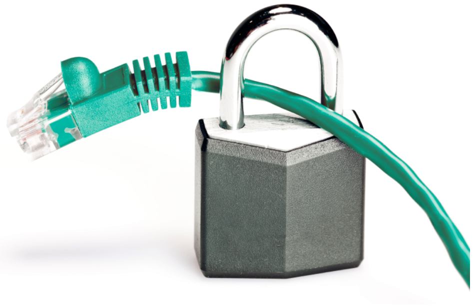
INDUSTRIAL SECURITY

Measures to protect network-capable devices with communication interfaces, solutions, and PC-based software against unauthorized access



Application note
107913_en_04

1 Introduction

In the context of cybersecurity, you have to protect components, networks, and systems against unauthorized access and ensure the integrity of data. For this, you must take organizational and technical measures to protect network-capable devices, solutions, and PC-based software.

Phoenix Contact strongly recommends using an Information Security Management System (ISMS) to manage all of the infrastructure-based, organizational, and personnel measures that are needed to ensure compliance with information security requirements.

Furthermore, Phoenix Contact recommends that the following measures should at least be considered.

More detailed information on the measures described in the following documents is provided here[1]:

- IT basic protection compendium of the German Federal Office for Information Security (BSI)
- Recommendations of the BSI for ICS (Industrial Control System) operators
- Cybersecurity best practices of the US CISA (Cybersecurity & Infrastructure Security Agency)

[1] This material is continuously updated. Make sure you are always using the latest versions.

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

Table of contents

2 Recommended measures for devices and solutions

2.1 Do not integrate components and systems into public networks

- Avoid integrating your components and systems into public networks.
- If you need to access your components and systems via a public network, use a VPN (Virtual Private Network).

2.2 Set up a firewall

- Set up a firewall to protect your networks and the components and systems integrated into them against external influences.
- Use a firewall to segment a network or to isolate a controller.

2.3 Deactivate unused communication channels

- Deactivate unused communication channels (e.g., SNMP, FTP, BootP, DCP, etc.) on the components that you are using.

2.4 Take Defense-in-Depth strategies into consideration when planning systems

When protecting your components, networks, and systems, it is not sufficient to implement measures that have only been considered in isolation. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

- Take Defense-in-Depth strategies into consideration when planning systems.

2.5 Restrict access rights

- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.
- Deactivate unused user accounts.

2.6 Secure access

- Change the default login information after initial startup.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Change passwords in accordance with the rules applicable for their application.
- Use a password manager with randomly generated passwords.
- Wherever possible, use a central user administration system to simplify user management and login information management.

2.7 Use secure access paths for remote access

- Use secure access paths, such as VPN (Virtual Private Network) or HTTPS, for remote access.

2.8 Activate security-relevant event logging

- Activate security-relevant event logging in accordance with the security guideline and the legal requirements on data protection.

2.9 Use the latest firmware version

Phoenix Contact regularly provides firmware updates. Available firmware updates can be found on the product page for the respective device.

- Make sure that the firmware of all devices used is always up to date.
- Observe the Change Notes for the respective firmware version.
- Check the website of the Phoenix Contact Product Security Incident Response Team (PSIRT) for security advisories regarding published security vulnerability.

2.10 Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks, such as viruses, Trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.
- Use allowlist tools for monitoring the device context.
- Use an intrusion detection system for checking the communication within your system.

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

2.11 Perform regular threat analyses

To determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, threat analyses should be performed on a regular basis.

- Perform a threat analysis on a regular basis.

2.12 Secure access to SD cards

Devices with SD cards require protection against unauthorized physical access. An SD card can be read with a conventional SD card reader at any time. If you do not protect the SD card against unauthorized physical access (e.g., by using a secure control cabinet), sensitive data is accessible to all.

- Ensure that unauthorized persons do not have access to the SD card.
- When destroying the SD card, ensure that the data cannot be retrieved.

3 Recommended measures for PC-based software

PC-based software is used, for example, to set up, configure, program, and monitor devices, networks, and solutions.

Engineering software can manipulate the device or solution.

- To reduce the risk of manipulation, perform security evaluations regularly.

3.1 PC-based hardening and organization measures

Protect any PCs used in automation solution environments against security-relevant manipulations. This can be facilitated, for example, by taking the following measures:

- Boot up your PC regularly, and only from data carriers that are secured against manipulation.
- Set up restrictive access rights for any personnel that absolutely must have authorization.
- Protect your systems against unauthorized access with strong passwords and with rules to ensure that they remain strong.
- Deactivate unused services.
- Uninstall any software hat is not used.
- Use a firewall to restrict access.
- Use allowlist tools to protect important directories and data against unauthorized changes.
- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.
- Activate the update feature in accordance with the security directive.
- Activate the automatic screen lock function and automatic logout after a specified time.
- Perform backups regularly.
- Only use data and software from approved sources.
- Do not follow any hyperlinks listed that are from unknown sources, such as emails.

3.2 Use the latest software

- Always use the latest software version (for engineering software, operating systems, etc.).
- Check for any software updates available on the respective product page from Phoenix Contact.
- Observe the Change Notes for the respective software version.
- Check the website of the Phoenix Contact Product Security Incident Response Team (PSIRT) for security advisories regarding published security vulnerability.

3.3 Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks, such as viruses, Trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.

4 Phoenix Contact security advisories

4.1 Product Security Incident Response Team (PSIRT)

The Phoenix Contact Product Security Incident Response Team (PSIRT) gathers and analyzes any potential security vulnerabilities in Phoenix Contact products, solutions, and services. If a security vulnerability is identified, it will be listed on the PSIRT website under “Recent security advisories”, and a corresponding security advisory will be published. The website is updated regularly.

To stay up to date, Phoenix Contact recommends subscribing to the PSIRT newsletter (listed in the SERVICE box, under “Subscribe to PSIRT news”).

Anyone can submit information on potential vulnerabilities to Phoenix Contact PSIRT via email.

The aim of PSIRT is to work with vulnerability reporters professionally to handle any vulnerability claim that is related to Phoenix Contact products, solutions, and services.

5 Cybersecurity when using functional safety components

If you use functional safety components, you must implement security measures to ensure functional safety.

In this case, the cybersecurity measures must not adversely affect safety functions within the scope of functional safety.

In particular, you must take into consideration and evaluate the following basic requirements within the scope of a threat analysis:

– Integrity against manipulation
– Confidentiality through generally recognized procedures
– Availability of the machine and system, including safety functions

⚠ **WARNING: Loss of functional safety through corruption**

Unauthorized access to your network or the communication interface of the device can result in the loss of functional safety. The safety function could be corrupted or manipulated unintentionally or intentionally.

- Consider the safety function in your threat analysis.
- Implement appropriate security measures for protection against the unintentional or intentional manipulation of functional safety.