

Industrial cybersecurity

As digitalization increases, so do security risks and thus the risk of a cyberattack. Companies are required by law to protect themselves against cyberattacks, in particular in the field of critical infrastructure.

Industrial security protects against downtime, sabotage, and data loss. Comprehensive protection against unauthorized access is therefore an important requirement for automation systems.



360° cybersecurity

Our complete range

Phoenix Contact offers standardized security in products, industry solutions, and services for the future-proof operation of machines, systems, and infrastructures. Security is firmly rooted in the entire life cycle of our products and solutions. From the secure development process (certified in accordance with IEC 62443-4-1), through the integration of important security functions in our products (certified

in accordance with IEC 62443-4-2), right through to regular updates and security patches (PSIRT, also certified in accordance with IEC 62443-4-1).

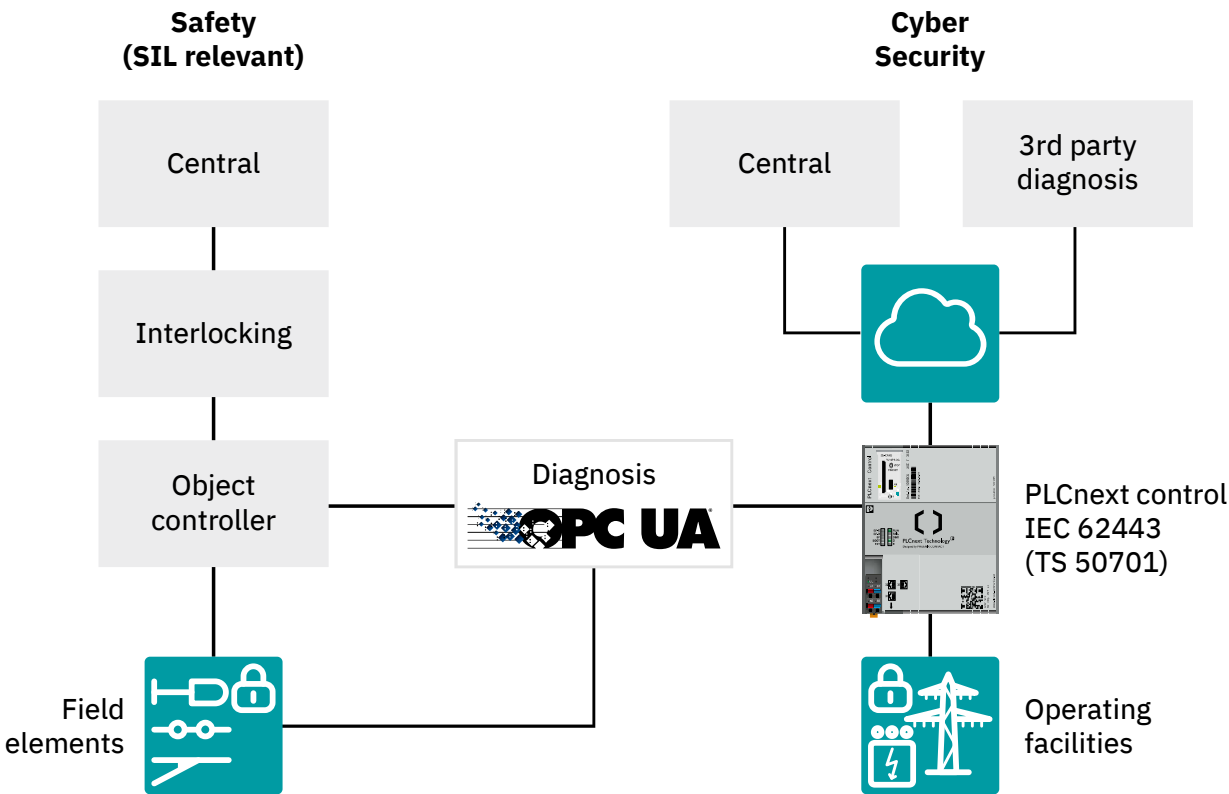
Our approach: we make state-of-the-art security manageable, e.g., through easy configuration, integrated security functions, sophisticated comprehensive solutions, and supportive consulting services (certified in accordance with IEC 62443-4-2). The

long-term availability of necessary updates also means that our components have a long useful life.

PLCnext Control for TS 50701 railway infrastructure applications

The TS 50701 standard describes the requirements on cybersecurity in the entire railway sector. The standard is derived from the IEC 62443-x-x-x series of industry standards for OT security. This means that industrial standard products that meet the requirements of IEC 62443-x-x can be used.

A selection of PLCnext Control and mGuard security routers already meet these requirements.



PLCnext Control combines control functionality, communication, and cybersecurity, e.g., in signal box applications

Control meets Security: PLCnext Technology

Compliant with IEC 62443-4-2

PLCnext Technology is the ecosystem for industrial automation, consisting of open hardware, modular engineering software, a global community, and a digital software marketplace.

PLCnext Control represents the first PLCs in the market to be certified by TÜV Süd in accordance with IEC 62443-4-1 ML 3 Full Process Profile in combination with IEC 62443-4-2. This confirms that the Secure Development Life Cycle was fully applied in developing PLCnext Control.

Product certification in accordance with IEC 62443-4-1 and -4-2 confirms that a product has been developed in accordance with secure design and provides information about which technical security requirements have been implemented.

In addition to the modular PLCnext Control AXC F 2152 and AXC F 3152 controllers, our high-performance RFC 4072S safety controller and the AXC F XT SPLC 1000 safety PLC extension have also been certified.

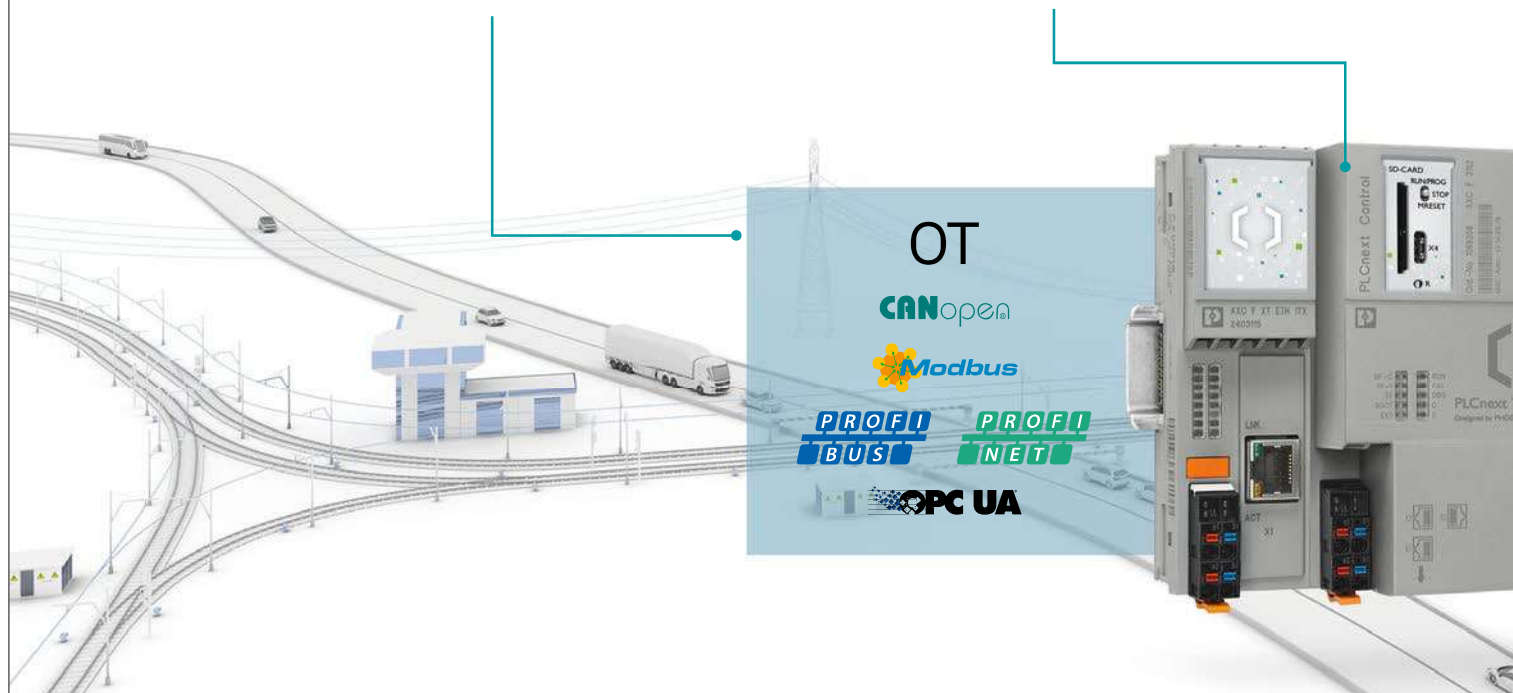
Benefit from the limitless possibilities of PLCnext Control

Communication protocols

PLCnext Control supports a wide range of relevant communication protocols. These are either already integrated, can be implemented via hardware components, or can be loaded later as function blocks. The fieldbus protocols include PROFINET, EIP, and CAN. HTTP, HTTPS, SFTP, SNMP, IPsec, syslog, and OPC UA are already available as common Ethernet protocols. MQTT, CODESYS, and Modbus/TCP can be loaded later as function blocks.

Edge computing

PLCnext Control for edge applications allows you to create IoT edge solutions for making the best cloud-based use of data from the field. This allows you to close the gap between the IT and OT worlds. You can reduce development and provision times using pre-installed software tools such as Node-RED, a local time series database, and a simple cloud connection. Simple and secure management is guaranteed via an integrated web-based management tool.



Product list PLCnext Technology

The automation technology portfolio for PLCnext Technology can be found in a clearly arranged online listing: phoenixcontact.com/plcnexttechnology_portfolio



PLCnext Community

Benefit from the experience of other users of PLCnext Technology. Whether you are looking for testimonials, apps, expert advice, 24/7 support, events and webinars, launch news, or industry trends, you will find everything in one place right here.

Find out more about the PLCnext Community. plcnext-community.net



PLCnext Technology
Designed by Phoenix Contact

Real-time capability, combinability of IEC 61131-3 and high-level languages

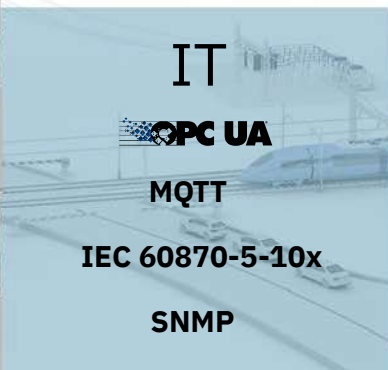
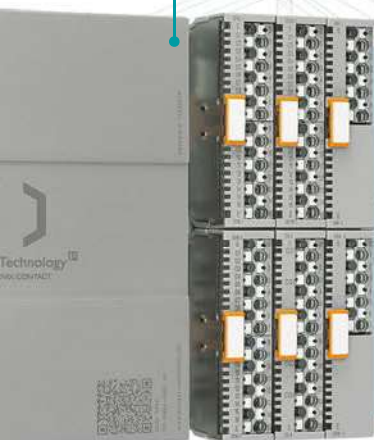
PLCnext Control enables the implementation of automation projects without the limitations of proprietary systems. The PLCs based on a Linux kernel are characterized by their real-time capability, for both IEC 61131-3 and high-level languages such as C/C++ and Matlab® Simulink®. The patented task handling allows any combination of IEC 61131-3 code, high-level languages, and model-based tools in one task.

Device und update management

The smarter automation components become and the more they communicate with remote (cloud) systems, for example, the more important it is to have up-to-date firmware for the individual components. Updates can be rolled out manually or automatically – and across manufacturers – with OPC UA-based device and update management. This saves time and costs, and minimizes the risk of cyberattacks.



TLS/VPN



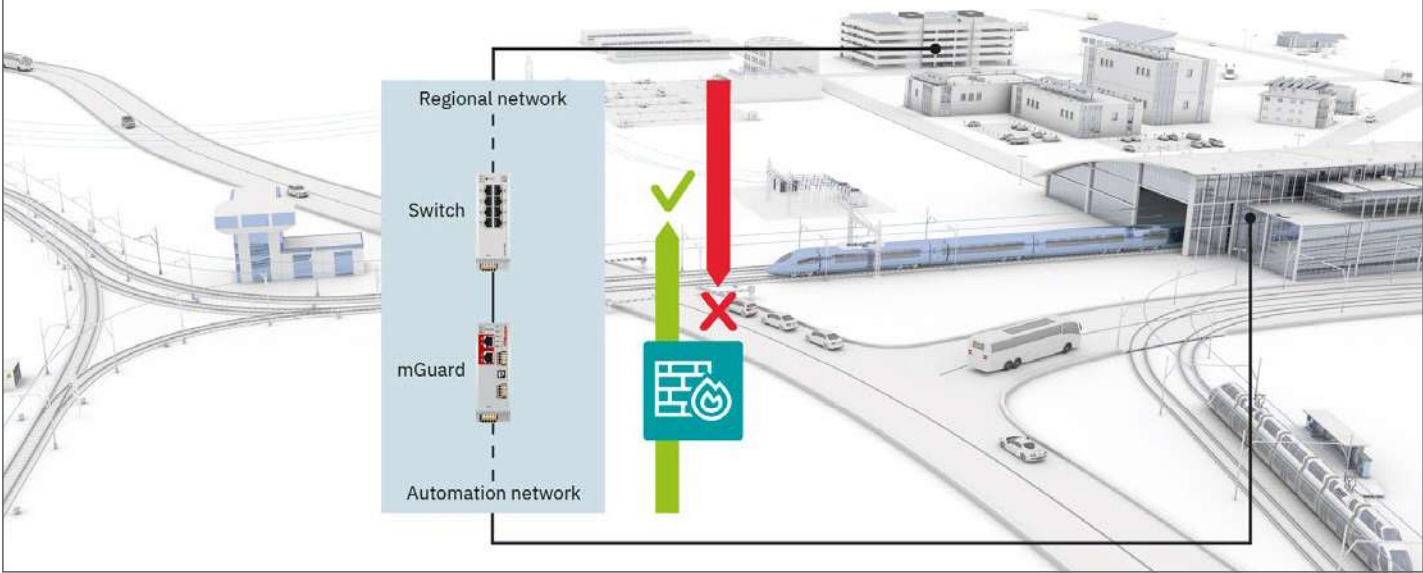
High-performance security routers

Protecting data communication against unauthorized access

As digitalization progresses, more and more communication and data networks are being set up for railway infrastructure. Although they are used for remote diagnostics or monitoring energy and systems and not in the vital area of control and safety technology, these networks must still be protected against unauthorized access by malware or people. After all, these systems are essential for smooth railway operations.

With their comprehensive security functions, mGuard security routers are the security backbone of your infrastructure. They are certified in accordance with IEC 62443-4-1 and IEC 62443-4-2. The integrated firewall protects against unwanted communication and access. With functions like network segmentation and high processing speed, a high level of security is guaranteed without any restrictions on data traffic. Secure remote

access is possible with encrypted VPN communication.



mGuard features



Gigabit data rate



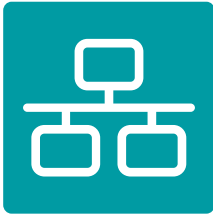
Firewall



Network Address Translation (NAT)



Network segmentation



Stealth mode



Secure remote maintenance

Product list

High-performance security routers: FL mGuard 2100/4300						
	Port configuration	Port speed	VPN	Special features	Type	Item no.
	2 x RJ45	10/100/1000 Mbps	Up to 2 VPN tunnels	–	FL MGuard 2102	1357828
			Up to 250 VPN tunnels	Extended firewall functions, DNV approval	FL MGuard 4302	1357840
			Up to 250 VPN tunnels	Extended firewall functions, PCIE-PC card	FL MGuard 4102 PCIE	1357842
				Extended firewall functions, PCI-PC card	FL MGuard 4102 PCI	1441187
	5 x RJ45	10/100/1000 Mbps	Up to 2 VPN tunnels	4-port unmanaged switch	FL MGuard 2105	1357850
			Up to 250 VPN tunnels	Advanced firewall functions, DMZ port, 3-port managed switch, DNV approval	FL MGuard 4305	1357875

mGuard security routers

Further information on the individual functions and benefits of the mGuard security routers:

[phoenixcontact.com/
security-router-mguard](https://phoenixcontact.com/security-router-mguard)



mGuard brochure for downloading

If you would like detailed information on our mGuard security routers, you can download the brochure here:

phoenixcontact.com/mGuard_brochure

