Installing and operating the AXC F 1252 controller

User manual

User manual

Installing and operating the AXC F 1252 controller

UM EN AXC F 1252, Revision 00 2025-12-15

This manual is valid for:

Designation	As of hardware version	As of firmware version	Item No.
AXC F 1252	01	2025.6.1	1646469

Phoenix Contact GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this 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.

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

🛡 This symbol indicates potential security risks in devices, solutions, or services from Phoenix Contact. These may be IT and security risks in industry automation, for example.

1.2 Qualification of users

The use of products described in this 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.

1.3 Field of application of the product

1.3.1 Intended use

The AXC F 1252 controller is a modular small-scale controller for use in industrial automation and control systems (IACS) in which industrial cybersecurity is of great importance. It is intended for use in a closed control cabinet with at least IP54 degree of protection.

1.3.2 Product changes

Modifications to the device hardware 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.

1.4 Trademarks

- Linux® is a registered trademark of Linus Torvalds in the USA and other countries.
- Visual Studio® and Windows® are registered trademarks of Microsoft Corporation.
- MATLAB® and Simulink® are registered trademarks of The MathWorks, Inc.
- OPC UA® is a registered trademark of the OPC Foundation.
- EtherNet/IP™ is a trademark of ODVA, Inc.
- Python® is a registered trademark of the Python Software Foundation.
- Eclipse® is a registered trademark of the Eclipse Foundation.
- IO-Link® is a registered trademark of the PROFIBUS Nutzerorganisation e.V., Germany.
- Arm® and Cortex® are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the USA and other countries.

1.5 Additional information

Observe the additional information provided about the device:

- PLCnext Technology - Info Center
  Information on the firmware of devices with PLCnext Technology
- PLCnext Technology - Security Info Center
  Information on industrial cybersecurity in the context of PLCnext Technology
- Product Security Incident Response Team
  Safety notes and information on current security vulnerabilities
- PLCnext Store - Info Center
  Information on PLCnext Store
- PLCnext Community
  Information on troubleshooting and answers to frequently asked questions

1.6 General safety notes

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

NOTE: Property damage due to impermissible stress
The IP20 degree of protection (IEC 60529/EN 60529) requires that the device is used in a clean and dry environment. Using the device in an environment that is outside of the specified limits may cause damage to the device.

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

NOTE: Device failure due to foreign objects in the 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 failures.

- Ensure that the device is operated within the permitted ambient temperature range.
  See Section 12.2, “Technical data”.

NOTE: Device failure due to vibration and shock 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 failures.

- Ensure that the permitted specifications for vibration and shock are adhered to when operating the device.
  See Section 12.2, “Technical data”.

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components.

- 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.

1.7 Security in the network

NOTE: Network security jeopardized by unauthorized access
Connecting devices to a network entails the danger of unauthorized access to the network.

Observe the following safety notes:

- If possible, deactivate unused communication channels.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- To ensure IT and OT security, operate the device only in areas that are exclusively accessible to authorized persons.
- Only allow authorized persons to access the device. Limit the number of authorized persons to the necessary minimum.
- If you want to operate the controller as a certified device in accordance with IEC 62443-4-2:
  Always install the latest LTS version of the firmware (see Section "Certification" on page 12).

  The firmware can be downloaded via the item (phoenixcontact.com/products).
- Observe the IT and OT security requirements and the standards applicable to your application. Take the necessary protective measures. These may include, for example, virtual networks for remote maintenance access or a firewall.
- In security-critical applications, always use the device with an additional security appliance.

  Phoenix Contact offers security appliances in the mGuard product range. The mGuard routers connect various networks for the remote maintenance and protection of the local network and protect these networks against cyberattacks.
- You must take defense-in-depth strategies into consideration when planning networks.

Additional measures for protection against unauthorized network access can be found in the "INDUSTRIAL SECURITY" application note. The application note can be downloaded via the item (phoenixcontact.com/products).
German: AH DE INDUSTRIAL SECURITY, 107913
English: AH EN INDUSTRIAL SECURITY, 107913

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

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 packaging, as well as the moisture, shock, tilt, and temperature indicators on the packaging.
- During transport, observe the specifications regarding humidity and temperature range.
  See Section 12.2, “Technical data”
- Protect the surfaces as necessary to prevent damage.
- When transporting the equipment or storing it temporarily, ensure 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 ... 106 kPa (up to 4500 m above sea level)
- Permissible humidity: 5% ... 95% (in accordance with DIN EN 61131-2)

2.3 Unpacking

NOTE: Electrostatic discharge

Electrostatic discharge can damage or destroy components.

- 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 packing, the device may become damaged.

- Observe the ESD notes during unpacking and packing.

Scope of supply

AXC F 1252 controller

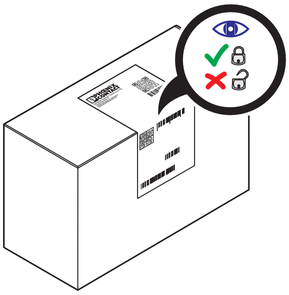
Checking the delivery

1. Check whether the packaging seal is intact (Figure 2-1).

   A damaged seal is an indicator that the packaging has been opened without authorization during transport. There is a possibility that the device has been tampered with. If the packaging seal is damaged, you must not use the device.

   - Submit claims for any damaged packaging seal to your supplier immediately.

Figure 2-1 Checking the packaging seal



2. 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.

   - Submit claims for any transport damage to your supplier immediately.

3. Immediately upon delivery, refer to the delivery note to ensure that the delivery is complete.

   - Submit claims for any incomplete packaging contents to your supplier immediately.

4. Check whether the security seal is attached to the device in the intended place and is intact.

   See Section 3.2, “Industrial cybersecurity”

   A damaged security seal or remnants of a security seal on the housing is an indicator that the housing of the device has been opened without authorization. There is a possibility that the device has been tampered with. The correct operation of the device is no longer guaranteed.

   You must not use the device!

   - Submit claims for a damaged security seal to your supplier immediately.

5. Check whether the housing latches are intact.

   See Section 3.2, “Industrial cybersecurity”

   Damage to the latches between the upper housing part and lower housing part indicates that the housing of the device has been opened without authorization. In this case, correct operation of the device is no longer guaranteed.

   - Submit claims for any devices with damaged housing latches to your supplier immediately.

General information about complaints

- Enclose photos that clearly document the damage to the packaging and/or delivery together with your claim.

3 Description of the controller

3.1 General

The AXC F 1252 controller forms the head of an Axioline F station. Axioline F modules and/or Axioline F backplanes with plugged-in Axioline Smart Elements are aligned with it (on the right). The Axioline F local bus is created automatically when the integrated bus base of the controller and the bus base modules of the Axioline F modules and/or Axioline F backplanes are aligned next to one another.

The controller is intended for use in industrial automation and control systems (IACS) in which industrial cybersecurity is of great importance.

The main area of application of the controller is industrial automation. Due to its open system architecture, it can also be used as an IoT device or remote terminal unit (RTU).

Restrictions

– The controller has an Ethernet interface.
– The controller **does not support left alignment** of Axioline F modules. Therefore, network segmentation is not possible.
– The controller **does not have a battery-buffered realtime clock** (RTC). After the supply voltage is interrupted, the system time must be reset (see Section 6.5, “Ensuring realtime clock synchronization”).

3.2 Industrial cybersecurity

Certification

The controller is developed in accordance with IEC 62443-4-1 (Maturity Level 3) (Secure Development Lifecycle [SDL]).

In preparation:
The device is certified in accordance with IEC 62443-4-2 SL-C2.
If you want to operate the controller as a certified device in accordance with IEC 62443-4-2, the following conditions must be met:

1. The latest **LTS** version of the firmware (≥ 2026.0.x LTS) must be installed on the controller.
2. The use of the controller must correspond to the defined security context.
   Information on this can be found in the PLCnext Technology - Security Info Center.

Secure by default

In the delivery state, various security functions are preset on the controller:

– The firewall is enabled.
– Only mandatory functions and ports are enabled.
  Information on system services and ports that are enabled in the delivery state can be found in Section 3.17, “Firewall” and Section 3.18, “System services”.
– Strong authentication: Secure password policies
– No unnecessary permissions: Applications and services are executed with the least possible rights.

Secure Boot

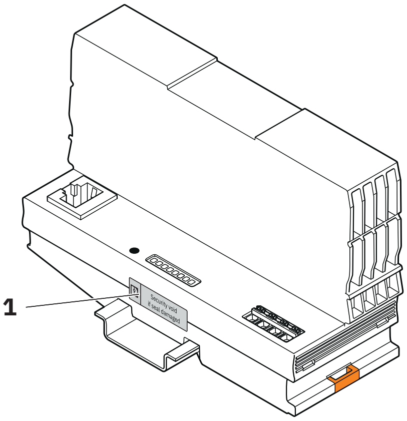
The controller supports the Secure Boot function. During the boot process, digital signatures are used to check whether the firmware has been compromised. Firmware that is detected as compromised is not loaded. In this case, the CSEC LED starts to light up **permanently** in blue or flash.
ℹ At the start of the boot process, the LED lights up briefly. This has no security-related meaning.

If the firmware has been compromised:

- Reset the controller with reset type 2 and install the latest firmware (see Section 3.8.1.2, “Resetting with reset type 2”).

Security seal

Figure 3-1 Security seal (1)



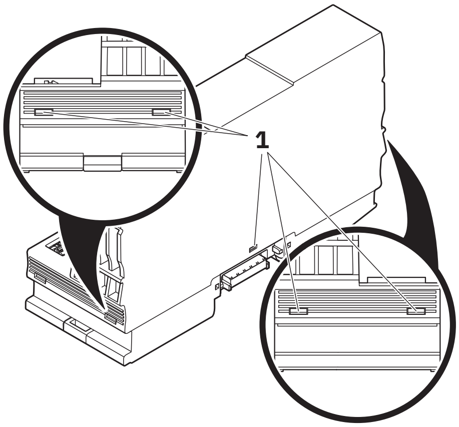
To detect unauthorized opening of the housing and to prevent tampering with the device, a security seal is attached to the housing of the device.

A damaged security seal or remnants of a security seal on the housing is an indicator that the housing of the device has been opened without authorization. In this case, correct operation of the device is no longer guaranteed.

- Check whether the security seal is attached in the intended place and is intact.
- Do not continue to use devices with damaged security seals.

Housing latches

Figure 3-2 Housing latches (1)



Damage to the latches between the upper housing part and lower housing part indicates that the housing of the device has been opened without authorization. In this case, correct operation of the device is no longer guaranteed.

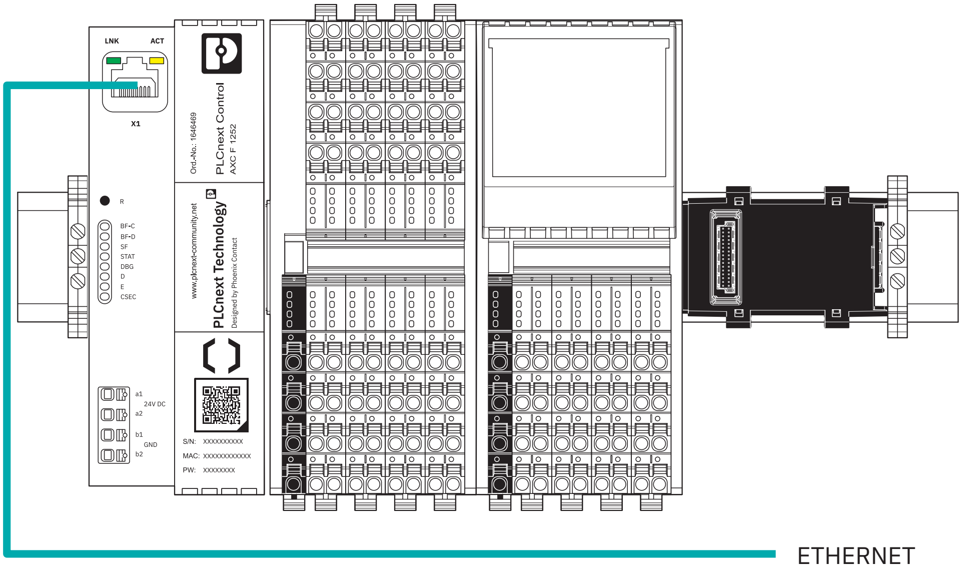
- Check whether the housing latches are intact.
- Do not use devices with damaged housing latches.

3.3 Possible fields of application of the controller

3.3.1 Operation as a distributed controller of an Axioline F station

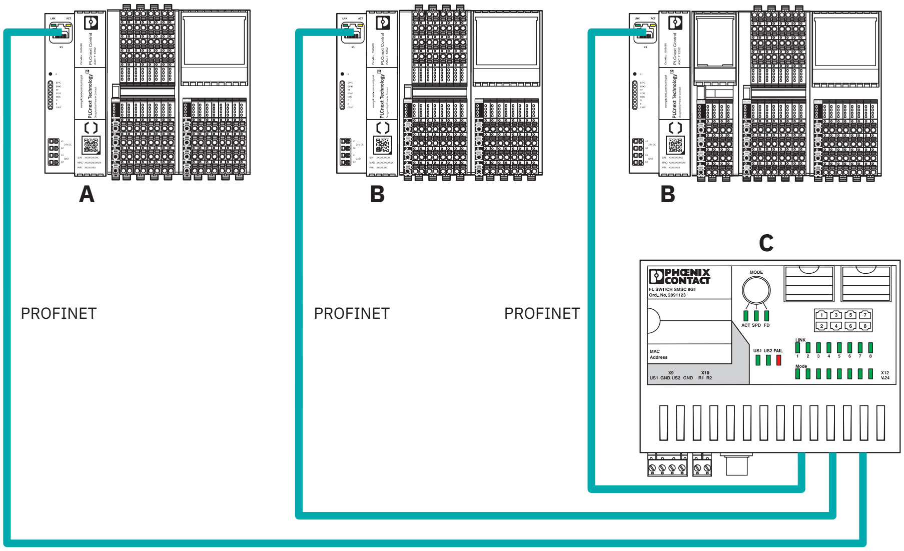
The controller can be used as a distributed controller of an Axioline F station that is connected to an Ethernet system (e.g., for connection to PLCnext Engineer).

Figure 3-3 Example: Axioline F station with AXC F 1252



3.3.2 Operation as a PROFINET controller

Figure 3-4 Example: AXC F 1252 as PROFINET controller



A AXC F 1252 PROFINET controller

B PROFINET devices (controller with aligned Axioline F modules)

C Managed switch

The PROFINET controller function is disabled in the delivery state (default setting). You can enable or disable the PROFINET controller function in the web-based management for the controller on the **System → System services** page.

For information on how to integrate the controller into a PROFINET network as a PROFINET controller, please refer to the PLCnext Engineer online help.

Please note: The PROFINET functionality is limited when the firewall is enabled (default setting). To use the PROFINET functionality, you must configure the firewall accordingly.

Information on this can be found in the PLCnext Technology - Security Info Center.

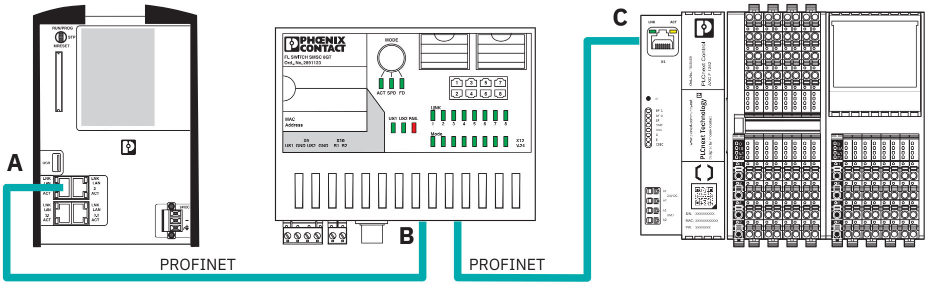
NOTE: Unauthorized access via PROFINET DCP

When the PROFINET controller function is enabled, the controller can be accessed via PROFINET DCP. Unauthorized persons could change the IP address and/or device name of the controller.

- Disable the PROFINET controller function when you operate the controller without a PROFINET connection.

3.3.3 Operation as a PROFINET device

Figure 3-5 Example: AXC F 1252 as a PROFINETdevice



A PROFINET controller
B Managed switch
C AXC F 1252 PROFINET device

The PROFINET device function is enabled in the delivery state (default setting). You can enable or disable the PROFINET device function in the web-based management for the controller on the **System → System services** page.

Please note: The PROFINET functionality is limited when the firewall is enabled (default setting). To use the PROFINET functionality, you must configure the firewall accordingly.

Information on this can be found in the PLCnext Technology - Security Info Center.

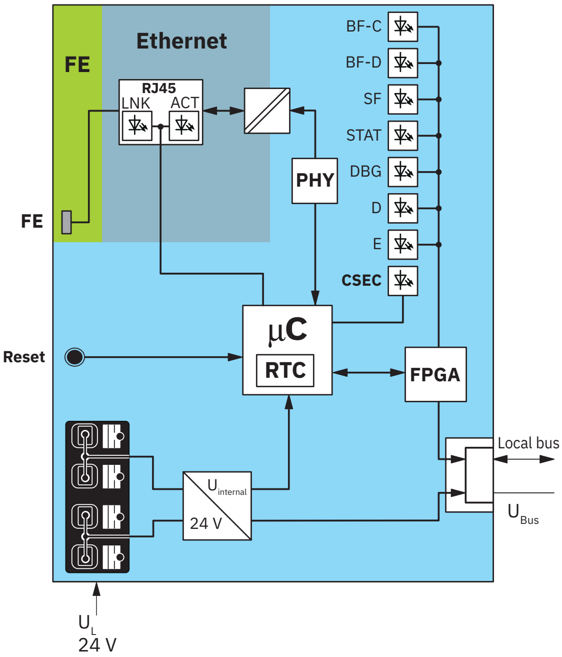
NOTE: Unauthorized access via PROFINET DCP

When the PROFINET device function is enabled, the controller can be accessed via PROFINET DCP. Unauthorized persons could change the IP address and/or device name of the controller.

- Disable the PROFINET device function when you operate the controller without a PROFINET connection.

3.4 Internal basic circuit diagram

Figure 3-6 Basic circuit diagram

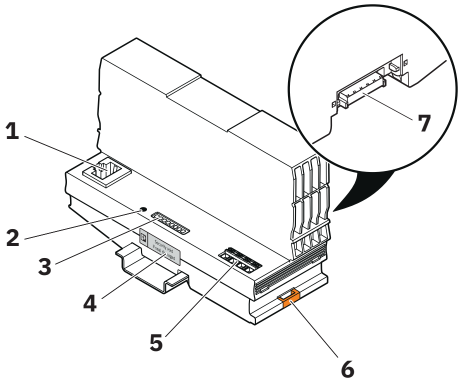


Key:

FE	Functional ground	RJ45	RJ45 interface
Ethernet	Ethernet	⍒	LED
Reset	Reset button	⫽	Electrical isolation for data or power supply
Local bus	Axioline F local bus	PHY	PHY
U_{Bus}	Axioline F local bus supply	µC RTC	Microcontroller with integrated realtime clock
$U_{internal}$	Internal supply	FPGA	FPGA
U_L	Communications voltage	╱	Power supply unit
		▨	Electrically isolated areas

3.5 Components

Figure 3-7 Components



1 Ethernet interface (RJ45 jack)

2 Reset button

3 LEDs

4 Security seal

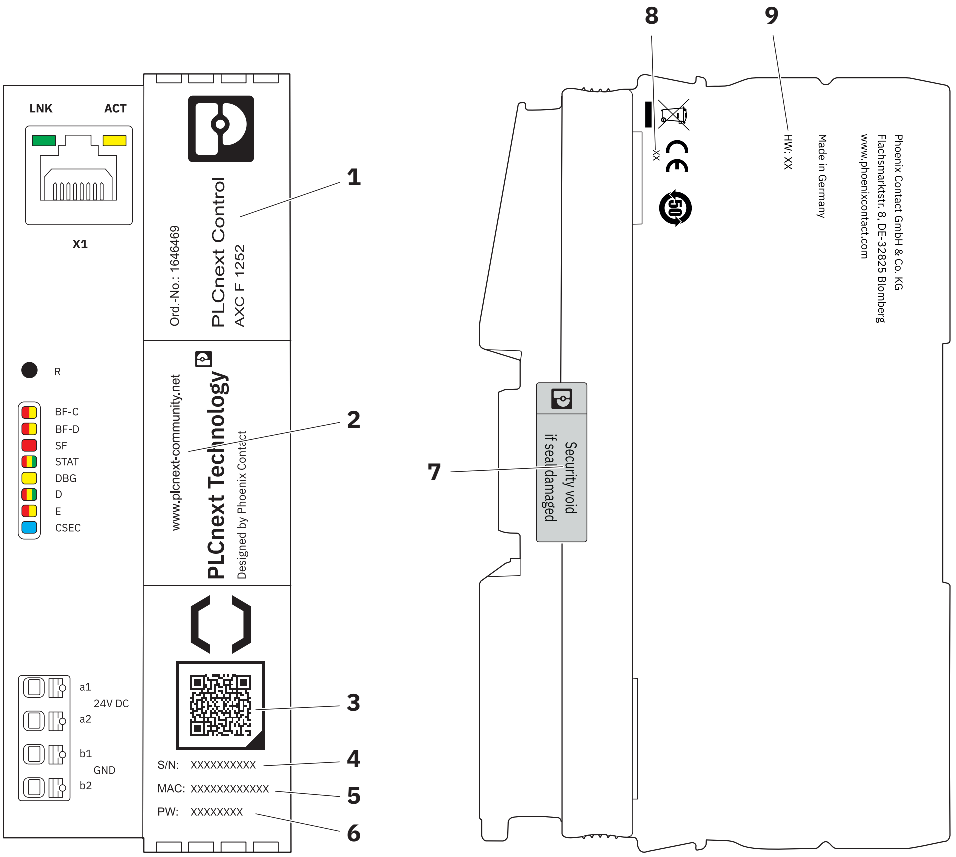
5 Connections for the power supply

6 Base latch

7 Integrated bus base
(connection for the bus base module of the following Axioline F module or the following Axioline F backplane)

3.6 Printing

Figure 3-8 Printing



1 Item number and item designation
2 PLCnext Community web address
3 QR code (identification link): Link to the website of the digital twin
See Section 3.12, “Digital twin”
4 Serial number
5 MAC address
6 Administrator password
7 Security seal
See Section 3.2, “Industrial cybersecurity”
8 Year of manufacture
9 Hardware version

3.7 LEDs

Figure 3-9 LEDs

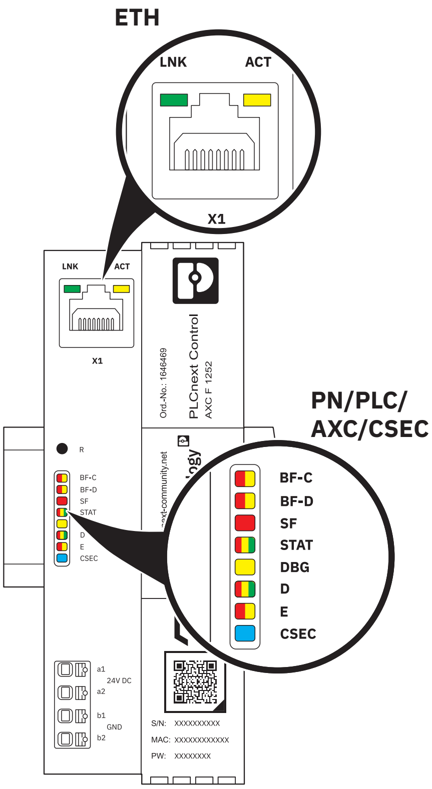


Table 3-1 LEDs on the controller

Designation	Meaning	Color	State	Description
PN: PROFINET controller/device function				
BF-C	Bus error at PROFINET controller	Red/yellow	**AXC F 1252 as PROFINET controller**	
			Red on	Bus error. No link status at the Ethernet interface and/or no 100 Mbit transmission and/or no full duplex mode.
			Flashing red (0.5 Hz)	Bus error. Link status present at the Ethernet interface but at least one configured PROFINET device has no communication connection.
			Flashing yellow (2 Hz)	No bus error. PROFINET device identification (DCP Signal Service) has been enabled.
			Off	No bus error. The AXC F 1252 has established an active communication connection to each configured PROFINET device. Or: No PROFINET devices are configured. Or: The PROFINET controller function is disabled.
BF-D	Bus error at PROFINET device	Red/yellow	**AXC F 1252 as PROFINET device**	
			Red on	Bus error. No link status at the Ethernet interface; a communication connection cannot be established.
			Flashing red (0.5 Hz)	Bus error. Link status present at the Ethernet interface but there is no communication connection to the PROFINET controller.
			Flashing yellow (2 Hz)	No bus error. PROFINET device identification (DCP Signal Service) has been enabled.
			Off	No bus error. An active communication connection has been established between the PROFINET controller and the AXC F 1252. Or: The PROFINET device function is disabled.
SF	Group error (PROFINET)	Red	On	Group error. PROFINET diagnostics present.
			Off	No group error.

Table 3-1 LEDs on the controller

Designation	Meaning	Color	State	Description
PLC: AXC F 1252 diagnostics				
STAT	AXC F 1252 status	Red/yellow/green	Green on	The PLCnext Runtime System has been successfully initialized. An application program is being executed or the controller is running at no load. The controller is in the RUN state.
			Flashing green (0.5 Hz)	The PLCnext Runtime System has been successfully initialized. No application program is being executed. The controller is in the STOP state.
	Reset type 2		Flashing red/yellow	The controller has been reset with reset type 2. The recovery system has been started. User action required (see Section 3.8.1.2, "Resetting with reset type 2").
	Error		Red on	An error has occurred in the application program.
			Flashing red (2 Hz)	System watchdog has been triggered.
	Firmware status		Yellow on	Firmware is faulty.
			Flashing yellow (2 Hz)	Firmware is being loaded (boot process).
DBG	Debug mode	Yellow	On	The PLCnext Runtime System is running in debug mode.

Table 3-1 LEDs on the controller

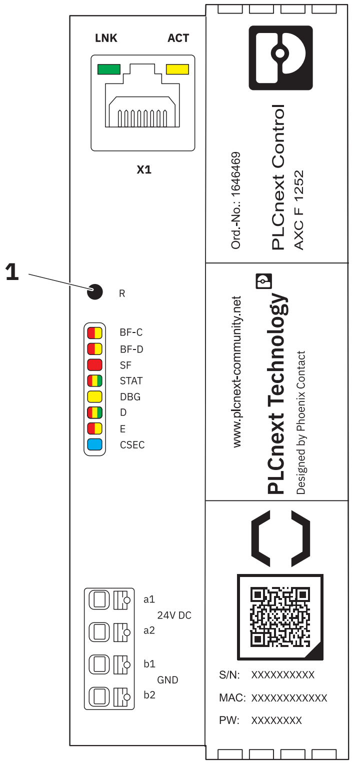
Designation	Meaning	Color	State	Description
AXC: Axioline F diagnostics				
D	Axioline F: Diagnostics for local bus communication	Red/yellow/ green	Green on	Run: The Axioline F station is ready for operation; communication within the Axioline F station is OK. All data is valid. No malfunction occurred.
			Flashing green	Active: The Axioline F station is ready for operation; communication within the Axioline F station is OK. The data is **not** valid. The AXC F 1252 is not providing valid data. No malfunction occurred on the controller.
			Yellow on	Ready: The Axioline F station is ready for operation. No data is being transmitted.
			Flashing red	Local bus error during startup Possible causes: – The configuration cannot be generated. Information from a local bus device is missing. – Chip version of a local bus device is < V 1.1 – Desired configuration and actual configuration differ – No local bus device connected – The maximum number of local bus devices has been exceeded
			Red on	Bus error in RUN state The Axioline F station is ready for operation but has lost connection to at least one local bus device. Possible causes: – Communication error – Local bus device has been removed or configured local bus device is missing – Reset at a local bus device – Serious device error at a local bus device (local bus device can no longer be reached)
E	Axioline F: Error/warning	Yellow/red	Yellow on	I/O warning at a local bus device
			Red on	I/O error at a local bus device
			Off	No I/O messages present.

Table 3-1 LEDs on the controller

Designation	Meaning	Color	State	Description
CSEC: Cybersecurity				
CSEC	Cybersecurity	Blue	On	Security incident detected (e.g., Secure Boot failed because the root file system could not be verified). The firmware has not been loaded. See Section 3.2, “Industrial cybersecurity” and PLCnext Technology - Security Info Center. ℹ At the start of the boot process, the LED lights up briefly. This has no security-related meaning and is only used to check the function of the LED and to indicate the first boot phase.
			Flashing	Security incident detected (e.g., Secure Boot failed because the kernel could not be verified). The firmware has not been loaded. See Section 3.2, “Industrial cybersecurity” and PLCnext Technology - Security Info Center.
			Off	No security incident detected. The firmware has been loaded.
ETH: Ethernet interface				
LNK	Link	Green	On	The Ethernet connection to a network device has been established.
			Off	No Ethernet connection has been established.
ACT	Activity	Yellow	On	The Ethernet interface of the AXC F 1252 is sending or receiving data.
			Off	No data is being transmitted.

3.8 Reset button

Figure 3-10 Reset button (1)



The reset button is approx. 1 cm below the corresponding opening in the housing.

Please note:
To actuate the reset button, you need a non-conductive, pointed object.

You can use the reset button to perform the following actions:

- Reset the controller (see Section 3.8.1)
- Restart the controller (see Section 3.8.2)

3.8.1 Resetting the controller

There are two reset types that you can use to reset the controller:
Reset type 1 and reset type 2.
Both reset types delete all the settings you have made. Reset type 2 also provides a recovery system that can be used to install new firmware.

- Perform reset type 1 if you wish to delete all the settings you have made.
- Perform reset type 2 if the firmware installed on the device is compromised or faulty and the controller is no longer booting correctly as a result.

Table 3-2 shows the scope of both reset types:

Table 3-2 Reset types

Component to be deleted during the reset	**Reset type 1**	**Reset type 2**
PLCnext Engineer project	√	√
IEC 61131-3 applications	√	√
High-level language applications	√	√
Configured bus configuration	√	√
Network settings	√	√
Changes and extensions that you have made to the operating system, to the firmware, or in the WBM	√	√
Proficloud connection	√	√
After the reset: **Recovery system is started**	–	√

Restoring the Proficloud connection

If you are operating the controller with a Proficloud connection:
After resetting with reset type 1 or 2, the controller can no longer be accessed in Proficloud. To make the controller accessible again, proceed as follows:

- Delete the controller from Proficloud.
- Reregister the controller in Proficloud and add it as a Proficloud device.
  Information on this can be found on the Internet at proficloud.io.

3.8.1.1 Resetting with reset type 1

NOTE: Unintentional reset with reset type 2
If you do not release the reset button in time, the controller is reset with reset type 2. In this case, the controller is not restarted automatically after resetting. You must open the recovery system and perform one of the possible actions (see Section 3.8.1.2, "Resetting with reset type 2").

- When resetting with reset type 1, observe the status of the STAT LED.
- Release the reset button as soon as the STAT LED flashes yellow.

- Disconnect the power to the controller.
- Press and hold down the reset button with a non-conductive, pointed object.
- Hold down the reset button and switch the supply voltage of the controller on.
- Continue to hold the reset button until the STAT LED flashes yellow. The process takes approx. 2 seconds.

  While the reset button is pressed, the LEDs behave as follows:

  1) The CSEC LED starts to light up blue.
  2) The STAT LED starts to flash yellow.
- As soon as the STAT LED flashes yellow, release the reset button.

↪ The STAT LED briefly lights up green, then the CSEC LED goes out.

↪ The controller is reset with reset type 1. During the reset process, all LEDs are off.

Once the reset process has been completed, the controller is restarted automatically.

After the reset:

- Before starting up the controller again, perform the steps described in Section 6, "Before initial startup and restarting".

Alternatively, you can also reset the controller via the WBM with reset type 1 (WBM page **System → Device maintenance**).

3.8.1.2 Resetting with reset type 2

- Disconnect the power to the controller.
- Press and hold down the reset button with a non-conductive, pointed object.
- Hold down the reset button and switch the supply voltage of the controller on.
- Press and hold the reset button until the STAT LED lights up green. The process takes approx. 40 seconds.

  While the reset button is pressed, the LEDs behave as follows:

  1) The CSEC LED starts to light up blue.
  2) The STAT LED starts to flash yellow.
  3) The STAT LED starts to light up green.
- Release the reset button as soon as the STAT LED lights up green.

↪ All LEDs go out.
Shortly thereafter, the STAT LED starts to flash red/yellow.

↪ The controller is reset with reset type 2 and the recovery system is started.

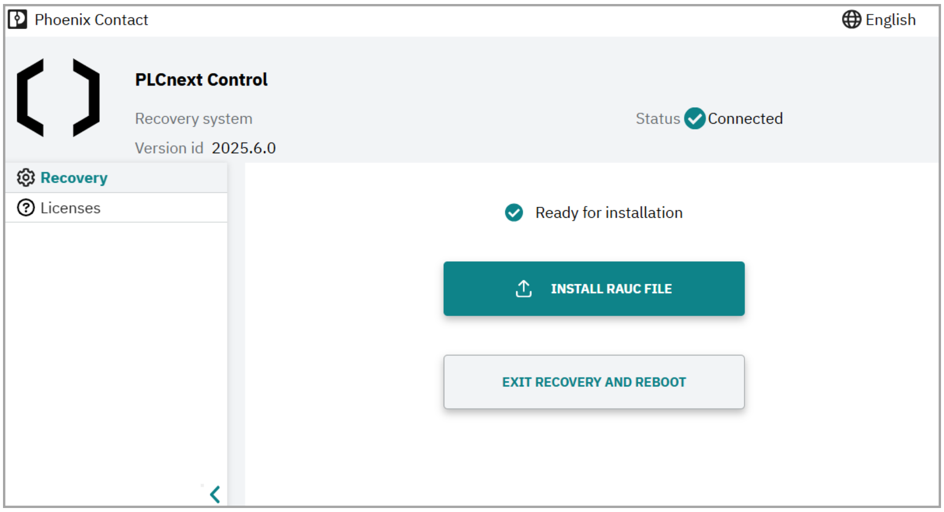
- Connect the controller to your PC using a suitable Ethernet cable.
- Open your web browser.
- Open the recovery system via the URL **http://192.168.1.10.**

  If the recovery system does not open:
  Check whether the URL you entered in the web browser actually starts with “http://”.
  The recovery system **cannot** be opened via an HTTPS connection.

  Please note:

  – As long as the recovery system is active, the LNK and ACT LEDs on the Ethernet interface are switched off (even when the Ethernet connection is active).
  – As long as the recovery system is active, the reset button has no function.

Figure 3-11 Recovery system



Phoenix Contact

English

PLCnext Control

Recovery system

Version id 2025.6.0

Status ✓ Connected

Ready for installation

You can perform the following actions in the recovery system:

– Install new firmware
– Restart the controller with the existing firmware

Installing new firmware

Perform this action if the firmware installed on the device is compromised or faulty.

- Click on “INSTALL RAUC FILE”.

↪ The File Explorer is opened.

- In the File Explorer, navigate to the directory containing the firmware file to be installed.

  Recommended: Always use the latest published firmware.

- Select the firmware file and click on “Open”.

↪ The firmware is installed.

Once the firmware is installed, the device restarts automatically.

After the reset:

- Before starting up the controller again, perform the steps described in Section 6, “Before initial startup and restarting”.

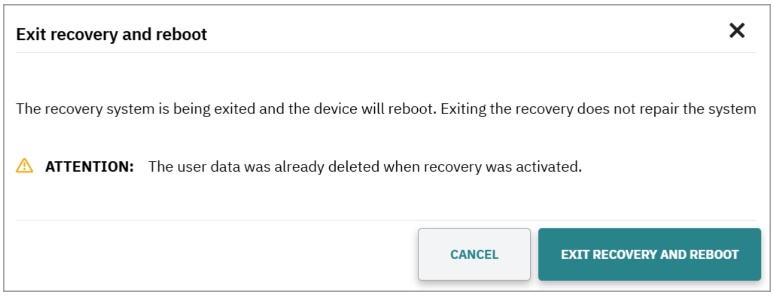
Restarting the controller with existing firmware

Perform this action if you have unintentionally reset the controller with reset type 2 and do not want to install any new firmware. The controller is restarted with the existing firmware.

- Click on “EXIT RECOVERY AND REBOOT”.

↪ The “Exit recovery and reboot” message opens.

Figure 3-12 “Exit recovery and reboot” message



Exit recovery and reboot

The recovery system is being exited and the device will reboot. Exiting the recovery does not repair the system

⚠ ATTENTION: The user data was already deleted when recovery was activated.

- To restart the controller with the existing firmware, click on “EXIT RECOVERY AND REBOOT”.

↪ The controller is restarted with the existing firmware.

  Please note: Before starting the recovery system, the controller was already reset with reset type 1, i.e., all components specified in Table 3-2 were deleted.
  Before starting up the controller again, perform the steps described in Section 6, “Before initial startup and restarting”.

3.8.2 Restarting the controller

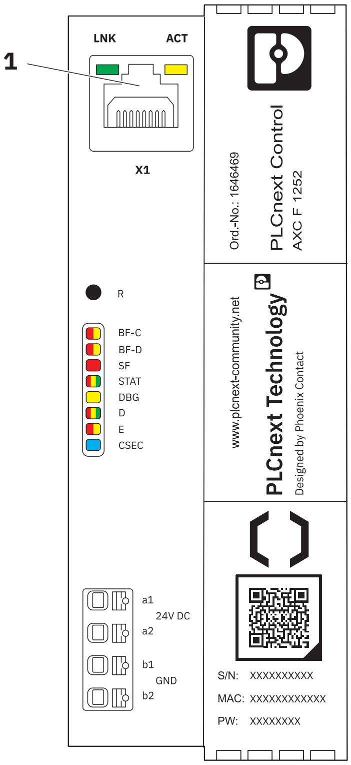
- During operation (boot process must be completed), press the reset button with a non-conductive, pointed object until the STAT LED briefly goes out. This process takes around 2 seconds.
- As soon as the STAT LED goes out, release the reset button.

↪ The controller is restarted.

ℹ Alternatively, you can also restart the controller via the WBM (WBM page **System → Device maintenance**).

3.9 Ethernet interface

Figure 3-13 Ethernet interface (1)



The controller has an Ethernet interface (RJ45 jack).
The default IP address of the Ethernet interface is 192.168.1.10.

3.10 Connections for the power supply

Figure 3-14 Connections for the power supply (1)

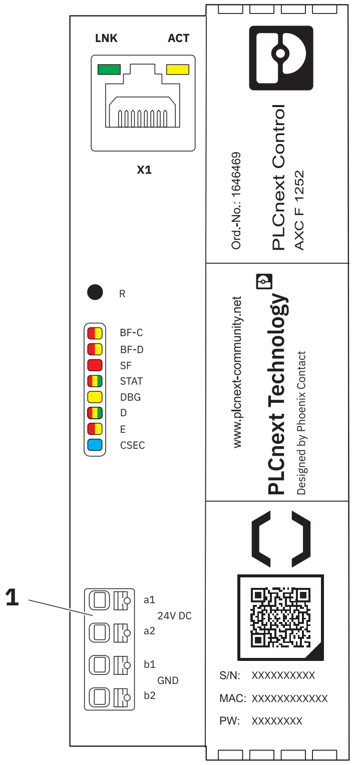
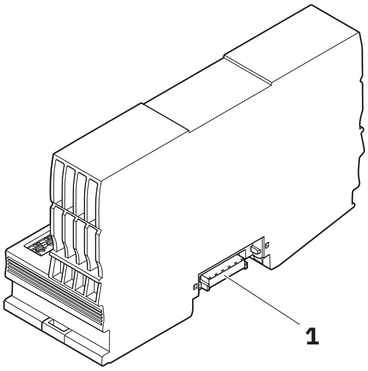


Table 3-3 Terminal point assignment

Terminal point	Assignment	
24 V DC (a1, a2)	24 V DC (U_L)	Supply voltage feed-in (communications voltage U_L, bridged internally)
GND (b1, b2)	GND	Supply voltage reference potential (communications voltage U_L, bridged internally)

3.11 Integrated bus base

Figure 3-15 Integrated bus base (1)



The controller has an integrated bus base. The bus base module of the following Axioline F module or the following Axioline F backplane is connected to this bus base (alignment on the right).

3.12 Digital twin

The digital twin is the virtual image of your device.

- To open the website of the digital twin, scan the QR code on the device (see Figure 3-8, 3).

The website of the digital twin includes:

– The digital nameplate
– Documentation (all documents with device-specific manufacturer information)
– The Asset Administration Shell (AAS)

3.13 Web-based management (WBM)

In the web-based management (WBM), you can access static and dynamic controller information and modify certain controller settings.

- To call the WBM, connect the controller to your PC via a suitable Ethernet cable and open the URL **https://controller IP address/wbm** using your web browser.
  The default IP address of the controller is 192.168.1.10.

3.14 Licensing information regarding open source software

The controller works with a Linux® operating system.

License information for the individual Linux® packages can be found in the following locations:

– In the controller file system under the path **/usr/share/common-licenses**.
– In the web-based management (WBM) for the controller (page **Help → Licenses**).

Notes on LGPL software libraries

All open source software used in the product is subject to the relevant license terms, which are not affected by the Phoenix Contact Software License Terms (SLT) for the product. In particular, the licensee may modify the respective open source software in accordance with the applicable license terms. If the licensee wishes to modify 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).

3.15 Directory structure of the file system

Access and access rights

You can access the controller via SFTP or via SSH and view the directories and files on the file system (on the internal flash memory), and modify them as necessary.

To avoid unauthorized access, port 22 is disabled in the delivery state. SFTP or SSH access to the controller is not possible.

- To access the controller via SFTP or SSH, you must configure the device firewall accordingly.
  Recommended:
  Define IP input and IP output rules for access via port 22.
  Disable port 22 if SFTP or SSH access is no longer required.
  Information on the configuration of the firewall can be found in the PLCnext Technology - Info Center.

Only users with administrator rights can access the file system. Access **always** requires authentication with a user name and password.

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

User name: admin
Password: Printed on the controller (see Figure 3-8, 6)

If necessary, you can create additional users with administrator rights in the WBM on the **Security → User management** page. Information on this can be found in the PLCnext Technology - Info Center.

Directory structure

Information on the directory structure of the file system can be found in the PLCnext Technology - Info Center.

3.16 Flash memory

All the settings and configurations that you have made are stored in the internal flash memory of the controller.
If you make changes to Linux® operating system files and directories on the flash memory, the Linux® operating system generates an overlay file system from the changed files and directories.

NOTE: Damage to the internal flash memory due to high data traffic
Frequent write access operations for applications with high data traffic can damage the internal flash memory of the controller (e.g., data logger applications). This results in a device defect.

- Keep the number of write access operations as low as possible.

3.17 Firewall

The controller firewall is enabled by default.

Information on the configuration of the firewall and on the ports can be found in the PLCnext Technology - Info Center and in the PLCnext Technology - Security Info Center.

Ports

The following ports are enabled for **incoming** connections in the delivery state:

- Port 41100 (remote access, e.g., for connecting to PLCnext Engineer)
- Port 443 (HTTPS, eHMI, WBM, and Proficloud)
- Port 4840 (OPC UA®)

The following ports are enabled for **outgoing** connections in the delivery state:

- UDP and TCP ports (permitted for easy startup)

  Please note: Only enable ports that are absolutely necessary for operation. Define the appropriate rules for this.

ICMP requests

Incoming and outgoing ICMP requests are permitted in the delivery state. The controller can be accessed via ping commands and can send ping commands.

3.18 System services

All available system services can be found on the **System → System services** page in the WBM for the controller.

Further information on the system services can be found in the PLCnext Technology - Security Info Center.

The following system services are enabled in the delivery state:

– App Manager
– Data Logger
– PLCnext Engineer HMI
– IEC 61131-3 Runtime for PLCnext Engineer
– OPC UA Server
– PROFINET Device
– Software Update via Device and Update Management

Recommended:

- Only enable the system services required for your application.
- Disable all system services that are not required.

3.19 System variables

Various system variables are provided for the application program. You can view the system variables in the PLCnext Engineer software.

Information on the individual system variables can be found in the PLCnext Technology - Info Center.

3.20 Proficloud

The controller can be managed and maintained remotely via the Proficloud plug-and-play IIoT platform.

Information on the available services (Smart Services) and on the connection of the controller to Proficloud can be found on the Internet at proficloud.io.

3.21 Requesting the source code

The controller 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 euros within three years after delivery of the controller.

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 AXC F 1252

4 Mounting the hardware

4.1 General safety notes

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components. 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: Device malfunction or damage to the contacts
When work is performed on the device while the power is connected, device malfunctions or damage to contacts may occur.

- Before performing any work, disconnect the controller and peripheral I/O devices from the power supply.
- Make sure that the supply voltage cannot be switched on again by unauthorized persons.

4.2 Basic information

Mounting location

The controller complies with IP20 degree of protection. It is intended for use in a closed control cabinet with IP54 degree of protection.

- When selecting the control cabinet, observe the recommended mounting distances for the controller as well as the Axioline F modules and/or Axioline F backplanes with plugged-in Axioline Smart Elements connected to the controller.
  See Section “Mounting distances”

NOTE: Risk of fire
Axioline F modules must be installed in the final protective housing, which provides sufficient resistance to mechanical strain and protection against the spreading of fire in accordance with the standards UL/IEC/EN 61010-1 and UL/IEC/EN 61010-2-201.

DIN rail

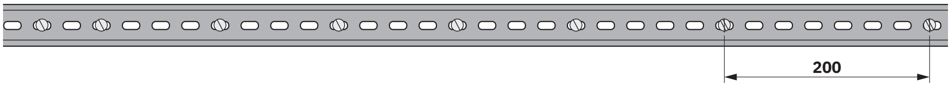
The controller is mounted on a grounded 35 mm standard DIN rail without any tools (recommended: DIN rail TH 35-7.5 in accordance with EN 60715). It is mounted perpendicular to the DIN rail.

NOTE: Damage to electronics and malfunctions due to inappropriate fastening elements
If the fastening elements (screws, rivets, etc.) for fastening the DIN rail are too high, the controller and the bus base modules of the Axioline F modules or the Axioline F backplanes will not snap onto the DIN rail correctly.

- For fastening the DIN rail, only use fastening elements with a maximum installation height of 3 mm.

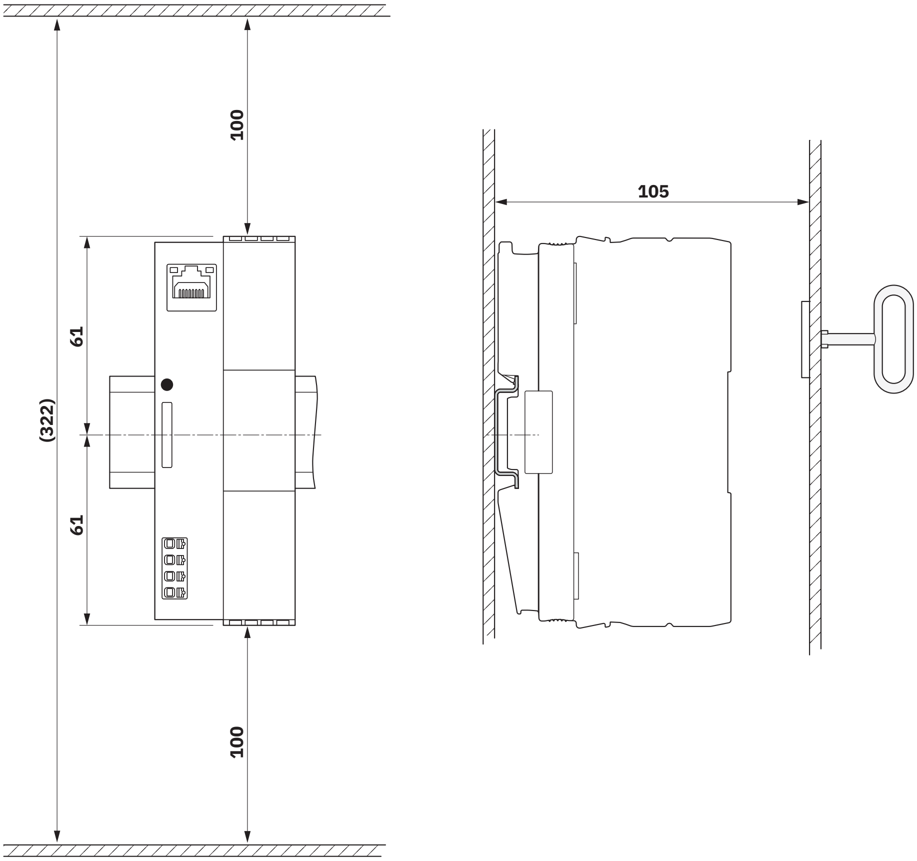
The distance between the fastening elements must not exceed 200 mm. This distance is necessary for the stability of the rail when mounting and removing devices.

Figure 4-1 Distance [in mm] between the DIN rail fastening elements



Mounting distances

Figure 4-2 Prescribed mounting distances from the AXC F 1252 controller to the upper and lower cable ducts and to the control cabinet door



- Observe the specified mounting distances.
- Only operate the controller within the permissible ambient temperature range (see Section 12.2, “Technical data”).

  Observe the temperature derating depending on the operating altitude.
  See Section A 1.
- Never cover the ventilation slots on the upper and lower sides of the controller.
- Depending on the ambient temperature, take one of the following measures:
  - Provide for air circulation within the control cabinet
  - Provide for control cabinet ventilation
  - Provide for control cabinet air conditioning

ℹ Also observe the recommended mounting distances for the Axioline F modules and/or Axioline F backplanes with plugged-in Axioline Smart Elements connected to the controller.
Information on this can be found in the user manual “Axioline F: system and installation”.
The user manual can be downloaded at http://www.phoenixcontact.com/product/1646469.

Mounting positions

Figure 4-3 Standard mounting position

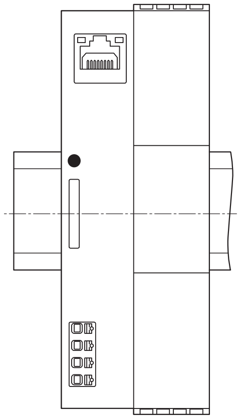
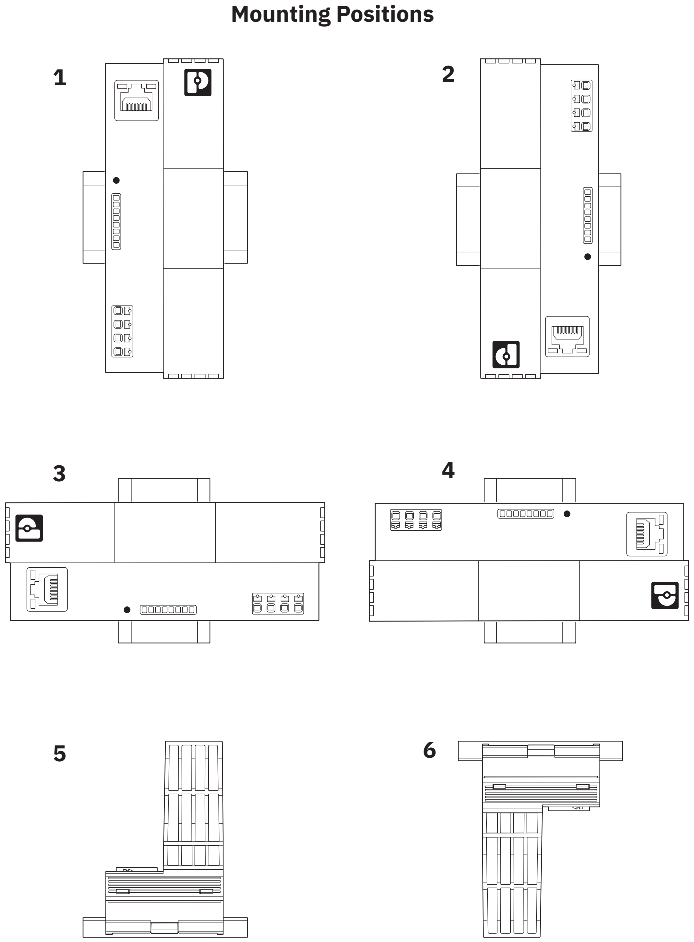


Figure 4-3 shows the standard mounting position of the controller (preferred mounting position).
Other mounting positions are possible (Figure 4-4).

Figure 4-4 Possible mounting positions



Please note:
If you mount the Axioline F station in a mounting position other than the standard mounting position, the connected Axioline F modules may require temperature derating.
Information on this can be found in the device-specific user documentation for the Axioline F modules.

End brackets

- Mount end brackets on both sides of the Axioline F station.

The end brackets ensure that the Axioline F station is correctly mounted. End brackets secure the station on both sides and keep it from moving from side to side on the DIN rail.

Recommended end brackets can be found in the user manual “Axioline F: system and installation”.
The user manual can be downloaded at http://www.phoenixcontact.com/product/1646469.

Functional ground (FE)

There are two FE springs (metal contacts) on the bottom of the controller which establish the connection to functional ground when the controller is snapped onto a grounded DIN rail.

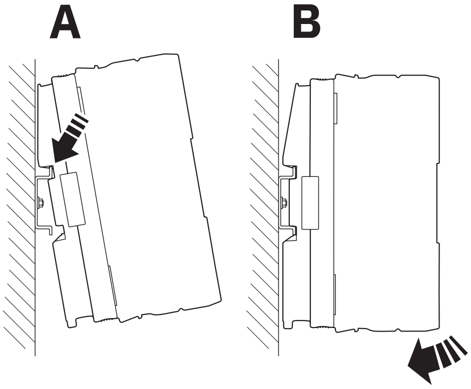
4.3 Mounting the hardware

NOTE: Tampering with the device through unauthorized physical access
There is a danger of the device being tampered with through unauthorized physical access.

- Protect the device against unauthorized physical access:
  Mount the device in a locked control cabinet, for example.

Mounting the controller

Figure 4-5 Mounting the controller



- Disconnect the Axioline F station from the power supply.
- Secure an end bracket to the DIN rail.
- Place the controller onto the DIN rail from above (Figure 4-5, A).
- Swivel the controller towards the DIN rail until the base latch audibly engages (Figure 4-5, B).

Mounting Axioline F modules

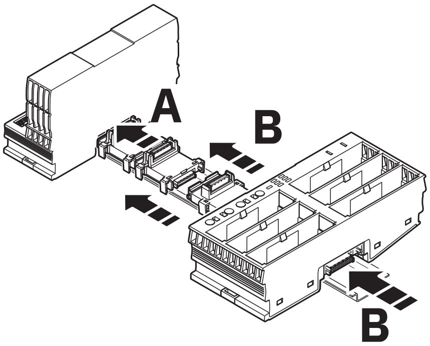
ℹ Detailed information on mounting Axioline F modules can be found in the user manual “Axioline F: system and installation”.
The user manual can be downloaded at http://www.phoenixcontact.com/product/1646469.

In the following, the term “bus base module” is used for both separate bus base modules and integrated bus bases.

Currently, the following devices have an integrated bus base:

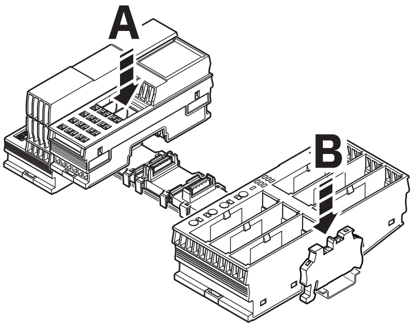
- AXC F 1252 controllers
- AXL F BP SE... Axioline F backplanes for Axioline Smart Elements

Figure 4-6 Mounting bus base modules of the Axioline F modules and Axioline F backplanes



- Place the bus base modules of all required Axioline F modules and all required Axioline F backplanes on the DIN rail as described in the device-specific user documentation.
- Push the connection of the first bus base module into the connection of the integrated bus base on the controller (Figure 4-6, A).
- Then push the connections of all bus base modules into each other (Figure 4-6, B).

Figure 4-7 Mounting the electronic modules of the Axioline F modules and end brackets



NOTE: Damage to the contacts when tilting
If you tilt the electronics modules of the Axioline F modules when placing them on the respective bus base modules, the contacts of the electronics modules may be damaged.

- Always place the electronics modules vertically on the bus base modules.

- Place the electronics modules of all Axioline F modules on the respective bus base modules (Figure 4-7, A).
- Attach an end bracket to the DIN rail to terminate the Axioline F station (Figure 4-7, B).
- Fit all the required connectors to the Axioline F modules.
  Observe the device-specific user documentation.
- Place all the required Axioline Smart Elements in the Axioline F backplanes.
  Observe the device-specific user documentation.

5 Connecting and wiring the hardware

5.1 General safety notes

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components. 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: Device malfunction or damage to the contacts
When work is performed on the device while the power is connected, device malfunctions or damage to contacts may occur.

- Before performing any work, disconnect the controller and peripheral I/O devices from the power supply.
- Make sure that the supply voltage cannot be switched on again by unauthorized persons.

5.2 Power supply

5.2.1 Safety notes

WARNING: Loss of electrical safety
The controller is designed exclusively for operation with safety extra-low voltage or protective extra-low voltage (**SELV/PELV**). If you operate the controller with another power supply, the loss of electrical safety can result in device damage or personal injury.

- Only use a power supply with double or reinforced insulation in accordance with IEC 61010-2-201 and EN 61010-2-201.
  This ensures safe isolation and prevents short circuit between the primary and secondary circuits.

WARNING: Loss of functional safety
For use in systems with **functional safety** components, note the following:

The controller may only be operated with a power supply with protective extra-low voltage (**PELV**). If you operate the controller with another power supply, the loss of functional safety can result in device damage or personal injury.

- Only use power supplies with protective extra-low voltage (PELV) in accordance with IEC 60204-1 and EN 60204-1.
- Observe the product-specific user documentation for the devices used.

NOTE: Damage to electronics due to overload

If external fuse protection is inadequate, the electronics in the device may be damaged in case of overload.

- Provide external fuse protection for the 24 V communications power of the controller. Take into account the current consumption of the controller as well as the current consumption of all connected Axioline F modules.
- Provide external fuse protection for the 24 V I/O supplies of the Axioline F modules that is suitable for the connected I/O devices.
- If using a fuse:
  To ensure reliable tripping in the event of an error, use a power supply that supplies four times the nominal current of the fuse.

NOTE: Damage to electronics due to excessive total current

The connections for the power supply are bridged internally on the PCB. This enables the supply voltage to be easily marshalled on the Axioline F devices. An excessively high total current can cause electronics damage to the device.

- Make sure that the maximum total current does not exceed 8 A.

NOTE: Device defect due to polarity reversal

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

- Avoid reversing the poles of the 24 V supply.

NOTE: Damage to the terminal points

There is risk of damage to the terminal points if they are mechanically overloaded.

- Implement strain relief for the connected cables.

A **power supply without a fall-back characteristic curve must** be used for correct operation of the controller.
When the controller is switched on, an increased inrush current occurs briefly. The controller behaves like a capacitive load when it is switched on.

IEC 61131-2 requires voltage failure resistance of 10 ms. To meet this requirement, only use power supply units (230 V AC/24 V DC, 400 V AC/24 V DC) that support voltage buffering for at least 10 ms.

5.2.2 Conductor cross-sections, stripping and insertion lengths

Conductor cross-sections

	[mm^2]	[mm^2]	[mm^2]	[mm^2]	AWG (Cu)
Push-in	—	0,2 - 1,5	0,2 - 1,5	0,2 - 1,5	24-16
	0,2 - 1,5	0,2 - 1,5	0,2 - 1,5	0,2 - 1,5	24-16

Stripping and insertion lengths

L [mm]	L [mm]	L [mm]	L [mm]
10	10	10	10

Recommended:

- Use CRIMPFOX 6 crimping pliers (item no. 1212034) to process ferrules.

5.2.3 Connecting the cables

Note the terminal point assignment in Section 3.10.

- Strip 10 mm of insulation off the cable.
- If necessary, fit a ferrule to the cable.

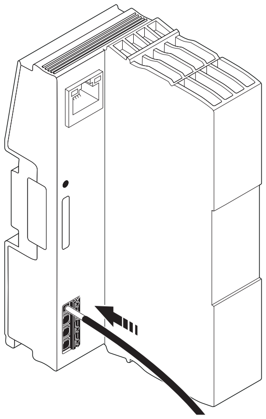
Without tools (Push-in)

The following cables can be connected without tools:

– Rigid cables

– Flexible cables with ferrules

Figure 5-1 Connecting cables without tools



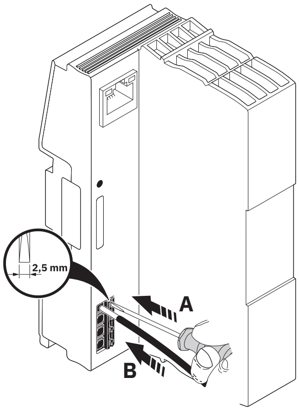
- Insert the cable into the terminal point.
  It is clamped into place automatically.

With tools

The following cables can be connected using a tool (e.g., a screwdriver):

– Flexible cables
– Rigid cables
– Flexible cables with ferrules

Figure 5-2 Connecting cables using a bladed screwdriver



- Open the spring by pressing the spring lever using the screwdriver (Figure 5-2, A). Use a bladed screwdriver with a blade width of 2.5 mm.

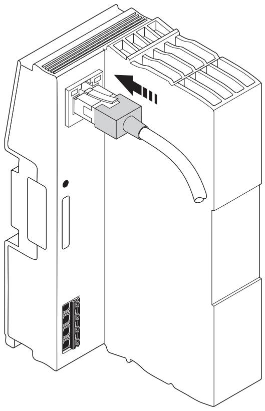
↪ The terminal point opens.

- Insert the cable into the terminal point (Figure 5-2, B).
- Remove the screwdriver to secure the cable.

5.3 Ethernet

Connecting the Ethernet cable

Figure 5-3 Connecting the Ethernet cable



- Use an Ethernet cable that complies with at least CAT5 of IEEE 802.3.
- Observe the bending radius of the Ethernet cable used.
- Insert the RJ45 connector of the Ethernet cable into the Ethernet interface until the connector audibly engages.

6 Before initial startup and restarting

- Before initial startup and restarting, perform all the steps described in this section in the order specified.

6.1 Checking the security context

- Check the security context of your application.
- Perform a risk analysis for your application.
  In particular, consider the following points:
  - Data protection
  - Integrity
  - Authenticity
  - Protection mechanisms against unauthorized access or malware

Information on this can be found in the PLCnext Technology - Security Info Center.

6.2 Adding the TLS certificate to the web browser as a trusted certificate

Before initial startup and restarting (i.e., after resetting the controller (see Section 3.8.1.1 and Section 3.8.1.2)), you should change the preset administrator password of the controller (see Section 6.3). To do this, you must access the web-based management for the controller.

For secure communication, the controller’s web server uses a self-signed TLS certificate generated by the controller. When you first access the WBM, the TLS certificate is not known to your web browser. Therefore, a security warning opens in the web browser, even though it is a secure connection.

Opening the WBM

- Connect the controller to your PC using a suitable Ethernet cable.
- Open your web browser.
- Open the URL **https://controller IP address/wbm**.
  The default IP address of the controller is 192.168.1.10.
- Allow the connection in your web browser.
  If no web page is opened in the web browser:
  Check whether the URL you entered in the web browser actually starts with “https://”. The WBM **cannot** be opened via an HTTP connection.

↪ The login page of the WBM opens.

- Log in to the WBM using the following access data:
  - User name: admin
  - Password: Printed on the controller (see Figure 3-8, 6)

Generating, downloading, and adding the TLS certificate to the web browser

To not receive a security warning when accessing the WBM in the future, proceed as follows:

- Open the **Configuration → Web Services** page in the WBM.
- Adjust the settings for your company and, if you have changed the IP address(es) of the controller, the IP address(es), and then generate the TLS certificate.

  See PLCnext Technology - Security Info Center
- Download the TLS certificate to your PC and add the certificate to the web browser as a trusted certificate.

  See PLCnext Technology - Security Info Center

6.3 Changing the administrator password

NOTE: Unauthorized administrator access

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

User name: admin
Password: Printed on the controller (see Figure 3-8, 6)

If you permanently use the printed password for the “admin” user, there is a risk of unauthorized administrator access.

- Change the password via the web-based management (WBM) before starting up the controller.

Changing the administrator password

- Open the **System → Device maintenance** page in the WBM.
- Change the password of the “admin” user.

  Observe the password complexity rules.
  You can customize the password rule set via the **Security → User management** page, if required.

6.4 Updating the firmware

- Open the **System → Update** page in the WBM.
- Update the firmware to the latest firmware version.
  Information regarding this can be found in the WBM.

↪ Immediately after the update process, the controller is restarted.

- Log in to the WBM again.
- Perform the firmware update for a second time.

↪ Immediately after the update process, the controller is restarted.

If the firmware update is performed twice, the new firmware version is saved in both the active and inactive boot partitions of the internal flash memory.
This is the only way to ensure that the controller always boots with the latest firmware version, even if the boot process has already failed five times.

Please note:
If you have previously reset the controller with reset type 2 and have already installed the latest firmware via the recovery system, you only need to perform the firmware update once before initial startup and restarting. With the firmware update via the recovery system and a subsequent firmware update via the WBM, the new firmware is saved in both boot partitions.

ℹ Information on the boot partitions and the behavior in the event of a boot process failure can be found in the PLCnext Technology - Info Center.

6.5 Ensuring realtime clock synchronization

NOTE: Impairment of security-related functions
The controller does not have a battery-buffered realtime clock (RTC). After the supply voltage is interrupted, the system time of the controller is reset. Security-related functions (e.g., event logging, time stamp for signing libraries) are impaired as a result.

- Make sure that the system time is automatically synchronized with an NTP server after every interruption of the supply voltage.

Adding an NTP server

- Log in to the WBM.
- Add the desired NTP server to your application as described in the PLCnext Technology - Security Info Center.
- Log out of the WBM.
- Make sure that there is an Ethernet connection to the NTP server at all times during operation.

Please note:
If the system time is not synchronized via the NTP server during the boot phase, the controller starts with the last system time before the supply voltage was interrupted.

7 Starting up (initial startup)

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

7.1 Installing PLCnext Engineer

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

- Download the software onto your Windows® PC.
- Double-click on the *.exe file to start installation.
- Follow the instructions in the installation wizard.

Make sure you install a version of the PLCnext Engineer software that is suitable for your controller:

Controller	PLCnext Engineer version
AXC F 1252	≥ 2026.0 LTS

7.2 Creating a new project

- Open PLCnext Engineer.
- On the start page, click on a project template, e.g., “AXC F 1252 v00 / 2026.0.0”.

↪ The project template for an empty AXC F 1252 project opens.

- Open the “File, Save Project As...” menu.
- Enter a unique and meaningful name for the project.
- Check the settings for the project integrity and enable the signature check if necessary.
  Information on this can be found in the PLCnext Technology - Security Info Center.
- Click on the “Save” button.

7.3 Connecting PLCnext Engineer to the controller

To be able to read the bus configuration of your Axioline F station or transfer an application program to the controller, you must connect PLCnext Engineer to the controller.

During initial startup, you can establish the connection directly, without making further settings in PLCnext Engineer.

The following requirements must be met for this:

- You have created your project with a project template (see Section 7.2, “Creating a new project”) and have not made any changes to the settings for the empty project.
- There is an Ethernet connection between your Windows® PC and the controller.
- The IP address 192.168.1.10 and the device name axc-f-1252-1 are set on the controller (default settings).
- Your PC is located in the same subnetwork as the controller.

If the requirements are not met (e.g., because you changed the IP address of the controller before startup):

- Customize the IP address range of the project and the IP settings of the controller according to your circumstances in PLCnext Engineer.
- Connect PLCnext Engineer to the controller.

Information on this can be found in the online help for PLCnext Engineer.

Establishing a connection

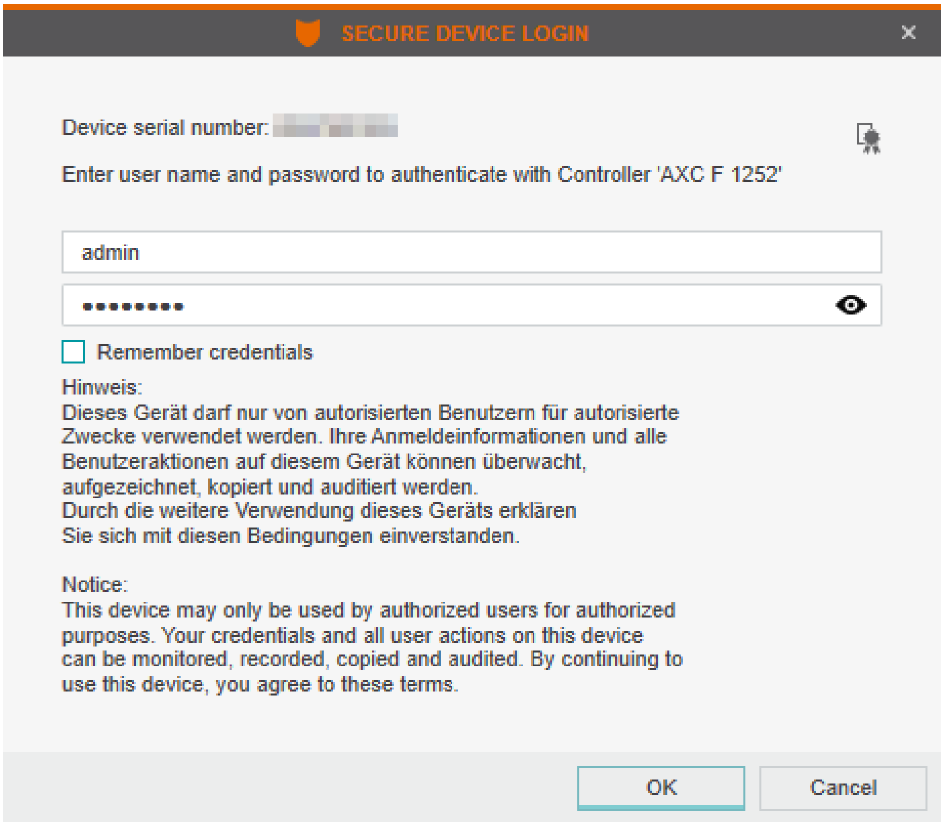
- Right-click on the controller node in the “PLANT” area.
- In the context menu, select the “ Connect/Disconnect” entry.

User authentication

You must authenticate yourself with the user name and password before establishing a connection between PLCnext Engineer and the controller:

The “SECURE DEVICE LOGIN” dialog opens.

Figure 7-1 “SECURE DEVICE LOGIN” dialog



Device serial number: [redacted]

Enter user name and password to authenticate with Controller 'AXC F 1252'

admin

●●●●●●●●●

□ Remember credentials

Hinweis:
Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

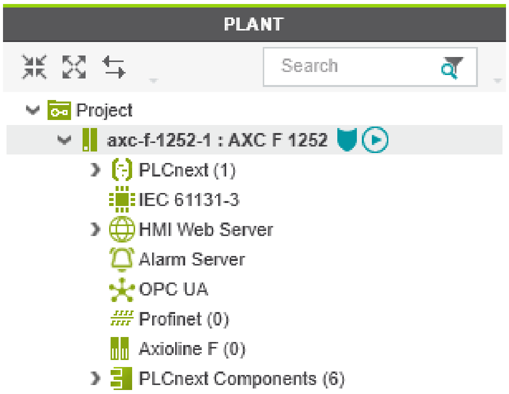
Notice:
This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

- Enter your user name and password.
  In the delivery state, the following access data is preset with administrator rights:
  User name: admin
  Password: Printed on the controller (see Figure 3-8).
- Optional:
  To save your login data, enable the “Remember credentials” check box.
- Close the dialog by clicking on “OK”.

↪ The connection between PLCnext Engineer and the controller is established.

The 🛡 ▶ icon next to the controller node in the “PLANT” area indicates that connection was successful.

Figure 7-2 Successful connection to the controller



- Make sure that your PC is connected to the correct controller.
  To do this, check the serial number of the device using the device certificate. The device certificate is displayed when you move the mouse pointer over the controller node in the “PLANT” area.

7.4 Setting the system time

Recommended:

- Set the system time of the controller.

You have two options for this:

1. Set the system time manually (see Section 7.4.1)
2. Synchronize the system time with a Windows® PC (see Section 7.4.2)

Please note:
The controller does not have a **battery-buffered realtime clock** (RTC). After the supply voltage is interrupted, the system time must be reset (see Section 6.5, “Ensuring realtime clock synchronization”).

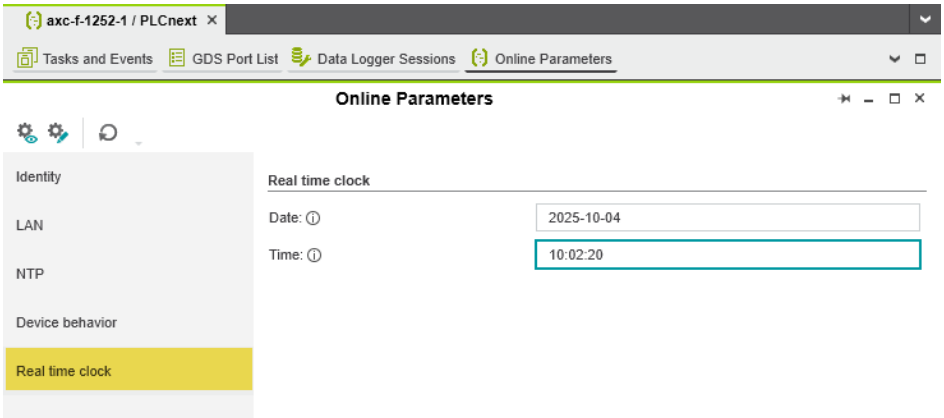
7.4.1 Setting the system time manually

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

↪ The “axc-f-1252-1 / PLCnext” editor group opens.

- Select the “Online Parameters” editor.
- Select the “Real time clock” view.

Figure 7-3 “Online Parameters” editor, “Real time clock” view



Date: 2025-10-04

Time: 10:02:20

- Enter the date in the “Date” input field (format: YYYY-MM-DD).
- Enter the time in the “Time” input field (format: hh:mm:ss).
- To transfer the system time to the controller, click on ⚙.

↪ The system time is transferred to the controller.

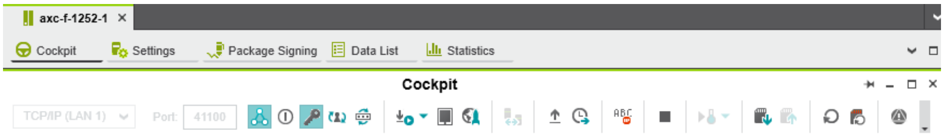
7.4.2 Synchronizing the system time with a Windows® PC

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

↪ The “axc-f-1252-1” editor group opens.

- Select the “Cockpit” editor.

Figure 7-4 “Cockpit” editor



TCP/IP (LAN 1) Port: 41100

- To synchronize the system time of the controller with the system time of your Windows® PC, click on 🕒.

↪ The system time of your Windows® PC is transferred to the device.

7.5 Further startup steps

Information on further startup steps can be found in the online help for PLCnext Engineer.

8 Removing hardware

8.1 General safety notes

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components. 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.

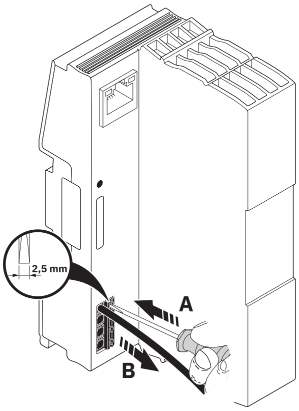
NOTE: Device malfunction or damage to the contacts
When work is performed on the device while the power is connected, device malfunctions or damage to contacts may occur.

- Before performing any work, disconnect the controller and peripheral I/O devices from the power supply.
- Make sure that the supply voltage cannot be switched on again by unauthorized persons.

8.2 Removing the hardware

8.2.1 Removing the cables

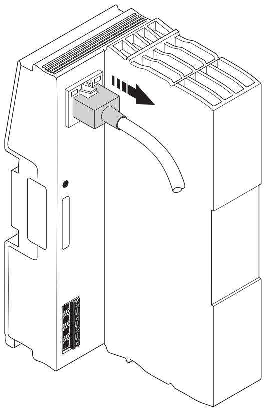
Figure 8-1 Removing the cables



- Remove all cables connected to the controller:
  - Open the spring by pressing the spring lever using the screwdriver (Figure 8-1, A). Use a bladed screwdriver with a blade width of 2.5 mm.
  - ↪ The terminal point opens.
  - Remove the cable (Figure 8-1, B).

8.2.2 Removing the Ethernet cable

Figure 8-2 Removing the Ethernet cable



- Release the RJ45 connector by pressing on the snap-in latch and remove the Ethernet cable from the controller.

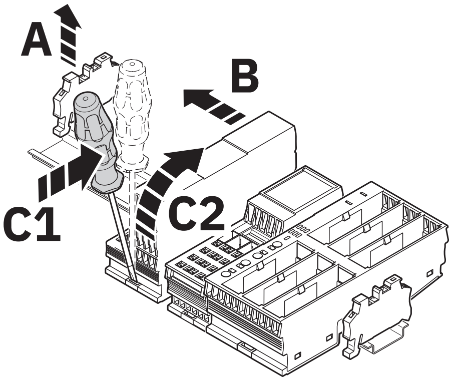
8.2.3 Removing the controller

NOTE: Damage to the connections

If you do not disconnect the integrated bus base of the controller from the adjacent bus base module, you can damage the connections during removal.

- Disconnect the adjacent bus base module from the controller’s integrated bus base by pushing the controller away from the adjacent bus base module on the DIN rail.
- Then snap the controller off the DIN rail.

Figure 8-3 Disconnecting the integrated bus base of the controller from the adjacent bus base module and removing the controller



- Remove the end bracket directly adjacent to the controller from the DIN rail (Figure 8-3, A).
- Slide the controller on the DIN rail toward the now open end until the controller connection is no longer in contact with the adjacent bus base module (Figure 8-3, B).
- Insert a suitable tool (e.g., bladed screwdriver) into the snap-on mechanism (base latch) of the controller and release it (Figure 8-3, C1).
- Swivel the controller upward away from the DIN rail (Figure 8-3, C2) and remove the controller from the DIN rail.

8.3 Removing the Axioline F modules

NOTE: Damage to the contacts when tilting
If you tilt the electronics modules of the Axioline F modules when removing them from the respective bus base modules, the contacts of the electronics modules may be damaged.

- Always remove the electronics modules vertically from the bus base modules.

- Remove the Axioline F modules and the Axioline F backplanes as described in the device-specific user documentation.

  Observe the notes in the user manual “Axioline F: system and installation”.
  The user manual can be downloaded at http://www.phoenixcontact.com/product/1646469.

9 Device replacement, device defects, and repairs

9.1 Device replacement

The controller can be replaced, if necessary.

The new device must meet the following requirements:

- Same device type (same item number)
- Same or later hardware version
- Same or later firmware version

Removing the controller to be replaced

- Disconnect the Axioline F station from the power supply.
- Remove all cables.
- Remove the controller.

Detailed information on the individual steps can be found in Section 8, “Removing hardware”.

Mounting the new controller

- Place the controller onto the DIN rail from above.
- Swivel the controller toward the DIN rail until the base latch audibly engages.
- Slide the controller toward the neighboring bus base module until the integrated bus base of the controller is fully connected to the connection of the neighboring bus base module.
- Fasten an end bracket to the DIN rail adjacent to the controller.
- Connect the power supply and Ethernet.
  See Section 5, “Connecting and wiring the hardware”

Configuring a new device

Please note: A device replacement is equivalent to initial startup.

- Carry out all the steps described in Section 6, “Before initial startup and restarting”.
- Configure the new device in the same way as the previous device.
- Transfer the previous PLCnext Engineer project to the new device.

In preparation: As of firmware 2026.0 LTS, device replacement is simplified by the backup and restore function.

Proficloud connection

In case you operate the controller with a Proficloud connection:

- Delete the controller to be replaced from Proficloud.

Following the device replacement:

- Register the new controller in Proficloud and add it as a Proficloud device.
  Information on this can be found on the Internet at proficloud.io.

9.2 Device defects and repairs

Repairs may only be carried out by Phoenix Contact.

- In the event of a device defect, please contact Phoenix Contact.
- Reset the device with reset type 1 before returning it to Phoenix Contact (see Section 3.8.1.1, “Resetting with reset type 1”).
- 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.
- If the original packaging is no longer available, observe the following points:
  - During transport, observe the specifications regarding humidity and temperature range.
    See Section 12.2, “Technical data”
  - Use suitable ESD packaging to protect components that are sensitive to electrostatic discharge.
  - Ensure that the packaging you select is large enough and sufficiently thick.
  - Use suitable filling material.
  - If necessary, attach warning notes to the transport packaging so that they are clearly visible.
  - For domestic packages: Insert the delivery note in the package.
  - For packages to be shipped internationally: Place the delivery note inside a delivery note pocket and attach it to the outside of the package so that it is clearly visible.

10 Maintenance, decommissioning, and disposal

10.1 Maintenance

The controller is maintenance-free.

10.2 Decommissioning

- Carry out decommissioning in accordance with the requirements of the machine or system manufacturer.

If the device is to be used as intended in the future:

- Observe the storage and transport requirements.
  See Section 2, “Transport, storage, and unpacking”

10.3 Disposal

Disposing of the device

The symbol with the crossed-out trash can indicates that this item must be collected and disposed of separately from other waste. Phoenix Contact or public collection sites will take the item back for free disposal. For information on the available disposal options, visit phoenixcontact.com. Delete personal and sensitive data before returning products.

Disposing of the packaging

- Dispose of packaging materials that are no longer needed (cardboard packaging, paper, bubble wrap sheets, etc.) with household waste in accordance with the currently applicable national regulations.

11 Troubleshooting and frequently asked questions (FAQs)

ℹ Information on troubleshooting and answers to frequently asked questions (FAQs) can be found in the PLCnext Community.

12 Ordering data and technical data

12.1 Ordering data

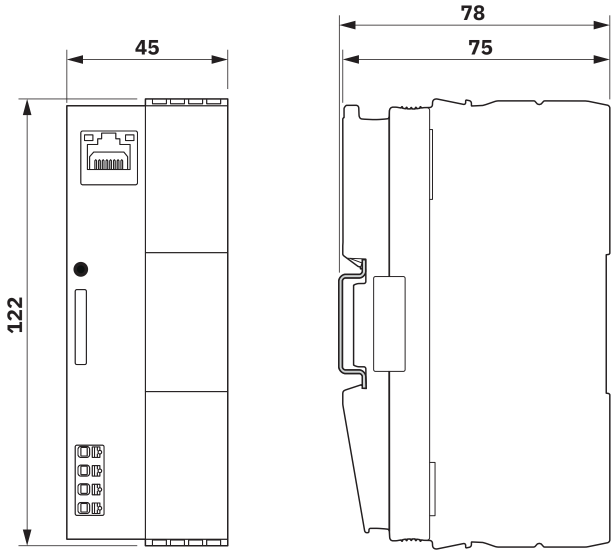
Description	Type	Item no.	Pcs./Pkt.
Controller (SPS), PLCnext Control; Programming: High-level language and IEC 61131-3; Operating system: Yocto/Linux® (real-time); Programming tool: PLCnext Engineer, Eclipse®, Visual Studio®, MATLAB®/ Simulink®; IoT connection: PROFICLOUD and every cloud via cloud connectors; Development process certified in accordance with IEC 62443-4-1, Product certified in accordance with IEC 62443-4-2 (Certification conditions see user documentation); Processor: Arm® Cortex®-A55, 2x 1.7 GHz.	AXC F 1252	1646469	1

Accessories	
For accessories, go to:	www.phoenixcontact.com/product/1646469

Documentation	
For further documentation, go to:	www.phoenixcontact.com/product/1646469

12.2 Technical data

Dimensions (nominal sizes in mm)	



Width	45 mm
Height	122 mm
Depth	75 mm
Note on dimensions	The depth applies when a TH 35-7.5 DIN rail is used (in accordance with EN 60715).

General data	
Color	Housing: traffic grey A (RAL 7042)
Weight	137 g
Type	modular
Mounting type	DIN rail mounting

ℹ Observe the temperature derating depending on the operating altitude specified in the appendix of the user manual.

Module classification	PLCnext Control for direct control of Axioline F I/Os.
Application type	distributed control technology

Features	
Industrial cybersecurity	yes
Safety function	no
Redundancy function	no
Diagnostics display	no
Web server	yes

Features	
External memory	no
Optical interface	no
Realtime clock	yes (not buffered)

System properties	
Operating system	Yocto/Linux® (real-time)
Processor	Arm®Cortex®-A55, 2x 1.7 GHz
Trusted Platform Module	TPM 2.0
RAM	1024 Mbyte
Flash memory	1.1 GByte (internal flash memory)
Application interface	OPC UA®

Ambient conditions	
Ambient temperature (operation)	-25 °C ... 60 °C up to 2000 m above mean sea level Operating altitude > 2000 m above mean sea level: Observe temperature derating
Ambient temperature (storage/transport)	-40 °C ... 85 °C
Air pressure (operation)	70 kPa ... 106 kPa (up to 3000 m above sea level)
Air pressure (storage/transport)	58 kPa ... 106 kPa (up to 4500 m above mean sea level)

Observe the temperature derating depending on the operating altitude specified in the appendix of the user manual.

Permissible humidity (operation)	5 % ... 95 % (according to DIN EN 61131-2)
Permissible humidity (storage/transport)	5 % ... 95 % (according to DIN EN 61131-2)
Degree of protection	IP20
Protection class	III (IEC 61140, EN 61140, VDE 0140-1)
Overvoltage category	II (IEC 60664-1, EN 60664-1)
Pollution degree	2 (IEC 60664-1, EN 60664-1)
Vibration (operation)	5g (IEC 60068-2-6)
Shock (operation)	30g (IEC 60068-2-27)
Continuous shock (operation)	10g (IEC 60068-2-27)

Do not use the device in an atmosphere that contains corrosive gas.

Connection data: Supply of the logic voltage U_L	
Connection method	Push-in connection
Conductor cross-section, rigid	0.2 mm^2 ... 1.5 mm^2
Conductor cross-section, flexible	0.2 mm^2 ... 1.5 mm^2
Conductor cross-section [AWG]	24 ... 16
Conductor cross-section flexible, with ferrule with plastic sleeve	0.2 mm^2 ... 1.5 mm^2
Conductor cross-section flexible, with ferrule without plastic sleeve	0.2 mm^2 ... 1.5 mm^2
Stripping length	10 mm

Interface Axioline F local bus	
Connection method	integrated bus socket
Number of interfaces	1
Transmission speed	100 Mbps
Electrical isolation	no
Number of supported devices	max. 63

Interface Ethernet	
Bus system	RJ45
Connection method	RJ45 jack
Note on the connection method	Auto negotiation and autocrossing
Number of interfaces	1
Transmission speed	10/100 Mbps (full duplex)
Transmission length	max. 100 m
Transmission physics	Ethernet in RJ45 twisted pair

System limits	
Amount of process data	max. 1482 Byte (per station (total input and output data)) max. 1024 Byte (Axioline F local bus (input)) max. 1024 Byte (Axioline F local bus (output))
Number of supported devices	max. 63 (per station)
Number of local bus devices that can be connected	max. 63 (observe current consumption)
Number of IO-Link masters	max. 8 (recommended)

NOTE: Electronics may be damaged when overloaded

Observe the logic current consumption of each device when configuring an Axioline F station. It is specified in every module-specific data sheet. The current consumption can differ depending on the individual module. The permissible number of devices that can be connected therefore depends on the specific station structure.

PROFINET	
Device function	PROFINET controller, PROFINET device
Number of supported devices	max. 16 (at PROFINET controller)
Conformance Class	B
Update rate	min. 8 ms (4 devices) min. 32 ms (16 devices)
Number of slots	1
Vendor ID	$00B0_{hex}$
Device ID	0193_{hex}
Process data width	2 Byte ... 512 Byte (PROFINET device)

Further specifications in relation to the firmware version used can be found in the PLCnext Technology - Info Center at the following address:
https://www.plcnext.help/te/Features_and_roadmaps/PLCnext_Technology_features.htm

Communications power U_L feed-in (the supply of the Axioline F local bus U_{Bus} is generated from U_L)	
Supply voltage	24 V DC
Supply voltage range	19.2 V DC ... 30 V DC (including all tolerances, including ripple (± 5 %))
Current consumption	typ. 63 mA (without I/Os and U_L = 24 V) max. 550 mA (with 2 A at U_{Bus} for the I/Os and U_L = 24 V)
Power consumption	typ. 1.5 W (without I/Os and U_L = 24 V) max. 13.2 W (with 2 A at U_{Bus} for the I/Os and U_L = 24 V)
Reverse polarity protection	electronic

NOTE: Electronics may be damaged when overloaded

Provide external fuses for the 24 V U_L area. If you are using an external fuse, the power supply unit must be able to supply four times the nominal current of the fuse. This ensures that it trips in the event of an error.

Axioline F local bus supply (U_{Bus})	
Supply voltage	5 V DC (via bus base module)
Power supply unit	2 A

Power dissipation	
Maximum power dissipation for nominal condition	3.2 W (3.2 W = 13.2 W - 10.0 W)

Programming Data	
Register length (master)	1482 Byte

Programming	
Programming tool	PLCnext Engineer Eclipse® Visual Studio® MATLAB®/ Simulink®
Programming languages supported	Symbolic flowchart (SFC) Ladder diagram (LD) Function block diagram (FBD) Structured text (ST) C++ C# Java Python® Simulink®

IEC 61131 runtime system	
Number of data blocks	depending on data storage
Number of control tasks	8
Cycle Time	4 ms (for cyclical task)
Program memory	8 Mbyte
Data storage system	12 Mbyte
Retentive data storage	16 kByte

Supported protocols	
Protocol	HTTP (only for access to the recovery system) HTTPS PROFINET INTERBUS Modbus/TCP Modbus/RTU (via corresponding library) CANopen® (via corresponding library) DALI (via corresponding library) DALI-2 (via corresponding app) HART (via corresponding library) IO-Link® (via corresponding library) MQTT (via corresponding app) OPC UA® Server OPC UA® Client (License required) DHCP (via corresponding library) SFTP SMTP (via corresponding library) SNTP (via corresponding library) SNMP (via corresponding library) DNS (via corresponding library) DNP3 (via corresponding library) IEC 60870-5-1 (via corresponding library) IEC 60870-5-104 (via corresponding library) IPsec syslog

Conformance with EMC Directive 2014/30/EU	
Immunity test in accordance with EN IEC 61000-6-2	
Electrostatic discharge (ESD) IEC 61000-4-2	Criterion B, ±6 kV contact discharge, ±8 kV air discharge
Electromagnetic fields IEC 61000-4-3	Criterion A, Field intensity: 10 V/m
Fast transients (burst) IEC 61000-4-4	Criterion B, ±2 kV
Transient overvoltage (surge) IEC 61000-4-5	Criterion B; DC supply lines: ±0.5 kV/±1.0 kV (symmetrical/ asymmetrical), fieldbus cable shielding: ±1.0 kV
Conducted interference IEC 61000-4-6	Criterion A, Test voltage 10 V
Noise emission test in accordance with EN IEC 61000-6-3	Class B

Approvals	
For the current approvals, go to:	www.phoenixcontact.com/product/1646469

Manufacturer's declarations	
For the current manufacturer’s declarations, go to:	www.phoenixcontact.com/product/1646469

A Appendix

A 1 Temperature derating depending on the operating altitude

The permissible ranges for ambient temperature and air pressure specified in Section 12.2, “Technical data” apply at an operating altitude of up to 2000 m above mean sea level.

If you use the device at an altitude of more than 2000 m above mean sea level up to 5000 m above mean sea level, the permissible maximum ambient temperature is reduced.

- Calculate the permissible maximum ambient temperature for the operating altitude of your device using the multiplication factor specified in Table A-1 and the maximum permissible ambient temperature specified in Section 12.2.

Temperature derating

Table A-1 Temperature derating depending on the operating altitude

Operating altitude	Multiplication factor in accordance with DIN EN 61131-2
0 m ... 2000 m amsl	1.00
2001 m ... 3000 m amsl	0.88
3001 m ... 4000 m amsl	0.78
4001 m ... 5000 m amsl	0.68

B Appendix for document lists

B 1 List of figures

Section 2

Section 3

Section 4

Section 5

Section 7

Section 8

B 2 List of tables

Section 3

Appendix A

B 3 Index

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 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 documentation 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.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document are prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.com/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

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
Email: info@phoenixcontact.com
phoenixcontact.com