

Industrial cyber security

Standardized and future-proof

PHOENIX CONTACT
INSPIRING INNOVATIONS

Industrial cyber security
Trust is the foundation

We are living in an age where the development of communication technologies is enabling millions of devices to exchange information on a global scale. Hence the need for a strategy to deal with network security and system availability. Phoenix Contact therefore develops solutions to protect your company's systems and to safeguard the know-how and all sensitive data sets that make up business or production processes.



More information on this topic

There are many reasons why cyber security is an important topic. This brochure is intended to provide you with a basic overview of the topic and illustrate solutions.

Up-to-date information on cyber security can always be found at:
https://phoe.co/cyber-security
You can also find many helpful videos on our YouTube channel:
https://phoe.co/youtube

Scan the QR code and find out more about industrial cyber security

Leave your worries behind

We provide all the tools you need to ensure the security of your machines and systems. Create your own individual "all-around carefree package" of products, services, and solutions.



Contents

Cyber security – Relevant in every industry 4

What could happen? Possible consequences of a security incident 6

360° security Our standard of quality 8

Typical security risks and solutions 10

Our objective: Establishing IT security 14
- Products 15
- Services 16
- Solutions 17

Complete the security check 18

Cyber security – Relevant in every industry

Whether manufacturers or operators, industry or critical infrastructure – cyber security concerns us all. Industrial control systems (ICS) are increasingly exposed to cyber attacks and unintentional changes due to the growing networking of these systems and their connection to the Internet.

ICS security is therefore becoming increasingly important.





Machine manufacturers

Security increases the reliability and availability of your machines. A secure remote connection is also required to conduct remote maintenance at the customer's site.



System operators

Security not only ensures the availability and reliable running of your systems and processes, but also safeguards your production know-how.



Automotive industry

The availability of your systems is your most important asset. Security mechanisms ensure and in some cases even increase the availability of your production lines.



Energy industry

Companies in the energy industry play an important role in supplying people with basic services. This is why in many countries the operators of systems within this critical infrastructure are required by law to protect their systems against unauthorized access.



Water/wastewater

Your primary concern is to ensure the continuous supply of drinking water and treatment of wastewater. Security ensures your remote access to far-flung pumping stations and lifting stations, and protects your automation systems from increasing Internet cyber attacks.



Oil and gas

Particularly in explosive and highly flammable areas, security is now regarded as a safety requirement. This is because a hacked system can quickly become not only a financial risk, but also a safety risk to your employees.

What could happen?
Possible consequences of a security incident

Companies can only succeed if their production systems operate securely and without errors. Failures, sabotage or data loss can cause substantial economic damage. This is because downtimes represent not only a financial loss, but also jeopardize delivery deadlines and consequently your reputation. In a site and process analysis, you can assess the relative risks of your industrial system and its interaction with the plant information system.



Loss of know-how

A competitor can access your sensitive production data. Are you able to quantify the economic damage?

Data loss

All business-critical data is suddenly lost. How much work and money would it take to reconstruct this data?

System downtime

Production has to be stopped for a few hours or days due to security problems. How much would this loss of production cost you?

What has already happened

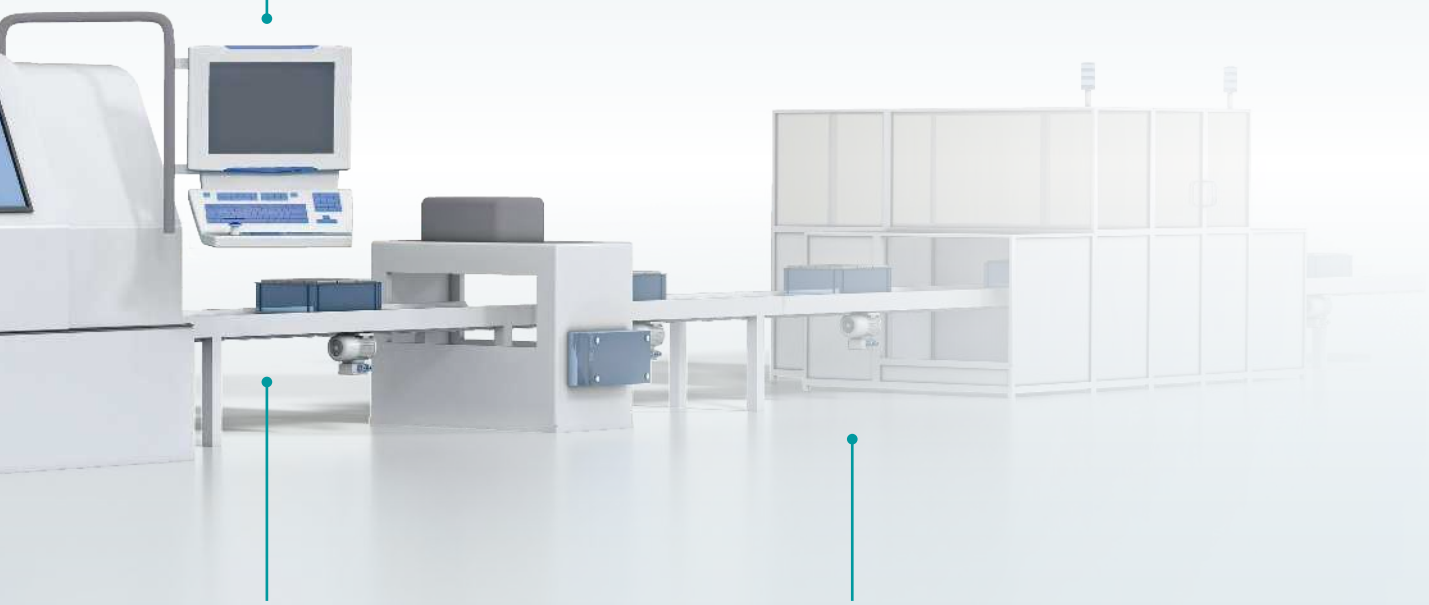
The list of security incidents in industry is growing longer all the time: it began with the “Stuxnet” malware that specifically targeted SCADA systems, this was followed by the “Industroyer” virus (2016) and the targeted “TRITON” attack (2017) on safety controllers, and most recently the “WannaCry” ransomware attack (2017) that affected over 230,000 systems worldwide.

Our social media channels and newsletter keep you up to date with all the latest information on security topics.



Reputation

What would happen if partners and customers called into question your reputation in relation to the reliability and security of your company's data?



Extortion with ransomware

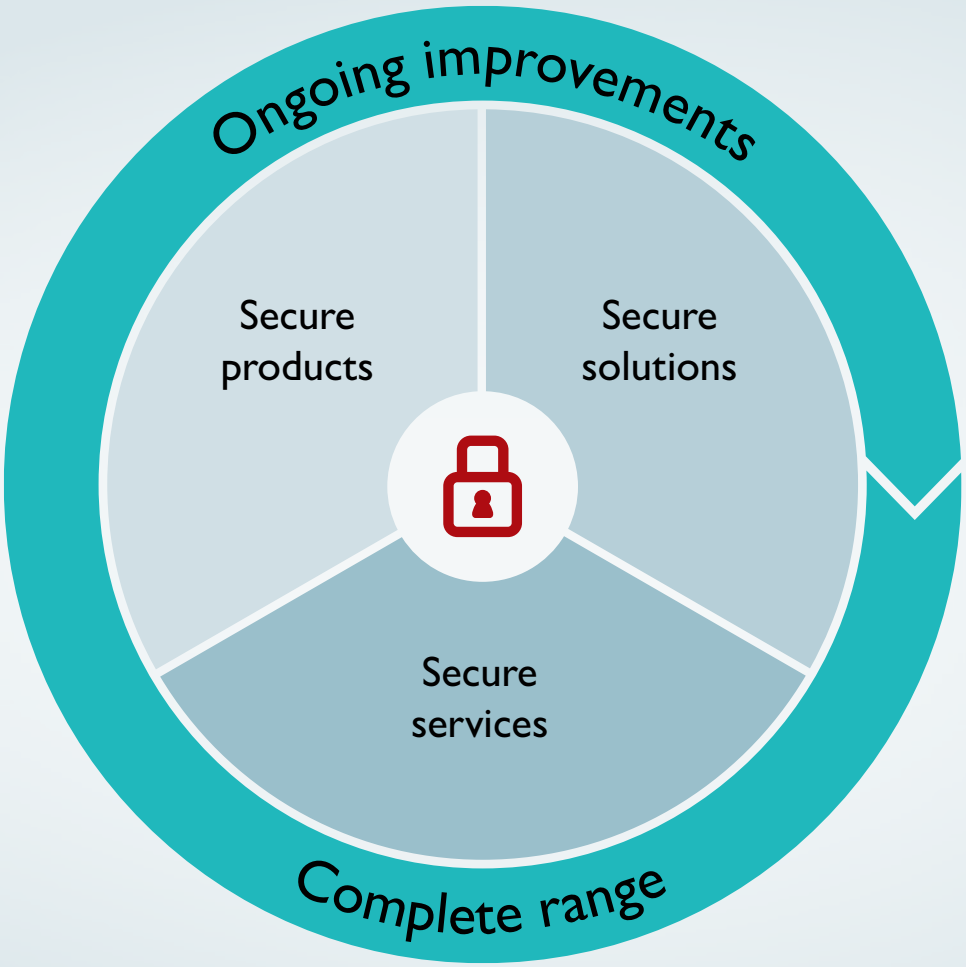
A total blockade of production and files. How much would it cost to pay the ransom in order to reactivate the production process?

Personnel costs

How many hours of work would it take for employees to repair the damage caused by inadequate security measures?

360° security
Our standard of quality

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



Complete range for all-around carefree security



Your data is safe with us

We are experts when it comes to security, so we can assure you that your data will always be treated confidentially by us. Phoenix Contact maintains an information security management system (ISMS) that sets out specifications for the handling of sensitive data and information in accordance with the requirements of ISO/IEC 27001, for example.



Secure products

Phoenix Contact operates a secure development process. Security measures are implemented, verified, and documented based on a threat analysis. Furthermore, our products feature various security functions such as encrypted communication or firewall functions. In addition, we run regular checks to identify any security vulnerabilities and provide security updates.



Secure services

Security cannot be achieved successfully unless security mechanisms are implemented correctly and each individual employee is mindful of security. Phoenix Contact therefore offers various services to support you: from assessing your individual security level and providing advice on how to improve your security to training your staff. All services conform to the highest security standards. Whatever the issue, you are in safe hands with us.



Secure solutions

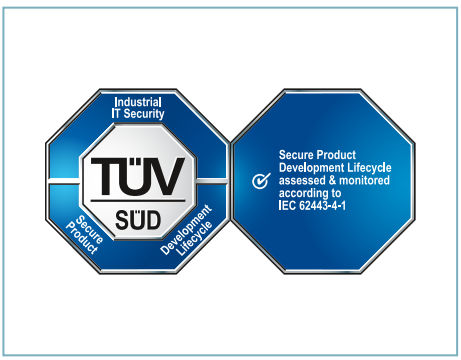
Phoenix Contact combines secure products and services with comprehensive solutions and security architectures. In addition to secure products, we can therefore also provide you with secure automation solutions for a wide range of requirements and industries.



Ongoing improvements

Our Product Security Incident Response Team (PSIRT) gathers and analyzes potential security vulnerabilities in our products and processes on an ongoing basis. If a security vulnerability is identified, we are therefore able to quickly eliminate it and guarantee maximum security for you.

All announcements can be found at:
https://phoe.co/PSIRT



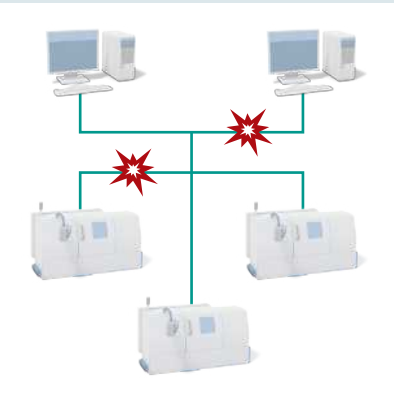
Certified security

Phoenix Contact was one of the first companies to be certified by TÜV SÜD in accordance with IEC 62443 Part 4-1:2018 Edition 1.0. This confirms that our development of security by design products is based on a secure development process. We are also certified in accordance with Part 2-4 of the standard as a provider for the design of secure automation solutions. Furthermore, we are constantly working on other certifications for our security portfolio.

Typical security risks and solutions

Risk: Malfunctions from the office

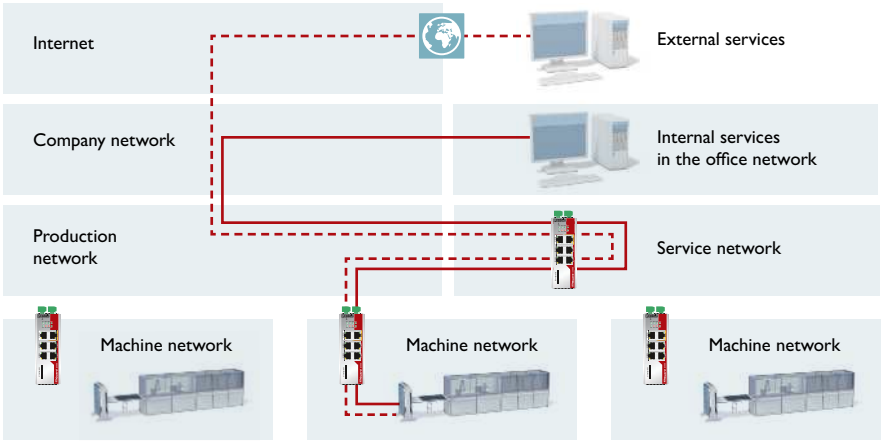
Malfunctions and viruses, e.g., from the office environment, can be transferred directly to the production area.



Solution: Network segmentation

By splitting large networks into small segments, data exchange between the various zones, e.g., between production and the office or between different system parts, can be controlled. The individual segments can be separated using VLANs or firewalls. Routers or Layer 3 switches then need to be used for communication between the individual network segments.

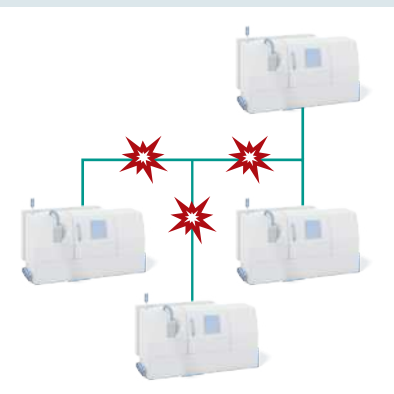
These devices intercept typical network errors, preventing them from spreading further to the rest of the network.



Network segmentation with mGuard security routers

Risk: Malware attack

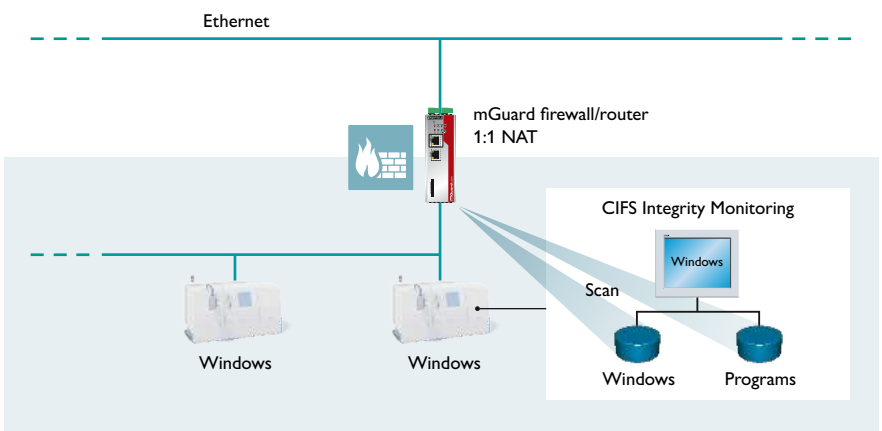
Malware is generally designed to spread to neighboring systems and infect them as well. One example of this is the WannaCry malware that infected unpatched Windows systems.



Solution: Restricting communication

The spread of malware can be restricted or prevented by using firewalls. If you were to eliminate all of the communication options that are not technically necessary, many of these attacks would not even be possible.

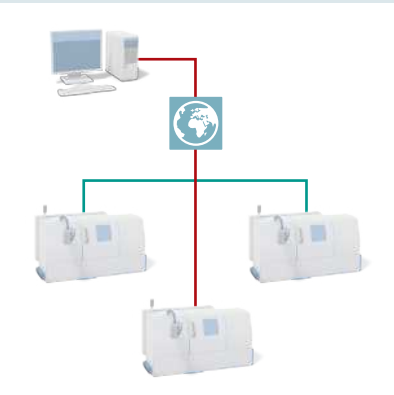
In addition, industrial integrity monitoring (e.g., CIM) helps you detect and halt the impact of changes and manipulations to Windows-based systems, such as controllers, operator interfaces or PCs, in good time.



CIFS Integrity Monitoring

Risk: Hacker attacks

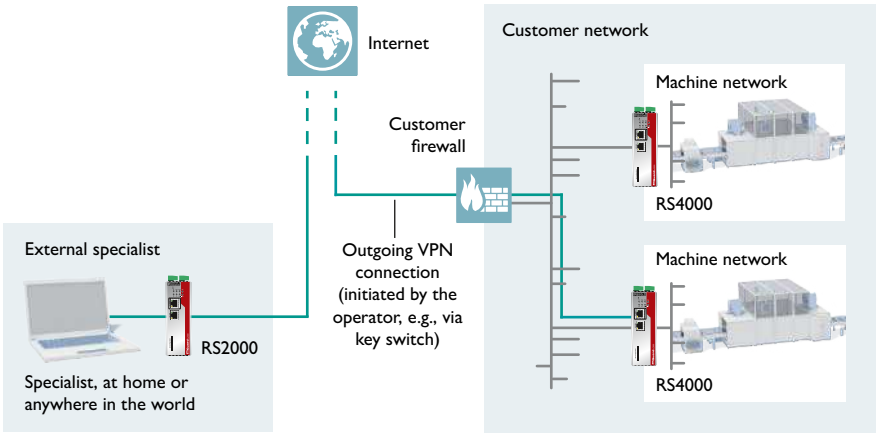
Criminals can copy data or make changes to the system via an open Internet connection.



Solution: Encrypted data transmission

It should not be possible to access automation systems from the Internet. This is achieved by using a firewall for Internet access, which restricts all incoming traffic as well as the outgoing traffic to the requisite, authorized connections.

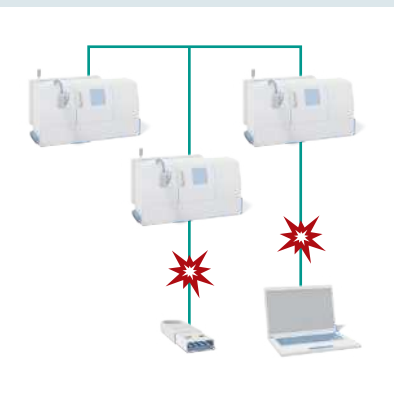
All wide area connections should be encrypted, e.g., by VPN with IPsec.



Secure remote maintenance with encrypted data transmission

Risk: Infected hardware

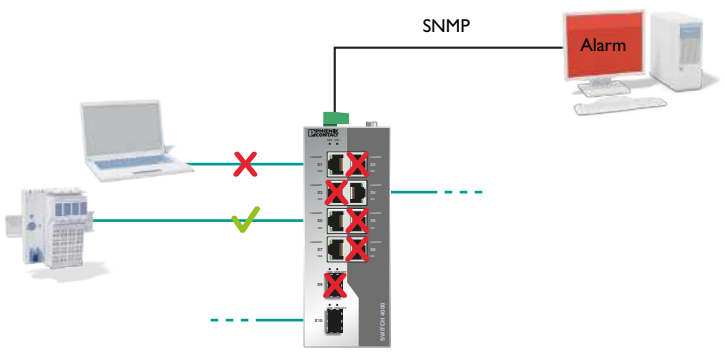
Infected hardware, like USB sticks or laptops, can transfer malware to the network.



Solution: Protect ports

Using the port security function, you can make settings directly on your network components preventing unknown devices from exchanging data with the network. Furthermore, any available ports that are not required should be switched off.

Some components also offer the option of sending alerts via SNMP and signal contact if unauthorized access to the network is registered.

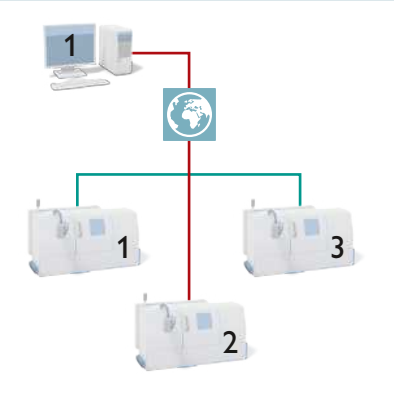


Port disconnection and alerts via SNMP

Typical security risks and solutions

Risk: Unauthorized access to systems

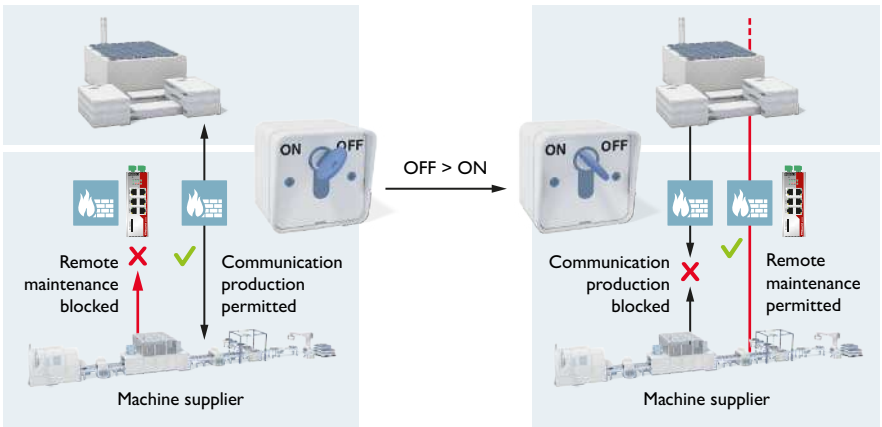
Changes are inadvertently made to the wrong system from a remote location.



Solution: Secure remote access

Secure remote access to one or more machines can be implemented using different technological solutions. Firstly, outbound communication can be encrypted, e.g., via IPsec or OpenVPN. Secondly, remote maintenance can be initiated via a key switch on the machine.

This ensures that only intended changes are made to the machine. At the same time, the key switch also enables the communication rules in the network to be blocked while remote maintenance is being carried out.



Control of remote maintenance using a key switch

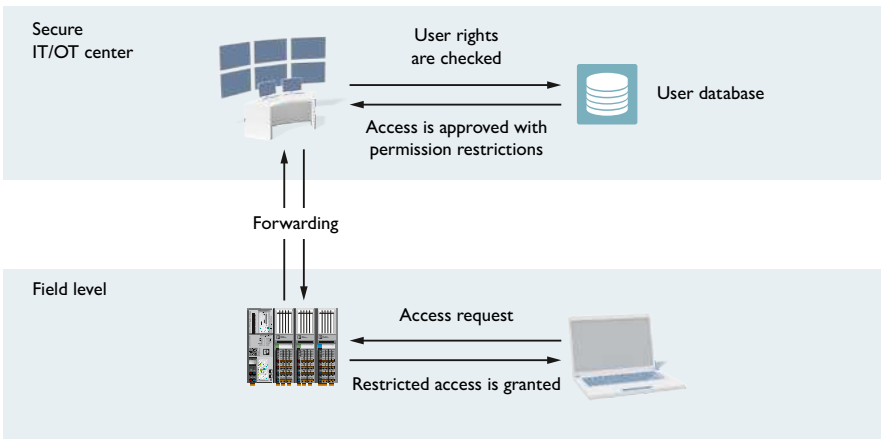
Risk: Inadequate user management

Collective passwords are often used for user access. When employees leave the company, passwords are not changed or access is not blocked. The collective password is therefore known to many users and can be abused.



Solution: Central user management

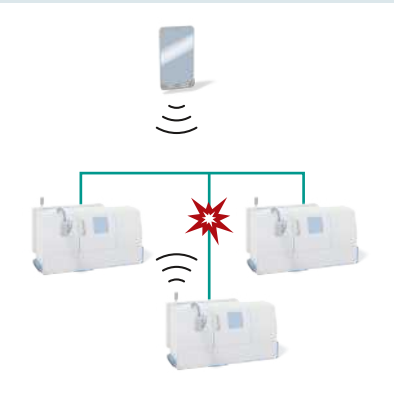
This problem can be solved by central user management where each employee is assigned individual access rights. Many Phoenix Contact devices support integration into a central user management system.



Central user management with individual assignment of rights

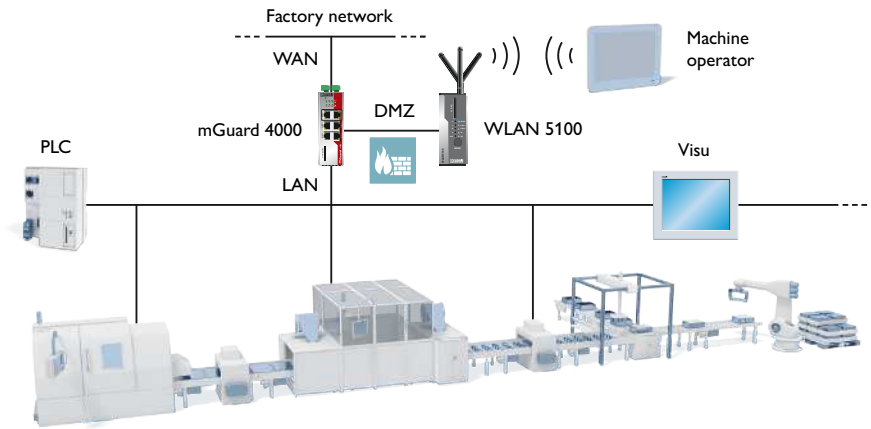
Risk: Mobile end devices

Unauthorized smart devices connect themselves via the WLAN interface.



Solution: Secure WLAN password assignment

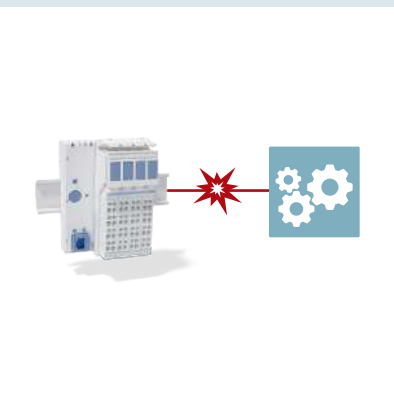
If WLAN passwords are known and have not been changed in a long time, this also affords third parties uncontrolled access to the machine network. WLAN components from Phoenix Contact therefore enable automated key management by the machine control system. This means that secure WLAN machine access can be easily implemented in the form of one-time passwords. In addition, WLAN communication can be protected and isolated from the rest of the network using a demilitarized zone (DMZ).



Secure integration of mobile end devices with one-time passwords and DMZ

Risk: Unsecure or incorrect device configuration

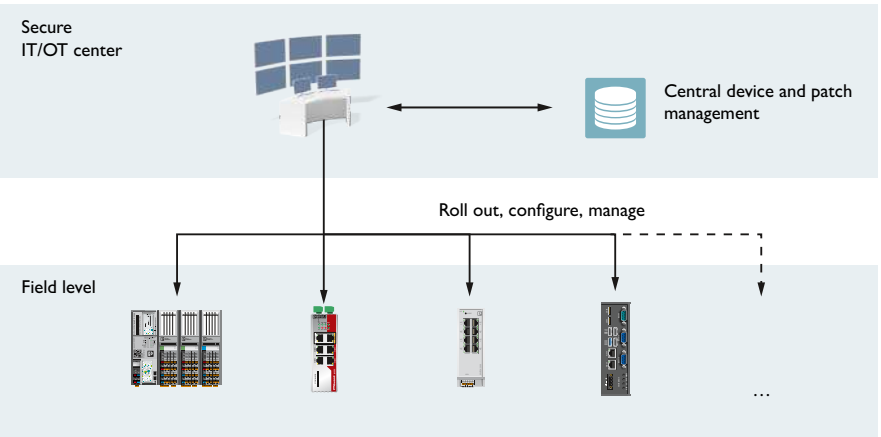
The default configurations of devices are designed so that the components function correctly and can be easily started up. Security mechanisms are often a secondary consideration here.



Solution: Device and patch management

When it comes to managing multiple devices, intelligent and efficient device and patch management can automate time-consuming processes and reduce the risk of incorrect configuration. It provides support for the configuration, roll out, and management of devices, and reduces security and compliance risks thanks to shorter patch and upgrade cycles.

Device and patch management enables the central creation and management of all security-related device settings and provides support for firmware upgrades.



Central patch and device management

Our objective: Establishing IT security

Long-term organizational and technical measures that are geared toward the life cycle of your system minimize the risk of possible attacks. To help you achieve maximum possible stability and transparency for your infrastructure, we support you in selecting the appropriate and necessary hardware, devising individual protection concepts, and implementing practical training.

We combine our experience, products, and services to create comprehensive industry solutions on request.



Products

Secure from development right through to patch management

The integration of security is an integral component of our product development. This starts with a secure development process.

In addition, many of our products offer security functions, such as secure user authentication, network segmentation, network monitoring, and firewall functions or the use of secure and encrypted communication protocols. Furthermore, throughout their life cycle, our products are subject to vulnerability management (PSIRT) where security patches and updates are provided for any security vulnerabilities that are identified.



mGuard security
mGuard security routers form the central security backbone of your system. They offer special firewall functions for industry, such as conditional firewall and user firewall, deep packet inspection for industrial protocols, and secure network access for service technicians. In addition, the mGuard Secure Cloud provides you with a system for easy, secure remote maintenance.



PLCnext Security
The PLCnext Control devices have been designed in line with security by design criteria. The development processes are certified in accordance with IEC 62443-4-1. Some of the key security measures include the use of a Trusted Platform Module (TPM), a configurable Linux kernel, and the Linux firewall, plus the implementation of a crypto store for certificates and keys.

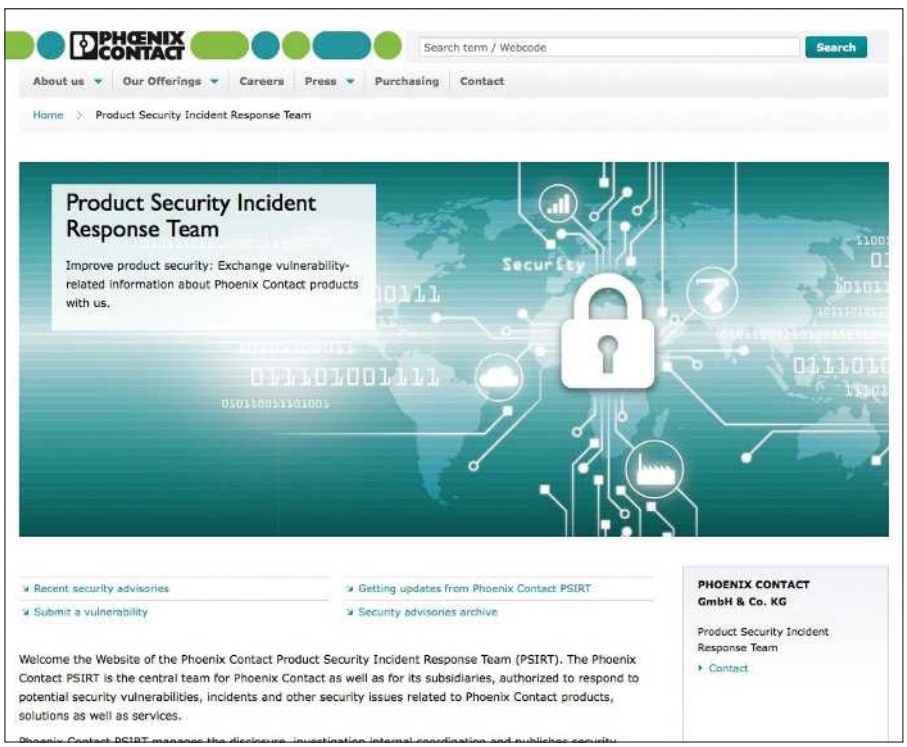
Vulnerability management: PSIRT

To ensure your optimum security at all times, Phoenix Contact has established a Product Security Incident Response Team (PSIRT). The Team:

- Responds to potential security vulnerabilities, incidents, and other security issues related to Phoenix Contact products, solutions, and services
- Manages the disclosure, investigation, and internal coordination of security advisories
- Publishes security advisories for confirmed vulnerabilities where measures for mitigation or fixes are available.

All current and past security advisories are communicated transparently on our website:

https://phoenixcontact.com/psirt



Subscribe to the PSIRT newsletter and report security vulnerabilities

Services

Evaluation and planning

Based on industry standards, we develop individual solutions and concepts:
- For failsafe network structures
- For the protection or remote maintenance of your machine
- For high-performance wireless networks

Together, we inspect your system and analyze your individual threat and risk situation, documentation, and processes.

Result:
You will receive a detailed report of vulnerabilities, recommended actions, and a list of measures required in order to provide standard protection for your system in compliance with IT baseline protection.



Implementation

So that you can continue to focus on your actual core competencies, we implement your security and network requirements for you:
- Configuration and documentation
- Introduction of management systems
- Detection and elimination of anomalies
- Network maintenance
- Testing systems that have been started up

Result:
The communication relationships in your network will be optimized, thereby increasing network performance and availability.



Maintenance and support

To ensure the availability of your system, updates must be installed on a regular basis, the firewall rules adapted, and messages evaluated.
We provide support for:
- Debugging (e.g., incorrect device configuration)
- Detecting anomalies
- On-site troubleshooting
- Individual product support

Result:
There is little administrative effort for you as a user, and you also satisfy the burden of proof for implementing measures in accordance with state-of-the-art technology.



Seminars

Information security concerns all employees in your company.
We offer the following:
- Basic training on security
- Security awareness training
- Basic training on Ethernet
- Product training
- Individual practical training that is tailored to your specific requirements

Result:
Security-conscious and responsible actions can be taken to avoid failures and damage to your systems, thereby contributing to the success of the company.



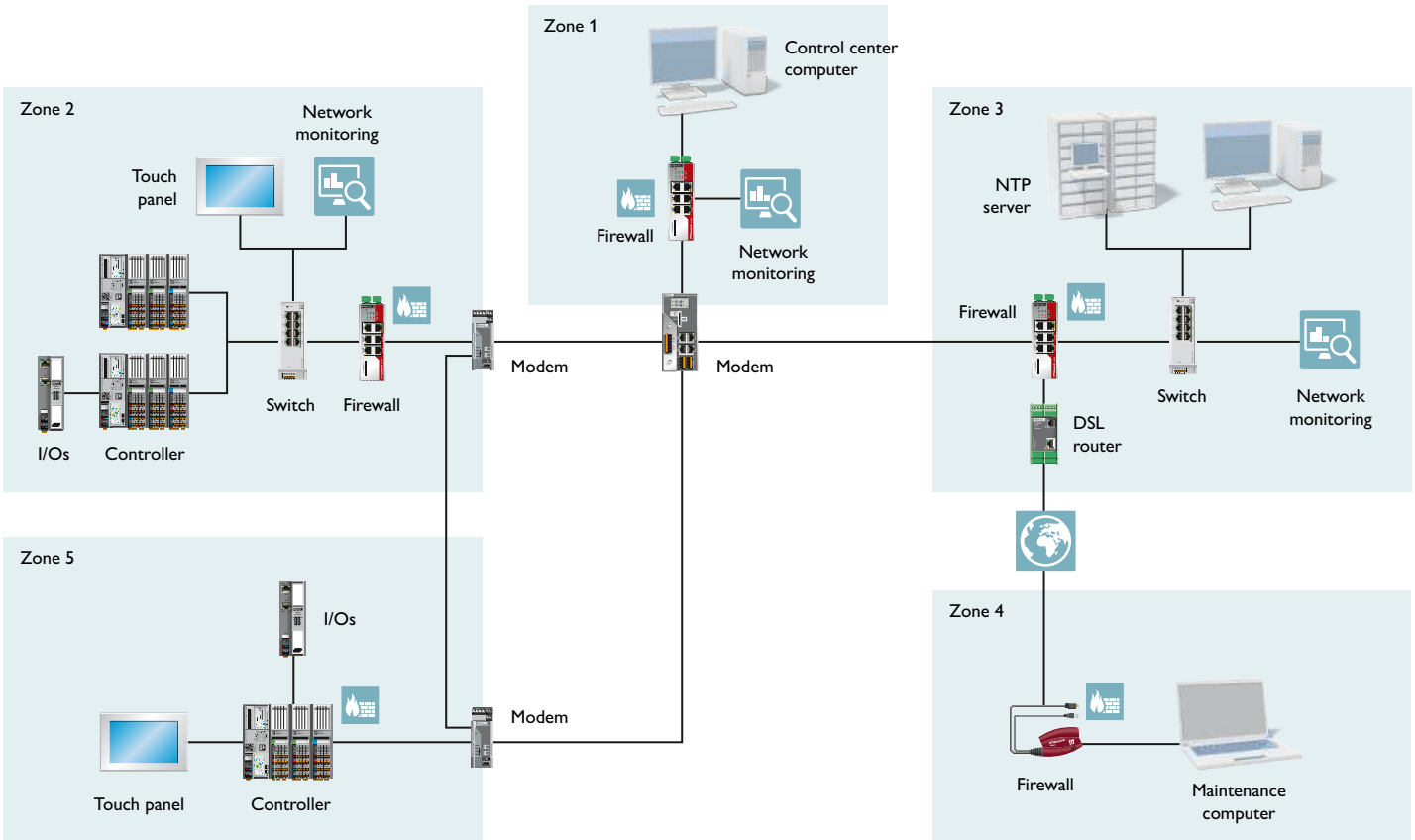
Solutions

Secure automation solutions

Phoenix Contact has the capabilities to develop and start up secure automation solutions in accordance with international standard IEC 62443-2-4.
We develop secure automation solutions within the scope of a protection requirements analysis and the following protection objectives: confidentiality, integrity, and availability. Our services also include a threat analysis and a security risk analysis.

At Phoenix Contact, security by design means:

- Determining the protection requirements
- Performing a threat/risk analysis
- Developing a secure network concept, with zones and conduits, in accordance with IEC 62443
- Selecting secure automation products
- Documentation and startup of the system
- System support services (e.g., patch management) throughout the life cycle of the system



Standardized data security:

Phoenix Contact maintains an information security management system (ISMS) established in accordance with the requirements of ISO/IEC 27001, for example. Among other things, the ISMS sets out specifications for the handling of sensitive data and information: from IT security and handling sensitive data and customer data through to network security.

Furthermore, Phoenix Contact Energy Automation GmbH is the first company in the Phoenix Contact Group to have been awarded ISO/IEC 27001 certification.



Complete the security check

Where do you stand when it comes to security? This checklist is intended to help you get an initial overview of the state of security in your system.

We will also be happy to provide you with the full "Quick Check" for industrial cyber security by e-mail or arrange a personal consultation on site with a detailed actual state analysis.



Checklist

Requirements	Yes	No	Notes
Have all internal and external staff signed a non-disclosure agreement?	☐	☐	
Has it been established which access rights have been assigned to which individuals within the scope of their roles?	☐	☐	
Are passwords personalized and changed on a regular basis?	☐	☐	
Do you provide employees with regular training on information security and raise awareness of this topic?	☐	☐	
Is the personal use of business hardware and software prohibited?	☐	☐	
Is the integration of portable data carriers (USB sticks, USB hard drives, etc.) in IT or automation systems documented in and regulated by guidelines?	☐	☐	
Are your networks segmented?	☐	☐	
Have you set up firewalls that filter data communication in the network and control access rights?	☐	☐	
Is remote maintenance access disabled in normal operation and only enabled on a case-by-case basis? Is this requirement documented?	☐	☐	
Is outbound communication encrypted, e.g., via a VPN tunnel?	☐	☐	
Are your systems regularly checked for vulnerabilities and updated?	☐	☐	
Do employees know what to do in the event of a security incident? Are there guidelines on this that describe how correct operation can be restored after a severe disruption?	☐	☐	

If you answered no to one or more of these questions, get in touch with Phoenix Contact.
We will be happy to advise you and support you with the appropriate consulting services and products.

In dialog with customers and partners worldwide

Phoenix Contact is a globally present, Germany-based market leader. Our group is synonym for future-oriented components, systems, and solutions in the fields of electrical engineering, electronics, and automation. A global network across more than 100 countries, and 17,400 employees ensure a close proximity to our customers, which we believe is particularly important.

The wide variety of our innovative products makes it easy for our customers to find future-oriented solutions for different applications and industries. We especially focus on the fields of energy, infrastructure, process and factory automation.



You will find our complete product range at:

phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 52 35 3-00
Fax: +49 52 35 3-4 12 00
E-mail: info@phoenixcontact.com
phoenixcontact.com

Printed in Germany
© PHOENIX CONTACT 2019

AI 05-19.000.L3
MNR 1101729/2019-03-15/00

PHOENIX CONTACT
INSPIRING INNOVATIONS