



Installation and operation of the RFC 4072S Remote Field Controller with integrated safety-related PROFINET controller

User manual
UM EN RFC 4072S

User manual

Installation and operation of the RFC 4072S Remote Field Controller with integrated safety-related PROFINET controller

UM EN RFC 4072S, Revision c06

2024-09-03

This user manual is valid for:

Designation	Revision	Order No.
RFC 4072S	HW/FW:	≥ 00/2019.0 LTS
	HW/FW	1051328
	(iSPNS 3000):	≥ 02/01.08.0000



Before starting up the controller, observe the following:

- Make sure you always operate the controller with the latest firmware version.
The latest firmware version can be downloaded at phoenixcontact.net/product/1051328.
- Observe the change notes regarding the firmware version.
- If necessary, update the firmware.
For information on running firmware updates, refer to [Section 6.5](#).

Table of contents

1	For your safety	9
1.1	Identification of warning notes	9
1.2	Qualification of users	9
1.3	Information about this user manual.....	10
1.3.1	Purpose of this user manual	10
1.3.2	Validity of the user manual	10
1.4	Licensing information on Open source software.....	10
1.5	Requesting the source code.....	11
1.6	General safety notes.....	12
1.6.1	Foreseeable misuse	14
1.6.2	Product changes	14
1.6.3	Notes on Security	14
1.6.4	Security in the network	15
1.7	Electrical safety	16
1.8	Safety of the machine or system.....	17
1.9	Standards and directives	18
1.10	Intended use.....	19
1.11	Documentation	20
1.12	System requirements (hardware and software)	21
1.13	Abbreviations used.....	22
1.14	Safety hotline.....	22
1.15	Transport, storage, and unpacking	23
1.15.1	Transport	23
1.15.2	Storage	23
1.15.3	Unpacking	23
2	Description of the RFC 4072S	25
2.1	General description of the RFC	25
2.2	Description of the safety-related functioning of the RFC 4072S	27
2.2.1	Behavior of the iSPNS 3000 as the F-Host in PROFIsafe	28
2.2.2	Behavior of the iSPNS 3000 as the F-Device in PROFIsafe	31
2.3	Calculating/determining the response time (Safety Function Response Time, SFRT)	35
2.3.1	Determining $SFRT_{max}$ and $F_WD_Time\ IN_{max}/F_WD_Time\ OUT_{max}$..	36
2.3.2	Determining $F_WD_Time\ IN_{min}/F_WD_Time\ OUT_{min}$	39
2.3.3	Determining $F_WD_Time\ IN/F_WD_Time\ OUT$ to be parameterized and checking/validating that the safety function can be implemented ..	45
2.4	Indicators, interfaces, and operating elements	46
2.5	Security seal and test mark.....	47

2.6	Fan module	48
2.7	Status and diagnostics indicators (Ethernet)	49
2.8	Touch screen display.....	49
2.9	Structure of the display (diagnostic display)	51
2.9.1	Indicators on the display	52
2.9.2	Status information	52
2.9.3	Diagnostics indicators	56
2.9.4	Home menu	59
2.9.5	“CONFIG DETAILS” menu	60
2.9.6	“PLCnext DETAILS” menu (standard controller)	62
2.9.7	“PLCnext DETAILS” menu (safety-related PROFINET controller)	62
2.9.8	“OPC UA DETAILS” menu (OPC UA server)	64
2.9.9	“PN-C DETAILS” menu (PROFINET controller)	64
2.9.10	“PN-D DETAILS” menu (PROFINET device)	65
2.10	USB interface (currently not supported)	66
2.11	Interfaces.....	67
2.11.1	Ethernet connection	68
2.11.2	Connection example of the Ethernet interfaces	69
2.12	Mode selector switch.....	70
2.13	Power supply	71
2.13.1	Sizing of the power supply	71
2.14	Directory structure of the file system.....	73
2.15	Using SFTP to access the file system.....	76
2.16	Firewall	76
3	Mounting, removal, electrical installation, and replacement	77
3.1	Safety notes for mounting and removal	77
3.2	Mounting the RFC FAN MODULE fan module.....	79
3.3	Mounting the RFC 4072S	80
3.4	Removing the RFC 4072S.....	81
3.5	Inserting/removing the SD card (parameterization memory).....	81
3.6	Inserting/removing the USB memory stick.....	82
3.7	Connecting the interfaces.....	83
3.7.1	Connecting an Ethernet network	83
3.8	Connecting the supply voltage	84
3.9	Replacing the RFC 4072S.....	85
4	Startup and validation	91
4.1	Initial startup	91
4.2	Restart after replacing the RFC 4072S	94

4.3	Example startup of the RFC 4072S	96
4.3.1	Example of a PROFINET/PROFIsafe configuration with PROFINET controller/F-Host	96
4.3.2	Integration of the RFC 4072S in PLCnext Engineer as a PROFINET controller	97
4.4	Software requirements	98
4.4.1	PLCnext Engineer software	98
4.4.2	Installing PLCnext Engineer	98
4.4.3	PLCnext Engineer licenses	98
4.4.4	User interface	99
4.4.5	Creating a new project	100
4.5	Configuring the controller IP settings	101
4.5.1	General information	101
4.5.2	Important information	101
4.5.3	Setting the IP address range	102
4.5.4	Setting the IP address	103
4.6	Defining a project password	104
4.7	Connecting to the controller.....	105
4.8	Configuring PROFINET devices	108
4.8.1	Adding PROFINET devices	108
4.8.2	Assigning online devices (device naming)	109
4.8.3	Adding I/O modules	110
4.9	Programming in accordance with IEC 61131-3 – Non-safety-related example program	114
4.9.1	Opening and creating the POU	114
4.9.2	Creating variables	116
4.9.3	Creating a program	117
4.10	Instantiating a program	118
4.11	Assigning process data	119
4.11.1	For programs in accordance with IEC 61131-3 without IN and OUT ports	119
4.11.2	For programs in accordance with IEC 61131-3 with IN and OUT ports	122
4.12	Transferring a project to the controller	124
4.13	Displaying online values	125
4.14	Creating a PLCnext Engineer HMI application.....	126
4.15	Programming in accordance with IEC 61131-3 – Safety-related example program	127
4.15.1	Assigning/checking the PROFIsafe address (F-Address) of PROFIsafe devices	127
4.15.2	Management/diagnostic variables for F-Devices	129
4.15.3	Checking/setting safety parameters for configured F-Devices	131
4.15.4	Creating variables (exchange variables)	133
4.15.5	Opening a safety-related POU	135

4.15.6	Creating variables	136
4.15.7	Creating a safety-related program	137
4.15.8	Assigning process data	139
4.16	Transferring a project to the controller	140
4.16.1	Transferring a non-safety-related project to the standard controller ...	140
4.16.2	Transferring a safety-related project to the safety-related controller (defining a controller password, if necessary)	142
4.17	Displaying online values	145
4.18	PLCnext Engineer – Debug mode	147
4.19	Operator acknowledge	148
5	Errors, diagnostic messages and troubleshooting	151
5.1	Diagnostics for PROFINET	151
5.2	Diagnostics for F-Devices.....	151
5.3	Diagnostics for iSPNS 3000	151
5.4	Possible errors.....	152
5.4.1	Errors with error codes	154
5.5	Evaluation and acknowledgment of module-specific diagnostic messages.....	160
5.5.1	AsynCom_PN_Info_V1_01 function block	160
5.5.2	PNFD_IL_Diag_V1_01 function block	161
6	Maintenance, replacement, firmware update, repair, decommissioning, and disposal	163
6.1	Maintenance.....	163
6.2	Caring for the display.....	163
6.3	Replacing the RFC 4072S.....	163
6.4	Replacing the RFC FAN MODULE fan module	164
6.5	Updating the device firmware	165
6.5.1	Updating the firmware	168
6.6	Repair.....	169
6.7	Decommissioning and disposal.....	170
7	Additional settings as well as features and what you need to know about the RFC 4072S	171
7.1	Resetting the controller to the default settings.....	171
7.2	Changing IP address settings via the display	172
7.3	Parameterization memory: directory structure and access	175
7.4	Setting the realtime clock under PLCnext Engineer.....	176
7.5	Download changes.....	177
7.6	Startup parameterization of PROFINET devices	177
7.7	Substitute value behavior for PROFINET devices and PROFIsafe F-Devices ...	179
7.8	Function blocks for handling files on the parameterization memory.....	180

7.9	Function blocks for Ethernet communication	181
7.10	Function block for managing PROFINET application relationships (AR)	182
7.11	Web server	182
7.12	OPC UA	182
8	System variables	183
8.1	General notes	183
8.2	System variables grouped into structures	183
8.3	PROFIsafe/PROFINET system variables	184
8.3.1	System variables of the iSPNS 3000	184
8.3.2	FDEV_INx and FDEV_OUTx (x = 0 ... 7) system variables	190
8.3.3	Management/diagnostic variables for each configured F-Device	191
8.3.4	Global management/diagnostic variables for F-Devices	195
8.3.5	Management/diagnostic variables of the iSPNS 3000 F-Device	197
8.3.6	PROFINET system variables	203
8.4	System time	205
8.5	PLC_CRC_PRJ	205
8.6	TCP_SOCKET, UDP_SOCKET, and TLS_SOCKET function blocks	205
8.7	DEVICE_STATE	206
8.8	Task handling	206
8.9	HMI_STATUS	208
8.10	HMI_CONTROL	208
9	Web-based management WBM	209
9.1	Requirements for the use of WBM	209
9.2	Establishing a connection to WBM	209
9.3	Licenses and legal information	212
9.4	Changing the language	213
9.5	Login	214
9.6	WBM start page – Areas and functions	215
9.6.1	“Information” area	216
9.6.2	“Administration” area	217
9.6.3	“Diagnostics” area	218
9.6.4	“Security” area	220
9.7	Firmware update via WBM	229
10	Technical data and ordering data	237
10.1	Technical data	237
10.2	Ordering data	244
10.2.1	Controller	244

	10.2.2	Modules	244
	10.2.3	Accessories	245
	10.2.4	Software	246
	10.2.5	Documentation	246
A	Appendix:		249
	A 1	Shell commands for controlling the firmware	249
	A 2	Replacing HTTPS certificate	249
	A 3	Interfaces of the RFC 4072S	250
	A 4	USB interface	251
	A 5	Ethernet interfaces	252
	A 6	Connection for the supply voltage	254
B	Appendix: terms for PROFIsafe		255
C	Appendix: checklists		257
	C 1	System-specific checklists	258
	C 2	Device-specific checklists	264
D	Appendix for document lists		269
	D 1	List of figures	269
	D 2	List of tables	277
	D 3	Index	281
E	Appendix: revision history		285

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes



This symbol indicates hazards that could lead to personal injury.

There are three signal words indicating the severity of a potential injury.

DANGER

Indicates a hazard with a high risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

WARNING

Indicates a hazard with a medium risk level. If this hazardous situation is not avoided, it could result in death or serious injury.

CAUTION

Indicates a hazard with a low risk level. If this hazardous situation is not avoided, it could result in minor or moderate injury.



This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.



Here you will find additional information or detailed sources of information.

1.2 Qualification of users

The use of products described in this user manual is oriented exclusively to:

- Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.
- Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

This user manual is addressed to persons, who are familiar with the relevant safety concepts for handling electrical machines. The persons must be able to recognize dangers.

1.3 Information about this user manual

1.3.1 Purpose of this user manual

The information in this document is designed to familiarize you with how the “RFC 4072S Remote Field Controller with integrated safety-related PROFINET controller for PROFIsafe iSPNS 3000” works, its controls and connection elements, and its integration into the software tools listed in [Section “System requirements \(hardware and software\)” on page 21](#). This information will enable you to use the device in a PROFINET/PROFIsafe system in accordance with your requirements.

1.3.2 Validity of the user manual

This user manual is only valid for the “RFC 4072S Remote Field Controller with integrated safety-related PROFINET controller for PROFIsafe iSPNS 3000” (referred to as “RFC” in this document) in the versions indicated on the inner cover page.

1.4 Licensing information on Open source software

The RFC 4072S works with a Linux operating system. License information on the individual Linux packages can be found in the file system of the RFC 4072S under:

`/usr/share/common-licenses`



Information on the directory structure of the file system can be found in [Section 2.14 on page 73](#).

Alternatively, you can also call up the license information via the Web-based management system of the RFC 4072S (see [Section “Licenses and legal information” on page 212](#)).

Notes on LGPL software libraries

All Open source software used in the product is subject to the respective license terms that are not affected by the Phoenix Contact Software License Terms (SLT) for the product. In particular, the license holder can change the respective Open source software in accordance with the applicable license terms. If the license holder wishes to change an LGPL software library contained in this product, reverse engineering is permitted for debugging such modifications.

Notes on OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

1.5 Requesting the source code

This RFC 4072S contains software components that are licensed by the rights holder as free software or Open source software under the GNU General Public License.

You can request the source code of these software components in the form of a CD or DVD-ROM for a processing fee of € 50 within three years after delivery of the RFC 4072S.

To do so, contact the Phoenix Contact After Sales Service in writing at the following address:

PHOENIX CONTACT GmbH & Co. KG
After Sales Service
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Subject: Source code for RFC 4072S

1.6 General safety notes



WARNING: Depending on the application, incorrect handling of the RFC 4072S can pose serious risks for the user

When working with the RFC 4072S within the PROFIsafe system, please observe all the safety notes included in this section.

Requirements

Knowledge of the following is required:

- The non-safety-related target system (PROFINET)
- The PROFIsafe system
- The components used in your application (e.g., of the Inline product range)
- Operation of the software tools specified under the software requirements (see [Section “System requirements \(hardware and software\)” on page 21](#))
- Safety regulations in the field of application

Qualified personnel

In the context of the use of the PROFIsafe system, the following operations may only be carried out by qualified personnel:

- Planning
- Configuration, parameterization, programming
- Installation, startup, servicing
- Maintenance, decommissioning

This user manual is therefore aimed at:

- Qualified personnel who plan and design safety equipment for machines and systems and are familiar with regulations governing occupational safety and accident prevention.
- Qualified personnel who install and operate safety equipment in machines and systems.

In terms of the safety notes in this user manual, qualified personnel are persons who, because of their education, experience and instruction, and their knowledge of relevant standards, regulations, accident prevention, and service conditions, have been authorized to carry out any required operations, and who are able to recognize and avoid any possible dangers.

Documentation

You must observe all information and especially all safety notes in this user manual as well as in the documents listed in [Section “Documentation” on page 20](#).

Safety of personnel and equipment

The safety of personnel and equipment can only be assured if the RFC 4072S is used correctly (see [Section “Intended use” on page 19](#)).

Error detection

Depending on the wiring and the parameterization of the safe input/output devices, the PROFIsafe system can detect various errors within the safety equipment.

Observe startup behavior

The PROFIsafe system and the RFC 4072S as the central component automatically initiate startup/restart of the safety function, e.g., after power-on.

- To prevent automatic startup/restart, the user must program a startup/restart protection function in the safety program using the programming software for PROFIsafe PLCnext Engineer.

After the supply voltage is switched on or after a software reset, the RFC 4072S starts up immediately if a parameterization memory with a valid project is plugged in and the operating mode switch is set to RUN (see [Section 2.12](#)).

By selecting one of the options (“Write and Start Project...” or “Write and Start Project Changes...”), the safety function becomes active immediately after downloading the PLCnext Engineer project and following the RFC startup phase. The outputs of the F-Devices and the non-safety-related PROFINET devices can be set in accordance with the programming.

Safety notes for starting applications

Take the following into consideration when determining and programming the start conditions for your machine or system:

- The machine or system may only be started if it can be ensured that nobody is present in the danger zone.
- Meet the requirements of EN ISO 13849-1 with regard to the manual reset function. The machine must not be set in motion and/or a hazardous situation must not be triggered by the following actions, for example:
 - Switching on safe devices
 - Acknowledging device error messages
 - Acknowledging communication errors
 - Acknowledging block error messages in the application
 - Removing startup inhibits for safety functions

Observe the following when programming/configuring the safety logic:

- Switching from the safe state (substitute value = 0) to the operating state can generate an edge change (zero/one edge).
- In the safety logic, take measures to prevent this edge change resulting in unexpected machine/system startup or restart.

**Note for starting applications**

Also observe these notes to prevent unexpected machine startup following acknowledgment by means of operator acknowledgment.

Measures to prevent mismatching and polarity reversal

Take measures to prevent mismatching, polarity reversal, and manipulation of connections.

Observe the country-specific installation, safety, and accident prevention regulations.

1.6.1 Foreseeable misuse



WARNING: Serious risks due to improper use

There is a serious risk to the user and/or equipment if the RFC 4072S is used inappropriately or not in accordance with the intended use or has been tampered with.

1.6.2 Product changes

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. If the device is defective, please contact Phoenix Contact.

Repairs may not be carried out on the RFC 4072S.

Do not carry out any repairs

**Do not open the housing/
security seal**

It is strictly prohibited to open the RFC 4072S housing. In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, a security seal is applied to the device (see [Figure 2-14 on page 47](#)). This security seal is damaged in the event of unauthorized opening. In this case, the correct operation of the device can no longer be ensured.

1.6.3 Notes on Security



NOTE: Unauthorized access to the SD card possible and unauthorized deletion/replacement of the safety-related project possible

- Only provide the roles for user authentication – “Admin”, “Commissioner”, and “Engineer” – to those users who are authorized to program the safety-related controller. Otherwise, the unauthorized replacement or deletion of the safety-related project by the user cannot be ruled out.

You can set the user roles in the Web-based management system of the RFC 4072S. A general description of the Web-based management system can be found in the [PLCnext Info Center](#).

- It is imperative that you install the RFC 4072S in a lockable housing or a lockable control cabinet.

The device housing is not protected against tampering, and access to the device cannot be proven.

- It is possible to access the SD card, meaning that data can be read off and tampered with.

We recommend securing the cover of the slot for the configuration memory (SD card) against tampering using a seal.



NOTE:

For notes on the use of the RFC 4072S in combination with the security profile, please refer to the [PLCnext Security Info Center](#).

1.6.4 Security in the network

**NOTE: Network security jeopardized by unauthorized access**

Connecting devices to a network via Ethernet always entails the risk of unauthorized access to the network.

Observe the following safety notes:

- If possible, deactivate unused communication channels.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Only allow authorized persons to access the device. Limit the number of authorized persons to the necessary minimum.
- Always install the latest firmware version. The firmware can be downloaded via the item (phoenixcontact.net/products).
- Observe the IT security requirements and the standards applicable to your application. Take the necessary protective measures. These may include, for example, virtual networks for remote maintenance access or a firewall.
- In security-critical applications, always use the device with an additional security appliance.

Phoenix Contact offers security appliances in the mGuard product range. The mGuard routers connect various networks for the remote maintenance and protection of the local network and protect these networks against cyberattacks.

- You must take defense-in-depth strategies into consideration when planning networks.



Additional measures for protection against unauthorized network access can be found in the AH EN INDUSTRIAL SECURITY application note. The application note can be downloaded at phoenixcontact.net/product/1051328.

German: AH DE INDUSTRIAL SECURITY, 107913

English: AH EN INDUSTRIAL SECURITY, 107913

If a security vulnerability exists for products, solutions, or services from Phoenix Contact, it will be published on the PSIRT (Product Security Incident Response Team) website: phoenixcontact.com/psirt.

1.7 Electrical safety



WARNING: Hazardous shock currents and the loss of functional safety

Disregarding instructions for electrical safety may result in hazardous shock currents and the loss of functional safety.

In order to ensure electrical safety, please observe the following points.

Direct/indirect contact

Protection against direct and indirect contact according to VDE 0100 Part 410 (IEC 60364-4-41) must be ensured for all components connected to the system. In the event of an error, parasitic voltages must not occur (single-fault tolerance). This also applies to devices and components with dangerous contact voltages that are permanently connected to the network and/or diagnostic interfaces of the devices used.

This requirement can be met by:

- Using power supplies with safe isolation (PELV)
- Decoupling circuits that are not PELV systems using optocouplers, relays, and other components that meet the requirements of safe isolation.

Safe isolation

Only use devices with safe isolation if dangerous contact voltages can occur at their connections during normal operation or as a result of an insulation error.

Power supply



WARNING: Loss of electrical safety and the safety function when using unsuitable power supplies

The RFC 4072S is designed exclusively for protective extra-low voltage (PELV) operation in accordance with EN 60204-1. Only PELV in accordance with the listed standard may be used for the supply.

The following applies to the PROFINET network and the I/O devices used in it:

Only use power supplies that meet EN 61204 and feature safe isolation and PELV according to IEC 61010-2-201 (PELV). These prevent short circuits between primary and secondary sides.

Insulation rating

When selecting the equipment, please take into consideration the dirt and surge voltages that may occur during operation.

The RFC 4072S is designed for overvoltage category III (according to DIN EN 60664-1). If you expect surge voltages in the system, which exceed the values defined in overvoltage category III, take into consideration additional measures for voltage limitation.

DC distribution network

DC distribution network according to IEC 61326-3-1:

A DC distribution network is a DC power supply network that supplies a complete industrial hall with DC voltage and to which any device can be connected. A typical system or machine distribution is not a DC distribution network. For devices that are provided for a typical system or machine distribution, the DC connections are viewed and tested as I/O signals according to IEC 61326-3-1.

When using an RFC 4072S in a DC distribution network, install appropriate surge protection (e.g., PT 2+1-S-48DC/FM, Order No. 2817958) directly before the device.

Installation and configuration

Please observe the instructions for installing and configuring the PROFIsafe system (see [Section “Documentation” on page 20](#)).

**WARNING: Incorrect installation and upgrades can pose serious risks**

The user is obliged to design the devices used and their installation in the system according to these requirements. This also means that existing plants and systems retrofitted with PROFIsafe must be checked and tested again in this respect.

1.8 Safety of the machine or system

The manufacturers and operators of machines and systems, in which the RFC 4072S is used, are responsible for adhering to all applicable standards, directives, and legislation.

Draw up and implement a safety concept

In order to use the device described in this document, you must have drawn up an appropriate safety concept for your machine or system. This includes a hazard and risk assessment in accordance with the directives and standards specified in [Section “Standards and directives” on page 18](#), as well as a test report (checklist) for validating the safety function (see [Section “Appendix: checklists” on page 257](#)).

The target safety integrity level (SIL in accordance with IEC 61508, SIL CL in accordance with EN 62061 or performance level (and category) in accordance with EN ISO 13849-1) is ascertained on the basis of the risk assessment. The required safety integrity level ascertained in this way determines how to use and parameterize the Remote Field Controller with safety-related controller within the overall safety function.

Check hardware and parameterization

Carry out a **validation** every time you make a safety-related modification to your overall system.

Use your test report to ensure that:

- The safe PROFIsafe devices (F-Devices) are connected to the correct safe sensors and actuators.
- The safe input and output devices have been parameterized correctly.
- The variables have been linked to the safe sensors and actuators correctly (single-channel or two-channel).

1.9 Standards and directives

- Machinery Directive 2006/42/EC
- EMC Directive 2014/30/EU
- Directive 2011/65/EU, Restriction of the use of certain hazardous substances
- PROFINET Installation Guideline for Cabling and Assembly
- PROFIsafe Policy, Guideline for PROFIBUS and PROFINET
- PROFIsafe System Description, Technology and Application
- PROFIsafe Environment, Guideline for PROFINET and PROFIBUS
- PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET
- PROFIsafe Test Specification, Test Specification for PROFIBUS and PROFINET
- Functional Bonding and Shielding of PROFIBUS and PROFINET, Guideline for PROFIBUS and PROFINET

For Information on current versions of the PROFINET and PROFIsafe documents, please refer to [Section “Documentation” on page 246](#).

The standards to which the device conforms are listed in the certificate issued by the approval body or in the EC declaration of conformity (see phoenixcontact.net/products).

1.10 Intended use



WARNING: Observe the intended use

Only use the RFC 4072S according to the instructions in this section.

This information will enable you to use the device according to your requirements in a:

- PROFINET system as a PROFINET controller
- Higher-level PROFINET system as a PROFINET device
- PROFIsafe system as an F-Host

The RFC 4072S can be used as a PROFINET controller and/or simultaneously as a PROFINET device in a PROFINET system. As a PROFINET controller, the device performs the function of a controller for the lower-level PROFINET system. For each PROFINET device function, the RFC 4072S can be operated on a lower level of the PROFINET controller. Concurrent operation of the RFC 4072S as PROFINET controller and device is only possible in two different subnetworks.

In a PROFIsafe system, the device performs the task of an F-Host using the integrated safety-related controller (safety-related PROFINET controller (iSPNS 3000)).

The safety function of the RFC 4072S is only available for use in a PROFIsafe system.

The RFC 4072S can only perform its safety-related tasks in a PROFIsafe system if the device has been integrated into the execution process correctly and in such a way as to avoid errors.

You must observe all the information in this user manual as well as in the documents listed in [“Documentation” on page 20](#). In particular, only use the device according to the technical data and ambient conditions specified in [Section 10, “Technical data and ordering data”](#) from [page 237](#) and onwards.

Within a PROFIsafe system, the RFC 4072S can be used to achieve safety functions with the following requirements depending on the conditions of use:

- Up to SIL 3 according to standard IEC 61508
- Up to SIL CL 3 according to standard EN 62061
- Up to PL e/Cat. 4 according to standard EN ISO 13849-1

Use the PLCnext Engineer software to implement safety-related programming in your application.

Degree of protection

Degree of protection of the device: IP20



NOTE:

The IP20 degree of protection (IEC 60529/EN 60529) of the device is intended for use in a clean and dry environment. Do not subject the device to mechanical or thermal stress that exceeds the specified limits.

To ensure correct operation, the RFC 4072S must be installed in housing or a control cabinet with a minimum of IP54 protection.

Assembly guidelines

During installation of the device, observe the instructions in [Section 3, “Mounting, removal, electrical installation, and replacement”](#).

1.11 Documentation



The symbol informs you that you have to observe the instructions. Only install and operate the device once you have familiarized yourself with its properties by means of the user documentation.



Use the latest documentation

Make sure you always use the latest documentation. Changes or additions to this document can be found on the Internet at phoenixcontact.net/products.

When working on the PROFIsafe system and/or PROFINET its components, you must always keep this user manual and other items of product documentation to hand and observe the information therein.

	Document	Description
PROFIsafe	<ul style="list-style-type: none"> – PROFIsafe System Description – PROFIBUS Guideline, PROFIsafe Policy – PROFIsafe – Environmental Requirements Guideline 	For more detailed information on these documents, please refer to Section “Documentation” on page 246 : Please also observe the relevant information on PROFINET and PROFIsafe, which is available on the Internet at www.profibus.com .
	<ul style="list-style-type: none"> – User manuals for the PROFIsafe I/O modules used in your application 	
PROFINET	<ul style="list-style-type: none"> – PROFINET Guideline for Cabling and Assembly – “Functional Earthing and Shielding of PROFIBUS and PROFINET”, guideline for PROFIBUS and PROFINET 	For more detailed information on these documents, please refer to Section “Documentation” on page 246 :
	<ul style="list-style-type: none"> – UM EN PROFINET SYS 	PROFINET basic principles
	<ul style="list-style-type: none"> – UM EN PROFINET CTRL DEV 	PROFINET controller/device functions
Software	<ul style="list-style-type: none"> – Online help for the PLCnext Engineer software 	
PLCnext Technology	<ul style="list-style-type: none"> – PLCnext Info Center 	Comprehensive documentation for PLCnext Technology
	<ul style="list-style-type: none"> – plcnext-community.net 	Information on troubleshooting and answers to frequently asked questions (FAQs) in the PLCnext Community
Security	<ul style="list-style-type: none"> – PLCnext Security Info Center 	Comprehensive documentation for security in the context of PLCnext Technology

1.12 System requirements (hardware and software)

An active connection to a lower-level PROFINET system is required for starting up the RFC 4072S according to the examples in this user manual.

In order to follow the examples illustrated in this user manual, corresponding PROFINET devices and Axioline F I/O modules are required.

The following table provides an overview of the required hardware and software. The parameterization memory listed in the table is not included with the RFC 4072S, but it is an essential requirement for operating the RFC. Install the PLCnext Engineer software listed in the table on your PC. For trouble-free operation, follow the instructions in the software documentation.



The PLCnext Engineer engineering software platform for Phoenix Contact automation controllers is compliant with IEC 61131-3. Its functionality can be expanded with add-ins. PLCnext Engineer can be used as an editor for programming safety-related user applications. In this way, F-Devices operated with safety-related controllers with PLCnext Technology can be configured and started up. PLCnext Engineer is certified by TÜV-Rheinland.

Hardware/software	Description	Ordering data
Remote Field Controller	RFC 4072S	For ordering data, see Section "Accessories" on page 245 .
SD card	Parameterization memory	
Ethernet cable	For connecting the RFC to a PC and PROFINET	
Power supply	For supplying power to the RFC 4072S	
Fan module	Optional	
USB memory stick	Optional	
PLCnext Engineer (including add-in for functional safety applications (Add-in Functional Safety Editor)	≥ 2019.0 LTS For the F-Device function: 2023.0.3 LTS or ≥2023.6 and the iSPNS 3000 with FW version ≥02.10.0000 as well as the PLCnext firmware in a version ≥2023.0 LTS.	

1.13 Abbreviations used

Abbreviation	Meaning	Standard	Example
SIL	Safety integrity level	EN 61508, IEC 61508	SIL 2, SIL 3
SIL CL	SIL claim limit	EN 62061	SIL CL 3
Cat.	Category	EN ISO 13849	Cat. 2, Cat. 4
PL	Performance level	EN ISO 13849	PL e, PL d

Abbreviation	Meaning
iSPNS 3000	Safety-related PROFINET controller with performance class 3000 In this document, the iSPNS 3000 is also referred to as a safety-related controller.
FO	Fiber optics
PELV	Protective extra-low voltage Circuit in which the voltage cannot exceed 30 V AC, 42.4 V peak value or 60 V DC under normal conditions, and under single-error conditions, except in the event of grounding errors in other circuits. A PELV circuit is like an SELV circuit, but is connected to protective earth ground. (According to EN 61131-2)
F_Source_Add	F-Source Address (F-Parameter) PROFIsafe source address; address of iSPNS 3000 safety-related PROFINET controller (F-Host)
F_Dest_Add	F-Destination Address (F-Parameter) PROFIsafe destination address; address of the safety-related device (F-Device)



For terms and abbreviations used for PROFIsafe, please refer to [“Appendix: terms for PROFIsafe” on page 255](#).

1.14 Safety hotline

Should you have any technical questions, contact our Safety hotline.

- Phone: +49 5281 946 2777
- E-mail: safety-service@phoenixcontact.com

1.15 Transport, storage, and unpacking

1.15.1 Transport

The device is delivered in cardboard packaging.

- Only transport the device to its destination in its original packaging.
- Observe the instructions on how to handle the package, as well as the moisture, shock, tilt, and temperature indicators on the packaging.
- Observe the humidity specifications and the temperature range specified for transport (see [Section “Technical data” on page 237](#)).
- Protect the surfaces as necessary to prevent damage.
- When transporting the equipment or storing it temporarily, make sure that the surfaces are protected from the elements and any external influences, and that they are kept clean and dry.

1.15.2 Storage

The storage location must meet the following requirements:

- Dry
- Protected from unauthorized access
- Protected from harmful environmental influences such as UV light
- Temperature range: -25 °C ... +70 °C
- Air pressure: 58 kPa ... 108 kPa (up to 4500 m above sea level)
- Permissible air humidity: 5 % ... 95 % (in accordance with DIN EN 61131-2)

1.15.3 Unpacking

The device is delivered in packaging together with a packing slip that provides installation instructions.

- Read the complete packing slip carefully before unpacking the device.



NOTE: Electrostatic discharge!

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according with EN 61340-5-1 and IEC 61340-5-1.



NOTE: Property damage due to noncompliance with ESD notes

If the ESD notes are not observed during unpacking and packaging, the device may become damaged.

- Observe the ESD notes during unpacking and packaging.

Checking the delivery

- Check the delivery for transport damage.
Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Check to ensure that the security seals are undamaged (see [Section 2.5](#)).
Any damage to the security seals is an indication of the device being opened without authorization, e. g., for unacceptable tampering purposes. In this case, correct operation of the device can no longer be ensured.
- Submit any claims for any transport damage and/or damaged security seals immediately and inform Phoenix Contact or your supplier as well as the shipping company without delay.
- Enclose photos that clearly document the damage to the packaging and/or delivery together with your claim.
- Immediately upon delivery, refer to the delivery note to ensure that the delivery is complete.

Scope of supply

- Safety-related RFC 4072S controller
- AXL CN S/UL supply connector (item no.: 2701421)

2 Description of the RFC 4072S

2.1 General description of the RFC

The RFC is a compact controller with integrated Ethernet interfaces. When using the Ethernet interfaces, the PROFINET/PROFIsafe protocol can be used. The I/O level is connected to the RFC via PROFINET. Ethernet interfaces are also available for networking with higher-level systems, such as the control level or servicing level.

The RFC is the solution for tasks in the area of distributed, modular automation. It supports you in solving your particular problem, thanks to its programmability in accordance with the IEC 61131 standard, high-level languages such as C++ and safety-related programming in accordance with the IEC 61131 standard.

The RFC features a safety-related controller part that supports the PROFIsafe protocol. This function enables you to implement functional safety applications.

As a compact DIN-rail-mountable controller, the RFC provides networked, PC-based control performance locally.

Programming

You configure and program the RFC using the PLCnext Engineer automation software. PLCnext Engineer is connected to the RFC via the local Ethernet network. The powerful processor ensures quick processing of control tasks. For this purpose, the IEC 61131-3 programming languages FBD/LD, ST and SFC as well as suitable editors are available in PLCnext Engineer. In addition or as an alternative, you can also use the C++ or MATLAB® Simulink® programming languages. The individual programs or program parts can be programmed in any development environment (e.g., Eclipse, Microsoft® Visual Studio®, etc.). These programs or program parts must then be imported into PLCnext Engineer as a library.

Ethernet

The RFC features four Ethernet interfaces for TCP/IP / UDP/IP communication within the Ethernet network. Two of these interfaces are switched internally.

PROFINET / controller/ device functions

The RFC can be integrated in a PROFINET system using Ethernet interfaces. Depending on the configuration, the RFC functions as a PROFINET controller and/or a PROFINET device.



For additional information on how to integrate the RFC 4072S as a PROFINET controller or device, please refer to the PLCnext Engineer online help.

Web-based management

By means of the Web-based management interface integrated in the RFC, you have the option to display static and dynamic information of the controller using a standard web browser. Status and diagnostic functions can be displayed in a graphical user interface after the device IP address was entered in a web browser.

OPC UA server

An embedded OPC UA server runs on the RFC. It provides data of the RFC according to the OPC UA protocol (currently supported: Data Access). This data can be used for visualization purposes, for example.

PLCnext Engineer provides different system variables for the OPC UA server.

In order for process data variables to be processed with an OPC UA server, e.g., for visualization purposes, the “OPC” check box must be enabled for the corresponding variables on the variables worksheet in PLCnext Engineer.

USB interface

The RFC 4072S is equipped with a type A USB 3.0 interface (see [Section “USB interface \(currently not supported\)” on page 66](#)).

You can use function blocks to access the inserted USB flash drive from your application program.



We recommend using the following USB stick: USB FLASH DRIVE (Order No. 2402809), USB memory stick, 8 GB. For ordering data, please refer to [Section “Accessories” on page 245](#).

Parameterization memory (SD card)

For operation, the RFC 4072S requires a pluggable parameterization memory in the form of an SD card.

This parameterization memory can be used to save programs and configurations, which belong to your project, e.g., the PLCnext Engineer project, the visualization project, and the PROFINET device name. The data is retained in the parameterization memory, even if the SD card is removed from the device when the RFC is disconnected from the power supply.



The pluggable parameterization memory is not supplied as standard with the RFC 4072S. Only use SD cards from Phoenix Contact that are intended for use with the RFC. For the ordering data, please refer to [Section “Accessories” on page 245](#).

Data buffering/backup in the event of voltage failures

In the event of a supply voltage failure, the RFC 4072S saves control data, e.g., retain data and log files, on the inserted parameterization memory (SD card).

The device firmware recognizes the voltage failure. The retain data (variables of the controller, which are marked as “Retain” in the PLCnext Engineer project) and log files are automatically backed up on the parameterization memory.

**NOTE: Startup of the RFC 4072S not ensured**

For proper startup of the device, the supply voltage must only be switched on 30 seconds after the display goes out at the earliest.

Realtime clocks

The RFC buffers the internal realtime clocks after the supply voltage is switched off. If the buffering equipment is discharged, supply the RFC with 24 V DC for 24 hours. In this way, the buffering equipment is recharged.

Indication elements (display/LEDs)

Diagnostic and status information can be displayed directly on the RFC 4072S via the diagnostics indicators (display and LEDs) without additional software.

Information of the following is displayed, for example:

- Safety-related controller
- Standard controller
- PROFINET/PROFIsafe
- Ethernet connection(s)

Function extensions using PLCnext apps

You can easily extend the scope of functions of the controller using apps from the PLCnext Store.

Visit the PLCnext Store at plcnextstore.com.

2.2 Description of the safety-related functioning of the RFC 4072S

Safety-related PROFINET controller in PROFIsafe / Safety-related controller

The RFC 4072S contains a powerful two-channel safety-related controller for PROFIsafe (safety-related PROFINET controller, abbreviated: iSPNS 3000). The iSPNS 3000 is permanently integrated into the RFC. The safety-related PROFIsafe protocol is transmitted via the PROFINET network. The safety function is programmed in the PLCnext Engineer software.

As an F-Host, the iSPNS 3000 monitors and controls the safety function in a PROFIsafe system. Its function is to decide whether or not a safe output may be set, for example.

In this document, the iSPNS 3000 is also referred to as a safety-related controller.



For further information on the behavior of the iSPNS 3000 as the F-Host, refer to [Section "Behavior of the iSPNS 3000 as the F-Host in PROFIsafe" on page 28](#).

The iSPNS 3000 can also be operated as a lower-level F-Device on a safety-related controller (F-Host).



For further information on the behavior of the iSPNS 3000 as the F-Device, refer to [Section "Behavior of the iSPNS 3000 as the F-Device in PROFIsafe" on page 31](#).

Request for a programmed safety function

Following the request for a programmed safety function (e.g., safety door open), the iSPNS 3000 executes the programmed safety function. The relevant safe outputs of the F-Devices are set to the programmed value of the safety function.

Behavior in the event of an error / safe state (failure state)

The integrated diagnostics function detects errors that have occurred. All serious errors detected in the RFC with safety-related controller iSPNS 3000 that can lead to the loss of or adversely affect the programmed safety function switch the device to the safe state (Failure State). In this state, the safe outputs of the F-Devices are set to zero (FALSE).

The safe state is displayed on the "Safety PLC" tile of the display:

- The FS (Failure State) diagnostic display (LED) is shown in red.
- The "Safety PLC" tile itself is highlighted red.

In the event of an error, if you are connected online to the PLCnext Engineer, information about the error is also displayed in the software.

For descriptions of error states, associated effects, and appropriate measures for error removal, please refer to [Section "Errors, diagnostic messages and troubleshooting" on page 151](#).

PROFIsafe: Communication diagnostics

The iSPNS 3000 supports the user in monitoring and checking the communication relationships of the device-internal F-Host or F-Device.

For this, you can create management/diagnostic variables for the F-Host and the F-Device of the iSPNS 3000 in the PLCnext Engineer software.



For further information on communication diagnostics of the iSPNS 3000 refer to [Section "Behavior of the iSPNS 3000 as the F-Host in PROFIsafe" on page 28](#) and ["Behavior of the iSPNS 3000 as the F-Device in PROFIsafe" on page 31](#).

Exchange area

For exchange variables, the following maximum memory is available for the exchange area:

- The sum of the standard input data (NSI, inputs exchange area) may not exceed 3072 bytes (data direction “I”: iSPNS 3000 ← standard controller).
- The sum of the standard output data (NSQ, outputs exchange area) may not exceed 3072 bytes (data direction “Q”: iSPNS 3000 ⇒ standard controller).



The data direction “I” and “Q” is specified from the point of view of the safety-related controller.



Also observe the information in section [“Characteristic data of the safety-related PROFINET controller iSPNS 3000” on page 242.](#)



Notes on the iSPNS 3000 F-Adresses

One F_Source_Address and one F_Destination_Address can be defined for the iSPNS 3000, because:

- The iSPNS 3000 itself can be used as an F-Host (F_Source_Address).
- The iSPNS 3000 can be used as a lower-level F-Device (F_Destination_Address), e.g., on a safety-related controller, such as the AXC F XT SPLC 3000.

In addition to the rules listed above, note that both F-Adresses must each be assigned in a separate number range.

Assign the F_Source_Address to the iSPNS 3000 as the F-Host.

Assign the F_Destination_Address as necessary depending on the settings in the higher-level network.

A maximum of 300 F-Devices can be connected to one RFC 4072S (iSPNS 3000 as a F-Host).

This results in the following maximum values:

- The sum of the safe input data (SI) may not exceed 24576 bytes (input user data and PROFIsafe backup data).
- The sum of the safe output data (SQ) may not exceed 24576 bytes (output user data and PROFIsafe backup data).



Also observe the information in section [“Characteristic data of the safety-related PROFINET controller iSPNS 3000” on page 242.](#)

2.2.1 Behavior of the iSPNS 3000 as the F-Host in PROFIsafe

As an F-Host the iSPNS 3000 monitors and controls the safety function in a PROFIsafe-System. Its function is to decide whether or not a safe output may be set, for example.

Passivation und reintegration

If the communication relationship between the iSPNS 3000 and an F-Device is aborted, for example due to a communication error, the F-Device will be passivated. Passivation prevents the F-Device from starting up immediately as soon as the communication relationship is reactivated. Passivation and reintegration are displayed via Boolean variables, which the PLCnext Engineer automatically generates for each F-Device. F-Devices can also be passivated or reintegrated from the application program via these variables.

If an operator acknowledge request of the passivated F-Device is present, PROFIsafe-specific acknowledgment can be performed with a subsequent operator acknowledge reintegration. A non-safety-related signal can be used, for example. This overrides the passivation. As a result, the F-Device is reintegrated.



For more information about passivation and reintegration, please refer to [Section 4, “Startup and validation”](#) and sections [“Management/diagnostic variables for F-Devices” on page 129](#), [“Management/diagnostic variables for each configured F-Device” on page 191](#) und [“Global management/diagnostic variables for F-Devices” on page 195](#).

PROFIsafe: F-Host communication diagnostics

The iSPNS 3000 supports the user in monitoring and checking the communication connection. The PLCnext Engineer software indicates why the communication connection was disabled. A distinction is made between the F_WD_Time being exceeded (F_WD_Time OUT) and an F_CRC error (see [Figure 2-1](#)).

Variable (Safety PLC)	Type	Usage	I/Q/M	Comment	Init	Confirm	Variable (PLC)
Standard							
Systemvariablen							
F_ADDR_00001_ACK_REI	BOOL	Global	Q		FALSE		Select Variable (PLC) here
F_ADDR_00001_ACK_REQ	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00001_CE_CRC	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00001_DEVICE_FAULT	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00001_PASS_ON	BOOL	Global	Q		FALSE		Select Variable (PLC) here
F_ADDR_00001_PASS_OUT	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00001_WD_TIMEOUT	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00002_ACK_REI	BOOL	Global	Q		FALSE		Select Variable (PLC) here
F_ADDR_00002_ACK_REQ	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00002_CE_CRC	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00002_DEVICE_FAULT	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00002_PASS_ON	BOOL	Global	Q		FALSE		Select Variable (PLC) here
F_ADDR_00002_PASS_OUT	BOOL	Global	I		FALSE		Select Variable (PLC) here
F_ADDR_00002_WD_TIMEOUT	BOOL	Global	I		FALSE		Select Variable (PLC) here

Figure 2-1 PROFIsafe: management-/diagnostic variables for communication diagnostics

To support the user, seven non-safety-related management/diagnostic variables are created by default in PLCnext Engineer for each F-Device in the data list of the safety-related controller.

If required by the application, PLCnext Engineer allows the user to specify whether more or fewer management/diagnostic variables are created.

Alternatively, other management/diagnostic variables can be created. The user can link these variables to non-safety-related exchange variables of the standard controller in PLCnext Engineer. To do this, the user must define non-safety-related exchange variables in the software, where they can be linked to the management/diagnostic variables.



You can read more about management/diagnostic variables in [Section “Management/diagnostic variables for F-Devices” on page 129](#).

Various functions can be implemented using the management/diagnostic variables:

- Global acknowledgment of individual or multiple communication errors
- Reintegration of F-Devices
- System diagnostics using global management/diagnostic variables
- Diagnostics/control of intelligent F-Devices.

Device identification / number of safe devices

In PROFIsafe, safe devices (F-Devices) are identified by means of F-Addresses, which must be assigned uniquely for each safe device. PROFIsafe destination address F_Dest_Add (F_Destination_Address) is used to uniquely identify safe devices. This address is defined on the F-Device via DIP switch (see [Section 4.15.1](#)) and in the PLCnext Engineer software and checked immediately after it is entered in PLCnext Engineer. PLCnext Engineer checks the entered addresses for uniqueness in the configured network and for correct value range.

The value of the F_Destination_Address can be set from 0_{dec} to 65534_{dec} .



For safety modules from Phoenix Contact, you can set PROFIsafe destination addresses from 1 to 999_{dec} , maximum. For safety modules from other manufacturers, you can set PROFIsafe destination addresses from 1_{dec} to 65534_{dec} .

Source address F_Source_Address (F_Source_Add for short) uniquely identifies the F-Host of a communication relationship. The F_Source_Address is assigned to the safety-related controller and is used for all communication relationships that are assigned to this safety-related controller. In this way, the iSPNS 3000 obtains a source address (F_Source_Add).

The value of the F_Source_Address must be between 1_{dec} and 65534_{dec} .



NOTE: Use unique F-Addresses

Please note that the combination of F_Source_Address and F_Destination_Address must be unique within the network.

2.2.2 Behavior of the iSPNS 3000 as the F-Device in PROFIsafe



Please note that the F-Device function of the iSPNS 3000 is only available as of the revisions that are listed in the table in [Section “System requirements \(hardware and software\)” on page 21](#).

The iSPNS 3000 in the RFC 4072S can be operated as a lower-level F-Device, e.g., on a safety-related controller, such as the AXC F XT S PLC 3000. The iSPNS 3000 in the RFC 4072S is then treated as an F-Device by the higher-level F-Host (S PLC 3000).



The iSPNS 3000 can be used simultaneously as an F-Host and as an F-Device in two different PROFIsafe networks.

PROFIsafe: F-Device communication diagnostics

The iSPNS 3000 supports the user in monitoring and checking the communication relationships of the device-internal F-Device. For this purpose, analogous to the above described management/diagnostic variables of the F-Host, management/diagnostic variables can also be created in the PLCnext Engineer for the F-Device of the iSPNS 3000. The default setting for these variables is “Do not create”.



For additional information, please refer to [Section “Management/diagnostic variables of the iSPNS 3000 F-Device” on page 197](#).

Variable (Safety PLC)	Type	Usage	I/Q/M	Comment	Init	Confirm	Variable (PLC)
Standard							
Systemvariablen							
F_ADDR_00001_WD_TIMEOUT	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_ACK_REQ_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_PASS_ON_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_PASS_OUT_DEV	BOOL	Global	Q		FALSE		Select Variable (PLC) here
FD_ADDR_00001_IPAR_EN_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_IPAR_OK_DEV	BOOL	Global	Q		FALSE		Select Variable (PLC) here
FD_ADDR_00001_DEVICE_FAULT_DEV	BOOL	Global	Q		FALSE		Select Variable (PLC) here
FD_ADDR_00001_CHF_ACK_REI_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_CHF_ACK_REQ_DEV	BOOL	Global	Q		FALSE		Select Variable (PLC) here
FD_ADDR_00001_CE_CRC_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here
FD_ADDR_00001_WD_TIMEOUT_DEV	BOOL	Global	I		FALSE		Select Variable (PLC) here

Figure 2-2 PROFIsafe: Management/diagnostic variables for communication diagnostics of the iSPNS 3000 F-Device

System variables for the data exchange of the F-Device of the iSPNS 3000

These system variables are used for the data exchange between the F-Device of the iSPNS 3000 and the higher-level safety-related controller (F-Host).

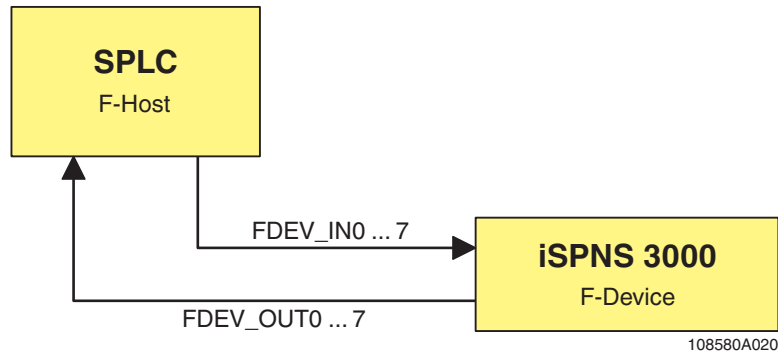


Figure 2-3 Data exchange between the F-Device of the iSPNS 3000 and the higher-level F-Host

- The eight system variables FDEV_IN0 to FDEV_IN7 contain the input process data (8 * 1 SAFEBYTE) of the F-Device instance of the iSPNS 3000.
- The eight system variables FDEV_OUT0 to FDEV_OUT7 contain the output process data (8 * 1 SAFEBYTE) of the F-Device instance of the iSPNS 3000.

The data direction is described from the view of the engineering:

- FDEV_INx = I
- FDEV_OUTx = Q



Please observe the information in [Section “FDEV_INx and FDEV_OUTx \(x = 0 ... 7\) system variables” on page 190.](#)

F_Destination_Address (F_Dest_Add)

For the iSPNS 3000 in the RFC 4072S, an F_Destination_Address (F_Dest_Add) must be defined, if the iSPNS 3000 is to be used as a lower-level F-Device, e.g., on a safety-related controller, such as the AXC F XT S PLC 3000.



Notes on the F_Dest_Add of the iSPNS 3000 F-Device

- Assign the F_Dest_Add in a separate number range.
- Assign the F_Dest_Add as necessary depending on the settings in the higher-level network.
- The F-Device of the iSPNS 3000 supports “FSCP 3/1 address type 1 (Functional Safety Communication Profile FSCP 3/1 (PROFIsafe™))” corresponding to the document:
 PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET Profile part, related to IEC 61784-3-3
 Technical Specification, Version 2.6MU1, August 2018

Setting F_Dest_Add

When the iSPNS 3000 is used as an F-Device, its F_Dest_Add can be set in the PLCnext Engineer software (see [Figure 2-4](#)).

- Set the F_Dest_Add of the iSPNS 3000 in the “Safety Parameters” editor in the editor group of the controller.
- Set the F_Dest_Add of the iSPNS 3000 in a range from 1 to a maximum of 65534_{dec} .
- Only assign F_Dest_Add values once.

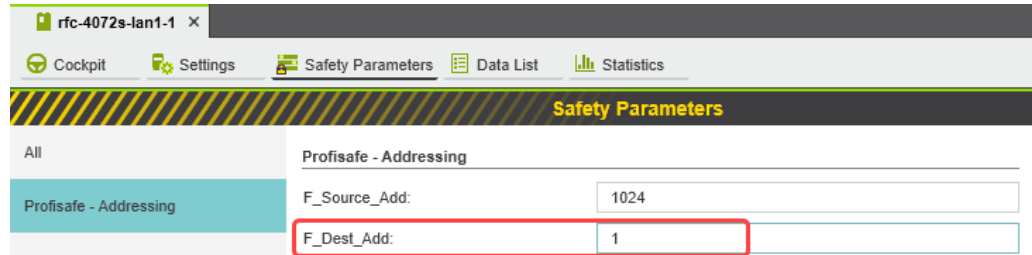


Figure 2-4 F-Address of the iSPNS 3000 F-Device in PLCnext Engineer: F_Dest_Add (F_Destination_Address)

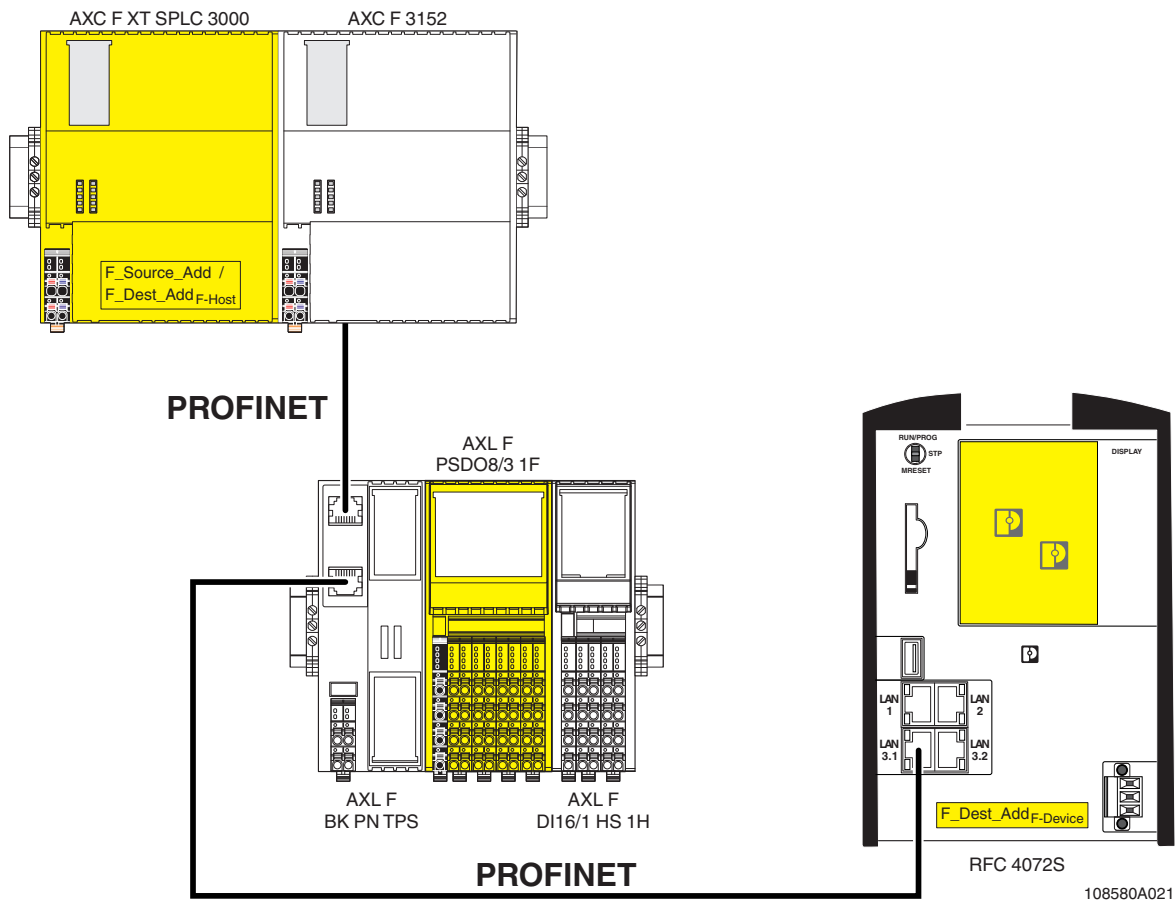


Figure 2-5 F-Addresses of the F-Host (SPLC 3000) and F-Device (iSPNS 3000)

**F-Addresses in
PLCnext Engineer**

For the above example application, the following F-Addresses are to be set in the PLCnext Engineer software for the AXC F XT S PLC 3000 (S PLC 3000 as an F-Host) and for the RFC 4072S (iSPNS 3000 as an F-Device):

AXC F XT S PLC 3000 (S PLC 3000 as an F-Host):

- F_Source_Add
- F_Dest_Add_{F-Host}

RFC 4072S (iSPNS 3000 as an F-Device):

- F_Dest_Add_{F-Device}

Additional information



Observe the following notes on the F-Device of the iSPNS 3000

- For the F-Device of the iSPNS 3000, the following applies: DAT = HAT.
 - Refer to the information on DAT (cycle time of the F-Device) and HAT (cycle time of the iSPNS 3000) in [Section "Determining F_WD_Time IN_{min}/F_WD_Time OUT_{min}"](#) on page 39.
- PROFIenergy is not supported.
- iParameter are not supported.

2.3 Calculating/determining the response time (Safety Function Response Time, SFRT)

The procedure for determining the necessary times, which is explained in more detail below, is recommended.

1. Determining the maximum permissible safety function response time ($SFRT_{max}$) depending on the relevant safety function to be implemented and determining the resulting maximum monitoring/watchdog times ($F_WD_Time\ IN_{max}/F_WD_Time\ OUT_{max}$) as an upper limit for each individual safety function (see Section [2.3.1 on page 36](#)).
2. Determining the minimum monitoring/watchdog times ($F_WD_Time\ IN_{min}/F_WD_Time\ OUT_{min}$) required for optimum system availability as a lower limit (see Section [2.3.2 on page 39](#)).
3. Defining the monitoring/watchdog times ($F_WD_Time\ IN/F_WD_Time\ OUT$) to be parameterized within the determined upper and lower limits and checking/validating that each of the safety functions to be implemented may be implemented with the defined monitoring/watchdog times (see Section [2.3.3 on page 45](#)).

2.3.1 Determining SFRT_{max} and F_WD_Time IN_{max}/F_WD_Time OUT_{max}

In the application, the maximum permissible SFRT must be determined for each safety function implemented in the application. This maximum permissible SFRT also includes the part of the SFRT that applies to the PROFIsafe system if PROFIsafe and the RFC 4072S are involved in the safety function.

A method of calculation for determining the part of the SFRT that applies to PROFIsafe is specified in the PROFIsafe system description (see Figure 2-6). The method of calculation specified is subject to certain general conditions.



For detailed information regarding the PROFIsafe system description, please refer to Section "Documentation" on page 246.

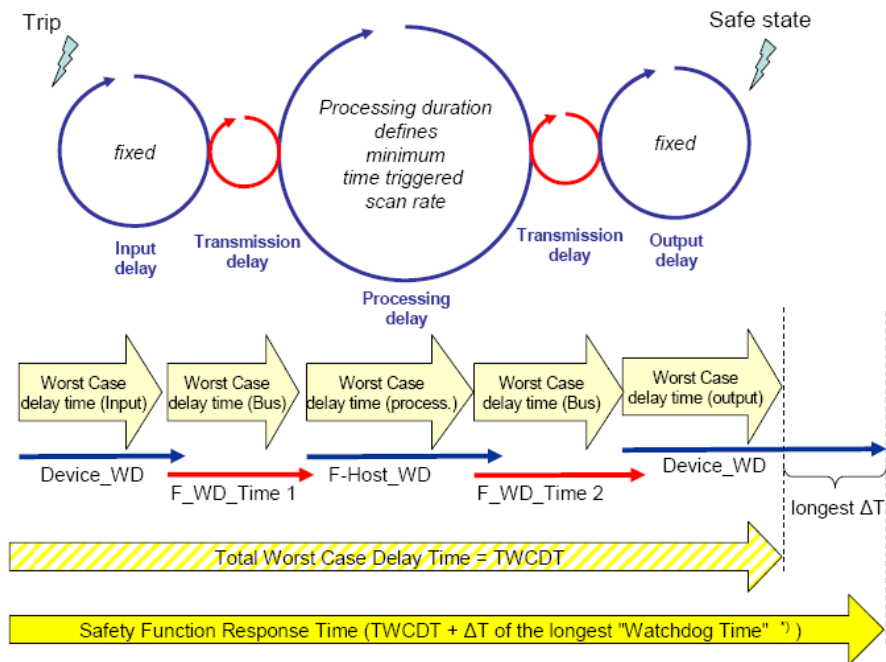


Figure 2-6 Calculation of the SFRT response time
 (*) = Not necessarily the output device

The TWCDT (total worst case delay time) is therefore the sum of all maximum signal runtimes that may occur in the individual elements during normal operation.

The individual elements are:

- (PROFIsafe) F-Devices
- Transmission (PROFIsafe via PROFINET including all network infrastructure components and lower-level subsystems, e.g., Inline/Axioline F local bus)
- iSPNS 3000

Due to a closely synchronized sequence of F-Host/iSPNS 3000 processing, this model is simplified when using the RFC 4072S. The runtimes, cycle times, and watchdog times of the iSPNS 3000 (processing delay and F-Host_WD) are not actually relevant when determining the SFRT.

The following figure illustrates the relationship:

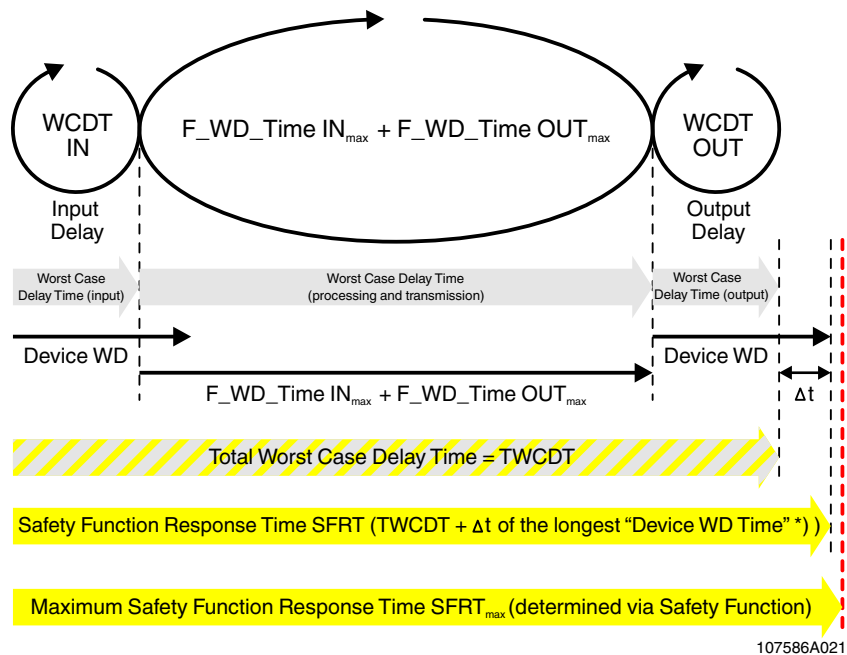


Figure 2-7 Simplified calculation of the SFRT response time
(*) = Not necessarily the output device

Key:

$SFRT_{max}$	Maximum permissible safety function response time of the PROFIsafe system involved in the safety function that is determined for each safety function to be implemented .
SFRT	Safety function response time of the PROFIsafe system involved in the safety function and the RFC 4072S that is actually implemented.
WCDT IN	Worst case delay time of the F-Device with input function. For this time, please refer to the device-specific user documentation for the F-Device used.
$F_WD_Time\ IN_{max}$	Value of the monitoring time F_WD_Time (watchdog time) which may be set as the maximum value for each individual F-Device with an input function that is involved in the safety function in order that $SFRT_{max}$ is not exceeded (see equation [2] page 38).
$F_WD_Time\ OUT_{max}$	Value of the monitoring time F_WD_Time (watchdog time) which may be set as the maximum value for each individual F-Device with an output function that is involved in the safety function in order that $SFRT_{max}$ is not exceeded (see equation [2] on page 38).

WCDT OUT	Worst case delay time of the F-Device with output function. For this time, please refer to the device-specific user documentation for the F-Device used.
Device WD	Internal watchdog time of the F-Device involved in the safety function.

The central component in [Figure 2-7 on page 37](#) is deemed to be the sum of $F_WD_Time\ IN_{max}$ and $F_WD_Time\ OUT_{max}$.

The sum of these times specifies the maximum internal processing time that is required for point-to-point communication via PROFIsafe between the PROFIsafe input device and the PROFIsafe output device using the iSPNS 3000 in the RFC 4072S, even in the event of an error, such as a telegram delay.

The actual SFRT to be implemented for the PROFIsafe system can be determined according to the following equation:

$$SFRT = WCDT\ IN + (F_WD_Time\ IN_{max} + F_WD_Time\ OUT_{max}) + WCDT\ OUT \quad [1]$$



SFRT must therefore be $\leq SFRT_{max}$

Take into consideration all the links that are involved in the safety function and programmed in the safety-related application program.

Maximum permissible watchdog times

To incorporate the maximum permissible watchdog times $F_WD_Time\ IN_{max}/F_WD_Time\ OUT_{max}$ in the PROFIsafe system, the following equation should be used:

$$F_WD_Time\ IN_{max} + F_WD_Time\ OUT_{max} \leq SFRT_{max} - WCDT\ IN - WCDT\ OUT \quad [2]$$



Please refer to the F-Device-specific user documentation to check whether further information is available regarding watchdog times within the internal device function.
If F-Devices are used where there is a difference (Δt) between their worst case delay time (WCDT) and the implemented device watchdog time (Device WD), this difference must be taken into consideration in accordance with the PROFIsafe model for determining the SFRT.



Timer functions that are used within the safety function in the safety-related application program must be taken into consideration.

2.3.2 Determining $F_WD_Time\ IN_{min}/F_WD_Time\ OUT_{min}$

The F_WD_Time , which you as the user must determine according to your application, is set in the PLCnext Engineer software (“Safety Parameters” editor, see [Figure 4-46 on page 131](#)). If the safe communication connection has been established between the partners, monitoring is performed independently by both F-Host (iSPNS 3000) and F-Device to ensure that the set F_WD_Time is observed during safe communication.



Please note that if the F_WD_Time is too short for a safety-related communication relationship, systems and applications will not be available.

This is because the value for F_WD_Time must be greater than or equal to the total maximum telegram runtime from F-Host to F-Device and back again in order that safe communication via PROFIsafe can, at the very least, be established during error-free network operation. In addition to the transmission times on the network (PROFINET cycle), internal stack and firmware runtimes in devices, delays caused by subsystem buses (e.g., device bus for modular I/O systems), etc. must also be taken into consideration.

The following figure from the PROFIsafe specification illustrates the relationship:



For detailed information on the PROFIsafe specification (PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Order No. 3.192), please refer to [Section “Documentation” on page 246](#).

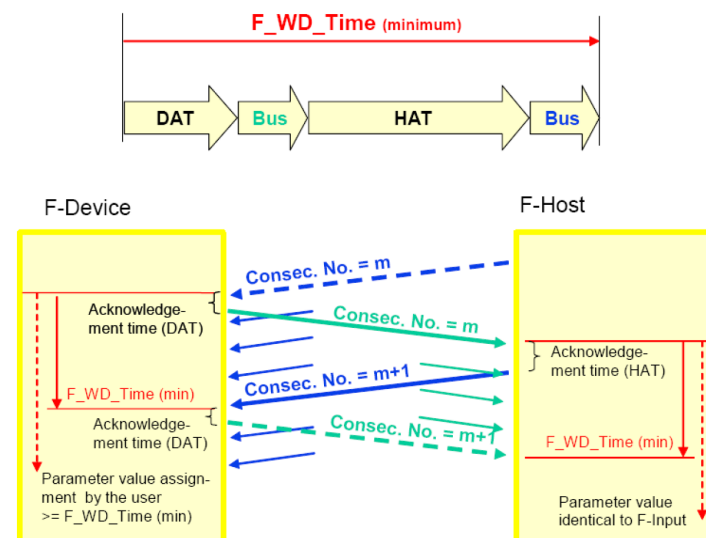


Figure 2-8 F_WD_Time (minimum)

Key:

- DAT Cycle time of the F-Device (F-Device acknowledge time)
- Bus Bus runtime including all relevant runtime components in the devices, backplane buses, bus heads (bus couplers or controllers) etc. of modular systems
- HAT Cycle time of the iSPNS 3000 (F-Host acknowledge time)

Determining the necessary times

DAT For the cycle time of the F-Devices, please refer to the device-specific user documentation for the F-Devices used.

Bus The “Bus” value is the sum of all the following times in the network/bus system used:

1. External bus runtime in the network:

- Update time of the I/O data between PROFINET controller and device set via the “Reduction ratio” multiplied by the “Monitor factor” (multiplier of the update time).

The result (monitor time) determines the time at which the communication link is disconnected if no cyclic data has been transmitted in the specified time (see [Figure 2-9](#)).

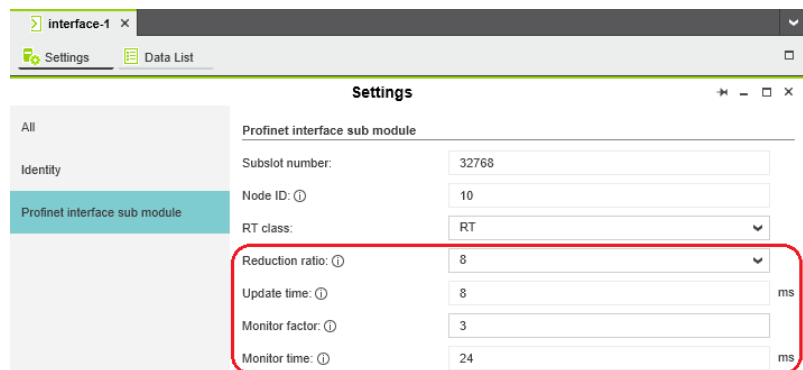


Figure 2-9 “Settings” editor of the interface editor group of the PROFINET device (settings of the AXL F BK PN or AXL F BK PN TPS PROFINET bus coupler)

- Relevant runtime components in bus heads (bus coupler or controllers) and backplane buses of modular systems.
For these values, please refer to the manufacturer’s information.
- Any runtimes within infrastructure components.
For these values, please refer to the manufacturer’s information.

2. Internal bus runtime within the RFC 4072S

- The internal runtime of the RFC 4072S, which is to be taken into consideration in the “Bus” value, is equivalent to one iSPNS 3000 cycle (T_{ZSPNS})

HAT The cycle time of the iSPNS 3000 (T_{ZSPNS}) can be estimated during the system/machine planning phase using the diagram in [Figure 2-10](#). Here, an application program that grows in proportion to the number of F-Devices is taken into consideration.



The cycle time of the iSPNS 3000 (T_{ZSPNS}) is marginally dependent on the size of the safe application program (iSPNS 3000 program runtime (S-PLC runtime)), the amount of safe process data, and the number of standard exchange variables for the standard controller.

Both values, iSPNS 3000 cycle time (S-PLC cycle time) and program runtime (S-PLC runtime), can be viewed in the display of the RFC 4072S (see [Figure 2-11 on page 42](#)).

The "Safety Cockpit" editor in the editor group of the "Safety PLC" in PLCnext Engineer (see [Figure 2-12 on page 42](#)) displays the iSPNS 3000 cycle time if the software is connected online to the RFC 4072S.

The following diagram shows the dependency of the iSPNS 3000 cycle time T_{ZSPNS} as the number of F-Devices in the application increases.

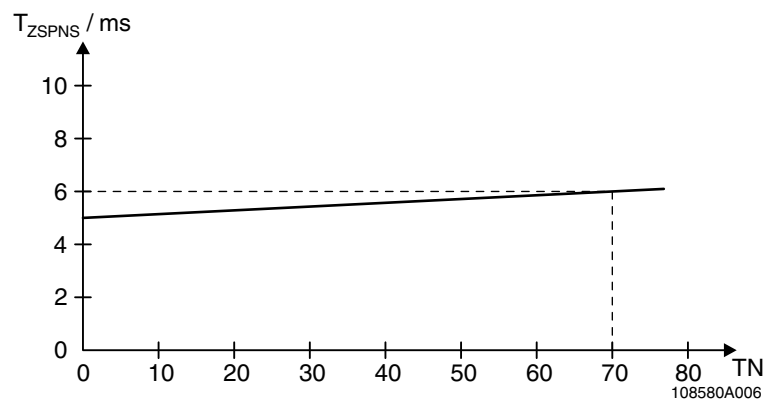


Figure 2-10 Cycle time of the iSPNS 3000 T_{ZSPNS}

Key:

T_{ZSPNS} Cycle time of the iSPNS 3000 (S-PLC cycle time) [in milliseconds]
 TN Number of F-Devices in the application

To verify the value of the iSPNS 3000 cycle time roughly determined during the planning phase, the actual value reached for the iSPNS 3000 cycle time should be read on the display of the RFC 4072S during the startup phase (S-PLC cycle time).

- For this, open the "S-PLC DETAILS" menu by tapping the "Safety PLC" tile (A in [Figure 2-11 on page 42](#)).

- Then tap the “DIAGNOSTICS” button.

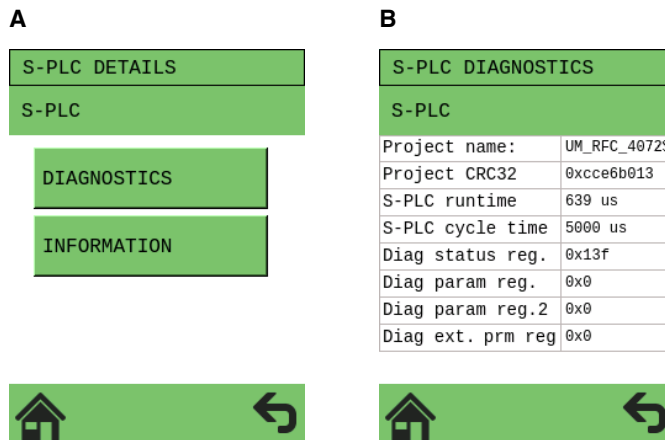


Figure 2-11 RFC 4072S display: cycle and program runtime of the iSPNS 3000 (B)

The value of the iSPNS 3000 cycle time (S-PLC cycle time) is available in the PLCnext Engineer software as the CYCLE_TIME system variable (see “SPNS” system variable on [page 184](#)).

The value of the iSPNS 3000 program runtime (S-PLC runtime) is available in the PLCnext Engineer software as the EXEC_TIME system variable (see “SPNS” system variable on [page 184](#)).

The iSPNS 3000 cycle time is displayed in the “Safety Cockpit” editor in the PLCnext Engineer software:

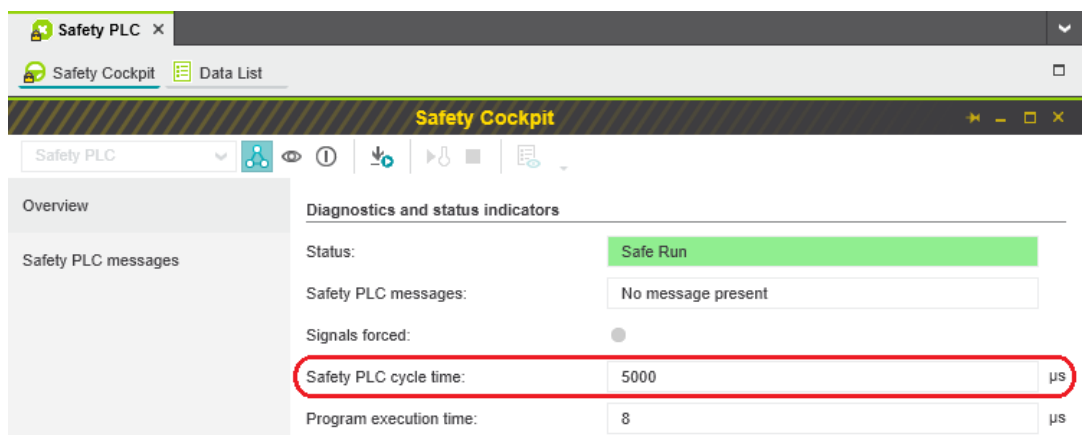


Figure 2-12 PLCnext Engineer: “Safety Cockpit” editor in the editor group of the “Safety PLC”



Based on the actual determined value of the iSPNS 3000 cycle time, it may be necessary to adjust the F_WD_Time in order to increase system availability, for example.



WARNING: Avoid possible danger that may be caused by the safety function being triggered too late

Make sure that the maximum permissible values for $F_WD_TIME\ IN_{max}$ and $F_WD_TIME\ OUT_{max}$ are not exceeded (see [Section “Determining SFRT_{max} and F_WD_Time IN_{max}/F_WD_Time OUT_{max}” on page 36](#)).

The minimum F_WD_Time that can be set can be determined for each communication connection using the following equation:

$$F_WD_Time_{min} > DAT + 2 \times Bus + HAT \quad [3]$$

Since the iSPNS 3000 cycle and the PROFINET cycle run asynchronously with one another, the iSPNS 3000 cycle must be included twice in the total when determining the minimum F_WD_Time , once as the “HAT” and again as the “internal bus runtime”. The external bus runtime is based on the relevant times of the PROFINET configuration.

$$F_WD_Time_{min} > DAT + 2 \times (\text{external bus runtime} + \text{internal bus runtime}) + HAT$$

$$F_WD_Time_{min} > DAT + 2 \times (\text{external bus runtime} + T_{ZSPNS}) + T_{ZSPNS}$$

$$F_WD_Time_{min} > DAT + 2 \times \text{external bus runtime} + 3 \times T_{ZSPNS} \quad [4]$$

For the example configuration in [Section “Example of a PROFINET/PROFIsafe configuration with PROFINET controller/F-Host” on page 96](#), taking into consideration the values below, the minimum $F_WD_Time\ OUT$ for communication with the F-Device AXL F PSDO8/3 1F is calculated as follows:

T_{ZSPNS}	= 5 ms	Cycle time of the safety-related controller (here: iSPNS 3000)
T_{ZPNIO}	= 8 x 3 ms	Monitor time: PROFINET update time x monitor factor (see Figure 2-9 on page 40).
$T_{D\ AXL\ F\ BK\ PN}$	= 1 ms	Update rate of the AXL F BK PN (or AXL F BK PN TPS) PROFINET bus coupler.
$T_{Z\ AXL\ LB}$	= 10 μs	Update rate of the Axioline F local bus with one device



Due to the low value this time is negligibly small in the following calculation for the given example. For larger local bus configurations, consider corresponding times in the calculation.

$$DAT_{PSDO} = 1.5\ ms \quad \text{Processing time of the AXL F PSDO8/3 1F}$$

$$T_{Bus} = T_{ZPNIO} + 1 \times T_{D\ AXL\ F\ BK\ PN} + 2 \times T_{Z\ AXL\ LB}$$

$$T_{Bus} = 24 + 1 \times 1\ ms + 2 \times 0\ ms$$

$$T_{Bus} = 25\ ms$$

The F_WD_Time OUT for available and robust system behavior with the specified PROFINET settings results as follows for the example configuration from the bus head (bus coupler AXL F BK PN) and the Axioline F output module (AXL F PSDO8/3 1F). The values listed and calculated above must be used in the following equation based on [4].

$$\mathbf{F_WD_Time\ OUT_{min} = DAT + 2 \times \text{external bus runtime} + 3 \times T_{ZSPNS}}$$

$$\mathbf{F_WD_Time\ OUT_{min} = 1.5\ ms + 2 \times 25\ ms + 3 \times 5\ ms}$$

$$\mathbf{F_WD_Time\ OUT_{min} = 66.5\ ms}$$

From this example it is clear that the bus cycle and transfer times, and in particular here the PROFINET update time as well as the monitor time, are the values that determine the minimum achievable F_WD_Time. In particular, the monitor factor (multiplier of the update time for aborting the connection if no data is exchanged) acts as the cut-off between availability/robustness and the minimum achievable SFRT in the overall system.

If the PROFINET update time is maintained at 1 ms via "Reduction ratio (= 1)" and the monitor factor is maintained at 3, the minimum achievable F_WD_Time OUT in the example is calculated as follows:

$$\mathbf{T_{Bus} = T_{ZPNIO} + 1 \times T_{D\ AXL\ F\ BK\ PN} + 2 \times T_{Z\ AXL\ LB}}$$

$$\mathbf{T_{Bus} = 3\ ms + 1 \times 1\ ms + 2 \times 0\ ms}$$

$$\mathbf{T_{Bus} = 4\ ms}$$

The minimum F_WD_Time OUT is calculated as follows for the example configuration:

$$\mathbf{F_WD_Time\ OUT_{min} = 1.5\ ms + 2 \times 4\ ms + 3 \times 5\ ms}$$

$$\mathbf{F_WD_Time\ OUT_{min} = 24.5\ ms}$$

2.3.3 Determining F_WD_Time IN/F_WD_Time OUT to be parameterized and checking/validating that the safety function can be implemented

Having calculated the upper and lower limits of the F_WD_TimeIN/F_WD_TimeOUT as described in the two previous sections, you now need to determine the F_WD_TimeIN/F_WD_TimeOUT watchdog times that are to be parameterized within these limits for the safety function that is to be implemented. You then need to check/validate that the required safety function can be implemented using the determined values.

The values are essentially determined as follows:

$$(F_WD_Time\ IN_{min} + F_WD_Time\ OUT_{min}) < (F_WD_Time\ IN + F_WD_Time\ OUT) < (F_WD_Time\ IN_{max} + F_WD_Time\ OUT_{max})$$

The relationship between the values for F_WD_Time IN and F_WD_Time OUT is based on the relationship for the minimum F_WD_Time and the system availability determined in Section 2.3.2 on page 39.

Example

Based on the maximum possible safety function response time, the following requirement must be met:

$$F_WD_Time\ IN_{max} + F_WD_Time\ OUT_{max} = 200\ ms \quad (\text{Upper limit from the safety function})$$

$$F_WD_Time\ OUT_{min} = 24.5\ ms \quad (\text{From the example in Section 2.3.2})$$

$$F_WD_Time\ IN_{min} = 50\ ms \quad (\text{Assumed for the example calculation})$$

The watchdog times to be parameterized are chosen as follows in the example:

$$F_WD_Time\ OUT \approx 2 \times 24.5\ ms \Rightarrow F_WD_Time\ OUT = 50\ ms$$

$$F_WD_Time\ IN = 2 \times 50\ ms = 100\ ms$$

Factor 2 has been chosen here so that it is still possible to later increase the PROFINET repeat cycles by the monitor factor or the PROFINET update time without endangering system availability by exceeding the F_WD_Time monitoring time.

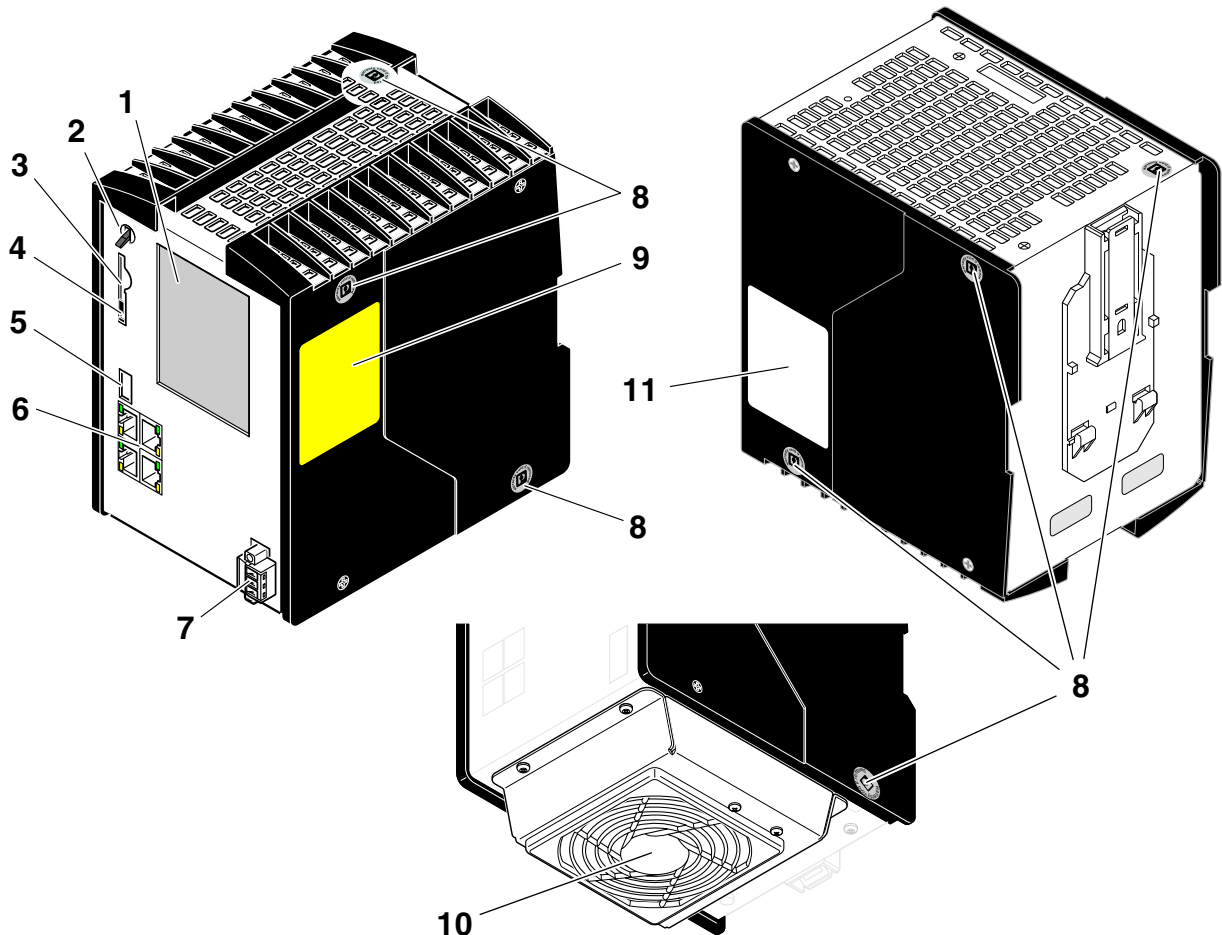
As a result, the values selected in the example project (see Figure 4-46 on page 131 and Figure 4-47 on page 132) described in Section 4.3.1 are within the permissible range:

$$\text{Minimum } F_WD_Time\ (IN+OUT) < F_WD_Time\ (IN+OUT)\ \text{to be parameterized} < \text{Maximum } F_WD_Time\ (IN+OUT)$$

$$(50 + 24.5)\ ms < (100 + 50)\ ms < 200\ ms$$

⇒ Sum of the watchdog times is less than 200 ms.

2.4 Indicators, interfaces, and operating elements



108580A010

Figure 2-13 Structure of the RFC 4072S Remote Field Controller including fan module

Key:

- 1 Touch screen display
- 2 Mode selector switch
- 3 Slot for the parameterization memory/card holder (SD card)
- 4 Ejector for the parameterization memory
- 5 USB interface (type A USB 3.0 socket)
- 6 Ethernet interfaces (RJ45 sockets; LAN1/LAN2: 10/100/1000 Mbps; LAN3.1/LAN3.2 (switched internally): 10/100 Mbps)
- 7 Connection for external supply voltage (24 V DC)
- 8 Security seal
- 9 Test marks and revision status (hardware/firmware of iSPNS 3000)
- 10 Fan module (optional)
- 11 Label with revision status of the standard controller, MAC addresses and serial number of the RFC as well as the user name and password for user authentication

**NOTE: Electrostatic discharge!**

The RFC contains components that can be damaged or destroyed by electrostatic discharge. When handling the RFC, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1.

**Scope of supply**

Please note that the SD card (parameterization memory) and the fan module are not supplied as standard with the RFC 4072S.

For the ordering data, please refer to [Section "Accessories" on page 245](#).

2.5 Security seal and test mark

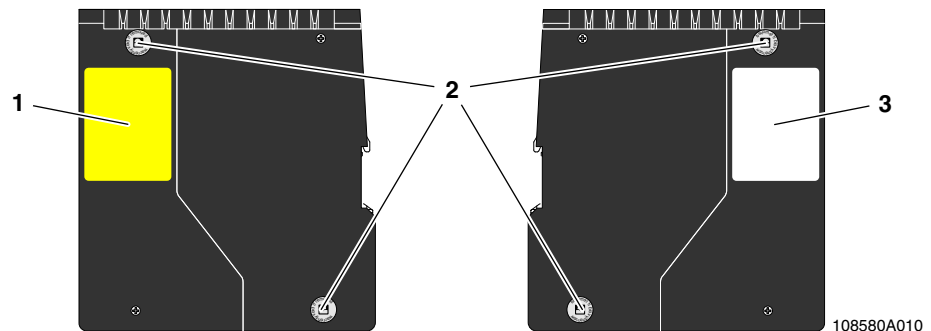


Figure 2-14 Security seal and test mark

- 1 Test marks and revision status (hardware/firmware) of the safety-related PROFINET controller iSPNS 3000
- 2 Security seal (see also item 8 in [Figure 2-13 on page 46](#))
- 3 Revision status (hardware/firmware) of the standard controller, MAC addresses and serial number of the RFC as well as the user name and password for user authentication (see [Section 2.15](#))

2.6 Fan module

The fan module is not supplied as standard with the RFC; it is available as an accessory. For the ordering data, please refer to [Section "Accessories" on page 245](#).



NOTE: The RFC 4072S can overheat – use the fan module.

The RFC can be operated from 0 m to 2000 m above sea level at ambient temperatures up to 40 °C without a fan module. Warning messages and switching off may occur at higher ambient temperatures. For this reasons, the fan module is required for operation above ambient temperatures of 40 °C.

We recommend using the fan module at an ambient temperature of 35 °C and above to increase the service life of the RFC.

From 2000 m to 3000 m above sea level at ambient temperatures from 0 °C to 55 °C the RFC must be operated with a fan module.

From 3000 m to 4000 m above sea level at ambient temperatures from 0 °C to 50 °C the RFC must be operated with a fan module.

The fan module is attached to the bottom of the RFC using four screws. Tighten all four M4 screws equally using a recommended tightening torque of 2.2 Nm (3.0 Nm, maximum) so that they cannot loosen accidentally (e.g., due to vibration).



See the detailed information in [Section "Mounting the RFC FAN MODULE fan module" on page 79](#).

The electrical connection between the RFC and the fan module is established automatically when attaching the fan module. The fan module contains a fan.



NOTE: The RFC 4072S can overheat – keep vents clear

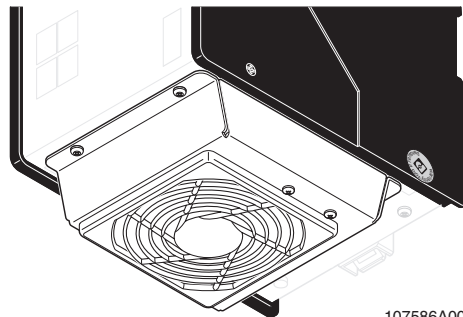
When installing the RFC make sure that the vents can be freely accessed. Otherwise, the RFC may overheat. To ensure good ventilation, leave a gap of more than 10 cm above and below the RFC.

Do not install devices below the RFC that could additionally heat it up.



NOTE: Potential RFC 4072S malfunction

The fan module must not be replaced during operation. The RFC must be switched off before the fan module can be replaced. To replace the fan module, remove the RFC from the DIN rail.



107586A003

Figure 2-15 RFC with fan module

2.7 Status and diagnostics indicators (Ethernet)

The LNK and ACT LEDs indicate the status of the Ethernet interface. The LEDs have the following meaning:

LNK	The LNK LED (link, green) lights up when the RFC is able to contact another network device.
ACT	The ACT LED (activity, yellow) flashes when the Ethernet interface is transmitting or receiving data.

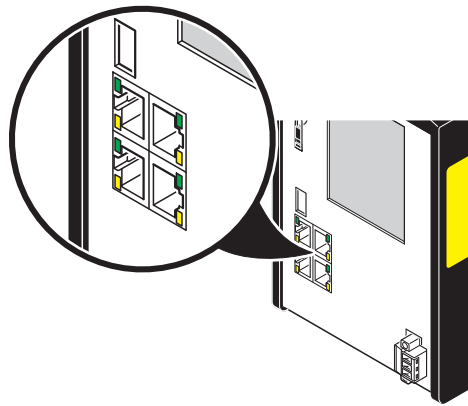


Figure 2-16 LNK and ACT LEDs

2.8 Touch screen display

The RFC 4072S has a Touch screen display (referred to as “display” in the following). This display shows tiles containing various information on the device and the connected network. The display allows you to retrieve information about the iSPNS 3000 and OPC UA connections, for example. The depth of information shown varies by tapping the individual tiles.

The display allows menu-guided operation of the device. Among other things, you can carry out IP address settings of the RFC 4072S or reset the device to the factory default.

The RFC 4072S is equipped with a resistive Touch screen display.

Avoid damage (e.g., scratches) by only using slight pressure when operating the display.



NOTE: Damage to the display

Pointed or sharp-edged objects or tools can cause irreparable damage to the display. Therefore, only use your fingertips or the tools specified in the technical data for operating the touch screen.



DANGER: Poisoning

If the display is damaged, avoid direct skin contact, swallowing or inhaling of escaping fluids or gases.



DANGER: Chemical burns

If the display is damaged, avoid direct skin contact, swallowing or inhaling of escaping fluids or gases.

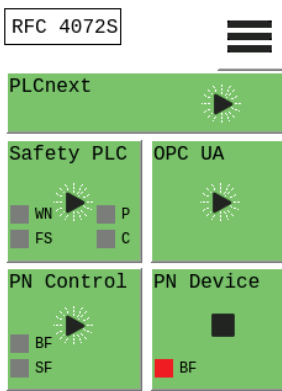


Figure 2-17 Display of the RFC

You can activate following menu-specific functions by tapping the symbols on the display. Symbols can be found in the main menu and submenus.



When a symbol is tapped, it changes color. This gives you a visual feedback that the tapping has been registered by the operating system.

Table 2-1 Functions of the symbols

Operating button	Description
	Return to home menu.
	Open the "CONFIG DETAILS" menu.
	<ul style="list-style-type: none"> - Confirm and accept entries that were previously made. - Confirm and execute selection (e.g., RFC reset and restart).
	Cancel and do not accept entries that were previously made.
	Jump back to the next higher menu level. Non-confirmed entries that were previously made are not accepted.
	Jump left to the previous character in the value to be edited.
	Jump right to the next character in the value to be edited.

2.9 Structure of the display (diagnostic display)

The display contains important diagnostic and status information for the RFC and its interfaces. Depending on the selected view, more detailed information can be selected for individual items. For example, the IP addresses of the RFC can be requested via the display and set if necessary.

Possible indicators of the display are described below:

The following figure shows the structure of the display (home menu and submenus):

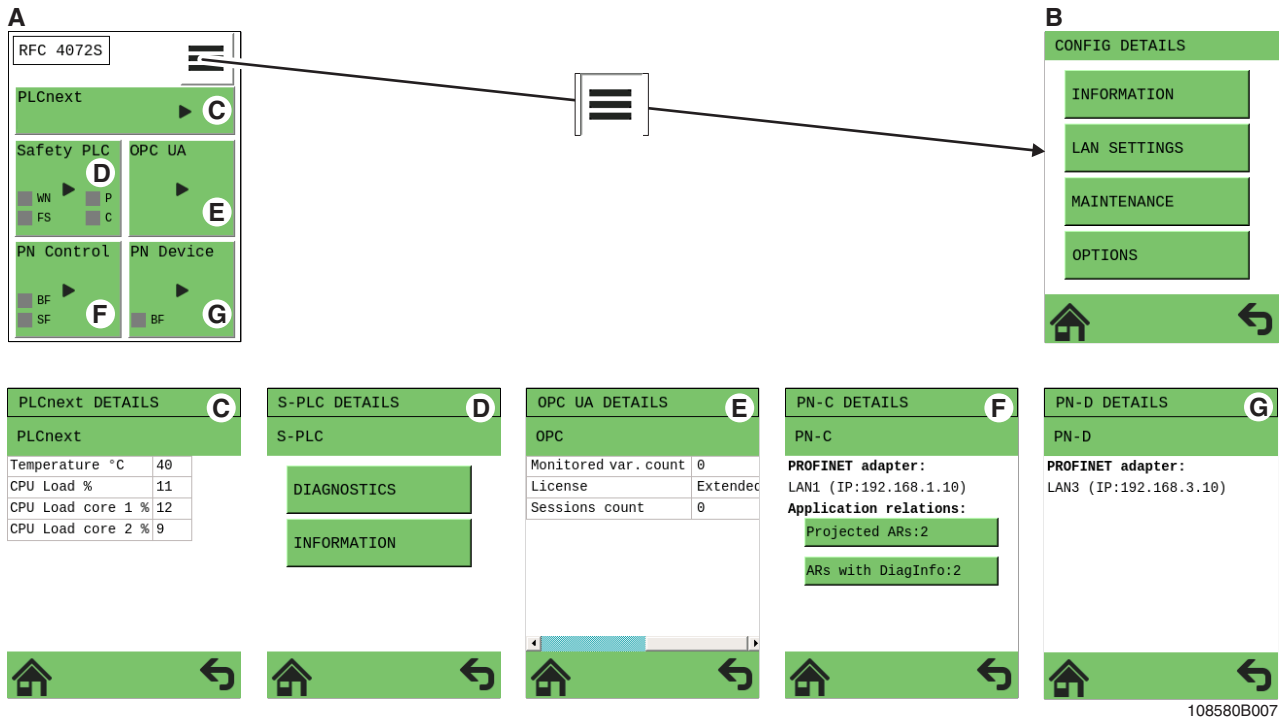


Figure 2-18 Structure of the display

Key:

- A** Home menu
- B** "CONFIG DETAILS" menu
- C** "PLCnext DETAILS" menu (standard controller)
- D** "S-PLC DETAILS" menu (safety-related iSPNS 3000 PROFINET controller)
- E** "OPC UA DETAILS" menu (OPC UA server)
- F** "PN-C DETAILS" menu (PROFINET controller)
- G** "PN-D DETAILS" menu (PROFINET device)

2.9.1 Indicators on the display

The following figure shows the general meaning of the indicators in the home menu of the display.

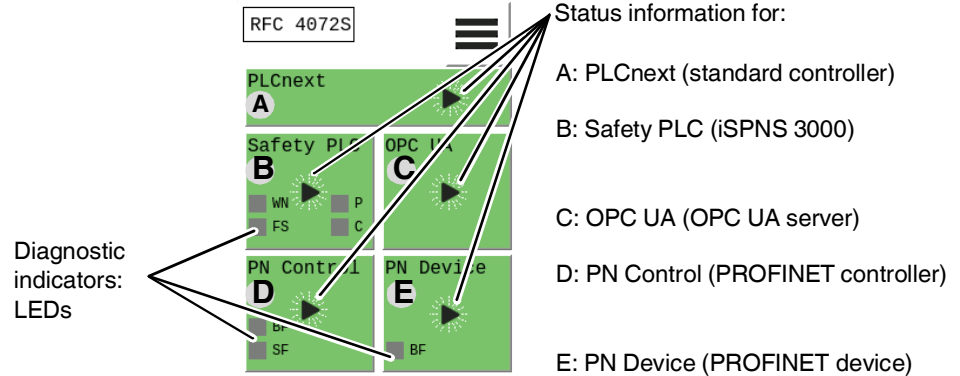


Figure 2-19 Display: indicators in the home menu

The diagnostic indicators (LEDs) and status information of the standard controller inside the device, of the safety-related iSPNS 3000 PROFINET controller inside the device, and of the OPC UA server are displayed on the individual tiles A to E in Figure 2-19. In addition, the diagnostic indicators (LEDs) and status information of the RFC as a PROFINET controller and/or PROFINET device are displayed.

The background color in the individual areas varies depending on the states.

2.9.2 Status information

The status information of the individual tiles is displayed only in the home menu. The background color on the individual tiles varies depending on the state.

The status information on the individual tiles has the following meaning:







PLCnext (standard controller)

Table 2-2 Status information: PLCnext (standard controller)

Indicator	Color	Meaning
	Green	The standard controller is in the "Run" state.
	Green	The standard controller is in the "Stop" state.
	Red	The standard controller has switched to the "Stop" state as a result of an error.

Safety PLC (iSPNS 3000)

Table 2-3 Status information: safety PLC (iSPNS 3000)

Indicator	Color	Meaning
	Gray	The function of the iSPNS 3000 is deactivated. No safety-related program is loaded.
	Blue	Initial state in which the iSPNS 3000 passes through various phases until it is ready for operation (e.g., self-test, synchronization with the standard controller). The iSPNS 3000 is ready for operation once it has passed through these phases. FS is off.
	Green	Cyclical processing of the safety-related application program has started. FS is off.
	Orange	The iSPNS 3000 is in the "Debug Run" state. This state was invoked from the PLCnext Engineer software with an active online connection. FS is off.
	Orange	The iSPNS 3000 is in the "Debug Stop" state. This state was invoked from the PLCnext Engineer software with an active online connection. The iSPNS 3000 is ready. Cyclical processing of the safety-related application program has stopped. The iSPNS 3000 must be started manually via the PLCnext Engineer software. FS is off
	Red	The iSPNS 3000 is in the safe state (failure state). FS is red.





**WARNING: Avoid possible danger – outputs can be set**

Take appropriate measures to ensure that your system/machine does not present any danger.

Variables can be overwritten in the "Debug Run" state. These are then also transmitted to the PROFIsafe output devices and output.





OPC UA (OPC UA server)

Table 2-4 Status information: OPC UA (OPC UA server)

Indicator	Color	Meaning
	Green	The OPC UA server is in the “Stop” state and no OPC UA license is available.
	Green	<ul style="list-style-type: none"> – OPC UA licence available. – There is no connection to a OPC UA client. – No OPC UA process data is exchanged.
	Green	<ul style="list-style-type: none"> – OPC UA licence available. – There is a connection to at least one OPC UA client. – OPC UA process data is exchanged.
	Red	Internal device error.





PN Control (PROFINET controller)

Table 2-5 Status information: PN Control (PROFINET controller)

Indicator	Color	Meaning
	Green	No PROFINET device was configured in the PLCnext Engineer software.
	Green	<p>At least one PROFINET device was configured in the PLCnext Engineer software.</p> <p>The RFC 4072S (PROFINET controller) attempts to establish an application relationship to this PROFINET device.</p>
	Green	<p>The RFC 4072S (PROFINET controller) has established an application relationship with at least one configured PROFINET device and exchanges process data with this device.</p> <p>For PROFINET devices that cannot be reached, the RFC 4072S (PROFINET controller) cyclically attempts to establish a connection approximately every five seconds.</p> <p>A connection cannot be established if the corresponding PROFINET device is ready, but a correct PROFINET device name has not yet been assigned to it, for example.</p>
	Red	An error occurred while configuring the RFC 4072S (PROFINET controller).

**PN Device
(PROFINET device)**

Table 2-6 Status information: PN Device (PROFINET device)

Indicator	Color	Meaning
	Green	No connector is inserted into the LAN3 PROFINET device interface (link not present). BF is red.
	Green	A connector is inserted into the LAN3 PROFINET device interface (link is present). No application relationship established. BF flashing red.
	Green	An application relationship is established between the higher-level PROFINET controller and the RFC 4072S (PROFINET device).
	Red	Internal firmware error of the RFC 4072S (PROFINET device).

2.9.3 Diagnostics indicators

The diagnostic indicators of all the tiles are displayed in the home menu using virtual LEDs. They have the following meaning:

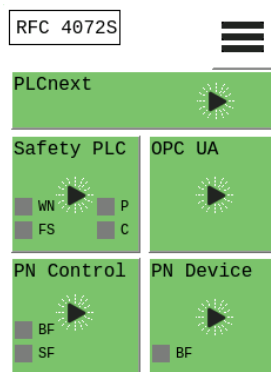


Figure 2-20 Diagnostic indicators in the home menu (LEDs)

Safety PLC (safety-related PROFINET controller iSPNS 3000)

Table 2-7 Diagnostics indicators: safety PLC (safety-related PROFINET controller iSPNS 3000)

LED	Color		Meaning
WN	Warning of the iSPNS 3000		
	Yellow	On	A group warning message of the iSPNS 3000 is present (see section “System variables of the iSPNS 3000” starting on page 184). Bit 7 WARN in the SPNS.DIAG.STATUS_REG diagnostic status register is set to TRUE. Additional information is contained in the associated diagnostic parameter registers of the iSPNS 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG).
	Gray	Off	There is no warning of the iSPNS 3000.
FS	Failure State: Safe State of the iSPNS 3000		
	Red	On	A critical error has occurred and been detected. The iSPNS 3000 has switched to the “safe state”.
		Flashing (1 Hz)	<ul style="list-style-type: none"> – Initialization phase is running (firmware boot process with power-on self-test, loading the parameterization and configuration data from the parameterization memory, booting the safe application program) or – Initialization phase has been aborted with an error or – Error-free DEBUG state of the iSPNS 3000
Gray	Off	Error-free operating state of the iSPNS 3000 (if supply voltage is present)	

Table 2-7 Diagnostics indicators: safety PLC (safety-related PROFINET controller iSPNS 3000)

LED	Color	Meaning	
P	The state of the safety-related communication relationship between the iSPNS 3000 (F-Device) and a superordinate safety-related controller (F-Host).		
	Green	On	The safety-related communication relationship to the superordinate safety-related controller has been initialized and established without errors.
		Flashing (1 Hz)	<p>The safety-related communication relationship between the F-Device of the iSPNS 3000 and the higher-level safety-related controller (F-Host) was interrupted due to a previous communication error.</p> <p>Safety-related communication between the F-Host and F-Device has been restored. However, safety-related process data is not exchanged because the F-Device of the iSPNS 3000 was passivated.</p> <p>In order to continue the exchange of safety-related process data, an operator acknowledge request generated by the F-Device must be acknowledged.</p> <p>The F_ADDR_[nnnnn]_ACK_REQ management/diagnostic variable set to TRUE displays the operator acknowledge request.</p> <p>The user acknowledges the operator acknowledge request by means of a deliberate operator acknowledge reintegration of the iSPNS 3000 F-Device in the safety-related application program of the higher-level safety-related controller (F-Host).</p> <p>For this, the user sets the F_ADDR_[nnnnn]_ACK_REI management/diagnostic variable to TRUE.</p>
	Gray	Off	The safety-related communication relationship to the superordinate safety-related controller has not been initialized.
C	State of the safety-related communication relationship between the iSPNS 3000 (F-Host) and configured subordinate F-Devices.		
	Green	On	All safety-related communication relationships to configured subordinate F-Devices have been initialized and established without errors. Safety-related process data will be transmitted.
		Flashing (1 Hz)	A communication error that must be acknowledged is still present for at least one safety-related communication relationship to a subordinate F-Device.
	Gray	Off	At least one configured safety-related communication relationship to a subordinate F-Device has not yet started or has been interrupted.

OPC UA (OPC UA server) No LED indicators present.

**PN Control
(PROFINET controller)**

Table 2-8 Diagnostic indicators: PN Control (PROFINET controller)

LED	Color		Meaning
BF	Red	On	No link status on the Ethernet port and/or no 100-Mbit transmission and/or no full duplex mode present.
		Flashing	Link status present, at least one configured PROFINET device has no PROFINET communication connection.
	Gray	Off	The PROFINET controller has established an active communication connection to each configured PROFINET device.
SF	Red	On	Group error message: At least one diagnostic alarm is present.
	Gray	Off	No group error message is present. No diagnostic alarms.

**PN Device
(PROFINET device)**

Table 2-9 Diagnostics indicators: PN device (PROFINET device)

LED	Color		Meaning
BF	Red	On	No link status on the Ethernet port and/or no 100-Mbit transmission and/or no full duplex mode present.
		Flashing	Link status present, there is no PROFINET communication connection to the PROFINET controller.
	Gray	Off	A PROFINET controller has established an active communication connection to the PROFINET device

2.9.4 Home menu

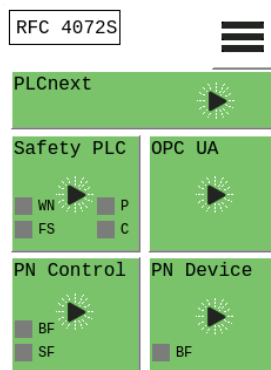




Figure 2-21 Home menu


The home menu displays the following operating states and diagnostic LEDs:

- PLCnext (standard controller)
- Safety PLC (iSPNS 3000); LEDs: WN, FS, P, C
- OPC UA (OPC UA server)
- PN Control (PROFINET controller; LEDs: BF, SF)
- PN Device (PROFINET device); LED: BF

In the home menu, tap on the individual tiles or the symbol for the “CONFIG DETAILS” menu to open the desired menu. A stylized 3D effect (animated keystroke) indicates whether the operating system recognized the tap. Then one of the menus briefly described in the following sections opens.

- You can always return to the home menu by tapping the  symbol.
- Tapping the  symbol changes to the next higher level in the menu structure.

2.9.5 “CONFIG DETAILS” menu

- Open the “CONFIG DETAILS” menu by tapping the  symbol in the home menu.

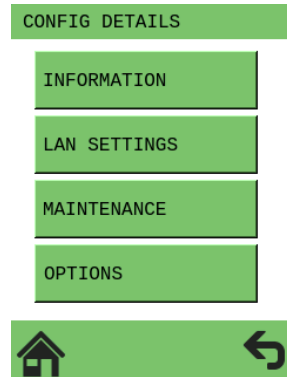


Figure 2-22 “CONFIG DETAILS” menu

The “CONFIG DETAILS” menu provides further menus for selection that you can open by tapping the relevant button.

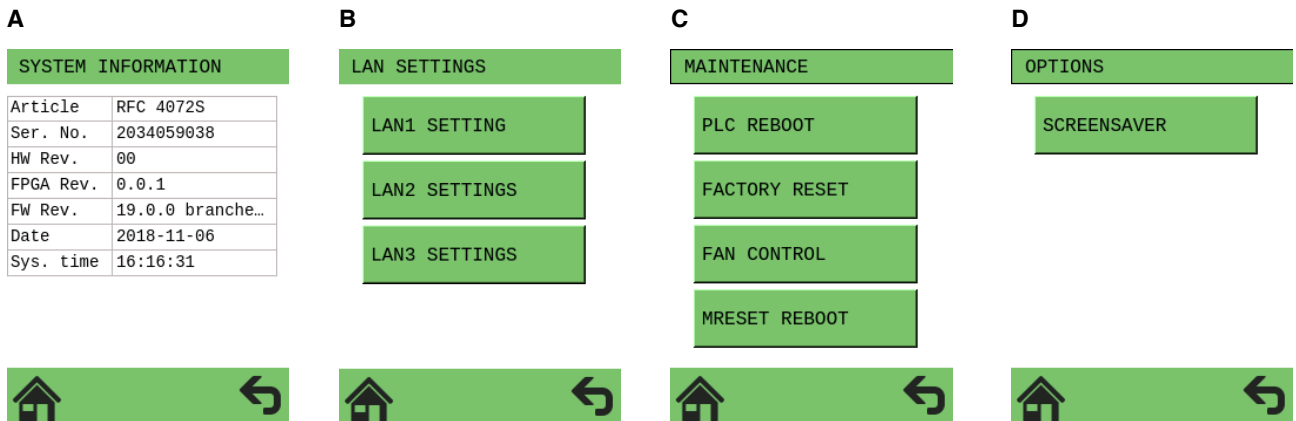


Figure 2-23 “CONFIG DETAILS” menu: submenus

The menus show information on the device and enable different settings, e.g., device IP address settings.

Menus in [Figure 2-23 on page 60](#):

A SYSTEM INFORMATION

The menu shows information on the RFC 4072S:

- Order designation
- Serial number
- Hardware version
- FPGA version
- Firmware version
- Current Date
- System time

B LAN SETTINGS

The menu shows the current IP address settings of the LAN1, LAN2, LAN3.1/3.2 Ethernet interfaces of the RFC 4072S.

The IP address settings can be changed in the menu and assigned to the Ethernet interfaces permanently.

C MAINTENANCE

The menu allows for the following maintenance settings:

- PLC REBOOT
Restarts the RFC 4072S
- FACTORY RESET
Resets the RFC 4072S to the factory settings
- FAN CONTROL
Information on the fan of the RFC 4072S (e.g., maintenance demand or defect) and calibration of the fan
- MRESET REBOOT
See also MRESET in [Section "Mode selector switch" on page 70](#).
The application program in the RAM of the standard controller is deleted. In addition, the retain data is deleted.
The RFC 4072S is then restarted.

D OPTIONS

The menu provides the following settings:

- SCREENSAVER
Setting the time after which a screensaver is shown on the display.

2.9.6 “PLCnext DETAILS” menu (standard controller)

- Open the “PLCnext DETAILS” menu by tapping the “PLCnext” tile in the home menu.

PLCnext DETAILS	
PLCnext	
Temperature °C	40
CPU Load %	11
CPU Load core 1 %	12
CPU Load core 2 %	9



Figure 2-24 “PLCnext DETAILS” menu (standard controller)

The menu shows the following information on the standard controller of the RFC 4072S:

- Device temperature
- Processor load

2.9.7 “PLCnext DETAILS” menu (safety-related PROFINET controller)

- Open the “S-PLC DETAILS” menu by tapping the “Safety PLC” tile in the home menu.

S-PLC DETAILS
S-PLC
DIAGNOSTICS
INFORMATION



Figure 2-25 “S-PLC DETAILS” menu (iSPNS 3000)

The “S-PLC DETAILS” menu provides further menus for selection that you can open by tapping the relevant button.

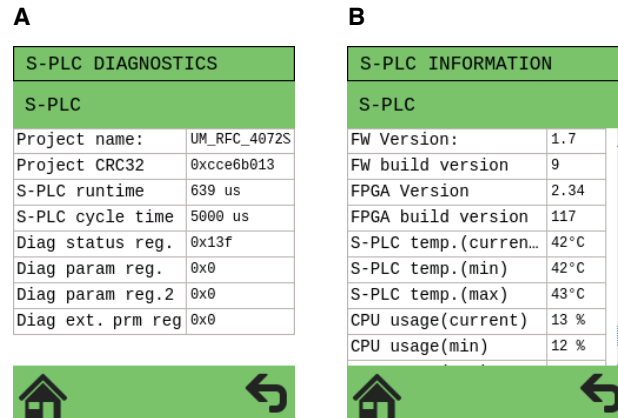


Figure 2-26 “S-PLC DETAILS” menu: submenus

The menus show information on the iSPNS 3000 and on the safe application program.

Menus in [Figure 2-26 on page 63](#):

A S-PLC DIAGNOSTICS

The menu shows information on iSPNS 3000 diagnostics:

- Project name
- CRC checksum of the PLCnext Engineer project
In PLCnext Engineer, this value can be found in the “Safety Cockpit” editor (“Safety PLC” editor group) in the “Overview” area of the engineering project information.
- Program runtime and cycle time of the iSPNS 3000 in μs
- Contents of the iSPNS 3000 register:
 - DIAG_STATUS_REG
 - DIAG_PARAM_REG
 - DIAG_PARAM_2_REG
 - DIAG_EXT_PARAM_REG

The contents are also displayed in the corresponding PLCnext Engineer variables in the SPNSV2_TYPE structure.

B S-PLC INFORMATION

The menu shows the following information:

- Firmware and FPGA versions
- Minimum, maximum and current CPU utilization of the iSPNS 3000
- Minimum, maximum and current temperature of the iSPNS 3000

2.9.8 “OPC UA DETAILS” menu (OPC UA server)

- Open the “OPC UA DETAILS” menu by tapping the “OPC UA” tile in the home menu.

OPC UA DETAILS	
OPC	
Monitored var. count	0
License	Extended
Sessions count	0



Figure 2-27 “OPC UA DETAILS” menu (OPC UA server)

The menu shows information on the OPC UA connections:

- Number of monitored variables
- Availability of a OPC UA licence
- Number of logged-in connections to OPC UA clients (sessions)

2.9.9 “PN-C DETAILS” menu (PROFINET controller)

- Open the “PN-C DETAILS” menu by tapping the “PN Control” tile in the home menu.

PN-C DETAILS	
PN-C	
PROFINET adapter:	
LAN1 (IP:192.168.1.10)	
Application relations:	
Projected ARs:	2
ARs with DiagInfo:	2



Figure 2-28 “PN-C DETAILS” menu (PROFINET controller)

The menu shows information on the PROFINET controller:

- Ethernet interface and IP address used
- Details on application relationships (number of configured (total/of which are secure) and diagnostic information on ARs)

Using the “Projected ARs: ...” and “ARs with DiagInfo: ...” buttons displays a list of configured application relationships or a list of error codes assigned to PROFINET device names.

2.9.10 “PN-D DETAILS” menu (PROFINET device)

- Open the “PN-D DETAILS” menu by tapping the “PN Device” tile in the home menu.

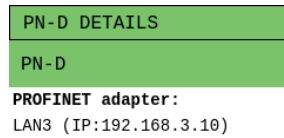


Figure 2-29 “PN-D DETAILS” menu (PROFINET device)

The menu shows information on the PROFINET device:

- Ethernet interface and IP address used

2.10 USB interface (currently not supported)

The RFC 4072S is equipped with a USB 3.0 interface. It is designed as a type A USB socket. You can connect a USB memory stick to this interface.



We recommend using the following USB stick: USB FLASH DRIVE (Order No. 2402809), USB memory stick, 8 GB. For the ordering data, please refer to [Section "Accessories" on page 245](#).

The USB interface enables the non-safety-related firmware of the RFC 4072S to be updated using the USB memory stick. In addition, you can access the inserted USB stick from your application program via the PLCnext Engineer file function blocks, for example.

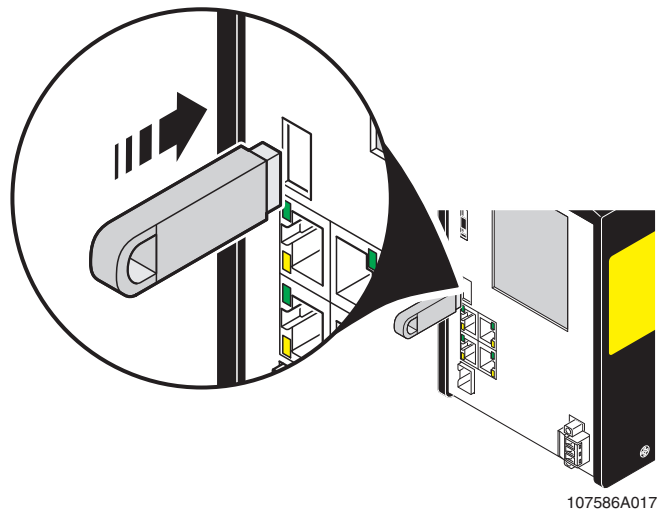


Figure 2-30 USB interface of the RFC 4072S



NOTE: Potential RFC 4072S malfunction

A RFC 4072S malfunction can occur if the USB memory stick is inserted or removed while the RFC 4072S is supplied with power.

Only insert or remove the USB memory stick when the power supply of the RFC 4072S is switched off.

2.11 Interfaces

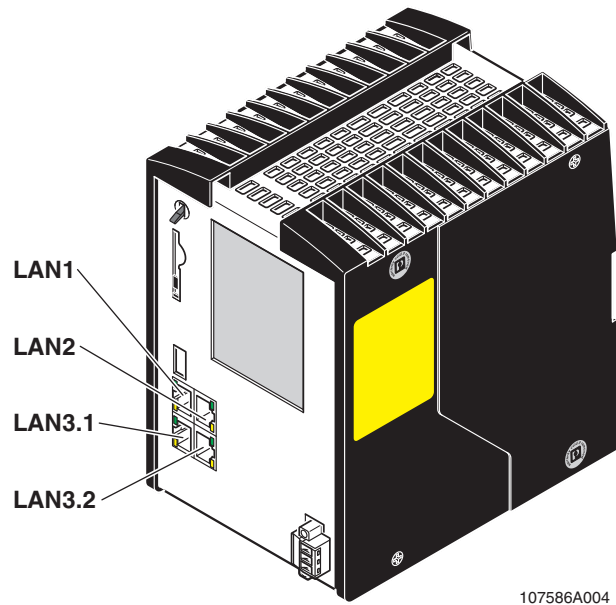


Figure 2-31 Interfaces of the RFC 4072S

107586A004

The RFC 4072S is equipped with the following interfaces:

Interfaces		Description
LAN1	1 x Ethernet	10/100/1000 BASE-T(X); PROFINET: controller interface function
LAN2	1 x Ethernet	10/100/1000 BASE-T(X)
LAN3.1/LAN3.2	2 x Ethernet	10/100/1000 BASE-T(X), internally switched; PROFINET: device interface function

2.11.1 Ethernet connection

Four standardized Ethernet interfaces are available for connecting the Ethernet network.

The LAN1 and LAN2 interfaces are each assigned a separate MAC address. A common MAC address is assigned to the LAN3.1 and LAN3.2 interfaces that are switched device-internally.

LAN1 is preconfigured as the PROFINET controller interface. The LAN3.1 and LAN3.2 interfaces are preconfigured as the device interface.

**Operating the RFC 4072S as a PROFINET device (firmware version: 2019.0 LTS)**

If you are operating the RFC as a PROFINET device via the LAN3.1 or LAN3.2 interface, avoid disconnecting and connecting the Ethernet cable during runtime. Otherwise, the RFC must be restarted to reestablish the application relationship with the higher-level PROFINET controller.



More detailed information on the interfaces:

IP address assignment: [Section “Configuring the controller IP settings” on page 101](#).

The Ethernet network is connected via an RJ45 socket.



Use Ethernet cables according to CAT5 of IEEE 802.3 for operation with up to 100 Mbps. Please note that for operation with 1000 Mbps (Gigabit), cables with four wire pairs (twisted pairs, eight wires in total), which at least meet the requirements of CAT5e, must be used.

When working on PROFINET/PROFIsafe and its components, the following documents must always be available and observed at all times.

- PROFINET Installation Guideline for Cabling and Assembly
- PROFIsafe System Description
- PROFIBUS Guideline, PROFIsafe Policy
- PROFIsafe – Environmental Requirements Guideline

These documents are available on the Internet at www.profinet.com or you can contact your local Phoenix Contact representative regarding these documents (see also [Section “Documentation” on page 246](#)).

Please also observe the relevant information on PROFINET and PROFIsafe, which is available on the Internet at www.profisafe.net.

For the interface assignment, please refer to [“Ethernet interfaces” on page 252](#).

2.11.2 Connection example of the Ethernet interfaces

At present the RFC 4072S supports the following connection in a PROFINET system.

In the following example, the RFC 4072S is operated as a lower-level PROFINET device connected to a higher-level PROFINET controller (optional). In this case, the connection is established via the LAN3.2 interface. To operate the RFC 4072S as a PROFINET controller, PROFINET devices are connected to the LAN1 interface (see [Figure 2-32](#)).

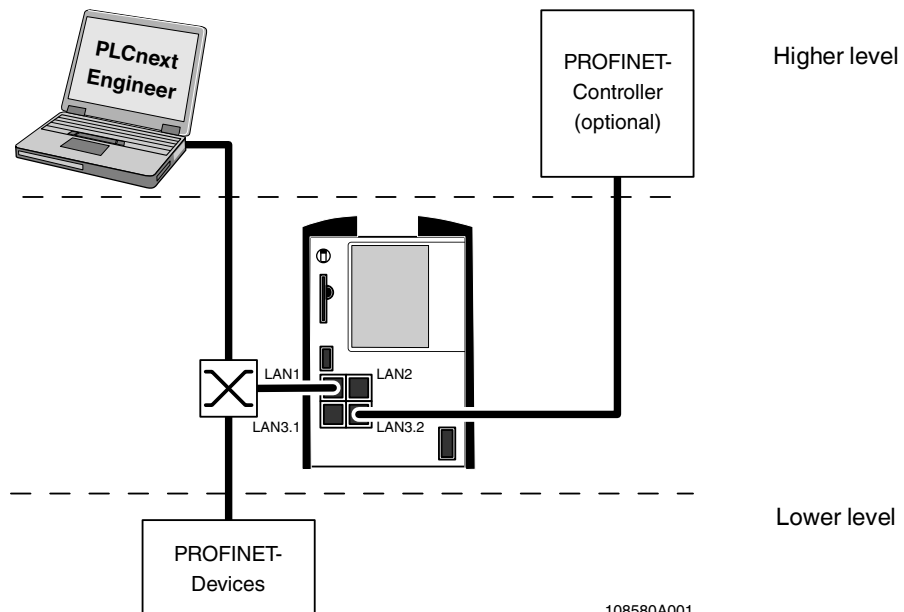


Figure 2-32 PROFINET example installation



A PC can be operated on each Ethernet interface of the RFC. Depending on the configuration of the interfaces, this may not be possible in individual cases (see [Section "Ethernet connection" on page 68](#)).



Please note:

- The IP addresses of interfaces LAN1 / LAN2 / LAN3.1/3.2 must be in different subnets.
- The PROFINET controller function of the RFC is available at interface LAN1. This interface must then be assigned an IP address if the PROFINET controller function of the device is to be used in the application.
- An IP address must be assigned to interfaces LAN3.1/3.2 if you want to use the PROFINET device function of the RFC at either of these interfaces.
- The LAN2 and LAN3.1/3.2 interfaces do not necessarily have to be assigned an IP address if, for example, communication between a PC with PLCnext Engineer and the RFC is also implemented via the LAN1 interface. Nevertheless, we recommend that appropriate IP addresses are assigned to all interfaces.

2.12 Mode selector switch

The mode selector switch is used to define the operating state of the standard controller. The mode selector switch does not influence the operating state of the safety-related PROFINET controller (SPNS).

The RUN/PROG and STP (STOP) positions have a toggle button function, and the MRESET position has a pushbutton function. After the switch has been released in the MRESET position, it returns to the STOP position.

Table 2-10 Operating modes of the RFC

Operating mode	Explanation
RUN/PROG	<p>The application program of the standard controller is in the “Run” state.</p> <p>The PLCnext Engineer software can be used for program and configuration modifications.</p> <p>The monitoring and online functions can be used.</p>
STOP	<p>The application program of the standard controller is in the “Stop” state.</p> <div style="border: 1px solid black; padding: 5px;"> <p>WARNING: PROFIsafe process data exchange interrupted</p> <p>If the operating mode switch is in the STOP position, process data between F-Host and F-Devices is not exchanged in the network via PROFIsafe. The F-Devices assume the safe state (failure state) after the defined watchdog time has expired.</p> </div>
MRESET	<p>The application program in the RAM of the standard controller is deleted. In addition, the retain data is deleted.</p> <div style="border: 1px solid black; padding: 5px;"> <p>WARNING: PROFIsafe process data exchange interrupted</p> <p>If the MRESET function is executed, process data is not exchanged between the F-Host and F-Devices in the network via PROFIsafe. The F-Devices assume the safe state (failure state) after the defined watchdog time has expired.</p> </div> <p>Set the mode selector switch in the following sequence:</p> <ul style="list-style-type: none"> • Hold the switch in the MRESET position for three seconds. • Release the switch for less than three seconds. • Hold the switch in the MRESET position for three seconds.

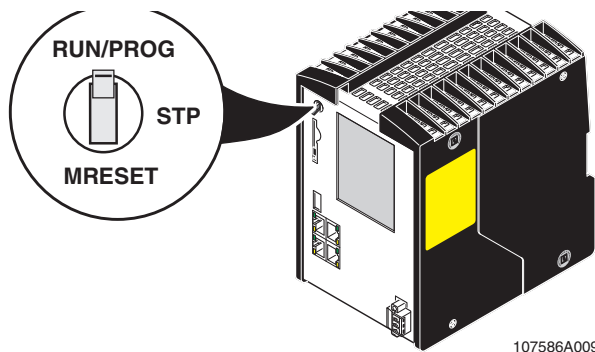


Figure 2-33 Mode selector switch

2.13 Power supply

2.13.1 Sizing of the power supply

A power supply with an output current of at least 5.0 A or higher is recommended for operating the RFC.



A **power supply without a fall-back characteristic curve** must be used for correct operation of the RFC (see [Figure 2-35 on page 72](#)). When the RFC is switched on, an increased inrush current temporarily occurs. The RFC behaves like a capacitive load when it is switched on.

Make sure the power supply and the externally required fuse are compatible. The power supply must be able to temporarily provide the tripping current. Observe the information in Section ["Technical data"](#) on ["Power supply"](#) from [page 237](#).



WARNING: Loss of electrical safety and the safety function when using unsuitable power supplies

The RFC 4072S is designed exclusively for protective extra-low voltage (PELV) operation in accordance with EN 60204-1. Only PELV in accordance with the listed standard may be used for the supply.

The following applies to the PROFINET network and the I/O devices used in it:

Only use power supplies that meet EN 61204 and feature safe isolation and PELV according to IEC 61010-2-201 (PELV). These prevent short circuits between primary and secondary sides.

Please also observe the information in [Section "Electrical safety" on page 16](#).

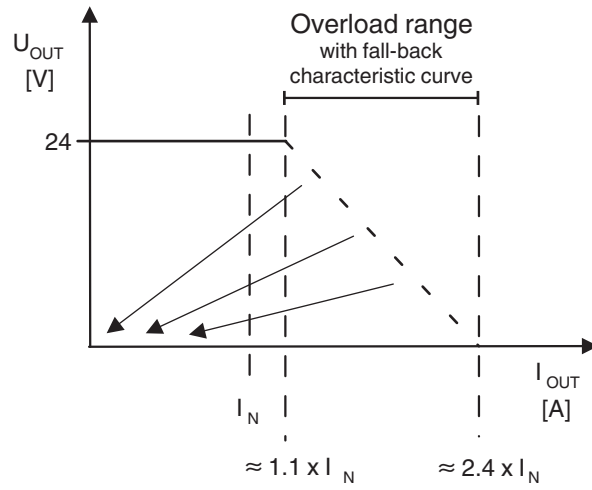
Some electronically controlled power supplies have a fall-back characteristic curve (see [Figure 2-34 on page 72](#)). They are not suitable for operation with capacitive loads.

The following power supply (without fall-back characteristic curve) is recommended for operating the RFC:

- Primary-switched power supply QUINT POWER with SFB technology:
QUINT4-PS/1AC/24DC/20/+ Order No. 2904617

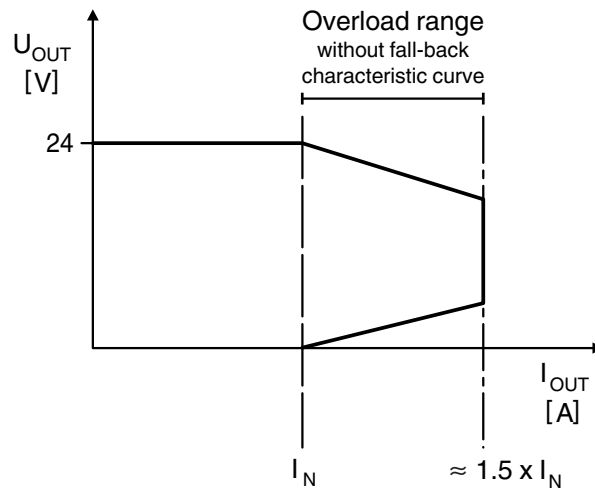


Other power supplies can be used as an alternative. For examples of suitable Phoenix Contact power supplies, please refer to ["Accessories" on page 245](#).



6219B070

Figure 2-34 Overload range with fall-back characteristic curve



6219B071

Figure 2-35 Overload range without fall-back characteristic curve

2.14 Directory structure of the file system

The RFC 4072S controller works with a Linux operating system. You can access the controller via SFTP or via SSH and view the directories and files on the file system (on the SD card) and modify them as necessary.

Directories and files that are provided by Phoenix Contact (also through firmware updates) are stored in the parameterization memory of the RFC 4072S.

If you make changes to the directories or files, the Linux operating system generates an overlay file system.

The overlay file system is generated on the SD card.

Settings that you have configured yourself (e.g., network configuration, project bus configuration, PLCnext Engineer project, etc.) are also saved to the SD card.

Table 2-11 Storage of firmware components in the root file system

Directory in the root file system	Description
/usr/local/lib	Directory for storing additional open source libraries that are used by customized C++ programs. Further information on programming the controller with C++ can be found in the PLCnext Community at plcnext-community.net .
/usr/share/common-licenses	License information on the individual Linux packages of the controller
/opt/plcnext	Home directory of the "admin" Linux user and working directory of the device firmware Files written by the application program are stored in this directory if the specified file name does not contain a storage path.
/opt/plcnext/logs	Directory for storing the log files of the Diagnostic Logger as well as the database of the Notification Logger This directory contains the output.log file. It contains information on the startup behavior of the firmware, status and error messages as well as warning notes that help you find the source of error.
/opt/plcnext/projects	Directory for storing project directories and files
/opt/plcnext/projects/PCWE	Directory for storing PLCnext Engineer projects All files and subdirectories in this directory are managed exclusively by PLCnext Engineer. <ul style="list-style-type: none"> Do not make any changes to this directory.
/opt/plcnext/Security	Directory for storing certificates of the IdentityStores and TrustStores
/opt/plcnext/Security/Certificates/https	Directory for storing HTTPS certificates For additional information on the exchange of HTTPS certificates, please refer to Section "Replacing HTTPS certificate" on page 249 .

Table 2-11 Storage of firmware components in the root file system

Directory in the root file system	Description
/opt/plcnext/Security/TrustStores	<p>Directory for storing the TrustStores configured in WBM</p> <p>Each subdirectory corresponds to the name of a TrustStore.</p> <p>A TrustStore directory contains the following subdirectories:</p> <ul style="list-style-type: none"> – trusted: The directory contains CA certificates that are trusted. – issuers: The directory contains CA certificates that are not automatically trusted but that are required for creating a certificate chain. – trusted/crl: The directory contains files with Certificate Revocation Lists (CRL) for the CA certificates. – issuers/crl: The directory contains files with Certificate Revocation Lists (CRL) for issuer certificates.
/opt/plcnext/Security/IdentityStores	<p>Directory for storing the IdentityStores configured in WBM</p> <p>Each subdirectory corresponds to the name of an IdentityStore. An IdentityStore contains identities (X.509 certificates with the corresponding private key).</p> <p>An IdentityStore directory contains the following files:</p> <ul style="list-style-type: none"> – certificate.pem: The file in PEM format contains the X.509 certificate of the identity. The file may additionally contain several certificates of the certificate chain. – key.pem: The file in PEM format contains the private key for the certificate. – tpmkey.pem: The file contains the private key linked to the TPM (Trusted Platform Module) of the controller.
/opt/plcnext/apps	<p>All active apps downloaded from the PLCnext Store to the controller are mounted in this directory.</p> <p>Each active app is mounted with the name of the app identifier in a subdirectory. The entire content of the app container is available in this directory (read-only).</p> <p>The directory is managed by the PLCnext Store.</p> <ul style="list-style-type: none"> • Do not make any changes to this directory.
/opt/plcnext/installed_apps	<p>Directory for storing all installed app containers</p> <p>The directory belongs to the PLCnext Store.</p>
/opt/plcnext/appshome	<p>Directory for storing and managing app data</p> <p>The directory is managed by the PLCnext Store and the installed apps.</p> <ul style="list-style-type: none"> • Do not make any changes to this directory.
/opt/plcnext/ltng	<p>Directory for storing the default configuration files for tracing via LTTng</p>

Table 2-11 Storage of firmware components in the root file system

Directory in the root file system	Description
/opt/plcnext/ltng_traces	<p>Directory for storing trace files</p> <p>The directory is created during runtime of the trace controller when the trigger function for storing the trace files is called for the first time. Each time the trigger function of the memory is called, a new subdirectory (trace directory) for storing the current trace data is created.</p> <p>The designation of a trace directory is structured as follows: YYYYMMDD_hhmmss E.g.: /opt/plcnext/ltng_traces/20190418_190615/<trace_data></p> <p>The memory functions as a ring memory. If the configured maximum memory space is exceeded, the respectively oldest trace directory is deleted.</p>
/opt/plcnext/backup	<p>Directory download change operations</p> <p>The directory is used for creating a backup of the project directory. In the event of an error, the content of the backup directory is restored. The backup directory is created following the first successful project download and following every successful project download.</p>
/opt/plcnext/retaining	<p>Directory for managing residual data</p>
/opt/plcnext/shadowing	<p>Directory for internal storage of copies of C++ user libraries that have been configured in PLCnext Engineer and downloaded to the controller.</p>
/opt/plcnext/profinet	<p>Directory for storing temporary PROFINET files.</p>

2.15 Using SFTP to access the file system

The file system (on the parameterization memory of the RFC 4072S) is accessed via the SFTP protocol. SFTP client software is required for this (e.g., WinSCP).

Access to the file system via SFTP requires authentication with a user name and password.



Please note:

Authentication via a user name and password is **always** required for SFTP access and cannot be deactivated.

Only users with administrator rights can access the file system.

You can create additional users with administrator rights in Web-based management of the RFC 4072S via the User Manager, see [Section ““User Authentication” page” on page 220](#).

The following access data is set by default with administrator rights:

User name: admin

Password: printed on the controller (see [Figure 2-36](#)).



Figure 2-36 Administrator password on the controller

2.16 Firewall



The firewall of the RFC 4072S is deactivated by default.

Recommended:

- Activate the firewall.

Please note:

If you use the RFC 4072S as a PROFINET controller, you must authorize all incoming connections via all UDP ports if the firewall is activated. Otherwise, establishing a connection to PROFINET devices is not possible.

3 Mounting, removal, electrical installation, and replacement

3.1 Safety notes for mounting and removal



Only qualified personnel must pack and unpack the RFC 4072S while observing the following ESD regulations.



WARNING: Loss of electrical safety and the safety function when using unsuitable power supplies

The RFC 4072S is designed exclusively for protective extra-low voltage (PELV) operation in accordance with EN 60204-1. Only PELV in accordance with the listed standard may be used for the supply.

The following applies to the PROFINET network and the I/O devices used in it:

Only use power supplies that meet EN 61204 and feature safe isolation and PELV according to IEC 61010-2-201 (PELV). These prevent short circuits between primary and secondary sides.

Please also observe the information in [Section “Electrical safety” on page 16](#).



NOTE: Electrostatic discharge!

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-1.



WARNING: Unintentional machine startup

Do not mount or remove the RFC 4072S while the power is connected.

Make sure the entire system is reassembled before switching the power back on. Observe the diagnostic indicators and any diagnostic messages.

The system may only be started provided neither the device nor the system poses a hazard.



Observe the PROFINET Installation Guideline for Cabling and Assembly

Observe the PROFINET Installation Guideline for Cabling and Assembly when mounting and installing the RFC 4072S.

Observe the corresponding information in the Installation Guideline for Cabling and Assembly and in the “Functional Earthing and Shielding of PROFIBUS and PROFINET” document for the grounding concept in particular.

Both documents can be downloaded at www.profinet.com or you can contact your nearest Phoenix Contact representative regarding the two documents.



Only mount the device on DIN rails in accordance with DIN EN 60715 (TH 35-15 DIN rail, e.g., NS 35/15... from Phoenix Contact).

Degree of protection of the device when mounted: IP20.

To ensure correct operation, the device mounted on a DIN rail must be installed in a housing or a control cabinet with at least IP54 protection.



Shielding

The shielding ground of the connected twisted pair cables is electrically connected to the RJ45 socket of the RFC 4072S. When connecting network segments, avoid ground loops, potential transfers, and equipotential bonding currents via the braided shield.



NOTE:

Please observe the following notes when using a shield connection clamp.

- Ensure the cable shields for Ethernet are correctly secured in the connectors and when routing a cable through a control cabinet.
- Only use shielded data cables. As much of the shield as possible must be connected to the ground on both sides.
- Immediately following entry in the control cabinet or housing, connect as much of the cable shield as possible to a shield/protective conductor bar and secure the shield with a cable clamp. Route the shield to the module without interruption; but do not connect it to the ground again when connecting it there.
- The connection between the shield/protective conductor bar and the control cabinet/housing must have no impedance.
- Only use metal or metal-plated connector housings for shielded data cables.

3.2 Mounting the RFC FAN MODULE fan module



Attach the fan module to the RFC before placing the Remote Field Controller on the DIN rail.

Mount the fan module to the bottom of the RFC using the four screws, as shown in [Figure 3-1](#).

- Position the fan module on the bottom of the RFC according to [Figure 3-1](#).
- Make sure that the COMBICON connector and the four screws fit properly. Upon delivery of the fan module, the four screws are premounted in the fan module housing.
- Tighten all four M4 screws equally using a recommended tightening torque of 2.2 Nm (3 Nm, maximum) so that they cannot loosen accidentally (e.g., due to vibration).

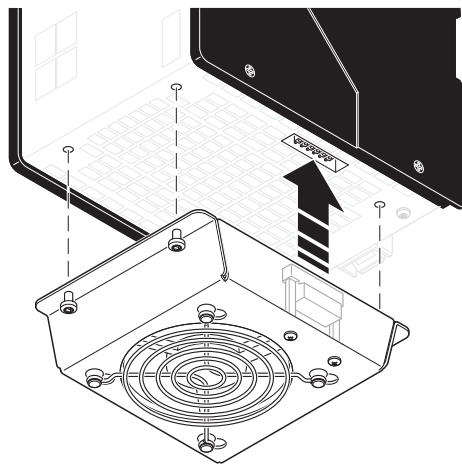


Figure 3-1 Mounting the RFC FAN MODULE fan module

3.3 Mounting the RFC 4072S

Mount the RFC 4072S on 35 mm standard DIN rails with a height of 15 mm (for ordering data, see [Section “Accessories” on page 245](#)). The distance between the DIN rail fastening points must not exceed 160 mm (see [Figure 3-3 on page 81](#)).



To avoid contact resistance only use clean, corrosion-free DIN rails. Before mounting the devices, an end bracket should be mounted to the left of the RFC 4072S to stop the devices from slipping on the DIN rail. The end bracket should only be mounted on the right-hand side once the RFC 4072S has been mounted.

The following end brackets can be used:

- E/NS 35N (Order No. 0800886, fixed using a screw)
- CLIPFIX 35 (Order No. 3022218, snapped on without using tools)
- E/UK (Order No. 1201442, fixed using screws)



NOTE: Overheating of the RFC possible

When installing the RFC make sure that the vents can be freely accessed. Otherwise, the RFC may overheat. To ensure good ventilation, leave a gap of more than 10 cm above and below the RFC.

Do not install devices below the RFC 4072S that could additionally heat the RFC 4072S up.



If you wish to operate the RFC with the RFC FAN MODULE fan module (Order No. 2404085), you must mount the fan module first, before mounting the RFC on the DIN rail. Please refer to the instructions in [Section “Mounting the RFC FAN MODULE fan module” on page 79](#)

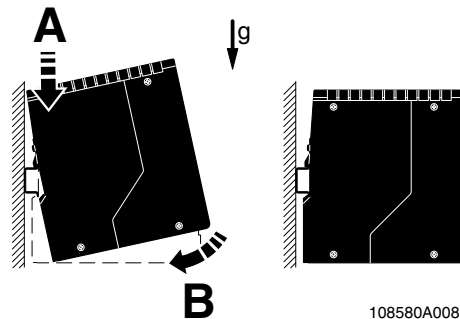


Figure 3-2 Mounting the RFC 4072S

- Place the RFC onto the DIN rail from above (A in [Figure 3-2](#)).
- Tilt the RFC downwards until the spring-loaded holder on the back of the device snaps into place with a click (B).
- Finally, make sure that the RFC is securely mounted on the DIN rail.

The following [Figure 3-3](#) shows the RFC 4072S which is mounted on a DIN rail in its standard installation position.

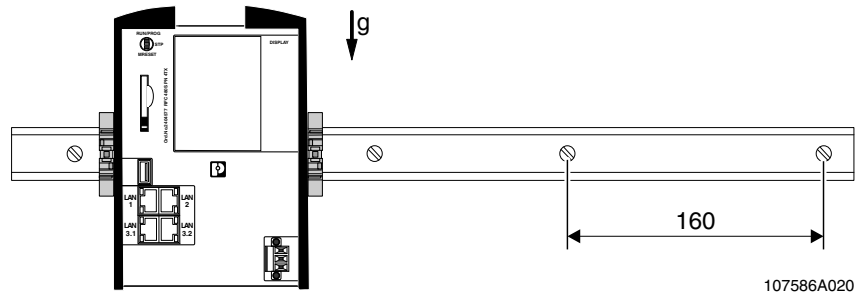


Figure 3-3 Mounted RFC 4072S with end brackets and maximum distance between the DIN rail fastening points (160 mm)

3.4 Removing the RFC 4072S

To remove the device, follow the instructions in [Section “Replacing the RFC 4072S” on page 85](#) up to step 5.

3.5 Inserting/removing the SD card (parameterization memory)



NOTE: Please note that the SD card may not be inserted or removed during operation. If the SD card is removed/inserted during operation, the RFC 4072S will switch to the safe state (failure state).

Always disconnect the power supply to the RFC 4072S before inserting or removing the SD card.



The SD card is recognized during initialization of the RFC 4072S. Make sure that the SD card has been inserted before switching on the RFC 4072S to enable the device to use it.



NOTE: SD card (parameterization memory) – formatting note

The SD card is already formatted and is intended for use with Phoenix Contact devices. Make sure that the SD card is not reformatted outside the RFC 4072S.

Inserting (A) and removing (B) the SD card is graphically shown in [Figure 3-4](#).



NOTE: Potential damage to the device

When inserting the SD card, make sure that it is located in the guide rails on both sides of the card holder.

To prevent damage to the device, make sure that the SD card is properly aligned and never forced into the slot.

Inserting the SD card

- Insert the SD card in the slot provided with the contact strip to the front (A). When pressed lightly, the SD card snaps into place.

Removing the SD card

- Push the ejector downwards (B1).
The SD card moves out of the slot (B2).
- Remove the SD card.

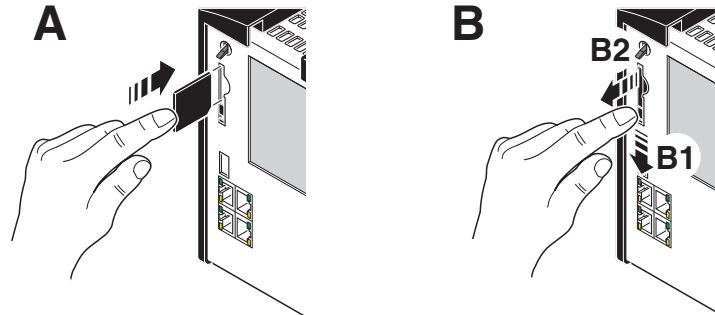


Figure 3-4 Inserting (A) or removing (B) the SD card (parameterization memory)

Replacing the SD card

- Remove the SD card to be exchanged according to the above description.
- Then insert the replacement SD card.

3.6 Inserting/removing the USB memory stick



NOTE: Potential RFC 4072S malfunction

A RFC 4072S malfunction can occur if the USB memory stick is inserted or removed while the RFC 4072S is supplied with power.

Only insert or remove the USB memory stick when the power supply of the RFC 4072S is switched off.

Procedure

- Switch off the supply voltage of the RFC 4072S.
- Insert the USB memory stick into the USB socket of the RFC 4072S.
- Or
- Remove the USB memory stick from the USB socket of the RFC 4072S.
- Switch on the supply voltage of the RFC 4072S.

3.7 Connecting the interfaces

3.7.1 Connecting an Ethernet network

- Connect the Ethernet cable to the Ethernet interface (RJ45 sockets: LAN1, LAN2 or LAN3.1/3.2) of the RFC 4072S.

The cable connects the RFC 4072S to a higher-level or lower-level Ethernet network.

- Use Ethernet cables according to CAT5 of IEEE 802.3 for operation with up to 100 Mbps. (LAN1, LAN2, LAN3.1, LAN3.2)
- For operation with 1000 Mbps (Gigabit), cables with four wire pairs (twisted pairs, eight wires in total), which at least meet the requirements of CAT5e, must be used. (LAN1, LAN2)



Observe the information on the Ethernet interfaces of the device in [Section “Ethernet connection” on page 68](#)

For the ordering data for the Ethernet cable, please refer to [Section “Ordering data” on page 244](#).

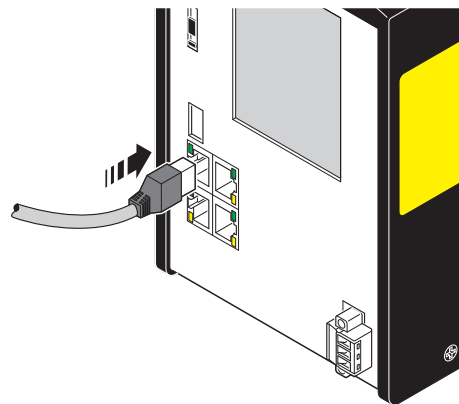


Figure 3-5 Cabling between an Ethernet network and the RFC 4072S

3.8 Connecting the supply voltage

The RFC 4072S is operated using 24 V DC voltage.



WARNING: Loss of electrical safety and the safety function when using unsuitable power supplies

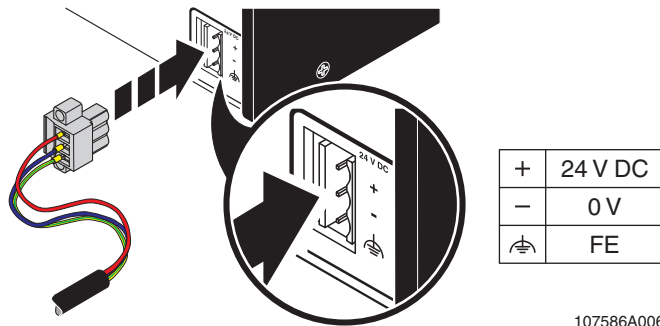
The RFC 4072S is designed exclusively for protective extra-low voltage (PELV) operation in accordance with EN 60204-1. Only PELV in accordance with the listed standard may be used for the supply.

The following applies to the PROFINET network and the I/O devices used in it:

Only use power supplies that meet EN 61204 and feature safe isolation and PELV according to IEC 61010-2-201 (PELV). These prevent short circuits between primary and secondary sides.

Please also observe the information in [Section "Electrical safety" on page 16](#).

The RFC is supplied from an external power supply (24.0 V DC). The permissible voltage ranges from 19.2 V DC to 30.0 V DC (ripple included).



107586A006

Figure 3-6 Connecting the supply voltage



Please note that the RFC 4072S requires approximately two minutes to start up. This is due to the comprehensive selftests the device must perform. The status is indicated on the display.

3.9 Replacing the RFC 4072S



NOTE: The following tasks must be carried out prior to mounting:

- Disconnect the supply voltage
- Make sure that the supply voltage cannot be switched on again by unauthorized persons



Only qualified personnel should pack and unpack the device while observing the ESD regulations in [Section 1.7, "Electrical safety"](#).

Only replace the device with a device of the same hardware/firmware version or with a compatible device approved by Phoenix Contact. Information on compatible devices can be found on the Internet at phoenixcontact.com.



WARNING: Unintentional machine startup

Do not replace the RFC 4072S while the power is connected.

Do not remove the device until:

- The device has been disconnected from the power supply and it is ensured that it cannot be switched on again
- The COMBICON connector (supply voltage) has been removed
- The Ethernet cable connector/s has/have been removed
- The USB stick (if present) has been removed

1. Switch off the power supply to the RFC.
2. Unplug the supply cable from the RFC.

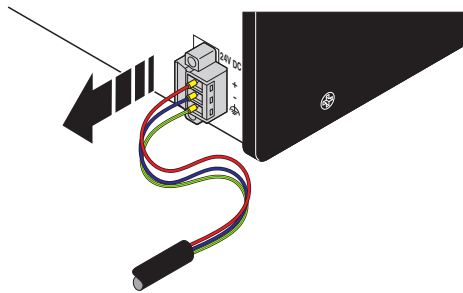


Figure 3-7 Removing the power supply

3. If present, disconnect the Ethernet connection.

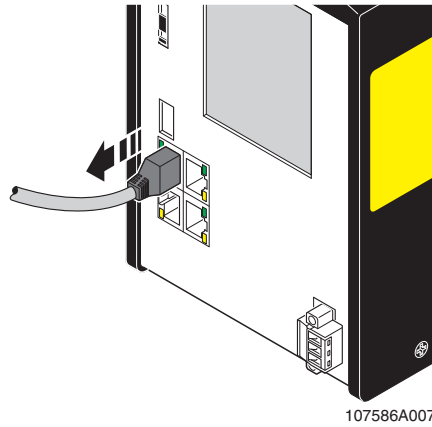


Figure 3-8 Disconnecting the Ethernet connection

4. Remove the RFC to be replaced from the DIN rail.

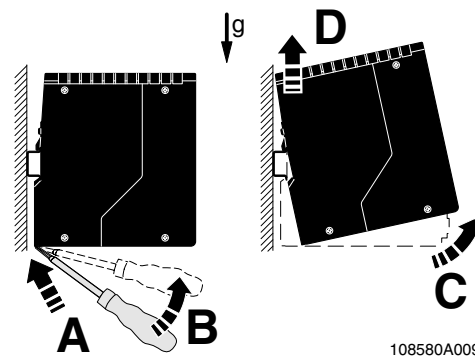


Figure 3-9 Removing the RFC from the DIN rail



If the fan module is mounted to the RFC, proceed as follows:

5. Unscrew the four screws used to fix the fan module to the bottom of the RFC. Make sure that the fan module does not fall down after unscrewing the screws.

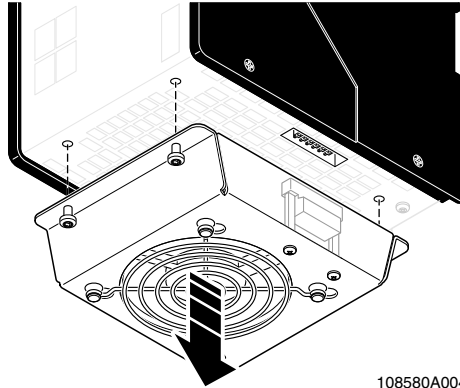


Figure 3-10 Removing the fan module

6. Take the replacement device out of its packaging.



If you wish to operate the replacement device with the fan module, proceed as follows:

7. Mount the fan module to the bottom of the RFC using the four screws, as shown in [Figure 3-11](#).
 - a) Position the fan module on the bottom of the RFC according to [Figure 3-11](#). Make sure that the COMBICON connector is fitted properly.
 - b) Tighten all four M4 screws equally using a recommended tightening torque of 2.2 Nm (3 Nm, maximum) so that they cannot loosen accidentally (e.g., due to vibration).

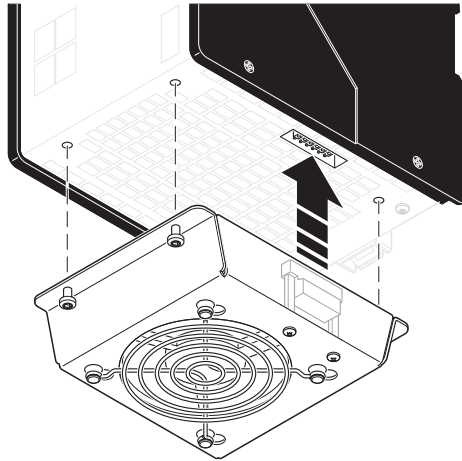


Figure 3-11 Mounting the RFC FAN MODULE fan module

8. Mount the replacement device according to [Section “Mounting the RFC 4072S” on page 80](#). Make sure that the device is secured on the DIN rail.
9. Snap the RFC onto the DIN rail and check that it is securely locked in place (see [Figure 3-12](#)).

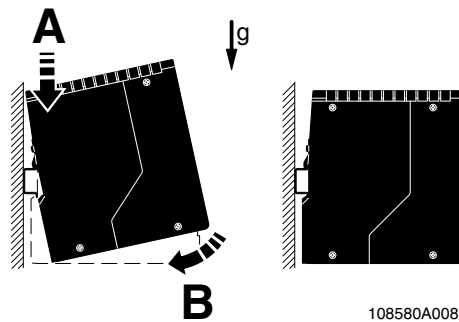


Figure 3-12 Snapping the RFC onto the DIN rail

10. Remove the parameterization memory from the device that was replaced and insert it in the replacement device. See [Section "Inserting/removing the SD card \(parameterization memory\)" on page 81](#).
11. Connect the Ethernet cable, if present.

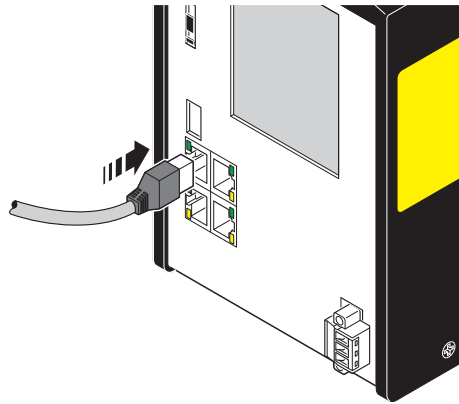


Figure 3-13 Establishing the Ethernet connection

12. Connect the power supply with the RFC.



Figure 3-14 Connecting the power supply



WARNING: Do not connect the RFC 4072S supply voltage yet.

Take appropriate measures to ensure that your machine/system does not present any danger for the time specified in the validation plan for the machine/system and for the validation measures to be carried out when replacing the RFC 4072S.

13. When restarting the RFC 4072S after replacement, first carry out the appropriate measures specified in the validation plan for the machine/system. Follow the instructions and corresponding notes in [Section "Restart after replacing the RFC 4072S" on page 94](#).

4 Startup and validation


WARNING:

Take appropriate measures to ensure that your system/machine does not present any danger during startup and validation.


WARNING:

The planned system/machine safety function is only available following validation.

4.1 Initial startup

The following information starting up the RFC 4072S must be observed.

- Familiarization with the previous sections of this user manual is essential in order to carry out the steps listed in the following table correctly. Therefore, if you have not done so already, please read the previous sections carefully. The section in the appendix of this user manual which corresponds to the previous sections must also be observed.
- The RFC 4072S starts up immediately:
 - After power up, if a parameterization memory (SD card) with a valid project is inserted.
 - After a download from PLCnext Engineer, if you have selected the corresponding option: “Write and Start Project (Project Changes)”.

With appropriate safety-related programming, the safety function is active immediately after the startup phase of the SPNS, and the outputs of the F-devices and the outputs of the non-safety-related PROFINET devices and I/O devices (e.g., Axioline F or Inline modules) can be set depending on the programming.

For initial startup, proceed as described in [Table 4-1](#).



The following table describes all the steps from unpacking the RFC 4072S through mounting/installation to startup.

Table 4-1 Steps for initial startup of the RFC 4072S

Step	Relevant section and literature
Remove the device from the packaging while observing the ESD regulations.	Section “Safety notes for mounting and removal” on page 77
Mount the device in accordance with your application.	Section “Mounting the RFC 4072S” on page 80
Insert the parameterization memory.	Section “Inserting/removing the SD card (parameterization memory)” on page 81
Connect the device to an Ethernet network.	Section “Connecting an Ethernet network” on page 83

Table 4-1 Steps for initial startup of the RFC 4072S






Step	Relevant section and literature
Connect the power supply to the device.	<ul style="list-style-type: none"> - Notes on using PELV power supplies in Section “Electrical safety” on page 16 - Section “Connecting the supply voltage” on page 84
<div style="border: 1px solid black; padding: 5px;">  <p>Make sure that the PROFINET devices and F-Devices used in your application have been mounted and installed correctly before switching on the supply voltage.</p> </div>	
Switch on the power supply to the device.	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">  <p>WARNING: Take appropriate measures to ensure that your system/machine does not present any danger during startup and validation.</p> </div> <div style="border: 1px solid black; padding: 5px;">  <p>WARNING: The planned system/machine safety function is only available following validation.</p> </div>
<div style="border: 1px solid black; padding: 5px;">  <p>Please note that the RFC 4072S requires approximately two minutes to start up. This is due to the comprehensive selftests the device must perform. The status is indicated on the display.</p> </div>	
<div style="border: 1px solid black; padding: 5px;">  <p>The following steps must be performed in the PLCnext Engineer software. When carrying out the following steps, please refer to the online help of the software. The online help assists you in programming and parameterizing the PLCnext Engineer software.</p> </div>	
Carry out all the steps in order to integrate the device as a PROFINET controller in a PLCnext Engineer project.	<ul style="list-style-type: none"> - Online help for PLCnext Engineer - Section “Integration of the RFC 4072S in PLCnext Engineer as a PROFINET controller” on page 97
Assign the necessary IP address settings for your application to the device.	Section “Configuring the controller IP settings” on page 101
Check the PROFINET controller settings and adapt the settings, if necessary.	
You can operate the RFC 4072S concurrently as a PROFINET controller and PROFINET device. Send your settings to the controller.	Section “Important information” on page 101
Create the bus configuration in PLCnext Engineer.	Section “Adding PROFINET devices” on page 108
Assign a PROFINET device name for the connected devices (device naming).	Section “Assigning online devices (device naming)” on page 109
In PLCnext Engineer, set the F_Source_Address (F_Source_Add) and the F_Destination_Addresses (F_Dest_Add) that are set on the safe F-Devices.	

Table 4-1 Steps for initial startup of the RFC 4072S

Step	Relevant section and literature
Check the settings for management/diagnostic variables and adapt the settings, if necessary.	<ul style="list-style-type: none"> – Section “Description of the safety-related functioning of the RFC 4072S” on page 27 – Section “Management/diagnostic variables for F-Devices” on page 129 – Section “Management/diagnostic variables for each configured F-Device” on page 191 – Section “Global management/diagnostic variables for F-Devices” on page 195
Specify a new project password.	Section: “Defining a project password” on page 104
Create the variables for the devices for process data exchange.	
Link the created variables to the process data according to your application.	

**WARNING: Safety-related steps**

The following steps include safety-related operations in the PLCnext Engineer software and the safety validation of the PROFIsafe system.

For the following steps, please also observe the checklists in [Section C, “Appendix: checklists”](#).

In addition, refer to the online help for the PLCnext Engineer software.

Carry out the necessary device parameterization in the PLCnext Engineer software.	Section “Programming in accordance with IEC 61131-3 – Safety-related example program” on page 127
Check the bus configuration and variable assignment (exchange variables).	
Specify a new controller password.	Section: “Defining a controller password for the safety-related controller” on page 142
Carry out the validation using the checklist ““Initial startup” and “restart/device replacement” validation” on page 267.	Section “Appendix: checklists” on page 257

**WARNING: Carry out verification in accordance with safety standards**

Carry out verification for all the steps involved in creating the safety program for your application in accordance with the applicable safety standards for your application.

4.2 Restart after replacing the RFC 4072S



The device does not have to be parameterized again following a restart (see [Table 4-1 “Steps for initial startup of the RFC 4072S”](#)). If a parameterization memory is inserted, which contains the configuration project created for your application, the configuration is still available after successful startup of the device. However, your application must not have been modified.

The area for safety-related programming in PLCnext Engineer supports you during the necessary verification process with the aid of a CRC checksum of the safety-related project (refer to the online help for PLCnext Engineer).

To restart the device after it has been replaced, proceed as described in [Table 4-2](#). Make sure that:

- The device to be replaced has been removed from the application
- The parameterization memory of the device to be replaced has been removed



Table 4-2 Steps for restarting the RFC 4072S

Step	Relevant section and literature
Remove the device from the packaging while observing the ESD regulations.	Section “Safety notes for mounting and removal” on page 77
Mount the device in accordance with your application.	Section “Mounting the RFC 4072S” on page 80
Insert the parameterization memory.	Section “Inserting/removing the SD card (parameterization memory)” on page 81
Connect the device to an Ethernet network.	Section “Connecting an Ethernet network” on page 83
Connect the power supply to the device.	<ul style="list-style-type: none"> – Notes on using PELV power supplies in Section “Electrical safety” on page 16 – Section “Connecting the supply voltage” on page 84



Make sure that the PROFINET and PROFIsafe devices used in your application have been mounted and installed correctly before switching on the supply voltage.

Table 4-2 Steps for restarting the RFC 4072S

Step	Relevant section and literature
Switch on the power supply to the device.	<div data-bbox="820 359 890 422" style="display: inline-block; vertical-align: top;"></div> <div data-bbox="916 359 1426 489" style="border: 1px solid black; padding: 5px; display: inline-block; vertical-align: top;"> <p>WARNING: Take appropriate measures to ensure that your system/machine does not present any danger during startup and validation.</p> </div> <div data-bbox="820 520 890 583" style="display: inline-block; vertical-align: top;"></div> <div data-bbox="916 520 1426 705" style="border: 1px solid black; padding: 5px; display: inline-block; vertical-align: top;"> <p>WARNING: The planned system/machine safety function is only available after the appropriate measures have been taken, which are specified in the validation plan of the machine/system for replacing the RFC 4072S.</p> </div>



Please note that the RFC 4072S requires approximately two minutes to start up. This is due to the comprehensive selftests the device must perform. The status is indicated on the display.

**Please note:**

- If a parameterization memory from the old device is used, which contains the configuration created for your application, only carry out the safety-related steps.
- If a parameterization memory with a valid project is not available, perform the steps for initial startup in this case.

**WARNING: Safety-related steps**

The following step includes the safety validation of the PROFIsafe system.

For the following step, please also observe the checklists in [Section C, "Appendix: checklists"](#).

Carry out the validation using the checklist ["Initial startup"](#) and ["restart/device replacement" validation](#) on page 267.

[Section "Appendix: checklists" on page 257](#)

**WARNING: Carry out verification in accordance with safety standards**

Carry out verification for all the steps involved in creating the safety program for your application in accordance with the applicable safety standards for your application.

4.3 Example startup of the RFC 4072S

4.3.1 Example of a PROFINET/PROFIsafe configuration with PROFINET controller/F-Host

To make your introduction to working with the RFC 4072S as straightforward as possible, the descriptions in later sections are based on the following PROFINET and PROFIsafe configuration. The RFC 4072S is used as a PROFINET controller and F-Host, which communicates with the devices of the lower-level Axioline F stations via PROFINET/PROFIsafe.



Lower-level PROFINET devices and PROFIsafe F-Devices

Please note that in principle you can use Axioline F and/or Inline bus couplers as well as the corresponding I/O devices and devices from other manufacturers as lower-level PROFINET devices and/or PROFIsafe F-Devices. In the following example, two Axioline F bus couplers are coupled to the RFC 4072S PROFINET controller on a lower level.

Example configuration

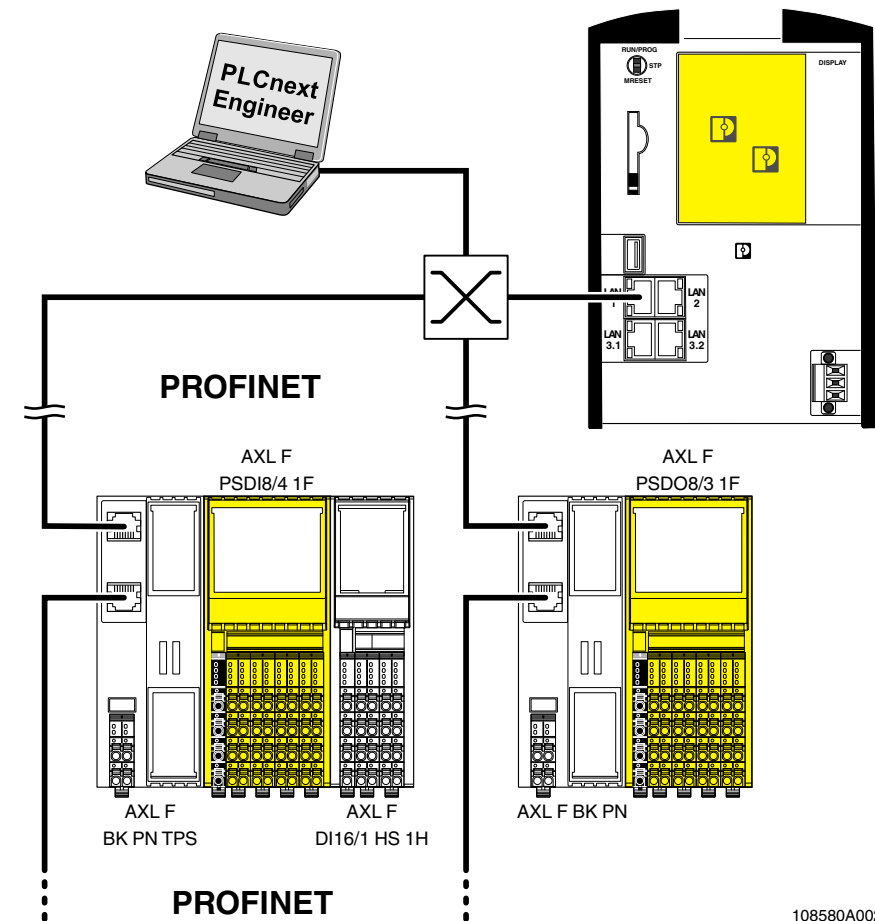


Figure 4-1 Example configuration

108580A002

4.3.2 Integration of the RFC 4072S in PLCnext Engineer as a PROFINET controller

The following sections describe how to:

- Create a new project in PLCnext Engineer.
- Assign IP addresses to the RFC.
- Read the PROFINET devices connected to the RFC.
- Program a non-safety-related and a safety-related project in PLCnext Engineer, including creating and linking variables.
- Configure F-Devices in PLCnext Engineer.
- Download the non-safety-related and safety-related project to the RFC.
- Start execution of the projects.



For the chronological sequence of the steps carried out, please refer to the example application.

This section assumes the following:

- You have installed the PLCnext Engineer software on your PC in accordance with the online help.
- You have installed the connected PROFINET devices and PROFIsafe F-Devices in accordance with the device-specific user documentation.



When carrying out the following steps, please refer to the online help of the PLCnext Engineer software. The online help assists you in programming and parameterizing the software.

4.4 Software requirements

4.4.1 PLCnext Engineer software



Detailed information on PLCnext Engineer and PLCnext Technology is available in the PLCnext Community at plcnext-community.net.

The PLCnext Engineer software is required for starting up the controller.

4.4.2 Installing PLCnext Engineer

The software can be downloaded at phoenixcontact.net/products.

- Download the software onto your PC.
- Double-click the executable “*.exe” file to start installation.
- Follow the instructions of the installation wizard.

4.4.3 PLCnext Engineer licenses

Once installed, a demo version of PLCnext Engineer is available for one-time use on a single PC.

- Go to phoenixcontact.net/product/1046008 to configure your desired software license and follow the instructions provided.

You must activate PLCnext Engineer via the Phoenix Contact Activation Wizard.

- Download the Phoenix Contact Activation Wizard at the link provided above.
- Follow the instructions in the Phoenix Contact Activation Wizard to activate your PLCnext Engineer license.

4.4.4 User interface

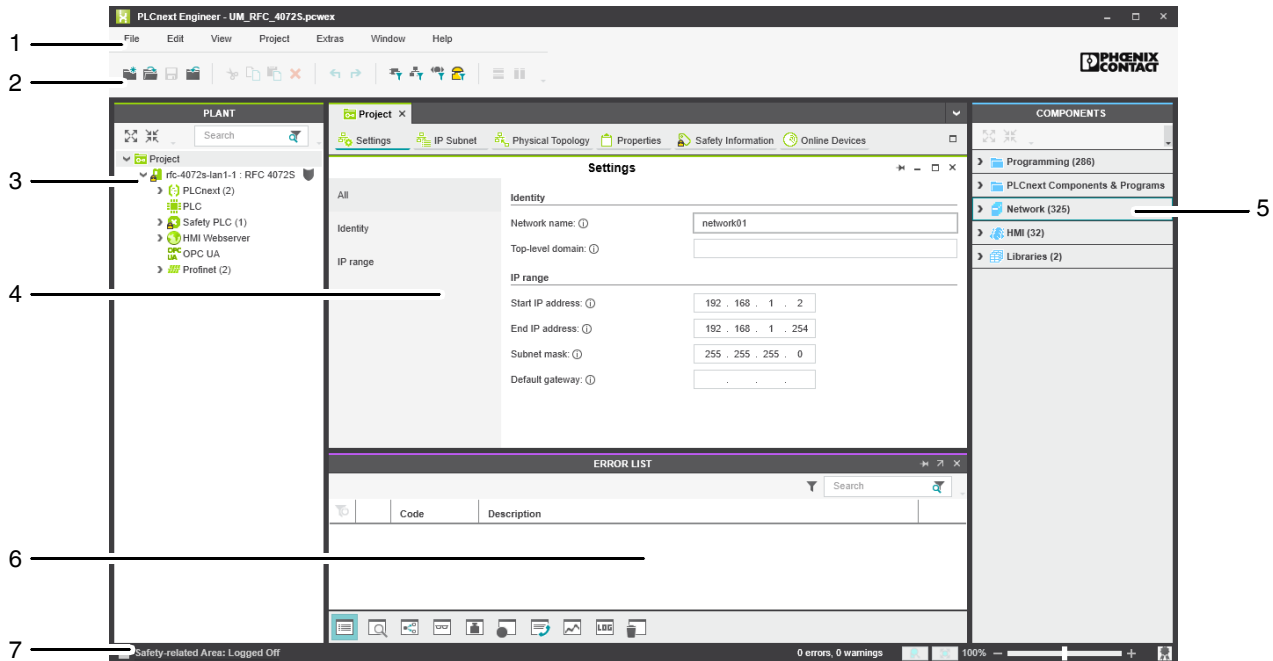


Figure 4-2 PLCnext Engineer user interface

1. Menu bar
2. Tool bar
3. “PLANT” area
4. Editors area
5. “COMPONENTS” area
6. Cross-functional area
7. Status bar

“PLANT” area

All of the physical and logical components of your application are mapped in the form of a hierarchical tree structure in the “PLANT” area.

Editors area

Various color-coded editor groups can be shown in the editors area. To do this, double-click in the relevant area. The color coding distinguishes an instance editor (green, “PLANT” area) from a type editor (blue, “COMPONENTS” area), for example.

“COMPONENTS” area

The “COMPONENTS” area contains all of the components available for the project. The components are subdivided according to their function.

Cross-functional area

The cross-functional area contains functions that extend across the entire project (e.g., ERROR LIST, WATCHES, LOGGING, and RECYCLE BIN).

4.4.5 Creating a new project

- Open PLCnext Engineer.
- Click on the “Empty RFC 4072S project” project template on the start page.

The project template for an empty RFC 4072S project opens.

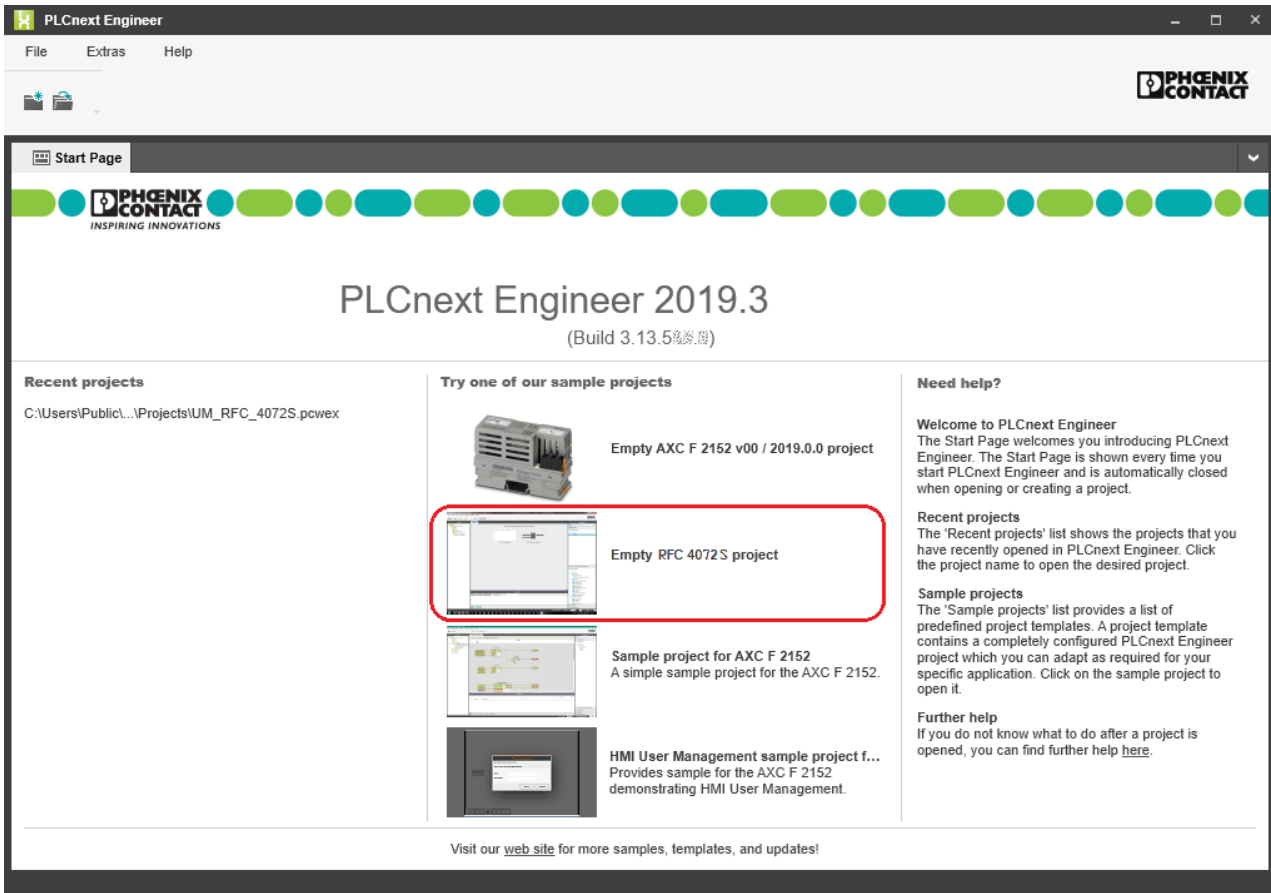


Figure 4-3 Start page, “Empty RFC 4072S project” project template

- Open the “File, Save Project As...” menu.
- Enter a unique and meaningful name for the project (in the example: “UM_RFC_4072S”).
- Click on “Save”.

4.5 Configuring the controller IP settings

4.5.1 General information

In the delivery state, the preset IP address of the RFC on the LAN1 interface is 192.168.1.10. You can manually change the IP addresses using the PLCnext Engineer software via the Ethernet interface or via the display.



Setting IP addresses via the display

Refer to [Section 7.2 on page 172](#) for how to change the IP address settings via the display directly on the RFC.

PC/network adapter

To determine whether your network permits the IP settings used in the example project, proceed as follows:

- In the Windows Control Panel, check the settings for your PC network adapter.
- If necessary, adjust these settings so that the RFC 4072S can be accessed in your network via the IP address used in the example project.

If your network does not permit the use of the IP addresses used in the example project, adjust the settings accordingly.

4.5.2 Important information



Please note that the RFC has **several MAC addresses**. The LAN1 and LAN2 interfaces are each assigned a separate MAC address. A common third MAC address is assigned to the LAN3.1 and LAN3.2 interfaces that are switched internally in the device.

LAN1 is preconfigured as the PROFINET controller interface.

The LAN3.1 and LAN3.2 interfaces are preconfigured as the device interface.

Depending on the connected interface, the RFC can then be accessed in the Ethernet via **three different IP addresses**.

Please note:

- The IP addresses of interfaces LAN1 / LAN2 / LAN3.1/3.2 must be in different sub-nets.
- The PROFINET controller function of the RFC is available at interface LAN1. This interface must then be assigned an IP address if the PROFINET controller function of the device is to be used in the application.
- An IP address must be assigned to interfaces LAN3.1/3.2 if you want to use the PROFINET device function of the RFC at either of these interfaces.
- The LAN2 and LAN3.1/3.2 interfaces do not necessarily have to be assigned an IP address if, for example, communication between a PC with PLCnext Engineer and the RFC is also implemented via the LAN1 interface. Nevertheless, we recommend that appropriate IP addresses are assigned to all interfaces.



WARNING: Network error/network conflict

If you use more than one F-Host (controller with integrated safety-related controller) with the same F_Source_Address in different networks connected via routers, use routers with the following property:

In the event of a network error/network conflict, the router does not switch to “switch operation”. Use a router with “secure network separation”.



NOTE: Limited number of gateway addresses

In order to avoid uncontrolled transmission of data via all Ethernet interfaces, do not enter more than one gateway address in the “Ethernet” view in the “Settings” editor of the controller editor group in PLCnext Engineer.

The following IP address settings apply in this example:

Table 4-3 IP address settings in the example

Interface	IP address	Subnet mask
LAN1	192.168.1.10	255.255.255.0
LAN2	192.168.2.10	255.255.255.0
LAN3 (3.1/3.2)	192.168.3.10	255.255.255.0

4.5.3 Setting the IP address range

- Double-click on the “Project (x)” node in the “PLANT” area.

The “Project” editor group opens.

- Select the “Settings” editor.
- Set the desired IP address range and the subnet mask for the project.

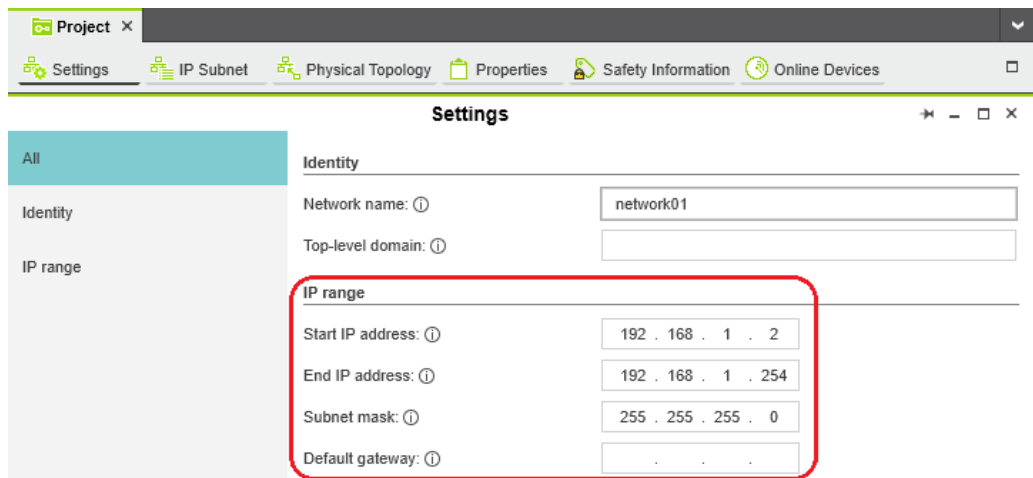


Figure 4-4 Setting the IP address range

4.5.4 Setting the IP address

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Settings” editor.
- Select the “Ethernet” view.

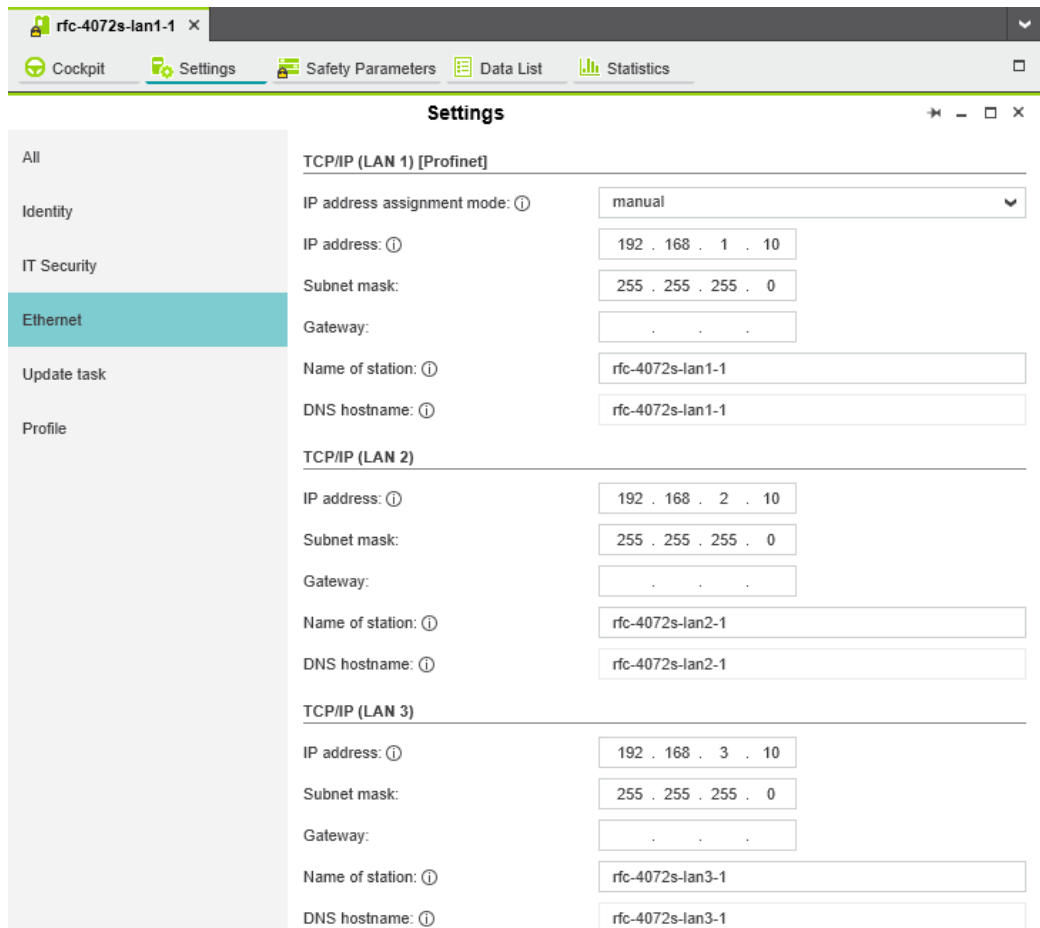


Figure 4-5 Setting the IP address

The IP address of the controller can be set automatically or manually. The IP address is assigned to the controller when you have connected PLCnext Engineer to the controller, see [Section 4.7](#).

Setting the IP address automatically

- Select “automatic” in the “IP address assignment mode” drop-down list.

PLCnext Engineer automatically assigns an IP address to the controller from the set IP address range (see [Section 4.5.3, “Setting the IP address range”](#)) as soon as a connection is established to the controller (see [Section 4.7](#)).

Setting the IP address manually

- Select “manual” in the “IP address assignment mode” drop-down list.
- Enter the IP address, subnet mask, and gateway in the respective input fields.

PLCnext Engineer assigns the manually set IP address to the controller as soon as a connection is established to the controller (see [Section 4.7](#)).

4.6 Defining a project password

If prompted by PLCnext Engineer, enter a project password in the “PROJECT PASSWORD DEFINITION” dialog.

The project password in PLCnext Engineer allows you to edit safety-related parts of the PLANT, the COMPONENT area, the code, and the variables. Safety-related parts of the project can only be edited if you are logged into the safety-related area. This area is only accessible to authorized users.

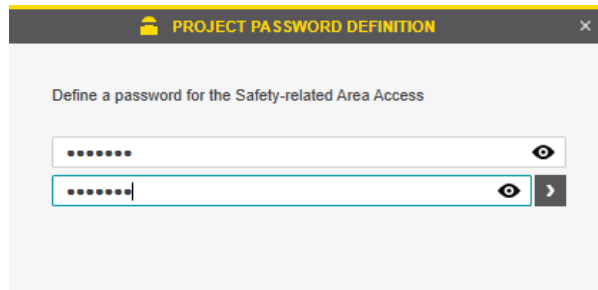


Figure 4-6 Defining a project password

4.7 Connecting to the controller

To be able to transfer a project to the controller, you must first connect PLCnext Engineer to the controller. To do this, proceed as follows:

- Double-click on the “Project (x)” node in the “PLANT” area.

The “Project” editor group opens.

- Select the “Online Devices” editor.
- Select the appropriate network card from the drop-down list.

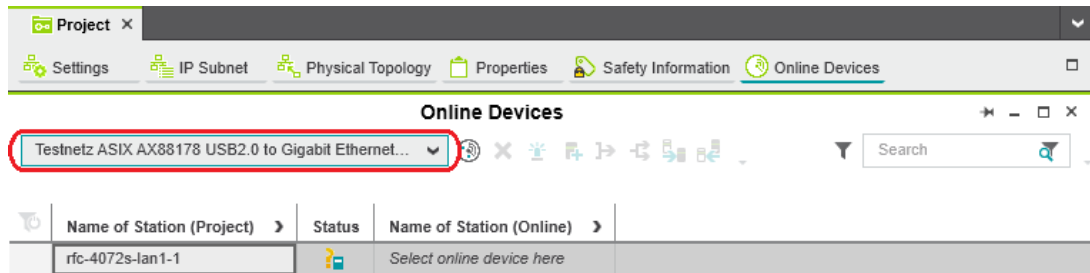


Figure 4-7 Selecting the network card



You can show and hide more detailed information by clicking on the arrows next to “Name of Station (Project)” and “Name of Station (Online)” (see [Figure 4-7](#)).

- Click on the button to search the network for connected devices.

You can see the configured devices under “Name of Station (Project)”.

You can see the devices that have been found online in the network (online devices) under “Name of Station (Online)”.

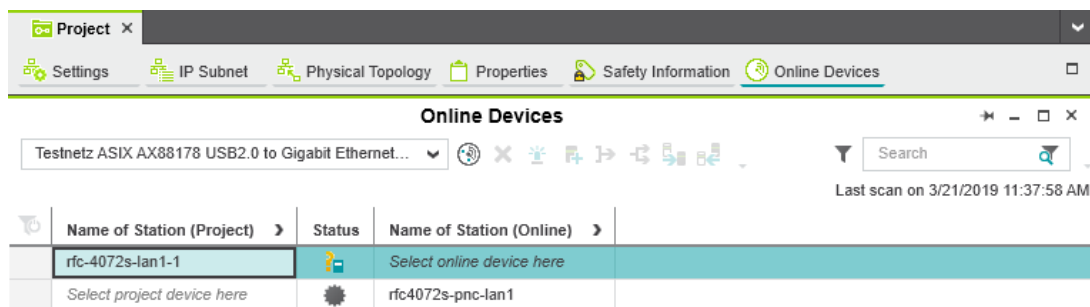


Figure 4-8 Assigning online devices

If you select the device (“Select project device here”) under “Name of Station (Project)”, the configured controller receives the IP settings of the online device found in the network.

If you select the device (“Select online device here”) under “Name of Station (Online)”, the controller found in the network (the online device) receives the IP settings of the configured controller.

- Select the desired device.

The configured controller has now been assigned to an online device.



If the IP address of an online device found in the network already matches the IP address of the configured controller, the online device is automatically assigned to the configured controller. In this case, you do not need to select the desired device for the assignment.

The icon in the “Status” column indicates that assignment was successful.

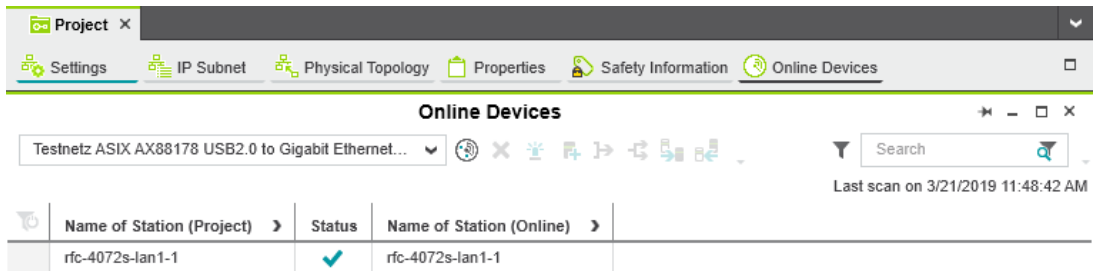


Figure 4-9 Successful assignment of the configured controller to an online device

Once the configured controller has been assigned to an online device, you can connect PLCnext Engineer to the controller:

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Cockpit” editor.
- Click on the button to connect PLCnext Engineer to the controller.



Observe user authentication:

When user authentication is enabled, authentication with a user name and password is required in order to execute this function. User authentication is enabled by default. You can disable user authentication in the RFC web-based management.

If user authentication is enabled, the function can only be executed by users whose user roles have the necessary authorization.

If you do not have the necessary authorization to execute the function, PLCnext Engineer informs you of this in a message.

For information on user authentication, refer to [Section 9.6.4.1](#).

The following dialog opens:

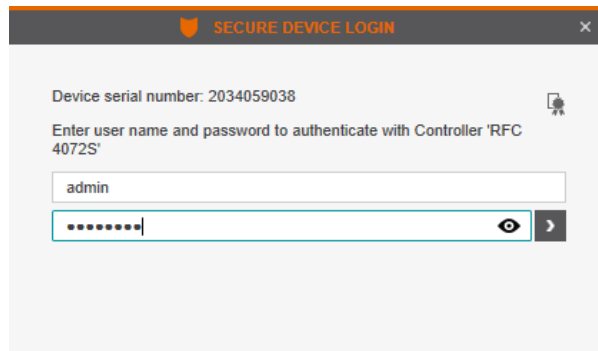



Figure 4-10 User authentication: entering a user name and password

In the delivery state, the “admin” user is already created with a default password (see label/printing in [Figure 2-36 on page 76](#)).

- Enter the user name and password.

The  icon next to the controller node and bold font in the “PLANT” area indicates that connection was successful (see [Figure 4-11](#)).

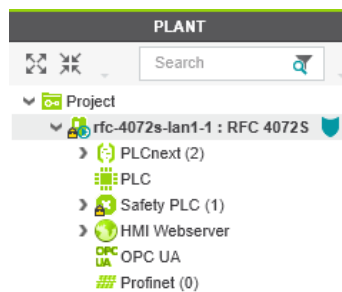



Figure 4-11 Successful connection to the controller

The  button also indicates successful connection.

4.8 Configuring PROFINET devices

4.8.1 Adding PROFINET devices

- Double-click on the “Profinet (x)” node in the “PLANT” area.

The “/ Profinet” controller editor group opens.

- Select the “Device List” editor.

Add the PROFINET devices in the “Device List” editor. To do this, proceed as follows:

- Select “Select Type here” in the first row of the “Device List” editor.

The role picker opens. Only the elements from the “COMPONENTS” area that you can actually use are displayed in the role picker.

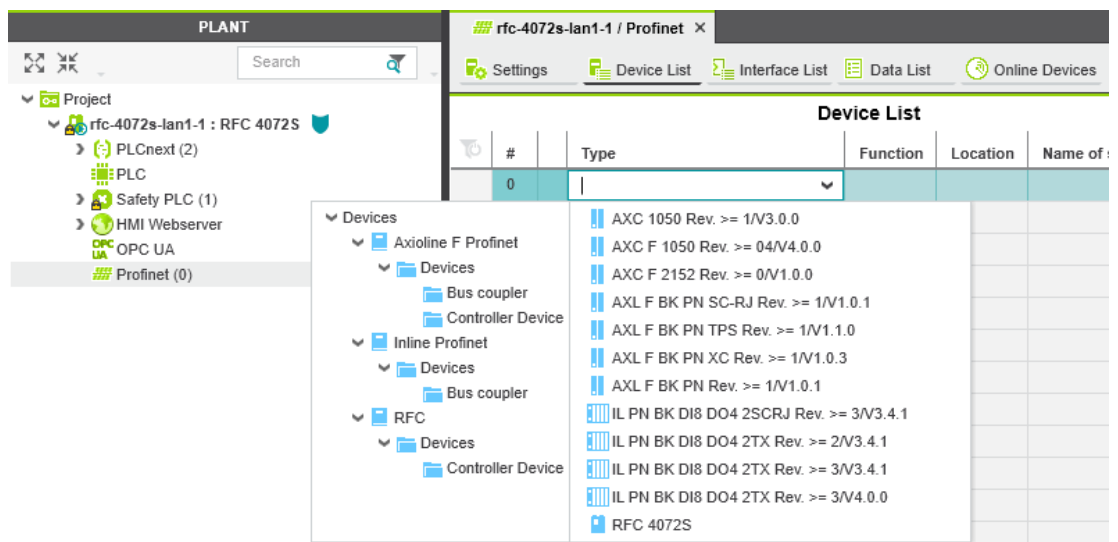


Figure 4-12 Role picker for selecting PROFINET devices

- Select the relevant PROFINET device in the role picker.

The PROFINET device is automatically added and mapped under the “Profinet (x)” node in the “PLANT” area.

- Proceed as described above to add more PROFINET devices.

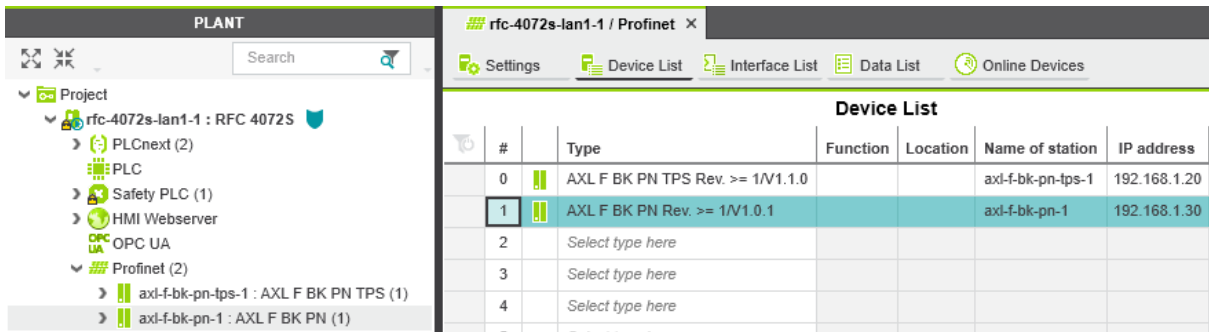


Figure 4-13 PROFINET devices in the “PLANT” area and in the Device List

4.8.2 Assigning online devices (device naming)

After you add PROFINET devices to the project, you must assign each configured PROFINET device to the corresponding PROFINET device of your actual bus configuration (online device). By performing this assignment, you are giving the PROFINET devices their IP settings and their PROFINET device names. To do this, proceed as follows:

- Double-click on the “Profinet (x)” node in the “PLANT” area.
- The “/ Profinet” controller editor group opens.
- Select the “Online Devices” editor.
 - Select the appropriate network card from the drop-down list.

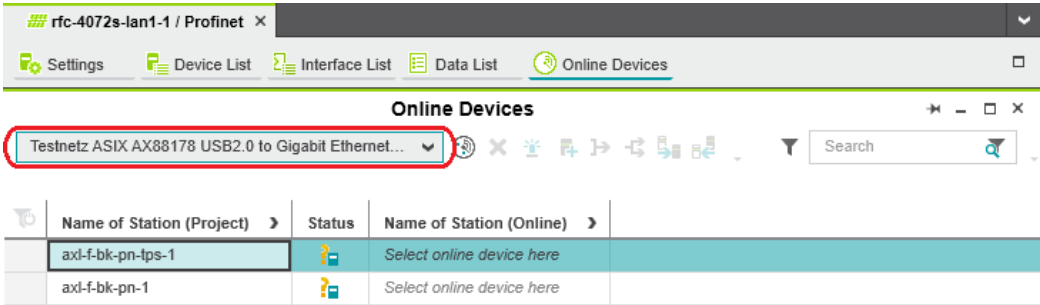



Figure 4-14 Selecting the network card

- Click on the  button to search the network for connected PROFINET devices.
- You can see the configured PROFINET devices under “Name of Station (Project)”.
- You can see the PROFINET devices that have been found online in the network (online devices) under “Name of Station (Online)”.

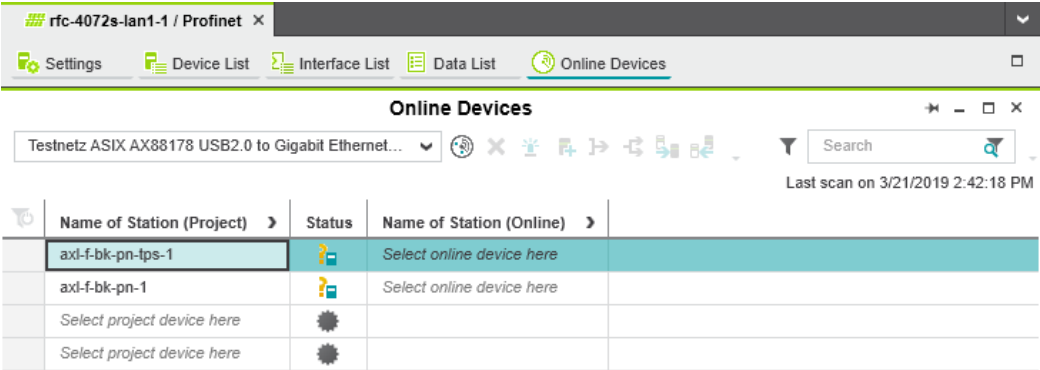


Figure 4-15 Assigning online devices

If you select the PROFINET device (“Select online device here”) under “Name of Station (Online)”, the PROFINET device found in the network (the online device) receives the IP settings of the configured PROFINET device (device naming).



Please note:

The PROFINET device does not have an IP address in the delivery state.

- When starting up the PROFINET device for the first time, choose the device under “Name of Station (Online)”.

The PROFINET device receives the IP settings of the configured PROFINET device.

If you select the device (“Select project device here”) under “Name of Station (Project)”, the configured PROFINET device receives the IP settings of the online device found in the network.

- Select the desired device.

The configured PROFINET device has now been assigned to an online device. The ✓ icon in the “Status” column indicates that assignment was successful.

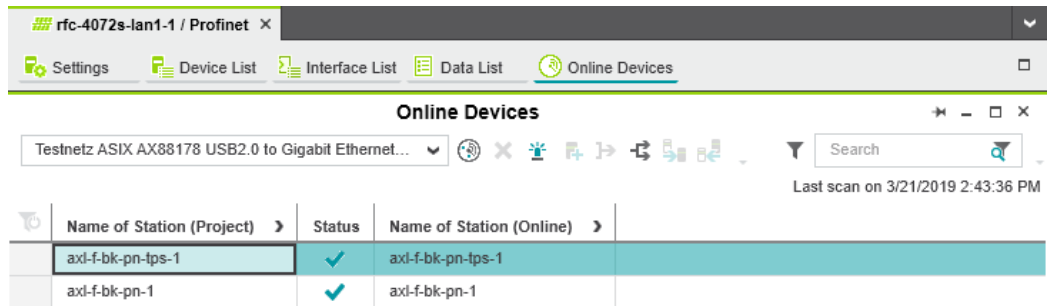


Figure 4-16 Successful assignment of the configured PROFINET devices to an online device

4.8.3 Adding I/O modules

Once you have added all the PROFINET devices from your bus configuration to the project, you can add the I/O modules connected to the PROFINET device. There are two ways to add I/O modules. You can add I/O modules manually or have them read in automatically.

Adding I/O modules manually

To add I/O modules manually, proceed as follows:

Double-click in the “PLANT” area on the PROFINET device whose I/O modules you wish to add.

The editor group of the selected PROFINET device opens; “axf-f-bk-pn-tps-1” in the example.

- Select the “Module List” editor.
- Select “Select type here” in the first row of the “Module List” editor.

The role picker opens. Only the elements from the “COMPONENTS” area that you can actually use are displayed in the role picker.

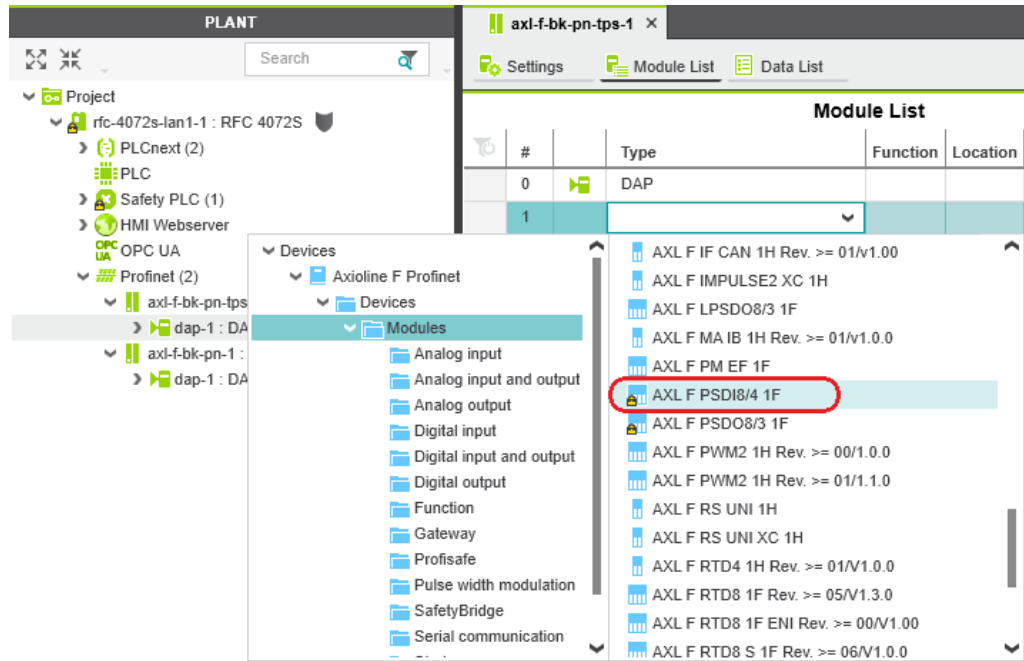


Figure 4-17 Role picker for selecting I/O modules

- Select the relevant I/O module in the role picker.

Project login required



Enter project password

Safety-related changes to the project – Login required

If you make changes to the safety-related project at this point, PLCnext Engineer requires you to enter a password (e.g., if you add F-Devices to your project).

- Enter the project password in the “PROJECT AUTHENTICATION” dialog (see [Figure 4-18](#)).

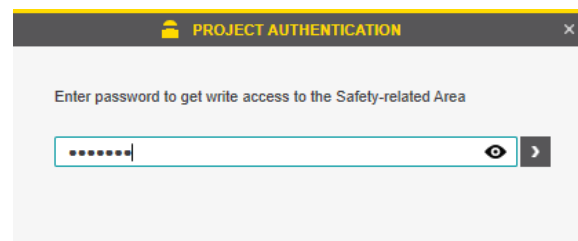


Figure 4-18 Entering the project password

- Click on the arrow in the dialog to confirm your entry.

Successful login to the safety-related area is indicated by the text highlighted in yellow shown in [Figure 4-19 on page 112](#):

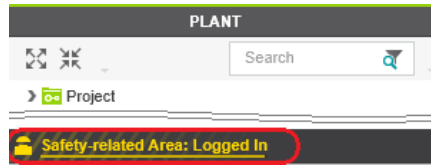


Figure 4-19 Successful login to the safety-related area

The I/O module is added and shown in the “PLANT” area under the “Profinet (x)” node for the respective PROFINET device (see Figure 4-20).

- Proceed as described above to add more I/O modules.

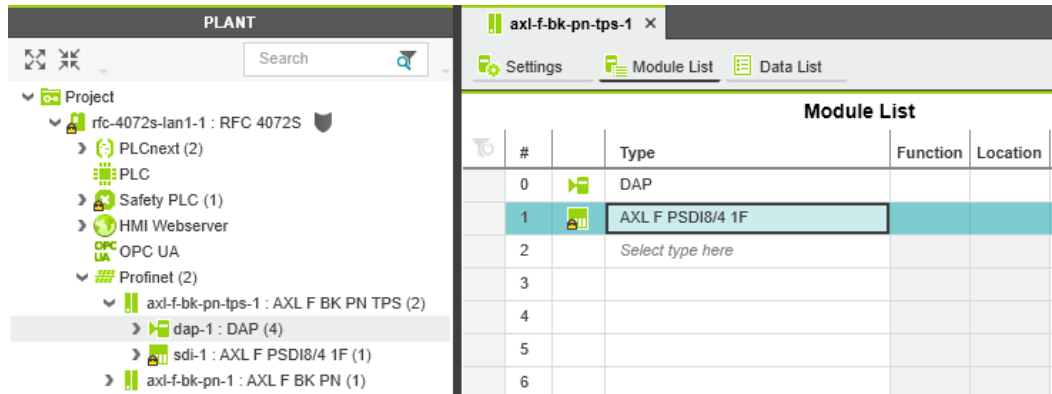


Figure 4-20 I/O modules of a PROFINET device in the “PLANT” area and in the module list

Reading I/O modules automatically

The following requirements must be satisfied before you can read the I/O modules of a PROFINET device automatically:

- The controller has valid IP settings (see Section 4.5).
- The PROFINET device has valid IP settings and is connected to PLCnext Engineer (see Section 4.8.2).

To read the I/O modules of a PROFINET device automatically, proceed as follows:

- Under the “Profinet” node in the “PLANT” area, right-click on the PROFINET device whose I/O modules you wish to read.
- Select “Read Profinet modules” from the context menu.

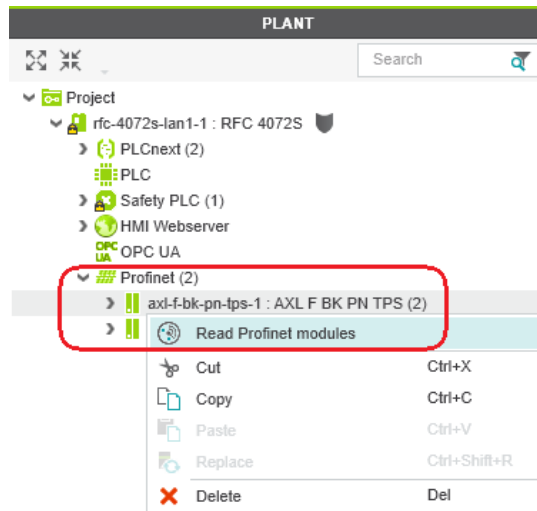


Figure 4-21 Reading I/O modules of a PROFINET device automatically

The I/O modules connected to the PROFINET device are now read automatically.

- Repeat this step for all PROFINET devices in the project.

The figure below shows all the manually and automatically added I/O modules in the example project.

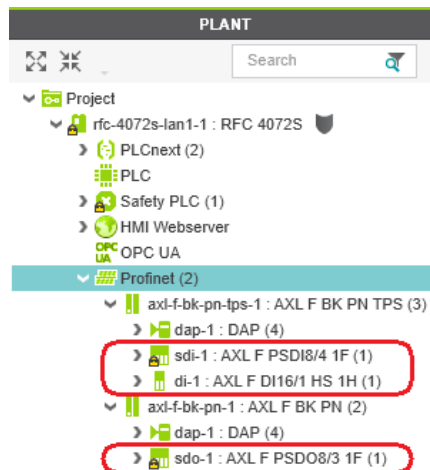


Figure 4-22 Axioline F modules in the example project

4.9 Programming in accordance with IEC 61131-3 – Non-safety-related example program



Please note:

Programming with C++ or MATLAB® Simulink® is not described in this user manual.

Detailed information on programming with C++ or Matlab® Simulink® is available in the PLCnext Community at plcnext-community.net.

You will find operating instructions, tutorials, FAQs, and software and firmware downloads in the PLCnext Community.

4.9.1 Opening and creating the POU

When you create a project, a Program Organization Unit (POU) with the name “Main” is created automatically for standard controllers in the “COMPONENTS” area under “Programs” (see [Figure 4-24 on page 115](#)).

Opening the POU

To open a POU, proceed as follows:

- Click on “Programming (x)” in the “COMPONENTS” area.
- Then click in turn on the arrow next to “Local (x)” and “Programs (x)”.
- Double-click on the desired POU (in the example: “Main” program).

The editor group for the selected POU opens. You are prompted to select the programming language for the first worksheet of the POU.

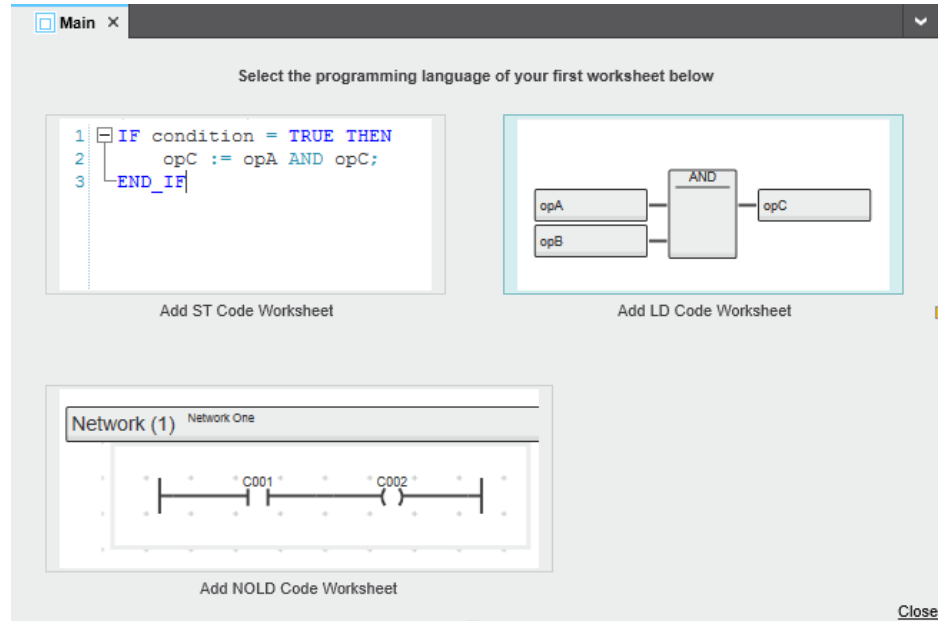


Figure 4-23 Selecting the programming language for the first worksheet

- Click on the desired programming language (in the example: “Add LD Code Worksheet”).

You can now define variables, for example (see [“Creating variables” on page 116](#)).

Creating a new POU

To create a new POU, proceed as follows:

- Click on “Programming (x)” in the “COMPONENTS” area.
- Click on the arrow next to “Local (x)”.
- Right-click on “Programs (x)”.
- In the context menu, select “Add Program”.

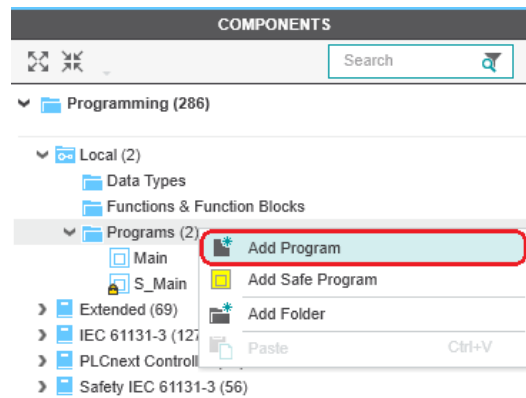


Figure 4-24 “Add Program” context menu

If you have created a new POU, you will be prompted to select the programming language when you open the worksheet for the first time (see [Figure 4-23](#)).

Once you have selected the programming language, the POU editor group opens.

4.9.2 Creating variables

The following table shows the variables to be created in the non-safety-related example program (logical ANDing), which will later be connected to process data in PLCnext Engineer.

Table 4-4 Input/output variables in the example (logical ANDing)

Variable	Data type	Use	Description
IN_1	BOOL	External	Input IN0_CH1 (IN00) AXL F DI16/1 HS 1H
IN_2	BOOL	External	Input IN0_CH2 (IN01) AXL F DI16/1 HS 1H
OUT	BOOL	External	Output variable (not linked to a process data item)

- Select the “Variables” editor.
- Create the variables that you need for the selected POU (in the example in [Figure 4-25: Main](#)).
- Set the type and use for all created variables.

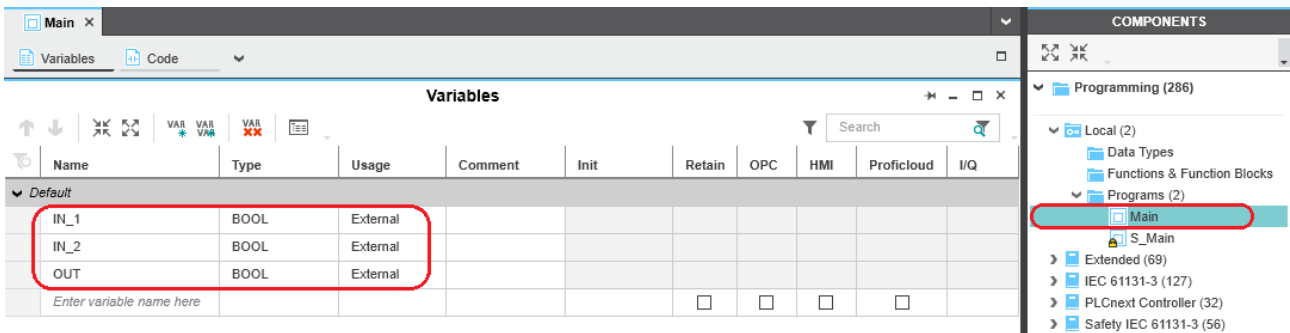


Figure 4-25 Creating variables for a POU (in the example: for the “Main” POU)

Once you have created all of the necessary variables, create the program for the selected POU, see [Section 4.9.3](#).

4.9.3 Creating a program

Non-safety-related example program

The example program in [Figure 4-26](#) involves logical ANDing of two input variables. The result of the ANDing is connected to an output variable. The input variables are connected to input process data in due course. The output variable is not connected further. Its value is considered online in PLCnext Engineer.

Creating a program

To create a program, proceed as follows:

- Select the program editor.

The program editor is referred to as “Code” by default. You can change the designation of the program editor as desired.

- Create the program.

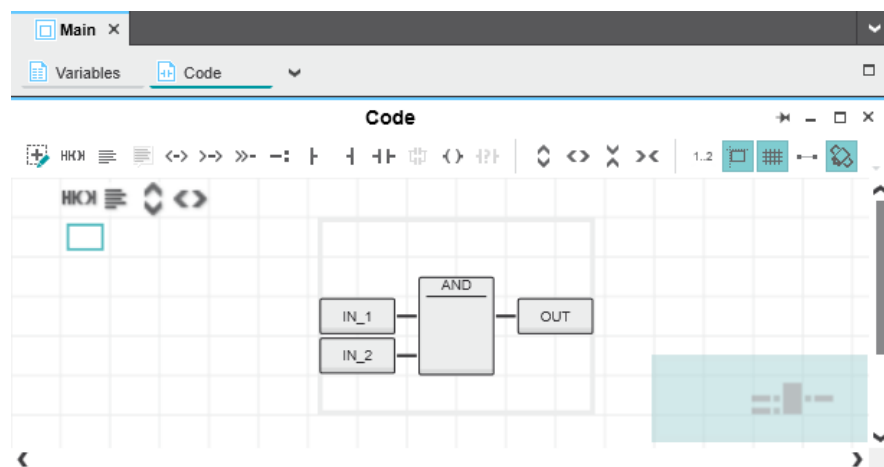


Figure 4-26 Example program in FBD

Adding worksheets

The program for a POU can consist of several worksheets and different programming languages. For each required programming language, add a corresponding worksheet (Code Worksheet) to the POU. Each worksheet is inserted in the POU editor group as an additional “Code” editor.

To add additional worksheets to a POU, proceed as follows:

- Select a worksheet in the program editor (in [Figure 4-27](#): “Code” editor).
- Click on the arrow on the right next to the designation of the program editor.
- From the drop-down list that opens, select the desired code worksheet.

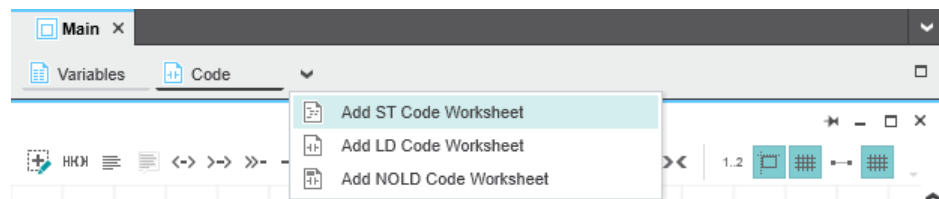


Figure 4-27 Adding a code worksheet to a POU

4.10 Instantiating a program

Instantiate the program in the “Tasks and Events” editor. To instantiate a program, create the required task and assign it to the desired program instance. Individual tasks are coordinated and processed in the Execution & Synchronization Manager (ESM). The RFC 4072S uses a dual core processor and has one ESM (“ESM1” and “ESM2” in the “Tasks and Events” editor) per processor core.

Opening the “Tasks and Events” editor

To open the “Tasks and Events” editor, proceed as follows:

- Double-click on the “PLCnext (x)” node in the “PLANT” area.

The “/ PLCnext” editor group opens.

- Select the “Tasks and Events” editor.

Creating tasks

To create a new task, proceed as follows:

- In the “Name” column, enter a name for the new task in the “Enter task name here” input field.

The name must not contain any spaces.

- In the “Task Type” column, click in the input field.
- Select the “Task Type” from the drop-down list.
- Make all of the required settings for the task in the remaining columns.

Instantiating a program

To instantiate a program, proceed as follows:

- In the “Name” column, enter a name for the program instance under a task in the “Enter program instance name here” input field (“Main1” in the example in [Figure 4-28](#)).

The name must not contain any spaces.

- Click on “Select program type here” in the “Program Type” column.
- Select the program to be instantiated from the drop-down list (“Main” in the example in [Figure 4-28](#)).

The selected program is instantiated and assigned to a task.

Name	Component Name	Task Type	Event Name	Program Type	Interval (ms)	Priority	Threshold (ms)	Watchdog (ms)	Comment
ESM1									
Task1		Cyclic Task			100	0	0	100	
Main1	Arp.Plc.Eclr			Main					
Enter program instance name here				Select program type here					
Enter task name here									
ESM2									
SafetyProxyTask		Cyclic Task			5	0	0	100	
sproxy_1	Arp.Services.SpnsProxy			SpnsProxyProgram					
Enter task name here									

Figure 4-28 Tasks and program instances in the “Tasks and Events” editor

4.11 Assigning process data

4.11.1 For programs in accordance with IEC 61131-3 without IN and OUT ports

There are two ways to assign process data:

- You can assign a process data item to a variable.
- You can assign a variable to a process data item.

Process data is assigned in the “Data List” editor.

Assigning a process data item to a variable

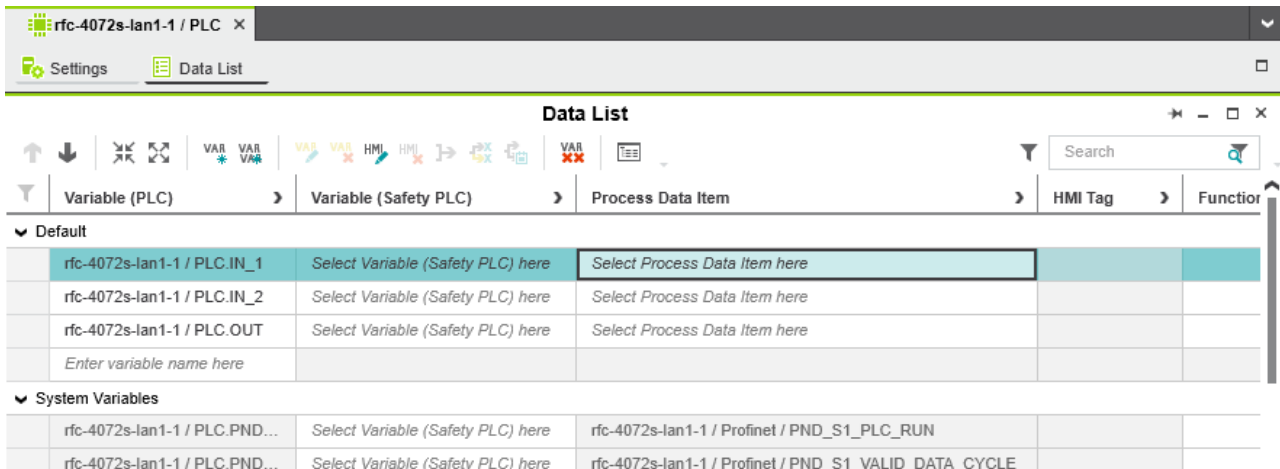
To assign a process data item to a variable, proceed as follows:

- Double-click on the “PLC (x)” node in the “PLANT” area.

The “/ PLC” controller editor group opens.

- Select the “Data List” editor.

You can see an overview of all available variables in the “Data List” editor.



The screenshot shows the 'Data List' editor in PLCnext Engineer. The window title is 'rfc-4072s-Ian1-1 / PLC'. The 'Data List' editor has a toolbar with various icons for variable and HMI management. Below the toolbar is a table with columns: Variable (PLC), Variable (Safety PLC), Process Data Item, HMI Tag, and Function. The table is divided into 'Default' and 'System Variables' sections.

Variable (PLC)	Variable (Safety PLC)	Process Data Item	HMI Tag	Function
▼ Default				
rfc-4072s-Ian1-1 / PLC.IN_1	Select Variable (Safety PLC) here	Select Process Data Item here		
rfc-4072s-Ian1-1 / PLC.IN_2	Select Variable (Safety PLC) here	Select Process Data Item here		
rfc-4072s-Ian1-1 / PLC.OUT	Select Variable (Safety PLC) here	Select Process Data Item here		
Enter variable name here				
▼ System Variables				
rfc-4072s-Ian1-1 / PLC.PND...	Select Variable (Safety PLC) here	rfc-4072s-Ian1-1 / Profinet / PND_S1_PLC_RUN		
rfc-4072s-Ian1-1 / PLC.PND...	Select Variable (Safety PLC) here	rfc-4072s-Ian1-1 / Profinet / PND_S1_VALID_DATA_CYCLE		

Figure 4-29 Example: list of all available variables PLCnext Engineer



You can also see an overview of all the available variables when you click on the node for the controller in the “PLANT” area and also open the “Data List” editor there. You can also assign the process data at this point.

- To assign a process data item to a variable, click on “Select Process Data Item here” in the “Process Data Item” column.

The role picker opens. Only the process data that you can actually assign to the respective variable is displayed in the role picker.

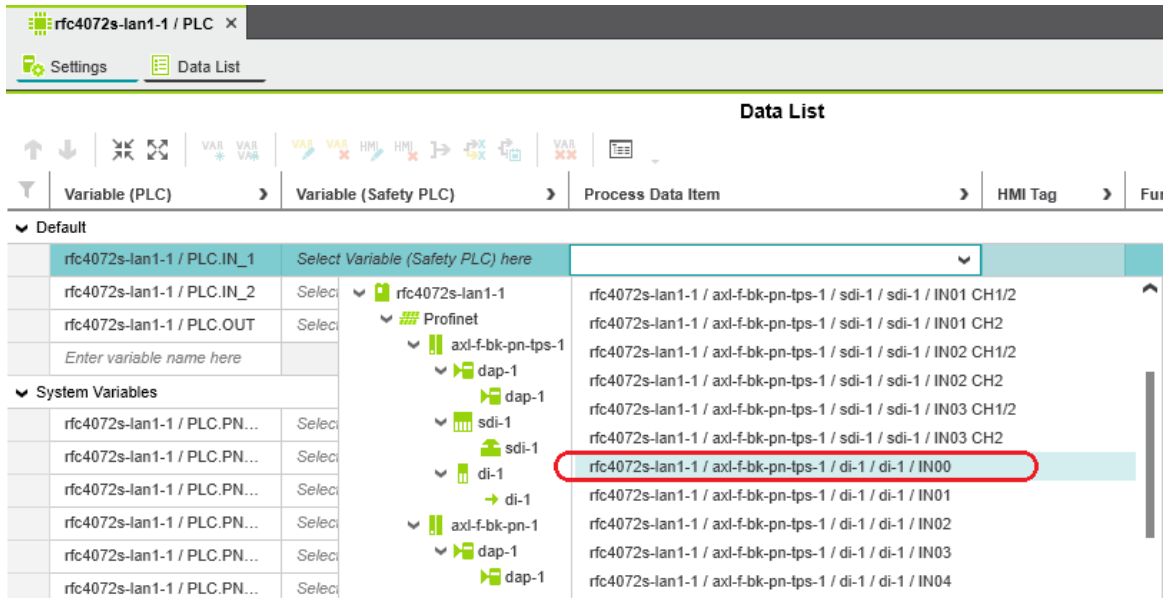


Figure 4-30 Role picker for selecting process data

- In the role picker, select the process data item that you want to assign to the respective variable.

The process data item is assigned to the variable.

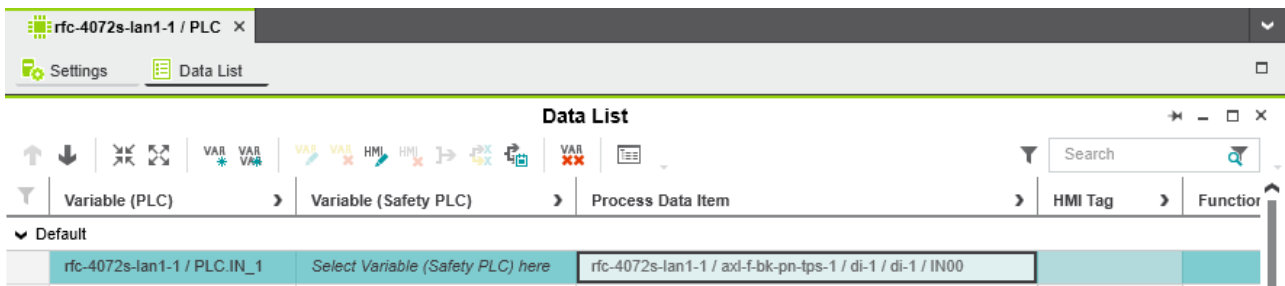


Figure 4-31 Selected process data item

- Proceed as described to add more variables.

Assigning a variable to a process data item

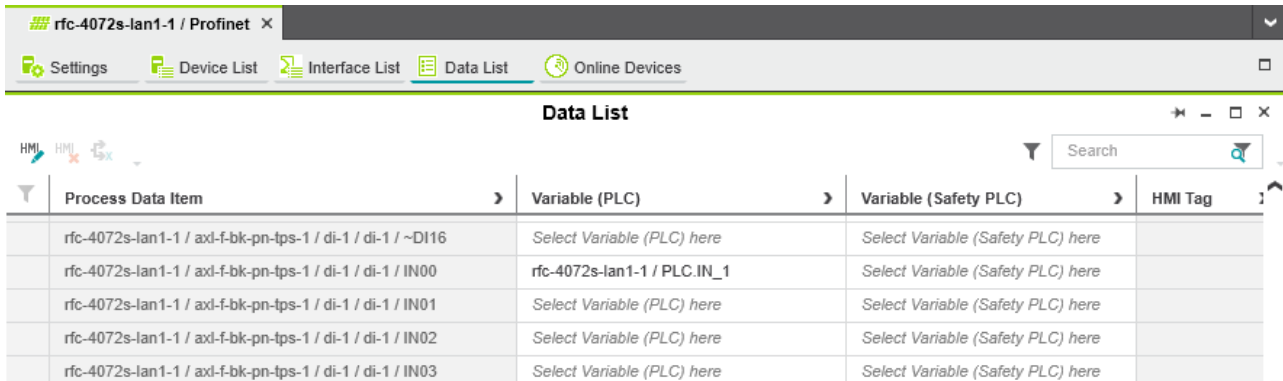
To assign a variable to a process data item, proceed as follows:

- Double-click on the “Profinet (x)” node in the “PLANT” area.

The “/ Profinet” controller editor group opens.

- Select the “Data List” editor.

You can see an overview of all the available process data items in the “Data List” editor.

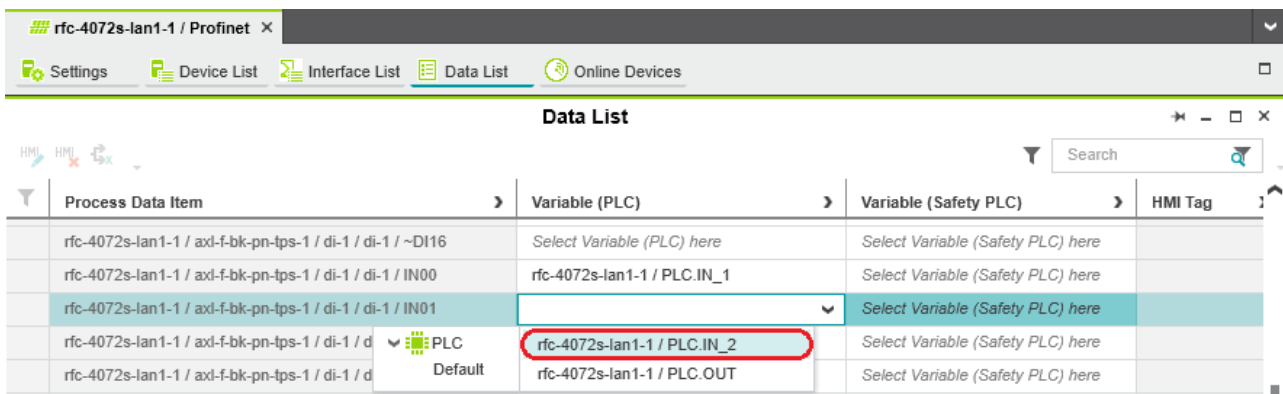


Process Data Item	Variable (PLC)	Variable (Safety PLC)	HMI Tag
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / ~DI16	Select Variable (PLC) here	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN00	rfc-4072s-lan1-1 / PLC.IN_1	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN01	Select Variable (PLC) here	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN02	Select Variable (PLC) here	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN03	Select Variable (PLC) here	Select Variable (Safety PLC) here	

Figure 4-32 Example: list of all available process data items

- To assign a variable to a process data item, click on “Select Variable (PLC) here” in the “Variable (PLC)” column.

The role picker opens. Only the variables that you can actually assign to the respective process data item are displayed in the role picker.



Process Data Item	Variable (PLC)	Variable (Safety PLC)	HMI Tag
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / ~DI16	Select Variable (PLC) here	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN00	rfc-4072s-lan1-1 / PLC.IN_1	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / IN01	Select Variable (PLC) here	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / di-1 / d	▼ PLC Default rfc-4072s-lan1-1 / PLC.IN_2 rfc-4072s-lan1-1 / PLC.OUT	Select Variable (Safety PLC) here	
rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / di-1 / d	Select Variable (PLC) here	Select Variable (Safety PLC) here	

Figure 4-33 Role picker for selecting variables

- In the role picker, select the variable that you want to assign to the respective process data item.

The variable is assigned to the process data item.

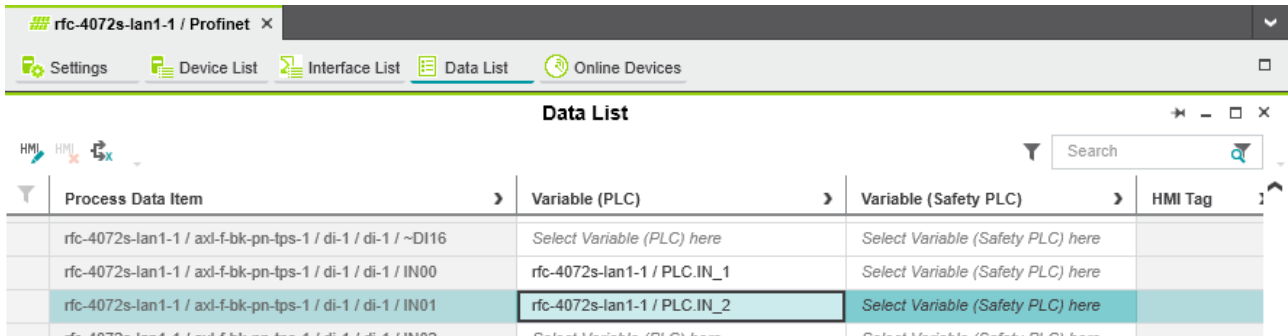


Figure 4-34 Selected variable

- Proceed as described above to add more process data items.

4.11.2 For programs in accordance with IEC 61131-3 with IN and OUT ports

If you have created variables as IN and/or OUT ports in your program, the process data is assigned in the “Port List” editor of the “PLCnext (x)” node.

There are two ways to assign process data:

- You can assign an IN port to an OUT port.
- You can assign an OUT port to an IN port.

Opening the “Port List” editor

- Double-click on the “PLCnext (x)” node in the “PLANT” area.

The “/ PLCnext” editor group opens.

- Select the “Port List” editor.

You can see an overview of all the available IN and OUT ports in the “Port List” editor.



IN and OUT ports are **only** displayed in the “Port List” editor of the “PLCnext (x)” node.

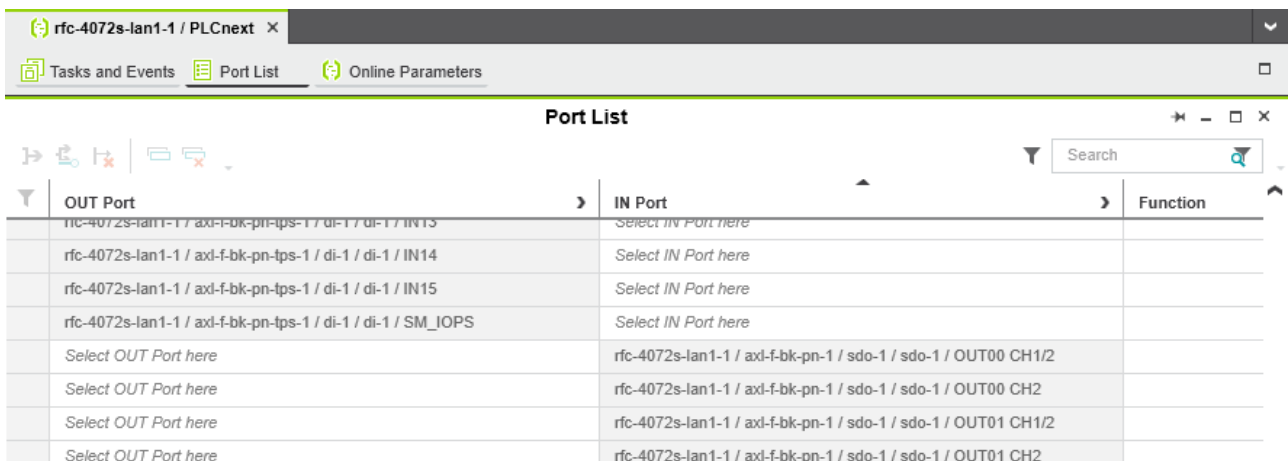


Figure 4-35 Example: list of all available IN and OUT ports

Assigning an IN port to an OUT port

- To assign an IN port to an OUT port, click on “Select IN Port here” in the “IN Port” column.

The role picker opens. Only the IN ports that you can actually assign to the respective OUT port are displayed in the role picker.

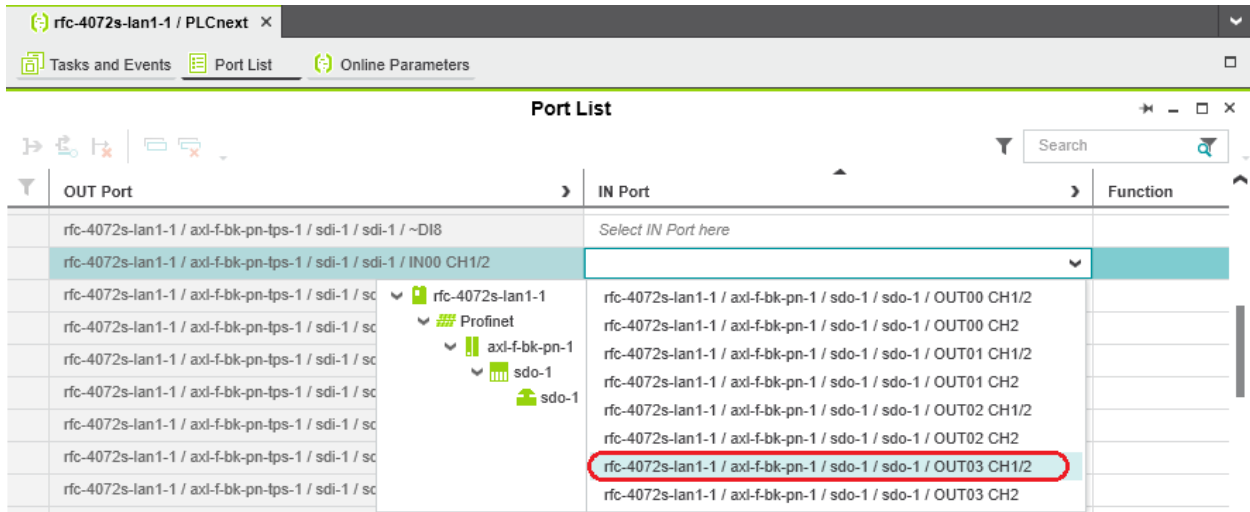


Figure 4-36 Role picker for selecting IN ports

- Select the IN port that you want to assign to the relevant OUT port in the role picker.
- The IN port is assigned to the OUT port.
- Proceed as described to add other IN ports.

Assigning an OUT port to an IN port

- To assign an OUT port to an IN port, click on “Select OUT Port here” in the “OUT Port” column.

The role picker opens. Only the OUT ports that you can actually assign to the respective IN port are displayed in the role picker.

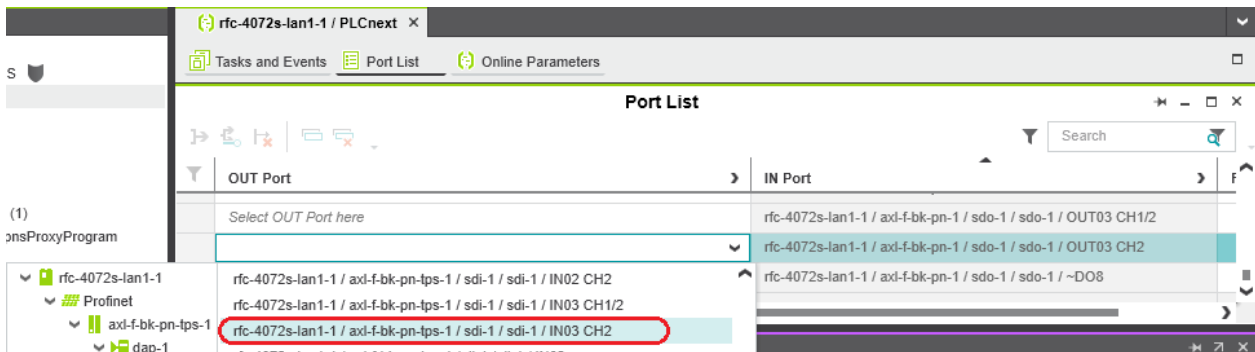


Figure 4-37 Role picker for selecting OUT ports


- Select the OUT port that you want to assign to the relevant IN port in the role picker.
- The OUT port is assigned to the IN port.
- Proceed as described to add other OUT ports.

4.12 Transferring a project to the controller

To transfer the project to the controller, proceed as follows:

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Cockpit” editor.
- Click on the  button (“Write project to controller and start execution. (F5)”).



User authentication

If necessary, refer to the information about user authentication on [page 106](#).

- If necessary, enter the user name and password in the dialog that opens.

The project is compiled, transferred to the controller, and executed.

If startup was carried out successfully, the following appears on the RFC 4072S display:

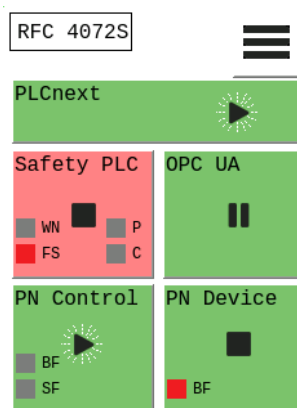


Figure 4-38 Controller in the RUN state, PROFINET controller in the ACTIVE state

If an installation error prevents the system from starting up, a corresponding error message appears on the display and in PLCnext Engineer.



The iSPNS 3000 is in the FAIL state, as no safety programming has been performed in the example project.



4.13 Displaying online values

To view online variable values, you can “attach to the controller”. To do this, you must have successfully compiled the project, transferred it to the controller, and started it.

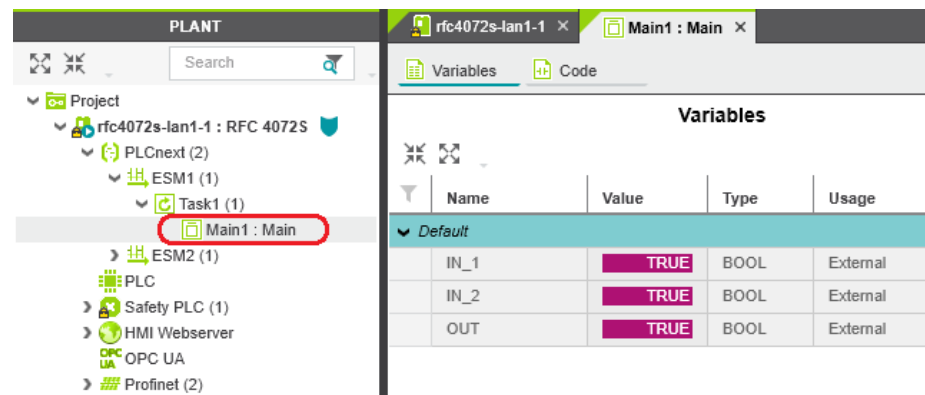
Proceed as follows:

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

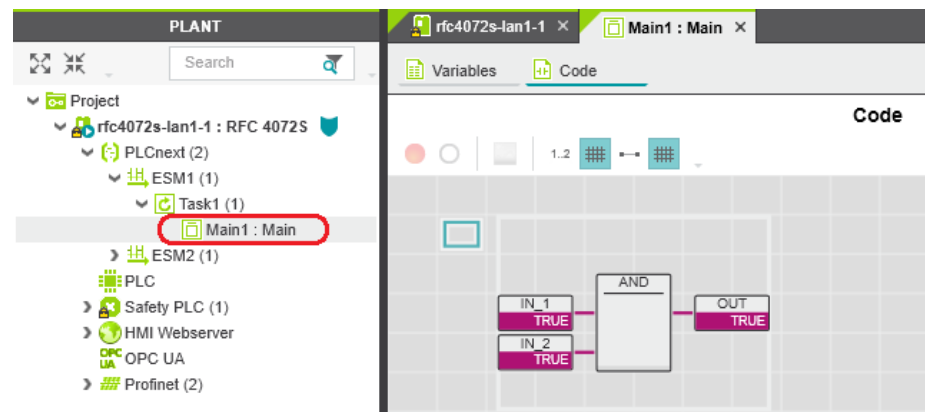
- Select the “Cockpit” editor.
- Click on the  button (“Connect to the controller to establish communication with online services.”).
- Click on the  button (“Attach to the PLC runtime to see online values and enable debugging.”).
- Open the instance editor of the “Main” POU by double-clicking on the “Main1 : Main” node.

The online values of the variables used in the “Main” POU are displayed in the “Variables” and “Code” editors.



Name	Value	Type	Usage
IN_1	TRUE	BOOL	External
IN_2	TRUE	BOOL	External
OUT	TRUE	BOOL	External

Figure 4-39 “Variables” editor: online values of the variables used



```

graph LR
    IN_1[IN_1 TRUE] --> AND[AND]
    IN_2[IN_2 TRUE] --> AND
    AND --> OUT[OUT TRUE]
  
```

Figure 4-40 “Code” editor: online values of the variables used

4.14 Creating a PLCnext Engineer HMI application

In PLCnext Engineer, you can create a PLCnext Engineer HMI application, which can be used to visualize, monitor, and control the application on your controller.



For information on creating a PLCnext Engineer HMI application, refer to the “Installing and operating the PLCnext Engineer software” quick start guide and the online help for PLCnext Engineer.

4.15 Programming in accordance with IEC 61131-3 – Safety-related example program

Once you have created the non-safety-related part of the example project, you can start creating the safety-related part.

4.15.1 Assigning/checking the PROFIsafe address (F-Address) of PROFIsafe devices

The PROFIsafe address (F-Address) is a unique ID for each F-Device in the network. The F-Host is assigned an F_Source_Address (F_Source_Add), while each F-Device is assigned its own F_Destination_Address (F_Dest_Add).

You must set the PROFIsafe address via the DIP switches directly on the F-Device prior to installation. Check the set F-Address in the project in PLCnext Engineer and adapt the settings there, if necessary.



Unique F-Address assignment – Avoid addresses overlapping

Assign a unique F-Address to each F-Device that is used. In the example, the AXL F PSDI8/4 1F is assigned F-Address “1” and the AXL F PSDO8/3 1F is assigned F-Address “2”. Each F-Address assigned within a network must be unique and must not overlap with other addresses.

For more detailed information on setting the PROFIsafe F-Addresses, please refer to [“Device identification / number of safe devices” on page 30](#) and the device-specific user documentation.

F_Source_Address (F_Source_Add)

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Safety Parameters” editor.



If you are not currently logged into the safety-related area, you will now be prompted to enter the password in the “PROJECT AUTHENTICATION” dialog that opens (see [“Project login required” on page 111](#)).

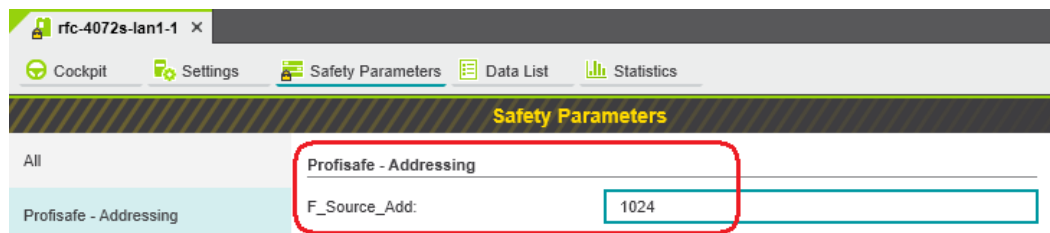


Figure 4-41 F-Address of the F-Host: F_Source_Add (F_Source_Address)

- In the “PROFIsafe addressing” view, check the setting for the F_Source_Add F-Address. In the example, set F_Source_Add to “1024”. If necessary, adapt the value of F_Source_Add to your application.

An adjustable range of “1 ... 65534_{dec}”, maximum, is permitted.

**F_Destination_Address
(F_Dest_Add)**



When using the RFC 4072S as an F-Host, an adjustable range of “1 ... 65534_{dec}”, maximum, is permitted for the F-Addresses of the safety modules used (F_Dest_Add / F_Destination_Address). Please note the following points:

- Only assign F_Dest_Add values once.
- For safety modules from Phoenix Contact, you can set PROFIsafe destination addresses from 1 to 999_{dec}, maximum.
- For safety modules from other manufacturers, you can set PROFIsafe destination addresses from 1 to 65534_{dec}.

- Under the “Profinet (x)” node in the “PLANT” area, double-click on the lower-level node of the safety module whose F-Address you want to set.

The safety module editor group opens.

- Select the “Safety Parameters” editor.



If you are not currently logged into the safety-related area, you will now be prompted to enter the password in the “PROJECT AUTHENTICATION” dialog that opens (see “Project login required” on page 111).

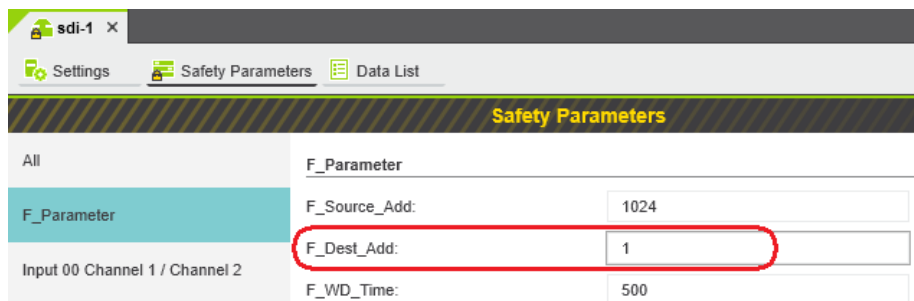


Figure 4-42 F-Address of the PROFIsafe F-Device: F_Dest_Add (F_Destination_Address)

- In the “F_Parameter” view, check the setting for the F_Dest_Add F-Address.
- Set F_Dest_Add to the value that corresponds to the DIP switch setting of the safety module.
- Set F_Dest_Add to “1” for the AXL F PSDI8/4 1F safety module in the example.
- If necessary, adapt the value of F_Dest_Add to your application.

An adjustable range of “1 ... 65534_{dec}”, maximum, is permitted.

- Set F_Dest_Add to “2” for the AXL F PSDO8/3 1F safety module in the example.
- Proceed as described for other safety modules in your application.

4.15.2 Management/diagnostic variables for F-Devices

In PLCnext Engineer, you can specify whether management/diagnostic variables are to be created for F-Devices in the project.

One part of these management/diagnostic variables is created by default.

These non-safety-related variables support you in the reintegration of passivated F-Devices, for example.

For this purpose, you can define non-safety-related exchange variables in PLCnext Engineer. You then connect these exchange variables to corresponding management/diagnostic variables in the safety-related “S_Main” POU (see [Section “Creating a safety-related program” on page 137](#)).



For further information on management/diagnostic variables, please refer to [“Management/diagnostic variables for each configured F-Device” on page 191](#) and [“Global management/diagnostic variables for F-Devices” on page 195](#).

- Double-click on the “Profinet (x)” node in the “PLANT” area.

The “/ Profinet” editor group opens.

- Select the “Settings” editor.

In the “Profisafe - device diagnostic variables” view, you can specify which management/diagnostic variables are to be generated for each F-Device configured in the project (see [Figure 4-43](#)).

The screenshot shows the 'Settings' window in PLCnext Engineer. The left sidebar contains a tree view with the following categories: All, Profinet controller, Update tasks, Profisafe - device diagnostic variables (highlighted), Profisafe - summarizing diagnostic variables, and Profile. The main area displays the 'Profisafe - device diagnostic variables' configuration table.

Variable Name	Setting
F_ADDR_[nnnnn]_ACK_REQ: ①	create
F_ADDR_[nnnnn]_ACK_REI: ①	create
F_ADDR_[nnnnn]_PASS_OUT: ①	create
F_ADDR_[nnnnn]_PASS_ON: ①	create
F_ADDR_[nnnnn]_DEVICE_FAULT: ①	create
F_ADDR_[nnnnn]_CE_CRC: ①	create
F_ADDR_[nnnnn]_WD_TIMEOUT: ①	create
F_ADDR_[nnnnn]_IPAR_OK: ①	do not create
F_ADDR_[nnnnn]_IPAR_EN: ①	do not create
F_ADDR_[nnnnn]_CHF_ACK_REI: ①	do not create
F_ADDR_[nnnnn]_CHF_ACK_REQ: ①	do not create
F_ADDR_[nnnnn]_CE_CRC_H: ①	do not create
F_ADDR_[nnnnn]_WD_TIMEOUT_H: ①	do not create
F_ADDR_[nnnnn]_LOOPBACK: ①	do not create

Figure 4-43 Management/diagnostic variables for each configured F-Device

In the “Profisafe - summarizing diagnostic variables” view, you can specify which management/diagnostic variables are to be globally generated once for all PROFIsafe F-Devices configured in the project (see Figure 4-43).

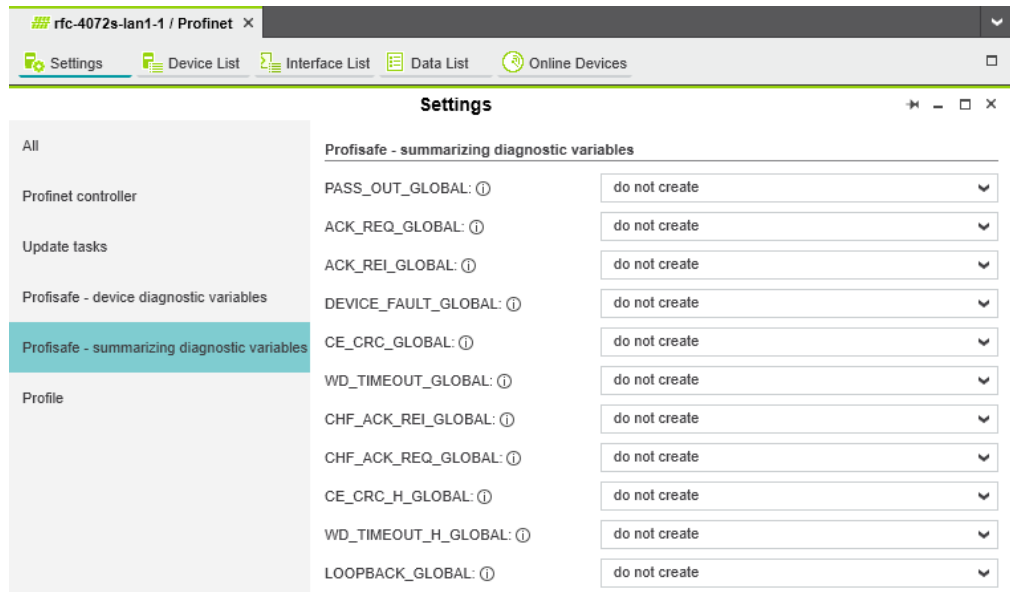


Figure 4-44 Management/diagnostic variables for all configured F-Devices

Created variables are displayed in the “Data List” editor of the controller node:

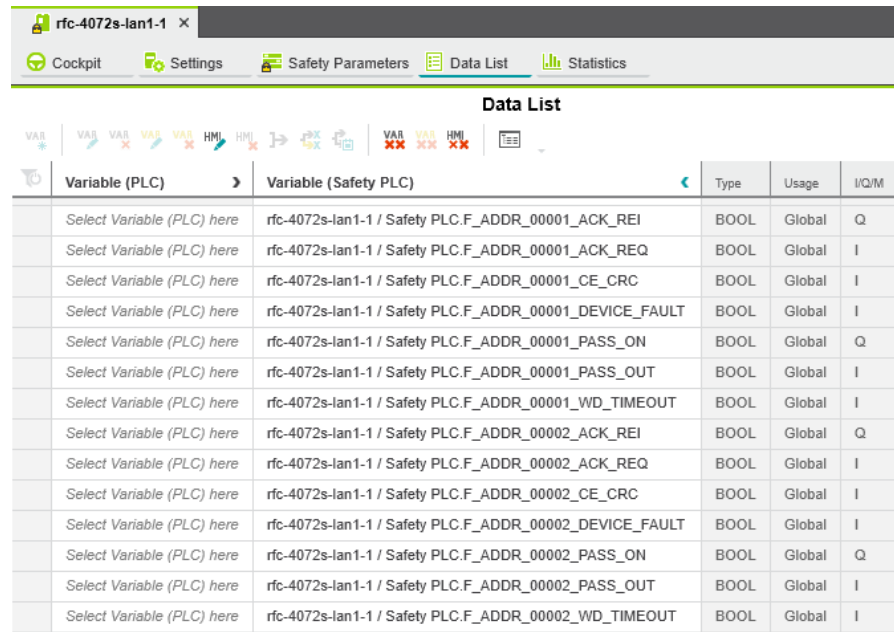


Figure 4-45 Management/diagnostic variables of F-Devices (default)

For the two F-Devices used in the example, PLCnext Engineer creates 14 variables by default.

4.15.3 Checking/setting safety parameters for configured F-Devices

For configured F-Devices, you must check and possibly set various safety parameters, depending on the safety function and safety integrity. Specifically, these are F-Address F_Dest_Add, watchdog time F_WD_Time, and the input/output parameters.



WARNING: Safety and availability of the system/machine

Select a suitable watchdog time (F_WD_Time) to ensure the safety and availability of your system/machine.

Select a watchdog time that is long enough to ensure the safety of your system/machine with maximum possible availability.



For further information on selecting the watchdog time, please refer to [Section 2.3](#) on [page 35](#).

- Under the “Profinet (x)” node in the “PLANT” area, double-click on the lower-level node of the safety module whose safety parameters you want to set (in the example in [Figure 4-46](#) on [page 131](#): AXL F PSDI8/4 1F).

The safety module editor group opens.

- Select the “Safety Parameters” editor.



If you are not currently logged into the safety-related area, you will now be prompted to enter the password in the “PROJECT AUTHENTICATION” dialog that opens (see [“Project login required”](#) on [page 111](#)).

All	F_Parameter
F_Parameter	F_Source_Add: 1024
Input 00 Channel 1 / Channel 2	F_Dest_Add: 1
Input 01 Channel 1 / Channel 2	F_WD_Time: 100
Input 02 Channel 1 / Channel 2	Assignment: both single-channel
Input 03 Channel 1 / Channel 2	Max Filter Duration: 3 ms
	Symmetry: deactivated
	Start inhibit due to symmetry violation: off
	Cross-circuit detection: cross-circuit detection

Safety-related Area: Logged In

Figure 4-46 “Safety Parameters” editor: AXL F PSDI8/4 1F

- Set the required safety parameters. In the example in [Figure 4-46](#), these are F-Address F_Dest_Add, watchdog time F_WD_Time, and the assignment of channels 1 and 2 of the inputs.
If necessary, adapt the settings to your application.
- Under the “Profinet (x)” node in the “PLANT” area, double-click on the lower-level node of the safety module whose safety parameters you want to set (in the example in [Figure 4-47](#) on page 132: AXL F PSDO8/3 1F).

The safety module editor group opens.

- Select the “Safety Parameters” editor.

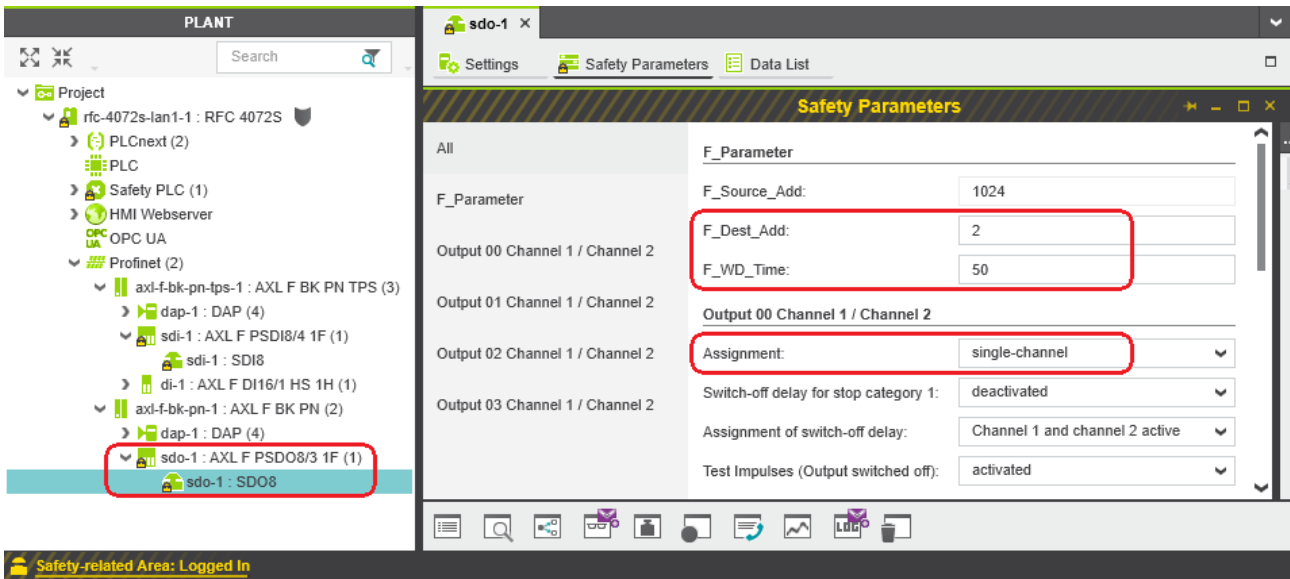


Figure 4-47 “Safety Parameters” editor: AXL F PSDO8/3 1F

- Set the required safety parameters. In the example in [Figure 4-47](#), these are F-Address F_Dest_Add, watchdog time F_WD_Time, and the assignment of channels 1 and 2 of the outputs.
If necessary, adapt the settings to your application.
- Repeat the above safety parameter settings for each safety module used in your application.

4.15.4 Creating variables (exchange variables)

To exchange data between a standard controller and safety-related PLC, you can define “exchange variables” in PLCnext Engineer. These exchange variables are a non-safety-related data type, even though they are variables for a safety-related controller.



Data direction for exchange variables

A data direction must be specified for exchange variables. The data direction determines whether the variable can be read (“I” data direction) or written (“Q” data direction) by the safety-related application. Depending on the set data direction, the standard application has write or read access to the respective variable.

In the example, first create the “Exchange” variable group in PLCnext Engineer as shown in [Figure 4-48](#). Next, create 4 variables for each PROFIsafe F-Device used in the “Variable (PLC)” column in this group. Then, in the “Variable (Safety PLC)” column, create the corresponding 8 non-safety-related exchange variables. These exchange variables are assigned to the safety-related PLC. Finally, set the data direction of the exchange variables.

The screenshot shows the PLCnext Engineer interface. On the left, the project tree under 'PLANT' shows 'rfc-4072s-lan1-1 : RFC 4072S' with 'PLC' selected. On the right, the 'Data List' editor is open, showing a table with two columns: 'Variable (PLC)' and 'Variable (Safety PLC)'. A red box highlights a group named 'Exchange' containing 8 rows of variables. Below the table, there are sections for 'Default' and 'System Variables'.

Variable (PLC)	Variable (Safety PLC)
rfc-4072s-lan1-1 / PLC.PSDI_ACK_REQ	rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REQ
rfc-4072s-lan1-1 / PLC.PSDI_ACK_REI	rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REI
rfc-4072s-lan1-1 / PLC.PSDI_PASS_OUT	rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_OUT
rfc-4072s-lan1-1 / PLC.PSDI_PASS_ON	rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_ON
rfc-4072s-lan1-1 / PLC.PSDO_ACK_REQ	rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REQ
rfc-4072s-lan1-1 / PLC.PSDO_ACK_REI	rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REI
rfc-4072s-lan1-1 / PLC.PSDO_PASS_OUT	rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_OUT
rfc-4072s-lan1-1 / PLC.PSDO_PASS_ON	rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_ON

Figure 4-48 Exchange variables in the example

- Double-click on the “PLC” node in the “PLANT” area.

The “/ PLC” controller editor group opens.

- Select the “Data List” editor.
- Click on the button to generate a new variable group.
- Rename the new variable group “Exchange”.
- Enter the names of the variables in the “Variable (PLC)” column in turn as shown in [Figure 4-48](#).

- In the “Variable (Safety PLC)” column, select “Add Variable (Safety PLC)” in the context menu for each variable you created earlier in turn (see [Figure 4-49](#)).

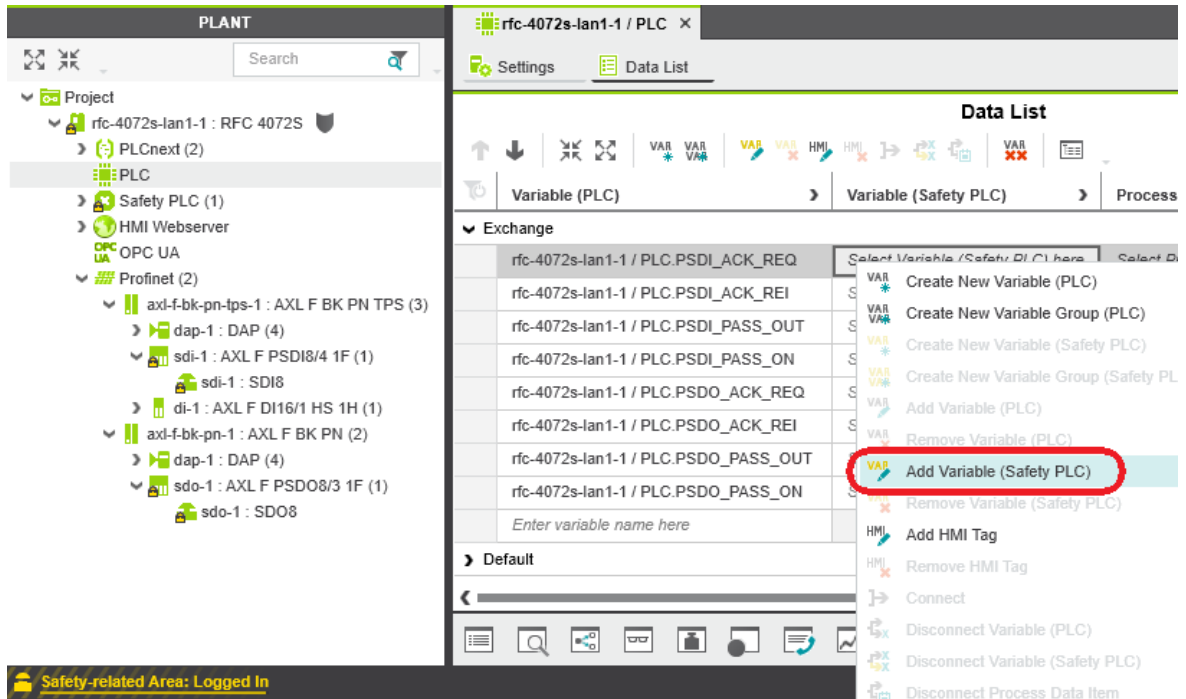


Figure 4-49 “Add Variable (Safety PLC)” context menu

After you have created the exchange variables, you need to specify the data direction (I/Q).

Data direction

Set the data direction for the exchange variables. Refer to the information provided at the start of this section on [page 133](#).

- Set the data direction in turn for each variable created earlier as shown in [Figure 4-50](#).

The screenshot shows the 'Data List' window for project 'rfc-4072s-lan1-1 / PLC'. The 'Exchange' section is expanded, displaying a table of variables. The variable 'rfc-4072s-lan1-1 / PLC.PSDO_PASS_ON' is selected, and its data direction is set to 'I' (Input), which is highlighted with a red circle.

Variable (PLC)	Variable (Safety PLC)	Type	Usage	I/Q/M	Comr
rfc-4072s-lan1-1 / PLC.PSDI_ACK_REQ	rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REQ	BOOL	Global	Q	
rfc-4072s-lan1-1 / PLC.PSDI_ACK_REI	rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REI	BOOL	Global	I	
rfc-4072s-lan1-1 / PLC.PSDI_PASS_OUT	rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_OUT	BOOL	Global	Q	
rfc-4072s-lan1-1 / PLC.PSDI_PASS_ON	rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_ON	BOOL	Global	I	
rfc-4072s-lan1-1 / PLC.PSDO_ACK_REQ	rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REQ	BOOL	Global	Q	
rfc-4072s-lan1-1 / PLC.PSDO_ACK_REI	rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REI	BOOL	Global	I	
rfc-4072s-lan1-1 / PLC.PSDO_PASS_OUT	rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_OUT	BOOL	Global	Q	
rfc-4072s-lan1-1 / PLC.PSDO_PASS_ON	rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_ON	BOOL	Global	I	
Enter variable name here				I	

Figure 4-50 Setting the data direction

4.15.5 Opening a safety-related POU



For further information on opening and creating POU, please refer to [Section “Opening and creating the POU” on page 114](#).

For detailed notes on operating the PLCnext Engineer software, please refer to the online help for the software.

When you create a project, a Program Organization Unit (POU) with the name “S_Main” is created automatically for safety-related controllers in the “COMPONENTS” area under “Programs” (see [Figure 4-24 on page 115](#)).

- Click on “Programming (x)” in the “COMPONENTS” area.
- Then click on the arrow next to “Local (x)”, then on “Programs (x)”.
- Double-click on the desired safety-related POU (in the example: “S_Main” program).

The editor group for the selected POU opens.

4.15.6 Creating variables

Creating variables for safe logical ANDing

The following table shows the variables to be created in the safety-related example program (safe logical ANDing), which will later further be used in PLCnext Engineer.

Table 4-5 Input/output variables in the example (safe logical ANDing)

Parameter	Variable name	Data type	Use	Description
IN1	PSDI_IN_1 (input 0, channel 1)	SAFEBOOL	External	Input IN0_CH1 (AXL F PSDI8/4 1F)
IN2	PSDI_IN_2 (input 0, channel 2)	SAFEBOOL	External	Input IN0_CH2 (AXL F PSDI8/4 1F)
OUT	PSDO_OUT_1 (output 0, channel 1)	SAFEBOOL	External	Output OUT0_CH1 (AXL F PSDO8/3 1F)

- Select the “Variables” editor.
- Create the variables that you need for the selected POU (in the example in [Figure 4-51](#): S_Main).
- Set the type and use for all created variables.

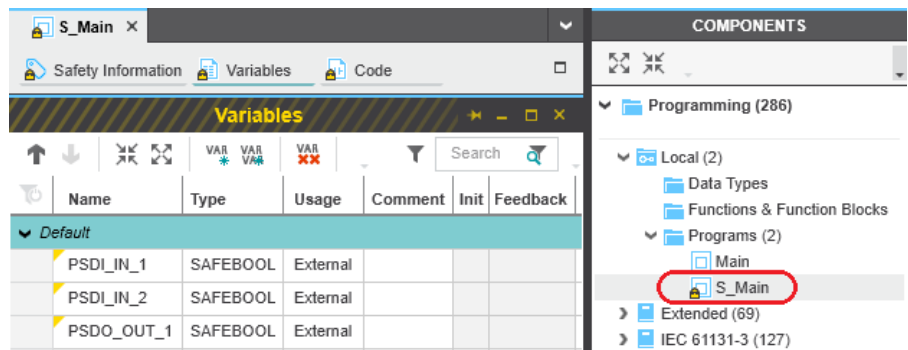


Figure 4-51 Creating variables for a POU (in the example: for the “S_Main” POU)

Selecting management/diagnostic variables and exchange variables

Before you can use previously created exchange variables and default management/diagnostic variables in the code worksheet, you must select these variables in the variables worksheet.

- Select the “Variables” editor.
- Open the selection list by clicking on the arrow in the “Name” field (see [Figure 4-52](#)).
- Select the “Safety PLC”.
- Select the corresponding variable on the right-hand side of the window.
- Repeat this step for all the management/diagnostic variables and exchange variables shown in [Figure 4-52](#).

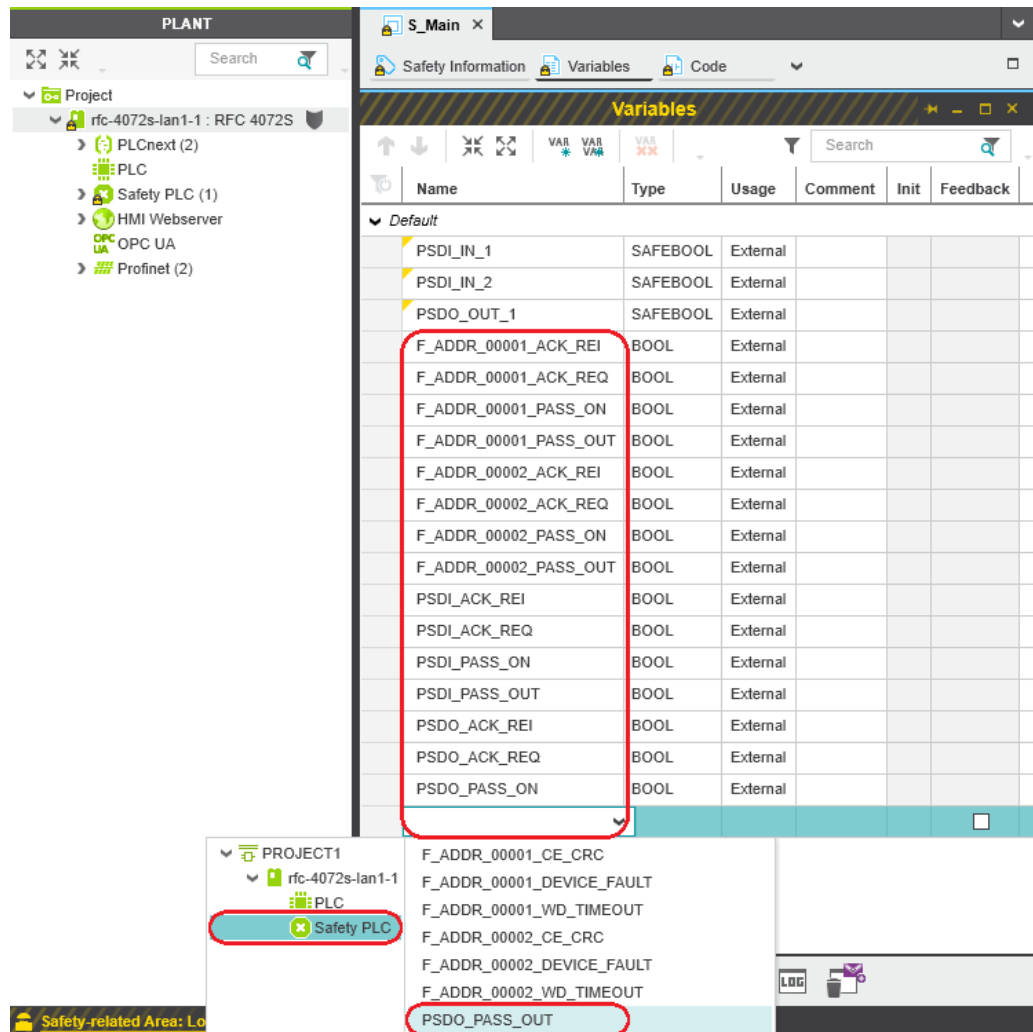


Figure 4-52 Selecting management/diagnostic variables

Once you have created all of the necessary variables, create the program for the selected POU, see [Section 4.15.7](#).

4.15.7 Creating a safety-related program

Safety-related example program

The safety-related example program in [Figure 4-53 on page 138](#) involves safe logical AND-ing of two input variables. The result of the ANDing is connected to an output variable. The input/output variables are connected to process data in due course.

In addition, all the variables from the “Exchange” variable group that were created earlier (see [Figure 4-48 on page 133](#)) are connected to the corresponding exchange variables that were created earlier.

Creating a program

To create a program, proceed as follows:

- Select the program editor.

The program editor is referred to as “Code” by default. You can change the designation of the program editor as desired.

- Create the program as shown in [Figure 4-53 on page 138](#).

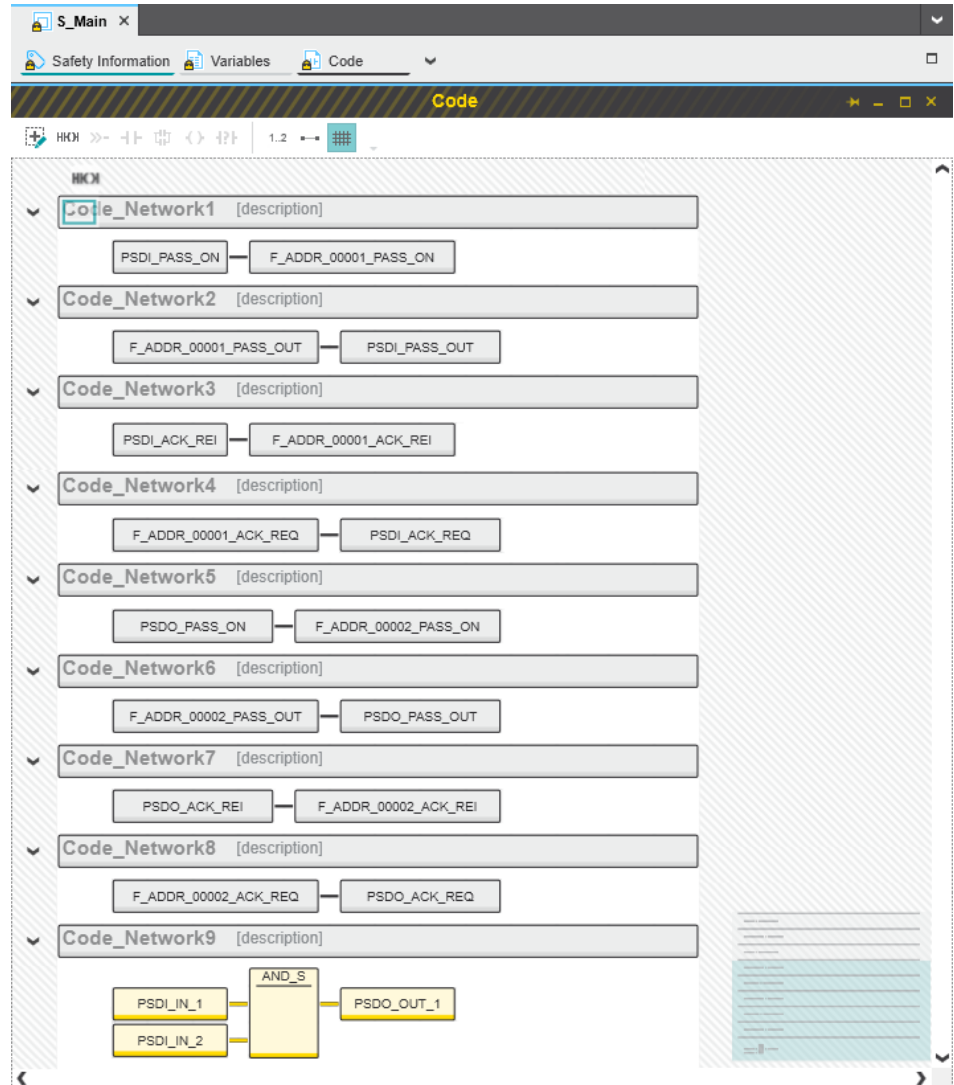


Figure 4-53 Safety-related example program

4.15.8 Assigning process data

To assign a process data item to a variable, proceed as follows:

- Double-click on the “Safety PLC (x)” node in the “PLANT” area.

The “Safety PLC (x)” controller editor group opens.

- Select the “Data List” editor.

You can see an overview of all available variables in the “Data List” editor.

- In the “Process Data Item” column, use the role picker to assign the corresponding process data (see also [Section “Assigning process data” on page 119](#)) to all variables (see marked section in [Figure 4-54](#)).

Variable (Safety PLC)	Variable (PLC)	Process Data Item	I/Q	Type	Offset
rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REQ	rfc-4072s-lan1-1 / PLC.PSDI_ACK_REQ	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDI_ACK_REI	rfc-4072s-lan1-1 / PLC.PSDI_ACK_REI	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_OUT	rfc-4072s-lan1-1 / PLC.PSDI_PASS_OUT	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDI_PASS_ON	rfc-4072s-lan1-1 / PLC.PSDI_PASS_ON	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REQ	rfc-4072s-lan1-1 / PLC.PSDO_ACK_REQ	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDO_ACK_REI	rfc-4072s-lan1-1 / PLC.PSDO_ACK_REI	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_OUT	rfc-4072s-lan1-1 / PLC.PSDO_PASS_OUT	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDO_PASS_ON	rfc-4072s-lan1-1 / PLC.PSDO_PASS_ON	Select Process Data Item here			
rfc-4072s-lan1-1 / Safety PLC.PSDI_IN_1	Select Variable (PLC) here	rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / sdi-1 / sdi-1 / IN00 CH1/2	I	BOOL	0.0
rfc-4072s-lan1-1 / Safety PLC.PSDI_IN_2	Select Variable (PLC) here	rfc-4072s-lan1-1 / axl-f-bk-pn-tps-1 / sdi-1 / sdi-1 / IN00 CH2	I	BOOL	0.1
rfc-4072s-lan1-1 / Safety PLC.PSDO_OUT_1	Select Variable (PLC) here	rfc-4072s-lan1-1 / axl-f-bk-pn-1 / sdo-1 / sdo-1 / OUT00 CH1/2	Q	BOOL	0.0

Figure 4-54 Assigned safety-related process data

4.16 Transferring a project to the controller




For further information on transferring a non-safety-related project to the standard controller, please refer to [Section “Transferring a project to the controller” on page 124](#).

4.16.1 Transferring a non-safety-related project to the standard controller

To transfer the project to the standard controller, proceed as follows:

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Cockpit” editor.
- Click on the  button.



User authentication

If necessary, refer to the information about user authentication on [page 106](#).

- If necessary, enter the user name and password in the dialog that opens.

The project is compiled and transferred to the standard controller. Execution of the project is started and the standard controller (“PLCnext” tile) switches to the “RUN” state.

If startup was carried out successfully, the following appears on the RFC 4072S display:

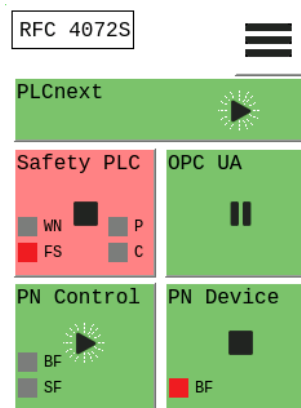
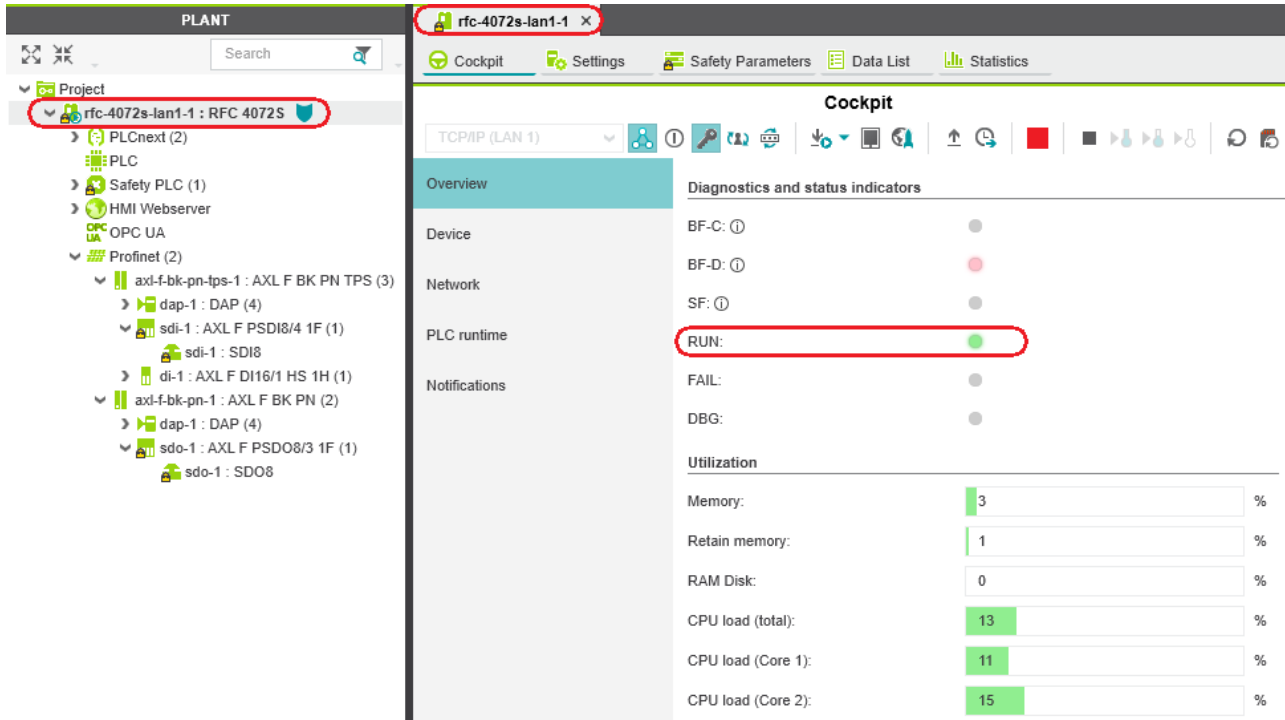


Figure 4-55 Standard controller in the RUN state

The following information is displayed in the “Cockpit” editor:



The screenshot shows the Cockpit editor interface. The left sidebar displays a project tree with the following structure:

- Project
 - rfc-4072s-lan1-1 : RFC 4072 S (highlighted)
 - PLCnext (2)
 - PLC
 - Safety PLC (1)
 - HMI Webserver
 - OPC UA
 - Profinet (2)
 - axl-f-bk-pn-tps-1 : AXL F BK PN TPS (3)
 - dap-1 : DAP (4)
 - sdi-1 : AXL F PSDI8/4 1F (1)
 - sdi-1 : SDI8
 - di-1 : AXL F DI16/1 HS 1H (1)
 - axl-f-bk-pn-1 : AXL F BK PN (2)
 - dap-1 : DAP (4)
 - sdo-1 : AXL F PSDO8/3 1F (1)
 - sdo-1 : SDO8

The main area displays the 'Cockpit' interface for 'rfc-4072s-lan1-1'. The 'Diagnostics and status indicators' section shows the following indicators:

Indicator	Status
BF-C:	Off
BF-D:	Off
SF:	Off
RUN:	On
FAIL:	Off
DBG:	Off

The 'Utilization' section shows the following metrics:

Metric	Value	Unit
Memory:	3	%
Retain memory:	1	%
RAM Disk:	0	%
CPU load (total):	13	%
CPU load (Core 1):	11	%
CPU load (Core 2):	15	%

Figure 4-56 Standard controller in the “RUN” state

If an installation error prevents the system from starting up, a corresponding error message appears on the display and in PLCnext Engineer.



The iSPNS 3000 is in the FAIL state because the example project has not yet been transferred to the iSPNS 3000.

4.16.2 Transferring a safety-related project to the safety-related controller (defining a controller password, if necessary)

To transfer the project to the safety-related controller, proceed as follows:

- Double-click on the “Safety PLC (x)” node in the “PLANT” area.

The “Safety PLC” editor group opens.

- Select the “Safety Cockpit” editor.
- Click on the  button.



User authentication

If necessary, refer to the information about user authentication on [page 106](#).

- If necessary, enter the user name and password in the dialog that opens.

Defining a controller password for the safety-related controller

The safety-related controller is protected by a controller password. Writing data to the safety-related PLC or changing its operating mode is only possible after entering the controller password in PLCnext Engineer.

If this is the first time you are attempting to connect to the safety-related controller, PLCnext Engineer will prompt you to define a controller password.

- Specify a controller password, if you have not already done so, and the following dialog will be displayed.

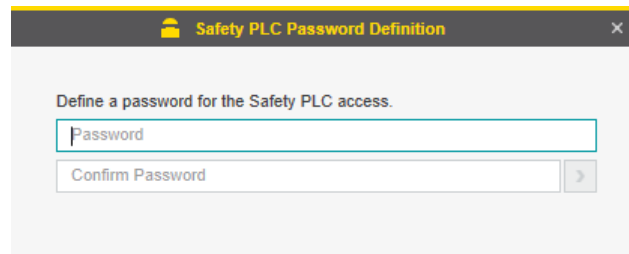


Figure 4-57 Controller password: entering the password for the safety-related controller



Please note: read information dialogs carefully and follow the instructions provided

If information dialogs appear, please refer to the online help for PLCnext Engineer for further information.

- Acknowledge the messages in accordance with your application.

In the example:

Make sure no hazard is posed by the safety-related controller being started and/or stopped, e.g., after downloading a project.

Ensure the safety function is in order.

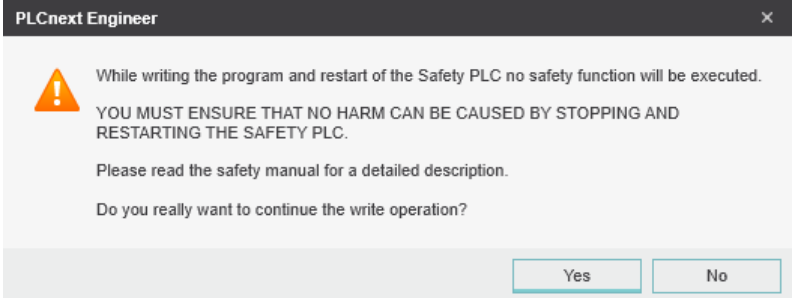


Figure 4-58 Information dialog: prevent any hazard posed by the safety-related controller being started and stopped

The project is compiled and transferred to the safety-related controller. Execution of the safety-related project is started and the safety-related controller (“Safety PLC” tile) switches to the “RUN” state.

If startup was carried out successfully, the following appears on the RFC 4072S display:

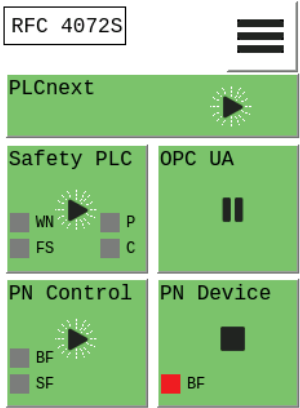


Figure 4-59 Safety-related controller in the RUN state

The following information is displayed in the “Safety Cockpit” editor:

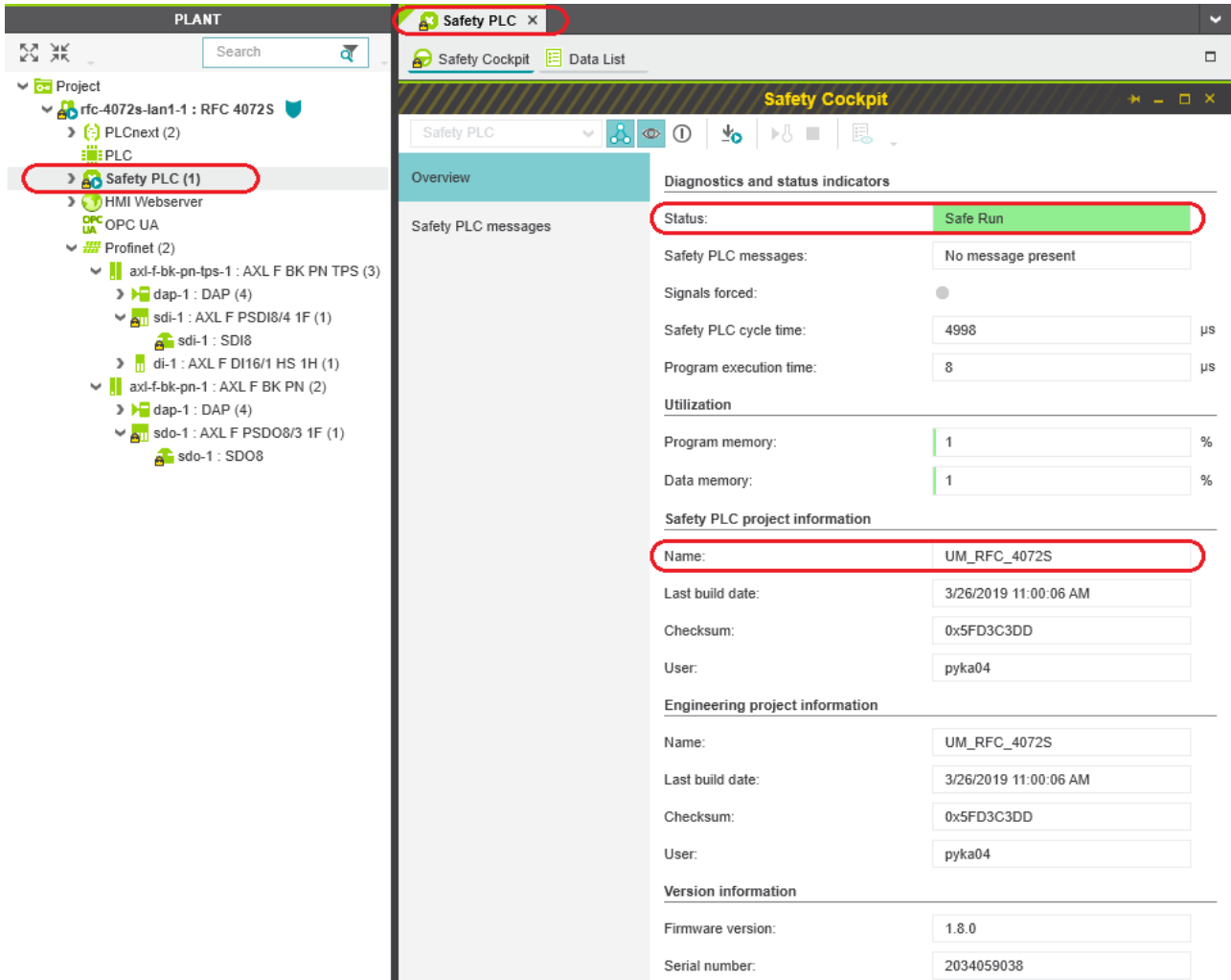


Figure 4-60 Safety Cockpit: safety-related controller in the “RUN” state – Safe Run

If an installation error prevents the system from starting up, a corresponding error message appears on the display and in PLCNext Engineer.



4.17 Displaying online values

To view online variable values, you can “attach to the controller”. To do this, you must have successfully compiled the project, transferred it to the controller, and started it.

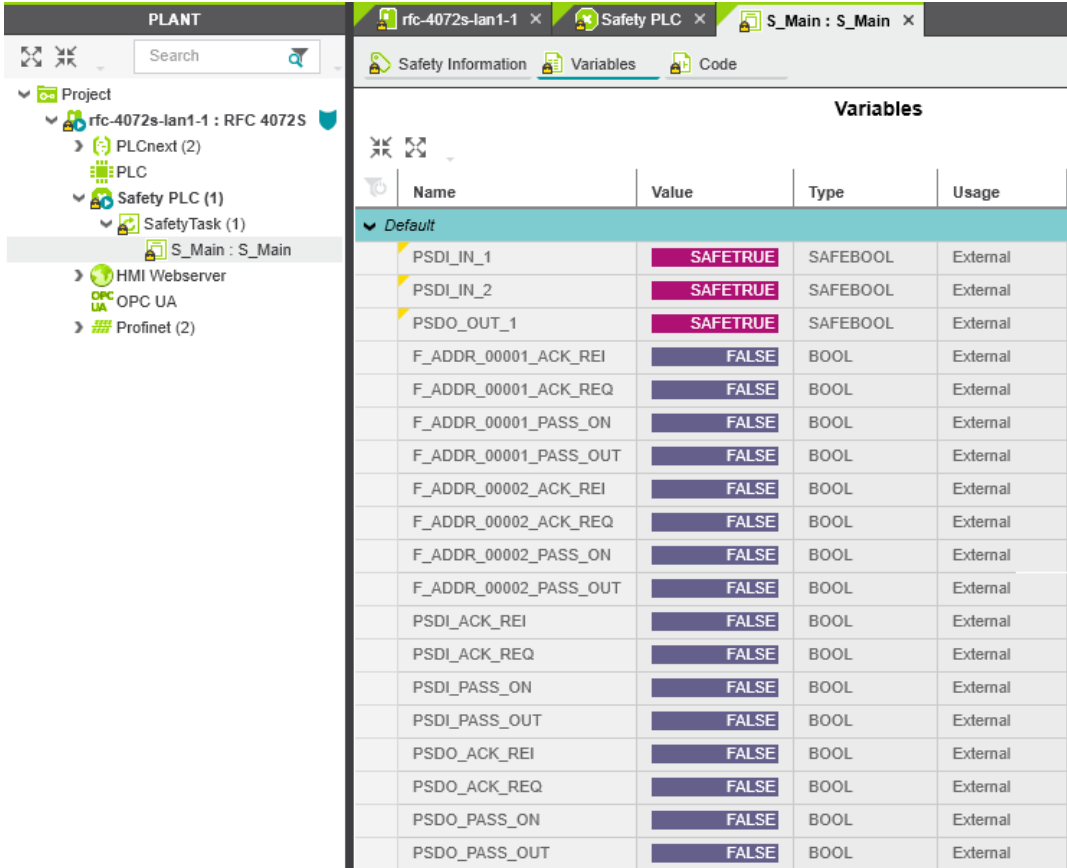
Proceed as follows:

- Double-click on the “Safety PLC (x)” node in the “PLANT” area.

The “Safety PLC” editor group opens.

- Select the “Safety Cockpit” editor.
- Click on the  button (“Connect to the controller to establish communication with online services.”).
- Click on the  button (“Enables or disables the monitoring mode for safety related editors to see online values.”).
- Open the instance editor of the “S_Main” POU by double-clicking on the “S_Main : S_Main” node.

The online values of the variables used in the “S_Main” POU are displayed in the “Variables” and “Code” editors.



Name	Value	Type	Usage
Default			
PSDI_IN_1	SAFETRUE	SAFEBOOL	External
PSDI_IN_2	SAFETRUE	SAFEBOOL	External
PSDO_OUT_1	SAFETRUE	SAFEBOOL	External
F_ADDR_00001_ACK_REI	FALSE	BOOL	External
F_ADDR_00001_ACK_REQ	FALSE	BOOL	External
F_ADDR_00001_PASS_ON	FALSE	BOOL	External
F_ADDR_00001_PASS_OUT	FALSE	BOOL	External
F_ADDR_00002_ACK_REI	FALSE	BOOL	External
F_ADDR_00002_ACK_REQ	FALSE	BOOL	External
F_ADDR_00002_PASS_ON	FALSE	BOOL	External
F_ADDR_00002_PASS_OUT	FALSE	BOOL	External
PSDI_ACK_REI	FALSE	BOOL	External
PSDI_ACK_REQ	FALSE	BOOL	External
PSDI_PASS_ON	FALSE	BOOL	External
PSDI_PASS_OUT	FALSE	BOOL	External
PSDO_ACK_REI	FALSE	BOOL	External
PSDO_ACK_REQ	FALSE	BOOL	External
PSDO_PASS_ON	FALSE	BOOL	External
PSDO_PASS_OUT	FALSE	BOOL	External

Figure 4-61 “Variables” editor (S_Main): online values of the variables used

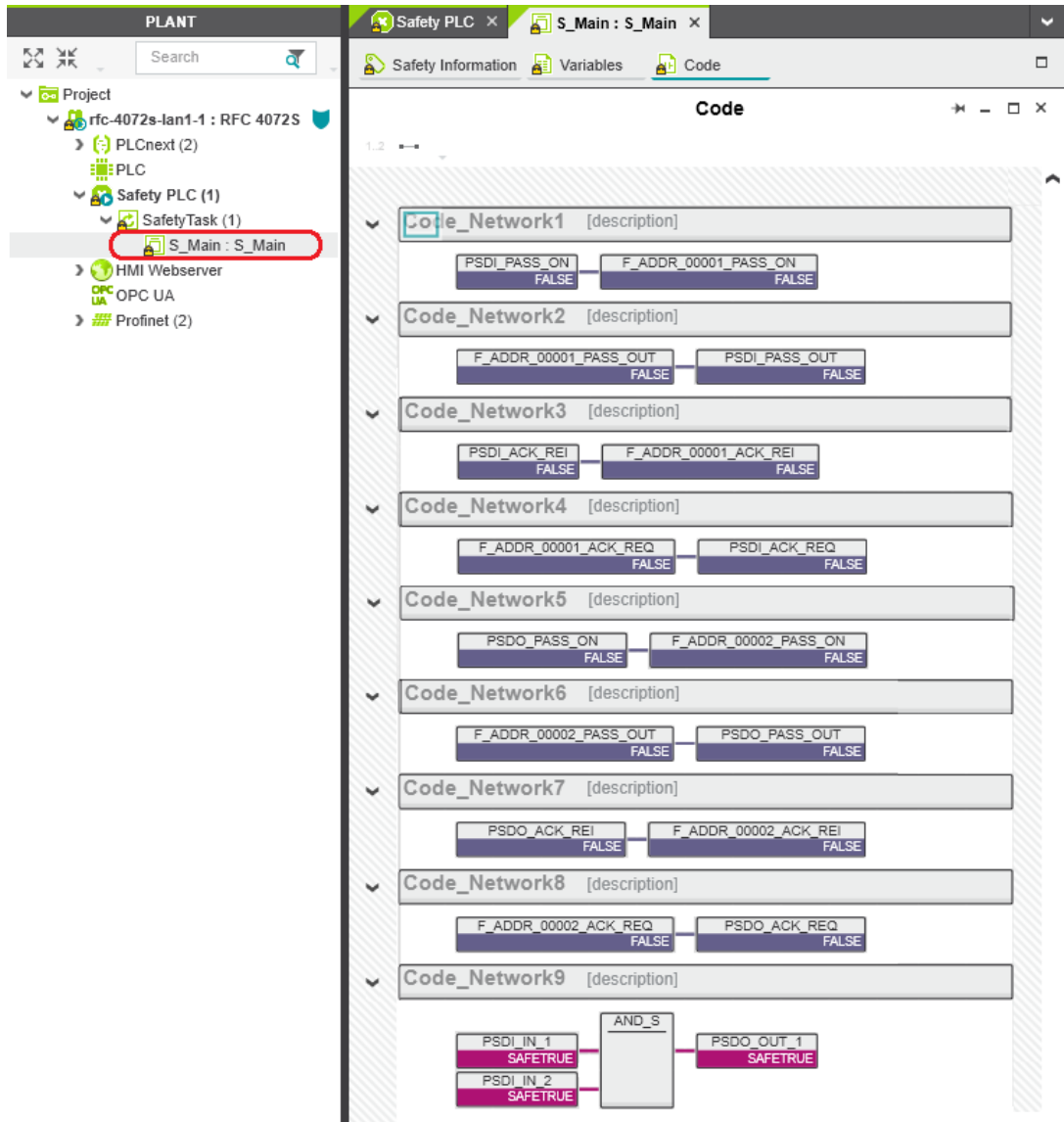




Figure 4-62 “Code” editor (S_Main): online values of the variables used

4.18 PLCnext Engineer – Debug mode

- Double-click on the “Safety PLC (x)” node in the “PLANT” area.

The “Safety PLC” editor group opens.

- Select the “Safety Cockpit” editor.
- Click on the  button (“Connect to the controller to establish communication with online services.”).
- To enable debug mode, click on the  button (“Enables or disables the debug mode at the safety related PLC.”).



WARNING:

Switching to debug mode means that you will exit normal mode.

Make sure that your system/machine cannot pose a hazard to people or equipment.

- Acknowledge the following message to switch to debug mode.

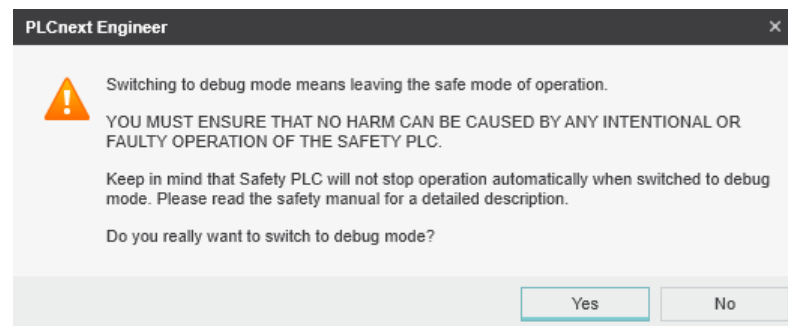


Figure 4-63 Exiting safe mode – switching to debug mode

Debug mode is indicated as follows on the display:

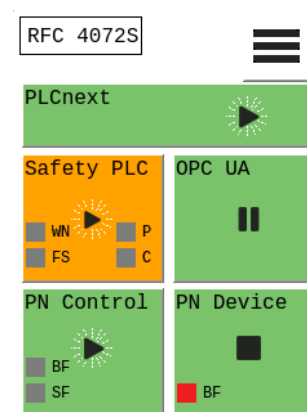



Figure 4-64 Display: debug mode indicated

- To disable debug mode and switch to safe mode, click on the  button.

**WARNING:**

Make sure that your system/machine cannot pose a hazard to people or equipment.

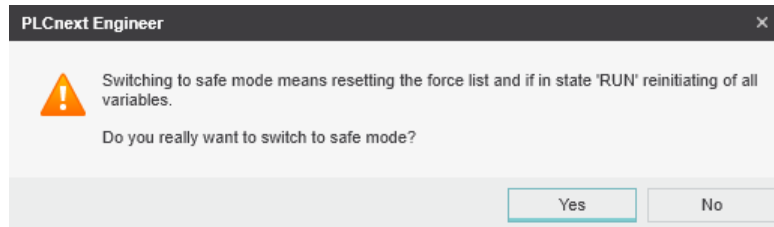


Figure 4-65 Exiting debug mode – switching to safe mode

4.19 Operator acknowledge

F-Devices whose communication relationship with the iSPNS 3000 is aborted, e.g., due to a communication error, are passivated. The passivated F-Device indicates this by means of the `F_ADDR_XXXX_PASS_OUT` variables. As soon as the communication relationship between the F-Host and F-Device has been reestablished, the F-Device generates an operator acknowledge request (indicated by means of the `F_ADDR_XXXX_ACK_REQ` variable) to request its reintegration. This operator acknowledge request can be acknowledged by an operator acknowledge reintegration (`F_ADDR_XXXX_ACK_REI`).

**WARNING: Outputs can be set**

Do not acknowledge an operator acknowledge request automatically from the application program. Acknowledgment must be triggered by an intentional user action.

When reintegrating passivated PROFIsafe devices, safety-related outputs can be set.

Take appropriate measures to ensure that your system/machine does not present any danger when passivated PROFIsafe devices are reintegrated.

In the following example, the communication relationship between the AXL F PSDI8/4 1F and AXL F PSDO8/3 1F F-Devices and the iSPNS 3000 is lost, e.g., due to an error in the network. Passivation prevents the disabled F-Devices being started up immediately as soon as the communication relationship is reactivated. Passivation using the `F_ADDR_00001_PASS_OUT` and `F_ADDR_00002_PASS_OUT` Boolean values is shown. The passivated F-Devices each send an operator acknowledge request using the `F_ADDR_00001_ACK_REQ` and `F_ADDR_00002_ACK_REQ` Boolean variables if their communication relationship has been reestablished without errors. This means they are waiting for a reintegration acknowledgment. By setting the `PSDI_ACK_REI` and `PSDO_ACK_REI` Boolean variables in the non-safety-related part of the example program, passivation of each F-Device can be overridden, i.e., the F-Devices can be reintegrated into the network and their communication relationship restored. [Figure 4-66](#) below shows the passivated F-Devices.

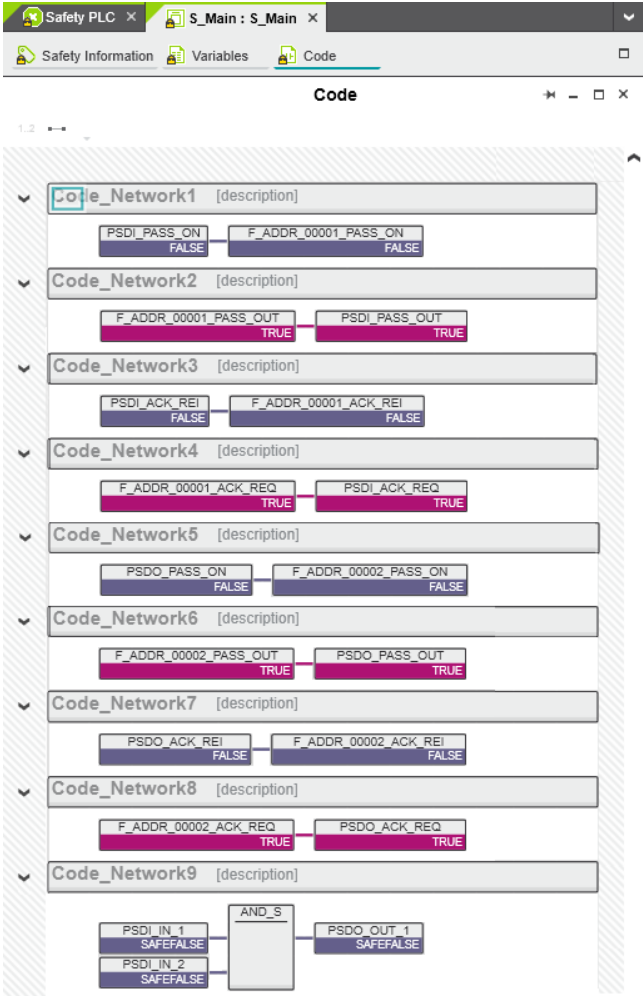


Figure 4-66 PLCnext Engineer – Passivated PROFIsafe F-Devices

In the example in [Figure 4-66](#), the safe inputs and safe outputs have entered the SAFE-FALSE state. This behavior is due to the passivation of the F-Devices.

5 Errors, diagnostic messages and troubleshooting

The RFC combines various systems whose diagnostic and troubleshooting mechanisms are described below.

These include:

- PROFINET (see [“Diagnostics for PROFINET” on page 151](#))
- PROFIsafe (see [“Diagnostics for F-Devices” on page 151](#) and [“Diagnostics for iSPNS 3000” on page 151](#))

5.1 Diagnostics for PROFINET

Diagnostic messages for PROFINET are available as follows:

- Indication on the display
- Entries in the Notification Logger (Notification Manager)
- PROFINET-specific system variables in PLCnext Engineer (can be accessed in the application program)



For detailed information on the Notification Logger and the Notification Manager, please refer to the UM EN PLCNEXT TECHNOLOGY user manual.

5.2 Diagnostics for F-Devices

PROFIsafe provides comprehensive diagnostic mechanisms that are defined in the PROFIsafe specification. For information on the PROFIsafe specification, please refer to [Section “Documentation” on page 246](#).

Diagnostic messages for F-Devices are available as follows:

- Entries in the Notification Logger (Notification Manager)
- PROFIsafe-specific system variables in PLCnext Engineer (can be accessed in the application program, see [Section 8.3.1 on page 184](#))



For detailed information on the Notification Logger and the Notification Manager, please refer to the UM EN PLCNEXT TECHNOLOGY user manual.

Refer to the device-specific user documentation for the F-Devices being used.

5.3 Diagnostics for iSPNS 3000

The diagnostic and monitoring function integrated in the iSPNS 3000 detects errors that have occurred. All serious errors detected in the iSPNS 3000, which can lead to the loss of or adversely affect the programmed safety function, switch the device to the failure state. In this state, the outputs of the F-Devices are set to zero after the parameterized F_WD_TIME for the relevant output has elapsed at the latest. The PROFIsafe system switches to the safe state.

**Exiting the failure state of the iSPNS 3000**

Note that you can only leave the failure state by doing the following:

- Download the safety-related project in the PLCnext Engineer software again, or
- Switch off the supply voltage of the RFC for at least 30 s and then switch it back on again (power UP), or
- Restart the RFC via the display or in the “Cockpit” editor of the standard controller in the PLCnext Engineer software.

Diagnostic messages for the iSPNS 3000 are available as follows:

- Entries are stored in the diagnostic memory of the iSPNS 3000 (can be read with PLCnext Engineer)
- Indication on the display (“Safety PLC” tile)
- As a hexadecimal value in the diagnostic parameter registers of the iSPNS 3000. The registers are elements of the SPNSV2_TYPE structure, see [Table 8-1 on page 184](#).
Diagnostic parameter register 1: DIAG.PARAM_REG and
Diagnostic parameter register 2: DIAG.PARAM_2_REG



For detailed information on diagnostics in the PLCnext Engineer software, please refer to the online help for the software.



Please contact your nearest Phoenix Contact representative if:

- One of the errors described in [Section “Errors with error codes” on page 154](#) occurs again.
- Errors occur that are not listed in [Section “Possible errors” on page 152](#).

5.4 Possible errors

This section describes possible errors, their causes, effects, and remedy. [Section “Errors with error codes” on page 154](#) lists errors according to their error code.

Important notes:**FS LED/FS bit/failure state**

Please note that for all error codes listed in [Table 5-1 on page 154](#), the FS LED is always on in the diagnostic display of the RFC 4072S and the FS bit is set in the SPNS_DIAG_STATUS_REG register.

The iSPNS 3000 enters the failure state.



Observe error codes

If errors occur, always provide the service/support personnel from Phoenix Contact with the complete error code. These details provide important information for error analysis and repair.

The error codes are displayed on the RFC 4072S display, in the SPNS_DI-AG_PARAM_REG and SPNS_DIAG_PARAM_2_REG diagnostic parameter registers, or in the PLCnext Engineer software.

For the safety hotline number, please refer to [Section “Safety hotline” on page 22](#).



Error codes – Channel-dependent representation

Identical errors may occur on both independent processing channels of the iSPNS 3000. Depending on the channel they are marked as follows:

- 0x8xxx Channel 1
- (0x9xxx) Channel 2

For example:

0x8001
(0x9001)

In the following tables, both channel-dependent codes are listed for each error.



Order of project downloads

If further project downloads are required to ensure the consistency of projects, for example, please proceed as follows:

1. Download the non-safety-related project to the standard controller.
2. Download the safety-related project to the iSPNS 3000.

Manual, user-initiated compilation of projects is not required. The PLCnext Engineer software compiles the projects prior to each project download.



Parameterization memory

The terms “SD card” and “(pluggable) parameterization memory” used in this user manual are synonyms.



Phoenix Contact

If the measures/remedies listed in the following tables do not help to remove the error, please contact your nearest Phoenix Contact representative.

5.4.1 Errors with error codes

Table 5-1 RFC 4072S error codes

Error code (hex)	Error cause	Remedy or response
0x8001 (0x9001) to 0x8007 (0x9007)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8008 (0x9008)	The boot project is missing or incomplete.	<ul style="list-style-type: none"> • Check whether the non-safety-related project is loaded on the standard controller. <ul style="list-style-type: none"> – If the non-safety-related project is not loaded on the standard controller, download the safety-related project to the iSPNS 3000 again. – If the non-safety-related project is not loaded on the standard controller, follow the instructions in the note on “Order of project downloads” above this table.
0x8009 (0x9009) to 0x8012 (0x9012)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8013 (0x9013)	The CPU load is higher than 90%.	<ul style="list-style-type: none"> • Reduce the processor load. • Analyze the safety-related project. Optimize the program code for better performance. • Avoid redundancies in the safety-related project so that the CPU load is not increased unnecessarily. • Check if the maximum number of F-Devices to be configured was exceeded. Reduce the number according to the information in Section “Technical data” on page 237, if necessary.

Table 5-1 RFC 4072S error codes

Error code (hex)	Error cause	Remedy or response
0x8014 (0x9014) to 0x8031 (0x9031)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8041 (0x9041) to 0x804A (0x904A)		
0x8061 (0x9061) to 0x806A (0x906A)		
0x8081 (0x9081) to 0x8085 (0x9085)		
0x80A1 (0x90A1) to 0x80A8 (0x90A8)		
0x80AA (0x90AA) to 0x80B0 (0x90B0)		
0x80C1 (0x90C1) to 0x80CE (0x90CE)		
0x80D1 (0x90D1) to 0x80D5 (0x90D5)		
0x80E1 (0x90E1) to 0x80E8 (0x90E8)		
0x80E9 (0x90E9)		

RFC 4072S

Table 5-1 RFC 4072S error codes

Error code (hex)	Error cause	Remedy or response
0x80EA (0x90EA), 0x80EB (0x90EB)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8101 (0x9101) to 0x8107 (0x9107)		
0x8110 (0x9110), 0x8111 (0x9111)		
0x8121 (0x9121) to 0x8125 (0x9125)		
0x8126 (0x9126)	Unknown version of the "pniodev.bin" file.	<ul style="list-style-type: none"> • Check the PLCnext Engineer version that you are using. • Load the non-safety-related project to the standard controller. Download the safety-related project to the iSPNS 3000. Follow the instructions provided in the note on "Order of project downloads" above this table. • If the error cannot be removed, please contact your nearest Phoenix Contact representative.
0x8127 (0x9127)	Unknown version of the "sdevpara.saf" file.	
0x8128 (0x9128)	Unknown version of the "swap.list" file.	

Table 5-1 RFC 4072S error codes



Error code (hex)	Error cause	Remedy or response
0x8129 (0x9129)	Inconsistent device parameter.	<ul style="list-style-type: none"> • Check the device parameterization in your safety-related program. • Boot the iSPNS 3000 by powering off/powering on the RFC 4072S. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  NOTE: Startup of the RFC not ensured For proper startup of the device, the supply voltage must only be switched on 30 seconds after the display goes out at the earliest. </div> <ul style="list-style-type: none"> • Load the non-safety-related project to the standard controller. Download the safety-related project to the iSPNS 3000. Follow the instructions provided in the note on “Order of project downloads” above this table. <p>If none of the steps described above remove the error:</p> <ul style="list-style-type: none"> • Replace the RFC 4072S. • Next, insert a properly working SD card containing the project in the device or carry out the project downloads described in the note on “Order of project downloads” above this table if using a card not containing a project. • Boot the iSPNS 3000 by powering off/powering on the RFC 4072S. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  NOTE: Startup of the RFC not ensured For proper startup of the device, the supply voltage must only be switched on 30 seconds after the display goes out at the earliest. </div> <p>If the procedure described above does not rectify the error, please contact your nearest Phoenix Contact representative.</p>

Table 5-1 RFC 4072S error codes

Error code (hex)	Error cause	Remedy or response
0x812A (0x912A)	Inconsistent process data description.	<ul style="list-style-type: none"> • Check process data assignment in your safety-related project. • Load the non-safety-related project to the standard controller. Download the safety-related project to the iSPNS 3000. Follow the instructions provided in the note on “Order of project downloads” above this table. • If the error cannot be removed, please contact your nearest Phoenix Contact representative.
0x812B (0x912B)	Internal error	Please contact your nearest Phoenix Contact representative.
0x812C (0x912C)	Maximum number of supported F-Devices exceeded.	Reduce the number of F-Devices connected to the RFC.
0x812D (0x912D)	Internal error	Please contact your nearest Phoenix Contact representative.
0x812E (0x912E)		
0x812F (0x912F)	The F-Destination address is invalid or outside the permissible range.	<ul style="list-style-type: none"> • Check the F-Destination addresses used in the project. • If necessary, correct the corresponding addresses.
0x8130 (0x9130)	Maximum number of supported process data descriptions exceeded.	Reduce the number of the process data descriptions.
0x8131 (0x9131) to 0x8136 (0x9136)	Inconsistent process data description.	<ul style="list-style-type: none"> • Check the process data and process data assignment. • Load the non-safety-related project to the standard controller. Download the safety-related project to the iSPNS 3000. Follow the instructions provided in the note on “Order of project downloads” above this table. • If the error cannot be removed, please contact your nearest Phoenix Contact representative.

Table 5-1 RFC 4072S error codes

Error code (hex)	Error cause	Remedy or response
0x8137 (0x9137) to 0x813C (0x913C)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8141 (0x9141) to 0x8150 (0x9150)		
0x8161 (0x9161) to 0x8165 (0x9165)		
0x8181 (0x9181) to 0x8186 (0x9186)		
0x8241 (0x9241) to 0x8247 (0x9247)		
0x8248 (0x9248)	The supply voltage (24 V) is below the specified range.	<ul style="list-style-type: none"> • Check the supply voltage. • Make sure the supply voltage is OK.
0x8249 (0x9249)	The supply voltage (24 V) is above the specified range.	<ul style="list-style-type: none"> • Check the supply voltage. • Make sure the supply voltage is OK.
0x824A (0x924A) to 0x824C (0x924C)	Internal error	Please contact your nearest Phoenix Contact representative.
0x824D (0x924D)	Ambient temperature is not in the specified range.	Check the ambient conditions (e.g., sufficient ventilation in the control cabinet) and operate the RFC 4072S within the range specified.
0x824E (0x924E) to 0x825C (0x925C)	Internal error	Please contact your nearest Phoenix Contact representative.
0x8F00 (0x9F00) to 0x8F02 (0x9F02)		
0x8F03 (0x9F03) to 0x8F07 (0x9F07)	Hardware fault.	
0x8F08 (0x9F08) to 0x8F0B (0x9F0B)	An error occurred during the firmware upgrade.	Observe further instructions from a person instructed in performing the update.

5.5 Evaluation and acknowledgment of module-specific diagnostic messages

Depending on the error type, errors that are diagnosed in the Inline PROFIsafe modules from Phoenix Contact used are transmitted to the RFC 4072S as diagnostic messages using PROFINET.



The product documentation for the modules used contains an overview of the diagnosed errors, their causes, effects, and possible measures for error removal, as well as information regarding module behavior following acknowledgment of diagnostic messages.

- For every error that occurs, the cause of the error must first be removed. If necessary, the error is then acknowledged.

Phoenix Contact provides special function blocks for device-specific diagnostics for the Inline and Axioline backplane bus systems. These function blocks enable global or local device-specific diagnostics.

On the one hand, the AsynCom_PN_Info function block from the AsynCom_V1_06_610200 library must be used for this purpose. This function block is used for reading information of the connected PROFINET devices. The function block receives this information from the configuration of the RFC 4072S (device IDs, PROFINET names, etc.).

On the other hand, function blocks from the PN_Dev_Diag_V1_13 library must be used. An example of device-specific PROFIsafe diagnostics is the PNFD_IL_Diag function block. This function block is used for diagnostics of a safety-related device of the Inline product range via the PROFIsafe address. Displayed diagnostic messages can be confirmed (acknowledged) with the help of the function block.

5.5.1 AsynCom_PN_Info_V1_01 function block

Function block for reading information of the connected PROFINET devices.

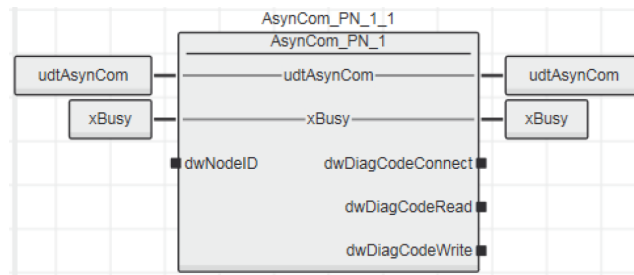


Figure 5-1 AsynCom_PN_1 function block (instance: AsynCom_PN_1_1)

5.5.2 PNFD_IL_Diag_V1_01 function block

Function block for diagnostics of a secure device of the Inline product range via the PROFIsafe address. Diagnostic messages that need to be confirmed can be confirmed with the help of the block.

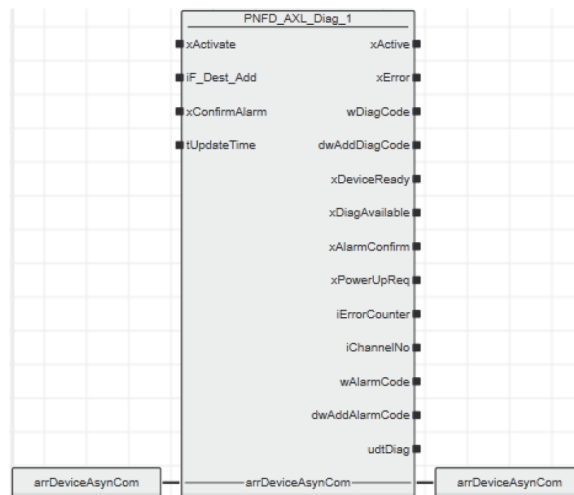


Figure 5-2 Function block PNFD_AXL_Diag_1
(Instance: PNFD_IL_Diag_V1_01_1)

Safety notes for starting applications

Take the following into consideration when determining and programming the start conditions for your machine or system:

- The machine or system may only be started if it can be ensured that nobody is present in the danger zone.
- Meet the requirements of EN ISO 13849-1 with regard to the manual reset function. The machine must not be set in motion and/or a hazardous situation must not be triggered by the following actions, for example:
 - Switching on safe devices
 - Acknowledging device error messages
 - Acknowledging communication errors
 - Acknowledging block error messages in the application
 - Removing startup inhibits for safety functions

Observe the following when programming/configuration the safety logic:

- Switching from the safe state (substitute value = 0) to the operating state can generate an edge change (zero/one edge).
- In the safety logic, take measures to prevent this edge change resulting in unexpected machine/system startup or restart.



Note for starting applications

Also observe these notes to prevent unexpected machine startup following acknowledgment by means of operator acknowledgment.

6 Maintenance, replacement, firmware update, repair, decommissioning, and disposal

6.1 Maintenance

The RFC 4072S does not require maintenance.

The RFC 4072S does not require repeat testing during mission time.

6.2 Caring for the display

- To clean the display, wipe gently using a soft absorbent cotton cloth soaked in ethanol.
- Avoid scratches on the display by wiping horizontally or vertically instead of with circular movements.



NOTE: Damage to the display

Do not use harmful chemicals when cleaning the display surface, such as acetone, toluene, or isopropyl alcohol.

6.3 Replacing the RFC 4072S

To replace the RFC 4072S, proceed as described in [Section “Replacing the RFC 4072S” on page 85](#).

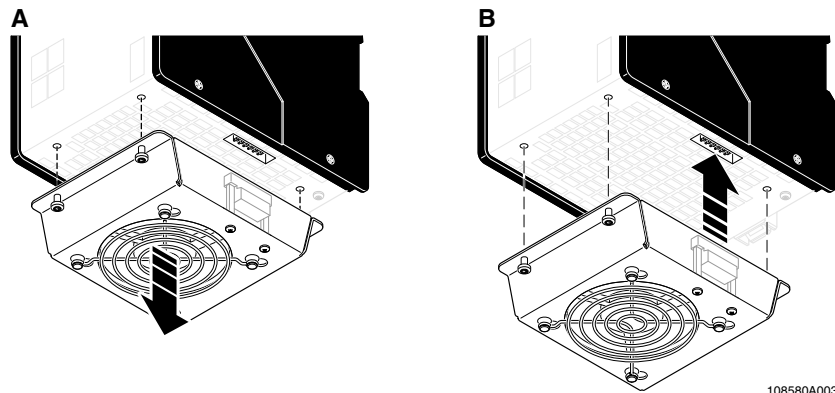
6.4 Replacing the RFC FAN MODULE fan module



NOTE: Potential RFC 4072S malfunction

The fan module must not be replaced during operation. The RFC must be switched off before the fan module can be replaced. To replace the fan module, remove the RFC from the DIN rail.

The procedure for installing and removing the RFC is described in Section “[Replacing the RFC 4072S](#)” on page 85.



108580A003

Figure 6-1 Replacing the RFC FAN MODULE fan module (removal (A), mounting (B))

- Position the fan module on the bottom of the RFC according to [Figure 6-1](#) (B).
- Make sure that the COMBICON connector and the four screws fit properly. Upon delivery of the fan module, the four screws are premounted in the fan module housing.
- Tighten all four M4 screws equally with a recommended tightening torque of 2.2 Nm (3 Nm, maximum).

6.5 Updating the device firmware

Non-safety-related firmware updates of the RFC 4072S are exclusively used for adding new functions that are implemented in the non-safety-related device firmware within the scope of continuous product improvement. No non-safety-related device firmware update is required for normal system operation.

To update, proceed as described in the following in this section.



NOTE: Potential RFC malfunction

Do not interrupt the RFC 4072S supply voltage during the firmware update process. Interruption of the supply voltage can result in a malfunction on the RFC 4072S. In this case, the device can no longer be used.



WARNING:

Take appropriate measures to ensure that the system/machine does not present any danger during the update of the non-safety-related firmware.



NOTE: Important notes on updating the firmware

- Safety-related firmware updates may only be carried out by authorized Phoenix Contact personnel. To update this firmware, please contact your nearest Phoenix Contact representative.
- In terms of safety, updating the non-safety-related firmware is similar to replacing a device. For instructions on how to proceed, refer to [Section “Replacing the RFC 4072S” on page 85](#).
- Please note additional information regarding firmware updates, if applicable. If available, this will be included with the firmware update files.
- Please note that only combinations of firmware and device versions that have been approved by Phoenix Contact may be created.
For information on compatible and approved firmware versions for your devices, and instructions on how to perform updates, please visit phoenixcontact.net/products.

Procedure




NOTE: STOP state required

Only run a firmware update of the RFC 4072S if the standard controller and the iSPNS 3000 are in the **STOP** state.

Creating STOP states

- Double-click on the controller node in the “PLANT” area.

The controller editor group opens.

- Select the “Cockpit” editor.
- Click on the  button to connect PLCnext Engineer to the controller.
- Click on the “Stop the controller” button.

The standard controller switches to the “STOP” state. The state is indicated on the display.

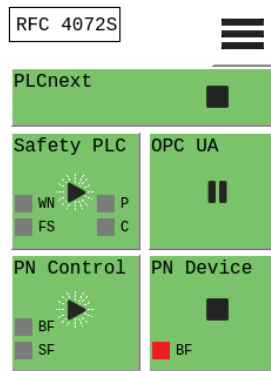




Figure 6-2 Standard controller in the “STOP” state

- Double-click on the “Safety PLC” node in the “PLANT” area.
The editor group of the safe PLC opens.
- Select the “Safety Cockpit” editor.
- Click on the  button to connect PLCnext Engineer to the safe PLC.
- Click on the  button to switch to the debug mode of the iSPNS3000.



WARNING: Excluding hazards

Switching to debug mode means that you will exit normal mode.
Make sure that your system/machine cannot pose a hazard to people or equipment.

- Acknowledge the following message to switch to debug mode of the SPNS.

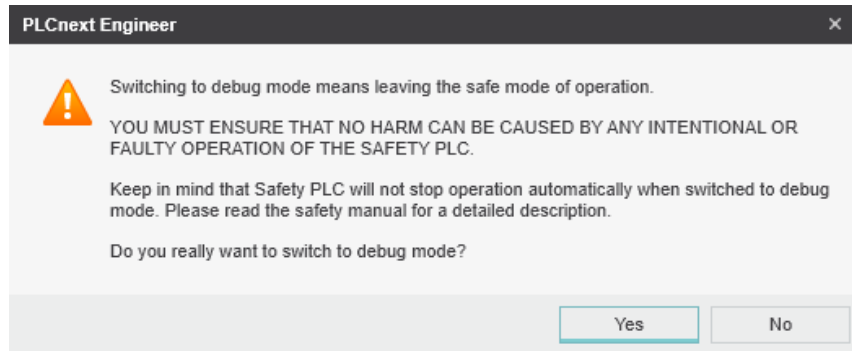


Figure 6-3 PLCnext Engineer safety prompt: switching to debug mode

Switch-over to debug mode is displayed on the display.

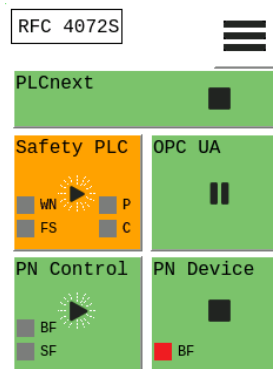


Figure 6-4 SPNS state: Debug Run

- Click on the “Stop the controller” button.

Shortly thereafter, the iSPNS 3000 switches to the “Debug Stop” state:

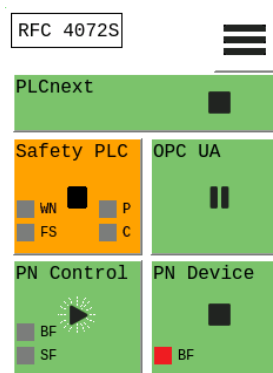


Figure 6-5 SPNS state: Debug Stop

You can update the non-safety-related device firmware via the Web-based management system of the RFC 4072S or the Linux shell using a command-line tool.

For information about updating the firmware using a command-line tool, please refer to [Section 6.5.1](#) below. For an explanation of how to update the firmware via WBM, please refer to [Section 9.7](#).

6.5.1 Updating the firmware

To update the controller firmware, proceed as follows:

- Download the *.zip firmware file at phoenixcontact.net/product/1051328.
- Unzip the *.zip firmware file.
- Run the *.exe setup file.
- Follow the instructions of the installation wizard.

During installation, the update file (*.raucb) and files containing device-specific information (such as change notes and Phoenix Contact software license terms) are copied to the selected destination directory.

- Open the SFTP client software (e.g., WinSCP).
- Log in as an administrator.

The following access data is set by default:

User name: admin

Password: printed on the controller (see [Figure 2-36 on page 76](#))

- Copy the *.raucb update file to the /opt/plcnext directory (home directory of the Linux user “admin”).
- Open the shell using a command-line tool (e.g., PuTTY or Tera Term).
- Log in as an administrator.

The following access data is set by default:

User name: admin

Password: printed on the controller (see [Figure 2-36 on page 76](#))

- Switch to the /opt/plcnext directory (command: “cd /opt/plcnext”).
- To start the firmware update, enter the “sudo update-plcnext” command.

You will be asked to enter the administrator password.

- Enter the administrator password.

The firmware is updated.

The RFC is restarted during the firmware update.

Once the firmware update has been completed successfully and the RFC is completely initialized, the display shows the following information, provided the RFC ran without errors before the update (A in [Figure 6-6](#)):

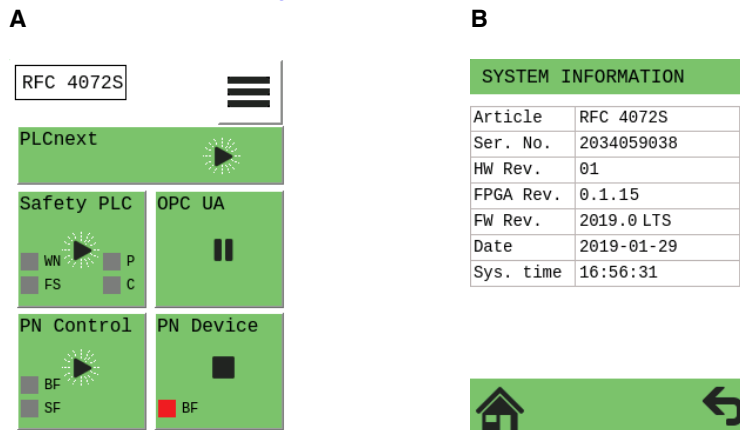


Figure 6-6 After successful firmware update, the RFC runs without any errors

The "SYSTEM INFORMATION" submenu displays the updated firmware version (see A in [Figure 6-6](#)).

The update file is automatically deleted from the /opt/plcnext directory.

6.6 Repair

Repairs may not be carried out on the RFC 4072S. Send faulty devices with detailed error information (see [Section "Errors, diagnostic messages and troubleshooting" on page 151](#)) to Phoenix Contact.



NOTE: Possible RFC malfunction – Do not open housing

It is strictly prohibited to open the RFC 4072S. In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the RFC 4072S (see [Figure 2-13 on page 46](#)). These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the RFC 4072S can no longer be ensured.

6.7 Decommissioning and disposal

- Always carry out decommissioning in accordance with the requirements of the machine or system manufacturer.

When decommissioning the system or parts of the system, ensure the following for the devices used.

The device continues to be used as intended:

- Observe the storage and transport requirements (see [Section “Transport, storage, and unpacking” on page 23](#))

The device is not used anymore:



The symbol with the crossed-out trash can indicates that this item must be collected and disposed of separately from other waste. Phoenix Contact or public collection sites will take the item back for free disposal. For information on the available disposal options, visit phoenixcontact.com. Collect and dispose of included batteries separately from other waste. Delete personal data before returning the item.

Make sure that existing PROFIsafe projects are deleted from the parameterization memory (SD card) when decommissioning your application. Only then may the SD card be used in another device in another application.

In the event of device replacement due to decommissioning of an old device, do not delete the SD card, as the configuration saved on it will still be required for the new device.

SD Card disposal

Sensitive data is stored on the SD card. This data can even be restored after reformatting the SD card. To ensure that your data does not fall into unauthorized hands, you should physically destroy the SD card before disposal.

- Physically destroy the SD card, e. g., by cutting up the SD card.
- Dispose of the irreparably damaged SD card in accordance with the national regulations.

Packaging disposal

- Dispose of packaging materials that are no longer needed (cardboard packaging, paper, bubble wrap sheets, tubular bags, etc.) with household waste in accordance with the currently applicable national regulations.

7 Additional settings as well as features and what you need to know about the RFC 4072S

7.1 Resetting the controller to the default settings

- Open the “CONFIG DETAILS” menu.
- Select the “MAINTENANCE” menu item in the “CONFIG DETAILS” menu.
- Select the “FACTORY RESET” menu item in the “MAINTENANCE” menu.

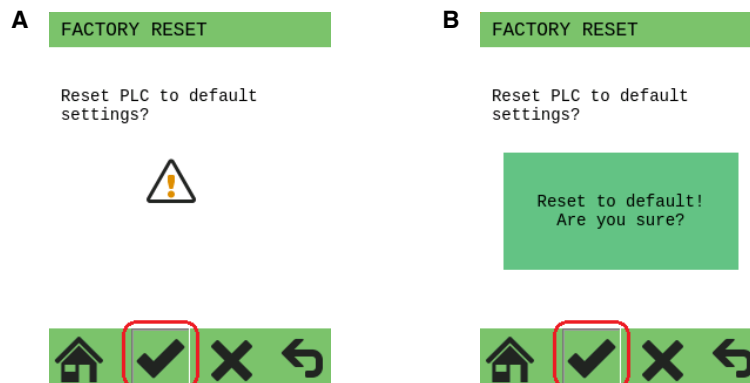


Figure 7-1 “FACTORY RESET” menu

- Start the reset process by tapping the ✓ symbol (A in Figure 7-1).
- Acknowledge the “Reset to default! Are you sure?” dialog by tapping on the ✓ symbol (B in Figure 7-1) again.

The RFC 4072S is restarted after the resetting process. The display then shows the following:

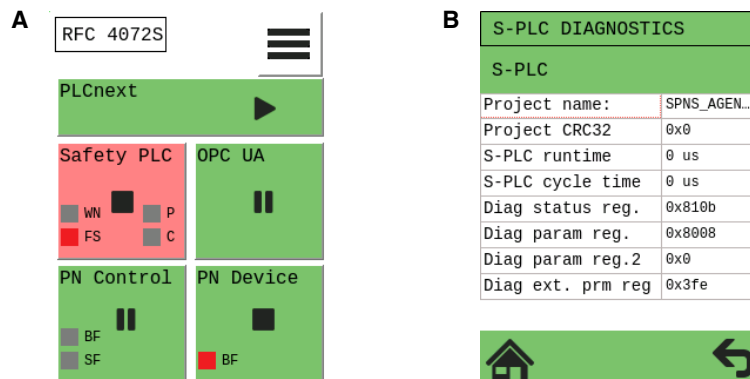


Figure 7-2 Default settings of the RFC 4072S: indication on the display

Key:

- A** RFC 4072S is reset to the default settings
- B** iSPNS 3000 with error code 8008_{hex} (diagnostic parameter register (Diag param reg.): boot project missing)

After successful reset to the default settings, the RFC 4072S reboots and then shows error code 8008_{hex} on the display (see [Figure 7-2](#)).

Resetting to the default settings has the following effects:

- All settings were reset to the default settings.
- Project and boot project were deleted.
- All the firmware changes resulting from firmware updates that have been executed until the time of reset are retained.
- Settings of the device-internal realtime clock are retained.

In order to start up the RFC 4072S again, proceed as described in [Section “Startup and validation” on page 91](#).

7.2 Changing IP address settings via the display

You can also set the IP addresses directly on the device via the display.



The procedure for assigning the IP address settings is essentially the same for the LAN1, LAN2 and LAN3.1/3.2 interfaces. Interface LAN2 is described in this example.



You can view and change the IP address defined in the RFC 4072S via the display at any time, even during operation.

The change to the IP address will only take effect after the RFC has been restarted (e.g., via the CONFIG DETAILS menu on the display). The changed IP address is permanently stored in the parameterization memory. The RFC can then be reached in the network under the changed IP address.

Assuming the new IP address is in the same subnet as before, the application program will continue to run without errors after the RFC restart.

- Open the “CONFIG DETAILS” menu.
- Select “LAN SETTINGS”, then the “LAN2 SETTING” menu item.

Additional settings as well as features and what you need to know about the RFC 4072S

The following menu shows the default IP-settings of the LAN2 interface:

EDIT LAN2

Ip address:
192.168.02.10

Subnet mask:
255.255.255.0

Gateway:
00.00.00.00



Figure 7-3 “CONFIG DETAILS, ... EDIT LAN2” menu: default settings

- Select the “IP address: ...” menu item.

The following menu appears (A):

A

192.168.002.010

1	2	3
4	5	6
7	8	9
←	0	→

Home Back

B

192.168.002.112

1	2	3
4	5	6
7	8	9
←	0	→

Home Back

Figure 7-4 “CONFIG DETAILS, ... EDIT LAN2” menu: edit LAN2 IP address

- Set the IP address “192.168.2.112” shown in [Figure 7-4 \(B\)](#).
- Change the number position in the IP address by tapping → .
- Select the corresponding numbers by tapping on the numbers.
- Exit the entry window by tapping ↩ .

The following menu appears:

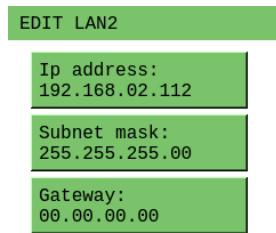


Figure 7-5 “CONFIG DETAILS, ... EDIT LAN2” menu: LAN2 IP address

- Confirm your entries by tapping .

The activated symbol appears as a pressed button when it is tapped. This change in appearance is a visual indicator that tapping has been recognized by the system (A in [Figure 7-6](#)). An additional dialog on the display shows that the change has been accepted (B).

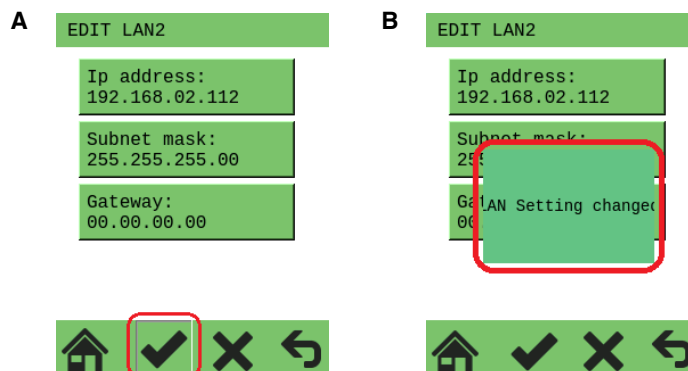


Figure 7-6 “CONFIG DETAILS, ... EDIT LAN2” menu: LAN2 IP settings changed

- If you do not want to apply your settings, press the button instead of the button.

The following message is displayed:

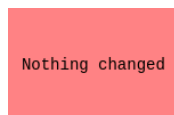


Figure 7-7 “CONFIG DETAILS” menu: nothing has been changed

In this example, the settings for the gateway and the subnet mask are not changed. If necessary, proceed as described above for the IP address.

Changes to IP settings are stored in the parameterization memory. The changes will only take effect once the RFC has been restarted.

7.3 Parameterization memory: directory structure and access

The parameterization memory is accessed via the SFTP protocol. SFTP client software is required for this (e.g., WinSCP).



Read the information in [Section “Using SFTP to access the file system” on page 76](#) before accessing the parameterization memory via the SFTP client software.

- Start the SFTP client software (WinSCP in the following example).

Log into the RFC 4072S using the SFTP client software.

- Enter the IP address of the RFC on the input screen (in the example: 192.168.1.10).
- Enter the user name and the administrator password (in the example: user name: admin; administrator password: see printing on the RFC).
- Confirm your entries.

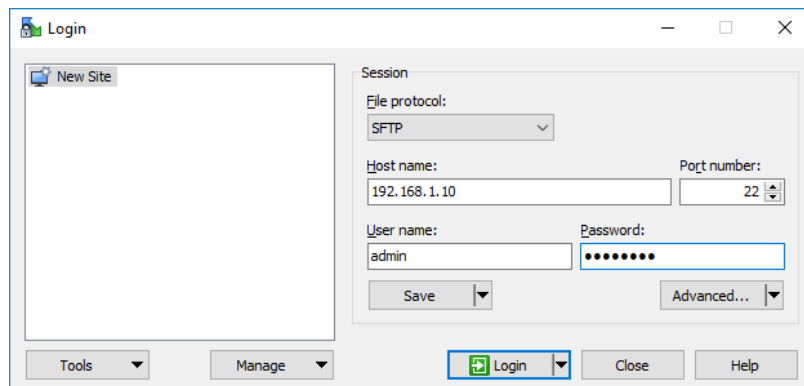


Figure 7-8 Logging into the RFC 4072S via WinSCP

After successful login, the following directory is displayed in the parameterization memory:

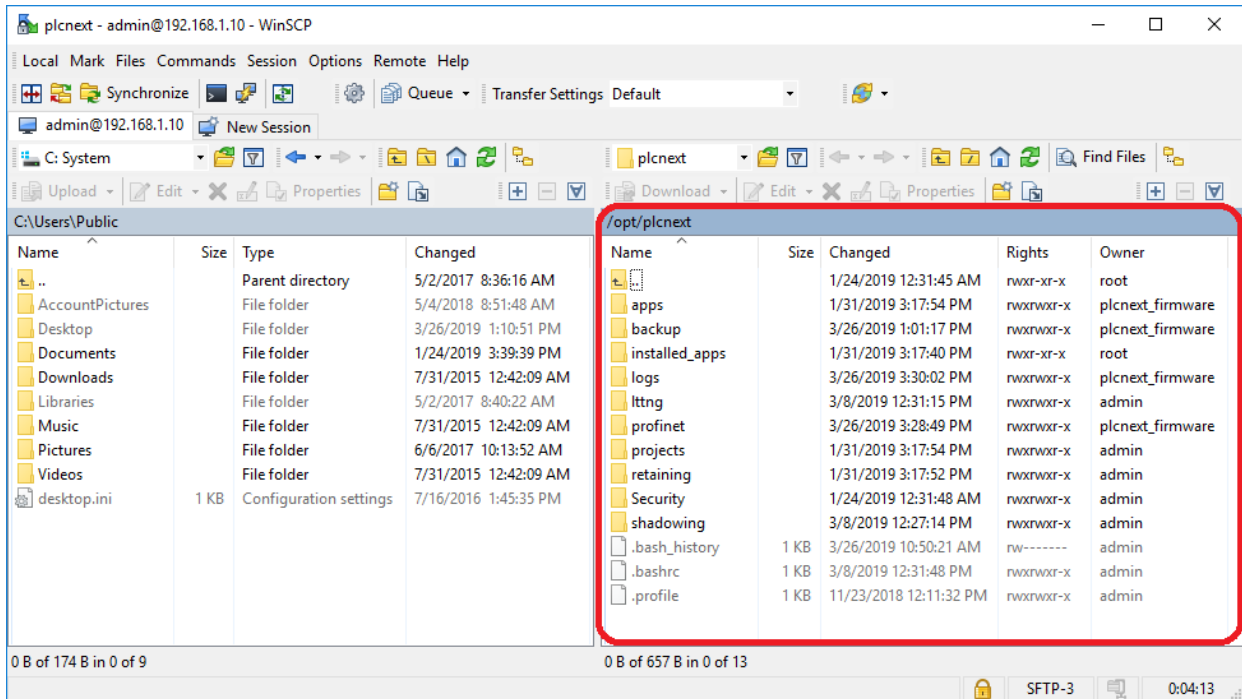


Figure 7-9 PLCnext directory “/opt/plcnext” in the parameterization memory.

7.4 Setting the realtime clock under PLCnext Engineer

You can set the realtime clock in the PLCnext Engineer software.

- In the “PLANT” area, double-click on the “PLCnext” node.

The editor group of the “/ PLCnext” controller opens.

- Select the “Online Parameters” editor.

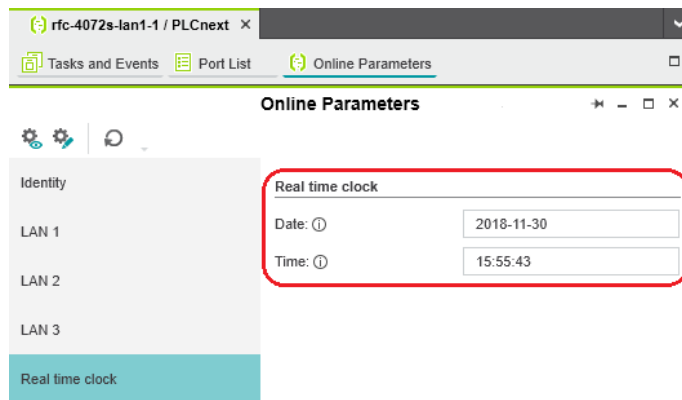




Figure 7-10 Realtime clock settings for the RFC 4072S

- Click on the  button to read the values from the device and apply them to the project.

- Click on the  button to write the configured values to the device.

7.5 Download changes

7.6 Startup parameterization of PROFINET devices

In a PROFINET network used in systems manufacturing, devices must be coupled and decoupled. This function is managed by the program, depending on the application. In the off state, the device should be viewed as a missing device, with the difference being that the PROFINET controller does not search for it cyclically. Switching on and switching off correspond to application-driven connection establishment and release of the PROFINET device.



Make sure that the basic specifications of a PROFINET controller (e.g., maximum number of PROFINET devices that can be connected) cannot be exceeded by deactivating devices in the configuration.

In the “Settings” editor of the PROFINET device, you must specify whether the controller establishes an application relationship when the PROFINET device is started.

When set to “No”, an application relationship is created for each PROFINET device but is not started; it remains inactive. In this case, an application relationship to the PROFINET device can be established using the AR_MGT function block (see [Section “Function block for managing PROFINET application relationships \(AR\)” on page 182](#)).

When set to “Yes”, the PROFINET device is started up directly. If an application relationship is not started, the PROFINET device is not started up.

This option is set to “Yes” by default.

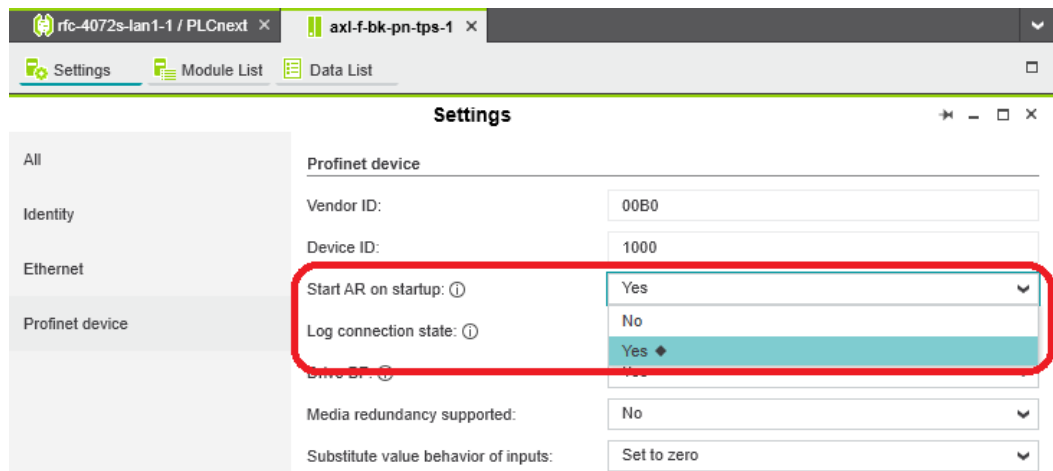


Figure 7-11 PROFINET device – “Start AR on startup”

Safety notes for starting applications

Take the following into consideration when determining and programming the start conditions for your machine or system:

- The machine or system may only be started if it can be ensured that nobody is present in the danger zone.
- Meet the requirements of EN ISO 13849-1 with regard to the manual reset function. The machine must not be set in motion and/or a hazardous situation must not be triggered by the following actions, for example:
 - Switching on safe devices
 - Acknowledging device error messages
 - Acknowledging communication errors
 - Acknowledging block error messages in the application
 - Removing startup inhibits for safety functions

Observe the following when programming/configuring the safety logic:

- Switching from the safe state (substitute value = 0) to the operating state can generate an edge change (zero/one edge).
- In the safety logic, take measures to prevent this edge change resulting in unexpected machine/system startup or restart.



Note for starting applications

Also observe these notes to prevent unexpected machine startup following acknowledgment by means of operator acknowledgment.

7.7 Substitute value behavior for PROFINET devices and PROFIsafe F-Devices

The substitute value behavior for the input data of the controller must be specified in your PLCnext Engineer project. By default, the input data of the RFC 4072S is set to zero if the connection to a PROFINET device is interrupted.

Set the substitute value behavior for each PROFINET device individually in PLCnext Engineer (see [Figure 7-12](#)).

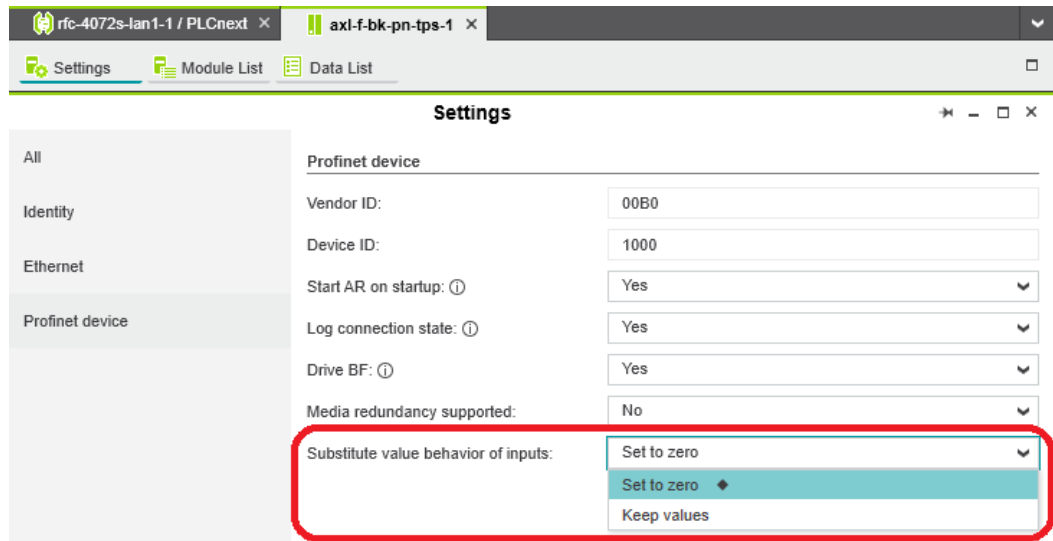


Figure 7-12 PROFINET device – “Substitute value behavior of inputs”

If the connection to a PROFINET device is interrupted, the “Set to zero” option means that the corresponding input data of the controller is set to zero. The “Keep values” option means that if the connection to a PROFINET device is interrupted, the input values that were valid immediately before the interruption are present as the input data in the application program.

When the connection to the PROFINET device is restored, the substitute values remain valid as input data until the PROFINET device has been started up completely. Once the connection has been established again, the latest input data is used.



Note on the substitute value behavior for F-Devices

Observe the following when programming/configuring the safety logic:

- Switching from the safe state (substitute value = 0) to the operating state can generate an edge change (zero/one edge).
- In the safety logic, take measures to prevent this edge change resulting in unexpected machine/system startup or restart.

7.8 Function blocks for handling files on the parameterization memory

The function blocks are used to access files from within the application program. Some of the blocks support multiple instantiation. This means that it is possible to work with a number of different files within the same project. The blocks perform the standard functions that are required for typical file access operations.



All file operations are subject to the following restrictions:
 No directory hierarchies are supported. All file operations only affect the root directory of the parameterization memory.

Table 7-1 Overview of the function blocks

Function block	Short description
FILE_OPEN	Opens a file with a specific name
FILE_CLOSE	Closes a file with a specific handle
FILE_READ	Reads from a file with a specific handle
FILE_WRITE	Writes to a file with a specific handle
FILE_REMOVE	Deletes a file with a specific name
FILE_TELL	Determines the current position of the file pointer in a file
FILE_SEEK	Moves the current file pointer to a new position



The function blocks for handling files on the parameterization memory are described in the PLCnext Engineer online help.

7.9 Function blocks for Ethernet communication

The function blocks are used to establish Ethernet communication between two communication partners.

The IP communication blocks listed below enable IEC 61131-5-compliant communication between controllers via Ethernet or communication between controllers and Ethernet devices via TCP/IP or UDP/IP.

Implement all time and connection monitoring in the application program.

The RFC 4072S supports a maximum of 32 Ethernet connections to other communication partners.

Table 7-2 Overview of the function blocks

Function block	Short description
TCP_SOCKET	Establishes a connection between two communication partners
TCP_SEND	Sends data to a communication partner
TCP_RECEIVE	Receives data from a communication partner



The communication blocks are described in the PLCnext Engineer online help.

7.10 Function block for managing PROFINET application relationships (AR)

You can use the AR_MGT function block to activate or deactivate PROFINET application relationships (AR) from a project. For example, process data and process data states (IOPS) are transmitted via the application relationships between the PROFINET controller and PROFINET device.

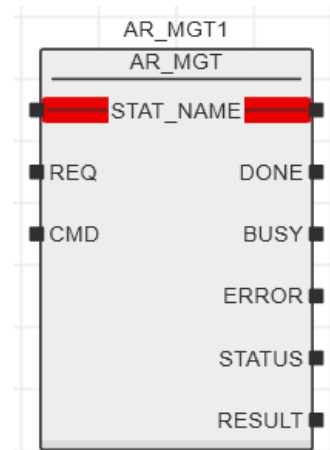


Figure 7-13 AR_MGT function block

The function block supports multiple instantiation. The maximum possible number of function block instances that can be activated simultaneously is limited by the maximum number of application relationships permitted by the PROFINET controller.



The function block for managing communication blocks is documented in the PLCnext Engineer online help.

7.11 Web server

The RFC 4072S has a web server. With its visualization software, you can use the web server to visualize control variables, for example, in a web browser. The Web-based management system of the RFC 4072S is also available via the web server (see [Section “Web-based management WBM” on page 209](#)).



The Hypertext Transfer Protocol (HTTP) is set on the controller by default.

7.12 OPC UA

The RFC 4072S supports communication via the OPC UA protocol.



For further information about OPC UA and PLCnext Technology can be found in the PLCnext Community at plcnext-community.net.

8 System variables

8.1 General notes

This section describes the system variables that are available for the controller.

The controller has a register set, which is used for diagnostics and easy control of the controller.

The diagnostic data is stored in the diagnostic status register and the diagnostic parameter register. These registers are available to the application program as system variables (system markers, global variables).

8.2 System variables grouped into structures

Certain system variables of the RFC 4072S are grouped into structures in PLCnext Engineer. You can display these system variables and elements of the structure in the PLCnext Engineer Init Value Configuration editor.

The screenshot shows the PLCnext Engineer interface. The 'Data List' window displays the following table:

Variable (PLC)	Type	Usage	Init
rfc-4072s-lan1-1 / PLC.ESM_DATA	ESM_DAT	Global	
rfc-4072s-lan1-1 / PLC.RTC	RTC_TYPE	Global	
rfc-4072s-lan1-1 / PLC.DEVICE_STATE	DEVICE_STATE_4xxx_TYPE	Global	
rfc-4072s-lan1-1 / PLC.PNIO SYSTEM BF	BOOL	Global	FALSE

The 'Init Value Configuration' window is open, showing the following table:

Member Name	Member Init Value
HOURS	USINT#0
MINUTES	USINT#0
SECONDS	USINT#0
DAY	USINT#0
MONTH	USINT#0
YEAR	UINT#0

Figure 8-1 System variables grouped into structures

8.3 PROFIsafe/PROFINET system variables

PROFINET provides extremely detailed diagnostic information for each device down to channel level.

Diagnostic states are important for system operation. If error messages occur, the process has to be stopped in case of doubt. For this purpose, controllers from Phoenix Contact provide the following status information for the PROFINET network.

8.3.1 System variables of the iSPNS 3000

The SPNS system variable uses the SPNSV2_TYPE structure to provide the following information about the iSPNS 3000.

Table 8-1 SPNS system variable and elements of the SPNSV2_TYPE structure

System variable/elements	Type	Meaning
SPNS	SPNSV2_TYPE	The SNPS system variable provides the information in the SPNSV2_TYPE structure.
PRJ		
NAME	STRING	PLCnext Engineer project name.
CRC	DWORD	Project CRC (32 bits) of the iSPNS 3000 boot project.
EXEC_TIME	UDINT	Runtime of the iSPNS 3000 program cycle in μ s.
HAS_PRJ	BOOL	The safety-related application program and the program sources are available in the memory of the iSPNS 3000.
DIAG		
STATUS_REG	WORD	Diagnostic status register of the iSPNS 3000 The diagnostic status register of the iSPNS 3000 contains the status information of the iSPNS 3000. It mirrors the state of the iSPNS 3000 at all times including any error states that have occurred on the iSPNS 3000. Additional information and error parameters, in particular in the failure state (FS), are included in the relevant diagnostic parameter registers of the iSPNS 3000 (elements SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2). The information in the diagnostic status register is detailed in Table 8-2 on page 186 .
PARAM_REG	WORD	Diagnostic parameter register 1 of the iSPNS 3000 (error code).
PARAM_2_REG	WORD	Diagnostic parameter register 2 of the iSPNS 3000 (additional error messages for service/support).
EXT_PARAM_REG	DWORD	Extended diagnostic parameter register of the iSPNS 3000 (additional error messages for service/support).
CH2_PARAM_REG	WORD	Diagnostic parameter register 1 of the iSPNS 3000 channel 2 (CH2) (error code).
CH2_PARAM_2_REG	WORD	Diagnostic parameter register 2 of the iSPNS 3000 channel 2 (CH2) (additional error messages for service/support).

Table 8-1 SPNS system variable and elements of the SPNSV2_TYPE structure

System variable/elements	Type	Meaning
CH2_EXT_PARAM_REG	DWORD	Extended diagnostic parameter register of the iSPNS 3000 channel 2 (CH2) (additional error messages for service/support).
INFO		
CYCLE_TIME	UDINT	iSPNS 3000 cycle in μ s
TEMP		
TEMP_CURRENT	INT	Currently measured iSPNS 3000 temperature
TEMP_MIN	INT	Minimum measured iSPNS 3000 temperature since the last power-on of the device.
TEMP_MAX	INT	Maximum measured iSPNS 3000 temperature since the last power-on of the device.
STATUS_REG	WORD	iSPNS 3000 temperature status register 0x0000: The temperature of the iSPNS 3000 is in the non-critical range ≤ 63 °C. 0x0080: The temperature of the iSPNS 3000 is in the critical range, close to the tolerance threshold ≥ 64 °C and ≤ 73 °C. The iSPNS 3000 remains in RUN state and, in parallel, issues a warning with error code 0xFA41. 0x8000: The temperature of the iSPNS 3000 is beyond the permitted range (≥ 74 °C). The iSPNS 3000 goes into safe state and issues an error message with error code 0x924D.
CPU		
LOAD_CURRENT	INT	Current iSPNS 3000 CPU load
LOAD_MIN	INT	Minimum measured iSPNS 3000 CPU load since the last power-on of the device.
LOAD_MAX	INT	Maximum measured iSPNS 3000 CPU load since the last power-on of the device.
STATUS_REG	WORD	iSPNS 3000 CPU status register
FW_Version		
VERSION_MAJOR	BYTE	Major version of the iSPNS 3000 firmware
VERSION_MINOR	BYTE	Minor version of the iSPNS 3000 firmware
VERSION_BUILD	WORD	Build number of the iSPNS 3000 firmware
FPGA_VERSION		
VERSION_MAJOR	BYTE	Major version of the iSPNS 3000 hardware FPGA
VERSION_MINOR	BYTE	Minor version of the iSPNS 3000 hardware FPGA
VERSION_BUILD	WORD	Build number of the iSPNS 3000 hardware FPGA
NUM_OF_ACTIVE_ARS	UINT	Number of active PROFINET application relations (AR)
FW_UPDATE_STATUS	UINT	Status of safety-related firmware update
SOFT_RESET_REG	WORD	Software reset register of the iSPNS 3000

The following table describes the information of the individual bits (0 ... 15) in the diagnostic status register (SPNS.DIAG.STATUS_REG.xxx)

Table 8-2 Elements in the diagnostic status register (SPNS.DIAG.STATUS_REG.xxx)

System variable/elements	Type	Meaning
SPNS	See above	See above
DIAG	See above	See above
STATUS_REG	See above	See above
DBG ³	BOOL	Non-safe debug mode of the iSPNS 3000 The iSPNS 3000 is in one of the two DEBUG states (DEBUG RUN or DEBUG STOP/SINGLE).
EST	BOOL	There is an entry in the error memory of the safe operating system (error stack) of the iSPNS 3000. Diagnostic and error messages from the safe iSPNS 3000 operating system are present. These messages are shown on the display and can be read and evaluated by PLCnext Engineer. This variable is always set to TRUE if there is at least one entry in the error memory of the safe operating system. As soon as the error memory has been read and emptied via PLCnext Engineer, the value of the variable changes to FALSE.
FS	BOOL	Failure state of the iSPNS 3000 An error has been detected which sets the iSPNS 3000 to the failure state. The corresponding additional error code is included in this state in the diagnostic parameter registers of the iSPNS 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG).
INIT ²	BOOL	Initialization of the iSPNS 3000 The iSPNS 3000 firmware (safe operating system) was initialized completely without errors.
IO ²	BOOL	Initialization of the iSPNS 3000 F-Host for I/O channel communication Initialization of the F-Host for PROFIsafe communication with the PROFIsafe I/O devices has been completed without any errors.
PON ²	BOOL	Power-on process The iSPNS 3000 is supplied with power. The firmware was downloaded to the RAM memory of the RFC and started. The comprehensive selftest routines of the device have been completed successfully.
POST	BOOL	Power-on selftest of the iSPNS 3000 (POWER ON SELFTEST) Power-on selftest of the iSPNS 3000 is active.
PRO ²	BOOL	Loading and starting of the safety-related application program The safety-related application program, which was created using PLCnext Engineer, has been loaded without any errors to the safe iSPNS 3000 operating system and started.

Table 8-2 Elements in the diagnostic status register (SPNS.DIAG.STATUS_REG.xxx)

System variable/elements	Type	Meaning
RUN ³	BOOL	Execution of the safety-related application program (RUN) The iSPNS 3000 executes the safety-related application program and is in one of the two RUN states (SAFE RUN or DEBUG RUN).
SYN ²	BOOL	Synchronization of iSPNS 3000 and PROFINET controller Synchronization between the iSPNS 3000 and the PROFINET controller was completed successfully.
WARN	BOOL	Warning of the iSPNS 3000 A group warning message of the iSPNS 3000 is present.
²	The variables indicate the startup status of the safety-related PROFINET iSPNS 3000 controller. The startup sequence of the iSPNS 3000 is divided into the following five consecutive sections: <ul style="list-style-type: none"> 1. Power-on process 2. Initialization of the iSPNS 3000 3. Loading and starting of the safety-related application program 4. Synchronization of the iSPNS 3000 and the standard controller 5. Initialization of the iSPNS 3000 F-Host for I/O channel communication 	
³	The variables indicate the RUN and DEBUG operating states of the iSPNS 3000.	

SPNS.DIAG.STATUS_REG – Meaning of the individual bits

The SPNS.DIAG.STATUS diagnostic status register contains the status information of the iSPNS 3000. It mirrors the state of the iSPNS 3000 at all times including any error states that have occurred on the iSPNS 3000. Additional information and error parameters, in particular in the failure state (FS), are included in the relevant diagnostic parameter registers of the iSPNS 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG), and in the extended diagnostics parameter register (SPNS.DIAG.EXT_PARAM_REG).

Table 8-3 Diagnostic status register of the iSPNS 3000: SPNS.DIAG.STATUS_REG

Bit 15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
FS	POST	Res.	EST	Res.	Res.	Res.	Res.	WARN	DBG	RUN	I/O	SYN	PRO	INIT	PON

Bits 0 to 4

Bits 0 to 4 indicate the startup status of the iSPNS 3000. The startup sequence of the iSPNS 3000 is divided into the following five steps:

- PON** Power-on process complete
This bit is set as soon as the iSPNS 3000 is supplied with power. The firmware was downloaded to the RAM memory of the RFC and started. The comprehensive selftest routines of the device have been completed successfully.
- INIT** Initialization of the iSPNS 3000 complete
This bit is set as soon as initialization of the iSPNS 3000 firmware (safe operating system) has been completed without errors.
- PRO** Safety-related application program loaded and started
This bit is set as soon as the safety-related application program, which was created using PLCnext Engineer, has been loaded to the safe iSPNS 3000 operating system without any errors and started.
- SYN** Synchronization of the iSPNS 3000 and the standard controller
The bit is set when the iSPNS 3000 and the standard controller are synchronized.
- I/O** I/O channel communication initialized
This bit is set as soon as initialization of the F-Host for PROFIsafe communication with the PROFIsafe I/O devices has been completed without any errors.

Bits 5 and 6

The RUN and DBG bits indicate the operating status of the iSPNS 3000.

- RUN** RUN mode of the iSPNS 3000
This bit is set when the iSPNS 3000 executes the safety-related application program and is in one of the two RUN states (SAFE RUN or DEBUG RUN). This bit is not set in the SAFE STOP and DEBUG STOP/SINGLE states.

DBG Non-safe debug mode of the iSPNS 3000

This bit is set when the iSPNS 3000 is in one of the two DEBUG states (DEBUG RUN or DEBUG STOP/SINGLE). This bit is not set in the SAFE STOP and SAFE RUN states.

Table 8-4 Contents of bits 5 and 6 and corresponding LED indicators¹

RUN bit	DBG bit	State	FS LED
0	0	Startup sequence (bits 0 to 4) or SAFE STOP	Flashing Off
0	1	DEBUG STOP/SINGLE	Flashing
1	0	SAFE RUN	Off
1	1	DEBUG RUN	Flashing

¹ Indicated by means of the virtual FS LEDs in the "Safety PLC" tile of the display

Bits 7 and 10

WARN The set WARN (WARNING) bit indicates a group warning message of the iSPNS 3000.

Bit 12

EST The EST (error stack) bit indicates that diagnostic and error messages for the safe iSPNS 3000 operating system are present. These messages are shown on the display and can be read and evaluated by PLCnext Engineer.

This bit is always set if there is at least one entry in the error memory of the safe operating system. As soon as the error memory has been read and emptied via PLCnext Engineer, this bit is automatically reset to zero.

Bit 14

POST POWER-ON SELFTEST

This bit is set for the duration of the comprehensive power-on selftest of the iSPNS 3000. It is reset once the power-on selftest is complete.

Bit 15

FS Failure state

This bit is set as soon as an error has been detected, which sets the iSPNS 3000 to the failure state. The corresponding additional error code is included in this state in the diagnostic parameter registers of the iSPNS 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG).

Res. Reserved

The SPNS_V2_PROFISAFE_DIAG system variable uses the PROFISAFE_DIAG_OUT structure to provide further information about the iSPNS 3000.

Table 8-5 SPNS_V2_PROFISAFE_DIAG system variable and elements of the PROFISAFE_DIAG_OUT structure

System variable/elements	Type	Meaning
SPNS_V2_PROFISAFE_DIAG	PROFISAFE_DIAG_OUT	The structure provides PROFIsafe diagnostic information of the individual configured F-Devices.
MAX_PS_RECORDS	UINT	Maximum number of F-Devices to be configured
USED_PS_RECORDS	UINT	Configured number of F-Devices
PS_RECORDS		
[1] ... [300]		PROFIsafe records 1 ... 300
CODE_NAME	DWORD	–
DIAG_BIT_FIELD	DWORD	–
SRT_MIN	UINT	Minimum roundtrip time between F-Host and F-Device
SRT_MAX	UINT	Maximum roundtrip time between F-Host and F-Device
SRT_CUR	UINT	Current roundtrip time between F-Host and F-Device
FWD_TIME	UINT	Watchdog time
VALID_REG	UINT	–
NODE_ID	UDINT	Node ID
Reserved	UINT	Reserved
PS_GLOBAL_RECORD	DWORD	–

8.3.2 FDEV_INx and FDEV_OUTx (x = 0 ... 7) system variables

These system variables are used for the data exchange between the F-Device of the iSPNS 3000 and the superordinate safety-related controller (F-Host).

Tabelle 8-6 FDEV_INx and FDEV_OUTx (x = 0 ... 7) system variables

System variable	Type	Meaning
FDEV_IN0 ... FDEV_IN7	SAFEBYTE	Input process data of the F-Device instance of the iSPNS 3000
FDEV_OUT0 ... FDEV_OUT7	SAFEBYTE	Output process data of the F-Device instance of the iSPNS 3000



Please observe the information in section [“System variables for the data exchange of the F-Device of the iSPNS 3000”](#) on page 32.

8.3.3 Management/diagnostic variables for each configured F-Device

The table below lists management/diagnostic variables. These variables can be created in PLCnext Engineer for each configured F-Device. The table shows which variables are created by default. This setting can be modified by changing the value (create / do not create) (see [Figure 4-47 on page 132](#)).

Management/diagnostic variable	Default setting
F_ADDR_XXXXX_ACK_REQ	Create
F_ADDR_XXXXX_ACK_REI	Create
F_ADDR_XXXXX_PASS_OUT	Create
F_ADDR_XXXXX_PASS_ON	Create
F_ADDR_XXXXX_DEVICE_FAULT	Create
F_ADDR_XXXXX_CE_CRC	Create
F_ADDR_XXXXX_WD_TIMEOUT	Create
F_ADDR_XXXXX_IPAR_OK	Do not create
F_ADDR_XXXXX_IPAR_EN	Do not create
F_ADDR_XXXXX_CHF_ACK_REI	Do not create
F_ADDR_XXXXX_CHF_ACK_REQ	Do not create
F_ADDR_XXXXX_CE_CRC_H	Do not create
F_ADDR_XXXXX_WD_TIMEOUT_H	Do not create
F_ADDR_XXXXX_LOOPBACK	Do not create

Table 8-7 Management/diagnostic variables for each configured F-Device


System variable	Type	Meaning
F_ADDR_XXXXX_PASS_ON *)	BOOL	<p>F-Device XXXXX is passivated when this variable is set to TRUE from the application program.</p> <div style="border: 1px solid black; padding: 5px;"> <p> WARNING: Resetting this variable to FALSE means that the safe input and output data is transmitted immediately. Take appropriate measures to ensure that your system/machine does not present any danger when passivation of the F-Device is reset.</p> </div>
F_ADDR_XXXXX_PASS_OUT *)	BOOL	<p>F-Device XXXXX is passivated.</p> <p>Possible reasons for passivation:</p> <ul style="list-style-type: none"> – Programmed passivation via the F_ADDR_XXXXX_PASS_ON system variable – Communication, device, and parameterization errors (see F_ADDR_XXXXX_ACK_REQ system variable)

Table 8-7 Management/diagnostic variables for each configured F-Device


System variable	Type	Meaning
F_ADDR_XXXXX_ACK_REQ *)	BOOL	<p>F-Device XXXXX requires an operator acknowledge request after removing an error. Possible reasons for activating the operator acknowledge request:</p> <ul style="list-style-type: none"> - Communication error (CRC, F_WD_TIME_OUT) - Error in an F-Device. Please refer to the user documentation for the F-Devices used.
F_ADDR_XXXXX_ACK_REI *)	BOOL	<p>If F-Device XXXXX requires an operator acknowledge request, it can be acknowledged by an operator acknowledge reintegration (F_ADDR_XXXXX_ACK_REI).</p>
F_ADDR_XXXXX_DEVICE_FAULT *)	BOOL	<p>Error in an F-Device.</p> <p>If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out using the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variable. If the cause has been removed, the F_ADDR_XXXXX_DEVICE_FAULT variable is set to FALSE again.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>For information on which errors cause the used F-Device to control this variable, please refer to the device-specific user documentation.</p> </div>

Table 8-7 Management/diagnostic variables for each configured F-Device




System variable	Type	Meaning
F_ADDR_XXXXX_CE_CRC *)	BOOL	<p>Communication error (F_CE_CRC)</p> <p>This parameter is set if at least one of the following reasons applies:</p> <ul style="list-style-type: none"> – The F-Device has detected a communication error during operation that was caused by an incorrect CRC checksum. – Inconsistent parameterization between PROFIsafe controller and F-Device. – Communication error between PROFIsafe controller and F-Device. <p>If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out using the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variable. If the cause has been removed, the F_ADDR_XXXXX_CE_CRC variable is set to FALSE again.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> In terms of system availability, this type of CRC error should only occur once every ten hours at the most (see PROFIsafe specification regarding “SIL Monitor” and “Operator Acknowledge”).</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> During PROFIsafe system startup, e.g., following a program download in PLCnext Engineer, this variable is briefly set as a result of the PROFIsafe system startup behavior. This is not relevant for the 10-hour monitoring period described above following a CRC error that occurred during operation.</p> </div>
F_ADDR_XXXXX_WD_TIME_OUT *)	BOOL	<p>Communication error (F_WD_TIME_OUT)</p> <p>Set if the F-Device has detected a communication error caused by the parameterized F_WD_Time being exceeded.</p> <p>If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out using the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variable. If the cause has been removed, the F_ADDR_XXXXX_WD_TIME_OUT variable is set to FALSE again.</p>
F_ADDR_XXXXX_IPAR_OK *)	BOOL	<p>F-Device indicates that the iParameters have been applied</p> <p>This variable is set when the F-Device indicates that it has applied the iParameters.</p>

Table 8-7 Management/diagnostic variables for each configured F-Device

System variable	Type	Meaning
F_ADDR_XXXXX_IPAR_EN *)	BOOL	<p>Initiate application of the iParameters</p> <p>This variable is set in the application in order to initiate the application of the iParameters.</p> <p>Intentionally setting of the F_ADDR_XXXXX_IPAR_EN variable starts the process for applying the iParameters. The process depends on the F-Device used. For more detailed information, please refer to the device-specific user documentation.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>WARNING: Depending on the application, applying the iParameters can result in hazardous states Take appropriate measures to ensure that your system/machine does not present any danger when the application of the iParameters is initiated and/or iParameters are applied.</p> </div>
F_ADDR_XXXXX_CHF_ACK_REQ *)	BOOL	<p>A channel error in the F-Device can be acknowledged (CHF_ACK_REQ_S).</p> <p>(Only for F-Devices in accordance with PROFIsafe profile V2.6.1.)</p>
F_ADDR_XXXXX_CHF_ACK_REI *)	BOOL	<p>Channel error acknowledgement (CHF_ACK_C)</p> <p>(Only for F-Devices in accordance with PROFIsafe profile V2.6.1.)</p>
F_ADDR_XXXXX_CE_CRC_H *)	BOOL	<p>Communication error (F_CE_CRC_H)</p> <p>Local F-Host driver reports communication error.</p>
F_ADDR_XXXXX_WD_TIMEOUT_H *)	BOOL	<p>Communication error (F_WD_TIMEOUT_H)</p> <p>Local F-Host driver reports communication error.</p>
F_ADDR_XXXXX_LOOPBACK *)	BOOL	<p>Communication error (loopback check)</p> <p>Local F-Host driver reports communication error.</p>
*) XXXXX = Number of the F-Device (e.g., F_ADDR_00001_PASS_ON, see Figure 4-65 on page 148)		



WARNING:

The variables specified in the table can be toggled. Program an evaluation function in the PLCnext Engineer software (e.g., using edge detection).

8.3.4 Global management/diagnostic variables for F-Devices

The table below describes management/diagnostic variables, which are globally created in PLCnext Engineer for all F-Devices. These variables indicate that the condition for setting these variables applies to at least one configured F-Device. The variables are not created by default. To create them, the relevant parameters must be set to “create” in PLCnext Engineer (see [Figure 4-48 on page 133](#)).



WARNING: Outputs can be set

Do not acknowledge an operator acknowledge request automatically from the application program. Acknowledgment must be triggered by an intentional user action.

When reintegrating passivated PROFIsafe devices, safety-related outputs can be set.

Take appropriate measures to ensure that your system/machine does not present any danger when passivated PROFIsafe devices are reintegrated.

Table 8-8 Management/diagnostic variables for F-Devices



System variable	Type	Meaning
PASS_OUT_GLOBAL	BOOL	At least one F-Device is passivated. Possible reasons for passivation: <ul style="list-style-type: none"> - Programmed passivation via the F_ADDR_XXXXX_PASS_ON system variable - Communication, device, and parameterization errors (see F_ADDR_XXXXX_ACK_REQ system variable)
ACK_REQ_GLOBAL	BOOL	At least one F-Device requires an operator acknowledge request after removing an error. Possible reasons for activating the operator acknowledge request: <ul style="list-style-type: none"> - Communication error (CRC, F_WD_TIME_OUT) - Error in an F-Device. Please refer to the user documentation for the F-Devices used.
ACK_REI_GLOBAL	BOOL	If at least one F-Device requires an operator acknowledge request, this can be acknowledged by means of an operator acknowledge reintegration (ACK_REI_GLOBAL).
DEVICE_FAULT_GLOBAL	BOOL	Error in at least one F-Device. If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out via the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variables. If the cause has been removed, the F_ADDR_XXXXX_DEVICE_FAULT variable is set to FALSE again. <div style="border: 1px solid black; padding: 5px; display: inline-block;">  <p>For information on which errors cause the used F-Device to control this variable, please refer to the device-specific user documentation.</p> </div>

Table 8-8 Management/diagnostic variables for F-Devices [...]

System variable	Type	Meaning
CE_CRC_GLOBAL	BOOL	<p>Communication error (F_CE_CRC)</p> <p>This parameter is set if at least one of the following reasons applies:</p> <ul style="list-style-type: none"> - At least one F-Device has detected a communication error during operation that was caused by an incorrect CRC checksum. - Inconsistent parameterization between F-Host and F-Device. - Communication error between F-Host and F-Device. <p>If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out via the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variables. If the cause has been removed, the F_ADDR_XXXXX_CE_CRC variable is set to FALSE again.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  In terms of system availability, this type of CRC error should only occur once every ten hours at the most (see PROFIsafe specification regarding "SIL Monitor" and "Operator Acknowledge"). </div>
WD_TIME_OUT_GLOBAL	BOOL	<p>Communication error (F_WD_TIME_OUT)</p> <p>Set if at least one F-Device has detected a communication error caused by the parameterized F_WD_Time being exceeded.</p> <p>If this variable was set to TRUE during operation, the cause of the error must be removed first so that acknowledgment can be carried out via the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variables. If the cause has been removed, the F_ADDR_XXXXX_WD_TIME_OUT variable is set to FALSE again.</p>
CHF_ACK_REI_GLOBAL	BOOL	<p>At least one F-Device reports a channel error in the F-Device and can be acknowledged (CHF_ACK_C).</p> <p>(Only for F-Devices in accordance with PROFIsafe profile V2.61.)</p>
CHF_ACK_REQ_GLOBAL	BOOL	<p>At least one F-Device reports a channel error in the F-Devices and can be acknowledged (CHF_ACK_REQ_S).</p> <p>(Only for F-Devices in accordance with PROFIsafe profile V2.61.)</p>
CE_CRC_H_GLOBAL	BOOL	At least one local F-Host driver reports a communication error (F_CE_CRC_H).
WD_TIMEOUT_H_GLOBAL	BOOL	At least one local F-Host driver reports a communication error (F_WD_TIMEOUT_H).
LOOPBACK_GLOBAL	BOOL	At least one local F-Host driver reports a communication error (loopback check).



WARNING:

The variables specified in the table can be toggled. Program an evaluation function in the PLCnext Engineer software (e.g., using edge detection).

8.3.5 Management/diagnostic variables of the iSPNS 3000 F-Device

8.3.5.1 PROFIsafe: Device diagnostics variables (local device)

The table below lists management/diagnostic variables. These variables can be created in PLCnext Engineer for the iSPNS 3000 configured as an F-Device. The table shows which variables are created by default. This setting can be modified by changing the value (Create/Do not create).

The F_Destination_Address of the iSPNS 3000 (F_Dest_Add) is specified by the “[nnnn]” in the variable name.

Management/diagnostic variable	Default setting
FD_ADDR_[nnnn]_ACK_REQ_DEV	Do not create
FD_ADDR_[nnnn]_PASS_ON_DEV	Do not create
FD_ADDR_[nnnn]_PASS_OUT_DEV	Do not create
FD_ADDR_[nnnn]_IPAR_EN_DEV	Do not create
FD_ADDR_[nnnn]_IPAR_OK_DEV	Do not create
FD_ADDR_[nnnn]_DEVICE_FAULT_DEV	Do not create
FD_ADDR_[nnnn]_CHF_ACK_REI_DEV	Do not create
FD_ADDR_[nnnn]_CHF_ACK_REQ_DEV	Do not create
FD_ADDR_[nnnn]_CE_CRC_DEV	Do not create
FD_ADDR_[nnnn]_WD_TIMEOUT_DEV	Do not create



WARNING: Variables can be toggled

The variables specified in [Table 8-9](#) can be toggled.

- Program an evaluation function in the PLCnext Engineer software (e.g., using edge detection).

Table 8-9 PROFIsafe: Device diagnostics variables (local device)



System variable	Type	Meaning
FD_ADDR_[nnnn]_ACK_REQ_DEV *)	BOOL	The iSPNS 3000 F-Device requests an operator-acknowledge request from the higher-level safety-related controller (F-Host) after removing an error. Possible reasons for activating the operator acknowledge request: – Communication error (CRC, F_WD_TIME_OUT)
FD_ADDR_[nnnn]_PASS_ON_DEV *)	BOOL	The iSPNS 3000 F-Device will be passivated by the higher-level safety-related controller (F-Host) when this variable is set to TRUE from the application program.  WARNING: Resetting this variable to FALSE means that the safe input and output data is transmitted immediately. <ul style="list-style-type: none"> • Take appropriate measures to ensure that your system/machine does not present any danger when passivation of the iSPNS 3000 F-Device is reset.
FD_ADDR_[nnnn]_PASS_OUT_DEV *)	BOOL	The iSPNS 3000 F-Device is passivated. Possible reasons for passivation: – Programmed passivation via the FD_ADDR_[nnnn]_PASS_ON_DEV system variable – Communication, device, and parameterization errors (see FD_ADDR_[nnnn]_ACK_REQ_DEV system variable)
FD_ADDR_[nnnn]_IPAR_EN_DEV *)	BOOL	Initiate application of the iParameters This variable is set in the application in order to initiate the application of the iParameters. Intentionally setting the FD_ADDR_[nnnn]_IPAR_EN_DEV from the higher-level safety-related controller (F-Host) starts the process for applying the iParameters to the iSPNS 3000 F-Device. The process depends on the higher-level safety-related controller used. For more detailed information, please refer to the device-specific user documentation.  WARNING: Depending on the application, applying the iParameters can result in hazardous states. <ul style="list-style-type: none"> • Take appropriate measures to ensure that your system/machine does not present any danger when the application of the iParameters is initiated and/or iParameters are applied.

Table 8-9 PROFIsafe: Device diagnostics variables (local device)


System variable	Type	Meaning
FD_ADDR_[nnnn]_IPAR_OK_DEV *)	BOOL	<p>The iSPNS 3000 F-Device indicates that “the iParameters have been applied”.</p> <p>This variable is set when the iSPNS 3000 F-Device reports that it has applied the iParameters.</p>
FD_ADDR_[nnnn]_DEVICE_FAULT_DEV *)	BOOL	<p>Error in the iSPNS 3000 F-Device.</p> <p>This variable can be set to TRUE or FALSE in the application program during operation.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>WARNING:</p> <p>The status change of this variable from TRUE to FALSE leads to the immediate transmission of the safe input and output data by the iSPNS 3000 F-Device.</p> <ul style="list-style-type: none"> • Take appropriate measures to ensure that your system/machine does not present any danger if the error state of the iSPNS 3000 F-Device has been removed. </div>

Table 8-9 PROFIsafe: Device diagnostics variables (local device)



System variable	Type	Meaning
FD_ADDR_[nnnn]_CE_CRC_DEV *)	BOOL	<p>Communication error (F_CE_CRC)</p> <p>This parameter is set if at least one of the following reasons applies:</p> <ul style="list-style-type: none"> - The iSPNS 3000 F-Device has detected a communication error during operation that was caused by an incorrect CRC checksum. - Inconsistent parameterization between the higher-level safety-related controller (F-Host) and the iSPNS 3000 F-Device. - There is a communication error between the higher-level safety-related controller (F-Host) and the iSPNS 3000 F-Device. <p>If this variable was set to TRUE during operation, the cause of the error must be removed first to enable the higher-level safety-related controller (F-Host) to carry out acknowledgment and reintegration. If the cause has been removed, the FD_ADDR_[nnnn]_CE_CRC_DEV variable is set to FALSE again.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  In terms of system availability, this type of CRC error should only occur once every 10 hours at the most (see PROFIsafe specification regarding "SIL Monitor" and "Operator Acknowledge"). </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  During PROFIsafe system startup this variable is briefly set as a result of the PROFIsafe system startup behavior. This is not relevant for the 10-hour monitoring period described above following a CRC error that occurred during operation. </div>
FD_ADDR_[nnnn]_CHF_ACK_REQ_DEV *)	BOOL	A channel error in the iSPNS 3000 F-Device can be acknowledged.
FD_ADDR_[nnnn]_CHF_ACK_REI_DEV *)	BOOL	Channel error acknowledgement

Table 8-9 PROFIsafe: Device diagnostics variables (local device)

System variable	Type	Meaning
FD_ADDR_[nnnn]_WD_TIME_OUT_DEV *)	BOOL	<p>Communication error (F_WD_TIME_OUT)</p> <p>Set if the iSPNS 3000 F-Device has detected a communication error caused by the parameterized F_WD_Time being exceeded.</p> <p>If this variable was set to TRUE during operation, the cause of the error must be removed first to enable the higher-level safety-related controller (F-Host) to carry out acknowledgment and reintegration. If the cause has been removed, the FD_ADDR_[nnnn]_WD_TIME_OUT_DEV variable is set to FALSE again.</p>
*) [nnnn] = F_Destination-Address (F_Dest_Add) of the iSPNS 3000 used in the application as an F-Device is in the range: 1 ... 65534.		

8.3.5.2 PROFIsafe: Collective diagnostics variables (local device)

The table below describes management/diagnostic variables, which are globally created in PLCnext Engineer for the iSPNS 3000 as an F-Device. These variables indicate that the condition for setting these variables applies to at least one iSPNS 3000 configured as an F-Device. The variables are not created by default. To create them, the relevant parameters must be set to "Create" in PLCnext Engineer (see [Figure 4-44 on page 130](#)).



WARNING: Outputs can be set

- Do **not** acknowledge an operator acknowledge request automatically from the application program.
- Trigger acknowledgment only by an intentional user action.
When reintegrating passivated PROFIsafe devices, safety-related outputs can be set.
- Take appropriate measures to ensure that your system/machine does not present any danger when passivated PROFIsafe devices are reintegrated.



WARNING: Variables can be toggled

The variables specified in [Table 8-10](#) can be toggled.

- Program an evaluation function in the PLCnext Engineer software (e.g., using edge detection).

Table 8-10 PROFIsafe: Collective diagnostics variables (local device)

System variable	Type	Meaning
ACK_REQ_DEV_GLOBAL	BOOL	At least one iSPNS 3000 configured as an F-Device requires an operator-acknowledge request after removing an error. Possible reasons for activating the operator acknowledge request: – Communication error (CRC, F_WD_TIME_OUT)
CE_CRC_DEV_GLOBAL	BOOL	Communication error (F_CE_CRC) The iSPNS 3000 currently only supports one F-Device instance: see FD_ADDR_[nnnn]_CE_CRC_DEV system variable.
WD_TIMEOUT_DEV_GLOBAL	BOOL	Communication error (F_WD_TIME_OUT) The iSPNS 3000 currently only supports one F-Device instance: see FD_ADDR_[nnnn]_WD_TIMEOUT_DEV system variable.

8.3.6 PROFINET system variables

The table below describes the PROFINET system variables of the integrated PROFINET controller functionality.

Table 8-11 PROFINET system variables (PROFINET controller functionality)

System variable	Type	Meaning
PNIO_SYSTEM_BF	BOOL	No connection to a configured PROFINET device An error has occurred in the PROFINET network, i.e., a connection could not be established to at least one configured PROFINET device. This value is not set if the "Control BF" parameter was set to FALSE for a PROFINET device. This PROFINET device has therefore been excluded from connection monitoring.
PNIO_SYSTEM_SF	BOOL	Diagnostic alarm on a configured PROFINET device At least one PROFINET device is indicating a system error (diagnostic alarm or maintenance alarm). The error priority can be determined from the PNIO_DIAG_AVAILABLE, PNIO_MAINTENANCE_DEMANDED, and PNIO_MAINTENANCE_REQUIRED variables.
PNIO_MAINTENANCE_DEMANDED	BOOL	Maintenance demand At least one PROFINET device is indicating the "maintenance demand" alarm (high-priority maintenance alarm) with an active connection. The RALRM diagnostic block can be used to identify the PROFINET device.
PNIO_MAINTENANCE_REQUIRED	BOOL	Maintenance required At least one PROFINET device is indicating the "maintenance requirement" alarm (low-priority maintenance alarm) with an active connection. The RALRM diagnostic block can be used to identify the PROFINET device.
PNIO_CONFIG_STATUS	WORD	Configuration status of the PROFINET controller
PNIO_CONFIG_STATUS_ACTIVE	BOOL	The variable is set if the desired configuration for the PROFINET controller has been loaded. In this state, the PROFINET controller attempts to establish a connection cyclically to all PROFINET devices in the desired configuration (under the PROFINET icon).
PNIO_CONFIG_STATUS_READY	BOOL	This variable is set if the PROFINET controller has been initialized correctly. No desired configuration has been loaded by PLCnext Engineer.
PNIO_CONFIG_STATUS_CFG_FAULT	BOOL	The desired PROFINET controller configuration has not been applied due to a serious error. Please contact Phoenix Contact.
PNIO_FORCE_FAILSAFE	BOOL	All PROFINET devices are prompted to set their configured substitute values.

If one of these values is set, it is now possible to decide from the program whether the system should continue operating. For example, system errors such as maintenance requirement and maintenance demand can only result in a message to the service personnel, which informs them of the location, cause, and urgency of the error.

The table below describes the PROFINET system variables of the integrated PROFINET device functionality.

Table 8-12 PROFINET system variables (PROFINET device functions)

System variable	Type	Meaning
PND_S1_PLC_RUN	BOOL	Status of the higher-level PROFINET controller Information on whether the higher-level PROFINET controller is active. The value is TRUE if the higher-level PROFINET controller is in the RUN state (program is being processed). The display only applies when there is an existing PROFINET connection (PND_S1_VALID_DATA_CYCLE).
PND_S1_VALID_DATA_CYCLE	BOOL	The higher-level PROFINET controller has established the connection. Information indicating whether a connection exists and cyclic data is being exchanged between the PROFINET controller and PROFINET device and whether the last frame received contained valid data (DATA_VALID_BIT).
PND_S1_OUTPUT_STATUS_GOOD	BOOL	IOP status of the higher-level PROFINET controller Information on whether the input process data (PND_S1_INPUTS) was received by the PROFINET device with the "valid" status. The value is TRUE if the output process data of the higher-level PROFINET controller is valid (provider status).
PND_S1_INPUT_STATUS_GOOD	BOOL	IOC status of the higher-level PROFINET controller
PND_S1_DATA_LENGTH	WORD	Process data length that was configured for the PROFINET device.
PND_S1_OUTPUTS	PND_IO_512	Output process data Memory area for output process data that the PROFINET device sends to the higher-level PROFINET controller.
PND_S1_INPUTS	PND_IO_512	Input process data Memory area for input process data that the PROFINET device receives from the higher-level PROFINET controller.

8.4 System time

The RTC system variable uses the RTC_TYPE structure to provide information about the system time.

Table 8-13 RTC system variable and elements of the RTC_TYPE structure

System variable/elements	Type	Meaning
RTC	RTC_TYPE	The structure provides information about the realtime clock inside the device.
HOURS	USINT	System time (hours)
MINUTES	USINT	System time (minutes)
SECONDS	USINT	System time (seconds)
DAY	USINT	System time (day)
MONTH	USINT	System time (month)
YEAR	UINT	System time (year)

8.5 PLC_CRC_PRJ

The PLC_CRC_PRJ system variable provides information about the CRC of the non-safety-related project.

Table 8-14 PLC_CRC_PRJ system variable

System variable	Type	Meaning
PLC_CRC_PRJ	UINT	Information about the CRC of the non-safety-related project

8.6 TCP_SOCKET, UDP_SOCKET, and TLS_SOCKET function blocks

The TCP_SOCKET and UDP_SOCKET function blocks are used to open and close the IP sockets that are used for IP communication via TCP (Transmission Control Protocol) or via UDP (User Datagram Protocol). You can use the TLS_SOCKET function block to open and close IP sockets, which are used for secure IP communication via TLS (Transport Layer Security).

You can request the number of opened IP sockets using the following system variables:


Table 8-15 System variables for the TCP_SOCKET, UDP_SOCKET, and TLS_SOCKET function blocks

System variable	Type	Meaning
IP_ACTIVE_SOCKETS	UINT	Number of IP sockets opened using the TCP_SOCKET and UDP_SOCKET function blocks
TLS_ACTIVE_SOCKETS	UINT	Number of IP sockets opened using the TLS_SOCKET function block

8.7 DEVICE_STATE

The DEVICE_STATE system variable uses the DEVICE_STATE_4xxx_TYPE structure to provide information about the temperature of the processor board, the optional fan module, and the processor load.

Table 8-16 DEVICE_STATE system variable and elements of the DEVICE_STATE_4xxx_TYPE structure

System variable/elements	Type	Meaning
DEVICE_STATE	DEVICE_STATE_4xxx_TYPE	The system variable provides the information in the DEVICE_STATE_4xxx_TYPE structure.
BOARD_TEMPERATURE	SINT	Currently measured temperature of the processor board. Internal device temperature in degrees Celsius
FAN_FAIL	BOOL	The fan is defective.  NOTE: Device defect due to overheating • Immediately replace the fan when the defect occurs.
RAMDISK_USAGE	USINT	Memory used on the RAM disk
CPU_LOAD_ALL_CORES	USINT	Current processor load of the system (average expressed as percentage)
CPU_LOAD_PER_CORE		Information about the load per processor core
[1]	USINT	Current processor load of CPU 1 (percentage)
[2]	USINT	Current processor load of CPU 2 (percentage)

8.8 Task handling

Programs and program parts are treated as tasks in PLCnext Engineer. Individual tasks are coordinated and processed in the Execution and Synchronization Manager (ESM). The ESM_DATA system variable uses the ESM_DAT structure to provide information about task handling of the ESM:

Table 8-17 ESM_DATA system variable for task handling and elements of the ESM_DAT structure

System variable/elements	Type	Meaning
ESM_DATA	ESM_DAT	Information about task handling of Execution and Synchronization Manager for both processor cores of the RFC
ESM_COUNT	USINT	Number of the ESM (one ESM for each processor core)
ESM_INFOS		Information on ESMs [1 ... 2]
[1] ... [2]		
TASK_COUNT	UINT	Number of tasks that have been configured for the ESM

Table 8-17 ESM_DATA system variable for task handling and elements of the ESM_DAT structure

System variable/elements	Type	Meaning
TICK_COUNT	UDINT	Number of system ticks This variable shows the total number of pulses delivered by the system clock since the last startup.
TICK_INTERVAL	UDINT	Time interval of system ticks in ms
TASK_INFOS		Information on tasks [1 ... 16]. The information is displayed in the assigned elements.
[1] ... [16]		
INTERVAL	LINT	For cyclic tasks: interval time in μ s For acyclic tasks: 0
PRIORITY	INT	Priority of the task
WATCHDOG	LINT	Watchdog time in μ s (0 = No watchdog)
LAST_EXEC_DURATION	LINT	Execution duration of tasks in the previous cycle in μ s (including interruptions by higher-priority tasks)
MIN_EXEC_DURATION	LINT	Minimum execution duration of tasks in μ s (including interruptions by higher-priority tasks)
MAX_EXEC_DURATION	LINT	Maximum execution duration of tasks in μ s (including interruptions by higher-priority tasks)
LAST_ACTIVATION_DELAY	LINT	Delay of the task in the previous cycle in μ s
MIN_ACTIVATION_DELAY	LINT	Minimum delay of tasks in μ s (delay occurs if higher-priority tasks are pending at the time of task activation)
MAX_ACTIVATION_DELAY	LINT	Maximum delay of tasks in μ s (delay occurs if higher-priority tasks are pending at the time of task activation)
EXEC_TIME_THRESHOLD	LINT	Configured time in μ s.
EXEC_TIME_THRESHOLD_CNT	UDINT	If the execution time of the task exceeds the time configured via EXEC_TIME_THRESHOLD, the value of the EXEC_TIME_THRESHOLD_CNT variable is incremented.
NAME	STRING	Name or designation of task
EXCEPTION_COUNT	USINT	Number of exceptions ...
EXCEPTION_INFOS		Information on exceptions [1 ... 2]
[1] ... [2]		
TYPE_ID	UDINT	
SUB_TYPE		Name of exception
SUB_TYPE_ID	UDINT	
TASK_NAME	STRING	Name of the ESM task in which the exception was triggered
PROGRAM_NAME		Name of the program instance in which the exception was triggered
INFORMATION		

8.9 HMI_STATUS

The HMI_STATUS system variable uses the HMI_STATUS_TYPE structure to provide information about the web server that can be programmed in PLCnext Engineer.

Table 8-18 HMI_STATUS system variable and elements of the HMI_STATUS_TYPE structure

System variable/elements	Type	Meaning
HMI_STATUS	HMI_STATUS_TYPE	Information on the web server that can be programmed in PLCnext Engineer
CLIENT_COUNT	UINT	Number of existing client connections to the web server at runtime
CLIENTS		Information on existing client connections
[1] ... [256]		Client connections 1 ... 256
SESSION_ID	STRING	Session ID of client connection
STATION_ID	STRING	Station ID of client connection
LAST_REQ	LINT	
IP_ADDRESS		IP address of the connected client
[0] ... [3]	BYTE	IP address in hexadecimal format: [C0].[A8].[01].[64] ⇒ 192.168.1.100

8.10 HMI_CONTROL

The HMI_CONTROL system variable uses the HMI_CONTROL_TYPE structure to provide information on the individual client connections.

Table 8-19 HMI_CONTROL system variable and elements of the HMI_CONTROL_TYPE structure

System variable/elements	Type	Meaning
HMI_CONTROL	HMI_CONTROL_TYPE	Information on individual client connections
Clients		
[1] ... [256]		Client connections 1 ... 256
DISABLE	BOOL	Set this bit to disconnect the corresponding client from the server.

9 Web-based management WBM

The Web-based management interface integrated in the controller allows you to display static and dynamic information from the controller from anywhere in the network via a web browser (e.g., Internet Explorer 9).

The status and diagnostic functions are clearly displayed on a graphical user interface. Every user with a network connection to the device has read access to that device via a browser. A wide range of information about the device itself, set parameters, and the operating state can be viewed.

In Web-based management, you can manage the credentials of users who are permitted to access the controller.

9.1 Requirements for the use of WBM

WBM via Ethernet

As the web server operates using the Hyper Text Transfer Protocol, a web browser can be used. Access is via URL "http://IP address of the device". Example: "http://192.168.1.10". You can call WBM via every Ethernet interface of the RFC 4072S.



Calling Web-based management – Valid IP address required

WBM can only be called using a valid IP address. In the delivery state, IP address "192.168.1.10" is preset for Ethernet interface LAN1.

Also refer to the information in [Section "Web server" on page 182](#) when calling WBM.

9.2 Establishing a connection to WBM

To establish a connection to WBM, proceed as follows:

- Open the web browser on your PC.
- In the address field, enter URL "http://IP address of the controller" (example: "http://192.168.1.10").



If there is a PLCnext Engineer HMI application on the controller, entering URL "http://IP address of the controller" calls the PLCnext Engineer application.

- To call WBM in this case, enter URL "http://IP address of the controller/wbm".

Initial access: TLS certificate

The controller web server uses a self-signed TLS certificate automatically generated by the controller for secure communication. Before the controller web server can be accessed, you must authorize the TLS certificate in your web browser.



Please note the following points:

- The controller generates the TLS certificate during its startup phase.
- The certificate uses the IP address of the Ethernet interface with PROFINET control function.
- The certificate is used for all Ethernet interfaces of the controller.
- Each IP address assigned to the controller must be permitted in the web browser before a PLCnext Engineer HMI application is accessed via the address and therefore via the corresponding Ethernet interface.
- The certificate is regenerated after the controller is reset to factory settings.
- The certificate and a private key are located in the following directory:
 - /opt/plcnext/Security/Certificates/https/https_cert.pem
 - /opt/plcnext/Security/Certificates/https/https_key.pem

For information on how to access the parameterization memory via the SFTP protocol using SFTP client software (e.g., WinSCP), please refer to [Section “Using SFTP to access the file system” on page 76](#) and [Section “Parameterization memory: directory structure and access” on page 175](#)

**Initial access:
welcome page**

The RFC 4072S welcome page is shown when accessing the controller web server for the first time.

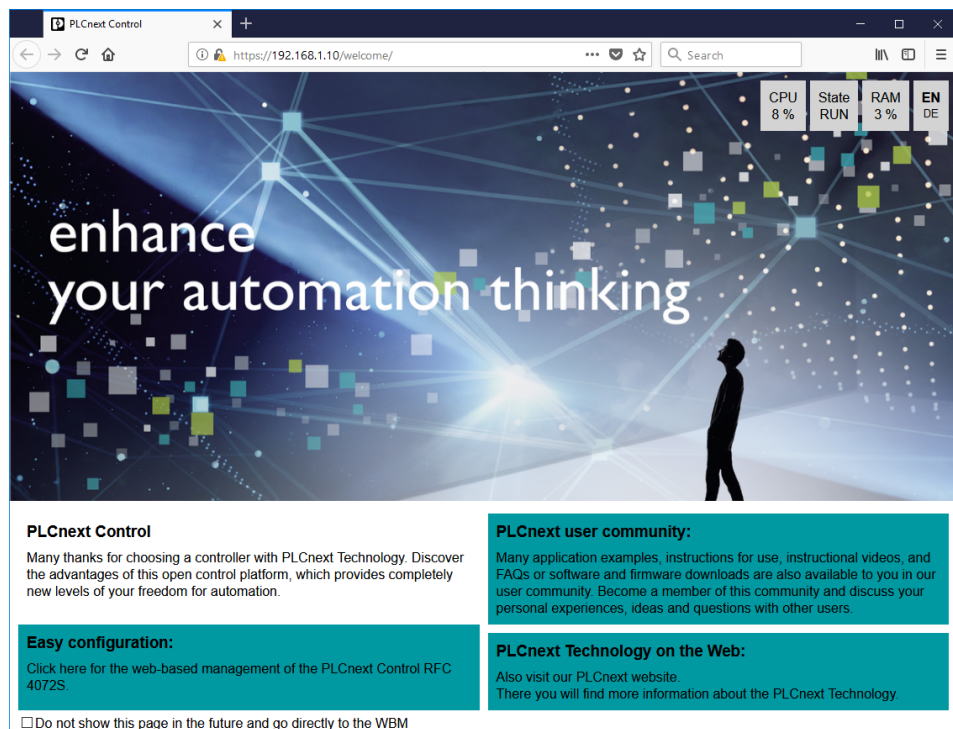


Figure 9-1 RFC 4072S welcome page

The welcome page contains links to the following web content:

- WBM of the RFC
- PLCnext Community
- PLCnext website



If you do not want the welcome page to be displayed each time the controller web server is accessed:

- Click the “Do not show this page in the future and go directly to the WBM” check box.

The next time you access the controller web server, the login page of WBM opens, see [Section 9.5](#).

Alternatively, you can enter URL “http://IP address of the controller/wbm” (example: “http://192.168.1.10/wbm”) in your browser address field. In this case, WBM is displayed immediately.

The welcome page remains accessible via URL “http://IP address of the controller/welcome”.

9.3 Licenses and legal information

The RFC 4072S uses a Linux operating system.

All the license information stored on the RFC can be called using the “Licenses and Legal Information” link on every page of WBM:

- Click on the “Licenses and Legal Information” link on the bottom of a WBM page.



Figure 9-2 “Licenses and Legal Information” link

All licenses of the Open source software used are shown in the window that opens.

9.4 Changing the language

You can change the language for the WBM user interface in the top left of the web browser window.

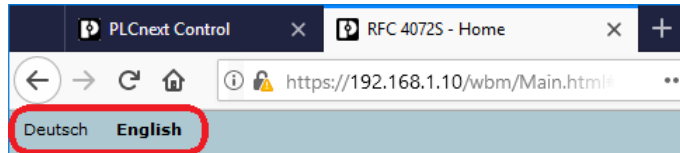


Figure 9-3 WBM user interface: selecting the language

Click the “Deutsch” or “English” link to change the language.
WBM then immediately switches to the desired language.

9.5 Login

The WBM login page is displayed when

- You access WBM for the first time
- You have activated the WBM user authentication function, see [Section 9.6.4.1](#).

If you disable user authentication, logging in is not necessary to access WBM. In this case, the WBM start page is displayed when WBM is accessed, see [Section 9.6](#).

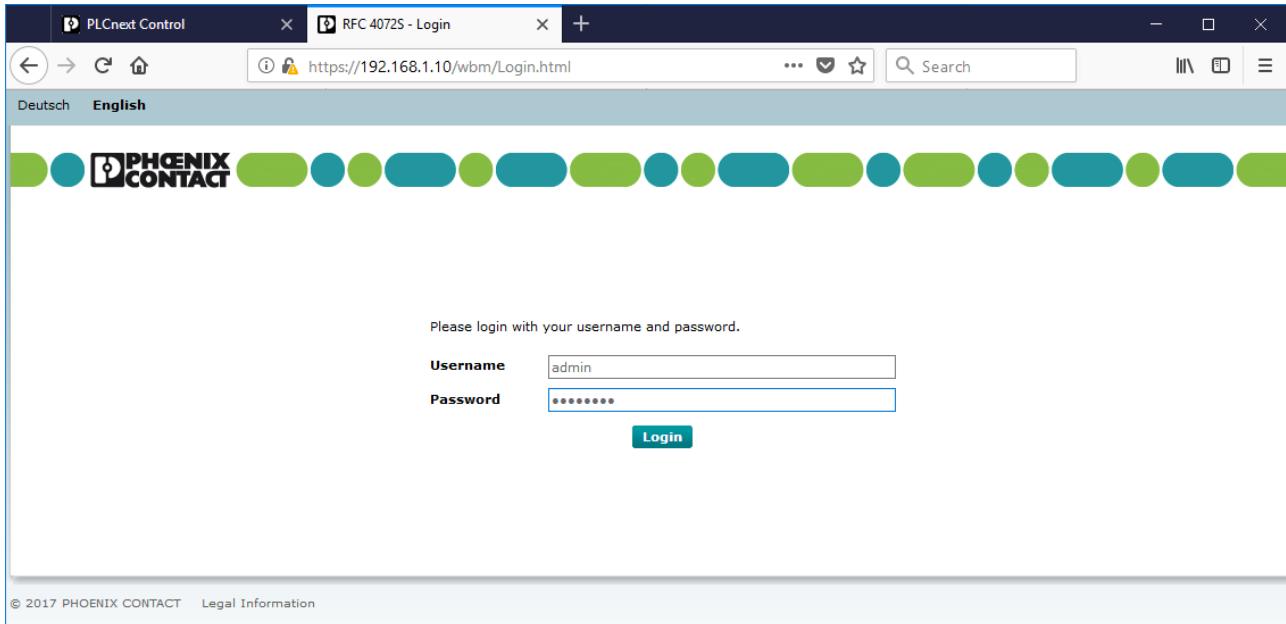


Figure 9-4 WBM: Login page

Initial access as administrator

When you access WBM for the first time, log in as the administrator.

- Enter the user name “admin” in the “Username” input field.
- Enter the administrator password in the “Password” input field. The administrator password is printed on the controller (see [Figure 2-36 on page 76](#)).
- To open WBM, click on the “Login” button.

The WBM start page opens (see [Section 9.6](#)).



Recommended:

- Only use the administrator password for initial login.
- Once you have logged in successfully, change the administrator password to prevent unauthorized administrator access (see [Section 9.6.4.1](#)).

**Please note:**

After changing the access data for the administrator, it is no longer possible to login with the user name “admin” and the administrator password printed on the controller.

Logging in as user

If WBM user authentication is activated, log in using your user details.

- Enter your user name in the “Username” input field.
- Enter your password in the “Password” input field.
- To open WBM, click on the “Login” button.

The WBM start page opens (see [Section 9.6](#)).

9.6 WBM start page – Areas and functions



Figure 9-5 WBM start page

WBM is organized into the following areas:

- Information: general device information
- Diagnostics: PROFINET
- Configuration: update of the non-safety-related device firmware
- Security: user authentication, certificate authentication and firewall
- Administration:

9.6.1 “Information” area

This area includes general device information.

9.6.1.1 “General Data” page

Here you will find general details on the device, e.g., device version and order number as well as manufacturer details.

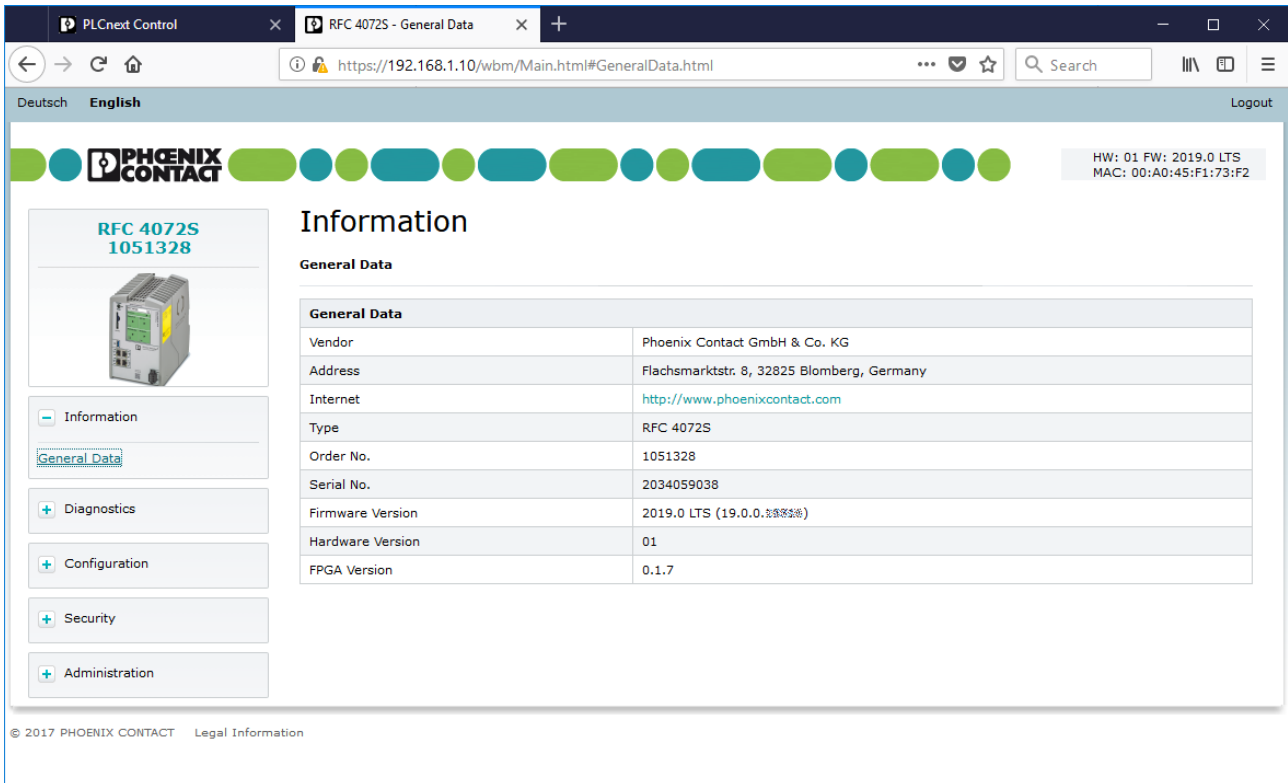


Figure 9-6 WBM: “General Data” page

9.6.2 “Administration” area

9.6.2.1 “Update Firmware” page

Here you can start the update of the non-safety-related device firmware.

The procedure is described in [Section 9.7](#).

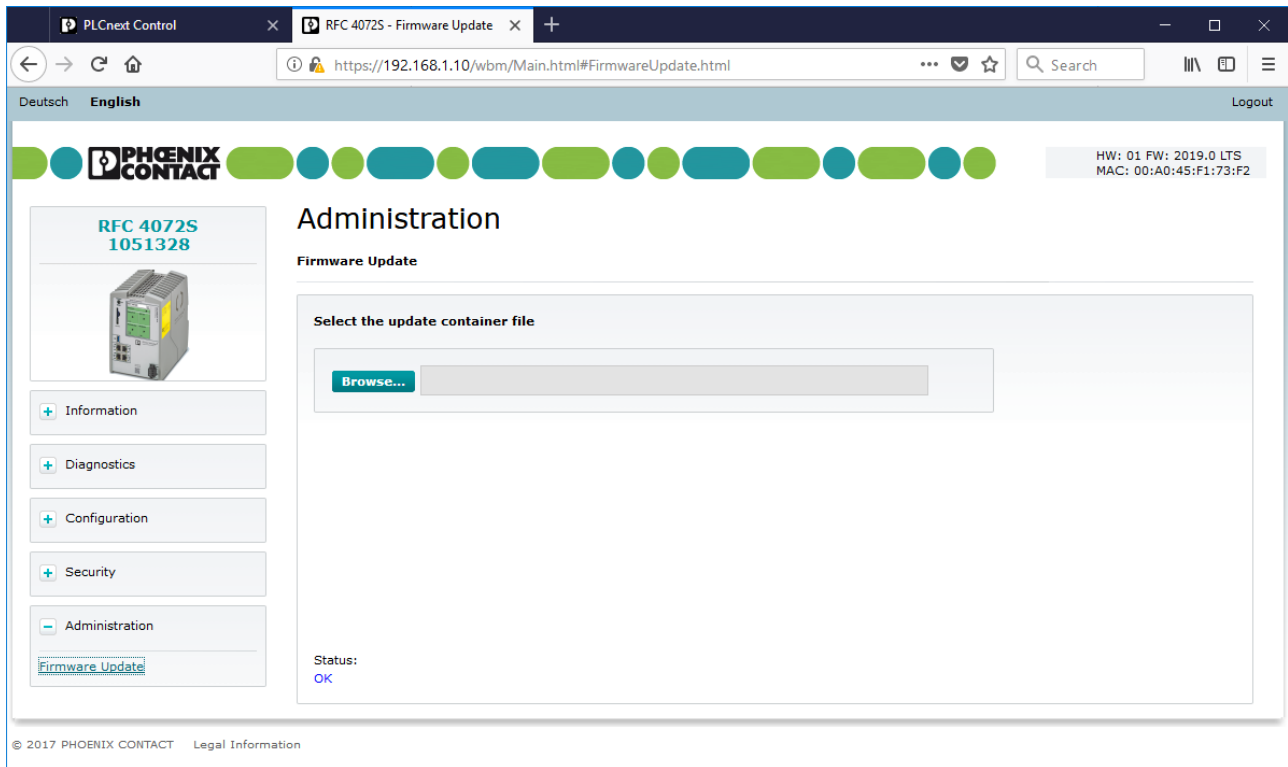


Figure 9-7 WBM: “Firmware Update” page

9.6.3 “Diagnostics” area

9.6.3.1 “PROFINET” page

PROFINET diagnostics: overview

The “Overview” tab displays information about the PROFINET controller.

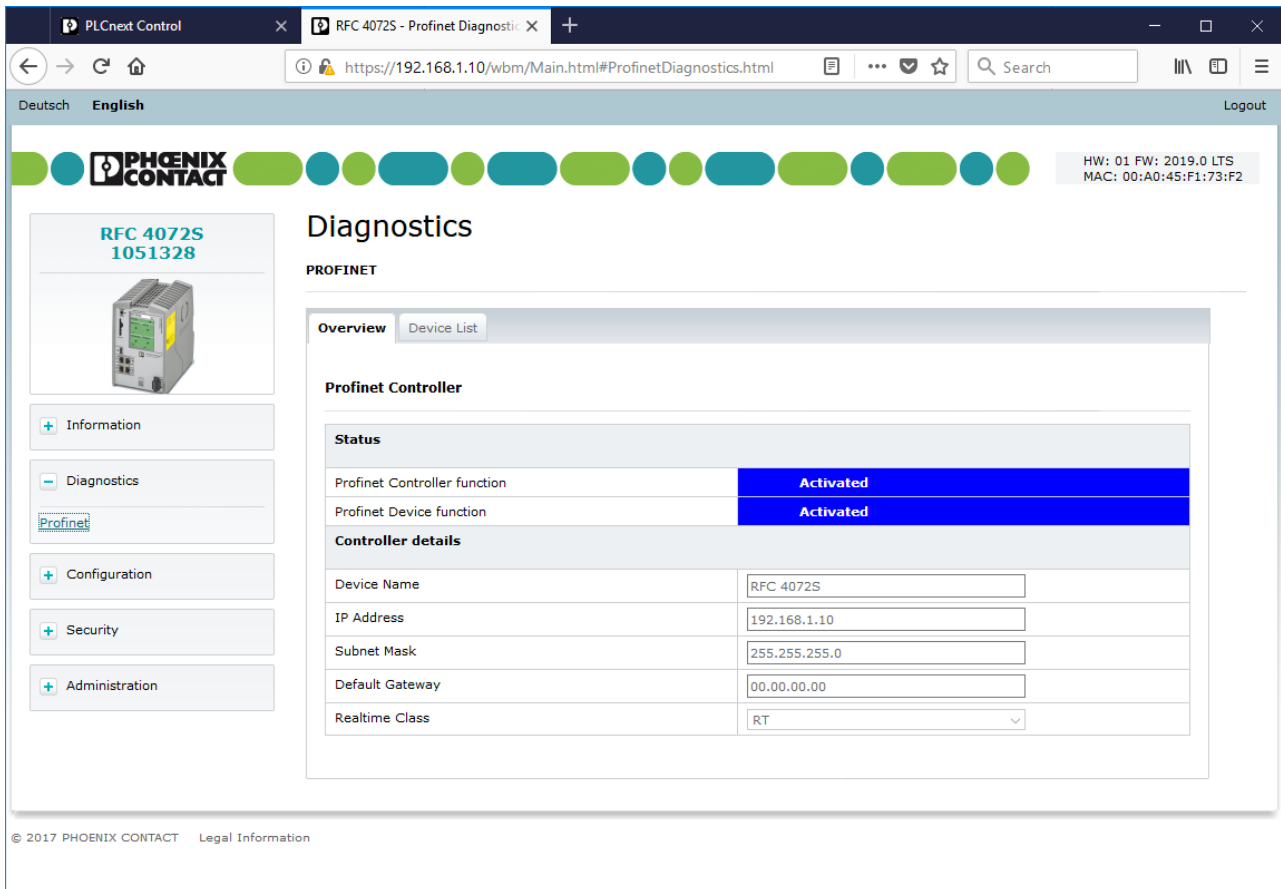


Figure 9-8 WBM: “PROFINET Diagnostics – Overview” page

PROFINET diagnostics: device list The “Device List” tab displays information about the PROFINET controller.

The screenshot displays the 'PROFINET Diagnostics' page in a web browser. The browser address bar shows the URL: `https://192.168.1.10/wbm/Main.html#ProfinetDiagnostics.html`. The page title is 'Diagnostics' and the sub-section is 'PROFINET'. The 'Device List' tab is selected, showing a table of connected devices.

No.	Device Name	IP Address	Active	Diagnostics	Details
1	AXL-F-BK-PN-TPS-1*	192.168.1.20	TRUE	0x0020	
2	AXL-F-BK-PN-1*	192.168.1.30	TRUE	0x0020	

Below the table, there is a legend for diagnostic status:
 ● OK (Green)
 ● Warning (Yellow)
 ● Error (Red)

At the bottom of the table area, it shows:
 * - Profinet participants with own Web Based Management (Reachable via the link)
 Diagnostics: ● Online | Status: OK

Figure 9-9 WBM: “PROFINET Diagnostics – Device List” page

9.6.4 “Security” area

This area contains settings and information about the following topics:

- User Authentication
- Certificate Authentication
- Firewall

9.6.4.1 “User Authentication” page

The IP address settings assigned to the device are displayed here.

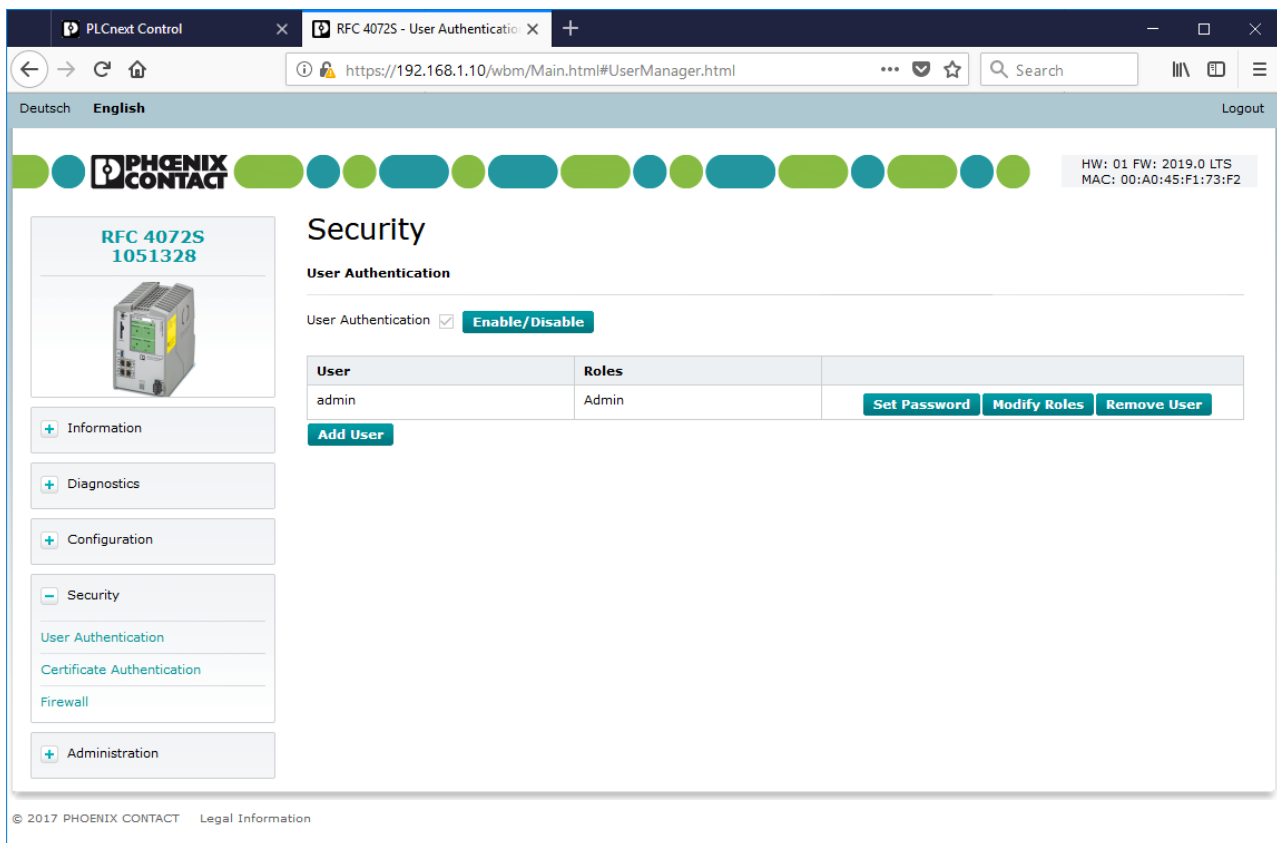


Figure 9-10 WBM: “User Authentication” page

User authentication

Enable or disable user authentication on the “User Authentication” page. When user authentication is enabled, authentication with a user name and password is required for access to certain components of the RFC 4072S and certain functions in PLCnext Engineer.

When user authentication is disabled, authentication is not necessary to access WBM, the RFC 4072S OPC UA server, or PLCnext Engineer. Access to the file system via SFTP and access to the shell via SSH requires authentication (with administrator rights) even if user authentication is disabled.

User authentication is enabled by default. Upon delivery, the “admin” user is already created with administrator rights.

**Recommended:**

- Only use the administrator password printed on the controller for logging into WBM for the first time.
- Once you have logged in successfully, change the administrator password to prevent unauthorized administrator access.

The modified access data of the administrator is stored on the SD card.

**Please note:**

Enabled user authentication only provides a limited degree of protection against unauthorized network access.

Because of its communication interfaces, the controller should not be used in safety-critical applications without additional security appliances.

- Ensure that you always operate the controller with the latest firmware version.
- Follow the security advice on unauthorized network access in [Section 1.6.4](#).

Enabling/disabling user authentication

To enable/disable user authentication, proceed as follows:

- Click on the “Enable/Disable” button next to the “User Authentication” check box.

The “Enable/Disable User Authentication” dialog opens.

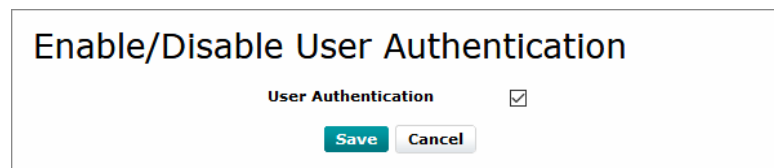


Figure 9-11 WBM: “Enable/Disable User Authentication” dialog

- To enable user authentication, enable the “User Authentication” check box.
- To disable user authentication, disable the “User Authentication” check box.
- Click the “Save” button to apply the settings.

User management

On the “User Authentication” page, the access data of all users who are authorized to access the RFC 4072S is managed and the required access permissions are assigned to each user.

The access data of all newly created users is stored on the SD card.

If the SD card is inserted into another RFC 4072S, the access data stored on the SD card is used for access to the controller.



Please note when inserting the SD card into another RFC 4072S:

If you have changed the administrator access data after logging into WBM for the first time, the modified access data stored on the SD card is used for accessing the controller. It is no longer possible to log in with the “admin” user name and the administrator password printed on the device in this case.

Adding a user

Proceed as follows to add a user:

- Click on the “Add User” button on the “User Authentication” page.

The “Add User” dialog opens.

Add User

Username

Password

Confirm Password

Figure 9-12 “Add User” dialog

- Enter the desired user name in the “Username” input field.
- Enter the desired new password in the “Password” input field.
- Re-enter the desired password in the “Confirm Password” input field.
- To add the user in the User Manager, click on the “Add” button.

Setting a password

Proceed as follows to change a user password:

- Click on the “Set Password” button in the row of the desired user on the “User Authentication” page.

The “Set User Password” dialog opens.

Set User Password

Username

New Password

Confirm Password

Figure 9-13 “Set User Password” dialog

- Enter the desired new password in the “New Password” input field.
- Re-enter the desired new password in the “Confirm Password” input field.
- To save the new password, click on the “Save” button.

Modifying user roles

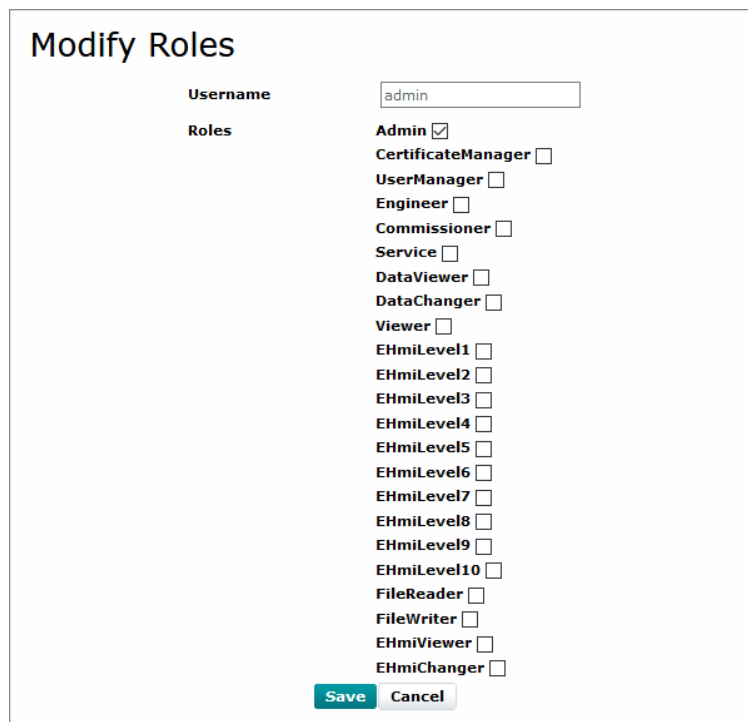
You can select one or more user roles with different permissions for each user. These permissions control access to

- The controller SD card
- PLCnext Engineer
- The PLCnext Engineer HMI
- WBM
- The RFC 4072S OPC UA server

To assign one or more user role(s) to a user, proceed as follows:

- Click on the “Modify Roles” button in the row of the desired user on the “User Authentication” page (see [Figure 9-10 on page 220](#)).

The “Modify Roles” dialog opens.



Modify Roles

Username:

Roles:

- Admin
- CertificateManager
- UserManager
- Engineer
- Commissioner
- Service
- DataViewer
- DataChanger
- Viewer
- EHmiLevel1
- EHmiLevel2
- EHmiLevel3
- EHmiLevel4
- EHmiLevel5
- EHmiLevel6
- EHmiLevel7
- EHmiLevel8
- EHmiLevel9
- EHmiLevel10
- FileReader
- FileWriter
- EHmiViewer
- EHmiChanger

Figure 9-14 “Modify Roles” dialog

- Enable the check box of the user role(s) that you would like to assign to the user.



You can open PLCnext Engineer HMI applications with or without authentication. With authentication, the user name and password are required.

Recommended:

- If you do not wish to use authentication, use an upstream firewall (e.g., in a switch) to enable access to the PLCnext Engineer HMI application only through certain devices.

Detailed information on the prepared security functions in a PLCnext Engineer HMI application as well as on using the EHmiLevelxx can be found in the online help of PLCnext Engineer.

- Click on the “Save” button to save the selected user role(s) for the user.

Table 9-1 User roles and their assigned access permissions in the various applications

Application or component of the RFC 4072S	Access permission	User role													
		Admin	CertificateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer	EHmiLevelIX	File Reader	FileWriter	EHmiViewer	EHmiChanger
SD card / parameterization memory	SFTP access to the file system with an SFTP client Please note: Authentication with a user name and password is always required for SFTP access, even when user authentication is disabled.	J													
Shell	SSH access to the shell Please note: Authentication with a user name and password is always required for SSH access, even when user authentication is disabled.	J													
PLCnext Engineer	View values in the cockpit (e.g., utilization, etc.)	J			J	J	J	J	J						
PLCnext Engineer	Transfer a project to the controller	J			J										
PLCnext Engineer	Start or stop the controller (cold/warm start)	J			J	J	J								
PLCnext Engineer	Restart the controller (reboot)	J													
PLCnext Engineer	Reset the controller to default setting type 1	J													
PLCnext Engineer	View online variable values	J			J		J	J	J						
PLCnext Engineer	Overwrite variables	J			J		J		J						
PLCnext Engineer	Set and delete breakpoints	J			J		J								

Table 9-1 User roles and their assigned access permissions in the various applications

Application or component of the RFC 4072S	Access permission	User role													
		Admin	CertificateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer	EHmiLevelIX	File Reader	FileWriter	EHmiViewer	EHmiChanger
WBM	View "General Information" page	J		J	J										
WBM	Manage users	J		J											
OPC UA client	View online variable values	J			J		J	J	J	J					
OPC UA client	Overwrite variables	J			J		J	J							
Access to PLCnext Engineer HMI application	View online variable values	J												J	
Access to PLCnext Engineer HMI application	Overwrite variables	J													J
WBM	Edit TrustStores and IdentityStores	J	J												
OPC UA client	Read files	J										J ¹			
OPC UA client	Write files	J											J ²		

¹ FileReaders can only read files as an OPC UA client if OPC UA file transfer is activated in PLCnext Engineer (see Figure 9-15).

² FileWriters can only write files as an OPC UA client if OPC UA file transfer is activated in PLCnext Engineer (see Figure 9-15).

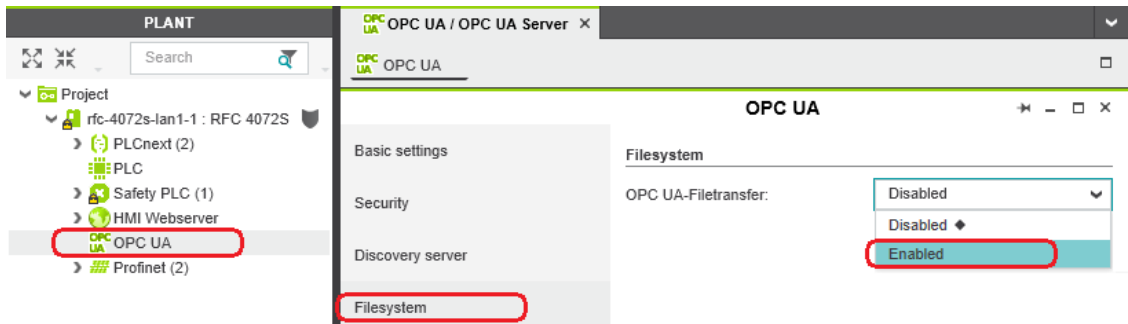


Figure 9-15 Enabling OPC UA file transfer

Removing a user

Proceed as follows to remove a user:

- On the “User Authentication” page, click the “Remove User” button in the row of the user you want to delete.

The “Remove User” dialog opens.

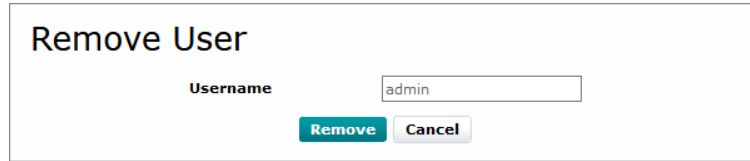


Figure 9-16 “Remove User” dialog

- Click on the “Remove” button to delete the user.

9.6.4.2 “Certificate Authentication” page



Further information on “Security - Certificate Authentication” can be found in the UM EN PLCNEXT TECHNOLOGY user manual.

“TrustStores” tab

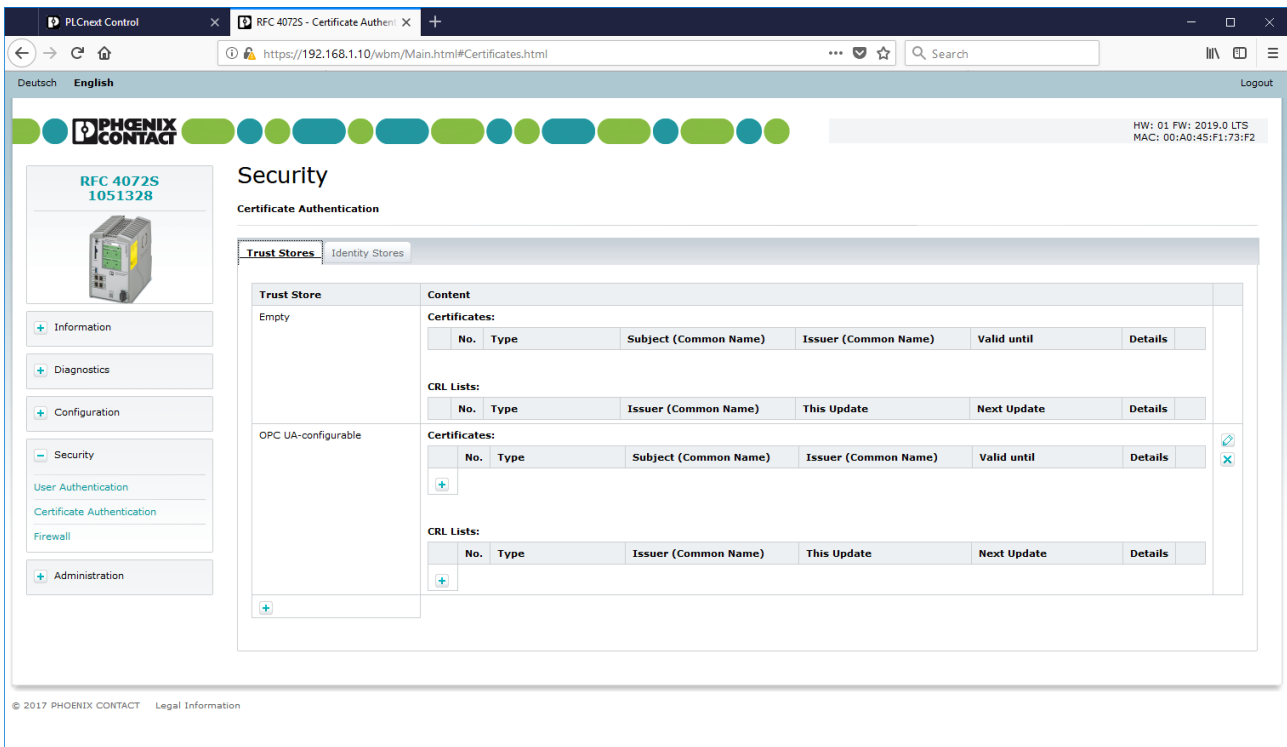


Figure 9-17 WBM: “Certificate Authentication” page – “TrustStores” tab

“IdentityStores” tab

The screenshot shows the 'IdentityStores' tab in the WBM interface. The page title is 'Security' and the sub-section is 'Certificate Authentication'. The interface includes a sidebar with navigation options like Information, Diagnostics, Configuration, Security, User Authentication, Certificate Authentication, Firewall, and Administration. The main content area displays a table of Identity Stores and their contents.

Identity Store	Content				
IDeVID	No.	Element	Type	Description	Details
IDeVID	1	Key Pair	RSA TPM 2048	RSA Key Pair	[Details] [Download]
	2	Certificate	Key Certificate	Common Name: RFC 4072S Valid not after: 9999-12-31T23:59:59 UTC	[Details] [Download]
	3	Certificate	Issuer Certificate	Common Name: PLCnext Device Signing CA Valid not after: 2018-10-17T23:59:59 UTC	[Details]
	4	Certificate	Issuer Certificate	Common Name: PhoenixSign License PLCnext Sub CA G1 Valid not after: 2024-09-06T23:59:59 UTC	[Details]
	5	Certificate	Issuer Certificate	Common Name: PhoenixSign License Root CA G1 Valid not after: 2024-09-06T23:59:59 UTC	[Details]
OPC UA-self-signed	No.	Element	Type	Description	Details
OPC UA-self-signed	1	Key Pair	RSA 2048	RSA Key Pair	[Details] [Download] [Refresh] [Delete]
	2	Certificate	Key Certificate	Common Name: eUAServer@rfc-4072s-1 Valid not after: 9999-12-31T23:59:59 UTC	[Details] [Download] [Refresh] [Delete]
+					
OPC UA-configurable	No.	Element	Type	Description	Details
OPC UA-configurable	1	Key Pair	RSA 2048	RSA Key Pair	[Details] [Download] [Refresh] [Delete]
	2	Certificate	Key Certificate	Certificate not available. Please add a Key Certificate via the "Set" button on the right.	[Details] [Refresh] [Delete]
+					

Figure 9-18 WBM: “Certificate Authentication” page – “IdentityStores” tab

9.6.4.3 “Firewall” page



Further information on “Security - Firewall” can be found in the UM EN PLCNEXT TECHNOLOGY user manual.

It contains information and possible settings for the firewall.

The screenshot displays the 'Security Firewall' configuration page in the WBM interface. The page includes a sidebar with navigation options like Information, Diagnostics, Configuration, Security, and Administration. The main content area is divided into sections: System Message, System Status (with a 'Show Rules' button), General Configuration (showing status as 'stopped'), and Basic Configuration (with sub-sections for ICMP and Basic Rules). The Basic Rules section contains a table with columns for Seq., Direction, Protocol, To Port, Comment, and Action.

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Accept
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Accept
3	Input	TCP	22	SSH	Accept
4	Input	TCP	80	HTTP	Accept
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Accept
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Accept
8	Input	TCP	161	SNMP (Simple Network Management Protocol)	Reject
9	Input	UDP	34962-34964	Profinet Uni-/Multicast Ports	Accept

Figure 9-19 WBM: “Firewall” page

9.7 Firmware update via WBM

This section describes the procedure for updating the non-safety-related firmware of the RFC 4072S via Web-based management (WBM).

- Download the *.zip firmware file at phoenixcontact.net/product/1051328.
- Unzip the *.zip firmware file.
- Run the *.exe setup file.
- Follow the instructions of the installation wizard.

During installation, the update file (*.raucb) and files containing device-specific information (such as change notes and Phoenix Contact software license terms) are copied to the selected destination directory.

- Open WBM of the RFC 4072S by entering the IP address in the web browser.
- Log onto the RFC with your user name and password. The user name and password are printed on the label attached to the side of the device (see [Figure 2-36 on page 76](#)).
- First, select “General Data” in the “Information” area (A in [Figure 9-20](#)). Take down the firmware version specified (B in [Figure 9-20](#)). You will need it for the final check after the update.

The screenshot shows the WBM interface for an RFC 4072S device. The browser address bar shows the URL <https://192.168.1.10/wbm/Main.html#GeneralData.html>. The page title is "Information" and the sub-section is "General Data". On the left, there is a navigation menu with "General Data" highlighted and labeled 'A'. The main content area displays a table of device information:

General Data	
Vendor	Phoenix Contact GmbH & Co. KG
Address	Flachmarktstr. 8, 32825 Blomberg, Germany
Internet	http://www.phoenixcontact.com
Type	RFC 4072S
Order No.	1051328
Serial No.	2034059038
Firmware Version	2019.0 LTS (19.0.0.16298)
Hardware Version	01
FPGA Version	0.1.7

The "Firmware Version" row is highlighted with a red circle and labeled 'B'. The bottom of the page shows the copyright notice: © 2017 PHOENIX CONTACT Legal Information.

Figure 9-20 WBM: Information – General Data (firmware version)

- In the “Administration” area, click on “Firmware Update” (A in [Figure 9-21](#)).

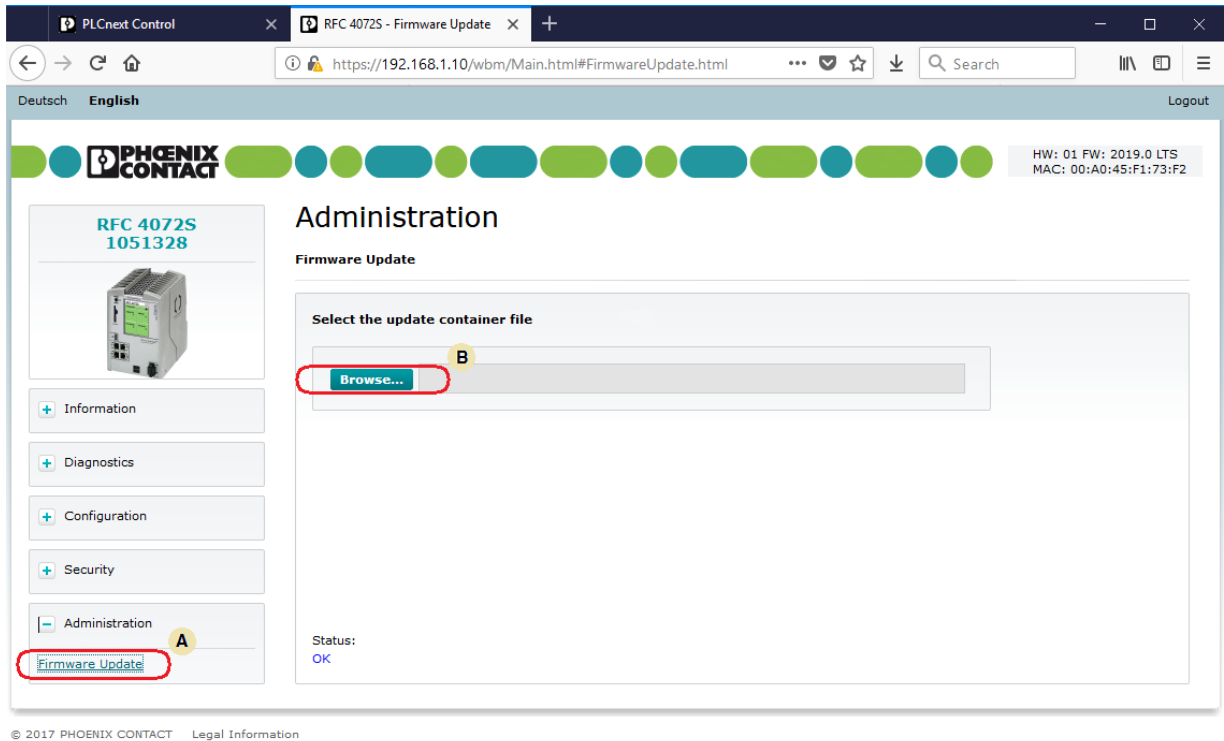


Figure 9-21 WBM: Administration – Firmware Update

- Click on the “Browse” button (B in Figure 9-21) and follow the further instructions.
- In the window that opens, select the destination directory to which you have copied the update file.
- Click on the update file (*.raucb).

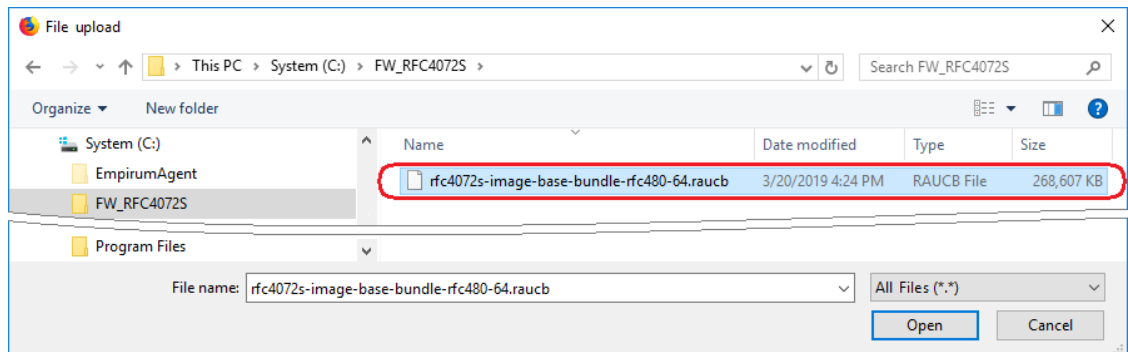


Figure 9-22 WBM: Administration – Selecting the firmware container

- Click on the “Open” button.

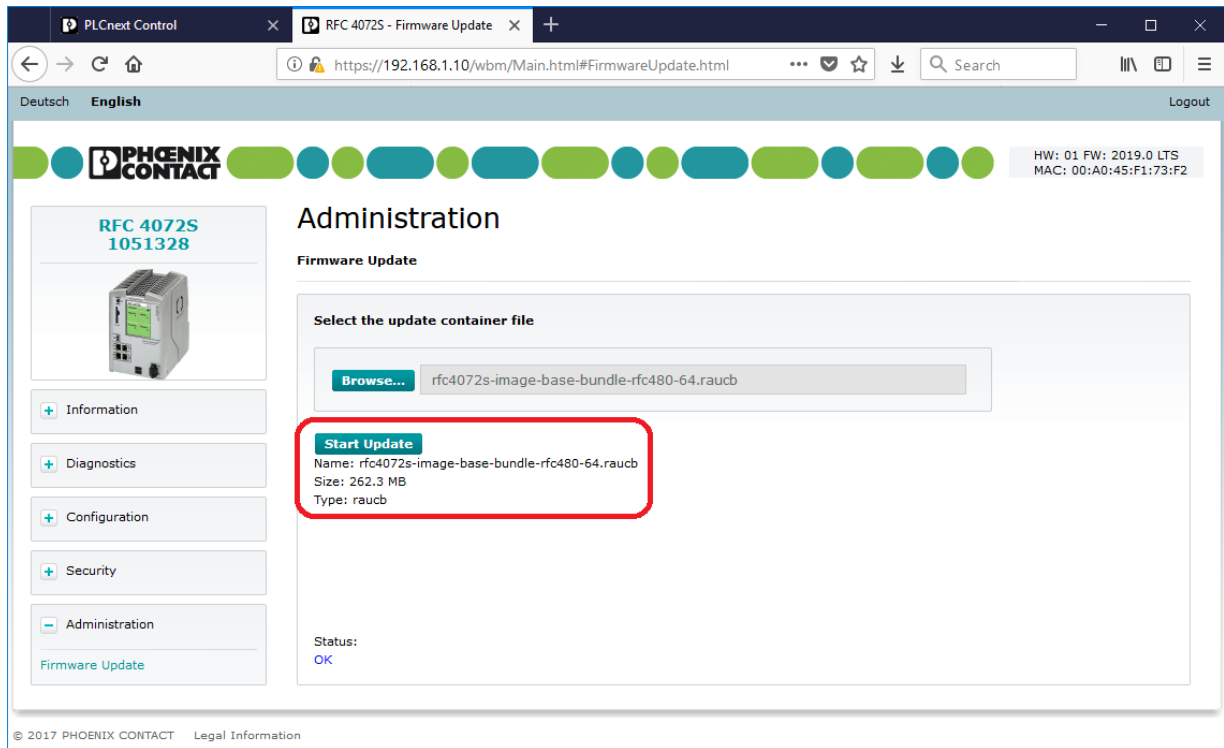


Figure 9-23 WBM: Administration – Firmware container selected – Start update

**CAUTION:**

Note that the standard controller is set to the STOP state when the update process is started. In this state, process data is not exchanged between F-Host and F-Devices in the network via PROFIsafe. The F-Devices switch to safe state (failure state) after the defined watchdog time has expired.

We recommend setting the safety-related controller and the standard controller to the STOP state before you perform the next step.

- Click on the “Start Update” button. Follow the instructions.

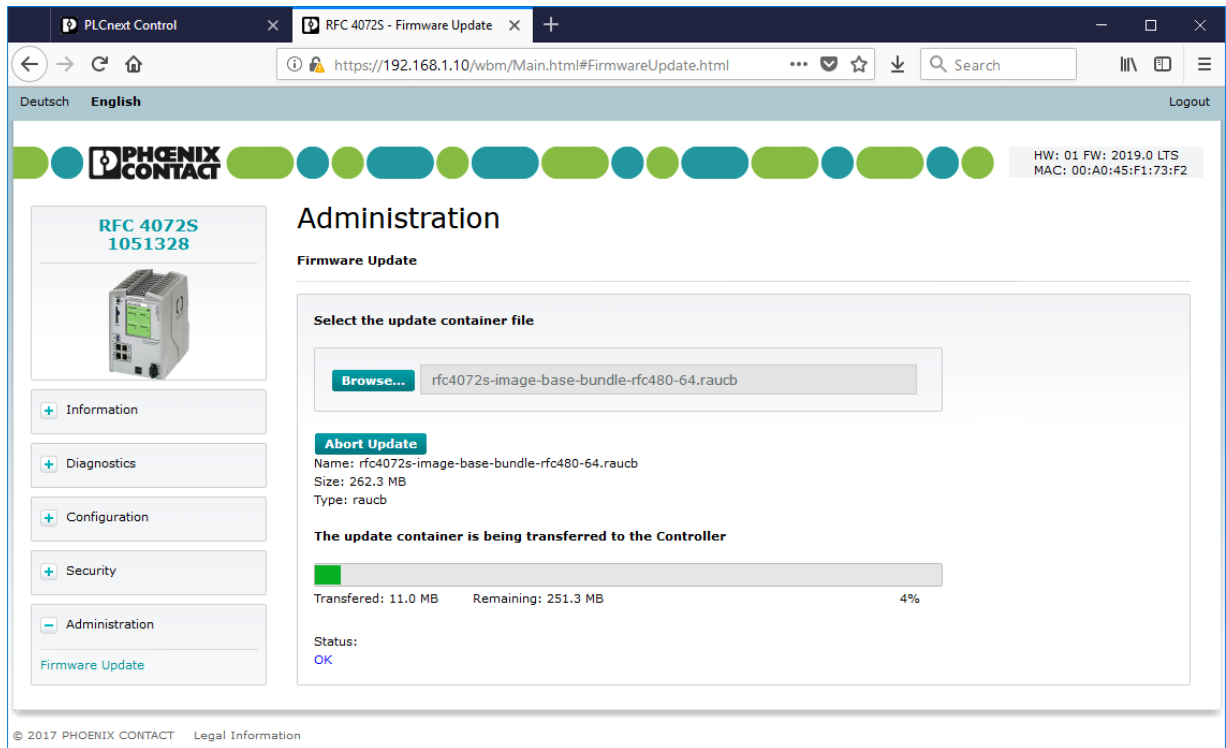


Figure 9-24 WBM: Administration – Firmware Update – Transferring the firmware container to the RFC

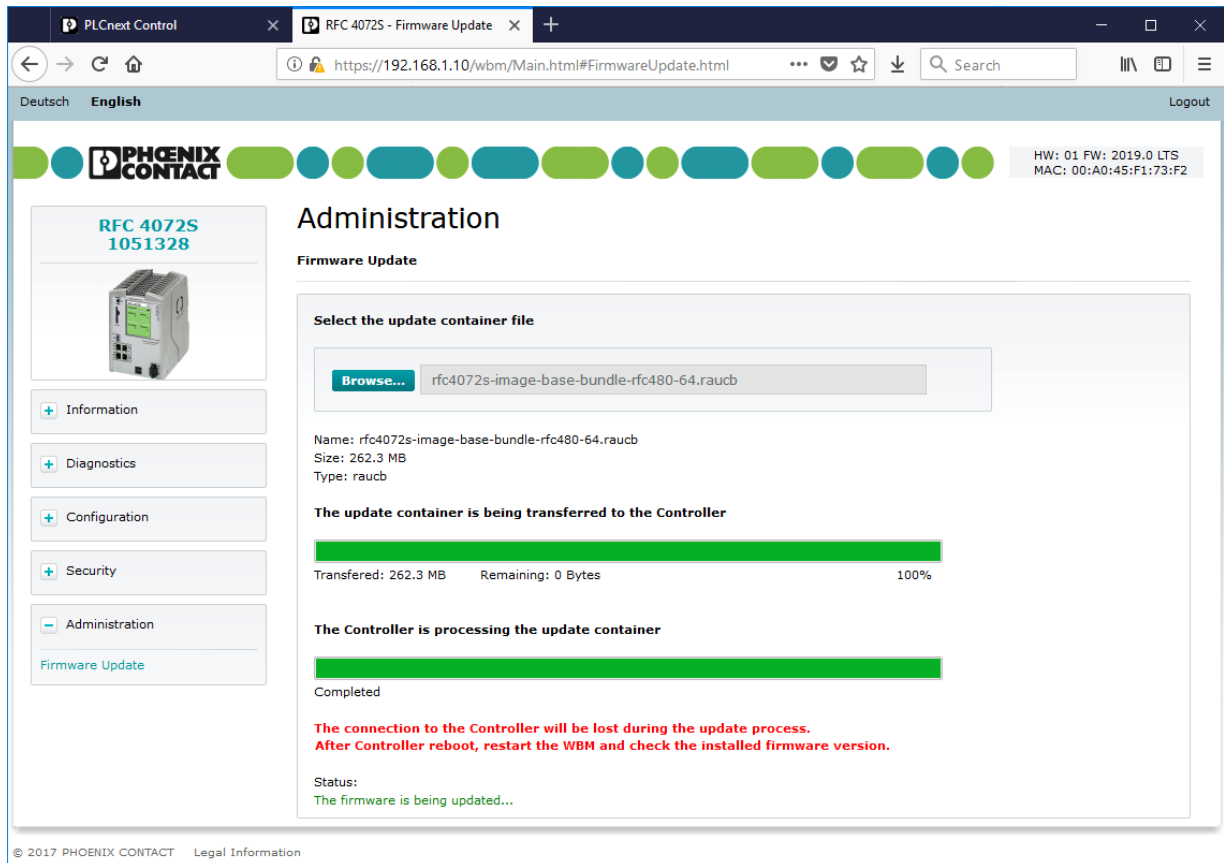


Figure 9-25 WBM: Administration – Firmware Update – Firmware is being updated

The RFC 4072S is restarted to complete the firmware update.

- Open WBM again once the device has been successfully restarted.
- Open the “General Data” in the “Information” area.
- Check whether the correct firmware version is displayed.

The screenshot shows a web browser window with the URL `https://192.168.1.10/wbm/Main.html#GeneralData.html`. The page title is 'RFC 4072S - General Data'. The interface includes a navigation menu on the left with options like 'Information', 'General Data', 'Diagnostics', 'Configuration', 'Security', and 'Administration'. The main content area displays 'Information' for 'RFC 4072S 1051328'. A table titled 'General Data' lists various device details, with the 'Firmware Version' row circled in red.

General Data	
Vendor	Phoenix Contact GmbH & Co. KG
Address	Flachsmarktstr. 8, 32825 Blomberg, Germany
Internet	http://www.phoenixcontact.com
Type	RFC 4072S
Order No.	1051328
Serial No.	2034059038
Firmware Version	2019.0 LTS (19.0.0.18169)
Hardware Version	01
FPGA Version	0.1.7

Figure 9-26 WBM: Information – Checking firmware version after firmware update

If the firmware update is unsuccessful, the following status is displayed:

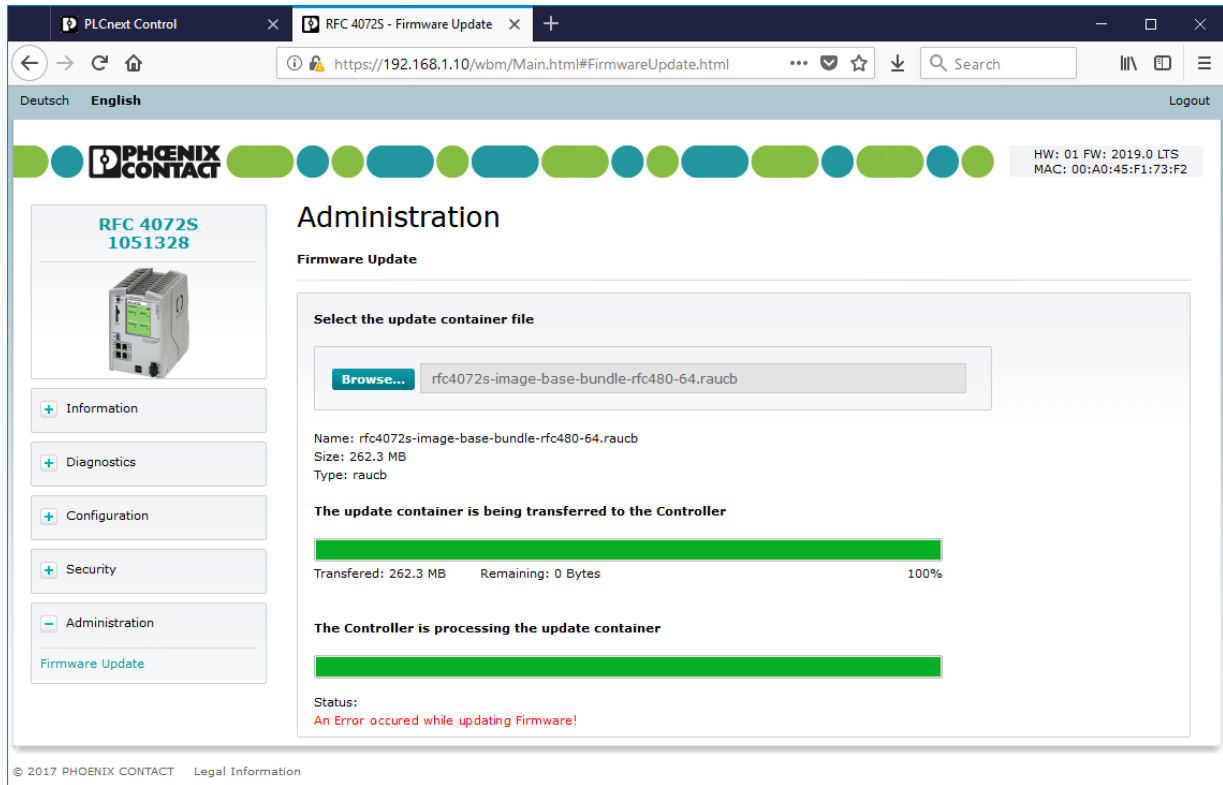


Figure 9-27 WBM: Administration – Firmware update error

10 Technical data and ordering data

10.1 Technical data

General data	
Dimensions without fan (width x height x depth)	122 mm x 182 mm x 173 mm
Dimensions with fan (width x height x depth)	122 mm x 220 mm x 173 mm
Weight without fan	2.85 kg, approximately
Weight with fan	3.08 kg, approximately
Mounting type	DIN rail (TH 35-15 according to DIN EN 60715), e.g., NS 35/15... from Phoenix Contact

Touch screen display	
Type	TFT LCD, resistive
Resolution	240 x 320 pixels
Diagonal	8.9 cm (3.5")
Operation	With the finger or a pen with a rounded end



NOTE: Damage to the display

Pointed or sharp-edged objects or tools can cause irreparable damage to the display.

Power supply



WARNING: Loss of electrical safety and the safety function when using unsuitable power supplies

The RFC 4072S is designed exclusively for protective extra-low voltage (PELV) operation in accordance with EN 60204-1. Only PELV in accordance with the listed standard may be used for the supply.

The following applies to the PROFINET network and the I/O devices used in it:

Only use power supplies that meet EN 61204 and feature safe isolation and PELV according to IEC 61010-2-201 (PELV). These prevent short circuits between primary and secondary sides.

Please also refer to the information in [Section "Electrical safety" on page 16](#).



Select the correct power supplies

Refer to the information on selecting the power supply in [Section "Electrical safety" on page 16](#).

Only use power supplies with safe isolation with 24 V DC.



Use a **power supply without fall-back characteristic curve** (see [Section "Power supply" on page 71](#)).

Power supply [...]	
Connection	Via COMBICON connector
U_S	24 V DC
Permissible range	19.2 V DC to 30.0 V DC
Ripple	3.6 V _{PP}
Power consumption	
Typical	25 W (without fan module)
Maximum	35 W (with fan module)
Protection	5 A, slow-blow, required externally
Connection data for COMBICON connectors	
Conductor cross-section (solid/stranded)	0.2 mm ² ... 2.5 mm ²
Conductor cross-section [AWG]	24 ... 12
Minimum tightening torque	0.5 Nm
Maximum tightening torque	0.6 Nm
External power supply	Only use power supplies without fall-back characteristic curve. The power supply must be suitable for operation with capacitive loads. Make sure the power supply and the fuse are compatible. The power supply must be able to temporarily provide the tripping current.

PROFINET	
Type	Modular PROFINET controller
Conformance class	B
Performance class	RT
Vendor ID	00B0 _{hex} /176 _{dec}
Device ID	014A _{hex} /330 _{dec}
Supported functions	<ul style="list-style-type: none"> – Topology detection – Automatic device replacement – Parameterizable alarm and startup behavior

Network interface	
Type	LAN1/LAN2: 2 x Ethernet, 10/100/1000Base-T LAN3.1/LAN3.2: 2 x Ethernet (internally switched), 10/100BASE-T
Transmission speed	LAN1/LAN2: 10 Mbps, 100 Mbps or 1000 Mbps LAN3.1/LAN3.2: 10 Mbps or 100 Mbps



This speed cannot be set manually. It is set automatically by means of auto negotiation.

Network interface [...]	
Connection technology	RJ45 socket; ≤ 100 Mbps: twisted pair cable according to CAT5 of IEEE 802.3 1000 Mbps: cables with four wire pairs (twisted pairs, eight wires in total) according to at least CAT5e of IEEE 802.3
Functions	<ul style="list-style-type: none"> - Half duplex or full duplex - Autocrossing - Auto negotiation - Auto polarity exchange - Line monitoring (link status)
Diagnostic and status indicators	
Ethernet	LED: LINK (green), ACTIVITY (yellow)
PROFINET	Display
IEC 61131 runtime system	Display
IEC 61131 runtime system	
Programming system	PLCnext Engineer
CPU (Central Processing Unit)	Intel® Core™ i5-6300U (Dual Core, 2.4 GHz)
Shortest cycle time (for cyclic task)	$t_{\min} = 1 \text{ ms}$
Program memory	16 Mbytes
Data storage	32 Mbytes
Memory for retentive data	2 Mbytes
Number of control tasks	32
Parameterization memory	
Integrated	100 MB flash memory
Pluggable, SD card	Size depending on the SD card used (see "Program and configuration memory" in Section "Accessories" on page 245)



Please note that the number of write access operations to the parameterization memory is limited.

Fan module (optional accessories not included in the scope of delivery of the RFC)	
Number of fans	1
Bearings	Ball bearings
Speed monitoring	Yes, through the RFC 4072S
Mounting	4 x M4 screws: Recommended tightening torque: 2.2 Nm Maximum tightening torque: 3.0 Nm
Service life	50,000 h at an ambient temperature of 25 °C



NOTE: Overheating of the RFC 4072S possible – Use the fan module

The RFC can be operated from 0 m to 2000 m above sea level at ambient temperatures up to 40 °C without a fan module. Warning messages and switching off may occur at higher ambient temperatures. For this reasons, the fan module is required for operation above ambient temperatures of 40 °C.

We recommend using the fan module at 35 °C and above to increase the service life of the RFC.

From 2000 m to 3000 m above sea level at ambient temperatures from 0 °C to 55 °C the RFC must be operated with a fan module.

From 3000 m to 4000 m above sea level at ambient temperatures from 0 °C to 50 °C the RFC must be operated with a fan module.

Ambient conditions	
Degree of protection	IP20 (EN 60529:1991) (Manufacturers declaration, not evaluated by UL.)



To ensure correct operation, the Remote Field Controller must be installed in a housing or a control cabinet with a minimum of IP54 protection.

Pollution degree	2, when installed in a housing or control cabinet with IP54 protection or higher
Air clearances and creepage distances	According to IEC 60439-1
Protection class	III, IEC 61140, EN 61140, VDE 0140-1
Ambient temperature (operation)	Without fan module: 0 °C to +40 °C (0 m to 2000 m above sea level) At temperatures of 40 °C and higher the SPNS may output a warning message. At temperatures above 45 °C, approximately, the SPNS enters the failure state. With fan module: 0 °C to +60 °C (0 m to 2000 m above sea level) 0 °C to +55 °C (2000 m to 3000 m above sea level) 0 °C to +50 °C (3000 m to 4000 m above sea level)
Ambient temperature (storage/transport)	-25 °C ... +70 °C
Permissible humidity (operation)	10% ... 95% (non-condensing)
Permissible humidity (storage/transport)	5% ... 95% (non-condensing)

Ambient conditions [...]

Air pressure (operation)	60 kPa ... 108 kPa (up to 4000 m above sea level)
Air pressure (storage/transport)	58 kPa ... 108 kPa (up to 4500 m above sea level)
Resistance to gases that may endanger functions according to DIN 40046-36, DIN 40046-37	Use of the device in these ambient conditions is prohibited.

Mechanical requirements

Vibration resistance in accordance with EN 60068-2-6/ IEC 60068-2-6	1g
Shock according to EN 60068-2-27/IEC 60068-2-27	20g
Continuous shock according to EN 60068-2-27/ IEC 60068-2-27	5g

Safety characteristic data according to EN ISO 13849

Performance level (PL)	e, maximum
Category	4, maximum
Probability of dangerous failure per hour (PFH _D)	1 * 10 ⁻⁹
Diagnostic coverage (DC _{avg})	99 %
Mean time to dangerous failure (MTTF _D)	> 80 years

Safety characteristic data according to EN 62061

Safety integrity level claim limit (SIL CL)	3, maximum
Probability of a dangerous failure per hour (PFH _D)	1 * 10 ⁻⁹
Hardware fault tolerance (HFT)	1
Duration of use (mission time)	300 months, therefore no restrictions, no maintenance intervals
Safe failure fraction (SFF) according to DIN EN 62061	99%

Safety characteristic data according to IEC 61508 – High demand

Safety Integrity Level (SIL)	3, maximum
Probability of dangerous failure per hour (PFH)	1 * 10 ⁻⁹
Hardware fault tolerance (HFT)	1
Duration of use (mission time)	300 months, therefore no restrictions, no maintenance intervals

Characteristic data of the safety-related PROFINET controller iSPNS 3000

Programming system	PLCnext Engineer, IEC 61131
CPU1 (Central Processing Unit 1)	ARM® Cortex®-A9, 800 MHz
CPU2 (Central Processing Unit 2)	ARM® Cortex™-A8, 600 MHz
Shortest cycle time $T_{ZSPNSmin}$	5 ms
Program memory	1 Mbyte (safety program)
Data storage	1 Mbyte (addressable area)
Sum of the safe input data (SI)	24576 bytes
Sum of the safe output data (SQ)	24576 bytes
Sum of the non-safety input data (NSI, inputs exchange area)	3072 bytes
Sum of the non-safety output data (NSQ, outputs exchange area)	3072 bytes
Device diagnostics input data (DI)	6144 bytes
Device diagnostics output data (DQ)	6144 bytes
Function block diagnostics output data (FBQ)	8192 bytes
Number of function block instances	16384, maximum

PROFIsafe IO

Device function	PROFIsafe F-Host, PROFIsafe F-Device
Number of supported devices	300
Profile version	V2.6MU1 / V2.4

Buffer times of the integrated realtime clock (RTC)

Typical buffer time	15 days
Guaranteed buffer time	10 days

Conformance with EMC directive 2014/30/EU

Immunity test in accordance with EN 61000-6-2

Electrostatic discharge (ESD)	EN 61000-4-2/ IEC 61000-4-2	Criterion B 6 kV contact discharge 8 kV air discharge
Electromagnetic fields	EN 61000-4-3 IEC 61000-4-3	Criterion A Field strength: 10 V/m
Fast transients (burst)	EN 61000-4-4/ IEC 61000-4-4	Criterion B Supply lines: 2 kV Signal/data lines: 2 kV
Transient overvoltages (surge)	EN 61000-4-5 IEC 61000-4-5	Criterion B Signal/data lines: 1 kV Supply lines: 0.5 kV

Conformance with EMC directive 2014/30/EU

Conducted disturbance variables

EN 61000-4-6
IEC 61000-4-6

Criterion A
Test voltage 10 V

Noise emission test according to EN 61000-6-4

Class A



NOTE: Radio interference

This is a Class A item of equipment. When using the equipment in residential areas, it may cause radio interference. In this case, the operator may be required to implement appropriate measures and to pay the resulting costs.

Approvals

For the latest information about approvals, visit phoenixcontact.net/product/1051328.

UL: Additional information



NOTE: UL Warning Instructions

- If the device is not used in the specified manner, the protection provided by the device may be impaired.
- Minimum temperature rating of the cables to be connected to the field wiring terminals: 70 °C
- The device has to be built in the final safety enclosure, which has adequate rigidity according to UL 61010-1, UL 61010-2-201 and meets the requirements with respect to spread of fire.
- Use copper conductors only.
- The external circuits intended to be connected to the device shall be galv. separated from mains supply or hazardous live voltage using reinforced or double insulation and meet the requirements of PELV circuit.

10.2 Ordering data

10.2.1 Controller

Description	Type	Order No.	Pcs./Pkt.
Remote Field Controller with integrated safety-related PROFINET controller for PROFIsafe, 4 x 10/100/1000 Ethernet interfaces, PROFINET controller, PROFINET device, IP20 protection, pluggable parameterization memory	RFC 4072S	1051328	1

10.2.2 Modules

Description	Type	Order No.	Pcs./Pkt.
Axioline F bus coupler for PROFINET	AXL F BK PN TPS	2403869	1
Axioline F bus coupler for PROFINET	AXL F BK PN	2701815	1
Axioline F module with safe digital inputs	AXL F PSDI8/4 1F	2701559	1
Axioline F module with safe digital outputs	AXL F PSDO8/3 1F	2701560	1
Axioline F digital input module, 16 inputs, high-speed, 24 V DC, 1-wire connection technology	AXL F DI16/1 HS 1H	2701722	1

10.2.3 Accessories

Description	Type	Order No.	Pcs./Pkt.
Primary-switched QUINT POWER supply for DIN rail mounting, with selectable output characteristic curve and SFB (selective fuse breaking) Technology, protective coating and integrated decoupling MOSFET, input: 1-phase, output: 24 V DC/20 A	QUINT4-PS/1AC/24DC/20/+	2904617	1
Primary-switched QUINT POWER power supply with free choice of output characteristic curve, SFB (selective fuse breaking) technology, and NFC interface, input: 1-phase, output: 24 V DC/10 A	QUINT4-PS/1AC/24DC/10	2904601	1
Primary-switched QUINT POWER power supply with free choice of output characteristic curve, SFB (selective fuse breaking) technology, and NFC interface, input: 1-phase, output: 24 V DC/5 A	QUINT4-PS/1AC/24DC/5	2904600	1
Alternatively, Phoenix Contact provides various QUINT POWER and TRIO POWER power supplies	See latest Phoenix Contact INTERFACE catalog		
Program and configuration memory for storing the application programs and other files in the file system of the PLC, pluggable, 2 GBytes	SD FLASH 2 GB PLCNEXT MEMORY	1043501	1
Program and configuration memory for storing the application programs and other files in the file system of the PLC, pluggable, 8 GBytes	SD FLASH 8 GB PLCNEXT MEMORY	1061701	1
Fan module for the RFC 4072S Remote Field Controller	RFC FAN MODULE	2404085	1
USB memory stick, 8 Gbytes	USB FLASH DRIVE	2402809	1
Gray RJ45 connector set for linear cable	FL PLUG RJ45 GR/2	2744856	2
Green RJ45 connector set for crossed cable	FL PLUG RJ45 GN/2	2744571	2
Universal end bracket (fixed using a screw)	E/NS 35 N	0800886	50
Quick mounting end bracket (snapped on without using tools)	CLIPFIX 35	3022218	50
End bracket (fixed using screws)	E/UK	1201442	50
Assembly tool for RJ45 connector	FL CRIMPTOOL	2744869	1
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT PATCH 0,3	2832250	10
Patch cable, CAT 5, pre-assembled, 0.5 m long	FL CAT PATCH 0,5	2832263	10
Patch cable, CAT 5, pre-assembled, 1.0 m long	FL CAT PATCH 1,0	2832276	10
Patch cable, CAT 5, pre-assembled, 1.5 m long	FL CAT PATCH 1,5	2832221	10
Patch cable, CAT 5, pre-assembled, 2.0 m long	FL CAT PATCH 2,0	2832289	10
Patch cable, CAT 5, pre-assembled, 3.0 m long	FL CAT PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m long	FL CAT PATCH 5,0	2832580	10
Patch cable, CAT 5, pre-assembled, 7.5 m long	FL CAT PATCH 7,5	2832616	10
Patch cable, CAT 5, pre-assembled, 10.0 m long	FL CAT PATCH 10	2832629	10

Description	Type	Order No.	Pcs./Pkt.
DIN rail, non-perforated, standard profile, width: 35 mm, height: 15 mm, similar to EN 60715, material: steel, galvanized, thick-layer passivated, length: 2000 mm, color: silver	NS 35/15 UNPERF 2000MM	1201714	5
Screwdriver, Torx®, VDE-insulated, TX 20 x 80, two-component handle	SF-TX 20X80 VDE	1200158	1

10.2.4 Software

Description	Type	Order No.	
PLCnext Engineer	See latest Phoenix Contact catalog		

10.2.5 Documentation



Make sure you always use the latest documentation.
It is available for download at phoenixcontact.net/products.

Description	Type	Order No.	Pcs./Pkt.
General safety technology			
PROFINET			
User manual PROFINET basic principles	UM EN PROFINET SYS	–	1
User manual PROFINET controller/device functions	UM EN PROFINET CTRL DEV	–	1
PROFINET Assembling Guideline, Version 2.8, September 2019, Order No.: 8.072 „PROFINET_Assembling_8072_V28_Sep19.pdf“	For the latest versions of the documents visit www.profibus.com or contact your nearest Phoenix Contact representative regarding the document		
Functional Bonding and Shielding of PROFIBUS and PROFINET, Guideline for PROFIBUS and PROFINET, Version 2.6, February 2021, Order No. 8.102 “Earthing-Shielding_8102_V26_Feb21.pdf”			

Description	Type	Order No.	Pcs./Pkt.
PROFIsafe			
PROFIsafe System Description, Technology and Application, Version April 2016, Order No. 4.342 "PROFIsafe_SystemDescription_ENG__2016_web.pdf"			
PROFIsafe Policy, Guideline for PROFIBUS and PROFINET, Version 1.5, July 2011, Order No. 2.282 "PROFIsafe-Policy_2282_V15_Jul11.pdf"			
PROFIsafe Environment related to PROFIsafe V2.6.1 Guideline for PROFINET and PROFIBUS, Version 2.6, December 2015, Order No. 2.232 "PROFIsafe-Environment_2232_V26_Dec15.pdf"			
PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET, Order No.: 3.192 Profile part, related to IEC 61784-3-3 Technical Specification, Version 2.6MU1, August 2018 „PROFIsafe_3192_V26MU1_Aug18.pdf“			
PROFIsafe Test Specification, related to PROFIsafe V2.6, Test Specification for PROFIBUS and PROFINET Version 2.3, March 2018, Order No.: 2.242 „Psafe-Testspec_2242_V23_Mar18.pdf“			
PLCnext Technology			
PLCnext Technology			
	Further information on PLCnext Technology can be found in the PLCnext Community at plcnext-community.net .		
Documentation for software			
Online help PLCnext Engineer			
Security			
Application note Measures to protect network-capable devices with communication interfaces, solutions and PC-based software against unauthorized access	AH EN INDUSTRIAL SECURITY	-	1

For the latest versions of the documents visit www.profibus.com or contact your nearest Phoenix Contact representative regarding the documents.

A Appendix:

A 1 Shell commands for controlling the firmware

The plcnext script in the /etc/init.d directory controls the controller firmware.

You can control the firmware with the following shell commands:

Table A-1 Shell commands for controlling the firmware

Shell command	Description
sudo /etc/init.d/plcnext stop	Stops all PLCnext firmware processes If all PLCnext firmware processes are stopped, you will no longer be able to access the controller from PLCnext Engineer.
sudo /etc/init.d/plcnext start	Starts all PLCnext firmware processes
sudo /etc/init.d/plcnext restart	Restarts all PLCnext firmware processes

A 2 Replacing HTTPS certificate

You have the option of replacing the HTTPS certificate used by the controller with a third-party certificate. The HTTPS certificate comprises the two files https_cert.pem and https_key.pem.

To replace the files on the controller, proceed as follows:

- Connect to the RFC via an SFTP client software package (e.g., WinSCP).
- Open the /opt/plcnext/Security/Certificates/https directory.

The two files https_cert.pem and https_key.pem are located in this directory.

- Replace the two files with the third-party certificate files.



Please note:

The third-party certificate files must have the same designation as the original files.

- If necessary, rename the third-party certificate files to https_cert.pem and https_key.pem.

A 3 Interfaces of the RFC 4072S

The following figure shows the interfaces of the RFC 4072S. Contact assignment of the individual interfaces is described in the sections that follow. For notes on connecting these interfaces, please refer to [Section "Mounting, removal, electrical installation, and replacement" on page 77](#).

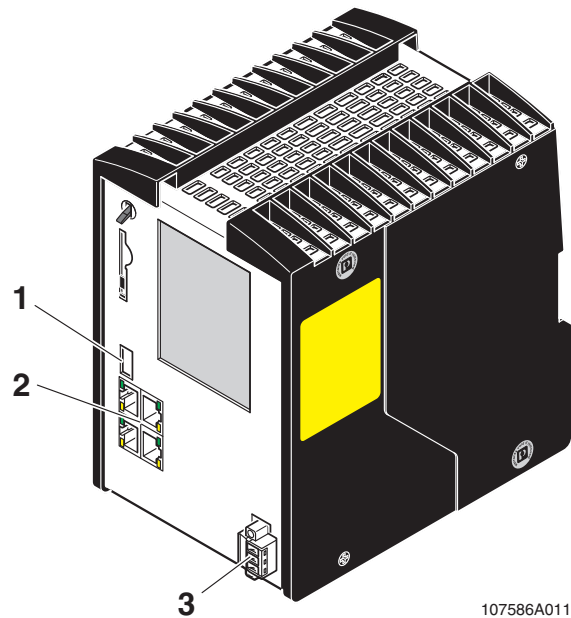


Figure A-1 Interfaces of the RFC 4072S

- 1 USB interface (type A USB socket)
- 2 Ethernet interfaces (RJ45 sockets)
LAN1 and LAN2: 10/100/1000 Mbps;
LAN3.1 and LAN3.2 (switched internally): 10/100 Mbps
- 3 Supply voltage

A 4 USB interface

You can connect a USB memory stick to this interface.

We recommend using the USB memory stick:

USB FLASH DRIVE (Order No. 2402809), USB memory stick, 8 Gbytes

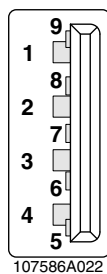


Figure A-2 Contact assignment of the USB 3.0 interface (type A)

Table A-2 Contact assignment of the USB 3.0 interface (type A)

Pin	Signal	Description
1	VCC	5 V DC
2	D-	Data-
3	D+	Data+
4	GND	Ground
5	SSRX-	Super-speed receive data-
6	SSRX+	Super-speed receive data+
7	GND	Ground
8	SSTX-	Super-speed transmit data-
9	SSTX+	Super-speed transmit data+

A 5 Ethernet interfaces

The RFC 4072S has four Ethernet interface. Interfaces LAN1 and LAN 2 are also designed for Gigabit Ethernet. Interfaces LAN3.1 and LAN3.2 are switched device-internally and do not support Gigabit Ethernet.



Use Ethernet cables according to CAT5 of IEEE 802.3 for operation with up to 100 Mbps. Please note that for operation with 1000 Mbps (Gigabit), cables with four wire pairs (twisted pairs, eight wires in total), which at least meet the requirements of CAT5e, must be used.

When working on PROFINET/PROFIsafe and its components, the following documents must always be available and observed at all times.

- PROFINET Installation Guideline for Cabling and Assembly
- PROFIsafe System Description
- PROFIBUS Guideline, PROFIsafe Policy
- PROFIsafe – Environmental Requirements Guideline

These documents are available on the Internet at www.profinet.com or you can contact your local Phoenix Contact representative regarding these documents (see also [Section “Documentation” on page 246](#)).

Please also observe the relevant information on PROFINET and PROFIsafe, which is available on the Internet at www.profisafe.net.

- Connect the lower-level PROFIsafe system to the LAN1 or LAN2 RJ45 socket depending on the configuration.
- Connect the higher-level PROFINET network to the LAN1, LAN2 or LAN3 RJ45 socket depending on the configuration.

The following figure shows the contact assignment of an Ethernet interface (RJ45 socket).

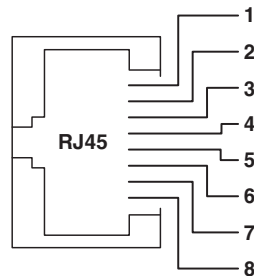


Figure A-3 Contact assignment of an Ethernet interface in RJ45 format

Table A-3 Contact assignment of the Ethernet interfaces depending on the transmission speed.

PIN	LAN1, LAN2, LAN3.1/LAN3.2:		LAN1, LAN2:
	10Base-T (10 Mbps)	100Base-T (100 Mbps)	1000Base-T (1000 Mbps)
1	TD+ (Transmit data+)	TD+ (Transmit data+)	DA+ (Bidirectional)
2	TD- (Transmit data-)	TD- (Transmit data-)	DA- (Bidirectional)
3	RD+ (Receive data+)	RD+ (Receive data+)	DB+ (Bidirectional)
4	Reserved	Reserved	DC+ (Bidirectional)
5	Reserved	Reserved	DC- (Bidirectional)
6	RD- (Receive data-)	RD- (Receive data-)	DB- (Bidirectional)
7	Reserved	Reserved	DD+ (Bidirectional)
8	Reserved	Reserved	DD- (Bidirectional)

A 6 Connection for the supply voltage

The Remote Field Controller is supplied from an external power supply (24.0 V DC). The permissible voltage ranges from 19.2 V DC to 30.0 V DC (ripple included).

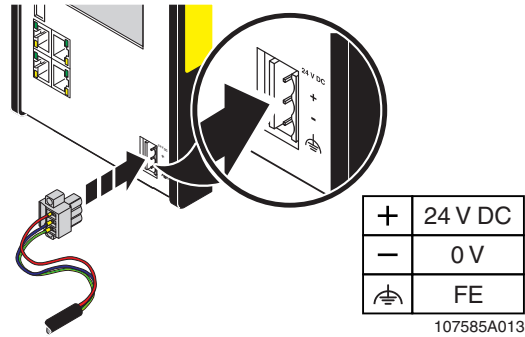


Figure A-4 Connecting the supply voltage

- Connect the “+” terminal to the positive pole of the power supply.
- Connect the “-” terminal to 0 V.
- Connect the “FE” terminal to functional ground.
- Use the retaining screws to secure the COMBICON connector in place.
- Observe additional data on the supply voltage in [Section “Technical data” on page 237](#).

B Appendix: terms for PROFIsafe

Terms that are used in connection with PROFIsafe in this user manual are described below. A definition of PROFIsafe terms is also provided in the PROFIsafe profile.

CRC	Cyclic Redundancy Check										
	A cyclic redundancy check is used to verify the validity of the process data contained in the safety telegram, check whether the assigned address relationships are correct, and verify the safety-related parameters. This value is part of the safety telegram.										
Consecutive number	Consecutive number										
	Method for ensuring that the safe data is transmitted completely and in the correct order.										
Reintegration	Removal of passivation for the reintegration of previously passivated F-Devices (see also "Passivation").										
F-Parameters	(According to PROFIsafe System Description, version of April 2016)										
	F-Parameters contain information for adapting the PROFIsafe layer to specific customer specifications and for checking the parameterization by means of a separate method (diverse). The main F-Parameters are:										
	<table> <tr> <td>F_Source_Address / F_Destination_Address / F_Source_Add / F_Dest_Add (F-address for short)</td> <td> <p>Unique address for F-Devices within a PROFIsafe island. The technology part of the F-Device compares the value with the local address switch or with an assigned F-Address in order to check authenticity of the connection.</p> <p>As of PROFIsafe profile V2.6.1, a distinction is made between two address types, which must be specified by the manufacturer in the F-Device-specific user documentation:</p> <p>Address type 1: The F-Device only checks the F_Destination_Address.</p> <p>Address type 2: The F-Device checks the F_Destination_Address and the F_Source_Address.</p> </td> </tr> <tr> <td>F_WD_Time</td> <td>Specifies the time for the watchdog timer in milliseconds. The timer monitors the time that elapses until the next valid PROFIsafe message is received.</td> </tr> <tr> <td>F_SIL</td> <td>Indicates the SIL that the user can expect from the relevant F-Device. It is compared with the manufacturer's specification that is stored locally.</td> </tr> <tr> <td>F_iPar_CRC</td> <td>Checksum that is calculated from all iParameters of the technology-specific part of the F-Device.</td> </tr> <tr> <td>F_Par_CRC</td> <td>CRC signature that is created across all F-Parameters and ensures error-free transmission of the F-Parameters.</td> </tr> </table>	F_Source_Address / F_Destination_Address / F_Source_Add / F_Dest_Add (F-address for short)	<p>Unique address for F-Devices within a PROFIsafe island. The technology part of the F-Device compares the value with the local address switch or with an assigned F-Address in order to check authenticity of the connection.</p> <p>As of PROFIsafe profile V2.6.1, a distinction is made between two address types, which must be specified by the manufacturer in the F-Device-specific user documentation:</p> <p>Address type 1: The F-Device only checks the F_Destination_Address.</p> <p>Address type 2: The F-Device checks the F_Destination_Address and the F_Source_Address.</p>	F_WD_Time	Specifies the time for the watchdog timer in milliseconds. The timer monitors the time that elapses until the next valid PROFIsafe message is received.	F_SIL	Indicates the SIL that the user can expect from the relevant F-Device. It is compared with the manufacturer's specification that is stored locally.	F_iPar_CRC	Checksum that is calculated from all iParameters of the technology-specific part of the F-Device.	F_Par_CRC	CRC signature that is created across all F-Parameters and ensures error-free transmission of the F-Parameters.
F_Source_Address / F_Destination_Address / F_Source_Add / F_Dest_Add (F-address for short)	<p>Unique address for F-Devices within a PROFIsafe island. The technology part of the F-Device compares the value with the local address switch or with an assigned F-Address in order to check authenticity of the connection.</p> <p>As of PROFIsafe profile V2.6.1, a distinction is made between two address types, which must be specified by the manufacturer in the F-Device-specific user documentation:</p> <p>Address type 1: The F-Device only checks the F_Destination_Address.</p> <p>Address type 2: The F-Device checks the F_Destination_Address and the F_Source_Address.</p>										
F_WD_Time	Specifies the time for the watchdog timer in milliseconds. The timer monitors the time that elapses until the next valid PROFIsafe message is received.										
F_SIL	Indicates the SIL that the user can expect from the relevant F-Device. It is compared with the manufacturer's specification that is stored locally.										
F_iPar_CRC	Checksum that is calculated from all iParameters of the technology-specific part of the F-Device.										
F_Par_CRC	CRC signature that is created across all F-Parameters and ensures error-free transmission of the F-Parameters.										

F_Source_Address	F-Parameter (F_Source_Add for short); PROFIsafe source address, address of the safety-related SPNS PROFINET controller (F-Host)
F_Destination_Address	F-Parameter (F_Dest_Add for short); PROFIsafe destination address; address of the PROFIsafe device (F-Device)
iParameters	Individual safety parameters of a device
Consecutive number	See “Consecutive number”
Passivation	<p>If the safety module detects an error, it switches the affected channel or all channels of the module to the safe state; the channels are then passivated. The detected errors are reported to the safety-related controller.</p> <p>For a safe input module, when passivation is enabled, substitute values (0) are provided for the safety program instead of the process values present at the safe inputs.</p> <p>For a safe output module, when passivation is enabled, substitute values (0) are transferred to the safe outputs instead of the output values provided by the safety program.</p>
PROFIsafe	Safety-related bus profile based on PROFIBUS DP or PROFINET. It defines the communication between a safety program and the safe I/O devices in a safe system.
PROFIsafe address	Each safe module has a PROFIsafe address. This address must be set on the safety module via DIP switches, for example, and then configured in the configuration tool for the safety-related controller used.
PROFIsafe monitoring time	<p>Monitoring time for safety-related communication between the iSPNS 3000 and the safe I/O devices.</p> <p>This time is parameterized in the F_WD_Time F-Parameter.</p>

C Appendix: checklists



NOTE: Observe supporting checklists

The checklists listed in this section provide support during planning, assembly and electrical installation, startup, parameterization, and validation of the RFC 4072S and the PROFIsafe system.



These checklists may be used as additional planning documentation and/or as additional verification to ensure the steps in the specified phase are carried out carefully.

The checklists do not claim to be complete.

Observe the applicable standards for your application and, based on these, create individual specific checklists for your system/machine.

Archive the completed checklists to use as reference for recurring tests.

The checklists do not replace validation, initial startup, as well as regular testing performed by qualified personnel.

The following section of a checklist shows an example of a filled in checklist.

Checklist . . .			
Device type / equipment identification		RFC 4072S / BK15NA11	
Version:		Date	2019-02-18
HW/FW	≥ 00/2019.0 LTS		
HW/FW (iSPNS 3000)	≥ 02/01.08.0000		
Editor	John Smith	Test engineer	Jane Brown
Comment	System XXX has been checked for engine hood production		
No.	Requirement	Yes	Comment
X	...	<input type="checkbox"/>	

Key:

Device type / equipment identification Enter the device type and/or the equipment identification for the relevant device.

Version: Enter the hardware and firmware version as well as firmware and iSPNS 3000 hardware and firmware versions of the device (see revision specification on the label, item 9 in [Figure 2-13 on page 46](#)).

HW/FW

HW/FW (iSPNS 3000)

Date

Enter the date on which you began to fill in this checklist.

Editor

Enter the name of the editor.

Test engineer

Enter the name of the test engineer.

Comment

Where necessary, enter a comment.

Requirement (mandatory)

These requirements must be met for a safety application, in order to complete the relevant phase using the checklist.

Requirement (optional)

These requirements are optional. For points that are not met (No), please enter an appropriate remark in the relevant field.

C 1 System-specific checklists

This section contains checklists that relate to the phases of life of the PROFIsafe system.

C 1.1 Planning

Checklist for planning the use of the PROFIsafe system			
Equipment identification			
		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Have the applicable standards for the system/machine been selected and are the resulting requirements known for each safety function and phase of life of the system/machine?	<input type="checkbox"/>	
2	Has risk assessment for the system/machine been carried out?	<input type="checkbox"/>	
3	Has the corresponding safety category/safety integrity level been derived from risk assessment?	<input type="checkbox"/>	
4	Have the individual safety functions been fully defined/specified?	<input type="checkbox"/>	
5	Does the planned PROFIsafe system meet the required safety integrity for all defined safety functions?	<input type="checkbox"/>	
6	Has the power supply been planned according to the specifications for protective extra-low voltage according to PELV according to EN 60204-1 (including safe isolation with PELV voltage according to IEC 61010-2-201)?	<input type="checkbox"/>	
7	Has the maximum permissible response time (SFRT) for each individual safety function within the PROFIsafe system in your system/machine been determined and documented?	<input type="checkbox"/>	
8	Can the planned system/machine be implemented when the determined SFRT is observed with the specified PROFINET infrastructure?	<input type="checkbox"/>	
9	Can the planned application be implemented with the programming options (e.g., by using function blocks) and has a specification been created for the safety-related application program?	<input type="checkbox"/>	
10	Have the user rights for the safety-related application program been defined in the PLCnext Engineer software?	<input type="checkbox"/>	
11	Has a project password been provided?	<input type="checkbox"/>	
12	Who is authorized to “develop” the safety-related application program?	<input type="checkbox"/>	Names:
13	Has a controller password been provided?	<input type="checkbox"/>	
14	Were the settings for user authentication defined in the RFC 4072S web-based management?	<input type="checkbox"/>	Names:
15	Has the location where the software is to be installed (e.g., on the system PC) been specified?	<input type="checkbox"/>	


System-specific checklists

No.	Requirement	Yes	Comment
16	Are measures planned which prevent unintentional, automatic restart with hazardous states?	<input type="checkbox"/>	
17	Are measures planned to ensure unique F-Addresses throughout the network (F-Source Addresses of PROFIsafe devices and F-Destination Addresses of safety-related PROFINET controllers (iSPNS 3000))?	<input type="checkbox"/>	
18	Does the planned use correspond to the intended use of the system?	<input type="checkbox"/>	
19	Has the technical data of the PROFIsafe system been observed?	<input type="checkbox"/>	
20	Have the requirements of the PROFINET Installation Guideline for Cabling and Assembly been observed and met during planning?	<input type="checkbox"/>	
21	Have the accessories to be used been planned (e.g., cables, connectors)?	<input type="checkbox"/>	
22	Are the period of use / proof test intervals and maintenance intervals of the PROFIsafe devices used known and documented?	<input type="checkbox"/>	
23	Is the assignment of responsibility for subsequent phases of life specified (e.g., for assembly/installation/programming/startup/validation, etc.)?	<input type="checkbox"/>	Name/company:
24	Are measures planned against unauthorized network access?	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

C 1.2 Programming

Checklist for programming the PROFIsafe system			
Equipment identification			
		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	
1	Have the requirements from the applicable standards for the system/machine been observed and met in the programming phase?	<input type="checkbox"/>	
2	Have the user rights for the safety-related application program been defined in PLCnext Engineer?	<input type="checkbox"/>	
3	Has the complete safety-related application program been created in PLCnext Engineer?	<input type="checkbox"/>	
4	Have additional application-specific programming guidelines been created and observed within the program specification for the planning phase?	<input type="checkbox"/>	
5	Are standard input signals exclusively used to program standard operations (e.g., for the enable principle using the EN_OUT block or for acknowledgment)?	<input type="checkbox"/>	
6	Are the parameterized F-Addresses (F-Source Addresses of PROFIsafe controllers and F-Destination Addresses of PROFIsafe devices) unique throughout the network?	<input type="checkbox"/>	
7	Is the F_WD_Time calculated for each PROFIsafe device parameterized in the "Safety Parameters" editor in PLCnext Engineer?	<input type="checkbox"/>	
8	Has a project password been defined?	<input type="checkbox"/>	
9	Who is authorized to "develop" the safety-related application program?	<input type="checkbox"/>	Names:
10	Has a controller password been defined?	<input type="checkbox"/>	
11	Has project information been entered in the "Description" field in the "Properties" editor in the "Project" editor group?	<input type="checkbox"/>	Type: Location:
12	Are possible reciprocal effects due to exchange variables between the programming of the standard controller and the iSPNS 3000 in the RFC 4072S taken into consideration and clear?	<input type="checkbox"/>	
13	Has the following been observed when programming/configuring your safety logic? <ul style="list-style-type: none"> - Switching from the safe state (substitute value = 0) to the operating state can generate an edge change (zero/one edge). - In the safety logic, take measures to prevent this edge change resulting in unexpected machine/system startup or restart. 	<input type="checkbox"/> <input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

C 1.3 Startup

Checklist for starting up the PROFIsafe system			
Equipment identification			
		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Have the requirements from the applicable standards for the system/machine been observed and met in the startup phase?	<input type="checkbox"/>	
2	Is safety ensured during the startup phase by means of additional measures and if so what are these measures (see also No. 1)? 1 _____ <input type="checkbox"/> 2 _____ <input type="checkbox"/> 3 _____ <input type="checkbox"/> 4 _____ <input type="checkbox"/> 5 _____ <input type="checkbox"/> 6 _____ <input type="checkbox"/> 7 _____ <input type="checkbox"/> 8 _____ <input type="checkbox"/> 9 _____ <input type="checkbox"/> 10 _____ <input type="checkbox"/> Additional requirements in: _____ <input type="checkbox"/>		
3	Are adjustments to the $F_WD_Time_{min}$ required in order to ensure ruggedness of the system and system availability, since the actual iSPNS 3000 cycle time may deviate from the iSPNS 3000 cycle time estimated during the planning phase?  NOTE: Do not exceed $F_WD_Time_{max}$ The set F_WD_Time must not exceed the $F_WD_Time_{max}$ from the defined SFRT. (See also "Validation" checklist)	<input type="checkbox"/>	
4	Are measures implemented against unauthorized network access?	<input type="checkbox"/>	
5	Are specifications for the startup phase applicable and have they been met?	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

C 1.4 Validation

Checklist for validating the PROFIsafe system			
Equipment identification			
		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Have the requirements from the applicable standards for the system/machine been observed and met for validation?	<input type="checkbox"/>	
2	Have the requirements from the previous planning, programming, and startup phases been met?	<input type="checkbox"/>	
3	Has validation of the PROFIsafe devices used been carried out and are the results available?	<input type="checkbox"/>	
4	Have safety distances to be observed been calculated and checked according to the implemented response and delay times (response times, SFRT, F_WD_Time _{max})?	<input type="checkbox"/>	
5	Have all the safety functions been checked successfully?	<input type="checkbox"/>	
6	Does the CRC checksum displayed in the "Project" view in the "Project" editor group in the "Safety Information" editor match the CRC checksum displayed on the RFC ("S-PLC DETAILS, S-PLC DIAGNOSTICS" sub-menu)? Alternatively, both checksums can be checked in the "Overview" view in the "Safety PLC" editor group in the "Safety Cockpit" editor. If you are connected online to the safety-related controller, the checksums are displayed under "Safety PLC project information" and under "Engineering project information".	<input type="checkbox"/>	
7	Have measures against unauthorized network access been implemented and checked?	<input type="checkbox"/>	

System-specific checklists

8	Are the directives and standards used listed in the declaration of conformity?	<input type="checkbox"/>	
9	Have the programs created in PLCnext Engineer been archived as zip files? Enter the archiving location (e.g., drive or cabinet) in the "Comment" column.	<input type="checkbox"/>	
10	Has a complete printout of the safety-related application program programmed in PLCnext Engineer been stored in the system?	<input type="checkbox"/>	
11	Have all fully filled in checklists been stored in the system?	<input type="checkbox"/>	
12	Completion of validation Has the latest program version (including the "project information") been downloaded to the safety-related PROFINET controller on automatic startup?	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

C 2 Device-specific checklists

This section contains checklists that relate to the phases of life of the RFC 4072S.

C 2.1 Planning

Checklist for planning the use of the RFC 4072S			
Device type / equipment identification			
Version: HW/FW HW/FW (iSPNS 3000)		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Has the systematic "Planning" checklist been observed?	<input type="checkbox"/>	
2	Are all measures that are based on applicable standards and the PROFINET Installation Guideline for Cabling and Assembly planned?	<input type="checkbox"/>	
3	Has the current RFC 4072S user manual been used as the basis for planning?	<input type="checkbox"/>	
4	Has the power supply for the device and direct I/Os been planned according to the specifications for protective extra-low voltage in accordance with PELV according to EN 60204-1 (including safe isolation with PELV voltage according to IEC 61010-2-201)?	<input type="checkbox"/>	
5	Are measures planned to prevent simple tampering? If so, what are they? 1 _____ 2 _____ 3 _____ 4 _____ 5 _____	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
6	Does the planned use correspond to the intended use?	<input type="checkbox"/>	
7	Have the ambient conditions according to the technical data been observed?	<input type="checkbox"/>	
8	Has the degree of protection been observed?	<input type="checkbox"/>	
9	Have the accessories to be used been planned according to the ordering data in this user manual (cables, connectors, fiber optic adapters)?	<input type="checkbox"/>	
10	Have specifications for assembly and electrical installation been defined (e.g., EPLAN) and communicated to the relevant personnel?	<input type="checkbox"/>	
11	Have specifications for parameterization been defined and communicated to the relevant personnel?	<input type="checkbox"/>	
12	Have specifications for startup been defined and communicated to the relevant personnel?	<input type="checkbox"/>	
13	Has the technical data of the interfaces been observed?	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)


C 2.2 Assembly and electrical installation

Checklist for assembly and electrical installation of the RFC 4072S			
Device type / equipment identification			
Version: HW/FW HW/FW (iSPNS 3000)		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Has assembly and electrical installation been carried out according to the specifications of the planning phase?	<input type="checkbox"/>	
2	Has assembly and electrical installation been carried out according to the specifications in the user manual for the RFC 4072S?	<input type="checkbox"/>	
3	Has assembly and electrical installation been carried out according to the specifications of the applicable standards and the PROFINET Installation Guideline for Cabling and Assembly?	<input type="checkbox"/>	
4	Has the power supply for the device and direct I/Os been installed according to the specifications for protective extra-low voltage in accordance with PELV according to EN 60204-1 (including safe isolation with PELV voltage according to IEC 61010-2-201)?	<input type="checkbox"/>	
5	Have measures been taken to prevent simple tampering (e.g., control cabinet can be locked, PLCnext Engineer access rights, etc.)? If so, what are they?		
	1 _____	<input type="checkbox"/>	
	2 _____	<input type="checkbox"/>	
	3 _____	<input type="checkbox"/>	
	4 _____	<input type="checkbox"/>	
	5 _____	<input type="checkbox"/>	
	6 _____	<input type="checkbox"/>	
	7 _____	<input type="checkbox"/>	
	8 _____	<input type="checkbox"/>	
	9 _____	<input type="checkbox"/>	
	10 _____	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

C 2.3 Startup and parameterization



Refer to the online help for the PLCnext Engineer software.

Checklist for startup and parameterization of the RFC 4072S			
Device type / equipment identification			
Version: HW/FW HW/FW (iSPNS 3000)		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Have the systematic "Programming" and "Startup" checklists been observed?	<input type="checkbox"/>	
2	Was startup completed according to the specifications (specifications from the planning phase and/or according to the RFC 4072S user manual, see Table 4-1 "Steps for initial startup of the RFC 4072S")?	<input type="checkbox"/>	
3	Is it ensured that when the supply voltage of the RFC 4072S is switched on, automatic startup does not cause a hazardous movement on the machine/system?	<input type="checkbox"/>	
	 <div style="border: 1px solid black; padding: 5px; display: inline-block;"> <p>WARNING: Preventing automatic startup Take appropriate measures to ensure that automatic startup of your system/machine is prevented.</p> </div>		
		Date	Signature (editor)
		Date	Signature (test engineer)

C 2.4 “Initial startup” and “restart/device replacement” validation

Carry out a validation every time you make a safety-related modification to the PROFIsafe system.



In addition, refer to the online help for the PLCnext Engineer software.

Checklist for validation on initial startup or restart/device replacement of the RFC 4072S			
Device type / equipment identification			
Version: HW/FW HW/FW (iSPNS 3000)		Date	
Editor		Test engineer	
Comment			
No.	Requirement	Yes	Comment
1	Has the systematic “Validation” checklist been observed?	<input type="checkbox"/>	
2	Have all the requirements of the “Planning” checklist been met?	<input type="checkbox"/>	
3	Have all the requirements of the “Assembly and electrical installation” checklist been met?	<input type="checkbox"/>	
4	Have all the requirements of the “Startup and parameterization” checklist been met?	<input type="checkbox"/>	
5			
5a	Initial startup: Has a function test been performed to check all the safety functions in which the RFC 4072S is involved?	<input type="checkbox"/>	
5b	Restart after replacing the RFC 4072S: The CRC checksum of the PLCnext Engineer project corresponds to the version validated and documented for the machine/system under 5a.	<input type="checkbox"/>	
6	Does the power supply for the device and direct I/Os meet the specifications for protective extra-low voltage in accordance with PELV according to EN 60204-1 (including safe isolation with PELV voltage according to IEC 61010-2-201)?	<input type="checkbox"/>	
7	Do all cables correspond to the specifications?	<input type="checkbox"/>	
8	Wiring check: Have all the inputs and outputs of all PROFIsafe devices physically present in the network and configured in PLCnext Engineer been properly wired?	<input type="checkbox"/>	
9	Have measures been taken to prevent simple tampering?	<input type="checkbox"/>	
		Date	Signature (editor)
		Date	Signature (test engineer)

D Appendix for document lists

D 1 List of figures

Section 2

Figure 2-1:	PROFIsafe: management-/diagnostic variables for communication diagnostics	29
Figure 2-2:	PROFIsafe: Management/diagnostic variables for communication diagnostics of the iSPNS 3000 F-Device	31
Figure 2-3:	Data exchange between the F-Device of the iSPNS 3000 and the higher-level F-Host	32
Figure 2-4:	F-Address of the iSPNS 3000 F-Device in PLCnext Engineer: F_Dest_Add (F_Destination_Address)	33
Figure 2-5:	F-Addresses of the F-Host (SPLC 3000) and F-Device (iSPNS 3000)	33
Figure 2-6:	Calculation of the SFRT response time (*) = Not necessarily the output device	36
Figure 2-7:	Simplified calculation of the SFRT response time (*) = Not necessarily the output device	37
Figure 2-8:	F_WD_Time (minimum)	39
Figure 2-9:	“Settings” editor of the interface editor group of the PROFINET device (settings of the AXL F BK PN or AXL F BK PN TPS PROFINET bus coupler)	40
Figure 2-10:	Cycle time of the iSPNS 3000 T _{ZSPNS}	41
Figure 2-11:	RFC 4072S display: cycle and program runtime of the iSPNS 3000 (B)	42
Figure 2-12:	PLCnext Engineer: “Safety Cockpit” editor in the editor group of the “Safety PLC”	42
Figure 2-13:	Structure of the RFC 4072S Remote Field Controller including fan module	46
Figure 2-14:	Security seal and test mark	47
Figure 2-15:	RFC with fan module	48
Figure 2-16:	LNK and ACT LEDs	49
Figure 2-17:	Display of the RFC	50
Figure 2-18:	Structure of the display	51
Figure 2-19:	Display: indicators in the home menu	52
Figure 2-20:	Diagnostic indicators in the home menu (LEDs)	56
Figure 2-21:	Home menu	59
Figure 2-22:	“CONFIG DETAILS” menu	60
Figure 2-23:	“CONFIG DETAILS” menu: submenus	60

Figure 2-24:	“PLCnext DETAILS” menu (standard controller)	62
Figure 2-25:	“S-PLC DETAILS” menu (iSPNS 3000)	62
Figure 2-26:	“S-PLC DETAILS” menu: submenus	63
Figure 2-27:	“OPC UA DETAILS” menu (OPC UA server)	64
Figure 2-28:	“PN-C DETAILS” menu (PROFINET controller)	64
Figure 2-29:	“PN-D DETAILS” menu (PROFINET device)	65
Figure 2-30:	USB interface of the RFC 4072S	66
Figure 2-31:	Interfaces of the RFC 4072S	67
Figure 2-32:	PROFINET example installation	69
Figure 2-33:	Mode selector switch	70
Figure 2-34:	Overload range with fall-back characteristic curve	72
Figure 2-35:	Overload range without fall-back characteristic curve	72
Figure 2-36:	Administrator password on the controller	76

Section 3

Figure 3-1:	Mounting the RFC FAN MODULE fan module	79
Figure 3-2:	Mounting the RFC 4072S	80
Figure 3-3:	Mounted RFC 4072S with end brackets and maximum distance between the DIN rail fastening points (160 mm)	81
Figure 3-4:	Inserting (A) or removing (B) the SD card (parameterization memory)	82
Figure 3-5:	Cabling between an Ethernet network and the RFC 4072S	83
Figure 3-6:	Connecting the supply voltage	84
Figure 3-7:	Removing the power supply	85
Figure 3-8:	Disconnecting the Ethernet connection	86
Figure 3-9:	Removing the RFC from the DIN rail	86
Figure 3-10:	Removing the fan module	87
Figure 3-11:	Mounting the RFC FAN MODULE fan module	88
Figure 3-12:	Snapping the RFC onto the DIN rail	88
Figure 3-13:	Establishing the Ethernet connection	89
Figure 3-14:	Connecting the power supply	89

Section 4

Figure 4-1:	Example configuration	96
Figure 4-2:	PLCnext Engineer user interface	99
Figure 4-3:	Start page, “Empty RFC 4072S project” project template	100
Figure 4-4:	Setting the IP address range	102

Figure 4-5:	Setting the IP address	103
Figure 4-6:	Defining a project password	104
Figure 4-7:	Selecting the network card	105
Figure 4-8:	Assigning online devices	105
Figure 4-9:	Successful assignment of the configured controller to an online device	106
Figure 4-10:	User authentication: entering a user name and password	107
Figure 4-11:	Successful connection to the controller	107
Figure 4-12:	Role picker for selecting PROFINET devices	108
Figure 4-13:	PROFINET devices in the “PLANT” area and in the Device List	108
Figure 4-14:	Selecting the network card	109
Figure 4-15:	Assigning online devices	109
Figure 4-16:	Successful assignment of the configured PROFINET devices to an online device	110
Figure 4-17:	Role picker for selecting I/O modules	111
Figure 4-18:	Entering the project password	111
Figure 4-19:	Successful login to the safety-related area	112
Figure 4-20:	I/O modules of a PROFINET device in the “PLANT” area and in the module list	112
Figure 4-21:	Reading I/O modules of a PROFINET device automatically	113
Figure 4-22:	Axioline F modules in the example project	113
Figure 4-23:	Selecting the programming language for the first worksheet	114
Figure 4-24:	“Add Program” context menu	115
Figure 4-25:	Creating variables for a POU (in the example: for the “Main” POU)	116
Figure 4-26:	Example program in FBD	117
Figure 4-27:	Adding a code worksheet to a POU	117
Figure 4-28:	Tasks and program instances in the “Tasks and Events” editor	118
Figure 4-29:	Example: list of all available variables PLCnext Engineer	119
Figure 4-30:	Role picker for selecting process data	120
Figure 4-31:	Selected process data item	120
Figure 4-32:	Example: list of all available process data items	121
Figure 4-33:	Role picker for selecting variables	121
Figure 4-34:	Selected variable	122
Figure 4-35:	Example: list of all available IN and OUT ports	122
Figure 4-36:	Role picker for selecting IN ports	123
Figure 4-37:	Role picker for selecting OUT ports	123
Figure 4-38:	Controller in the RUN state, PROFINET controller in the ACTIVE state	124

Figure 4-39:	“Variables” editor: online values of the variables used	125
Figure 4-40:	“Code” editor: online values of the variables used	125
Figure 4-41:	F-Address of the F-Host: F_Source_Add (F_Source_Address)	127
Figure 4-42:	F-Address of the PROFIsafe F-Device: F_Dest_Add (F_Destination_Address)	128
Figure 4-43:	Management/diagnostic variables for each configured F-Device	129
Figure 4-44:	Management/diagnostic variables for all configured F-Devices	130
Figure 4-45:	Management/diagnostic variables of F-Devices (default)	130
Figure 4-46:	“Safety Parameters” editor: AXL F PSDI8/4 1F	131
Figure 4-47:	“Safety Parameters” editor: AXL F PSDO8/3 1F	132
Figure 4-48:	Exchange variables in the example	133
Figure 4-49:	“Add Variable (Safety PLC)” context menu	134
Figure 4-50:	Setting the data direction	135
Figure 4-51:	Creating variables for a POU (in the example: for the “S_Main” POU)	136
Figure 4-52:	Selecting management/diagnostic variables	137
Figure 4-53:	Safety-related example program	138
Figure 4-54:	Assigned safety-related process data	139
Figure 4-55:	Standard controller in the RUN state	140
Figure 4-56:	Standard controller in the “RUN” state	141
Figure 4-57:	Controller password: entering the password for the safety-related controller	142
Figure 4-58:	Information dialog: prevent any hazard posed by the safety-related controller being started and stopped	143
Figure 4-59:	Safety-related controller in the RUN state	143
Figure 4-60:	Safety Cockpit: safety-related controller in the “RUN” state – Safe Run	144
Figure 4-61:	“Variables” editor (S_Main): online values of the variables used	145
Figure 4-62:	“Code” editor (S_Main): online values of the variables used	146
Figure 4-63:	Exiting safe mode – switching to debug mode	147
Figure 4-64:	Display: debug mode indicated	147
Figure 4-65:	Exiting debug mode – switching to safe mode	148
Figure 4-66:	PLCnext Engineer – Passivated PROFIsafe F-Devices	149

Section 5

Figure 5-1:	AsynCom_PN_1 function block (instance: AsynCom_PN_1_1)	160
Figure 5-2:	Function block PNFD_AXL_Diag_1 (Instance: PNFD_IL_Diag_V1_01_1)	161

Section 6

Figure 6-1:	Replacing the RFC FAN MODULE fan module (removal (A), mounting (B))	164
Figure 6-2:	Standard controller in the "STOP" state	166
Figure 6-3:	PLCnext Engineer safety prompt: switching to debug mode	166
Figure 6-4:	SPNS state: Debug Run	167
Figure 6-5:	SPNS state: Debug Stop	167
Figure 6-6:	After successful firmware update, the RFC runs without any errors ..	168

Section 7

Figure 7-1:	"FACTORY RESET" menu	171
Figure 7-2:	Default settings of the RFC 4072S: indication on the display	171
Figure 7-3:	"CONFIG DETAILS, ... EDIT LAN2" menu: default settings	173
Figure 7-4:	"CONFIG DETAILS, ... EDIT LAN2" menu: edit LAN2 IP address	173
Figure 7-5:	"CONFIG DETAILS, ... EDIT LAN2" menu: LAN2 IP address	174
Figure 7-6:	"CONFIG DETAILS, ... EDIT LAN2" menu: LAN2 IP settings changed	174
Figure 7-7:	"CONFIG DETAILS" menu: nothing has been changed	174
Figure 7-8:	Logging into the RFC 4072S via WinSCP	175
Figure 7-9:	PLCnext directory "/opt/plcnext" in the parameterization memory.	176
Figure 7-10:	Realtime clock settings for the RFC 4072S	176
Figure 7-11:	PROFINET device – "Start AR on startup"	177
Figure 7-12:	PROFINET device – "Substitute value behavior of inputs"	179
Figure 7-13:	AR_MGT function block	182

Section 8

Figure 8-1:	System variables grouped into structures	183
-------------	--	-----

Section 9

Figure 9-1:	RFC 4072S welcome page	210
Figure 9-2:	“Licenses and Legal Information” link	212
Figure 9-3:	WBM user interface: selecting the language	213
Figure 9-4:	WBM: Login page	214
Figure 9-5:	WBM start page	215
Figure 9-6:	WBM: “General Data” page	216
Figure 9-7:	WBM: “Firmware Update” page	217
Figure 9-8:	WBM: “PROFINET Diagnostics – Overview” page	218
Figure 9-9:	WBM: “PROFINET Diagnostics – Device List” page	219
Figure 9-10:	WBM: “User Authentication” page	220
Figure 9-11:	WBM: “Enable/Disable User Authentication” dialog	221
Figure 9-12:	“Add User” dialog	222
Figure 9-13:	“Set User Password” dialog	222
Figure 9-14:	“Modify Roles” dialog	223
Figure 9-15:	Enabling OPC UA file transfer	225
Figure 9-16:	“Remove User” dialog	226
Figure 9-17:	WBM: “Certificate Authentication” page – “TrustStores” tab	226
Figure 9-18:	WBM: “Certificate Authentication” page – “IdentityStores” tab	227
Figure 9-19:	WBM: “Firewall” page	228
Figure 9-20:	WBM: Information – General Data (firmware version)	229
Figure 9-21:	WBM: Administration – Firmware Update	230
Figure 9-22:	WBM: Administration – Selecting the firmware container	230
Figure 9-23:	WBM: Administration – Firmware container selected – Start update	231
Figure 9-24:	WBM: Administration – Firmware Update – Transferring the firmware container to the RFC	232
Figure 9-25:	WBM: Administration – Firmware Update – Firmware is being updated	233
Figure 9-26:	WBM: Information – Checking firmware version after firmware update	234
Figure 9-27:	WBM: Administration – Firmware update error	235

Appendix A

Figure A-1:	Interfaces of the RFC 4072S	250
Figure A-2:	Contact assignment of the USB 3.0 interface (type A)	251
Figure A-3:	Contact assignment of an Ethernet interface in RJ45 format	252
Figure A-4:	Connecting the supply voltage	254

D 2 List of tables

Section 2

Table 2-1:	Functions of the symbols	50
Table 2-2:	Status information: PLCnext (standard controller).....	52
Table 2-3:	Status information: safety PLC (iSPNS 3000)	53
Table 2-4:	Status information: OPC UA (OPC UA server)	54
Table 2-5:	Status information: PN Control (PROFINET controller)	54
Table 2-6:	Status information: PN Device (PROFINET device)	55
Table 2-7:	Diagnostics indicators: safety PLC (safety-related PROFINET controller iSPNS 3000)	56
Table 2-8:	Diagnostic indicators: PN Control (PROFINET controller)	58
Table 2-9:	Diagnostics indicators: PN device (PROFINET device).....	58
Table 2-10:	Operating modes of the RFC	70
Table 2-11:	Storage of firmware components in the root file system.....	73

Section 4

Table 4-1:	Steps for initial startup of the RFC 4072S	91
Table 4-2:	Steps for restarting the RFC 4072S	94
Table 4-3:	IP address settings in the example	102
Table 4-4:	Input/output variables in the example (logical ANDing).....	116
Table 4-5:	Input/output variables in the example (safe logical ANDing)	136

Section 5

Table 5-1:	RFC 4072S error codes.....	154
------------	----------------------------	-----

Section 7

Table 7-1:	Overview of the function blocks	180
Table 7-2:	Overview of the function blocks	181

Section 8

Table 8-1:	SPNS system variable and elements of the SPNSV2_TYPE structure	184
Table 8-2:	Elements in the diagnostic status register (SPNS.DIAG.STATUS_REG.xxx)	186
Table 8-3:	Diagnostic status register of the iSPNS 3000: SPNS.DIAG.STATUS_REG	188
Table 8-4:	Contents of bits 5 and 6 and corresponding LED indicators	189
Table 8-5:	SPNS_V2_PROFISAFE_DIAG system variable and elements of the PROFISAFE_DIAG_OUT structure	190
Tabelle 8-6:	FDEV_INx and FDEV_OUTx (x = 0 ... 7) system variables	190
Table 8-7:	Management/diagnostic variables for each configured F-Device	191
Table 8-8:	Management/diagnostic variables for F-Devices	195
Table 8-9:	PROFIsafe: Device diagnostics variables (local device)	198
Table 8-10:	PROFIsafe: Collective diagnostics variables (local device).....	202
Table 8-11:	PROFINET system variables (PROFINET controller functionality).....	203
Table 8-12:	PROFINET system variables (PROFINET device functions)	204
Table 8-13:	RTC system variable and elements of the RTC_TYPE structure	205
Table 8-14:	PLC_CRC_PRJ system variable	205
Table 8-15:	System variables for the TCP_SOCKET, UDP_SOCKET, and TLS_SOCKET function blocks	205
Table 8-16:	DEVICE_STATE system variable and elements of the DEVICE_STATE_4xxx_TYPE structure	206
Table 8-17:	ESM_DATA system variable for task handling and elements of the ESM_DAT structure.....	206
Table 8-18:	HMI_STATUS system variable and elements of the HMI_STATUS_TYPE structure.....	208
Table 8-19:	HMI_CONTROL system variable and elements of the HMI_CONTROL_TYPE structure	208

Section 9

Table 9-1:	User roles and their assigned access permissions in the various applications	224
------------	---	-----

Appendix A

Table A-1:	Shell commands for controlling the firmware	249
Table A-2:	Contact assignment of the USB 3.0 interface (type A)	251
Table A-3:	Contact assignment of the Ethernet interfaces depending on the transmission speed.	253

D 3 Index

A

Administrator password	76
Authentication	76
Password	76
User name	76

C

Checklists	257
“Initial startup” and “restart/device replacement” validation.....	267
Assembly and electrical installation	265
Planning	264
Startup and parameterization	266
Validation “restart/device replacement”	267
Communication paths	67
Consecutive number	255, 256
Controller	
IP settings.....	101
CRC	255

D

Decommissioning	170
Diagnostic display	51
Disposal	170

E

Electrical installation	
Connecting an Ethernet network	83
Replacing the RFC 4072S	85
Ethernet connection	68

F

F_Destination_Address	256
F_Source_Address	256
Failure state	
Exit	152
Quit.....	152
Fall-back characteristic curve.....	71
Fan module	
Attaching	48
Replacement	164

File system

Directory structure	73
SFTP access	76
Firewall	76

Firmware

Update	165
--------------	-----

For your safety

Abbreviations used.....	22
Electrical safety	16
General safety notes	12
Hardware and software requirements	21
Intended use	19
Safety hotline	22
Safety of the machine or system	17
Standards and directives.....	18

Functional safety

Loss of functional safety	16
---------------------------------	----

G

Gap during installation	48, 80
-------------------------------	--------

General

Mounting/removal/electrical installation.....	77
Grounding concept	77

H

HTTPS certificate	249
-------------------------	-----

I

Interfaces

Ethernet.....	68
---------------	----

Interfaces of the RFC 4072S

Ethernet interface	252
--------------------------	-----

IP settings	101
-------------------	-----

iParameters.....	256
------------------	-----

M

Maintenance	163
-------------------	-----

Mode selector switch	70
----------------------------	----

Mounting/removal

Mounting the RFC 4072S.....	80
-----------------------------	----

Removing the RFC 4072S.....	81
-----------------------------	----

O

Overlay file system 73

P

Parameterization memory

 Inserting/removing the SD card 81

 Note on formatting 81

Passivation 28, 256

Password 76

PLCnext Engineer

 Assigning process data 119

 Connecting to a controller 105

 HMI application 126

 Instantiating a program 118

 IP settings 101

 New project 100

 PROFINET devices 108

 Programming 114, 127

 Transferring a project to the controller 124

 User interface 99

Power supply 71

Power supply without fall-back characteristic curve .. 237

PROFINET Installation Guideline 77

PROFIsafe 256

 Communication diagnostics 29, 31

 Communications diagnostics 27

 Device identification 30

 F-Parameters 255

PROFIsafe address 256

PROFIsafe monitoring time 256

R

Reintegration 28, 255

Reintegration (depassivation) 255

Repair 169

Restart

 Validation 89

RFC 4072S

 Behavior in the event of an error 27

 Inserting/removing the parameterization memory . 81

 Mounting 80

 Removal 81

 Replacement 85

 Safe state (failure state) 27

 Security seal 47

 Test mark 47

Root file system 73

S

Safe state

 Failure State 27

Safety function response time

 SFRT 35

Safety hotline 22

Safety notes

 Mounting 77

 Removal 77

SD card

 Inserting/removing 81

 Note on formatting 81

SFRT

 Safety function response time 35

SFTP

 Authentication 76

Shielding 78

Startup

 Initial startup 91

 Restart 94

Status and diagnostic indicators (Ethernet) 49

T

Technical data

 Buffer times of the realtime clock 242

 Safety characteristic data 241

Third-party certificate 249

U

User name 76

W

Watchdog time

F_WD_Time IN.....	36
F_WD_Time OUT.....	36

WBM

Login	214
TLS certificate	209
User roles	223

E Appendix: revision history

Revision	Date	Contents	
01	2019-05-09	First publication of the user manual for the RFC 4072S.	
02	2020-03-03	Revision with the following changes:	
		Terminology updated (safety-related, power supply, touch screen display/display, PLCnext Engineer).	
		Inner cover page	Added note box: Observe controller firmware.
		Section 2.1	Section added: Function extensions using PLCnext apps
		Section 2.9.3	Section "Safety PLC (...)": "SPNS" replaced by "iSPNS 3000".
		Section 2.12	Table 2-10 "Operating modes of the RFC": Explanation of the MRESET operating mode corrected.
		Section 2.14	Table 2-11 "Storage of firmware components in the root file system" updated.
		Section 7.12	OPC UA Note box updated: Link to the PLCnext Community added.
		Section 8.3.1	System variable: iSPNS 3000 temperatur status register (STATUS_REG) Description of diagnostic codes added.
		Section 8.3.3	Added note box: "Warning: Outputs can be set"
		Section 8.5	System variable: PLC_CRC_PRJ Information about the CRC of the non-safety-related project
		Section 10.1	Technical Data <ul style="list-style-type: none"> - Power supply <ul style="list-style-type: none"> - Connection data for COMBICON connectors: Correction of the „Conductor cross-section [AWG]“ value. - IEC 61131 runtime system <ul style="list-style-type: none"> - Programming system: Information corrected. - Number of control tasks: Value corrected. - Ambient conditions <ul style="list-style-type: none"> - Degree of protection: UL information added. - Air pressure (operation): Value range corrected. - Resistance to gases...: Translation correction: Use of the device in these ambient conditions is prohibited. - Safety characteristics data in acc. with EN ISO 13849: <ul style="list-style-type: none"> - PFH_D added. - UL: Additional information added. <ul style="list-style-type: none"> - UL Warning Instructions added.
		Section 10.2.5	Documentation <ul style="list-style-type: none"> - PLCnext Technology: Information updated. - Security: Information updated.

Revision	Date	Contents		
03	2021-03-04	Revision with the following changes:		
		<table border="1"> <tr> <td>Section 2.6</td> <td>Note box "NOTE: The RFC ... can overheat – use the fan module.": Value range of the ambient temperature during operation with regard to altitude (3000 m ... 4000 m) added.</td> </tr> <tr> <td>Section 10.1</td> <td> <ul style="list-style-type: none"> – Fan module (...) Note box updated: "NOTE: The RFC ... can overheat – use the fan module.": Value range of the ambient temperature during operation with regard to altitude (3000 m ... 4000 m) added. – Ambient conditions <ul style="list-style-type: none"> – Ambient temperature (operation): with fan module: Value range with regard to altitude (3000 m ... 4000 m) added. – Air pressure (operation): Value range corrected. </td> </tr> </table>	Section 2.6	Note box "NOTE: The RFC ... can overheat – use the fan module.": Value range of the ambient temperature during operation with regard to altitude (3000 m ... 4000 m) added.
Section 2.6	Note box "NOTE: The RFC ... can overheat – use the fan module.": Value range of the ambient temperature during operation with regard to altitude (3000 m ... 4000 m) added.			
Section 10.1	<ul style="list-style-type: none"> – Fan module (...) Note box updated: "NOTE: The RFC ... can overheat – use the fan module.": Value range of the ambient temperature during operation with regard to altitude (3000 m ... 4000 m) added. – Ambient conditions <ul style="list-style-type: none"> – Ambient temperature (operation): with fan module: Value range with regard to altitude (3000 m ... 4000 m) added. – Air pressure (operation): Value range corrected. 			
04	2022-07-08	Revision with the following changes:		
		Section 1.6	Observe startup behavior: First paragraph replaced by two new paragraphs.	
		Section 1.6.2	Heading changed: "Security in the network".	
		Section 1.7, 2.13.1, 3.1, 3.8, 10.1	In the WARNING box regarding the loss of electrical safety, standard EN 50178/VDE 0160 (PELV) replaced with standard IEC 61010-2-201 (PELV).	
		Section 1.9	Section on standards and guidelines revised.	
		Section 1.12	Device name corrected.	
		Section 1.15	"...24-hour hotline" replaced with "...Safety hotline".	
		Section 2.3.1 (page 31)	Sentence „Always take into consideration..." removed as this information appears in the sentence above.	
		Section 2.13.1	Power supply QUINT POWER changed.	
		Section 4.5.2	Note box added: "WARNING: Network error/network conflict".	
		Section 10.2.3	Ordering data for accessories: Power supplies replaced with new QUINT POWER power supplies.	
		Section 10.2.5	Ordering data for documentation: <ul style="list-style-type: none"> – PROFINET and PROFIsafe documents updated. – Links to www.profibus.com changed. 	
Appendix C 1.1, C 2.1, C 2.2, C 2.4	In the checklists, standard EN 50178/VDE 0160 (PELV) replaced with standard IEC 61010-2-201 (PELV): "Planning" (C 1.1) No. 6, "Planning" (C 2.1) No. 4, "Assembly and electrical installation" (C 2.2) No. 4, "Initial startup" ... (C 2.4) No. 6.			
05	2023-12-05	Revision not created in english.		
06	2024-07-31	Revision with the following changes:		
		Entire document:	<ul style="list-style-type: none"> – "Management/diagnostic variables" term standardized. – Cover page photo updated (new LEDs: WN, P, C). – Various display images updated (new LEDs: WN, P, C). 	
		Section 1.6	Observe startup behavior: The first and second paragraphs have been updated.	
		Section 1.6.1	New section: Foreseeable misuse	
Section 1.6.3	New section: Notes on Security			

Revision	Date	Contents
		Section 1.6.4 Section updated: Security in the network
		Section 1.7 ESD note deleted and moved to Section 1.15.3.
		Section 1.8 The term “risk analysis” has been exchanged with “risk assessment”.
		Section 1.11 <ul style="list-style-type: none"> – Link to the PROFIsafe documentation updated. – Note on PLCnext Technology and security documentation updated.
		Section 1.12 <ul style="list-style-type: none"> – System requirements for PLCnext Engineer updated. – OPC UA server removed from the “system requirements” table.
		Section 1.13 Section “Disposal” deleted (content is included in Section 6.7 “Decommissioning and disposal”).
		Section 1.15 New section added: Transport, storage, and unpacking
		Section 2.2 <ul style="list-style-type: none"> – Restructuring of the entire Section 2.2 incl. subsection (division into behavior of the iSPNS 3000 as F-Host and F-Device). – Paragraph “Exchange area”: Specification of the data direction “I” and “Q” for NSI and NSQ corrected.
		Section 2.3.2 Rewording of the title in the first NOTE box.
		Section 2.9.3 Description of the WN, P, and C LEDs added.
		Section 2.9.4 Safety PLC: WN, P, and C LEDs added.
		Section 2.9.5 <ul style="list-style-type: none"> – Figure 2-22: CONFIG DETAILS menu with new OPTIONS tile – Figure 2-23 (C): MAINTENANCE submenu with new tiles FAN CONTROL and MRESET REBOOT – Figure 2-23 (D): OPTIONS submenu added – Description of the MAINTENANCE (C) and OPTIONS (D) submenus updated/added. – Description of the MAINTENANCE (C) submenu corrected: MRESET REBOOT.
		Section 2.12 Table 2-10: <ul style="list-style-type: none"> – MRESET: Description corrected and WARNING box added. – STOP: Text in the WARNING box updated with regard to MRESET. – RUN/PROG: First line updated with regard to STOP and MRESET.
		Section 4.15.1 Change to F_Source_Address and F_Destination_Address: An adjustable range of “1 ... 65534 _{dec} ”, maximum, is permitted.
		Section 4.15.6 “Selecting management/diagnostic variables and exchange variables” section: first paragraph “Before the management/diagnostic variables...” corrected.
		Section 6.7 Section adapted in accordance with current specifications.
		Section 8.3.1 Table 8-2: BATT and DD elements are not supported: deleted
		Section 8.3.2 New section on the FDEV_INx and FDEV_OUTx (x = 0 ... 7) system variables of the F-Device of the iSPNS 3000.
		Section 8.3.5 New section on management/diagnostic variables of the F-Device of the iSPNS 3000.

Revision	Date	Contents	
		Section 10.1	Technical Data: <ul style="list-style-type: none">- Characteristic data of the safety-related PROFINET controller iSPNS 3000 updated- PROFIsafe IO data updated
c06	2024-09-03	Section 2.9.5	Description of the MAINTENANCE (C) submenu MRESET REBOOT: Translation corrected.

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:

phoenixcontact.com

Make sure you always use the latest documentation.

It can be downloaded at:

phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.

Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG

Flachmarktstraße 8

32825 Blomberg

GERMANY

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:

tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

© PHOENIX CONTACT 2024-09-03

108580_en_c06
Order No. —