SIEMENS
Ingenuity for life

siemens.com/ruggedcom

Cybersecurity: What we do at Siemens

RUGGEDCOM

Concord, May 2020

Introduction

With RUGGEDCOM, our mission is to deliver peace of mind to customers by providing innovative, secure and rugged communication solutions for mission critical infrastructure in harsh environments.

With the increased need for securing assets and data in a more digitalized world, cybersecurity has become increasingly important for all of us at our customers and at Siemens. In order to address this critical demand, 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.

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

With three cyber defense centers, Siemens monitors its own systems and supplies secure products and services to customers e.g. utilities, power grid operators, virus protection for tomographs and other imaging products.[1]

Our end-to-end Supply Chain Management from the source to the end user fully utilizes the potential of Siemens global purchasing markets, and at the same time provides reliable, end-to-end processes. That is why we concentrate only on the best and most reliable suppliers. [2]

Contents

What We do at Siemens

Our Cybersecurity Program outlined in this document encompasses all relevant processes and information, in particular:

- Siemens internal organizations and processes designated to Cybersecurity
- Our "secure by design" certification and international compliance
- Binding cybersecurity requirements with suppliers
- Siemens Ruggedcom 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 at Siemens. In some cases, data and documents (like costs, contracts or technical documents) are classified as "confidential" or even "strictly confidential". To ensure secure communication and collaboration of such information, Siemens' InfoSec (Information Security) department has created a use case-based IT Service overview. It helps Siemens 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 emails and files sent through the Siemens corporate network have to be labeled with specific security levels, and larger confidential files that cannot be transmitted by email are sent via the Siemens SecuFEx (**Secu**re **F**ile **Ex**change), a secure web-based platform with a temporary user account setup for the external business partner or internal Siemens 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 Siemens products, solutions, services, or infrastructure. They support Siemens employees as well as our customers deal with cybersecurity incidents and vulnerabilities.

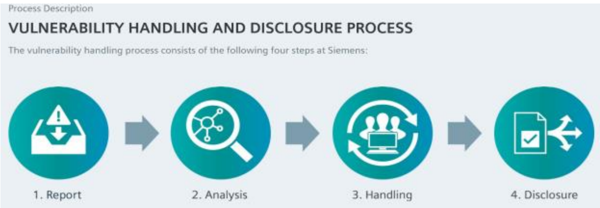
Siemens ProductCERT is a separate team of over 100 seasoned security experts that was formed in 2010 tomanage the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks. It acts as the central contact point for security researchers, industry groups, government organizations, and vendors to report potential Siemens 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 Siemens products and solutions.

Siemens CERT is a dedicated team of Security Engineers with the mission to secure Siemens infrastructure. CERT monitors the current Cyber Threat Landscape for Siemens and assesses its potential impact to the enterprise. Based on that know-how and the latest technological trends, it consults the Information Technology department in Siemens to improve the enterprise IT Security. It is also responsible for coordinating the response to cybersecurity incidents within Siemens. To achieve its mission, CERT leverages its relationships with various internal and external stakeholders world-wide, 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]

Siemens End-to-End Approach in Vulnerability Handling and Disclosure Process

Siemens is committed to ensuring the safety and security of our customer's 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 Vulnerability and Incident handling process. [4]

Figure 1. Vulnerability Handling and Disclosure Process


Process Description
VULNERABILITY HANDLING AND DISCLOSURE PROCESS
The vulnerability handling process consists of the following four steps at Siemens:
1. Report
2. Analysis
3. Handling
4. Disclosure

The complete process is documented at 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. Siemens 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").
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 workarounds
- The location of available fixes
- Credit for reporting and collaboration, with the reporting party's consent.

Contact Information

Siemens ProductCERT - Contact for Products, Solutions, and Services
Email productcert@siemens.com

Siemens CERT - Contact for Infrastructure Email
cert@siemens.com

Comprehensive Cybersecurity Policy Framework

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

Siemens has continuously complied with the strictest security requirements and continuously improved security through certification 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 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. The Siemens processes certified through TUV demonstrate our commitment to quality, security and sustainability.

The TÜV SÜD Certificate based on IEC 62443 confirms Siemens security in the development process for automation products and the whole Product Lifecyle which includes the security of After Sales processes. Siemens is the first company to receive TÜV SÜD certification based on IEC 62443-4-1 for the interdisciplinary process of developing Siemens 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, Siemens is continuously improving its products and solutions for industrial security. This also includes the certification based on IEC 62443-4-1. With this achievement, we are documenting our "Security by Design" approach for automation products and are giving 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 Siemens technology and the "Defense in Depth" protection concept.

To ensure comprehensive protection of industrial plants from internal and external cyber-attacks, 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 is the supplier to critical infrastructure customers, and therefore supports in complying with the NERC CIP-013-1 Cybersecurity Requirements and Measures with regards 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 been already published in an existing Advisory.

We also provide a list of Security Recommendations in our user guides providing information to customers on how to make/keep their purchased RUGGEDCOM equipment more secure.

Siemens publishes 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 (particular NERC-CIP-013-1 reference R1.2.1, R1.2.2 and R1.2.4). Onsite 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 are 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 Siemens is installed into 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 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 that the Release file. The hash checksums of all release files are provided via the Siemens Industry Online Support web site.

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 web site.

For RUGGEDCOM ROS, the hash-checksums (SHA2) for each release and how to verify the firmware integrity by the 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

External suppliers to Siemens are required to fulfill the same high-level security requirements as Siemens itself. That is why we establish binding cybersecurity requirements for suppliers. New Siemens suppliers must comply with minimum binding cybersecurity requirements and 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, Siemens is 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 so as to prevent vulnerabilities and malicious codes at suppliers – and thus within Siemens products as well. In the future, suppliers themselves must, for example, perform security reviews, conduct tests and take corrective actions on a regular basis. Siemens is making these requirements mandatory for its own activities as well.

In the fall of 2018, Siemens further strengthened its internal capacities for repelling hacker attacks and restructured its cyberorganization (PSS = Product & Solution Security). Operating as a world-wide network, the new unit combines what were once separate areas. As a result, Siemens is now the first major company to take a holistic approach to the topic of cybersecurity. Not only does the new Siemens 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, the company has strengthened its network of cybersecurity officers and experts.

Siemens has been active in the field of cybersecurity for about 30 years. Its 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]

Siemens Defense in Depth

Siemens has created a multi-faceted approach to provide in-depth protection and end-to-end security controls in 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 Secure File Exchange (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 weeks retention period.

Customer documents and information are securely stored on Siemens IT managed servers, where Siemens' strict Information Security policies covering personal data protection, Virus/Malware protection, and retention period applies.

Corporate policies are published and available for all employees for the 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.

Onsite Professional Service work is performed after authorization is granted by the customer. Siemens follows the customer security policies as related to connection to the customer network locally or remotely. Network consultants will most often login into the customer network through dedicated terminal workstation 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 where we conduct the assessment from, and
- ➢ Enable built-in firewall on the PC where the assessment is conducted from

All work at the customer facility is supervised by the customer or 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. Below list is a summary of internal actions we take at our own facility:

- All employees are subject to background check during hiring process
- Encrypted communication with a network control center via VPN/IPSEC
- Assist system for Technical Support tickets / E-mail communication
- Circuit and FastViewer tools for remote access to customer setups to troubleshoot
- Siemens SecuFEx system for secure files transfer
- Siemens corporate laptops, for customer files analysis and direct E-mail exchange
- 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 needs to be changed frequently and regularly
- All data on any systems is stored and encrypted
- Hardware TPM (Trusted Platform Module) is used as applicable.

At Siemens, we also raise awareness of proper cybersecurity habits through mandatory training to ensure our workforce is prepared and has enough knowledge of cyber threats and 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 Siemens Products and System Solutions

Siemens is committed to providing a complete Cybersecurity solution. By combining the security features of the RUGGEDCOM switches with that of the Multi Service Platform cybersecurity appliance, Siemens customers can establish an electronic security perimeter around their critical infrastructure to prevent the disruption of mission critical applications by accidental or malicious acts.

Product Test and Quality Assurance

Cybersecurity software delivered by Siemens 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 testing 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

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 compliance in managing, securing and reporting on remote access.

Multi Service Platform

The Multi Service Platform has been specifically developed to provide an Electronic Security Perimeter for the protection of critical assets. The RUGGEDCOM Multi Service Platform 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. 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. 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 Switches

The 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 secures switch against unauthorized configuration

Siemens offers fully customized 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

Siemens has 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 out on www.chatert-of-trust.com

Siemens didn't initiate the Charter by accident, as digital value added is rapidly becoming fundamental to industrial competitiveness. Due to its unique combination of technological expertise in cybersecurity for everything from factories and power grids to health care systems, Siemens is 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.**
11

REFERENCES

[1] Innovation Field, Cybersecurity,
Siemens Supplier Innovation Platform - Start

[2] Collaborating with Siemens,
https://new.siemens.com/global/en/company/about/corporate-functions/supply-chain-management/collaborating-with-siemens.html

[3] Siemens ProductCERT and Siemens CERT
https://new.siemens.com/global/en/products/services/cert.html

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

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

[6] Cybersecurity, Ruggedcom
https://new.siemens.com/global/en/products/automation/industrial-communication/rugged-communications/technology-highlights/cybersecurity.html

[7] Certified Security, TÜV SÜD certificate
https://www.automation.siemens.com/certificates-static/di-pa/secure-product-development-lifecycle-iec62443-4-1-en.pdf

[8] As defined in NERC-013-1
https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

[9] Siemens Industry Online Support portal
https://support.industry.siemens.com/cs/start?lc=en-WW

[10] Binding Cybersecurity Requirements for Suppliers
https://www.siemens.com/press/PR2019020139COEN

[11] The Charter of Trust
http://www.siemens.com/press/cybersecurity

For more information on cybersecurity related topics, please visit:

Siemens Industrial Security
http://www.siemens.com/industrialsecurity

Cybersecurity
https://new.siemens.com/global/en/company/stories/home/cybersecurity.html

Cybersecurity at Siemens
https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity/partner-siemens.html

Siemens Ruggedcom
Digital Industries
300 Applewood Crescent
Concord Ontario L4K 5C7
Canada

The information provided in this document only contains general 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.