Cyber Security for Industrial Controls
Contents

Overview .................................................................................................................................................. 3

Cyber Asset Protection (CAP) Software Update Subscription ............................................................ 4

SecurityST Solution Options .................................................................................................................. 5
  Centralized Account Management Options ....................................................................................... 5
  Network Management Options ........................................................................................................... 5

Related Security Options and Integration Alternatives ........................................................................ 6
Overview

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. Many of the product security features available for current controls, such as Mark* VIe and EX2100e, are also available as enhancements for older controls, such as the EX2000, Mark V, EX2100, Mark VI. GE supports customer compliance efforts by providing baseline configuration documentation for current and certain legacy controls, supporting asset operator cyber vulnerability assessments and associated mitigations.

GE’s cyber security solution is comprised of the Cyber Asset Protection (CAP) Software Update Subscription, and the SecurityST* Appliance. The solution supports cyber security best practices such as centralized patch management, anti-virus/host intrusion detection updates, account management, logging and event management, intrusion detection and automated backup. The solution supports confidentiality, integrity and availability of critical controls and related networks, which in turn can be applied to support owner compliance towards cyber security regulations, standards, and guidelines, such as NEI 08-09, NERC CIP, WIB and ISA 99.
Cyber Asset Protection (CAP) Software Update Subscription

“A single solution does not exist that adequately addresses the patch management processes of both traditional information technology (IT) data networks and industrial control systems (ICSs). While IT patching typically requires relatively frequent downtime to deploy critical patches, any sudden or unexpected downtime of ICSs can have serious operational consequences. As a result, there are more stringent requirements for patch validation prior to implementation in ICS networks. The Department of Homeland Security (DHS) Control Systems Security Program (CSSP) recognizes that control systems owners/operators should have an integrated plan that identifies a separate approach to patch management for ICS management in order to strengthen overall ICS security.”


The CAP Software Update Subscription supports critical infrastructure owners’ efforts to manage current patch levels and anti-virus/host intrusion detection signatures, as well as enhanced backup to support continuity of operations. The patches and anti-virus/host intrusion detection signatures provided through the CAP Software Update Subscription have been evaluated for applicability, tested in a representative operational lab environment, documented securely delivered.

Additionally, as patch change management is a core component of most cyber security standards, the CAP Software Update Subscription also provides a reporting application that supports related compliance documentation. The CAP Software Update Subscription can be applied locally or via the SecurityST appliance in a user acknowledged, centrally deployed fashion that provides significant time savings.

Testing: GE maintains a validation lab in which OS and application patches and anti-virus/host intrusion detection signature updates are tested in a controlled, operationally representative environment, OS and major ControlST platform software revision at the customer site. Testing demonstrates that functional operation of the control and related interfaces, as well as the communication to the system is not adversely impacted by the updates. Further, updates are also tested for optional customer scope such as hardened switches, firewalls and SecurityST appliance. Any updates that are identified to potentially impact operations are excluded; these updates are documented and a mitigation strategy is developed to compensate for this security update. Any false positive identified by new signatures, which would quarantine files needed for “Normal and Emergency” operations are noted, and instruction on how to allow “whitelist” these files are included.

Scripting: The updates are scripted into a single file that the operator can load manually onto each HMI or can deploy via the optional virtual CAP Security and Application Server. Either deployed at the host or network level, any scripted update actions must be acknowledged by the operator before being deployed. This limits potential for operator error or tampering.

Secure Delivery: Scripted updates are transmitted to the site via secure sealed shipping envelope, whereby the chain of custody of the update is also maintained throughout transit until being delivered to site.

Back Up and Recovery: Software provided to support backup and automated recovery of back up to support disaster recovery policy and practices.

Applicability Evaluation and Status Reporting: GE reviews patches and anti-virus/host intrusion signatures for applicability on GE provided Windows OS machines, such as HMIs and servers, as well as network devices such as hardened switches and related SecurityST appliances. From this review, a candidate list of patches and updates is then tested in a representative lab environment to evaluate potential to impact “Normal and Emergency Operations”. Each update disk provides cumulative updates that provide the latest revision of updates and signatures, even if a previous update disk was not applied.

Lastly, GE’s patch management application 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)
- Update 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 applying update in the representative operational test environment and whether or not a reboot is required
SecurityST Solution Options

Centralized Account Management Options

Centralized account management supports unified administration of role based access control and least privilege. GE’s cyber security solution for industrial controls uses an industry accepted, best-in-class Active Directory to easily integrate into plant wide, account management.

- **Active Directory**: Centrally updated security policies on GE Windows Based Machines and Active Directory Users, allowing unique identification, authentication and administration of users. Active directory can also be used to execute account policies related to aging and record retention.

- **MS Radius Server**: Integrates with Active Directory to extend centralized account management to Network Switches and Firewalls.

- **The Certificate Authority Server**: Maintains session authenticity between the GE provided controllers and the Authenticated User on domain controlled HMIs, enabling the Mark VIe control system and EX2100e generator excitation to operate in secure mode during normal operations. When operating in secure mode, the controller solely permits executables, on a hash protected, encrypted list defined in firmware.

  Additionally, when the controller(s) are operating in secure mode, all controller access is encrypted. This enables only users with the necessary certificate on authorized HMIs to access the controller.

Network Management Options

- **Network Intrusion Detection and Firewall**: An integrated security appliance that monitors and protects the GE HMI network (Plant Data Highway) and GE Controller(s) (Unit Data Highway) network, providing detection of known or suspicious network activity.

- **Security Information Event Management (SIEM)**: Collects logs from switches, Controller(s), HMIs, SecurityST appliance, Network Intrusion Detection/Firewall. The SIEM provides a single, centralized, and real-time display of activity throughout the GE network (Plant Data Highway and Unit Data Highway) to support correlation analysis.

Example status report

<table>
<thead>
<tr>
<th>Status</th>
<th>Patch Number</th>
<th>Bulletin ID</th>
<th>Bulletin Title</th>
<th>US-CERT Criticality Rating</th>
<th>Restart Requirement</th>
<th>Estimated Patch Install Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>KB2510690</td>
<td>Q2510690</td>
<td>Office 2010 Service Pack 1</td>
<td>High</td>
<td>May require restart</td>
<td>20 minutes</td>
</tr>
<tr>
<td>Missing</td>
<td>KB2553070</td>
<td>Q2553070</td>
<td>Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution</td>
<td>High</td>
<td>May require restart</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Missing</td>
<td>KB2553091</td>
<td>Q2553091</td>
<td>Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution</td>
<td>High</td>
<td>May require restart</td>
<td>2 Minutes</td>
</tr>
<tr>
<td>Missing</td>
<td>KB2553096</td>
<td>Q2553096</td>
<td>Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution</td>
<td>High</td>
<td>May require restart</td>
<td>2 Minutes</td>
</tr>
<tr>
<td>Missing</td>
<td>KB2584066</td>
<td>Q2584066</td>
<td>Vulnerabilities in Microsoft Office Could Allow Remote</td>
<td>High</td>
<td>May require restart</td>
<td>2 Minutes</td>
</tr>
</tbody>
</table>
Related Security Options and Integration Alternatives

GE can provide integration support to help GE controls and their associated CAP architecture to be incorporated into higher level plant security architecture. GE can also provide additional engineering support of baseline device configurations, as needed per corporate or site policy.

- **Integrated Factory Acceptance Testing of Security Scope:** GE is able to support integrated cyber security Factory Acceptance Testing that allows the customer to minimize risk as it relates to integrating solutions into a broader plant policy and related architecture.