INDUSTRIAL SECURITY

Measures to protect network-capable devices with Ethernet connection against unauthorized access

Application note
107913_en_01

1 Introduction

For Phoenix Contact devices that can be integrated in an industrial network via Ethernet, organizational and technical measures must be taken in order to protect components, networks, and systems against unauthorized access and to ensure data integrity.

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

For more detailed information regarding the measures described, visit the following websites[1, 2]:

– ics-cert.us-cert.gov/content/recommended-practices
– bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS-Betreiber/empfehlungen-betreiber_node.html
– bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

2 Recommended measures

2.1 Do not integrate components and systems in public networks

- Avoid integrating your components and systems in public networks.
- If you have 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 in order to protect your networks and the components and systems integrated in 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.

[1] Last accessed on June 02, 2017

[2] Websites available in German language only

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

2.4 Consider Defense-in-Depth strategies when planning systems

- When planning systems, consider Defense-in-Depth strategies.

When it comes to protecting your components, networks, and systems, it is not enough to simply implement measures viewed in isolation. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

2.5 Restrict access rights

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

2.6 Protect passwords

- Change default passwords following initial startup.
- Change passwords regularly.
- Use secure passwords, e.g., at least ten characters long containing a mix of upper and lower case letters, numbers, and special characters.

2.7 Use secure access paths for remote access

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

2.8 Perform a regular threat analysis

- Perform a threat analysis on a regular basis.

In order to determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, a regular threat analysis is required.

2.9 Use up-to-date security software

- Install security software on all PCs in order to detect and eliminate security risks such as viruses, trojans, and other malware.
- Make sure that the security software is always up to date.

For the protection of networks for remote maintenance via VPN, Phoenix Contact offers the mGuard product series security appliances which you can find described in the latest Phoenix Contact catalog (phoenixcontact.net/products).