Mandatory implementation of verifiable security measures

How to make industrial networks more resilient

Learn how

- Modern production facilities are more vulnerable to cyberattacks than ever before
- Using IEC 62443-certified network components helps make industrial networks more secure
- By complementing certified products with secure development processes, solution architectures, and incident response structures, operators can implement a defense-in-depth security strategy

Introduction

While the increasing digitalization of industrial processes boosts efficiency and flexibility, it also makes modern production facilities more vulnerable to attacks. Cyberthreats no longer target only IT systems – they increasingly affect operational technology (OT) as well. To ensure adequate protection, a growing number of standards and legal requirements have been established (Figure 1).

Among the key regulatory frameworks is the IEC 62443 series of standards, which defines the requirements for components, systems, and processes in industrial automation. It is supplemented by European legislation such as the NIS 2 Directive and the Cyber Resilience Act (CRA), which require operators and manufacturers to implement verifiable security measures. NIS 2 extends responsibility beyond critical infrastructure systems to large parts of the industrial value chain. The CRA, on the other hand, addresses the cybersecurity of products with digital elements throughout their entire lifecycle. Together, these requirements aim to make industrial networks more resilient and ensure their continuous availability. ■

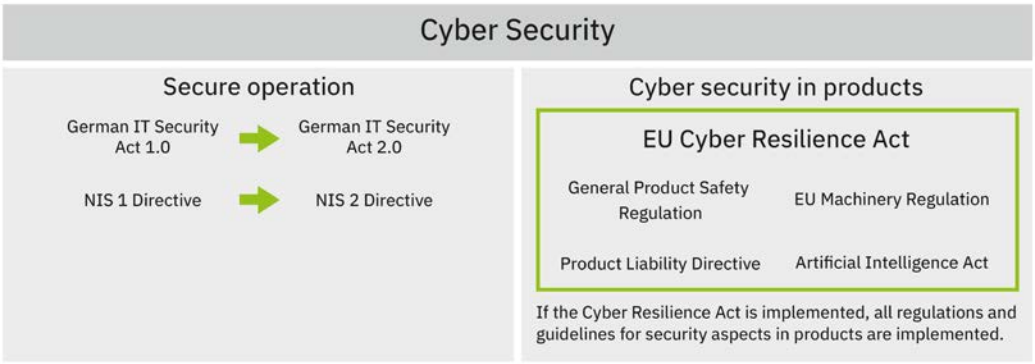

Figure 1: A comparison of the European NIS 2 and CRA legislation.

Securely developed devices with comprehensive security functions

Industrial networks consist of many components, each performing its own security-related role. Manufacturers such as Phoenix Contact offer solutions for these device categories that are developed using secure processes and are equipped with comprehensive security functions.

Managed switches form the backbone of communication. They ensure the segmentation, prioritization, and stability of data traffic. Security routers with firewall functionality protect the boundaries between zones or network segments and control who is allowed to access what. Wireless infrastructures, ranging from industrial WLAN access points to cellular routers, enable flexible applications and remote access. At the same time, however, they open up additional attack vectors via wireless technologies in the public sphere (Figure 2).

Many of these devices operate over long lifecycles within heterogeneous system structures. Over time, misconfigurations, inadequately secured interfaces, or firmware updates that have not been installed can expose critical vulnerabilities, leading to a major security risk.

Contents

Figure 2: Use of managed switches and security routers in the control cabinet.

Diverse requirements for network components

How can certified network components actually increase the cybersecurity of industrial networks? From the point of view of IEC 62443, components must contribute to achieving the security levels defined by the standard within a system. For network technology components, this means secure management access, role-based user and rights administration, cryptographically protected communication channels, firmware integrity checks, and traceable logging of security-related events.

In addition, there are hardening measures such as disabling unnecessary services or ports, protection against brute-force attacks, and secure update mechanisms. Only when these capabilities are present at the device level can operators efficiently map the zone and line models described in the standard in practice (Figure 3).

The benefits of such functions are especially evident in machine building and systems manufacturing. Today, production cells are typically designed as separate security zones with strictly defined communication relationships. Managed switches in these zones do more than just perform switching. They also logically separate the various machine components via VLANs, prioritize time-critical protocols (such as PROFINET or EtherNet/IP), and support ring redundancy mechanisms to ensure high availability.

Security routers installed at the boundary between the security zones enforce the strictly defined communication relationships mentioned above using integrated firewalls with stateful inspection. Remote service access can be enabled via IPsec or OpenVPN tunnels for a limited period of time and with unique authentication. This includes logging which connection was active when and which controllers were addressed. ■

Comprehensive protection of critical infrastructure and older systems

Public infrastructure and critical supply networks face even stricter requirements. Here, the control room, remote control, and field levels must be protected against both external attacks and misconfigurations. For example, managed switches ensure that only authorized devices are permitted access to specific ports (e.g., via port security, 802.1X, or MAC filters). This makes Layer 2 manipulation attempts more difficult. Time-stamped logs and integration with central Syslog or SIEM systems make it possible to track security-related events in the control center.

A third common scenario involves retrofitting older systems. Many control systems were originally developed without a focus on security. As a result, they do not use encrypted protocols or modern authentication mechanisms. Here, operators use certified security routers as an upstream layer of protection to operate these components in isolated segments. Typical measures include the strict allowlist configuration of permitted connections, the establishment of defined engineering access, and the

Figure 3: Network components from Phoenix Contact are certified in accordance with IEC 62443.

restriction of remote access to clearly defined maintenance windows. Combined with switch functions such as the port security described above, this approach significantly reduces the attack surface without requiring a fundamental overhaul of the existing automation infrastructure. ■

Collaboration based on clear processes

Certified individual devices alone are not enough, however. They only unleash their full potential within a coordinated system architecture, as specified by IEC 62443: defense in depth, zoning, defined communication paths, and consistent hardening measures. It is crucial that all stakeholders, including operators, integrators, and manufacturers, speak the same language and follow clear processes.

Figure 4: Phoenix Contact offers a holistic 360-degree security concept.

Companies like Phoenix Contact complement certified products with secure development processes, solution architectures, and incident response structures. Operators can rely on end-to-end security concepts that extend beyond the individual device. IEC 62443 supports operators not only in developing holistic security concepts but also in complying with new legal requirements, such as the CRA, because IEC 62443 already addresses them (Figure 4). ■

Certified cybersecurity from Phoenix Contact

Phoenix Contact offers a comprehensive portfolio of IEC 62443-4-2-certified products for industrial networks. These include the managed switches from the FL Switch 2000 series, security routers from the mGuard product family, and industrial cellular solutions such as the Cellulink routers for 4G/5G networks. Other series – such as the FL WLAN infrastructure devices with Wi-Fi 6/6E technology and the FL Switch 5900 series managed switches for 19-inch rack mounting – already meet key requirements of IEC 62443-4-2.

All products are developed using secure development processes, certified in accordance with IEC 62443-4-1. They comply with the security functions described for use in demanding OT environments. In addition to secure products and processes, Phoenix Contact's 360-degree security strategy also encompasses secure solutions and active vulnerability management by a Product Security Incident Response Team (PSIRT). The company thus supports operators in holistically securing industrial networks – from planning and operation to incident handling.

Learn more at www.phoenixcontact.com/cybersecurity.

About Phoenix Contact

Since 1923, Phoenix Contact has created products to connect, distribute, and control power and data flows. Our products are found in nearly all industrial markets. Sustainability and responsibility guide every action we take, and we are proud to collaborate with our customers to empower a smarter and better world for future generations. Together, we are creating a sustainable world based on our passion for technology and innovation.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com**, call technical service at **800-322-3225**, or email **us-info@phoenixcontact.com**.

Jan Aulenberg
Product Marketing Network Technology, Phoenix Contact GmbH & Co. KG, Bad Pyrmont, Germany, and Stephen Socash, Product Marketing Manager – Networking Components, Phoenix Contact USA