GE Oil & Gas

Top 10 Cyber Vulnerabilities for Control Systems

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.

Contents

NERC Cyber Infrastructure Protection (CIP), 10 CFR73/54/NEI 08-09, and International Instrument Users' Association Working – Party on Instrument Behaviour (WIB) Compliance 4

Vulnerability 1: 4

Vulnerability 2: 4

Vulnerability 3: 4

Vulnerability 4: 5

Vulnerability 5: 5

Vulnerability 6: 5

Vulnerability 7: 5

Vulnerability 8: 6

Vulnerability 9: 6

Vulnerability 10: 6

NERC Cyber Infrastructure Protection (CIP), 10 CFR73/54/NEI 08-09, and International Instrument Users' Association Working – Party on Instrument Behaviour (WIB) Compliance

GE's cyber security solution provides Power, Oil, and Gas customers an integrated solution to meet industry compliance mandates and to protect their Industrial Computer Systems (ICS) against the continuously increasing threat in the cyberspace with increase system integrity, availability, performance, and confidentiality; and real-time change monitoring and audit-readiness system status reports to sustaining compliance.

U.S. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."

"The security of SCADA systems used in critical energy infrastructure installations throughout the United States relies on a cooperative effort between SCADA product vendors and the owners of critical infrastructure assets. These recommendations can be used by SCADA vendors to deliver and support systems that are able to survive attack without compromising critical functionality, by SCADA integrators to configure their systems securely before they are put into production, and by SCADA owners to perform due diligence in procuring, configuring, securing, and protecting these energy delivery control systems." Idaho National Laboratory, September 2011, http://www.inl.gov

GE's cyber security solution addresses the ten common vulnerabilities of the Control Systems identified by the NERC Control Systems Security Working Group.

Vulnerability 1:	**Inadequate policies and procedures governing control system security.**
	GE works with customers for continuous improvement for implementation and enforcement of policies and procedures governing protection and control system security. GE participates in Integrated Factory Acceptance Test (IFAT). An IFAT validates hardware and software performance across multiple systems in an offline environment where any issues or complications can be mitigated before a live rollout. This best practice safeguards against in-plant failures that could be costly or insecure. GE works closely with system vendors in hardening cyber assets to be NERC/NEI/WIB compliant—for examples: take advantage of advanced management features of Windows 7, patching, appropriate use banner, no backdoor exit, syslog forwarding and event correlation.
Vulnerability 2:	**Rely on "security through obscurity."**
	GE adopts a process for continuous improvement of defense-in-depth network topology and Host-based Intrusion Prevention System (HIPS). GE's cyber security solution provides a stateful firewall which protects against unsolicited in-bound traffic and prevent intrusion via behavioral rules and signatures. Implementing a Network Intrusion Detection System (NIDS) gives system administrators better visibility of potential and actual threats. With 24/7 monitoring, analysis, and logging of network traffic, the NIDS speeds incident response time and simplifies forensics.
Vulnerability 3:	**Untimely implementation of software and firmware patches. Inadequate testing of patches prior to implementation.**
	GE has a predefined checklist to verify the proper functioning of control systems to meet regulatory requirement for adequate testing of patches. GE's monthly security patches are released on the second Tuesday of each month to provide timely risk assessment. The validated patches, updates, and signatures for the operating system and software applications installed on HMIs and other cyber assets. By replicating a client's platform in GE's technology partner, FoxGuard's secure lab environment, FoxGuard can test these updates to ensure safe and smooth deployments. Patch management is purchased as a subscription with solution disks and documentation delivered in monthly intervals. It is available for implementation at discrete control devices or across a network via a central server.

Vulnerability 4: Use of inappropriate wireless communication. Lack of authentication in the 802.11 series of wireless communication protocols. Use of unsecured wireless communication for control system networks.

GE supports encryption for administration of network devices within the control system over Ethernet and enforces two-way authentication of all network traffic (WIB BP.07.06: role-based access for network devices). GE encourages customers who use wireless communication on laptops to implement wireless fidelity protected access (WPA) encryption and 802.1x device registration along with unregistered device detection; use public key infrastructure (PKI) and certificate servers; use non-broadcasting server set identifications (SSIDs); utilize media access control (MAC) address restrictions; and implement 802.11i.

Vulnerability 5: Use of nondeterministic communication for command and control such as Internet-based SCADA. Inadequate authentication of control system communication protocol traffic.

GE implements defense-in-depth architecture of multiple firewalls between control network and other networks. GE's solution provides a stateful firewall which protects against unsolicited in-bound traffic and prevent intrusion via behavioral rules and signatures to reduce operational risk for network operations. GE will provide firmware hashes as an additional tool to verify the integrity of GE firmware files to ensure customers that the firmware received from the factory is complete and unaltered prior to sending the firmware to the vendor controlled device. Customers can use the GE portal to verify that the firmware file in their possession is a known good GE firmware release by comparing the calculated hash value of the firmware in their possession with the hash value provided on the GE Portal.

Vulnerability 6: Poor password standards and maintenance practices. Limited use of virtual private network (VPN) configurations in control system networks.

GE implements role-based access control. GE's solution provides an integrated protocol anomaly-detection and active response technology, behavior-based HIPS to protect VPNs. It provides an integrated Password Policy Enforcer to enforce granular password policies for Windows for NERC CIP-007 R5 and WIB BP.20.03: minimum password strength and BP.20.04: password lifetimes and reuse restrictions.

For networked devices, GE assists with the configuration of an Access Management console to regulate logons, set user and group permissions, and strengthen security policies (e.g., password parameters and session locks) as part of IFAT to increase overall accountability and authorization control and reduces the time and resources needed to manage user accounts.

Vulnerability 7: Lack of quick and easy tools to detect and report on anomalous or inappropriate activity among the volumes of appropriate control system traffic.

GE's security solution includes Network Intrusion Detection/Prevention device (NIDS) and Security Incident and Event Management (SIEM) with event correlation appliance for monitoring virtual devices and enable SNMPv3 privacy/encryption method as required by NEI and WIB BP.10.03 Log and event management. SIEM aggregates data from many sources – including firewalls, applications, databases, etc. – and presents it from a single interface using graphical dashboards. SIEM determines potential threats by correlating this data and instantaneously detects incidents through automated log file parsing. Autorun is a major infection threat vector identified by National Institute of Standards and Technology (NIST) and Nuclear Energy Institute (NEI). GE encourages customers to disable autorun as a best practice.

Vulnerability 8: Dual use of critical control system low bandwidth network paths for noncritical traffic or unauthorized traffic.

GE's security solution includes Network Intrusion Detection/Prevention device (NIDS) and SonicWall NSA 240 Unified Threat Management (UTM). During the Integrated Factory Acceptance Test (IFAT) GE works with customers in defining critical network paths and work on fine-tuning NIDS to evaluate network traffic and control system point counts and polling rates. SIEM provides analytical data for optimizing existing resources for critical network paths and fine-tuning prevention devices against protocol anomalies.

Vulnerability 9: Lack of appropriate boundary checks in control systems that could lead to "buffer overflow" failures in the control system software itself.

GE's solution monitors applications and critical address space for buffer overflow protection. The NETCAP system is designed to operate during normal plant operations. The bandwidth of the backups is set to 10 percent to minimize network resources, patches are set to never reboot the machine, so that the operators can schedule the reboot as needed. This design is tested as part of the Factory Acceptance Test (FAT). The SIEM is collecting logs at all times, but does not impose any noticeable impact to the network bandwidth to ensure plant operations personnel are in complete control over the system and will operate the system within their parameters. GE's security solution collects logs locally on the Windows machines as well as the network equipment through the use of buffering mechanisms.

Vulnerability 10: Lack of appropriate change management/change control on control system software and patches.

GE's solution houses a vast amount of data that is critical for CIP compliance. The Security Server has a database that keeps an inventory of machines and the history related to security related patches that were applied to those particular machines. It also has a database of information concerning the status of Anti-Virus signatures that are loaded on the HMIs. A backup will be performed by and stored on the Security Server.

The Security Server was designed to store up to one (1) years' worth of backups for up to ten (10) machines. The SIEM will store all the event logs from all Windows HMIs in the GE ICS. It will also store all the security events that are created on the network equipment, such as logon and logoff events, configuration change events, etc. This information will be stored and backed up using a stored procedure on the SIEM. The NIDS logs will also be stored on the SIEM, showing any incident that matched the NERC/NEI/WIB rules that are set up in the NIDS device, giving customers the confidence of audit-readiness.

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