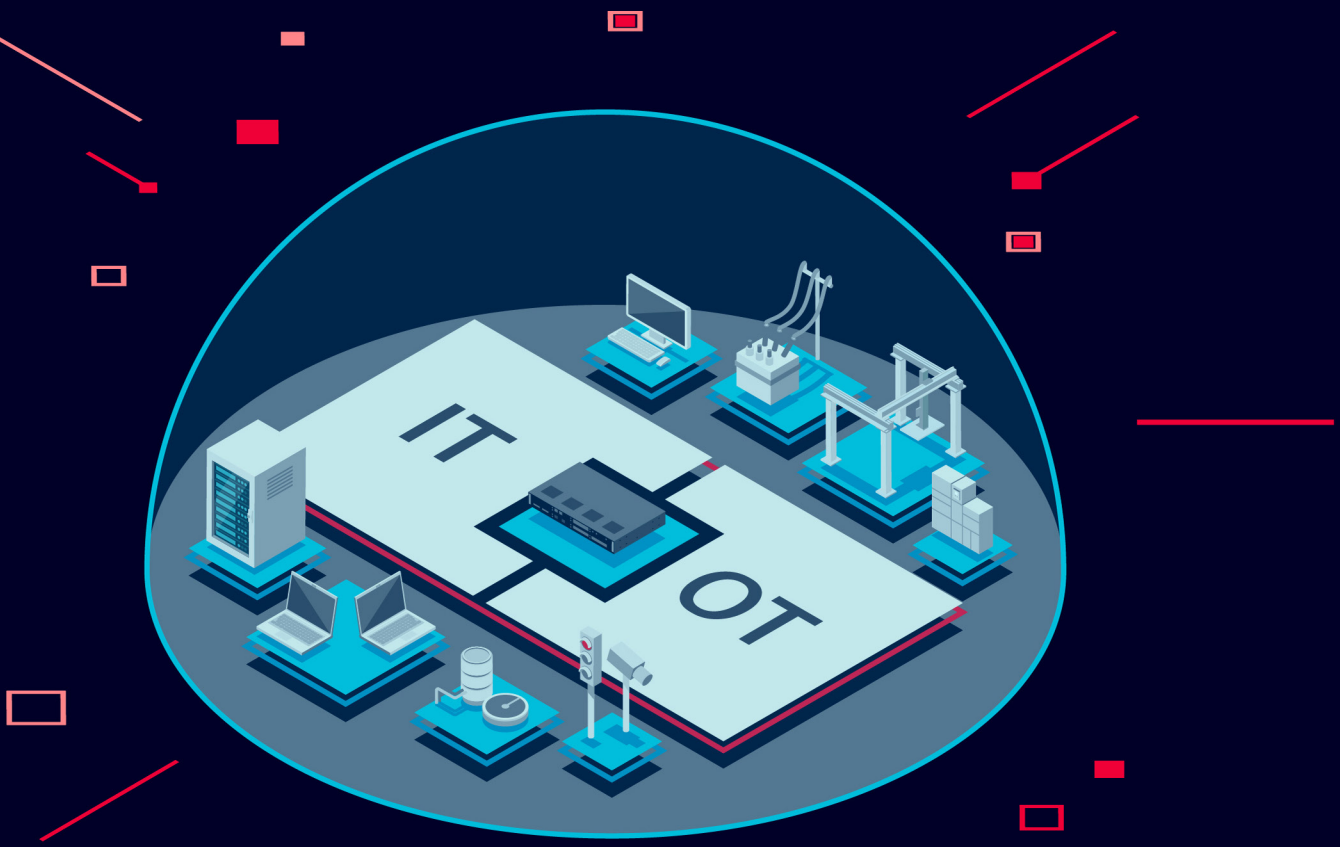


WHITE PAPER

Cybersecurity: What we do at Siemens

Discover the stringent processes and measures that we follow for our Rugged Communications Solutions portfolio to ensure that we deliver products and services that comply with the highest of international cybersecurity standards.

SIEMENS

Introduction

We have established a comprehensive program of technical solutions, services, and processes and combined them with certifications of external governance organizations and market-leading partner solutions. With our rugged communications solutions for industry, i.e., the RUGGEDCOM family, our mission is to deliver peace of mind to customers by providing innovative, secure, and reliable communication solutions for mission critical applications in harsh environments.

Cybersecurity is a top priority for Siemens. We hold ourselves accountable to the highest cybersecurity standards and endeavor to lead by example.

We monitor our own systems with three cyber defense centers and supply secure products and services to customers, e.g., utilities, power grid operators, ITS and rail systems, oil and gas installations, and other critical infrastructure industries.[1]

Our end-to-end supply chain management from the source to the end user utilizes the potential of our global purchasing markets, with only the best and most dependable suppliers, and at the same time provides reliable end-to-end processes.[2]

Contents

What we do at Siemens

Processes & measures followed for rugged communications solutions
Our Cybersecurity Program outlined in this document encompasses all relevant processes and information, in particular:

- Internal organizations and processes designated to cybersecurity
- Our "secure by design" certification and international compliance
- Binding cybersecurity requirements with suppliers
- Defense-in-Depth
  - Customer data protection
  - At our facility and our network protection
  - Products and system solutions
- The Charter of Trust

Each section of the document summarizes the main aspects of each area, and these sections collectively form the Cybersecurity Program.

We secure communication and collaboration
As a leading provider of network and communication solutions, the exchange of information with business partners is part of our daily business. In some cases, data and documents (like costs, contracts, or technical documents) are classified as "confidential" or even "strictly confidential". To ensure secure communication of such information and thereby facilitate secure collaboration, our InfoSec (Information Security) department has created a use case-based IT Service overview. It helps end users as well as their business partners to identify the appropriate Siemens IT Service and security controls to be used for exchanging information and securing the communication and related documentation, to know where to order the respective service from (if required), and how to use it. For example, all e-mails and files sent through the Siemens corporate network have to be labeled with specific security levels. Larger confidential files that cannot be transmitted by e-mail are sent via Siemens SecuFEx (**S**ecure **F**ile **E**xchange), a secure web-based platform with a temporary user account setup for the external business partner or internal employees. This ensures that only authorized persons receive confidential data, such as system logs.

Focused cybersecurity expert teams
ProductCERT and Siemens CERT are the central expert teams for immediate response to security threats and issues affecting our products, solutions, services, or infrastructure. They support employees as well as our customers in dealing with cybersecurity incidents and vulnerabilities.

Siemens ProductCERT
Siemens ProdcutCERT is a separate team of over 100 seasoned security experts that was formed in 2010 to manage the receipt, investigation, internal coordination, and public reporting of security issues related to our products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance our product security, to enable and support development of industry best practices, and most importantly to help our customers manage security risks. It acts as the central contact point for security researchers, industry groups, government organizations, and vendors to report potential product security vulnerabilities. This team also coordinates and maintains communication with all internal and external stakeholders to appropriately respond to identified security issues ("coordinated disclosure" policy). They also release "Security Advisories" to inform customers about necessary steps to securely operate our products and solutions.

Siemens CERT

Siemens Cert is a dedicated team of security engineers with the mission to secure our infrastructure. CERT monitors the current cyber threat landscape and assesses its potential impact on our enterprise. Based on this know-how and the latest technological trends, it consults the Information Technology department to improve the enterprise IT security. It is also responsible for coordinating the response to cybersecurity incidents. To achieve its mission, CERT leverages its relationships with various internal and external stakeholders worldwide, such as CSIRT networks, technical communities, and the security researcher communities. CERT is also recognized as a trusted research partner by academia and industry, with numerous projects and publications in its domain.[3]

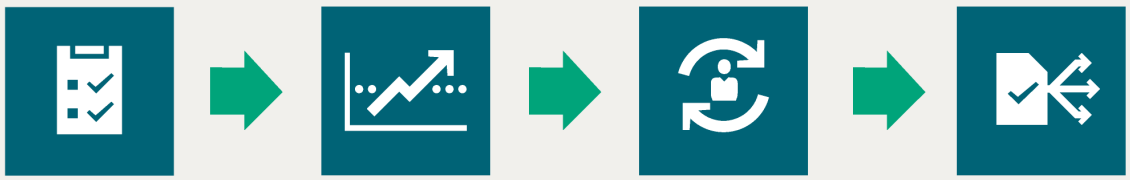
End-to-end approach in vulnerability handling and disclosure process

We are committed to ensuring the safety and security of our customers' facilities. We follow a holistic and comprehensive approach to secure our products, solutions, services, and IT infrastructure. We have formalized a process for handling reported security vulnerabilities in our product portfolio and IT infrastructure. Recovery Planning is included within the scope of the Vulnerability and Incident handling process.[4]

Process Description

Vulnerability handling and disclosure process

The vulnerability handling process consists the following four steps at Siemens:



Vulnerability handling and disclosure process

The complete process is documented under this link, which customers may also bookmark in their browser or subscribe to for up-to-date information:

Link: Siemens Vulnerability Handling and Disclosure Process
https://new.siemens.com/global/en/products/services/cert/vulnerability-process.html

Following the reporting of a vulnerability, analysis, and handling, we disclose the respective information as follows:

Customer disclosure
After the issue is successfully analyzed and if a fix is necessary to cope with the vulnerability, corresponding fixes will be developed and prepared for distribution. We will use existing customer notification processes to manage the release of patches, which may include direct customer notification, or public release of a security advisory containing all necessary information on the Siemens CERT Services website (see section "Contact Information").

Contact Information

Siemens ProductCERT – Contact for Products, Solutions, and Services
E-mail productcert@siemens.com

Siemens CERT – Contact for Infrastructure
E-mail cert@siemens.com

A Siemens Security Advisory usually contains the following information:

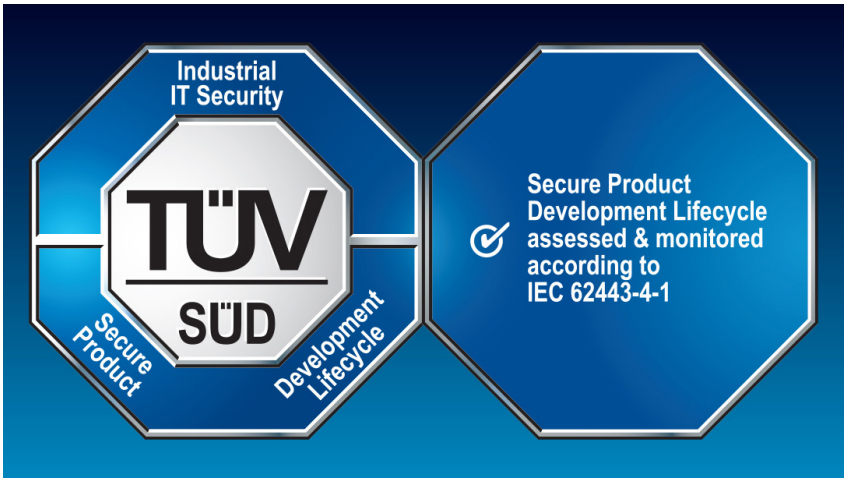
- Description of the vulnerability with CVE reference and CVSS score
- Identity of known affected products and software/hardware versions
- Information on mitigating factors and work-arounds
- The location of available fixes
- Credit for reporting and collaboration, with the reporting party's consent

Comprehensive Cybersecurity Policy Framework
The Cybersecurity Policy Framework outlines our security rules and regulations at Siemens. All information is documented and defined, from roles and responsibilities to set rules and practices to ensure the protection of the company information and business processes, published on the Siemens Intranet and available to all employees.

Established Information Security Management System (ISMS)
An Information Security Management System consists of policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives.[5]

Industrial and electric power security standards and certifications

We have continuously complied with the strictest security requirements and continuously improved security through certifications and standards. We have been monitoring the developments of the various industry specific security standards, including NERC CIP, ISA S99, AGA 12, IEC 62443, ISO 17799:2005, and PCSRF SPP-ICS, to ensure all RUGGEDCOM products contain the features necessary to comply with the identified requirements.[6]



TÜV SÜD certification based on IEC 62443 standard

TÜV SÜD is a world leader in testing and product certification. Our processes certified through TÜV demonstrate our commitment to quality, security, and sustainability.

The TÜV SÜD Certificate based on IEC 62443-4-1 confirms our security in the development process for automation products and the whole product lifecyle, which includes the security of After Sales processes. We are the first company to receive TÜV SÜD certification based on IEC 62443-4-1 for the interdisciplinary process of developing automation and drive products, including industrial software. The international series of standards IEC 62443 defines the security measures for industrial automation systems, with Part 4-1 of the standard describing the requirements of the manufacturer's development process of automation components. The TÜV SÜD certificate is based on the standard IEC 62443-4-1 (Secure Product Development Lifecycle Requirements, Draft 3 Edition 10, 01.2016). This standard includes security-relevant requirements such as capabilities and expertise, security of third-party components including open-source software clearing, process and quality assurance, secure architecture and design, and issue handling as well as security updates, patches, and change management.

As a leading industrial hardware and software supplier for multiple verticals, we are continuously improving our products and solutions for industrial security. This also includes the certification based on IEC 62443-4-1. With this achievement, we document our "Security by Design" approach for automation products and give integrators and operators a transparent insight into our IT security measures. Integrators and operators use this for the conception and operation of automation processes and systems using our technology and the "Defense-in-Depth" protection concept.

To ensure comprehensive protection of industrial plants from internal and external cyberattacks, all levels must be protected simultaneously – ranging from the plant management level to the field level and from access control to copy protection. Therefore, our approach to comprehensive protection offers defense throughout all levels – "Defense-in-Depth". This concept is according to the recommendations of ISA99/IEC 62443 – the leading standard for security in industrial applications.[7]

NERC CIP 13 standard

Siemens supplies to critical infrastructure customers and therefore support them in complying with the NERC CIP-013-1 Cybersecurity Requirements and Measures with regard to Supply Chain Management.

The purpose of the NERC CIP 13 Standard is to mitigate cybersecurity risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.[8]

We regularly provide new software releases that include security fixes. These fixes are communicated as part of the software release bulletin so that customers are aware of any security updates included in the latest release. New products are shipped with the most recent software version that includes the latest security fixes. Furthermore, we also mention the Advisory number in our SIOS (Siemens Industry Online Support) portal[9] product release note when we fix a vulnerability that has already been published in an existing Advisory.

We also provide a list of security recommendations in our user guides giving information to customers on how to make their purchased RUGGEDCOM equipment more secure and keep it secure.

We publish security advisories outlining new security fixes in new software releases through ProductCERT. This includes RUGGEDCOM products as well.

A link to these can be found below:
https://new.siemens.com/global/en/products/services/cert.html

A customer can monitor and subscribe to this list to determine whether the RUGGEDCOM devices they have in their utility are affected (NERC-CIP-013-1 reference R1.2.1, R1.2.2, and R1.2.4).

On-site work is performed after authorization of the work by the customer. This is agreed and scheduled with the customer in advance. All work at customer facilities is supervised by the customer or their nominated representative(s).

Technical support staff can only access a customer setup remotely with customer permission and only in specific situations where no other problem resolution methods, such as e-mails or phone calls, worked. The secure Siemens Circuit-Remote view/control tool is used for this remote access. The Circuit remote view/control sessions are agreed and scheduled with the customer in advance. During remote sessions, the customer is in control and responsible for starting/stopping the remote session. During the remote session, the customer is required to be present, to supervise, and to answer any of the support consultant's questions/changes to be performed. RUGGEDCOM customer support does not use tools for unsupervised/unattended access. After each remote session is completed, the same is messaged to the customer over the phone or the Circuit application access/session is terminated/closed right away, as per NERC-CIP-013-1 reference R1.2.3 and R1.2.6.

Verification of software integrity and authenticity of all software and patches are provided through digitally signed software that is flashed/downloaded into our products, ensuring their authenticity and integrity. In addition, hash checksums are provided to allow our customers to manually validate the integrity and authenticity of our software. These methods are used to verify that only software provided by us is installed on our products, as per NERC-CIP-013-1 reference R1.2.5.

For ROX-II products, the release file, provided with each upgrade package, contains hash checksums (SHA2) of the software packages downloaded as part of the upgrade image. If any of these packages have been modified in transit, then the hash checksum will not match and the upgrade will not continue. The release file is digitally signed with a Siemens private key. The public key required to decrypt the digital signature is stored in ROX. If this public key is invalid/replaced or not present, then the digital signature of the release file cannot be verified and the upgrade will fail. For a flash or downgrade of the image, the entire binary is signed, rather than the release file. The hash checksums of all release files are provided via the Siemens Industry Online Support website.

For the CROSSBOW secure remote access solution, all Windows installer files (*.msi) are digitally signed by the Siemens Trust Center with the Siemens private key. The Siemens Trust Center is identified as a trusted publisher in the Windows certificate store, and Windows can be used to validate that the signer is trusted and the collection of files was not altered after it was published. The hash checksums of all release files are provided via the Siemens Industry Online Support website.

For RUGGEDCOM ROS, the hash checksums (SHA2) for each release and how to verify the firmware integrity with the hash checksums are published in the following document, which is available at the Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ca/en/view/109779935

To stay informed about product updates as they occur, sign up for a product-specific newsletter.
For more information, visit: http://support.industry.siemens.com/

Binding cybersecurity requirements for suppliers and Siemens FOCUS

Our external suppliers are required to fulfill the same high-level security requirements as we do. That is why we establish binding cybersecurity requirements for suppliers. New suppliers must comply with minimum binding cybersecurity requirements, which must be anchored in a separate, binding clause in all new contracts. These requirements will apply primarily to suppliers of security-critical components such as software, processors, and electronic components for certain types of control units. Existing suppliers who do not yet comply with the requirements are to implement them gradually. The goal is to increase security along the entire supply chain. In this regard, we are following the course laid out in the Charter of Trust for cybersecurity. The requirements stipulate, for example, the supplier must integrate special standards, processes, and methods into their products and services to prevent vulnerabilities and malicious codes at suppliers – and thus within our products as well. In the future, suppliers themselves must, for example, perform security reviews, conduct tests, and take corrective actions on a regular basis. We are making these requirements mandatory for our own activities as well.

In the fall of 2018, we further strengthened our internal capacities for repelling hacker attacks and restructured our cyberorganization (PSS = Product & Solution Security). Operating as a worldwide network, the new unit combines what were once separate areas. As a result, we are now the first major company to take a holistic approach to the topic of cybersecurity. Not only does the new organization investigate, analyze, and repel hacker attacks; it also develops cybersecurity services and teams up with the company's business units to launch these services in the market. The goal is to react to attacks with even greater speed and flexibility. In every region and at every division, we have strengthened our network of cybersecurity officers and experts.

> Siemens has been active in the field of cybersecurity for more than 30 years.

Our first cybersecurity team was established back in 1986. The company currently has around 1,275 employees worldwide working exclusively on cybersecurity-related matters. Other employees at the divisions and in the regions also contribute to the company's activities in the cybersecurity field.[10]

Defense-in-Depth

The IEC 62443 standard recommends Defense-in-Depth, a risk-based, multi-layered security concept for industrial automation and control systems. This standard takes a risk-based approach to ensuring cybersecurity by addressing not only the technology that comprises a control system, but also the work processes, countermeasures, and employees. This includes establishing a security program with physical security to authorize access and ensure security of sensitive areas, network security, for the ICS with DMZ (demilitarized zone), network segmentation and data encryption and, finally, system integrity with system hardening to make OT networks resilient to cyberattacks.

We implement this approach to provide in-depth protection and end-to-end security controls throughout the organization from execution of the service and engagement with the customer to implementation of technical, physical, and administrative measures to provide confidentiality, integrity, and accountability.

Customer data protection

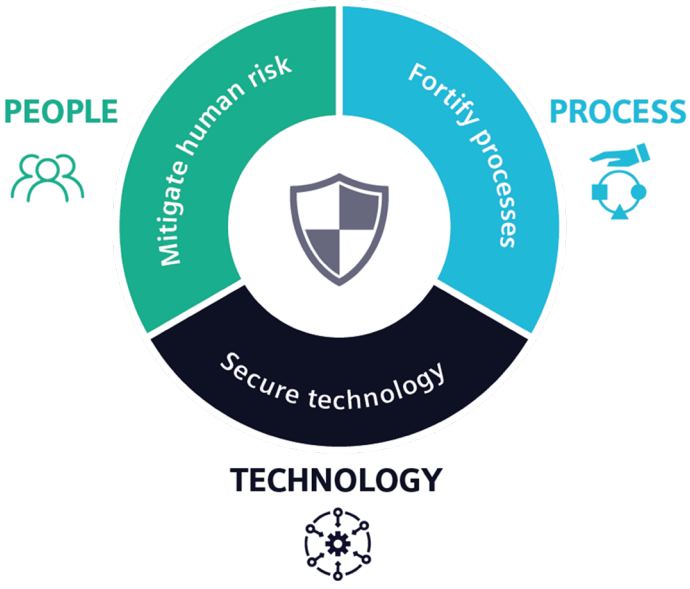
Documents that include sensitive information, of confidential nature, or include information such as Internet Protocol (IP) addresses, customer name, and contact details are exchanged via Siemens' hosted SecuFEx and protected by a personalized password. The person who shares the file decides when the data will be deleted, and the files are permanently removed after a 1 to 3 week retention period.

Customer documents and information are securely stored on our IT managed servers, where our strict Information Security policies covering personal data protection, virus/malware protection, and retention period apply.

Corporate policies are published and available for all employees for maintaining and monitoring the security of customer data.

Only an authorized Siemens PC can access the corporate network. Siemens corporate laptops used by the Services and Support teams are equipped with firewalls, encrypted hard drives, and two factor authentication (password + user-based authentication Public Key Infrastructure or PKI) as well as documented secure configurations, logging, patching, and asset management.

On-site Professional Service work is performed after authorization is granted by the customer. We follow the customer's security policies as related to connection to the customer network locally or remotely. Network consultants will most often log-on to the customer network through dedicated terminal workstations provided by the customer. Any specialized tools are deployed on designated service laptops, such as Siemens field laptops, which are kept offline and not connected to the internet or used for any office-related applications.



If the consultant is allowed to use his/her dedicated PC loaded with specialized tools, then we:

- Disable the services and ports on the PC from which we conduct the assessment from, and
- Enable a built-in firewall on the PC from which the assessment is conducted from

All work at the customer facility is supervised by the customer or a nominated representative. The use or exchange of data using removable drives (USB pens) is not allowed. The customer is also required to sign a job completion form after completion of the work.

At our facility and network protection

We use different methods and security measures to protect our critical components, sensitive data, our network, and workforce. The list below provides a summary of what we do at our facility.

- All employees are subject to a background check at the time of hiring
- Communication is encrypted within a network control center via VPN/IPsec
- Technical support tickets/e-mail communication is done via the assist system
- Troubleshooting is performed with remote access to customer setups via Circuit and FastViewer tools
- Secure file transfers is ensured via Siemens SecuFEx
- Customer files analysis and direct e-mail exchange is done with Siemens corporate laptops
- Role-based access control
- All employees have their assigned key card access and designated levels of security access
- Strict building access: locks, and security cameras are installed throughout the plant
- All systems involved in customer data handling are equipped with virus/malware scanners

- All systems have the latest security features such as: all connections are encrypted, two factor user-based authentication, PKI (Siemens PC + PKI Card + Pin), or OTP (Siemens PC + Active Directory Auth. + one-time mobile PIN)
- Where passwords are used, password complexity is enforced and passwords need to be changed frequently and regularly
- All data on every system is stored and encrypted
- Hardware TPM (Trusted Platform Module) is used as applicable

At Siemens, we also raise awareness for proper cybersecurity habits through mandatory training to ensure our workforce is prepared and has enough knowledge of cyber threats as well as to prevent and protect from cyberattacks.

Equipment physical security is also in place as described by the Siemens Corporate Security Department.

Overview of cybersecurity in our products and system solutions

We are committed to providing a holistic cybersecurity solution. By combining the security features of the RUGGEDCOM switches with the RUGGEDCOM Multi-Service Platform cybersecurity appliance, our customers can establish an electronic security perimeter around their critical infrastructure to prevent the disruption of mission critical applications by accidental or malicious acts. Furthermore, with the RUGGEDCOM APE (application processing engine) and Siemens-verified partners, our customers can also deploy advanced applications for cyber threat detection and prevention, right at the OT edge.

Product test and quality assurance

Cybersecurity software delivered by us is tested and developed as per quality and security guidelines.

Security is an integral part of the software development lifecycle for the RUGGEDCOM product line. Software and firmware releases incorporate the following security-focused activities: Threat & Risk Analysis (TRA), vulnerability scanning, robustness and penetration testing.

Cybersecurity software or patches are delivered using Siemens SecuFEx, and integrity of the software is confirmed via a documented process.

RUGGEDCOM CROSSBOW

RUGGEDCOM CROSSBOW is a proven Secure Access Management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices. The CROSSBOW solution focuses on delivering productivity gains for administrators and users while achieving full NERC CIP compliance in managing, securing, and reporting on remote access.

RUGGEDCOM Multi-Service Platform

The Multi-Service Platform has been specifically developed to provide an electronic security perimeter for the protection of critical assets. It is the main point of entry between the local area network (plant floor or substation) and the WAN. The Multi-Service Platform combines a layer 3 router, a firewall, and a VPN in one device.

Key RUGGEDCOM Multi-Service Platform cybersecurity features include:

- Firewall – Stateful firewall to control traffic between different zones of trust within a network. It includes Network Address Translation (NAT) to prevent unauthorized or malicious activity, initiated by outside hosts, from reaching the internal LAN.
- Virtual Private Networking (VPN) – Provides secure communication links over networks. It ensures confidentiality, sender authentication, message integrity, and uses IPSec (IP Security) for encryption and authentication of all IP packets at the network layer.
- Strong Encryption – Utilizes various encryption algorithms (AES, RSA, and ECC) to obscure information and make it unreadable without special knowledge.

RUGGEDCOM APE1808

The RUGGEDCOM APE1808 utility-grade application processing engine is a standards-based hardware platform to deploy third-party Edge computing applications. As a line module for the RUGGEDCOM RX1500 series, it is available either with Linux or Windows 10 OS and offers a convenient way to deploy industrial applications to the OT edge.

RUGGEDCOM Switches

RUGGEDCOM Ethernet Switches provide security at the local area network level.
The key cybersecurity features of these switches include:

- MAC-based Port security – The ability to secure ports on a switch so only specific devices/MAC addresses can communicate via that port
- 802.1x Port Based Network Access Control – The ability to lock down ports on a switch so that only authorized clients can communicate via this port
- Radius – Provides centralized authentication
- SNMPv3 – Encrypted authentication and access security
- SSH/SSL – Extends capability of password protection to add encryption of passwords and data as they cross the network
- Enable/Disable ports – Capability to disable ports so that traffic cannot pass
- 802.1Q VLAN – Provides the ability to logically segregate traffic between predefined ports on switches
- Passwords – Multi-level user passwords secure switch against unauthorized configuration

Integrated cybersecurity solutions

Siemens offers fully customizable solutions, combining not just the field-proven RUGGEDCOM hardware, but also its associated Professional Services team and tried and tested cybersecurity software solutions sourced from leading external cybersecurity partners to address the customer needs on additional needs such as IDS (Intrusion Detection Systems)/IPS (Intrusion Prevention Systems) and NGFW (Next Generation Firewalls). Each customer's network infrastructure, operation, and cybersecurity requirements are vastly different, and demand a cybersecurity tailored to it specifically, and so we encourage having a conversation with one of our in-house experts to tailor a solution suited to your network. Let's talk!

Siemens: Initiator and founding member of the Charter of Trust

We have teamed up with the Munich Security Conference and other governmental and business partners to present the Charter of Trust initiative. One of the initiative's key goals is to develop and implement rules for ensuring cybersecurity throughout the networked environment.

The signatories now include Siemens, MSC, the IT giant IBM, Daimler, the insurance company Allianz, Airbus, the world's leading inspection, verification, testing, and certification company SGS, the telecommunications company Deutsche Telekom, Dell, Cisco, the oil company Total, TÜV SÜD, the semiconductor producer NXP, the energy company AES Corporation, and the IT giant Atos. This list of renowned global companies is steadily growing – check it out on **www.charter-of-trust.com**

Due to our unique combination of technological expertise in cybersecurity for everything from factories and power grids to health care systems, we are ideally suited to taking on a pioneering role in this field.

> "The Charter contains ten principles that should make the digital world more secure and also sets three important goals: protect the data of individuals and companies; prevent damage to people, companies, and infrastructures; and create a reliable foundation for instilling trust in a networked, digital world.

References

[1] **Innovation Field, Cybersecurity**

[2] **Collaborating with Siemens**

[3] **Siemens ProductCERT and Siemens CERT**

[4] **Siemens Vulnerability Handling and Disclosure Process**

[5] Source derived from the intranet of **Siemens, (Information Security Management)**

[6] **RUGGEDCOM cybersecurity solutions**

[7] **Certified Security, TÜV SÜD certificate**

[8] As defined in **NERC-013-1**

[9] **Siemens Industry Online Support portal**

[10] **Binding Cybersecurity Requirements for Suppliers**

[11] **The Charter of Trust**

For more information on cybersecurity related topics, please visit:

Siemens Industrial Security

Cybersecurity

Cybersecurity at Siemens

For more information, please visit:
siemens.com/ruggedcom

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

Siemens Canada Limited
300 Applewood Crescent
Concord, Ontario, L4K 5C7
Canada

Article No. 6ZB5530-0DR02-0BA0
Dispo 26000
BR 1121 0. PoD 12 En
Printed in Germany

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**

The information provided in this brochure contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.