Cyber Security Management System for Mark VIe Control

fact sheet

GEA-S1289B

As a global leader in automation and control for the power utility industry, GE provides state-of-the-art control solutions that seamlessly merge security management and protection as a fundamental element of the Integrated Control System (ICS) architecture for the power plant.

The Cyber Security Management System meets rigorous compliance mandates, and protects the ICS against continuously increasing security threats. It helps to implement effective security policy to ensure system confidentiality, integrity and availability at all times, providing real-time change monitoring and audit capabilities.

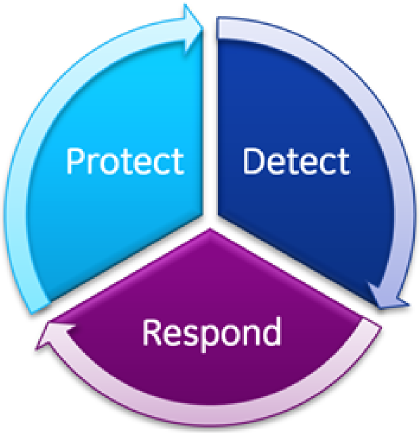
The solution consists of three complementary protective measures against cyber attacks:

- Cyber-hardened control system components
- A set of best-in-class security features
- Security software patch service for Mark VIe control

Protect. Layered security measures to protect against internal and external cyber threats

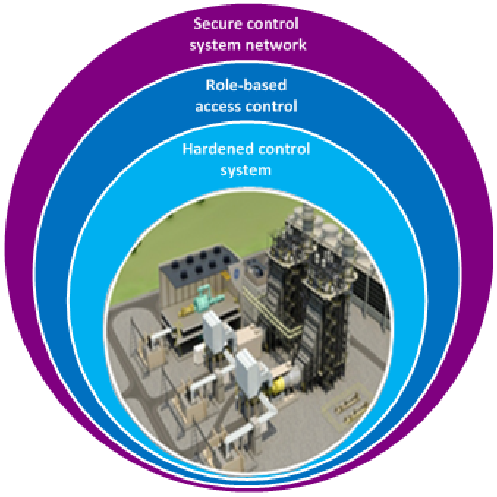
Detect. Real-time detection of security events in Mark VIe control

Respond. Swift and appropriate notification of detected security events



Features

- Easy integration into broader plant-level security
- Compliance reporting
- Network segmentation
- Centralized role-based account management
- Public Key Infrastructure (PKI) for controller protection
- Appliance-based Network Intrusion Detection systems (NIDS)
- Security information and event management (SIEM)
- Enterprise virus and malware detection, and quarantine
- Hardened Human-machine Interfaces (HMIs), controllers, and network switches



Security System Configuration

The security system provides secure control system operations that are aligned with key security industry best practices. GE provides a world-class defense-in-depth solution for its turbine, plant, and generator controls environments. Using multiple, defensive services and technologies, the solution 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.

Secure Network Architecture

The control system network is protected by several layers of defense. The first layer prevents unauthorized network access. All administrative access to the network devices is controlled using the centralized access and account management tool, Microsoft® Active Directory® Domain Services with RADIUS.
The second layer monitors firewall and network traffic for known cyber-attack patterns and abnormal traffic using an Intrusion Detection System (IDS).

The final layer is at the network switch. GE provides robust Cisco® switches, which have been cyber-hardened in accordance with National Security Agency (NSA) guidelines and Cisco best practices. Only switch ports and services necessary for normal and emergency control system operations are enabled.

Secure Controller Operations

Command and control over plant equipment is protected by layers of security measures built into GE controllers and the equipment that interacts with them. The security design restricts controller access to authorized users only. Security certificates provide two-way authentication.

The controller is protected by operating system hardening, a native whitelisting function, and a code integrity checker, which allows only authenticated code to be installed and run. The Mark VIe controller is certified through Achilles® Certification Level 1.

Secure Human-machine Interface (HMI) Operations

HMIs are the gateways to the control system. The Microsoft Active Directory Domain Services with RADIUS tool enforces the security policy on each HMI to prevent both unauthorized user access and unauthorized configuration changes. Weak and default passwords are detected and prohibited. After authentication using a proper password, a user is assigned the least privilege necessary for the assigned role. All privilege escalations are logged by the system.

Each HMI has its ports, services, and installed applications reduced to those required for normal and emergency operations only. Windows® 7 and Windows Server® 2008 R2 operating systems have been cyber-hardened using industry security best practices and industry standards.

Security Information & Event Management

SIEM continuously collects events from control system components, network devices, and security equipment. It then indexes them for quick retrieval, and stores them in a centralized location. This enables disparate and time-separated events to be analyzed for potential security threats. SIEM also provides a robust reporting tool to assist in compliance and regulatory reporting. The event data flow can be easily integrated into the existing SIEM.

Antivirus Patch Management

Antivirus and malware protection detects and removes viruses, spyware, rootkits, Trojans, and adware to prevent security-related attacks.

The malware protection for all HMIs is managed from a centralized console, and updates are controlled and dispatched. Connection to the Internet is not required to receive updates. The central console provides a dashboard to monitor protection status and events for all protected devices. A comprehensive reporting functionality assists with compliance and regulatory reports.

Security Patch Service

Releasing security patches at regular intervals is the best practice to combat evolving security threats. As part of its security solution, GE has established a service of validated and documented security software patches. This service allows the customer to control which patches are deployed, to what equipment, and when. It also provides a comprehensive update status through a color-coded status console. Patch reports provide US-CERT criticality, compatibility, estimated install time, and indicate whether a restart is required.

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

GEA-S1289B Issued: Sept 2012 Revised: July 2014