rexroth
A Bosch Company

ILC
MLC 15VRS

SafeLogic System Overview

Project Planning Manual
R911400164

Edition 02

Title	ILC MLC 15VRS SafeLogic System Overview
Type of Documentation	Project Planning Manual
Document Typecode	DOK-MLC***-SL**SYS*V15-PR02-EN-P
Internal File Reference	RS-dfa58d0ad80812290a347e8653619564-2-en-US-3
Change Record	Edition 02, 2021-04 Refer to chapter 1.1 "Change record" on page 1
Copyright	© Bosch Rexroth AG 2021 All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Liability	The specified data is intended for product description purposes only and shall not be deemed to be a guaranteed characteristic unless expressly stipulated in the contract. All rights are reserved with respect to the content of this documentation and the availability of the product.
Editorial Department	Engineering Automation Systems Solution Integration PLC, Safety controls, AnSt (MiNi/PiaSt)

Table of Contents

Page

Page

Page

1 About this documentation

1.1 Change record

Editions of this documentation

Edition	Release date	Note
01	2020-11	First edition
02	2021-04	Revision for version 15V12

Tab. 1-1: Change Record

1.2 Purpose

This project planning manual provides an overview of the safety technology system solutions by Bosch Rexroth. This project planning manuals describes the Safety control SafeLogic compact and the Safety extension module.

The Bosch Rexroth Safety extension module is a safety component. It only becomes a safety control system in connection with an XM or VPx control.

The Safety extension module is available in the following specifications:

- MLC SafeLogic (IoT-compatible PLC system ILC and Motion control system MLC)
- MTX SafeLogic (CNC system)

SafeLogic compact is a modular, scalable Safety control. SafeLogic compact can be operated without a superordinate control.

☞ The project planning manual supports the user in selecting, configuring and designing the Safety control. The manual is only valid in connection with the SafeLogic basic documentation as well as operating instructions, project planning manuals and assembly instructions about safety controls and connected hardware components, see chapter 1.4 "Required and supplementing documentation" on page 2

This project planning manual does not provide any instructions on the operation of a machine in which a Safety control is integrated in. For information on the operation, refer to the instructions of the respective machine.

1.3 Overview on target groups and product phases

In the following illustration, the framed activities, product phases and target groups refer to the present documentation.

Example: In the product phase "Selection", the target group "Design engineer" can execute the activities "Select, Prepare, Design, Construct" using this documentation.

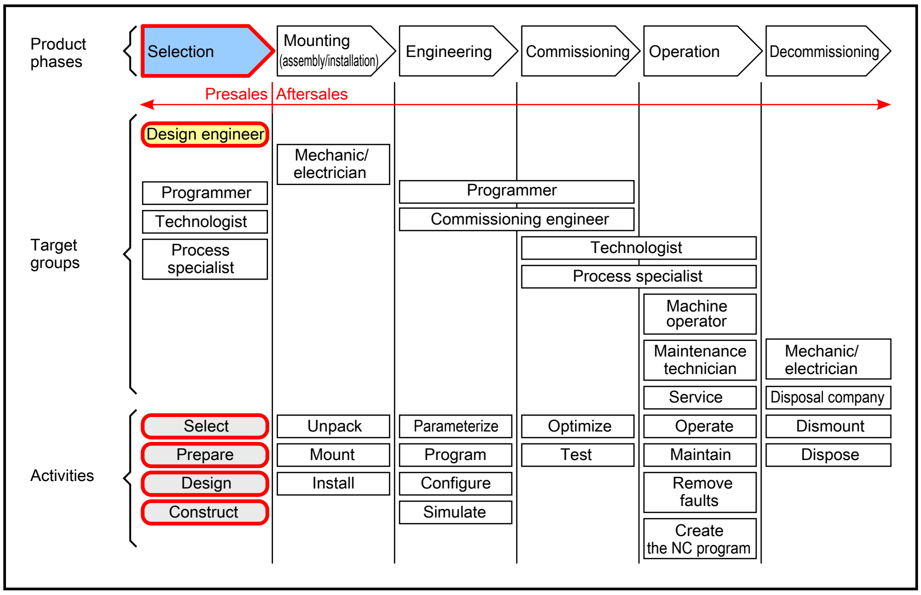


Fig. 1-1: Assigning this documentation to the target groups, product phases and target group activities

Qualification

Required qualification: Individual who is able to assess the tasks assigned and to identify possible safety risks owing to qualification in the subject, knowledge and experience. The individual should also be familiar with the standards and regulations.

Availability

This project planning manual is not part of the product delivery.

1.4 Required and supplementing documentation

1.4.1 SafeLogic/Safe Motion

Document	Part number, document type	Description
SafeLogic documentation		
IndraWorks SafeLogic 15VRS First Steps	R911400170 Commissioning Manual	This documentation contains a description for the creation of a 15VRS control project to commission a SafeLogic control.
IndraWorks SafeLogic 15VRS Project Configuration	R911398635 Application Description	This documentation describes the creation and the programming of SafeLogic projects in IndraWorks Engineering
ILC MLC 15VRS SafeLogic System Overview	R911400164 Project Planning Manual	This project planning manual describes the SafeLogic compact Safety control and the Safety extension module when using an IoT-compatible PLC system ILC and Motion Control system MLC SafeLogic
MTX 15VRS SafeLogic System Overview	R911398637 Project Planning Manual	This project planning manual describes the SafeLogic compact Safety control and the Safety extension module when using a CNC system MTX
Safe Motion documentations		

Document	Part number, document type	Description
Rexroth IndraDrive Integrated safety technology "Safe Torque Off" (from MPx-16)	R911332634 Application Description	This documentation describes the "Safe Torque Off" safety technology integrated in IndraDrive
IndraDrive Integrated safety technology "Safe Motion" (from MPx-18)	R911338920 Application Description	This documentation describes the "Safe Motion" safety technology integrated in IndraDrive

Tab. 1-2: SafeLogic/Safe Motion documentations

1.4.2 SafeLogic hardware

Document	Part number, document type	Description
Safety extension module		
IndraControl XFE01.1-SY-01 Safety extension module for XM devices	R911376654 Operating Instructions	This operating instructions provides information on the safe mounting and the electric installation of the Safety extension module for XM controls to the technical staff of the machine manufacturer or the machine operator
IndraControl PFC01.1-SY-01 Safety extension module for VPx devices	R911373152 Operating Instructions	This operating instructions provides information on the safe operation of the Safety extension module in the IndraMotion MLC VPx control to the technical staff of the machine manufacturer or the machine operator
Standard controls		
IndraControl XM21/XM22	R911340667 Operating Instructions	This documentation describes the IndraControl XM21/XM22 controls.
IndraControl XM42	R911345566 Operating Instructions	This documentation describes the IndraControl XM42 controls.
IndraControl VPx (based on VPB40.4)	R911383090 Operating Instructions	This documentation describes the MLC IndraControl VPx controls on the basis of the box PC VPB40.4
Bus coupler		
Rexroth Inline Bus Coupler for PROFIBUS-DP R-IL PB BK DI8 DO4/CN-PAC	R911324349 Application Description	This documentation describes the Rexroth Inline bus coupler R-IL PB BK DI8 DO4/CN-PAC
Rexroth Inline Bus Coupler for Profibus DP with Digital Inputs and Outputs R-IL PB BK DI8 DO4/CN-PAC	R911324351 Data Sheet	Contains the technical data of the Rexroth Inline bus coupler R-IL PB BK DI8 DO4/CN-PAC
Rexroth Inline Bus Coupler for PROFINET with digital Inputs and Outputs R-IL PN BK DI8 DO4-PAC	R911328682 Data Sheet	Contains the technical data of the Rexroth Inline bus coupler R-IL PN BK DI8 DO4-PAC

Document	Part number, document type	Description
Rexroth IndraControl S20 Bus Coupler for Profinet	R911342784 Data Sheet	This documentation describes the Rexroth S20 Profinet bus coupler S20-PN-BK+
IndraControl S20 bus coupler for Sercos	R911342782 Data Sheet	This documentation describes the Rexroth S20 Sercos bus coupler S20-S3-BK+
IndraControl S20 bus coupler for PROFIBUS-DP	R911343914 Application Description	This documentation describes den Rexroth S20 PROFIBUS-DP bus coupler S20-PB-BK
I/O modules with safe inputs/outputs		
Rexroth Inline Module with Safe Digital Inputs R-IB IL 24 PSDI 8-PAC	R911326026 Application Description	This documentation describes the Rexroth Inline module R-IB IL 24 PSDI 8-PAC
Rexroth Inline Module with Safe Digital Outputs R-IB IL 24 PSDO 8-PAC	R911326028 Application Description	This documentation describes the Rexroth Inline module R-IB IL 24 PSDO 8-PAC
Rexroth Inline Module with Safe Digital Outputs R-IB IL 24 PSDO 4/4-PAC	R911336653 Application Description	This documentation describes the Rexroth Inline module R-IB IL 24 PSDO 4/4-PAC
Rexroth Inline Module with Safe Digital Relay Outputs R-IB IL 24 PSDOR 4-PAC	R911336651 Application Description	This documentation describes the Rexroth Inline module R-IB IL 24 PSDOR 4-PAC
IndraControl S20 module with safe digital Outputs S20-PSDO-8/3	R911369164 Application Description	This documentation describes the Rexroth S20 module S20-PSDO-8/3 (PROFIsafe)
IndraControl S20 module with safe digital Inputs S20-PSDI-8/4	R911369168 Application Description	This documentation describes the Rexroth S20 module S20-PSDI 8/4 (PROFIsafe)
IndraControl S20 module with safe digital Outputs S20-SSDO-8/3	R911342482 Application Description	This documentation describes the Rexroth S20 module S20-SSDO-8/3 (CSoS)
IndraControl S20 module with safe digital Inputs S20-SSDI-8/4	R911342480 Application Description	This documentation describes the Rexroth S20 module S20-SSDI 8/4 (CSoS)

Tab. 1-3: SafeLogic hardware documentations

1.4.3 IndraWorks/WebAssistant

Document	Part number, document type	Description
IndraWorks 15VRS Software Installation	R911393450 Commissioning Manual	This documentation describes the IndraWorks installation.
IndraWorks 15VRS Engineering	R911393303 Application Description	This documentation describes the use of IndraWorks in which the Rexroth Engineering tools are integrated. It includes instructions on how to work with IndraWorks and how to operate the oscilloscope function.
IndraWorks 15VRS PLC Programming System IndraLogic 2G	R911396137 Application Description	This documentation describes the PLC programming tool IndraLogic 2G and its use. The documentation includes the basic use, first steps, visualization, menu items and editors.
IndraWorks 15VRS Basic Libraries, IndraLogic 2G	R911398633 Library	This documentation describes the system-comprehensive PLC libraries.
IndraWorks 15VRS Field buses	R911393284 Application Description	This documentation describes the field bus and local periphery connections supported by the MLC and MTX systems. The focus of this documentation lies in the configuration, parameterization, commissioning and diagnostics of different periphery connections. It is the basis for the online help.
IndraWorks 15VRS Field Bus Libraries	R911393275 Library	This documentation describes the field bus libraries for the IndraLogic ILC, IndraMotion MLC and IndraMotion MTX systems
IndraWorks 14VRS HMI	R911343569 Application Description	This documentation describes the functions, configuration and operation of the user interfaces IndraWorks HMI Engineering and IndraWorks HMI Operation.
WebAssistant	R911381469 Application Description	This documentation describes the WebAssistant. The WebAssistant is a web-based diagnostic tool used to access a control system via an Ethernet high-speed connection. The WebAssistant allows OEMs, end users and service engineers to access and to remotely diagnose a system.

Tab. 1-4: IndraWorks/WebAssistant documentations

1.4.4 SafeLogic compact

Document	Part number, document type	Description
IndraControl SafeLogic compact Designer software	R911332749 Operating Instructions	Instructs technical staff of the machine vendor on how to configure the software and on how to operate and diagnose a SafeLogic compact system with the SafeLogic Designer software
IndraControl SafeLogic compact Hardware	R911332746 Operating Instructions	Instructs the technical staff of the machine vendor and the machine operator on safe assembly, electrical installation, commissioning as well as maintenance of the SafeLogic compact Diagnostic Gateway
Rexroth IndraControl SafeLogic compact Diagnostic Gateways	R911332752 Operating Instructions	Describes the SafeLogic compact diagnostic gateways and their functions in detail
IndraControl SafeLogic compact Sercos Gateway	R911338436 Project Planning Manual	Instructs the technical staff of the machine vendor and the machine operator on safe assembly, configuration, electrical installation, commissioning as well as maintenance of the SafeLogic compact Sercos Gateway
Safety controls network solutions SafeLogic compact	R911332754 Safety instructions	These safety instructions provide information to the planner, developer and operator as well as persons installing the protective equipment in a machine/system, and initially commission and operate it

Document	Part number, document type	Description
SLC-3-GS3S00300 SafeLogic compact Sercos Gateway	R911339570 Assembly Instructions	This assembly instruction describes the assembly of the modules of the SafeLogic compact Safety control
SLC-0-GPNT00300 SafeLogic compact Ethernet Gateway Profinet I/O	R911334404 Assembly Instructions	
SLC-0-GPRO00300 SafeLogic compact Profibus Gateway	R911334403 Assembly Instructions	
SLC-3-MOC000300 SafeLogic compact Motion Control Module	R911343758 Assembly Instructions	
SLC-3-CPU000300/ SLC-3-CPU130302/ SLC-3-CPU320302 SafeLogic compact Main Modules	R911334402 Assembly Instructions	
SLC-3-XTDI80302/SLC-3-XTIO84302/ SLC-3-XTDS84302/SLC-0-STIO68302 SafeLogic compact Extension modules	R911334401 Assembly Instructions	
SLC-A-UE410-2RO4/ SLC-A-UE410-4RO4 SafeLogic compact Digital Output Modules	R911334400 Assembly Instructions	
SLC-A-MOC-MFSB-RX/ SLC-A-MOC-DECB-RX SafeLogic compact Encoder Junction Boxes	R911343761 Assembly Instructions	

Tab. 1-5: SafeLogic compact documentation

1.5 Documentation structure

The first part of the document provides important instructions on use and safety (chapter 2 "About safety" on page 11).

chapter 3 "Introduction in the Safety technology" on page 15 provides a short introduction in the Safety technology.

chapter 4 "System overview" on page 43 contains an overview of the SafeLogic components.

The chapter is structured as follows:

- Areas of application
- System requirements
- Safety controls

- Safe communication
- System structure
- System solutions

chapter 5 "Safe bus systems" on page 55 describes the safe data transfer in Bosch Rexroth Safety systems.

chapter 6 "Development interface" on page 81 describes the available development interfaces for configuration and commissioning.

chapter 7 "Commissioning" on page 95 contains information about the commissioning of SafeLogic components.

chapter 8 "Diagnostics and trouble shooting" on page 111 describes the options for diagnostics and trouble shooting for a Safety system.

For information on the Bosch Rexroth customer service help desk, refer to chapter 9 "Service and support" on page 123.

1.6 Information representation

1.6.1 Safety instructions

If there are safety instructions in the documentation, they contain certain signal words ("Danger", "Warning", "Caution", "Notice") and sometimes a safety alert symbol (according to ANSI Z535.6-2006).

The signal word draws attention to the safety instruction and indicates the risk potential.

The safety alert symbol (triangular safety reflector with exclamation marks), preceding the signal words "Danger", "Warning", "Caution" indicates hazards for persons.

The safety instructions are represented as follows in this documentation:

⚠ DANGER

In case of non-compliance with this safety instruction, death or serious injury **will** occur.

⚠ WARNING

In case of non-compliance with this safety instruction, death or serious injury **can** occur.

⚠ CAUTION

In case of non-compliance with this safety instruction, minor or moderate injury can occur.

NOTICE

In case of non-compliance with this safety instruction, material damage can occur.

1.6.2 Symbols used

Note Notes are represented as follows:

☞ This is a note for the user.

Tip

Tips are represented as follows:

💡 This is a tip for the user.

1.6.3 Terms and abbreviations

Term	Explanation
IndraWorks Engineering Framework	Project planning and commissioning tool of Bosch Rexroth
SafeLogic Designer	Project planning and commissioning tool of Bosch Rexroth for SafeLogic compact components
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
DIN	German Institute for Standardization (Deutsches Institut für Normung e. V.
ISO	International Organization for Standardization
IndraDrive	Drive controller
Sercos	Sercos (Serial Realtime Communication System) is a world-wide standardized digital interface used for communication between controls and drives

Tab. 1-6: Names and abbreviations used

1.6.4 Customer feedback

Customer requests, comments or suggestions for improvement are of great importance to us. Please email your feedback on the documentations to Feedback.Documentation@boschrexroth.de. Directly insert comments in the electronic PDF document and send the PDF file to Bosch Rexroth.

2 About safety

2.1 General information

This chapter deals with your own safety and the safety of the equipment operators.

Read this chapter carefully before working with either a Safety control or a machine protected by a Safety control.

2.2 Qualified safety personnel

Only qualified staff is permitted to mount, commission and maintain the Safety control.

Qualified safety personnel are defined as persons who …

- have undergone the appropriate technical training

and

- have been instructed by the responsible machine operator in the operation of the machine and the current valid safety guidelines

and

- have access to the instructions, project planning manuals and assembly instructions about the Safety control and have read and acknowledged the instructions, project planning manuals and assembly instructions

and

- have access to the instructions to the safety devices connected to the Safety control (e.g. light arrays) and have to have read and acknowledge these instructions

2.3 Use cases of the devices

The modular safety control SafeLogic compact and the Safety extension modules XFE01.1-SY-01 (for XM controls) and PFC01.1-SY-01 (for VPx controls) can be used…

- acc. to IEC 61 508 to SIL3
- acc. to EN 62 061 to SILCL3
- acc. to EN ISO 13 849-1 up to category 4 and Performance Level e

The actual degree of safety depends on the external wiring, the wiring design, the parameterization, the selection of the command initiators and their locations at the machine.

2.4 Intended use

☞ The Safety controls comply with the requirements of class A (industrial applications) according to the "emission" standard.

The Safety controls are thus only suitable for the use in the industrial environment and not in the private sector.

NOTICE **Material damage to Safety control components!**

Safety controls can only be used within their specified operating limits (voltage, temperature, etc.).

Any warranty claim against the Bosch Rexroth AG shall be waived in case of unintended use if the device is modified or changed in any way - even within the framework of mounting or installation.

The external power supply of the devices has to bridge a short power failure of 20 ms according to EN 60 204. Suitable PELV- and SELV-compatible power supply units are available as accessories from Bosch Rexroth.

2.5 General safety instructions and protective measures

Observe the safety instructions and protective measures!

Comply with the following to ensure the intended use of the Safety function module:

- Comply with the specific standards and directives of the country you reside in when assembling, installing and using the Safety function module
- The following national/international statutory provisions apply to installation and use as well as commissioning and periodic technical inspections of the safety control
  - Machine Directive 2006/42/EC
  - EMC Directive 2004/108/EC
  - Provision and use of work equipment directive 2009/104/EC
  - Low Voltage Directive 2006/42/EC
  - The accident prevention regulations/safety rules
- The machine manufacturer and the machine operator are responsible for the coordination of and the compliance with all applicable safety regulations and provisions with the responsible authorities
- Information, in particular the test instructions of the instructions, the project planning manuals and the assembly instructions (such as for use, assembly, installation or integration in the control of the machine) must be complied with
- The tests must be carried out by specialized personnel or specially qualified and authorized personnel and must be recorded and documented to ensure that the tests can be reconstructed and retraced at any time by third parties

2.6 Environmentally-friendly behavior

2.6.1 General information

The safety controls are designed to reduce environmental damage. The safety controls only consume a minimum of energy and resources.

- At work, always act in an environmentally responsible manner

2.6.2 Disposal

Defective or irreparable devices always should be disposed of according to the statutory national waste disposal regulations (e.g. European waste entry 16 02 14).

We would be pleased to be of assistance to you on the disposal of these devices. Contact us.

2.6.3 Separation of materials

Only appropriately trained personnel are allowed to separate materials!

Caution is required when dismantling devices. Risk of injuries.

Prior to recycling the devices in an environmentally responsible manner, it is required to separate the different materials of the Safety extension module.

- Remove the housing from the other component parts (in particular the PCB)
- Dispose of the separated components in the corresponding recycling centers (see the following table)

Components	Disposal
Product	
• Housing	Plastic recycling
• PCBs, cables, plugs and electrical connection pieces	Electronic recycling
Packaging	
• Cardboard, paper	Paper and cardboard recycling

Tab. 2-1: Overview on disposal according to materials

3 Introduction in the Safety technology

☞ The "Introduction in Safety engineering" does not claim to be exhaustive or up-to-date! Always comply with the current standards and regulations that apply for the use case and the respective country!

3.1 Safety-related characteristic parameters

3.1.1 Overview

With regard to the control part of the machine or the system, the configuration refers to the automation task itself, the additional process-conditioned monitoring tasks and the task for functional machine safety.

This chapter is exclusively about the tasks of functional safety and describes the preparing activities to realize the safety system or to determine the required structures and parameters which then supply the input variables required for implementation with the Engineering tool. The Engineering tool is described in chapter 6 "Development interface" on page 81.

Planning the functional safety

Configuring the safety system starts with creating a plan for functional safety. Planning includes all management activities and technical activities, from concept development to validation.

Planning functional safety includes among others:

- Asserting what standards and regulations apply to the machine or system
- Determining the limitations of the machine or system. These are:
  - Spatial limits
  - Location of use
  - Planned life cycle
  - Functions and operating modes
  - Malfunctions and faults to be expected
  - Foreseeable misuse
- Carrying out a risk analysis and a risk assessment on its basis. This determines the required Safety integrity level SIL according to IEC 61508/IEC 62061 or the required performance level PL according to EN ISO 13849-1 for the safety functions
- Defining all protective measures for risk reduction. These are:
  - Safe design
  - Technical protective measures
  - User information on residual risks
- Listing and describing all safety functions to be executed by the safety system
- Selecting all safeguards and defining their use according to any applicable standards
- Determining the response time requirements for all safety functions, considering the required safety distances
- Selecting and designing all safety measures for an emergency stop (E-Stop, emergency stop)

3.1.2 General information

Test basics/standards

The internationally applicable general basic standard on the functional safety of safety-related electric, electronic and programmable electronic systems is the seven-part standard IEC 61508 that is also the basis for the development and validation of the Bosch Rexroth safety system and its components.

In the engineering industry IEC 62061 was published as a sector standard of IEC 61508. Concerning machines, it deals with the functional safety of safety-related electric, electronic and programmable electronic control systems in particular.

In parallel, the international standard ISO 13849 (parts 1 and 2) was developed to replace the European standard EN 954 (parts 1 and 2). It deals with the design and validation of safety-relevant parts of machine controls.

All machines marketed in the European Economic Area have to comply with the EC Machinery Directive. Both standards, IEC 62061 and ISO 13849-1, are listed in their European versions, EN 62061 and EN ISO13849-1, in the Official Journal of the European Union. Their application is considered compliance with the basic requirements of the Machinery Directive (presumption of conformity). In this regard, both standards are applicable to the same extent. Both contain a decision table regarding their suitability for the implementation of an application.

Unlike IEC 62061, ISO13849-1 also concerns non-electric, safety-related parts and thereby allows for cross-technology considerations. Another argument in favor of using ISO13849-1 for the implementation of a safety-related system is its simplified quantification using the provided architectures known from EN 954-1. Since it is close to the basic standard IEC 61508, IEC 62061 is better suited for complex programmable electronic systems and suitable for all architectures. IEC 61508 is to be considered for applications other than machinery.

Risk monitoring

Risk monitoring of a machines requires risk analysis and risk assessment according to ISO 12100-1 (Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology). This is the basis for a risk reduction strategy that aims to reduce the risk to a tolerable level using protective measures.

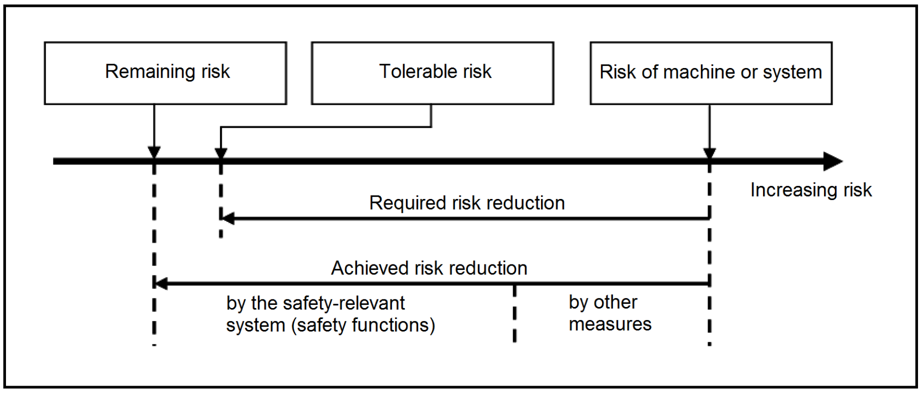


Fig. 3-1: Risk reduction

Safety functions

In addition to other protective measures, risk reduction is achieved by implementing safety functions that are realized on a technical level by the safety-related control system.

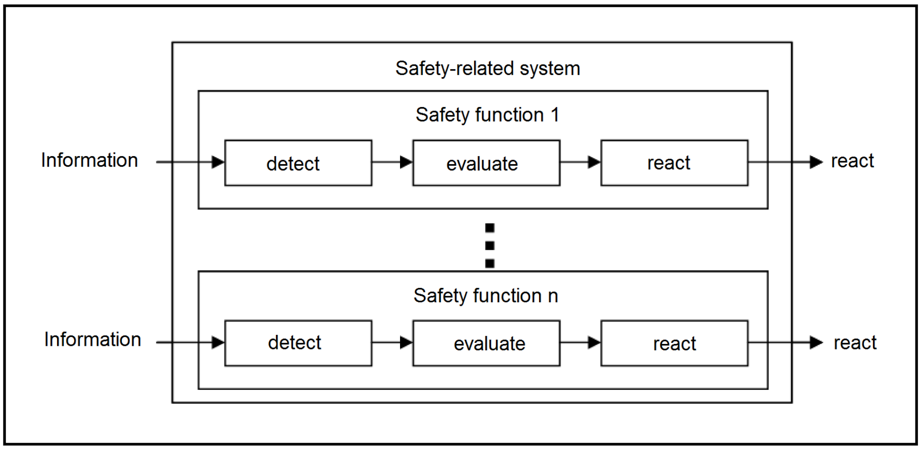


Fig. 3-2: Safety functions in the safety-related control system

The required risk reduction quality is characterized for every safety function by different safety-related characteristics according to the applied standard.

In addition to its function the safety function has the following properties:

- If it fails, the risk is immediately increased
- The safety function is characterized by its safety integrity, i.e. the probability that the safety-related control system executes the safety function as required in all specified conditions within a defined period of time. The deciding characteristic of the safety integrity is the failure limit value, i.e. the limit value of the probability of dangerous failures. This failure limit value applies to the entire safety function
- The safety function ranges from the input interface to the output interface of the safety-related control system
- Its technical implementation is divided in subsystems

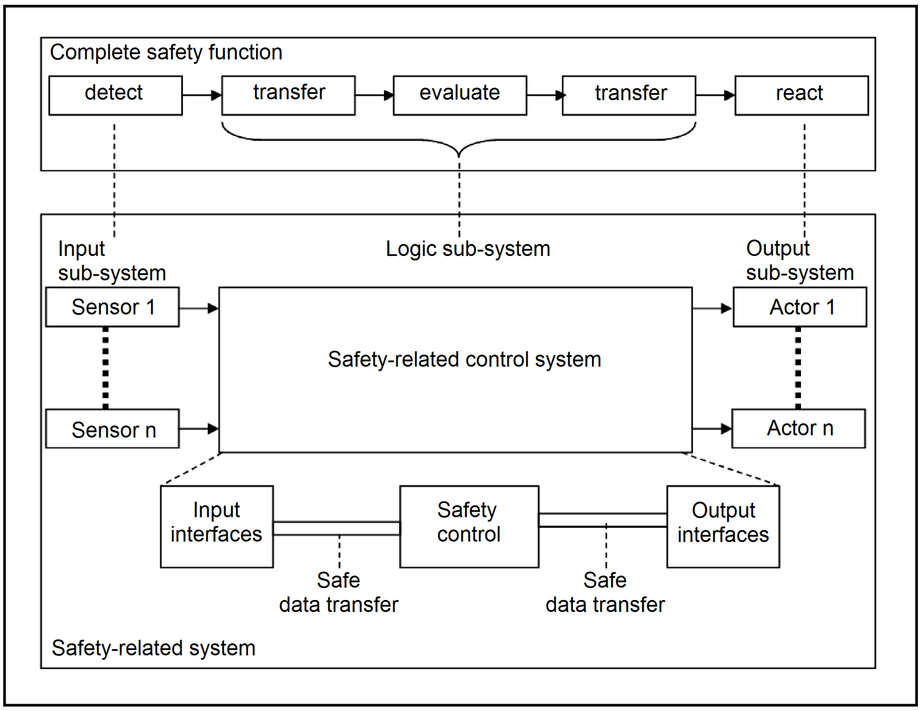


Fig. 3-3: Implementation of the safety function in the safety-related system

The safety integrity defined in the risk analysis and risk assessment has to be guaranteed for all safety functions.

The failure limit value is distributed to the subsystems of a safety function according to the following convention:

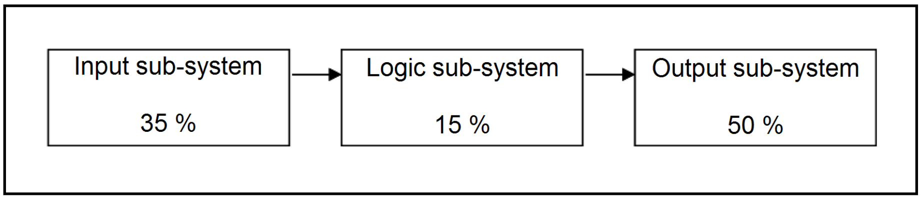


Fig. 3-4: Failure limit value distribution

Over time, the safety integrity of a safety function is reduced depending on the technical implementation of the safety-related system and/or its subsystems, e.g. due to wear and tear.

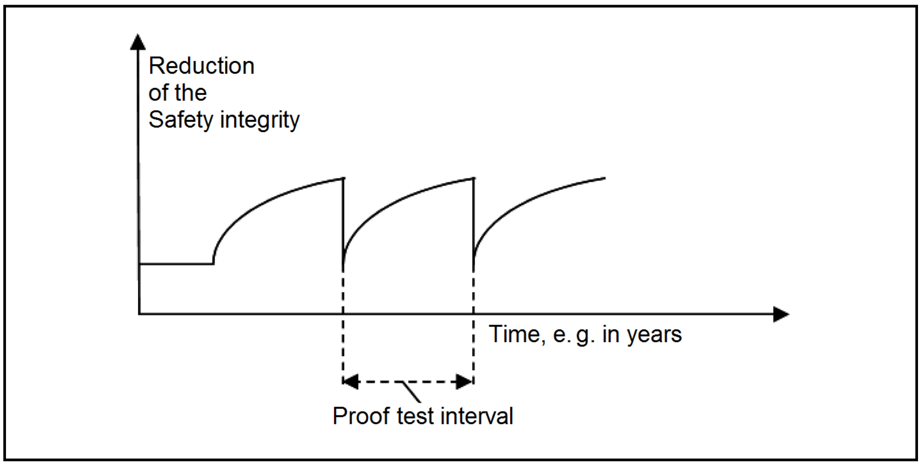


Fig. 3-5: Proof test interval

For each safety function the maximum period of use of the individual subsystems (time the subsystem may be used) and the specified proof test interval has to be taken into account.

When the proof test interval has expired, carry out a proof test. The proof test detects errors or a deterioration of the safety system and its subsystems. Take the respective measures to restore the system's default state.

3.1.3 Assessment according to IEC 61508

IEC 61508 represents the safety integrity value as four integrity levels SIL1 (lowest level) to SIL4 (highest level).

In general automation and in engineering only integrity levels SIL1 to SIL3 are of relevance.

To achieve the required SIL determined in the risk analysis for a safety function, the safety-related system has to meet the following requirements:

1. All subsystems that execute the safety function have to meet all the requirements of IEC 61508 for the required SIL. In particular, this refers to the requirements for the avoidance and control of systematic failures.
2. The probability of undetected, dangerous failures of the entire safety function has to be smaller than the specified failure limit value for the required SIL.

SIL3 according to IEC 61508

The Safety extension module and SafeLogic compact are suitable for use in applications up to SIL3 according to IEC 61508.

The period of use of the Safety extension module and SafeLogic compact is 20 years. In this period (beginning with the date of manufacture), no proof test is required. When this period has expired, the Safety extension module and SafeLogic compact have to be replaced by a new device.

According to IEC 61508, the failure limit value depends on the operating mode of the safety function. IEC 61508 distinguishes between operating modes with a low request rate (a maximum of one request per year) and modes with a high (more than one request per year) or continuous request rate.

According to the SIL, the following is specified for the entire safety function:

SIL	PFD_{avg}
4	≥ 10^{-5} to < 10^{-4}
3	≥ 10^{-4} to < 10^{-3}
2	≥ 10^{-3} to < 10^{-2}
1	≥ 10^{-2} to < 10^{-1}

PFD_{avg} Average probability of a dangerous failure when requesting the safety function

Tab. 3-1: Failure limit values for low requirement rate

SIL	PFH
4	≥ 10^{-9} to < 10^{-8}
3	≥ 10^{-8} to < 10^{-7}
2	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-6} to < 10^{-5}

PFH Average frequency of a dangerous failure per hour

Tab. 3-2: Failure limit values for high or continuous requirement rate

For the intended safety function implementation, the failure probability for the overall safety function has to be calculated depending on the operating mode and taking all subsystems into account. This failure probability has to be less than the failure limit value of the SIL to be achieved.

In general automation and in engineering operating modes with a high or continuous request rate are usually used. In this case, add the dangerous failure frequency (per hour) of all subsystems involved with the safety function according to the following formula:

$$PFH_D = \sum_1^n PFH_{DS} + \sum_1^m PFH_{DSDI} + PFH_{DSIS} + \sum_1^i PFH_{DSDO} + \sum_1^k PFH_{DA}$$

PFH_D Probability of a dangerous failure (per hour) of the complete safety function

PFH_{DS} PFH value of one of the sensors involved in the safety function

PFH_{DSDI} PFH value of one of the input devices involved in the safety function

PFH_{DSIS} PFH values of the safety control and the safe transmission

PFH_{DSDO} PFH value of one of the safe output devices involved in the safety function

PFH_{DA} PFH value of one of the actuators involved in the safety function

Fig. 3-6: Probability of a dangerous failure per hour

This calculation has to be made for each safety function. For safety functions with a low requirement rate, calculate the PFD_D value in the same way.

For the failure rates, refer to the safety-related components of the device manuals.

The failure probabilities of standard components are not considered for the failure limit value of a safety function, since there is no safety-relevant contribution for the implementation of the safety function.

3.1.4 Assessment according to IEC 62061

Being a sector standard of IEC 61508, IEC 62061 requires the same principle as above.

Here, the target parameter is the Safety Integrity Level SIL, too. Since the application range of the standard is restricted to machines, only SIL1 to SIL3 are to be considered. The required failure limit values correspond to those of IEC 61508. However, only an operating mode with a high or continuous request rate is considered. The operating mode with a low request rate is deemed irrelevant for use in safety-related systems of machines.

There are major differences in terminology and a strictly systematic process for the design of a safety-related control system (SRECS = Safety-Related Electrical Control System), ranging from the compilation of a safety plan up to the overall validation process. The requirements of the standard specified for all stages of this process have to be met according to the SIL to be achieved.

The SILCL (SIL Claim Limit) is the SIL claim limit for a subsystem according to IEC 62061. This is the maximum SIL that may be claimed for a SRECS subsystem for the implementation of a safety function (SRCF = Safety-Related Control Function) concerning specified structural limitations and systematic safety integrity. The Safety extension module and SafeLogic compact meet the SILCL for SIL3.

For the assessment of a SRECS according to IEC 62061, apply the safety-related characteristic values specified above for the Safety extension module and SafeLogic compact.

3.1.5 Assessment according to ISO 13849-1

The assessment of a safety-related control system or safety-related parts of a control (SRP/CS) according to ISO 13849-1 uses the performance level PL as reference.

Like the SIL, the PL measures the quality of risk reduction of a safety function and the safety integrity of the control-related implementation. The norm defines 5 different PLs (a to e), that each correspond to a value range of the average probability of a dangerous failure per hour.

Performance level PL	Average frequency of a dangerous failure per hour (PFH in 1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

Tab. 3-3: Performance level

As a result of the risk assessment, the required performance level PL_r (r = required) is specified for all safety functions.

The PL to be achieved by the safety-related parts of the control for this safety function is determined by:

- The calculated failure probability ($MTTF_d$ = Mean Time To Dangerous Failure)
- The diagnostic effectiveness (self-tests) = DC_{avg} (average diagnostic coverage)
- The error tolerance of the structure referring to the categories of EN 954-1

The bar chart of ISO 13849 is a simple graphic procedure to determine the PL value. The bar chart is based on complex calculations and estimations on the safe area.

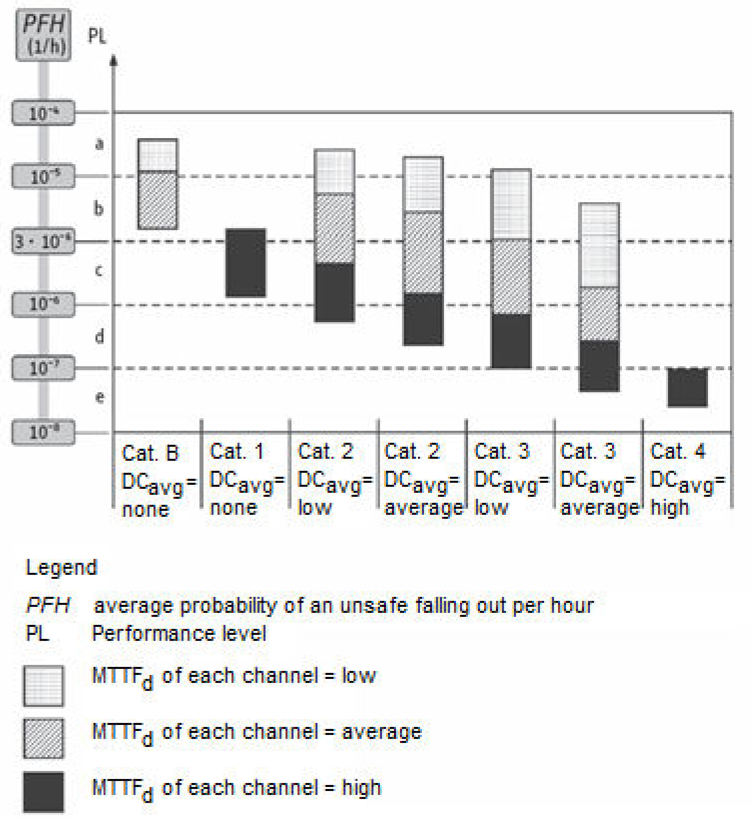


Fig. 3-7: Bar chart for PL determination

Procedure:

1. Determine the relevant bar on the horizontal axis by including the achieved category and DC_{avg} class.
2. The level of the $MTTF_d$ achieved by the SRP/CS on the selected bar determines the PL to be read from the vertical axis.

With this method, it is possible to quickly estimate the achieved PL without exact quantity data. If more accurate PFH values are required, the standard includes a numerical representation of the bar chart in annex K.

However, the following is required to use the bar chart:

- Categories 2, 3 and 4 assume that there are sufficient measures to prevent failures with a common cause (Common Cause Failures = CCF). For this purpose, ISO 13849-1 contains a checklist with eight important countermeasures that are assessed using a point scheme. 100 points can be achieved. ISO 13849-1 requires a minimum of 65 points for categories 2, 3 and 4 which corresponds to a deterioration of the $MTTF_d$ by 2 %. This factor is implicitly allowed for in the bar chart
- A 20 year period of use is assumed for the SRP/CS. Components that are subjected to wear and tear and do not comply with this requirement have to be exchanged at a specified time
- The bars for category 2 assume that the test frequency is at least 100 times greater than the medium request frequency of the safety function and that the testing equipment is at least 50% as reliable as the logic
- In addition to the failure probability, quality aspects also have to be considered to achieve a certain PL. These aspects include systematic failures and software errors

The considerations above refer to a SRP/CS that can be entirely displayed in a category or architecture with an intended PL. In principle, this also applies to the connection of subsystems that have the same PL, taking the exact portion of a subsystem in the safety function into consideration and the exact interface definition where additional subsystems may be connected. The standard also includes procedures to determine the resulting PL of a safety function for the connection of subsystems with different PLs.

If there are PFH values for all subsystems, they may be added to calculate the value required for the overall PL. The PFH values can also be calculated according to IEC 61508 or IEC 62061.

As all subsystem PLs are always at least as high as the overall PL, this ensures that all measures concerning unquantifiable, qualitative aspects (e.g. systematic failures or software) are sufficiently considered if they are combined.

However, the interfaces of the subsystems have to be considered in particular:

- All connections (e.g. lines or data communication via bus systems) have to be included in the PL of one of the involved subsystems or connection errors have to be excluded or are neglectable
- All output statuses of a controlling subsystem that signal the request of the safety function have to be suitable trigger events for switching to the safe state of the downstream subsystem

The interfaces of the safety-related components of the Bosch Rexroth safety system meet these conditions.

☞ Bosch Rexroth provides comprehensive brochures

"On the safe side with Rexroth: 10 Steps to performance level"

for the realization of functional safety according to ISO 13849. The brochure is suitable for use in practice to design safe machinery (ordering number of the German version: R961006998, ISBN number 978-3-9814879-1-6, 264 pages).

The Institute for Occupational Safety and Health of the German Social Accident Insurance IFA (formerly BGIA) supports users of the ISO 13849-1 standard as follows:

- BGIA report 2/2008: Functional safety of machine controls – use of DIN EN ISO13849 – all aspects of how to use the standard are explained in detail
- SISTEMA©

  The software tool determines the required performance level (PL_r) and allows the automatic calculation of the resulting quantification values. The IFA provides the tool as freeware

  Rexroth provides SISTEMA libraries for certain technologies that grow continually. These libraries may be used as of version 1.1.1. Please find the SISTEMA libraries at:

  http://www.boschrexroth.com/de/de/trends-und-themen/maschinensicherheit/rexroth-safety-on-board-unsere-loesung/sistema/sistema

  To simplify the use of the SISTEMA software, the open SISTEMA series may be downloaded for free
- The "Performance Level Calculator©" is also provided for free by the IFA. The "Performance Level Calculator" is a convenient disc calculator to determine the performance level according to ISO 13849

3.2 Design of the safety-related control system

3.2.1 Topology

In principle, the basic topology of the safety-related control system is independent from the machine or system structure.

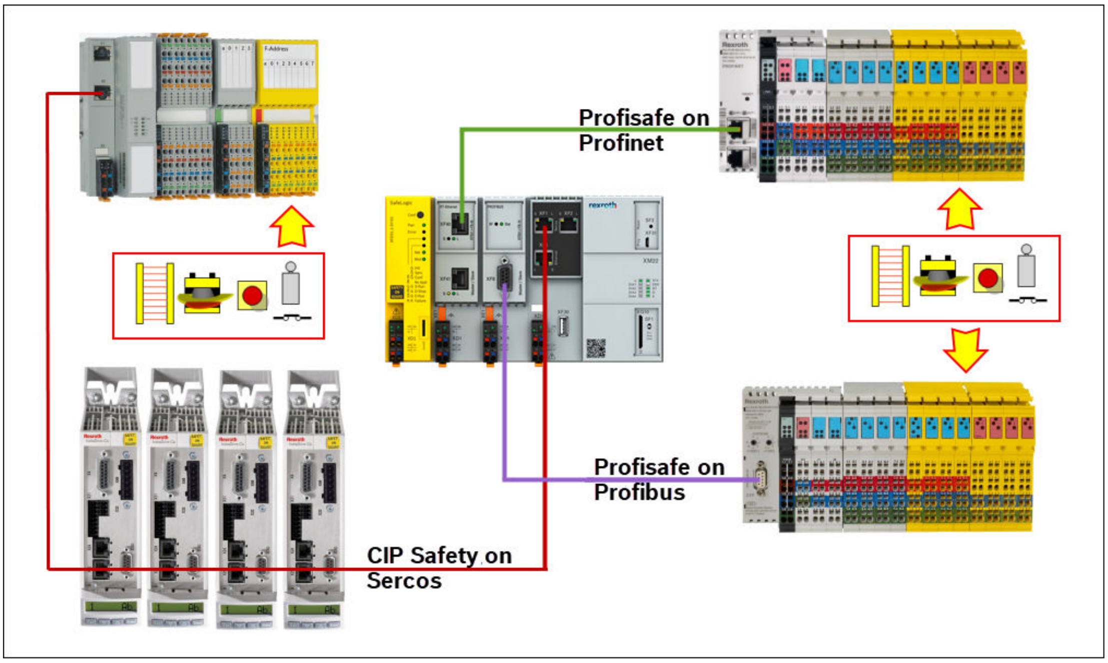


Fig. 3-8: Topology of a safety-related control system

For the application ranges MLC/ILC the risk assessments usually result in the safety-related requirements SIL2 (based on IEC 61508 or IEC 62061) or PL d (based on EN ISO 13849-1).

SIL3 or PL e safety functions are also often required for PLC applications using the IoT-compatible PLC system (ILC).

The Safety extension module is the core of the safety-related control system and can generally be used to realize safety functions up to SIL3 or PL e. With regard to the input/output components, Bosch Rexroth offers a range of Safety I/Os for all applications that are connected via Profibus and Profinet via PROFIsafe or via Sercos via CIP Safety on Sercos (CSos). Please find an overview in chapter 5.3 "Hardware for Rexroth Inline system" on page 56.

SafeLogic compact can also be used to realize safety functions up to SIL3 or PL e. For an overview of the supported main and extension modules, see "CPU modules" on page 46 and "Extension modules" on page 46.

3.2.2 System design

While the basic topology of the safety system is independent of the application range, the properties of the standard automation system are important boundary conditions for the design of the safety system. Per definition, these properties are not important regarding the safety. However, they are relevant regarding the performance of the safety system, in particular the response time of the safety functions.

Influence of the standard system

The following has to be considered

- The used standard control
  - Hardware

  - Software
- The size of the standard application
- The bus system(s) used; i.e.:
  - Profibus DP
  - Sercos III
- The load of the bus system
  - Number of bus participants
  - Data width of the standard telegrams
  - Use of acyclic transmission services (parameter or diagnostics channels)
- The drives used (including motors)

Installation in a control cabinet

All safety components with a protection class of IP 54 or less have to be installed into a control cabinet with a protection class of at least IP 54. This applies to both, SafeLogic compact and the Safety extension module and the Bosch Rexroth safety I/O components (SIL2, SIL3). These components have protection class IP 20.

Voltage supply

Plan the power supply of the safety system according to the specifications in DIN EN 60204-1.

Only use power supply units with protective separation according to EN 50178 (or power sources with the same degree of safety) with PELV voltage according to EN 61131-2. Additional devices may only be connected to these power supply units if they also comply with the PELV specification.

EMC

The electric equipment of the machine has to meet the requirements of electromagnetic compatibility, in particular it has to resist the expected faults. Even if the individual devices meet the European EMC directive and the individual safety components additionally possess increased interference resistance, aim for an EMC compliant structure when designing the electrical equipment of the machine.

Observe the following basic rules to avoid any EMC problems:

- Continuous equipotential bonding between machine and system parts
- Spatial separation between supply, power parts and control parts
- Attach shields shortly and over the entire surface
- Avoid any equipotential bonding current via the shield
- Connect any available functional grounding connections
- Install all communication connections according to the specifications

☞ Pay close attention to the installation instructions of all components, in particular those of the field bus systems.

Architecture design

The architecture of a safety-related control system for the implementation of the intended safety functions can be illustrated as in the following figure. The safety system may include several safety functions for risk reduction.

Every single safety function is implemented in this basic architecture using sequential subsystems.

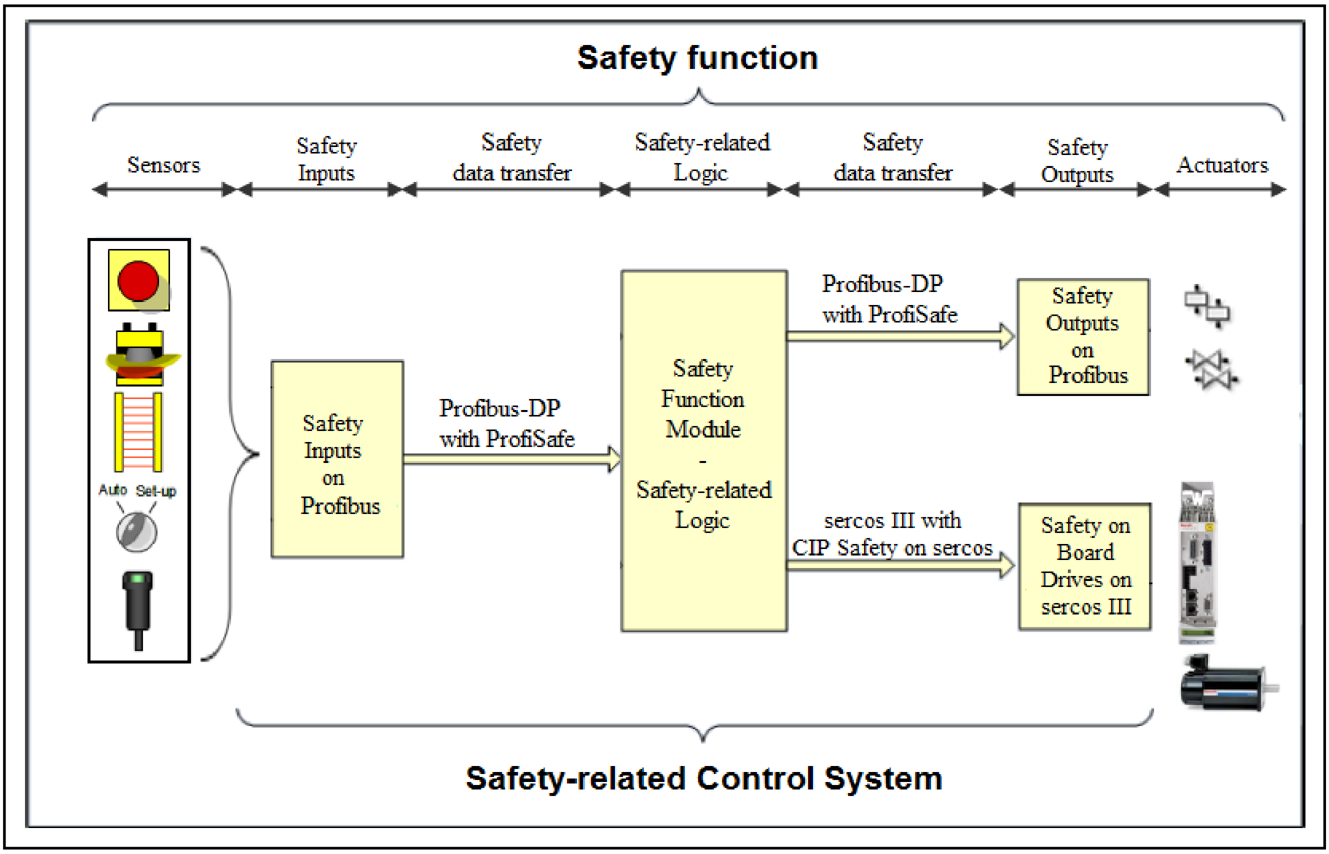

Safety function
Sensors
Safety Inputs
Safety data transfer
Safety-related Logic
Safety data transfer
Safety Outputs
Actuators
Auto Set-up
Safety Inputs on Profibus
Profibus-DP with ProfiSafe
Safety Function Module - Safety-related Logic
Profibus-DP with ProfiSafe
Safety Outputs on Profibus
sercos III with CIP Safety on sercos
Safety on Board Drives on sercos III
Safety-related Control System

Fig. 3-9: Safety-related control system: Example of Profisafe on Profibus and CSOs

3.2.3 Subsystem design

For every safety function, the following always has to be considered when designing the subsystems for the implementation of the safety functions and in the final assessment of the safety integrity:

Safe inputs/outputs

- Selection of input/output modules taking the required safety level of the safety function into account (depending on the applied standard)
  - SIL2 or PL d
  - SIL3 or PL e

☞ If various parallel input or output modules are used to implement a safety function, all modules have to be suitable for the required SIL or PL.

- Selection of input/output modules taking the required response time for the safety function into account

☞ If various parallel input or output modules are used to implement a safety function, use the slowest component regarding runtime and error reaction time to determine the resulting response time.

Also monitor the differently configured monitoring times for the safe bus communication.

- Extension of decentralized I/O stations, considering the required response time. The extension of a decentralized station with safety-related and unsafe modules influences the signal runtime. With time-critical signals it may be advisable to use a dedicated I/O station
- Combining inputs/outputs that are functionally related. The safety control offers a procedure for group coordination, e.g. to implement common switch-off behavior. Error reactions usually refer to the entire module and not individual signals. When assigning actuators to the outputs, keep in mind that an error reaction may switch off all outputs of a module
- Connecting inputs under consideration of input dynamization. Safety-related inputs usually have to be dynamized to detect "dormant" errors in the input channel and the input wiring. Safe input modules provide test outputs for input dynamization. These test signals have to be included in the input wiring and taken into account in input configuration

Safe Bosch Rexroth input/output devices are available as decentralized modules for PROFIsafe and CIP Safety on Sercos.

> ☞ For all information on system integrity, time behavior and parameterization of the safe input/output devices, see the respective device descriptions.

Safe drives

Bosch Rexroth drive systems of the IndraDrive series may optionally be used with an integrated safety technology. Safety applications designed with them differ from systems with conventional safety technology in that the safety functions are directly integrated in the smart drives in the form of hardware and software. This results in particularly short response times with maximum safety in all operating modes. Furthermore, the following conventional safety technology components are no longer required:

- Motor standstill guard for monitoring safe stop
- Speed governor for monitoring safety-related reduced speeds
- Power contactors between controllers and motors
- Limit switches and position cams for area detection

> ☞ For information on the integrated safety technology with Rexroth IndraDrive, please refer to the following documentation:
>
> - "Rexroth IndraDrive Integrated Safety Technology "Safe Torque Off" (from MPx-16)" (R911332634)
> - "Rexroth IndraDrive Integrated Safety Technology According to IEC 61508" (R911327664)

Secure data transfer

The safe data transfer in Bosch Rexroth safety systems is realized together with the standard process data transfer via the following bus systems by using the safety-related transmission profiles PROFIsafe or CIP Safety on Sercos that both provide for safety-related applications up to SIL3 or PL e.

- Profibus DP
- Profinet I/O
- Sercos III

When planning the data transmission comply with the installation instructions for the field busses in any case, in particular with the special requirements for safe transmission profiles. For this purpose, see chapter 5 "Safe bus systems" on page 55.

Both bus systems may be involved at the input and output in the safe data transmission for different input/output modules within a safety function.

To determine the resulting response time of the safety function, use the slowest data connection regarding runtime, monitoring time and error reaction time. Also take into account the physical structure, the specified transmission parameters (e.g. baud rate), and the bus system with safety-related and unsafe devices.

3.3 Determining the achieved safety integrity

After designing the safety system and implementing the safety function, determine the achieved safety integrity. That means determine the achieved SIL or PL and ascertain if the SIL or PL required according to the risk assessment with the intended period of use of the machine or system is achieved.

In doing so, observe the specifications of the standard that the safety system is based on.

Use the safety-related characteristics of the individual safety system components. For the specifications required for the Safety extension module or the SafeLogic compact control, see chapter 4.4.2 "SafeLogic" on page 47 of this documentation. The unsafe standard components of the automation system do not affect the safety integrity and do no need to be considered.

If the safety system design does not achieve the required safety integrity for all safety functions, adapt the system design until all requirements are met. It may be necessary to complete this repetitive process several times.

3.4 Determining the guaranteed switch-off time

3.4.1 Response time

Safety processes are processes that have to trigger a reliable and calculable shut-off in a very short time. Often, there is only very little time between the detection of a dangerous interference and the required shut-off. Therefore, planning a safety system requires calculable response and switch-off times.

Safety distance

Safety distances of a machine, e.g. the distance of a light grid to the dangerous movement, result from the risk analysis and the machine configuration. In addition to the access velocity, the switch-off time of the machine is the decisive parameter for their dimensioning.

The general formula for the safety distance is:

$$S = K \times T + C$$

S	Safety distance in mm
K	Access velocity in mm/s
T	Switch-off time [s]
C	Extra in mm

Fig. 3-10: Safety distance according to EN 999

The access velocity is derived from the possibilities and type of approach.

The switch-off time T refers to the time from triggering the sensor function to stopping the dangerous movement.

The extra C is an additional distance that takes the intrusion into the danger zone prior to triggering the safety function into account.

Other parameters have to be considered in the calculation of the safety distance, depending on the type of access protection.

☞ For information on the calculation of the safety distance, see standard: DIN EN 999: "Positioning of safeguards with respect to the approach speeds of parts of the human body".

Required switch-off time

From the specified access velocity a maximum switch-off time for the safety functions is derived to achieve the required safety distance.

Typical response time

The typical response time of the safety system is the time that elapses from applying the signal to the safe input terminal to the response at the safe output terminal. During normal operation (no error occurred) of the safety system the typical time is achieved and can be measured.

The typical response time of the safety system is not relevant and unsuitable for the determination of the guaranteed switch-off time and the safety distances.

The processing time of the standard control is not relevant for the determination of the typical response time of the safety system.

Guaranteed switch-off time

The guaranteed switch-off time of the safety function corresponds to the maximum response time of the machine. The switch-off time is determined in a worst case assessment and has to take into account errors in the safety chain of the safety function.

The guaranteed switch-off time consists of the longest processing time of the safety function inputs, outputs, communication connections and the safety logic. For the maximum processing times of the individual components, see the respective data sheets. The guaranteed switch-off time has to be less than the required switch-off time.

During project planning it is important to ensure that the designed safety system in the machine complies with the switch-off times for all safety functions. These switch-off times have to be less than the required maximum switch-off time in all cases, during normal operation (no error occurred) and in case of an error.

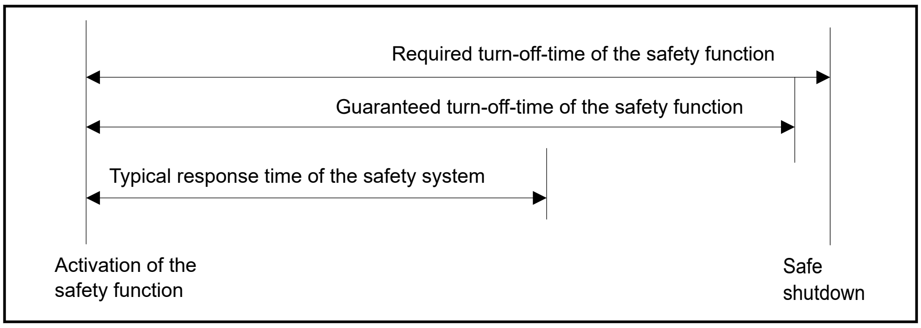
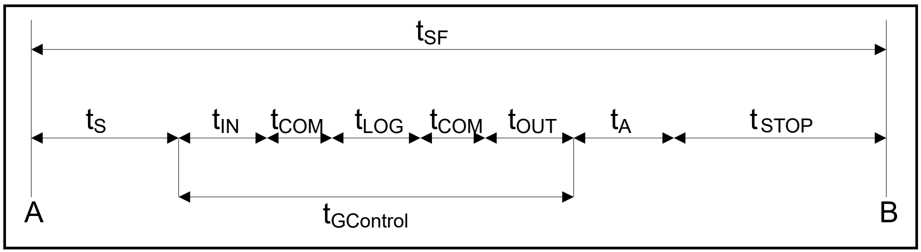

Required turn-off-time of the safety function
Guaranteed turn-off-time of the safety function
Typical response time of the safety system
Activation of the safety function
Safe shutdown

Fig. 3-11: Typical response time - guaranteed switch-off time

Normal operation (no error)

Determine the switch-off time in normal operation (no error occurred) using runtime assessments of the individual subsections of the safety function.



A	Safety function request
B	Safe state of the System
t_{SF}	Guaranteed switch-off time for the safety function
t_S	Sensor response time
t_{IN}	Processing time of the input
t_{KOM}	Transmission time
t_{LOG}	Logic processing time
t_{OUT}	Output switch-off time
t_A	Actuator response time
t_{STOPP}	Machine stopping time
$t_{GControl}$	Time slot of the safety system

Fig. 3-12: Overview of switch-off times

Use the following formula to calculate the guaranteed switch-off time:

$$t_{SF} = t_{S_{\max}} + t_{GControl_{\max}} + t_{A_{\max}} + t_{STOP_{\max}}$$

Fig. 3-13: Guaranteed switch-off time for the safety function

For the maximum response times of sensors and actuators, see the respective device descriptions. Usually, two reliable measurements are needed to determine the stopping time of the machine.

☞ If several sensors and actuators feature in the safety function, the longest response time of the devices involved is used for calculation.

Calculate the maximum time slot of the control system. In doing so, take into account the following factors and worst case errors for your use case:

- Used input/output components and their parameterization
- Used bus system (used bus systems) for safe data transmission and its parameterization and configuration (bus cycle time, number of bus devices, number of user data bytes). For the runtime calculation of safe data transmissions, the design of the standard automation system also has to be considered:
  - Standard load and time behavior of the busses
  - Standard load and time behavior of the decentralized stations
  - Time behavior of the standard application
  - Use of asynchronous transmission services for parameterization or diagnostics
- Processing time of safe logic

If the sequential subsections of the safety system are not synchronized, their time slots have to be used twice in the calculation (worst case)

$$t_{GControl} = 2 \cdot t_{IN_{\max}} + 4 \cdot t_{COM_{\max}} + 2 \cdot t_{LOG} + 2 \cdot t_{OUT_{\max}}$$

Fig. 3-14: Calculation of the maximum time slot of the control system

If several inputs or outputs or different communication paths are involved in the safety function, use the longest processing time of the involved components or subsystems.

In case of error

In case of an error, the outputs of the safety-related components report "Fail state values". These values can be transmitted with the respective error messages via the communication system. If the communication system is no longer available, parameterizable time monitoring starts on the safety components to switch the outputs of the safety components into safe state. During parameterization of the safety components the time out values are set in such a way that the guaranteed switch-off times are achieved without unnecessarily impairing the availability of the system.

Processing time of the safe logic

The processing time of the safe logic is guaranteed as a cyclic task with a fixed task runtime is used. Set the processing time during parameterization of the Safety task. Select a value between 2 ms and 500 ms. The Safety extension module monitors the task runtime. If the time is exceeded, an error reaction is triggered and the safety system goes into safe state.

SafeLogic compact is not equipped with a parameterizable Safety task. Here, the cycle time depends on the number of used function blocks and is between 4 ms and 40 ms.

3.4.2 Checking the required switch-off time

Carry out the following checks for all safety functions:

- Does the guaranteed switch-off time determined result in the required switch-off time of the safety function?
- If the determined value is greater than the required switch-off time for safety function t_{SF}, change one of the parameters as the safety of the machine is not guaranteed in all cases under these circumstances
- If the determined value is less than t_{SF}, use the specified values to parameterize the monitoring times of the units in the safety chain. If the determined value is significantly smaller than t_{SF}, it is possible to increase the value for the monitoring times to increase availability. Carry out the check for the new value of the parameterized switch-off time!

Carry out the above checks for all safety functions.

3.5 Address assignment/names

Components have to be uniquely identified within their unique communication relations by using additional addresses. Set these addresses according to the respective devices. There are the following known possibilities:

- Manual setting using a DIP switch or device tool
- Automatic setting by parameterization from the safety control

These additional addresses are independent from standard addressing. The addresses are stored in the safety application when the safety components are parameterized (e.g. F-Parameters in PROFIsafe). They are used in cyclic operation to verify the communication relation.

3.6 Example application

3.6.1 Overview

☞ The following example is fictitious and not authentic regarding a practical application. Therefore, the used distances and times are only approximations. For this reason, it is not possible to use the data from this example in a practical application.

The data carrier of the SafeLogic compact Designer Software (R911334897) contains application examples from various industries.

The example describes a drive application in connection with the Safety extension module with the motion of a motor axis being the only identified hazard (in addition to the general electrical hazard). Following a detailed analysis, the required risk reduction is to be achieved by protecting the danger zone from access by hand or arm using a vertical light curtain.

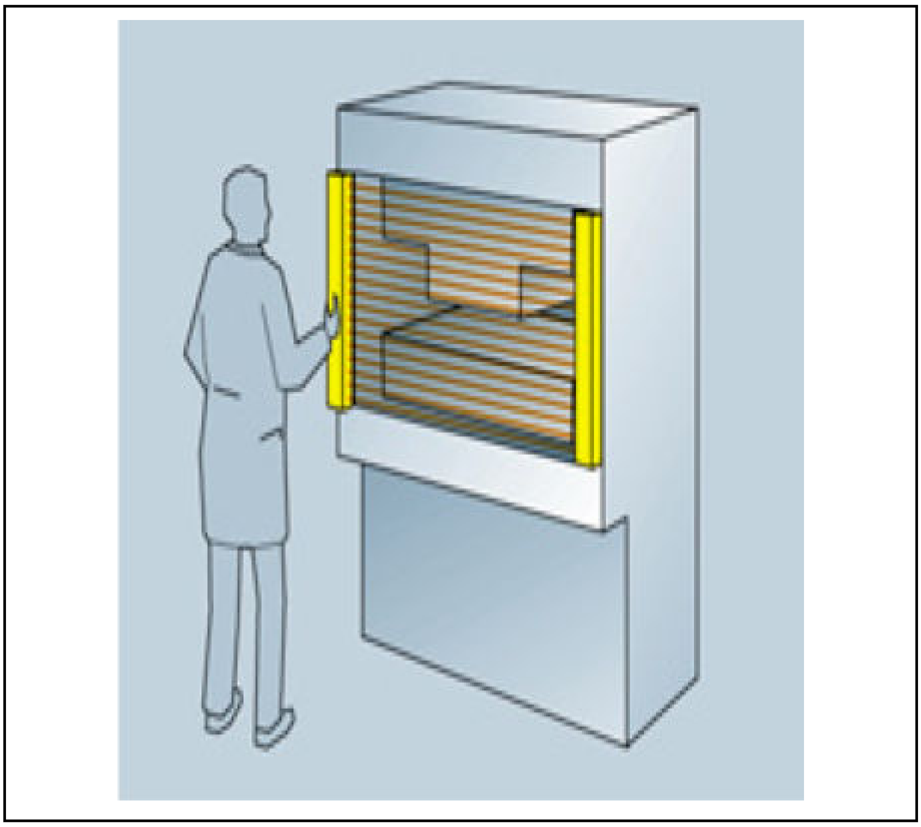


Fig. 3-15: Configuration example

3.6.2 Requirements

The following standards and regulations exemplary apply to this fictitious machine:

⚠ DANGER

Always comply with the current standards and regulations that apply for the use case and the respective country!

- Machinery directive 2006/42/EC
- EMC directive 2004/108/EC
- Work Equipment Directive 2009/104/EC
- Low Voltage Directive 2006/95/EC
- Accident prevention regulations/safety rules
- DIN EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests
- IEC 61496-2: Active opto-electronic protective devices
- DIN EN 60204-1: Safety of machinery – Electrical equipment of machines - Part 1: General requirements
- EN 999: Positioning of safeguards with respect to the approach speeds of parts of the human body

Safety-related assessment is to be carried out according to EN 62061 and EN ISO 13849-1.

Based on a risk assessment considering the limitations of the machine, the following required safety level was specified:

- SIL 2 according to EN 62061
- PL d according to EN ISO 13849-1

3.6.3 Safety function

Functional safety of the machine is achieved by implementing a single safety function:

SF1: "If the light curtain is interrupted, the motor has to stop in a controlled way. The energy supply is to be maintained (stop category 2 according to EN 60204-1)".

The necessary shutdown in case of emergency (emergency stop) is an additional protective measure and not a primary measure for risk reduction. Therefore, this function is not considered a safety function and not taken into account in this example. However, this function has to bring the machine to a safe standstill using a category 0 or 1 stop according to EN 60204-1.

SF1 can be subdivided into safety subfunctions:

SF1:	"If the light curtain is interrupted, the motor has to stop"		
Safety subfunctions:	Sensor	Logic and data transmission	Actuator
Tasks:	Detection	Transmission and evaluation	Response
Units:	Light curtain	Safety extension module, safe inputs (SIL2 I/O system), PROFIsafe	Safe drive control, motor

Tab. 3-4: Safety function

3.6.4 Structure and wiring

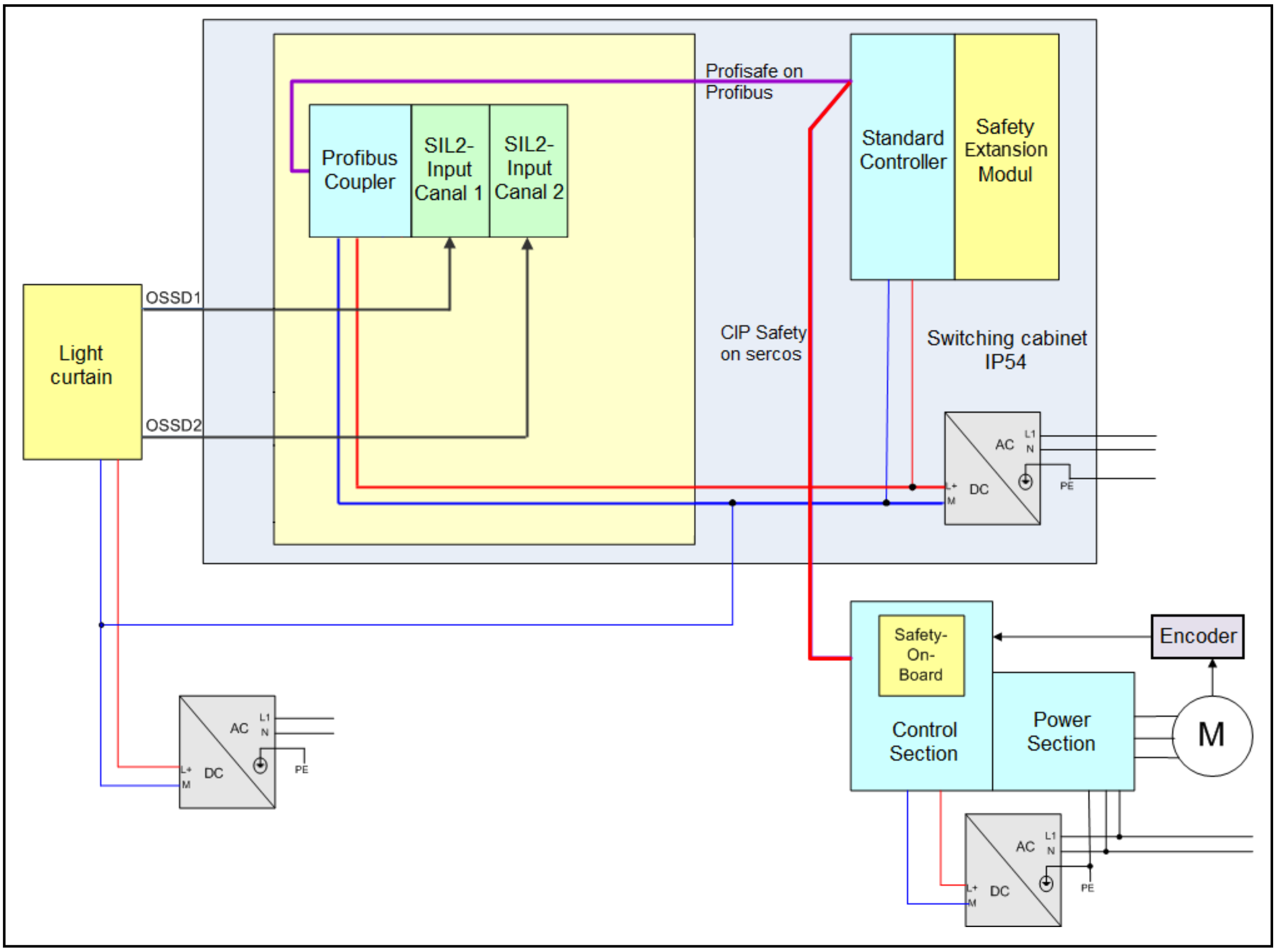


Fig. 3-16: Schematic structure of an example system

Without giving details on the structure and wiring, the following requirements have to be met:

- The light curtain power supply may not supply other machine parts. The power supply requires the same ground as the control components
- The power supply is supplied with 230 VAC (overvoltage category II)
- All power supply units provide PELV (protective extra low voltage)
- All control components have to be installed in a control cabinet with protection class IP 54

3.6.5 Components

Light curtain

- The light curtain is connected to the safe control system via signals OSSD1 and OSSD2

  OSSD1 and OSSD2 are safety-relevant switching outputs (Output Signal Switching Devices). The two switching outputs are connected to a safety-relevant, digital input module (F-DI) and evaluated in the input module (2o2 evaluation). If the light curtain is interrupted, the safety-related control reads a "0"-Signal from the F-DI. The safety program in the safety control then stops the application

- To safely detect access by hand or arm, a suitable light curtain has to have a physical resolution of 30 mm.

  Due to the design, the approach is only possible at a right angle. The design also ensures that the danger zone can only be accessed via the protected area. It is not possible to reach above or below it or to step around it. The distance to reflecting surfaces as described in IEC 61496-2 ("Active opto-electronic protective devices") also has to be considered
- To reach SIL2, the light curtain has to be at least a type 3 AOPD according to EN 61496-1. Light curtains are opto-electronic devices that use diffuse reflection (AOPDDR). These AOPDs meet a number of special requirements, in particular:
  - The AOPD is equipped with two independent semiconductor outputs (24 V) OSSD1 and OSSD2 to connect it to the safe control system
  - The AOPD carries out internal tests at least every 5 s and at every reset
- A type 4 AOPD according to EN 61496-1 is used as light curtain

  SILCL according to EN 62061 = 3

  PL according to EN ISO 13849-1 = e

  PFH = 2.5 x 10^{-8}

  This is divided in:

  PFH (receiver) = 2 x 10^{-8} PFH (sender) = 5 x 10^{-9}

  Maximum response time: 15 ms

Safe inputs

Bosch Rexroth SIL2 I/O system

- SIL2 I/O system in minimum configuration, consisting of Profibus coupler and 2 Safety input components
- The OSSD1 and OSSD2 outputs of the light curtain are connected via two channels

The following specifications of the SIL2 I/O system can be found in the technical data:

SILCL according to EN 62061 = 2

PL according to EN ISO 13849-1 = d

PFH = 2 x 10^{-8}

The cycle time of the SIL2 I/O system with this minimum configuration is 10 ms.

Secure data transfer

Profibus with PROFIsafe is used for safe data transmission.

PROFIsafe can be used up to SIL3 or PL e. The PFH value used can be 10^{-9}.

The Profibus is operated at 12 MBaud. Assuming that the Profibus is loaded with 32 additional Profibus devices, a bus cycle time of 1.5 ms is used.

Safety control

The Safety extension module XFE01.1-SY-01 can be used for applications up to SIL3 or PL e.

PFH: 4.5 x 10^{-10}

The cycle time of the safety application is set to 10 ms.

Drive control

Bosch Rexroth drive control with Safety on Board.

With the option Safety on Board, the drive can be used for encoder-dependent safety functions up to SIL2 or PL d. Encoder-independent Safety functions meet the SIL3 requirements.

The time to respond to a safety request is 2 ms.

In connection with the encoder, the PFH value is set to 2.5 x 10^{-8}.

Motor We assume that the motor has a stopping time of 100 ms (time to safe standstill).

3.6.6 Parameterization

The following table only lists the component parameters that are relevant for the implementation of the example safety function.

Component	Parameters	Value	Meaning
Light curtain	None		
SIL2 inputs	**Profibus:**		
	Station address	1	
	F-parameter:		
	F_Slot Number	1	
	F_Check_SegNr	No Check	
	F_Check_iPar	No Check	
	F_SIL	SIL2	SIL2
	F_CRC_Length	2 Byte CRC	
	F_Block_ID	0	
	F_Par_Version	V1mode	PROFIsafe version 1
	F_Source_Add	1	PROFIsafe addresses that refer to the Profibus station number
	F_Dest_Add	8	
	F_WD_Time	50	Monitoring time (ms)
	F_Par_CRC	27761	Generated automatically

Component	Parameters	Value	Meaning
	I-parameters:		
	Inline module 1	IL 24 DI8	2 input modules
	Inline module 2	IL 24 DI8	
	Inline module 3	No Module	
	Start modules Input channel 1	Module 1	
	Start modules Input channel 2	Module 2	
	Feedback start modules	No Module	No outputs with feedbacks
	Output start modules	No Module	
	Input 0	Active	
	Input 0 channel	Two channel	Input channel 1, monovalent
	Input 0 type	Monovalent	
	Input 0 discrepancy	5 ms	Discrepancy time to channel 2: 5 ms
	Input 0 filter	0 ms	No input filter
	...		
	Input 8	Active	
	Input 8 channel	Two channel	Input channel 1, monovalent
	Input 8 type	Monovalent	
	Input 8 discrepancy	5 ms	Discrepancy time to channel 2: 5 ms
	Input 8 filter	0 ms	No input filter
Profibus Master	Station address	0	
	Highest station address	2	
	Baud rate	12 000 kBit/s	
	Maximum number of repetitions in case of error	2	
	...		

Component	Parameters	Value	Meaning
Safety control	**Safety task:**		
	Priority	1	With respect to standard tasks
	Type	Externally event-controlled	Event_Safety Interrupt
	Cycle time	10 ms	Cycle time of safety logic
	...		
Drive with Safety on Sercos	Sercos address	1	
	Safety Network Number (SNN)	0x00060000xxxx	Date/Time format: Date is constant 0x0006, Time of 0x0001..270F is freely configurable. All targets need to have the same SNN as the CSos Originator
	Safety Device ID (SDID)	0x1	Safe address for the CIP Safety configuration. The originator and all targets require different addresses
	Network Time Expectation (NTE)	50	Transmission time from producer to consumer in the worst case
	Expected Packet Interval (EPI)	10	Cycle time of the CIP Safety connections
	Timeout Multiplier (TiMu)	2	The TiMu determines the number of CIP Safety telegrams that can be lost before the CIP Safety connection is closed. A TiMu of 1 indicates that no telegram can be lost. In case of an TiMu of 2, 1 telegram can be lost, etc.
	Ping Interval EPI Multiplier (PIEM)	19	The interval in which a time coordination is to be sent, is specified as a multiple of the EPI
	Time Coord. Msg. Min Multiplier (TCMM)	2	Minimum transmission time required for time coordination

Component	Parameters	Value	Meaning
	Max. fault number	5	Number of corrupt telegrams that may occur within one hour
	Timeout	1000	Time monitoring for connection establishment (Forward Open timeout)

Tab. 3-5: Parameterization of the safety-related components

3.6.7 Considered safety chain

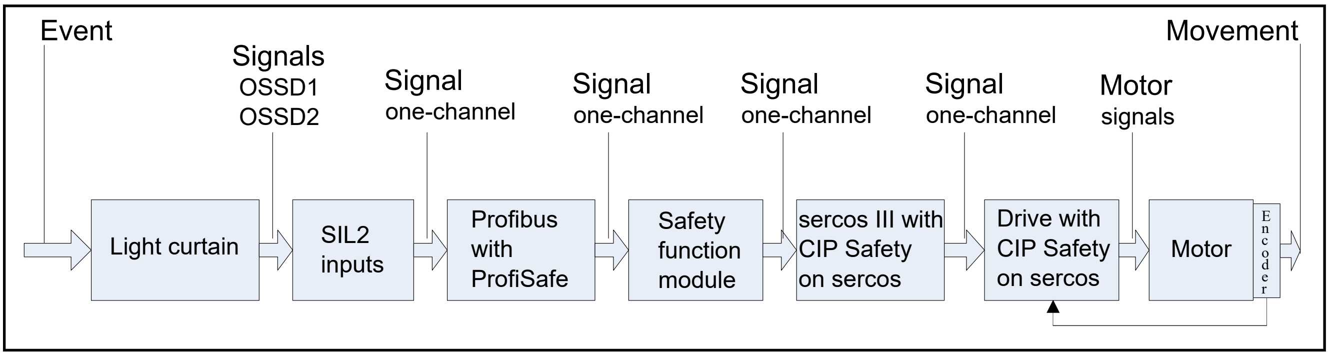
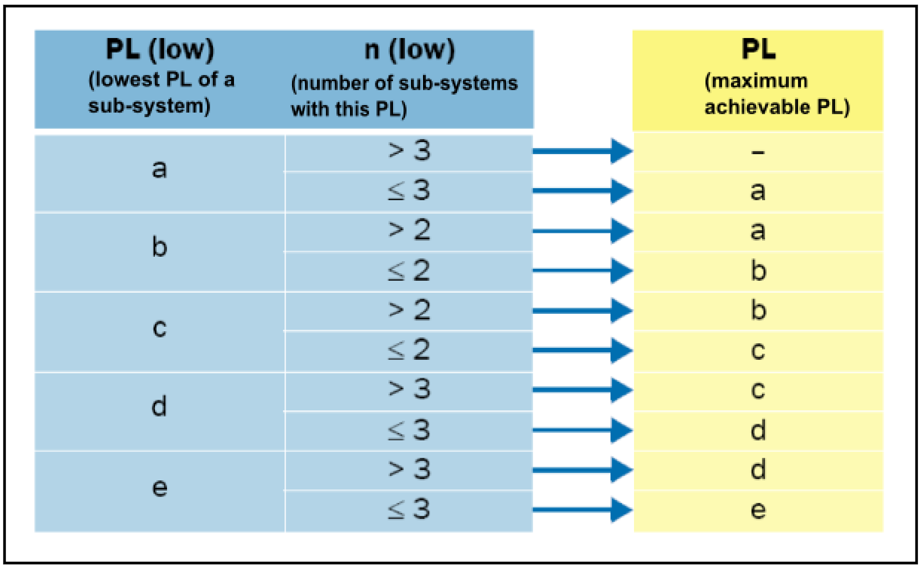


Fig. 3-17: Considered safety chain

3.6.8 Determining the achieved PL value according to EN ISO 13849-1

For this purpose, EN 13849-1 permits a simple procedure that can be used if the individual performance levels of the subsystems are known. The standard provides a table where the resulting PL value can be found after determining the lowest PL in the safety chain (PL low) and its frequency in the safety chain.



PL (low) (lowest PL of a sub-system)	**n (low)** (number of sub-systems with this PL)	**PL** (maximum achievable PL)
a	> 3	-
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

Fig. 3-18: PL determination for the safety function (simplified procedure)

According to the information on the subfunctions PL (low) = "d". This PL can be found twice in the entire safety chain, therefore the total PL of the safety function is PL "d", according to the table. The requirement specified at the input is thereby met.

3.6.9 Determining the achieved SIL according to EN 62061

Regarding the overall safety function, the hardware safety integrity is determined by the following:

- The lowest SILCL of a subsystem limits the maximum SIL of the overall system to be achieved
- The PFH_D of the entire chain is calculated from the sum of the individual PFH; the safety integrity level is read from the following table

Safety integrity level	Probability of a dangerous failure per hour (PFH)
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Tab. 3-6: Safety integrity level according to EN 62061

The calculation yields: $PFH_D = 0.7 \times 10^{-7}$

Assuming that all requirements according to EN 62061 for systematic safety integrity are met, safety function SF1 complies with the SIL2 requirement according to EN 62061.

3.6.10 Determining the required safety distance

The components have to be installed with a sufficient safety distance. The safety distance calculation formulas depend on the type of protection. For installation positions and calculation formulas, see standard EN 999 ("Positioning of safeguards with respect to the approach speeds of parts of the human body").

According to EN 999 the used light curtain belongs to category: "Electro-sensitive protective equipment using active opto-electronic protective devices with a detection capacity of a maximum of 40 mm in diameter".

General equation for the minimum distance from the protected area to the danger zone:

$$S = (K \bullet T) + C$$

S Minimum distance in mm, measured from the danger zone to the protected area
K Approach velocity in mm/s according to EN 999
T Lag of the overall system in seconds
C Additional distance in mm that is based on the intrusion into the danger zone prior to triggering the safety function.

Fig. 3-19: Minimum distance

The following applies to our example:

- K = 2000 mm/s
- C = 8 (d – 14 mm), but not less than 0

d is the detection capacity of the device in millimeters, i.e. 30 mm in this example.

T = T is generally subdivided in

- t1: The maximum time between triggering the sensor function and the time until the safeguard switches the output signal to OFF state

- t2: The response time of the machine, i.e. the time required until the machine is stopped or risks are removed after the safeguard transmits the output signal

Therefore:

- S = (2000 mm/s x T) + 128 mm

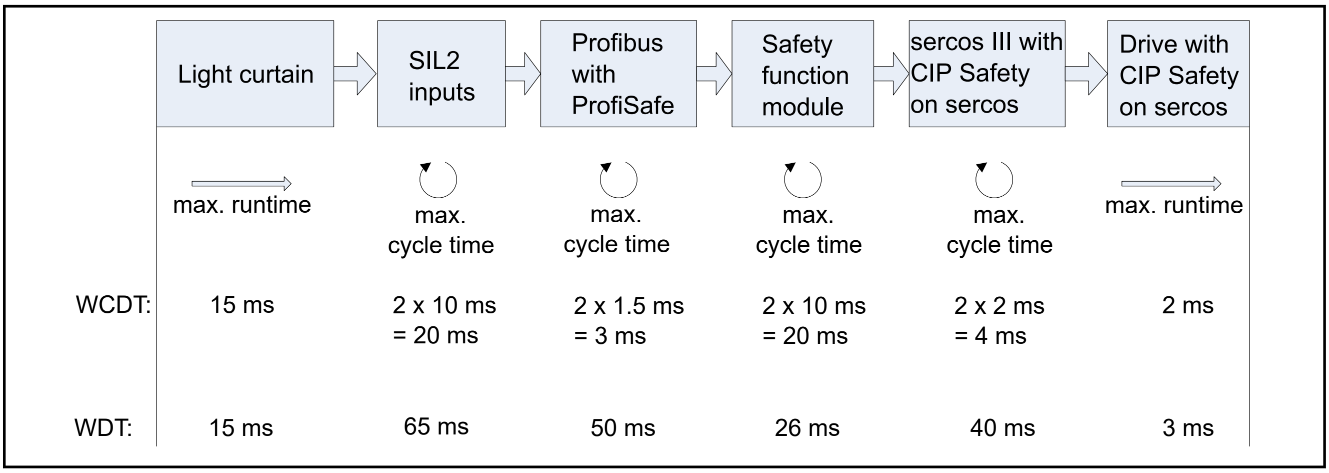
This equation applies to all minimum distances S up to and including 500 mm. The minimum value of S may not be less than 100 mm.

To calculate the required safety distance, determine time T:

- T = t1 + t2

Time "t2" is the maximum stopping time of the motor and includes the safe standstill message via the encoder to the drive safety logic and any required error reaction. The time depends on the used motor and encoder. The time determination is not explained in detail. In this example, "t2" is 150 ms.

Time "t1" consists of the individual worst case times of the subsystems in the safety chain from the light curtain to the input interface of the integrated drive safety function, considering all asynchronous procedures and any errors anywhere in the safety chain. Start calculation by using the worst case runtime in normal operation (no error occurred).



	Light curtain	SIL2 inputs	Profibus with ProfiSafe	Safety function module	sercos III with CIP Safety on sercos	Drive with CIP Safety on sercos
	max. runtime	max. cycle time	max. cycle time	max. cycle time	max. cycle time	max. runtime
WCDT:	15 ms	2 x 10 ms = 20 ms	2 x 1.5 ms = 3 ms	2 x 10 ms = 20 ms	2 x 2 ms = 4 ms	2 ms
WDT:	15 ms	65 ms	50 ms	26 ms	40 ms	3 ms

Runtime	Unique sequential runtime
Cycle time	Cycle time of an asynchronous unit
WCDT	Worst case runtime
WDT	Error monitoring time

Fig. 3-20: Time calculation of the safety function

WCDT is the worst case runtime of all components of the safety chain and WDT is the error monitoring/detection time of all components of the safety chain. With the light curtain and relays there is no internal monitoring and/or the maximum runtime in case of error is equal to the maximum runtime in normal operation (no error occurred).

WDT at the SIL2 inputs includes the time from detecting an input signal error, considering the parameterized discrepancy and filter time as well as the time for internal error diagnostics.

The PROFIsafe error reaction times differ for input and output transmissions. In addition to the bus runtimes and the maximum cycle and processing time of the concerned PROFIsafe master or slave instance, they take into account the F-Watchdog time, a so-called PROFIsafe F-Parameter.

When setting the F-Watchdog time, pay attention to safety considerations and to the availability of the transmission that depends on environmental conditions and EMC considerations, for example.

It is possible to configure the cycle time of the application for the Safety extension module. This cycle already includes the time of internal error monitoring. Therefore, the worst case cycle time remains valid in case of an error.

The required time for troubleshooting in the drive is already included in time "t2" = 150 ms. Therefore, only the response time of the drive in case of normal operation (no error occurred) has to be taken into account for "t1".

Based on these conditions, "t1" is calculated according to the general formula:

$$t_1 = \sum_{i=1}^{n} WCDT_i + \max_{1,2..n}(WDT_i - WCDT_i) = 63+50-3=110$$

Fig. 3-21: Response time of the safety chain

Thereby, T is: 110 ms + 150 ms = 260 ms = 0.26 s

In this time, a faulty drive movement has to be assumed in any case. Using this result in the formula for the required safety distance yields:

- S = (2,000 mm/s x 0.26 s) + 128 mm = 648 mm

If "S" is greater than 500 mm (as in this example), the assumed approach velocity may be reduced to 1600 mm/s. However, the distance may not be less than 500 mm.

This yields the following:

- S = (1600 mm/s x 0.26 s) + 128 mm = 544 mm

The light curtain therefore has to be installed at a 544 mm distance from the danger zone. Only then it is ensured that an operator entering the light curtain is not put at risk in case of an error.

3.6.11 Next steps

The structures, addresses and parameters specified in project planning, provide all input variables for the configuration of the safety system, parameterization of the components and the creation of the application program in the Safety extension module.

☞ Refer to the document "Rexroth IndraWorks 15VRS SafeLogic - Project Configuration" (see chapter 1.4 "Required and supplementing documentation" on page 2)

4 System overview

4.1 Overview

The safety solutions "SafeLogic" and "SafeLogic compact" facilitate a freely programmable, safe logic processing.

The **SafeLogic compact** Safety system is composed of the following components:

- Safety CPU
- Safety I/O
- Safety gateway for Sercos
- Safe drives

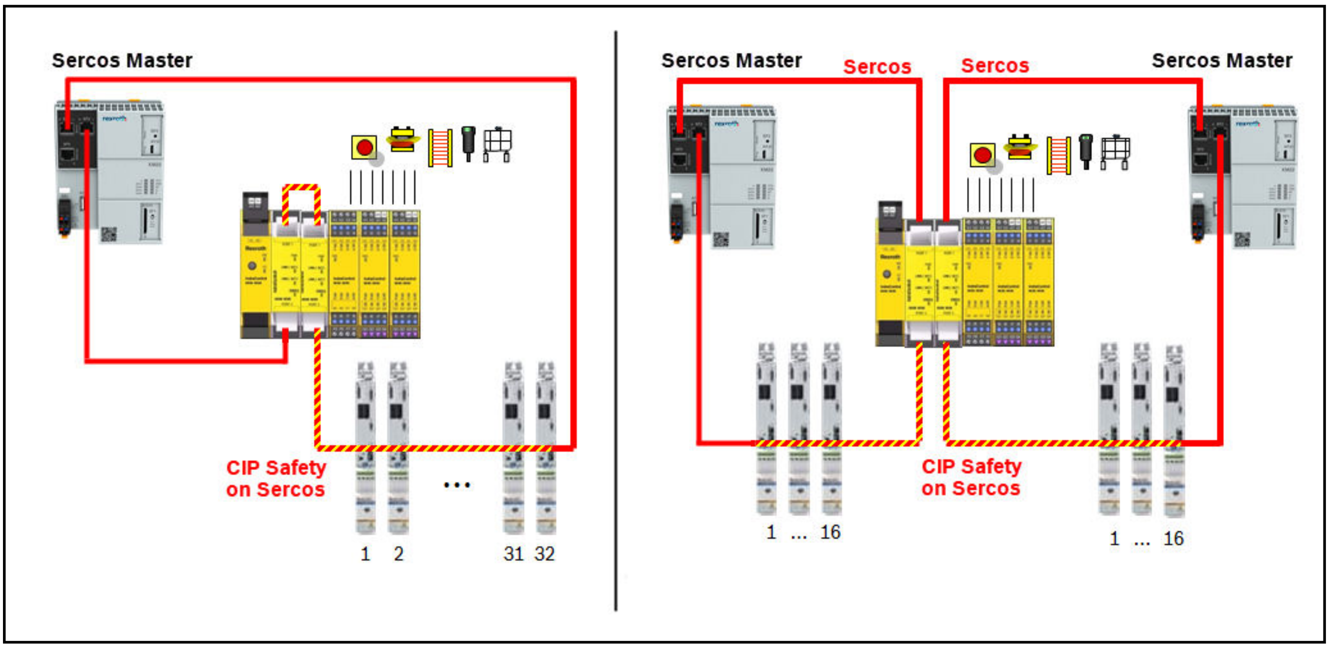


Fig. 4-1: Example topologies of SafeLogic compact with Sercos

The **SafeLogic** safety system is composed of the following components:

- Safety extension module as component of Rexroth controls
- Safety I/O via Profibus, Profinet and Sercos
- Safe drives via Sercos
- Safe network variables

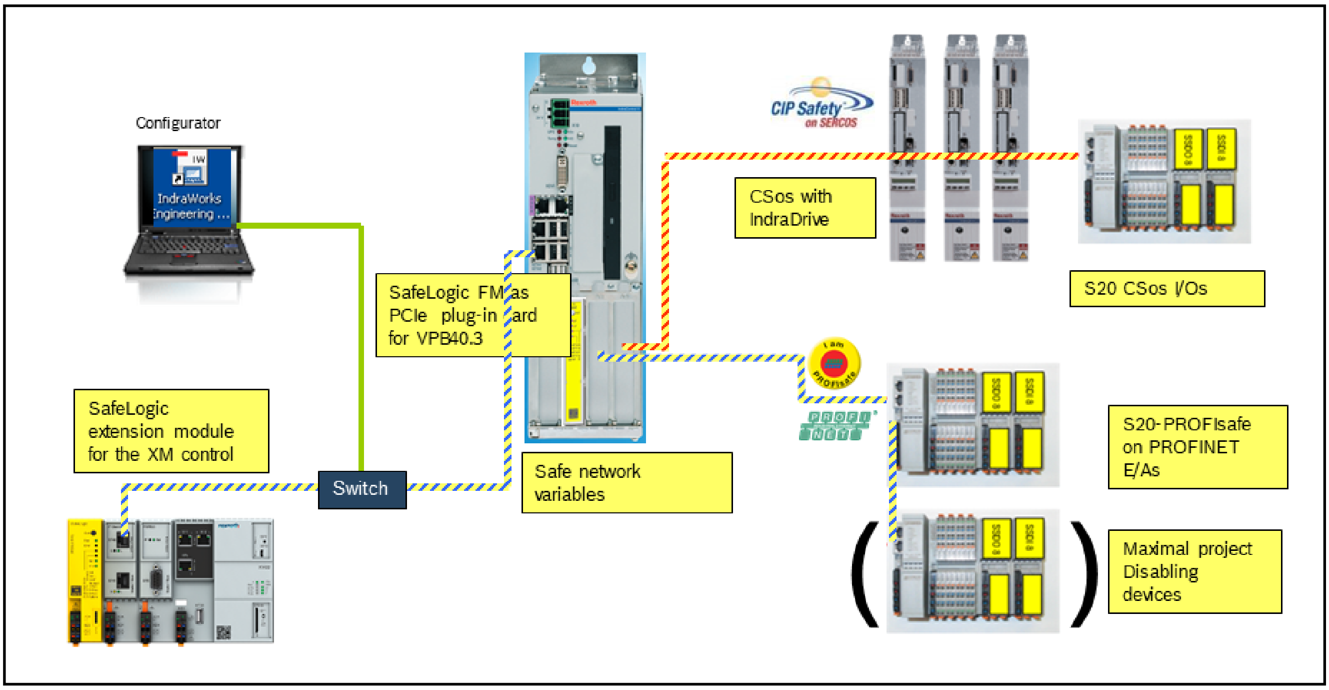

Configurator
IW
IndraWorks Engineering ...
SafeLogic extension module for the XM control
Switch
SafeLogic FM as PCIe plug-in card for VPB40.3
Safe network variables
CIP Safety on SERCOS
CSos with IndraDrive
S20 CSos I/Os
PROFIsafe
PROFI NET
S20-PROFIsafe on PROFINET E/As
Maximal project Disabling devices

Fig. 4-2: System overview SafeLogic

4.2 Areas of application

SafeLogic as well as SafeLogic compact are intended for use in factory automation. Both system use the fail-safe principle.

The de-energized state is the safe state:

- All outputs are disabled
- Inputs report "Zero" to the control

SafeLogic compact is certified according to IEC 61508 and EN ISO 13849-1 and is approved for the following application:

- up to SIL3 according to EN 61508
- up to SILCL3 according to EN 62061
- up to PLe according to EN ISO 13849-1

SafeLogic Safety extension module is certified according to IEC 61508 and EN ISO 13849-1 and is approved for the following application:

- up to SIL3 according to EN 61508
- up to SILCL3 according to EN 62061
- up to PLe according to EN ISO 13849-1

Safety functions cover a wide range from sensor to actuator. According to the risk classification by the risk analysis, the Safety functions required an appropriate resistance against the loss of the Safety function. Safety extension module as well as SafeLogic compact are only one part of the entire Safety function.

The actual degree of safety depends on the external wiring, the wiring design, the parameterization, the selection of the command initiators and their locations at the machine.

4.3 System requirements

☞ For the system requirements of the installation and operation of **SafeLogic compact** development tools, refer to the SafeLogic compact Designer Software documentation in the Rexroth media directory

☞ The system requirements for **SafeLogic** development tools are contained in the "Project Configuration" documentation in the Rexroth media directory

4.4 Safety controls

4.4.1 SafeLogic compact

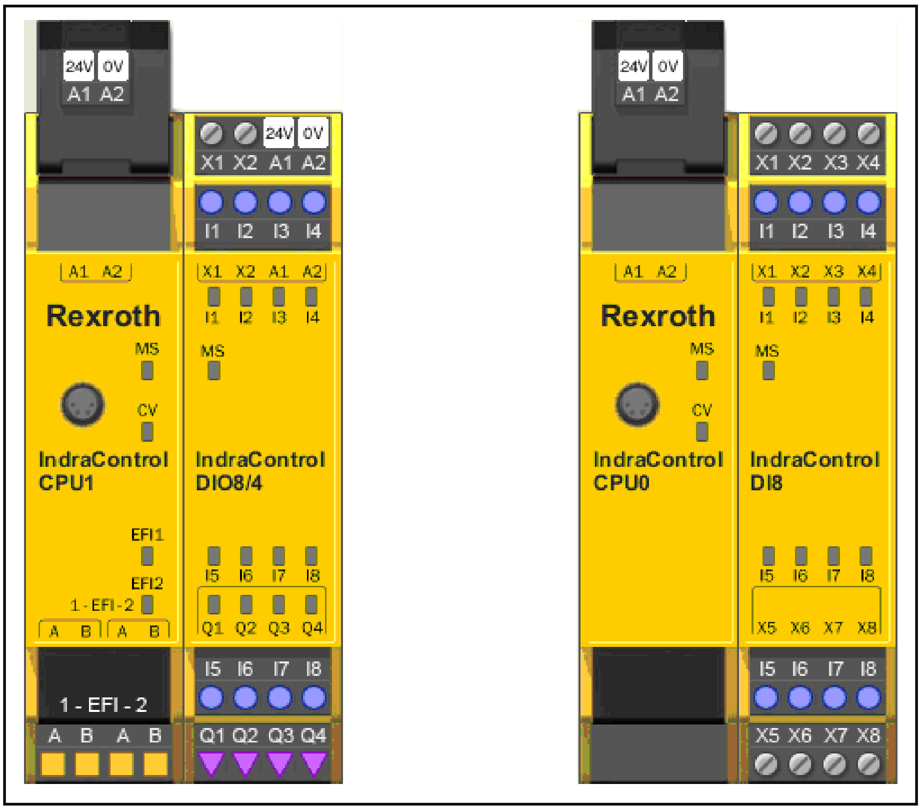


Fig. 4-3: Examples of the minimum design of a SafeLogic compact system with CPU0 and XTDI or CPU1 and XTIO

SafeLogic compact can be used for Safety projects with a locally limited number of safe I/Os.

System properties

- Modular design: 1 main module, up to 2 different gateways and up to 12 input/output extension modules, each with a compact width of 22.5
- 8 to 96 one-channel inputs and 4 to 48 one-channel outputs
- Programmable
- Use of up to 255 standard-specific and application-specific logic blocks
- Standard logic blocks, such as
  - AND
  - OR

  - NOT
  - XNOR
  - XOR
- Application-specific logic blocks, such as
  - E-Stop
  - Two hand
  - Muting
  - Presses
  - Lagging detection
  - Operation mode selection switch
  - Reset
  - Restart
- Can be integrated in different field buses with gateways
  - Profinet I/O Gateway for diagnostics
  - Profibus DP Gateway for diagnostics
  - Sercos Gateway to connect up to 16 CIP Safety on Sercos targets (drives/IndraDrive) at a Sercos Gateway. Therefore, there is no discrete drive wiring

CPU modules

The following CPU modules are available:

Type	Name	Inputs	Outputs	Max. number in the system	Part number
SLC-3-CPU0	Main module	–	–	1	R911172284
SLC-3-CPU1	Main module	2 x EFI	–		R911172285
SLC-3-CPU3	Main module	2 x EFI 2 x Flexi Line	–		R911173402

Tab. 4-1: SafeLogic compact CPUs

Extension modules

More modules can be connected to the CPU module. The following modules are supported:

Type	Name	Inputs	Outputs	Max. number in the system	Part number
SLC-0-GPNT	Profinet I/O Gateway	2	–	2	R911172290
SLC-0-GPRO	Profibus DP Gateway	1	–		R911172287
SLC-3-GS3S	Sercos Gateway	2	–		R911172765
SCL-3-XTIO	Input/output extension	8	4	12	R911172291
SLC-3-XTDI	Input extension	8	–		R911172292

Type	Name	Inputs	Outputs	Max. number in the system	Part number
SLC-3-XTDS	Eight safe inputs and four or six unsafe outputs	8	4/6	12	R911173404
SLC-3-STIO	Six or eight unsafe inputs, six or eight unsafe outputs	6/8	6/8	12	R911173405
SLC-3-MOCx	Connection and safe evaluation of two encoders	2	–	6	R911173406
UE410-2RO	Relay output extension	–	2	8[1)]	R911172293
UE410-4RO	Relay output extension	–	4	4[1)]	R911172294

[1)] In combination max. 16RO

Tab. 4-2: Extension modules for SafeLogic compact CPU

EFI link

With the EFI link, it is possible to combine up to four SafeLogic compact stations via EFI for a **safe data exchange**. Only SLC-3-CPU1 modules can be used in an EFI Link system. The connection of SLC-3-CPU0 modules is not possible. The process data of all stations (inputs and outputs, logic results, etc.) can be provided to all other stations in the EFI link system. The “Teach” function allows to temporarily deactivate single stations without impairing the function of the overall system

Moreover, it is possible to connect EFI-compatible Safety sensors by SICK (e.g. Safety laser scanner, light curtains).

The XTIO extension module provides the option of "fast shut-off". By direct shut-off on the extension module, shut off times of 8ms can be reached, irrespective of the logic cycle time.

If shielding is required, for example due to EMC reasons, when connecting the EFI devices, use an earth terminal that is placed in the control cabinet near the SafeLogic compact main module for this purpose. Connect the grounding terminal to the shielding.

Flexi Line

Flexi Line enables you to safely network up to 32 SafeLogic compact stations. Only SLC-3-CPU3 modules can be used in a Flexi Line system. It is not possible to connect any other main modules (SLC-3-CPU0, SLC-3-CPU1).

.The EFI interface remains available without restrictions.

The process image can have a size of 12 bytes or 96 bits.

The maximum cable length between two stations is 1.000 meters. The total possible length of a system with 32 stations is therefore 31 kilometers.

Technical data of the CPUx

For technical data, refer to the SafeLogic compact operating instruction in the Rexroth media directory.

4.4.2 SafeLogic

The SafeLogic control provides the resource to process safety-oriented application programs and to connect Safety periphery. A Safety control extends the function control. The SafeLogic uses the field bus connectivity of the function control. The SafeLogic control is available in several designs for the embedded controls XM21, XM22 and XM42 and the panel PCs V.

Standard and Safety periphery (Safety I/O, safe drives, ...) can be operated at the same communication system. The safe data are transferred via the corresponding Safety protocols.

The Rexroth SafeLogic control supports the following safe periphery components:

- Rexroth SIL3 I/O system
- Rexroth IndraDrive with integrated Safety technology

SafeLogic control characteristics:

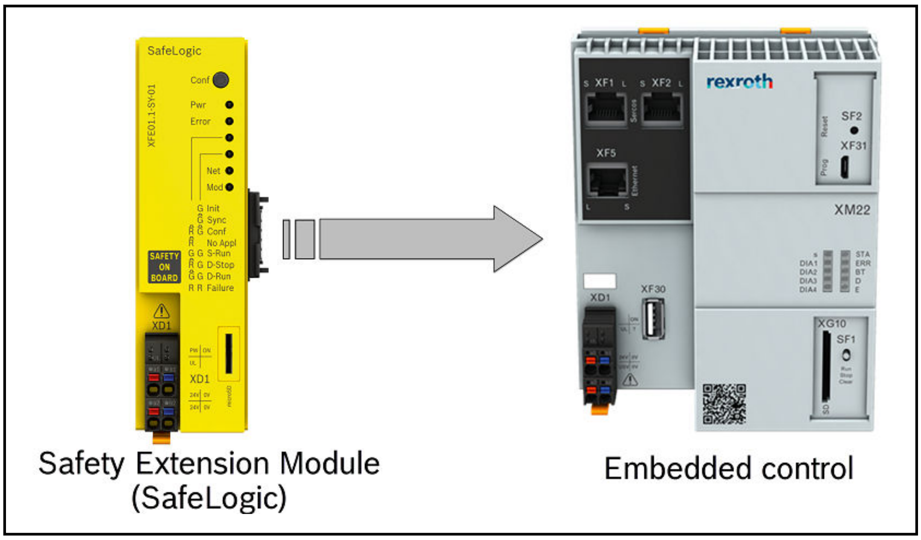


Fig. 4-4: Extension module "Safety CPU (XFE01.1-SY-01)" for embedded controls XM

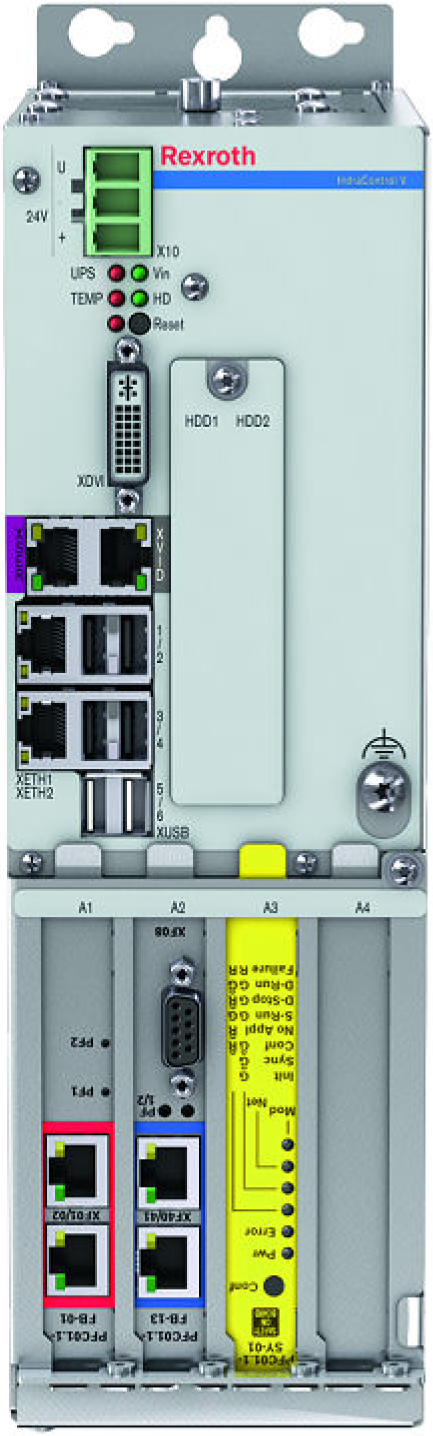


Fig. 4-5: PFC01.1-SY-01 extension card installed in a VPx control (box PC)

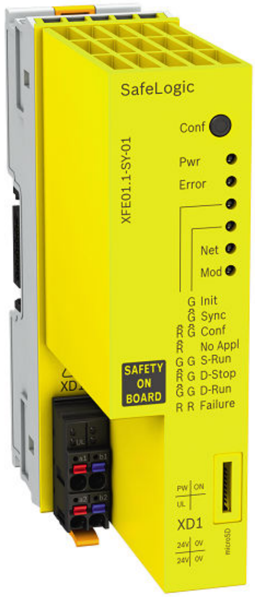


Fig. 4-6: Extension module XFE01.1-SY-01 for the XMxx control

System properties

- XFE01.1-SY-01: align to the left of the control variants XM21, XM22 and XM42
- PFC01.1-SY-01: installed as plug-in card in the VPx control (box PC)
- Up to 99 safe devices (I/O modules and axes)
- Up to 96 axes with Safety control circuit
- Can be programmed, see documentation "SafeLogic Project Configuration"
- Connected to different field busses via the control
  - Profibus DP via PROFIsafe on Profibus
  - ProfiNetIO via PROFIsafe on ProfiNet
  - Sercos via CIP Safety on Sercos
  - Safe cross communication

Technical data

For technical data, refer to the documentation in the Rexroth media directory:

- Operating instructions XFE01.1-SY-01
- Operating instructions PFC01.1-SY-01

Related documentation

For further documentation, refer to chapter 1.4 "Required and supplementing documentation" on page 2.

Hardware portfolio

For more information about the hardware of the Rexroth Inline system, refer to chapter 5 "Safe bus systems" on page 55.

4.5 Safe communication

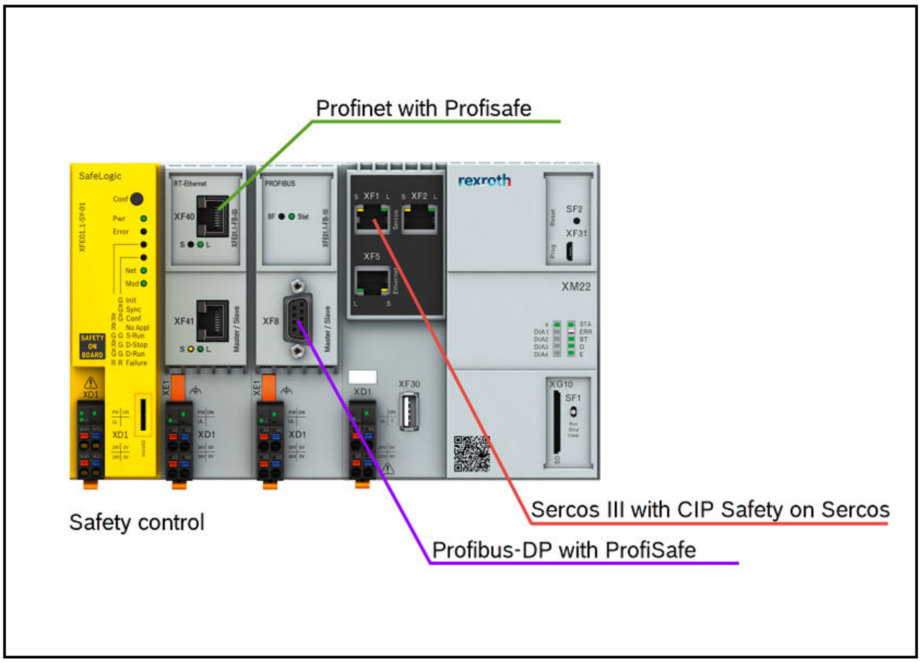

Profinet with Profisafe
Safety control
Sercos III with CIP Safety on Sercos
Profibus-DP with ProfiSafe

Fig. 4-7: Safe communication interface

The following Safety protocols are used to transfer safe data:

- CIP Safety on Sercos (CSos)
- PROFIsafe
- Safe cross communication (safe network variables)

The following can be used as physical media:

- Profibus DP (with PROFIsafe)
- Profinet I/O (with PROFIsafe)
- Sercos (with CSos)
- Ethernet (with safe cross communication)

4.6 System setup

SafeLogic compact

A SafeLogic compact system consists of the following modules:

- a memory plug SLC-3-MPL
- a main module SLC-3-CPU0, SLC-3-CPU1 or SLC-3-CPU3
- Up to two gateways
- Up to 12 additional I/O extension modules, e.g. SLC-3-XTIO, SLC-3-XTDI and SLC-0-STIO
- Up to 8 UE410-2RO relay output modules and/or 4 UE410-4RO relay output modules (i.e. up to 16 safe relay outputs)

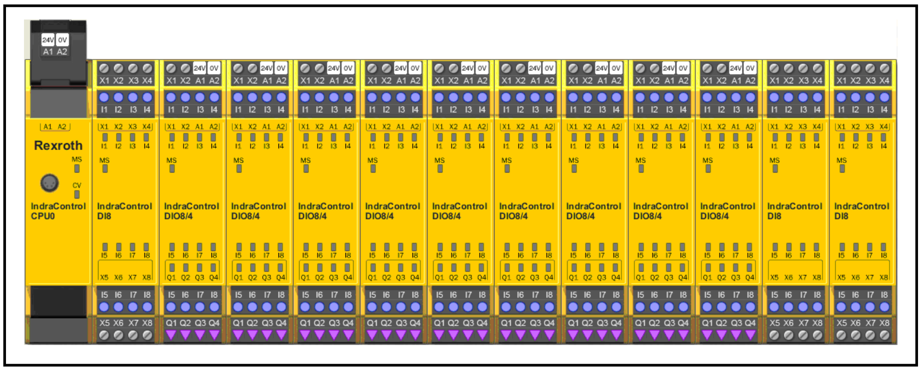


Fig. 4-8: Maximum setup of a SafeLogic compact system (without relay output extensions and gateways)

The safe I/O directly connected to the CPU module is protected by the internal bus.

SafeLogic

The Safety extension module is available to all resources as optional extension module of the standard control for safe logic processing. Between the end devices of a data connection, e.g. between Safety extension module and Safety I/O, the information is exchanged as safe data telegrams. If the devices detect that the received data is incorrect or that there is a communication error, the devices go to a defined, safe fault reaction state. The transmission path thus becomes the "Black channel" and does not affect the safety, irrespective of which media or which transmission path is selected.

The following safety protocols are supported:

- PROFIsafe
- CIP Safety on Sercos
- Safe cross communication

Both protocols are supported simultaneously so that CIP Safety as well as PROFIsafe devices can be operated simultaneously.

The Safety extension module does not have any own interfaces. The module uses the interface of the standard control. Thus, the operation of safe and not safety-relevant devices can be at one and the same communication medium is possible.

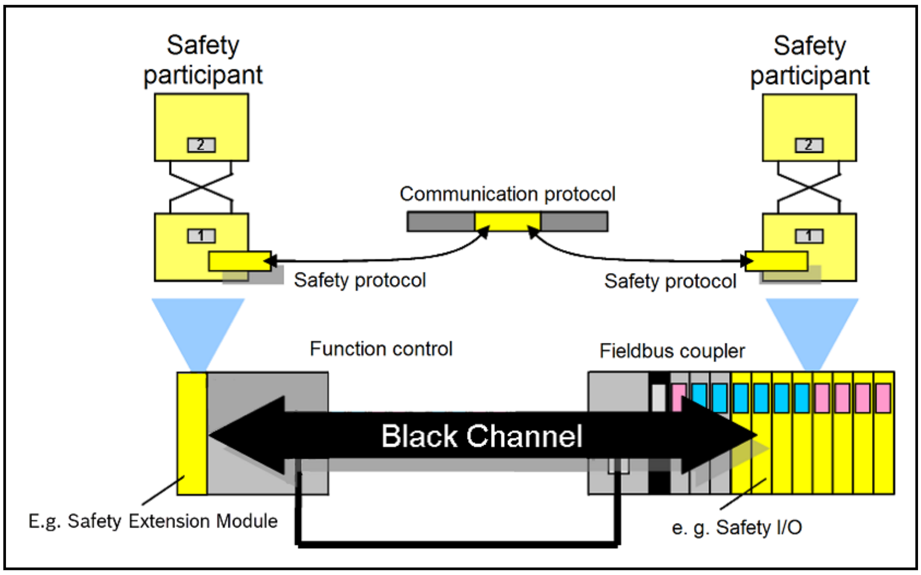


Fig. 4-9: Functional principle

According to the requirements of the applied Safety standards, the Safety application is processed as enclosed by the standard application on the Safety extension module in a dual-channel. The Engineering system provides a universal project view to the user and provides the data exchange between safety-relevant application and an application that is not safety-relevant.

The Safety extension module exclusively controls the Safety devices and acts as enabling unit of the process control. A Safety output only becomes "TRUE" if the process signal and the Safety signal are "TRUE".

4.7 ILC – IoT-compatible PLC system

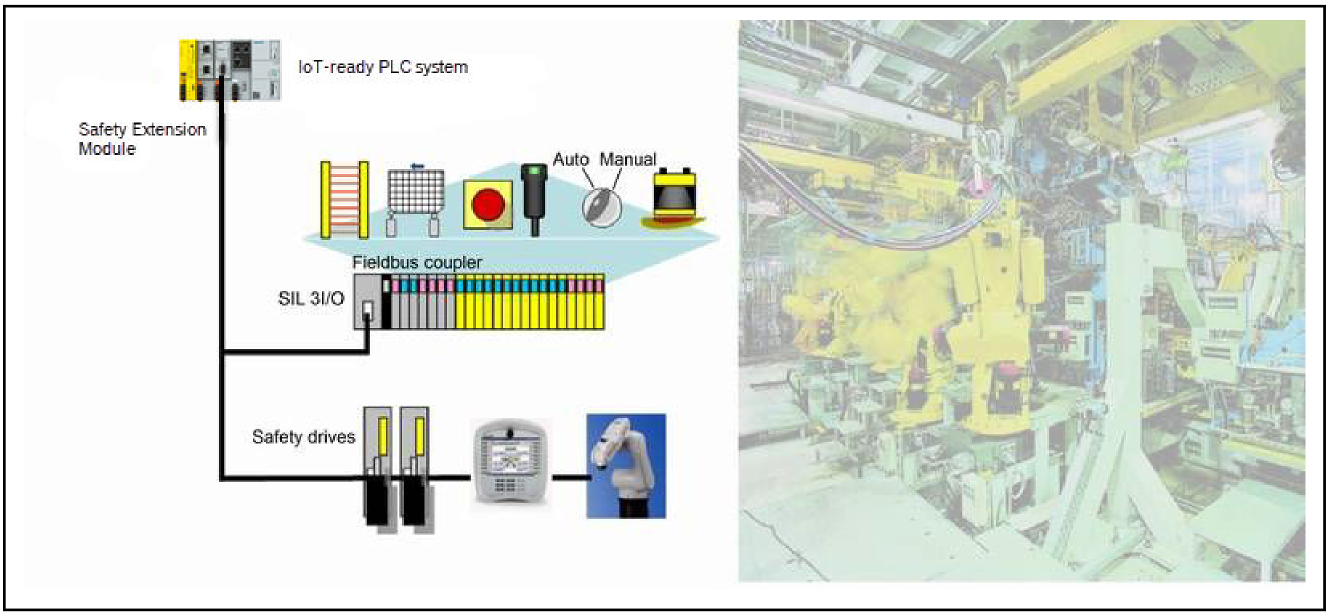


Fig. 4-10: Example of the IoT-capable PLC system ILC mounting/core

The example shows the application of the Safety engineering of an assembly cell in body-in-white. The workspace of several linked robots is to be protected by isolating protective equipment. The operator requires access, to eliminate process malfunctions or material faults or to set up the robots, e.g. for new production orders. Linking of the periphery signals (emergency stop, door monitoring, light barriers, laser scanners, robots, etc.) takes place on the Safety extension module which is an integral part of the system solution. Safe motion functions are provided by the safe drive technology. Requirements such as ISO 10218 can be implemented safely and user-friendly using the "Safety on Board" safety system.

⚠ DANGER

Always comply with the current standards and regulations that apply for the use case and the respective country!

Further information

Refer to chapter 1.4 "Required and supplementing documentation" on page 2

4.8 MLC – System solutions for Motion Logic applications

Amongst others, the MLC system is used in printing presses. The safety requirement for printing presses are specified in the C-standard EN 1010-1

"Safety of machinery — Safety requirements for the design and construction of printing and paper converting machines — Part 1: Common requirements".

The requirements on the EMERGENCY STOP are specified in ISO 13850. The requirements for safety-relevant parts of the electric/electronic control are specified in the B1 standard ISO 13849-1.

The example shows the application of the Safety engineering at a printing tower of a newspaper rotary printing machine. The individual print positions are protected by isolating protective equipment. The safety of the motion functions is ensured by the safe drive technology. Linking of the periphery signals (door monitoring, zone protection, stop/locking etc.) takes place on the Safety extension module which is an integral part of the MLC system. The requirements of EN 1010 and EN 415 are met using the "Safety on Board" safety system.

⚠ DANGER	Always comply with the current standards and regulations that apply for the use case and the respective country!

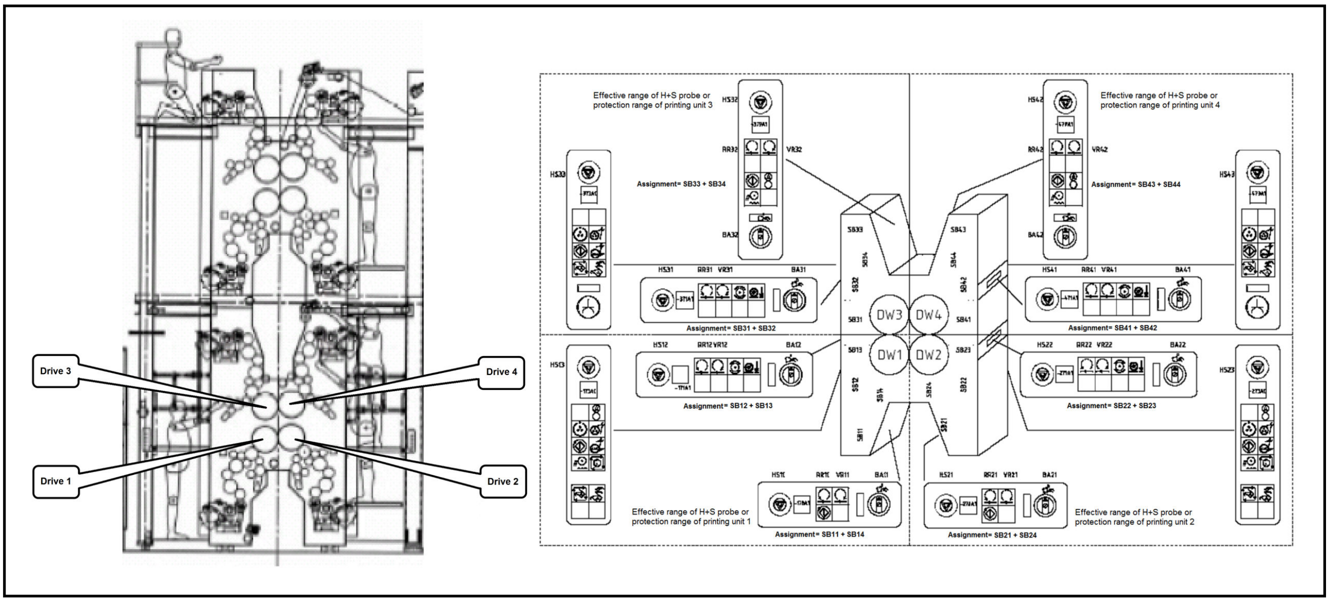


Fig. 4-11: Model of a typical printing tower

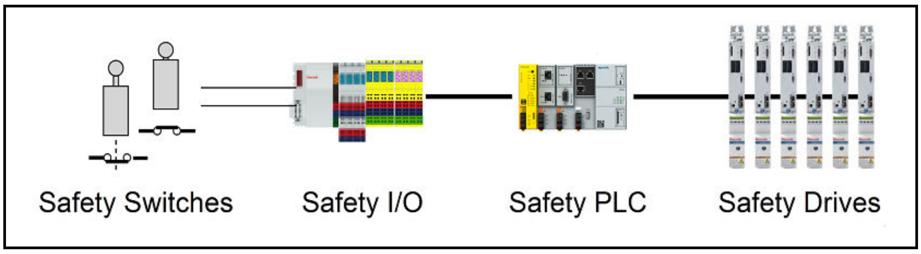


Fig. 4-12: Functional chain of logic operations from sensors to actuators

Further information

Refer to chapter 1.4 "Required and supplementing documentation" on page 2

5 Safe bus systems

5.1 Overview

Standard bus systems

The safe data transmission in Bosch Rexroth safety systems is realized via the Sercos and/or Profibus DP and/or Profibus I/O bus systems, together with the standard process data transmission.

Profibus-DP is specified in IEC 61158 and IEC 61784. For more information about Profibus DP, refer to the Profibus user organization - Profibus Nutzer-organisation e. V. (PNO).

Profinet is defined by Profibus & Profinet International (PI) and is part of the IEC 61158 and IEC 61784-2 standards since 2003.

Sercos is the third generation Sercos interface according to IEC/EN 61491, based on standard Ethernet IEEE 802.3. Sercos belongs to the international standards IEC 61800-7, IEC 617843 and IEC 611584. For further information on Sercos, contact Sercos International e. V. (SI).

Secure data transfer

The safe data transmission is implemented in the standard bus systems via the safety-oriented application profiles.

PROFIsafe is the safety-oriented application profile for Profibus DP and Profinet and internationally in the IEC 61784-3-3.

Sercos Safety is the safety-oriented application profile for Sercos. CIPsafety is the basis, the safety-oriented extension of the Common Industrial protocol (CIP), specified by the ODVA (Open DeviceNet Vendor Association) for Ethernet IP and DeviceNet.

5.2 General information for safe data transfer

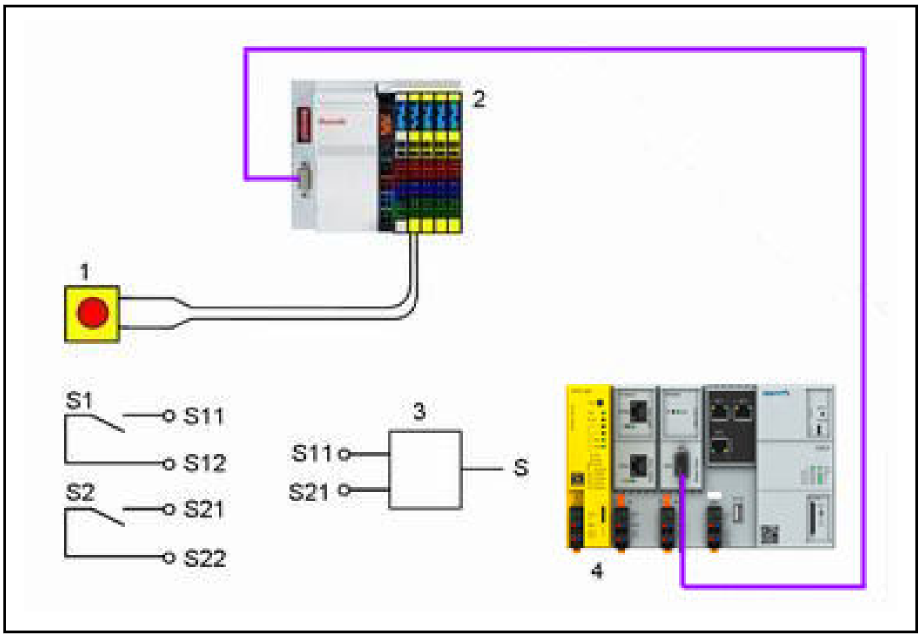
Essential features of safe data transfer, irrespective of the used bus system:

- The safe data transfer between the Safety extension module (host) or the SafeLogic compact CPU module and the safety-oriented bus devices (slaves) is always based on an individual, unique communication relation that is time-monitored
- The safety-related data is realized as protected data containers in the user data stream of the bus protocols. The protocol mechanisms of the buses are not used to generate the safety. The safety-related data is thus neither changed nor extended and correspond to the standard protocols. Safe data transfer and standard data transfer is executed non-reacting in co-existence
- Telegrams with safe data and telegrams with standard data use the same physical characteristics. The transfer channels, starting from the electronics via the connectors up to the transmission cables do not influence the safety. These transfer channels are referred to as black channels and can be assumed to be faulty without the safety being compromised by this characteristics. The high availability requirements on safe data transfer are met by standard bus systems if the specified ambient conditions are complied with
- The safety is exclusively ensured by the safe software in the Safety extension module (Safety Host Layer) and the safe software in the safe devices (Safety Slave Layer). Transfer safety refers to freedom from potential transmission errors:
  - Loss of telegrams
  - Incorrect repeating of telegrams

  - Inserting telegrams
  - Incorrect sequence
  - Invalid data delay
  - Data delay

  The measures to handle these errors depend on the Safety bus

- The Safety layers are an additional layer of the ISO-OSI model (Open Systems Interconnection Reference Model) above the application layer. In the Safety extension module, there is an individual Safety host layer for each communication relation that has to be implemented as function block instance in the safe program and whose input/output parameters are the interface to the Safety logic
- The safe data transfer is always realized via one channel, irrespective of whether sensors and actuators are connected as one channel or dual channel. Two bits of two periphery channels are mapped on safe transmission bit in case of this one-bit principle. The one bit-principle is applied in the data communication as well as in the Safety logic. By introducing the variable types Safe Bool, Safe byte, Safe int, ...the one-bit principle has been taken account of in the Safety logic



1 EMERGENCY STOP operating device, dual-channel port
2 Safe input device, two input terminals connected
3 Logic processing in the safe input device (two input bits are summarized to one transfer bit (SafeBool))
4 Embedded control XM2x with Safety extension module with safety logic

Fig. 5-1: One-bit principle

5.3 Hardware for Rexroth Inline system

Introduction

The Rexroth Inline system integrates I/O modules (Inline terminals) of the embedded control Inline bus.

Safe Inline terminals are colored yellow. The safe communication is realized via PROFISafe.

Profibus Inline bus coupler

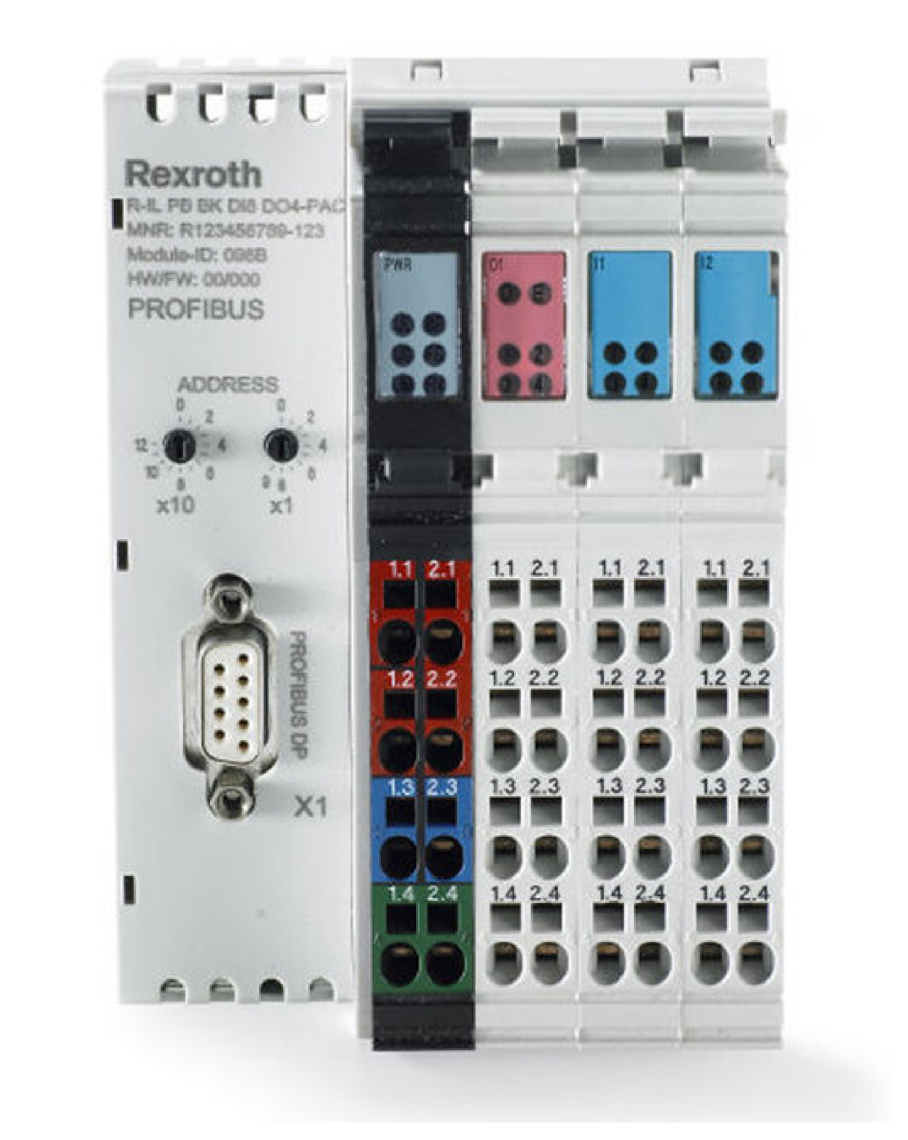


Fig. 5-2: Rexroth Profibus Inline bus coupler

The Profibus Inline bus coupler integrates the embedded control Inline bus I/O modules into the Profibus DP. Profibus structurally permits the connection of up to 125 field bus couplers with 61 additional I/O modules each. The maximum number depends on the DP master and the user data of the connected I/O modules.

Type code: R-IL PB BK DI8 DO4/CN-PAC

Part number: R911172194

Overview on the field bus coupler features:

- Eight digital inputs, type 1, 24 V DC
- Four digital outputs, 24 V DC, 0.5 A
- Extendable with modules by up to 61 external I/O modules
- up to 6 safe I/O modules can be connected (the max. number results form the number of assigned bytes in the configuration channel (max. 230 bytes), see tab. 5-2 "PROFIsafe channel assignment by Safety Inline terminals" on page 60). Each safe I/O module has a PCP channel

- Up to 16 devices can be connected. Each safe Inline I/O module represents a PCP device
- Maximum of 244 bytes in each data direction of the process data
- Parameterization and configuration via GSD including diagnostics

For a detailed description, refer to the documentation

- "Rexroth Inline Bus Couplers for Profibus-DP R-IL PB BK DI8 DO4/CN-PAC", part number R911324349

Only the first PROFIBUS master (extension module Profibus (XFE01.1-FB-10)) is intended for the PROFIsafe device operation at the XM2x and XM4x standard controls.

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapter "Inline Profibus coupler R-IL PB BK DI8 DO4/CN"

Profinet Inline bus coupler

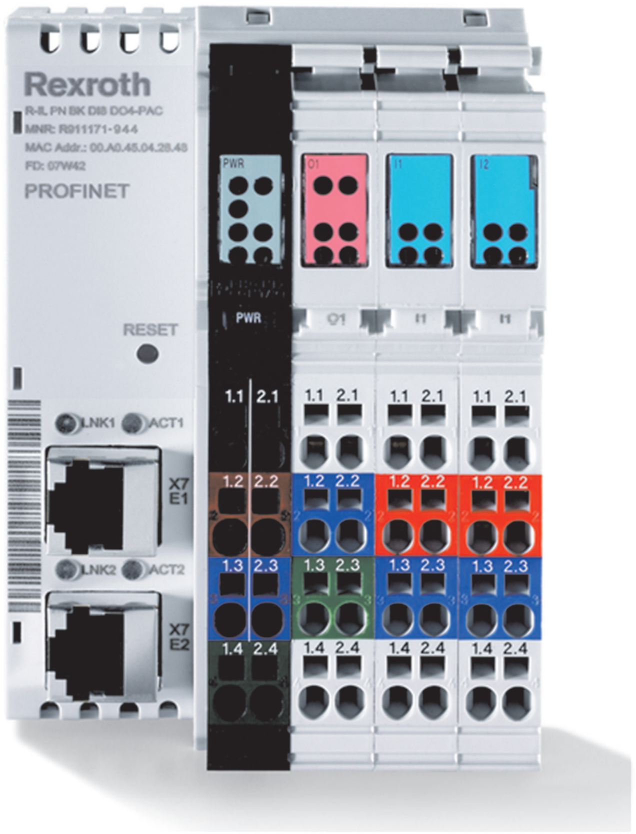


Fig. 5-3: Rexroth Profinet Inline bus coupler

The Profinet Inline bus coupler integrates the embedded control Inline bus I/O modules into the Profinet. Profinet structurally permits the connection of up to 125 field bus couplers with 61 additional I/O modules each. The maximum number depends on the used Profinet master and the user data of the connected I/O modules.

Type code: R-IL PN BK DI8 DO4-PAC

Part number: R911171944

Overview on the field bus coupler features:

- Eight digital inputs, type 1, 24 V DC
- Four digital outputs, 24 V DC, 0.5 A
- Extendable with modules by up to 61 external I/O modules
- up to 16 safe I/O modules can be connected
- A maximum of up to 16 PCP devices can be connected. Each safe Inline I/O module represents a PCP device
- Typ. 512 bytes in each data direction of the process data
- Parameterization and configuration via GSDML including diagnostics

For a detailed description, refer to the documentation

- "Rexroth Inline Bus Couplers for Profinet with Digital Inputs and Outputs R-IL PN BK DI8 DO4-PAC", part number R911328681

- The Profinet Inline bus coupler requires at least firmware version 3.30 to use the Inline PROFIsafe modules (PSDx)
- Only the first PROFINET controller (extension module RT-Ethernet (XFE01.1-FB-03)) is intended for the PROFIsafe device operation at the XM2x and XM4x standard controls.

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapter "Inline Profibus coupler R-IL PN BK DI8 DO4"

Inline modules

The Rexroth Inline system for Profibus and Profinet consists of the following PROFIsafe-compatible components:

Type code	Brief description	Part number
R-IB IL 24 PSDI 8-PAC	PROFIsafe module with 8 safe digital inputs; DC 24 V	R911172846
R-IB IL 24 PSDI 16-PAC	PROFIsafe module with 16 safe digital inputs; DC 24 V	R911173314
R-IB IL 24 PSDO 8-PAC	PROFIsafe module with 8 safe digital inputs; DC 24 V	R911172847
R-IB IL 24 PSDOR 4-PAC	PROFIsafe module with 4 safe relay outputs	R911172848
R-IB IL 24 PSDO 4/4-PAC	PROFIsafe module with 4 safe digital outputs; configurable positive or negative switching	R911172849

Tab. 5-1: Overview PROFISafe I/O modules

Fig. 5-4: PROFIsafe-compatible I/O modules

The Inline terminals assign the following number of bytes in the configuration channel:

Safety Inline terminal	Communication data	Number of bytes in the configuration channel
R-IB IL 24 PSDI 8	8	54
R-IB IL 24 PSDI 16	16	36
R-IB IL 24 PSDO 8	8	60
R-IB IL 24 PSDO 4/4	8	48
R-IB IL 24 PSDOR 4	8	48

Tab. 5-2: PROFIsafe channel assignment by Safety Inline terminals

These PROFIsafe inline modules can be connected the Inline bus couplers.

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapters "Inline PSDI 8 and PSDI 16 (PROFIsafe Data Input)" and "Inline PSDO 8 and PSDOR 4 (PROFIsafe Data Output)"

5.4 Hardware of the Rexroth embedded control S20 system

Introduction

Embedded control S20 of Bosch Rexroth is a high-speed real-time I/O system.

The communication to the superordinate system is realized via an Ethernet-based protocol (e.g. Profinet or Sercos).

Within the embedded control S20 product family, modules with different functions are available, e.g. bus coupler, standard input and output modules, safe input and output modules, modules for temperature recording, etc.

Safe embedded control S20 terminals are yellow. The safe communication is realized via "CIP Safety on Sercos" (CSos).

Sercos bus coupler S20-S3-BK+

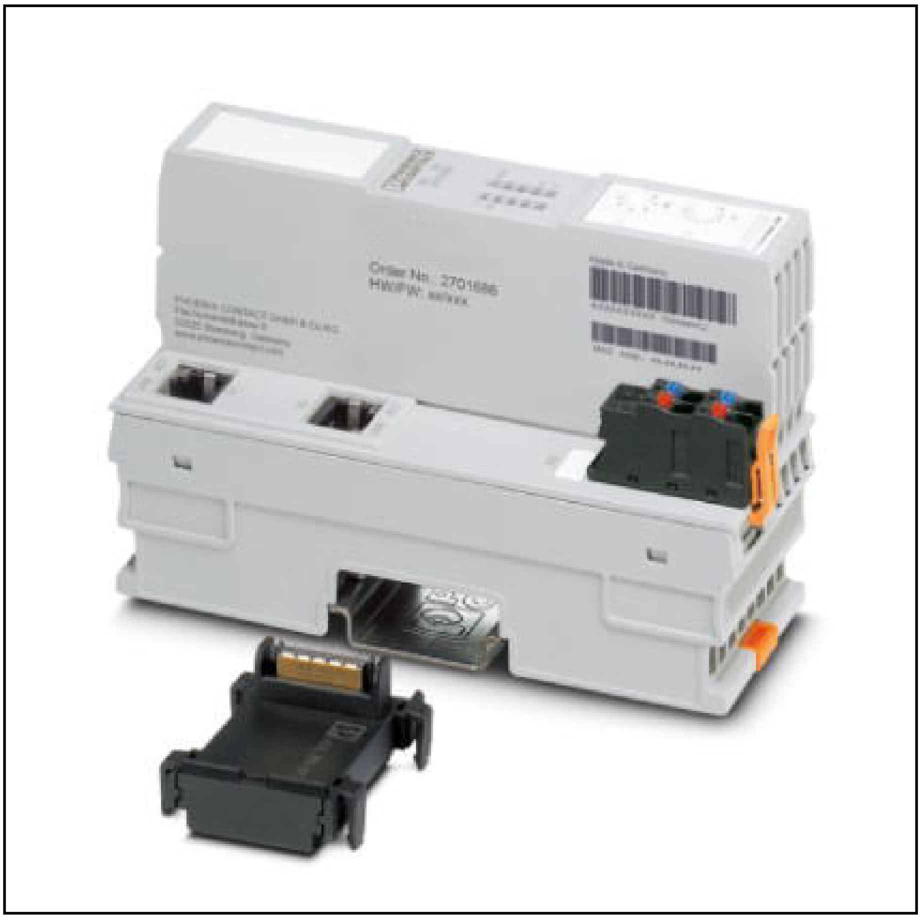


Fig. 5-5: Rexroth Sercos bus coupler S20-S3-BK+

The bus coupler is intended for use within a third generation Sercos network and is the link to the embedded control S20 system.

It is modular extendable with S20 modules. Using the bus coupler, up to 63 S20 devices can be connected to an existing Sercos network.

Type code: S20-S3-BK+

Part number: R911173318

Overview on the field bus coupler features:

- 2 Ethernet ports
- Transfer rate 100 Mbit/s at a minimum Sercos cycle time of 31.25 μs
- Sercos diagnostic LED
- Support of up to 63 Safety I/O modules (CSos I/O modules)

  The number of CSos I/O modules that can be connected is limited by the power input from the logic voltage of the bus coupler

The following CSos I/O modules can be operated at the Sercos bus coupler S20-S3-BK+:

Type code	Brief description	Part number
S20-SSDI-8/4	8 one-channel or 4 dual-channel safe inputs in 4-wire connection method	R911173191
S20-SSDO-8/3	8 one-channel or 4 dual-channel safe outputs in 3-wire connection method	R911173192

Tab. 5-3: Overview on CSos I/O modules

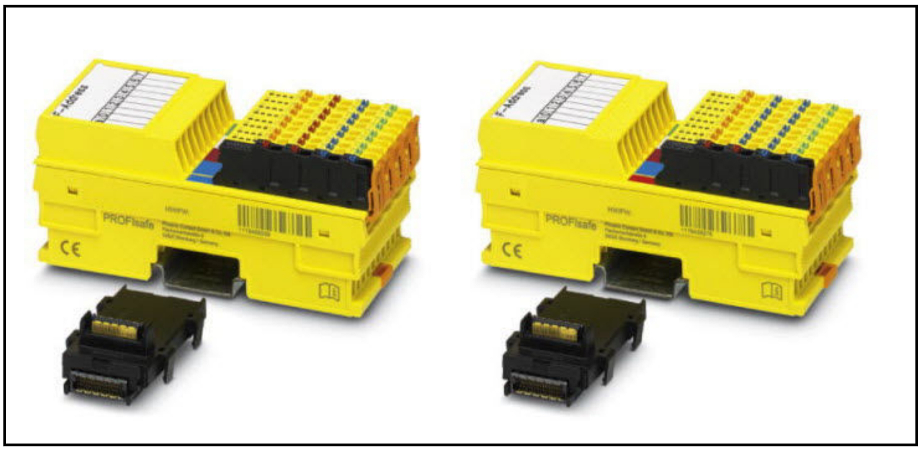


Fig. 5-6: Sercos CSos I/O modules

For a detailed description, refer to the documentations:

- "IndraControl S20 Bus Coupler for Sercos", part number: R911342782
- Application description "Rexroth IndraControl S20: System and Installation", part number R911335988
- Application description "IndraControl S20 Module with Safe Digital Inputs S20-SSDI-8/4", part number R911342480
- Application description "IndraControl S20 module with Safe Digital Outputs S20-SSDO-8/3", part number R911342482

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapter "CSos"

Profibus bus coupler S20-PB-BK

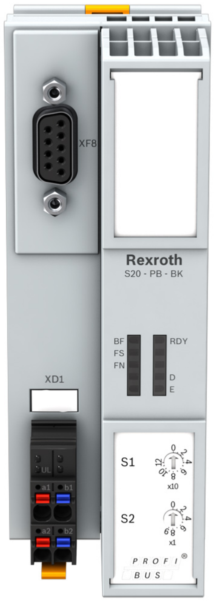


Fig. 5-7: Rexroth Profibus bus coupler S20-PB-BK

The bus coupler is intended for use within a Profibus network and is the link to the embedded control S20 system.

It is modular extendable with S20 modules. Using the bus coupler, up to 63 S20 devices can be connected to an existing Profibus network.

Type code: S20-PB-BK

Part number: R911173247

Overview on the field bus coupler features:

- RS-485 for Profibus
- Transmission rate from 9.6 kBit/s to 12 MBit/s (automatic detection)
- Diagnostic LED
- It is recommended to not use more than 16 Safety-I/O module (PROFIsafe IO module) at the S20-PB-BK.

  The number of PROFIsafe I/O modules that can be connected is limited by the power input from the logic voltage of the bus coupler

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapter "S20 Profibus coupler S20-PB-BK"

- Use den PROFIBUS bus coupler S20-PB-BK from change index AB1
- Only the first PROFIBUS master (extension module Profibus (XFE01.1-FB-10)) is intended for the PROFIsafe device operation at the XM2x and XM4x standard controls.

The following PROFIsafe I/O modules can be operated at the Profibus bus coupler S20-PB-BK:

Type code	Brief description	Part number
S20-PSDI-8/4	8 one-channel or 4 dual-channel safe inputs in 4-wire connection method	R911173254
S20-PSDO-8/3	8 one-channel or 4 dual-channel safe outputs in 3-wire connection method	R911173255

Tab. 5-4: Overview PROFISafe I/O modules

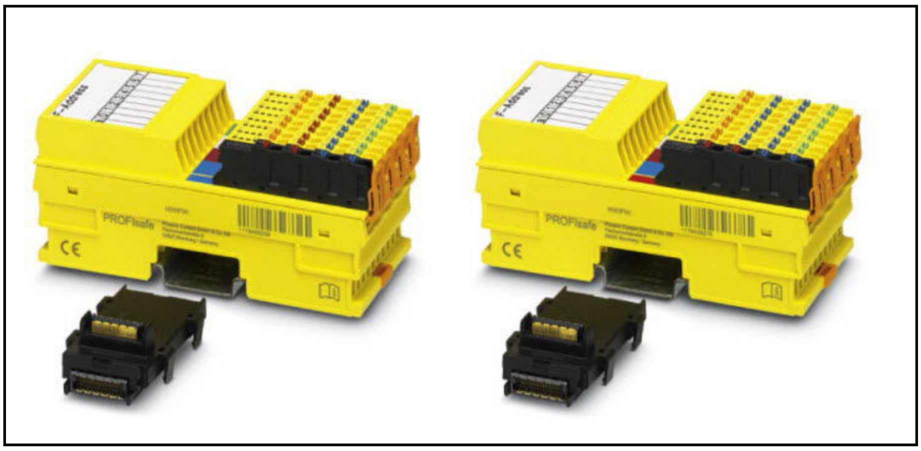


Fig. 5-8: PROFIsafe I/O modules

For a detailed description, refer to the documentations:

- "Rexroth IndraControl S20 Bus Coupler for Profibus DP", part number R911342760
- Application description "Rexroth IndraControl S20: System and Installation", part number R911335988
- Application description "Rexroth IndraControl S20 Module with Safe Digital Inputs S20-PSDI-8/4", part number R911369168
- Application description "IndraControl S20 module with Safe Digital Outputs S20-PSDO-8/3", part number R911369164

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapters "S20-PSDI 8/4 (PROFIsafe Data Input)" and "S20-PSDO 8/3 (PROFIsafe Data Output)"

PROFINET bus coupler S20-PN-BK+

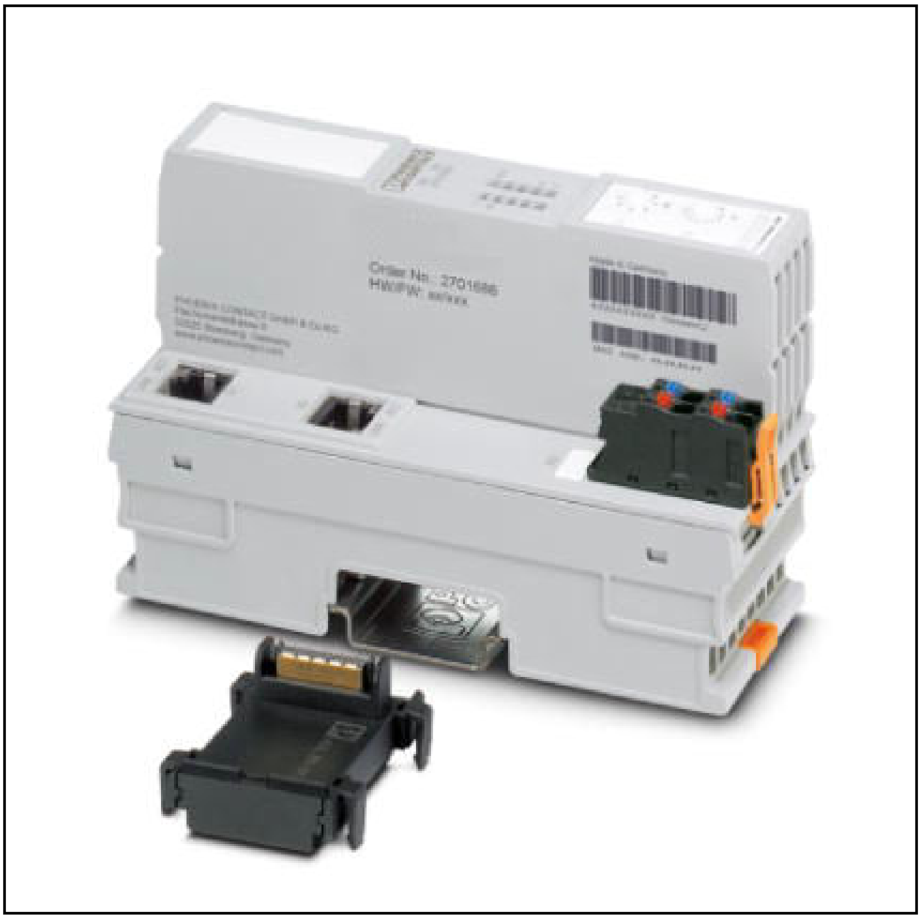


Fig. 5-9: Rexroth Profinet bus coupler S20-PN-BK+

The bus coupler is intended for use within a Profinet network and is the link to the embedded control S20 system.

It is modular extendable with S20 modules. Using the bus coupler, up to 63 S20 devices can be connected to an existing Profinet network.

Type code: S20-PN-BK+

Part number: R911173359

Overview on the field bus coupler features:

- 2 Ethernet ports
- Transfer rate 100 Mbit/s
- Diagnostic LED
- Support of up to 63 Safety I/O modules (PROFIsafe I/O modules)

  The number of PROFIsafe I/O modules that can be connected is limited by the power input from the logic voltage of the bus coupler

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapter "S20 Profinet coupler S20-PN-BK+"

☞ Only the first PROFINET controller (extension module RT-Ethernet (XFE01.1-FB-03)) is intended for the PROFIsafe device operation at the XM2x and XM4x standard controls.

The following PROFIsafe I/O modules can be operated at the PROFINET bus coupler S20-PN-BK+:

Type code	Brief description	Part number
S20-PSDI-8/4	8 one-channel or 4 dual-channel safe inputs in 4-wire connection method	R911173254
S20-PSDO-8/3	8 one-channel or 4 dual-channel safe outputs in 3-wire connection method	R911173255

Tab. 5-5: Overview PROFISafe I/O modules

Fig. 5-10: PROFIsafe I/O modules

For a detailed description, refer to the documentations:

- "Rexroth IndraControl S20 Bus Coupler for PROFINET", part number R911342784
- Application description "Rexroth IndraControl S20: System and Installation", part number R911335988
- Application description "Rexroth IndraControl S20 Module with Safe Digital Inputs S20-PSDI-8/4", part number R911369168
- Application description "IndraControl S20 module with Safe Digital Outputs S20-PSDO-8/3", part number R911369164

For more information, refer to document "IndraWorks SafeLogic 15VRS First Steps" in chapters "S20-PSDI 8/4 (PROFIsafe Data Input)" and "S20-PSDO 8/3 (PROFIsafe Data Output)"

5.5 Rexroth IndraDrive drive system

5.5.1 What is "integrated safety technology (Safe Motion)"?

IndraDrive Cs

The control sections of the IndraDrive Cs range can be equipped with the optional modules "S4", "S5" and "SB".

Using the mentioned optional modules, IndraDrive Cs is equipped with integrated safety technology which provides the user with universally parameterizable safe motion monitoring or standstill monitoring.

The **encoder-dependent** safety functions are applicable for personal protection at machines according to ISO 13849-1 Category 3, PL d and IEC 62061 SIL 2; the safety functions **independent of an encoder** are applicable for personal protection at machines according to ISO 13849-1 Category 4, PL e and IEC 62061 SIL 3.

Using the optional expansion package "SIL3-MOTION" or "SIL3-PLUS", the **encoder-dependent** safety functions are also applicable for personal protection at machines according to IEC 62061 SIL 3.

IndraDrive Mi

The IndraDrive Mi systems with the motor-integrated servo drive KSM02 and the near motor servo drive KMS02 can be equipped with the optional module "S3" [Safe Motion (without SBC)].

Using the optional module "S3", IndraDrive Mi is equipped with integrated safety technology which provides the user with universally parameterizable safe motion monitoring or standstill monitoring.

The IndraDrive Mi systems with the motor-integrated servo drive KSM02 and the near motor servo drives KMS02 / KMS03 can be equipped with the optional module "SD" [Safe Motion (with SBC)].

The **encoder-dependent** safety functions are applicable for personal protection at machines according to ISO 13849-1 Category 3, PL d and IEC 62061 SIL 2; the safety functions **independent of an encoder** are applicable for personal protection at machines according to ISO 13849-1 Category 4, PL e and IEC 62061 SIL 3.

Using the optional expansion package "SIL3-MOTION" or "SIL3-PLUS", the **encoder-dependent** safety functions are also applicable for personal protection at machines according to IEC 62061 SIL 3.

Using the KCU02.**2** drive connection box, the safety functions are applicable for personal protection at machines according to ISO 13849-1 Category 3, PL d and IEC 62061 SIL 3.

☞ For using the integrated safety technology "S3"/"SD", at least the design "2" or higher of the KCU02 drive connection box has to be used.

IndraDrive ML / IndraDrive M / IndraDrive C

The Cxx02 control sections of the IndraDrive ML / IndraDrive M / IndraDrive C ranges can be equipped with the optional modules "S4", "S5" and "SB".

Using the mentioned optional modules, IndraDrive ML / IndraDrive M / IndraDrive C are equipped with integrated safety technology which provides the user with universally parameterizable safe motion monitoring or standstill monitoring.

The **encoder-dependent** safety functions are applicable for personal protection at machines according to ISO 13849-1 Category 3, PL d and IEC 62061 SIL 2; the safety functions **independent of an encoder** are applicable for personal protection at machines according to ISO 13849-1 Category 4, PL e and IEC 62061 SIL 3.

Using the optional expansion package "SIL3-MOTION" or "SIL3-PLUS", the **encoder-dependent** safety functions are also applicable for personal protection at machines according to IEC 62061 SIL 3.

Selecting the function

The safety functions can be selected as follows:

- centrally via 24 V inputs of a safety zone module (HSZ01) (not possible with IndraDrive Mi)
- via the Safety bus communication
- with MPx-21 and above: via the inputs of the optional safety technology modules "S3", "S4", "S5" and "SD", configured as safe inputs

Certification

The safety technology was certified by TÜV Rheinland ®; the NRTL listing by TÜV Rheinland of North America is in preparation.

Certificates are available on "Certipedia", the certificates database of TÜV Rheinland ®.

Requirements that can be realized

The integrated safety technology is independent of the type of master communication, the higher-level control unit and the supply modules. It is available as a functional characteristic of the standard drive system. The following requirements can be implemented in the machine or in the installation:

- Measures in accordance with ISO 12100-2, if accessing the danger zone is required, for example, for equipping, teaching or material withdrawal.
- Requirements for safety-related parts of control systems according to ISO 13849-1 Category 4, PL e and IEC 62061 SIL 3, as required in EN 1010-1 (printing and paper converting machines), ISO 23125 (turning machines) and EN 12417 (machining centres).
- Control functions in the case of an error according to IEC 60204-1 ("homogeneous redundancy").

5.5.2 Supported safety technology functions

The table below shows the dependency on safety functions, SIL and on the availability with the optional safety technology modules.

Safety technology function	Available with optional safety technology module					SIL	Notes
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Cxx02 control section) and IndraDrive ML				
	S3 (KMS02 and KSM02)	SD (KSM02, KMS02 and KMS03)	S4	S5	SB		
Safety Zone Acknowledge (SZA) The safety technology function can only be used in conjunction with the safety zone module (HSZ01). Using "Safety zone acknowledge" and the safety zone module "HSZ", an acknowledgment master can monitor the safety of a safety zone and acknowledge the safety to a higher-level control unit. It is also possible for the acknowledgment master of the safety zone to directly control a safety door locking device connected to the safety zone module.	–	–	✓	✓	–	3	
Safe Door Locking (SDL) The safety technology function can only be used in conjunction with the safety zone module (HSZ01). The locking device of an interlocking guard is controlled via two channels when the safety zone acknowledge signals "Safety" and the user with a pushbutton requests the safety door to be unlocked. The position of the locking device is safely monitored.	–	–	✓	✓	–	3	

	Available with optional safety technology module						
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Cxx02 control section) and IndraDrive ML				
Safety technology function	S3 (KMS02 and KSM02)	SD (KSM02, KMS02 and KMS03)	S4	S5	SB	SIL	Notes
Safe Zone Error (SZE) The safety technology function can only be used in conjunction with the safety zone module (HSZ01). The "Safe zone error" function is a subfunction of the safety function "Safety zone acknowledge". The "Safe zone error" function allows locally present safety technology errors to be signaled by the zone nodes to all zone nodes via a safe output and to trigger individual error reactions. It is also possible for the acknowledgment master of a safety zone to signal zone errors via the safe communication to the higher-level control unit.	–	–	✓	✓	–	3	
Safe Torque Off (STO) The energy supply to the drive is interrupted in a safe way. The drive cannot generate any torque/force and, as a consequence, it cannot generate any dangerous motions, either.	✓	✓	✓	✓	✓	3	
Safe Operating Stop (SOS) With the safety function "Safe operating stop", the drive is in controlled standstill, i.e. all control functions between the electronic control unit and the drive are maintained. The dual-channel monitoring prevents the drive from carrying out dangerous movements due to errors although the energy supply is not interrupted.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safe Brake Control (SBC) With the safety function "Safe brake control", the connected brake is switched off safely (via two channels).	✓1) 2)	✓	✓ 2)	✓ 2)	✓ 2)	3	1) available with MPx-21 and above 2) With IndraDrive M / IndraDrive C (Cxx02 control section), IndraDrive ML and IndraDrive Mi with optional safety technology module "S3", the safety technology function can only be used in conjunction with a control module (HAT02.1).
Safe Braking and Holding System (SBS) The safety function "Safe braking and holding system" safely prevents unintended axis motion (e.g. of vertical axes), even if the drive is not in control.	–	✓	✓	✓	–	3	available with MPx-21 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS" Safety function "SBT" is required
Safe Maximum Speed (SMS) With the safety function "Safe maximum speed", dual-channel monitoring prevents the drive from exceeding the preset velocity limit value.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"

Safety technology function	Available with optional safety technology module						
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Cxx02 control section) and IndraDrive ML			SIL	Notes
	S3 (KMS02 and KSM02)	SD (KSM02, KMS02 and KMS03)	S4	S5	SB		
Safe Direction (SDI) The safety function "Safe direction" ensures by dual-channel monitoring that motion is only possible in one direction.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safely-Limited Speed (SLS) The safety function "Safely-limited speed" monitors via two channels that the drive does not exceed a previously defined limitation of the velocity window.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safely-Monitored Transient Oscillation (SLS-LT) Using a velocity window and a tolerance time, the safety function "Safely-monitored transient oscillation" monitors the transient oscillation with regard to a "Safely-limited speed".	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safely-Limited Increment (SLI) The safety function "Safely-limited increment" monitors via two channels that the drive moves only within the maximum increment.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safe Stop 1 (SS1) When the transition function "Safe stop 1 (SS1)" is activated, the drive is decelerated in a safely monitored way. After the deceleration process has been completed, the safety function "Safe torque off (STO)" is activated and the energy supply to the motor is safely interrupted. The motor cannot generate any torque/any force and therefore no dangerous movements.	✓	✓	✓	✓	✓	3	SS1, time-monitored
						2 / 3*	SS1, delay monitoring * SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safe Stop 2 (SS2) When the transition function "Safe stop 2" is activated, the drive is stopped in a safely monitored way. After the deceleration process has been completed, the safety function "Safe operating stop" is activated and it is safely prevented that the motor deviates from the stopping position by more than a specified absolute value.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safely-Monitored Deceleration (SMD) Given a change in the operating status or in the case of an error reaction, the safety function "Safely-monitored deceleration" monitors via two channels whether the actual velocity of the drive is within a parameterized velocity envelope curve.	✓	✓	✓	✓	✓	2 / 3*	* SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safely-Monitored Position (SMP) The safety function "Safely-monitored position" monitors whether or not the parameterized position range is exceeded in positive or negative direction.	✓	✓	✓	✓	✓	2	available with MPx-20V06 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS"

Safety technology function	Available with optional safety technology module					SIL	Notes
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Cxx02 control section) and IndraDrive ML				
	S3 (KMS02 and KSM02)	SD (KSM02, KMS02 and KMS03)	S4	S5	SB		
Safely-Limited Position (SLP) The safety function "Safely-limited position" monitors via two channels that the drive can be decelerated within the parameterized **position limits** with the current velocity and the parameterized minimum delay.	✓	✓	✓	✓	✓	2	available with MPx-20V06 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS"
Safely-Limited End Position (SLE) The safety function "Safely-limited end position" monitors via two channels that the drive can be decelerated within the parameterized **end position limit value** with the current velocity and the parameterized minimum delay.	✓	✓	✓	✓	✓	2	available with MPx-20V06 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS"
Safe CAM (SCA) The safety function "Safe CAM" monitors via two channels whether or not the axis is within a defined position range (cam range). The result is provided via status words.	✓	✓	✓	✓	✓	2	available with MPx-20V08 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS"
Safe Speed Monitor (SSM) The safety function "Safe speed monitor" monitors via two channels whether or not the axis is within a defined velocity range. The result is provided via status words.	✓	✓	✓	✓	✓	2 / 3*	available with MPx-21 and above * SIL 3 is only attained with firmware option (FWS) "SIL3-MOTION" or "SIL3-PLUS"
Safe Homing Procedure With the auxiliary function "Safe homing procedure", another homing event is expected at a separate position after the functional homing procedure. The second homing event is used to validate the functional homing procedure.	✓	✓	✓	✓	✓	2	available with MPx-20V06 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS"
Safe Brake Test (SBT) The auxiliary function "Safe brake test" regularly checks via two channels if one or two brakes controlled via SBC are still operational and generate a defined holding torque.	✓	✓	✓	✓	✓	2 / 3*	available with MPx-21 and above with firmware option (FWS) "SAFETY-PLUS" or "SIL3-PLUS" * SIL 3 is only attained with firmware option (FWS) "SIL3-PLUS"

Tab. 5-6: Functions for safe motion monitoring and safe standstill monitoring

☞ Optional safety technology modules can be neither retrofitted nor replaced "in the field"; i.e. drive controllers have to be ordered ex works with the required safety technology option.

5.6 Profibus DP or Profinet with PROFIsafe

5.6.1 General information

PROFIsafe has been specified in 1999 in version V1 as safety-oriented profile exclusively for Profibus DP and has been released in release V1.3 (2004).

PROFIsafe is available in the versions V1 (until 2004 exclusively for Profibus DP) and V2 for Profibus DP and Profinet.

PROFIsafe in version V2 is standardized in the international standard IEC 61784-3-3.

For more information about PROFIsafe, refer to the Profibus user organization (PNO).

Make sure that you always use the latest documents about Profibus DP or Profinet and PROFIsafe.

The Safety extension module supports PROFIsafe V2 devices. The programming system differentiates this in the configuration using the GSD file (Generic Station Description).

5.6.2 PROFIsafe application

Structure and ambient conditions

When using PROFIsafe at the Profibus DP or PROFINET, take the machine or system configuration, the general Profibus or Profinet requirements and the special requirements of PROFISafe on the structure, the system limits and the ambient conditions of the Profibus or Profinet system into consideration.

Make sure that you always use the latest documents about Profibus DP or Profinet and PROFIsafe.

When complying with all specifications, the PROFIsafe data communication up to SIL3 according to IEC 61508 or IEC 62061 or PL e according EN ISO 31849-1 can be used. To calculate the failure rates of your system or your Safety functions, the following remaining failure rate can be used for safe data communication with PROFIsafe:

$$\Lambda = 3 \cdot 10^{-10}$$

Fig. 5-11: Remaining error rate PROFIsafe

Configuration

Insert the safe PROFIsafe devices in the topology of your Profibus DP and/or the Profinet system. As for standard devices, take the PROFIsafe devices to be used of the device library of the programming system and integrate the PROFIsafe devices in the desired positions in the device tree of your application. The devices are described by their GSD or GSDML files and are equipped with a basic parameterization.

Due to this information, the programming system provides several configuration and parameterization windows for each PROFIsafe device. In these windows, all configuration and parameterization settings can be selected.

- Safety parameters (PROFIsafe F-parameters)
- Safety mapping (I/O channels)
- I-parameters (individual parameters, if available)
- Status (display of device diagnostic messages)
- Information (general information on the device from the device description: name, manufacturer, version, order number, description, image)

In the window "I/O image" assign the I/O channels of the device to the symbolic variables that are used in your Safety logic.

Parameterization

The PROFIsafe specification describes two different parameter types for PROFIsafe devices.

F-parameters are used particularly for parameterization of the safe communication. The F-parameters are specified in the profile specification (V1/V2) or in IEC 61784-3-3 and are implemented by each PROFIsafe device. The F-parameters are transmitted to the PROFIsafe device during the initialization within the framework of the standard Profibus parameterization dialog. After having received the valid F-parameter block, a PROFIsafe device sends process data at the inputs of the Safety control. At the outputs to the periphery, fail-safe values are sent until other values are specified by the Safety logic. The entries of the F-parameters in the configuration window are compared to the values in the safe device, in case of addresses and the monitoring time, they are compared continuously during the cyclic communication. Differences result in an error reaction and diagnostic message.

Device-specific parameters are referred to as I-parameters. The I-parameters are described in the individual device descriptions.

General F-parameter description

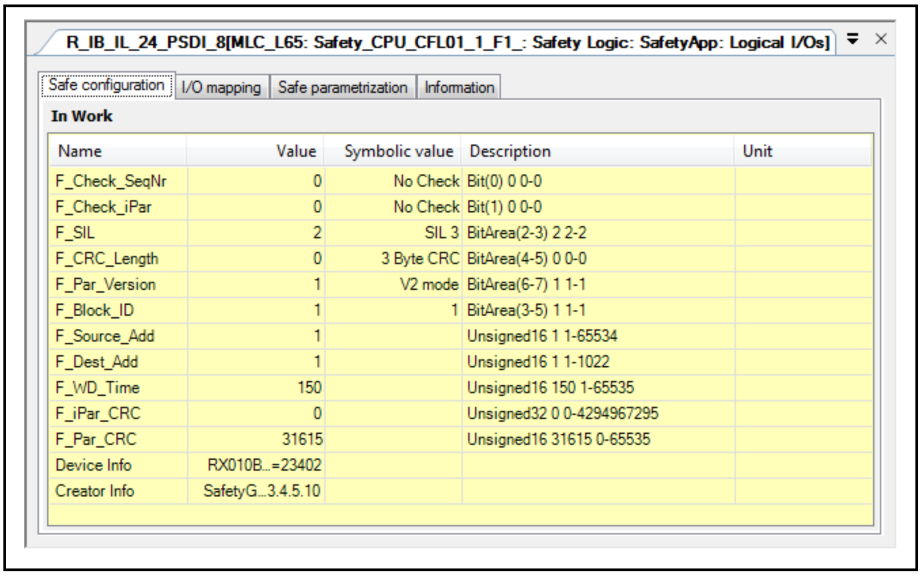
Parameters	Meaning	Value range
F_SlotNumber	Module number within a modular Profibus or Profinet station	Device-dependent
F_Check_SeqNr	Is the consecutive number taken into consideration in the calculation of the CRC2 signature? Only relevant to V1. For V2 always 0, entry is don’t care Usually 0 (no check)	0: No 1: Yes
F_Check_iPar	Device-specific use. See device description Usually 0 (no check)	0: No 1: Yes
F_SIL	The safe device compares its SIL with the assigned SIL	00: SIL1 01: SIL2 10: SIL3 11: No SIL
F_CRC_Length	The CRC2 signature can have different lengths: 2 bytes (only in V1 mode) 3 bytes (only in V2 mode) 4 bytes (optional in V1 or V2 mode)	00: 3 bytes 01: 2 bytes 10: 4 bytes 11: Reserved
F_Block_ID	F-parameter type identification: 0 = no F-iPar_CRC in F-parameter block 1 = F-iPar_CRC in F-parameter block	0-1

Parameters	Meaning	Value range
F_Par_Version	Version number of the F-parameter set 0 = valid for V1 mode 1 = valid for V2 mode	0-1
F_Source_Add	Source address of the communication channel; here PROFIsafe address of the Safety extension module	Unsigned 16
F_Dest_Add	Target address of the communication channel	Unsigned 16
F_WD_Time	Monitoring time for cyclic communication, time basis 1 ms	Device-dependent
F_Par_CRC	CRC1 signature via F-parameters, has to be applied from the safe parameterization	Unsigned 16
F_iPar_CRC	CRC signature via I-parameters, is calculated and entered by IndraWorks	Unsigned 32

Tab. 5-7: List of F-parameters

The entries of the F-parameters in the configuration window are compared to the values in the safe device, in case of addresses and the monitoring time, they are compared continuously during the cyclic communication.

Differences result in an error reaction and diagnostic message.



R_IB_IL_24_PSDI_8[MLC_L65: Safety_CPU_CFL01_1_F1_: Safety Logic: SafetyApp: Logical I/Os]

In Work

Name	Value	Symbolic value	Description	Unit
F_Check_SeqNr	0	No Check	Bit(0) 0 0-0	
F_Check_iPar	0	No Check	Bit(1) 0 0-0	
F_SIL	2	SIL 3	BitArea(2-3) 2 2-2	
F_CRC_Length	0	3 Byte CRC	BitArea(4-5) 0 0-0	
F_Par_Version	1	V2 mode	BitArea(6-7) 1 1-1	
F_Block_ID	1	1	BitArea(3-5) 1 1-1	
F_Source_Add	1		Unsigned16 1 1-65534	
F_Dest_Add	1		Unsigned16 1 1-1022	
F_WD_Time	150		Unsigned16 150 1-65535	
F_iPar_CRC	0		Unsigned32 0 0-4294967295	
F_Par_CRC	31615		Unsigned16 31615 0-65535	
Device Info	RX010B...=23402			
Creator Info	SafetyG...3.4.5.10			

Fig. 5-12: Example: Configuration window and F-parameters in SafeLogic

Interface to Safety logic

The interface between the PROFIsafe channel and the Safety logic is generated by the input/output parameters of the PROFIsafe layer function block instantiated for each PROFIsafe channel. Via these parameters, the Safety logic can control the PROFIsafe communication of this channel or query its status.

For a complete description of the function block, refer to document "SafeLogic Project Configuration" in chapter "Profisafe-Host", see Rexroth media directory

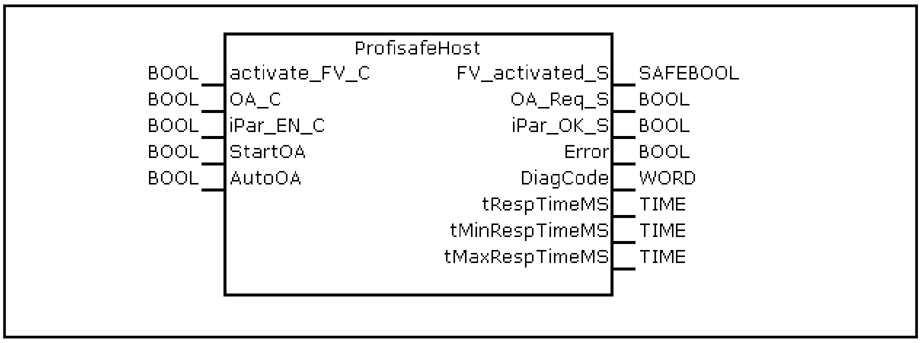


Fig. 5-13: Interface ProfisafeHost function block

5.6.3 Error reaction at PROFIsafe

All fatal errors causing the loss or limitation of the safety function, cause that the PROFIsafe device goes into the safe state. A device returns fail-safe values at inputs and outputs and reports this to the Safety application via the bus. In the Safety logic, you can intervene by changing the program. Following the debugging, the device can be actively integrated in the Safety function again by outputting a targeted acknowledgement signal ("Operator Acknowledge") in the Safety logic.

The malfunction depends on the device type as well as the diagnostic messages regarding the Safety control. For details, please refer to the respective device description. Usually, the error message is displayed at the device using LEDs. The transmission of diagnostic messages to the safety control is not safety-related.

5.6.4 Diagnostic properties of PROFIsafe

Upon the system initialization, the Safety control detects the following PROFIsafe-specific errors and provides diagnostic information to the programming system (online mode).

- Incorrect PROFIsafe address at the device
- Invalid parameterized PROFIsafe address
- Invalid parameterized monitoring time
- Invalid parameterized SIL class
- Invalid CRC length
- Invalid F-parameter block version

In operation, the host layer instance in the Safety extension module assigned to the device contains the following messages within the framework of the status bytes of the protocol data (PDU):

- Fail-save values

  The safe device outputs assume the safe state, the safe inputs report the safe state to the host
- Communication failure

Exceeding the parameterized monitoring time (WD timeout), data corruption (CRC) or errors during the telegram sequence (consecutive number)

- Failure exists in F-slave or F-module

  Periphery and device errors detected by the PROFIsafe device are reported via the cyclic PROFIsafe telegram. There errors include wire break, short circuit, divergence time exceedance and others, if the component detects and forwards these errors

Requirement to transmit the diagnostic messages: a functional component and an at least temporarily functional communication. If this cannot be ensured, the F-host instance detects a communication time out.

The error messages are reported to the programming system as diagnostic information and are "Or"-gated via the PROFIsafe layer interface of the application and then provided to the application for program-technical evaluation.

An extended diagnostics can be transmitted to the standard control via acyclic devices, depending on the diagnostic capability of the device, and can then be displayed via the programming system. See the device descriptions.

Safe inputs

Depending on the device type and the parameterization, the following errors can be detected at safe inputs:

- Short circuit
- Cross-fault
- Overload/short circuit at clock outputs

Upon detection of an error, the safe state is assumed for this input, i.e., a "0" is entered in the input data.

Safe outputs

Depending on the device type and the parameterization, the following errors can be detected at safe outputs:

- Short circuit
- Cross-fault
- Overload
- Violation of the parameterization switch-off time

Upon detection of such an error, the affected output is switched off ("0" = off = safe state).

5.7 Sercos III with "CIP Safety on Sercos"

5.7.1 General information

"CIP Safety on Sercos" is the protocol defined in cooperation with the ODVA (Open DeviceNet Vendor Association) and according to IEC 61508 to SIL 3 certified protocol on the basis of the CIP Safety mechanism to transmit safety-relevant signals via the Sercos interface. An additional Safety bus is not required as the safe data is loaded real-time capable with the standard data of the Sercos interface network. The integration of drive, periphery and safety bus as well the standard Ethernet in a single network simplifies the handling and reduces hardware and installation costs. Integrated Safety controls and homogeneous Safety solutions can easily be implemented.

5.7.2 Using "CIP Safety on Sercos"

Brief description

"CIP Safety on Sercos" is the protocol to transmit safety-relevant signals via the Sercos interface. The safe bus communication via "CIP Safety on Sercos" has the following features:

- The consumer and producer connection is not freely configurable. Only fixed preference configurations can be used
- All required information to establish the connection are provided to the control via the device description file (SDDML)
- The achievable Safety level depends on the used Safety functions

Configuration

First insert the safe CSos-compatible devices in the topology of your Sercos system. As for standard devices, take the CSos-compatible devices to be used of the device library of the programming system and integrate these devices in the desired positions in the device tree of your application. The devices are described by their SDDML files and are equipped with a basic parameterization.

Due to this information, the programming system provides several configuration and parameterization windows for each Csos device. In these windows, all configuration and parameterization settings can be selected, amongst others:

- Safe configuration (CipSafety parameter)
- Safety mapping (I/O channels)
- I-parameters (individual parameters, if available)
- Information (general information on the device from the device description: name, manufacturer, version, order number, description, image)

Analog to the PROFIsafe application, in the window "I/O image" assign the I/O channels of the device to the symbolic variables that are used in your Safety logic.

Parameterization

The parameterization is identical to the PROFIsafe device parameterization.

F-parameters are used particularly for parameterization of the safe communication, see "General F-parameter description" on page 73. The device-specific parameters are referred to as I-parameters and are described in the individual device descriptions.

Interface to Safety logic

The CSosOriginator function block monitors the connection establishment and the cyclic communication of a safe Sercos device. The function block provides diagnostics and facilitates acknowledging of reported messages. With the logic Csos device, a control instance of this function block is automatically added to the Safety application. Each input and output group requires a control instance of this function block

When creating an IndraDrive with a SafeLogic Safety profile, a control instance for control (outputs) and status (inputs) is automatically created. One instance is created per S20 Csos I/O module.

☞ For a complete description of the function block, refer to document "SafeLogic Project Configuration" in chapter "CSosOriginator", see Rexroth media directory

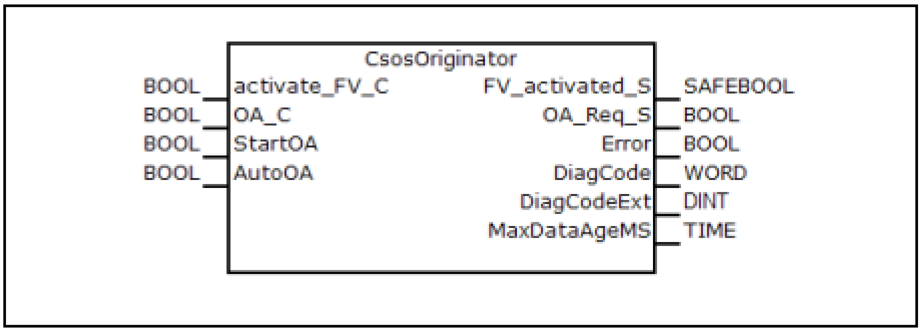


Fig. 5-14: Interface CSosOriginator function block

5.8 Safe cross communication via Ethernet

5.8.1 General information

The safe cross communication facilitates the exchange of safe PLC variables between several SafeLogic controls via Ethernet-based bus systems. The data is transmitted via the IP communication protocol and are protected with end-to-end Safety mechanism between the controls. The integration of drive, periphery and safety bus as well the standard Ethernet in a single network simplifies the handling and reduces hardware and installation costs. Integrated Safety controls and homogeneous Safety solutions can easily be implemented.

The connection is established according to the subscriber principle. The sending SafeLogic control provides the data. The receiving SafeLogic control establishes the connection to the sending control. Several recipients can connect to a sender. The sending SafeLogic control requires an adjustable connection number.

With the safe cross communication, the data are safely transmitted on the same medium and with the same interface as the standard communication. Safe communication between all network levels is possible, even in case of direct cross communication and communication across networks. The safety-relevant data is transmitted via the IP layer using a UDP package, protected via safe communication protocols.

☞ The logic data connections are not limited as the safe cross communication is routable. Thus, a Safety network can comprise several IP-compatible networks. Comply with the standards and regulations for configuration and acceptance for Safety network variables in the "SafeLogic Project Configuration" documentation, see Rexroth media directory.

5.8.2 Using the safe cross communication

Brief description

The safe cross communication is used to transmit safety-relevant signals via Ethernet-based bus systems. The safe cross communication has the following features:

- The transmitted safe variables can be user-defined
- All required information to establish the connection are provided to the control via the Safety project
- The achievable Safety level is SIL 3

The following safe data types can be transmitted via the safe cross communication:

- SAFEBOOL
- SAFEINT
- SAFEWORD

Configuration

Insert a "Safety NVL sender" (safe network variable list) on the sending SafeLogic control. Define the variables to be transmitted. Select the Safety address of the sender list. Insert a "Safety NVL receiver" in the receiving SafeLogic control. Subsequently, both lists can be connected by selecting the assigned sender in the "Safety NVL receiver".

Interface to Safety logic

The function block NetVarSender provides the safe variables. Using the Safety NVL sender, a control instance of this function block is automatically added to the Safety application. Each sending list requires a control instance of this function block.

The NetVarSender function block does not have any monitoring function. There is not possibility to verify that the recipient is connected to the network list. The process data transfer is activated via the S_ActivateOut input. If S_ActivateOut is FALSE, fail-safe values are transmitted.

☞ For a complete description of the function block, refer to document "SafeLogic Project Configuration" in chapter "NetVarSender", see Rexroth media directory

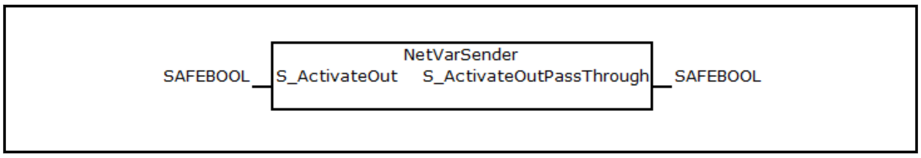


Fig. 5-15: NetVarSender interface

The NetVarReceiver function block monitors the connection establishment and the cyclic communication of a Safety network variable list of received data. The function block provides diagnostics and facilitates acknowledging of reported messages. Using the Safety NVL receiver, a control instance of this function block is automatically added to the Safety application. Each list of received data requires a control instance of this function block.

☞ For a complete description of the function block, refer to document "SafeLogic Project Configuration" in chapter "NetVarReceiver", see Rexroth media directory

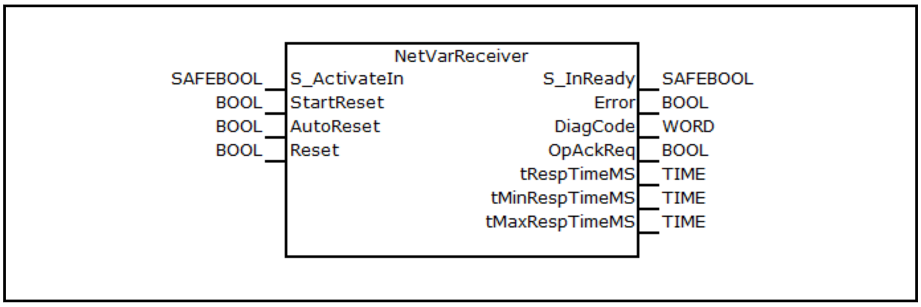


Fig. 5-16: Interface NetVarReceiver function block

6 Development interface

6.1 Overview

Both SafeLogic programming systems "SafeLogic" and "SafeLogic compact" use different development interfaces.

The user interfaces of both programming systems is explained in the following chapters:

- chapter 6.2 "SafeLogic compact (SafeLogic Designer)" on page 81
- chapter 6.3 "SafeLogic" on page 86

6.2 SafeLogic compact (SafeLogic Designer)

6.2.1 License

The SafeLogic Designer is not subject to a license.

6.2.2 Standard views

The SafeLogic Designer has the following views that can be accessed via buttons below the menu bar.

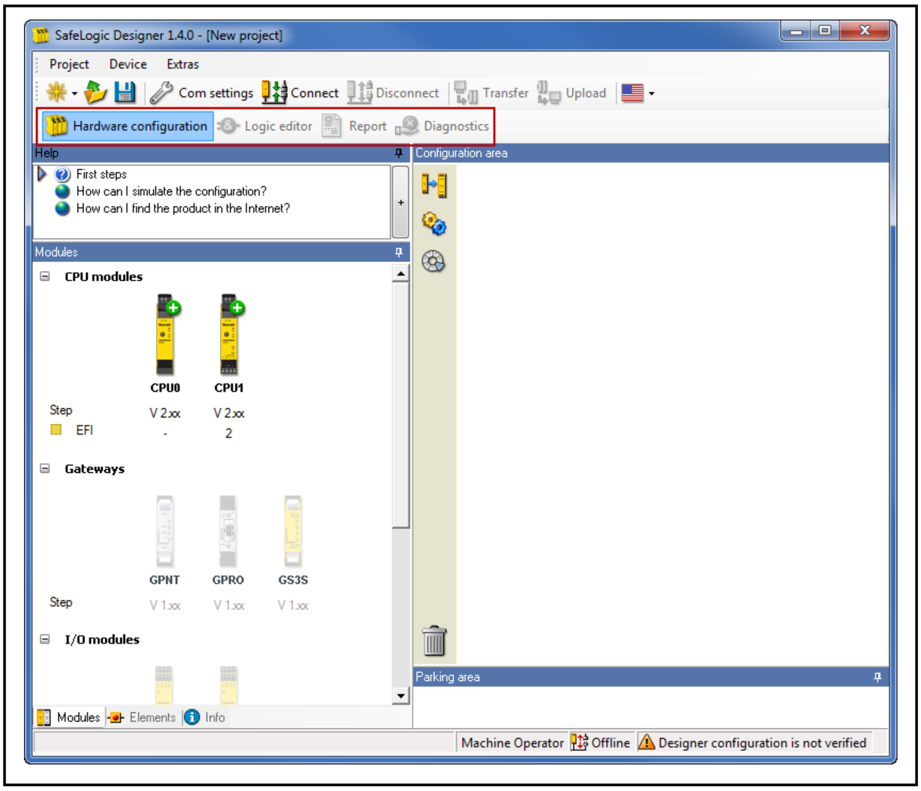
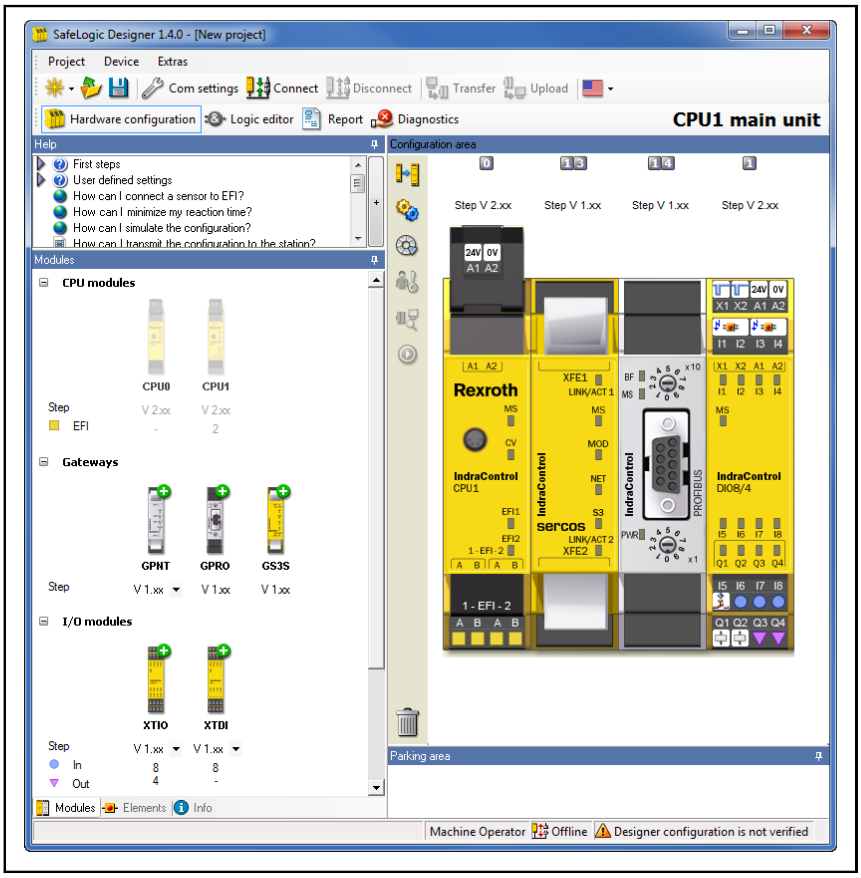


Fig. 6-1: The view can be selected below the menu bar

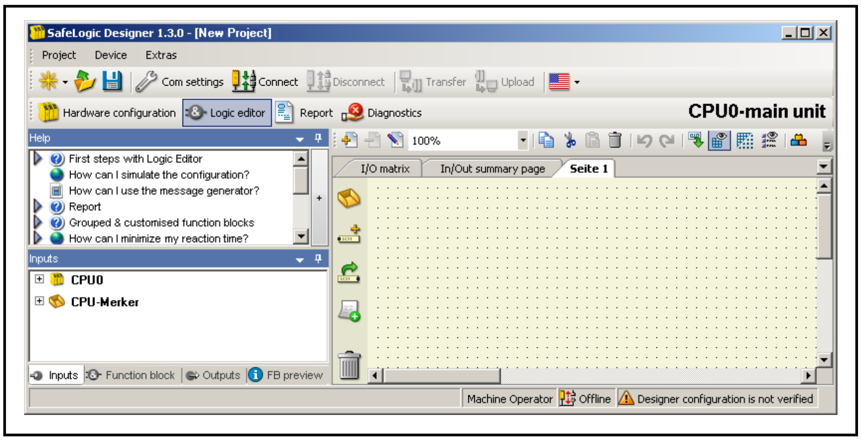
- The structure of a SafeLogic compact system consisting of various hardware modules as well as the configuration of the inputs and outputs and the connected elements is specified in the **Hardware configuration** view



First steps
User defined settings
How can I connect a sensor to EFI?
How can I minimize my reaction time?
How can I simulate the configuration?
How can I transmit the configuration to the station?

Fig. 6-2: "Hardware configuration" view

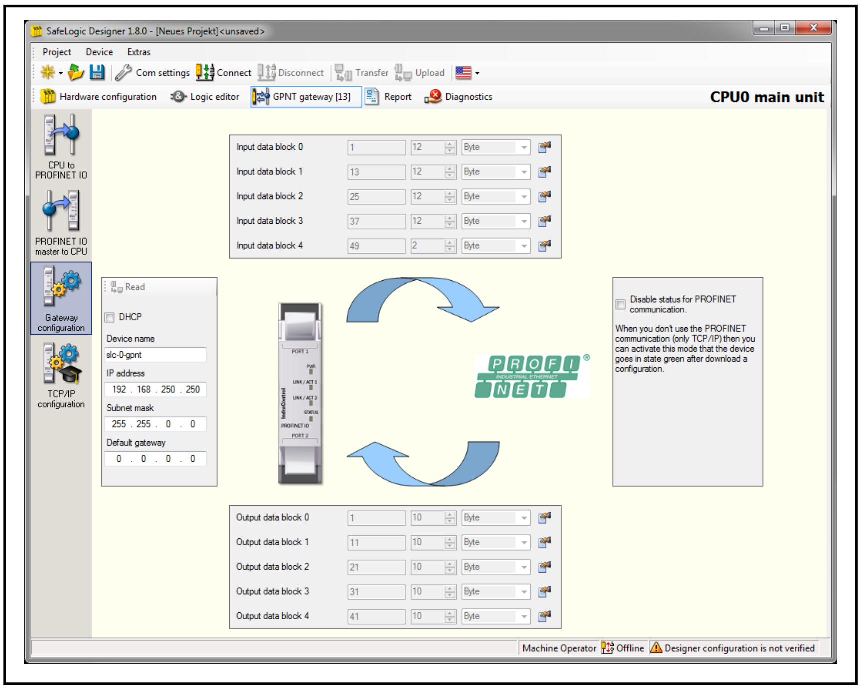
- The function logic can be configured by means of logic function blocks and application-specific function blocks in the **Logic editor** view. This view is not available unless a main module has first been selected in the hardware configuration



First steps with Logic Editor
How can I simulate the configuration?
How can I use the message generator?
Report
Grouped & customised function blocks
How can I minimize my reaction time?

Fig. 6-3: "Logic editor" view

- If the project contains at least one SafeLogic compact diagnostic gateway or if RS-232 communication is enabled, the **Gateways** view is available. This view is used to configure the SafeLogic compact diagnostic gateways and the data that is transferred to and from the network



Input data block 0	1	12	Byte
Input data block 1	13	12	Byte
Input data block 2	25	12	Byte
Input data block 3	37	12	Byte
Input data block 4	49	2	Byte

□ DHCP

Device name: slc-0-gpnt

IP address: 192 . 168 . 250 . 250

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 0 . 0 . 0 . 0

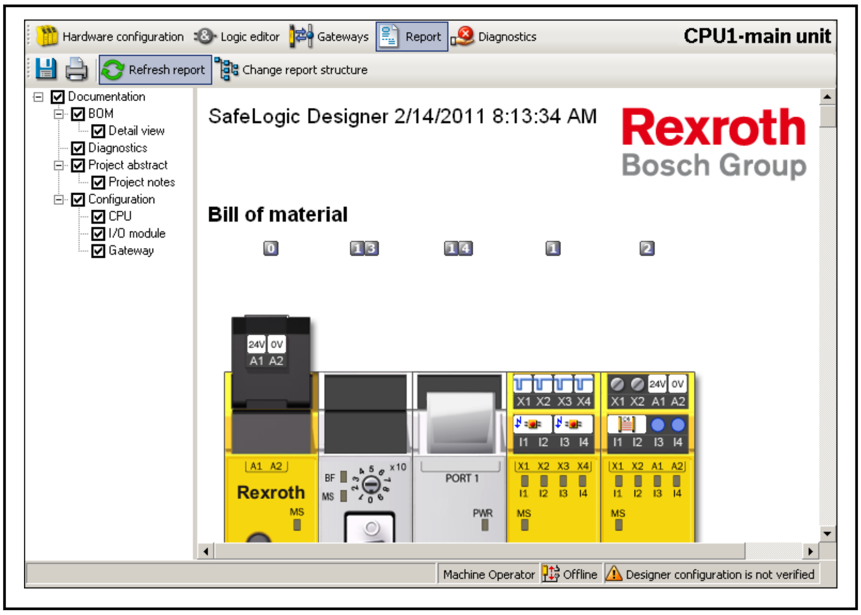
□ Disable status for PROFINET communication.

When you don't use the PROFINET communication (only TCP/IP) then you can activate this mode that the device goes in state green after download a configuration.

Output data block 0	1	10	Byte
Output data block 1	11	10	Byte
Output data block 2	21	10	Byte
Output data block 3	31	10	Byte
Output data block 4	41	10	Byte

Fig. 6-4: "Gateway" view

- Complete information on the currently loaded project and all settings including the logic programming and wiring diagrams is available in the **Report** view. Furthermore, additional information on the project can be entered here. All information can be saved in standard file formats and printed out. The scope of the report can be compiled individually depending on the selection



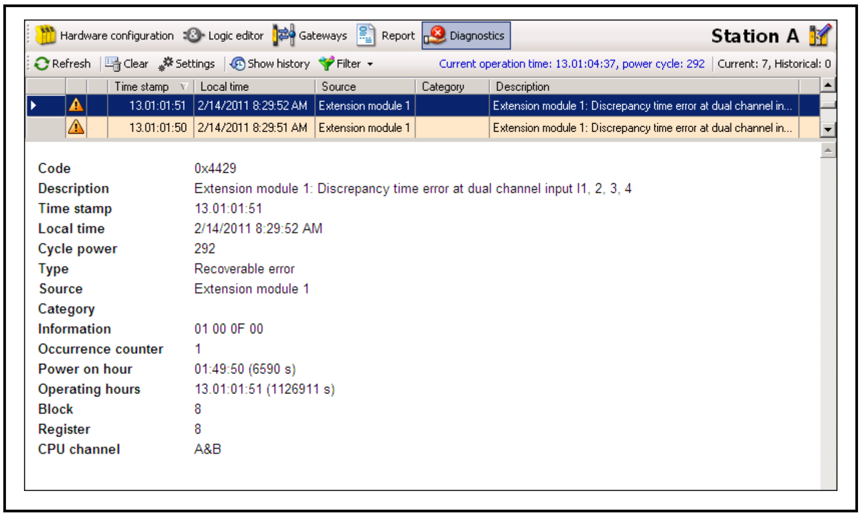
☑ Documentation
- ☑ BOM
  - ☑ Detail view
- ☑ Diagnostics
- ☑ Project abstract
  - ☑ Project notes
- ☑ Configuration
  - ☑ CPU
  - ☑ I/O module
  - ☑ Gateway

SafeLogic Designer 2/14/2011 8:13:34 AM

Bill of material

Fig. 6-5: The "Report" view

- The stored error messages are displayed as the history of a connected SafeLogic compact system in the **Diagnostics** view



Current operation time: 13.01:04:37, power cycle: 292 | Current: 7, Historical: 0

	Time stamp	Local time	Source	Category	Description
⚠	13.01:01:51	2/14/2011 8:29:52 AM	Extension module 1		Extension module 1: Discrepancy time error at dual channel in...
⚠	13.01:01:50	2/14/2011 8:29:51 AM	Extension module 1		Extension module 1: Discrepancy time error at dual channel in...

Code	0x4429
Description	Extension module 1: Discrepancy time error at dual channel input I1, 2, 3, 4
Time stamp	13.01:01:51
Local time	2/14/2011 8:29:52 AM
Cycle power	292
Type	Recoverable error
Source	Extension module 1
Category	
Information	01 00 0F 00
Occurrence counter	1
Power on hour	01:49:50 (6590 s)
Operating hours	13.01:01:51 (1126911 s)
Block	8
Register	8
CPU channel	A&B

Fig. 6-6: The "Diagnostics" view

6.2.3 Logic programming

The functional logic for the SafeLogic compact system is programmed using function blocks. These function blocks are certified for use in safety-relevant functions if all safety standards are observed during implementation. The following sections provide information on important aspects of using function blocks in the SafeLogic compact system.

Function blocks

The SafeLogic compact system supports up to 255 function blocks in a specified application. The logic cycle time results from the number of used function blocks and is between 4ms and 40ms.

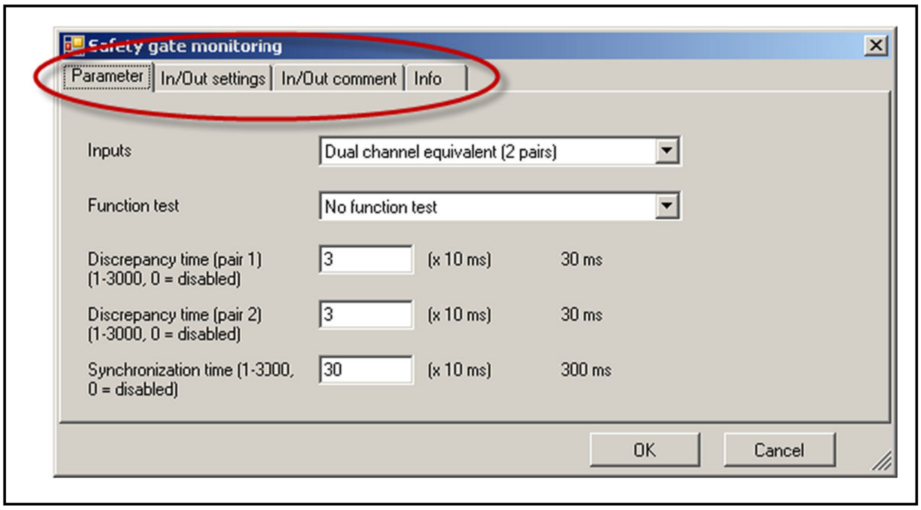
The following function blocks are available in the SafeLogic compact system:

- *Logic*
  - AND
  - OR
  - XOR
  - XNOR
  - NOT
  - RS Flip-Flop
  - JK Flip-Flop
  - Binary decoder
  - Binary encoder
  - Routing 1:N
  - Routing N:N
  - Multi release
  - Multi latch
- *Start/edge*
  - Reset
  - Restart
  - Start warning
  - Edge detection

- *Delays*
  - On-delay timer
  - Off-delay timer
  - Adjustable on-delay timer
  - Adjustable off-delay timer
- *Counter and cycle*
  - Event counter (up, down, up and down)
  - Clock generator
  - Lagging detection
  - Message generator
  - Frequency monitoring
- *EDM/output function blocks*
  - EDM
  - Valve monitoring
  - Fast shut off with bypass
  - Fast shut off
- *Muting/press*
  - Sequential muting
  - Parallel muting
  - Cross muting
  - Universal press contact
  - Press single stroke
  - Press setup
  - Press Automatic
  - Clock mode
  - Eccentric press contact
- *Other*
  - Operation mode selection switch
  - E-Stop
  - Safety gate monitoring
  - Magnetic switch
  - Light curtain monitoring
  - Two-hand control type IIIA
  - Two-hand control type IIIC
  - Multi operator (multiple two-hand control)
  - Switch synchronization
  - Error output combination
  - Tolerant dual-channel evaluation
- *User-defined function blocks*
  - Grouped function block
  - Customized function block

Function block properties

Function blocks offer a number of different properties that you can use. The configurable parameters differ depending on the function block. Double-click on the function block to access the configurable parameters and to select the tab with the desired properties. The following example shows the "Safety gate monitoring" function block:



Safety gate monitoring

Inputs	Dual channel equivalent (2 pairs)		
Function test	No function test		
Discrepancy time (pair 1) (1-3000, 0 = disabled)	3	(x 10 ms)	30 ms
Discrepancy time (pair 2) (1-3000, 0 = disabled)	3	(x 10 ms)	30 ms
Synchronization time (1-3000, 0 = disabled)	30	(x 10 ms)	300 ms

Fig. 6-7: Configurable parameters of function blocks

Function block inputs

Possible sources for function block inputs are all input elements listed in the input selection tree of the logic editor as well as the outputs of function blocks.

Function block outputs

Function blocks provide various output signal connections for connecting to physical outputs or to other function blocks.

I/O modules

The I/O extension modules, (e.g. XTIO or XTDI) can carry out a dual-channel evaluation if predefined input elements from the Elements window (e.g. RE27, C4000, …) are connected to them. If such an input element is selected, you do not need a separate function block for dual-channel evaluation (e.g. "light curtain monitoring", "safety gate monitoring" or "magnetic switch"). The two-channel evaluated input is configured as "one channel" signal path in the logic editor.

The dual-channel evaluation evaluates the correct sequence of the two input signals. It is expected that if one of the two signals has caused a switching off, the other signal will follow accordingly. Which values the two signals must have depends on the type of the dual-channel evaluation. There are two possibilities:

- Equivalent evaluation
- Complementary evaluation

An optional "discrepancy time" can be configured. The discrepancy time defines for how long the two inputs may have discrepant values after one of the both input signals has changed without this being considered as an error.

6.3 SafeLogic

6.3.1 License

IndraWorks SafetyManager license

There are two types of SafetyManager licenses:

- IndraWorks SafetyManager (R911322463)

  This license is required to develop Safety programs.

  It allows the following:

  – Logging into the Safety control including all debugging actions

  - Setting passwords
  - Downloading Safety programs
  - Creating boot projects
  - Retrieving control log
  - Updating firmware

- IndraWorks SafetyManager Lite (R911383338)

  This license is required for the remote support and for the servicing of Safety applications.

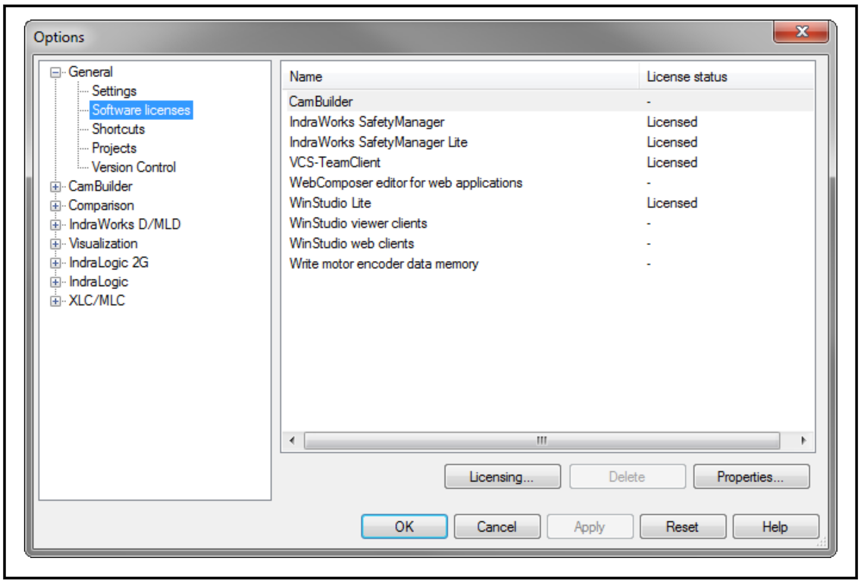
  It allows the following:

  - Logging into the control via remote support access
  - Debugging without the option to change values
  - Retrieving control log

The licenses are installed as follows:

1. Open license overview

   For the license overview, go to **Tools** ▸ **Options...**, **General** ▸ **Software licenses.**

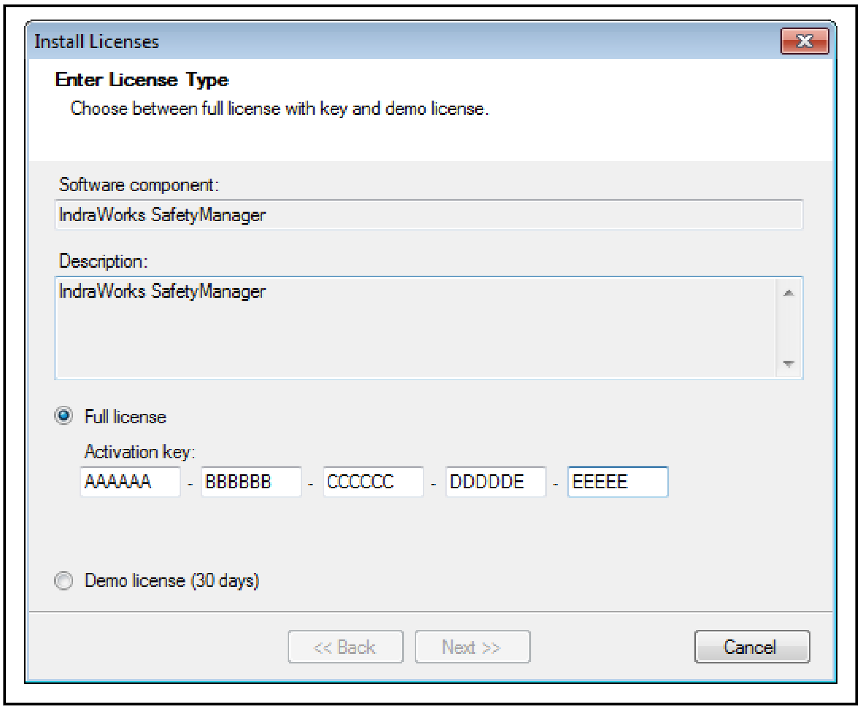


Name	License status
CamBuilder	-
IndraWorks SafetyManager	Licensed
IndraWorks SafetyManager Lite	Licensed
VCS-TeamClient	Licensed
WebComposer editor for web applications	-
WinStudio Lite	Licensed
WinStudio viewer clients	-
WinStudio web clients	-
Write motor encoder data memory	-

Fig. 6-8: License overview

2. Licensing

   For the license dialog, click on the **Licensing...** button. Enter the activation key here.



Install Licenses

Enter License Type

Choose between full license with key and demo license.

Software component: IndraWorks SafetyManager

Description: IndraWorks SafetyManager

● Full license

Activation key: AAAAAA - BBBBBB - CCCCCC - DDDDDE - EEEEE

○ Demo license (30 days)

Fig. 6-9: License dialog

To verify the activation key and to apply the license, press **Next >>**.

The IndraWorks SafetyManager license (Lite) is now installed and activated.

6.3.2 Project structure

The SafeLogic system is completely integrated in IndraWorks. All components can be accessed via the IndraWorks standard functionality.

In the following, the project tree structure and the project tree objects are described, available for the creation of a safe application with Safety according to the IEC 61508 and ISO 13849 guidelines.

The IndraWorks operating concept is used to create a project and to operate the interface. IndraWorks commands not available in Safety are visible but cannot be activated.

After inserting the Safety extension module below the control, the required objects to create the application are automatically generated below the Safety extension module node.

Yellow Safety structure

Using yellow structures, the Safety objects are highlighted in the project structure and the Safety editors and optically differentiate themselves from standard objects and standard editors.

Additionally, the safe signal flows are also highlighted in yellow. This supports and facilitates activities in the development, verification and acceptance of the Safety application.

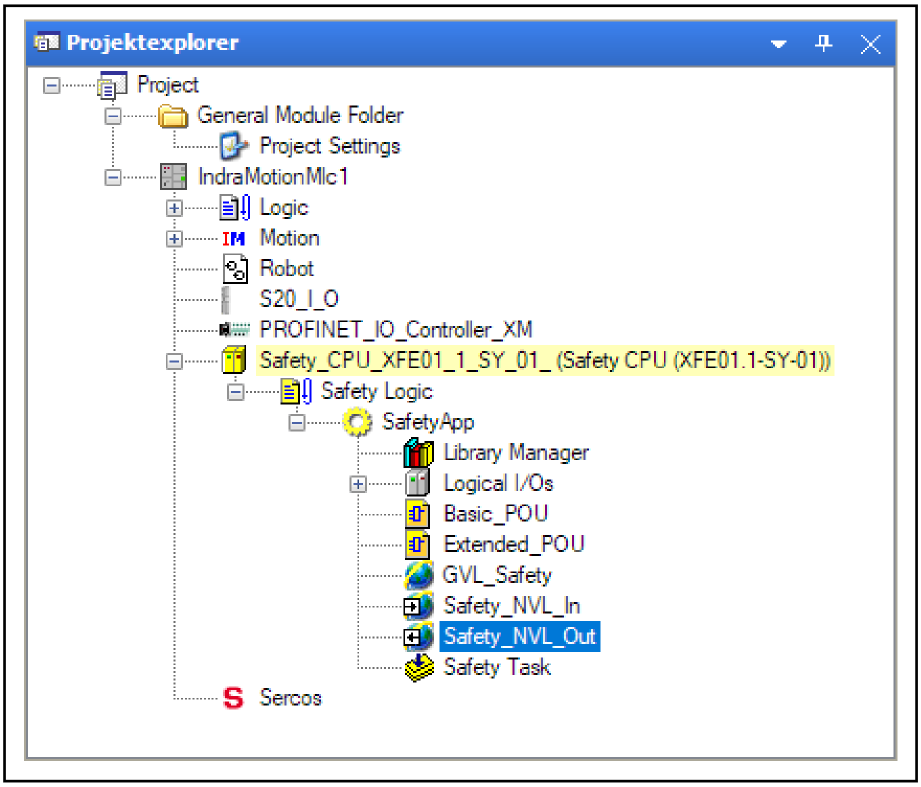


Fig. 6-10: Safety application in the Project Explorer of a control project

The objects below the Safety extension module are subject to the following limitations:

- Only one application allowed. The application is created automatically
- There is only one task. This task is created automatically
- The library manager is inserted automatically

The following objects and nodes exist exactly once below the Safety extension module:

- Safety logic:

  Logic node of the Safety control under which exactly one Safety application can be used

- SafetyApp:

  Node under which the Safety application objects can be found.

  Object specifying the code execution version and the current status (pin) of the application (see chapter "Pinning" on page 104).

  The object editor manages the list of the current Safety application objects:

  – Library manager:

    Contains the libraries available on the inserted Safety control (refer to chapter 6.3.2 "Project structure" on page 88)

  – Logic I/Os:

    Nodes to which logic I/O objects can be added. These added logic I/Os are used for data exchange with the standard control (see chapter 6.3.2 "Project structure" on page 88)

  – Safety task:

This object lists al programs that are loaded to the control and can be executed

The following objects can be added below the application (see chapter 6.3.2 "Project structure" on page 88):

- Basic_POU (Safety):

  POU (program or function block) with programming level Basic
- Basic_POU (Safety):

  POU (program or function block) with programming level Extended
- GVL_Safety (Global Variable List Safety):

  Declaration of global variables only valid within the Safety application

All objects can be protected from unauthorized access via the user management (see chapter 7 "Commissioning" on page 95).

6.3.3 Logic programming

A Safety application is programmed in POUs (programming organizational units), GVLs (Global Variable Lists) and in the task object.

In the POUs, the program code is implemented in IEC 61131-3 language FBD (function block diagram). Main features of the FBD: unambiguity, easy detection of programming errors and clear data flow.

The operating interface and handling of the SafeLogic FBD editor corresponds to the FBD editor of the standard control with regard to operating interface and handling.

Language scope

The FBD language scope is limited according to the language subset defined in PLCopen "Basic" and "Extended". The corresponding selection for the language selection "Basic Level" or" Extended Level" is specified by the developer when recreating a POU (program or function block):

- in **Basic Level**, a Safety application can be easily implemented and subsequently verified by linking the already certified function blocks of the PLCopen library (SafetyPLCopen)
- the **Extended Level** provides additional operators (Boolean, mathematical and others) and conditioned jumps/returns to create more comprehensive Safety applications. These operators and conditioned jumps/returns subsequently require a more complicated verification process.

Data types

The following data types are available in SafeLogic:

- *Standard data types*
  - BOOL
  - INT
  - DINT
  - BYTE
  - WORD
  - DWORD
  - TIME
- *Safety data types*
  - SAFEBOOL
  - SAFEINT
  - SAFEDINT

  - SAFEBYTE
  - SAFEWORD
  - SAFEDWORD
  - SAFETIME

Operators

SafeLogic provides the following operators:

Operators in "Basic level"

- AND
- OR

Operators in "Extended level"

- *Boolean operators*
  - AND
  - OR
  - XOR
  - NOT
- *Mathematical operators*
  - ADD
  - SUB
  - DIV
  - MUL
  - NE
  - LE
  - GE
  - GT
  - LT
  - EQ
  - NE
- *Other operators*
  - SEL
  - MUX

Safe data flow

The safe data flow of the FBD programming is highlighted as follows in SafeLogic:

- Constants and as constant declared variables are highlighted in yellow
- Variables with safe data type (SAFExxx) are highlighted in yellow
- Data flow of SAFE values in SAFE variables and inputs is highlighted by thick yellow lines
- Function blocks are highlighted in yellow if the function blocks have at least one SAFE output
- Operator call boxes are yellow if the output is SAFE. This is the case if:
  - in operator AN: the output is SAFE if at least 1 input is SAFE
  - all other operators including the conversions: the output is SAFE if all inputs are SAFE

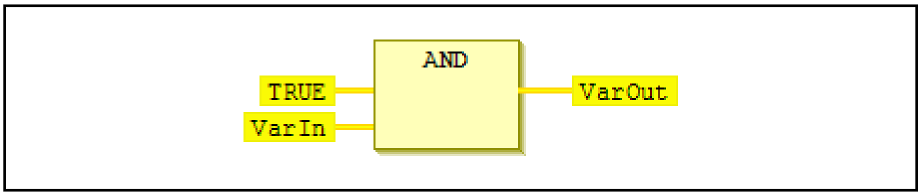


Fig. 6-11: Example of safe data flow: Operator AND with constant: TRUE, SAFE variables: VarIn and VarOut

Function blocks

Apart from "Operators" on page 91, libraries with several function blocks are available in SafeLogic. The libraries available for the Safety extension module are listed in the editor window of the library management of the Safety application.

The following function blocks are provided by the libraries:

- *SafetyStandard*
  - SF_RS
  - SF_SR
  - SF_CTD
  - SF_CTU
  - SF_CTUD
  - SF_TOF
  - SF_TON
  - SF_TP
  - SF_F_TRIG
  - SF_R_TRIG
- *SafetyUtilities*
  - SF_ClockGenerator
  - SF_StartupWarning
  - SF_IOConfig
  - SF_IOConfigCntl
  - BinaryDecoder_4_16
  - BinaryEncoder_16_4
  - SF_BinaryDecoder_4_16
  - SF_BinaryEncoder_16_4
  - BoolToByte
  - BoolToWord
  - BoolToDWord
  - SF_BoolToByte
  - SF_BoolToWord
  - SF_BoolToDWord
  - ByteToBool
  - WordToBool
  - DWordToBool
  - SF_ByteToBool
  - SF_WordToBool
  - SF_DWordToBool

- *SafetyPLCopen*
  - SF_Antivalent
  - SF_Equivalent
  - SF_EmergencyStop
  - SF_EnableSwitch
  - SF_ESPE
  - SF_EDM
  - SF_GuardLocking
  - SF_GuardMonitoring
  - SF_ModeSelector
  - SF_MutingPar
  - SF_MutingPar_2Sensor
  - SF_MutingSeq
  - SF_OutControl
  - SF_SafetyRequest
  - SF_TestableSafetySensor
  - SF_TwoHandControlTypeII
  - SF_TwoHandControlTypeIII
- *SafetyDriveMotion*
  - SF_MotionEmergencyStop
  - SF_MotionSafeStop
  - SF_SMMSelector
  - SF_AxisGroup
- *SafetyPLCopenPress*
  - SF_PressControl
  - SF_CamShaftMonitor
  - SF_CamMonitoring
  - SF_CycleControl
  - SF_SingleValveMonitoring
  - SF_SingleValveCycleMonitoring
  - SF_DoubleValveMonitoring
  - SF_ValveGroupControl

6.3.4 I/Os

The Safety extension module does not have any options to connect I/O devices. The periphery compatible with Safety is connected to the bus systems of the standard control.

The I/O signals to be processed on the Safety extension module are configured in the programming system. The input signals intended for the Safety extension module are filtered from the pool of the total I/Os on the standard control and are then transported to the Safety extension module. The output signals are transmitted from the Safety extension module to the standard control and are mixed in the pool of total I/O data by the standard control. Thus, a consistent I/O configuration has to be available on the standard control as well as on the Safety control. In case the I/O configuration is not identical, a "Caution symbol", superimposing the control icon, is displayed in the IndraWorks Project Explorer at the Safety extension module node.

☞ In case of I/O configuration inconsistency, no data is exchanged between the periphery and the Safety extension module.

Data is exchanged between the standard control and the Safety extension module via the same mechanism as with the periphery. This means, that no data is exchanged between standard control and Safety extension module in case of an I/O configuration inconsistency.

I/O accesses

The mapping variables are edited on the "mapping page" of the logic I/Os and are available for code implementation as variable of the category "Global variables".

6.3.5 TCI interface for PROFINET devices in IndraWorks

Tool Calling Interface (TCI)

The TCI is an interface to call device tools (Windows programs) from an engineering system (e.g. IndraWorks).

The device tools are used to parameterize field bus devices and they are provided by the device manufacturers.

A use case for device tools is the proprietary computation of the checksum (iParCRC) using the individual device parameters (iParameter) of PROFIsafe devices entered into the engineering system. The device parameters are sent to the device tool via TCI.

TCI was specified by "PROFIBUS International / PNO".

Usage in IndraWorks

The IndraWorks Engineering system supports the TCI interface in the version TCI 1.1 for PROFINET devices in the Conformance Class C2:

The device tool can be called in the Project Explorer via the context menu of the device/module node.

During the call, IndraWorks sends data (TPF file) to the device tool.

TCI is supported by the following systems:

- MLC
- MTX

Further information

A more detailed description about this topic can be found in the "IndraWorks Field Buses" documentation in chapter "Profinet IO, Tool Calling Interface (TCI)" in the Rexroth media directory

7 Commissioning

7.1 Overview

Refer to the installation and commissioning instructions in the user manuals of the used devices for information on the installation and commissioning the automation system.

Responsibilities

Clarify the responsibilities for installation and commissioning:

- Total responsibility
- Responsibility for individual subdomains (electronic engineering, mechanical engineering)
- Responsibility for switch on

☞ Please note: Installation and commissioning must only be carried out by qualified personnel. These persons have been instructed with regard to relevant standards, regulations, accident prevention regulations and operating conditions and are thus capable of performing the required activities and to identify and avoid potential risks.

User management of SafeLogic

In the user management, the access rights to a safety-oriented application can be structured and managed.

To open a project, the following is required:

- User name
- Password
- Group affiliation

The following user groups are available in the programming system:

- Maintenance
- Commissioning
- Developer
- Administrator

Refer to the programming system description for individual rights of the different user groups.

When the user management is activated for the first time, you are initially assigned administrator status. An administrator can:

- Create users
- Define user groups
- Assign users to different user groups

Each user may belong to several user groups. Any changes in the user management are documented with a log entry.

User management SafeLogic compact

These user administration provides user groups with different authorizations for the transfer of configurations to the devices:

- Machine operator
- Maintenance personnel
- Authorized client

Refer to the programming system description for individual rights of the different user groups.

A password can be assigned or changed for each user group.

7.2 Installation and commissioning sequence

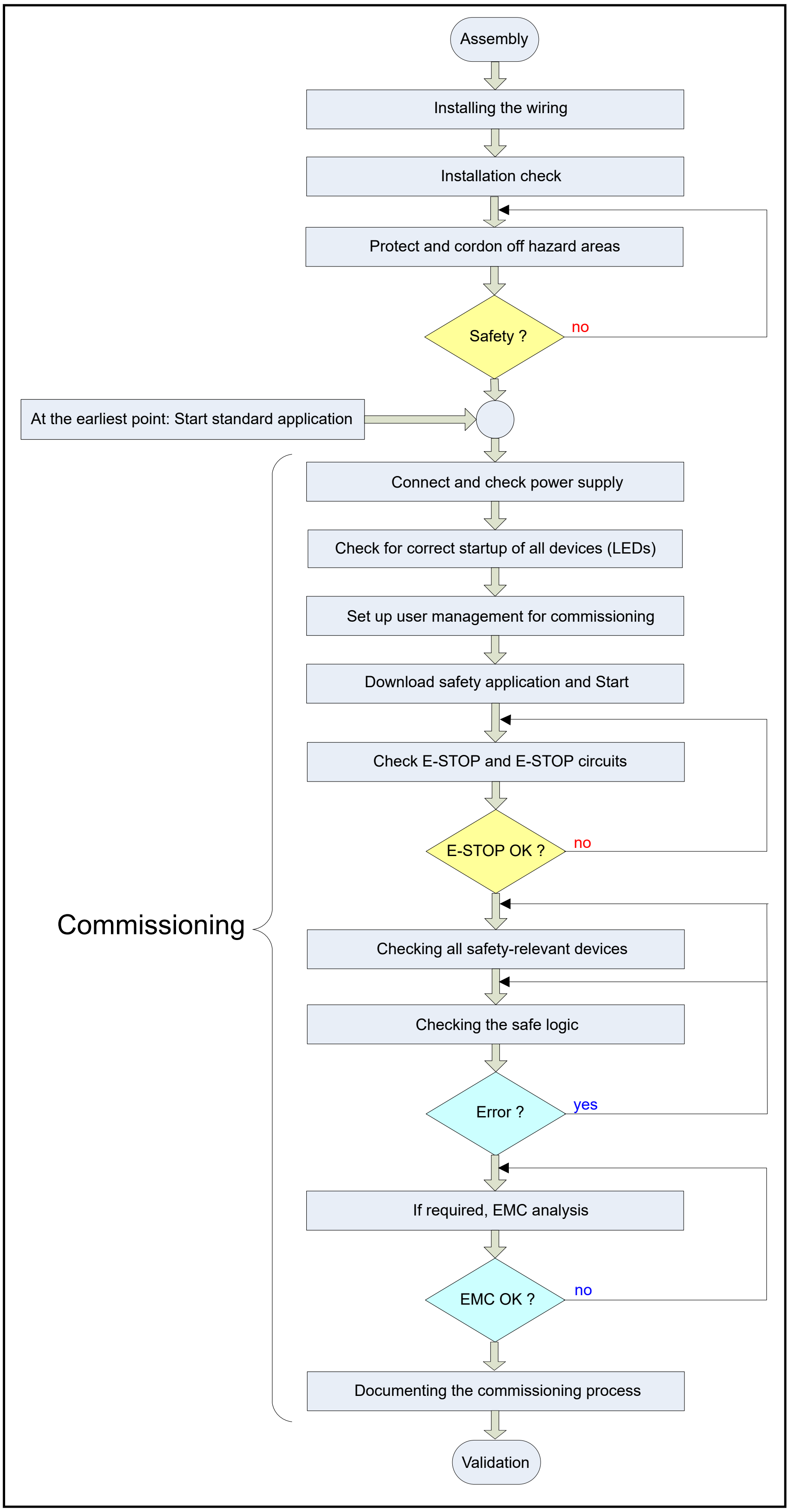

Assembly
Installing the wiring
Installation check
Protect and cordon off hazard areas
Safety ?
no
At the earliest point: Start standard application
Commissioning
Connect and check power supply
Check for correct startup of all devices (LEDs)
Set up user management for commissioning
Download safety application and Start
Check E-STOP and E-STOP circuits
E-STOP OK ?
no
Checking all safety-relevant devices
Checking the safe logic
Error ?
yes
If required, EMC analysis
EMC OK ?
no
Documenting the commissioning process
Validation

Fig. 7-1: Installation and commissioning sequence

7.3 Unpacking

When unpacking and handling electronic components, comply with the following:

NOTICE **Damages to the device due to electrostatic discharges!**

Comply with all ESD protective measures while working with modules and components! Avoid electrostatic discharges!

Packaging

Dispose of the packaging according to your national, country-specific regulations.

7.4 Mounting and installation

7.4.1 Device mounting of the Safety extension module

Mount the Safety control, the safe and unsafe I/O devices, the sensors and actuators according to the installation instructions of the individual devices. Take the device dimensions into consideration.

☞ Mount the Safety control horizontally in a control cabinet or in a corresponding housing with protection type IP54 according to IEC 60529.

Standard control and S20 I/O modules

To mount the control, install the standard control to the mounting rails and engage the control by exerting slight pressure on the bottom part of the housing. If required, position the Rexroth S20-I/O modules to the right side.

Function modules

A number of extension modules can be connected to the left side of the standard control using the function module plug connected to the control. The number and type of the supported function modules depends on the used standard control.

☞ Refer to the respective manual for all information about mounting the standard control, the S20-I/O modules and the function modules.

☞ Any warranty claim against the Bosch Rexroth AG shall be waived in case the device is modified - even within the framework of mounting or installation.

7.4.2 Device mounting of SafeLogic compact

Assembly and disassembly

General information

This chapter explains how modules of the SafeLogic compact safety control are disassembled.

Steps for module disassembly

⚠ **CAUTION**

The SafeLogic compact system has to be installed in a control cabinet with protection class IP 54 or higher!

- In a SafeLogic compact system either the main module SLC-3-CPU0, SCL-3-CPU1 or SLC-3-CPU3 is on the far left
- The two optional gateways are immediately on the right of the main module
- Install any additional SafeLogic compact extension modules (e.g. SLC-3-XTI, SLC-3-XTDIO or SLC-0-STIO) to the right of the gateways or to the right of the main module if no gateways are used
- Install any additional relay modules (UE410-2RO or UE410-4RO) on the far right in the SafeLogic compact system
- The modules are housed in an installation housing with a width of 22.5 mm for 35 mm rails according to EN 60 715
- The modules are interconnected via the FLEXBUS+ plug-in connection integrated into the housing. Keep in mind that the SafeLogic compact modules have to be separated by approx. 10 mm to remove a module from the rail for module exchange.
- Install the modules according to EN 50 274
- Take suitable ESD protective measures during installation. Otherwise, the FLEXBUS+ bus may be damaged
- Take suitable measures to prevent any foreign objects from entering the openings of the connector, in particular those of the flash drive
- Modules with ventilation slots have to be installed vertically in such a way that vertical air circulation is possible, i.e. the ventilation slots have to be positioned at the top and at the bottom

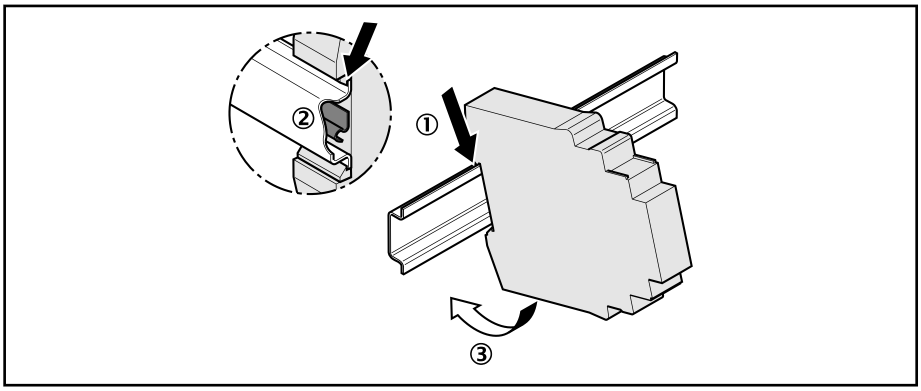


Fig. 7-2: Placing the module on the rail

- Make sure that the operating voltage of the SafeLogic compact system is turned off
- Place the device on the rail ①
- Verify correct position of the grounding spring ②. The grounding spring of the module has to rest safely and with good electrical conduction on the rail
- Lock the module on the rail by applying slight pressure in the direction of the arrow ③

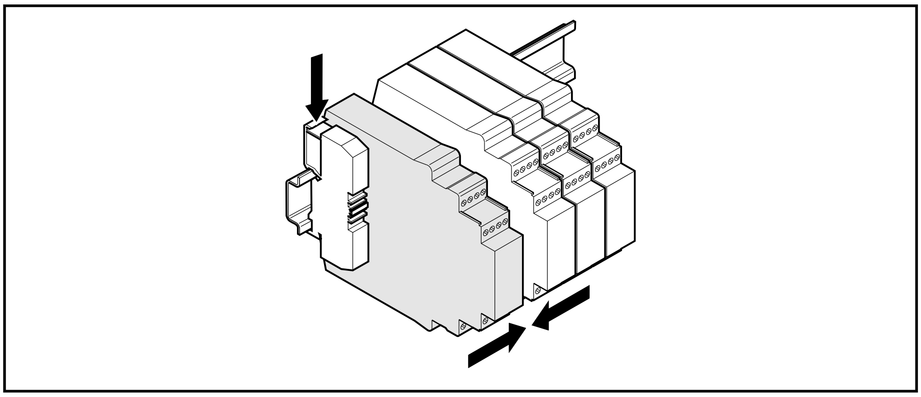


Fig. 7-3: Installing end brackets

- If there are several modules, push the individual modules together in the direction of the arrow until the lateral plug-in connection locks in place
- Install end brackets on the left and on the right

Following assembly, the following steps are required:

- Establishing the electrical connections
- Configuration (see operating instructions "Rexroth IndraLogic SafeLogic compact Designer Software")
- Checking the installation

Steps for module disassembly

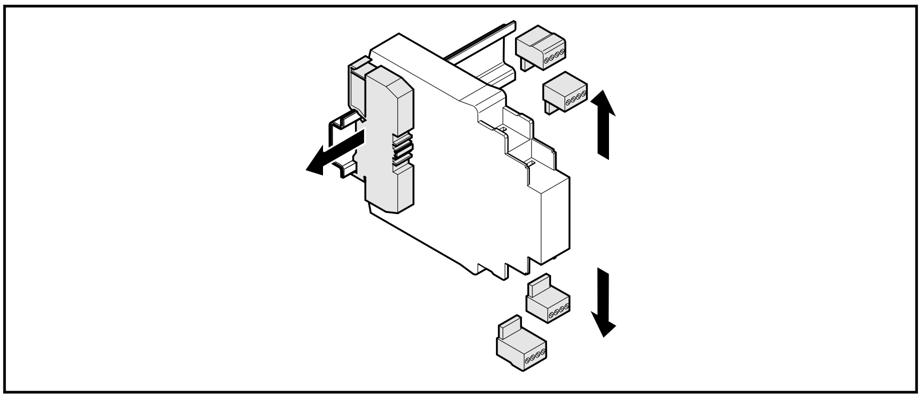


Fig. 7-4: Removing plug-in terminal blocks

- Remove the plug-in terminal blocks with the wires and the end brackets

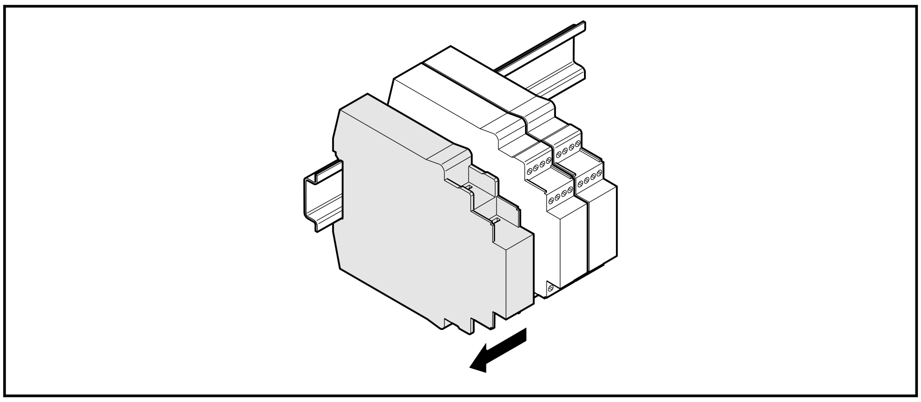


Fig. 7-5: Disconnecting the plug-in connection

- If there are several modules, push the individual modules apart in the direction of the arrow until the lateral plug-in connection disconnects

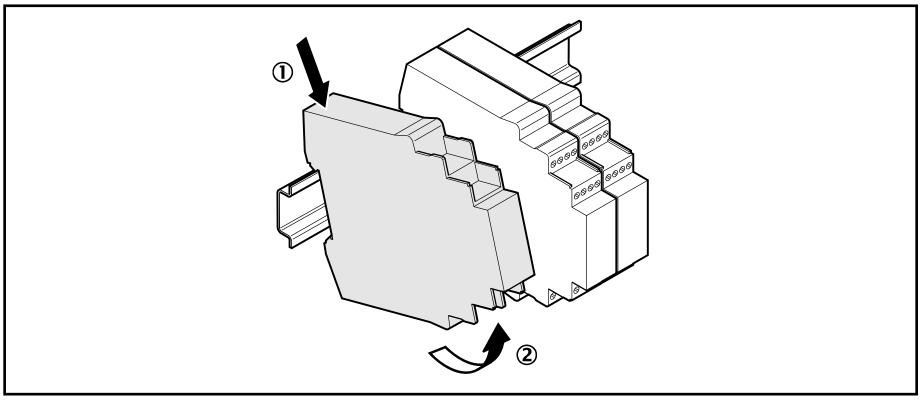


Fig. 7-6: Removing the module from the rail

- Push the module down at the rear ① and remove it in the direction of the arrow from the rail ② keeping it pushed down

7.4.3 Wiring installation

Install the wiring according to the specified connection diagram and the installation instructions in the relevant device descriptions.

Also take the installation instructions for bus systems into consideration; in particular the special requirements on the installation when using safety-oriented profiles of the bus systems for safe data communication.

Ensure that cross sections of the cables correspond to the specifications.

Uniquely mark all connections (connecting cables and plug-in connectors) at the Safety control to avoid confusion.

Voltage supply

Note:

The power supply of the Safety control must only be provided by power supply units with safe isolation according to EN 50178 (or power sources with an identical degree of safety) with PELV voltage according to EN 61131-2.

The Safety extension module does not have an individual power supply, refer to the specifications in the manual of the standard control regarding the electrical installation.

Devices

Wire the safe and unsafe I/O devices, the sensors and actuators and the Safety control.

Field buses

Wire the field buses according to the installation instructions of Profibus DP, PROFINET, PROFIsafe or Sercos III.

- Only use approved cables
- Refer to the installation instructions according EMC
- Check the Emergency stop or emergency stop circuits

7.4.4 Check

Verify the correct mounting and wiring.

Verify the wiring according to the specified connection diagrams. It is recommended to specify an acceptance report for wiring in the safety plan.

- Be aware of short circuits and cross-circuits in all wires
- Perform measurements using a multimeter
- Verify that the grounding is safe

7.5 Commissioning the components

7.5.1 Before switching on

Note:

Commissioning all components is only allowed once the machine or system the components are installed in correspond to the country-specific regulations, safety regulations and standards of the application.

Ensure the system safety!

- Before commissioning, ensure that no individual is in the danger zone.
- Before commissioning, always connect the ground conductor or connect to the ground wire, even for test purposes. Otherwise, very high voltages can occur on housings, causing electrical shock
- Position emergency switches easily accessible in the direct vicinity
- Avoid hazards by additional access protections as long as not all safety functions have been commissioned. Possible access protection: Covers, barriers or obstacles, so-called guards
- Take mechanical precautionary measure if parts can be ejected out of the machine
- Another measure that is recommended is to limit the motion velocity, the motion force or the motion duration (jog mode) by using a manual operator station with enabling switch and +/– keys if the corresponding safety functions have already been commissioned
- Supplementing measures to classic safety functions are locking indicators, signal lights and other start-up alarm devices

☞ Connect the voltage only after the system has been set up completely.

The system can only start if no hazards can arise from the system.

7.5.2 Connecting the supply voltage

Check the correct power supply of all components using your configuration specifications.

Subsequently, check the function of the emergency stop function before continuing the commissioning.

☞ Do not operate the machine or the system in case of a malfunction of the emergency stop function.

7.5.3 Function test and trouble shooting

Systematically scan the system for:

- Installation error
- Errors caused by disturbances (EMC influences)
- Errors caused by disturbances in the power supply, voltage dips or power failure
- Influences on network wirings and communication
- Application errors

The component diagnostics and the programming system support the user in this task.

The programming system provides the following functionalities:

- Monitoring the variables
- Forcing variables
- Debugging and sequence control
- Online changes of variables, function blocks, parameters

EMC

Avoid the operation of high frequency, remote control device and radio units in close proximity to the device electronics and their supply cables. If the use of the devices cannot be avoided, check the system for potential malfunctions.

The individual components are checked by type checks for compliance with standards (generic standards for the industrial sector and/or EMC product standards) and meet the EC EMC guideline.

The limit values and standards that are complied with are specified in the respective product. The checks are carried out at a system-typical set-up on a test bench that complies with the standard.

The test results, however, cannot always be applied to the installed condition in the end product, the machine or the system. If necessary, perform a special electromagnetic compatibility (EMC) test on the installation.

Device start-up

- Use the LED display to verify that all devices and modules start up correctly or if errors are reported

Check device connections

- Verify that the safe devices are correctly connected to the assigned sensors and actuators

Checking the inputs/outputs

- Measure the input and output voltages to ensure that the voltages are within the valid range
- If possible, measure the waveform of the signals to ensure that the dynamic behavior corresponds to the expectations
- Are the inputs - connected as dual-channel - parameterized in a way that they match each other?
- Is the assignment to the correct clock outputs parameterized at the inputs?

Configuration check

- Verification of the variable link between the function blocks and the inputs/outputs

Data communication check

- Verify the communication parameters of the bus communication
- Were all addresses specified correctly?
- Was the correct transmission rate selected?

7.5.4 Commissioning SafeLogic

Commissioning the application

Commissioning steps of the Safety extension module

1. Download and start the standard PLC.
2. Download motion and set to P4.
3. Download and start the Safety PLC.
4. Acknowledge start-up errors of the bus systems.

☞ The multi-device functionality with SafeLogic is supported by the system MLC.

For more information, refer to the "SafeLogic Project Configuration" documentation in the Rexroth media directory

Debug mode

To test the application program functionality and for trouble shooting purposes, use the debug mode. In this operating state, the Safety control is in operation and processes the application program. The debug mode provides comprehensive commissioning options, starting with forcing of inputs up to single-step mode, in particular the option to change the application online.

Thus, not only errors can be diagnosed in the application program but the Safety system and the Safety functions can be commissioned step-by-step. Due to its extended options, this operating state is not safe, debug commands can potentially be dangerous.

☞ In the "Debug" operating state, use organizational measures to ensure that no damage can be caused by an intended function or a malfunction of the Safety control.

Make sure that no individual is in the danger zone and that nobody has access to the danger zone.

Commissioning the safety functions

Test the function of the Safety functions. This technical test may only be performed by qualified safety personnel.

The technical test includes the following test items:

- Uniquely mark all connecting cables and plug-in connectors to avoid confusion. Ensure that loosened connection cables are not reconnected to the incorrect connection
- Perform a complete verification of the Safety functions of the system in each operating mode and an error simulation. In particular, test the response time of the individual applications
- Check the signal paths and the correct inclusion in higher-level controllers
- Check the correct data transfer from and to the SafeLogic compact safety control
- Check the logic program of the safety control
- Completely document the configuration of the system, the individual devices and the results of the safety check
- Check the safety functions of the machine or system completely and ensure that the safety functions work perfectly
- Check the devices connected to the Safety control according to the test instructions in the relevant operating instructions
- In order to prevent unintentional overwriting of the configuration, activate the write protection

Commissioning documentation

Information documented during commissioning have to include:

- The documentation of commissioning activities
- Notes to failure reports
- Elimination of failures and incompatibilities

Log of the Safety extension module

The Safety extension module provides support in the commissioning documentation by maintaining a logbook that is displayed at the programming system in online mode.

This logbook logs a number of events in the Safety control, including date and time of the events, the person responsible (identified via the user management), the type (information, warning, error, exception) and other type-dependent plain text information.

The following events are entered:

- Login/logout
- Downloading application
- Stop/run switching
- Forcing inputs
- Generating the boot application
- Acceptance note
- System error messages
- General reset (deleting the application and the user management)

The logbook is organized as ring buffer and provides the capacity for several thousand entries. The logbook cannot be deleted so that the last entries are irrevocably documented within the framework of capacity.

Pinning

Preparing measures for verification

To verify the Safety application, the developer has to provide preparing measures. An essential aspect is to specify the Safety application version for verification and to ensure that only this Safety application version is used for verification, validation and subsequent acceptance.

In particular, the IndraWorks Safety Manager provides the **Pinning** function.

Prior to verify the programmed or changed Safety application, re-pin the Safety application.

Only pinned applications can be verified and accepted. No application object can have the status "In Work".

The check for the "In Work" status is carried out in the individual verification steps.

☞ A pinned application can only be considered as checked after the verification (see chapter 7.5.4 "Commissioning SafeLogic" on page 102).

What is pinning

Pinning means that a reference point is set to the current status of a Safety application, identifying the correct status of the Safety application and its corresponding objects.

By using pinning, it is possible to identify a certain application version in the project, of an object in the editor and a boot application on the Safety control. Furthermore, changes to the application structure, the object content and the referenced library function blocks can be detected at any time - based on pin.

☞ By setting a pin, a concrete version can be identified, however, the concrete version is not duplicated!

💡 A pinned object can be transmitted to another application by export/import, without having to identify the object again. Only the object pin has to be verified.

Comparison view

The pin functions are contained in the application object editor. Select the Safety application object from the project tree and open it via the context menu command **Open**. The **Objects** tab shows the comparison view, displayed the version and checksum of the objects of the current project and the pinned project.

☞ For more information, refer to chapter "Pinning" of the "Rexroth IndraWorks 15VRS SafeLogic Project Configuration" documentation.

Verification

Requirement: The user has to have specified the desired software application behavior in earlier development phases (software specification). The user also has to specify the desired programming and commenting rules (programming guidelines).

The software verification process is used to verify that the specification and the programming guidelines are complied with and thus verified. The software is verified by the combination of static and dynamic verification methods (tool-based checks, code review, tests).

After the software is verified, as a second verification step, the programmed Safety functions in the set-up machine is validated.

Both steps are a prerequisite for the acceptance of the machine and the Safety application.

☞ Only pinned Safety applications can be verified and accepted. No application object can have the status "In Work".

💡 The yellow data flow is not intended as support for verification, validation and acceptance.

💡 The IndraWorks standard project view is **not suited** for verification and acceptance of a Safety application. As identification which objects are part of the Safety application, the comparison view has to be used.

💡 The IndraWorks standard project view is **not suited** for verification and acceptance of a Safety application. The project comparison can only be used as auxiliary function to open the comparison editor of changed objects.

☞ To simplify and accelerate the entire verification and validation process, SafeLogic provides the already validated and certified PLCopen function block and the function blocks of the Safety standard library.

☞ For more information, refer to chapter "Verification" of the "Rexroth IndraWorks 15VRS SafeLogic Project Configuration" documentation.

Acceptance

Acceptance, introduction

☞ During the entire process, starting from the development until the acceptance of a Safety application, the user has to make sure that the correct object versions, the correct libraries and the correct device description files are used (see chapter "Pinning" on page 104).

☞ The user is has to ensure that the all relevant standards have been complied with for acceptance of the Safety application.

☞ To assess the correct use of the function block interface, use the user documentation for this function block and for this control in the relevant version.

☞ The IndraWorks standard project view is **not suited** for verification and acceptance of a Safety application. As identification which objects are part of the Safety application, the comparison view has to be used.

☞ The IndraWorks standard project view is **not suited** for verification and acceptance of a Safety application. The project comparison can only be used as auxiliary function to open the comparison editor of changed objects.

Requirements and verifications for acceptance

☞ Prior to acceptance of the Safety application, the user has to verify that the application from which the boot application is generated is pinned, the correct pin ID is displayed and that no project version deviation is reported by the pinned version.

☞ For the acceptance, the user has to verify if the device description compatible with the device in the machine is used in the project.

☞ For more information, refer to chapter "Acceptance" of the "Rexroth IndraWorks 15VRS SafeLogic Project Configuration" documentation.

7.5.5 Technical commissioning SafeLogic compact

General information

The configuration of the SafeLogic compact system has to be completed before you begin with the technical commissioning.

Wiring and voltage supply

⚠ CAUTION

When connecting the SafeLogic compact system, refer to the technical data in the "IndraControl SafeLogic compact Hardware" operating instructions!

- Connect the individual field devices to the corresponding signal connections and check whether each safety input, test/signal output and safety output behaves as required by the application. Diagnostics information from the SafeLogic compact LEDs support you in validating the individual field signals. Check whether the external circuit, the implementation of the wiring, the choice of the pick-ups and their location on the machine meet the required safety level
- Eliminate any faults (e.g. incorrect wiring or crossed signals) at each safety input, test/signal output or safety output before you continue with the next step
- Switch on the voltage supply. As soon as the supply voltage is applied to the connections "A1" and "A2" of the controller modules CPU0/CPU1/CPU3 or of the XTIO/XTDS/STIO modules, the SafeLogic compact system automatically carries out the following steps:
  - Internal self-test
  - Loading of the saved configuration
  - Testing of the loaded configuration for validity

The system does not start up if the steps described above could not be carried out successfully. If there is an error, this is indicated correspondingly by the LEDs (see the SafeLogic compact hardware operating instructions) and the SafeLogic compact system only transfers Low values.

Transferring the configuration

After you have configured the hardware and the logic in the SafeLogic compact system and have checked whether they are correct, transfer the configuration to the SafeLogic compact system via the SafeLogic Designer.

Technical test and commissioning

The machine or system that is protected by a SafeLogic compact safety controller may only be started up after a successful technical check of all safety functions. The technical test may only be performed by qualified safety personnel.

The technical test includes the following test items:

- Uniquely mark all connection cables and connectors at the SafeLogic compact system to avoid confusion. Since the SafeLogic compact system has several connections of the same design, ensure that loosened connection cables are not connected again to the incorrect connection
- Verify the configuration of the SafeLogic compact system
- Check the signal paths and the correct inclusion in higher-level controllers
- Check the correct data transfer from and to the SafeLogic compact safety controller
- Check the logic program of the safety controller
- Completely document the configuration of the entire system, the individual devices and the results of the safety check
- Check the safety functions of the machine or system completely and ensure that the safety functions work perfectly
- In order to prevent unintentional overwriting of the configuration, activate the write protection of the configuration parameters of the SafeLogic compact system. Modifications are now no longer possible unless the write protection has been deactivated

7.5.6 Modifications

When adding or replacing components or other modifications of the Safety system or subsystems already commissioned, the commissioning of all affected parts and Safety functions has to be repeated.

Module replacement

Do not replace any modules if the system is energized. Please make sure that the new device type and the device version are correct.

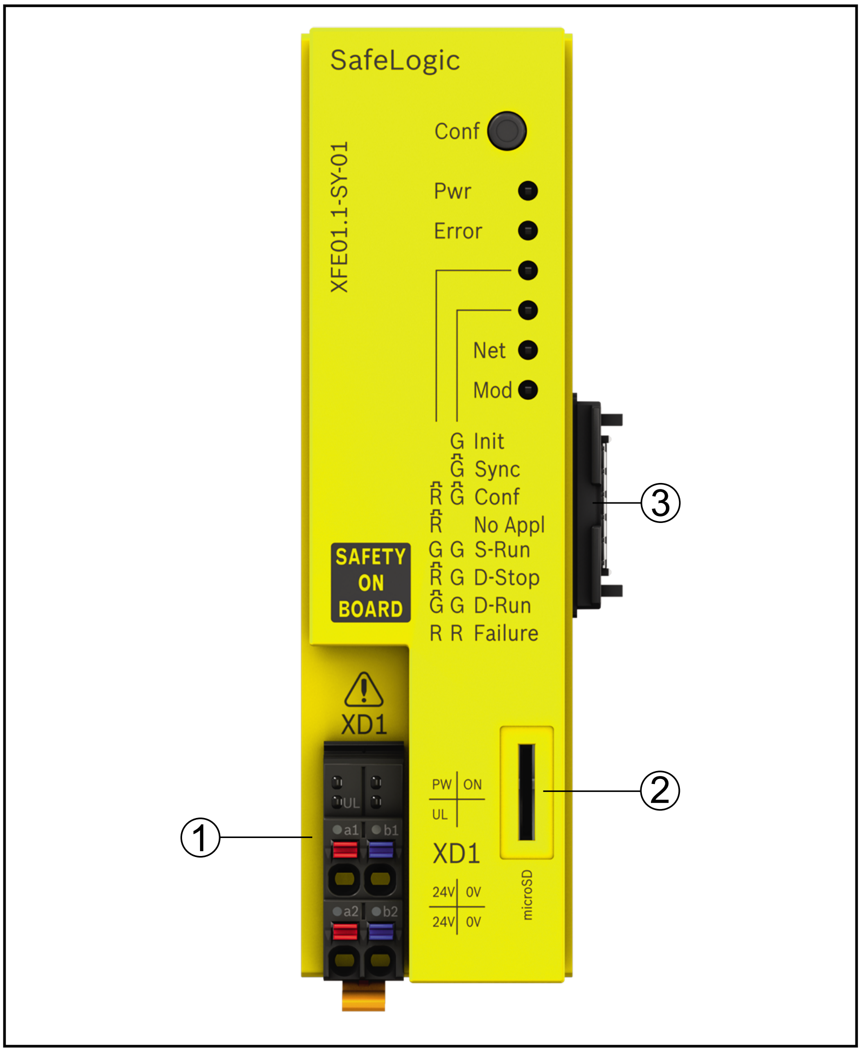
- SLc

  The system configuration of the entire SafeLogic compact system is only stored to the memory plug. The advantage when replacing extension modules is that the SafeLogic compact system does not have to be reconfigured

- SL

  When replacing the SafeLogic extension module, the microSD card of the old extension module can be used. The microSD card contains:

  - Application program (boot application)
  - User management data
  - Logbook
  - Firmware of the Safety extension module



① 24 V voltage supply

② microSD slot with microSD card

③ plugged bus base module

Fig. 7-7: microSD card position on the SafeLogic extension module

- Profibus Inline bus coupler/S20 bus coupler

  When replacing the Profibus coupler, the Profibus address has to be set again at the coupler. When replacing the PROFIsafe I/O, the DIP switch position has to be applied form the old module

- Profibus Inline bus coupler/S20 bus coupler

  When replacing the PROFIsafe I/Os, the DIP switch position has to be applied from the old module.

  For more information about the device replacement of the Profinet Inline bus coupler or S20 bus coupler, refer to the documentation "Rexroth IndraWorks 15VRS Field Buses", chapter "PROFINET I/O", subchapter "PROFINET I/O, topology and device replacement" (see chapter 1.4 "Required and supplementing documentation" on page 2).

- Sercos coupler

  When replacing the CSos S20 I/Os, the DIP switch position has to be applied from the old module.

For more information about the device replacement of the Sercos S20-S3-BK+ bus coupler, refer to the documentation "Rexroth IndraWorks 15VRS Field Buses", chapter "Sercos III I/O", subchapter "Adding a Sercos III master, slave" in the Rexroth media directory.

- IndraDrive

  In IndraDrive, all parameters including the SafeMotion are saved in the display. The display is applied to the new drive. During booting of the drive, "Load New Safety" is displayed. Check the drive function

8 Diagnostics and trouble shooting

8.1 Diagnostic concept

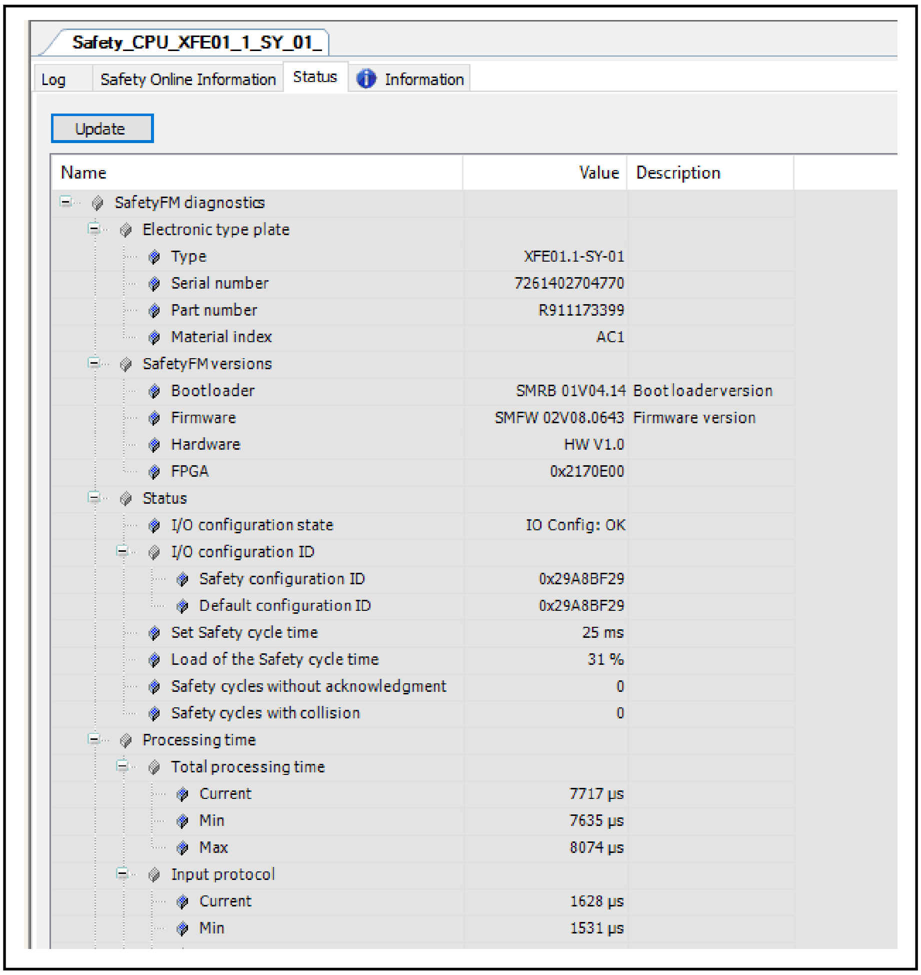
Comprehensive options for diagnostics are available in the safety system.

Initially, the operating and error states are displayed at the LED displays. For details, please refer to the device descriptions. The Safety extension module as well as SafeLogic compact are described in chapter 4.4 "Safety controls" on page 45.

Furthermore, error messages and status information are displayed during online mode of the programming system. These diagnostic messages are not safety-relevant and are sent to the programming system via the standard channels.

Device diagnostics of the Safety extension module

The device dialog displays status information (e.g. "Running", "Stopped") and specific diagnostic messages from the device and the bus system. This information is displayed in the display field "Status" of the device editor.



Name	Value	Description
SafetyFM diagnostics		
Electronic type plate		
Type	XFE01.1-SY-01	
Serial number	7261402704770	
Part number	R911173399	
Material index	AC1	
SafetyFM versions		
Bootloader	SMRB 01V04.14	Bootloaderversion
Firmware	SMFW 02V08.0643	Firmware version
Hardware	HW V1.0	
FPGA	0x2170E00	
Status		
I/O configuration state	IO Config: OK	
I/O configuration ID		
Safety configuration ID	0x29A8BF29	
Default configuration ID	0x29A8BF29	
Set Safety cycle time	25 ms	
Load of the Safety cycle time	31 %	
Safety cycles without acknowledgment	0	
Safety cycles with collision	0	
Processing time		
Total processing time		
Current	7717 µs	
Min	7635 µs	
Max	8074 µs	
Input protocol		
Current	1628 µs	
Min	1531 µs	

Fig. 8-1: Device status display (example: Safety extension module)

Depending on the device, different diagnostic information is available. There may be status messages, error messages and additional information. Error messages may refer to component errors, communication errors and peripheral errors, such as short-circuits or discrepancy time exceedance.

Safety control

The current module status for standard control and Safety extension module is displayed at the programming system during online mode. Errors, warnings, exceptions and further information are registered and saved including the data and notes about the localization in logbooks (Safety module and standard control separately). This further information refers to the CPU, the module firmware, the operating sequence and the online dialog.

Program diagnostics

To diagnose the application behavior, the programming system provides different debug services. Amongst others, these are the most important features:

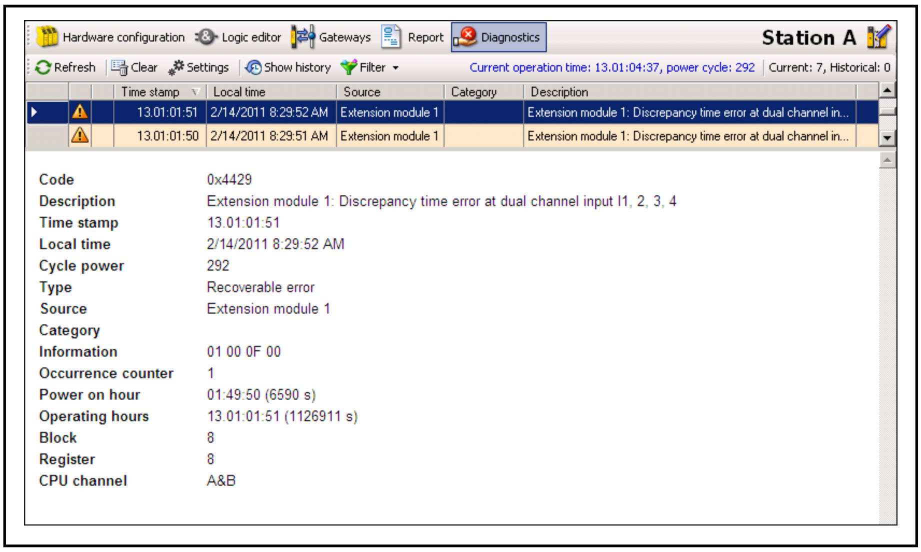
- Current variable state representation
- Information about the task behavior (cycles, cycle times, status)
- Dynamic block analysis (execution times, number of calls, code lines that have not been run)

The application program can be systematically analyzed, step-by-step, due to the option to set breakpoints.

Refer to the documentation of the programming system "SafeLogic Designer" and " IndraWorks" (see chapter 1.4 "Required and supplementing documentation" on page 2).

8.2 SafeLogic compact logbook

Once a connection has been established to your SafeLogic compact system, you can perform a diagnostics on your system. In the "Diagnostics" view, a complete history of all messages, information, warnings and error messages of a connected SafeLogic compact system is available in the upper part of the window. If you click on one of the entries in the list, details on the selected message are displayed in the lower part of the window.



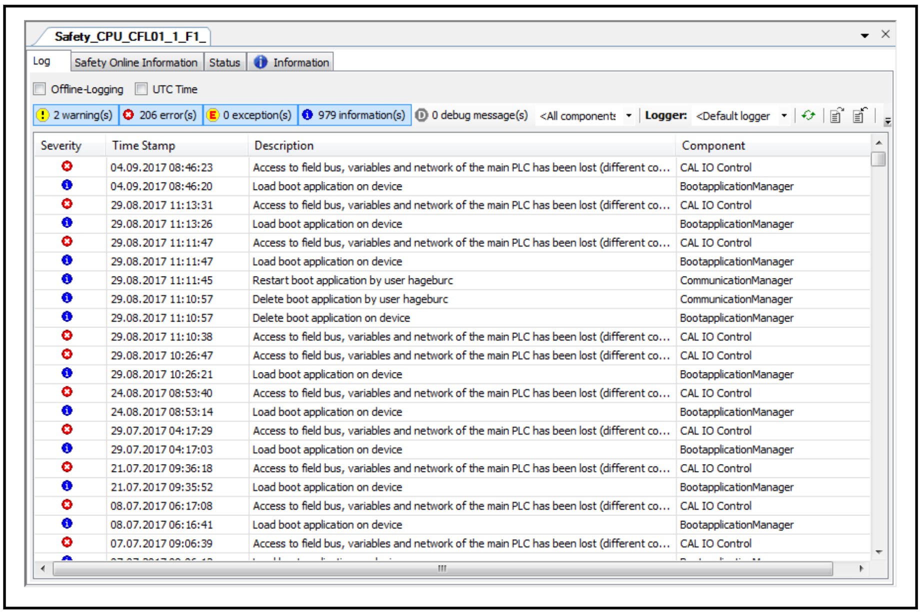
Current operation time: 13.01:04:37, power cycle: 292 | Current: 7, Historical: 0

		Time stamp	Local time	Source	Category	Description
▶	⚠	13.01:01:51	2/14/2011 8:29:52 AM	Extension module 1		Extension module 1: Discrepancy time error at dual channel in...
	⚠	13.01:01:50	2/14/2011 8:29:51 AM	Extension module 1		Extension module 1: Discrepancy time error at dual channel in...

Code	0x4429
Description	Extension module 1: Discrepancy time error at dual channel input I1, 2, 3, 4
Time stamp	13.01:01:51
Local time	2/14/2011 8:29:52 AM
Cycle power	292
Type	Recoverable error
Source	Extension module 1
Category	
Information	01 00 0F 00
Occurrence counter	1
Power on hour	01:49:50 (6590 s)
Operating hours	13.01:01:51 (1126911 s)
Block	8
Register	8
CPU channel	A&B

Fig. 8-2: Diagnostic overview

8.3 Logbook of the Safety extension module



Safety_CPU_CFL01_1_F1_

Log | Safety Online Information | Status | Information

□ Offline-Logging □ UTC Time

2 warning(s) | 206 error(s) | 0 exception(s) | 979 information(s) | 0 debug message(s) | <All components | **Logger:** <Default logger

Severity	Time Stamp	Description	Component
✖	04.09.2017 08:46:23	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	04.09.2017 08:46:20	Load boot application on device	BootapplicationManager
✖	29.08.2017 11:13:31	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	29.08.2017 11:13:26	Load boot application on device	BootapplicationManager
✖	29.08.2017 11:11:47	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	29.08.2017 11:11:47	Load boot application on device	BootapplicationManager
ℹ	29.08.2017 11:11:45	Restart boot application by user hageburc	CommunicationManager
ℹ	29.08.2017 11:10:57	Delete boot application by user hageburc	CommunicationManager
ℹ	29.08.2017 11:10:57	Delete boot application on device	BootapplicationManager
✖	29.08.2017 11:10:38	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
✖	29.08.2017 10:26:47	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	29.08.2017 10:26:21	Load boot application on device	BootapplicationManager
✖	24.08.2017 08:53:40	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	24.08.2017 08:53:14	Load boot application on device	BootapplicationManager
✖	29.07.2017 04:17:29	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	29.07.2017 04:17:03	Load boot application on device	BootapplicationManager
✖	21.07.2017 09:36:18	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	21.07.2017 09:35:52	Load boot application on device	BootapplicationManager
✖	08.07.2017 06:17:08	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control
ℹ	08.07.2017 06:16:41	Load boot application on device	BootapplicationManager
✖	07.07.2017 09:06:39	Access to field bus, variables and network of the main PLC has been lost (different co...	CAL IO Control

Fig. 8-3: Safety control logbook

The logbook is displayed in the **Log** tab of the Safety control and is used as protocol and to diagnose runtime errors of the application and system errors. This might help to find the error cause in the PLC or application.

There are two logs in IndraWorks:

- Device logbook
- Application log

The device log is part of the device and is intended for entries concerning the device, such as system errors or generating new boot applications.

The application log is part of the IEC application and is intended for entries concerning the application, such as runtime errors, errors while loading the boot application and errors during online communication.

The application log is the default log of the Safety control. The device log is only available if the default log (application log) has been loaded.

Press the ⟳ button to cyclically load all available logs ("Devices" and "Application" log) from the control. They can be subsequently selected in the **Logger** window.

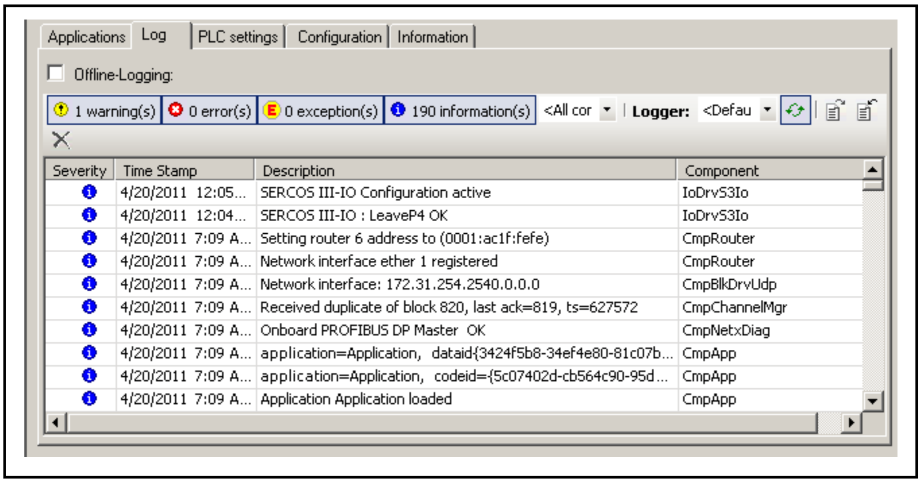
The information displayed in the logs are structured as follows:

- Weighting (information, warning, error, exception)
- Time stamp
- Error description
- Component (generator)

8.4 Logbook of the standard control

For example, the logbook of the standard control logs problems occurring when trying to establish a connection and during the data transfer from or to safe bus devices. Double-click on the control and select the tab **Log** to open the logbook.

The log of the standard PLC is in the RAM of the control. The logbook is lost during switch on/off of the control.



Severity	Time Stamp	Description	Component
ℹ	4/20/2011 12:05...	SERCOS III-IO Configuration active	IoDrvS3Io
ℹ	4/20/2011 12:04...	SERCOS III-IO : LeaveP4 OK	IoDrvS3Io
ℹ	4/20/2011 7:09 A...	Setting router 6 address to (0001:ac1f:fefe)	CmpRouter
ℹ	4/20/2011 7:09 A...	Network interface ether 1 registered	CmpRouter
ℹ	4/20/2011 7:09 A...	Network interface: 172.31.254.2540.0.0.0	CmpBlkDrvUdp
ℹ	4/20/2011 7:09 A...	Received duplicate of block 820, last ack=819, ts=627572	CmpChannelMgr
ℹ	4/20/2011 7:09 A...	Onboard PROFIBUS DP Master OK	CmpNetxDiag
ℹ	4/20/2011 7:09 A...	application=Application, dataid{3424f5b8-34ef4e80-81c07b...	CmpApp
ℹ	4/20/2011 7:09 A...	application=Application, codeid={5c07402d-cb564c90-95d...	CmpApp
ℹ	4/20/2011 7:09 A...	Application Application loaded	CmpApp

Fig. 8-4: Device editor, log

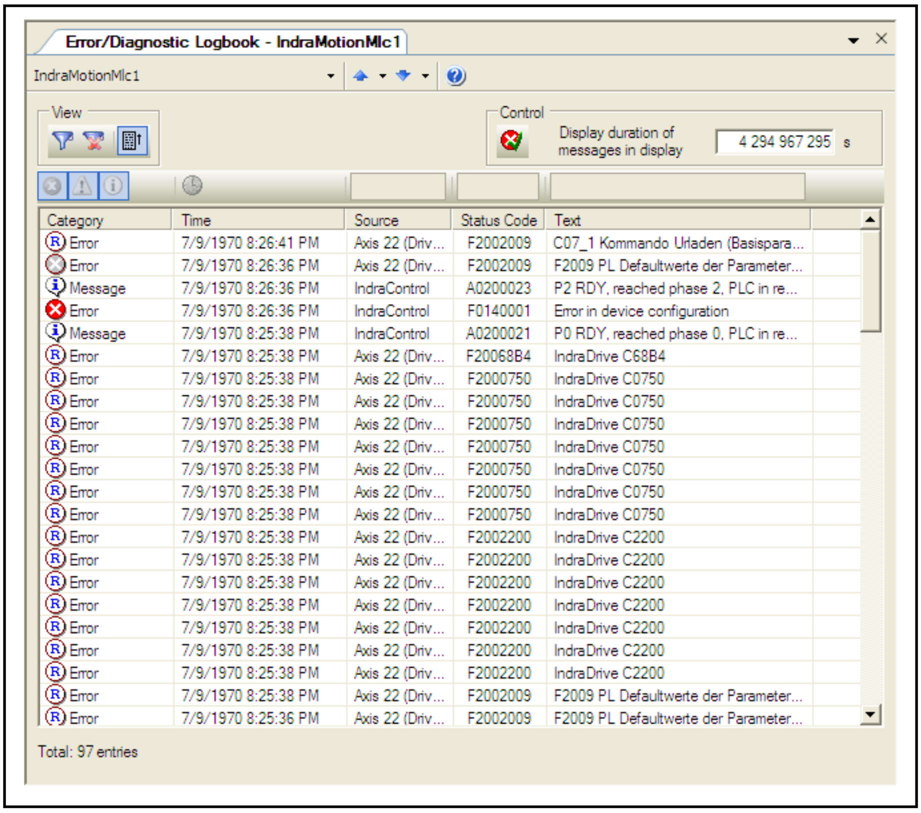
To activate the logbook, go to **Tools ▸ Options...** and subsequently to **IL2G ▸ General Settings**.

8.5 Device diagnostics of the standard control

IndraLogic XLC/IndraMotion MLC

The "Error/diagnostic memory" dialog provides an overview on all diagnostic messages of the control and the connected devices. The diagnostic messages are sorted automatically. The latest messages are on top of the list. All standard PLC messages are saved in abbreviated form in the "Error/diagnostic memory".

The logbook entries are saved as non-volatile on the control. Thus, they are still available even when the control is switched off and on again. The memory of the device diagnostics is limited to 100,000 entries.



Display duration of messages in display 4 294 967 295 s

Category	Time	Source	Status Code	Text
Error	7/9/1970 8:26:41 PM	Axis 22 (Driv...	F2002009	C07_1 Kommando Urladen (Basispara...
Error	7/9/1970 8:26:36 PM	Axis 22 (Driv...	F2002009	F2009 PL Defaultwerte der Parameter...
Message	7/9/1970 8:26:36 PM	IndraControl	A0200023	P2 RDY, reached phase 2, PLC in re...
Error	7/9/1970 8:26:36 PM	IndraControl	F0140001	Error in device configuration
Message	7/9/1970 8:25:38 PM	IndraControl	A0200021	P0 RDY, reached phase 0, PLC in re...
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F20068B4	IndraDrive C68B4
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2000750	IndraDrive C0750
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002200	IndraDrive C2200
Error	7/9/1970 8:25:38 PM	Axis 22 (Driv...	F2002009	F2009 PL Defaultwerte der Parameter...
Error	7/9/1970 8:25:36 PM	Axis 22 (Driv...	F2002009	F2009 PL Defaultwerte der Parameter...

Total: 97 entries

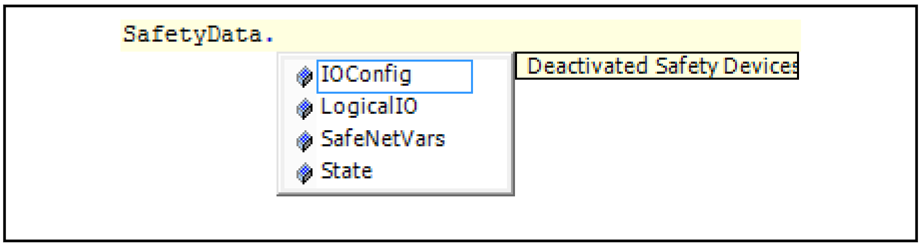
Fig. 8-5: Example of an MLC diagnostic logbook representation

The dialog can be opened online and offline. In offline mode, some functions are disabled.

8.6 Diagnostics in the standard PLC

The safe control system SafeLogic provides access to diagnostic information of the safe control and the safe I/O data in the PLC of the standard control. Data required for diagnostics can be easily read out and used in the PLC program.

The PLC data structure `SafetyData` is used as entry point. This global variable is automatically generated during the compilation of the standard control, if a SafeLogic is contained below the main control.



```
SafetyData.
    IOConfig
    LogicalIO
    SafeNetVars
    State
```

Fig. 8-6: Top level of the global variable SafetyData.

`SafetyData` contains the following entries:

- `SafetyFM` - Status information of the Safety control:

  This entry contains general diagnostic information of the SafeLogic control

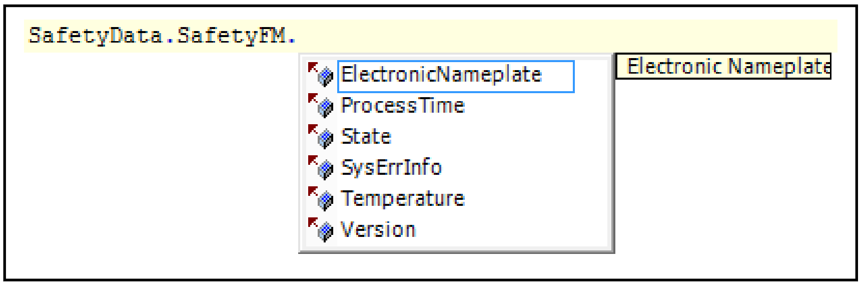

SafetyData.SafetyFM.

Fig. 8-7: Subitems of the SafetyData.SafetyFM entry

- `LogicalIO` - Access to safe connections:

  This entry facilitates access to safe connections. It hierarchically maps the devices below the "Logic I/O" node and the Safety control. Connection information is also available apart from the access to the transmitted variables.

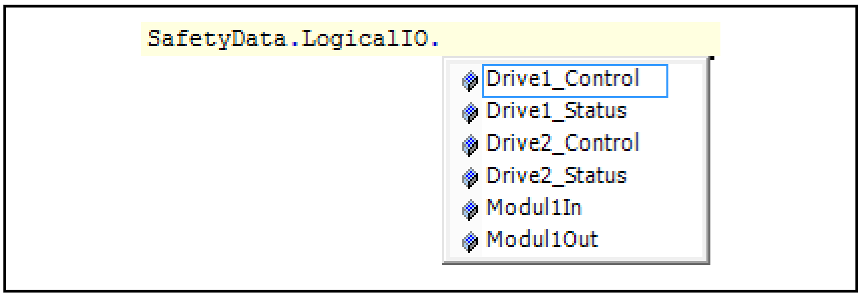

SafetyData.LogicalIO.

Fig. 8-8: Example of logic I/Os below the entry SafetyData.LogicalIO

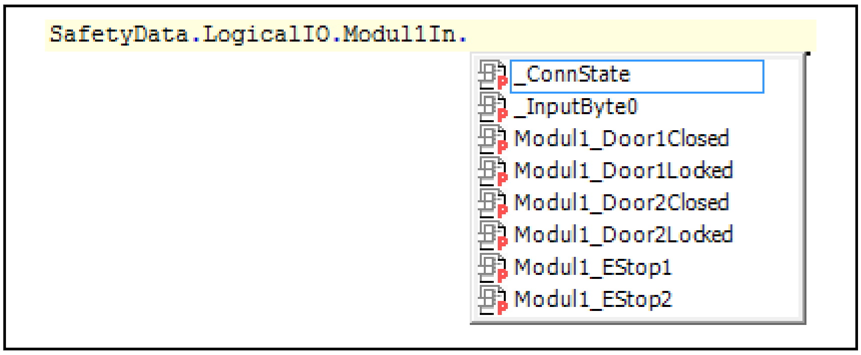

SafetyData.LogicalIO.Modul1In.

Fig. 8-9: Example of the logic I/O below the entry SafetyData.LogicalIO

- `SafeNetVars` - Access to safe network variables:

  This entry provides all safe network variable lists known to the control (see chapter 5.8 "Safe cross communication via Ethernet" on page 78). Each configured connection is individually visible in case of sender lists. The connection status is displayed in addition to the access to the transmitted safe variables.

- `IoConfig` - Disables safe devices:

  This entry maps the functionality to teach disabled safe devices. Apart from the check sum (CRC) of the current configuration, the access to deactivation bits is also possible.

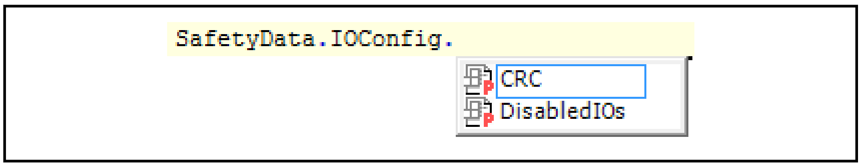

SafetyData.IOConfig.

Fig. 8-10: Subitems of the SafetyData.IOConfig entry

8.7 WebAssistant

General information

The "WebAssistant" is an integrated, web-based interface of the control and facilitates a remote access to the control access. This chapter describes the application options of the WebAssistant within the context of a Safety control.

For more information, refer to the "WebAssistant" documentation (see tab. 1-4 "IndraWorks/WebAssistant documentations" on page 5).

WebAssistant functions:

- Display of the system configuration
- Display of the status (diagnostics/logbook)
- Operating state control (Motion/PLC)
- Remote access, e.g. for remote maintenance for OEMs, end users and service providers

The WebAssistant does neither have to be installed nor set up.

All required files and tools are contained in the firmware of the control.

System support

The WebAssistant is supported by the controls of the following systems:

- MLC 15VRS
- ILC 15VRS

Security/access rights

The access to the WebAssistant or the web server of the control is password-protected.

The access rights of the logged in user determines which sites and contents are display and which control rights have to be assigned to the user.

The project or the hardware configuration also has an impact on the displayed contents.

WebAssistant/Calling the safety module

To start the "WebAssistant", refer to the **WebAssistant** documentation, chapter "Starting the WebAssistant"

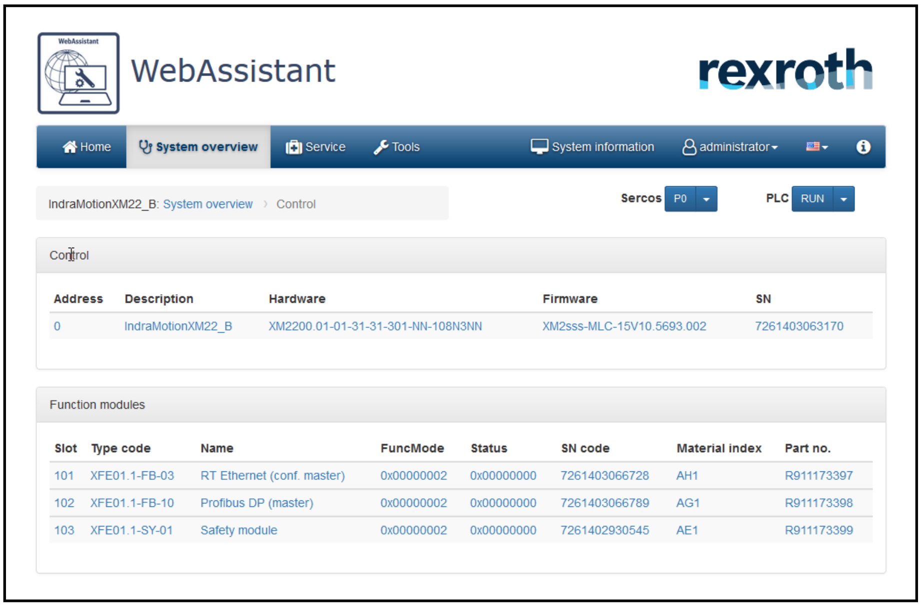
The control or the connected devices can be selected in the system overview and their data can be displayed.

When selecting the control in the system overview, the control data and the function module data is listed.

When selecting the safety module in the **function module** list, the function module data is displayed via the following tabs:

- Hardware
- Status
- Processing time
- System error

WebAssistant System overview



IndraMotionXM22_B: System overview › Control

Control

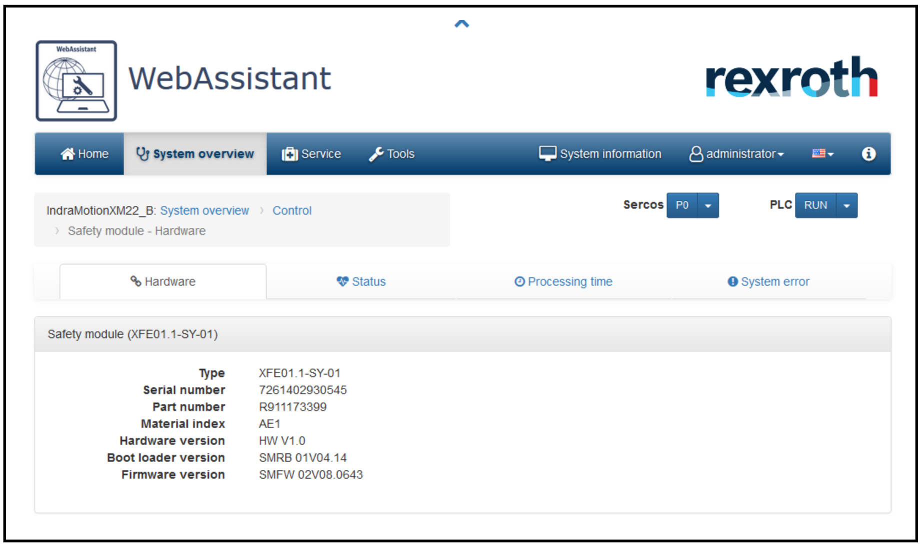
Address	Description	Hardware	Firmware	SN
0	IndraMotionXM22_B	XM2200.01-01-31-31-301-NN-108N3NN	XM2sss-MLC-15V10.5693.002	7261403063170

Function modules

Slot	Type code	Name	FuncMode	Status	SN code	Material index	Part no.
101	XFE01.1-FB-03	RT Ethernet (conf. master)	0x00000002	0x00000000	7261403066728	AH1	R911173397
102	XFE01.1-FB-10	Profibus DP (master)	0x00000002	0x00000000	7261403066789	AG1	R911173398
103	XFE01.1-SY-01	Safety module	0x00000002	0x00000000	7261402930545	AE1	R911173399

Fig. 8-11: WebAssistant system overview - System configuration display of control and function modules

WebAssistant system overview/ hardware



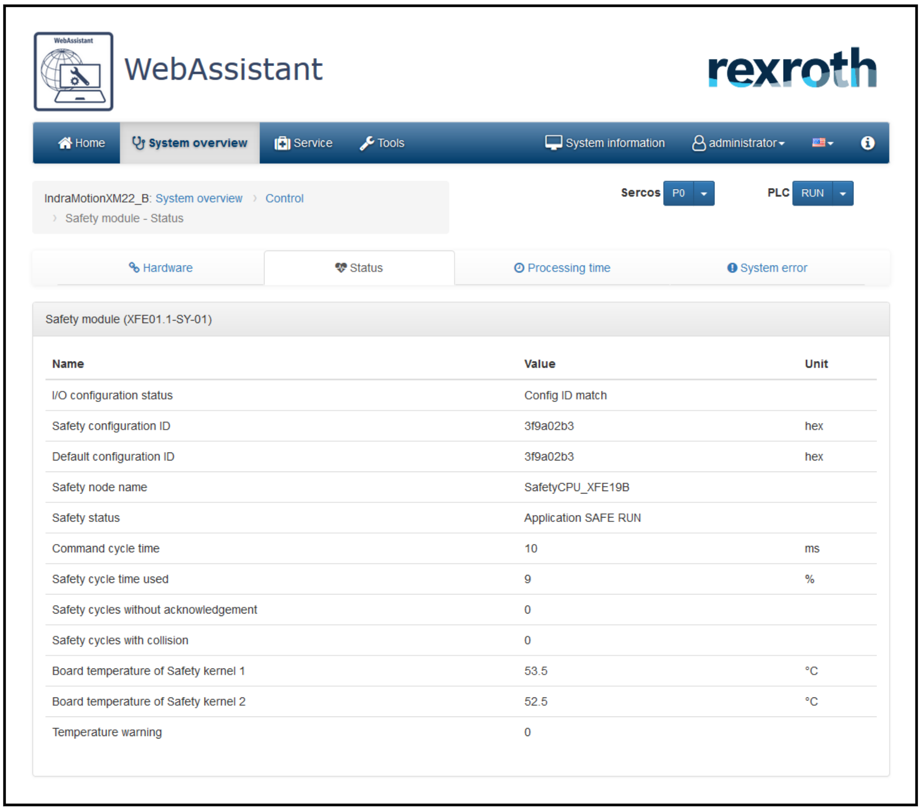
IndraMotionXM22_B: System overview › Control › Safety module - Hardware

Safety module (XFE01.1-SY-01)

Type	XFE01.1-SY-01
Serial number	7261402930545
Part number	R911173399
Material index	AE1
Hardware version	HW V1.0
Boot loader version	SMRB 01V04.14
Firmware version	SMFW 02V08.0643

Fig. 8-12: WebAssistant system overview – "Hardware" tab

WebAssistant system overview/ status

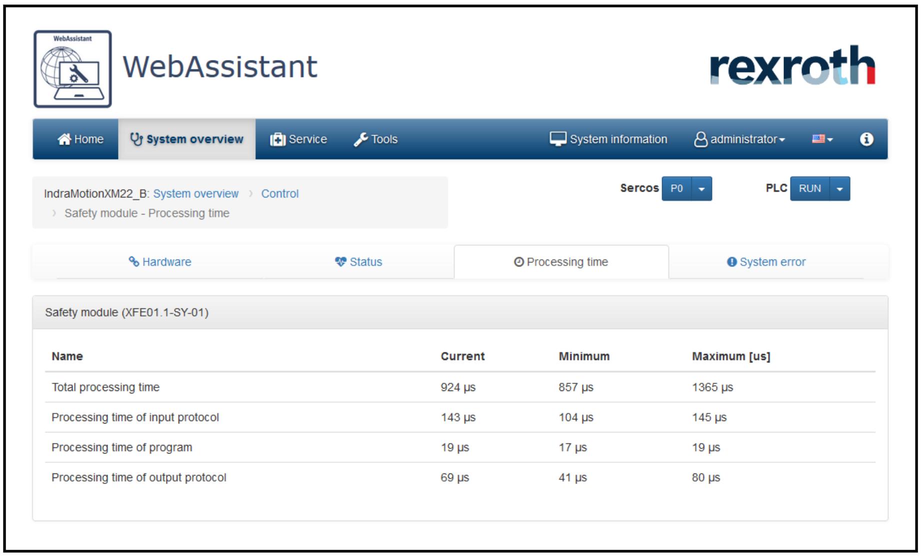


Safety module (XFE01.1-SY-01)

Name	Value	Unit
I/O configuration status	Config ID match	
Safety configuration ID	3f9a02b3	hex
Default configuration ID	3f9a02b3	hex
Safety node name	SafetyCPU_XFE19B	
Safety status	Application SAFE RUN	
Command cycle time	10	ms
Safety cycle time used	9	%
Safety cycles without acknowledgement	0	
Safety cycles with collision	0	
Board temperature of Safety kernel 1	53.5	°C
Board temperature of Safety kernel 2	52.5	°C
Temperature warning	0	

Fig. 8-13: WebAssistant system overview – "Status" tab

WebAssistant system overview/ processing time

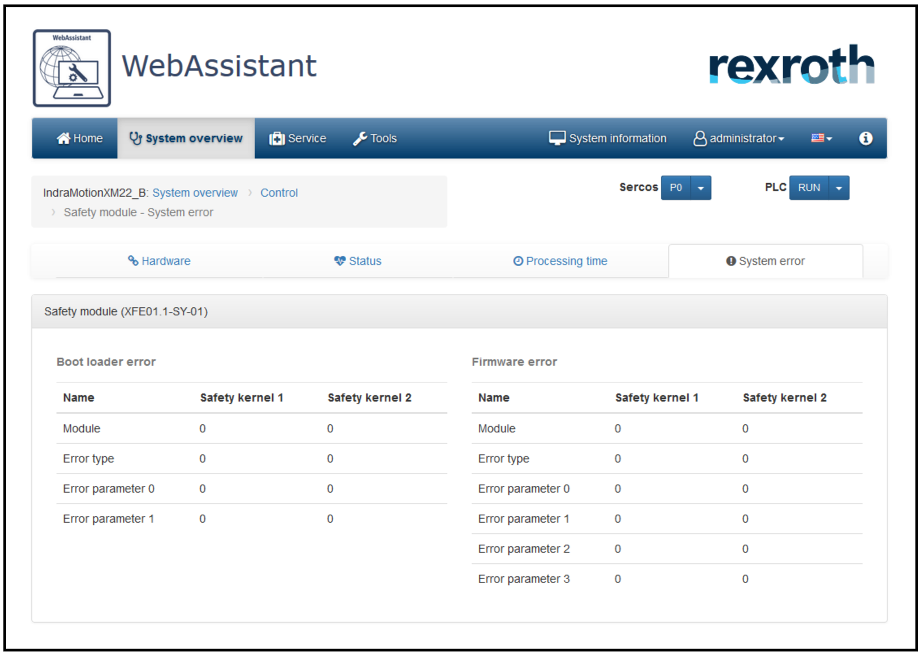


Safety module (XFE01.1-SY-01)

Name	Current	Minimum	Maximum [us]
Total processing time	924 µs	857 µs	1365 µs
Processing time of input protocol	143 µs	104 µs	145 µs
Processing time of program	19 µs	17 µs	19 µs
Processing time of output protocol	69 µs	41 µs	80 µs

Fig. 8-14: WebAssistant system overview – "Processing time" tab

WebAssistant system overview/ system error



WebAssistant rexroth

Home | System overview | Service | Tools | System information | administrator

IndraMotionXM22_B: System overview › Control › Safety module - System error

Sercos P0 PLC RUN

Hardware | Status | Processing time | System error

Safety module (XFE01.1-SY-01)

Boot loader error

Name	Safety kernel 1	Safety kernel 2
Module	0	0
Error type	0	0
Error parameter 0	0	0
Error parameter 1	0	0

Firmware error

Name	Safety kernel 1	Safety kernel 2
Module	0	0
Error type	0	0
Error parameter 0	0	0
Error parameter 1	0	0
Error parameter 2	0	0
Error parameter 3	0	0

Fig. 8-15: WebAssistant system overview – "System error" tab

8.8 Function blocks "CSosOriginator" and "ProfisafeHost"

All error messages in the configuration are output at the DiagCode or DiagCodeExt outputs of the "CSosOriginator" or "ProfisafeHost" function blocks.

Example call in the application:

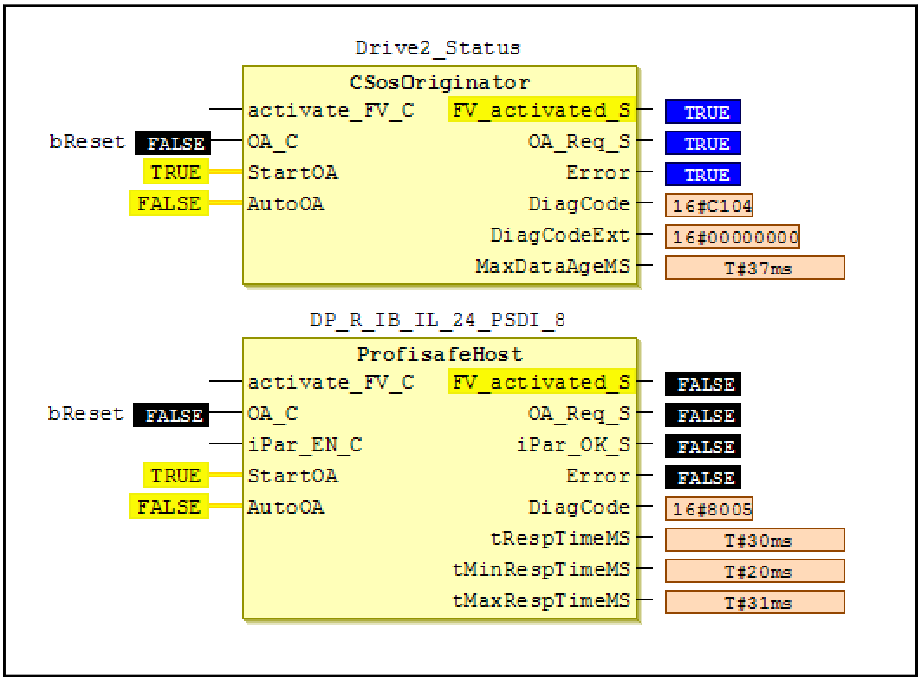


Fig. 8-16: Example call of the CsosOriginator and of the ProfisafeHost function block

DiagCode/DiagCodeExt

DiagCode	DiagCodeExt	Description
16#C104	0	Acknowledgment requested by operator
16#8005	-	"Prepare Message" (data exchange): Preparing the next message for the F-device

Tab. 8-1: DiagCode/DiagCodeExt

9 Service and support

Our worldwide service network provides an optimized and efficient support. Our experts offer you advice and assistance should you have any queries. You can contact us **24/7**.

Service Germany

Our technology-oriented Competence Center in Lohr, Germany, is responsible for all your service-related queries for electric drive and controls.

Contact the **Service Hotline** and **Service Helpdesk** under:

Phone:	**+49 9352 40 5060**
Fax:	**+49 9352 18 4941**
E-mail:	service.svc@boschrexroth.de
Internet:	http://www.boschrexroth.com

Additional information on service, repair (e.g. delivery addresses) and training can be found on our internet sites.

Service worldwide

Outside Germany, please contact your local service office first. For hotline numbers, refer to the sales office addresses on the internet.

Preparing information

To be able to help you more quickly and efficiently, please have the following information ready:

- Detailed description of malfunction and circumstances
- Type plate specifications of the affected products, in particular type codes and serial numbers
- Your contact data (phone and fax number as well as your e-mail address)

Index

Notes

rexroth
A Bosch Company

Bosch Rexroth AG
P.O. Box 13 57
97803 Lohr a.Main, Germany
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr a.Main, Germany
Phone +49 9352 18 0
Fax +49 9352 18 8400
www.boschrexroth.com/electrics

R911400164

DOK-MLC***-SL**SYS*V15-PR02-EN-P