GE
Grid Solutions

CyberSentry

Substation Cybersecurity

With electrical substations evolving to benefits from digitization, various aspects of the systems and networks need to be revisited, including cybersecurity. GE's CyberSentry* solution has been specifically created to respond to that new and increasingly critical need, not only to provide the necessary levels of data protection but also to maintain regulatory compliance.

In line with the latest cybersecurity directives from NERC*, IEC*, IEEE* and BDEW, GE's CyberSentry solution employs a "defence-in-depth" multi-layer strategy to mitigate the risks associated with cyber-attacks. It enables GE's IEDs and substation control systems to provide cybersecurity by working as integrated component of the customer's secured IT system.

GE's Grid Solutions CyberSentry offer revolves around 3 complementary aspects:

- Products are delivered with the **CyberSentry Core Protection** capabilities installed, configured, and tested, providing all necessary features for a standalone hardened system.
- In addition, **CyberSentry Advanced Security** offers centralized management of cyber security components, either at the substation level or integrated into a larger system and provides secure remote access and network monitoring.
- **CyberSentry Security Services** are always available to accompany and assist customers from the initial security assessment, past the security roadmap definition, to deployment and long-term security maintenance.

Finally, to reassure customers that our complete solution has been conceived with the utmost rigour, we are proud to confirm that is has been evaluated and certified to the IEC 62443 international cybersecurity standard.

Multi-Layer Security

- Secure by design
- Network security
- Host hardening
- Malware prevention
- Authentication
- Security event logging

Security Services

- Risk assessment, audit
- User training
- System upgrades
- Consulting
- Security updates

Standards and Guidelines

- IEC62443-2-4 certified
- IEC62443-3-3 certified
- IEC62443-4-1 certified
- Conforms to BDEW Whitepaper
- Conforms to NERC CIP

Applications

- Power generation
- Transmission and distribution
- Oil & gas, petrochemicals
- Industrial customers
- Data centres

CyberSentry™ Core Protection

GE products, especially those showing the CyberSentry logo, include a core set of security features to provide the following.

Host Security

Device Hardening

Hardening aims at improving security by reducing the number of possibilities a threat has to disrupt or take control of the operating system on which the solution's software is installed.
Unnecessary network services, physical communication ports and users are disabled.
Audit, password, user account locking and session time out policies are set.
Host firewalls are configured to allow only the required communication flows between authorized devices.

Malware Prevention

Preventing malicious software (including viruses, ransomware and spyware,) from running and potentially causing extensive damage to data and systems or gaining unauthorized access to a network.
Application whitelisting is used to guarantee binary files integrity and authenticity and effectively block unknown malware from running.
An anti-virus scanner is installed for on-demand scans.

Secure Communications

Encrypted communication to avoid eavesdropping. Configuration and maintenance protocols are secured either with TLS or SSH.

Application Security

Authentication and Authorization

All users are required to authenticate to interact with any IED.
Users have individual accounts and passwords (no shared accounts). Each user account is assigned one or more roles (RBAC).

There are no backdoors or hardcoded user accounts.
All passwords are securely stored to ensures that clear text passwords cannot be extracted from the system.

Software Integrity

All GE software and firmware are digitally signed to guarantee authenticity and integrity at installation time.

Security Event Logging

All basic security events are logged on each device. The logs include the username, originating IP, timestamp, and action description. No sensitive information (such as passwords) is logged.

IEC 62443-4-1 Certification - Secure development lifecycle (SDL)

IEC standard 62443-4-1 specifies the process requirements for the "secure development of products used in industrial automation and control systems". Our certification to this standard means that our products are designed following a certified security development lifecycle. This ensures that the products are designed, implemented, and tested according to the highest cybersecurity standards, under the supervision of a Product Security Leader.

CyberSentry™ Advanced Security

GE's Protection, Automation and Control solutions can be delivered fully integrated into a centralized security infrastructure. A state of the art network topology with proper zoning and remote access security completes the defence-in-depth strategy.

Network Security

Network segregation

Global protection is ensured by a firewall that denies all communications by default and allows only required communication protocols between specific zones.

Network Intrusion Detection System (NIDS)

The network IDS is configured to detect and report malicious traffic allowing an authorised operator to react quickly upon threat detection to block the threat and minimize its impact.

Virtual Private Network

Communication between the substation and other remote systems (remote centers or other substations) are tunnelled in a virtual private network (VPN) - a secure encrypted point-to-point communication channel.

Remote access thru Jump Box

Remote maintenance is done by connecting to a "jump box" (a PC with Ethernet access in the DMZ zone), and from there accessing a restricted list of devices and applications on the private zone. This allows controlling the traffic to the substation IEDs.

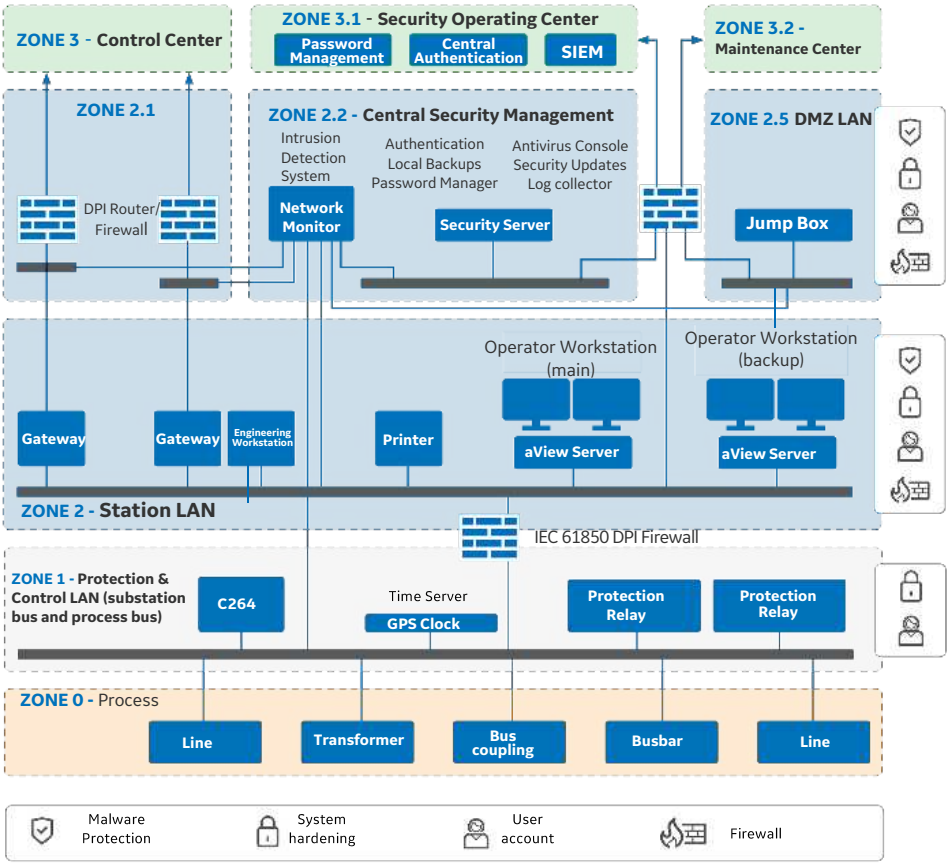
Remote Access - Authentication

Authentication can be required to access the substation LAN remotely by configuring the firewall as a proxy authentication.

Switches

Network switches are configured to reduce threat impact by managing the traffic (broadcast storm limitation, QoS to prioritize IEC-61850 traffic, VLANs to segregate traffic, MAC address filtering, ...).

Standard Network Architecture



Centralized Security Management

User Management

Centrally manage user accounts, passwords, and roles from Microsoft Active Directory, using LDAP over TLS and RADIUS protocols.

Security Logs

Collect security logs at a single point in the substation, using the syslog protocol (over UDP, TCP or TLS) and forward logs to a Security Information Event Management (SIEM).

Backup and Restore Plan

Prepare to recover from disaster with a comprehensive backup and restoration strategy, as well as backup automation solutions. With offline and online, onsite and offsite backup options.

Advanced Malware Protection

Manage anti-malware policies centrally and deploy virus definition updates (DAT files) automatically (tested monthly by GE).

Centralized Security Updates

Automate the deployment of Microsoft* Windows security updates. Windows security updates are tested monthly by GE.

IEC 62443-3-3 Certification - Certified Automation Solution

IEC standard 62443-3-3 provides detailed “technical control system requirements associated with the seven foundational requirements described in IEC 62443-1-1 including defining the requirements for control system capability security levels”. Our certification to this standard means that our solution has the required cybersecurity capabilities. It is delivered with its Secure Deployment Guide which documents the system’s installation steps and best practices to get the most of its security.

CyberSentry™ Security Services

GE offers a comprehensive portfolio of services to support our customers in their cybersecurity journey. The content can be tailored to specific customer requirements and can include some of the following:

Substation security assessment

- Security awareness training
- Systems cybersecurity risk assessment
- Security improvements without any process change and minimizing the need for an outage
- Upgrade services to benefit from the state-of-art security of the latest versions
- On-going support to sustain security

Substation Vulnerability Watch

- Monthly security bulletins about the compatibility of Microsoft Windows 10 security updates with the solution. Security updates are first tested in our R&D lab in a representative environment simulating the customer's typical control system
- Monthly security notices of newly discovered vulnerabilities for every IED in the system's inventory, including severity and possible mitigation measures
- Firmware security updates for GE products, with security update deployment, on site or remotely

IEC 62443-2-4 Certification - Certified Integrator

IEC standard 62443-2-4 specifies a "comprehensive set of requirements for security capabilities for IACS (Industrial Automation and Control Service) providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution". Our certification to this standard means that we are a certified integrator of our substation protection, automation, and control systems. By choosing GE to deliver a full solution, customers prevent and manage risk during the solution's implementation, improving their supply chain's security.

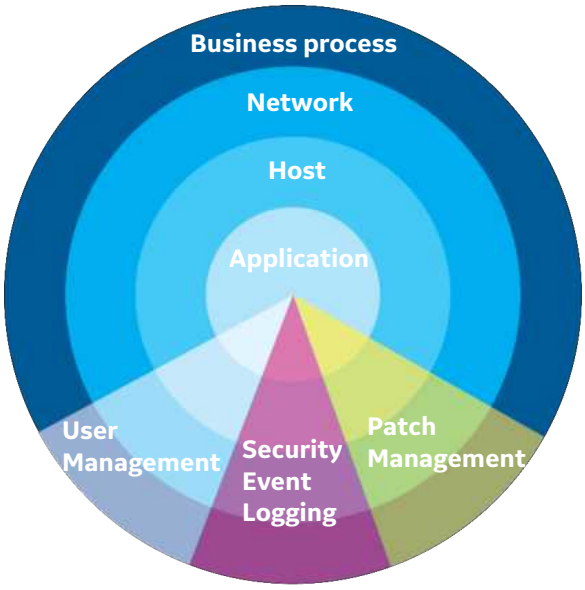


Figure 2: CyberSentry™ Defence-in-depth

For more information please contact
GE
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Phone: +44 (0) 1785 250 070

GEGridSolutions.com

Imagination at work