GE Oil & Gas

NEI 08-09 Cyber Security Capabilities

Cyber Security for NEI 08-09

As a vendor of industrial controls, GE embraces its responsibilities to assist critical infrastructure owners to improve their security postures and support compliance efforts as they relate to GE-provided equipment. GE supports customer compliance efforts by providing cyber security solutions and documentation for current and certain legacy controls.

Standards Background

NEI 08-09 is a cyber security plan for nuclear power reactors published by the Nuclear Energy Institute. The purpose of the plan is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" are implemented at nuclear sites. Further, 10 CFR 50.34(c)(2) requires those who apply for an operating license for a utilization facility must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54. NEI 08-09 establishes the licensing basis for the Cyber Security Program for these sites.

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

GE hardens customer systems using a combination of technical and procedural measures that are encouraged in NEI 08-09. This paper presents an overview of GE's hardening capabilities as well as other procedural capabilities that meet NEI 08-09 standards.

Security Services and Solutions

GE provides security consulting services to asset owners and operators in the nuclear 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 NEI 08-09 include the following:

SecurityST* Mark* VIe Solution and Commissioning Services

This solution set is Achilles® Practiced Certified for IEC 62443-2-4. 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 international standards.

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, application 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.

GE's solutions support confidentiality, integrity and availability of critical controls and related networks, which in turn can be applied to support owner compliance towards NEI 08-09. 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 Capabilities Supporting NEI 08-09

The following table provides an overview of GE’s NEI 08-09 supported capabilities and related functionality.

1.0	Access Controls	
1.2	**Account Management**	SecurityST uses Active Directory (AD) to centrally create and manage all user, service and application accounts associated with computers and users in the HMI Domain. All accounts are assigned to GE-specific Active Directory Groups to ensure access rights are job function based. If a user job function changes, the user can be moved into or added to a new Group to support new access requirements. All account management functions, such as limiting account access rights; terminating temporary, guest and emergency accounts within set time period of inactivity; disabling inactive accounts; and creating, protecting audit records for account creation, deletion, and modification are included with Microsoft® Active Directory capabilities.
1.3	**Access Enforcement**	SecurityST’s Active Directory Server supports Role Based Access Control to enforce policies that are assigned based on “least privilege.” In addition, controller-based policies are supplied to enforce controller access restrictions on Mark VIe and EX21000e controllers running in secured state.
1.4	**Information Flow Enforcement**	SecurityST includes redundant firewalls to assist in the enforcement of information flow. Session enforcement between the controllers and the HMI is provided by the Certificate of Authority Server, and prioritization of flows is handled with Quality of Service on the switches. In addition to switches and standard firewalls, Deep Packet Inspection firewalls such as GE’s OpShield can further enhance the capabilities through filtering (monitoring and blocking) OT-specific protocols such as Ethernet Global Data (EGD) between HMIs and controllers.
1.5	**Separation of Functions**	GE SecurityST uses security groups in Active Directory to assign and enforce user privileges within User Groups using Group Policies. Users within the HMI domain are assigned to the appropriate group that is required for their job.
1.6	**Least Privilege**	GE models best practices by using the principle of least privilege when defining roles and assigning users to roles through Active Directory groups and group policies. SecurityST supports Role Based Access Control to enforce policies that are assigned based on “least privilege.”
1.7	**Unsuccessful Login Attempts**	The SecurityST Active Directory Group Policies and Security Information Event Management (SIEM) solution address the requirement to enforce limited number of invalid login attempts and logging. The policy can be adjusted to meet customer requirements.
1.8	**System Use Notification**	SecurityST Active Directory Group Policies support this requirement on all domain computers, and can be customized to meet frequency, content and configurability needs. In addition, GE supplied routers, switches and NIDs devices can be configured to meet this requirement.
1.9	**Previous Logon Notification**	SecurityST Active Directory Group Policies support this requirement, and can be configured per customer requirement or request. By default, this is not included in the AD Group Policies.
1.10	**Session Lock**	SecurityST Active Directory Group Policies support this requirement. Although not a default configuration, GE can configure per customer request to automate the session lock. Group policies also will allow users to initiate a session lock manually. Please refer to 4.4. as Session Lock must not hinder safety.
1.11	**Supervision and Reviewer-Access Control**	SecurityST Active Directory and SIEM provide the technical capabilities to support this requirement. GE will configure the systems to meet customer requirements as well as support the review of user activities to detect security-related issues.

1.0	Access Controls	
1.15	**Network Access Control**	During SecurityST implementation, all associated network switches are hardened including configuration for media access control address locking to address this cyber security control requirement.
1.16	**"Open/Insecure" Protocol Restrictions**	GE's Mark Vie Control System uses Ethernet Global Data (EGD) proprietary protocol, which by default is open and insecure. By implementing Secure State communications in ControlST and SecurityST, all control commands are encrypted and group policies enforce Role Based Access Control verifying the identity of the user and the actions they can perform. Using Deep Packet Inspection firewalls such as GE's OpShield can further enhance this requirement to mediate or restrict protocol exchanges.
1.20	**Proprietary Protocol Visibility**	GE's Mark Vie Control System uses Ethernet Global Data (EGD) proprietary protocol. This protocol is restricted to GE's control system network (UDH). By implementing Secure State communications in ControlST and SecurityST, all controllers send log events to the SIEM. Using Deep Packet Inspection firewalls such as GE's OpShield can also be used to further enhance security using monitoring and filtering on protocol commands. This event information can then be supplied to the SIEM to support visibility.
1.21	**Third-Party Products and Controls**	SecurityST Active Directory Group Policies are configured to deny operators rights from installing software on the HMIs. In addition, SIEM can be configured to detect and report on software installed by authorized users.
1.22	**Use of External Systems**	GE has a documented network security architecture design that can be tailored to meet NEI 08-09 and RG 5.71 requirements.

2.0	Audit And Accountability	
2.2	**Auditable Events**	SecurityST's Security Information Event Management (SIEM) provides a fully automated logging solution for all of GE's associated Mark VIe Control CDAs. This scalable solution includes logging of all cyber activities such as login events, configuration changes, privileged access and more.
2.3	**Content of Audit Records**	SecurityST's SIEM allows for centralized log and event management of devices within the network, using a comprehensive and configurable attribute set that includes synchronized time stamp.
2.4	**Audit Storage Capacity**	SecurityST's SIEM provides for configurable storage capacities and retention settings based upon the types of customer-defined auditable events, alarms, event correlation, and associated documentation.
2.5	**Response to Audit Processing Failures**	SecurityST Active Directory and SIEM will be configured to align with customer policies. Notifications can be customized for recipients and methods of notification.
2.6	**Audit Review, Analysis, and Reporting**	The SIEM system provides an automated mechanism to centrally collect and audit logs, allowing rapid review and analysis. Customized dashboards can be created in the SIEM to assist the customer with reviewing, analyzing and managing the logs as needed on request.
2.7	**Audit Reduction and Report Generation**	The SIEM system provides audit reduction and report generation capabilities for all associated CDA equipment including but not limited to GE's Mark VIe controllers, HMIs, HIDs and NIDs, anti-virus security monitoring activities, and network device activities. GE 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.

2.0	Audit And Accountability	
2.8	**Time Stamps**	GE can work with the customer if necessary to configure Network Time Protocol (NTP) communications securely. The time source solution can use either GE or customer-provided time source such as Secure Network Time Protocol (SNTP). GE recommends that the time source be restricted to the same security zone as the controllers, not through an external network service.
2.9	**Protection of Audit Information**	SecurityST Active Directory role-based access control provides user access to the SIEM appliance and data. Only authorized users are provided with user or administrator access to the data. The data is also backed up on two separate devices to ensure it can be recovered as part of standard GE Disaster Recovery processes.
2.10	**Non-Repudiation**	SecurityST SIEM captures and stores logs from all Windows Servers, HMIs, Controllers, VM Hypervisor and network devices. All devices and computers are time synchronized. SecurityST Active Directory Group Policies are configured to log all required security information to ensure all user actions are captured, thus ensuring non-repudiation. All CDAs and audit records are physically and administratively secured. The audit records are also backed up to further protect the data.
2.11	**Audit Record Retention**	SecurityST SIEM and Active Directory can be configured for audit record retention. GE will configure the system to meet customer and regulatory requirements. The solution is designed to typically store up to three years of SIEM log data with default configuration.
2.12	**Audit Generation**	SecurityST SIEM provides audit record generation and allows authorized users to refine list of auditable events to be included in report generation. Reports are time stamped to allow for correlation across disparate devices.

3.0	CDA, System and Communications Protection	
3.2	**Application Partitioning/Security Function Isolation**	The SecurityST Active Directory user and management functions can be used to limit functions for operators while enabling security functions for administrative users only. There is physical partitioning in the network levels between the Control Network (UDH) and the Supervisory Network (PDH). In addition, the control system I/O network is physically separated from all other networks with role-based access to the controller provided.
3.4	**Denial of Service Protection**	All of GE's Mark VIe and EX2100e controllers are Achilles Communication Certified, thus ensuring that if such an attack did occur, the controllers would maintain critical functionality during this time. The SecurityST base configuration includes endpoint protection with Host Intrusion Detection to detect and log such events. Optional components include Network Intrusion Detection and Prevention appliances as well as Application Whitelisting to prevent such attacks from occurring.
3.5	**Resource Priority**	GE's HMIs and Servers rely on Windows System Resource Manager which includes five built-in resource management policies customers can use to quickly implement management. In addition, GE can assist in creating custom resource management policies to meet the customers' specific needs to manage system resources (processor and memory). Network switches also use Quality of Service (QoS) to prioritize network resources and ensure controller traffic has the highest priority. GE's Cyber Asset Protection (CAP) subscription solution has a secured network design that segments control network traffic from other network traffic and guarantees the per forma need of the control network by prioritizing the control network traffic over supervisory traffic via QoS which relegates non-control network traffic to best effort delivery.

3.0	CDA, System and Communications Protection	
3.6	**Transmission Integrity**	SecurityST includes a Certificate Authority Server with security certificates supporting transmission integrity and authenticated access between the HMIs and controllers, allowing the Mark VIe Control System and EX2100e Generator Excitation to operate in secure state during normal operations. In addition, all associated network switches and firewalls are hardened during commissioning of SecurityST to prevent “man-in-the-middle attacks” and ARP poisoning as well as transmission monitoring which is sent to the SIEM.
3.7	**Transmission Confidentiality**	The SecurityST Certificate Authority solution supports transmission confidentiality and authenticated access between the HMIs and controllers, allowing the Mark VIe Control System and EX2100e Generator Excitation to operate in secure state during normal operations.
3.8	**Trusted Path**	SecurityST requires Active Directory and Radius for access and authentication to network security devices which are not members of the domain. Active Directory supplies the trust of identification and authentication to Windows security applications.
3.10	**Unauthorized Remote Activation of Services**	GE’s Controls and SecurityST solution does not include any collaborative computing hardware or software on any devices in the Supervisory Controls or Controls networks. All systems are hardened and protected through Active Directory Role Based Access Control.
3.11	**Transmission of Security Parameters**	Windows WCF and DCOM protocols incorporate Kerberos and the transmission of security tokens to protect connections between applications. GE ensures that these capabilities are appropriately configured during installation of the system.
3.17	**Session Authenticity**	SecurityST includes a Certificate Authority Server to help establish transmission integrity and provide authenticated access to the controller, allowing the Mark VIe and EX2100e to operate in secure state during normal operations. The Certificate of Authority Server maintains session authenticity between the controller and the HMIs. In addition, the network firewalls, NIDS, and V-LAN switch control support session authenticity.
3.19	**Confidentiality of Information at Rest**	HMI local security policy can be configured to restrict access of file-based information to authorized users. Additionally, file data encryption can be enabled to support data security in the event of theft. SecurityST includes a centralized backup tool that can be configured to back up encrypted data to the SecurityST to protect the confidentiality of information at rest. To increase the security of confidential data, the backup archive can be encrypted with the strong, industry-standard Advanced Encryption Standard (AES) cryptographic algorithm.
3.20	**Heterogeneity**	The SecurityST design employs multiple layers of defense in our solution to address this requirement. At a high level, these include Role-Based Access Control; Encryption and Authentication between HMIs and Controllers; Host Intrusion Detection; Network Intrusion Detection; Whitelisting OT protocols; Universal Threat Management; Patch Management of Windows, Network Devices, Applications and Controllers; Network Architecture (redundant and segmentation); SIEM; Hardening Operating Systems, Network Infrastructure and embedded systems; and a Disaster Recovery Backup/Restore solution.

4.0	Identification and Authentication	
4.2	**User Identification and Authentication**	SecurityST's Active Directory employs centralized user identification and authentication to uniquely identify and authenticate individuals and processes acting on behalf of users. The SecurityST domain is physically and logically segmented in the Supervisory Control network. No external trusts are provided to outside security zones.
4.3	**Password Requirements**	SecurityST implements role-based access control and controls inbound access. The solution uses an integrated Password Policy Enforcer to enforce granular password policies for Windows: minimum password strength and password lifetimes and reuse restrictions. Network components, including switches, firewalls and intrusion detection system authenticate to Active Directory.
4.4	**Non-Authenticated Human Machine Interaction (HMI) Security**	For Control Room HMIs, SecurityST Group Policies are configured for no session lock to ensure SSEP functions are not affected by authentication, session lock or session termination controls. All HMIs are also audited through Group Policies and SIEM.
4.5	**Device Identification and Authentication**	SecurityST Active Directory provides for domain based communications between Windows systems which addresses device identification and authentication. In addition to Active Directory, SecurityST Certificate Authority provides for device identification and authentication between the HMIs and Controllers.
4.6	**Identifier Management**	SecurityST uniquely verifies the identity of users and can disable user accounts within 31 days of inactivity. Active Directory authenticates centralized access and account management.
4.7	**Authenticator Management**	SecurityST can authenticate passwords based on length and composition. Multi-factor authentication via RADIUS, RSA token, or authentication key is supported through Active Directory. Active Directory also provides centralized access and account management. Password complexity has already been addressed, and by default, configures the complexity for length, use of upper and lower characters, expiration, etc. By default, tokens and keys are not included but can be configured upon request. The hand-over process of SecurityST includes changing all passwords by the customer.
4.8	**Authenticator Feedback**	SecurityST obscures feedback of authentication information during the authentication process through Active Directory. In addition, password characters entered by the user are not displayed. All password transmission protocols are secured (SSH, Active Directory, SSL, etc.)

5.0	System Hardening	
5.1	**Removal of Unnecessary Services and Programs**	GE's HMIs and controllers are configured and hardened through SecurityST Active Directory Group Policies using industry guidelines and standards such as NIST 800-52 and NSA, as well as, industry accepted third-party accreditations. GE provides lists of ports, services, and programs that allow the user to document and track services, programs, drivers, and ports in use or installed on HMIs and servers. With the inclusion of the CAP subscription service, all systems are patched on a monthly basis. Validation testing and flaw remediation is performed in a secure lab prior to distributing to customers. 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
5.2	**Host Intrusion Detection System (HIDS)**	The GE SecurityST Endpoint Protection solution includes HIDs protection. All Windows Servers and HMIs within the HMI domain are installed and centrally managed to monitor and alert against malicious or anomalous activity. The CAP subscription service includes HIDS definition updates and patches to maintain the level of system security as new security issues are identified. These updates and patches are tested in a lab environment prior to being deployed on customer production systems to ensure the safety, security and emergency preparedness functions of the CDAs are not impacted.
5.3	**Changes to File System and Operating System Permissions**	SecurityST's Active Directory Role Based Access Control is configured to enforce policies that are assigned based on "least privilege." This ensures that users only have rights required to perform their job. In addition, all rights to make changes to the controllers is also restricted using Active Directory Group Policies and Certificates.
5.4	**Hardware Configuration**	Hardware configuration includes the disabling of communication ports and removable media drives. GE's solution includes role-based USB port control that can be configured based on customer requirements. CD/DVD devices are needed for software installation and disaster recovery backup. During normal operation, these devices can be disabled, and administrators can re-enable them as needed. BIOS passwords on HMIs are configured upon request.
5.5	**Installing Operating Systems, Applications, and Third-Party Software Updates**	The CAP subscription service includes a Patch Applicability Report which inventories the system for current revision levels, defines which updates are applicable, update status, associated US-CERT criticality/security ratings, whether a reboot may be required, and the estimated time required for patch installation.

8.0	Cyber Security Contingency Plan (Continuity of Operations)	
8.1	**Contingency Plan**	SecurityST provides centralized, automated and operator acknowledged, rule-based, backups and documentation to support restoration. The solution can be implemented in a redundant, high-availability mode with redundant hardware and applications. The solution provides logs to demonstrate completion of backups.

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