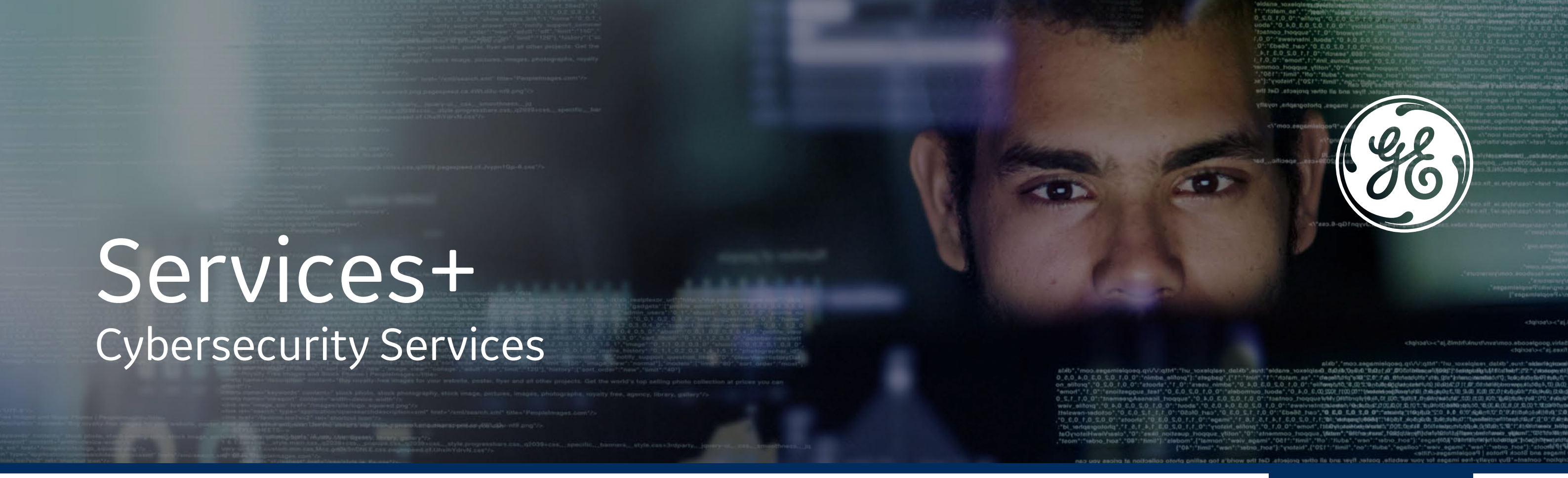

Services+

Cybersecurity Services

Services +

If you're looking for ways to reduce downtime and enhance the performance of operations and assets, GE Power Conversion's simple suite of clever software applications can help. Its flexibility includes 'on-prem' and cloud-based options which help to optimize operations and energy, and enable predictive maintenance and cyber-secure service solutions. GE Power Conversion's digital suite is based on a straightforward, modular range of digital app's, tools and services, connecting data with the right people. Already, more than 500 sites are benefiting from Power Conversion's digital solutions. Each of our three easy-to-navigate modules focuses on a key area of improvement: Operations+, Maintenance+ and Services+ tools and apps

The need to protect Operational Technology assets from cyber threats

The breakout of Stuxnet malware – the world's first publicly known digital weapon – in 2010, dramatically changed how Operational Technology (OT) asset owners around the globe perceived cybersecurity.

Since that event, OT owners have recognized the need to effectively address rapidly evolving cyber threats to the industry. A successful cyber attack on the control system could result in mild to devastating consequences, including:

- Recoverable unplanned shutdown
- Non-recoverable unplanned shutdown
- Partial shutdown
- Remote control of the plant process
- Damage to plant equipment
- Production impacts, from small to enormous
- Financial loss to the plant or country
- Threat to on-site personnel
- Threat to the general public

These potential consequences make clear the critical need to address security threats, vulnerabilities and risks to industrial automation and control systems.

INFAMOUS OT CYBER ATTACKS

2010
- Stuxnet malware attack
- Duqu/Flame/Gauss malware attack

2012
- Gas pipeline intrusion campaign
- Shamoon malware attack

2015
- Ukraine power grid attack

DIGITAL

Global cybersecurity standards

These standards help OT asset owners improve their control system security posture:

Standard	Provides OT asset owners with...
ISA/IEC 62443-2-4	An outline of the security requirements for installing and maintaining an automation solution
ISA/IEC 62443-3-2	Risk assessment and security level estimation guidelines for industrial automation and control systems
ISA/IEC 62443-3-3	A comprehensive guideline for estimating and increasing system security levels

These standards help product suppliers improve the security level of their products:

Standard	Provides product suppliers with...
ISA/IEC 62443-4-1	Requirements for securing the product development lifecycle using maturity assessment methods
ISA/IEC 62443-4-2	Requirements for securing control system components
ISA/IEC 62443-2-3	Guidelines for developing and maintaining a patch management process between the asset owner and product supplier

Our cybersecurity certifications and compliance

Since 2020, GE Power Conversion has held certifications to provide secure development lifecycle assurance for our new products (via IEC-62443-4-1) and security level 1 (SL1) component security assurance for our HPCi controller with firmware version 7.1 (via IEC-62443-4-2).GEPC complies to NIST CSF framework and SP 800-82 by fulfilling the requirements of ISA/IEC 62443-2-1 and ISA/ IEC 62443-3-3. The Role Based Access Control (RBAC) on GEPC products is implemented as per IEC-62351-8.

Our cybersecurity services for OT asset owners

GE Power Conversion offers OT asset owners three services to facilitate their preparedness and management of any cyber threats:

- Cybersecurity awareness workshops
- High level risk assessment services
- Detailed level risk assessment services

Cybersecurity awareness workshop

We offer three workshops tailored to meet your specific cybersecurity needs:

- Fundamental issue awareness
- Best practices for system maintenance engineers
- Best practices for operators

High level risk assessment services

Our HLRA services help you gain an initial understanding of the worst-case risks for your control network.

We evaluate your entire control system using our proprietary model of evaluation for potential cyber risks that may impact a variety of factors, including: health, safety, business interruption, production loss, product quality and reputation as well as environmental, financial, legal and regulatory concerns.

The main steps performed during a HLRA are:

- Identifying the System Under Consideration (SuC)
- Identifying and recording the worst-case scenario for each component, without countermeasures such as safety systems, firewalls, and operator intervention
- Rating the severity of each consequence of the worst-case scenario (based on the scoring system from ISA/IEC 62443-3-2)
- Estimating the security level target (SL-T) for each component under the SuC

The key outputs of the HLRA are:

- Updated system architecture diagram with identified OT external services
- High level risk assessment report that provides risk evaluations with SL-T estimates for device based on our proprietary assessment models

Detailed level risk assessment services

Using the security level target (SL-T) and overall risk score estimates from the HLRA, our DLRA segments the system under consideration into zones and conduits. We then perform a detailed risk assessment using our proprietary assessment models for any zones and conduits with risk scores that are above your defined tolerance level.

The key outputs of the DLRA are:

- Initial or revised zone and conduit diagram
- Detailed risk assessment report that includes suggestive countermeasures to enable you to increase the security level for specific zones with risk scores greater than the tolerable risk

Required HLRA and DLRA inputs include:

- Overall system architecture
- Network diagram
- Asset inventory
- Company policies and regulations
- Tolerable risk guidelines
- Process hazard analysis report
- Functional safety assessments report (IEC-61511-2)
- Asset owner risk matrix (if available)

Conceived for Operators

GE Power Conversion's Digital Suite is built on GE's industry wide expertise in IT, OT (operating technology) and IIoT (the industrial internet of things). Above all we believe it should be intuitive, visual and customized for your operational needs. Featuring simple, clear interfaces it provides organizations of all sizes with access to GE's powerful data analytics, made accessible and usable by providing better intel and situational awareness. Genuine performance improvements are within reach, to help your organization work with increased efficiency and profitability.

To find out more:
contactus.powerconversion@ge.com

DIGITAL