OCTOGON

MANUAL

ESMD

PROGRAMMABLE SAFETY CONTROLLER SIL3 / PL e

Installation manual



Document	Version	Date	Applies to
Installation manual	V00x	10/2026	ESMD, versions 10 / 20 / 30, with expansion and communication modules

This installation manual describes safety, device types, safety related characteristics, connection and installation, response times, start-up, safety related examination and maintenance of the ESMD programmable safety controller and its expansion and communication modules.

octogon GmbH · Roseggerstrasse 16 · 8700 Leoben · Austria · office@octogon.org

Contents

1 Important notes ... 3
1.1 Definitions ... 3
1.2 Co-valid documents ... 4
1.3 Abbreviations used ... 4
1.4 Device ... 5
2 Safety regulations ... 6
2.1 Intended use ... 6
2.2 Use in regions with UL/CSA requirements ... 6
2.3 General safety regulations ... 7
2.4 Operation and service ... 7
2.5 Transport/storage ... 7
3 Device types ... 8
3.1 Module overview ... 8
3.2 Device characteristics ... 8
3.2.1 Basic modules ... 8
3.2.2 Central expansion modules ... 10
3.2.3 Communication interface ... 11
3.3 Identification ... 12
3.3.1 Type plate / product label ... 12
3.3.2 Scope of delivery ... 12
4 Safety related characteristics ... 14
4.1 General design, safety related architecture and characteristics ... 14
4.2 Safety related characteristics and wiring for the connected sensors ... 15
4.2.1 Digital sensors ... 15
4.2.2 Analog sensors ... 23
4.3 Safety related characteristics and output wiring ... 25
4.3.1 Characteristics of output elements ... 25
4.3.2 Diagnoses in cut-off circuit ... 26
4.3.3 Permissible capacitive and inductive load at safe outputs ... 27
4.3.4 Digital outputs ... 28
4.3.5 Digital outputs I/Os (EAAx) ... 30
5 Connection and installation ... 38
5.1 General notes on installation ... 38
5.2 Installation and assembly of the module ... 38
5.3 Installation of backplane bus system ... 38
5.4 Assembling the modules ... 39
5.4.1 Assembly on C-rail ... 39
5.4.2 Assembly on backplane bus ... 40
5.4.3 I/O-extension installation ... 41
5.5 Terminal assignment ... 42
5.5.1 Terminal assignment ESMD ... 42
5.5.2 Terminal assignment expansion module ... 43
5.5.3 Terminal assignment communication modules ... 43
5.6 External 24 VDC – voltage supply ... 43
5.7 Connection of digital inputs ... 44
5.8 Connection of analog inputs ... 45
6 Response times of the ESMD ... 46
6.1 Response times in standard operation ... 46
6.2 Response time for FAST_CHANNEL ... 47
6.3 Response times for fault distance monitoring ... 47
6.4 Response times when using the expansion module ... 48
7 Start-up ... 50
7.1 Procedure ... 50
7.2 Start-up sequences ... 50
7.3 Reset-function ... 50
7.3.1 Types of reset functions ... 50
7.3.2 Reset timing ... 50
7.3.3 Reset function ... 51
7.4 LED display ... 53
7.5 Parameterization ... 53
7.6 Function test ... 53

7.7 Validation ... 54
8 Safety related examination ... 55
9 Maintenance ... 55
9.1 Modification / handling changes to the device ... 55
9.2 Exchanging a module ... 55
9.3 Maintenance intervals ... 55
10 Technical data ... 56
10.1 Environmental conditions ... 56
10.2 Safety related characteristics ... 56
10.3 Dimensions ... 56
10.4 Connection example ... 57
11 Switch types ... 58
12 Notes on designing, programming, validating and testing safety related applications ... 64
12.1 Risk assessment ... 64
12.2 Required technical documents ... 65
12.3 Necessary steps for draft, realization and testing ... 66
12.3.1 Phases of the V-model ... 67
12.3.2 Specification of safety requirements (structural schematic) ... 67
12.3.3 Specification of the functional safety system ... 71
12.3.4 Software specification ... 73
12.3.5 Hardware specification ... 74
12.3.6 Hard and software design ... 76
12.3.7 Testing of the hardware design ... 76
12.3.8 Verification software (program) and parameters ... 78
12.3.9 Performance of the system test / FIT (fault injection test) ... 81
Appendix A Classification of switch types ... 82

1 Important notes

Validity

Installation manual for the devices ESMD, ESMD version 20 (FSoE) and ESMD version 30 (PROFIsafe) of the ESMD series and their extension modules (expansion module, communication modules).

Versions 20 and 30 are options for ESMD:

- Version 20: Standard-fieldbus and safety-protocol FSoE
- Version 30: Standard-fieldbus and safety-protocol PROFISAFE

Note The German version is the original version of the installation manual.

Valid from FW release 2.0.2.46. Subject to change without prior notification.

Definition of individual target groups

Target group	Personnel
Project engineers for safe drive systems	Engineers and technicians
Assembly, electric installation, maintenance and replacement of devices	Maintenance electricians and service technicians
Commissioning, operation and configuration	Technicians and engineers

1.1 Definitions

The designation ESMD is used as generic term for all derivatives from the product range. Wherever this description refers to a certain derivative, the complete designation is used.

The term "safe" used in the following text in any case refers to the classification as a safe function for application up to PL e acc. to EN ISO 13849-1 or SIL3 acc. to IEC 61508.

The system software (programming software) serves the purpose of configuring and programming the modules.

Internally, the modules of the series are composed of two independent processing units. In the following these are referred to as system A and system B.

1.2 Co-valid documents

Description	Reference
Configuration of the module for stand-alone applications without field-bus interfacing with the programming software	Programming manual of the programming software (System CD)
Validation report for implemented parameterization and PLC-program	Safety inspection with acceptance protocol
Acceptance for general safety relevant applications	Certificate for type approval test as safety control acc. to machine guideline 2006/42/EG for the product groups ESMD, ESMD version 20 and 30, expansion module

Note

- Thoroughly read the manuals before you start the installation and the commissioning of the module.
- Paying attention to the documentation is a prerequisite for trouble-free operation and fulfilment of possible warranty claims.

1.3 Abbreviations used

Abbreviation	Meaning
AC	Alternating voltage
AWL	Instruction list
ELIA	Employer's liability insurance association
CLK	Clock (cycle)
CPU	Central Processing Unit
DC	Direct voltage
I1..I14	Digital Input
DIN	Deutsches Institut für Normung (German Institute for Standardization)
DO	Digital Output
EMU	Emergency Monitoring Unit
EMC	Electromagnetic compatibility
ELC	Emergency Limit Control
EN	European Standard
HISIDE	Output with 24 VDC nominal level switching to plus
IP20	Protection type for housing
ISO	International Organisation for Standardisation
LED	Light Emitting Diode
LOSIDE	Output switching to reference potential
OLC	Operational Limit Control
PIA	Process image of outputs
PII	Process image of inputs
SMMC	Safe Master-Master Communication
P1, P2	Pulse outputs
PLC	Programmable Logic Controller
POR	Power on Reset
PSC	Position Supervision Control
SELV	Safety Extra Low Voltage
SSI	Synchronous Serial Interface
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik e. V. (association for electrical engineering, electronics and information technology)
SDDC	Safe Device-Device Communication
DOx.y (1)	Auxiliary Output
G. P.	General purpose (general use)
(1)	Module address x = 0 ... 2, Channel address y = 1 ... 40

1.4 Device

Feature	Version
Design	Programmable safety controller SIL3 / PL e (base device), for DIN rail, IP20
Versions	10 standard · 20 with FSoE, ETHERCAT integrated · 30 with PROFISAFE, PROFINET integrated
Accessories	Expansion module (I/O); communication modules CAN, Profibus-DP, Profinet, CANopen, EtherCAT; programming software; programming unit; backplane bus connectors (standard and circuit breaker design)
Manufacturer type	SCU-DR

2 Safety regulations

2.1 Intended use

Devices of the ESMD are programmable fail-safe control system intended for the establishment of emergency shut-down features and functions. The devices are intended for use in

- EMERGENCY STOP facilities,
- as safety component as defined by the EC machine directive 2006/42/EG,
- as PES for risk reduction as defined by IEC 61508,
- in safety circuits acc. to EN 60204-1 u. EN 60204-32,
- as PES for functional safety as defined by EN 62061,
- as SRP/CS as defined by EN ISO 13849-1,
- as device for establishing the safety functions acc. to EN 61800-5-2,
- as logic unit for converting and processing signals in two-hand control acc. to EN 574.

The devices of series ESMD including expansion module are safety components as specified in appendix IV of the EC machine directive 2006/42/EC. They were developed, designed and manufactured in compliance with the above mentioned directive as well as the EU-directive EU-EMC directive 2014/30/EU.

2.2 Use in regions with UL/CSA requirements

In case of modules of the series which do not have UL/CSA approval, these modules can be used in USA and Canada under the following conditions:

- switching voltage of the output relays must be limited to max. 24 V.
- a power supply unit meeting the requirement SELV/PELV must be used for supplying electric power to the modules and their inputs and outputs.

Under these prerequisites no UL/CSA approval is required and the series can be used in switchgear in accordance with IEC 61010.

2.3 General safety regulations

Safety note

- In order to avoid damage to persons and property only qualified personnel is entitled to work on the device. The term qualified personnel refers to persons who have successfully completed electrotechnical training and are fully familiar with the applicable rules and standards of electrical engineering.
- The qualified person must become familiar with the operating instructions (see IEC 364, DIN VDE 0100).
- The qualified person must have profound knowledge of the national accident prevention regulations.
- The use of the device must be strictly limited to the intended use as specified in the following list. The values of data listed under section 3.2 Device characteristics must also be observed.
- The contents of this installation manual is restricted to the basic function of the device or its installation. The programming manual of the programming software contains a more detailed description of the programming and re-parameterization of the devices. Exact knowledge and understanding of these instructions is mandatory for a new installation or modification of device functions or device parameters.
- Commissioning (i.e. starting up the intended operation) is only permitted in strict compliance with the EMC-directive. The EMC-testing regulations EN 55011:2009 + A2:2010 and EN 61000-6-2:2005 are used as basis.
- Compliance with the conditions acc. to IEC 60068-2-6 related to the values specified under Technical characteristics is mandatory for storage and transport.
- The wiring and connecting instructions in chapter 5 Connection and installation must be followed strictly.
- The applicable VDE-regulations and other special safety regulations of relevance for the application must be strictly followed.
- Evidence of the configured monitoring functions as well as their parameters and links must be issued by means of a validation report.
- The implementation of the module must be coordinated with the demands of the responsible acceptance testing authority (e.g. TÜV or ELIA).
- Do not install or operate damaged products. Report damages immediately to the responsible forwarding agent.
- Never open the housing and/or make unauthorized conversions.
- Inputs and outputs for standard functions or digital and analog data transmitted via communication modules must not be used for safety relevant applications.

WARNING **Using our devices contrary to the rules and conditions specified hereunder can lead to injuries or fatalities as well as damage to connected devices and machines!**

This will also cause the loss of all warranty and compensation claims against the manufacturer.

2.4 Operation and service

The module must always be de-energized before installation and removal, or before disconnecting signal lines. For this purpose all live supply lines to the device must be checked for safe isolation from supply.

When installing or removing the module appropriate measures must be applied to prevent electrostatic discharge to the externally arranged terminal and plug connections. Contact with such terminals should be reduced to a minimum and earthing by means of e.g. an earthing strap should take place before and during these procedures.

2.5 Transport/storage

Information concerning transport, storage and proper handling must be strictly followed. The climate related specifications in chapter 10 Technical data must be complied with.

3 Device types

The ESMD series consists of:

- Basic devices ESMD
- Extension modules
- communication modules with standard field bus
- Programming unit
- integrated communication modules with safe field bus ESMD version 20 and 30

Basic devices

Series ESMD is a compact fail-safe control system. The device is freely programmable for safe processing of EMERGENCY OFF buttons, two-handed controls, light barriers, operating mode selection switches etc. as well as drive-related safety functions. Pre-configured modules for safety relevant signal pre-processing are available for a vast number of input devices. The same applies for safety functions serving the purpose of drive monitoring. Detailed information can be found in the programming manual.

The basic version of the device has 14 safe inputs and up to 5 safe cut-off channels.

Extension modules

Central or decentralised I/O expansion modules for the ESMD series. A maximum of 2 expansion modules can be used.

Communication modules and integrated interface

The communication interface has a bi-directional data transfer from and to a subordinate control via standard field bus or secure standard field bus.

3.1 Module overview

Description	Basic unit ESMD	Expansion module	Communication module
Max. no. of expansion modules	2*	–	–
Safe digital inputs	14	12	–
Safe digital I/O	–	10	–
Safe analog inputs	2	–	–
Relay outputs	6	–	–
Auxiliary outputs	2	–	–
Pulse outputs	2	–	–
Integrated communication interface	Optional (version 30 and 20): Profinet-PROFIsafe, FSoE	–	–
Extended communication interface	Optional (communication module): CAN 2.0, Profibus, Profinet, CANopen, EtherCAT	–	CAN 2.0, Profibus, Profinet, CANopen, EtherCAT
Technical data	See technical characteristics of the respective module		

3.2 Device characteristics

3.2.1 Basic modules

ESMD

Design of module with the following periphery:

Number	Periphery
14	Digital inputs
2	Pulse outputs
6	Relay outputs
2	Auxiliary outputs
2	Analog inputs
1	diagnostic- and configuration interface
1	function button
1	7-segment display
1	status-LED
14	status LEDs for inputs
2	status-LEDs for pulse outputs
2	status-LEDs for relay outputs
6	status LEDs for outputs
1	Optional: Communication interface (communication module)

Module characteristics:

- Extendable to: max. 38 safe digital inputs + max. 2 safe digital outputs; max. 20 safe digital I/Os; max. 12 safe relay outputs + max. 6 auxiliary outputs
- Logic processing up to PL e acc. to EN ISO 13849-1 or SIL 3 acc. to IEC 61508
- Freely programmable modular controller for up to 800 IL instructions
- Logic diagram oriented programming
- Pulse outputs for cross-shorting detection of digital input signals
- External contact monitoring of connected switchgear (EMU)
- Monitored relay outputs for safety relevant functions
- Parameter management for expansion modules in base device
- Speed- and position-related safety functions for drive monitoring are integrated into the firmware, as per IEC 61800-5-2; spatial functions for safe speed- and area-monitoring are possible
- Comprehensive diagnostics functions integrated
- Coded status display via front-side 7 segment display and status LEDs
- Multifunction buttons (quit, start, reset) can be operated from the front side
- CAN communication in connection with the communication module for diagnostics via rear wall bus; assembly on profile rail (see communication module)
- Assembly on top hat rail

Technical characteristics: ESMD

Item	Value
Safety related characteristics	
PL acc. to EN ISO 13849-1	PL e
PFH / architecture	12,6 FIT / Kat 4; plus 1-channel per Rel 20 FIT (max. 4), 2-channel per Rel 1,0 FIT (max. 2)
SIL as per IEC 61508	SIL 3
Proof test interval	20 years = max. operating period
General data	
Max. no. of expansion modules	2
Interface for expansion modules	T-bus connector, pluggable in top-hat rail
Number of safe digital inputs	14 (OSSD capable)
Number of relay outputs	6
Number of safe analog inputs	2
Number of auxiliary outputs	2
Number of pulse outputs (clock outputs)	2
Type of connection	Plug-in terminals with spring or screw connection
Electrical data	
Supply voltage (tolerance)	24 VDC; 2 A (–15 %, +20 %)
Fuse X11.1	min. 30 VDC; max. 3,15 A
Max. power consumption (logic)	2,4 W
Digital input ratings	24 VDC; 20 mA, Typ1 as per EN 61131-2

Item	Value
Digital output ratings – auxiliary outputs	24 VDC; 250 mA
Pulse outputs (clock outputs)	24 VDC; 250 mA
Relay ratings – normally open	DC13: 24 VDC; 2 A · AC15: 230 VAC; 2 A
Relay ratings – normally closed (read back contact)	DC13: 24 VDC; 2 A
Analog input ratings	ESMD: 4 ... 20 mA
Environmental data	
Temperature	0 °C ... +50 °C operation; –25 °C ... +70 °C storage and transport
Class of protection	IP 20
Climatic category	3k3 acc. to DIN 60 721-3
Min-, maximum relative humidity (no condensation)	5 % – 85 %
EMC	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Operating altitude	2000 m
Overvoltage category	III
Degree of pollution	2
Mechanical data	
Dimensions (H × D × W [mm])	ESMD = 100 × 115 × 90; ESMD version 20/30 = 100 × 115 × 115
Weight (g)	ESMD = 500; ESMD version 20/30 = 600
Mounting	To snap on top-hat rail
Number of T-bus	ESMD: 4; ESMD version 20 and 30: 5
Min. terminal cross-section / AWG	0,2 mm^2 / 24
Max. terminal cross-section / AWG	2,5 mm^2 / 12

3.2.2 Central expansion modules

Expansion module

Design of module with the following periphery:

Number	Periphery
12	Digital inputs
10	Digital I/Os
2	Pulse outputs
2	Auxiliary outputs
12	status LEDs for inputs
10	Status-LEDs for I/O

Module characteristics:

- Pulse outputs for cross-shorting detection of digital input signals
- External contact monitoring of connected switchgear (EMU)
- Comprehensive diagnostics functions integrated
- Assembly on top hat rail
- Expansion module – with a total of 10 I/Os

Technical characteristics: expansion module

Item	Value
Safety related characteristics	
PL as per EN ISO 13849-1	PL e
PFH / architecture	9,2 FIT / Kat 4 1)
SIL as per IEC 61508	SIL 3
Proof test interval	20 years = max. operating period
MTTFd	213 years
General data	
Max. no. of expansion modules	–
Interface for expansion modules	T-bus connector, pluggable in top-hat rail
Number of safe digital inputs	12 (OSSD capable)
Number of safe digital outputs	–
Number of safe digital I/O	10

Item	Value
Number of safe analog inputs	–
Number of auxiliary outputs	2
Number of pulse outputs (clock outputs)	2
Type of connection	Plug-in terminals with spring or screw connection
Electrical data	
Fuse X11.1	min. 30 VDC; max. 3,15 A
Max. power consumption (logic)	2,4 W
Digital input ratings	24 VDC; 20 mA, Typ1 as per EN 61131-2
Digital output ratings – auxiliary outputs	24 VDC; 250 mA
Digital output ratings – pulse outputs (clock outputs)	24 VDC; 250 mA
Digital output ratings – digital I/O	24 VDC; 250 mA
Relay ratings – normally open	DC13: 24 VDC; 2 A · AC15: 230 VAC; 2 A
Relay ratings – normally closed (read back contact)	DC13: 24 VDC; 2 A
Analog input ratings	–
Environmental data	
Temperature	0 °C ... +50 °C operation; –25 °C ... +70 °C storage and transport
Class of protection	IP 20
Climatic category	3k3 acc. to DIN 60 721-3
Min-, maximum relative humidity (no condensation)	5 % – 85 %
EMC	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Operating altitude	2000 m
Overvoltage category	III
Degree of pollution	2
Mechanical data	
Dimensions (H × D × W [mm])	100 × 115 × 45
Weight (g)	300
Mounting	To snap on top-hat rail
Number of T-bus	2
Min. terminal cross-section / AWG	0,2 mm² / 24
Max. terminal cross-section / AWG	2,5 mm² / 12

1) Value applies only for extension module. For a total assessment in accordance with EN ISO 13849-1 one must use a series connection with the corresponding basic device => PFH logic = PFH basic + PFH extension

3.2.3 Communication interface

3.2.3.1 Communication modules (standard field bus)

Design of module with the following periphery:

- 1 field bus interface: communication module CAN 2.0 or Profibus or Profinet or CANopen or EtherCAT
- 1 backplane bus interface
- 1 status LED for operating status
- 1 status LED CAN-communication

Module characteristics:

- Communication modules CAN or PROFIBUS or PROFINET or CANopen or EtherCAT or DeviceNet
- 2 × 8 Byte PAA with free allocation
- 32 Bit PAE
- You can take detailed information from the installation manuals of the respective field bus modules.

Technical characteristics: communication module

Item	Value
Safety related characteristics	
PL as per EN ISO 13849-1	n. a.
PFH / architecture	n. a.
SIL as per IEC 61508	n. a.
Proof test interval	n. a.

Item	Value
General data	
Field bus interface	1
Type of connection	Standard acc. to field bus type
Max. size PIA	2 × 64 Bit
Max. size PII	32 Bit
Typ. update time for data	16 ms
Electrical data	
Power consumption	Max. 0,5 W
Field bus ratings	Standard acc. to field bus type
Environmental data	
Temperature	0 °C ... +50 °C operation; –25 °C ... +70 °C storage and transport
Class of protection	IP 20
Climatic category	3k3 acc. to DIN 60 721-3
Min-, maximum relative humidity (no condensation)	5 % – 85 %
EMC	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Operating altitude	2000 m
Overvoltage category	III
Degree of pollution	2
Mechanical data	
Dimensions (H × D × W [mm])	100 × 115 × 22,5
Weight (g)	110
Mounting	To snap on top-hat rail

3.2.3.2 ESMD version 20 / 30 (integrated safe field bus)

Designs of the module with following peripherals:

- 1 field bus interface: ESMD version 30 PROFISAFE over Profinet or ESMD version 20 FSoE FailSafe over EtherCAT
- 1 status LED for operating status
- 1 status LED internal SPI communication
- 1 status LED field bus

Module characteristics:

- Communication modules PROFISAFE over PROFINET or FSoE FailSafe over EtherCAT
- You can take detailed information from the installation manuals of the respective field bus modules.

Note **This must be specified when ordering a base module!**

3.3 Identification

The type plate is located on the left side wall of the module and contains the following information:

3.3.1 Type plate / product label

- Type designation
- Part number
- Serial number
- Identification of hardware release
- Identification of software release
- Safety category
- Input characteristics
- Output characteristics
- Date of manufacture (week/year)

3.3.2 Scope of delivery

Scope of delivery contains:

- Module: Plug for all signal terminals without sensory supply

Not included in the scope of delivery:

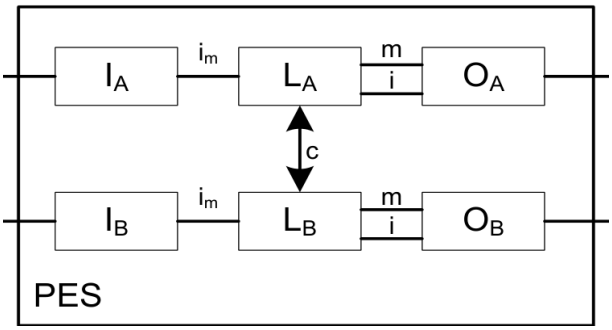
- Configuration software CD of the programming software with installation manual, programming manual and driver for programming adapter
- Programming adapter (programming unit)
- License key (USB-Dongle) for the programming software
- System CD with manuals
- Backplane bus plug (expansion module and use of communication interfaces)

4 Safety related characteristics

4.1 General design, safety related architecture and characteristics

The inner structure of the series consist of two separate channels with reciprocal comparison of results. High quality diagnoses for fault detection are made in each of the two channels.

With respect to architecture and function the internal structure corresponds with category 4 of EN 13849-1.



Internal structure (PES)

The overall architecture therefore corresponds with the following structure:



Dual reading of each input and diagnose by cross-comparison

The specific safety related characteristic data of the corresponding module can be taken from the technical characteristic data in chapter 3.

The characteristic data specified in chapter 3 (e.g. PL e and PFH-value acc. to table as evidence acc. to EN 13849) for the partial system PES can be used for the safety related assessment of the overall system.

Characteristics

Characteristic	Value
Max. obtainable safety class	SIL 3 acc. to IEC 61508; Category 4 acc. to EN ISO 13849-1; Performance-Level e as per EN ISO 13849-1
System structure	System structure 2-channel with diagnose (1oo2) acc. to IEC 61508; Architecture category 4 acc. to EN 13849
Rating of operating mode	"high demand" acc. to IEC 61508 (high demand rate)
Probability of an endangering failure per hour (PFH-value); specific values acc. to table "safety-technical characteristics"	Expansion module: PFH = 9,2 FIT; ESMD (1-channel): PFH = 20 FIT; ESMD (2-channel): PFH = 1,0 FIT
Proof-Test-Interval (IEC 61508)	20 years, after this time the module must be replaced

Safety note

- The specific safety related characteristic data of the corresponding module can be taken from the technical characteristic data in chapter 3.
- When using several sensors with different functions (e.g. position indicator access door + speed detection) for a safety function (e.g. safe reduced speed when access door is open), these must be assumed as being connected in series for the safety related assessment of the overall system. See also exemplary calculation in section 12.3.7.
- The safety regulations and EMC-directives must be strictly followed.
- Concerning the applicable fault exclusions please refer to the tables under D in the appendix of EN ISO 13849-2.
- The characteristic data specified in chapter 3 for the partial system PES (e.g. PL e and PFH-value acc. to table as evidence acc. to EN ISO 13849-1) can be used for the safety related assessment of the overall system.

The following examples and their characteristic architecture are mainly responsible for the assignment to a category acc. to EN ISO 13849-1.

The maximum possible Performance Levels acc. to EN ISO 13849-1 resulting from this still depend on the following factors of the external components:

- Structure (simple or redundant)
- Detection of common cause faults (CCF)
- Degree of diagnostic coverage on request (DCavg)
- Mean time to dangerous failure of a channel (MTTFd)

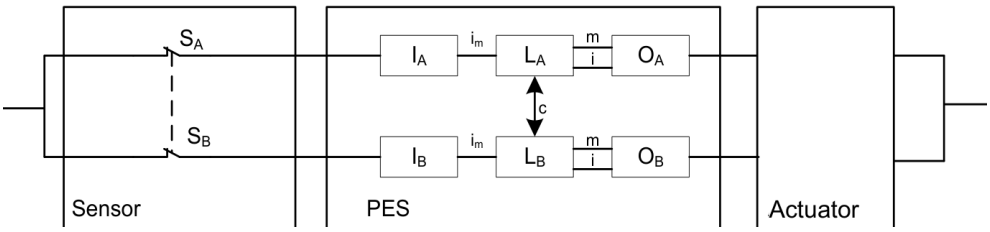
4.2 Safety related characteristics and wiring for the connected sensors

The modules have completely separated signal processing paths for each safety input. This applies for both the digital and the analog inputs. Furthermore, measures for achieving the highest possible DC-values have been implemented.

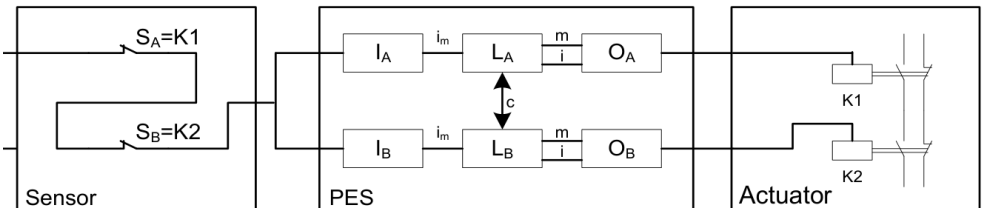
4.2.1 Digital sensors

Digital inputs and outputs are generally of a completely redundant design, except the electro-magnetic input terminal. The following list contains details for classification, the DC and the achievable PL or SIL.

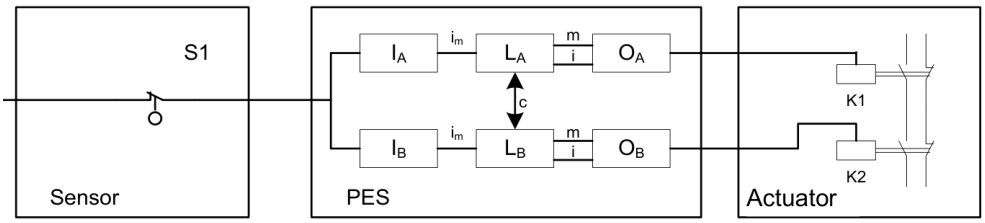
4.2.1.1 Characteristics of sensors / input elements



Two-channel input element in parallel connection (Cat. fault tolerance 1) with high DC caused by signal in two channels and diagnose by means of cross-comparison in the PES



Two-channel input element in series connection (Cat. 4, fault tolerance 1) with low to medium DC caused by signal processing in two channels and diagnose by means of cyclic testing



Single channel input element and dual channel processing with low to medium DC by signal processing in two channels and diagnose by means of cyclic testing, PL / SIL depending on permissible fault exclusions and test rate for input element.

4.2.1.2 DC digital sensors/inputs

The modules ensure far reaching diagnostics functions for the input element. These are carried out permanently, or optionally (cross-shorting monitoring by means of pulse identifier, cross-comparison, 2- or multi-channel sensor with/without time-out, start-up test).

Permanently active diagnostics functions:

Cross-comparison: Module inputs are in general internally designed with two channels. The status of input signals is permanently compared crosswise. Only with High signals in both partial input systems the input is considered a High input, should the signal level deviate between both channels, the input is set to Low state.

Dynamic test of the partial input system switching threshold: The switching thresholds for detecting the High level are tested cyclically with a high cycle rate. Falling below the defined threshold value a module triggers a module alarm.

Dynamic test of the input system's switchability: The switchability of the input system to Low level is tested for all inputs with a high rate, except DI05 ... DI08. Falling below the defined threshold value a module triggers a module alarm.

Diagnostics functions to be activated by parameterization:

Cross-shorting test: The modules have pulse signal outputs, identified by an unambiguous signature. When performing the cross-shorting test the switching elements of the digital sensors / input elements are supplied with auxiliary voltage by the module via the pulse signal outputs. The signature is thus stamped on the High signal level of the sensors / input elements and checked by the module. With the signature test short-circuits and cross-shorting to High signals can be recognized. With alternating use of the pulse signals of multi-contacts, parallel signal lines or adjacent terminal assignment, cross-shorting between the respective input elements is detected.

Sensors / input elements with 2- or multi-pole contacts without time-out: Several contacts can be assigned to the sensors / input elements. These are therefore compatible with at least 2-channel elements. A High level of the sensor/input element requires a logic series connection of both contacts.

Example 1: Input element with 2 normally closed contacts: High level when both contacts are closed.

Example 2: Input element with 1 normally closed and 1 normally open contact: High level when normally open contact is actuated and normally closed contact is not actuated.

Sensors / input elements with 2- or multi-pole contacts with time-out: Same test as before, but additional monitoring of the input signals for compliance with the defined level connections within a time window of 0.5 seconds. Defining the levels over a time period of > 0.5 seconds triggers a module alarm.

Start test: Each time the safety module is switched on, the input element must be tested in direction of the Low signal status (defined Safe State), e.g. by actuating the Emergency Stop button or a door lock after the system has been started.

Operational / organizational tests: Apart from the previously mentioned diagnostic measures for the modules, cyclic testing can be performed within the application. These tests can also be used when assessing the DC.

Note Operational/organizational tests can also be used for a combination of hardware inputs and functional inputs (input information transferred via standard field bus). However, an exclusive use of functional inputs is ruled out in this context (combination of two or more functional inputs).

The modules therefore ensure far reaching diagnostics functions for the partial input system. These are performed permanently or optionally (cross-shorting monitoring by means of pulse identifier).

The following diagnoses for input sensors can generally be used for the safety related assessment of the entire system:

Input element characteristic	Cross-shorting test	With time-out	Start test	Cyclic test during operation	DC	Definition of measure	Note
Single-channel			O	O	>60	Cyclic test pulse by dynamic change of input signals	A sufficiently high test rate must be ensured.
	X				90	Cyclic test pulse by dynamic change of input signals	Only effective if pulse assignment is active
	X		O	O	90-99	Cyclic test pulse by dynamic change of input signals	DC depending on frequency of start / cyclic test; DC = 90 test only in > 4 week intervals; DC = 99 test at least 1 x day / or 100-time request rate

Input element characteristic	Cross-shorting test	With time-out	Start test	Cyclic test during operation	DC	Definition of measure	Note
Dual channel					90	Cross-comparison of input signals with dynamic test, if short-circuits cannot be detected (for multiple inputs/outputs)	For fault exclusion short-circuit up to DC = 99 possible
			O	O	90-99	Cyclic test pulse by dynamic change of input signals	DC depending on frequency of start / cyclic test
	X				99	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).	Only effective if pulse assignment is active
		X			99	Plausibility test, e.g. use of normally open and normally closed contacts = non-equivalent signal comparison of input elements.	Only effective in connection with activated time-out function for input element

Safety note

- The manufacturer's data (MTTFd, FIT-numbers, etc.) must be used for a safety related assessment of the partial system "Sensors".
- The DC-values listed in the table must be used conservatively and compliance with the boundary conditions (see table under „Remarks“) must be ensured.
- According to the applicable standards, fault exclusions are permitted. The boundary conditions mentioned in this context must permanently be met.
- If several sensor systems are required for the correct function of a single safety function, their partial values must be correctly merged by following the chosen method.

4.2.1.3 Classification of digital inputs

Digital inputs DI01 ... DI14

Digital inputs	Achievable performance level	Comment
DI01 ... DI04, DI09 ... DI14	PL e	Suitable for any kind of input elements, with / without pulse, achievable PL depending on the MTTFd of the input element, as well as fault exclusions in the external wiring.
DI05 ... DI08	PL e	Single-channel with pulse: – Mainly High level required (THigh > 100 * TLow) – At least one request/day required by application – Fault detection upon request
	PL d	Single-channel without pulse: – Fault exclusion short-circuit between signals and to VCC – Fault detection upon request
	PL e	Dual channel: – At least one request/day required by application – Fault detection upon request

Digital inputs I/Os (EAEx)

Note The achievable PL for a combination of HW-inputs and functional inputs depends on the chosen operational/organizational tests as well as on the independence of both channels in the system structure. The determination of the PL requires an application related analysis.

Digital inputs	Achievable performance level	Comment
EAEx		Without pulse, single channel static signal -> auxiliary input
	PL e	Without pulse, dual channel static signal – At least one request/day required by application – Fault detection only upon request
	PL d	Without pulse, dual channel static signal – Less than one request/day required by application
	PL e	Single-channel with pulse – Mainly High level required (THigh > 100 * TLow) – At least one request/day required by application – Fault detection only upon request
	PL d	Single-channel with pulse – Less than one request/day
	PL e	Dual channel with pulse1 and pulse2

4.2.1.4 Exemplary connections of digital sensors

Single-channel sensor, without cross-shorting test

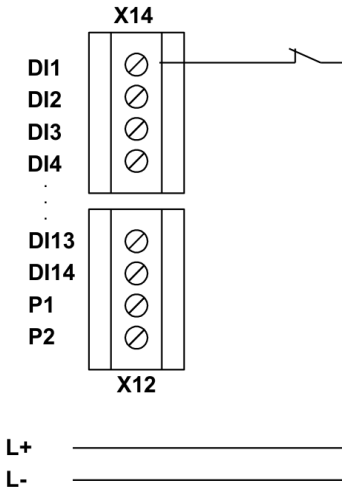


Fig.: Single-channel sensor, without cross-shorting test

The single-channel sensor is connected to the module without pulses or without cross-shorting test. This design is not recommended for safety applications. PL b acc. to EN ISO 13849-1 can maximally be reached.

Single-channel sensor with cross-shorting test

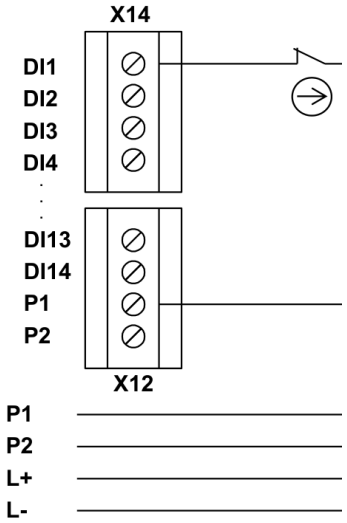


Fig.: Single-channel sensor with cycling

When using a single-channel sensor with pulses, the power supply of the switching element is attached to the pulse outputs P1 or P2. The clock must subsequently be assigned to the module.

The use of a single-channel sensor with pulse detects:

- short-circuit to supply voltage DC 24 V
- short-circuit to DC 0 V
- cable interruption (current interruption is safe state!)

However, be cautious in case of a cable short between the two sensor connections, because this is not detected! A short-circuit between T1 and I01.

Due to the single-channel character of the switching element / sensor its failure requires a fault exclusion. This is permissible when using positively disconnecting switches with correct constrained actuation.

A series connection of 2 switching elements with corresponding fault exclusion of a double fault is on equal footing with the application (occurrence of two errors at the same time). These may be e.g. the safety outputs of an electronic monitoring device (light curtain, switching mat) with internal dual-channel switch-off.

PL d acc. to EN ISO 13849-1 can be achieved by using a suitable switching element and with cautious wiring of the sensor. In special cases, i.e. in connection with suitable switching elements and permissible fault exclusions one may also achieve PL e as per EN ISO 13849-1.

Safety note

- PL e or higher acc. to EN ISO 13849-1 is achieved if the short-circuit between input and associated pulse output as well as the short-circuit between the sensor connections can be excluded. Here one must take care that in a fault scenario the switch must be positively opening in accordance with EN 60947-5-1. The sensor must additionally be triggered in regular intervals and the safety function requested. Fault exclusions can be achieved in accordance with EN ISO 13849-2 table D8. In case of single-channel use of the inputs, the achievable safety level must be limited to SIL 2 or PL d, if the safety function is demanded at regular intervals.
- A series connection of 2 switching elements with fault exclusion for double fault requires testing of the suitability in accordance with the intended safety level of this element. We would like to draw your attention to the applicable regulations in the EC machine directive 2006/42/EC.
- For single-channel sensors a safety related use of the inputs is only intended in connection with the pulse outputs.

Dual-channel sensor without timeout with cross-shorting test

Faults are at least detected when requested. The DC is medium and by using cyclic tests (start test, operational/organizational tests) can be changed up to high level depending on the test frequency.

Only normally closed contacts should be used for safety related applications.

PL d acc. to EN 13849-1 can be achieved when using sensors / switching elements with fault exclusion for not opening the switch contacts. This is permissible when using positively disconnecting switches with correct constrained actuation. The use of sensors with self-monitoring output contacts is also permitted.

PL e in accordance with EN ISO 13849-1 can be achieved when using sensors / input elements with sufficiently high MTTFd in connection with temporal plausibility monitoring and a sufficiently high change of the switching state = dynamic testing.

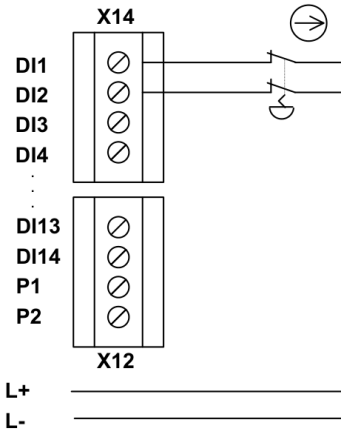


Fig.: Dual-channel sensor homogeneous without pulses, with positive disconnection

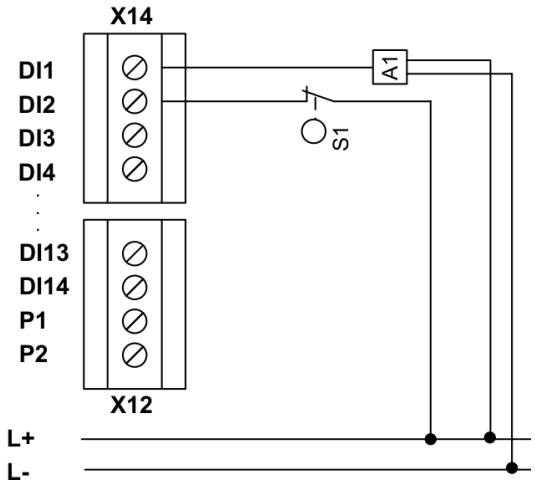


Fig.: Dual-channel input element heterogeneous, without pulses

Safety note

- PL d or higher in accordance with EN ISO 13849-1 is achieved by using switching elements / sensors with positively opening contacts or positive actuation acc. to EN 60947-5-1.
- Using devices for which the fault exclusion double fault for the intended safety level can be specified for the switching elements, is permitted. We would like to draw your attention to the applicable regulations in the EU machine directive 2006/42/EC.

Dual-channel sensor with time-out and cross-shorting test

Cross-shorting as well as connections to DC 24 V and DC 0 V can be detected by using two independent clock signals on the homogeneous sensor.

PL d or higher acc. to EN ISO 13849-1 can be achieved when:

- Use of sensors/switching elements with forced actuation.
- Use of 2 sensors/switching elements with independent manipulation
- dto. However with actuation via a common actuation device in connection with an error exclusion for this device.

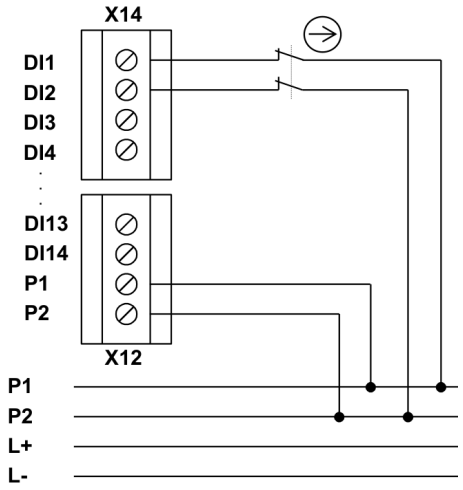


Fig.: Two-channel sensor, homogeneous with pulses

Safety note

- PL d or higher in accordance with EN ISO 13849-1 is achieved by using switching elements / sensors with positively actuation.
- When using two independent sensors with independent actuation, PL d or higher acc. to EN ISO 13849-1 can be achieved.
- When using common elements in the actuation chain, a fault exclusion is required for this purpose. The corresponding limitations and criteria acc. to EN 13849-1 must be observed.

4.2.1.5 Overview of achievable PL for digital safety inputs

Type of sensor / input element	Input	Cross-shorting test	With time-out	Start test	Cyclic test	PL	Fault exclusion for input element	Condition for input element
Single-channel	DI01..DI14					b		Operation proven input element
	DI01..DI14			O	O	d	All faults at the input element; short-circuit at input/signal line	MTTFd = high; connection in control cabinet or protected routing

Type of sensor / input element	Input	Cross-shorting test	With time-out	Start test	Cyclic test	PL	Fault exclusion for input element	Condition for input element
	DI01..DI04, DI09..DI14					e	All faults at the input element; short-circuit at input/signal line	Input element does not comply with min. PLr; connection in control cabinet or protected routing
	all	X				d	Getting caught; short-circuit at input/signal line	Mainly High level required (THigh > 100 * TLow). Positively disconnectin g, MTTFd = high; connection in control cabinet or protected routing
	all	X		O	O	e	All faults at the input element; short-circuit at input/signal line	Input element does not comply with min. PLr; connection in control cabinet or protected routing; MTTFd = high
Dual-channel parallel	all					d	Short-circuit between input/signal line	Connection in control cabinet or protected routing; MTTFd = medium
	all	X				e		MTTFd = high
Dual-channel parallel	all		X			e	Short-circuit between input/signal line (only with common switching elements = 2xNO or 2xNC)	Connection in control cabinet or protected routing; MTTFd = high

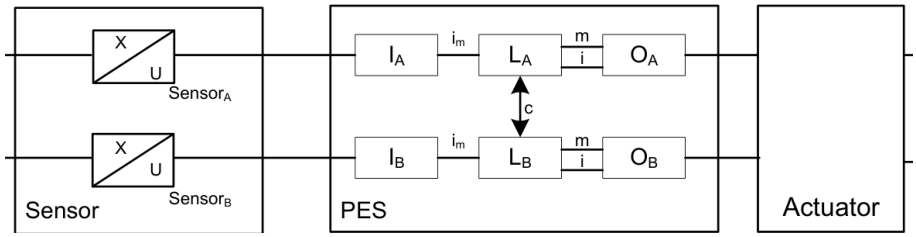
Type of sensor / input element	Input	Cross-shorting test	With time-out	Start test	Cyclic test	PL	Fault exclusion for input element	Condition for input element
Two-channel serial	DI01..DI04, DI09..DI14					d	Short-circuit at input/signal line; getting caught / positively disconnecting	Connection in control cabinet or protected routing; MTTFd = medium
	DI01..DI04, DI09..DI14			O	O	e	Short-circuit at input/signal line	Connection in control cabinet or protected routing; MTTFd = high
	all			O	O	d	Short-circuit at input/signal line	Connection in control cabinet or protected routing; MTTFd = medium
	all	X		O	O	e		MTTFd = high

X: Diagnostic measure activated · O: min. 1 diagnostic measure activated · PL: achievable PL acc. to EN ISO 13849-1

4.2.2 Analog sensors

The basic module ESMD has two analog inputs with two input channels each. Only 2-channel sensors can generally be connected to this interface.

The internal signal processing takes place separately in the two channels with cross-comparison of the results.



Dual-channel sensor system with separate signal processing in two channels, diagnose by cross-comparison in the PES

As with other sensor systems, a vast number of diagnostic measures has been implemented.

With respect to their type and effectiveness, diagnostic measures can generally be classified using the following table:

Diagnoses for sensors for position and/or speed detection:

Measure	DC	Note	Use
Cross-comparison of input signals with dynamic test, if short-circuits cannot be detected (for multiple inputs/outputs)	90 %	Comparison of the analog input values with identical characteristics for both channels	Monitoring of dual-channel systems with identical characteristic of the input signals
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 %	Comparison of the analog input values with diverse characteristic for both channels. E.g. inverse signal course, etc.	Monitoring of dual-channel systems with diverse characteristic of the input signals

Safety note

- The manufacturer's data (MTTFd, FIT-numbers, etc.) must be used for a safety related assessment of the partial system "Sensors".
- The DC-values listed in the table must be used conservatively and compliance with the boundary conditions (see table under „Remarks") must be ensured.
- According to the applicable standards, fault exclusions are permitted. The boundary conditions mentioned in this context must permanently be met.
- If several sensor systems are required for the correct function of a single safety function, their partial values must be correctly merged by following the chosen method. This applies also for a combination of digital and analog sensors (e.g. safely reduced speed with open safety door = door contact + encoder for speed detection).

Exemplary connection of analog sensors

By using suitable sensors and careful wiring of the sensor PL e acc. to EN ISO 13849-1 can be achieved.

The analog current inputs are all equipped with the fixed loading resistor of 500 Ohm. For analog voltage inputs this resistor is omitted.

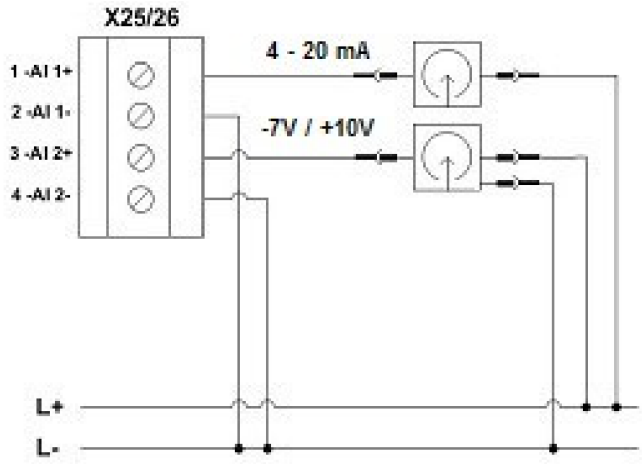


Fig.: Example for analog sensor connection

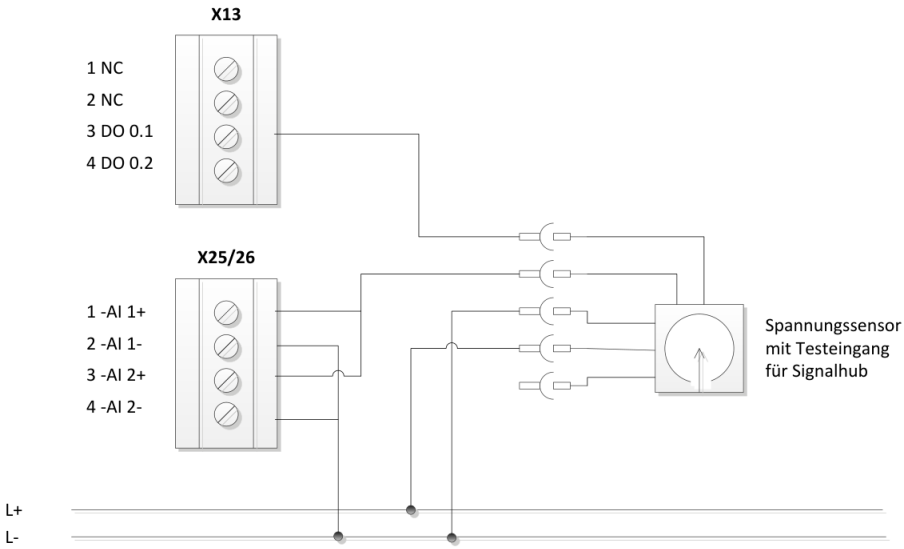


Fig.: Voltage sensor with test pulse

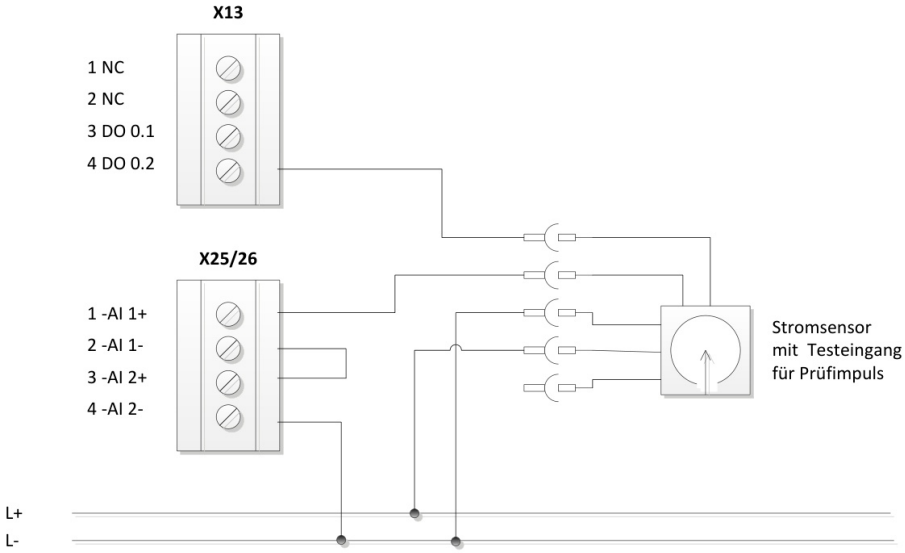


Fig.: Current sensor with test pulse

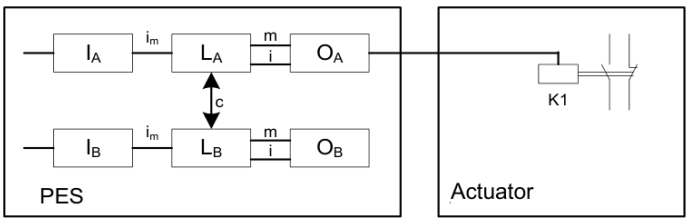
Safety note

– PL e acc. to EN ISO 13849-1 is achieved when using two non-reactive sensors, for which Common Cause faults can be ruled out.

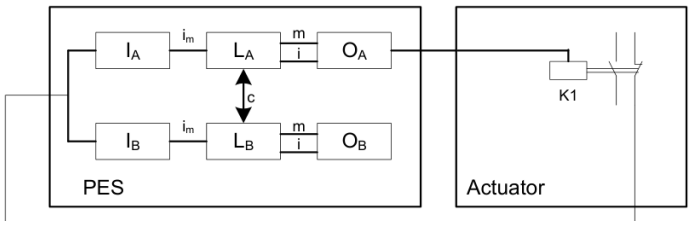
4.3 Safety related characteristics and output wiring

The modules all have safe outputs of various types. For wiring, the corresponding characteristic as specified in the following description, must be accounted for.

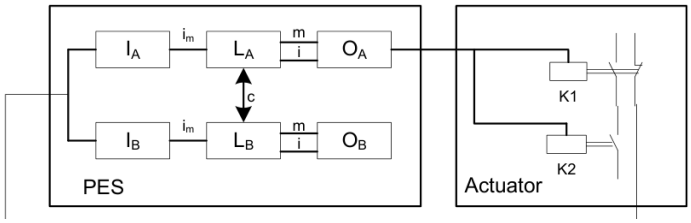
4.3.1 Characteristics of output elements



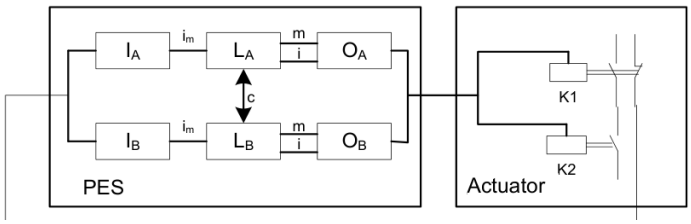
Single-channel output ESMD and single-channel actuator without diagnostics



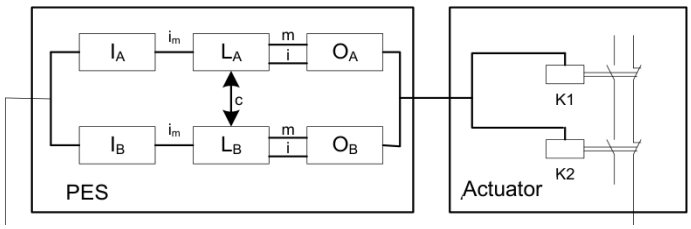
Single-channel output ESMD and single-channel actuator with diagnostics



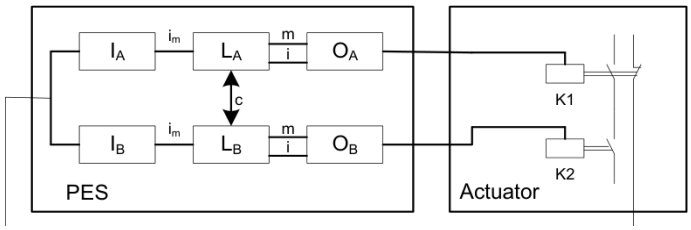
Single-channel output ESMD (Rel 1 / 2, DO 0/1P, DO 0/1M) and dual-channel actuator with at least single-channel diagnostics.



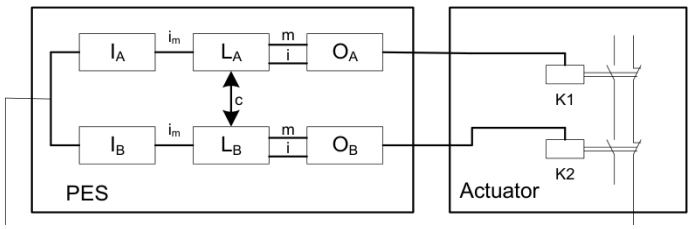
Single-channel output with internal dual-channel processing (EAAx) and dual-channel actuator with at least single-channel diagnose



Single-channel output with internal dual-channel processing (EAAx) and dual-channel actuator with dual-channel diagnose



Dual-channel output ESMD and dual-channel actuator with single-channel diagnose



Dual-channel output ESMD and dual-channel actuator with dual-channel diagnose

4.3.2 Diagnoses in cut-off circuit

The cut-off circuit is equipped with durably implemented and parametrizable diagnostics functions. Certain diagnostics functions also include the external part of the cut-off channel. Depending on the use of these diagnostics functions, different DC-values will arise.

4.3.2.1 Diagnostic functions

Durably implemented diagnostics functions:

Cross-wise readback of outputs: All safety outputs are read back in the complementary channel. Faults in the internal cutout circuit of the module are thus detected with DC = High.

Test of cutout ability for K1 and K2 (only control of relay): The cutout ability of these outputs is cyclically tested. Failure of the cutout possibility is clearly detected.

Parametrizable diagnostics functions:

Readback of the actuator status via auxiliary contacts, position indicators, etc.: The current status of the actuator is detected by correspondingly suitable auxiliary contacts or position indicators and compared with the nominal status. Any deviation is thereby clearly recognized.

Note: The DC depends on a single-channel or dual-channel diagnose as well as on the switching frequency.

Testing the cutout ability for EAAx, EAA1 – EAA10 (digital outputs): Once this function has been activated, the cutout ability of these outputs is cyclically tested. Failure of the cutout possibility is clearly detected.

4.3.2.2 Overview DC with respect to the chosen diagnostics functions

Measure	DC	Note	Use
Monitoring of outputs by a channel without dynamic test.	0-90 %	DC depending on switching frequency. When using elements for switching amplification (external relays or contactors) only effective in connection with the readback function of the switching contacts	Monitoring of electro-mechanical, pneumatic or hydraulic actuators / outputs
Redundant cutout path with monitoring one of the drive elements	90 %	When using elements for switching amplification (external relays or contactors) only effective in connection with the readback function of the switching contacts	Monitoring of the outputs with direct functions as safety circuit or monitoring of safety circuits with elements for switching amplification of pneumatic / hydraulic control valves in connection with readback functions from their switching status
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 %	When using elements for switching amplification (external relays or contactors) only effective in connection with the readback function of the switching contacts. For applications with frequent safety shut-down requests these tests should be performed more frequently, e.g. at the beginning of the shift, 1 x per week. However, a test should at least be carried out cyclically 1 x year.	Monitoring of the outputs with direct functions as safety circuit or monitoring of safety circuits with elements for switching amplification of pneumatic / hydraulic control valves in connection with readback functions from their switching status

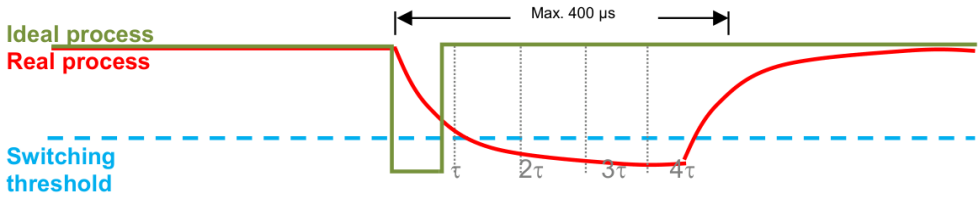
4.3.3 Permissible capacitive and inductive load at safe outputs

The safe outputs exhibit an OSSD character. That is, the outputs are cyclically switched off for the test of the switching off ability and the status is read back.

The examination of the switching off ability takes place according to the following criteria/functions:

- After switching the output off, the output voltage may max. be 5.6 V
- The permissible voltage level must be achieved at the latest after 400 µs
- If the permissible voltage level is reached, the test is seen as successful, the output is activated again without further delay
- If the permissible voltage level is still not reached after 400 µs, an alarm is triggered and all safe outputs (second channel with safe outputs!) are deactivated

The following diagram shows the ideal (green curve) and typical (red curve) distribution.



Ideal and real process of the output voltage during the test (max. 400 µs)

For the determination of the maximally permissible capacity or inductance, the time constant **τ** of the real RC or RL member at the output must be viewed.

This RC or RL member determines the real discharge curve:

The voltage level of max. 5.6 V is securely reached after 3**τ**. It thus applies: 3**τ** < 350 µs, **τ** < 100 µs.

With that connection:

$$\tau = RC = \frac{L}{R}$$

the max. usable capacitive or inductive load can be determined in connection to its Ohm's load:

$$C_{max} = \frac{\tau}{R} = \frac{10^{-4}}{R} \quad \text{bzw.} \quad L_{max} = \tau R = 10^{-4} \cdot R$$

Typical values for the capacity C are C = 20 nF and for longitudinal inductance L = 100 mH.

4.3.4 Digital outputs

The modules ESMD and expansion module all have basic outputs of identical design.

4.3.4.1 Characteristics of basic outputs

The series provides multiple different outputs, which can be interconnected individually or in groups.

Output	Architecture acc. to EN ISO 13849-1	Comment
Combination of 2 relays K1 – K2	4	Complete tripping channel in compliance with architecture category 4 acc. to EN ISO 13849-1
K1, K2	Not safe	Only functional
DO 0.1	Not safe	Auxiliary output
DO 0.2	Not safe	Auxiliary output

The outputs are subjected to a plausibility test in all operating states. In switched on state the correct function of all outputs is tested with a cyclic test pulse. For this purpose the output is switched to the corresponding inverse value for a test period TT < 500 µs (typically 200 µs) i.e. one pp-output is switched instantaneously to 0 VDC potential, while one pn-output is switched to 24 VDC potential.

The relay outputs are monitored for plausibility during each switching cycle. The relay outputs must be switched cyclically and thus tested to maintain the safety function. The switching/test cycle is determined in dependence on the application.

Safety note

- For applications with frequent safety shut-down requests these tests should be performed more frequently, e.g. at the beginning of the shift, 1 x per week. However, a test should at least be carried out cyclically 1 x year.
- The test function for the outputs is performed for groups and individual controls. The auxiliary outputs are not tested.
- A mixed operation with the relay contacts is not permitted! Mixed operation: A dangerous contact voltage potential may not be mixed with a protective low voltage.

Example FALSE: 230 VAC (120 VAC cULus) are switched over K1.1 + K1.2 and 24 V DC are switched over K2.1 + K2.2.

Example TRUE: 230 VAC (120 VAC cULus) are switched over K1.1 + K1.2 and over K2.1 + K2.2 respectively. Or 24 VDC are respectively switched over K1.1 + K1.2 and K2.1 + K2.2.

The outputs can be loaded as follows:

Output	Voltage	Current
Relay Kx	24 VDC	2,0 A (DC13)
Relay Kx	230 VAC	2,0 A (AC15)
DOx	24 VDC	250 mA
EAAx	24 VDC	250

Safety note

- For safety relevant applications only external switching elements with a minimum withstand current of > 1.2 mA may be used.
- For the output system a vast number of diagnostic measures have been implemented. Special attention must be paid to the inclusion of elements for switching amplification, such as relays, contactors, etc. in the cutout circuit.

4.3.4.2 Wiring examples basic outputs

Single-channel switching relay or semi-conductor output without test

For the connection of multi-phase applications or for higher current demands external contactors may be used. For a single-pole connection without external test please bear in mind that the module will not recognize bonding of one or several external contacts. The following circuit example is only limited suitable for safety applications, PL b acc. to EN ISO 13849-1 can maximally be achieved!

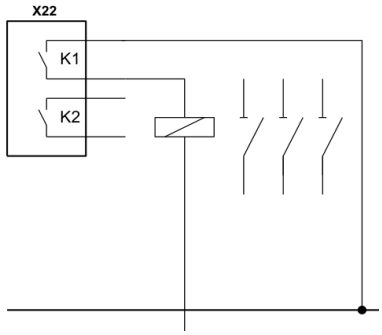


Fig.: Single-channel switching relay output

Safety note

- Not recommended for safety applications! In this context see also the notes in EN ISO 13849-1 concerning the application and the required fault exclusions.

Two-channel switching relay output with external monitoring – group feedback

For safety related applications from PL d acc. to EN ISO 13849-1 two relays on the module and two external power contactors are used.

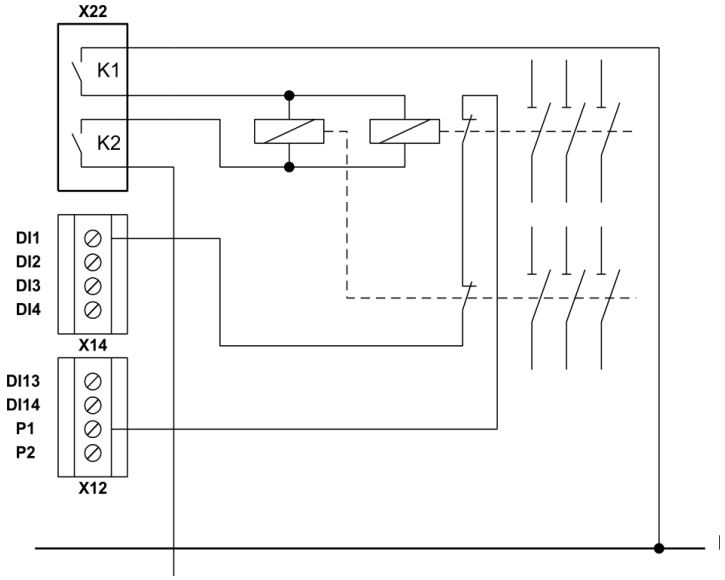


Fig.: Two-channel switching relay output with external monitoring – group feedback

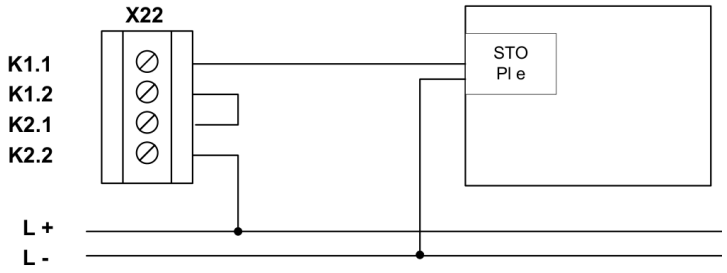
The two external monitoring contacts are switched in series, supplied by the pulse signal P1 and read in from DI01 (configured as EMU-input). In case of higher demands, one must consider that at least 1 switching process must take place every 24 hours.

Safety note

- For achieving PL e acc. to EN ISO 13849-1 a sufficiently high testing rate is required.
- For applications with frequent safety shut-down requests these tests should be performed more frequently, e.g. at the beginning of the shift, 1 x per week. However, a test should at least be carried out cyclically 1 x year.

Dual-channel output with relay output and external control circuit in PL e

For safety applications from PL d and higher acc. to EN ISO 13849-1. The external circuit is controlled in dual-channel mode via the relay outputs. For PL e acc. to EN ISO 13849-1 a sufficiently high testing rate and PL e is demanded for the external circuit.



Dual-channel output with relay output, external circuit (STO, PL e)

Auxiliary output wiring

Both semi-conductor outputs implemented on the module can be wired for functional applications. These outputs are not pulse-controlled.

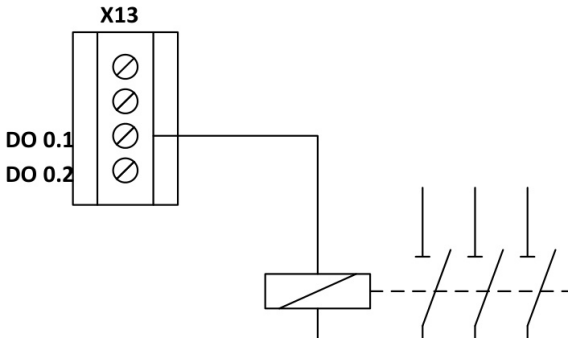


Fig.: Auxiliary output wiring

Safety note **Applications with auxiliary outputs are not approved for safety applications!**

4.3.5 Digital outputs I/Os (EAAx)

The expansion module has configurable safe digital I/Os (see chapter 3 module overview). This connection acts as safe digital pp-switching output parameterized as output.

4.3.5.1 Classification of the I/Os (EAAx) when used as output

Classification	Achievable PL acc. to EN ISO 13849-1	Comment
Static single-channel 2)	PL c	Fault detection or fault reaction acc. to cat. 2
Static two-channel 2)	PL d	Same group 1): – Time-shifted triggering on PLC level – Fault approach short-circuit on both outputs. Different group 1): – No further requirements necessary
	PL e	Different group 1) required
Dynamically single-channel 2), dynamically dual-channel 2)	PL e	No further requirements necessary

Note: 1) Group 1: EAA01 ... EAA06; Group 2: EAA07 ... EAA10. 2) Static: no pulse test on output; Dynamic: pulse test on output tTest ≤ 500 µs.

4.3.5.2 Wiring examples for safe digital outputs I/Os (EAAx)

Wiring single-channel without testing

When using a two-channel output (EAAx) in connection with a single-channel external wiring without external examination it must be taken into account that an adherence of one or several external contacts is not recognized by the module. The following circuitry example is only suitable in a restrictive manner, maximally PL b according to EN ISO 13849-1 can be reached!

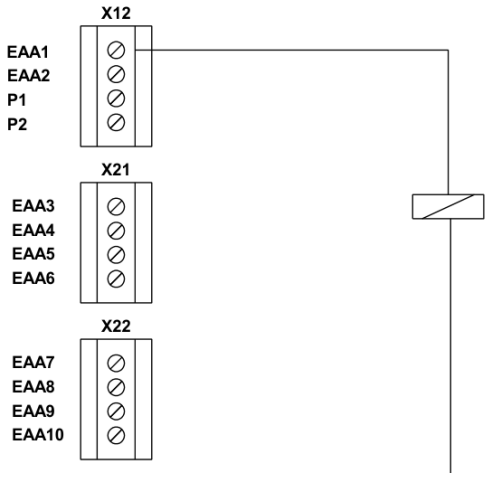


Fig.: Two-channel output with single-channel wiring without testing

Safety note

– Not recommended for safety applications! In this context see also the notes in EN ISO 13849-1 concerning the application and the required fault exclusions.

Wiring single-channel with testing

When using a two-channel output (EAAx) in connection with a single-channel external wiring with testing, positively guided auxiliary contacts are especially needed for electro-mechanical devices and message contacts for the valve position are required for hydraulic or pneumatic components. Furthermore, a message/warning device for indicating a failure is required. The message/warning device must ensure that the operator recognizes the dangerous situation immediately. The achievable PL is mainly depending on the test rate, PL d acc. to EN ISO 13849-1 can maximally be achieved!

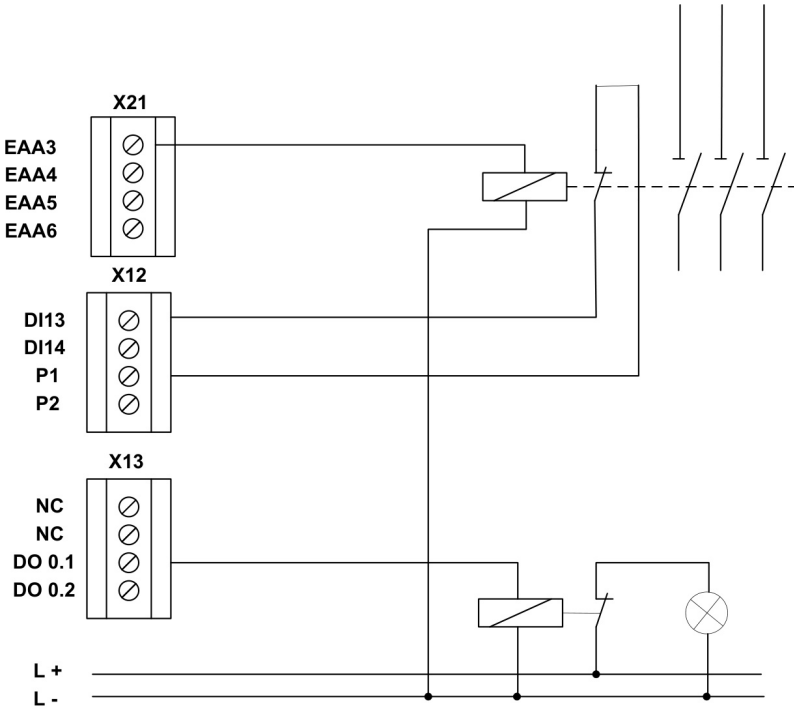


Fig.: Two-channel output with single-channel wiring with testing

Safety note

- Only conditionally recommended for safety applications! In this context see also the notes in EN ISO 13849-1 concerning the application and the required fault exclusions.
- For PL c or higher a test rate of > 100 * the request rate is required.
- If a dangerous situation is detected during a test of the safety function, suitable control measures must be initiated. For PL d a safe state must be initiated, which must not be cancelled until the fault has been eliminated. For PL up to and including PL c, it is also possible to indicate a fault by means of a warning or signalling device, if a safe state cannot be initiated.

Wiring with safe cut-off circuit

For safety applications from PL c and higher acc. to EN ISO 13849-1. The external circuit is controlled directly via a two-channel output. The achievable PL acc. to EN ISO 13849-1 depends on the use of dynamic testing (see 4.3.2.1 DC) and the PL of the downstream device.

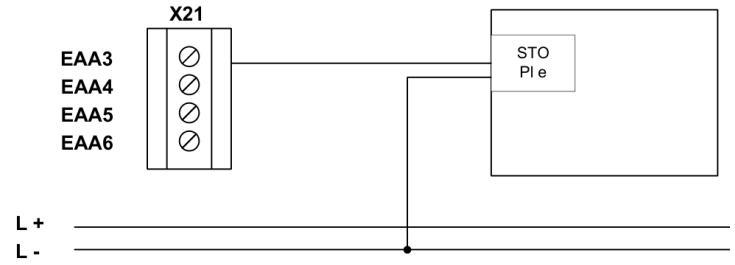


Fig.: Two-channel output in connection with a device with examined disconnection

Wiring in connection with two-channel switching-off circuit

Suitable for PL d and higher acc. to EN ISO 13849-1. Use of one output EAAx in conjunction with two-channel external wiring with test. Positively guided auxiliary contacts are especially needed for electro-mechanical devices and message contacts for the valve position are required for hydraulic or pneumatic components.

The achievable PL depends on the use of dynamic testing as well as the MTTFd-value of the external channel. PL e acc. to EN ISO 13849-1 can maximally be reached!

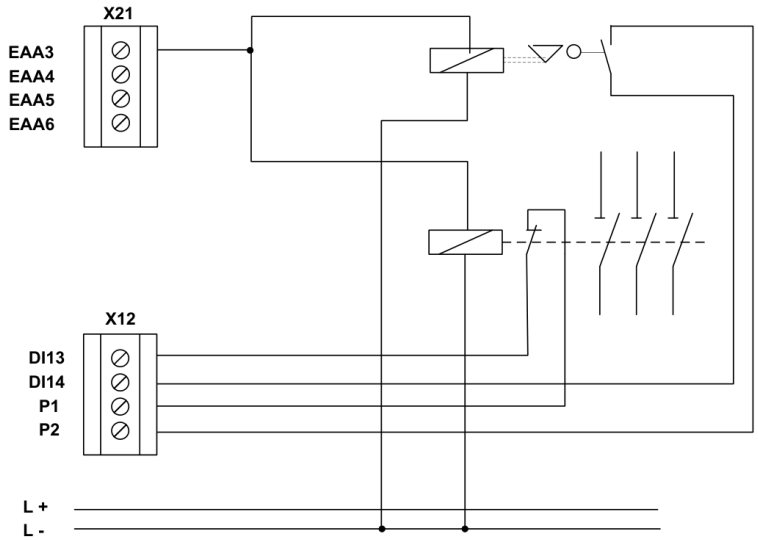


Fig.: Two-channel output in connection with two-channel switching-off circuit with testing

Redundant two-channel output

Suitable for PL d and higher acc. to EN ISO 13849-1. Use of two outputs EAAx in connection with a dual-channel external wiring.

Wiring dual-channel in the same group:

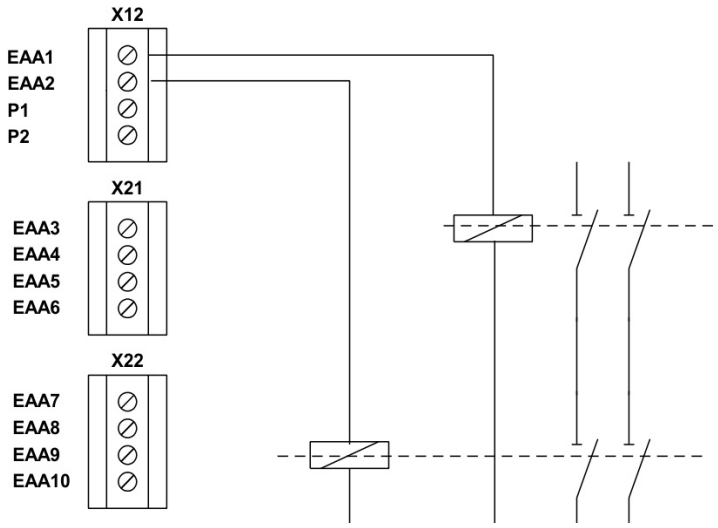


Fig.: Redundant two-channel outputs in the same group in connection with two-channel switching-off circuit

Wiring dual-channel in different groups:

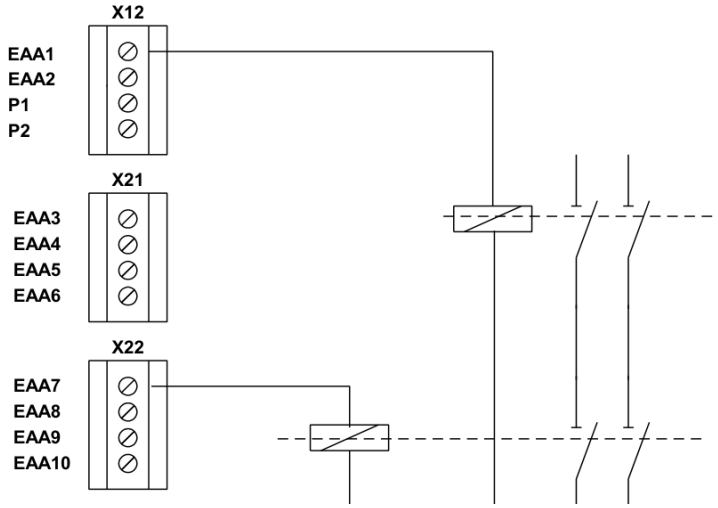


Fig.: Redundant two-channel outputs in different groups in connection with two-channel switching-off circuit

Safety note

- For a safety related assessment of the partial system output the data issued by the respective manufacturer (MTTFd, FIT-numbers, B10d-value, etc.) must be used when using external elements, e.g. for switching amplification, in the shut-down circuit.
- The DC-values listed in the table must be used conservatively and compliance with the boundary conditions (see table under „Remarks“) must be ensured.
- According to the applicable standards, fault exclusions are permitted. The boundary conditions mentioned in this context must permanently be met.
- When using elements for switching amplification in safety circuits, their function must be monitored by means of suitable readback contacts, etc. (see circuitry examples). Suitable readback contacts are contacts which are linked with the contacts in the shut-down circuit in a positively switching way.
- The switching ability of the external switching amplifier must be cyclically tested. The time between 2 tests must be determined in accordance with the requirements of the application and ensured by suitable measures. Suitable measures may be of organizational (On and Off switching at the beginning of a shift, etc.) or technical (automatic, cyclic switching) nature.

4.3.5.3 Overview of achievable PL for digital safety outputs

Output ESMD	Actuator / external shut-down circuit	Cat.	DC		MTTFd actuator	PL	Boundary conditions	Fault exclusion
Single-channel without dynamic output test K1, K2, EAAx	Single-channel contactor, valve, brake, etc. without direct feedback for diagnostics.	Cat. B	0 %		Medium	B	Contactor and downstream actuators appropriately designed for safety application	
	Single-channel contactor, valve, brake, etc. with monitored and positively guided auxiliary contact	Cat. 2	60-90 %	Depending on switching frequency	Medium	B	Auxiliary output required for warning in case of detected malfunction. Contactor and downstream actuators appropriately designed for safety application	
					High	C	As before	
						D	As before. DC = 90 % due to a sufficiently high test rate with reference to the application	
Single-channel without dynamic output test K1 or K2 or single-channel	Dual channel contactor, valve, brake, etc. with direct feedback for diagnostics at least in one channel or actuator single-channel controlled with safety function cat. 3 (e.g. STO)	Cat. 2	90 %	Monitoring only in an external shut-down circuit	Medium	c	Auxiliary output required for warning in case of detected malfunction. Contactor and downstream actuators appropriately designed for safety application	Short circuit on external control
					High	d		

Output ESMD	Actuator / external shut-down circuit	Cat.	DC		MTTFd actuator	PL	Boundary conditions	Fault exclusion
Single-channel without dynamic output test EAA01..EAA10	Dual channel contactor, valve, brake, etc. with direct feedback for diagnostics at least in one channel or actuator single-channel controlled with safety function cat. 3 (e.g. STO)	Cat. 3	90 %	Monitoring only in an external shut-down circuit	Medium or High	d	Contactor and downstream actuators appropriately designed for safety application	Short circuit on external control
Single-channel without dynamic output test EAA01..EAA10	Dual channel contactor, valve, brake, etc. with direct feedback for diagnostics at least in one channel or actuator with safety function cat. 4 (e.g. STO)	Cat. 4	99 %	Monitoring in both external shut-down circuits	High	e	Contactor and downstream actuators appropriately designed for safety application. Monitoring of electro-mechanical components by means of positively guided switches, position monitoring of control valves, etc.	

Output ESMD	Actuator / external shut-down circuit	Cat.	DC		MTTFd actuator	PL	Boundary conditions	Fault exclusion
Dual-channel without dynamic output test K1 and K2, 2 x EAA01..EAA 10	Dual-channel contactor, valve, brake, etc. with direct feedback for diagnostics at least in one channel or actuator with safety function cat. 4 (e.g. STO)	Cat. 3	90 %	Monitoring in both external shut-down circuits	Medium or High	d	Contactor and downstream actuators appropriately designed for safety application. Monitoring of electro-mechanical components by means of positively guided switches, position monitoring of control valves, etc.. Outputs EAA1..10 each 1 x from different groups (groups of 6/4 EAA-Ports each, e.g. EAA1..6, EAA7..10) or time-shifted triggering on PLC level	Short circuit on external control

Output ESMD	Actuator / external shut-down circuit	Cat.	DC		MTTFd actuator	PL	Boundary conditions	Fault exclusion
Dual-channel with dynamic output test 2 x EAA01..EAA 10	Dual-channel contactor, valve, brake, etc. with direct feedback for diagnostics at least in one channel or actuator with safety function cat. 4 (e.g. STO)	Cat. 4	99 %	Monitoring in both external shut-down circuits	High	e	Contactor and downstream actuators appropriately designed for safety application. Monitoring of electro-mechanical components by means of positively guided switches, position monitoring of control valves, etc.. For applications with frequent safety shut-down requests these tests should be performed more frequently, e.g. at the beginning of the shift, 1 x per week. However, a test should at least be carried out cyclically 1 x year.	Short-circuit in external control in both channels

PL: achievable PL acc. to EN ISO 13849-1; Cat.: category acc. to EN ISO 13849-1.

5 Connection and installation

5.1 General notes on installation

Strictly follow the safety regulations when installing!

Degree of protection IP20

- Route all signal lines for the interfacing of digital inputs and contact monitoring separately.
- You should in any case disconnect 230 VAC voltages from low voltage power lines, if these voltages are used in connection with the application.

The cable lengths for digital inputs and outputs and all sensors must normally not exceed 30 m.

If the cable lengths exceeds 30 m you must apply appropriate measures for fault exclusion concerning impermissible overvoltage. Appropriate measures include e.g. lightning protection for outdoor lines, overvoltage protection of the indoor system, protected routing of cables.

Measures concerning the electromagnetic compatibility (EMC)

The module is intended for use in a drive environment and meets the EMC-requirements mentioned above.

It is also assumed that the electromagnetic compatibility of the overall system is ensured by application of appropriate measures.

Safety note

- Electric power supply lines of the module and "discontinuous-action lines" of the power converter must be isolated from each other.
- Signal lines and power lines of the power converter must be routed through separate cable ducts. The distance between the cable ducts should be minimum 10 mm.
- Only shielded cables must be used to connect the position and speed sensors. The signal transmission cable must be RS-485-standard compliant (lines twisted in pairs).
- Care must be taken to ensure that the shielding is correctly connected in the 9-pin SUB-D plugs of the position and speed sensors. Only metal or metal coated plugs are permitted.
- The shielding on the sensor side must comply with appropriate methods.
- EMC-compliant installation of the power converter technology in the environment of the module must be assured. Special attention must be paid to the routing of cables, the shielding of motor cables and the connection of the braking resistor. Strict compliance with the installation instructions of the power converter manufacturer is mandatory.
- All contactors in the environment of the power converter must be equipped with appropriate suppressor circuits.
- Suitable measures to protect against overvoltages must be applied.

Used symbols acc. to UL 61010-1: Symbol 14 – The temperature at the connecting terminals can amount to over 60 °C. From this temperature, suitable cable types must be used.

5.2 Installation and assembly of the module

The module is solely to be installed in control cabinets with a degree of protection of at least IP54.

The modules must be vertically fastened on a top hat rail.

The ventilation slots must be kept unobstructed, to ensure adequate air circulation inside the module.

For air vents, there must be free space of 30 mm above and below the vents. Stringing of expansion modules is permitted. As the adjacent devices can generate waste heat, a distance of 20 mm should be maintained.

Note When using in non-closed spaces, it must be guaranteed that the environmental conditions of the individual modules (see technical data) are adhered to.

5.3 Installation of backplane bus system

Mounting several modules (ESMD, expansion module) on one top hat rail in connection with the backplane bus system is also possible. These modules can be combined with a communication extension. In this case the backplane bus system needs to be configured by the manufacturer when placing the order and delivered in accordance with the application in question.

The backplane bus system consists of a 5-pin plug connector with snap-in contacts. In these plug connectors all 5 contacts are equipped by standard. In this case the component is not specially marked. On a second variant of the plug connector only 3 contacts are equipped.

Comments Expansion modules have no own power supply unit and depend on a DC power supply via the backplane bus system. Base modules ESMD are equipped with a reinforced power supply unit and always feed in to the backplane bus.

There are two different types of backplane bus connectors:

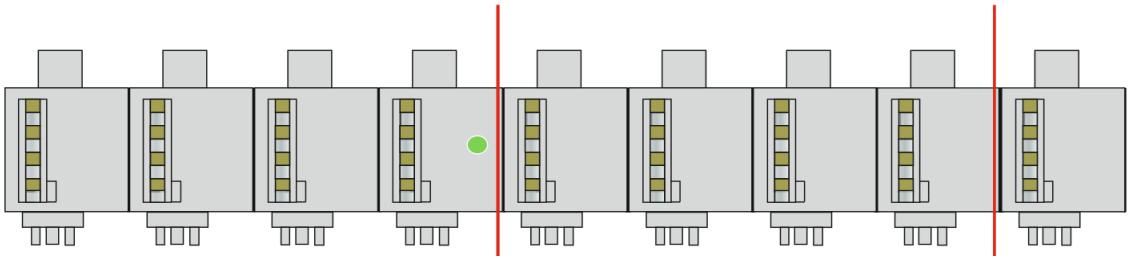
- Standard design (all contacts are present)
- Circuit breaker design (the two live conductors are not present and are marked with a green dot)

Using the backplane bus connector in standard design: The backplane bus connector in standard design can only be installed in connection with expansion modules without their own power supply. Connection of several standalone modules is not possible.

Using the backplane bus connector in circuit breaker design: The backplane bus connector in circuit breaker design is used for combining several base modules with expansion modules. A detailed description can be found under Arrangement examples (below).

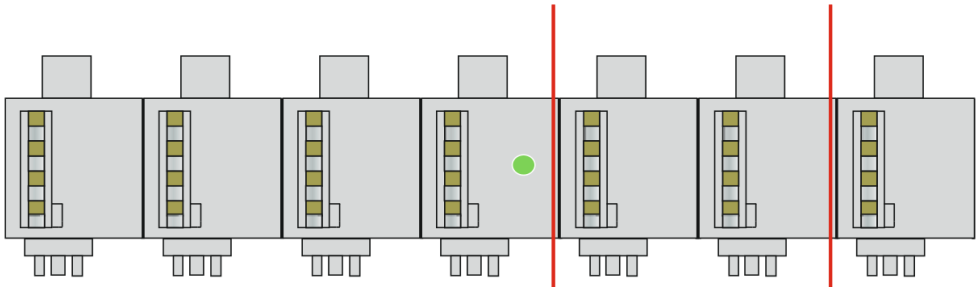
Arrangement examples

Note The arrangement examples serve only for illustration purposes and can deviate mechanically from the actual arrangement.



ESMD + ESMD + communication module (from left: communication module, ESMD, ESMD)

There is no backplane bus connector in circuit breaker design between the last ESMD module and the communication module, because the power supply for the communication module is fed in through the backplane bus system.



ESMD + expansion module + communication module (from left: ESMD, expansion module, communication module)

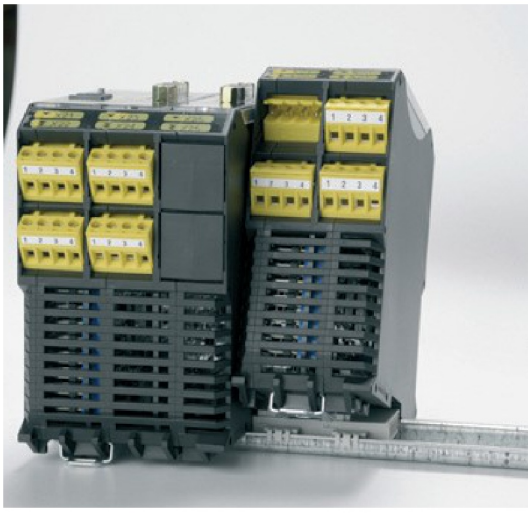
There is no backplane bus connector in circuit breaker design between the last expansion module and the communication module, because the power supply for the communication module is fed in through the backplane bus system.

5.4 Assembling the modules

The modules are mounted on C-standard rails by means of snap-on latches.

5.4.1 Assembly on C-rail

The devices are inserted into the rail under an oblique angle and then snapped on downwards. For disassembling use a screwdriver, insert it into the slot of the downwards pointing latch and then move it up.



5.4.2 Assembly on backplane bus

After assembling the backplane bus the device can be installed. For this purpose insert the module from above into the plug connection under an oblique angle and snap it onto the C-rail.



Insert the module from above under an oblique angle.



Snap-on downwards on to the C-rail.

The backplane plug connection can be extended later. This means the system configuration can be extended by additional modules.



Snap the backplane bus element into the C-rail and insert it into the counter-piece by sliding it sideways.

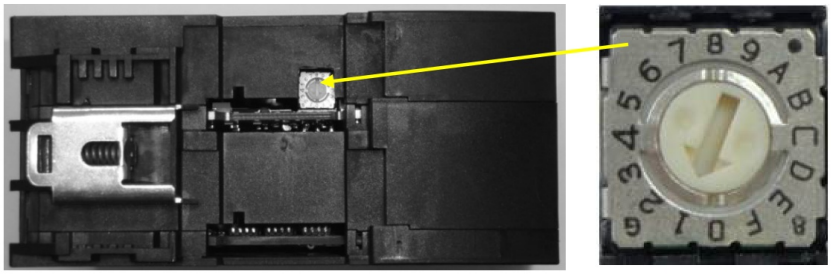
5.4.3 I/O-extension installation

Note Max. two expansion modules can be operated per one basic unit.

Physical address configuration of the slave modules (central)

On expansion modules the bus address has to be set with the help of the address switch.

The address switch is located on the back of the module.

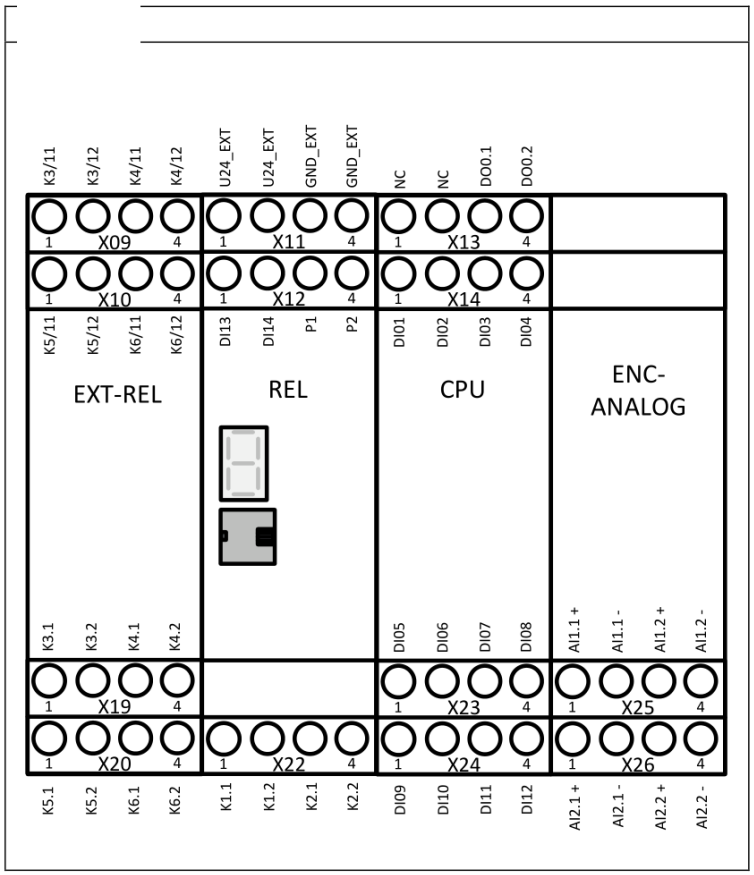


Note

- Address range of the expansion module from 1 ... 15.
- Address "0" is reserved for the basic device.

5.5 Terminal assignment

5.5.1 Terminal assignment ESMD

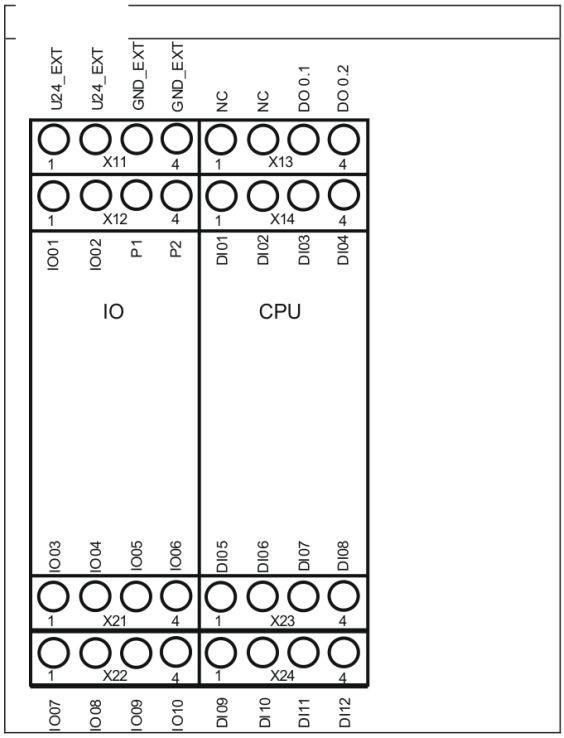


Terminal layout ESMD

Unit	Terminal	Pin	Description
EXT-REL	X09	1 – K3/11, 2 – K3/12	Read back contact relay 3
		3 – K4/11, 4 – K4/12	Read back contact relay 4
	X10	1 – K5/11, 2 – K5/12	Read back contact relay 5
		3 – K6/11, 4 – K6/12	Read back contact relay 6
	X19	1 – K3.1, 2 – K3.2	Safe relay output
		3 – K4.1, 4 – K4.2	Safe relay output
	X20	1 – K5.1, 2 – K5.2	Safe relay output
		3 – K6.1, 4 – K6.2	Safe relay output
REL	X11	1 – U24_EXT, 2 – U24_EXT	Voltage supply device +24 VDC
		3 – GND_EXT, 4 – GND_EXT	Voltage supply device 0 VDC
	X12	1 – DI13, 2 – DI14	Safe digital inputs
		3 – P1, 4 – P2	Pulse outputs
	X22	1 – K1.1, 2 – K1.2	Safe relay output
		3 – K2.1, 4 – K2.2	Safe relay output
CPU	X13	1 – NC, 2 – NC	No function
		3 – DO 0.1, 4 – DO 0.2	Auxiliary outputs
	X14	1 – DI1, 2 – DI2, 3 – DI3, 4 – DI4	Safe digital inputs
	X23	1 – DI5, 2 – DI6, 3 – DI7, 4 – DI8	Safe digital inputs
	X24	1 – DI9, 2 – DI10, 3 – DI11, 4 – DI12	Safe digital inputs
ENC-ANALOG	X25	1 – AI 1.1+, 2 – AI 1.1–, 3 – AI 1.2+, 4 – AI 1.2–	Safe analog input

Unit	Terminal	Pin	Description
	X26	1 – AI 2.1+, 2 – AI 2.1–, 3 – AI 2.2+, 4 – AI 2.2–	Safe analog input

5.5.2 Terminal assignment expansion module



Terminal layout expansion module

Unit	Terminal	Pin	Description
IO	X11	1 – U24_EXT, 2 – U24_EXT	Voltage supply device +24 V DC outputs
		3 – GND_EXT, 4 – GND_EXT	Voltage supply device 0 V DC
	X12	1 – IO01, 2 – IO02	Safe digital inputs, outputs pp-switching
		3 – DO0.3, 4 – DO0.4	Auxiliary outputs
	X21	1 – IO03, 2 – IO04, 3 – IO05, 4 – IO06	Safe digital inputs, outputs pp-switching
	X22	1 – IO07, 2 – IO08, 3 – IO09, 4 – IO10	Safe digital inputs, outputs pp-switching
CPU	X13	1 – NC, 2 – NC	No function
		3 – DO0.1, 4 – DO0.2	Auxiliary outputs
	X14	1 – DI1, 2 – DI2, 3 – DI3, 4 – DI4	Safe digital inputs
	X23	1 – DI5, 2 – DI6, 3 – DI7, 4 – DI8	Safe digital inputs
	X24	1 – DI9, 2 – DI10, 3 – DI11, 4 – DI12	Safe digital inputs

5.5.3 Terminal assignment communication modules

Please take the terminal assignments of the individual communication modules from the corresponding installation manuals.

5.6 External 24 VDC – voltage supply

The module requires a 24 VDC power supply with PELV characteristic in accordance to EN 50178. Please comply with the following boundary conditions when planning and installing the specified power supply unit:

Strictly comply with the minimum and maximum supply voltage tolerance.

Nominal voltage	DC 24 V
Minimum: 24 VDC – 15 %	20,4 VDC
Maximum: 24 VDC + 20 %	28,8 VDC

We recommend the use of a 3-phase power supply unit or an electronically controlled device to achieve an as little as possible residual ripple of the supply voltage. The power supply unit must meet the requirements acc. to EN 61000-4-11 (voltage dip).

Connecting cables must comply with local regulations.

The interference voltage resistance of the module is 32 VDC (protected by suppressor diodes at the input).

Safety note

– The module must be individually protected by a 3,15 A (min. 30 VDC) back-up fuse which must be placed near by the terminals of the modules.

Recommended fuse type: 3.15 A circuit breaker (Class B) or safety fuse (inert).

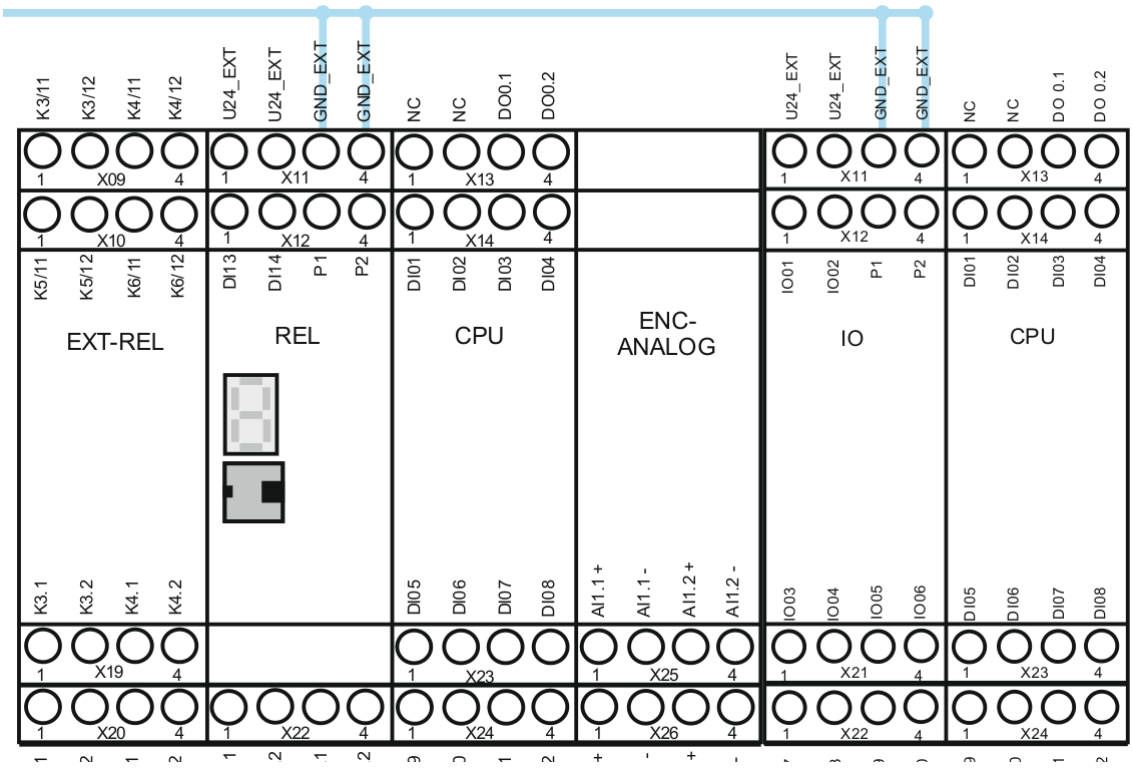
Comments Reliable galvanic isolation from the 230 VAC or 400 VAC network must be guaranteed in any case. This requires the selection of power supply units complying with the regulations DIN VDE 0551, EN 60 742 and DIN VDE 0160. Besides choosing a suitable device you must also ensure equipotent bonding between PE and 0 VDC on the secondary side.

Safety note

– All GND connections of the devices, which are connected to the inputs of the module must be connected to the GND of the module (voltage supply).

Inputs of the module are: digital inputs, digital I/Os, analog inputs, encoder connections.

Comments The connections GND_ENC and AIN are not internally connected to GND!



GND connection ESMD and expansion module

5.7 Connection of digital inputs

The module comes with 14 (ESMD) or 12 (expansion module) safe digital inputs. These are suitable for connecting single or two-channel signals with and without pulse, or without cross-shorting test.

The connected signals must have a "High"-level of 24 VDC (+15 VDC ... +30 VDC) and a "Low"-level of (–3 VDC ... +5 VDC, Type 1 acc. to IEC 61131-2). The inputs are provided with internal input filters.

A device internal diagnostic function cyclically tests the correct function of the inputs including the input filters. A detected fault will set the module into an alarm status. At the same time all outputs of the module are rendered passive.

Besides the actual signal inputs, the module holds two pulse inputs P1 and P2 available. The pulse outputs are switching-type 24 VDC outputs.

The pulse outputs are solely intended for monitoring the digital inputs (DI1 ... DI14) and cannot be used for any other function within the application.

The switching frequency is 125 Hz for each output. In the planning stage one must bear in mind that the outputs may only be loaded with a total current of max. 250 mA.

Furthermore, approved OSSD-outputs can be connected to the inputs I01-I14 without limitation.

In case of single-channel use of the inputs, the achievable safety level must be limited to SIL 2 or PL d, if the safety function is demanded at regular intervals.

A safety related use of the inputs is generally only intended in connection with the pulse outputs.

If pulse outputs are not used, short circuits in the external wiring between different inputs and against the supply voltage for the module must be ruled out by external measures, appropriate routing of cables in particular.

Each input of the module can be configured individually for the following signal sources:

- Input is assigned to the pulse P1
- Input is assigned to the pulse P2
- Input assigned to continuous voltage 24 VDC

5.8 Connection of analog inputs

With the designs using analog processing, max. 2 analog signals can be processed safely. The analog inputs can be connected as follows:

	min	max.
Voltage	–10 VDC	+10 VDC

Note The modules can optionally be equipped with voltage and, or current inputs.

Safety note

- The GND connection AIN must be connected to the GND of the module.

6 Response times of the ESMD

The response time is a very important safety related characteristic and must be strictly observed for each application / application related safety function. The following chapter lists the response times for individual functions, probably also in dependence on further parameters. If these data are insufficient for a specific application you should validate the actual time behaviour against the nominal behaviour by means of separate measurements. This applies also for the use of filter functions in particular.

Safety note

- The response times must be determined for each application related safety function in nominal behaviour and must then be compared with the actual value by using the following data.
- Special care must be taken when using filter functions. Depending on the filter length / time the response time may be extended, which must be taken into account in the safety related design.
- In case of particularly critical problem formulations the temporal behaviour must be validated by means of measurements.
- During start-up of the device / alarm or fault reset the outputs may (depending on the application program) become active over the response time period. This must be taken into consideration when planning the safety function.
- When using safe field bus connections (e.g. PROFIsafe, FSoE), the system run-time (watchdog) must also be included in the calculation.

6.1 Response times in standard operation

The cycle time of the system serves as basis for calculating the response times. The cycle time is adjustable in 3 settings and is **T_Cycle = 8 ms** during operation. The specified response times comply with the corresponding maximum running time for the actual application within the module. Depending on the application, further, application dependent response times of the sensors and actuators used must be added, in order to obtain the total running time.

Function	Response time [ms]	Explanation
Activation of a monitoring function by means of ENABLE with subsequent shut-down via digital output	24 *)	Activation of a monitoring function by means of the ENABLE signal.
Activation of a monitoring function by means of ENABLE with subsequent shut-down via safety relay	47 *)	Activation of a monitoring function by means of the ENABLE signal.
Response of an already activated monitoring function including PLC editing in case of position and speed processing via digital output	16 *)	With a monitoring function that has already been activated via ENABLE, the module requires one cycle to calculate the current speed value. During the next cycle after calculation of the monitoring function the information is further processed and output by the PLC, i.e. according to the implemented logic this will lead to e.g. switching of an output.
Response of an already activated monitoring function including PLC editing in case of position and speed processing via safety relays	39 *)	With a monitoring function that has already been activated via ENABLE, the module requires one cycle to calculate the current speed value. During the next cycle after calculation of the monitoring function the information is further processed and output by the PLC, i.e. according to the implemented logic this will lead to e.g. switching of an output.
Activation of digital output via digital input	16	Activation of an input and switching of the output
Activation output relay via digital input	26	Activation of an input and switching of the output
Deactivation of digital output via digital input	16	Deactivation of an input and thus deactivation of the output
Deactivation output relay via digital input	47	Deactivation of an input and thus deactivation of the output

Function	Response time [ms]	Explanation
Average filter (setting see encoder dialog of the programming software)	0 - 64	Group running time of the averager. This running time only effects the monitoring function in connection with position / speed / acceleration, but not the logic processing.
Analog filter: 1 (2 Hz) · 2 (2 Hz) · 3 (2 Hz) · 4 (4 Hz) · 5 (6 Hz) · 6 (8 Hz) · 7 (10 Hz) · 8 (20 Hz)	760 · 760 · 760 · 512 · 268 · 143 · 86 · 56	The analog filter only affects the safe analog inputs of all modules with analog variants. Response times of the analog input filters in relation to the input frequency

Note: *) When using an average filter the response time of this filter must also be added.

6.2 Response time for FAST_CHANNEL

FAST_CHANNEL describes a characteristic of the module to respond quicker to speed requirements than this would be possible with the execution of the safety programs in normal cycle (= 8 msec). The sampling time of **FAST_CHANNEL** is 2 msec.

The following response times can be specified: 4 msec (Worst Case Condition)

Safety note

- When using FAST_CHANNEL you should bear in mind that shutting down within the time specified above for a given speed threshold is only possible, if the sensor information has a sufficient resolution. The smallest resolvable switching threshold of the FAST_CHANNEL requires at least 2 edge changes on the corresponding sensor system within a period of 2 msec.
- This function can only be used in connection with semi-conductor outputs.
- The FAST_CHANNEL may not act on SSI Listeners.

6.3 Response times for fault distance monitoring

The following calculation schematic applies for calculating the Worst Case condition.

Quantity	Symbol
System speed to the sampling instant	V(t)
System speed in case of module response	VA
Threshold value for monitoring (SLS or SCA)	VS = constant for all t
Parameterized filter value	XF = constant for all t
Maximum possible acceleration of the application	aF = constant for all t
Deceleration after shut-down	aV = constant for all t
Sampling instant for occurrence of the Worst Case event	TFault
Response time of the system	tResponse

For the Worst Case assessment it is assumed that the drive will initially move exactly to the parameterized threshold with a speed v(k) and then will accelerate to the maximum possible value a0.

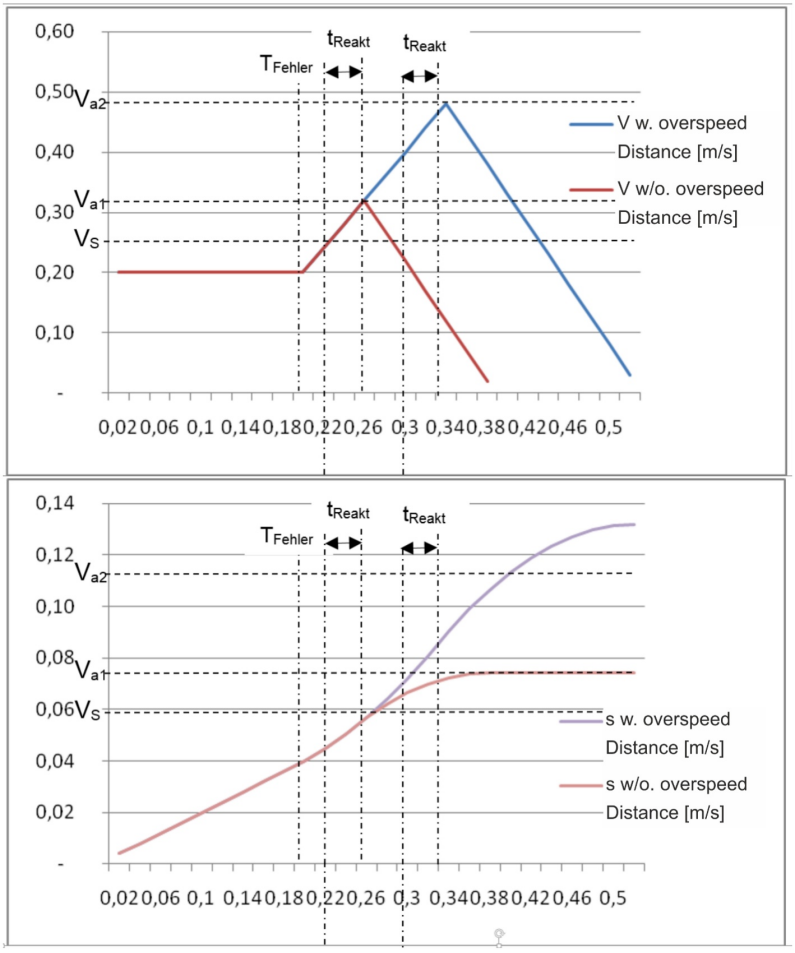


Diagram: Behavior of the drive with / without overspeed distance

Without overspeed distance the following connections result for the course of V and s.

Parameters	Calculation methods	Comments
tResponse	Value from the specified response time ESMD + deceleration time in external shut-down chain	Deceleration time in external shut-off chain derived from relay/contactor and brake data, etc. issued by the manufacturer
aF, aV	n. a.	Estimation of the application
Va1	= VS + aF * tResponse	

With overspeed distance the following connections result for the course of V and s.

Parameters	Calculation methods	Comments
tResponse	Value from the specified response time ESMD + deceleration time in external shut-down chain	Deceleration time in external shut-off chain derived from relay/contactor and brake data, etc. issued by the manufacturer
aF, aV	n. a.	Estimation of the application
Va2	= aF * tResponse + (VS² + 2 * aF * XF)^1/2	

With its effect the filter displaces the set speed threshold Va upwards by the amount delta_v_filter. For the application one must consider the new response time values (Treact = Tscu + Tfilter), as well as the speed at shut-down by the module resulting from this.

6.4 Response times when using the expansion module

The cycle time of the system serves as basis for calculating the response times. In operation this is **T_zyklus = 8 ms**. The specified response times comply with the corresponding maximum running time for the actual application within the module. Depending on the application, further, application dependent response times of the sensors and actuators used must be added, in order to obtain the total running time.

Function	Designation	Response time [ms]	Explanation
Worst Case deceleration time inlet in basic module to PAE	**TIN_BASE**	10	e.g. activation of a monitoring function by an input signal in the basic module
Worst Case deceleration time input expansion module to PAE in basic module	**TIN_31**	18	e.g. activation of a monitoring function by an input signal in the extension module
Processing time PAE to PAA in basic module	**TPLC**	8	Shut-down by a monitoring function or an input in PAE
Activation / deactivation digital output in basic module from PAA	**TOUT_BASE**	–	Activation or deactivation of an output in the basic module after changes to the PAA.
Activation / deactivation digital output in extension module via PAA in basic module	**TOUT_31**	8	Activation or deactivation of an output in the extension module after changes to the PAA in the basic module.

Determination of the total response time

TTOTAL = TIN + TPLC + TOUT

Example 1: Input to extension module, activation of SLS and processing in PLC, output to basic module.

TTOTAL = TIN_31 + TPLC + TOUT_Base = 18 ms + 8 ms + 0 ms = 24 ms

Example 2: Input to basic module, activation of SLS and processing in PLC, output to extension module.

TTOTAL = TIN_Base + TPLC + TOUT_31 = 10 ms + 8 ms + 8 ms = 26 ms

Example 3: Input to extension module, activation of SLS and processing in PLC, output to extension module.

TTOTAL = TIN_31 + TPLC + TOUT_31 = 18 ms + 8 ms + 8 ms = 34 ms

7 Start-up

7.1 Procedure

Safety note **Start-up must only be performed by qualified personnel!**
Strictly follow the safety regulations when commissioning!

7.2 Start-up sequences

The following phases are passed through and displayed by the front side seven segment display after each new start and fault-free running of the module:

7 segment display	Mode	Description
1	STARTUP	Synchronization between both processor systems and checking of configuration/firmware data
2	SENDCONFIG	Distribution of configuration/firmware data and renewed checking of these data. Subsequent area checking of configuration data.
3	STARTUP BUS	If available, initialization of a bus system
4	RUN	Normal system operation. All outputs are switched according to the current logic status.
5	STOP	In stop mode parameter and program data can be loaded externally.
A	ALARM	The alarm can be reset via the digital input or the front side reset button.
E	ECS-Alarm, ICS-Alarm, ACS-Alarm	The ECS alarm can be reset via the digital inputs or the front side reset button.
F	Fault	Fault can only be reset via ON/OFF of the module.
.	FBus Status	Slave F-Bus (PROFIsafe/FSoE): Off: unused by F-Bus · Slow flashing: F-Bus configured, no connection to the master · Fast flashing: connection to the master, F-Bus activation pending · On: F-Bus connected

7.3 Reset-function

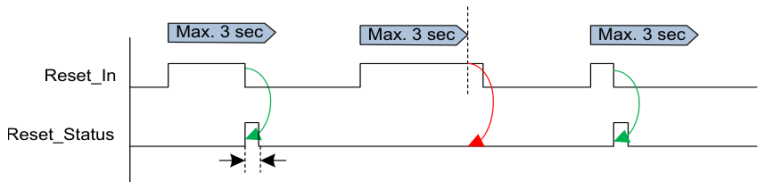
The reset function is divided into a startup-function after a power cycle (power off / on) and a status-/alarm-reset = internal reset-function. The internal reset is called by pushing the "Reset"-button on the front panel or by an input port, configured as "Reset-Element" with active "Alarmreset". The table below shows an overview of those reset-functions:

7.3.1 Types of reset functions

Reset-type	Triggering element	Comment
General Reset	Voltage return / equipment start-up	Reset-function after a complete power off / on
Internal Reset	Reset-button (front panel)	Internal reset called by pushing the Reset-Button on the front panel
	Reset-Element (configured input)	Configuration of a reset-element

7.3.2 Reset timing

The reset-input for an internal reset is time monitored in "RUN"-mode. An internal reset is called by a falling edge of the reset-input under the pre-condition of T < 3 sec between raising / falling edge.



Reset_In / Reset_Status, max. 3 sec

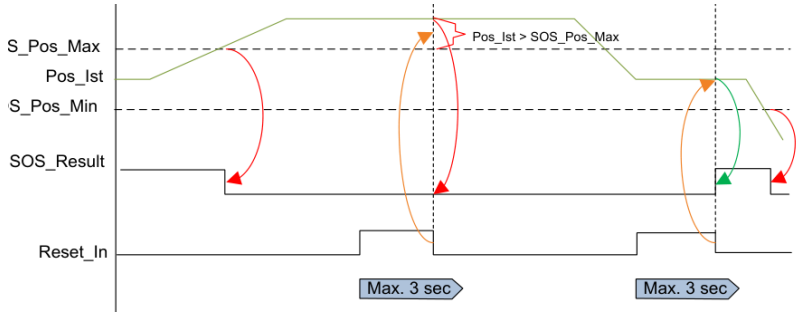
7.3.3 Reset function

Function block	General Reset	Internal Reset	Function
Fatal Error	X		Failure reset
Alarm	X	X	Alarm reset
Safe monitoring function	X	X	Reset of triggered safe monitoring functions
Flip-Flop	X	X	Status = Reset
Timer	X	X	Timer = 0

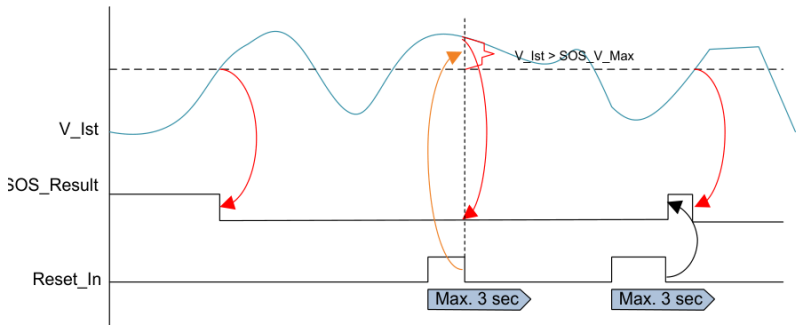
After a reset the status of the safe monitoring functions is rebuilt:

– If process values are beyond the parameterized trigger points, the status of the safe monitoring functions is kept unchanged.

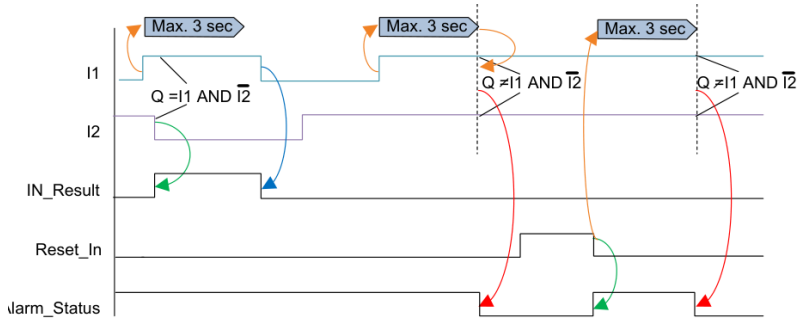
– On time based functions, the timer value is reset and therefore the output status of the related function too. The function is triggered again if the time value versus monitored status exceeds again the parameterized limits.



Process value (position) => no change of the output status with reset in the alarm condition



Process value (speed) => no change of the output status with reset in the alarm condition



Time based function => reset of the starting state, addressing when newly exceeding the limit

Safety note

- On time based functions, i.e. time based monitoring of complementary input signals, the reset-function causes a reset of a possible alarm status. Only if the time versus input status exceeds again the parameterized limits, the alarm status is recalled.
- For safeguarding of false utilization of the reset-function, i.e. reiterated call of the reset-function to bypass the alarm status, adequate measures in the application program (PLC-program) have to be implemented.

Example reset function with safeguarding against false utilization

Function: On a machine for normal operation mode, the hazardous area shall be protected by a mechanical guard system. If in setup mode, the safety level is kept by a release button in conjunction with standstill monitoring respective safe limited speed.

The guard closed position is monitored by a sensor. With the guard in open position movement is only possible with the released button pressed.

On the application program this function is implemented by use of the function "door monitoring" (2 channel mode with time monitoring) and the function "enabling switch".

The logic signal "door monitoring" is produced by computing of the input signals versus time monitoring. The time monitoring with an allowed difference on the expected input signals is fixed for 3 sec.

On the status "door open" (Signal "LOW" on output X23.1 and X23.2 (ID 369)) the axis can be moved with reduced speed if the enable button (X14.1 and X14.2 with ID 318) is on active status.

Task: If a faulty cross connection is detected, the device will show the alarm 6701.

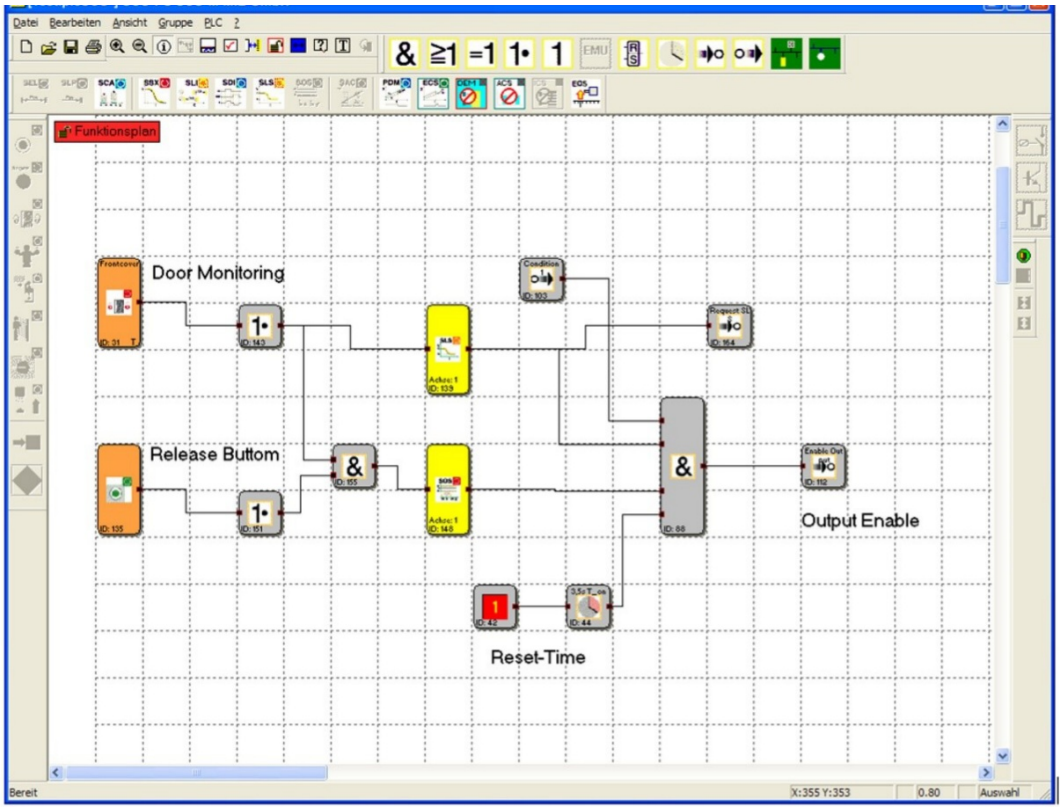
The alarm can be quit, which results in the signal "door monitoring" being kept correctly on "LOW" status.

After 3 sec. a time out will be applied, and the alarm 6701 will return.

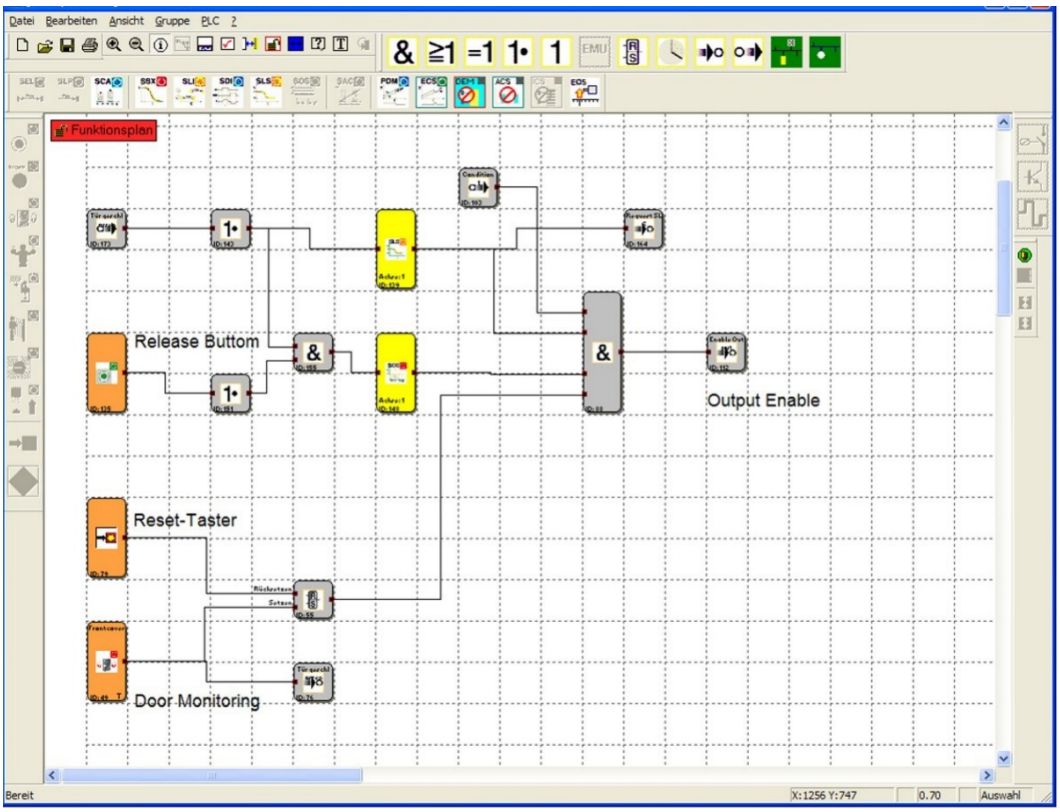
If within this time frame the enable button is activated, the axis can be moved on reduced speed for max. 3 sec.

The task is now to prevent axis movement if the alarm will come potentially back after a reset.

Applicative measure: By logic combination within the PLC-program of the programming software the activation of the outputs by false utilization of the reset-function is prevented.



Example 1: The release function of the outputs (ID 88) is additionally AND combined with a "Reset-Timer". This timer prevents activation of the outputs for T > 3 sec after a call of the reset-function.



Example 2: The release function of the outputs (ID 88) is additionally AND combined with a FF. This FF-element prevents activation of the outputs after a reset with still applied failures on the inputs. Just after a first correct detection of the input signals – both input lines on "HIGH" within 3 sec. – the outputs are released.

7.4 LED display

Colour	Mode	Description
green	flashing	System OK, configuration validated
yellow	flashing	System OK, configuration not yet validated
red	flashing	Alarm
red	permanent	Fatal Fault
yellow – red	flashing	System OK, configuration not yet validated, SMMC configured however participant is missing
green – red	flashing	System OK, configuration validated, SMMC configured however participant is missing

Note For all operating states except RUN the outputs are rendered passive by the firmware, i.e. safely switched off. In status RUN the state of the outputs depend on the implemented PLC-program.

7.5 Parameterization

Parameterization takes place via the programming software. The transmission of these data to the module requires a programming adapter, the drivers of which must first be installed by the user.

Parameterization is described in the programming manual.

7.6 Function test

In order to guarantee safety of the module, the user must carry out a functional test of the safety functions at least once in a year. For this purpose the modules used in the parameterization (inputs, outputs, monitoring functions and logic modules) must be checked with respect to function or shut-down. See programming manual of the programming software.

7.7 Validation

In order to assure the reliability of the implemented safety functions the user must check and document the parameters and links after the start-up and parameterization has taken place. This is supported by a validation assistant in the programming desktop (see chapter 8 Safety related examination).

8 Safety related examination

In order to assure the reliability of the implemented safety functions the user must check and document the parameters and links after the start-up and parameterization has taken place. This is supported by the programming software (see programming manual).

On the first page one can enter general system data.

On the following pages of the validation report, all used functions with their parameters are printed as single verification of the safety-technological examination.

After the transmission of the configuration and program data to the module the status LED flashes yellow. This indicates that the configuration data have not yet been validated.

Pressing the button "LOCK CONFIGURATION" at the end of the validation dialog highlights the data as "Validated" and the LED flashes in green.

9 Maintenance

9.1 Modification / handling changes to the device

Maintenance work must solely be carried out by qualified personnel.

Regular maintenance work is not required.

Repair: The devices must always be replaced as whole units. Repair work on the device can only be performed in the factory.

Warranty: By opening the module without permission the warranty will become null and void.

Note **By modifying the module the safety approval will become null and void!**

9.2 Exchanging a module

The following should be noted when exchanging a module:

- Disconnect the electric power converter from the main supply.
- Switch off the electric power supply for the device and disconnect.
- Pull off the encoder plug.
- Disconnect any other pluggable connections.
- Take the module off the top hat rail and pack up EMC-compliant.
- Mount the new module on the top hat rail.
- Reconnect all connections.
- Switch on the electric power converter.
- Switch on the supply voltage.
- Configure the device.

Note Do not disconnect or connect pluggable connections of the module in live condition. There is a danger of sensor damage, particularly with connected position or speed sensors.

9.3 Maintenance intervals

Activity	Interval
Module replacement	See technical data (chapter 10)
Function test	See chapter 7 "Start-up"

10 Technical data

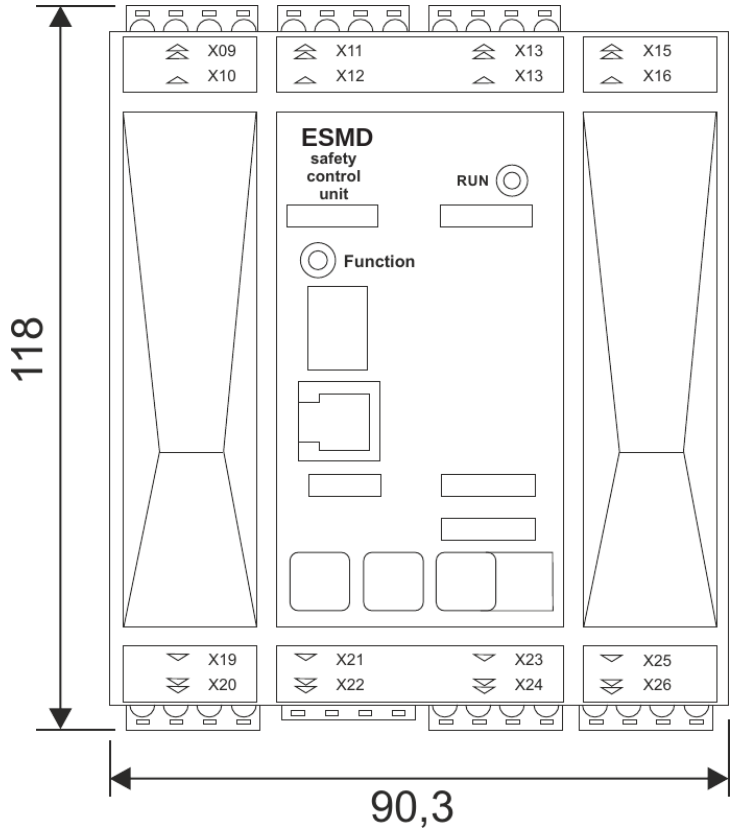
10.1 Environmental conditions

Item	Value
Class of protection	IP 20
Ambient temperature	0 °C* ... 50 °C
Climatic category	3k3 acc. to DIN 60 721
Min-, maximum relative humidity (no condensation)	5 % – 85 %
Overvoltage category	III
Degree of contamination	2
Operating materials	2000 m
Lifetime	90000 h at 50 °C ambient

10.2 Safety related characteristics

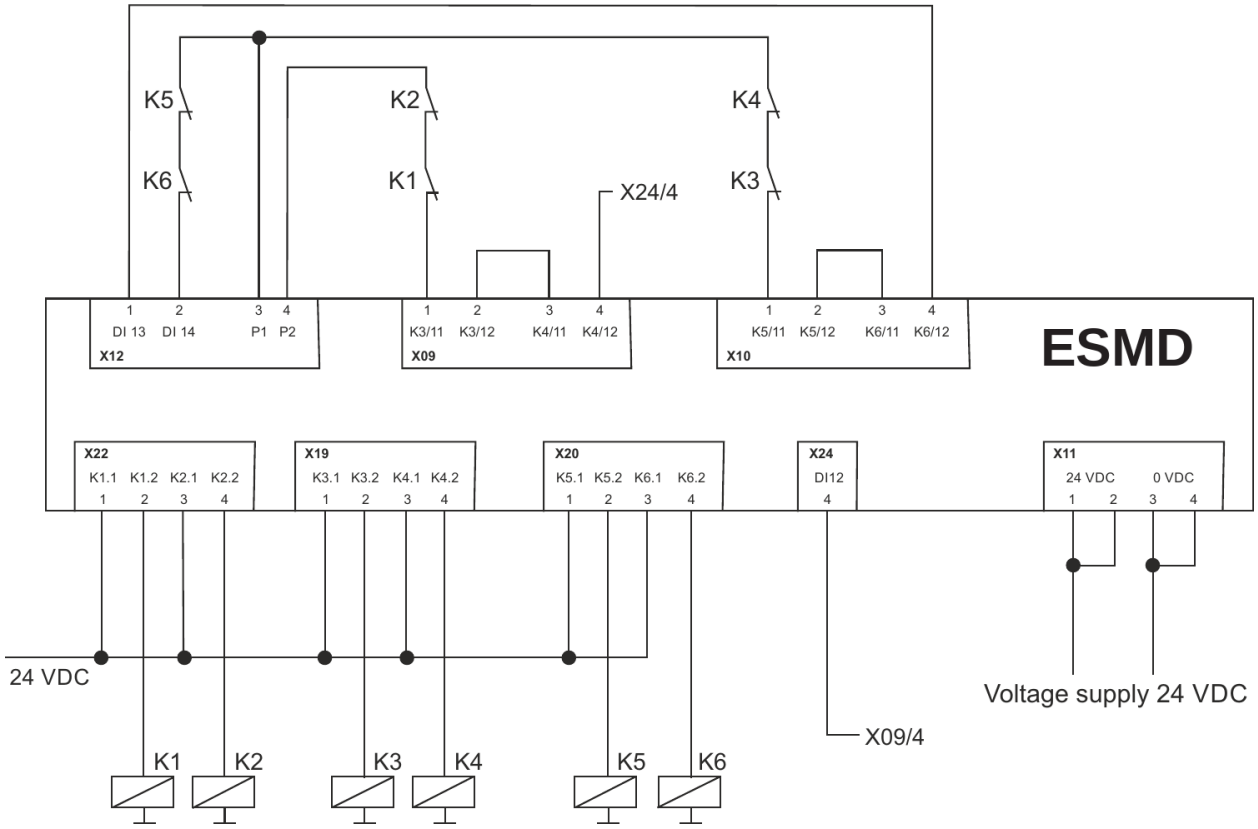
Characteristic	Value
Max. obtainable safety class	SIL 3 as per IEC 61508; Kategorie 4 as per EN ISO 13849-1; Performance-Level e as per EN ISO 13849-1
System structure	2-channel with diagnose (1oo2) acc. to IEC 61508; Architecture category 4 acc. to EN ISO 13849-1
Rating of operating mode	"high demand" acc. to IEC 61508 (high demand rate)
Probability of an endangering failure per hour (PFH-value); specific values acc. to table "Safety related characteristic data"	Expansion module: PFH = 9,2 FIT; ESMD (1-channel): PFH = 20 FIT; ESMD (2-channel): PFH = 1,0 FIT
Proof-Test-Intervall (IEC 61508)	20 years, after this time the module must be replaced

10.3 Dimensions



The device front with the connectors X09 to X26, the RUN and Function keys and the status display. Dimensions in mm.

10.4 Connection example

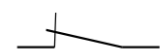


Connection example: six relays K1 ... K6 wired to the connectors X09, X10, X19, X20 and X22, with the read-back contacts K3/11 ... K6/12 fed back to X09 and X10 and the cross-fault pulses P1 and P2 on X12. External contact monitoring (EMU) of the connected switching devices is a built-in safety function; contact multiplication through external contactors is possible with that monitoring in place.

11 Switch types

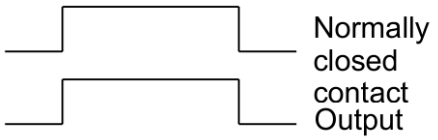
For each switch type: graphic symbol and truth table (left) and timing diagram (right), below logic function (AWL), function block and function. Ö = normally closed, S = normally open, A = output.

Type 1 – eSwitch_1o



eSwitch_1o

Ö	A
0	0
1	1

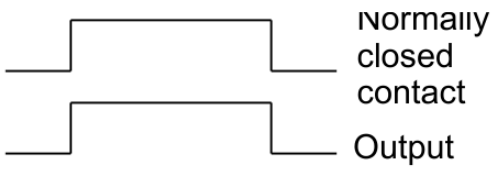


Logic function	Function block	Function
LD E.1 **ST IE.X**		Closing contact (S), only in display opening contact (O)

Type 2 – sSwitch_1s

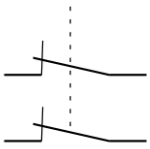
sSwitch_1s

S	A
0	0
1	1



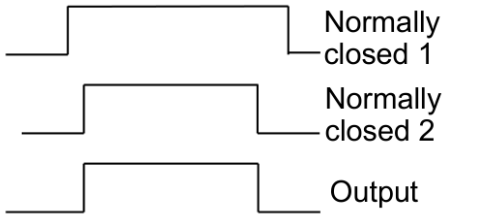
Logic function	Function block	Function
LD E.1 **ST IE.X**		Normally open, as type 1

Type 3 – eSwitch_2o



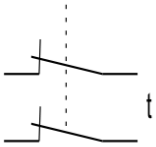
eSwitch_2o

Ö1	Ö2	A
0	0	0
1	0	0
0	1	0
1	1	1



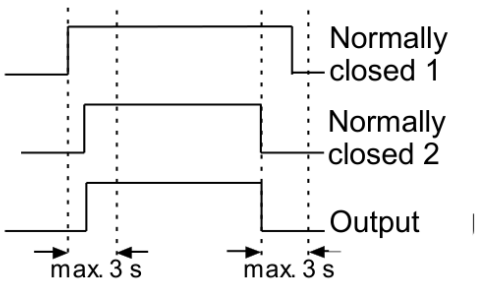
Logic function	Function block	Function
LD E.1 **AND E.2** **ST IE.X**		AND operation of both inputs

Type 4 – eSwitch_2oT



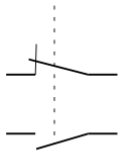
eSwitch_2oT

Ö1	Ö2	A
0	0	0
1	0	0
0	1	0
1	1	1



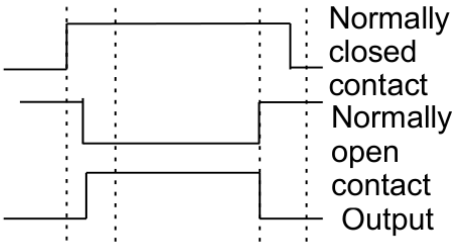
Logic function	Function block	Function
LD E.1 **OR E.2** **ST META_EN.1** **LD E.1** **AND E.2** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Time monitoring MET1..MET4	Like 3, but with time monitoring of state changes. In case of signal changes at S or Ö a complementary signal must follow within a period of t = 3 s. If not, detect fault and A = 0

Type 5 – eSwitch_1s1o



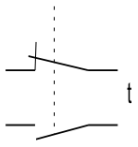
eSwitch_1s1o

S	Ö	A
0	0	0
1	0	0
0	1	1
1	1	0



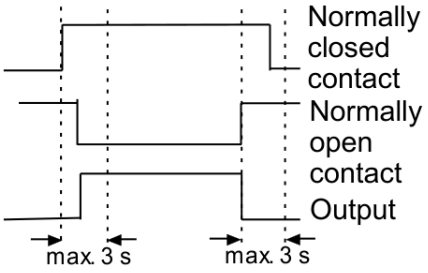
Logic function	Function block	Function
LD E.1 **AND NOT E.2** **ST IE.X**		Monitoring for S = inactive and Ö = active

Type 6 – eSwitch_1s1oT



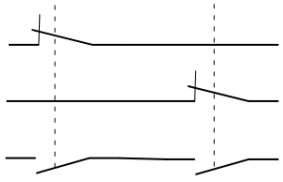
eSwitch_1s1oT

S	Ö	A
0	0	0
1	0	0
0	1	1
1	1	0



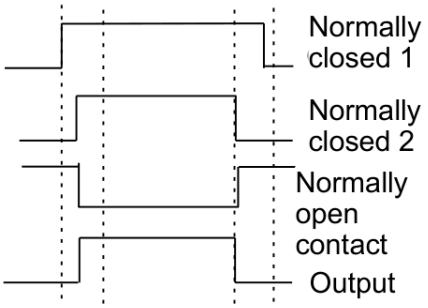
Logic function	Function block	Function
LD E.1 **OR NOT E.2** **ST META_EN.1** **LD E1** **AND NOT E2** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Time monitoring MET1..MET4	Like 5, but with time monitoring of state changes. In case of signal changes at S or Ö a complementary signal must follow within a period of t = 3 s. If not, detect fault and A = 0

Type 7 – eSwitch_2s2o



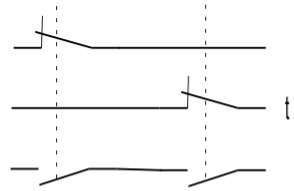
eSwitch_2s2o

S1	Ö1	S2	Ö2	A
1	0	1	0	0
0	1	1	0	0
0	1	0	1	1
1	0	0	1	0



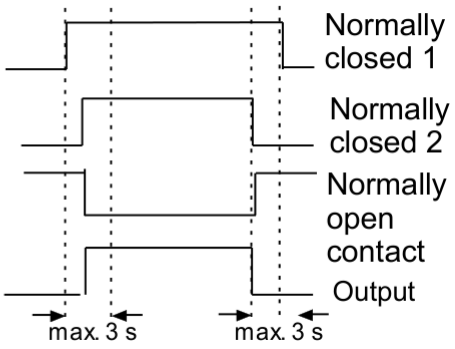
Logic function	Function block	Function
LD E.1 **AND E.2** **AND NOT E.3** **ST IE.X**		Monitoring for S1*S2 = inactive and Ö1*Ö2 = active

Type 8 – eSwitch_2s2oT



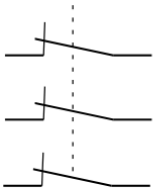
eSwitch_2s2oT

S1	Ö1	S2	Ö2	A
1	0	1	0	0
0	1	1	0	0
0	1	0	1	1
1	0	0	1	0



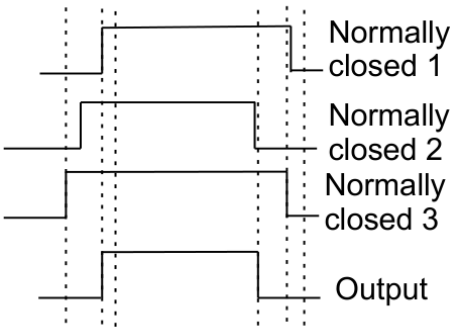
Logic function	Function block	Function
LD E.1 **OR E.2** **OR NOT E.3** **ST META_EN.1** **LD E.1** **AND E.2** **AND NOT E.3** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Time monitoring MET1..MET4	Like 6, but with time monitoring of state changes. In case of signal changes at S (Attention: bus line) or Ö a complementary signal must follow within a period of t = 3 s. If not, detect fault and A = 0

Type 9 – eSwitch_3o



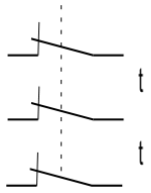
eSwitch_3o

Ö1	Ö2	Ö3	A
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
1	1	1	1



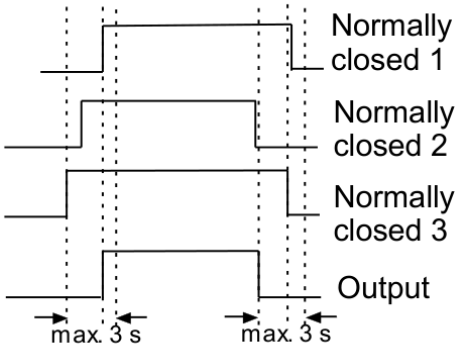
Logic function	Function block	Function
LD E.1 **AND E.2** **AND E.3** **ST IE.X**		AND operation of both inputs

Type 10 – eSwitch_3oT



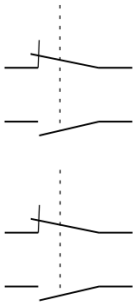
eSwitch_3oT

Ö1	Ö2	Ö3	A
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
1	1	1	1



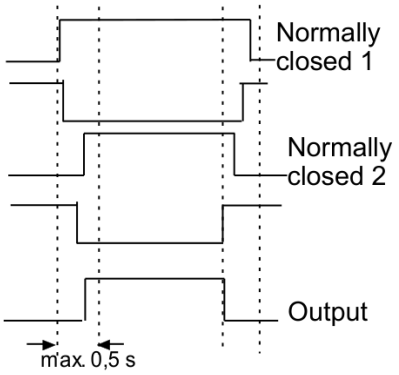
Logic function	Function block	Function
LD E.1 **OR E.2** **OR E.3** **ST META_EN.1** **LD E.1** **AND E.2** **AND E.3** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Time monitoring MET1..MET4	Like 8, but with time monitoring of state changes. In case of signal change on one of the Ö-inputs the other inputs must follow within a period of t = 3 s. If not, detect fault and A = 0

Type 11 – eTwoHand_2o



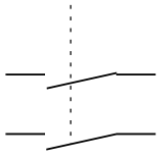
eTwoHand_2o

Ö 1	S 1	Ö 2	S 2	A
0	1	0	1	0
1	0	0	1	0
1	0	1	0	0
0	1	0	1	1



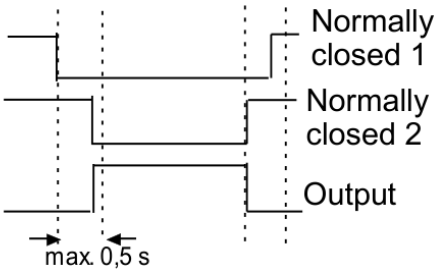
Logic function	Function block	Function
LD NOT E.1 **OR E.2** **OR NOT E.3** **OR E.4** **ST MEZ_EN.1** **LD E.1** **AND NOT E2** **AND E3** **AND NOT E4** **ST MEZ_EN.2** **LD NOT E1** **AND E.2** **AND NOT E3** **AND E.4** **ST MEZ_EN.3** **LD MEZ.1** **ST IE.X**	Two-hand operation MEZ	Monitoring for S1*S2 = inactive and Ö1*Ö2 = active + temporal monitoring of this status. This means that in case of a signal change of an S from 1->0 or Ö from 0->1, the other signals (i.e. further S = 0 or Ö = 1) must follow within a period of 0.5 s. If not, the output = 0. No interference evaluation! No temporal monitoring when changing to inactive state.

Type 12 – eTwoHand_2s



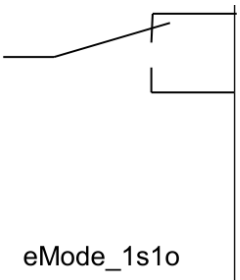
eTwoHand_2s

S1	S2	A
1	0	0
0	1	0
0	0	0
1	1	1



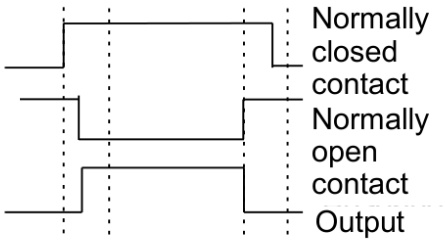
Logic function	Function block	Function
LD E.1 **OR E.2** **ST MEZ_EN.1** **LD NOT E.1** **AND NOT E.2** **ST MEZ_EN.2** **LD E.1** **AND E.2** **ST MEZ_EN.3** **LD MEZ.1** **ST IE.X**	Two-hand operation MEZ	Monitoring for S1*S2 = inactive + temporal monitoring of this status. This means that in case of a signal change of one S from 1->0 the other signal (i.e. another S = 0) must follow within a period of 0.5 s. If not, the output = 0. No interference evaluation! No temporal monitoring when changing to inactive state.

Type 13 – eMode_1s1o



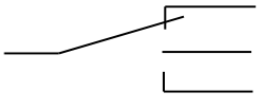
eMode_1s1o

S1	S2	A 1	A 2
1	0	1	0
0	1	0	1
0	0	0	0
1	1	0	0



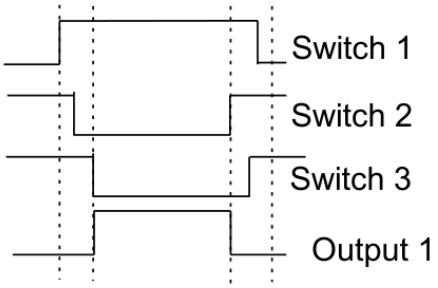
Logic function	Function block	Function
LD E.1 **AND NOT E.2** **ST IE.X1** **LD NOT E.1** **AND E.2** **ST IE.X2**	Selector switch	Clear linkage of permissible switch positions

Type 14 – eMode_3switch



eMode_3switch

S1	S2	S3	A 1	A 2	A 3
1	0	0	1	0	0
0	1	0	0	1	0
0	0	1	0	0	1
1	1	0	0	0	0
1	0	1	0	0	0
0	1	1	0	0	0
1	1	1	0	0	0
0	0	0	0	0	0



Logic function	Function block	Function
LD E.1 **AND NOT E.2** **AND NOT E.3** **ST IE.X1** **LDN E.1** **AND E2** **AND NOT E.3** **ST IE.X2** **LDN E.1** **AND NOT E.2** **AND E.3** **ST IE.X3**	Selector switch	Clear linkage of permissible switch positions

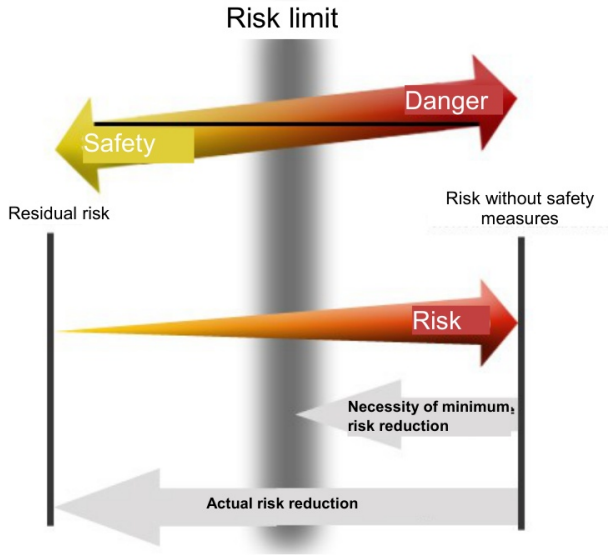
12 Notes on designing, programming, validating and testing safety related applications

The following notes describe the procedure for designing, programming, validating and testing safety related applications.

The information should help the user to classify, to easily understand and to use all steps from risk assessment all the way to the system test. For better understanding the respective subjects, the individual steps are explained by means of examples.

12.1 Risk assessment

The manufacturer of a machine must generally guarantee the safety of any machine designed or delivered by him. The assessment of safety must be based on the applicable and appropriate regulations and standards. Objective of the safety assessment and the measures derived from this must be the reduction of risks for persons down to an acceptable minimum.

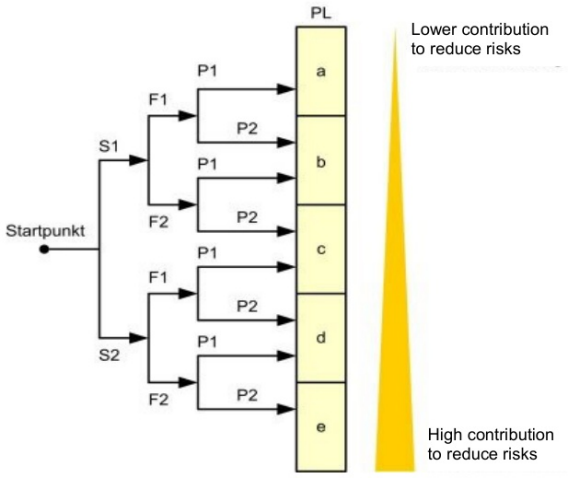


The risk analysis must account for all operating conditions of the machine, such as operation, setup work and maintenance or installation and decommissioning as well as predictable erroneous operation.

The procedure required for the risk analysis and the measures for reducing such risks can be found in the applicable standards

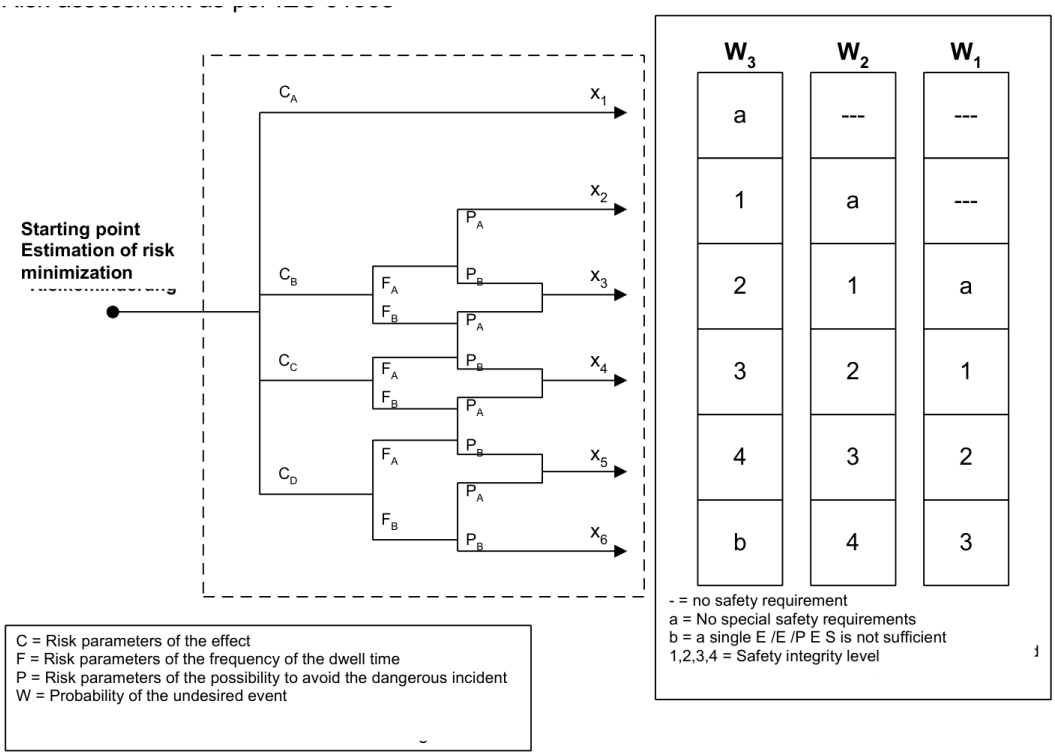
- EN ISO 13849-1 Safety of machines
- IEC 61508 Functional safety of safety related E/E/PE systems.

Risk assessment as per EN ISO 13849-1



Parameter	Meaning
S – Severe physical injury	S1 = minor, reversible injury; S2 = severe, irreversible injury
F – Frequency and/or duration of exposure to danger	F1 = rarely, not cyclic; F2 = frequently up to permanent and/or long duration, cyclic operation
P – Possibility to avoid the danger	P1 = possible, slow movement / acceleration; P2 = hardly possible, high acceleration in case of a fault

Risk assessment as per IEC 61508



The risks to be examined can also be found in applicable regulations and standards, or must be considered separately by the manufacturer based on his specific knowledge of the machine.

For machines sold within the EU the minimum risks to be examined are specified in the EU machine directive 2006/42/EU or in the latest version of this directive.

Further information concerning the risk assessment and the safe design of machines can be found in the standards

- EN 14121 Safety of machines – risk assessment
- EN 12100 Safety of machines – basic terms, general design guidelines

Measures to be applied in order to reduce identified risks must at least be of the same level as the danger itself. The regulations and standards specified above contain examples of such measures and the associated requirements.

12.2 Required technical documents

The manufacturer is obliged to supply various technical documents. The minimum extent is also contained in the applicable regulations and standards. The EU machine directive, for example, requires the delivery of the following documents:

1. The technical file shall comprise the following:
   a) a construction file including:
      - a general description of the machinery,
      - the overall drawing of the machinery and drawings of the control circuits, as well as the pertinent descriptions and explanations necessary for understanding the operation of the machinery,
      - full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the machinery with the essential health and safety requirements,
      - the documentation on risk assessment demonstrating the procedure followed, including:
        i) a list of the essential health and safety requirements which apply to the machinery,
        ii) the description of the protective measures implemented to eliminate identified hazards or to reduce risks and, when appropriate, the indication of the residual risks associated with the machinery,
      - the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,
      - any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorised representative,
      - a copy of the instructions for the machinery,
      - where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery,
      - where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery,
      - a copy of the EC declaration of conformity;
   b) for series manufacture, the internal measures that will be implemented to ensure that the machinery remains in conformity with the provisions of this Directive.

Source BGIA Report 2/2008

The documents must be easy to understand and should be written in the language of the corresponding country.

12.3 Necessary steps for draft, realization and testing

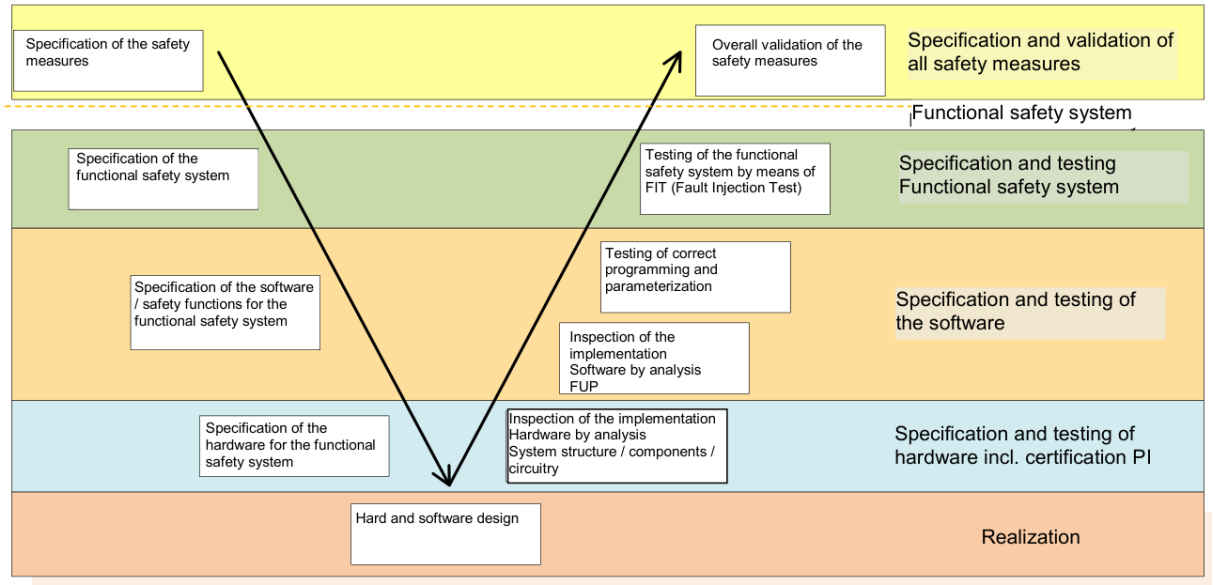
The realization of plant sections with safety related function requires special attention in planning, realization and testing. Also for this the standards (see ISO 13849-2 or EN ISO 61508) contain specific guidelines. The effort thereby is orientated on the complexity of the task for system components with safety related function.

For the realization of such functions the ESMD series offers safety relevant control and monitoring functions to support the system architecture (architecture Cat. 4 acc. to EN ISO 13849-1) and, above all, also the programming language and tested safety functions. Programming uses the form FUP (function plan oriented programming) recommended by the safety standards. It fully meets the requirements on the programming language with limited scope of languages (LVM) for the essential simplifications in documentation and testing.

The individual steps in any case require careful planning and analysis of the methods and systems used. Furthermore, the individual steps must be documented in an understandable way.

V-model (simplified)

The implementation of safety related functions requires a structured approach, like the V-model that is exemplary described in applicable standards. The following shows an exemplary approach for applications with modules of the ESMD series.



12.3.1 Phases of the V-model

Designation	Description design phase	Validation phase
Specification and validation of all passive and active safety measures.	Specification of all safety measures to be applied, such as covers, barriers, max. machine parameters, safety related functions, etc.	Testing of all passive and active safety measures for correct implementation and effectiveness.
Specification of the functional safety systems	Specification of the active safety systems and their assignment to the risks to be reduced, such as e.g. reduced speed in setup operation, stop-mode, monitoring of access areas, etc. Specification of the PLr or the demanded SIL for each individual safety function	Testing of all active safety systems regarding effectiveness and compliance with specific parameters, such as e.g. erroneous increased speed, faulty stop, responding of monitoring facilities, etc. by means of practical tests
Specification of software / safety functions	Specification of the functionality of individual safety functions incl. the definition of the shut-down circuit, etc. Definition of parameters for individual safety functions, such as e.g. max. speed, stop ramps and -categories, etc.	Testing of correct implementation of specified functions by analysis FUP programming. Validation of application programs and parameters by comparing the validation report with FUP or specifications for parameters
Specification of the hardware	Specification of the system structure and the functions of the individual sensors, command units, control components and actuators regarding their safety functions	Testing of the correct implementation of specifications. Determination of the failure probability or PL by means of analysis of the overall architecture and the characteristic data of all components involved, each related to the individual safety functions
Hard and software design	Actual planning and implementation of system structure / wiring. Actual implementation of safety functions by programming in FUP	nil

12.3.2 Specification of safety requirements (structural schematic)

The safety requirements must be individually analysed on the basis of applicable standards, e.g. product standard.

1	**General product and project information**
1.1	Product identification
1.2	Author, version, date, document name, file name
1.3	Contents
1.4	Terminology, definitions, glossary
1.5	Version history and changes
1.6	Directives, standards and technical rules relevant to development
2	**Functional information on the machine, where relevant to safety**
2.1	Intended use and reasonably foreseeable misuse
2.2	Process description (operating functions)
2.3	Operating modes (e.g. setup mode, automatic mode, operation of localized relevance or of parts of the machine)
2.4	Characteristic data, e.g. cycle times, response times, overrun distances
2.5	Other characteristics of the machine
2.6	Safe state of the machine
2.7	Interaction between processes (see also 2.2) and manual actions (repair, setup, cleaning, troubleshooting, etc.)
2.8	Emergency operations
3	**Required Performance Level(s) (PL_r)**
3.1	Reference to existing documentation concerning the hazard analysis and risk assessment for the machine
3.2	Results of the risk assessment for each identified hazard or hazardous situation and specification of the safety function(s) required in each case for risk reduction

4 Safety functions (information applies to each safety function)

- Description of the function ("input – logic – output") including all functional characteristics (refer also to Tables 5.1 and 5.2)
- Activation/deactivation conditions or events (e.g. operating modes of the machine)
- Behaviour of the machine when the safety function is triggered
- Conditions to be observed for re-starting
- Performance criteria/performance data
- Process (timing behaviour) of the safety function, including response time
- Frequency of actuation (i.e. demand rate), recovery time following demand
- Other data
- Adjustable parameters (where provided)
- Classification and assignment of priorities in the event of simultaneous demand for and processing of multiple safety functions
- Functional concept for separation or independence/freedom of reciprocal action from non-safety functions and further safety functions

5 Required information for the SRP/CS design

5.1 Allocation of the SRP/CS and the form of technology by which the safety function is to be implemented; intended equipment

5.2 Selection of the Category, designated architecture (structure) in the form of a safety-related block diagram and description

5.3 Description of the interfaces (process interfaces, internal interfaces, user interfaces, control and display elements, etc.)

5.4 Behaviour at switch-on, implementation of the required starting and restarting behaviour

5.5 Performance data: cycle times, response times, etc.

5.6 Behaviour of the SRP/CS in the event of component failures and faults (achieve and maintain the safe state), including timing behaviour

5.7 Failure modes of components, modules or blocks which are to be considered; where applicable, reasoning for fault exclusions

5.8 Concept for implementation of the detection and control of random and systematic failures (self-tests, test circuits, monitoring arrangements, comparisons, plausibility tests, fault detection by the process, etc.)

5.9 Quantitative aspects

5.9.1 Target values for $MTTF_d$ and DC_{avg}

5.9.2 Switching frequency of components subject to wear

5.9.3 Frequency of measures for fault detection

5.9.4 Mission time, where different from the assumption upon which the intended architecture is based (20 years)

5.10 Operating and limit data (operating and storage temperature range, humidity class, IP degree of protection, resistance values for shock/vibration/EMC, supply data with tolerances, etc.)

5.11 Generic standards to be applied for design (for the equipment, for protection against electric shock/hazardous shock currents, for resistance to environmental conditions, etc.)

5.12 Technical and organizational measures for protected access to safety-related parameters and to SRP/CS characteristics (protection against tampering, access protection, program/data protection) and for protection against unauthorized operation (key switch, code, etc.), for example in non-standard operating modes

5.13 General technical requirements and organizational framework for commissioning, testing and acceptance, and for maintenance and repair

Source: General specification, excerpt from BGIA Report 2/2008 concerning EN ISO 13849-1

Example for an automatic handling machine

Description of function: The automatic handling machine serves the purpose of automatically picking up truck cabins of different heights. After being picked up, the height of the cabin is correctly detected, so that within the working area the cabin cannot be lowered below a certain height. Within the working area the automatic machine must not exceed a maximum speed. Once the cabin has been completely finished, it is put down at the end of the processing line and the automatic handling machine moves along a return track back to the beginning of the track to pick up the next cabin …

Limits of the machine: Spatial limits: The working area must provide sufficient space for the workers, so that they are able to carry out all necessary work on the cabin … In the return pass there must be sufficient space for the empty suspension gear of the automatic handler …

Temporal limits: Description of lifetime, description of ageing processes, which could cause changes of machine parameters (e.g. brakes). Monitoring mechanisms must be implemented for such cases.

Limits of use: The automatic machine automatically fetches new cabins and moves these through a processing area. Workers work in the processing area … etc. The following operating modes are intended: Setup operation, automatic operation and service operation … etc.

Identification of dangers: The following dangers are of relevance with the automatic handling machine: Danger 1: Crushing by cabin / lifting beam falling down; Danger 2: Impact by moving cabin / lifting beam; Danger 3: Crushing by too fast lowering of the cabin in case of a fault; Danger 4: …

Risk analysis: G1: The weight of cabin and lifting beam is so high, that it will cause irreversible crushing or even fatalities. G2: The moving cabin/lifting beam may cause impacts that can lead to irreversible injuries. G3: …

Risk assessment: A risk reduction is required under due consideration of all operating conditions.

Inherently (risk from the project) safe design: Movement of the cabin in direction x and y within the working area cannot be avoided. In the processing area the cabin must be moved up/down … The following measures can be applied: Avoid dangers caused by too fast movements; Avoid dangers caused by too small distances; …

12.3.3 Specification of the functional safety system

Derived from the general danger and risk analysis for the machine, the active safety functions must be identified and specified.

Active safety functions are, e.g. safely reduced speed under certain system conditions, monitored stop and standstill functions, area monitoring facilities, processing of monitoring facilities like light grid, switching mats, etc.

The safety functions must each be delimited and the specific requirements in function and safety level must be defined.

12.3.3.1 Definition of safety functions

Definition of the safety function must:

- specify the risk to be covered,
- describe the exact function,
- list all sensors, command equipment involved,
- specify the control units and
- designate the shut-down circuit mentioned.

The definition should serve as basis for the specification of the hardware and software design.

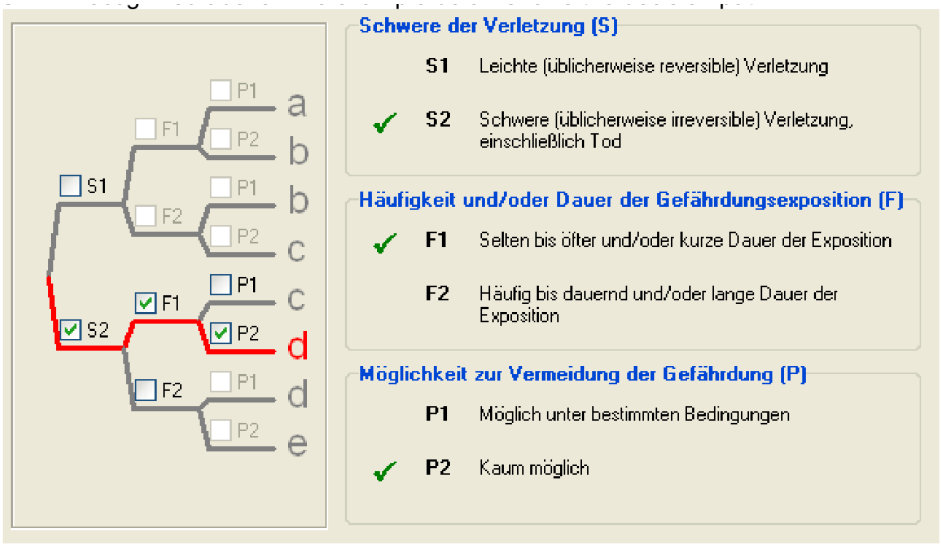
For each of the safety functions defined this way one may need to determine parameters to be used, like e.g. max. system speed in setup operation, etc.

Examples for safety functions:

- SF1: STO (safely switched off torque) to protect against safe starting
- SF2: Safe speeds
- SF3: Safe positions
- SF4: ...

12.3.3.2 Required performance level (PLr) (additional emergency stop)

The required performance level must now be determined on basis of the safety functions SF1 ... recognized above. The example below shows the decision path.



Example for SF1: Result PL = d (source Sistema)

12.3.3.3 Example – Specification of safety functions in form of a table

Cons.-No.	Safety function	Ref from GFA	PLr	Measuring value / sensor	Implementation of software	Nominal parameters	Input / activation	Response / output
1.1	Limitation of max. travel speed to limitation of the maximum speed	2.3	e	1 x WCS absolute encoder; 1 x incremental encoder on motor / drive wheel	Monitoring by means of tested safety function SLS for fixed limits	550 mm/s; fault distance monitoring 200 mm	Permanently	Operation stop; SF 1.7.1

Cons.-No.	Safety function	Ref from GFA	PLr	Measuring value / sensor	Implementation of software	Nominal parameters	Input / activation	Response / output
1.2	Limitation of max. travel speed in working area of workers; monitoring of the maximum speed to < 0.33 m/s	2.4	e	1 x WCS absolute encoder; 1 x incremental encoder on motor / drive wheel	Monitoring by means of tested safety function SLS for fixed limits	60 mm/s; fault distance monitoring 200 mm	Reset: Acknowledgement button	SF 1.7.1
1.3	Limitation of max. travel speed in setup operation; monitoring of the maximum speed to < 0.07 m/s	3.1	d	1 x WCS absolute encoder; 1 x incremental encoder on motor / drive wheel	Monitoring by means of tested safety function SLS for fixed limits	70 mm/s; fault distance monitoring 200 mm	Identification of worker's work area via position of carriage AND NOT Setup; Reset: Acknowledgement button	SF 1.7.1
1.4	Collision protection of carriage; monitoring of the distances between carriages for minimum distance by means of redundant laser distance measurement	2.5	d	2 x laser distance measuring facilities	Monitoring of distances by means of tested SAC function. The analog distance measurements are reciprocally compared for max. tolerance (diagnose of analog sensor); monitored for minimum value (SAC function)	Min distance value 25 % of the max. value of the measuring device.	Operating mode Setup AND button "Bridge safety"; Reset: Acknowledgement button	SF 1.7.1

Cons.-No.	Safety function	Ref from GFA	PLr	Measuring value / sensor	Implementation of software	Nominal parameters	Input / activation	Response / output
1.6.1	Monitoring of carriage sensor system (* the two carriage sensors)	5.1	e	1 x WCS absolute encoder; 1 x incremental encoder on motor / drive wheel	Muting of diagnoses for both carriage sensors by means of tested SCA function. Muting is started before each gap, a faulty encoder value will be temporarily suppressed. Within the gap an encoder value outside 2 to 160000 mm will cause muting.		Pos 1 (7626 - 7850); Pos 2 (11030-1263); Pos 3 (75134-5338); Pos 4 (145562-145622); Pos 5 (143935-143995); Pos 6 (80000-80060)	SF 1.6.2

12.3.4 Software specification

The software specification refers to the previous specification of the safety functions. It can also be replaced by a correspondingly worked out specification of the safety functions, as far as this contains all specifications (see example under 12.3.3.3).

However, it is recommended to prepare an extracted list. This list should contain the following data:

- Designation of safety function
- Description of function
- Parameters, as far as available
- Triggering event / operating status
- Response / output

The specification in detail should be suitable for later validation of the programming.

Example of software specification

Cons.-No.	Safety function	PLr	Measuring value / sensor	Solution new	Input / activation	Response / output
1.4	Monitoring V_Rope to V_Nominal; monitoring of differences between speed of main drive and rope drive for maximum value	d	Digital incremental encoder, tachometer generator rope sheave	Monitoring by means of tested function SLS + SAC with comparison of speed ranges / analog value ranges = comparison for diagnose of the speed detection. Shut-down dual-channel new (see below)	Permanently; Reset: Acknowledgement button	Operation stop SF 1.3.1

Cons.-No.	Safety function	PLr	Measuring value / sensor	Solution new	Input / activation	Response / output
1.6	Backstop; monitoring for reversing	d	Mechanical limit switch 22S2; digital incremental encoder	Monitoring by means of tested function direction monitoring SDI	EMERGENCY (auxiliary contact 28K4 – reversing); Reset: Acknowledgement button	Operation stop SF 1.3.1
1.15	Step-by-step shut-down 3; activation of the safety brake	e	–	Processing of SF in Safe PLC	SF 1.2, SF 1.3.2, SF 1.7, SF 1.8	Setting the safety brake
1.8	Standstill functional	d	Digital incremental encoder	Standstill monitoring by means of tested function SOS	Regulator lock OR set service brake	SF 1.15 / set safety brake
1.9	Direction monitoring	e	Digital incremental encoder	Monitoring by means of tested function direction monitoring SDI	28K1 = FORW., 28K2 = BACK = safe signals from control "Frey"	Operation stop SF 1.3.1

12.3.5 Hardware specification

The hardware specification should describe the entire system design and, in particular, the components used with their specific characteristic data. The hardware specification serves as basis for the determination of the achieved safety level based on the architecture and the characteristic data of all devices involved in a safety function.

Furthermore, the hardware specification should also specify the design measures applied for protecting against systematic and common cause faults.

12.3.5.1 Selection of SRP/CS and operating means

The selection of SRP/CS (Safety related parts of control system) is most suitable to achieve the intended safety level and should be made for any safety function. The components with safety relevant function must be designated in a total overview of the system structure and are to be assigned to the individual safety functions. The safety related code numbers must be determined for these components.

The code numbers cover the following values:

Code	Meaning
MTTFd	mean time to failure, the mean time until a danger imposing failure
DCavg	Mean diagnostic coverage
CCF	common cause failure, a failure caused on a common cause

For an SRP/CS both the software and systematic faults must be taken into consideration.

An analysis of the SRP/CS participating in the safety function must generally be performed in accordance with the schematic Sensor / PES / Actuator.



12.3.5.2 Example for default HW

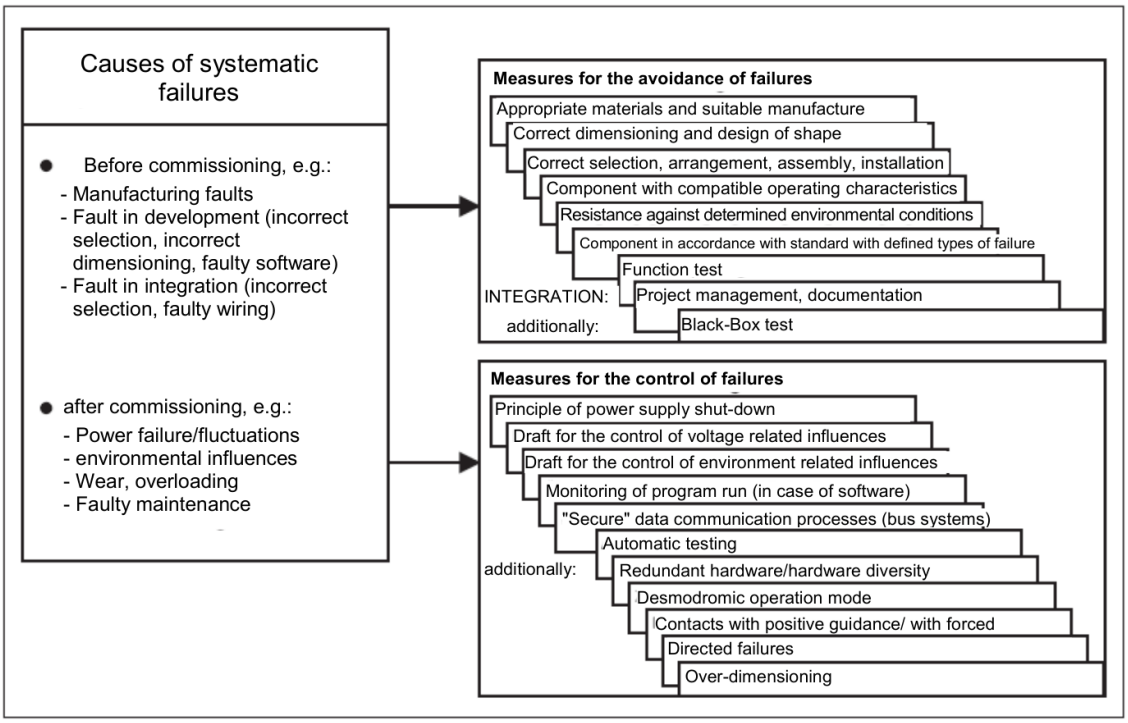
Safety function: Safely reduced speed – SF 2.2 – Safely monitored limited speed with door open

Type	Designation	Function	Design	Characteristics	Note
Sensor	Sensor 1	Door lock – monitoring of the access door	A 3.1	Architecture 4; B10d 100000 (source: data sheet); DC 99 % (source: inst. manual ESMD)	
	Sensor 2.1	Incremental encoder – motor feedback SIN/COS	G 1.1	Architecture 4; MTTFd 30 years (source: gen. specification); DC 99 % (source: inst. manual ESMD)	Cat. 4 in connection with selection ESMD
PES	Safety PLC	Central safety PLC for control and evaluation of safety relevant functions	A 4.1	PFH 1,4 E-8 1/h (source: data sheet ESMD)	
Actuator	STO	Safe Torque Off on inverter	A 5.1	Architecture 4; MTTFd 150 years (source: data sheet inverter); DC 99 % (source: inst. manual ESMD)	Cat. 4 in connection with dual-channel
	Mains contactor	Contactor in mains line of inverter	K 5.1	Architecture 4; B10d 20 E6 (source: data sheet contactor); DC 99 % (source: inst. manual ESMD)	Cat. 4 in connection with dual-channel

12.3.5.3 Consideration of systematic failures

Within the hardware specification one must also consider systematic failures.

Examples for measures against systematic failures: Power drop during operation. If this causes a danger, a power drop must be considered an operating status. The SRP/CS must be able to cope with this condition, so that a safe state is maintained.



Measures against systematic failures acc. to appendix G DIN EN ISO 13849-1 (source BGIA Report 2/2008)

Fault exclusions: If fault exclusions are made for certain devices or system components, these must be individually nominated and specified. Fault exclusions may be e.g. mech. shaft breakage, sticking of switching contacts, short-circuits in cables and lines, etc.

The permissibility of fault exclusions must be justified, e.g. by referencing to permissible fault exclusions acc. to applicable standards, e.g. EN ISO 13849-1. If these fault exclusions require special measures, these must be mentioned.

Examples for fault exclusions and associated measures:

- Positive connection for mechanical shaft connections
- Dimensioning based on sufficient theoretical bases in case of breakage of components in the safety chain.
- Positively guided connection with forced separation in case of sticking of switching contacts.
- Protected routing within switchgear in case of short-circuit in cables and lines, as well as routing of cables in cable ducts.

12.3.6 Hard and software design

The performance targets from the hardware and software specification are implemented in the actual system design.

The performance targets for the components to be used and their wiring from the hardware specification must also be met, the same applies for the performance targets for fault exclusions. Both must be achieved and documented with appropriate means.

In the software one must also account for and completely implement the targets from the software specification.

Furthermore one must consider the superimposed targets placed on the software by safety related programming. These are among others:

- Modular and clear program structure
- Assignment of functions to the safety functions
- Understandable representation of functions by: unambiguous designations, understandable comments
- Use of tested functions / function modules, as far as this is possible
- Defensive programming

12.3.7 Testing of the hardware design

After completing the planning the hardware design must be examined for compliance with the targets from the hardware specification.

Furthermore, one must check the compliance with the specified safety level for each safety function by using suitable analyses. The analysis methods have been described in applicable standards (e.g. EN ISO 13849-1).

Analysis of wiring diagram: Compliance with the targets set under safety related aspects can be checked by means of the wiring diagram and the bill of materials. The following must be checked in particular:

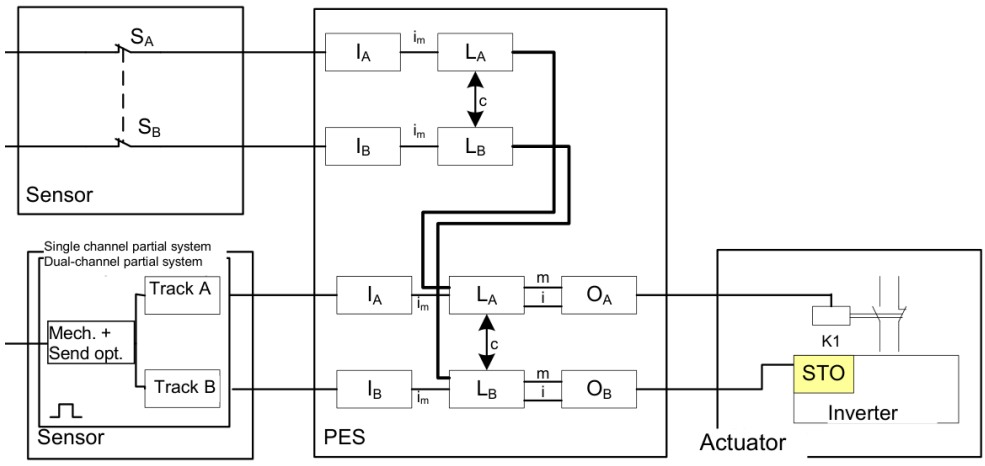
- the correct wiring of components as specified,
- the dual-channel structure, as far as specified,
- the non-reactivity of parallel, redundant channels,
- the use of components as specified,
- the checks should be made by understandable analysis.

Iterative testing of the achieved safety level: The achieved safety level must be determined by means of the circuit structure (= architecture single-channel / dual-channel / with or without diagnose), the characteristic device data (manufacturer's data or appropriate sources) and the diagnostic coverage (manufacturer's data PES or general sources). Appropriate measures can be taken from the underlying safety standard.

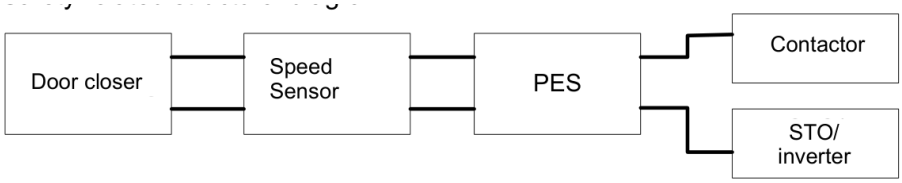
A calculation acc. to EN ISO 13849-1 shall serve as an example:

Safety function: Safely reduced speed with access door open

Structural diagram:



Safety related structural diagram:



Calculation acc. to EN ISO 13849-1:

Channel A – shut-down via mains contactor:

Component	$MTTF_d$ [years]	DC
Door closer[1]	B_{10d} = 100000 n_{op} = 30/AT = 9270/ year (309 AT/ year)	DC_{Switch} = 99%
SIN/COS-encoder	$MTTF_d$ = 30 years	$DC_{Encoder}$ = 99%
PES[2]	$\lambda_d = 1884{,}21$ fit	DC_{PES} = 94,5%
Main contactor[3]	$B_{10d} = 1{,}3 \cdot 10^6$ N_{op} = 20/AT = 6180/year (309 AT/year)	$DC_{Contactor}$ = 60%

$$\mathrm{MTTF_d} = \frac{\mathrm{B_{10d}}}{0{,}1 \cdot \mathrm{n_{op}}} = 107{,}87 \text{ years}$$

$$\mathrm{MTTF_d} = \frac{10^9}{365 \cdot 24 \cdot \lambda_d} = 60{,}59 \text{ years}$$

$$\mathrm{MTTF_d} = \frac{\mathrm{B_{10d}}}{0{,}1 \cdot \mathrm{n_{op}}} = 2103{,}56 \text{ years}$$

$$\mathrm{MTTF_d^A} = \frac{1}{\frac{1}{\mathrm{MTTF_d^{Switch}}} + \frac{1}{\mathrm{MTTF_d^{Encoder}}} + \frac{1}{\mathrm{MTTF_d^{PES}}} + \frac{1}{\mathrm{MTTF_d^{Contactor}}}} = 16{,}78 \text{ years}$$

1 Value for MTTFd acc. to EN ISO 13849-1, Table C.1 · 2 Value from company internal HW FMEA · 3 Value for MTTFd from EN ISO 13849-1, Table C.1; assumption "worst case" by "contactor with nominal load"

Channel B – shut-down via STO/inverter:

Component	$MTTF_d$ [years]	DC
Door closer	B_{10d} = 100000 n_{op} = 30/AT = 9270/year (309 AT/year) $MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = 107{,}87$ years	DC_{Switch} = 99%
SIN/COS-encoder	$MTTF_d$ = 30 years	$DC_{Encoder}$ = 99%
PES	$\lambda_d = 1884{,}21$ fit $MTTF_d = \frac{10^9}{365 \cdot 24 \cdot \lambda_d} = 60{,}59$ years	DC_{PES} = 94,5%
STO/converter	$MTTF_d$ = 150 years	DC_{STO} = 90%

Resulting PL for both channels:

Symmetry of both channels	$MTTF_d = \frac{2}{3}\left[MTTF_d^A + MTTF_d^B - \frac{1}{\frac{1}{MTTF_d^A} + \frac{1}{MTTF_d^B}}\right] = 16{,}00$ years
DC mean value	$DC_{avg} = \frac{\sum_i \frac{DC_i}{MTTF_i}}{\sum_i \frac{1}{MTTF_i}} = 97{,}2\ \%$
PL	$MTTF_d$ = 16 years = average DC avg = 97,4 % = average PL =“d“ (from EN ISO 13849-1, tables 5, 6 and 7) In this case the B10d value of the door monitoring feature is determining for PL. If an even higher safety level is to be reached, a correspondingly higher qualitative switch is to be used.

Note: The characteristic values of the individual components are examples and must be adjusted accordingly to user applications.

Note The PL can also be determined with the program tool "Sistema" from BGIA.

12.3.8 Verification software (program) and parameters

Verification takes place in two steps:

- Checking the FUP with respect to the specified functionality.
- Checking the FUP against the AWL-listing of the validation report, or the default parameters against the one listed in the validation report.

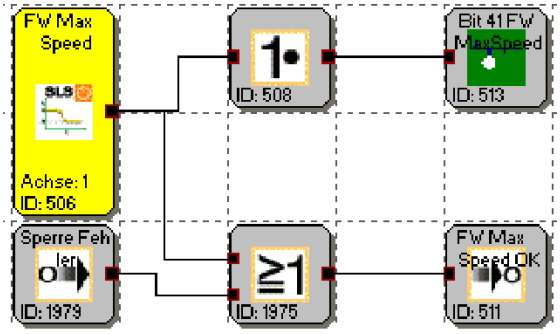
12.3.8.1 Checking FUP

The programmed FUP must be compared with the defaults in the specification.

Note The comparison is all the more efficient the more clearly the programming has been structured with respect to the safety functions.

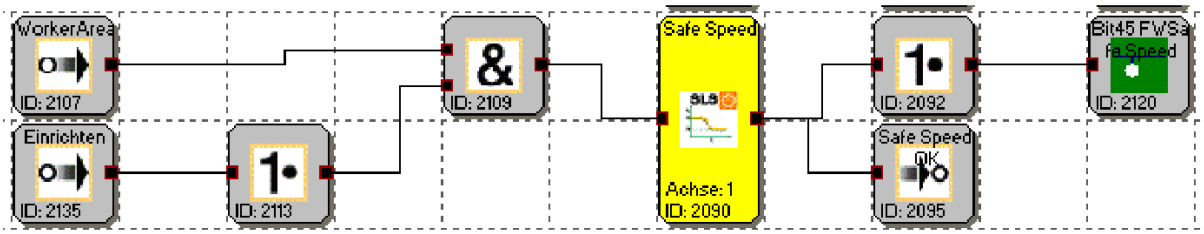
Example – Safety function: 1.1 Limitation of the max. travel speed of the carriage to 1.1 VMax; Monitoring of the maximum speed to < 1.1 VMax

FW Max Speed OK (ID 548) (is bridged by available gap): FW Max Speed is permanently activated and responds when a speed of 550 mm/s is exceeded.



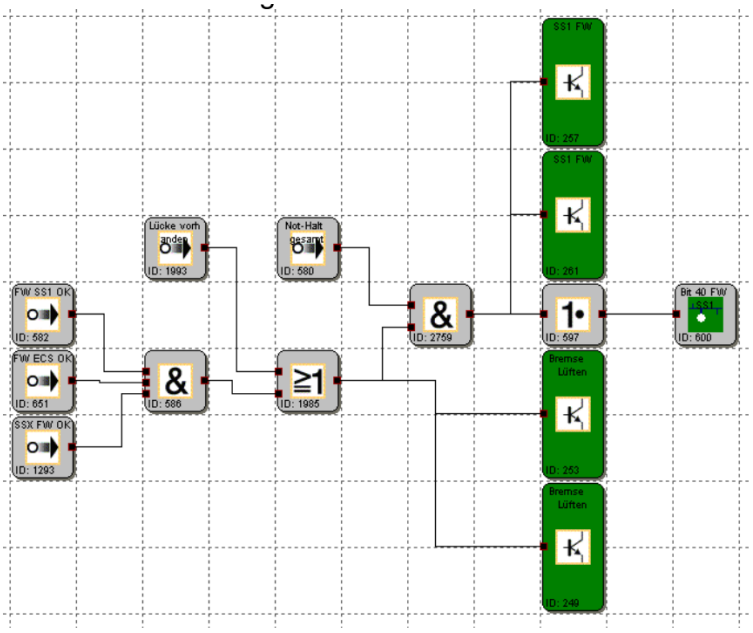
Safety function: Limitation of max. travel speed in carriage in the worker's area; Monitoring of the maximum speed to < 0.33 m/s

Safe Speed OK (ID 2124) (is bridged by available gap): Safe Speed OK responds when the safe speed SLS (ID 2090) is exceeded in the worker's area and during setup work.



Parameter SLS Safe Speed: 60 mm/s, no further parameters

Safety function: Carriage shut down; shut down of travel system and deactivation of brakes; shut down on carriage



The carriage is switched off via two outputs (IQQ1.5 ID 257 and 1.6 ID 261).

The brakes are released via two outputs (IQQ1.3 ID 253 and 1.4 ID 249).

The PLC receives a message concerning bit 40 (ID 600).

In case of an emergency stop the shut-down takes place immediately.

Lift – Safety function: Emergency stop switch inputs and shut-down outputs; 1.1 Emergency stop head control

Dual-channel emergency stop with pulse monitoring. If an emergency stop is triggered at the imposed control, this emergency stop can be bridged if the approval "Bridge safety" has been issued. Emergency stop button head control: Emergency stop contacts from emergency stop relay with pulsing from the module.

12.3.8.2 Validation of FUP against AWL and parameters with validation reports

The programming that took place in the FUP must be compared with the AWL-listing of the validation report.

Example AWL-listing in validation report (Validation report – PLC program)

Index	Command	Operand	validated
1	**S1**	**SLI_EN.1**	
2	**S1**	**SLI_EN.2**	
3	**S1**	**SLI_EN.3**	
4	**S1**	**SCA_EN.1**	
5	**S1**	**SCA_EN.2**	
6	**S1**	**SCA_EN.3**	
7	**S1**	**SLS_EN.2**	
8	**S1**	**SCA_EN.4**	
9	**S1**	**SLS_EN.3**	
10	**S1**	**SLS_EN.4**	
11	**S1**	**SLI_EN.5**	
12	**SQH**		
13	**LD**	**E0.1**	
14	**ST**	**MX.2**	
15	**SQC**		
16	**SQH**		
17	**LD**	**E0.3**	
18	**AND**	**E0.4**	
19	**ST**	**MX.3**	
20	**SQC**		

Step-by-step testing is recommended. The better the test, the more structured the programming in FUP has been made.

After checking the program one must also check the parameters against the targets set in the specifications by means of comparison.

Example SLS: Validation report – Safe Limited Speed (SLS)

Index	Parameters	Value		validated
SLS - 0	Chosen axis:	1		
	Speed threshold:	2	0	
SLS - 1	Chosen axis:	1		
	Speed threshold:	500	0	
SLS - 2	Chosen axis:	1		
	Speed threshold:	2	0	
	Acceleration threshold:	2	0	
SLS - 3	Chosen axis:	1		
	Speed threshold:	2	0	
	Assigned SSX-ramp:	0		

Example encoder configuration: Validation report – Axis configuration / sensor interface – Axis 1

General parameters	Value	
Measuring distance:	500	0
Type: Rotational	No	
Position processing:	Activ	
Maximum speed:	2000	0
Incremental shut-down:	10000	0
Shut-down speed:	100	0

Sensors	0	0
Type:	SSI-standard	SSI-standard
Format:	Binary	Binary
Direction of rotation:	Ascending	Ascending
Supply voltage:	0	0
Resolution:	1024 Steps/1000mm	64 Steps/1000mm
Offset:	0 Steps	0 Steps

- General parameters correctly configured
- Parameter sensor 1 correct
- Parameter sensor 2 correct

12.3.9 Performance of the system test / FIT (fault injection test)

For the FIT the manufacturer must prepare a complete list of the functions to be tested. This list includes the defined safety functions as well as the fault test for checking the right response of the SRP/CS to this fault.

Example test list:

No	Setup	Test	Result
1 Test SLS for max. speed in setup operation	Activate setup operation; travel with maximally allowed speed	Diagnose of the actual speed versus the SLS limit; manipulation of the setup speed beyond the permitted reduced speed	
2 Test SSX for Stop-category 2	Travel with max. speed; actuate the emergency stop	Diagnose of the SSX-ramp against the actual deceleration ramp; setting an impermissible weak deceleration; moving the axis after standstill is reached by manipulating the drive	
3 Test of the dual-channel door monitoring	Select operating mode for setup operation	Diagnose of inactive monitoring with door closed (using diagnostics function FUP); diagnose of active monitoring with door open (using diagnostics function FUP); disconnecting one channel and opening the door; generate cross-shorting between both inputs	

Appendix A Classification of switch types

Note The individual switches of the following input elements can be assigned to the digital inputs DI1 to DI8 as desired.

Enable switch

Switch type	Comment	Classification PL acc. to EN ISO 13849-1	Classification SIL acc. to IEC 61508
1 normally closed	Enable switch standard	PL d	SIL 2
1 normally open	Enable switch standard	PL d	SIL 2
2 normally closed	Enable switch higher requirements	PL e	SIL 3
2 normally closed time monitored	Enable switch monitored	PL e	SIL 3

Emergency Stop

Switch type	Comment	Classification category	Classification SIL
1 normally closed	Emergency Stop standard	PL d 1)	SIL 2
2 normally closed	Emergency stop higher requirements	PL e	SIL 3
2 normally closed time monitored	Emergency Stop monitored	PL e	SIL 3

1) Fault exclusions and boundary conditions acc. EN 13849-2 must be observed!

Door monitoring

Switch type	Comment	Classification category	Classification SIL
2 normally closed	Door monitoring higher requirements	PL e	SIL 3
2 normally closed time monitored	Door monitoring monitored	PL e	SIL 3
1 normally open + 1 normally closed	Door monitoring higher requirements	PL e	SIL 3
1 normally open + 1 normally closed time monitored	Door monitoring monitored		SIL 3
2 normally open + 2 normally closed	Door monitoring higher requirements	PL e	SIL 3
2 normally open + 2 normally closed time monitored	Door monitoring monitored	PL e	SIL 3
3 normally closed	Door monitoring higher requirements	PL e	SIL 3
3 normally closed time monitored	Door monitoring monitored	PL e	SIL 3

Two-hand button

Switch type	Comment	Classification category	Classification SIL
2 two-way switch	Two-hand button higher requirements	Type III C PL e	SIL3
2 normally open	Two-hand button monitored	Type III A PL e	SIL1

Note: With these input elements a fixed pulse assignment takes place, which cannot be influenced by the user!

Light curtain

Switch type	Comment	Classification category	Classification SIL
2 normally closed	Light curtain higher requirements	PL e	SIL 3
2 normally closed time monitored	Light curtain monitored	PL e	SIL 3
1 normally open + 1 normally closed	Light curtain higher requirements	PL e	SIL 3
1 normally open + 1 normally closed time monitored	Light curtain monitored	PL e	SIL 3

Mode selector switch

Switch type	Comment	Classification category	Classification SIL
2 positions	Mode selector switch monitored	PL e	SIL 3
3 positions	Mode selector switch monitored	PL e	SIL 3

Safety note When changing the status of the switch, the program to be created with the programming software must ensure that the outputs of the module are deactivated (Note: Standard 60204-Part1-Paragraph 9.2.3).

Sensor

Switch type	Comment	Classification category	Classification SIL
1 normally closed	Sensor input standard	PL d	SIL 2
1 normally open	Sensor input standard	PL d	SIL 2
2 normally closed	Sensor input higher requirements	PL e	SIL 3
2 normally closed time monitored	Sensor input monitored	PL e	SIL 3
1 normally open + 1 normally closed	Sensor input higher requirements	PL e	SIL 3
1 normally open + 1 normally closed time monitored	Sensor input monitored	PL e	SIL 3

Start- / reset element

Switch type	Comment	Classification category	Classification SIL
1 normally open	Alarm reset standard (evaluation of edge)	–	–
1 normally open	Logic reset standard	PL d	SIL 2
1 normally open	Start monitoring standard (optional function)	–	–

Note: The alarm reset input can be operated with 24 V continuous voltage and is edge triggered.