RUGGEDCOM CYBERSECURITY SOLUTIONS

The security **to be free**

usa.siemens.com/ruggedcom-cybersecurity

SIEMENS

Cybersecurity for your critical infrastructure

With billions of Internet-of-Things (IoT) devices worldwide, cybersecurity is crucial to the success of the digital economy. Industrial Control Systems (ICS), especially those pertaining to critical infrastructure, require a holistic cybersecurity approach to ensure business continuity while protecting people, assets and intellectual property. Look to Siemens as your trusted partner for a cybersecurity solution tailored to your requirements using the right blend of operational technology (OT) network expertise, tested software, and rugged hardware.

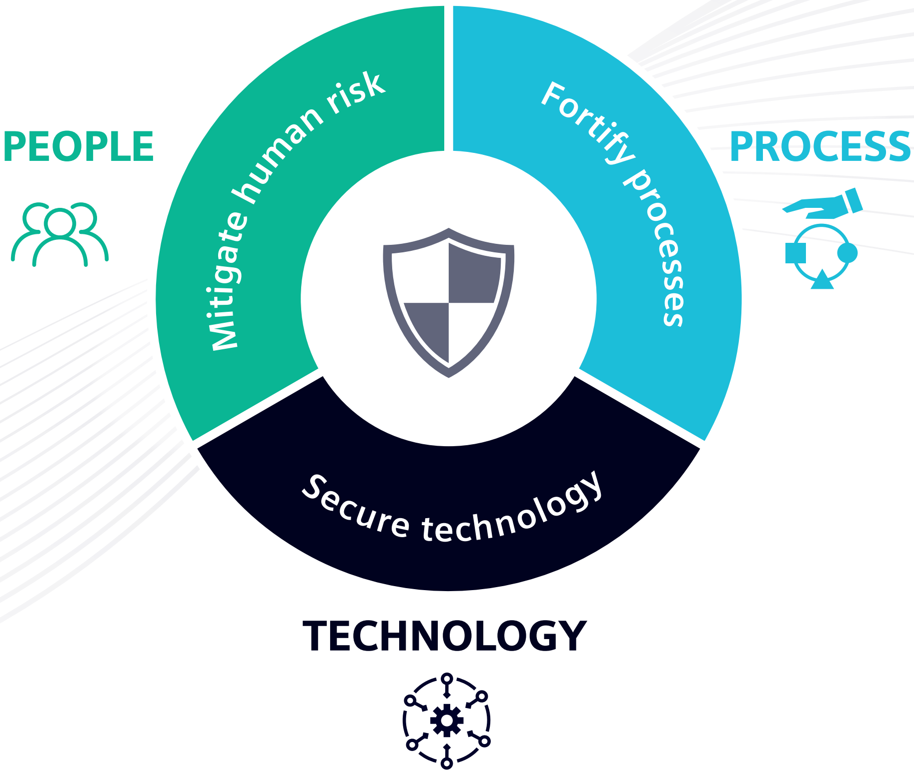
Defense in Depth

The benefits of interconnected operations also bring potential threats from web-based hackers, which can cause downtime and disruption. Threats from malware, external attacks or a vulnerable point in a network can also grind operations to a halt. In many countries, regulatory bodies often require the full disclosure of security breaches to ensure stakeholders are notified when personal and confidential industry information is compromised.

> **Critical infrastructure:** OT/IT infrastructures in operation (including assets, systems, solutions and services) which are essential for the maintenance of vital societal functions.

Siemens recommends “Defense in Depth” – a multilayer security concept for OT networks outlined in the international IEC 62443 standard. It is aimed at OT network operators, system integrators and component manufacturers.

“Defense in Depth” is a holistic approach with plant security, network security and system integrity that brings **people, processes** and **technology** together to achieve cybersecurity goals.



PEOPLE must be trained to be aware of and resistant to human vulnerabilities such as social engineering. They must follow appropriate policies and procedures when accessing secure systems.

PROCESS involves identifying and assessing the vulnerability of hardware and software assets, and prioritizing the protection of mission-critical assets. Given the inevitability of cyber intrusions: it is imperative to detect them, mitigate their impact, and swiftly return the network to normal operations.

TECHNOLOGY requires a trusted advisor to ensure that you have the right insights, tools and training to achieve the necessary security capabilities with the appropriate cybersecurity hardware and software.

The state of industrial cybersecurity

More than 330 industrial companies and organizations across the globe were surveyed on the state of industrial cybersecurity, as well as the current priorities and challenges of industrial organizations. Here are the results.

Tech trends forcing revised industrial cybersecurity practices

55%
Industrial IoT

55%
Cloud and SaaS

36%
Edge computing

33%
5G

Ongoing digitalization

44%

are working on cybersecurity initiatives for digital OT transformation

Prioritizing sustainable development

44%

have or plan to reintroduce environment-related roles such as a Chief Sustainability Officer

98%

believe this role will elevate cybersecurity within their company

SOURCE: ARC ADVISORY GROUP AND KASPERSKY LABS, THE STATE OF INDUSTRIAL CYBERSECURITY IN THE ERA OF DIGITALIZATION, 2020

A global leader in cybersecurity

As a founding member of the Charter of Trust, Siemens is a leader in advancing global cybersecurity. Signed in Munich with partners worldwide, the Charter calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

With a complete portfolio of state-of-the-art products, systems and services that protect customer data and equipment, Siemens is a reliable and preferred partner for companies that strive for the highest cybersecurity standards.

Gain a trusted partner with Professional Services from Siemens

Achieve your cybersecurity goals with the help of Professional Services for Industrial Networks. From assessment, pre-configuration and testing services to implementation and the support you need to self-manage your cybersecurity program, we have you covered.

ASSESS

Siemens professionals start by assessing the risk to your industrial control system. This stage includes:

- *Discovering and analyzing your assets, network architecture and processes*
- *Conducting a network vulnerability assessment*
- *Providing a security assessment report with recommendations*

IMPLEMENT

We will then help implement a robust cybersecurity program based on the assessment by:

- *Building a secure-by-design network*
- *Creating an implementation roadmap*
- *Supporting on-site mplementation*

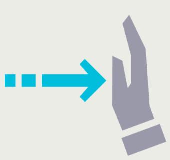
MANAGE

Finally, we will help you self-manage your cybersecurity program by:

- *Training your security personnel*
- *Ensuring continuous threat monitoring and keeping your installed software and signatures up to date*
- *Evolving a framework for incident response and recovery*

RUGGEDCOM **cybersecurity solutions**

Considering industry- and region-specific preferences to cybersecurity, Siemens has created an ecosystem of comprehensive and reliable solutions customized to customers' needs. Siemens offers cybersecurity solutions installed on the RUGGEDCOM Multi-Service Platform product family of cost-efficient Layer 2 and Layer 3 devices – ideal for mission-critical applications in harsh environments. Together with comprehensive network consulting services, on-site support, security assessments, integration, deployment and training: RUGGEDCOM cybersecurity solutions offer complete peace of mind when it comes to security.



Stateful Inspection Firewall
Filters traffic between different zones of trust within networks. Includes Network Address Translation (NAT) to prevent unauthorized or malicious activity initiated by outside hosts from reaching the internal Local Area Network (LAN).

Virtual Private Networking (VPN)
Provides secure communication links over networks. Ensures confidentiality, sender authentication and message integrity. It also uses IPsec (IP security) for encryption and authentication of all IP packets at the network layer.

Strong Encryption
Utilizes the latest encryption algorithms for authorization, authentication and privacy. Examples include TLS and SSH at upper protocol levels, RSA and ECC for public-key encryption, and 3DES and AES for stream encryption.

Rugged hardware for harsh environments

RUGGEDCOM Multi-Service Platform
A family of utility-grade Layer 2 or Layer 3 switches and routers specifically developed to provide multiple electronic defense layers to protect critical assets.
The RUGGEDCOM Multi-Service Platform forms the main point of entry between the local area network (on the plant floor or in a substation) and the Wide Area Network (WAN). It combines Layer 3 routing, firewall and VPN functions onto a single box.

The RUGGEDCOM RX1500 series of modular and field-replaceable Multi-Service Platforms allows customers to select from WAN, cellular, serial, and Ethernet connectivity options. Field-swappable modules guarantee flexibility and easy maintenance for critical applications and are certified for use in harsh environments associated with electric power, transportation, and oil and gas industries.

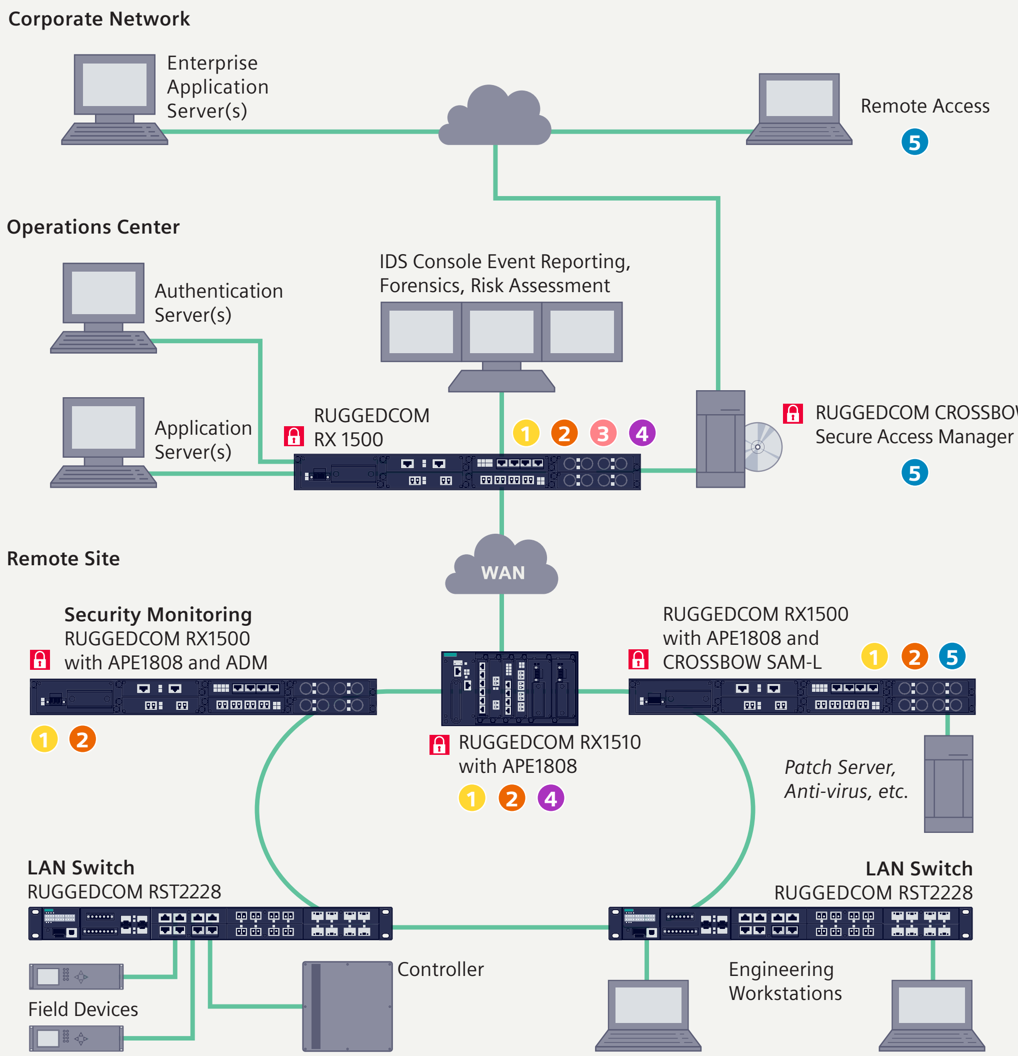
RUGGEDCOM APE1808

RUGGEDCOM RX1500

RUGGEDCOM Application Processing Engine (APE)
A powerful application processing engine based on Intel Quad-core CPU and x86_64 architecture with a Linux or a Windows 10 operating system. It provides a standards-based platform to install commercially available applications such as cyber threat detection and prevention, application-level firewalls, network logging, intrusion sensors, and software for secure access and network management. As a line module for the RUGGEDCOM RX1500 family, it eliminates the need for additional specialized security appliances or external industrial PCs for your OT network.

RUGGEDCOM Layer 2 Ethernet switches
These provide security at the local area network level, including MAC-based port security, RADIUS authentication, SSH/SSL encryption for passwords, VLANs and the ability to enable/disable ports.

RUGGEDCOM cybersecurity solutions installed on the RUGGEDCOM Multi-Service Platform designed for harsh environments and mission-critical applications.



- Industrial Ethernet
- 1 Anomaly-based Intrusion Detection System (IDS)
- 2 Deep Packet Inspection (DPI)
- 3 Intrusion Prevention System (IPS)
- 4 Next Generation Firewall (NGFW)
- 5 RUGGEDCOM CROSSBOW – Secure Access Control

Choose from tested software solutions that are just right for your network

RUGGEDCOM CROSSBOW – Secure Remote Access
An enterprise-level secure access management solution for cyber-security compliance. It assists with NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) and IEC 62443 compliant access to Intelligent Electronic Devices (IEDs), and includes managing, securing and reporting on secure access.

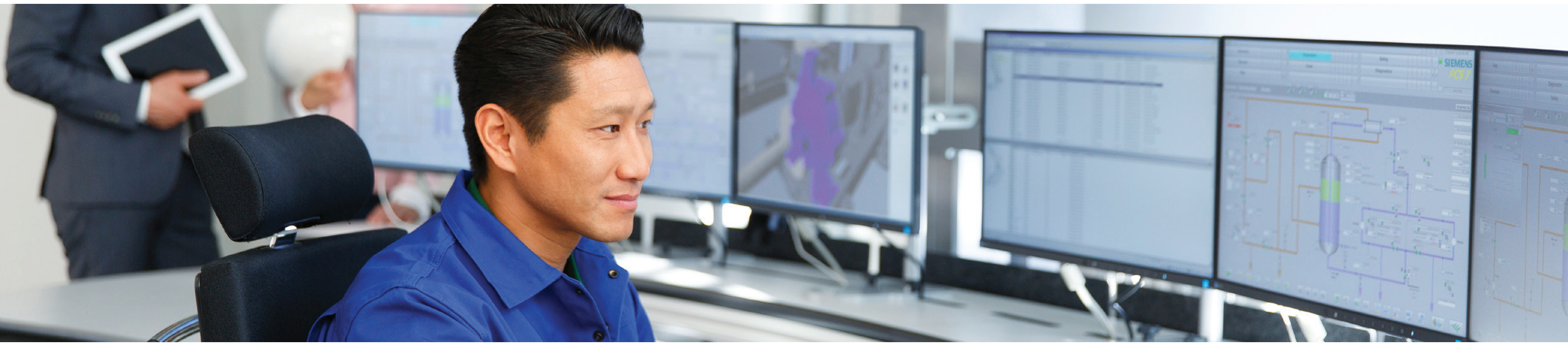
In addition to secure access, CROSSBOW automates device password management, configuration management, firmware version monitoring, remote connectivity verification, and data file retrieval – enhancing productivity for administrators and users alike.

The distributed architecture of CROSSBOW with the Station Access Controller (SAC) server and the Secure Access Manager - Local (SAM-L) ensures local and emergency connectivity to IEDs with the full support of automation functions (SAM-L only), even when there is a loss of communication between the central CROSSBOW server and the remote site.

With administrator-defined Role-Based Access Control (RBAC), CROSSBOW provides activity logging and data privacy as users connect to remote IEDs from the convenience and safety of the control room. Strong two-factor authentication through RSA SecurID, Active Directory and RADIUS ensures process security.

SINEC NMS – for industrial networks
A scalable network management system for the digital enterprise. It offers real-time monitoring, 24/7 visibility of the entire network, and the easy configuration of RUGGEDCOM and SCALANCE devices.

It is equipped with security features for logging, reports security events to a central server or a SIEM (Security Information and Event Management) system, and facilitates policy-based firewall configurations of network devices. SINEC NMS Operations can be deployed on the APE1808 for network management at a remote site with hundreds of network assets.



Global partnerships

Third-party applications from leading cybersecurity companies available on RUGGEDCOM devices provide more options for addressing various cybersecurity challenges.

Anomaly-based Intrusion Detection System (IDS)
Non-intrusive, anomaly-based and signatureless IDS software for mission-critical operational networks, operating on RUGGEDCOM hardware, provides early warning notification and alerts on vulnerabilities and sophisticated cyber threats that may be undetectable by conventional IT security tools.

Next Generation Firewall (NGFW)
The RUGGEDCOM switching and routing platform combined with a NGFW application on a single, integrated appliance provides application-layer visibility into protocols and vulnerabilities specific to OT environments. Designed for maximum throughput without degrading or compromising network performance: NGFWs ensure high availability for converged OT/IT networks.

Deep Packet Inspection (DPI)
DPI functionality for OT protocols like Modbus and DNP3 non-intrusively examines data packets passing through firewalls. It searches for potential non-compliant traffic, viruses, spam and intrusions together with user-defined criteria to determine whether the data packet may pass or should be routed to a different destination for further analysis and mitigation.

Intrusion Prevention System (IPS)
An IPS is a capability available on RUGGEDCOM hardware equipped with an NGFW solution. It is located between the WAN and the LAN to analyze data traffic patterns and deny the traffic representing known threats based on a security profile.

End-to-end cybersecurity solutions

Our full suite of hardware, software and service offerings lets you identify, protect against, detect and manage cyber threats to your ICS to achieve your desired cybersecurity outcomes.

IDENTIFY network strengths and vulnerabilities

Using a risk-based assessment approach, such as the NIST framework or the IEC 62443, our OT professionals will thoroughly analyze your network, identify existing strengths and vulnerabilities, and recommend a cyber risk-mitigation strategy suited to your business objectives. To ensure continued compliance to ever-changing regulations and mitigate risks associated with vulnerabilities in critical infrastructure networks, you can also conduct these assessments annually.

PROTECT your Industrial Control System (ICS)

Effectively protect your industrial control system and maximize network uptime with a "Defense in Depth" approach across all network layers. This includes:

- Secure-by-design rugged hardware that minimizes failures and network downtime
- Network security and asset integrity thanks to strong passwords, data encryption, network segmentation and patch management
- Network entry-point protection assurance with Next Generation Firewalls and Intrusion Prevention Systems to create an electronic security perimeter around your industrial control system.

DETECT threats and anomalies within your ICS

Ensuring threats and anomalies are detected early is critical to preventing the amount of damage they can cause to your critical infrastructure and operations. Effective intrusion detection solutions include an IDS with DPI capabilities. These applications utilize their complete visibility of the entire network, assets and processes to provide real-time, context-based alerts of potential threats conventional IT security tools might not detect.

MANAGE your cybersecurity program

Managing your overall cybersecurity regime, responding to cyber attacks and recovering from a cyber incident requires a coordinated effort throughout the organization addressing people, processes and technology. Our holistic cybersecurity approach supports your entire organization to ensure business continuity and regulatory compliance. So that you can focus on what matters.

Realize the benefits of comprehensive cybersecurity

- Gain peace of mind with a single trusted source for customized cybersecurity hardware, software and services
- Eliminate the need for specialized security appliances with versatile hardware
- Lower your total cost of ownership with verified solutions for legacy as well as modern systems

Published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article No.: DIPA-B10233-00-7600
Order No.: RCBR-CYSEC-0921

Printed in USA
© Siemens 2021

usa.siemens.com/ruggedcom-cybersecurity

This document contains a general description of available technical options only, and its effectiveness will be subject to specific variables including field conditions and project parameters. Siemens does not make representations, warranties, or assurances as to the accuracy or completeness of the content contained herein. Siemens reserves the right to modify the technology and product specifications in its sole discretion without advance notice.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement and continuously maintain a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

siemens.com/industrialsecurity