Function selection DOUT40	Output mapping for LOUT64 (DOUT40)
P05.01	Function selection DOUT41	Output mapping for LOUT65 (DOUT41)

Mapping		
No.	**Name**	**Description**
P05.02	Function selection DOUT42	Output mapping for LOUT66 (DOUT42)
P05.03	Function select, acknowledgement contact C1/C2	Output mapping for LOUT67 (signal relay)
Expert parameter		
P04.20	Status LIN0..LIN31	Actual values of LIN0..LIN31
P04.21	Status LIN32..LIN63	Actual values of LIN32..LIN63
P04.22	Status LIN64..LIN95	Actual values of LIN64..LIN95
P04.23	Status LIN96..LIN127	Actual values of LIN96..LIN127
P04.24	Status VIN0..VIN31	Actual values of VIN0..VIN31
P04.25	Status VIN32..VIN63	Actual values of VIN32..VIN63
P05.04	Function selection, brake output of basic unit	Output mapping for LOUT68 (holding brake of the basic unit)

Table 159: Mapping

Internal/hidden parameters		
No.	**Name**	**Description**
P06.14	Resolver, phase offset	Phase offset between pulse-width modulation toggling and sensing
P06.20	Single turn resolution in bits	Number of bits per angle value
P06.21	Number of measurable revolutions (Multiturn)	Number of measurable revolutions (Multiturn)
P06.22	Serial number of the EnDat encoder (Part 1)	Serial number of the EnDat encoder (Part 1)
P06.23	Serial number of the EnDat encoder (Part 2)	Serial number of the EnDat encoder (Part 2)
P06.24	Serial number of the EnDat encoder (Part 3)	Serial number of the EnDat encoder (Part 3)
P06.25	Ident. number of the EnDat encoder (Part 1)	Ident. number of the EnDat encoder (Part 1)
P06.26	Ident. number of the EnDat encoder (Part 2)	Ident. number of the EnDat encoder (Part 2)
P06.27	Ident. number of the EnDat encoder (Part 3)	Ident. number of the EnDat encoder (Part 3)
P06.38	Allowable time for incorrectly sent angle data	Maximum time for which the basic unit angle can be sent incorrectly.
P09.00	Filter for common message SFR or SSR	Mask, in order to exclude individual safety functions from the calculation of the common message
P09.01	Time between two Sync pulses (basic cycle)	Time between two Sync pulses (basic cycle)
P12.01	Switch-on delay	Time delay in case of a switch-on delay
P12.02	Switch-off delay	Time delay in case of a switch-off delay
P12.04	Switch-on delay	Time delay in case of a switch-on delay
P12.05	Switch-off delay	Time delay in case of a switch-off delay
P12.07	Switch-on delay	Time delay in case of a switch-on delay
P12.08	Switch-off delay	Time delay in case of a switch-off delay
P12.0A	Switch-on delay	Time delay in case of a switch-on delay
P12.0B	Switch-off delay	Time delay in case of a switch-off delay
P12.0D	Switch-on delay	Time delay in case of a switch-on delay
P12.0E	Switch-off delay	Time delay in case of a switch-off delay
P12.10	Switch-on delay	Time delay in case of a switch-on delay
P12.11	Switch-off delay	Time delay in case of a switch-off delay
P12.13	Switch-on delay	Time delay in case of a switch-on delay

Internal/hidden parameters		
No.	**Name**	**Description**
P12.14	Switch-off delay	Time delay in case of a switch-off delay
P12.16	Switch-on delay	Time delay in case of a switch-on delay
P12.17	Switch-off delay	Time delay in case of a switch-off delay
P1C.00	Software revision (main revision)	Software revision (main revision)
P1C.01	Software revision (application number)	Software revision (application number)
P1C.02	Software revision (KM / subrevision)	Software revision (KM / subrevision)
P20.06	[53-6] SDI0: Safety Condition Violated	Error response of the error 53-6
P20.07	[53-7] SDI1: Safety Condition Violated	Error response of the error 53-7
P20.08	[53-8] SLI0: Safety Condition Violated	Error response of the error 53-8
P20.09	[53-9] SLI1: Safety Condition Violated	Error response of the error 53-9
P20.0B	[54-1] SBT: Safety Condition Violated	Error response of the error 54-1
P20.2B	[57-3] Error, analogue input (value range)	Error response of the error 57-3
P20.2C	[57-4] Error in the current measurement	Error response of the error 57-4
P20.2D	[57-5] Error, motor voltage measurement	Error response of the error 57-5
P20.4A	Log safety function request	If set: Log safety function request
PFF.00	Operating status:	Current status of the parameterisation session
PFF.01	Identification "Delivery status" 1 = YES	Identification "Delivery status"
PFF.02	Identification "Complete validation" 1 = YES	Identification "Complete validation"
Expert parameter		
PFF.03	Validation code:	Validation code of the parameterisation session

Table 160: Internal/hidden parameters

9 Glossary

9.1 Safety terms and abbreviations

Term/abbreviation	Description
ALF	"Additional Logic Function". Not a safety function. Allows the logical interconnection of internal inputs and outputs.
Cat.	Category in accordance with EN ISO 13849-1, Stages 1 ... 4.
CCF	Common Cause Failure in accordance with EN ISO 13849-1.
DC avg	Average Diagnostic Coverage in accordance with IEC 61508 and EN 61800-5-2.
Emergency off	In accordance with EN 60204-5-1 Electrical safety is ensured in case of emergency by switching off the electrical energy to all or part of the installation. Emergency off is to be used where a risk of electric shock or other electrical risk exists.
Emergency stop	In accordance with EN 60204-5-1 Functional safety is ensured in an emergency by bringing a machine or moving parts to idle. Emergency stop is used to stop a movement which could lead to a hazard.
HFT	Hardware Fault Tolerance in accordance with IEC 61508.
MSC	Metronix ServoCommander®, software for configuration and commissioning.
MTTFd	Mean Time To Failure (dangerous): Time in years until the first dangerous failure will have occurred with 100% probability, in accordance with EN ISO 13849-1.
OSSD	"Output Signal Switching Device": Output signals with 24 V level cycle rates for error detection.
PFD	Probability of Failure on Demand in accordance with IEC 61508.
PFH	Probability of Dangerous Failures per Hour in accordance with IEC 61508.
PL	Performance Level in accordance with EN ISO 13849-1: Stages a ... e.
Safety switching device	Device for execution of safety functions or achievement of a safe status of the machine by switching off the energy supply to dangerous machine functions. The desired safety function is achieved only in combination with other measures for risk reduction.
SBC	Safe Brake Control in accordance with EN 61800-5-2.
SFF	Safe Failure Fraction [%], ratio of the failure rates of safe and dangerous (but recognisable) failures to the sum of all failures in accordance with IEC 61508.
SIL	Safety Integrity Level, discrete stages for defining the requirements for the safety integrity of safety functions in accordance with IEC 61508, EN 62061 and EN ISO 13849.
SILCL	Maximum SIL that can be required from a sub-system.
SLS	Safely-Limited Speed in accordance with EN 61800-5-2.

Term/abbreviation	Description
SOS	Safe Operating Stop in accordance with EN 61800-5-2.
SS1	Safe Stop 1 in accordance with EN 61800-5-2.
SS2	Safe Stop 2 in accordance with EN 61800-5-2.
SSF	"Safe Speed Function", combined safety functions for speed monitoring and control.
SSM	Safe Speed Monitor in accordance with EN 61800-5-2.
SSR	Safe Speed Range in accordance with EN 61800-5-2.
STO	Safe Torque Off in accordance with EN 61800-5-2.
T	Duration of use in accordance with EN ISO 13849-1.
USF	"Universal Safety Function", combined safety functions.

Table 161: Terms and abbreviations

9.2 Terms for the SafetyTool and for safe parameterisation

Term	**Meaning/function**
Actual value	The current value of a parameter in the safety module, converted to the desired display unit
Basic unit	Servo drive as the carrier of the safety module, here an ARS 2000 FS.
Check sum	Measure for guaranteeing the integrity of data which is sent or stored. In so doing, check sums are generated from the data, which guarantee data parity sufficient under normal circumstances.
Communication object	Individual data element, which can be read, written to and validated by the SafetyTool.
Display unit	Unit in which the appropriate parameters are displayed. The desired display units for position values, speed values and acceleration values are specified by the executing program when the SafetyTool is started.
Display value	The value of a parameter converted to the desired display unit.
Offline parameterisation	Operation of the SafetyTool, without a connection to the device (on the desk)
Online parameterisation	Operation of the SafetyTool, with a connection to the device (via the basic unit).
Product term	In order to configure switching conditions of the safety module, logic operations between the logical inputs and the virtual outputs and between the virtual outputs and the logical outputs are configured in the form of so-called product terms. A product term is an AND operation with or without inversion with a maximum of 7 inputs. Maximum of 4 product terms can be combined as an OR operation. The product terms (AND operation) and OR operations are generally termed gates.
Project	See SafetyTool project.
Quantisation	Some parameters are quantised (rasterised) by the safety module, e.g. if the value must be a multiple of a cycle time. In such cases, when reading out the safety module, a value can be fed back which is different than the written value. However, the specified quantising ranges do not create any relevant deviations.
Quantisation area	Tolerance between the written value and the read value of a parameter. Values within the quantisation limit can be viewed as identical. The quantisation limit is read from the safety module during writing parameter access.
Reference value	The display value of a parameter specified by the user.
Safe basic status	If the parameterisation is missing, invalid or not fully validated, the safety module switches to the safe basic status: – output stage switched off – clamping unit or holding brake closed – DOUT4x outputs switched off at safety module

Term	Meaning/function
Safe parameter set	The sum of all the parameters of the safety module forms a parameter set. If this parameter set contains a valid validation code, then it is a "safe parameter set". The safe parameter set of an application is thus always located in a safety module ready for operation. In addition, it can be read out with the SafetyTool and stored, including the validation code generated by the safety module. On the storage medium, it is protected against changes with a checksum.
Safety module	FSM 2.0 – MOV as a plug-in module in the basic device, which is responsible for the safety of the drive application. The parameterisation of this safety module takes place with the SafetyTool.
SafetyTool project	The SafetyTool allows the user to save the locally-available parameterisation as a "SafetyTool project". This file contains the parameters as a display value (in contrast to the safe parameter set to which device values are saved). The SafetyTool project can be sent to the safety module in an online session. The user must validate the sent parameters individually.
SCV	Safety Condition Violated.
SFR	Safety Function Requested.
SSR	Safe State Reached.
Validation code	Content of a special communication object generated by the safety module, when all the parameters have been validated.

Table 162: Terms for the SafetyTool and for safe parameterisation