GE Oil & Gas

Cyber Security Solutions for Industrial Controls

OVERVIEW

In a complex world of ever-changing technologies, GE realizes the importance of having an experienced partner to guide successful cyber security implementation. As a global leader of industrial controls, GE is well-equipped to help customers improve their security posture and support external and internal compliance policies and requirements. Our products are built with security in mind and are easily integrated into broader plant-level systems and IT architectures.

GE's SecurityST* centralized security management solution and Cyber Asset Protection subscription service are key parts of a defense-in-depth system for turbine, plant, and generator controls environments. The SecurityST Mark* VIe Solution and Commissioning Services is Achilles® Practice Certified – Bronze, indicating the solution has undergone strict cyber security best practices demonstrating to customers that systems are developed and implemented securely. Our solutions and related services are designed to support the plant operation's compliance to IEC 62443-2-4, the recently adopted international standard for vendors.

TYPICAL CYBER SECURITY DIRECTIVES

- Control system shall be protected from internal and external threats
- Control system network shall be segmented from other networks
- Network access points shall be protected and continuously monitored; potential threats are to be logged and appropriate notifications sent to the proper people
- All users and devices are to be authenticated and authorized with the least privileges necessary
- All control system equipment and interfaces shall be hardened to industry standards and best practices
- System shall be continuously monitored for unusual system activity and known cyber-attack signatures
- Validated and approved software security updates shall be applied to control system components when available
- Multiple defensive and detection measures shall be incorporated into the solution
- Fail safe – failure of security features will not impact system operations
- Implementation, facility and transfer shall be secure
- External Access Points (EAPs) shall be secure

GE's CYBER SECURITY CULTURE

GE is committed to a culture of security to protect our systems, products, and customer operations. We strive to support our customers' efforts to secure energy operations, and we embrace industry efforts toward achieving cyber security excellence. As energy producers further expand connectivity amidst the Industrial Internet era, we continue to evolve and strengthen our security efforts.

OUR SECURITY PROGRAM

GE's customer cyber security programs and postures depend on the security of our products and services. We embrace our responsibilities to:

- Help energy organizations continually improve their security postures
- Support industry security and risk compliance efforts as they relate to GE equipment

GE's security program is designed to meet the demands of operating in today's complex threat environment. Our security program addresses people, process and technology areas key to supporting secure energy operations. Backed by leadership directives, our security program includes dedicated teams accountable for implementing security controls in ten key areas that span a secure development lifecycle, from product design to ongoing operational support.

OUR PEOPLE

GE's commitment to security begins and ends with our employees. This effort begins at the top with comprehensive cyber security policies regularly communicated throughout our organization. We have dedicated teams committed to IT, industrial, and product security. These organizations work together to drive cyber security best practices.

INDUSTRY ENGAGEMENT

Through partnerships with industry leaders, customers, employees, suppliers and contractors, we are able to support major industry initiatives, such as Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC). We are dedicated to on-going security engagements through our GE Charter Technology customer relationships worldwide.

Our security experts readily share and train industry constituents on current topics through GE and third party symposia. These shared insights and experiences will continue to improve our solutions and processes. As industry standards and customer needs change, we will continually adapt our security methods to help protect customers from risk.

ADHERENCE TO GLOBAL SECURITY STANDARDS

GE understands the importance of leveraging and integrating industry cyber security practices that have been developed by organizations such as the National Institute of Standards and Technology (NIST) and the International Standardization Organization (ISO). Specifically, the internationally recognized frameworks we have chosen to adopt include:

- ISA-99 (Industrial Automation and Control Systems Security)
- ISA/IEC 62443 (Industrial Network and System Security)
- WIB M-2784 (Process Control Domain – Security Requirements for Vendors)
- NIST 800-82 (Guide to Industrial Control Systems)
- ISO 27002 (Enterprise Cyber Security)

OUR PROCESSES

GE has adopted international security standards related to our infrastructure, as well as processes that impact its resilience. Where applicable, GE seeks and obtains independent certifications aligned to internationally recognized security standards.

From product development through delivery and maintenance, our policies and procedures address security throughout an energy operation's lifecycle. Adoption of secure development lifecycle processes support the implementation of critical security controls for the delivery of both products and services. A dedicated GE team maintains relationships with key operating system, network device, and application vendors to closely track security issues, software updates, and newly released patches—with the intent to alert product users when needed. Newly available patches, malware detection signatures and anti-virus are evaluated and tested for applicability to the system.

OUR TECHNOLOGY

GE equipment is engineered with security in mind. Our product development lifecycle includes product assessments (both internal and third party testing) and security design reviews as a regular practice within our development process. Updated tools and methods in both IT and OT security are applied throughout the product lifecycle to reduce risk and address vulnerabilities.

CUSTOMER ROLE IN SECURITY PARTNERSHIP

We recognize that solid business relationships are fundamental to the success of our security programs. In the case of an incident, our product security incident response team (PSIRT) evaluates, takes actions and handles communication related to the vulnerability or incident. If a threat is detected, we will implement corrective action as appropriate. We encourage our customers to report suspicions and events pertaining to security or other irregular business matters to security@ge.com. Additionally, our public website for security reporting can be found at: ge.com/security.

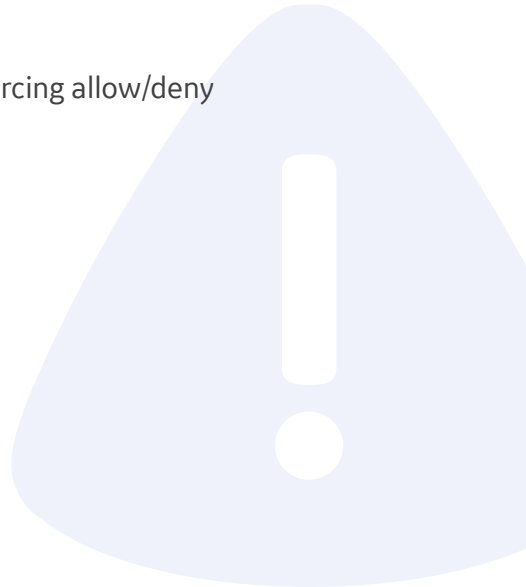
SecurityST – A CENTRALIZED SECURITY MANAGEMENT SOLUTION

GE's SecurityST centralized security management solution is a key part of a defense-in-depth system for turbine, plant, and generator controls environments. Employing modular defensive services and technologies, this centralized system gives companies a single vantage point to see their cyber security posture, implement proactive strategies and policies to protect critical control system and related networks, and provide a centralized reporting capability to manage cyber risk. This solution helps mitigate cyber vulnerabilities at the network, endpoint and controller levels.

NETWORK INTRUSION DETECTION AND PREVENTION SYSTEMS

This customizable network security option provides the ability to monitor and block malicious activity and attacks.

- Provides continuous visibility of unusual activity and potential threats on the control system network
- Captures traffic logs and enables ongoing network analysis at both a local and enterprise level
- Up-to-date protection enhanced by IDS/IPS signatures updates provided by GE, designed to detect or protect against known threats
- Promotes stronger control over OT application protocols, enforcing allow/deny rules on the control system network



ROLE-BASED ACCESS CONTROL

This feature provides centralized control and management alerting specific to the controls environment. Simply put, it allows you to manage who can access the industrial control system and what permissions they have.

Benefits include:

- Ease of set-up through use of pre-defined plant roles, created using industry best practices
- Reduced risk impact by limiting access to critical infrastructure
- Increased visibility to user access levels with immediate ability to provide or remove access to streamline employee and third-party needs
- Controller two-factor secure-mode capability further reducing access and increasing protection
- Centralized password management enforcement allows the customer to easily implement and manage a password policy with pre-set or customer-defined options available

SECURITY INFORMATION AND EVENT MANAGEMENT

We provide a scalable solution with both real-time and historic views of cyber activity such as changing of switch configurations, failed login attempts, unauthorized port access and USB usage.

Benefits include:

- A centralized function with real-time visual security status dashboard and events display, providing complete visibility to your assets and alerting you to potential threats
- Records and stores logs for all system components, allowing you to retrieve past activity and correlate events for incident alerts and audit reports; logs can be forwarded to enterprise team for additional assistance

REMOTE ACCESS SECURITY

We use best practices to assist with remote access security based on customer needs and standards. Our solution options include multi-factor authentication, lockbox, data-diode (one-way directional), VPN, intrusion prevention and read-only access. We help you control who can access your critical assets and what information they can access.

Benefits include:

- Segments access using clear enforcement zones between internal and external networks, helping to meet compliance requirements and prevent unauthorized access to the control system
- Defines and encapsulates the authorized users and systems they are permitted to interface within customer environments
- Monitors and inspects traffic between organizations for anomalous behavior, capturing device and user activity

BACKUP AND RECOVERY

- Automatic, centralized backup and recovery of the process control domain, saving time and money through availability of a quick disaster recovery plan with minimal downtime
- All backup activities are logged and easily accessed for generating reports to assist with compliance reporting

PATCH UPDATE SERVICE

The Cyber Asset Protection subscription provides monthly updates for your HMI, Historians, switches, firewalls, OSM and RSG.

Benefits include:

- Centralized deployment of GE's patch management subscription service with SecurityST can save 4 hours per HMI which can result in $10-20K USD monthly savings for a typical plant
- Increases your security posture by protecting your critical assets from known vulnerabilities on a monthly basis
- Easy-to-deploy updates are cumulative and can be automated or scheduled based on plant needs
- Receive an applicability report that defines criticality, time required for update and reboot necessity, providing intelligence that allows you to make informed decisions for your operations

ENDPOINT PROTECTION

Endpoint protection protects your data integrity and the systems running your assets. It monitors for malicious activity through internal access points (USB, CD/DVD, ethernet ports, etc.) and blocks unauthorized access.

With the new application whitelisting option, Windows® based devices have improved security posture by reducing the risk and cost of malware, improving network stability and reliability. This feature automatically identifies trusted software that is authorized to run on control system HMIs while preventing software that is unknown or unwanted.

SECURE IMPLEMENTATION AND CHAIN OF CUSTODY

As a vendor, security starts with us. We build and prepare each SecurityST with strict attention given to physical and digital security through the use of physical perimeters, access control with video surveillance, and secure custody transfer. Our Longmont, Colorado Headquarters is certified to meet the needs of nuclear, oil & gas and power generation customers through strict adherence to standards required by IEC 62443.

CYBER ASSET PROTECTION SUBSCRIPTION – VALIDATED PATCH MANAGEMENT SERVICE

GE's Cyber Asset Protection (CAP) Subscription solution is a key part of a defense-in-depth system for turbine, plant, and generator controls environments. The subscription service includes operating system and application patches as well as anti-virus/intrusion detection signatures to cover updates for HMIs, servers, switches, and network intrusion detection devices. Monthly updates can be applied to individual HMIs or via the SecurityST appliance for network-wide deployment.

WHY PATCHING IS CRITICAL

Patching your systems is one of the best things you can do to protect your assets and assure the operating systems and programs running are updated to provide the latest security protection without risking your operation. Listed as two of the "First Five Quick Wins" by The SANS Institute, a well-respected authority on information security and cyber security training, patching of application and system software is critical to improving and maintaining a high security posture.

THE IMPORTANCE OF VALIDATION

With validated patch management, the updates are validated in a lab that mimics the plant environment in order to identify any incompatibilities that may exist before the patch is applied. This allows operators to determine what alterations need to be made to ensure uptime and protection against cyber threats without having to create simulators themselves. Our testing is done in a secure lab environment using both physical hardware and software, which is the best method to guarantee industrial controls receive tailored patches and an applicability report on a monthly basis.

HOW CAP WORKS

The Cyber Asset Protection subscription provides monthly updates for your HMI, Historians, switches, firewalls, OSM and RSG. Software updates include:

- Windows® Operating System
- GE Cimplicity* (ICS-CERT-specific)
- Intrusion Detection signatures
- Anti-virus signatures
- Switch updates
- System 1*
- Microsoft Word® and Microsoft Excel®
- Adobe®

The subscription service also provides a monthly report of patches that need to be installed and the areas of which are critical for attention.

Benefits include:

- Provides tested updates to keep your legacy critical infrastructure running
- Reduces downtime by providing validated patches which are tested in an environment to assure applicability and compatibility
- Keeps your risk profile updated and increases your security posture by protecting your critical assets from known vulnerabilities on a monthly basis
- Helps you meet regulatory requirements and avoid fines
- Improves safety and reliability by preventing loss of view
- Provides a dedicated service manager for cyber issues

GE's SUPPORT FOR REGULATIONS AND STANDARDS – A TRUSTED PARTNER FOR COMPLIANCE

As a vendor of industrial controls, GE embraces its responsibilities to assist critical infrastructure owners as they improve their security postures and support compliance efforts related to GE-provided equipment throughout the 10- to 20-year lifecycle of the control system itself. Together with Wurldtech Security Technologies, GE is able to offer security support that spans from initial system design to commissioning, all the way through ongoing support and maintenance. Our solutions are built with security in mind, and are readily integrated into broader plant-level systems and IT architectures.

IEC 62443-2-4

IEC 62443-2-4 is a published international standard, defining cyber security capabilities that Industrial Automation and Control System (IACS) service providers may implement and offer. The standard can help asset owners consistently procure and manage control system security expertise. IEC 62443-2-4 was developed by IEC Technical Committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members.

GE hardens customer systems using a combination of technical and procedural measures that have been certified to meet IEC 62443-2-4 security standards. These standards specify a comprehensive set of security requirements for IACS installation and maintenance.

ISO 27002

GE is prepared to support customers working toward ISO 27002 compliance. Our documented processes and best practices for cyber security are in place to support companies as they develop their own policies within this regulation framework. Through process and technology, GE has capabilities to partner with customers for 27002 compliance.

NERC CIP REV 5 & 6

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology. Version 6 requires compliance by July 2016 (high and medium impact bulk electric system (BES)) or July 2017 (low impact bulk electric system (BES)). To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance.

GE's professional security services and operational technology (OT) security solutions are designed and tested for the industrial controls environment. Our Cyber Asset Protection (CAP) Software Update Subscription and SecurityST appliance are built to support best practices in security and facilitate more efficient compliance to NERC CIP 5 & 6.

NEI 08-09

GE supports nuclear compliance efforts for NEI 08-09 by providing baseline configuration documentation for current and certain legacy controls, and by supporting asset operator cyber vulnerability assessments and associated mitigations. GE's cyber solutions support cyber security best practices such as centralized patch management, anti-virus/host intrusion detection updates, account management, logging and event management, intrusion detection and automated backup. We support confidentiality, integrity and availability of critical controls and related networks, which in turn can be applied to support owner compliance toward NEI 08-09.

For more information, please contact:

GE Oil & Gas

Digital Solutions

North America: 1-888-943-2272; 1-540-387-8726

Latin America (Brazil): +55-11-3958-0098

Europe (France): +33-2-72-249901

Asia/China (Singapore): +65-6622 1623

Africa/India/Middle East (U. A.E.): +971-2-699 7119

Email: ControlsConnect@ge.com

Customer Portal: ge-controlsconnect.com

1800 Nelson Road

Longmont, CO, USA 80501

http://www.gemeasurement.com

GEA32714 08/2016