SecurityST* Cyber Security Management System

fact sheet

GEA-S1292A

As a global leader of industrial controls, GE embraces its responsibilities to help customers improve security and to support compliance efforts as they relate to our equipment. GE builds security into its core products, and offers complementary cyber security solutions for controls and associated networks that are easily integrated into broader plant-level systems and architectures.

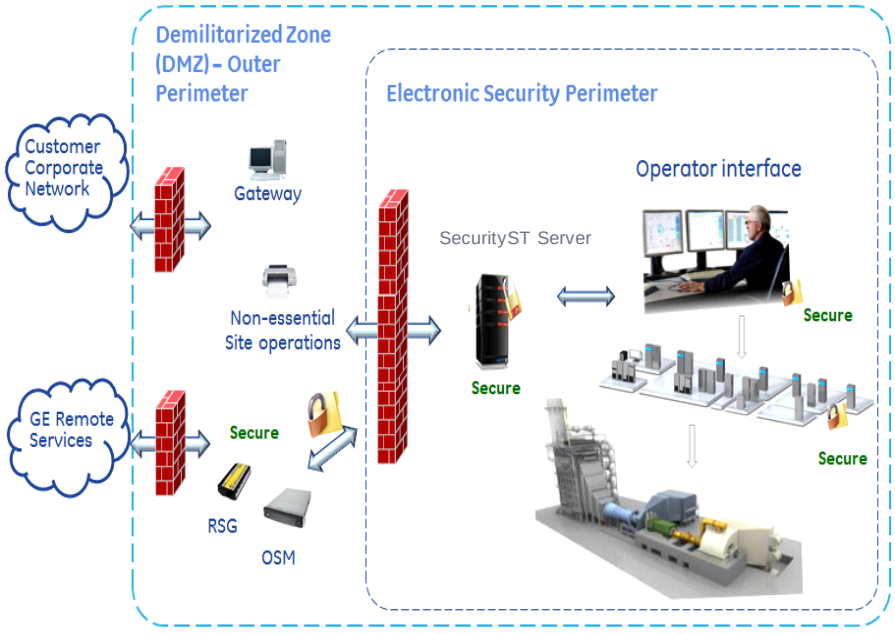
The SecurityST CSMS is a key part of the defense-in-depth solution for delivery systems used to monitor and control the production, transfer, and distribution of energy. Today's highly reliable and flexible energy infrastructure depends on the ability of energy generation and delivery systems to provide timely, accurate information. Employing multiple defensive services and technologies, it supports the reliability, availability, integrity, and maintainability of a plant's critical control and related networks. It also supports plant operator compliance to cyber security regulations, standards, and guidelines, such as NEI 08–08, NERC CIP, WIB, and ISA 99/IEC 62443.

SecurityST Features

- Intrusion detection system
- Role-based access control
- Security Information and Event Management (SIEM)
- Password management
- Public Key Infrastructure (PKI) security certificates
- Antivirus management
- Software update service
- Backup and recovery

Backup and Recovery

- Centralized backup function with intuitive, easy-to-use visual console
- Backup functionality comes with recommended strategy for regular backups but can be easily configured to meet specific customer needs
- All backup activities are logged and easily accessed for generating reports and audit logs



Typical Security Directives

- Control system to be protected from internal and external threats
- Control system network to be segmented from other networks
- Network access points to be protected and continuously monitored; potential threats logged
- All users and devices to be authenticated and authorized given least privilege necessary
- Only GE-approved and authenticated software should be installed and run on control system components
- All control system equipment to be hardened to industry standards and best practices
- System to be continuously monitored for unusual system activity and known cyber attack signatures
- Software security updates applied to control system components on a regular and as-needed basis
- System to include Multiple defensive and detection measures provided
- Fail safe — failure of security features will not impact system operations

Unified Threat Manager (UTM)

- Monitors the control system network for known attack signatures and unusual network activity and notifies of potential threats
- Provides easy-to-configure firewall rules engine to analyze and tune for a customer's unique network traffic
- Allows selected network traffic to be logged to the SIEM for use in ongoing network analysis
- Monthly updates of Intrusion Detection signatures provided by GE as part of its software update subscription

Role-based Access Control

- Enforces best practice of every user having a unique user name and password
- Access to controllers requires multi-factor authentication using PKI (security certificates)
- User access to system functions and equipment based on job function
- System duties separated into pre-defined roles with pre-defined privileges (operator, maintenance, administrator)
- All role changes and privilege escalations are deliberate actions that are logged

Password Management

- Enforces policies for Windows® password strength, life, and reuse restrictions
- Verifies every new password for compliance with customer's defined password policy and immediately rejects non-compliant passwords
- Manages multiple password policies for sets of users, groups, and levels of complexity

Security Information and Event Management

- Provides centralized function with real-time visual security status dashboard and events display
- Provides continuous monitoring of all system components
- Collects events from all system components, indexes them for quick and easy retrieval, and stores in a central location
- Provides easy-to-configure rules engine to analyze system and security events for potential threats
- Provides built-in reports for configuration management review, compliance, audit trail, and regulatory reporting

Whitelisting

- Provides enhanced protection against execution of unauthorized code
- Protects against zero-day threats and advanced persistent threats
- Protects executables, system files, scripts, batch files, DLLs, and drivers
- Provides predefined, layered whitelisting policies for easy customization at site
- Supports observation mode to simplify policy updates
- Provides centralized management console to review, update, and apply site policies

Security Patch Service

- Subscription service provides monthly updates for Windows operating system and all other installed third-party software for the latest security
- All updates validated by GE to be both applicable to, and compatible with, the customer's system
- GE also provides evaluation of US-CERT criticality and estimated installation time and instructions
- Software update management and distribution to HMIs is centrally managed and automated by best-in-class solution
- The software patch solution automatically detects system configurations, determines the applicable updates, and provides an easy-to-use visual dashboard of update status. Customer can deploy and implement updates at the most suitable time

Antivirus Patch Management

- Every Windows-based HMI is continuously monitored for viruses, spyware, rootkits, Trojans, and adware. When detected, offending files are blocked
- A visual dashboard on a centralized console provides real-time status and management of all monitored HMIs, including antivirus updates and scan results
- GE provides monthly updates of antivirus signatures as part of its software update subscription
- Antivirus updates are distributed from a central console and can be configured to meet customer policies

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

GEA-S1292A Issued: March 2013 Revised: July 2014