SecurityST* for Oil & Gas

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 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.

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. The Security ST solution 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

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, 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 you 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 with 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 ensurance 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

For more information please contact:
GE Oil & Gas
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
https://www.gemeasurement.com/machinery-control

Patch Update Service

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® Excel and Microsoft® Word
- Adobe

Benefits include:

- Centralized deployment of GE's patch management subscription service, saving 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. As we build and prepare each SecurityST, strict attention is 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.

GEA32527 (06/2016)