GE Oil & Gas

GEA32435A
March 2016

IEC 62443-2-4 Cyber Security Capabilities

Cyber Security for IEC 62443-2-4

Standards Background

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 systems 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 Oil & Gas Support for IEC 62443-2-4

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. This paper presents an overview of GE's hardening capabilities that meet IEC 62443-2-4 standards.

ISO 27002 Support

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.

Security Services and Solutions

GE provides security consulting services to asset owners and operators in the oil and gas sector. We also provide technical solutions designed and tested for the industrial controls environment. Our solutions are built with security in mind, and are readily integrated into broader plant-level systems and IT architectures. Together with Wurldtech Security Technologies, GE offers certified security services for the integration and maintenance of these solutions.

GE's solutions relevant to IEC 62443-2-4 include the following:

SecurityST* Mark* VIe Solution and Commissioning Services

This solution set is Achilles® Practiced Certified – Bronze. This indicates that GE has met strict cyber security best practices, including demonstrating the ability to configure and maintain the solution for secure operation. The solution is built to support best practices in security and to facilitate more efficient compliance to IEC 62443-2-4.

Cyber Asset Protection (CAP) Software Update Subscription and SecurityST Appliance

This solution set provides multiple capabilities to support cyber security best practices. Functionality includes centralized patch management, anti-virus/host intrusion detection updates, centralized account management, logging and event management, intrusion detection, whitelisting, and automated backup.

Wurldtech OpShield Technology

This solution is designed to protect critical infrastructure, control systems and operational technology (OT) assets. It monitors and blocks malicious activity and misconfiguration, providing easy-to-apply controls for network segmentation and improved visualization of the Electronic Security Perimeter. It helps mitigate the exploit of known equipment vulnerabilities as operators await vendor patches or patch maintenance windows.

These solutions offer an extensive list of features and benefits that are not fully documented in this standards specifications paper. For complete solution functionality information, review solution fact sheets located on our websites: www.gemeasurement.com and www.wurldtech.com.

GE's solution capabilities relevant to IEC 62443-2-4 are further specified in the following section.

GE's Capabilities Supporting IEC 62443-2-4

The following table provides an overview of GE's IEC 62443-2-4 supported capabilities and related functionality.

Service Type	GE's Cyber Security Capabilities	
Solution Staffing	Capabilities relate to staffing of automation solutions by service providers. All certification applications must include this conformance block.	• GE Oil & Gas staffs a Product Security team to drive security improvements across our solutions and processes.
		• We have various security subject matter experts to support applicable security solutions and services.
		• Our team maintains a training plan to share security staff knowledge.
		– The training plan identifies roles, training for those roles, and staff members identified for training.
		– Training is conducted on a recurring basis.
Solution Hardening	Capabilities relate to reducing automation solution attack surface, including risk assessments, detection of threats and vulnerabilities, and management of USB ports.	• GE's solutions begin with security-segmented reference architecture and hardening measures designed to reduce exposure to security threats.
		– System hardening evaluations specific to the security environment and policies of each customer are conducted.
		– Firewall and IDS placement and their rules are specified as part of the architecture.
		– Switches can be locked down.
		– Unnecessary ports, services, and programs are removed or disabled from workstations, servers, and controllers, thus eliminating them as an avenue of attack.
		– Workstations employ session locking for protection while unoccupied.
		– Identification of missing security patches is automated.
		– Workstations and servers employ anti-virus software and capabilities for validating and installing the latest virus definition files.
		– Procedures ensure that portable media used during integration and maintenance are authorized, virus-free, and not used for other purposes.
		– Network security and robustness testing is conducted on products used in solutions to ensure reliability and integrity.

Service Type	GE’s Cyber Security Capabilities	
Network Security	Capabilities relate to supporting the segmentation and administration of networks.	• GE has a documented network security architecture that can be tailored to customer needs.
		• Secure remote access connectivity is customized upon request, typically through a combination of RDP firewalls and access controls. SecurityST supports administration of network devices and enforces two-way authentication and encryption of network administration traffic.
		• Our network security architecture segments the plant network from the control system by a firewall and Intrusion Detection System (IDS) configured with recommended rules.
		• Cyber Asset Protection (CAP) Subscription Service and SecurityST include Host Intrusion Detection (HIDs) and anti-virus. SecurityST also includes Network Intrusion Detection (NIDs).
		• Our network security architecture protects internal interfaces with managed switches that can be locked down.
		• Wireless access is prohibited on the control system network.
		• Our control systems are designed and installed to reduce interactions between networks, specifically the supervisory/HMI network, the control network, and I/O networks. The I/O network, where control system I/O is located, is physically separated from all other networks.
User Security	Capabilities relate to supporting the administration of operating system security and user accounts.	• SecurityST provides centralized, role-based access control for both Windows workstations/servers through Active Directory servers running on redundant domain controllers. Active Directory centralizes management of user accounts and machines, as well as provides additional security constraints for managing functional isolation.
		• RADIUS servers integrate with Active Directory to control access to non-domain based elements (such as network switches, firewalls, and NIDs).
		• SecurityST ships preconfigured with a default set of devices, users/passwords, and groups to which both new and default users/devices are assigned. Groups represent roles of users and devices and define an appropriate set of privileges and restrictions for them.
		• Default passwords are configured to be changed on first use to ensure they do not become part of the operational system. In addition, we recommend local and domain user passwords be configured to automatically expire after a set interval. With Active Directory, users will be prompted to change passwords prior to expiration.
		• GE removes all temporary accounts used to deploy or maintain the system once they are no longer needed, and further recommends that all unnecessary accounts, such as “back-door,” “super-user,” and “guest” accounts be removed or disabled prior to system operation.

Service Type	GE's Cyber Security Capabilities	
Application Security	Capabilities relate to specific control and monitoring features of the automation solution.	• Configuration of the delivered solution, including architecture drawings and component version numbers, is maintained throughout the solution lifecycle with a combination of automated and manual procedures.
		• Two-way authentication and encryption for HMI access to the Mark VIe controllers is provided by the SecurityST Certificate Authority Server.
		• Configuration of control system parameters is provided through downloads to the Mark* VIe controller. ControlST* and Cimplicity* software enforce rules for development of these downloads. SecurityST User Security limits the ability to create and perform downloads to authorized users at HMI workstations.
		• Configuration downloads set value ranges for runtime parameters, such as setpoints, to ensure operators are unable to dynamically set them to unsafe or undesirable values.
		• Historians can be configured to collect runtime data and events to support process analysis and security forensics. Data collected can be compared to previous values to determine where changes have occurred in the system. The changes can be analyzed and corrective or approval actions can be taken.
Security Information and Event Management (SIEM)	Capabilities relate to supporting the management of security-related information and events, generally for the purpose of security incident handling and forensics.	• GE's Product Incident Response team follows a formal process for notifying customers of vulnerabilities discovered in its products.
		• A SIEM system provides a customizable, comprehensive logging and report generation capability.
		• The SIEM supports logical grouping of managed assets, providing the ability to create customizable reports based on event types.
		• The SIEM includes HMI security logs from GE's ICS and security event logs for network equipment, such as logon and logoff and configuration change events. For example, unsuccessful login attempts are logged for HMIs and networking devices (NIDs, firewall, switches, etc.).
		• The SIEM logs NIDs, HIDs and anti-virus security monitoring activities. These logs capture events associated with information flows to help operators with real-time detection and notification of malicious activity.
		• The Mark VIe and SecurityST solution also logs state changes and provides standard event reporting interfaces that provide secure event notification.
		• Custom SIEM reports can be easily generated to support event correlation and review, allowing for rapid incident response.
		• We will work with the customer to define the SIEM logging policy and fine tune event correlation based on defined types of events across user roles, origin host, impacted host, application, alerts on unauthorized or suspicious activity, and other measurements for audit log reduction.

Service Type	GE’s Cyber Security Capabilities	
Patch Management	Capabilities relate to supporting the validation and installation of security patches.	• SecurityST provides a centralized service to audit and deploy security patches.
		• The SecurityST patching service lab tests and validates all patches for compatibility with the Mark VIe and SecurityST solution before patches are released.
		• GE provides documentation on the SecurityST patching service, including recommended and documented rollout procedures, patching procedures process, workarounds for unapproved patches, and mitigation strategies.
		• Patches are provided monthly via DVD to prevent unnecessary opening of network ports and services required for online distribution. DVDs are distributed using tamper-evident seals and are scanned upon arrival at the customer site.
		• The CAP Patch Applicability report defines criticality information, time required for update and if a reboot is necessary.
Backup/Restore	Capabilities relate to supporting the backup and restore functions of the automation solution and its components.	• SecurityST provides documentation for the backup/restore of computers, networking devices, and other components, including scheduling of backups.
		• GE provides a Backup Architecture document that describes storage of onsite backups and provides recommendations for offsite storage. Encryption of backups and their archives is supported.
		• SecurityST provides scripts for configuring and customizing backup configurations. Instructions are provided for adding new components and creating additional backup plans. SecurityST backup capabilities are designed to operate during normal plant operations. The bandwidth of the backups is set to minimize network resources.

Imagination at work

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

www.gemeasurement.com/machinery-control