Product Cybersecurity at GE Power
The integration of cybersecurity throughout the Product Lifecycle

Introduction

Increased connectivity – including the increasing significance of industrial Internet of Things (IoT), supply chains, customers, and operations – brings new operational cybersecurity risks and threats which demand attention. The critical infrastructure sectors that GE Power's products support are subject to an ever-changing cyber threat landscape. As such, GE Power continuously integrates end-to-end cybersecurity to ensure integrity throughout the GE product lifecycle.

Background

GE Power has established a product security program driven by and tied to the NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)[1] and incorporates other leading industry practices, including NERC CIP[2], ISO[3] 27001/2, IEC 62443[4], and NIS[5]. The program is focused on reducing the cybersecurity risk associated with cyber applicable products, enabling GE Power to be vigilant towards emerging threats and continuously improve cybersecurity early on and throughout the product development lifecycle. To accomplish this, GE Power has established key areas of a product security program from a programmatic level, including, but not limited to, designating Product Security Leads (PSL), a defined product security program framework, a well-structured governance model, and product-level security controls (e.g., remote access, access management, logging and monitoring).

Due to the inextricable integration of design with manufacturing practices, maintenance of the integrity of the supply chain is crucial. GE Power incorporates industry leading security practices and principles by incorporating security into the product from conception rather than adding security features after the product is installed. Within this "cybersecurity-by-design" process, GE Power has implemented a secure supply chain process for ensuring that the process for procuring third-party supplier products and components meet GE Power requirements and expectations. The GE Power Product Cybersecurity – Secure Procurement Process Procedure drives these activities, aligned with NERC CIP-013-1 Cyber Security – Supply Chain Risk Management Standard which discusses solutions to mitigate cyber security risks. It is important to note that "cybersecurity-by-design" is not solely enough: staying ahead of adversaries in the evolving, threat landscape requires continuous security risk assessments and remediation of risks. For GE Power, it is important to provide transparency to customers to build the 'chain of trust' throughout the product lifecycle. This white paper will outline the activities towards cybersecurity throughout the GE Power product lifecycle, with focus on the secure procurement efforts as called out within NERC CIP-013: notification by the supplier of identified incidents, coordination of responses, notification of remote access, disclosure of known vulnerabilities, supplier verification of software integrity, and coordination of controls.

GE Power Secure Product Lifecycle overview

This program details the integration of cybersecurity into the product development process and the handoffs among stakeholders to show the chain of custody through the following:

Design and development

- **Customer expectation communications**: A General Engineering Knowledge (GEK) document is given to customers during the proposal process which includes a high-level summary of the product's cybersecurity functionality. In addition, a GEH is also provided to the customer during the proposal process. The GEH includes the lower-level cybersecurity technical features of the product. One level down is the Secure Deployment / Implementation Guide which details the security pre-requisites or post-delivery requirements

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[2] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf
[3] International Organization for Standardization
[4] The International Electrotechnical Commission
[5] Network Information Service

for the products and informs the customer of the security associated with deployment, including hardening guidelines.

- **A secure development lifecycle**: A lifecycle for the secure design, development, and maintenance of products, starting from conceptual design through post-release, is established with required reviews where security for the product is reviewed. GE Power assigns appropriate security activities (e.g., threat assessment, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), penetration testing, etc.) based on the assigned risk level.
- **Minimum technical requirements**: GE Power has minimum product technical requirements related to security (e.g., no hard-coded passwords) that it follows internally and requires suppliers to follow.
- **Technical security testing**: Based on the identified product risk level, additional rigor (e.g., SAST, DAST, penetration testing) is performed to provide a deeper analysis on the risk, control, and cybersecurity features of the product being procured from the supplier.

Procurement

- **Cyber "relevant product / component" supplier assessments:** Secure product procurement questions are used to evaluate a supplier's product security program and evaluate a product being procured for GE Power cybersecurity controls and requirements.
- **Supplier product lifecycle considerations**: GE power monitors to the best of its ability the end-of-life (EoL) of products procured and stipulates that no product be procured with an EoL of less than two (2) years.
- **Terms & conditions (T&Cs)**: GE Power formally and consistently integrates product security into contracting.

Manufacturing

- **Validation process / procedure**: A validation plan provides procedural steps related to the operational and security functionality that each component must meet and pass prior to shipping.
- **Software and hardware providence**: GE Power has a software authentication / certification process.
- **Remote access**: GE Power can monitor remote access and a level of restriction against code change from outside the organization's infrastructure is in place.
- **Physical security**: A level of physical access controls around the manufacturing facilities include role-based access to building / facility entry, electronic access control for physical perimeter, guards, and badge security.
- **Factory Acceptance Test (FAT):** FAT is performed prior to the final delivery of a manufactured product and includes a cybersecurity checklist of test and performance criteria to confirm the product / component and or system meets the specifications.

Shipping / Installation

- **Storage**: Products are stored, re-boxed, and shipped in wooden crates to either on premise of customer or to a warehouse where customers have access to record keeping. In addition, secure digital signatures are in place to secure the base platform and third party and operating systems and secure enclosures are used for shipping.
- **Product support team:** This team serves as the first level of defense for handling and managing field support inquiries.

Maintenance and monitoring

- **Asset management:** A Product Lifecycle Management (PLM) tool has been implemented to track each product and its sub-components. This system can be used to cross-reference a product's Cybersecurity Bill of Materials (CBoM) with Common Vulnerabilities and Exposures (CVE) lists to determine if there are vulnerable components.

- **Threat intelligence and monitoring**: GE Power subscribes to and participates in threat and information sharing feeds, including ICS-CERT, SANS ICS Forum, Kaspersky's ICS-CERT, and E-ISAC.

- **Vulnerability and patch management**: After a product is assessed, reviewed, and integrated, ongoing monitoring (e.g., incident response (IR), vulnerability response (VR)) and maintenance activities are performed in accordance with industry regulations and customer contracts (e.g., service contracts). GE Power reviews threats and vulnerabilities received from various sources (e.g., National Vulnerability Database (NVD)) and assesses them against the product inventory to identify affected products and works internally and with suppliers to identify the appropriate remediation actions.

- **Customer communications**: The Technical Information Letter (TIL) alerts customers of risk and actions needed to be taken, communicates to install base, sets the tone for ongoing engagement with GE services, and provides guidance that reduces system cyber-attack exposure. In addition, GE Power leverages customer support portals with dashboards to provide high-level product information.

- **Monitoring and metrics**: Select key performance and risk indicators are collected (e.g., code scan stats, adherence to controls) from product teams and reported to leadership to evaluate the effectiveness of the product security program and provide insight into operations. Program effectiveness is reviewed annually.

In addition, we expect that customers will take the following security activities to protect products and their associated ecosystems:

- **Adhere to the issued guidance:** Leverage the GEKs, GEHs, and Customer Deployment / Implementation Guides to securely deploy products from GE Power and third-party suppliers.

- **Product security program:** Establish an enterprise-level product security program, including the development of policies and procedures, that enables an organization to manage the cybersecurity risk associated with developed, marketed, and fielded products.

- **Physically secure products**: Protect the physical security of the GE Power product and operate it in a secure manner. Control and monitor physical access to the product using mechanisms such as security cameras, security badges, keypads, and biometrics.

- **Securely design, deploy, operate, and maintain applicable infrastructure**: Protect the network using network intrusion detection and prevention mechanisms and hardened network / application firewalls and network segmentation. Use secure principles (i.e., role-based access control, the principle of least-privilege) to help secure connected industrial products (e.g., human machine interfaces (HMIs), workstations, industrial control systems) and networks.

- **Limit access to authorized users**: Restrict access to GE Power in accordance with your organization's security policies and through the user accounts maintained by the product (e.g., change password upon transfer of ownership from GE Power to the customer)

Conclusion

GE Power seeks to maintain and constantly improve customer trust through increased supplier collaboration, monitoring, and compliance against leading industry standards. GE Power has focused efforts towards product cybersecurity assessments and capabilities development, particularly related to the secure procurement and supply chain processes. It is of utmost importance that GE Power instills the confidence and reassurance that cybersecurity is appropriately and accurately integrated into products that are built by GE Power and procured from third-party suppliers to help customers stay safe in an increasingly complex digital and connected world.