GE Oil & Gas

Cyber Security for NERC CIP Versions 5 & 6 Compliance

Contents

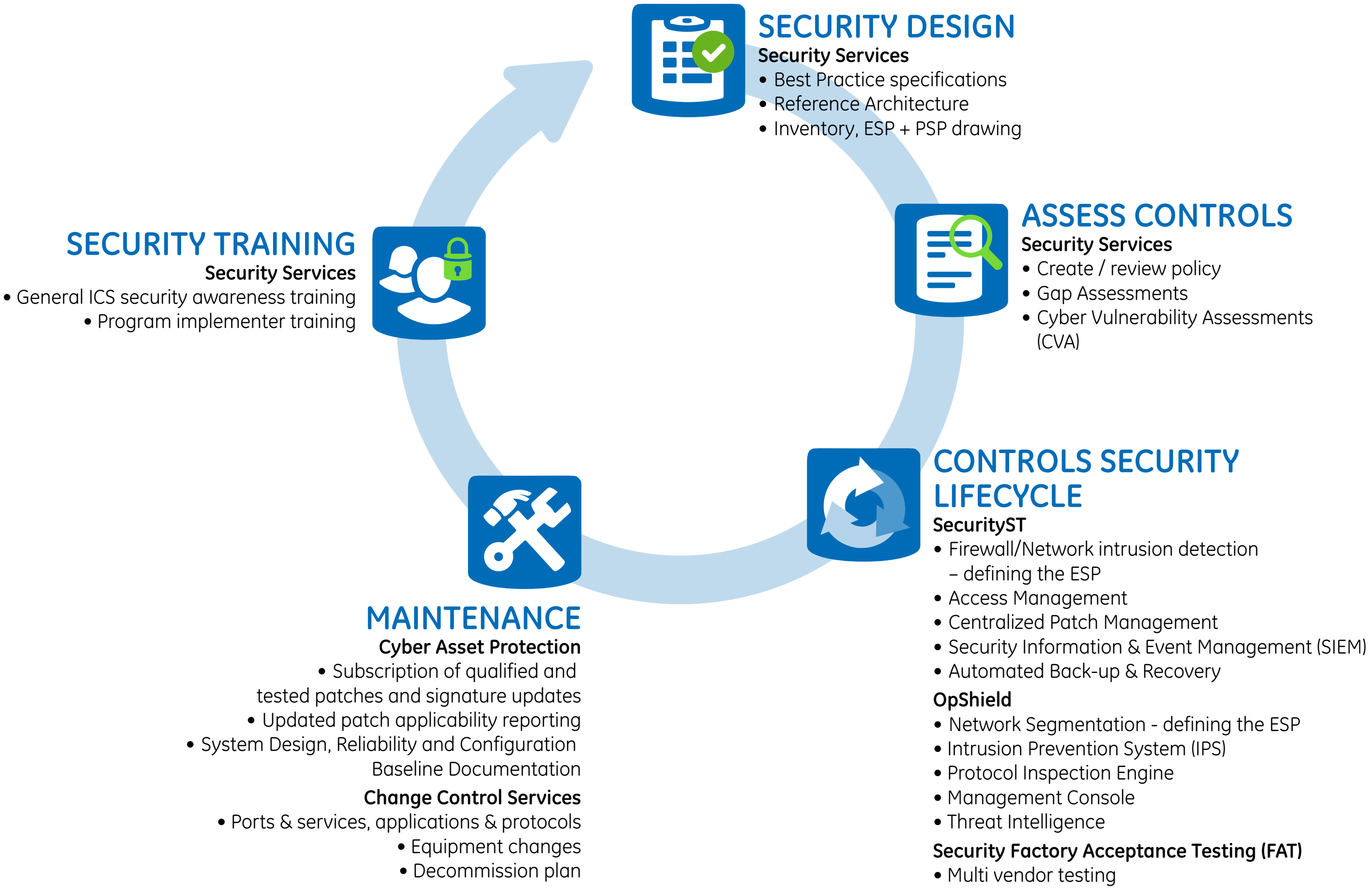
GE Proprietary Information: This document contains proprietary information of the General Electric Company and may not be used for purposes other than that for which it was originally furnished except with written permission of GE Oil & Gas.

Cyber Security for NERC CIP Versions 5 & 6 Compliance

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology. Version 6 requires compliance by July 2016 (high and medium impact BES) or July 2017 (low impact BES). To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance.

As a vendor of industrial controls, GE embraces its responsibilities to assist critical infrastructure owners as they improve their security postures and support compliance efforts related to GE-provided equipment throughout the 10 to 20 year lifecycle of the control system itself. Together with Wurldtech Security Technologies, GE is able to offer security support that spans from initial system design to commissioning, all the way through ongoing support and maintenance.

GE offers professional security services and operational technology (OT) security solutions designed and tested for the industrial controls environment. Our trained Operational Technology Security professionals can support in areas including design, assessments, policy development and training. Built to support best practices in security and facilitate more efficient compliance to NERC CIP 5 & 6, GE's Cyber Asset Protection (CAP) Software Update Subscription and SecurityST appliance provide centralized patch management, anti-virus/host intrusion detection updates, centralized account management, logging and event management, intrusion detection, whitelisting and automated backup. OpShield is purpose-built technology to mitigate known industrial vulnerabilities, providing easy-to-apply controls network zoning and improved visualization of the Electronic Security Perimeter.



SECURITY DESIGN

Security Services
- Best Practice specifications
- Reference Architecture
- Inventory, ESP + PSP drawing

ASSESS CONTROLS

Security Services
- Create / review policy
- Gap Assessments
- Cyber Vulnerability Assessments (CVA)

CONTROLS SECURITY LIFECYCLE

SecurityST
- Firewall/Network intrusion detection – defining the ESP
- Access Management
- Centralized Patch Management
- Security Information & Event Management (SIEM)
- Automated Back-up & Recovery

OpShield
- Network Segmentation - defining the ESP
- Intrusion Prevention System (IPS)
- Protocol Inspection Engine
- Management Console
- Threat Intelligence

Security Factory Acceptance Testing (FAT)
- Multi vendor testing

MAINTENANCE

Cyber Asset Protection
- Subscription of qualified and tested patches and signature updates
- Updated patch applicability reporting
- System Design, Reliability and Configuration Baseline Documentation

Change Control Services
- Ports & services, applications & protocols
- Equipment changes
- Decommission plan

SECURITY TRAINING

Security Services
- General ICS security awareness training
- Program implementer training

The following matrix provides more details on GE's recommended solutions and software to support security best practices and facilitate NERC CIP compliance efforts for Mark VIe and EX2100e control families.

NERC CIP V5 & 6 Standards – GE Support for Security and Compliance

CIP Standards	GE support for security and NERC CIP 5 & 6 compliance
Sabotage Reporting CIP-001-5	GE's Incident Response policy and procedure includes 3rd party researchers, ICS-CERT, and GE's internal Product Security Incident Response Team (PSIRT). Throughout the controls lifecycle, GE customers receive Technical Instruction Letters that detail known vulnerabilities and associated remediation/ mitigation. The Security Incident Event Management (SIEM) system centralizes and correlates cyber security event data. This reporting can be used to support forensics and event reporting.
Security Management Controls CIP-003-6 R2	As the scope of the NERC CIP standards expands to include Low Impact BES Cyber Assets, GE is ready to assist. Many of our solutions available for high and medium impact BES cyber assets apply to low impact assets, including: • Training for cyber security awareness • Hardware enclosure options for physical security • Electronic Access Point solutions for Electronic Access Controls • Factory Acceptance Testing and commissioning procedures for incident response
Personnel & Training CIP-004-6 R1-R5	Wurldtech has a comprehensive portfolio of security training courses for critical infrastructure and Industrial Control Systems (ICS). The training is developed and delivered by Wurldtech's security experts, people who analyze and implement real-world security solutions at operating facilities. They bring vast experience, examples and stories to provide applicable, actionable instruction.
	Service engineers supporting your operation receive routine NERC CIP training and background checks before accessing your site's controls.
Electronic Security Perimeter CIP-005-5 R1-R2	GE's Electronic Access Point (EAP) solutions support technical and procedural mechanisms for control of electronic access to the Electronic Security Perimeter. • Operationally validate router and switch configurations • Unified Threat Management firewalls protect against IT vulnerabilities • OT protocol aware firewalls support operational zones, reinforcing permitted commands between zones and access points • Network Intrusion Detection Systems inspect inbound and outbound traffic as well as capture baseline traffic • Application whitelisting to protect computers from harmful applications
Physical Security of BES Cyber Systems CIP-006-6 R1	Hardware options include a secure physical network rack. This rack can include a key lock and/or keycard access, including electronic contact switches alerting security personnel when the rack is opened. Secure and documented Chain of Custody in development and throughout the lifecycle, including ongoing delivery of cyber security updates. These updates are transmitted to site via secure sealed shipping envelope. In addition, the CD/DVD includes a hash file to validate the CD/DVD contents have not been altered.

CIP Standards	GE support for security and NERC CIP 5 & 6 compliance
System Security Management CIP-007-6 R1-R5	GE provides and maintains a list of required listening ports and services GE provides hardened switch and HMI configurations to disable unused ports and services. Through GE's CAP subscription service, the Responsible Entity receives a complete Baseline Configuration Report for all items in our scope of supply. Each month any baseline configuration changes (for example, by security update) are reported to the Responsible Entity.
	The CAP Program includes: • Monthly validated patch lists, including any workarounds • System Design, Reliability, and Configuration Baseline Documentation • When applicable, Cyber Security Technical Information Letter (TIL) • Review of impacts to Ports and Services • CAP Security Subscription validated testing procedures certificate • Patch applicability reporting showing impact, and vulnerability assessment procedures • CAP includes ongoing monthly updates for Malicious Code Preventions including Antivirus, Operating System updates, Host Intrusion Detection and Network Intrusion Detection signatures and switch updates. All updates are tested in a representative controls environment
	OpShield provides protection profile updates that include IDS/IPS signatures for vulnerabilities. SIEM provides real-time capability that centrally alerts, logs and detects cyber security events, allowing operators to monitor unauthorized activity.
	Access controls are managed through SecurityST's centralized Role Based Access Control. GE supports individual accounts in all of our controls applications. All passwords are changed from defaults and handed over to the Responsible Entity. GE supports complete NERC password parameter requirements including: length, complexity, required password changes, limits to unsuccessful authentication attempts and setting attempt thresholds. Access controls are centrally applied to GE HMIs, routers, switches, firewalls, Network Intrusion Detection Systems and our latest controllers.
	The SecurityST Appliance includes a Certificate Authority Server (CAS) for two-factor operator authentication between GE Controllers (with ControlST 4.7 or greater) and the GE HMIs. The CAS puts GE controllers in "Secure Mode", maintaining session authenticity between GE provided controllers & the Authenticated User on domain controlled HMIs. When in secure mode, all controller access is encrypted. This enables only users with the necessary certificate on authorized HMIs to access the controller.
	The SecurityST Appliance includes a password management program that extends Microsoft Active Directory capabilities and supports NERC CIP compliant password configuration.
Recovery Plans for BES Cyber Systems CIP-009-6 R1-R2	Backup/recovery support through SecurityST and associated network topology: • Centralized dashboard for backup and recovery includes backup status, recovery tasks and alerts for backup errors. • Redundant set of MS Active Directory Domain Controllers include one as a virtual machine and the other as a physical instance. If the primary or backup domain controller were to fail, the other instance would continue to authenticate authorized users. • Use of Virtual Machines (VM) support expedited backup and recovery when backups are executed per best practice. • GE Latest Network Design includes complete redundant information flows through redundant ethernet and fiber cabling and hardware. All HMIs and controllers support redundant network connections. • Centralized configuration backup and restoration of network devices includes alerting to the • Alerting via SIEM when switch configurations change. • Switches include stacking technology enabling a stacked pair to act as one switch, providing local built-in failover and recovery in the event of a switch failure. An unconfigured switch can be used to replace a failed switch in the stack, automatically uploading the running configuration from the surviving switch. GE switch configuration includes enhanced Quality of Service ensuring controls traffic (GE Unit Data Highway) has the highest priority.

CIP Standards	GE support for security and NERC CIP 5 & 6 compliance
Configuration Change Management & Vulnerability Assessments CIP-010-2 R1, R3	GE's CAP software update subscription supports patch change management compliance documentation by generating a report that shows the following: • Listing of applicable updates to your system • Status of the update (applied or missing) • Updated reference information, including patch number, bulletin ID and bulletin title • US Computer Emergency Readiness Team (US CERT) level of severity associated with update • Time required to apply update in the representative operational test environment and whether or not a reboot is required
	OpShield can monitor or block OT-specific protocols and commands not included in the baseline configuration which will issue an alert to the SIEM.
	GE provides several options with regards to Paper and Active Vulnerability Assessments: • Wurldtech provides expertise needed to perform a NERC CIP Vulnerability Assessment at Responsible Entity site. Wurldtech follows a proven methodology tailored to industrial control, automation and other real-time systems. The result is a comprehensive assessment providing actionable deliverables that will enable the Responsible Entity to mitigate immediate risks, while developing and implementing an effective long-term security strategy that will improve the overall security posture. • Performing an Active Vulnerability Assessment during Factory Acceptance Testing (FAT), before commissioning to Responsible Entity. Includes network discovery, port and service identification, vulnerability identification and remediation. • Included with the CAP monthly patch and signature updates is an applicability report that shows which updates are applicable, their status (applied or unapplied), the severity ranking of the vulnerability and the time the update took to apply in a test environment. The CAP program also provides the Responsible Entity a paper listing of ports and services identification.
Information Protection CIP-011-2 R1-R2	During the Secure Factory Acceptance Test (FAT), GE can provide the Responsible Entity complete "information flows enforcement" – the identification of the security of each information flow, why it is permitted or denied, including the configuration of flow enforcement polices via firewalls, switches and routers. During and after commissioning, GE uses a trusted delivery path with tamper evident seals on all packaging. After commissioning, the CAP Update Subscription Program includes tamper evident seals and an encrypted hash file. The hash file is used by Responsible Entity to validate the CD/DVD electronic contents are un-altered.

For more information please contact:

GE Oil & Gas
Digital Solutions
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
http://www.gemeasurement.com