Defense in depth

To provide industrial plants with comprehensive protection from internal and external cyber-attacks, all levels must be addressed: control rooms, control systems, distributed automation, and communication networks. Comprehensive, state-of-the-art security concepts are significantly more cost-effective and lead to higher plant availability. The primary objective is to prevent damage to people, companies, and infrastructures. The holistic industrial security concept must be based on IEC 62443 recommendations, the leading international standard for security in industrial automation. The concept comprises specific network security aspects which have already proven to disturb and limit market development, in network security.

- Authorization goes to network operators specific customized access through network access protectors, network segmentation, and an integrated system management. Without protection, the cyber-attack chain is completely untroubled. The holistic concept provides a comprehensive approach to both network and system security.
- As a complement to integrated solutions for the management and administration of networked environments, software components are available for physical network protection, such as the IEC 62443-3-3. The SCALANCE TAP104 supports the export of data traffic for advanced protection and communication networks in the energy sector and other industrial applications. The SCALANCE TAP104 manages data traffic and network parameters for physical network protection, such as the IEC 62443-3-3. The SCALANCE TAP104 supports the export of data traffic for advanced network protection, such as the IEC 62443-3-3.

- The robust RUGGEDCOM security routers and communication process processors are available for your systems.

With Siemens Industrial Security Services you benefit from the comprehensive know-how and technical expertise of a global network of automation and cybersecurity specialists. The holistic scheme for reliable protection of industrial plants includes a wide variety of Siemens products and solutions, such as SCALANCE S Industrial Security Appliances, SCALANCE M Industrial Security Appliances, RUGGEDCOM security routers, and RUGGEDCOM security communications processors. The robust RUGGEDCOM security routers and communication process processors are available for your systems.

"Charter of Trust" for a secure digital world

"We can’t expect people to support the digital transformation if the security of their data and networked systems is not guaranteed. We, at Siemens, believe that every company owner is committed to sign the "Charter of Trust" - a charter aimed at three important objectives:

Want to find out how secure your industrial plant is, or what further security measures are available for your systems?

Find out more about the key principles and our partners: www.charter-of-trust.com

© Siemens 2020
Software for control and transparent management of network accesses and accessories

Access control

Industrial Security Communications Processors (CPs) for remote SIMATIC controllers and IPCs

4) For use in North America

3) For further information on tested software applications, please contact your local Siemens partner

2) Suitable accessories and details can be found on the Internet at:

© Siemens 2020

Industrial Security ordering overview – Components for network security and access control

Network Security and Access Control

Ethernet

LTE (4G)
UMTS (3G)
GSM (2G)
Ethernet
wireless
GSM (2G)
Ethernet
wireless
LTE (4G)
UMTS (3G)

Industrial Security Communications Processors (CPs) for remote SIMATIC controllers and IPCs

Software for control and transparent management of network accesses and accessories

Access control

4) For use in North America

3) For further information on tested software applications, please contact your local Siemens partner

2) Suitable accessories and details can be found on the Internet at:

© Siemens 2020

Industrial Security ordering overview – Components for network security and access control

Network Security and Access Control

Ethernet

LTE (4G)
UMTS (3G)
GSM (2G)
Ethernet
wireless
GSM (2G)
Ethernet
wireless
LTE (4G)
UMTS (3G)

Industrial Security Communications Processors (CPs) for remote SIMATIC controllers and IPCs

Software for control and transparent management of network accesses and accessories

Access control

4) For use in North America

3) For further information on tested software applications, please contact your local Siemens partner

2) Suitable accessories and details can be found on the Internet at:

© Siemens 2020

Industrial Security ordering overview – Components for network security and access control

Network Security and Access Control

Ethernet

LTE (4G)
UMTS (3G)
GSM (2G)
Ethernet
wireless
GSM (2G)
Ethernet
wireless
LTE (4G)
UMTS (3G)