Installation and operation of the BPC 9102S industrial box PC with integrated safety-related controller

User manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

Installation and operation of the BPC 9102S industrial box PC with integrated safety-related controller

UM EN BPC 9102S, Revision 01 2021-11-02

This manual is valid for:

Designation	Revision		Item No.
BPC 9102S	HW/FW:	≥ 02/2021.6	1246285
	HW/FW (SPLC 3000):	≥ 03/02.00.0000	

Prior to commissioning the device, observe the following:

- Ensure that you operate the device with the latest firmware version.
  The latest firmware version is available for downloading at phoenixcontact.net/product/1246285.
- Observe the change notes regarding the firmware version.
- If necessary, update the PLCnext firmware.
  Information on performing a PLCnext firmware update is available in the PLCnext Info Center.

110088_en_01

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

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 and industrial security for handling electrical machines. The persons must be able to recognize dangers.

1.3 Information on this user manual

1.3.1 Purpose of this user manual

The information in this document describes how the “BPC 9102S industrial box PC with integrated SPLC 3000 safety-related controller” works, its control elements, and its connection elements. It also describes how the BPC 9102S industrial box PC is integrated into the software tools listed in Section “System requirements (hardware and software)” on page 22.

This information will enable you to use the device in accordance with your requirements.

1.3.2 Validity of the user manual

This user manual is only valid for the “BPC 9102S industrial box PC with integrated SPLC 3000 safety-related controller” in the versions indicated on the inner cover page.

The device will also be referred to in the following by its short form, “BPC 9102S”. The “integrated SPLC 3000 safety-related controller” will also be referred to in the following by its short form, “SPLC 3000”.

This user manual is only valid in association with the user manuals listed in Sections 1.11 on page 21 and 14.1.5 on page 184.

1.4 General safety notes

WARNING: Depending on the application, incorrect handling of the BPC 9102S can pose serious danger for the user

When working with the BPC 9102S within a PROFIsafe system, observe all the safety notes listed 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., from the Axioline F product group)
- Operation of the software tools specified under the software requirements (see Section “System requirements (hardware and software)” on page 22)
- 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 21.

Safety of personnel and equipment

The safety of personnel and equipment can only be assured if the BPC 9102S is used correctly (see Section “Intended use” on page 13).

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 BPC 9102S as the central component do not prevent automatic startup/restart of the safety function. The user must program this independently in the safety program using the programming software for PROFIsafe (PLCnext Engineer).

After switching on the supply voltage or after a software reset, the BPC 9102S starts immediately if a configuration memory with a valid project is inserted.

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 BPC 9102S startup phase. The outputs of the F-Devices and the non-safety-relevant 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 your 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

Observe these notes to prevent unexpected machine startup after operator acceptance via the “Operator Acknowledgment” command.

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.

1.5 Field of application of the product

1.5.1 Intended use

The products described in this document are designed for use in manufacturing and industrial environments.

The products are built in accordance with the latest safety requirements. However, dangerous situations or damage to the products or other property can arise from misuse of this device.

The products satisfy the requirements of the EMC directive and the harmonized European standards. Any modifications to the systems can influence the EMC behavior.

PROFIsafe

This information will enable you to use the BPC 9102S in accordance with your requirements in a PROFIsafe system.

- The device contains the SPLC 3000 safety-related controller which supports the PROFIsafe protocol.
- The device enables the implementation of functional safety applications.
  The safety function of the BPC 9102S is only available when used in a PROFIsafe system.
- The device can be used as an F-Host in a PROFIsafe system.
- A complete PROFIsafe system also includes F-Devices and the PLCnext Engineer software in addition to the BPC 9102S.
- The BPC 9102S 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.
- In a PROFIsafe system, the BPC 9102S can be used to realize safety functions with the following requirements depending on the operating conditions:
  - Up to SIL 3 in accordance with standard IEC 61508
  - Up to SIL CL 3 in accordance with standard EN 62061
  - Up to PL e/Cat. 4 in accordance with the standard EN ISO 13849-1

PROFINET

This information will also enable you to use the BPC 9102S as a PROFINET controller/device in a PROFINET system in accordance with your requirements.

In a PROFINET system, the BPC 9102S can be used as a PROFINET controller and/or simultaneously as a PROFINET device. As a PROFINET controller, the device performs the function of a controller for the lower-level PROFINET system. For each PROFINET device function, the BPC 9102S can be operated on a lower level of the PROFINET controller. Concurrent operation of the BPC 9102S as PROFINET controller and device is only possible in two different subnetworks.

Operating instructions

- Use the PLCnext Engineer software to implement safety-related programming in your application.
- Observe all information in this user manual as well as in the documents listed in “Documentation” on page 21.
- Only use the device in compliance with the technical data and ambient conditions stated in Section 14, “Technical data and ordering data” starting on page 183.

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 and/or thermal stress that exceeds the specified limits.

To ensure correct operation, the BPC 9102S must be installed in a lockable housing or a lockable control cabinet with a minimum degree of protection of IP54.

Assembly guidelines

During installation of the device, observe the sections 4 “Mounting hardware” and 5 “Connecting and wiring the hardware”).

1.5.2 Foreseeable misuse

WARNING: Serious risks due to improper use

There is a serious risk to the user and/or property if the BPC 9102S is used inappropriately or not in accordance with the intended use, or if it is subject to tampering.

1.5.3 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. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

Do not open the housing/ Security seal

It is strictly prohibited to open the BPC 9102S housing. In order to prevent tampering with the device supplied and to detect unauthorized opening of the device, security seals are applied to the device (see Section 3.5.1). These security seals are damaged in the event of unauthorized opening. In this case, the correct operation of the device can no longer be ensured.

1.5.4 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 exchange 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 BPC 9102S. A general description of the Web-based management system is available in the PLCnext Info Center.
- It is imperative that you install the BPC 9102S 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.

1.6 Safety notes

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

NOTE: Property damage due to incorrect use

The IP20 degree of protection (IEC 60529/EN 60529) requires that the device be used in a clean and dry environment. If you use the device in an environment that is outside of the specified limits, this may cause damage to the device.

- Do not subject the device to mechanical and/or thermal stress that exceeds the specified limits.

NOTE: Electrostatic discharge

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

NOTE: Device failure due to foreign objects in device

Foreign objects in the device can lead to malfunctions or even device failure.

- Ensure that no foreign objects find their way into the device (e.g., into the vents).

NOTE: Device failure if operated outside the permitted ambient temperature range

Operating the device in ambient temperatures that are not within the permitted range may lead to malfunctions or even device failure.

- Ensure that the device is operated within the permitted ambient temperature range; see Section 14.2.

NOTE: Device failure due to vibrations and shock levels above the permitted specifications during operation

If the device is subjected to vibrations and shock levels above the permitted specifications during operation, this may lead to malfunctions or even device failure.

- Ensure that the permitted specifications for vibrations and shocks are adhered to when operating the device; see Section 14.2.

NOTE: Device defect due to polarity reversal

Polarity reversal puts a strain on the electronics and can damage the device.

- To protect the device, avoid reversing the poles of the 24 V supply.

1.7 Security in the network

NOTE: Risk of unauthorized network access

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

Therefore, please check your application for the option of deactivating active communication channels (e.g., FTP, DCP, HTTP, HTTPS, etc.) or setting passwords to prevent third parties from accessing the BPC 9102S without authorization and modifying the system.

Due to its communication interfaces, the BPC 9102S should not be used in safety-critical applications unless additional security appliances are used.
Please take additional protective measures in accordance with the IT security requirements and the standards applicable to your application (e.g., virtual networks (VPN) for remote maintenance access, firewalls, etc.) for protection against unauthorized network access.

On first request, you shall release Phoenix Contact and the companies associated with Phoenix Contact GmbH & Co. KG, Flachsmarktstraße 8, 32825 Blomberg, Germany in accordance with §§ 15 ff AktG (German Stock Corporation Act), hereinafter collectively referred to as “Phoenix Contact”, from all third-party claims made due to improper use.

For the protection of networks for remote maintenance via VPN, Phoenix Contact offers the mGuard product range of security appliances, a description of which is provided in the latest Phoenix Contact catalog (phoenixcontact.net/products).

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/1246285.

1.8 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 in accordance with 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 BPC 9102S 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 satisfy the requirements of EN 60204-1 and feature safe isolation with PELV in accordance with IEC 61010-2-201 (PELV). They prevent short circuits between the primary and secondary side.

Insulation rating

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

The BPC 9102S is designed for overvoltage category III (as per DIN EN 60664-1). If you expect surge voltages in the system which exceed the values defined in overvoltage category III, take additional measures for voltage limitation into consideration.

DC distribution network

DC distribution network in accordance with 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 in accordance with IEC 61326-3-1.

When using an BPC 9102S in a DC distribution network, install appropriate surge protection (e.g., PT 2+1-S-48DC/FM, item 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 21).

WARNING: Incorrect installation and upgrades can pose serious risks
The user is obliged to design the devices used and their installation in the system in accordance with these requirements. This also means that existing plants and systems retrofitted with PROFIsafe must be checked and tested again in this respect.

1.9 Safety of the machine or system

The manufacturers and operators of machines and systems in which the BPC 9102S device 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 analysis in accordance with the directives and standards specified in Section “Standards and directives” on page 20, as well as a test report (checklist) for validating the safety function (see Section “Appendix: Checklists” on page 197).

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 analysis. The required safety integrity thus determined governs how the BPC 9102S industry box PC with integrated safety-related SPLC 3000 controller is to be used within the overall safety function and how it should be parameterized.

Checking 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).

1.10 Standards and directives

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

Directives considered in the development of the BPC 9102S device:

- Machinery Directive 2006/42/EC
- EMC Directive => 2014/30/EU

- PROFINET Assembling Guideline, Version 2.8, September 2019
- PROFIsafe System Description, Version April 2016
- PROFIBUS Guideline, PROFIsafe Policy, Version 1.5, July 2011
- PROFIsafe – Environment related to PROFIsafe V2.6.1
  Guideline for PROFINET and PROFIBUS, Version 2.6, December 2015
- PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET
  Profile part, related to IEC 61784-3-3
  Technical Specification, Version 2.6MU1, August 2018
- PROFIsafe Test Specification, related to PROFIsafe V2.6,
  Test Specification for PROFIBUS and PROFINET, Version 2.3, March 2018
- Functional Bonding and Shielding of PROFIBUS and PROFINET, Guideline for PROFIBUS and PROFINET, Version 2.4, October 2020

For additional information on the PROFINET and PROFIsafe documents, please refer to Section “Documentation” on page 184.

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. You will find changes or supplements to this documentation on the Internet at phoenixcontact.net/products.

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

	Document	Description
PROFIsafe	– 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 184. Please also observe the relevant information on PROFINET and PROFIsafe which is available on the Internet at www.profisafe.net and www.profinet.com.
	– User manuals for the PROFIsafe I/O modules used in your application	For example, Axioline F.
PROFINET	– PROFINET Assembling Guideline – Guideline for PROFIBUS and PROFINET "Functional Bonding and Shielding of PROFIBUS and PROFINET"	For more detailed information on these documents, please refer to Section "Documentation" on page 184.
	– UM EN PROFINET SYS	PROFINET basic principles
	– UM EN PROFINET CTRL DEV	PROFINET controller/device functions
Software	– Online help for the PLCnext Engineer software	
PLCnext Technology	– PLCnext Info Center – plcnext-community.net	Comprehensive documentation for PLCnext Technology Information on troubleshooting and answers to frequently asked questions (FAQs) in the PLCnext Community
Security	– AH EN INDUSTRIAL SECURITY	Application note with measures to protect network-capable devices with Ethernet connection against unauthorized access

1.12 System requirements (hardware and software)

An active connection to a lower-level PROFINET system is required for commissioning the BPC 9102S in accordance with 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.

- Install the PLCnext Engineer software listed in the table on your PC.
  For trouble-free operation, follow the instructions in the software documentation.

Please note:
The PLCnext Engineer engineering software platform for Phoenix Contact automation controllers is compliant with IEC 61131-3. Its functionality can be extended 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 commissioned. PLCnext Engineer is certified by TÜV Rheinland.

Hardware/software	Description	Ordering data
SPLC 3000 industrial box PC with integrated safety-related controller	BPC 9102S	For ordering data, see Section “Accessories” on page 183.
SD card	Configuration memory	
The configuration memory is essential for the operation of the BPC 9102S.		
Ethernet cable	For connecting the BPC 9102S to a PC and PROFINET	
Power supply	Power supply for the BPC 9102S	
Fan kit	Optional	
PLCnext Engineer	≥2021.6	

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
SPLC 3000	Safety-related controller with performance class 3000 integrated into the BPC 9102S. In this document, the SPLC 3000 is also referred to as a safety-related controller. In system variables and certificates, the SPLC 3000 is also referred to as iSPNS 3000.
PELV	Protective extra-low voltage Circuit in which, under normal conditions or under the conditions of an individual error, the voltage of 30 V AC, 42.4 V peak value, or 60 V DC is not exceeded, except by grounding errors in other circuits. A PELV circuit is like an SELV circuit, but is connected to protective earth ground. (In accordance with EN 61131-2)
F_Source_Add	F-Source Address (F-Parameter) PROFIsafe source address: Address of the SPLC 3000 as F-Host
F_Dest_Add	F-Destination Address (F-Parameter) PROFIsafe destination address: Address of F-Devices in the application

For terms and abbreviations used for PROFIsafe, please refer to “Appendix: Terms for PROFIsafe” on page 195.

1.14 Safety Hotline

If you have any technical questions, please contact the Safety Hotline.

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

2 Transport, storage, and unpacking

2.1 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 187).
- 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.

2.2 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: -40°C ... +85°C
- Air pressure: 58 kPa ... 108 kPa (up to 4,500 m above sea level)
- Permissible humidity: 5% ... 95% (non-condensing)

2.3 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) in accordance 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.

NOTE: Electrostatic discharge on the D-SUB COM pin strip

The BPC 9102S is supplied with a cover cap on the D-SUB COM pin strip. The cover cap protects the D-SUB pin strip against electrostatic discharge (ESD).

- If the D-SUB pin strip is not used, place the cover cap on the D-SUB pin strip for protection against electrostatic discharge.

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 3.5.1).

  Any damage to the security seals is an indication of the device being opened without authorization, e.g., for tampering purposes. In this case, the correct operation of the device can no longer be ensured.
- Submit claims for any transport damage and/or damaged safety 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

– BPC 9102S industrial box PC with integrated SPLC 3000 safety-related controller
– Supply connector MSTB 2,5/ 3-STF-5,08 (item no.: 1777992)

3 Description of the BPC 9102S

3.1 General description of the BPC 9102S

The BPC 9102S is an industrial box PC with integrated SPLC 3000 safety-related controller. This safety-related controller unit supports the PROFIsafe protocol and enables functional safety applications to be implemented. The SPLC 3000 can be used as an F-Host in a PROFIsafe system.

The BPC 9102S 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 I/O level is connected via the device-internal Ethernet interfaces. Supporting the PROFINET/PROFIsafe protocol, the Ethernet interfaces enable communication with PROFINET and F-Devices in the application.

Ethernet interfaces are also available for networking with higher-level systems, such as the control level or operating level.

Features

- Compact housing with IP20 degree of protection
- Fanless design
- Processor: Intel® Core™ i7-10700TE processor

Programming

You configure and program the BPC 9102S using the PLCnext Engineer automation software. PLCnext Engineer is connected to the BPC 9102S via the local Ethernet network. 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 BPC 9102S features three Ethernet interfaces for TCP/IP/UDP/IP communication within the Ethernet network.

PROFINET / controller/ device functions

The BPC 9102S can be integrated into a PROFINET system using Ethernet interfaces. Depending on the configuration, the BPC 9102S functions as a PROFINET controller and/or a PROFINET device.

For additional information on how to integrate the BPC 9102S as a PROFINET controller or device, please refer to the PLCnext Engineer online help.

Password and user name for user authentication

You must authenticate yourself as a user in PLCnext Engineer using a user name and password in order to transfer the safety-related project online from the software over to the BPC 9102S. In this respect, observe the information in Section “Notes on security” on page 15.

Information on user authentication is available in Section 6.5.5.

Web-based management WBM system

The Web-based management interface integrated into the BPC 9102S enables static and dynamic device information to be displayed via a standard web browser. Status and diagnostic functions can be displayed in a graphical user interface once the device IP address has been entered in a web browser.

OPC UA server

An OPC UA server is integrated into the BPC 9102S. It provides BPC 9102S data in accordance with the OPC UA protocol (currently supported: Data Access). This data can be used for visualization purposes, for example.

PLCnext Engineer provides various 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 BPC 9102S is equipped with a USB 3.0 type A interface which is reserved for internal service purposes.

Configuration memory (SD card)

The safety-related and non-safety-related programs and configurations are saved in the configuration memory as part of the PLCnext Engineer project.

NOTE:

– For operation, the BPC 9102S **needs** a plug-in configuration memory in the form of an SD card.

– Please note that the SD card may not be inserted or removed during operation. If the SD card is removed/inserted during operation, the BPC 9102S will switch to the safe state (failure state).

• Always disconnect the power supply to the BPC 9102S before inserting or removing the SD card.

– Observe Section “Notes on security” on page 15, in particular in terms of access protection for the SD card.

The plug-in configuration memory is not supplied as standard with the BPC 9102S. Only use SD cards from Phoenix Contact that are intended for use with the BPC 9102S.

The ordering data is listed in Section “Accessories” on page 183.

Data buffering/backup in the event of voltage failures

In the event of a supply voltage failure, the BPC 9102S saves control data, e.g., retain data and log files, on the inserted configuration memory (SD card).

The device firmware recognizes the voltage failure. The retain data (variables of the standard controller of the BPC 9102S that are marked as “Retain” in the PLCnext Engineer project) and log files are automatically backed up on the configuration memory.

NOTE: Startup of the BPC 9102S not ensured

For correct startup of the device, the supply voltage may only be switched on at the earliest 30 seconds after the device LEDs go out.

Real-time clocks

The BPC 9102S buffers the internal real-time clock after the supply voltage is switched off. If the buffering equipment is discharged, supply the BPC 9102S with 24 V DC for 24 hours. In this way, the buffering equipment is recharged.

Diagnostics and status indicators (LEDs)

Diagnostics and status information is displayed directly on the BPC 9102S via LEDs (see also Table 3-1 on page 47):

Function extensions with PLCnext apps

You can easily extend the scope of functions of the BPC 9102S with apps from the PLCnext Store.

Visit the PLCnext Store at plcnextstore.com.

3.2 Description of the safety-related functioning of the BPC 9102S

Behavior of the safety-related SPLC 3000 controller as the F-Host in PROFIsafe

The BPC 9102S industrial box PC contains the powerful two-channel SPLC 3000 safety-related controller for PROFIsafe. The SPLC 3000 is permanently integrated into the housing of the BPC 9102S.

The PROFIsafe safety protocol is transmitted via the connected PROFINET network. The safety function is programmed in the PLCnext Engineer software.

The SPLC 3000 monitors and controls the safety function in a PROFIsafe system. In its function as the F-Host, it decides, for example, whether a safe output may be set or not.

Request for a programmed safety function

Following the request for a programmed safety function (e.g., safety door open), the SPLC 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. Any serious errors detected in the BPC 9102S with SPLC 3000 safety-related controller that may lead to the loss of the programmed safety function or adversely affect the programmed safety function will result in a switchover to the safe state (failure state). In this state, the safe outputs of the F-Devices are set to zero (FALSE).

The safe state will be displayed via the FS-S (failure state) LED lighting up 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: Diagnostics, messages, and removal” on page 129.

Passivation and reintegration

If the communication relationship between the SPLC 3000 and the 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 6, “Startup and validation” and sections “Management/diagnostic variables for F-Devices” on page 108, “Management/diagnostic variables for each configured F-Device” on page 151, and “Global management/diagnostic variables for F-Devices” on page 154.

PROFIsafe: Communication diagnostics

The BPC 9102S supports the user in monitoring and checking the communication relationship. The PLCnext Engineer software indicates why the communication relationship was disabled. Here, a distinction is made between the F_WD_Time being exceeded (F_WD_Time OUT) and an F_CRC error (see Figure 3-1).

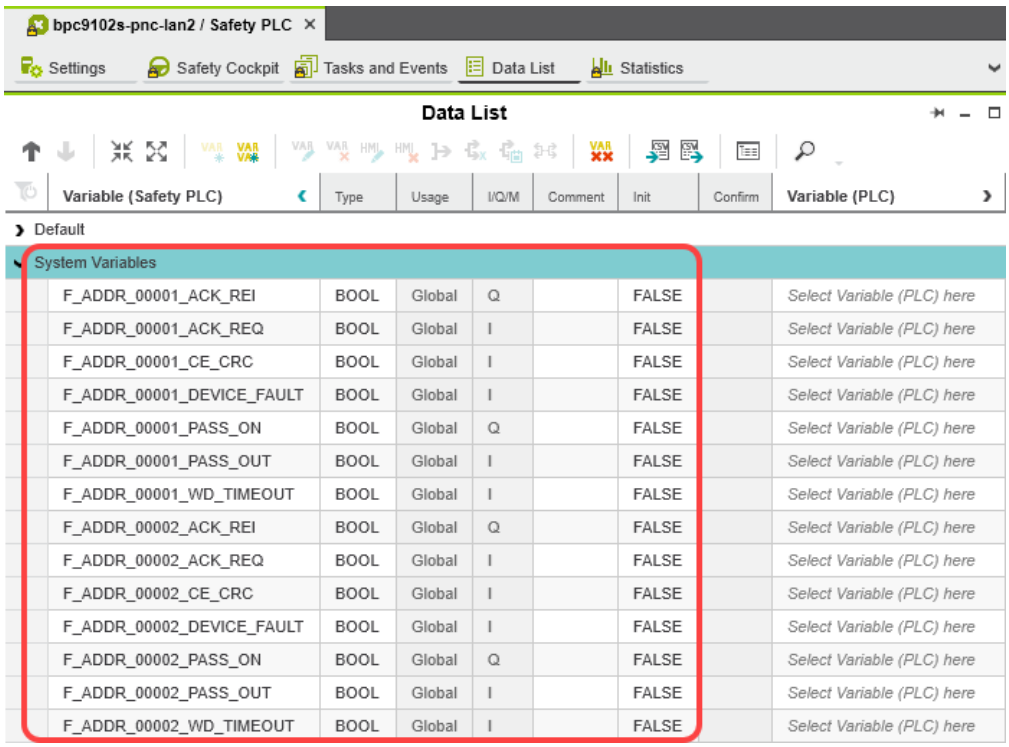


Figure 3-1 PROFIsafe: Management/diagnostic variables for communication diagnostics

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 SPLC 3000 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.

For further information on management/diagnostic variables, please refer to the sections 6.10.3 on page 108, 8.3.5 on page 151, and 8.3.6 on page 154.

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

– Local acknowledgment of individual communication errors
– Global acknowledgment of all communication errors
– Reintegration of F-Devices
– System diagnostics using global management/diagnostic variables
– Diagnostics/control of intelligent F-Devices

The following total maximum address area is available for exchange variables:

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

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

Also observe the information in section “Characteristic data of the SPLC 3000 safety-related controller” on page 192 regarding this.

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 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 65535_{dec}. It must be unique throughout the entire network.

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 BPC 9102S (SPLC 3000) receives a source address (F_Source_Add).

The value of the F_Source_Address must be between 0_{dec} and 65535_{dec} and must be unique throughout the entire network.

NOTE:
Please note that each F-Address assigned within a network must be unique and must not overlap with other addresses.

A maximum of 300 F-Devices can be connected to a BPC 9102S (SPLC 3000).

This results in the following maximum values:

– The sum of the safe input data (SI) may not exceed 24 kB (input user data and PROFIsafe backup data).
– The sum of the safe output data (SQ) may not exceed 24 kB (output user data and PROFIsafe backup data).

Also observe the information in section “Characteristic data of the SPLC 3000 safety-related controller” on page 192 regarding this.

3.3 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 3.3.1 on page 34).

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 3.3.2 on page 37).

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 3.3.3 on page 43).

3.3.1 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 BPC 9102S (SPLC 3000) 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 3-2). 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 184.

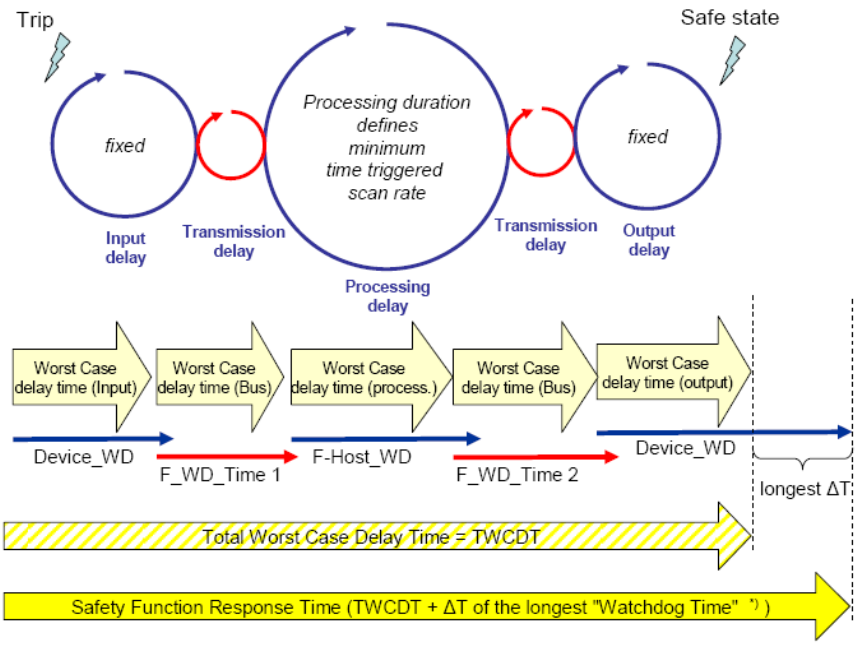


Figure 3-2 Calculation of the SFRT response time
(*) = Not necessarily the output device

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)
– SPLC 3000.

Due to a closely synchronized sequence of F-Host/SPLC 3000 processing, this model is simplified when using the BPC 9102S. The runtimes, cycle times, and watchdog times of the SPLC 3000 (processing delay and F-Host_WD) are not actually relevant when determining the SFRT.

The following figure illustrates the relationship:

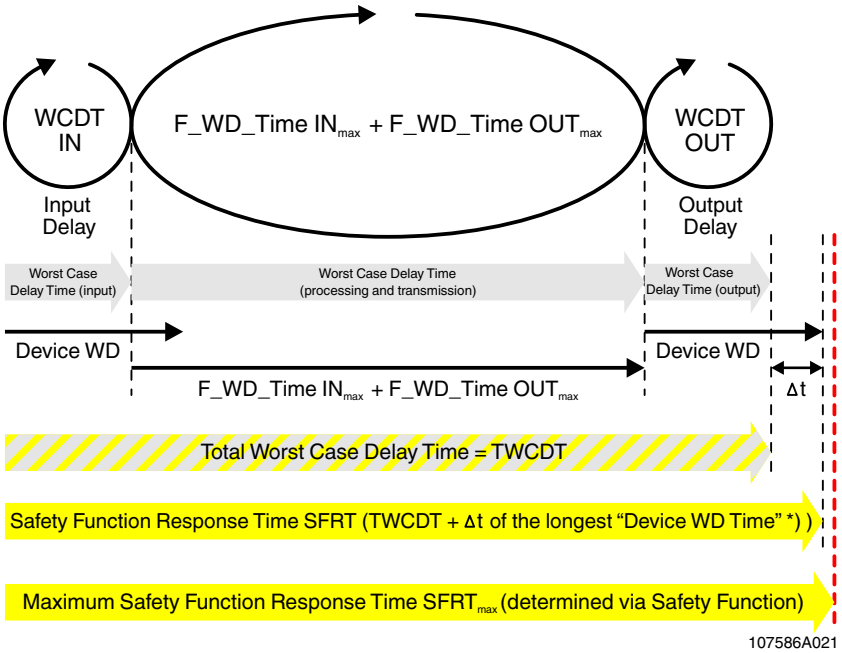


Figure 3-3 Simplified calculation of the SFRT response time
(*) = Not necessarily the output device

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 BPC 9102S (SPLC 3000) 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 so that SFRT$_{max}$ is not exceeded (see equation [2] page 36).
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 so that SFRT$_{max}$ is not exceeded (see equation [2] on page 36).
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 3-3 on page 35 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 SPLC 3000 in the BPC 9102S, 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 in accordance with the following equation:

$$\mathbf{SFRT = WCDT\ IN + (F\_WD\_Time\ IN_{max} + F\_WD\_Time\ OUT_{max}) + WCDT\ OUT} \quad [1]$$

SFRT must therefore be ≤ $\mathbf{SFRT_{max}}$

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

Always 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:

$$\mathbf{F\_WD\_Time\ IN_{max} + F\_WD\_Time\ OUT_{max} \leq SFRT_{max} - WCDT\ IN - WCDT\ OUT} \quad [2]$$

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 (Δ t) 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.

3.3.2 Determining F_WD_Time IN_{min}/F_WD_Time OUT_{min}

The F_WD_Time, which you as the user must determine in accordance with your application, is set in the PLCnext Engineer software (“Safety Parameters” editor, see Figure 6-33 on page 106). If the safety-related communication relationship has been established between the partners, monitoring is performed independently by both F-Host (SPLC 3000) and F-Device to ensure that the set F_WD_Time is observed during safety-related 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 to at least be able to establish safety-related communication via PROFIsafe 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 and PROFINET, item no. 3.192), please refer to Section “Documentation” on page 184.

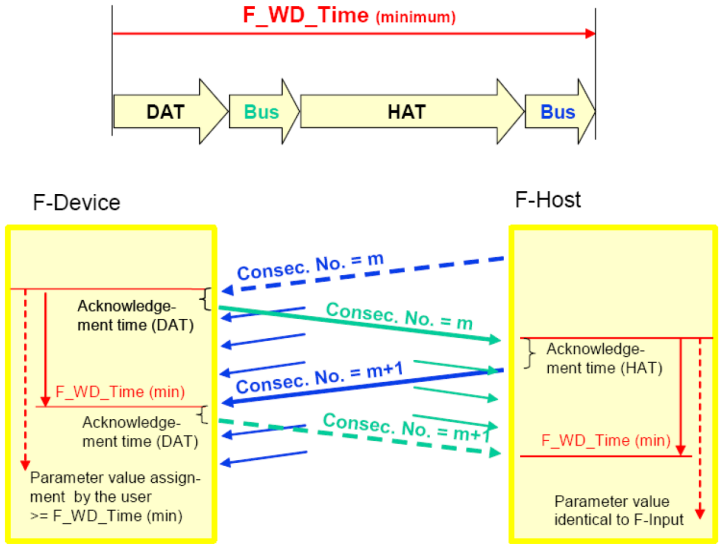


Figure 3-4 F_WD_Time (minimum)

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 SPLC 3000 (F-Host Acknowledge Time: T_{ZSPLC})

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 relationship is disconnected if no cyclic data has been transmitted in the specified time (see Figure 3-5).
     In the following example, the setting “Symmetric” has been selected for the “Timing”. An adjustment of the values may be necessary if the setting “Asymmetric” is selected.

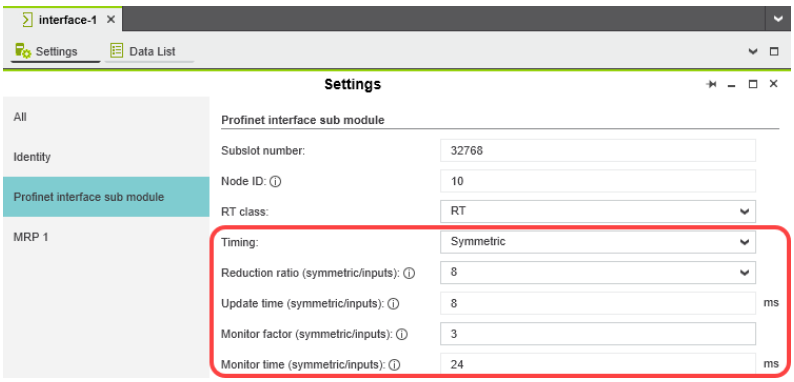


Figure 3-5 “Settings” editor of the interface editor group of the PROFINET device (settings of the AXL F BK PN TPS PROFINET bus coupler)

   - Relevant runtime components in bus heads (bus coupler or BPC 9102S) 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 BPC 9102S
   - The internal runtime of the BPC 9102S, which is to be taken into consideration in the “Bus” value, is equivalent to one SPLC 3000 cycle (T_{ZSPLC})

HAT The cycle time of the SPLC 3000 (T_{ZSPLC}) can be estimated during the system/machine planning phase using the diagram in Figure 3-6. Here, an application program that grows in proportion to the number of F-Devices is taken into consideration.

The cycle time of the SPLC 3000 is marginally dependent on the size of the safe application program (SPLC 3000 program runtime), the amount of safe process data, and the number of non-safe exchange variables for the standard controller.

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

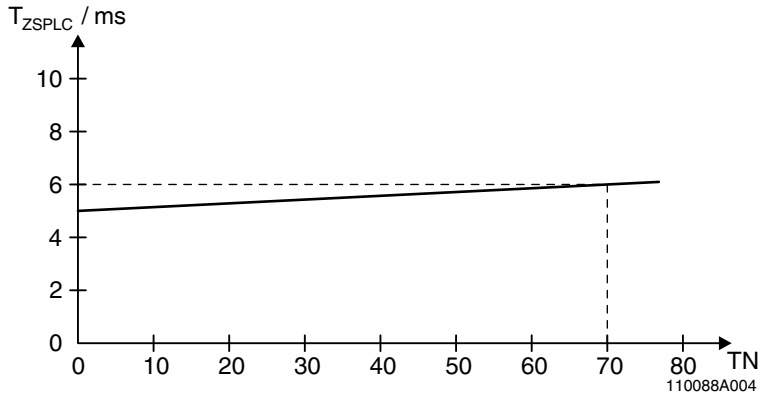


Figure 3-6 Cycle time of the SPLC 3000 (T_{ZSPLC})

Key:

T_{ZSPLC}	Cycle time of the SPLC 3000 [in milliseconds]
TN	Number of F-Devices in the application

You must verify the value of the SPLC 3000 cycle time roughly determined during the planning phase. Therefore, during the commissioning phase, take into account the value of the SPLC 3000 cycle time actually achieved.

If the PLCnext Engineer software is connected online with the SPLC 3000 and the PLCnext Control, the cycle time and the program runtime of the SPLC 3000 will be displayed there with the following two system variables (see Section “SPNS system variable” on page 143):

- Cycle time: CYCLE_TIME
- Program runtime: EXEC_TIME

To learn how you can access the SPLC 3000 online with the PLCnext Engineer software, refer to sections “Transferring projects to the BPC 9102S and displaying online values” on page 118 and “SPNS system variable” on page 143 as well as to the software online help function.

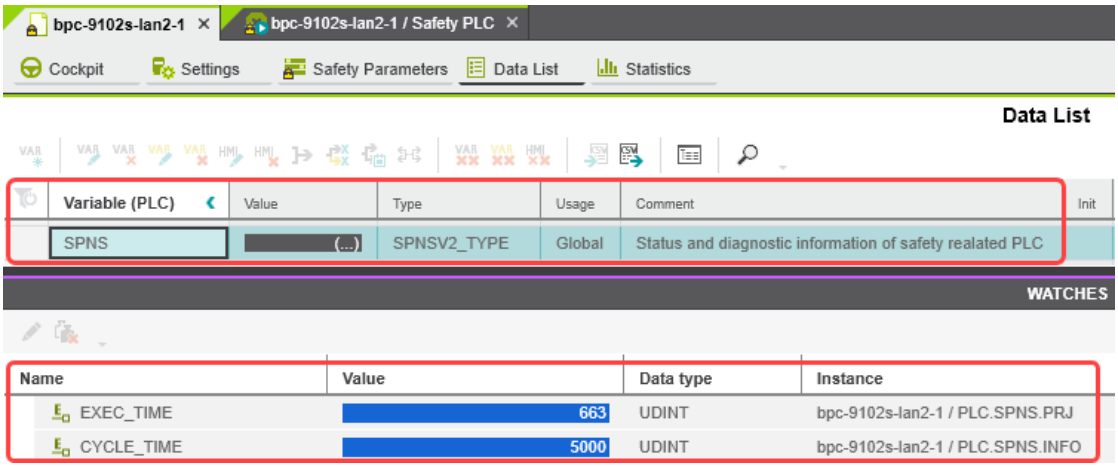


Figure 3-7 Online values of the SPLC 3000 cycle time and program runtime

The SPLC 3000 cycle time is also displayed in the “Safety Cockpit” editor:

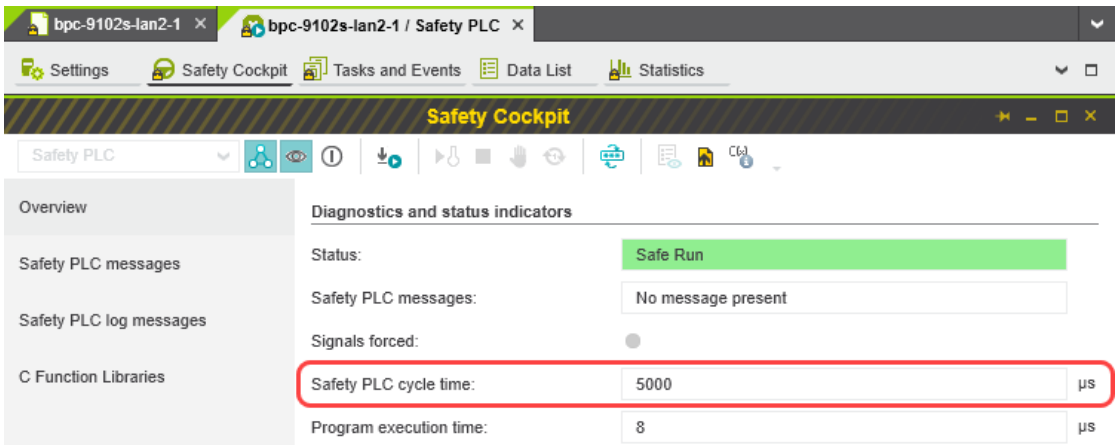


Figure 3-8 PLCnext Engineer: “Safety PLC cycle time”

Based on the actual determined value of the SPLC 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 3.3.1 on page 34).

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

$F\_WD\_Time_{min}$ > DAT + 2 x Bus + HAT **[3]**

Since the SPLC 3000 cycle and the PROFINET cycle run asynchronously with one another, the SPLC 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 x (external bus runtime + internal bus runtime) + HAT

$F\_WD\_Time_{min}$ > DAT + 2 x (external bus runtime + T_{ZSPLC}) + T_{ZSPLC}

$F\_WD\_Time_{min}$ > DAT + 2 x external bus runtime + 3 x T_{ZSPLC} **[4]**

For the example configuration in section 6.3.1 on page 76, 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_{ZSPLC}	=	5 ms	Cycle time of the safety-related controller (here: SPLC 3000)
T_{ZPNIO}	=	8 ms x 3	Monitor time: PROFINET update time x monitor factor (see Figure 3-5 on page 38).
$T_{D\ AXL\ F\ BK\ PN\ TPS}$	=	1 ms	Update rate of the 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	Processing time of the AXL F PSDO8/3 1F

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

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

$T_{Bus} = 25\ ms$

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 TPS) 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].

$F\_WD\_Time\ OUT_{min} = DAT + 2 \times external\ bus\ runtime + 3 \times T_{ZSPLC}$

$F\_WD\_Time\ OUT_{min} = 1.5\ ms + 2 \times 25\ ms + 3 \times 5\ ms$

$F\_WD\_Time\ OUT_{min} = 66.5\ ms$

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:

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

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

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

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

$$F\_WD\_Time\ OUT_{min} = 1.5\ ms + 2 \times 4\ ms + 3 \times 5\ ms$$

$$F\_WD\_Time\ OUT_{min} = 24.5\ ms$$

3.3.3 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:

$$(\text{F\_WD\_Time IN}_{min} + \text{F\_WD\_Time OUT}_{min}) < (\text{F\_WD\_Time IN} + \text{F\_WD\_Time OUT}) < (\text{F\_WD\_Time IN}_{max} + \text{F\_WD\_Time OUT}_{max})$$

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 3.3.2 on page 37.

Example

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

$\text{F\_WD\_Time IN}_{max} + \text{F\_WD\_Time OUT}_{max} = 200$ ms	(Upper limit from the safety function)
$\text{F\_WD\_Time OUT}_{min} = 24.5$ ms	(From the example in Section 3.3.2)
$\text{F\_WD\_Time IN}_{min} = 50$ ms	(Assumed for the example calculation)

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

F_WD_Time OUT ≈ 2 x 24.5 ms ⇒ F_WD_Time OUT = 50 ms

F_WD_Time IN = 2 x 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 6-33 on page 106) described in Section 6.3.1 are within the permissible range:

Minimum F_WD_Time (IN+OUT) < F_WD_Time (IN+OUT) to be parameterized < 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.

3.4 Possible fields of application of the BPC 9102S

Information on the possible fields of application of the SPLC 3000 can be found in Section “Example: The SPLC 3000 integrated into the BPC 9102S as the F-Host for Axioline F F-Devices” on page 76.

3.5 Components of the BPC 9102S

3.5.1 Connection and operating elements, test marks, and security seals

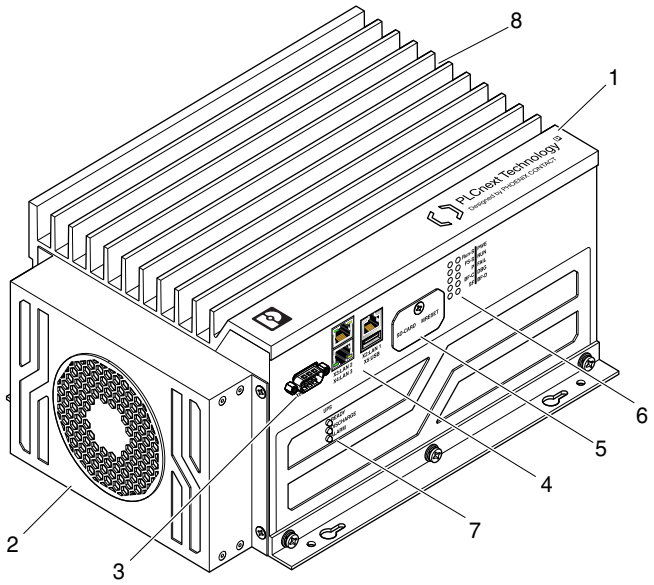


Figure 3-9 Connection and operating elements as well as test marks and security seals of the BPC 9102S

Key:

1 BPC 9102S

2 BPC 9102 FAN KIT fan kit (optional); see Section 3.6

3 COM service interface (D-SUB 9 pin strip)
Observe the ESD note on the cover in Section 2.3.

4
- LAN1/LAN2/LAN3 Ethernet interfaces (RJ45 jacks; 10/100/1000 Mbps)
- USB service interface (USB 3.0 type A socket)

5 Cover of the:
- SC card holder (slot for the configuration memory)
- MRESET button

6 Diagnostics and status indicators (LED)

7 Status LEDs of the device-internal UPS

8 Connection for external supply voltage (24 V DC)

9 Security seals (on all housing screws)

10 On the unillustrated side of the BPC 9102S, right alongside the LEDs:

– Test marks and revision statuses (hardware/firmware) of the safety-related SPLC 3000 controller (yellow label)

11 On the unillustrated side of the BPC 9102S:

– 2 labels with revision statuses (hardware/firmware) of the standard controller, MAC addresses and serial number of the BPC 9102S, UUID for connection to the PROFICLOUD, as well as the administrator password for user authentication[1]

[1] The following access data with administrator rights is preset in the BPC 9102S in the delivery state:

– User name: admin

– Password: printed on the BPC 9102S label

For information on user authentication, refer to Section 6.5.5.

3.6 BPC 9102 FAN KIT fan kit (optional)

The BPC 9102 FAN KIT fan kit is not included in the BPC 9102S scope of delivery. It is available as an accessory. The ordering data is listed in Section “Accessories” on page 183.

The fan kit is used for improving reliability in operating temperatures expected to be in the range of 50°C and 60°C.

The fan kit is affixed to the BPC 9102S using four screws.

The supply voltage of the fan kit is added to the BPC 9102S via a connection to be plugged in by the user.

The fan kit is controlled via the BPC 9102S PLCnext firmware.

Information on mounting the fan kit is listed in Section 4.2.

NOTE: Potential malfunction of the BPC 9102S

The fan kit may not be mounted or removed when the BPC 9102S is in operation.

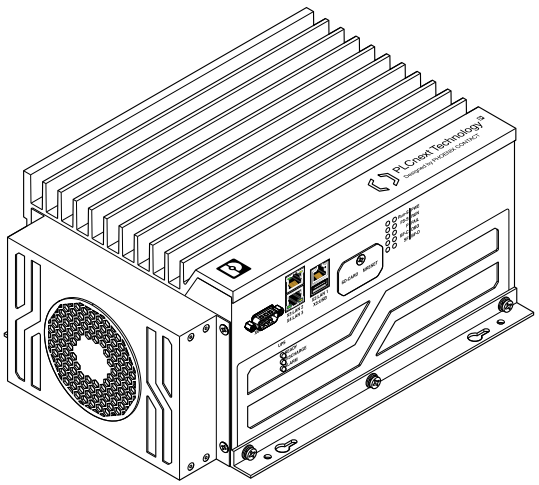


Figure 3-10 BPC 9102S with BPC 9102 FAN KIT fan kit

3.7 Diagnostics and status indicators

The diagnostics and status indicators provide information on the operating states of the BPC 9102S. Moreover, the LEDs enable rapid on-site error diagnostics.

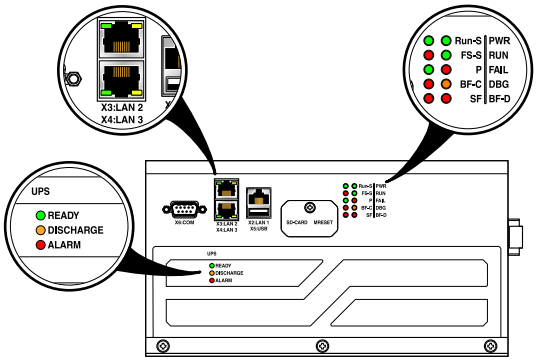


Figure 3-11 Diagnostics and status indicators

Table 3-1 Diagnostics and status indicators

Designation	Color	Meaning	Status	Description
Run-S	Green	Operating state of the safe application program	On	Cyclical processing of the safety-related application program has started.
			Off	Cyclical processing of the safety-related application program has stopped.
FS-S	Red	Failure state: Safe state of the SPLC 3000	On	A critical error has occurred and been detected. The SPLC 3000 has switched to the safe state (failure state).
			Flashing (1 Hz)	This can indicate: – Initialization phase is running (firmware boot process with power-on self-test; loading parameterization and configuration data from the configuration memory; booting the safe application program) – Initialization phase has been aborted with an error – Error-free BPC 9102S debug mode
			Off	Error-free operating state of the SPLC 3000 with supply voltage present
P	Green	–	–	The function of the P LED is not currently supported.

Table 3-1 Diagnostics and status indicators

Designation	Color	Meaning	Status	Description
BF-C	Red		On	No link status on the Ethernet port and/or no 100-Mbps transmission and/or no full duplex mode present.
			Flashing	Link status present; at least one configured PROFINET device has no PROFINET communication connection
			Off	The PROFINET controller has established an active communication connection to each configured PROFINET device.
SF	Red	Group error (PROFINET)	On	Group error message: At least one diagnostic alarm is present.
			Off	No group error messages. No diagnostic alarms.
PWR	Green	Supply voltage	On	24 V supply voltage feed-in is available.
			Off	24 V supply voltage feed-in is not available or too low.
RUN	Green	Operating state of the BPC 9102S (standard controller)	On	The PLCnext runtime system has initialized successfully and an application program is running. The BPC 9102S is in the RUN state.
			Flashing (0.5 Hz)	PLCnext runtime system successfully initialized. The BPC 9102S is in the READY/STOP state. The application program is not being processed.
			Flashing (2 Hz)	The BPC 9102S will be reset to the delivery state (see Section “MRESET button” on page 53 for this).
			Flashing (2 Hz)	System watchdog was triggered. FAIL flashes red with the same frequency.
			Off	PLCnext runtime system not ready to operate.
FAIL	Red	Failure	On	A runtime error has occurred in the application program of the PLCnext runtime system.
			Flashing (2 Hz)	System watchdog was triggered. RUN flashes green at the same frequency.
			Off	A runtime error has not occurred in the application program of the PLCnext runtime system.
DBG	Yellow	Debug mode (troubleshooting)	On	Non-safe debug mode active. The PLCnext runtime system/the standard controller is in debug mode, i.e., debug mode has been activated in PLCnext Engineer (breakpoint(s) set). The status of the RUN LED is not affected.
			Off	Non-safe debug mode inactive.

Table 3-1 Diagnostics and status indicators

Designation	Color	Meaning	Status	Description
BF-D	Red	Status of PROFINET communication/communication error	On	No link status on the Ethernet port or no transmission or no full duplex mode present.
			Flashing	Link status present; no PROFINET communication connection to the PROFINET controller
			Off	A PROFINET controller has established an active communication connection to the BPC 9102S PROFINET device

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.

LED indicators of the device-internal UPS

Table 3-2 LED indicators of the device-internal UPS

Designation	Color	Meaning	Status	Description
READY	Green	Status of the device-internal UPS	On	The supply voltage is present and the UPS is fully charged.
			Off	No voltage or incorrect voltage.
DISCHARGE	Yellow		On	Operation in battery mode.
			Off	Operation with supply voltage.
ALARM	Red		On	UPS failure; operation with supply voltage.
			Off	Operation with supply voltage.

LED indicators of the Ethernet interfaces

Table 3-3 LED indicators of the Ethernet interfaces

Designation	Color	Meaning	Status	Description
	Green	Link status	On	Connection established successfully (link): The BPC 9102S is able to contact another network device.
			Off	Connection not established successfully.
	Yellow	Activity status	On/flashing	Data transmission active (activity): The Ethernet interface is sending or receiving data.
			Off	Data transmission not active.

3.8 Interfaces

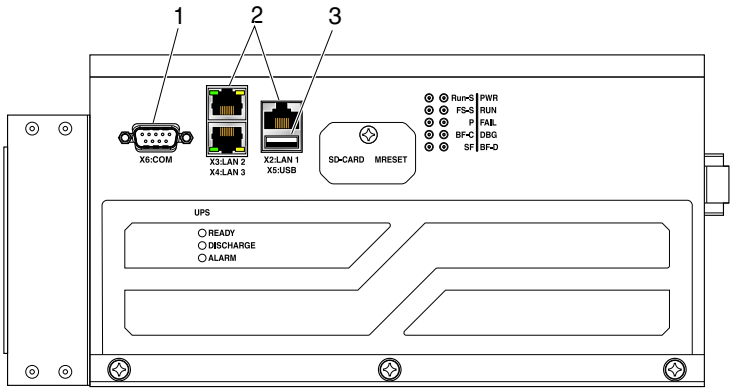


Figure 3-12 Interfaces of the BPC 9102S

The BPC 9102S is equipped with the following interfaces:

Table 3-4 Interfaces of the BPC 9102S

Pos.	Interfaces		Description
1	COM	RS-232	Service interface (reserved internally): D-SUB 9 pin strip (serial, RS-232)
2	LAN1	3x Ethernet	Ethernet: 1 Gbps or 2.5 Gbps
	LAN2		PROFINET: Controller interfaces function (max. 1 Gbps)
	LAN3		PROFINET: Device interfaces function (max. 1 Gbps)
3	USB		Service interface (reserved internally): USB 3.0 socket (type A)

3.8.1 Ethernet connection

Three standardized Ethernet interfaces are available for connecting the Ethernet network. The BPC 9102S can communicate via a Base-T Ethernet network via the three RJ45 interfaces. The LAN interfaces have specific purposes and speeds (see Table 3-4).

The LAN1, LAN2, and LAN3 interfaces are each assigned a separate MAC address.

LAN 1 can be used as an Ethernet interface for TCP/IP communication, for example. LAN2 is preconfigured as the PROFINET controller interface. LAN3 is preconfigured as the PROFINET device interface.

More detailed information on the interfaces:

IP address assignment: Section “BPC 9102S IP settings: General” on page 84.

The Ethernet network is connected via an RJ45 jack.

Use Ethernet cables in accordance with CAT5 of IEEE 802.3 up to 100 Mbps.

Please note that for operation with 1,000 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 Assembling Guideline
– 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 184).

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 Section "Ethernet interfaces".

3.8.2 Connection example of the Ethernet interfaces

At present, the BPC 9102S supports the following connection in a PROFINET system.

In the following example, the BPC 9102S 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 interface. To operate the BPC 9102S as a PROFINET controller, PROFINET devices are connected to the LAN2 interface (see Figure 3-13).

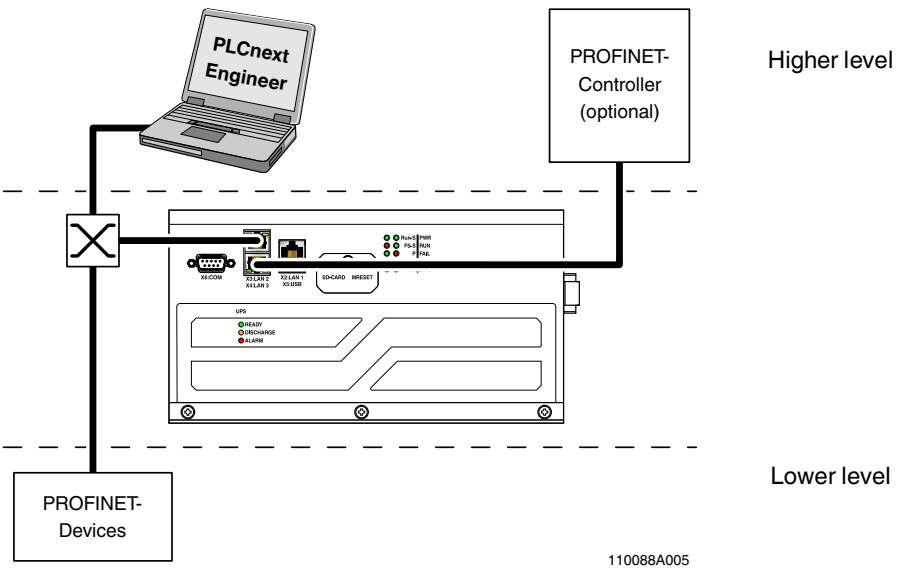


Figure 3-13 PROFINET example installation

In principle, one PC can be operated on each Ethernet interface of the BPC 9102S. Depending on the configuration of the interfaces, this may not be possible in individual cases (see Section “Ethernet connection” on page 50).

Please note:

– The IP addresses of interfaces LAN1/LAN2/LAN3 must be in different subnets.
– The PROFINET controller function of the BPC 9102S is available at interface LAN2. 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 the LAN3 interface if you want to use the PROFINET device function of the BPC 9102S on these interfaces.
– The LAN1 and LAN3 interfaces do not necessarily have to be assigned an IP address if, for example, communication between a PC with PLCnext Engineer and the BPC 9102S is also implemented via the LAN2 interface.
  We recommend that appropriate IP addresses be assigned to all interfaces.

3.8.3 USB service interface

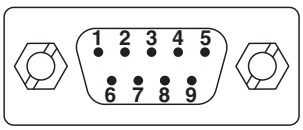
The USB interface (USB 3.0 socket, type A) is reserved for internal service purposes.

3.8.4 COM service interface (serial, RS-232)

The COM interface (D-SUB 9 pin strip) is reserved for internal service purposes.

Table 3-5 D-SUB 9 pin strip pin assignment

D-SUB 9 pin	RS-232
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	Wake-on-ring



3.9 SD card holder and MRESET button

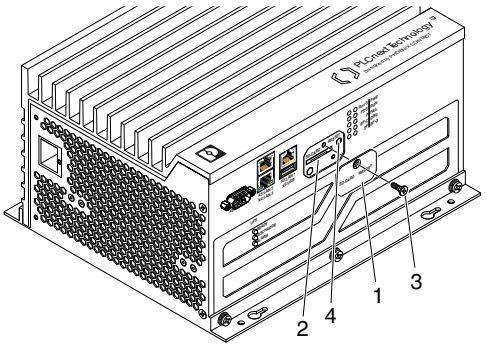


Figure 3-14 SD card holder (2) and MRESET button (4)

Key:

1 Cover
2 SC card holder (slot for the configuration memory)
3 Screw
4 MRESET button

3.9.1 SD card holder

The BPC 9102S has an SD card holder with push-pull technology. The SD card holder is located under the side cover of the BPC 9102S.

3.9.2 MRESET button

The MRESET button is located under the side cover of the BPC 9102S. The button can only be pressed with a pointed object (such as a pen).

Using the MRESET button will delete the application program in the BPC 9102S main memory and the retain data.

Procedure:

- To actuate the MRESET button (4), remove the screw (3) in the cover (1) with a Torx® TX 10 screwdriver (ordering data listed in Section 14.1.3, “Accessories”).
- Then swivel the cover (1) to the side so that you can easily access the MRESET button (4).
- To delete the application program and the retain data, actuate the MRESET button in the following sequence:
  - Press and hold down the button for three seconds.
  - Release the button for less than three seconds.
  - Press and hold down the button for three seconds.
- Re-affix the cover (1) after actuating the MRESET button by tightening the screw (3) to protect the MRESET button against accidental damage or actuation.

3.10 Licensing information on Open source software

The BPC 9102S uses a Linux operating system.
License information for the individual Linux packages can be found in the file system of the BPC 9102S under the path:

/usr/share/common-licenses

Information on the directory structure of the file system can be found in Section 3.12 on page 54.

Alternatively, you can also call up the license information via the Web-based management system of the BPC 9102S (see Section 9).

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).

3.11 Requesting the source code

This BPC 9102S 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 BPC 9102S.

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 BPC 9102S

3.12 Directory structure of the file system

The BPC 9102S works with a Linux operating system. You can access the BPC 9102S via SFTP or via SSH and view the directories and files on the file system (on the internal configuration memory and on the optional SD card) and modify them as necessary.

Information on the directory structure of the file system is available in the PLCnext Technology Info Center.

3.13 Using SFTP to access the file system

The file system (on the internal configuration memory and on the SD card of the BPC 9102S) is accessed via the SFTP protocol. An 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 with 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 the Web-based management system of the BPC 9102S via the User Manager.

In the event that you do not want to use SFTP accesses, we recommend blocking the respective port in the firewall.

Further information is available in the PLCnext Info Center.

In the delivery state, the following access data with administrator rights is preset:

User name: admin

Password: Printed on the BPC 9102S (see Figure 3-9 on page 44).

3.14 Firewall

The firewall of the BPC 9102S is deactivated by default.

Recommended:

- Activate the firewall.

Please note:

If you use the BPC 9102S 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.

Information on the firewall and an abstract of the most important open ports are available in the PLCnext Technology Info Center in the section Security under Firewall, and also directly via the following link: PLCnext Info Center.

4 Mounting hardware

4.1 Safety notes

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) in accordance with EN 61340-5-1 and IEC 61340-5-1.

WARNING: Unintentional machine startup

- Do not mount or remove the BPC 9102S while the power is connected.
- Ensure power cannot be switched on again.
- Make sure the entire system is reassembled before switching the power back on. Observe the diagnostic indicators and any diagnostic messages.

Starting the machine/system may only occur if the device does not pose a hazard.

Observe the PROFINET Assembling Guideline

Observe the PROFINET Assembling Guideline when mounting and installing the BPC 9102S.

Observe the corresponding information in the Assembling Guideline and in the “Functional Bonding 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.

Shielding

The shielding ground of the connected twisted pair cables is electrically connected to the RJ45 jack of the BPC 9102S. 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.

– Make sure that 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 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.

4.2 Mounting the BPC 9102 FAN KIT fan kit

If you want to operate the BPC 9102S with the BPC 9102 FAN KIT fan kit (optional; ordering data available in Section 14.1.3, “Accessories”), mount the fan kit in accordance with the following steps.

NOTE: Potential malfunction of the BPC 9102S

The fan kit may not be mounted when the BPC 9102S is in operation.

- Switch off the BPC 9102S power supply before mounting the fan kit.

Please note:

Use a Torx® TX 10 screwdriver (ordering data is available in Section 14.1.3, “Accessories”) to remove and tighten the screws in the following section.

1. Remove the cover plate over the socket for the power plug (pos. 2 in Figure 4-1).
2. Align the fan kit (pos. 1 in Figure 4-1) on the end of the BPC 9102S.
3. Align the power plug on the rear of the fan kit with the socket (pos. 2 in Figure 4-1) on the underside of the BPC 9102S.

   Push the power plug into the socket until it snaps into place.
4. Secure the fan kit using the four M4 screws (pos. 3 in Figure 4-1) included in the BPC 9102 FAN KIT scope of delivery.
5. Tighten all four screws equally with a tightening torque of 5 Nm so that they cannot loosen accidentally (e.g., due to vibrations).

When switching on the BPC 9102S power supply, the fan kit will also be supplied with power.

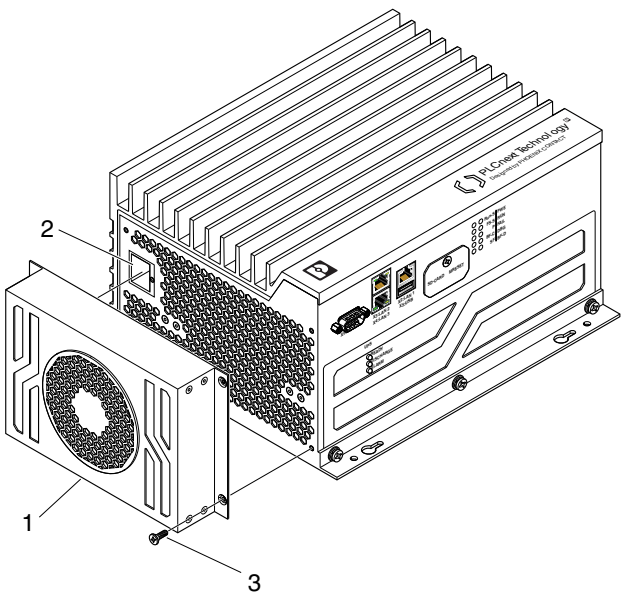


Figure 4-1 Mounting the BPC 9102 FAN KIT fan kit

4.3 Basic information

Mounting location

The BPC 9102S meets the IP20 degree of protection.

- Mount the BPC 9102S in the lockable control cabinet or lockable control box (standard junction box) with IP54 degree of protection or higher.

Mounting

The BPC 9102S must be mounted on a level mounting surface (mounting wall).

Supply connector

The BPC 9102S has a supply connector for connecting the power supply.

For additional information, please refer to Section 5.2.2.

Mounting position

- Mount the BPC 9102S on the mounting surface in the vertical position as standard. The connection for the supply voltage must be located at the top of the device.

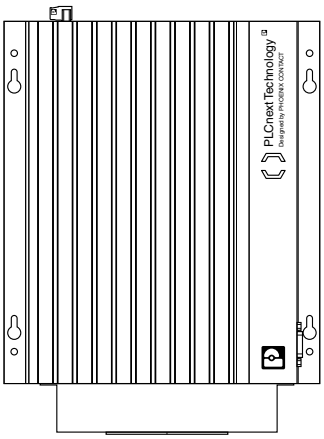


Figure 4-2 Mounting position of the BPC 9102S

4.4 Mounting the BPC 9102S

- Remove power from the BPC 9102S.

Please note:
Before you can mount the BPC 9102S, you must:
– Remove the BPC 9102S supply connector if required.
– Mount the BPC 9102 FAN KIT fan kit on the BPC 9102S if required.
Follow the descriptions listed in this section.

NOTE: The BPC 9102S can overheat – keep vents clear
When installing the BPC 9102S, ensure that the vents can be freely accessed. Otherwise, the BPC 9102S may overheat. To ensure good ventilation, leave a gap of more than 10 cm above and below the BPC 9102S.
Do not install devices below the BPC 9102S that could additionally heat the BPC 9102S up.

When installing the BPC 9102S in a control cabinet:
- Verify clearances within the control cabinet. As a general rule, leave at least 10 cm clear on each side to ensure correct cooling and access to the connections.
- Drill all holes on the mounting surface and tap any threads necessary before beginning installation.
  Be sure to protect previously installed components from shavings during this procedure.
– Supporting parts must be at least 1.9 mm thick to ensure sufficient support.
- Mount the BPC 9102S on a vibration-free mounting surface.
– The mounting brackets on the BPC 9102S housing are equipped with keyhole-shaped mounting holes.
- Mount the BPC 9102S using the keyhole-shaped mounting holes in a vertical mounting position (see Figure 4-3 on page 62).
– The mounting holes can accommodate bolts with a diameter of up to 4 mm.
- Obtain suitable fastening material for on-site mounting before you begin mounting.
- Use fastening material suitable for the mounting surface and affix the device securely to the mounting surface. Ensure that the fastening material is positioned in the thin end of the mounting holes.

If you want to operate the BPC 9102S with the BPC 9102 FAN KIT fan kit (item no. 1290834), you must first mount the fan kit before mounting the BPC 9102S on the mounting surface. To do this, follow the instructions in Section “Mounting the BPC 9102 FAN KIT fan kit” on page 58.

WARNING: Unintentional machine startup

- Do not mount or remove the BPC 9102S while the power is connected.
- Ensure power cannot be switched on again.
- Make sure the entire system is reassembled before switching the power back on. Observe the diagnostic indicators and any diagnostic messages.

Starting the machine/system may only occur if the device does not pose a hazard.

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 your 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

Observe these notes to prevent unexpected machine startup after operator acceptance via the “Operator Acknowledgment” command.

Installation

If suitable fastening material is available, perform the following steps taking the above notes into consideration:

- Use the BPC 9102S as a template and mark the positions of the mounting holes on the mounting surface. Alternatively, use a true-to-scale version of the template in Figure 4-3.
- Drill all holes.
- Mount the fastening material on the mounting surface just tightly enough to hold the BPC 9102S in place.
- Hang the BPC 9102S onto the fastening material on the mounting surface in accordance with the orientation in Figure 4-3.

  Ensure that the fastening material is positioned in the narrow sections of the mounting holes.
- Secure the BPC 9102S on the mounting surface against falling off by tightening the fastening material.

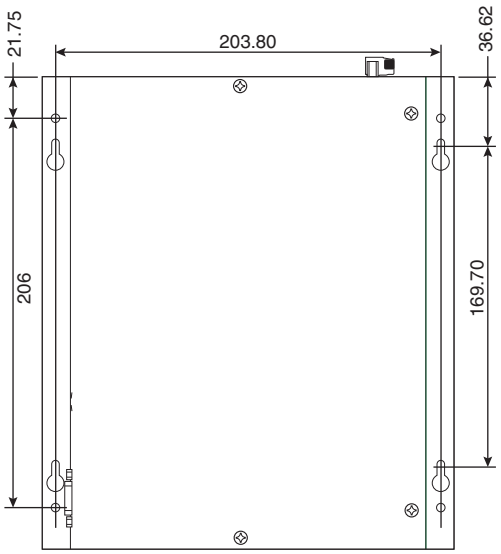


Figure 4-3 Template for wall mounting

4.5 Inserting the SD card (configuration memory)

NOTE:

– Please note that the SD card may not be inserted during operation. If the SD card is inserted during operation, the BPC 9102S will switch to the safe state (failure state).

• Always disconnect the power supply to the BPC 9102S before inserting the SD card.

– Observe Section “Notes on security” on page 15, in particular in terms of access protection for the SD card.

The SD card is recognized during initialization of the BPC 9102S. Make sure that the SD card has been inserted before switching on the BPC 9102S to enable the device to use it.

NOTE: SD card (configuration 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 of the BPC 9102S.

Figure 4-4 is a graphical representation of how to insert the SD card.

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

- To insert the SD card, remove the screw (3) in the cover (2) using a Torx® TX 10 screwdriver (ordering data is available in Section 14.1.3, “Accessories”).
- Then swivel the cover (2) to the side so that you can easily access the SD card holder (1).
- Insert the SD card with the contact strip to the front into the slot provided (see Figure 4-4, B).
- Gently push the SD card into the SD card holder until it engages with a click in the SD card holder.

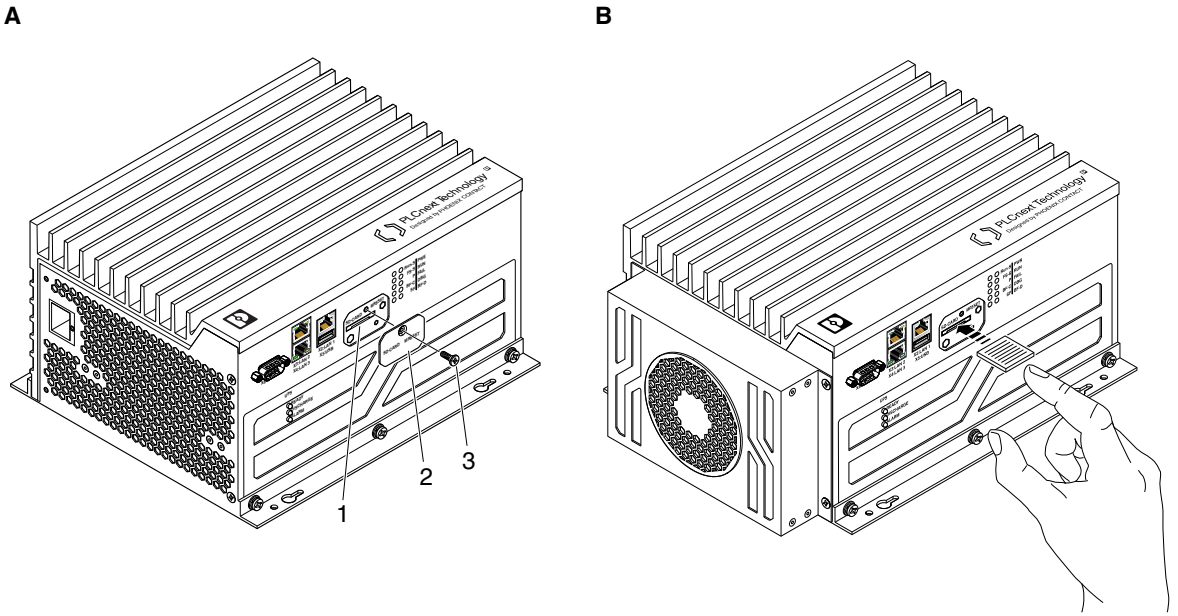


Figure 4-4 Inserting the SD card (configuration memory)

- Re-affix the cover (2) after inserting the SD card by tightening the screw (3) to protect the SD card slot against accidental damage or actuation.

4.6 Connecting the interfaces

4.6.1 Connecting an Ethernet network

- Connect the Ethernet cable to the Ethernet interface (RJ45 jacks: LAN1, LAN2, or LAN3) on the BPC 9102S.

The cable connects the BPC 9102S to a higher-level or lower-level Ethernet network.

- Use Ethernet cables in accordance with CAT5 of IEEE 802.3 for operation with up to 100 Mbps. (LAN1, LAN2, LAN3)
- For operation with 1,000 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, LAN3)

Observe the information on the Ethernet interfaces of the device in Section “Ethernet connection” on page 50

For the ordering data for the Ethernet cable, please refer to Section “Ordering data” on page 183.

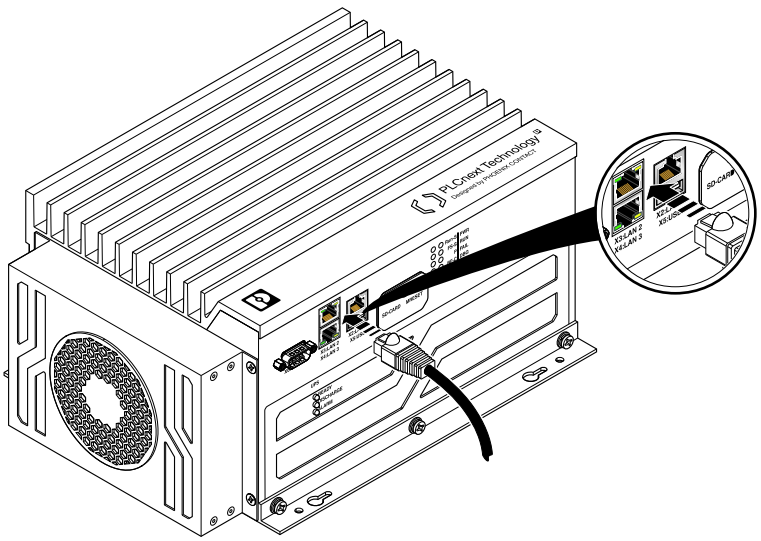


Figure 4-5 Cabling between an Ethernet network and the BPC 9102S

4.6.2 Connecting the COM service interface (reserved internally)

- Connect an appropriate cable with a D-SUB 9 female strip to the BPC 9102S COM service interface.

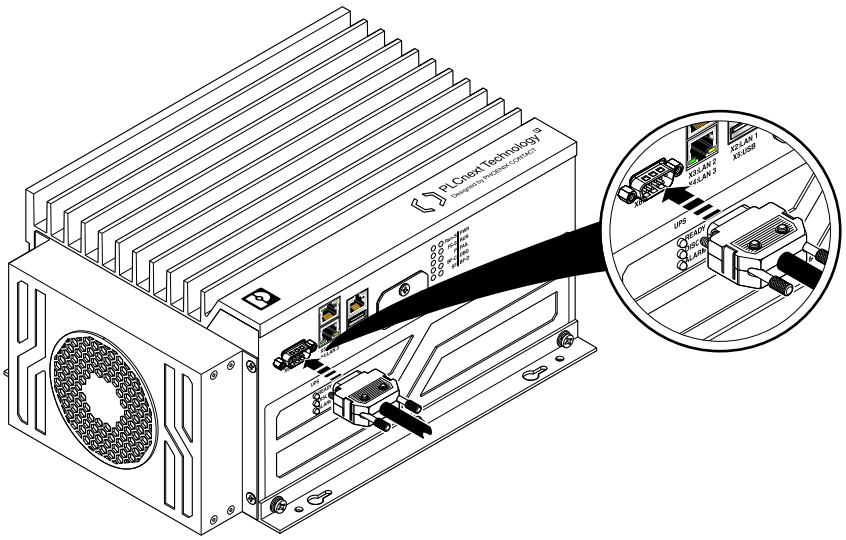


Figure 4-6 Cabling between an Ethernet network and the BPC 9102S

5 Connecting and wiring the hardware

5.1 Sizing of the power supply

Supply the BPC 9102S using external 24 V DC voltage sources. The permissible voltage range is 19.2 V DC to 30 V DC (ripple included).

- Select a power supply that is suitable for the currents in your application. The selection depends on the bus configuration and the resulting maximum currents.

WARNING: Loss of electrical safety when using unsuitable power supplies

The BPC 9102S 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 network (PROFINET and Axioline F) and the I/O devices used in it:

Only use power supplies that meet EN 61204-1 and feature safe isolation and PELV in accordance with IEC 61010-2-201. They prevent short circuits between the primary and secondary side.

Please also observe the information in Section “Electrical safety” on page 18.

A power supply without a **fall-back characteristic curve** must be used for correct operation of the BPC 9102S (see Figure 5-2).
When the BPC 9102S is switched on, an increased inrush current is temporarily triggered. The BPC 9102S 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 188.

Some electronically controlled power supplies have a fall-back characteristic curve (see Figure 5-1). These are not suitable for operation with capacitive loads.

The following power supply (without fall-back characteristic curve) is recommended for operating the BPC 9102S:

– Primary-switched QUINT POWER power supply with SFB technology:

  QUINT4-PS/1AC/24DC/20/+ Item number: 2904617

Other power supplies can be used as an alternative. For examples of suitable Phoenix Contact power supplies, please refer to “Accessories” on page 183.

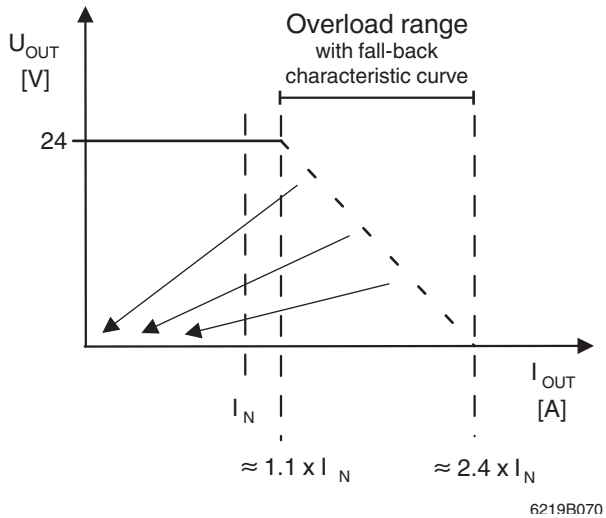


Figure 5-1 Overload range **with** fall-back characteristic curve

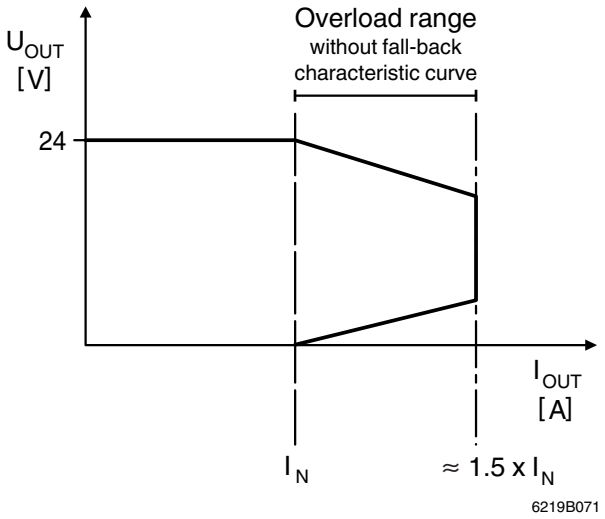


Figure 5-2 Overload range **without** fall-back characteristic curve

5.2 Supply voltage

5.2.1 DC distribution network in accordance with IEC 61326-3-1

A DC distribution network is a DC power supply network which 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 in accordance with IEC 61326-3-1.

When using a BPC 9102S in a DC distribution network, install appropriate surge protection (e.g., PT 2+1-S-48DC/FM, item no. 2817958) directly upstream of the device.

5.2.2 Connecting the supply voltage

A removable connector is provided on the BPC 9102S for connecting the supply voltage.

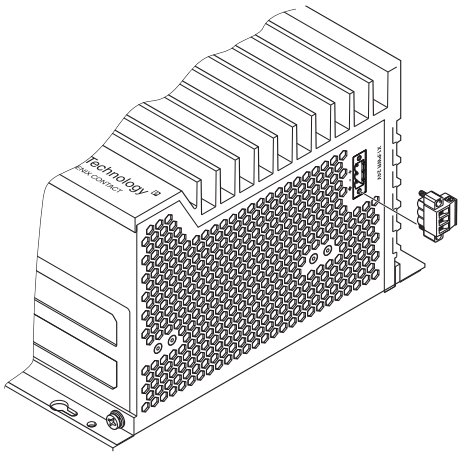


Figure 5-3 Connection of the supply voltage

- Connect the BPC 9102S to a 24 V DC power supply.
- Connect the supply voltage to the removable three-position COMBICON connector.
- Tighten the retaining screws for the conductors in the connector with a torque of 0.5 Nm.

Table 5-1 Connector pin assignment

Position	Assignment
⏚	Functional ground (FE)
–	0 V DC
+	24 V DC

NOTE:

The BPC 9102S utilizes an internal UPS. If the connection to the power supply is interrupted, the UPS will provide sufficient power to shut the system down safely. The UPS utilizes a capacitor for power backup. It is not accessible for service.

Please note that the BPC 9102S requires approximately two minutes to start up. This is due to the comprehensive self-tests the device must perform. During this process, the status is indicated via the LEDs.

6 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.

The PLCnext Engineer software is required for startup of the BPC 9102S.

The following topics are also available in the PLCnext Info Center:
- Configuring Axioline F modules
- Configuring PROFINET devices
- Programming with high-level languages such as C++
- Programming in accordance with IEC 61131-3
- Instantiating programs
- Assigning process data
- Specifying the refresh interval for Axioline F I/O data
- Creating a PLCnext Engineer HMI application

6.1 Initial commissioning

The following information for commissioning the BPC 9102S 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 BPC 9102S is commissioned immediately:
  - After switching on the supply voltage and subsequent successful startup, if an appropriate safety-related application program is available

  or
  - Once an appropriate safety-related application program has been downloaded from PLCnext Engineer.

  With appropriate safety-related programming, the safety function is active immediately after the startup phase of the SPLC 3000 and the outputs of the F-Devices and the outputs of the non-safety-related PROFINET devices and I/O participants can be set depending on the programming.

For initial commissioning, proceed as described in Table 6-1.

The following table describes all the steps from unpacking the BPC 9102S through mounting/installation to startup.

Table 6-1 Steps for initial startup of the BPC 9102S

Step	Relevant section and literature
Remove the device from the packaging while observing the ESD regulations.	Section “Safety notes” on page 57
Check that none of the seals on the housing screws are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered with. In this case, contact Phoenix Contact before using the device.	Section “Connection and operating elements, test marks, and security seals” on page 44
Mount the device in accordance with your application.	Section “Mounting hardware” on page 57
Insert the configuration memory (SD card).	Section “Inserting the SD card (configuration memory)” on page 62
Connect the device to an Ethernet network.	Section “Connecting an Ethernet network” on page 64
Connect the power supply to the device.	– Notes on using PELV power supplies in Section “Electrical safety” on page 18 – Section “Connecting the supply voltage” on page 68

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.

Switch on the power supply to the BPC 9102S.	**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.

Please note:
The BPC 9102S takes approximately 2 minutes to start up. This is due to the comprehensive self-tests the device must perform. The device LEDs indicate the status.

The following steps must be performed in the PLCnext Engineer software.

When carrying out the following steps, please refer to the software online help function. The online help function supports you during programming and configuration in PLCnext Engineer.

Carry out all the steps in order to integrate the device as a PROFINET controller in a PLCnext Engineer project.	– Online help for PLCnext Engineer – Section “Integration of the BPC 9102S as the PROFINET controller and the SPLC 3000 as the F-Host in PLCnext Engineer” on page 78
Assign the necessary IP address settings for your application to the device.	Section “Setting the IP address of the BPC 9102S (controller) in the project” on page 86

Table 6-1 Steps for initial startup of the BPC 9102S

Step	Relevant section and literature
Check the PROFINET controller settings and adapt the settings, if necessary.	
You can operate the BPC 9102S concurrently as a PROFINET controller and PROFINET device. Send your settings to the controller.	Section “BPC 9102S IP settings: General” on page 84
Create the bus configuration in PLCnext Engineer.	Section “Adding PROFINET devices” on page 90
Assign a PROFINET device name for the connected devices (device naming).	Section “Assigning online devices (device naming)” on page 91
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.	Section “Assigning/checking the PROFIsafe address (F-Address) of PROFIsafe devices” on page 104
Check the settings for management/diagnostic variables and adapt the settings if necessary.	– Section “Description of the safety-related functioning of the BPC 9102S” on page 30 – Section “Management/diagnostic variables for F-Devices” on page 108 – Section “Management/diagnostic variables for each configured F-Device” on page 151 – Section “Global management/diagnostic variables for F-Devices” on page 154
Specify a new project password.	Section “Defining a project password” on page 83
Create the variables for the devices for process data exchange.	– Section “Creating variables” on page 99 – Section “Creating safety-related variables” on page 112
Link the created variables to the process data in accordance with your application.	– Section “Assigning non-safety-related process data” on page 102 – Section “Assigning safety-related process data” on page 116

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 B, “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 104
Check the bus configuration and variable assignment (exchange variables).	
Specify a new controller password.	Section “Specifying the SPLC 3000 controller password” on page 120

Table 6-1 Steps for initial startup of the BPC 9102S

Step	Relevant section and literature
Carry out the validation using the checklist ""Initial commissioning" and "restart/device replacement" validation" on page 206.	Section "Appendix: Checklists" on page 197

NOTE: Unauthorized access to the SD card possible

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

Observe Section "Notes on security" on page 15, in particular in terms of access protection for the SD card.

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.

6.2 Recommissioning after replacing the BPC 9102S

The device does not have to be configured again following recommissioning after a replacement (see Table 6-1 "Steps for initial startup of the BPC 9102S").

If a configuration memory is inserted that contains the configuration project created for your application, the configuration is still available after successful startup of the BPC 9102S. 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).

For recommissioning after the device has been replaced, proceed as described in Table 6-2. Make sure that:

– The device to be replaced has been removed from the application in accordance with the instructions in Section "Removing the hardware" on page 165
– The configuration memory of the device to be replaced has been removed

Table 6-2 Steps for recommissioning the BPC 9102S

Step	Relevant section and literature
Remove the device from the packaging while observing the ESD regulations.	Section "Safety notes" on page 57
Check that none of the seals on the housing screws are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered with. In this case, contact Phoenix Contact before using the device.	Section "Connection and operating elements, test marks, and security seals" on page 44
Mount the device in accordance with your application.	Section "Mounting hardware" on page 57
Insert the previously used configuration memory (SD card) into the replacement device.	Section "Inserting the SD card (configuration memory)" on page 62
Connect the device to an Ethernet network.	Section "Connecting an Ethernet network" on page 64

Table 6-2 Steps for recommissioning the BPC 9102S

Step	Relevant section and literature
Connect the power supply to the device.	– Notes on using PELV power supplies in Section “Electrical safety” on page 18 – Section “Supply voltage” on page 68

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.

Switch on the power supply to the BPC 9102S.	**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 after the appropriate measures, which are specified in the validation plan of the machine/system for replacing the BPC 9102S, have been taken.

Please note:
The BPC 9102S takes approximately 2 minutes to start up. This is due to the comprehensive self-tests the device must perform. The device LEDs indicate the status.

Please note:
– If a configuration memory from the old device which contains the configuration created for your application is used, only carry out the safety-related steps.
– If a configuration 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 B, “Appendix: Checklists”.

Table 6-2 Steps for recommissioning the BPC 9102S

Step	Relevant section and literature
Carry out the validation using the checklist ""Initial commissioning" and "restart/device replacement" validation" on page 206.	Section "Appendix: Checklists" on page 197

NOTE: Unauthorized access to the SD card possible

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

Observe Section "Notes on security" on page 15, in particular in terms of access protection for the SD card.

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.

6.3 Example BPC 9102S commissioning

6.3.1 Example: The SPLC 3000 integrated into the BPC 9102S as the F-Host for Axioline F F-Devices

To make your introduction to working with the BPC 9102S as straightforward as possible, the descriptions in later sections are based on the following configuration.

The SPLC integrated into the BPC 9102S communicates as the F-Host via PROFINET/PROFIsafe with the safety-related Axioline F I/O modules.

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 configuration in Figure 6-1, two Axioline F bus couplers are coupled to the BPC 9102S PROFINET controller on a lower level. The two PROFINET devices are connected via a switch to the PROFINET controller LAN2 interface on the BPC 9102S.

Communication between the SPLC and the safety-related Axioline F I/O modules is via PROFINET/PROFIsafe via the respective Axioline F PROFINET bus coupler.

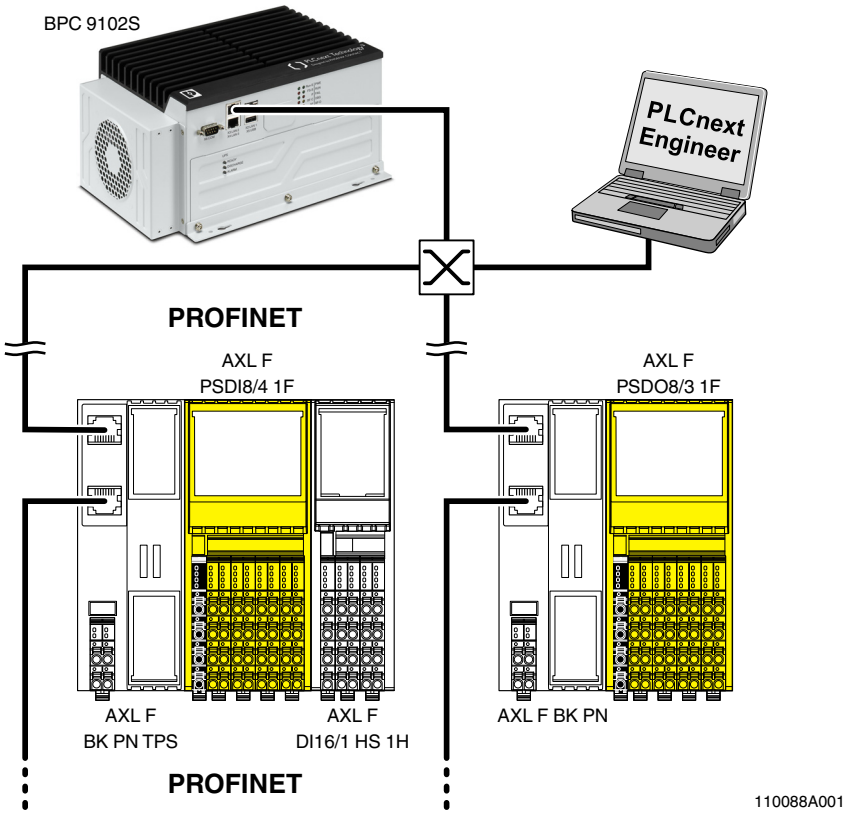


Figure 6-1 Example configuration: The SPLC 3000 integrated into the BPC 9102S as the F-Host with safety-related communication via PROFINET/PROFIsafe

6.3.2 Integration of the BPC 9102S as the PROFINET controller and the SPLC 3000 as the F-Host in PLCnext Engineer

The following sections describe how to:

- Create a new project in PLCnext Engineer (see Section 6.4.5)
- Assign IP-addresses to the BPC 9102S, e.g., to the PROFINET controller LAN2 interface (see Section 6.5.1 onward)
- Read in PROFINET and F-Devices connected to the BPC 9102S (see Section 6.6)
- Program a non-safety-related and a safety-related project in PLCnext Engineer, including creating and linking variables (see Section 6.7 and Section 6.10)
- Configure F-Devices in PLCnext Engineer (see Section 6.10.1 and Section 6.10.2)
- Download the non-safety-related project and the safety-related project to the BPC 9102S and initiate the execution of the projects (see Section 6.11.1 and Section 6.11.2).

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 F-Devices in accordance with the device-specific user documentation.

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

6.4 Software requirements

6.4.1 PLCnext Engineer software

Detailed information on PLCnext Engineer and on PLCnext technology can be found in the PLCnext community at plcnext-community.net and in particular in the PLCnext Info Center.

The PLCnext Engineer software is required for startup of the BPC 9102S.

6.4.2 Installing PLCnext Engineer

The software can be downloaded at phoenixcontact.net/product/1046008.

- Download the software onto your PC.
- Double-click the *.exe file to start installation.
- Follow the instructions in the installation assistant.

6.4.3 PLCnext Engineer license

Ensure that you install a version of the PLCnext Engineer software (≥2021.6) suitable for the BPC 9102S you will be using.

6.4.4 User interface

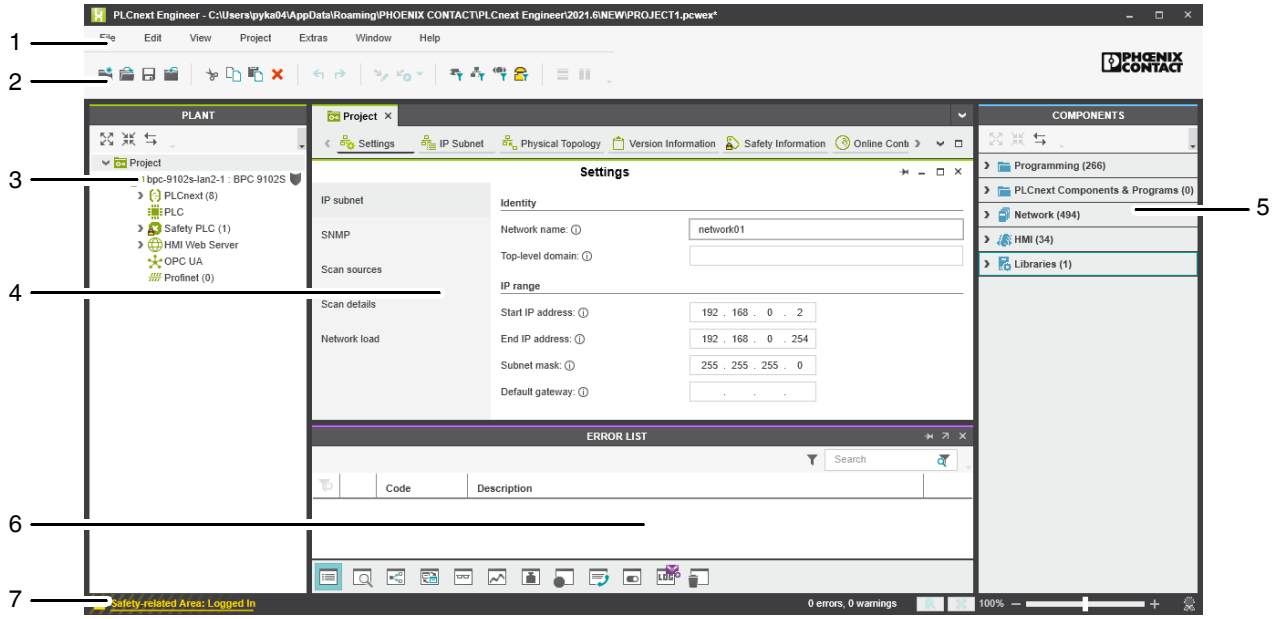


Figure 6-2 PLCnext Engineer user interface

1. Menu bar
2. Toolbar
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

Double-clicking on a node in the “PLANT” area or an element in the “COMPONENTS” area opens the associated editor group in the Editors area. Editor groups are always displayed in the center of the user interface. The color of the editor group indicates whether it is an instance editor (green; opened from the “PLANT” area) or a type editor (blue; opened from the “COMPONENTS” area). Each editor group contains several editors that can be opened and closed via buttons in the editor group.

“COMPONENTS” area

The “COMPONENTS” area contains all of the components available for the project.

The components can be divided into the following types based on their function:

– Developing program code (“Data Types”, “Programs”, and “Functions and Function Blocks”)
– Displaying all devices available for the “PLANT” area and adding them via GSDML or FDCML (“Devices”)
– Editing HMI pages (“HMI”)
– Adding libraries such as firmware libraries, IEC user libraries, or libraries provided by Phoenix Contact (“References”)

Cross-functional area

The cross-functional area contains functions that extend across the entire project.

– ERROR LIST:

  Shows all errors, warnings, and messages for the current project.
– GLOBAL FIND AND REPLACE:

  Finds and replaces strings in the project.
– CROSS REFERENCES:

  Displays all cross-references within the project, for example, the use and declaration of all variable types or HMI tags.
– WATCHES:

  Debug tool; shows the current values of the added variables in online mode.
– BREAKPOINTS:

  Debug tool for setting and resetting breakpoints when debugging within the application
– CALL STACKS:

  Debug tool that shows the order for calling up when executing the code and that contains commands for debugging with breakpoints
– LOGIC ANALYZER:

  Records and visualizes variable values at runtime.
– ONLINE STATE:

  While there is an online connection established to the controller and to the safety-related controller, a superordinate symbol of their operating state is displayed in the ONLINE STATE window.
– LOGGING:

  Shows all errors, warnings, and messages. A distinction is made between “online” (messages regarding the runtime environment, as well as errors and warnings that concern online communication) and “engineering” (messages regarding software events, e.g., GSDML and FDCML files; not project-related).
– RECYCLE BIN:

  Elements that have recently been deleted from the “PLANT” or “COMPONENTS” areas are moved to the recycle bin. Deleted elements can be restored from here, if needed.

6.4.5 Creating a new project

- Open PLCnext Engineer.
- Create a new project.

In the PLCnext Engineer software, select a controller for operating the BPC 9102S in accordance with the device firmware you are using (see Figure 6-3).

- In the COMPONENTS area under “Network, BPC 9xxx, Devices, Phoenix Contact, Box PC Controller, Controller”, click on the controller “BPC 9102S Rev. >= 00/2021.6.0”.

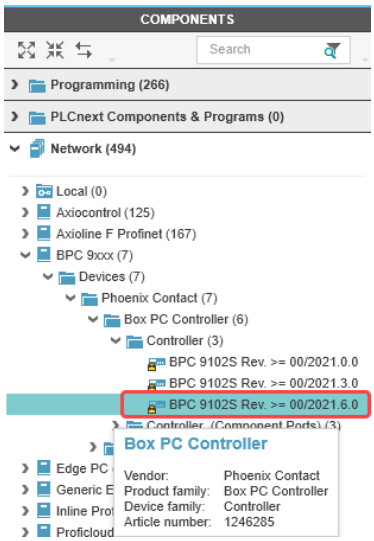


Figure 6-3 Selecting the BPC 9102S

- Drag the selected BPC 9102S into the “PLANT” area while pressing the mouse button.
- If the software prompts you to define a project password, proceed as described in Section 6.4.6.
- Paste the BPC 9102S to the project node.
- Open the “File, Save project as…” menu.
- Enter a unique and meaningful name for the project (in the example: “UM_BPC_9102S”).
- Click the “Save” button.

Further information on creating a new project is available in the PLCnext Engineer software online help function.

6.4.6 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 COMPONENTS 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.

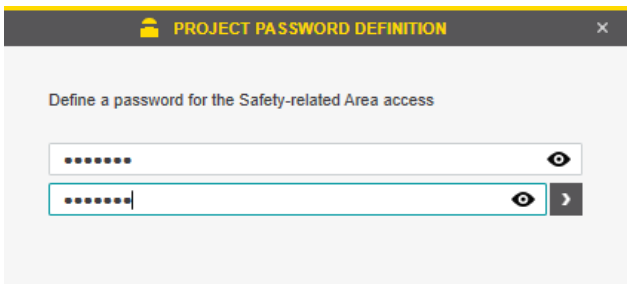


Figure 6-4 Defining a project password

The project password must contain between 6 and 24 characters.

6.5 Further actions/steps in the PLCnext Engineer software

6.5.1 Creating the IP address range in the project

- Double-click 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 to be able to operate it in your network.

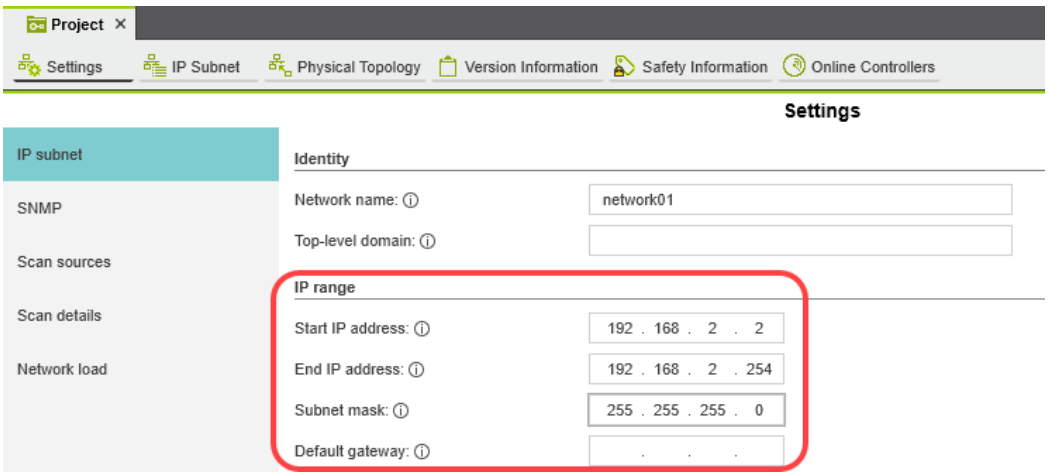


Figure 6-5 IP address range set in the project

6.5.2 BPC 9102S IP settings: General

In the delivery state, the IP address on the LAN2 interface (PROFINET controller interface) of the BPC 9102S is 192.168.2.10.

The IP addresses of the BPC 9102S can be set automatically or manually. The IP addresses will be assigned to the BPC 9102S once you connect PLCnext Engineer to the BPC 9102S (see Section 6.5.4).

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 BPC 9102S 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.

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”.

BPC 9102S: MAC addresses

Note that the BPC 9102S has **three MAC addresses**. The LAN1, LAN2, and LAN3 interfaces are each assigned a separate MAC address.

1. LAN 1 can be used as an Ethernet interface for TCP/IP communication, for example.
2. LAN2 is preconfigured as the PROFINET controller interface.
3. LAN3 is preconfigured as the PROFINET device interface.

All three interfaces are designed for a maximum transmission speed of 1 Gbps.

Depending on the connected interface, the BPC 9102S can then be accessed on the Ethernet via **three different IP addresses**.

Please note:

– The IP addresses of interfaces LAN1/LAN2/LAN3 must be in different subnets.
– The PROFINET controller function of the BPC 9102S is available at interface LAN2. 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 the LAN3 interface if you want to use the PROFINET device function of the BPC 9102S on these interfaces.
– The LAN1 and LAN3 interfaces do not necessarily have to be assigned an IP address if, for example, communication between a PC with PLCnext Engineer and the BPC 9102S is also implemented via the LAN2 interface.
  We recommend that appropriate IP addresses be assigned to all interfaces.

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 6-3 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	192.168.3.10	255.255.255.0

6.5.3 Setting the IP address of the BPC 9102S (controller) in the project

Specify an IP address for the controller that lies within the previously set IP address range.

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

The controller editor group opens.

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

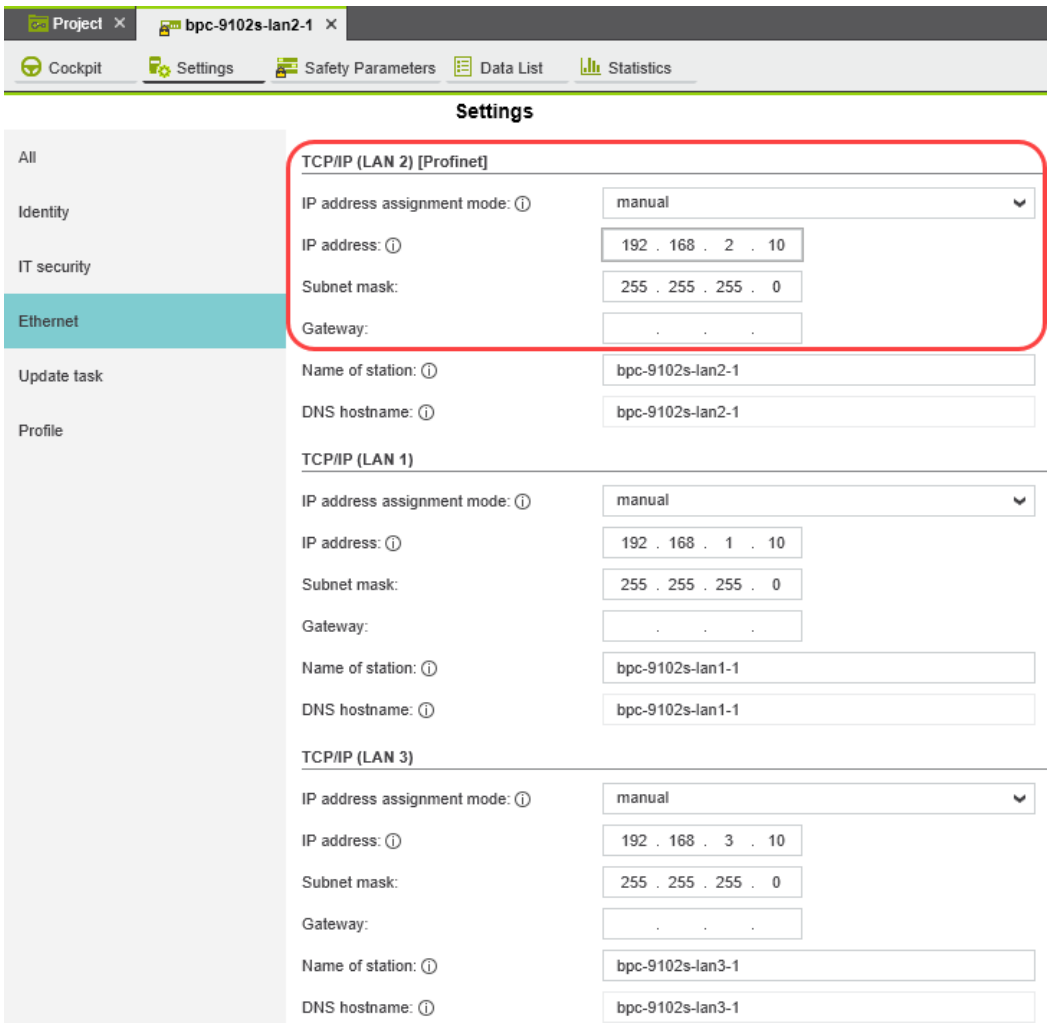


Figure 6-6 Controller IP address set

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 6.5.4.

Setting the IP address automatically

- Select “automatic” from 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 6.5.1) as soon as a connection to the controller is established (see Section 6.5.4).

Setting the IP address manually

- Select “manual” from 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 6.5.4).

6.5.4 Connecting PLCnext Engineer to the BPC 9102S (controller)

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

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

The “Project” editor group opens.

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

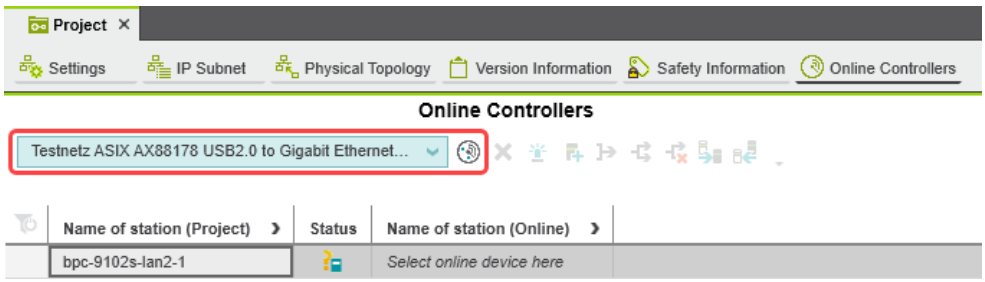


Figure 6-7 Selecting the network card

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 6-7).

- 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)”.

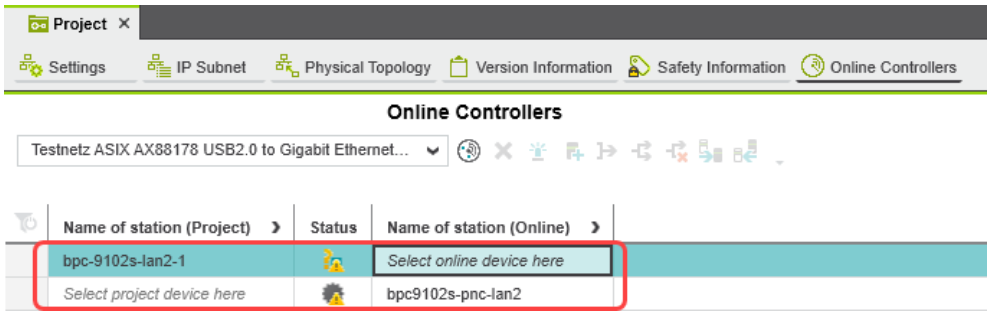


Figure 6-8 Assigning online devices

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.

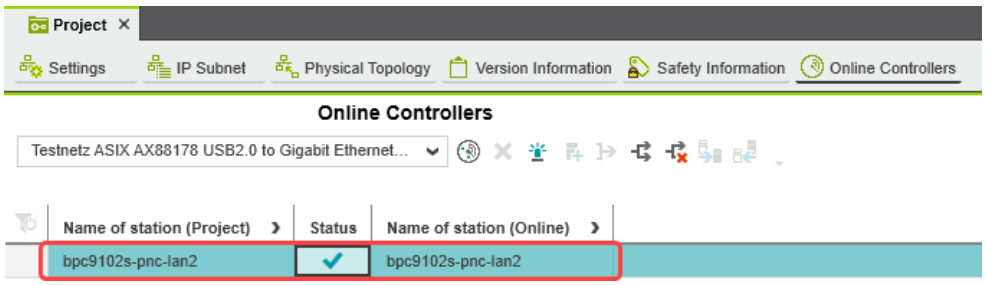


Figure 6-9 Successful assignment of the configured controller to an online device

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

- Double-click 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.

If the BPC 9102S user authentication is enabled (default setting), the “SECURE DEVICE LOGIN” dialog opens.

Observe the notes on the device user authentication function:
For information on user authentication, refer to Section 6.5.5.

- Enter the user name and password in the “SECURE DEVICE LOGIN” dialog.
  In the delivery state, the “admin” user is already created with a default password (see label/printing in Figure 3-9 on page 44).

The  icon next to the controller node and bold font in the “PLANT” area indicates that connection was successful (see Figure 6-10).

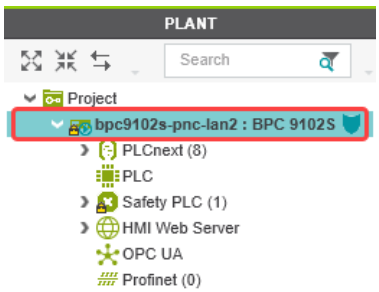


Figure 6-10 Successful connection to the controller

The  button also indicates successful connection.

6.5.5 User authentication

When the device user authentication function is enabled, logging in with a user name and password is required in order to execute certain functions (e.g., for establishing an online connection to the device).
In the delivery state, user authentication is enabled. You can disable user authentication in the BPC 9102S web-based management system.

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.

Further information on user authentication is available in the PLCnext Info Center.

- To log in to the BPC 9102S, enter a user name and password in the “SECURE DEVICE LOGIN” dialog in PLCnext Engineer.

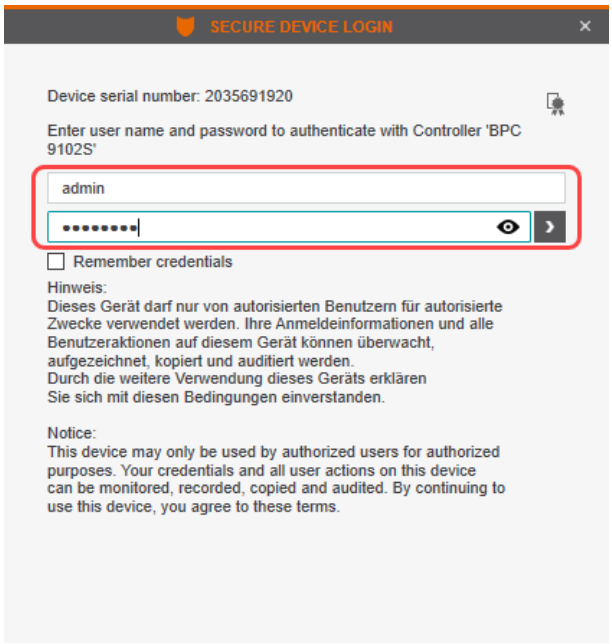


Figure 6-11 “SECURE DEVICE LOGIN” dialog

Further information is available in the PLCnext Info Center and in the PLCnext Engineer online help function.

6.6 Configuring PROFINET devices

A description of the procedure for configuring PROFINET devices is available in the PLCnext Community at plcnext-community.net and in particular in the PLCnext Info Center as well as in the PLCnext Engineer online help function.

6.6.1 Adding PROFINET devices

- Double-click 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 so, proceed as follows:

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

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

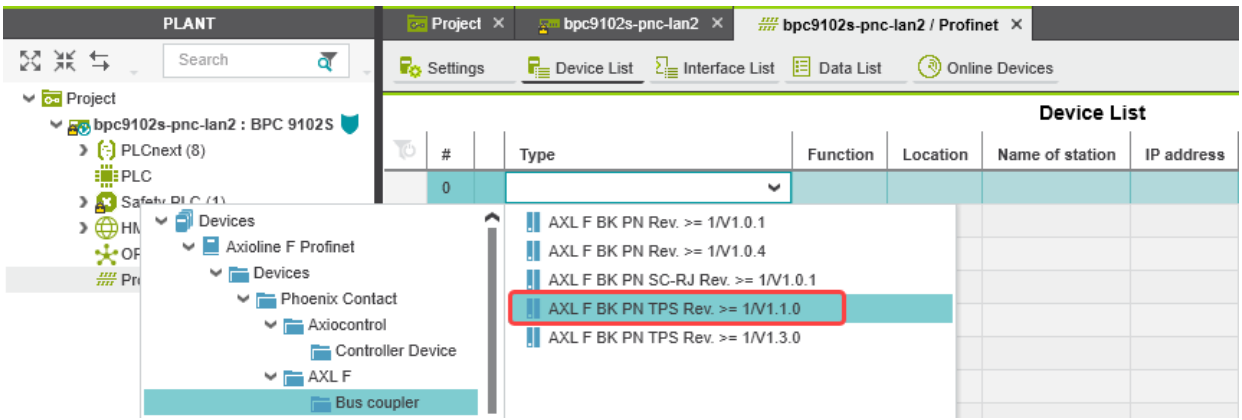


Figure 6-12 Role picker for selecting PROFINET devices

- 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.

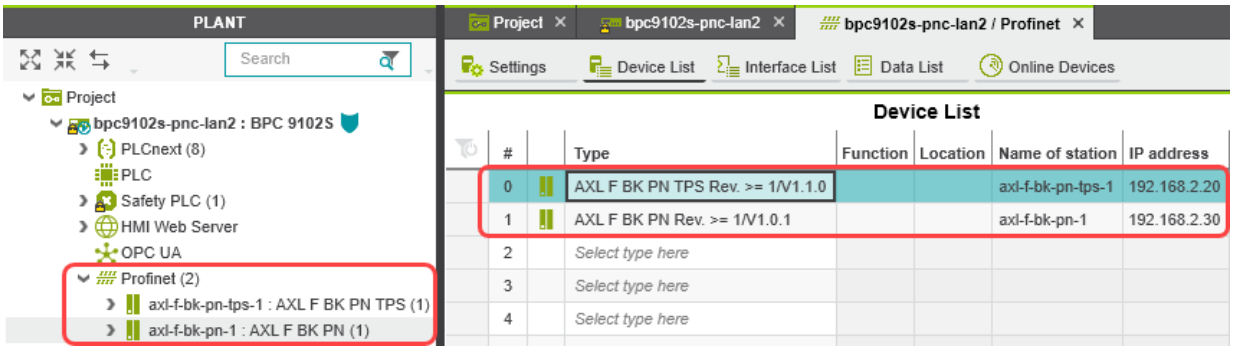


Figure 6-13 PROFINET devices in the “PLANT” area and in the Device List

6.6.2 Assigning online devices (device naming)

After you have added 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 so, proceed as follows:

- Double-click 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.

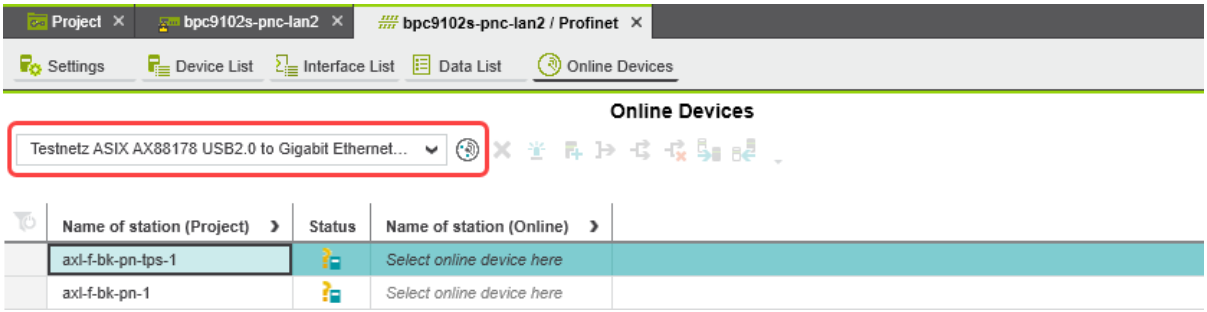


Figure 6-14 Selecting the network card

- 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)”.

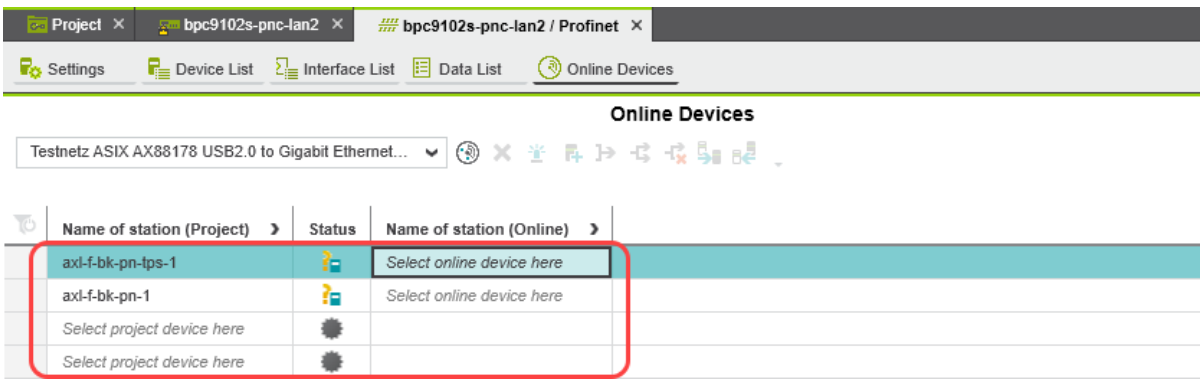


Figure 6-15 Assigning online devices

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.

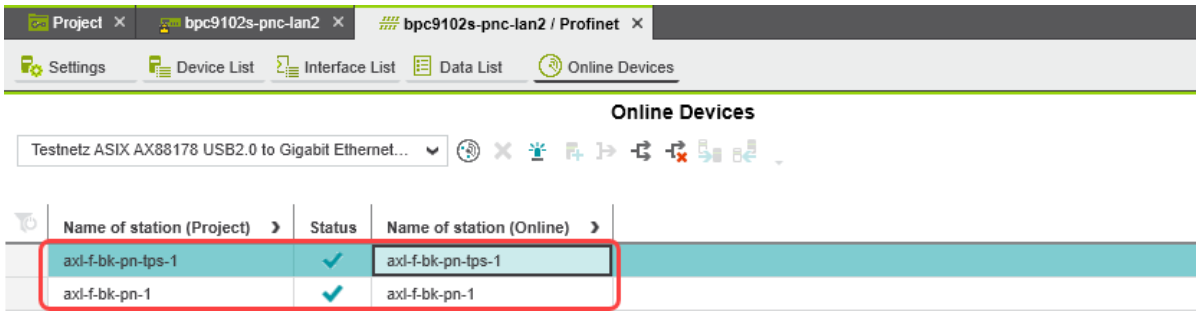


Figure 6-16 Successful assignment of the configured PROFINET devices to an online device

6.6.3 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.

An extensive description of the procedure for adding I/O modules is available in the PLCnext Community at plcnext-community.net and in particular in the PLCnext Info Center as well as in the PLCnext Engineer online help function.

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.

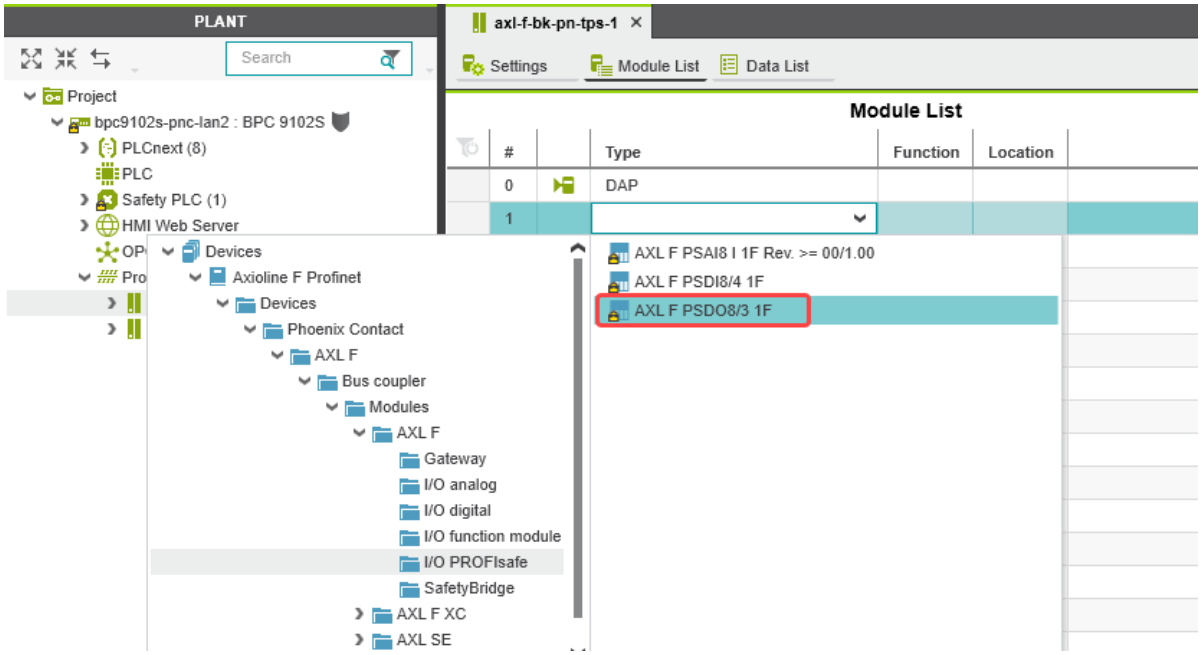


Figure 6-17 Role picker for selecting the I/O modules

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

Project password: Logging into the Safety-related Area

In this area, you will be changing the safety-related project by adding F-Devices. If you are not logged into the “Safety-related Area”, PLCnext Engineer will prompt you to enter a password.

Through the targeted distribution of the password, you can specify the circle of users who may make changes to the safety-related project.

- Enter the password in the following dialog and confirm your entry by clicking on the arrow.

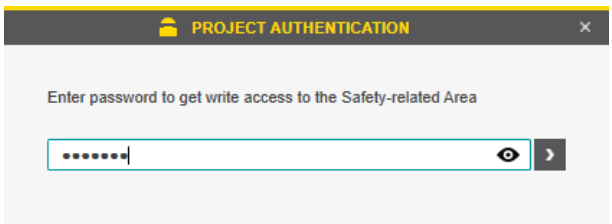


Figure 6-18 Entering the project password

A successful login is indicated by text highlighted in yellow:

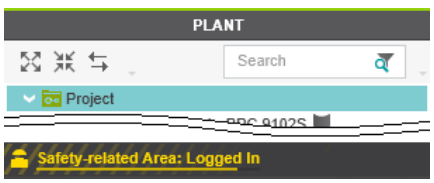


Figure 6-19 Successful login to the Safety-related Area

The I/O module is added and shown in the “PLANT” area under the “Profinet (x)” node for the respective PROFINET device (see Figure 6-20).

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

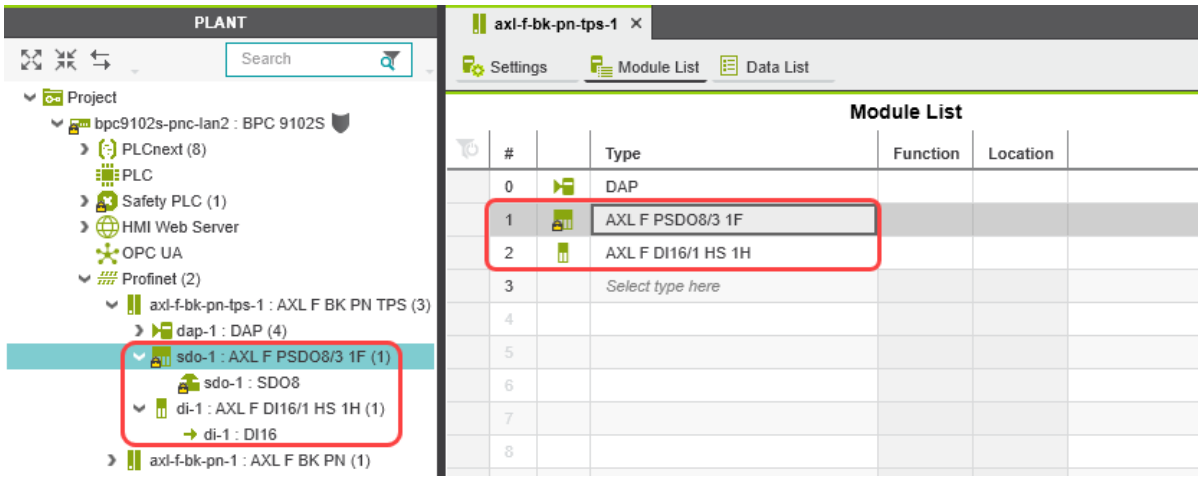


Figure 6-20 I/O modules connected to the PROFINET device

Reading in I/O modules automatically

To automatically read in I/O modules aligned to a PROFINET device, the following requirements must be met:

– The controller has valid IP settings (see Section 6.5.3).

– The PROFINET device has valid IP settings and is connected to PLCnext Engineer (see Section 6.6.2).

To read in the I/O modules 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 in.
- Select “Read Profinet Modules” in the context menu.

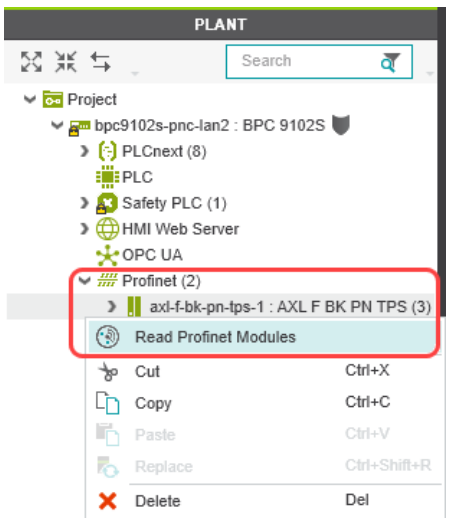


Figure 6-21 Reading in I/O modules of a PROFINET device automatically

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

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

I/O modules in the example project

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

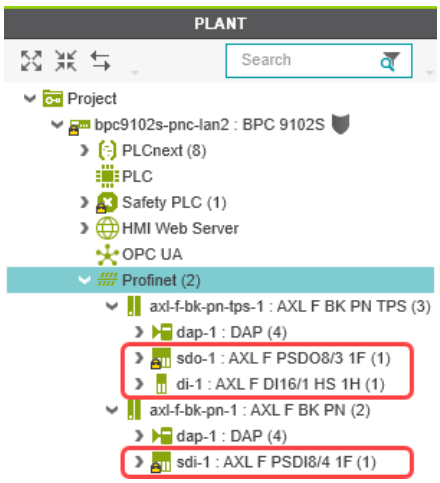


Figure 6-22 I/O modules () in the example project

6.7 Programming in accordance with IEC 61131-3 – non-safety-related example program

Information on programming in accordance with IEC 61131-3 can be found in the PLCnext community at plcnext-community.net and in particular in the PLCnext Info Center as well as in the PLCnext Engineer online help function.

Please note:

Due to the creation of a new project for the BPC 9102S described in Section 6.4.5, you have to carry out the steps in sections 6.7.1 “Creating a POU” and 6.7.5 “Instantiating programs” for the BPC 9102S yourself.

6.7.1 Creating a POU

If you have created a new project for the BPC 9102S, you must create the program organization unit (POU) with the name “Main” in the “COMPONENTS” area under “Programs” for the non-safety-related part of the project (see Figure 6-24 on page 98). The POU with the name “S_Main” has been created automatically.

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”.

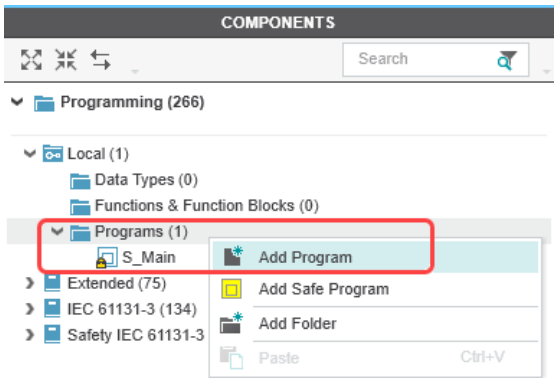


Figure 6-23 “Add Program” context menu

- Enter the name “Main” for the new POU.

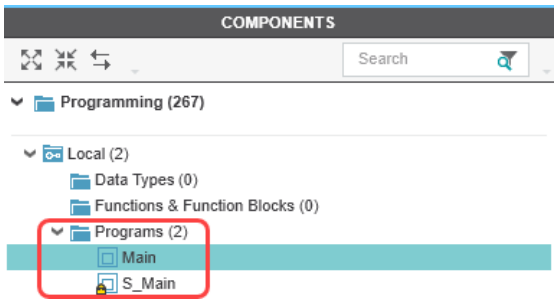


Figure 6-24 Program POUs: Main and S_Main

6.7.2 Opening a 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.

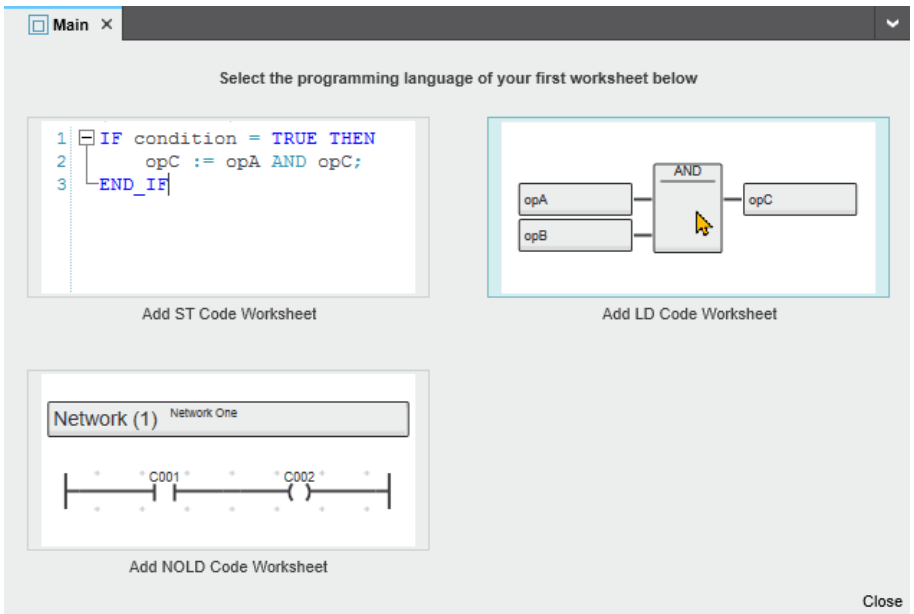


Figure 6-25 Selecting the programming language for the first worksheet

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

You can now define variables, for example (see Section 6.7.3, “Creating variables”).

6.7.3 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 6-4 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 6-26: Main).
- Set the type and use for all created variables.

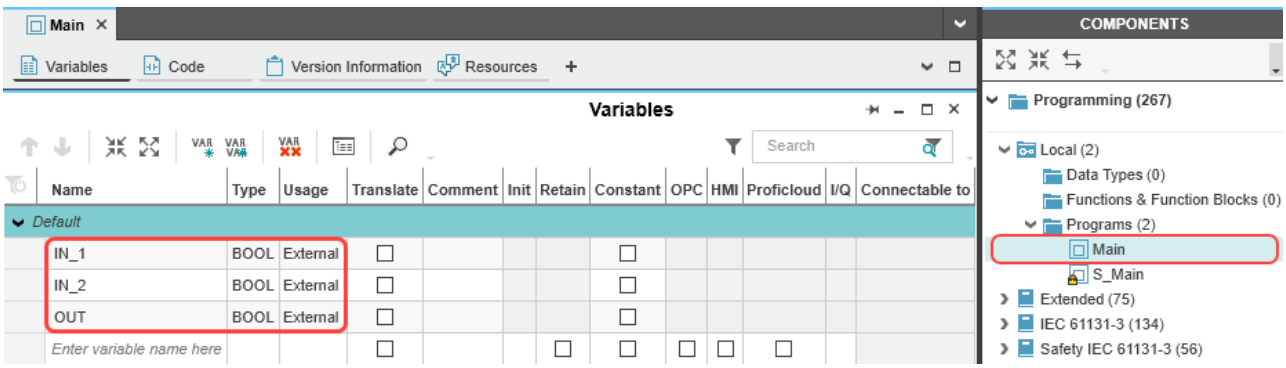


Figure 6-26 Creating variables for a POU (in the example: for the “Main” POU)

Once you have created all of the necessary variables, create the program for the selected POU; see Section 6.7.4.

6.7.4 Creating a program

Non-safety-related example program

The example program in Figure 6-27 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 code editor.

By default, the code editor is labeled with “Code”. You can change the designation of the code editor as desired.

- Create the program.

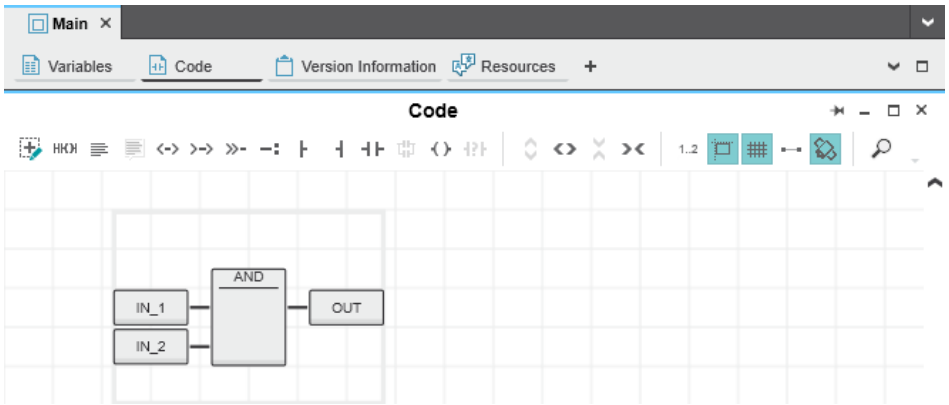


Figure 6-27 Example program in FBD

6.7.5 Instantiating programs

Programs are instantiated 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 BPC 9102S uses an eight-core processor and has one ESM (“ESM1” … “ESM8” 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 (“Task1” in the example in Figure 6-28).

  The name may not contain any spaces.
- In the “Task type” column, click on 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 6-28).
  The name may 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 6-28).

The selected program is instantiated and assigned to a task.

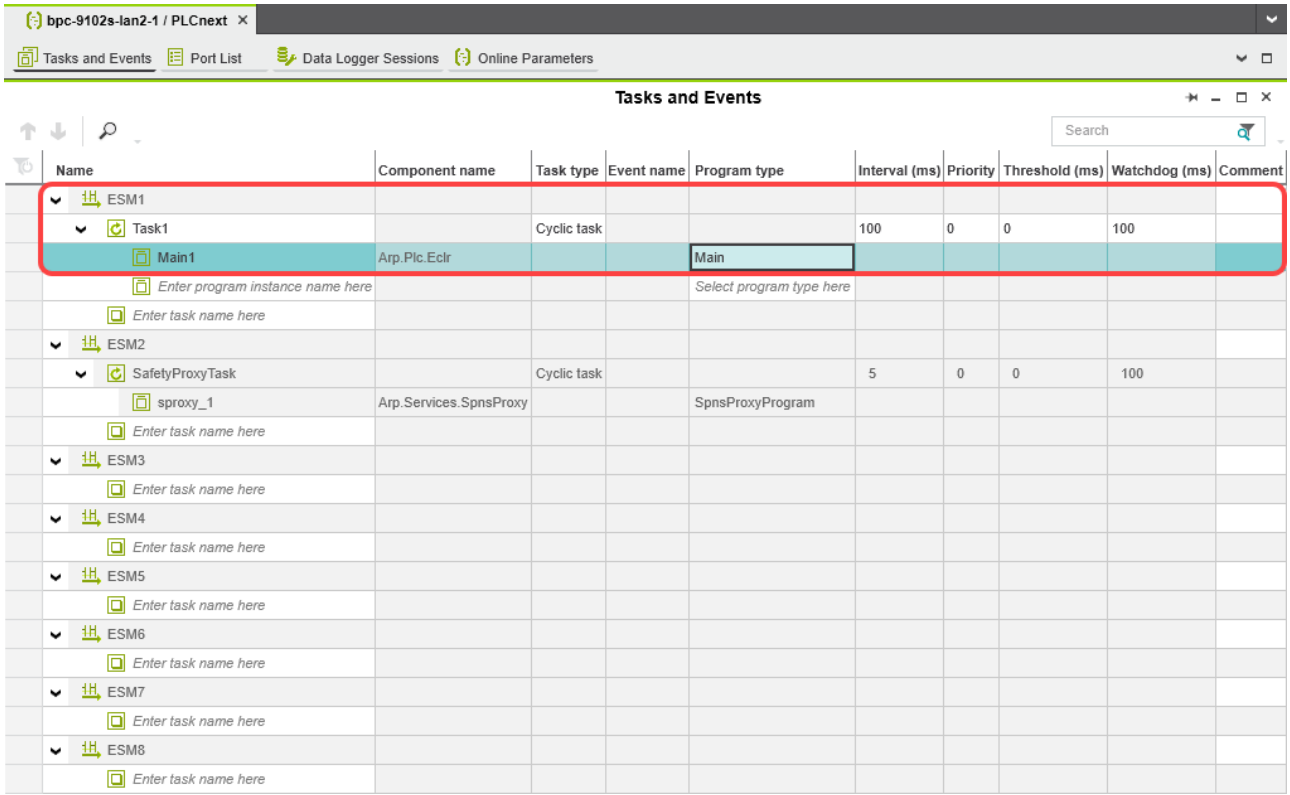


Figure 6-28 Tasks and program instances in the “Tasks and Events” editor

6.8 Assigning non-safety-related process data

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.

- In the “Process data item” column, use the role picker to assign the corresponding process data to all variables (see marking in section Figure 6-30).

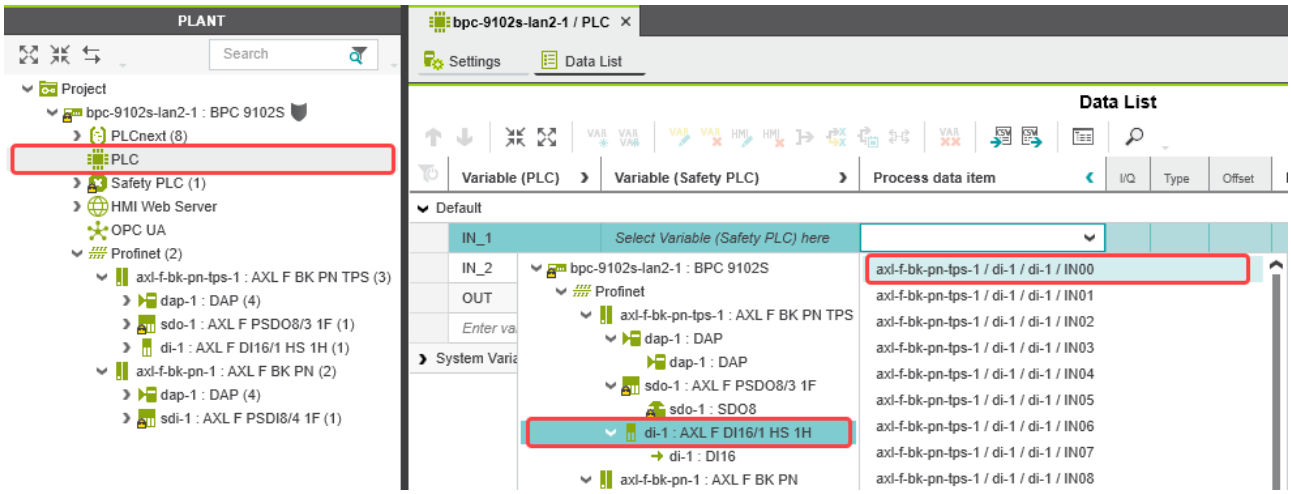


Figure 6-29 Assigning process data

The following figure shows all variables created and the assigned process data:

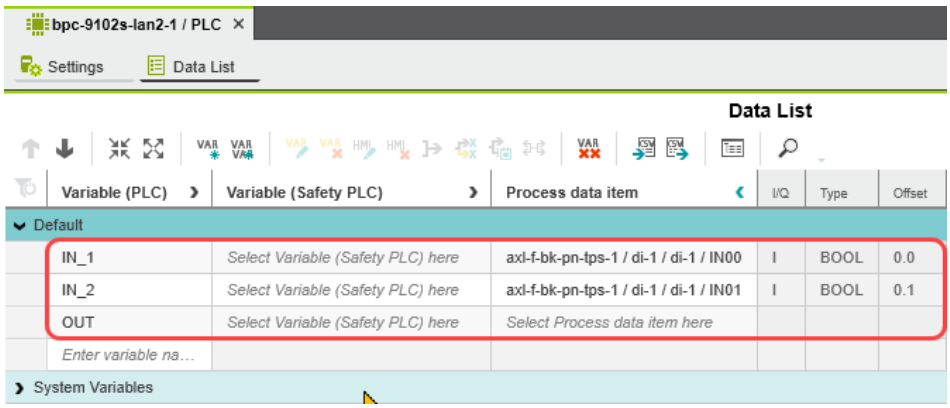


Figure 6-30 Variables: Process data assigned

6.9 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.

6.10 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.

6.10.1 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.
  Each F-Address assigned within a network must be unique
- Avoid overlapping F-Addresses. They are not permitted.

In the example, the F-Devices are assigned the F-Destination addresses:

– AXL F PSDO8/3 1F: 1

– AXL F PSDI8/4 1F: 2

For more detailed information on setting the PROFIsafe F-Addresses, please refer to “Device identification/number of safe devices” on page 32 and the device-specific user documentation.

F_Source_Address (F_Source_Add)

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

The controller editor group opens.

- Select the “Safety Parameters” editor.

PROJECT AUTHENTICATION may be necessary

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 password: Logging into the Safety-related Area” on page 94).

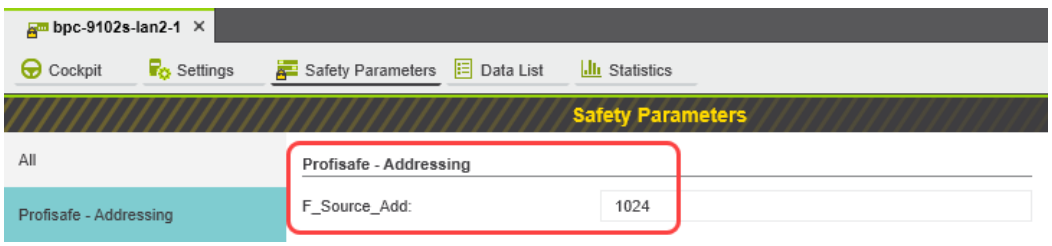


Figure 6-31 F-Address of the F-Host: F_Source_Add (F_Source_Address)

- 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 BPC 9102S 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.

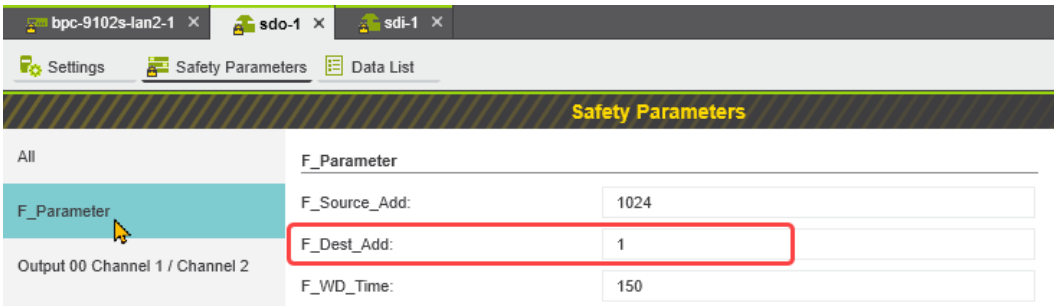


Figure 6-32 F-Address of the PROFIsafe F-Device: F_Dest_Add (F_Destination_Address)

- 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.
- In the example, set F_Dest_Add for the safety modules used to the following values:
  – “1” for the AXL F PSDO8/3 1F (see Figure 6-32)
  – “2” for the AXL F PSDI8/4 1F
- If necessary, adapt the F_Dest_Add values to your application.

An adjustable range of “1 ... 65535_{dec}” maximum is permitted.

- Proceed as described above for other safety modules in your application.

6.10.2 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 3.3 on page 33.

1. Call up the safety parameters for the AXL F PSDO8/3 1F:

- 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 6-33: AXL F PSDO8/3 1F).

The safety module editor group opens.

- Select the “Safety Parameters” editor.

PROJECT AUTHENTICATION may be necessary

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 password: Logging into the Safety-related Area” on page 94).

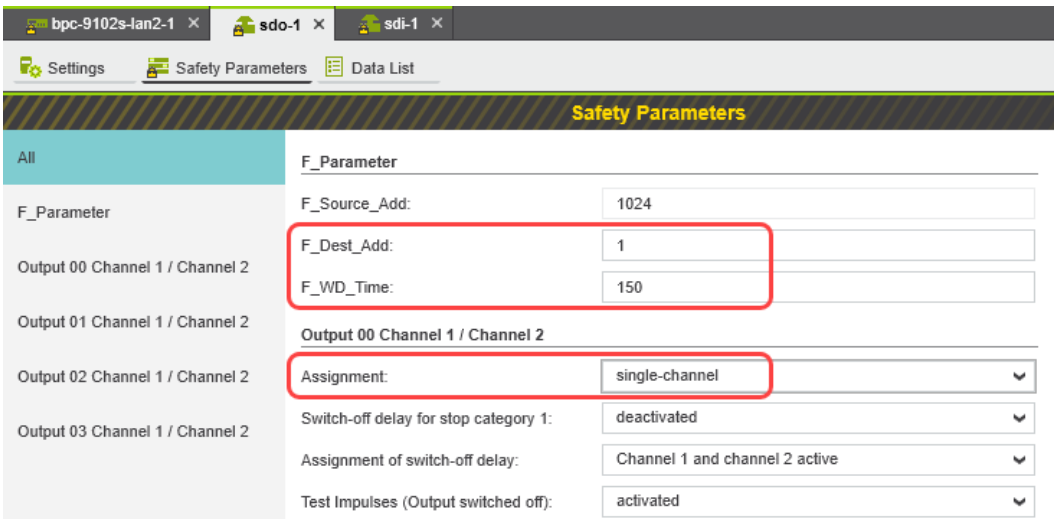


Figure 6-33 “Safety Parameters” editor: AXL F PSDO8/3 1F

2. Call up the safety parameters for the AXL F PSDI8/4 1F:

- 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 6-34: AXL F PSDI8/4 1F).

The safety module editor group opens.

- Select the “Safety Parameters” editor.

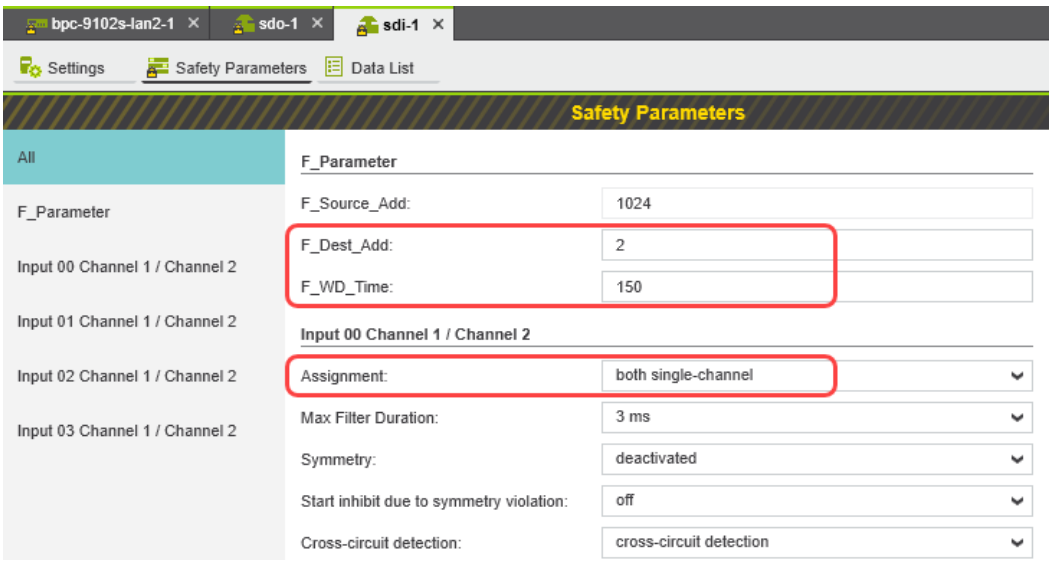


Figure 6-34 “Safety Parameters” editor: AXL F PSDI8/4 1F

3. Set the safety parameters:

- Set the required safety parameters.

  In the example in the figures 6-33 and 6-34, these values are as follows:

Value	AXL F PSDO8/3 1F	AXL F PSDI8/4 1F
Figure	Figure 6-33 on page 106	Figure 6-34 on page 107
F-Address: F_Dest_Add	1	2
Watchdog time: F_WD_Time	150 ms	150 ms
Assignment of channels 1 and 2 for the inputs or outputs	Output 00: single-channel	Input 00: both single-channel

  If necessary, adapt the settings to your application.

- Repeat the safety parameter settings described above for each safety module used in your application.

6.10.3 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 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 the corresponding management/diagnostic variables in the safety-related “S_Main” POU (see Section “Creating a safety-related program” on page 114).

For further information on management/diagnostic variables, please refer to section “PROFIsafe: Communication diagnostics” on page 30 and the sections 8.3.5 on page 151 and 8.3.6 on page 154.

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

The “/ Safety PLC” 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 6-35).

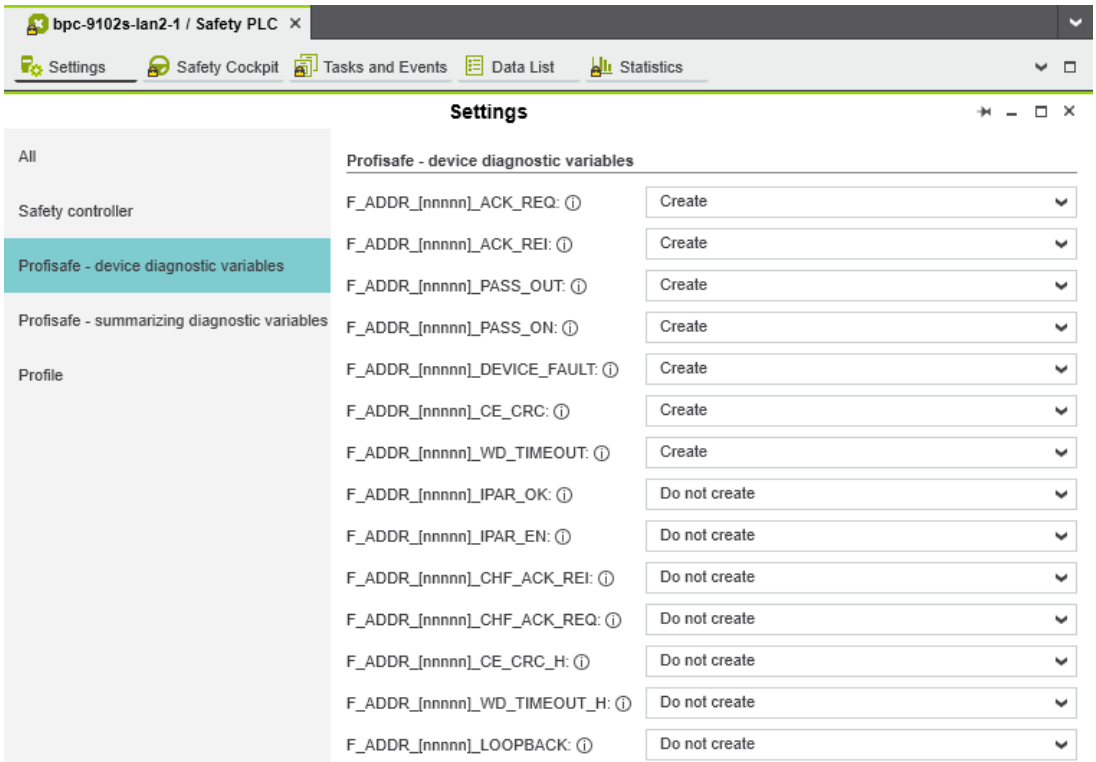


Figure 6-35 Management/diagnostic variables for each configured F-Device

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 6-36).

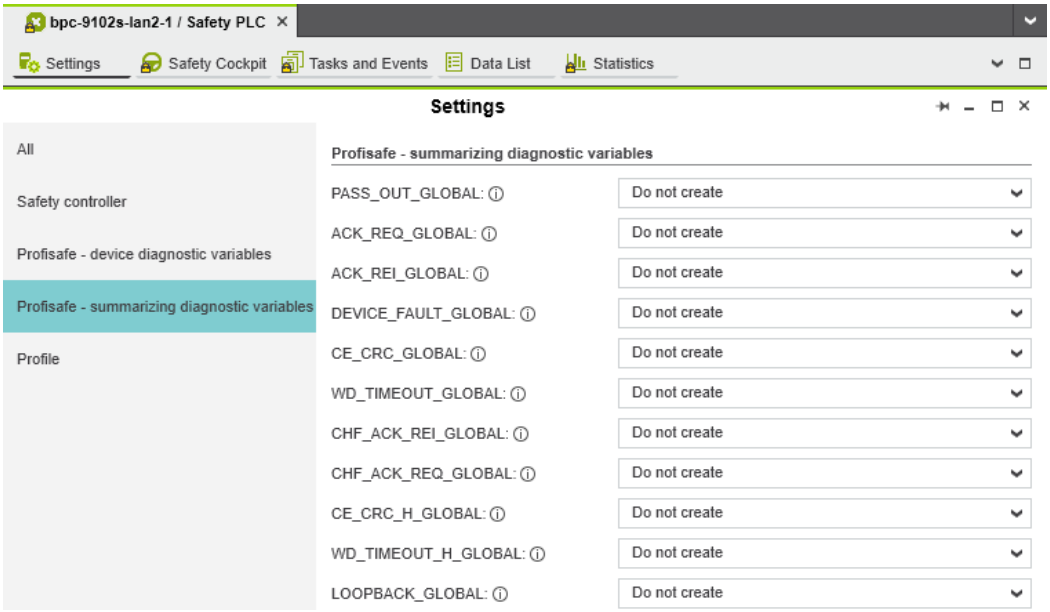


Figure 6-36 Management/diagnostic variables for all configured F-Devices

Created variables are displayed in the “Data List” editor of the “Safety PLC (x)” node and of the controller node:

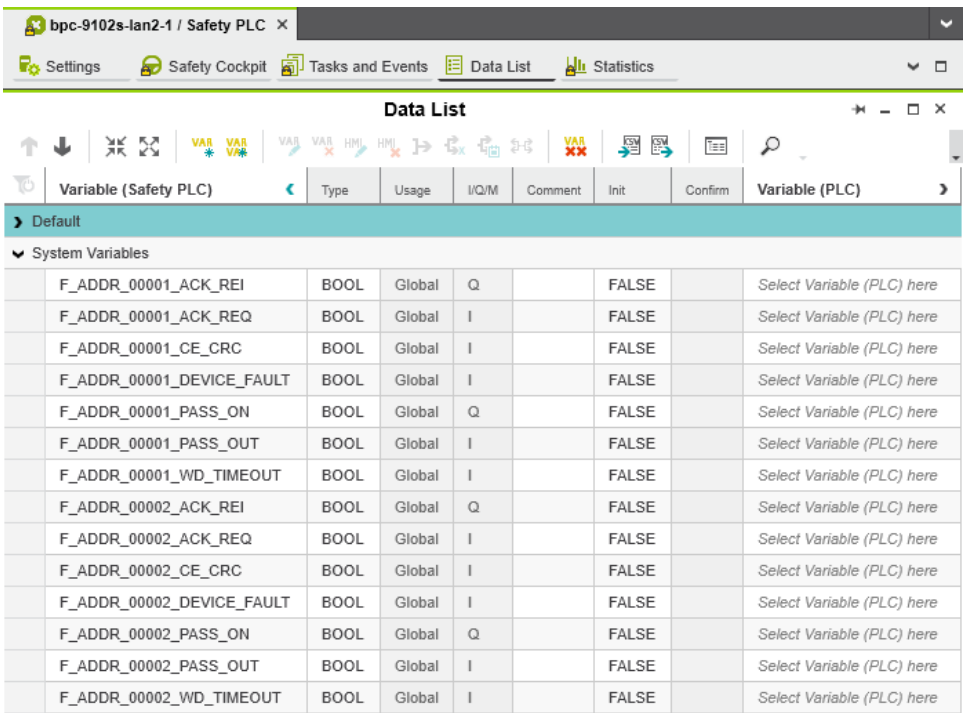


Figure 6-37 Management/diagnostic variables of F-Devices (default)

For the two F-Devices used in the example, PLCnext Engineer creates 14 management/diagnostic variables by default.

6.10.4 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 of a non-safety-related data type.

The aim is to link the created exchange variables with specific management/diagnostic variables described in Section 6.10.3.

Data direction for exchange variables

In accordance with the data direction to be specified for management/diagnostic variables, you must also specify a data direction 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.

Also refer to section “PROFIsafe: Communication diagnostics” on page 30 for this.

1. First create the “Exchange” variable group in PLCnext Engineer as shown in Figure 6-38.
2. Next, create 4 variables for each F-Device used in the “Variable (PLC)” column in this group.
3. Then, in the “Variable (Safety PLC)” column, create the corresponding non-safety-related exchange variables.

   These exchange variables are assigned to the safety-related PLC.
4. Finally, set the data direction of the exchange variables.

In the example in Figure 6-38, the 4 variables/exchange variables will be created for the AXL F PSDI8/4 1F F-Device.

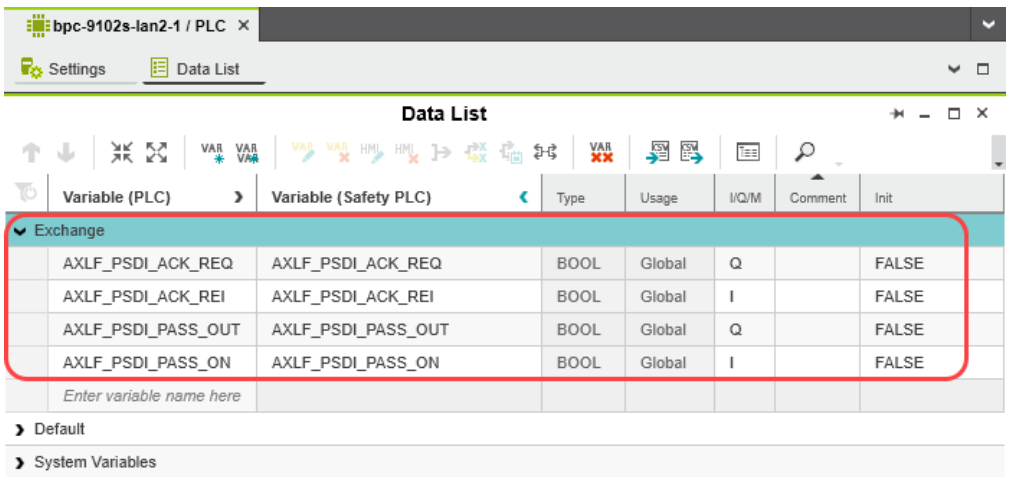


Figure 6-38 Exchange variables in the example

- Double-click on the “PLC (x)” 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 to “Exchange”, for example.

- Enter the names of the variables in the “Variable (PLC)” column in turn as shown in Figure 6-38.
- 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 6-39).

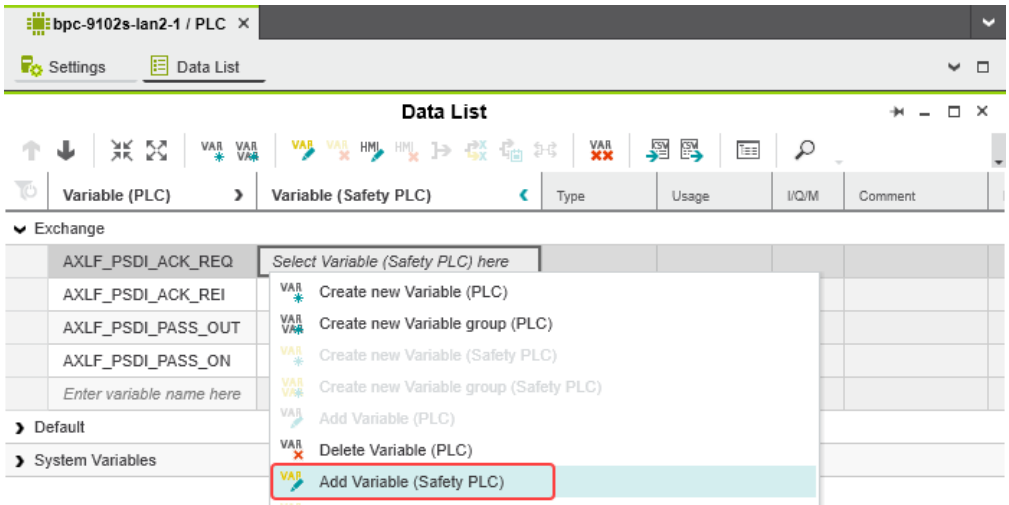


Figure 6-39 “Add Variable (Safety PLC)” context menu

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. When doing so, refer to the note at the beginning of the section on page 110.

- Set the data direction in turn for each variable created earlier as shown in Figure 6-40.

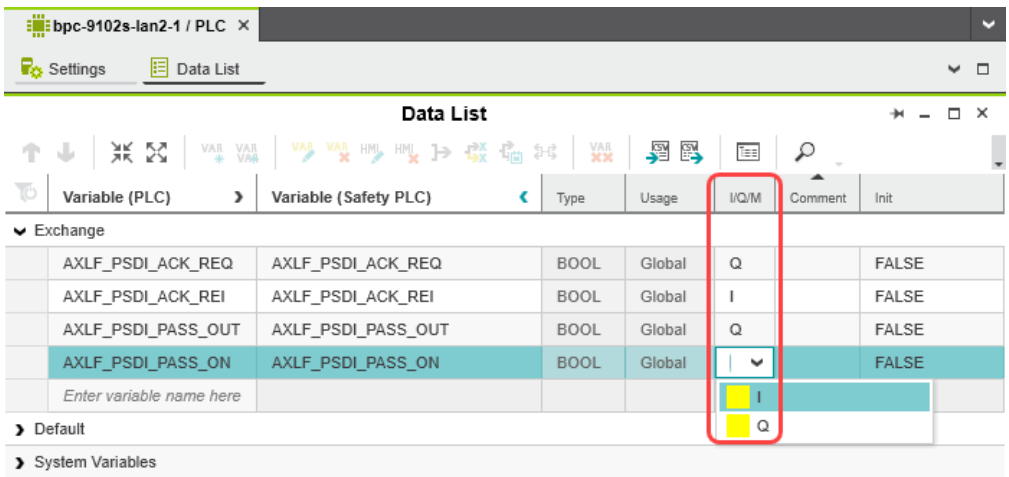


Figure 6-40 Setting the data direction

6.10.5 Opening a safety-related POU

For further information on opening and creating POUs, please refer to Section “Creating a POU” on page 97.

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 6-24 on page 98).

- 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 safety-related POU (in the example: “S_Main” program).

The editor group for the selected POU opens.

6.10.6 Creating safety-related variables

Variables in the example project

The following table lists the safety-related variables used in the safety-related example program.

Table 6-5 Input/output variables in the example (safe logical ANDing)

Parameter	Variable name	Data type	Use	Description
IN1	AXLF_PSDI_IN1	SAFEBOOL	External	AXL F PSDI8/4 1F: Input 0 channel 1 (IN0_CH1) PD: sdi-1 / IN0 CH1/2
IN2	AXLF_PSDI_IN2	SAFEBOOL	External	AXL F PSDI8/4 1F: Input 0 channel 2 (IN0_CH2) PD: sdi-1 / IN0 CH2
OUT	AXLF_PSDO_OUT	SAFEBOOL	External	AXL F PSDO8/3 1F: Output 0 channel 1 (OUT0_CH1) PD: axl-f-bk-pn-tps-1 / sdo-1 / sdo-1 / OUT00 CH1/2

Key: PD = Process Data element in PLCnext Engineer

- Select the “Variables” editor.
- Create the variables that you need for the selected POU (in the example in Figure 6-41: S_Main).
- Set the type and use for all created variables.

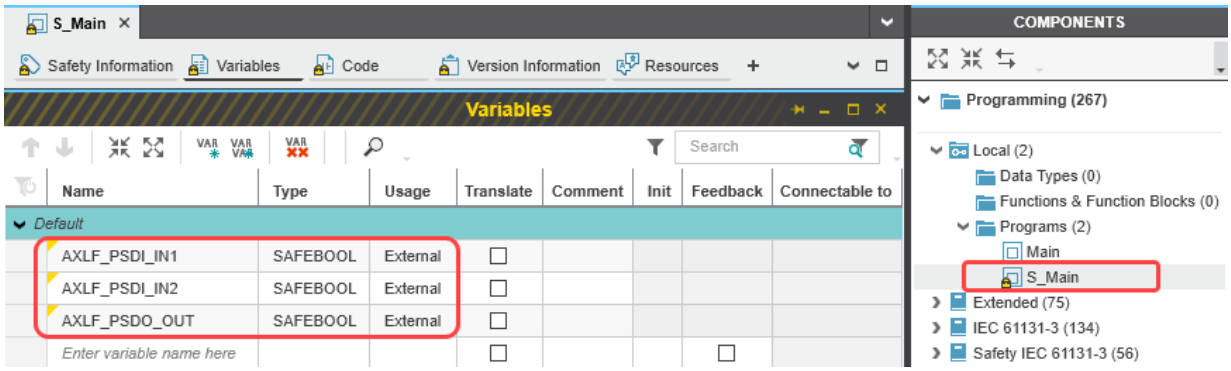


Figure 6-41 Creating variables for a POU (in the example: for the “S_Main” POU)

Selecting diagnostic/ management variables and exchange variables

Before the diagnostic/management variables and exchange variables that you created earlier can be used 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 6-42).
- Select the “Safety PLC”.
- Select the corresponding variable on the right-hand side of the window.
- Repeat this step for all the diagnostic/management variables and exchange variables shown in Figure 6-42.

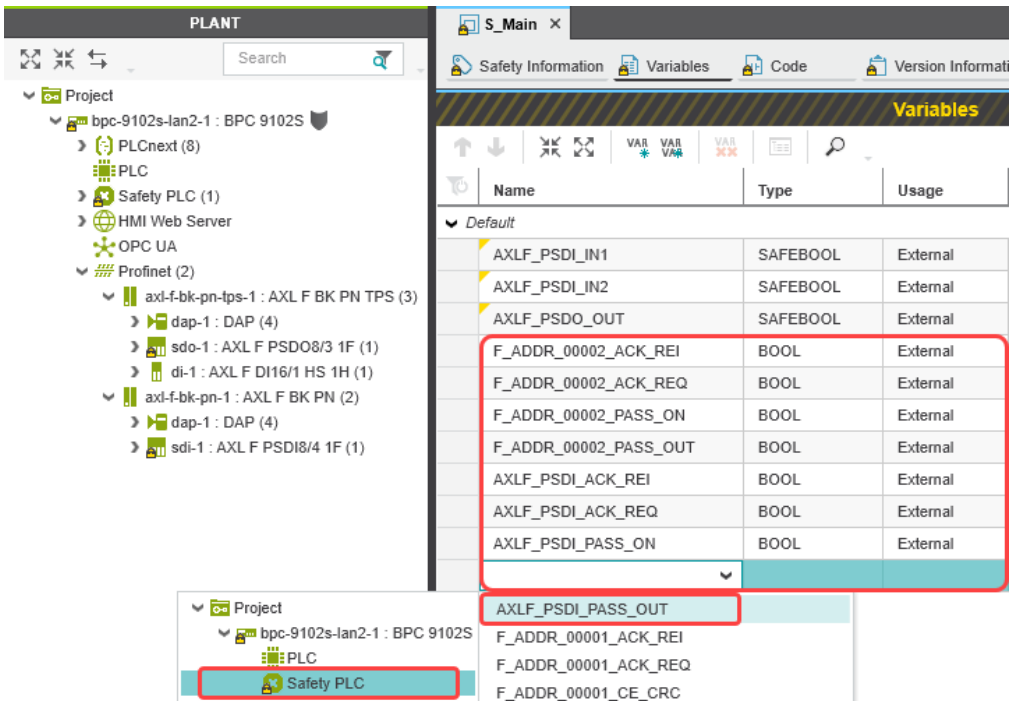


Figure 6-42 Selecting diagnostic/management variables

Once you have created all of the necessary variables, create the program for the selected POU; see Section 6.10.7.

6.10.7 Creating a safety-related program

Safety-related example program

The safety-related example program in Figure 6-43 on page 114 includes the following functions:

– In the first part of the example, two inputs of the safety-related AXL F PSDI8/4 1F input module are linked with AND logic via the safety-related AND_S function block. The result will be linked to an output of the safety-related AXL F PSDO8/3 1F output module.
– In the second part of the example, exchange variables for the safety-related AXL F PSDI8/4 1F input module from the “Exchange” variable group will be linked with the diagnostic/management variables. In the example, the passivation of an F-Device will be canceled via the variables with an operator acknowledge request and subsequent operator acknowledge reintegration (see Section “Operator acknowledge” on page 126).

The input/output variables are connected to process data in due course.

Creating a program

To create a program, proceed as follows:

• Select the code editor.

By default, the code editor is labeled with “Code”. You can change the designation of the code editor as desired.

• Create the program as shown in Figure 6-43 on page 114.

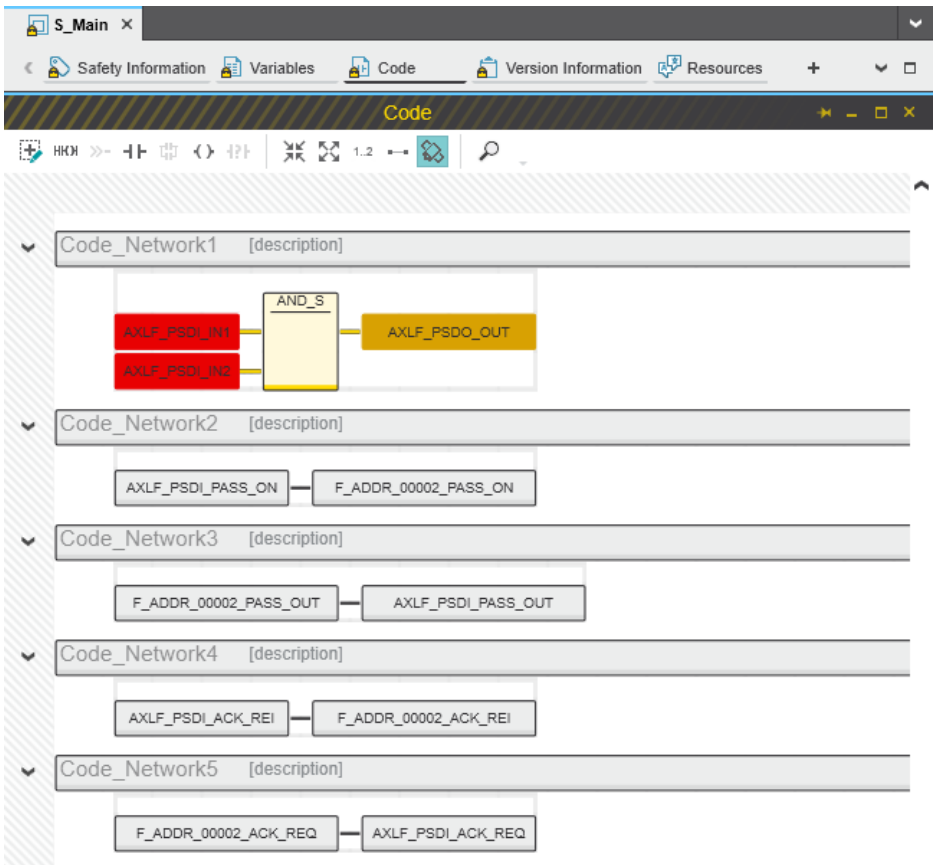


Figure 6-43 Safety-related example program with errors displayed

The errors and warnings shown in Figure 6-43 on page 114 (color-coded input and output variables in networks 1 to 3) are due to the fact that no process data has yet been assigned to these variables. You will execute this step in the following section.

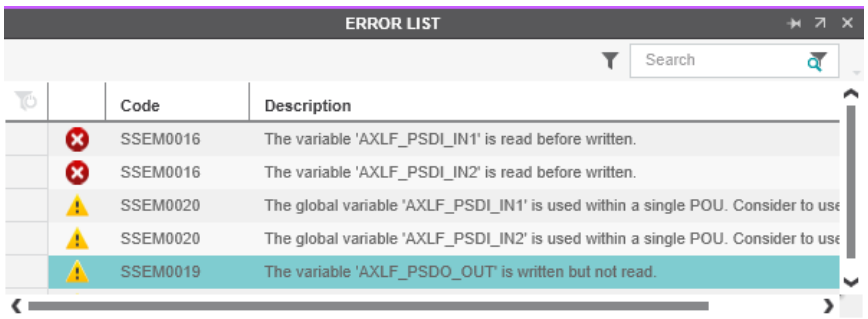


Figure 6-44 Error list

6.10.8 Assigning safety-related 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” 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 to all variables (see marking in section Figure 6-45).

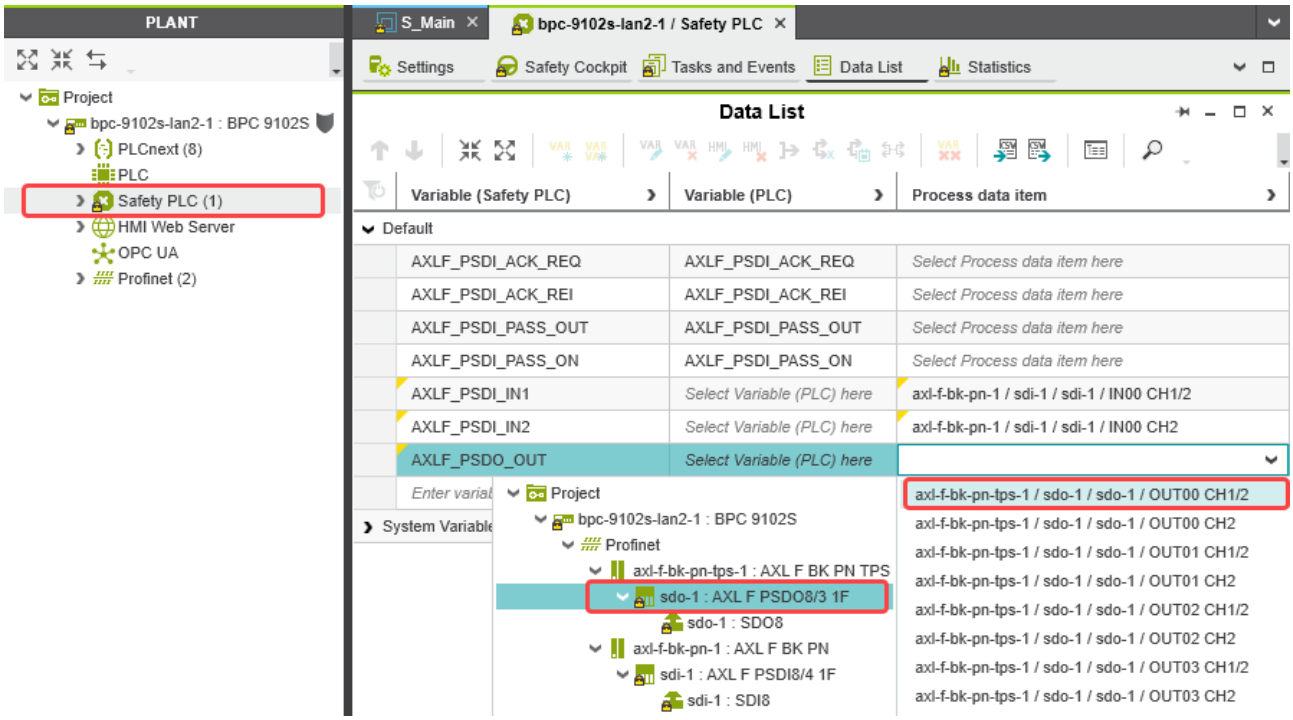


Figure 6-45 Assigning safety-related process data

The following figure shows all safety-related variables created and the assigned process data:

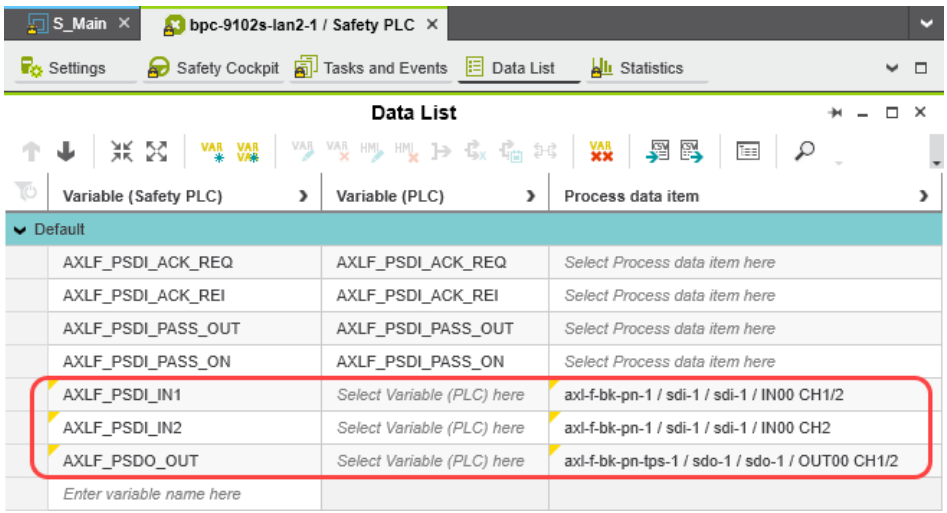


Figure 6-46 Safety-related variables: Process data assigned

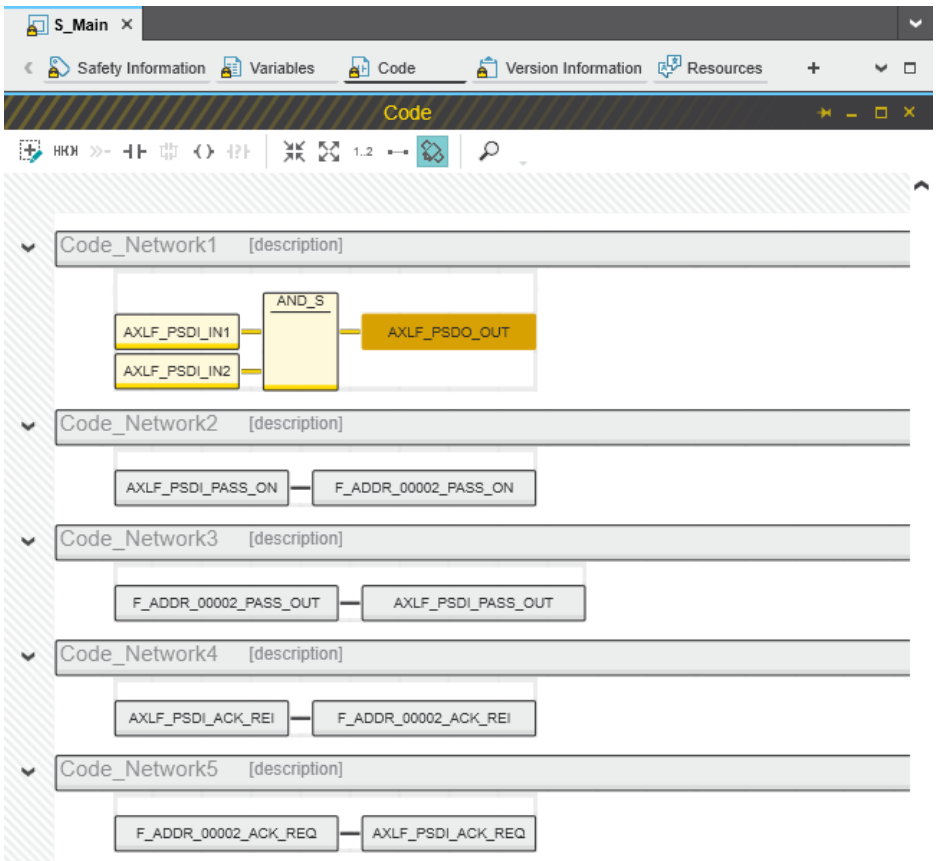


Figure 6-47 Safety-related program without errors

6.11 Transferring projects to the BPC 9102S and displaying online values

6.11.1 Transferring a non-safety-related project to the BPC 9102S

To transfer the non-safety-related project to the BPC 9102S (standard controller), proceed as follows:

- Double-click 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 note on user authentication in Section 6.5.5.

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

The non-safety-related project will be compiled and transferred to the BPC 9102S standard controller. Project execution will be initiated.

If the non-safety-related startup has been completed successfully, the standard control changes to the RUN state, indicated by the RUN LED continuously lit green.

The following information is displayed in the “Cockpit” editor:

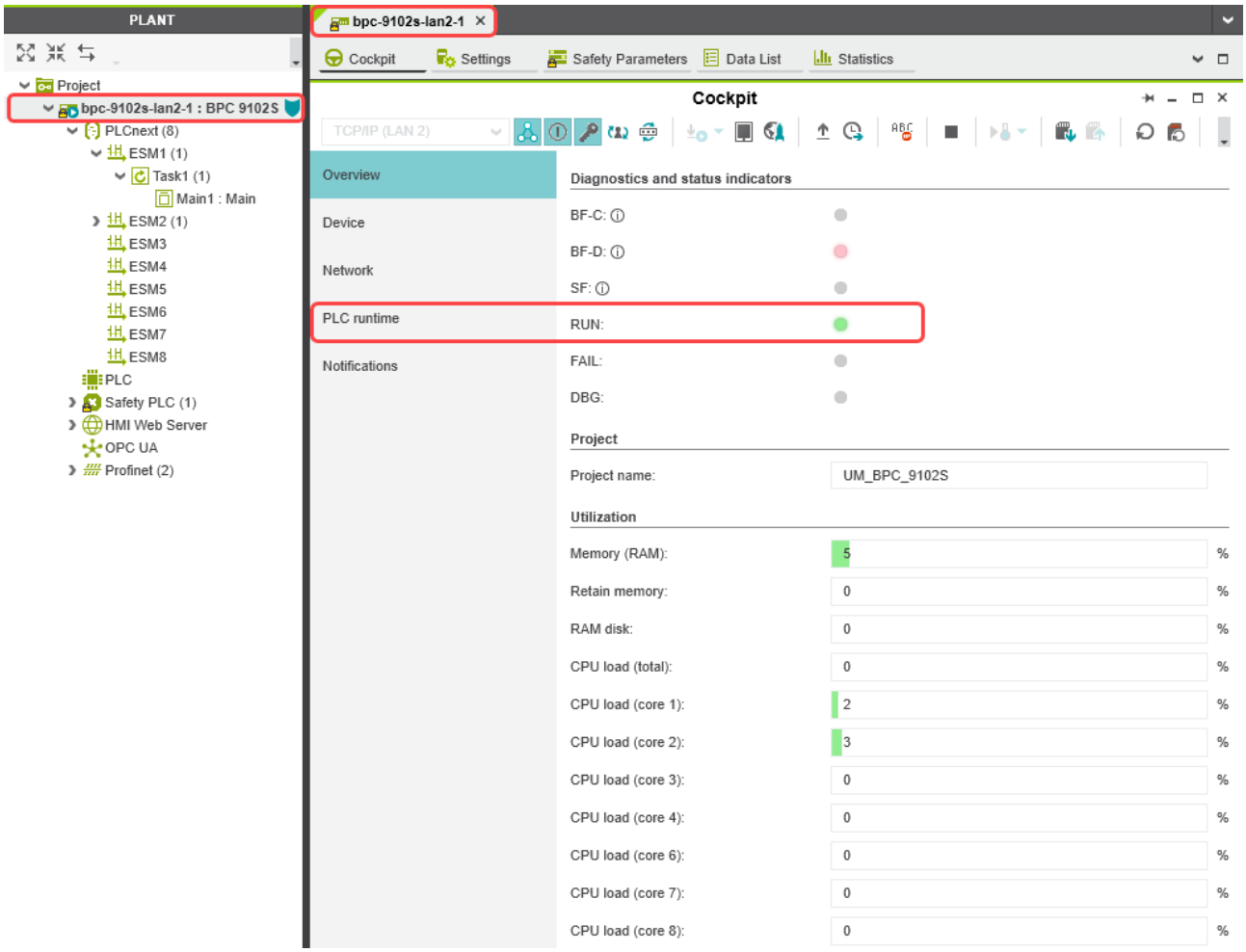


Figure 6-48 Standard controller in the “RUN” state

If the standard controller cannot be started up, for example due to an installation error, a corresponding error message appears in PLCnext Engineer.

The LEDs on the BPC 9102S indicate this status (see Section “Diagnostics and status indicators” on page 47).

The SPLC 3000 is in the safe state (failure state) because so far, a safety-related project has not been transferred to the SPLC 3000.

6.11.2 Transferring a safety-related project to the SPLC 3000 (specifying a controller password if necessary)

To transfer the project to the SPLC 3000, 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 note on user authentication in Section 6.5.5.

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

Specifying the SPLC 3000 controller password

The SPLC 3000 is protected by a controller password. Writing data to the SPLC 3000 or changing its operating mode is only possible after entering the controller password in PLCnext Engineer.

If this is the first time you are establishing a connection to the SPLC 3000, PLCnext Engineer will prompt you to specify a controller password.

- Specify a controller password, if you have not already done so, and the following dialog will be displayed.

  Use a password with a minimum length of eight characters. Use upper-case, lower-case, and special characters - the password is case sensitive.

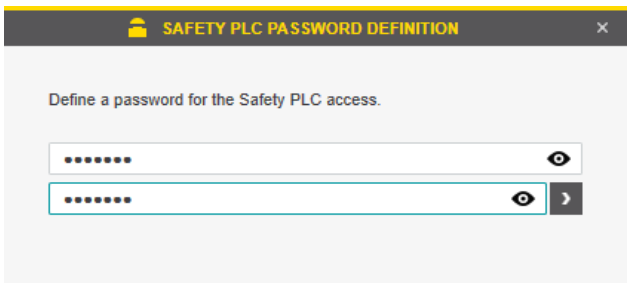


Figure 6-49 Controller password: entering the SPLC 3000 password

Please note: read information dialogs carefully and follow the instructions provided

If info dialogs appear, please refer to the PLCnext Engineer software online help function for further information.

- Acknowledge the messages in accordance with your application.

In the example:

Make sure no hazard is posed when the SPLC 3000 is started and/or stopped, e.g., after downloading a project.

Ensure the safety function is in order.

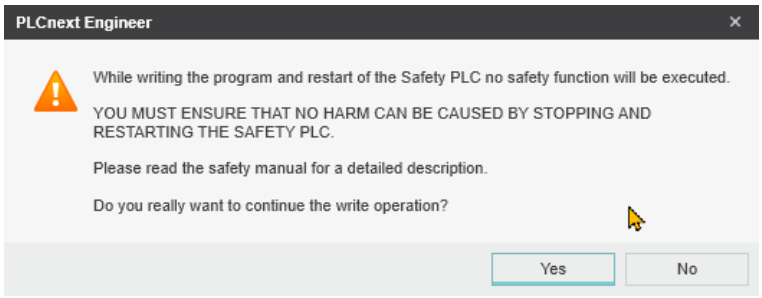


Figure 6-50 Info dialog: Avoid any hazard posed when starting and stopping the SPLC 3000

The project will be compiled and transferred to the SPLC 3000. Execution of the safety-related project will be initiated and the SPLC 3000 switches to the “RUN” state.

If commissioning was successful, the Run-S LED on the BPC 9102S is continuously lit green.

The following information is displayed in the “Safety Cockpit” editor:

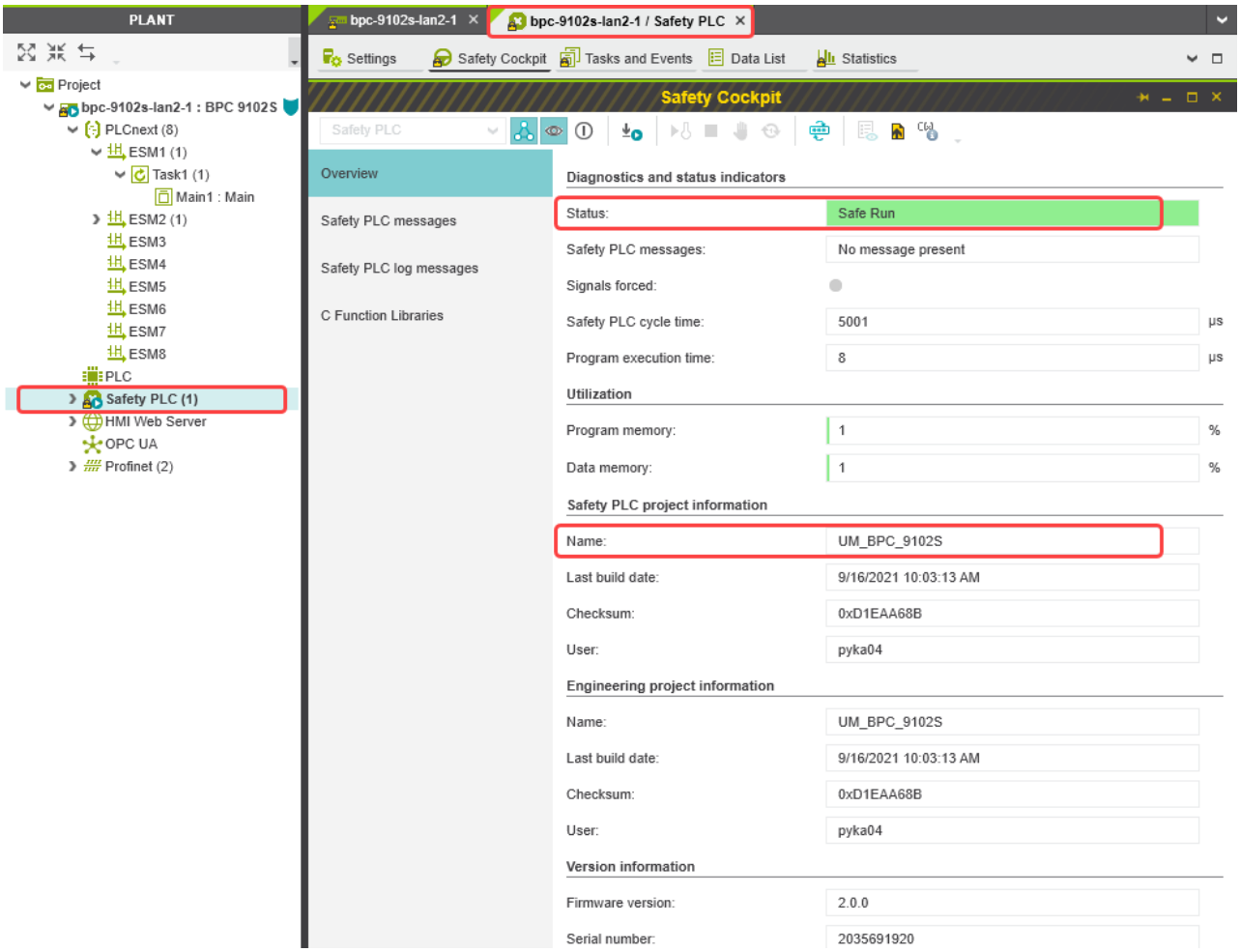


Figure 6-51 Safety Cockpit: SPLC 3000 in the “RUN” state – Safe Run

If the system cannot be commissioned, for example due to an installation error, a corresponding error message appears in PLCnext Engineer.

The LEDs on the BPC 9102S indicate this status (see Section “Diagnostics and status indicators” on page 47).

6.11.3 Displaying online values

In order for variable values to be displayed online, both projects (non-safety-related and safety-related) must have been transferred to the BPC 9102S (standard controller and SPLC 3000) and then successfully executed.
Moreover, you have to have established an online connection between PLCnext Engineer and the BPC 9102S.

Displaying non-safety-related online values

Proceed as follows:

- Double-click 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.

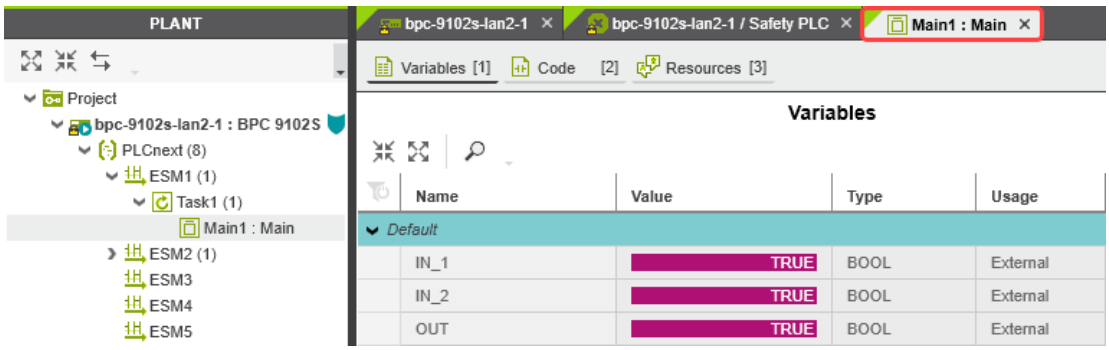


Figure 6-52 “Variables” editor: Online values of the variables used

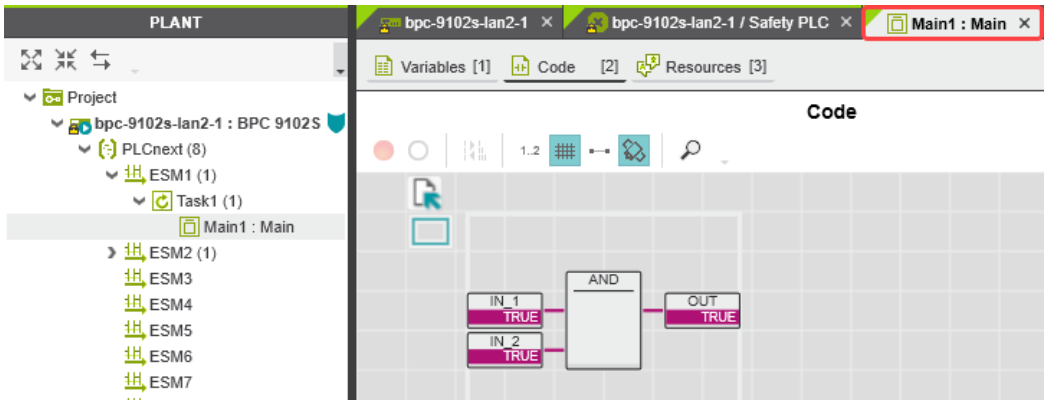


Figure 6-53 “Code” editor: Online values of the variables used

Displaying safety-related online values

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.

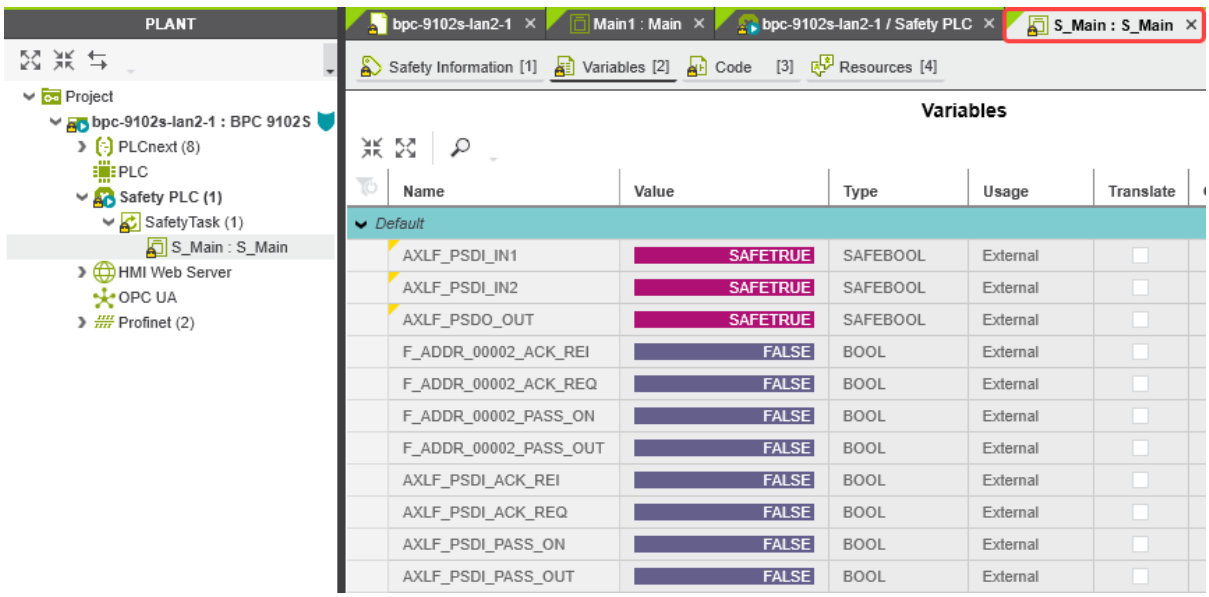


Figure 6-54 “Variables” editor (S_Main): Online values of the variables used

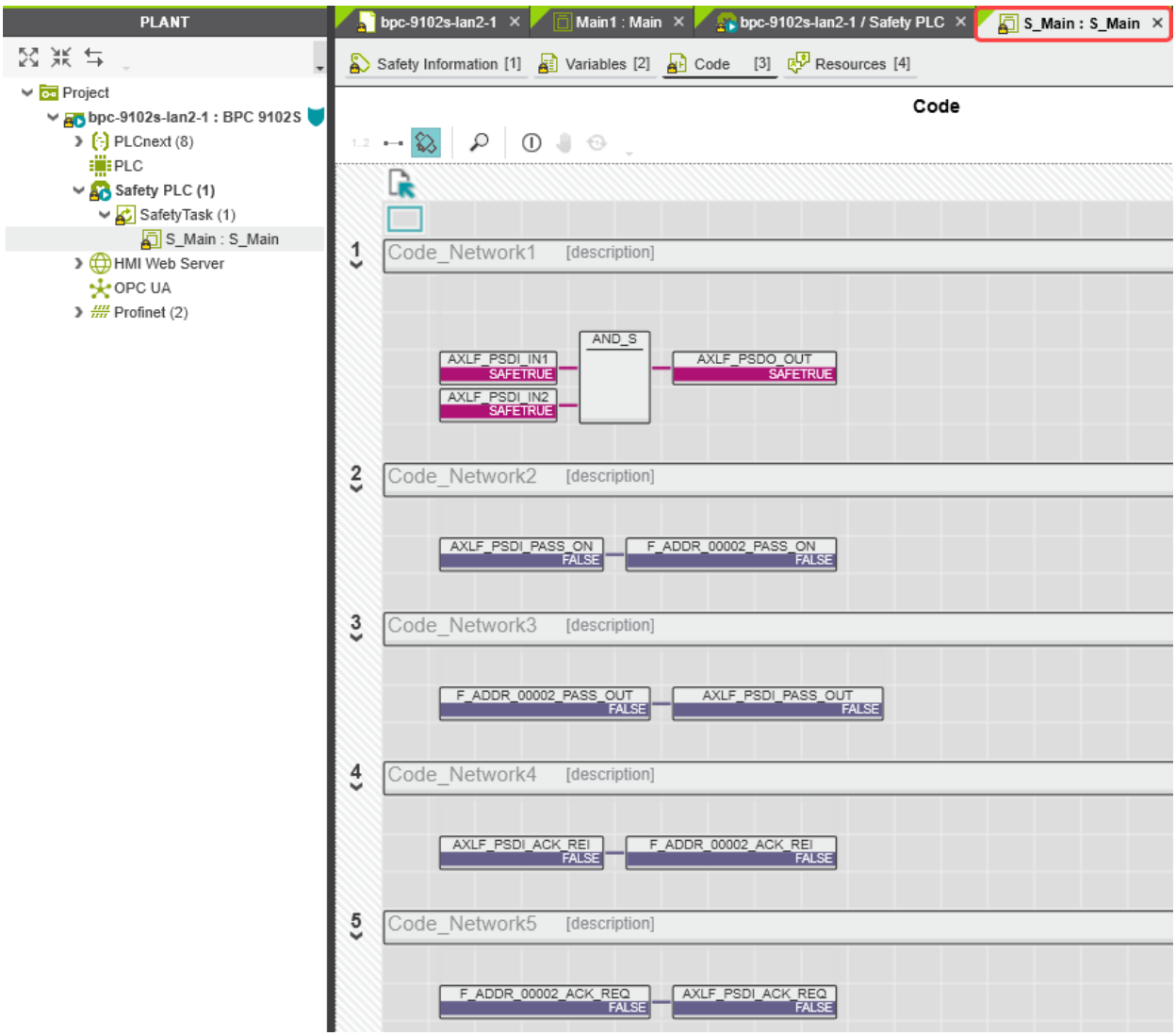


Figure 6-55 “Code” editor (S_Main): Online values of the variables used

6.12 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.

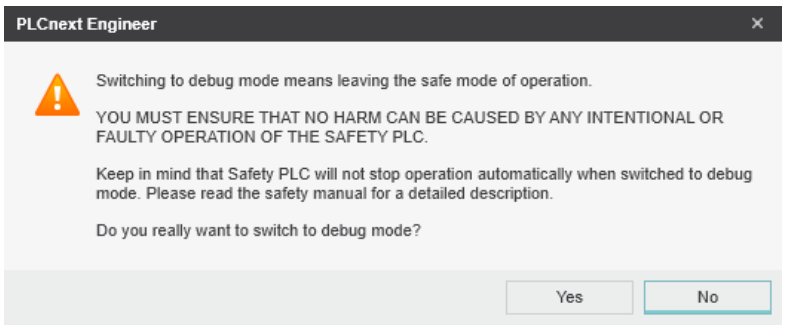


Figure 6-56 Exiting safe mode – switching to debug mode

The LED displays in debug mode are described in Table 3-1 on page 47.

- 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.

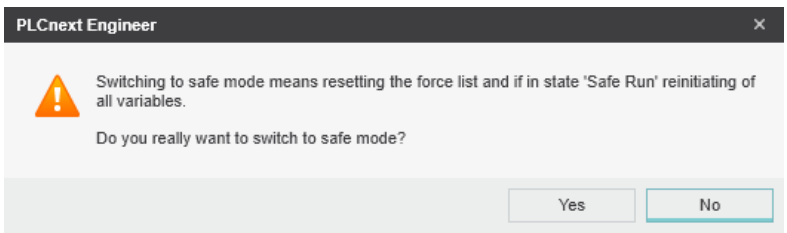


Figure 6-57 Exiting debug mode – switching to safe mode

6.13 Operator acknowledge

F-Devices whose communication relationship with the SPLC 3000 is aborted, for example due to a communication error, are passivated. Passivated F-Devices indicate this with the F_ADDR_XXXXX_PASS_OUT diagnostic/management variable.
To request reintegration immediately upon re-establishment of the communication relationship between the F-Device and F-Host, the F-Devices generate an operator acknowledge request. This is displayed with the F_ADDR_XXXXX_ACK_REQ diagnostic/management variable. This operator acknowledge request is acknowledged via an operator acknowledge reintegration (F_ADDR_XXXXX_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 F-Device and the SPLC 3000 is broken. The subsequent passivation of the F-Device prevents it from starting up again immediately once the communication relationship is re-established. This passivation is indicated by the Boolean diagnostic/management variable F_ADDR_00002_PASS_OUT.

Once the communication relationship has been re-established successfully, the passivated F-Device signals an operator acknowledge request via the Boolean diagnostic/management variable F_ADDR_00002_ACK_REQ. The F-Device thus waits for a reintegration acknowledgement.

Setting the Boolean exchange variable AXLF_PSDI_ACK_REI in the non-safety-related part of the example program cancels the passivation of the F-Device. As a result, the F-Device can be reintegrated into the network and re-establish the communication relationship.

The following Figure 6-58 shows the passivated AXL F PSDI8/4 1F F-Device.

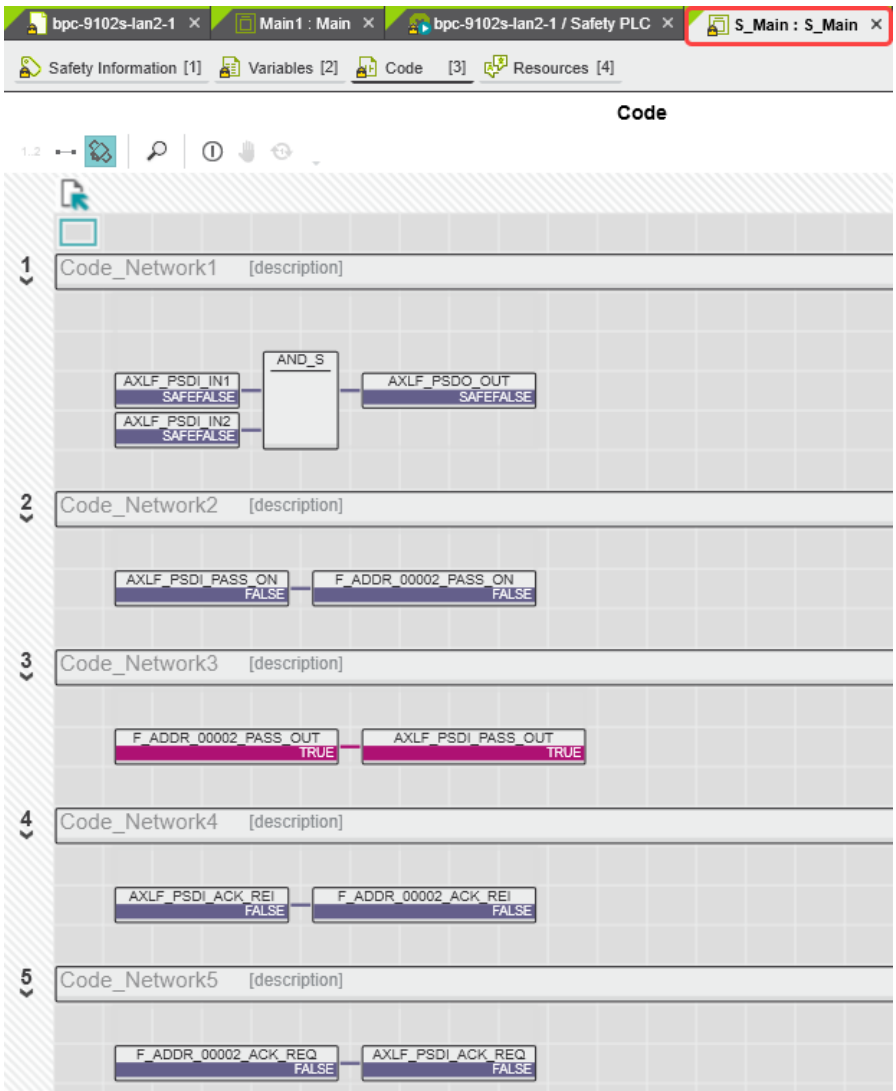


Figure 6-58 PLCnext Engineer – Passivated PROFIsafe F-Devices

In the example in Figure 6-58, the safe inputs and outputs have entered the SAFEFALSE state. This behavior is due to the passivation of the F-Device.

7 Errors: Diagnostics, messages, and removal

The BPC 9102S diagnostic and troubleshooting mechanisms are described in the following sections.

You will find further information on diagnostics for, among others, PLCnext Technology and PROFINET online at the listed addresses, in the listed user manuals, and in the PLCnext Engineer online help function:

– PLCnext Community at plcnext-community.net
  and in particular in the PLCnext Info Center

7.1 Diagnostics for PROFINET

Diagnostic messages for PROFINET are available as follows:

– Entries in the Notification Logger (Notification Manager)
– PROFINET-specific system variables in PLCnext Engineer (can be accessed in the application program)

7.2 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 184.

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 on page 143)

Refer to the device-specific user documentation for the F-Devices being used.

7.3 Diagnostics for SPLC 3000

The diagnostic and monitoring function integrated in the SPLC 3000 detects errors that have occurred. All serious errors detected in the SPLC 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 at the latest after the parameterized F_WD_TIME for the relevant output has elapsed. The PROFIsafe system switches to the safe state.

Exiting the failure state of the SPLC 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 BPC 9102S and wait at least 40 s after the LEDs have gone out before switching it back on again (Power UP), or
- Restart the BPC 9102S in the PLCnext Engineer software in the following editors:
  - "Cockpit" of the controller (standard controller)

Diagnostic messages for the SPLC 3000 are available as follows:

- Entries are stored in the diagnostic memory of the SPLC 3000 (can be read with PLCnext Engineer)
- As a hexadecimal value in the diagnostic parameter registers of the SPLC 3000. The registers are elements of the SPNSV2_TYPE structure; see Table 8-1 on page 143.
  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 "BPC 9102S errors and error codes" on page 132 occurs again.
- Errors occur that are not listed in Section "Possible errors" on page 130.

7.4 Possible errors

This section describes possible errors, their causes, effects, and remedy. Section "BPC 9102S errors and error codes" on page 132 lists errors in accordance with their error code.

Important notes:

FS-S-LED / FS-Bit / Failure State

Please note that for all error codes listed in the following Table 7-1 on page 132, the FS LED of the BPC 9102S is always on and the FS bit is set in the SPNS_DIAG_STATUS_REG register.

The SPLC 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 in the SPNS_DIAG_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 23.

Error codes – channel-dependent representation

Identical errors may occur on both independent processing channels of the SPLC 3000. Depending on the channel, they are marked as follows:

– 0x8xxx channel 1
(0x9xxx) channel 2
for example:
0x8001 channel 1
(0x9001) channel 2

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 PLCnext Control (standard controller) used.
2. Download the safety-related project to the SPLC 3000.

Manual, user-initiated compilation of projects is not required. The PLCnext Engineer software compiles the projects prior to each project download.

Configuration memory

The terms “SD card” and “(plug-in) configuration 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.

7.4.1 BPC 9102S errors and error codes

Table 7-1 BPC 9102S 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.	• Check whether the non-safety-related project is loaded on the PLCnext Control used. – If the non-safety-related project is not loaded on the standard controller, download the safety-related project to the SPLC 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%.	• 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 in accordance with the information in Section “Technical data” on page 187, if necessary.

Table 7-1 BPC 9102S 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)	The SD card was removed.	• Switch off the supply voltage of the BPC 9102S. • 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 BPC 9102S by means of power-off/power-on.  **NOTE: Startup of the BPC 9102S not ensured** For correct startup of the device, the supply voltage may only be switched on at the earliest 40 seconds after the device LEDs go out.

Table 7-1 BPC 9102S 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.	• 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 SPLC 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 7-1 BPC 9102S error codes

Error code (hex)	Error cause	Remedy or response
0x8129 (0x9129)	Inconsistent device parameters.	• Check the device configuration in your safety-related program. • Boot the SPLC 3000 by powering off/powering on the BPC 9102S. **NOTE: Startup of the BPC 9102S not ensured** For correct startup of the BPC 9102S, the supply voltage may only be switched on at the earliest 40 seconds after the device LEDs go out. • Download the non-safety-related project to the standard controller. Download the safety-related project to the SPLC 3000. Follow the instructions provided in the note on “Order of project downloads” above this table. If none of the steps described above remove the error: • Replace the BPC 9102S. • 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 SPLC 3000 by powering off/powering on the BPC 9102S. **NOTE: Startup of the BPC 9102S not ensured** For correct startup of the BPC 9102S, the supply voltage may only be switched on at the earliest 40 seconds after the device LEDs go out. If the procedure described above does not rectify the error, please contact your nearest Phoenix Contact representative.
0x812A (0x912A)	Inconsistent process data description.	• Check the 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 SPLC 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 BPC 9102S.

Table 7-1 BPC 9102S error codes

Error code (hex)	Error cause	Remedy or response
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.	• 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.	• 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 SPLC 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.
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 is below the specified range.	• Check the supply voltage. • Make sure the supply voltage is OK.
0x8249 (0x9249)	The supply voltage is above the specified range.	• 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 BPC 9102S within the range specified.

Table 7-1 BPC 9102S error codes

Error code (hex)	Error cause	Remedy or response
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.

7.5 Evaluation and acknowledgment of module-specific diagnostic messages

Depending on the error type, errors that are diagnosed in the Axioline F and Axioline Smart Elements PROFIsafe modules from Phoenix Contact used are transmitted to the BPC 9102S as diagnostic messages via 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 Axioline F backplane bus system. These function blocks enable global or local device-specific diagnostics.

For this purpose, the AsynCom_PN_1 function block from the AsynCom_9 library for PLCnext Engineer must be used. This function block is used for reading information of the connected PROFINET devices. The function block receives this information from the configuration of the BPC 9102S (device IDs, PROFINET names, etc.).

In addition, function blocks from the PN_Dev_Diag_5 library for PLCnext Engineer must also be used. An example of device-specific PROFIsafe diagnostics is the PNFD_AXL_Diag_2 function block. This function block is used to perform diagnostics on a safety-related device of the Axioline F product group via the PROFIsafe address. Displayed diagnostic messages can be confirmed (acknowledged) with the help of the function block.

7.5.1 AsynCom_PN_1 function block

Function block for reading information of the connected PROFINET devices.

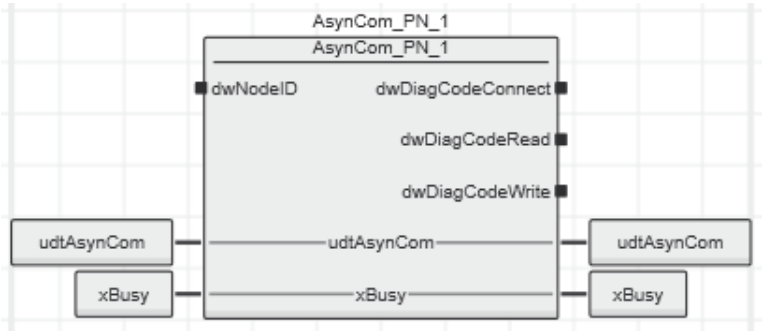


Figure 7-1 AsynCom_PN_1 function block (instance: AsynCom_PN_1)

7.5.2 PNFD_AXL_Diag_2 function block

Function block for diagnostics of a secure device of the Axioline F product group via the PROFIsafe address. Diagnostic messages that need to be confirmed can be confirmed with the help of the block.

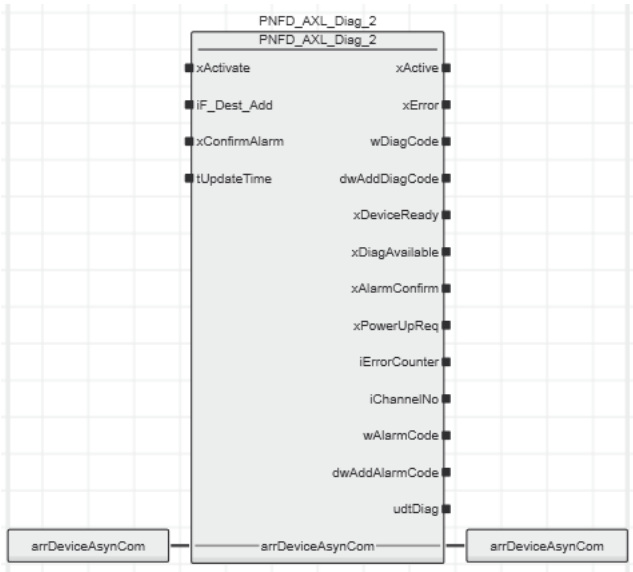


Figure 7-2 PNFD_AXL_Diag_2 function block (instance: PNFD_AXL_Diag_2)

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 your 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

Observe these notes to prevent unexpected machine startup after operator acceptance via the “Operator Acknowledgment” command.

8 System variables and status information

8.1 General information

This section describes the system variables that are available for the BPC 9102S.

The BPC 9102S has a register set that is used for diagnostics and simple control of the BPC 9102S.

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 flags, global variables).

8.2 Data structures

Some system variables of the BPC 9102S are organized as data structures. The data structure for this type of system variable contains further system variables.
In the Init Value Configuration of PLCnext Engineer, you can see which specific system variables belong to a system variable that is organized as a data structure.

To open the Init Value Configuration for a system variable organized as a data structure, proceed as follows:

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

The “/ PLC” controller editor group opens.

- Select the “Data List” editor.

Alternatively, you can open the “Data List” editor via the controller node in the “PLANT” area.

- Open the “System Variables” section.
- In the “Variable (PLC)” column, click on the arrow to display additional information.

The data type of the system variable is displayed in the “Type” column of the additional information.

- Select the row for the system variable organized as a data structure whose associated system variables you would like to view.
  To do this, click on the first column in the row for the system variable organized as a data structure.
- Click on the  button to open the Init Value Configuration for the system variable organized as a data structure.

The Init Value Configuration for the selected system variable organized as a data structure opens below the “Data List” editor.

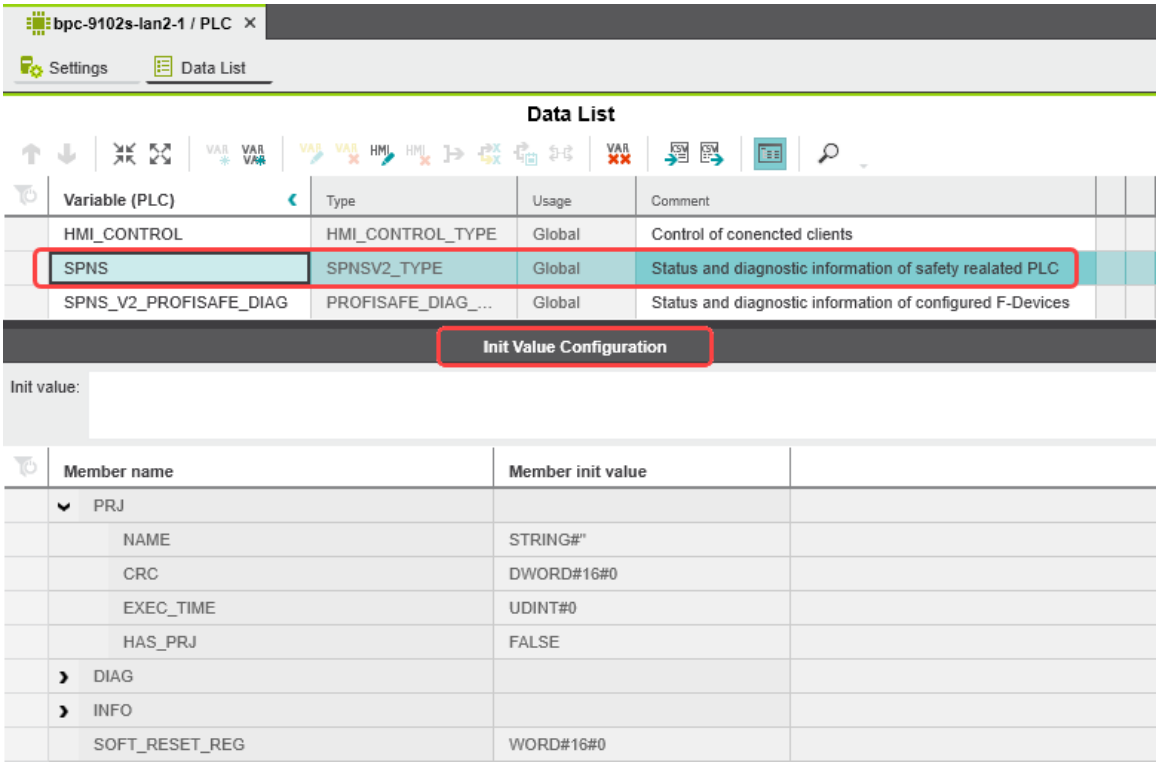


Figure 8-1 Example BPC 9102S: Init Value Configuration for the SPNS system variable organized as a data structure (SPNSV2_TYPE data type)

The “Member name” column in the Init Value Configuration displays all the system variables contained in the system variable which is organized as a data structure.

8.3 System variables of the SPLC 3000

8.3.1 SPNS system variable

The SPNS system variable uses the SPNSV2_TYPE data structure to provide the following information on the SPLC 3000.

Table 8-1 SPNS system variable and elements of the SPNSV2_TYPE data structure

System variable/elements	Type	Meaning
SPNS	SPNSV2_TYPE	The SNPS system variable provides the information in the SPNSV2_TYPE data structure.
PRJ		
NAME	STRING	PLCnext Engineer project name.
CRC	DWORD	Project CRC (32 bits) of the SPLC 3000 boot project.
EXEC_TIME	UDINT	Runtime of the SPLC 3000 program cycle in µs.
HAS_PRJ	BOOL	The safety-related application program and the program sources are contained in the memory of the SPLC 3000.
DIAG		
STATUS_REG	WORD	Diagnostic status register of the SPLC 3000 The diagnostic status register of the SPLC 3000 contains the status information of the SPLC 3000. It mirrors the state of the SPLC 3000 at all times including any error states that have occurred on the SPLC 3000. Additional information and error parameters, in particular in the failure state (FS), are included in the relevant diagnostic parameter registers of the SPLC 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 145.
PARAM_REG	WORD	Diagnostic parameter register 1 of the SPLC 3000 (error code).
PARAM_2_REG	WORD	Diagnostic parameter register 2 of the SPLC 3000 (additional error messages for service/support).
EXT_PARAM_REG	DWORD	Extended diagnostic parameter register of the SPLC 3000 (additional error messages for service/support).
CH2_PARAM_REG	WORD	Diagnostic parameter register 1 of the SPLC 3000 channel 2 (CH2) (error code).
CH2_PARAM_2_REG	WORD	Diagnostic parameter register 2 of the SPLC 3000 channel 2 (CH2) (additional error messages for service/support).
CH2_EXT_PARAM_REG	DWORD	Extended diagnostic parameter register of the SPLC 3000 channel 2 (CH2) (additional error messages for service/support).
INFO		
CYCLE_TIME	UDINT	SPLC 3000 cycle in µs
TEMP		
TEMP_CURRENT	INT	Currently measured SPLC 3000 temperature

Table 8-1 SPNS system variable and elements of the SPNSV2_TYPE data structure

System variable/elements	Type	Meaning
TEMP_MIN	INT	Minimum measured SPLC 3000 temperature since the last power-on of the device.
TEMP_MAX	INT	Maximum measured SPLC 3000 temperature since the last power-on of the device.
STATUS_REG	WORD	SPLC 3000 temperature status register 0x0000: The temperature of the SPLC 3000 is in the non-critical range. 0x0080: The temperature of the SPLC 3000 is in the critical range, close to the tolerance threshold. The SPLC 3000 remains in RUN state and, in parallel, issues a warning with error code 0xFA41. 0x8000: The temperature of the SPLC 3000 is beyond the permitted range. The SPLC 3000 switches to the safe state and issues an error message with error code 0x924D.
CPU		
LOAD_CURRENT	INT	Current SPLC 3000 CPU load
LOAD_MIN	INT	Minimum measured SPLC 3000 CPU load since the last power-on of the device.
LOAD_MAX	INT	Maximum measured SPLC 3000 CPU load since the last power-on of the device.
STATUS_REG	WORD	SPLC 3000 CPU status register
FW_VERSION		
VERSION_MAJOR	BYTE	Major version of the SPLC 3000 firmware
VERSION_MINOR	BYTE	Minor version of the SPLC 3000 firmware
VERSION_BUILD	WORD	Build number of the SPLC 3000 firmware
FPGA_VERSION		
VERSION_MAJOR	BYTE	Major version of the SPLC 3000 hardware FPGA
VERSION_MINOR	BYTE	Minor version of the SPLC 3000 hardware FPGA
VERSION_BUILD	WORD	Build number of the SPLC 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 SPLC 3000

8.3.2 SPNS.DIAG.STATUS_REG.xxx diagnostic status register

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
BATT	BOOL	Low capacity of the SPLC 3000 real-time clock energy storage system. TRUE: Energy storage device is being charged. FALSE: Energy storage device is fully charged. The charging process is complete.
DBG [3]	BOOL	Non-safe debug mode of the SPLC 3000 The SPLC 3000 is in one of the two DEBUG states (DEBUG RUN or DEBUG STOP/SINGLE).
DD	BOOL	Diagnostic message of an F-Device is present.
EST	BOOL	There is an entry in the error memory of the safe operating system (error stack) of the SPLC 3000. Diagnostic and error messages from the safe SPLC 3000 operating system are present. These messages can be read and evaluated via 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 SPLC 3000 An error has been detected which sets the SPLC 3000 to the failure state. The corresponding additional error code is included in this state in the diagnostic parameter registers of the SPLC 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG).
INIT [2]	BOOL	Initialization of the SPLC 3000 Initialization of the SPLC 3000 firmware (safe operating system) has been performed and completed without errors.
IO [2]	BOOL	Initialization of the SPLC 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 SPLC 3000 is supplied with power. The firmware was downloaded to the main memory of the BPC 9102S and started. The comprehensive self-test routines of the device have been completed successfully.
POST	BOOL	Power-on self-test of the SPLC 3000 (**P**OWER **O**N **S**ELF **T**EST) Power-on self-test of the SPLC 3000 is active.

Table 8-2 Elements in the diagnostic status register (SPNS.DIAG.STATUS_REG.xxx)

System variable/elements	Type	Meaning
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 SPLC 3000 operating system and started.
RUN [3]	BOOL	Execution of the safety-related application program (RUN) The SPLC 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 SPLC 3000 and PROFINET controller Synchronization between the SPLC 3000 and the PROFINET controller was completed successfully.
WARN	BOOL	Warning of the SPLC 3000 A group warning message of the SPLC 3000 is present.

2	The variables indicate the startup status of the safety-related SPLC 3000 controller. The startup sequence of the SPLC 3000 is divided into the following five consecutive sections: 1. Power-on process 2. Initialization of the SPLC 3000 3. Loading and starting of the safety-related application program 4. Synchronization of the SPLC 3000 and the standard controller 5. Initialization of the SPLC 3000 F-Host for I/O channel communication
3	The variables indicate the RUN and DEBUG operating states of the SPLC 3000.

SPNS.DIAG.STATUS_REG diagnostics status register: Meaning of the individual bits

The SPNS.DIAG.STATUS_REG diagnostic status register contains the status information of the SPLC 3000. It mirrors the state of the SPLC 3000 at all times, including any error states that have occurred on the SPLC 3000. Additional information and error parameters, in particular in the failure state (FS), are contained in the associated diagnostic parameter registers of the SPLC 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG) and in the extended diagnostic parameter register (SPNS.DIAG.EXT.PARAM_REG).

Table 8-3 Diagnostic status register of the SPLC 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 SPLC 3000. The startup sequence of the SPLC 3000 is divided into the following five steps:

PON Power-on process complete

This bit is set as soon as the SPLC 3000 is supplied with power. The firmware was downloaded to the main memory of the SPLC 3000 and started. The comprehensive self-test routines of the device have been completed successfully.

INIT Initialization of the SPLC 3000 complete

This bit is set as soon as initialization of the SPLC 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 SPLC 3000 operating system without any errors and started.

SYN Synchronization of the SPLC 3000 and the standard controller

The bit is set when the SPLC 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 SPLC 3000.

RUN RUN mode of the SPLC 3000

This bit is set when the SPLC 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 SPLC 3000

This bit is set when the SPLC 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 indicators

RUN bit	DBG bit	Status	LED FS-S
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

Bits 7 and 10

WARN The set WARN (WARNING) bit indicates a group warning message of the SPLC 3000.

Bit 12

EST The EST (error stack) bit indicates that diagnostic and error messages for the safe SPLC 3000 operating system are present. These messages can be read and evaluated via 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 SELF TEST

This bit is set for the duration of the comprehensive power-on self-test of the SPLC 3000. It is reset once the power-on self-test is complete.

Bit 15

FS Failure state

This bit is set as soon as an error has been detected that sets the SPLC 3000 to the failure state. The corresponding additional error code is included in this state in the diagnostic parameter registers of the SPLC 3000 (SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG).

Res. Reserved

8.3.3 SPNS_V2_PROFISAFE_DIAG system variable

The SPNS_V2_PROFISAFE_DIAG system variable uses the PROFISAFE_DIAG_OUT data structure to provide further information on the SPLC 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 data 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	–

8.3.4 SPNS_CONTROL_COMMAND and SPNS_CONTROL_CONFIRM system variables

The SPNS_CONTROL_COMMAND system variable is used to request the resetting of diagnostic values from the non-safety-related project. Via the system variable SPNS_CONTROL_CONFIRM, the SPLC 3000 confirms that the diagnostic values have been reset in the non-safety-related project.

SPNS_CONTROL_COMMAND

This system variable requests the resetting of diagnostic values from the non-safety-related project.

Table 8-6 SPNS_CONTROL_COMMAND system variable and elements of the SPNS_CONTROL_TYPE data structure

System variable/elements	Type	Meaning
SPNS_CONTROL_COMMAND	SPNS_CONTROL_TYPE	Data structure with 32 bits for enabling SPLC 3000 functions.
CODE	DWORD	Bit 0: Resets the minimum and maximum safety roundtrip times (SRT_MIN, SRT_MAX). Data direction: Standard controller → SPLC 3000 (F-Host)
PARAM	DWORD	Bits 1 ... 31: Reserved.

SPNS_CONTROL_CONFIRM

This system variable shows in the non-safety-related project the acknowledgement from the SPLC 3000 that diagnostic values have been reset.

Table 8-7 SPNS_CONTROL_CONFIRM system variable and elements of the SPNS_CONTROL_TYPE data structure

System variable/elements	Type	Meaning
SPNS_CONTROL_CONFIRM	SPNS_CONTROL_TYPE	Data structure with 32 bits for confirming functions of the SPLC 3000 that have been requested via the SPNS_CONTROL_COMMAND variable.
CODE	DWORD	Bit 0: Confirms the resetting of the minimum and maximum safety roundtrip times (SRT_MIN, SRT_MAX). Data direction: SPLC 3000 (F-Host) → standard controller
PARAM	DWORD	Bits 1 ... 31: Reserved.

8.3.5 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 6-35 on page 108).

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 8-8 Management/diagnostic variables for each configured F-Device

System variable	Type	Meaning
F_ADDR_XXXXX_PASS_ON *)	BOOL	F-Device XXXXX is passivated 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. Take appropriate measures to ensure that your system/ machine does not present any danger when passivation of the F-Device is reset.
F_ADDR_XXXXX_PASS_OUT *)	BOOL	F-Device XXXXX is passivated. Possible reasons for passivation include: – 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 8-8 Management/diagnostic variables for each configured F-Device

System variable	Type	Meaning
F_ADDR_XXXXX_ACK_REQ *)	BOOL	F-Device XXXXX requires an operator acknowledge request after an error has been eliminated. Possible reasons for activating the operator acknowledge request: – 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	If F-Device XXXXX requires an operator acknowledge request, it can be acknowledged by an operator acknowledge reintegration from the F-Host of the BPC 9102S (F_ADDR_XXXXX_ACK_REI).
F_ADDR_XXXXX_DEVICE_FAULT *)	BOOL	Error in an 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 using the F_ADDR_XXXXX_ACK_REI or ACK_REI_GLOBAL variable. If the cause has been eliminated, the F_ADDR_XXXXX_DEVICE FAULT variable is set to FALSE again. For information on which errors cause the used F-Device to control this variable, please refer to the device-specific user documentation.
F_ADDR_XXXXX_CE_CRC *)	BOOL	Communication error (F_CE_CRC) This parameter is set if at least one of the following reasons applies: – There is inconsistent parameterization between F-Host and F-Device. – A communication error between F-Host and F-Device is present; for example, the F-Device has detected a communication error during operation that was caused by an incorrect CRC checksum. 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. 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”). 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.

Table 8-8 Management/diagnostic variables for each configured F-Device

System variable	Type	Meaning
F_ADDR_XXXXX_WD_TIME_OUT *)	BOOL	Communication error (F_WD_TIME_OUT) Set if the F-Device has detected a communication error caused by the parameterized F_WD_Time being exceeded. 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.
F_ADDR_XXXXX_IPAR_OK *)	BOOL	F-Device indicates that the iParameters have been applied This variable is set when the F-Device indicates that it has applied the iParameters.
F_ADDR_XXXXX_IPAR_EN *)	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 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. **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.
F_ADDR_XXXXX_CHF_ACK_REQ *)	BOOL	A channel error in the F-Device can be acknowledged (CHF_ACK_REQ_S). (Only for F-Devices in accordance with PROFIsafe profile version **2.6MU1**)
F_ADDR_XXXXX_CHF_ACK_REI *)	BOO	Channel error acknowledgement (CHF_ACK_C) (Only for F-Devices in accordance with PROFIsafe profile version **2.6MU1**)
F_ADDR_XXXXX_CE_CRC_H *)	BOOL	Communication error (F_CE_CRC_H) Local F-Host driver reports communication error.
F_ADDR_XXXXX_WD_TIMEOUT_H *)	BOOL	Communication error (F_WD_TIMEOUT_H) Local F-Host driver reports communication error.
F_ADDR_XXXXX_LOOPBACK *)	BOOL	Communication error (loopback check) Local F-Host driver reports communication error.
*) XXXXX = Number of the F-Device (e.g., F_ADDR_00001_PASS_ON; see Figure 6-37 on page 109)		

WARNING:

The variables specified in the table can be toggled. Program an evaluation function in the PLCnext Engineer software (e.g., using edge detection).

8.3.6 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 6-36 on page 109).

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 8-9 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 include: – 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: – 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 eliminated 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 eliminated, the F_ADDR_XXXXX_DEVICE FAULT variable is set to FALSE again. For information on which errors cause the used F-Device to control this variable, please refer to the device-specific user documentation.

Table 8-9 Management/diagnostic variables for F-Devices [...]

System variable	Type	Meaning
CE_CRC_GLOBAL	BOOL	Communication error (F_CE_CRC) This parameter is set if at least one of the following reasons applies: – There is inconsistent parameterization between F-Host and F-Device. – A communication error between F-Host and F-Device(s) is present; for example, at least one F-Device has detected a communication error during operation that was caused by an incorrect CRC checksum. If this variable was set to TRUE during operation, the cause of the error must be eliminated 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. 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”).
WD_TIME_OUT_GLOBAL	BOOL	Communication error (F_WD_TIME_OUT) Set if at least one F-Device has detected a communication error caused by the parameterized F_WD_Time being exceeded. If this variable was set to TRUE during operation, the cause of the error must be eliminated 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.
CHF_ACK_REI_GLOBAL	BOOL	At least one F-Device reports a channel error in the F-Device and can be acknowledged (CHF_ACK_C). (Only for F-Devices in accordance with PROFIsafe profile version **2.6MU1**)
CHF_ACK_REQ_GLOBAL	BOOL	At least one F-Device reports a channel error in the F-Devices and can be acknowledged (CHF_ACK_REQ_S). (Only for F-Devices in accordance with PROFIsafe profile version **2.6MU1**)
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).

8.3.7 PROFINET system variables

The table below describes the PROFINET system variables of the integrated PROFINET controller functionality.

Table 8-10 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 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 of the type 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 8-11 PROFINET system variables (PROFINET device functions)

System variable	Type	Meaning
PND_S1_PLC_RUN	BOOL	Status of the higher-level PROFINET controller Information indicating 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.
PND_IO_DRIVEN_BY_PLC	INT	Applicative system redundancy: Number of the PROFINET controller currently connected to the PROFINET device. Specifies the higher-level PROFINET controller from which the data in the PROFINET device originates. 0: No PROFINET controller 1: PROFINET controller A 2: PROFINET controller B

8.3.8 RTC (System time) system variable

The RTC system variable is a system variable organized as a data structure. It uses the RTC_TYPE structure to provide information on the system time.

Table 8-12 RTC system variable and elements of the RTC_TYPE structure

System variable/elements	Type	Meaning
RTC	RTC_TYPE	The structure provides information about the real-time 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)

8.3.9 DEVICE_STATE system variable

The DEVICE_STATE system variable is a system variable organized as a data structure. It 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 8-13 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 a percentage)
CPU_LOAD_PER_CORE		Information on the utilization per processor core
[1] ... [8]	USINT	Current processor load of the processor cores 1 … 8 (percentage)

8.3.10 FAN_STATE system variable

The FAN_STATE system variable is a system variable organized as a data structure. It uses the FAN_INFO structure to provide information on the optional fan module.

Table 8-14 FAN_STATE system variable and elements of the FAN_INFO structure

System variable/elements	Type	Meaning
FAN_STATE	FAN_INFO	Data structure
FAN_MAINTENANCE	BOOL	Fan maintenance required.
FAN_DEFECT	BOOL	The fan is not connected or defective. **NOTE: Device defect due to overheating** • Immediately replace the fan when the defect occurs.

8.3.11 USER_PARTITION system variable

The USER_PARTITION system variable is a system variable organized as a data structure. You can use the USER_PARTITION system variable to can call up various pieces of information and memory statistics for the user partition (overlay file system). The partition can be on an external SD card or on the internal memory. This memory is organized in blocks. One block has a constant, fixed size, and a file always occupies one or more blocks.

A certain number of blocks are reserved in the Linux system for the root user. The reserved blocks are only available for the root user account and ensure its ability to act even if the memory is occupied (e.g., for log outputs).

Table 8-15 USER_PARTITION system variable and elements of the PARTITION_INFO data structure

System variable/elements	Type	Meaning
USER_PARTITION	PARTITION_INFO	Data structure
MEM_TOTAL	ULINT	Total memory of the partition in bytes (including reserved blocks)
MEM_FREE	ULINT	Free memory available for use in bytes (not including reserved blocks)
MEM_USED	ULINT	Used memory in bytes (including reserved blocks)
MEM_USAGE	USINT	Used memory as a % (not including reserved blocks)

8.3.12 ESM_DATA (task handling) system variable

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 8-16 ESM_DATA system variable for task handling and elements of the ESM_DAT structure

System variable/elements	Type	Meaning
ESM_DATA	ESM_DAT	Information on Execution and Synchronization Manager task handling for all eight processor cores of the RFC
ESM_COUNT	USINT	Number of ESMs (one ESM per processor core)
ESM_INFOS		Information on ESMs [1 ... 8]
[1] ... [8]		
TASK_COUNT	UINT	Number of tasks that have been configured for the ESM
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: time interval in µs For acyclic tasks: 0
PRIORITY	INT	Priority of the task
WATCHDOG	LINT	Watchdog time in µs (0 = no watchdog)
LAST_EXEC_DURATION	LINT	Execution duration of the task in the previous cycle in µs (including interruptions by higher priority tasks)
MIN_EXEC_DURATION	LINT	Minimum execution duration of the task in µs (including interruptions by higher priority tasks)
MAX_EXEC_DURATION	LINT	Maximum execution duration of the task in µs (including interruptions by higher priority tasks)
LAST_ACTIVATION_DELAY	LINT	Delay time of the task in the previous cycle in µs
MIN_ACTIVATION_DELAY	LINT	Minimum delay time of the task in µs (delay occurs if higher priority tasks are pending at the time of task activation)
MAX_ACTIVATION_DELAY	LINT	Maximum delay time of the task in µs (delay occurs if higher priority tasks are pending at the time of task activation)
EXEC_TIME_THRESHOLD	LINT	Configured time in µs.
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.

Table 8-16 ESM_DATA system variable for task handling and elements of the ESM_DAT structure

System variable/elements	Type	Meaning
NAME	STRING	Name or designation of task
EXCEPTION_COUNT	USINT	Number of exceptions ...
EXCEPTION_INFOS		Information on exceptions [1 ... 8]
[1] ... [8]		
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		

8.3.13 HMI_STATUS system variable

The HMI_STATUS system variable uses the HMI_STATUS_TYPE structure to provide information on client connections to an HMI web server that can be programmed in PLCnext Engineer.

Table 8-17 HMI_STATUS system variable and elements of the HMI_STATUS_TYPE structure

System variable/elements	Type	Meaning
HMI_STATUS	HMI_STATUS_TYPE	Data structure: 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	HMI_STATUS_ARRAY	Information on existing client connections
[1] ... [256]	HMI_STATUS_STRUCT	Client connections 1 ... 256
SESSION_ID	STRING	Session ID of the client connection
STATION_ID	STRING	Station ID of client connection
LAST_REQ	LINT	Time of the last request from the client to the controller.
IP_ADDRESS	IP_ADDRESS_ARRAY	IP address of the connected client
[0] ... [3]	BYTE	IP address in hexadecimal format: [C0].[A8].[01].[64] ⇒ 192.168.1.100

8.3.14 HMI_CONTROL system variable

The HMI_CONTROL system variable can be used to disconnect a client from a PLCnext Engineer HMI web server.

The HMI_CONTROL system variable is a system variable organized as a data structure.

Table 8-18 HMI_CONTROL system variable and elements of the HMI_CONTROL_TYPE structure

System variable/elements	Type	Meaning
HMI_CONTROL	HMI_CONTROL_TYPE	Data structure: Information on individual client connections
Clients	HMI_CONTROL_ARRAY	Information on existing client connections
[1] ... [256]	HMI_CONTROL_STRUCT	Client connections 1 ... 256
DISABLE	BOOL	• To break the connection between the respective client and the PLCnext Engineer HMI web server, set this bit to 1.

8.3.15 PLC_CRC_PRJ system variable

The PLC_CRC_PRJ system variable provides information on the CRC of the non-safety-related project.

Table 8-19 PLC_CRC_PRJ system variable

System variable	Type	Meaning
PLC_CRC_PRJ	ULINT	Information on the CRC of the non-safety-related project

8.4 TCP_SOCKET, UDP_SOCKET, and TLS_SOCKET function blocks

You can use the TCP_SOCKET and UDP_SOCKET function blocks 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 8-20 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

9 Web-based management WBM system

In the Web-based management (WBM) system, you can access static and dynamic BPC 9102S information and modify certain BPC 9102S settings. The WBM system can be called up via any of the BPC 9102S Ethernet interfaces.

You will find a description of the Web-based management system in the PLCnext Info Center.

9.1 Licenses and legal information

The BPC 9102S uses a Linux operating system.

All the license information stored in the BPC 9102S can be called up via the “Licenses and Legal Information” link on every page of the WBM BPC 9102S.

10 Removing the hardware

10.1 Safety notes

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) in accordance with EN 61340-5-1 and IEC 61340-5-1.

Please note:

- Disconnect the power to the BPC 9102S before any work on the device.
- Make sure that the supply voltage cannot be switched on again by unauthorized persons.

10.2 Removing the power supply

- Remove power from the BPC 9102S.
- Use a bladed screwdriver to loosen the two screws on the COMBICON connector.
- Remove the supply cable from the BPC 9102S by unplugging the three-position COMBICON plug from the device.

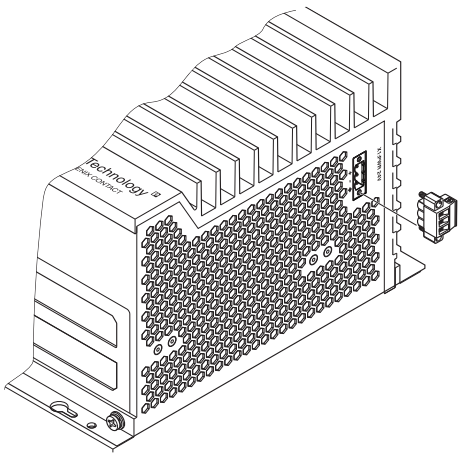


Figure 10-1 Removing the power supply

10.3 Removing the connectors

10.3.1 Removing the Ethernet connector

- Remove any Ethernet connectors connected to the BPC 9102S.

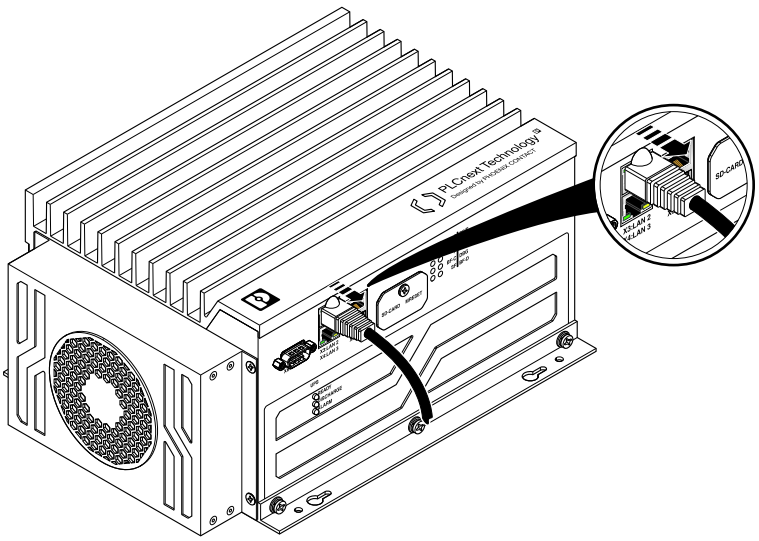


Figure 10-2 Cabling between an Ethernet network and the BPC 9102S

10.3.2 Removing connectors from the COM interface

- If necessary, loosen both screws on the D-SUB 9 connector.
- If necessary, remove the D-SUB 9 connector from the BPC 9102S.

10.4 Removing the SD card (configuration memory)

NOTE:

– Please note that the SD card may not be removed during operation. If the SD card is removed during operation, the BPC 9102S will switch to the safe state (failure state).

• Always disconnect the power supply to the BPC 9102S before removing the SD card.

– Observe Section “Notes on security” on page 15, in particular in terms of access protection for the SD card.

Removing the SD card

Please also refer to Figure 4-4 on page 63:

- To remove the SD card, loosen the screw (3) in the cover (2) using a Torx® TX 10 screwdriver (ordering data is available in Section 14.1.3, “Accessories”).
- Then swivel the cover (2) to the side so that you can easily access the SD card holder (1).
- Lightly push the SD card far enough into the SD card holder until the snap-in mechanism releases the SD card and partially ejects the SD card from the SD card holder.
- Remove the SD card.
- After removing the SD card, reattach the cover (2) by tightening the screw (3) to protect the SD card slot against unintentional damage and actuation.

NOTE: Unauthorized SD card and safety-related project manipulation

Note that after removing the SD card from the BPC 9102S, it is possible for the SD card and safety-related project to be manipulated without authorization.

- Take measures to protect the SD card and safety-related project against manipulation or ensure that the safety-related project is deleted completely.

10.5 Removing the BPC 9102S

Please note:

Before you can remove the BPC 9102S, you must:

– Disconnect the BPC 9102S from the power supply and remove the supply connector (see Section 10.2).

– Where necessary, remove any connectors from the BPC 9102S (see Section 10.3).

Follow the descriptions listed in this section.

1. Remove the BPC 9102S from the mounting surface.
2. To do so, unscrew the screws slightly.
3. Push the BPC 9102S upwards and remove the device from the mounting surface by lifting the large openings of the keyhole-shaped drill holes over the screw heads in the mounting surface.

10.6 Removing the BPC 9102 FAN KIT fan kit

If you have been operating the BPC 9102S with the BPC 9102 FAN KIT fan kit, remove the fan kit in accordance with the following steps.

NOTE: Potential malfunction of the BPC 9102S

The fan kit may not be removed while the BPC 9102S is in operation.

- Switch off the BPC 9102S power supply before removing the fan kit.

Please note:

Use a Torx® TX 10 screwdriver (ordering data is available in Section 14.1.3, “Accessories”) to remove and tighten the screws in the following section.

1. Loosen the four M4 screws (pos. 3 in Figure 10-3) and remove them.
2. Pull the feed-in plug on the rear of the fan kit from the socket (pos. 2 in Figure 10-3) on the underside of the BPC 9102S while slightly pressing on the connector snap-in latch to release the connector.
3. Position the cover plate in the housing cutout over the socket for the feed-in plug (pos. 2 in Figure 10-3).
4. Affix the cover plate to the BPC 9102S housing using an M4 screw.

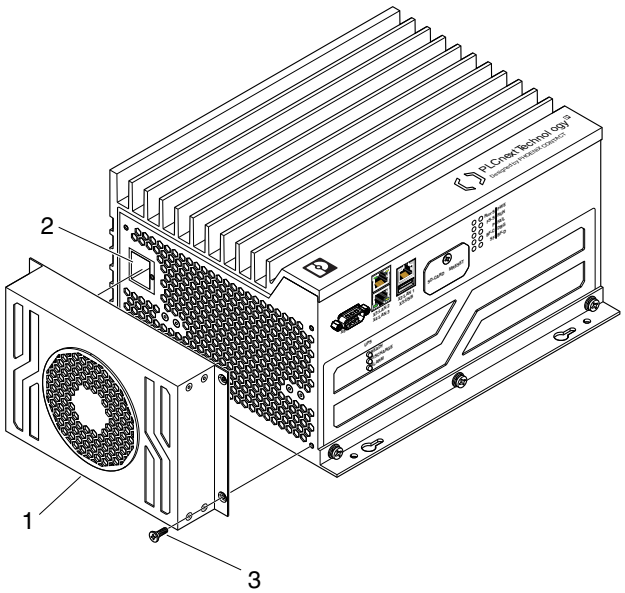


Figure 10-3 Removing the BPC 9102 FAN KIT fan kit

11 Device replacement, device defects, and repairs

11.1 Device replacement

The device can be replaced, if necessary.

Observe the device type and version

The replacement device must satisfy the following conditions (see pos.9 in Figure 3-9 on page 44):

- Same device type
- Same or later version

Procedure

If you want to replace the device, proceed in accordance with the following section:

- “Removing the hardware” on page 165
- “Mounting hardware” on page 57
- “Connecting and wiring the hardware” on page 67
- “Startup and validation” on page 71

WARNING: Unintentional machine startup

Do not replace the BPC 9102S 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.

1. Replace the BPC 9102S in your application with an identical device (same item number).

Please note:

If the firmware of the replacement device is of a later version than the firmware of the device to be replaced, you may have to recompile the project in the PLCnext Engineer software and/or in the integrated development environment. This procedure is only necessary for certain firmware versions. You will find information on this in the “Application notes for the BPC 9102S with an SPLC 3000 safety-related controller” application note.

The application note can be downloaded at phoenixcontact.net/product/1246285.

2. Once the controller is replaced, restore all the necessary connections.

WARNING: Do not connect the BPC 9102S 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 BPC 9102S.

3. When restarting the BPC 9102S 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 “Recommissioning after replacing the BPC 9102S” on page 74.

11.2 Device defects and repairs

Do not open the housing

Do not open the BPC 9102S housing. If the housing is opened, the function of the device can no longer be ensured.

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the BPC 9102S (see Section 3.5.1). These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the BPC 9102S can no longer be ensured.

Device defects/repairs

Please contact Phoenix Contact. Repairs may only be carried out by Phoenix Contact.

- Send defective devices back to Phoenix Contact for repair or to receive a replacement device.
- We strongly recommend using the original packaging to return the product.
- Include a note in the packaging indicating that the contents are returned goods.
- Where possible, provide a detailed description of the errors that have occurred.
- If the original packaging is no longer available, observe the following points:
  - Observe the humidity specifications and the temperature range specified for transport (see Section “Technical data” on page 187).
  - If necessary, use dehumidifying agents.
  - Use suitable ESD packaging to protect components that are sensitive to electrostatic discharge.
  - Secure any loose parts.
  - Make sure that the packaging you select is large enough and the material is sufficiently thick.
  - Only use plastic bubble wrap sheets as wadding.
  - Attach warnings to the transport packaging so that they are clearly visible.
  - Please be aware that the delivery note is to be placed inside the package if the package is sent within the same country. If the package is being sent abroad, the delivery note must be placed inside a delivery note pocket and attached to the outside so that it is clearly visible.

12 Maintenance, decommissioning, and disposal

12.1 Maintenance

The device is maintenance-free.

Repeat testing during the lifetime is not necessary.

12.2 Decommissioning and disposal

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 25).

The device is not used anymore:

The device contains valuable recyclable materials, which should be utilized. The electronic circuit board is fitted with a lithium battery.

Device disposal

- Do not dispose of the device with household waste; it should be disposed of in accordance with the currently applicable 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.

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 applicable national regulations.

13 Extended BPC 9102S settings and further useful information

13.1 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 175).

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.

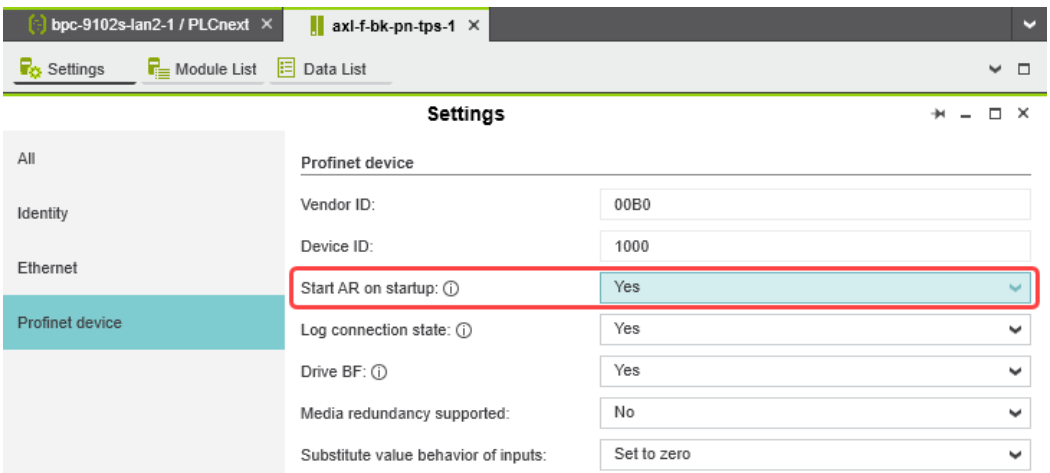


Figure 13-1 PROFINET device – “Start AR on startup”

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 your 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

Observe these notes to prevent unexpected machine startup after operator acceptance via the “Operator Acknowledgment” command.

13.2 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.

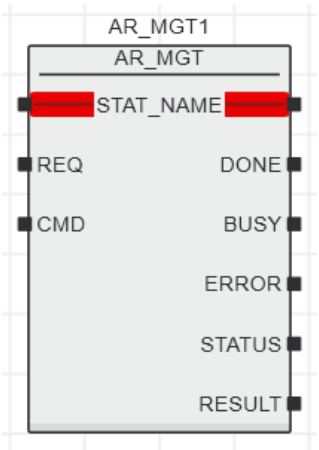


Figure 13-2 AR_MGT function block

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.

13.3 Substitute value behavior for PROFINET devices and PROFIsafe F-Devices

The substitute value behavior for the input data of the PROFINET controller must be specified in your PLCnext Engineer project. By default, the input data of the BPC 9102S 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 13-3).

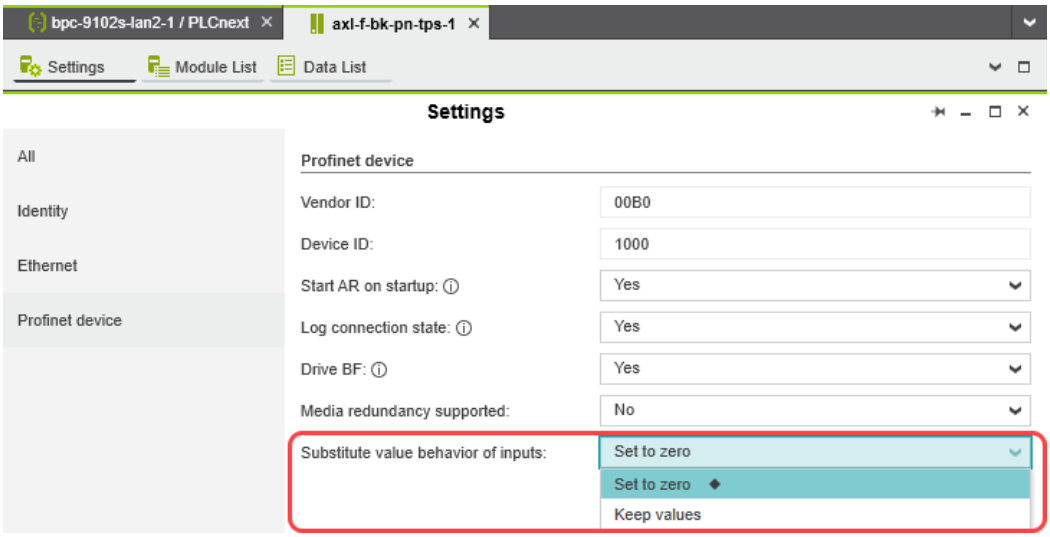


Figure 13-3 PROFINET device – “Substitute value behavior of inputs”

If the connection to a PROFINET device is interrupted, the “Set to zero” option means that the corresponding input data of the BPC 9102S 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 your 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.

13.4 Configuration memory: directory structure and access

The configuration memory is accessed via the SFTP protocol. An SFTP client software is required for this (e.g., WinSCP).

Read the information in Section “Using SFTP to access the file system” on page 55 before accessing the configuration memory via the SFTP client software.

- Start the SFTP client software (WinSCP in the following example).

Log into the BPC 9102S using the SFTP client software.

- Enter the IP address of the BPC 9102S on the input screen (in the example: 192.168.2.10).
- Enter the user name and the administrator password (in the example: user name: admin; administrator password: see printing on the BPC 9102S).
- Confirm your entries.

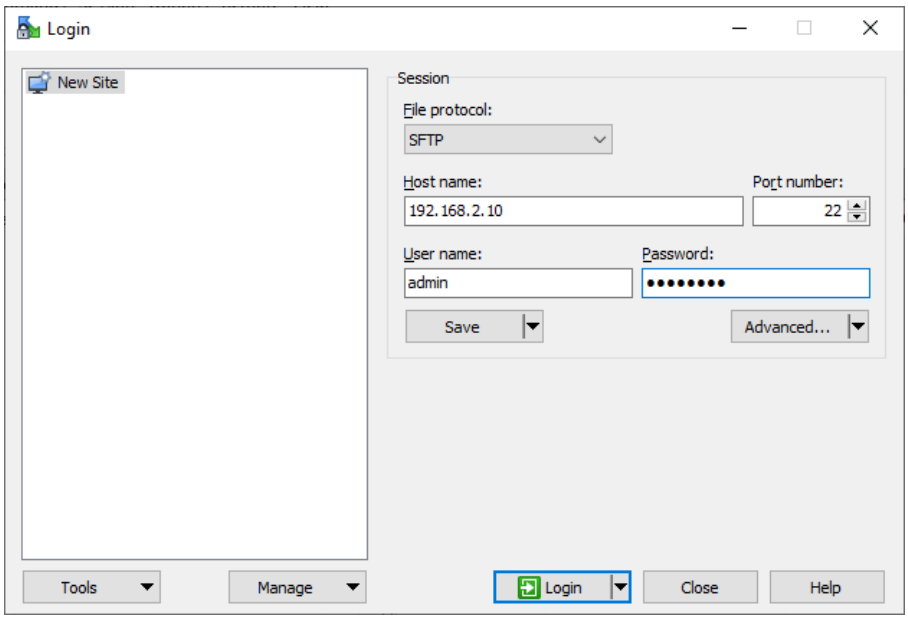


Figure 13-4 Logging into the BPC 9102S via WinSCP

After successful login, the following directory is displayed in the configuration memory:

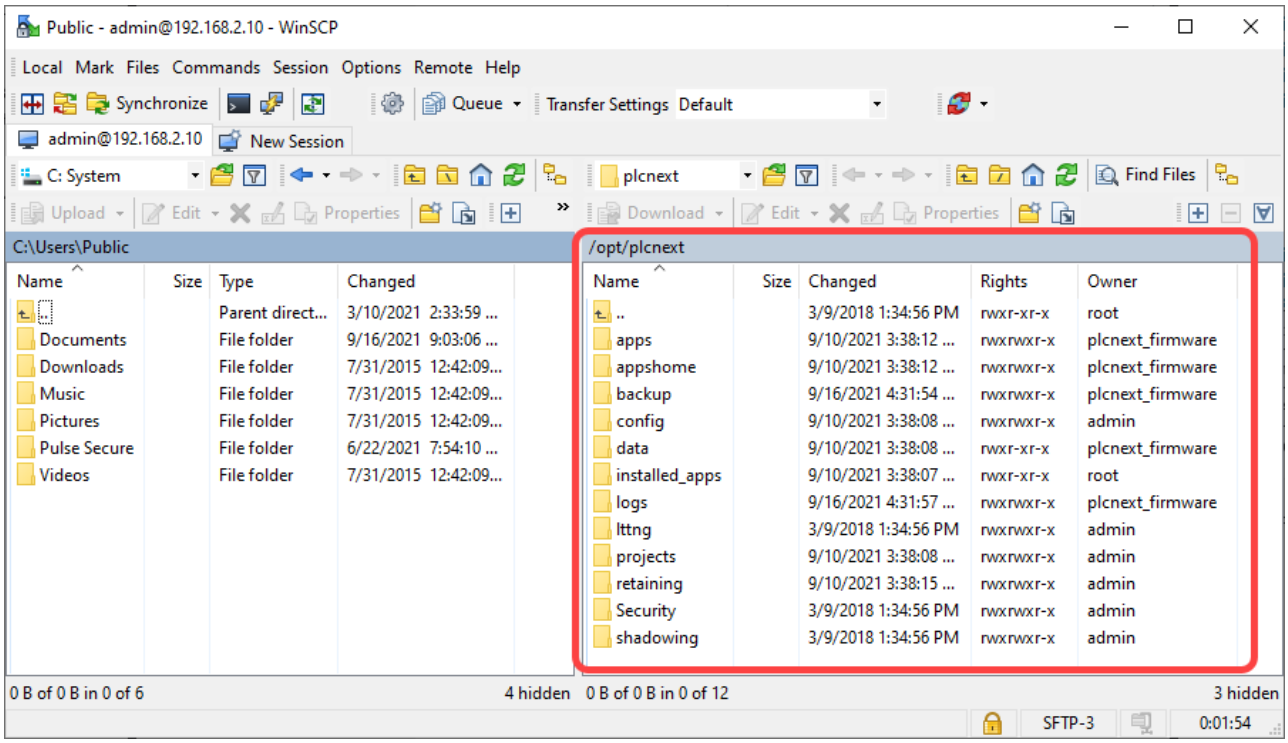


Figure 13-5 PLCnext directory “/opt/plcnext” in the configuration memory.

13.5 Setting the real-time clock via PLCnext Engineer

You can set the real-time 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.

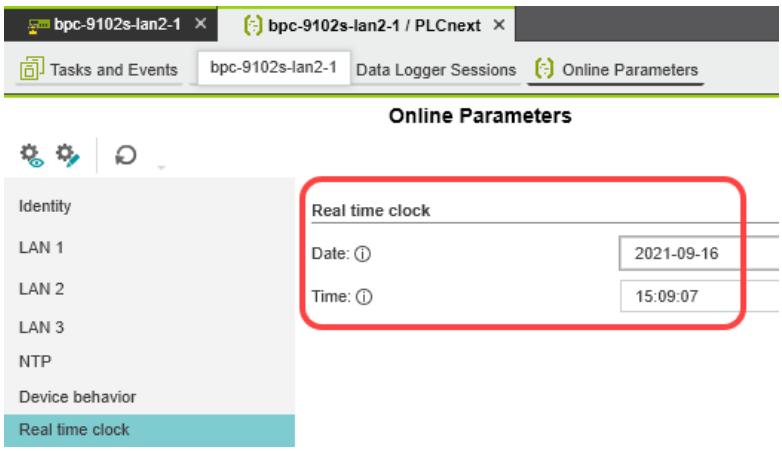


Figure 13-6 Real-time clock settings for the BPC 9102S

- 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.

13.6 Function blocks for handling files on the configuration 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 configuration memory.

Table 13-1 Overview of the function blocks

Function block	Brief 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 configuration memory are described in the PLCnext Engineer online help function.

13.7 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 BPC 9102S supports a maximum of 32 Ethernet connections to other communication partners.

Table 13-2 Overview of the function blocks

Function block	Brief 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 function.

13.8 Web server

The BPC 9102S 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 BPC 9102S is also available via the web server (see Section “Web-based management WBM system” on page 163).

The Hypertext Transfer Protocol (HTTP) is set on the controller by default.

13.9 OPC UA

The BPC 9102S has an integrated OPC UA server.

Further information on OPC UA and PLCnext Technology is available in the PLCnext Community at plcnext-community.net.

14 Technical data and ordering data

14.1 Ordering data

14.1.1 Industrial box PC

Description	Type	Item No.	Pcs./Pkt.
Industrial box PC with integrated SPLC 3000 safety-related controller, Intel® Core™ i7 10700TE processor, 2.00 GHz, IP20, 10 GB SSD, M.2, SATA	BPC 9102S	1246285	1

14.1.2 Modules

Description	Type	Item No.	Pcs./Pkt.
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, single-conductor connection technology	AXL F DI16/1 HS 1H	2701722	1
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

14.1.3 Accessories

Description	Type	Item No.	Pcs./Pkt.
Fan kit, optional	BPC 9102 FAN KIT	1290834	1
Service socket with USB A 3.0 (female/female), with protective cover	SI-RND-U1A	1425185	1
For further available accessories, see phoenixcontact.net/product/1246285			
Replacement part PCB connector	MSTB 2,5/ 3-STF-5,08	1777992	1
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

Description	Type	Item No.	Pcs./Pkt.
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 the 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 GB	SD FLASH 2GB 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 GB	SD FLASH 8GB PLCNEXT MEMORY	1061701	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
Assembly tool for RJ45 connector	FL CRIMPTOOL	2744869	1
Patch cable, CAT 5, 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, CAT 5, 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
Screwdriver, Torx®, VDE-insulated, TX 10 x 80, two-component handle	SF-TX 10X80 VDE	1200156	1

14.1.4 Software

Description	Type	Item No.	
PLCnext Engineer	See latest Phoenix Contact catalog		

14.1.5 Documentation

Make sure you always use the latest documentation.
It is available for download at phoenixcontact.net/products.

Description	Type	Item 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, Item No.: 8.072 “PROFINET_Assembling_8072_V28_Sep19.pdf”	For the latest versions of the documents visit www.profinet.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 2.4, October 2020, Item No.: 8.102 “Earthing-Shielding_8102_V24_Oct20.pdf”			
PROFIsafe			
PROFIsafe System Description, Technology and Application, Version April 2016, Item No.: 4.342 “PROFIsafe_SystemDescription_ENG__2016_web.pdf”	For the latest versions of the documents visit www.profisafe.net or contact your nearest Phoenix Contact representative regarding the documents.		
PROFIsafe Policy, Guideline for PROFIBUS and PROFINET, Version 1.5, July 2011, Item 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, Item No. 2.232 “PROFIsafe-Environment_2232_V26_Dec15.pdf”			
PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET, Item 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, Item No.: 2.242 “Psafe-Testspec_2242_V23_Mar18.pdf”			
PLCnext Technology			

Information on troubleshooting and answers to frequently asked questions (FAQs) can be found in the PLCnext Technology at plcnext-community.net.

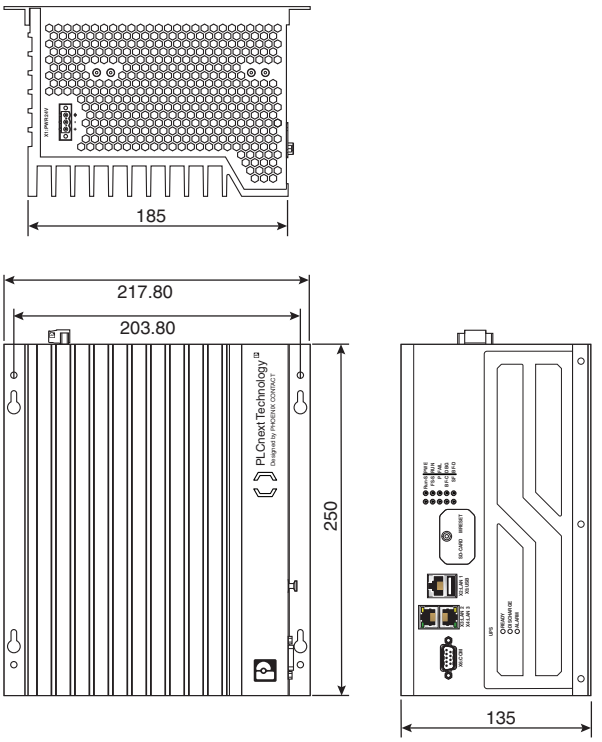
Comprehensive documentation on PLCnext Technology is available in the PLCnext Info Center.

Description	Type	Item No.	Pcs./Pkt.
Documentation for software			
Online help PLCnext Engineer			
Security			
Application note, English Measures to protect network-capable devices with communication interfaces, solutions, and PC-based software against unauthorized access	AH EN INDUSTRIAL SECURITY	–	1

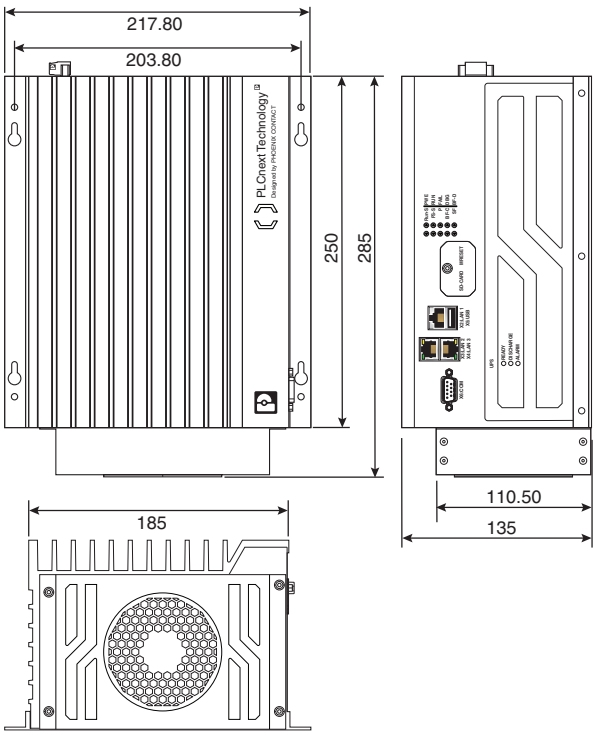
14.2 Technical data

Dimensions (nominal sizes in mm)

Without fan:



With fan:



General data	
Dimensions without fan (width x height x depth)	218 mm x 250 mm x 135 mm
Dimensions with fan (width x height x depth)	218 mm x 285 mm x 135 mm
BPC 9102 FAN KIT fan dimensions (width x height x depth)	175 mm x 35 mm x 110 mm
Weight without fan	Approx. 4772 g
Weight with fan	Approx. 5160 g
Mounting type	Wall mounting

Power supply

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

The BPC 9102S 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 satisfy the requirements of EN 61204-1 and feature safe isolation with PELV in accordance with IEC 61010-2-201 (PELV). They prevent short circuits between the primary and secondary side.

Please also observe the information in Section “Electrical safety” on page 18.

Select power supplies correctly!

Refer to the information on selecting the power supply in Section “Electrical safety” on page 18.

Use only power supplies with safe isolation with 24 V DC.

Use a **power supply without fall-back characteristic curve** (see Section “Sizing of the power supply” on page 67).

Connection type	COMBICON connector, removeable
Power supply	24 V DC
Permissible range	19.2 V DC to 30.0 V DC
Ripple	3.6 V_{PP}
Current consumption	
Typical	2.1 A
Maximum	2.3 A
Power consumption	
Typical	50 W
Maximum	55 W
Fuse protection	5 A, slow-blow, required externally
Connection data for COMBICON connectors	
Conductor cross-section (rigid/flexible)	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
UPS	Capacitor, minimum 10 s at max current consumption
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	$0175_{hex}/373_{dec}$

Interfaces	
USB	Service interface, reserved internally USB 2.0 type A
Serial connection	Service interface, reserved internally D-SUB 9 pin strip, RS-232
Removable media	SD
Ethernet connection	
Quantity	3 (LAN1/LAN2/LAN3)
Function	
– LAN1	Ethernet
– LAN2	PROFINET controller
– LAN3	PROFINET device
Transmission speed	
– LAN1	1 Gbps or 2.5 Gbps
– LAN2/LAN3	Max. 1 Gbps
LAN chipset	3x Intel Ethernet controller i225

IEC 61131 runtime system	
Programming system	PLCnext Engineer
Operating system	Linux developed by Yocto® Project; PLCnext
Processor data	
CPU (Central Processing Unit)	Intel® Core™ i7-10700TE
Clock rate	2.00 GHz
Cache	16 MB
Number of cores	8
Number of threads	16
Number of memory channels	1
Application interface	OPC UA
Shortest cycle time (t_{min})	500 µs (for cyclic task)
Main memory (RAM)	16 Gbps, DDR4-2400
User memory, internal	
Type	10 GB SSD, M.2, SATA

IEC 61131 runtime system	
Number of bays	1
Program memory	32 MB
Data storage	64 MB
Memory for retain data	4 MB
Number of control tasks	128
Configuration memory	SD card (plug-in) Size depending on the SD card used (see “Program and configuration memory” in Section “Accessories” on page 183)

Please note that the number of write access operations to the configuration memory is limited.

BPC 9102 FAN KIT fan module (optional accessory, not included in the scope of delivery of the RFC)	
Number of fans	1
Storage	Ball bearings
Speed monitoring	Yes, through the BPC 9102S
Mounting	4x M4 screws: Recommended tightening torque: 5.0 Nm
Service life	70,000 h at 40°C ambient temperature with 15% ... 65% rel. humidity

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 housing or a control cabinet with a minimum of IP54 degree of protection.

Pollution degree	2, when installed in a housing or control cabinet with IP54 degree of protection or higher
Air clearances and creepage distances	In accordance with IEC 60439-1
Protection class	III, IEC 61140, EN 61140, VDE 0140-1
Ambient temperature (operation)	-20°C to +60°C (up to 2,000 m above mean sea level) -20°C to +55°C (2,000 m to 3,000 m above mean sea level) -20°C to +50°C (3000 m to 4000 m above mean sea level)
Ambient temperature (storage/transport)	-40°C ... +85°C
Permissible humidity (operation)	10% ... 93% (non-condensing)
Permissible humidity (storage/transport)	5% ... 95% (non-condensing)

Ambient conditions	
Air pressure (operation)	60 kPa ... 108 kPa (up to 4000 m above mean sea level)
Air pressure (storage/transport)	58 kPa ... 108 kPa (up to 4,500 m above mean sea level)
Resistance to gases that may endanger functions in accordance with 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	3g
Shock in accordance with EN 60068-2-27/IEC 60068-2-27	15g
Continuous shock in accordance with EN 60068-2-27/IEC 60068-2-27	10g

Safety characteristic data in accordance with EN ISO 13849	
Performance level (PL)	Max. e
Category	Max. 4
Probability of a dangerous failure per hour (PFH_D)	$1 * 10^{-9}$
Diagnostic coverage (DC_{avg})	99%
Mean time to dangerous failure ($MTTF_D$)	>100 years

Safety characteristic data in accordance with EN 62061	
Safety integrity level claim limit (SIL CL)	Max. 3
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) as per DIN EN 62061	99%

Safety characteristic data in accordance with IEC 61508 – high demand	
Safety Integrity Level (SIL)	Max. 3
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 SPLC 3000 safety-related controller	
Programming system	PLCnext Engineer, IEC 61131
CPU1 (Central Processing Unit 1) CPU2 (Central Processing Unit 2)	ARM® Cortex®-A9, 800 MHz ARM® Cortex™-A8, 600 MHz
Shortest cycle time $T_{ZSPLCmin}$	5 ms
Program memory (safety program)	2 MB
Data storage (addressable area)	1 MB
PROFIsafe profile	V2.6MU1 (also includes support for V2.4)
Number of PROFIsafe F-Devices	300
Sum of the safe input data (SI)	24 kB
Sum of the safe output data (SQ)	24 kB
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)	6 kB
Device diagnostics output data (DQ)	6 kB
Function block diagnostics output data (FBQ)	8 kB
Number functions block instances	8192

Real-time clock RTC	
Typical buffer time	9 days
Power reserve	240 h
Real-time clock accuracy	1.73 s/day = 20 ppm at 25°C
RTC battery, typical service life	5 years

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 A 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 A Supply lines: 2 kV Signal/data lines: 2 kV
Transient overvoltages (surge)	EN 61000-4-5 IEC 61000-4-5	Criterion A Signal/data lines: 1 kV Supply lines: 1 kV
Conducted disturbance variables	EN 61000-4-6 IEC 61000-4-6	Criterion A Test voltage 10 V
Noise emission test in accordance with EN 61000-6-4		

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/1246285.

A 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:

F_Source_Address / F_Destination_Address / F_Source_Add / F_Dest_Add (F-address for short)	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. 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: Address type 1: The F-Device only checks the F_Destination_Address. Address type 2: The F-Device checks the F_Destination_Address and the F_Source_Address.
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 (in short: F_Source_Add);
PROFIsafe source address; address of the safety-related SPLC 3000 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	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 error is reported to the safety-related controller. 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. 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.
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	Monitoring time for safety-related communication between the SPLC 3000 and the safe I/O devices. This time is parameterized in the F_WD_Time F-Parameter.

B Appendix: Checklists

NOTE: Observe supporting checklists

The checklists listed in this section provide support during planning, assembly, and electrical installation, commissioning, parameterization, and validation of the BPC 9102S 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 commissioning, or regular testing performed by qualified personnel.

The following section of a checklist shows an example of a completed checklist.

Checklist …			
Device type/equipment identification		BPC 9102S/BK15NA11	
Version: **HW/FW** **HW/FW (SPLC 3000)**	 ≥ 02/2021.6 ≥ 03/02.00.0000	**Date**	2021-02-18
Editor	John Smith	**Test engineer**	Jane Brown
Comment	System XXX has been checked for engine hood production		

No.	**Requirement**	**Yes**	**Comment**
X	. . .	☐	

Key:

Device type/equipment identification	Enter the device type and/or the equipment identification for the relevant device.
Version: HW/FW	Enter the hardware and firmware version as well as the SPLC 3000 hardware and firmware version of the device (see revision specification on the label, item 9 in Figure 3-9 on page 44).
Date	Enter the date on which you began to fill out 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.

B 1 System-specific checklists

This section contains checklists that relate to the phases of life of the PROFIsafe system.

B 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?	☐	
2	Has risk assessment for the system/machine been carried out?	☐	
3	Has the corresponding safety category/safety integrity level been derived from risk assessment?	☐	
4	Have the individual safety functions been fully defined/specified?	☐	
5	Does the planned PROFIsafe system meet the required safety integrity for all defined safety functions?	☐	
6	Has the power supply been planned in accordance with the specifications on protective extra-low voltage (PELV) in accordance with EN 60204-1 (including safe isolation with PELV in accordance with IEC 61010-2-201)?	☐	
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?	☐	
8	Can the planned system/machine be implemented when the determined SFRT is observed with the specified PROFINET infrastructure?	☐	
9	Can the planned application be realized with the programming capacities (for example by using function blocks) and has a specification of the safety-related application program been created?	☐	
10	Have the user rights for the safety-related application program been specified in the PLCnext Engineer software?	☐	
11	Has a project password been provided?	☐	
12	Who is authorized to “develop” the safety-related application program?	☐	Names:
13	Has a controller password been provided?	☐	
14	Were the settings for user authentication defined in the BPC 9102S web-based management?	☐	Names:
15	Has the location where the software is to be installed (e.g., on the system PC) been specified?	☐	

No.	Requirement	Yes	Comment
16	Are measures planned which prevent unintentional, automatic restart with hazardous states?	☐	
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 SPLC 3000 controllers)?	☐	
18	Does the planned use correspond to the intended use of the system?	☐	
19	Has the technical data of the PROFIsafe system been observed?	☐	
20	Have the requirements of the PROFINET Assembling Guideline been observed and met during planning?	☐	
21	Have the accessories to be used been planned (e.g., cables, male connectors)?	☐	
22	Are the period of use / proof test intervals and maintenance intervals of the PROFIsafe devices used known and documented?	☐	
23	Is the assignment of responsibility for subsequent phases of life specified (e.g., for assembly/installation/programming/startup/validation, etc.)?	☐	Name/company:
24	Are measures planned against unauthorized network access?	☐	
		Date	Signature (editor)
		Date	Signature (test engineer)

B 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?	☐	
2	Have the user rights for the safety-related application program been created in the PLCnext Engineer software?	☐	
3	Has the safety-related application program been created entirely in PLCnext Engineer?	☐	
4	Have additional application-specific programming guidelines been created and observed within the program specification for the planning phase?	☐	
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)?	☐	
6	Are the parameterized F-Addresses (F-Source Addresses of the F-Host and F-Destination Addresses of the F-Devices) unique throughout the network?	☐	
7	Is the F_WD_Time calculated for each F-Device parameterized in the “Safety Parameters” editor in PLCnext Engineer?	☐	
8	Has a project password been defined?	☐	
9	Who is authorized to “develop” the safety-related application program?	☐	Names:
10	Has a controller password been defined?	☐	
11	Has project information been entered in the “Description” field in the “Properties” editor in the “Project” editor group?	☐	Type: Location:
12	Are possible reciprocal effects due to exchange variables between the programming of the standard controller and the SPLC 3000 in the BPC 9102S taken into consideration and clear?	☐	
13	Has the following been observed when programming/configuring your 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.	☐ ☐	
		Date	Signature (editor)
		Date	Signature (test engineer)

B 1.3 Commissioning

Checklist for commissioning 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 commissioning phase?	☐	
2	Is safety ensured during the commissioning phase by means of additional measures, and if so, what are these measures (see also No. 1)?		
	1 _____	☐	
	2 _____	☐	
	3 _____	☐	
	4 _____	☐	
	5 _____	☐	
	6 _____	☐	
	7 _____	☐	
	8 _____	☐	
	9 _____	☐	
	10 _____	☐	
	Additional requirements in: _____	☐	
3	Are adjustments to the F_WD_Time $_{min}$ required in order to ensure ruggedness of the system and system availability, since the actual SPLC 3000 cycle time may deviate from the SPLC 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)	☐	
4	Are measures implemented against unauthorized network access?	☐	
5	Are specifications for the startup phase applicable and have they been met?	☐	
		Date	Signature (editor)
		Date	Signature (test engineer)

B 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?	❒	
2	Have the requirements from the previous planning, programming, and startup phases been met?	❒	
3	Has validation of the F-Devices used been carried out and are the results available?	❒	
4	Have safety distances that must be observed been calculated and checked in accordance with the response and delay times (response times, SFRT, F_WD_Time $_{max}$) been implemented?	❒	
5	Have all the safety functions been checked successfully?	❒	
6	Do the two CRC checksums displayed in the "/ Safety PLC" editor group in the "Safety Cockpit" editor in the "Overview" view ("Safety PLC project information" and "Engineering project information") match? If you are connected online to the safety-related controller, the checksums are displayed in PLCnext Engineer.	❒	
7	Have measures against unauthorized network access been implemented and checked?	❒	
8	Are the directives and standards used listed in the declaration of conformity?	❒	
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.	❒	
10	Has a complete printout of the safety-related application program programmed in PLCnext Engineer been stored in the system?	❒	
11	Have all fully completed checklists been stored in the system?	❒	
12	**Completion of validation** Has the latest program version (including the "Project information") been downloaded to the safety-related SPLC 3000 controller on automatic startup?	❒	
		Date	Signature (editor)
		Date	Signature (test engineer)

B 2 Device-specific checklists

This section contains checklists that relate to the phases of life of the BPC 9102S.

B 2.1 Planning

Checklist for planning the use of the BPC 9102S			
Device type/equipment identification			
Version: **HW/FW** **HW/FW (SPLC 3000)**		**Date**	
Editor		**Test engineer**	
Comment			

No.	Requirement	Yes	Comment
1	Has the systematic “Planning” checklist been observed?	☐	
2	Are all measures that are based on applicable standards and the PROFINET Assembling Guideline planned?	☐	
3	Has the current BPC 9102S user manual been used as the basis for planning?	☐	
4	Have the power supply for the device and direct I/Os been planned as per the specifications for protective extra-low voltage (PELV) in accordance with EN 60204-1 (including safe isolation with PELV in accordance with IEC 61010-2-201)?	☐	
5	Are measures planned to prevent simple tampering? If so, what are they? 1 _____ 2 _____ 3 _____ 4 _____ 5 _____	 ☐ ☐ ☐ ☐ ☐	
6	Does the planned use correspond to the intended use?	☐	
7	Have the ambient conditions according to the technical data been observed?	☐	
8	Has the degree of protection been observed?	☐	
9	Have the accessories to be used been planned in accordance with the ordering data in this user manual (cables, plugs)?	☐	
10	Have specifications for assembly and electrical installation been defined (e.g., EPLAN) and communicated to the relevant personnel?	☐	
11	Have specifications for parameterization been defined and communicated to the relevant personnel?	☐	
12	Have specifications for startup been defined and communicated to the relevant personnel?	☐	
13	Has the technical data of the interfaces been observed?	☐	
		Date	Signature (editor)
		Date	Signature (test engineer)

B 2.2 Assembly and electrical installation

Checklist for assembly and electrical installation of the BPC 9102S			
Device type/equipment identification			
Version: **HW/FW** **HW/FW (SPLC 3000)**		**Date**	
Editor		**Test engineer**	
Comment			

No.	Requirement	Yes	Comment
1	Has assembly and electrical installation been carried out in accordance with the specifications of the planning phase?	☐	
2	Has assembly and electrical installation been carried out in accordance with the specifications in the user manual for the BPC 9102S?	☐	
3	Has assembly and electrical installation been carried out in accordance with the specifications of the applicable standards and the PROFINET Assembling Guideline?	☐	
4	Have the power supply for the device and direct I/Os been installed as per the specifications for protective extra-low voltage (PELV) in accordance with EN 60204-1 (including safe isolation with PELV in accordance with IEC 61010-2-201)?	☐	
5	Have measures been taken to prevent simple tampering (e.g., control cabinet can be locked, PLCnext Engineer access rights (user authorization), etc.)? If so, what are they?		
	1 _____	☐	
	2 _____	☐	
	3 _____	☐	
	4 _____	☐	
	5 _____	☐	
	6 _____	☐	
	7 _____	☐	
	8 _____	☐	
	9 _____	☐	
	10 _____	☐	

Date	Signature (editor)
Date	Signature (test engineer)

B 2.3 Commissioning and parameterization

Refer to the online help for the PLCnext Engineer software.

Checklist for commissioning and parameterization of the BPC 9102S			
Device type/equipment identification			
Version: **HW/FW** **HW/FW (SPLC 3000)**		**Date**	
Editor		**Test engineer**	
Comment			

No.	Requirement	Yes	Comment
1	Have the systematic “Programming” and “Commissioning” checklists been observed?	☐	
2	Was commissioning completed in accordance with the specifications (specifications from the planning phase and/or in accordance with the BPC 9102S user manual, see Table 6-1 “Steps for initial startup of the BPC 9102S”)?	☐	
3	Is it ensured that when the supply voltage of the BPC 9102S is switched on, automatic startup does not cause a hazardous movement on the machine/system?  **WARNING: Preventing automatic startup** Take appropriate measures to ensure that automatic startup of your system/machine is prevented.	☐	

Date	Signature (editor)
Date	Signature (test engineer)

B 2.4 “Initial commissioning” 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 commissioning or recommissioning/device replacement of the BPC 9102S			
Device type/equipment identification			
Version: **HW/FW** **HW/FW (SPLC 3000)**		**Date**	
Editor		**Test engineer**	
Comment			

No.	**Requirement**	**Yes**	**Comment**
1	Has the systematic “Validation” checklist been observed?	☐	
2	Have all the requirements of the “Planning” checklist been met?	☐	
3	Have all the requirements of the “Assembly and electrical installation” checklist been met?	☐	
4	Have all the requirements of the “Commissioning and parameterization” checklist been met?	☐	
5			
5a	Initial commissioning: Has a function test been performed to check all the safety functions in which the BPC 9102S is involved?	☐	
5b	Recommissioning after replacing the BPC 9102S: The CRC checksum of the PLCnext Engineer project corresponds to the version validated and documented for the machine/system under 5a.	☐	
6	Does the power supply for the device and direct I/Os comply with the specifications on protective extra-low voltage (PELV) in accordance with EN 60204-1 (including safe isolation with PELV in accordance with IEC 61010-2-201)?	☐	
7	Do all cables correspond to the specifications?	☐	
8	Wiring check: Have all the inputs and outputs of all F-Devices physically present in the network and configured in PLCnext Engineer been properly wired?	☐	
9	Have measures been taken to prevent simple tampering?	☐	
		Date	Signature (editor)
		Date	Signature (test engineer)

C Appendix for document lists

C 1 List of figures

C 2 List of tables

C 3 Index

R

S

T

U

W

D Appendix: Revision history

Revision	Date	Content
01	2021-11-02	First publication of the user manual for the BPC 9102S.

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 general Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

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
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

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
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

110088_en_01
Item No. —

INSPIRING INNOVATIONS