Digital Energy

Professional OT Cyber Security Services
Cyber Security Solutions

EXPERT SERVICES THAT STRENGTHEN SECURITY AND RESILIENCE

To manage your operations and serve your customers, your organization's GE HMIs need to be secure and performing optimally at all times. Maintaining, hardening, and patching of these critical systems is therefore vital. However, these tasks are time consuming, require specific expertise, and are ongoing in nature. Turn to GE's Digital Energy and get the services you need, so these vital efforts can be done right—right on time.

KEY BENEFITS

Boost staff efficiency by offloading maintenance, patching, and hardening.

Extend HMI investments by doing proactive, preventative maintenance.

Mitigate risk by more consistently and comprehensively employing patches.

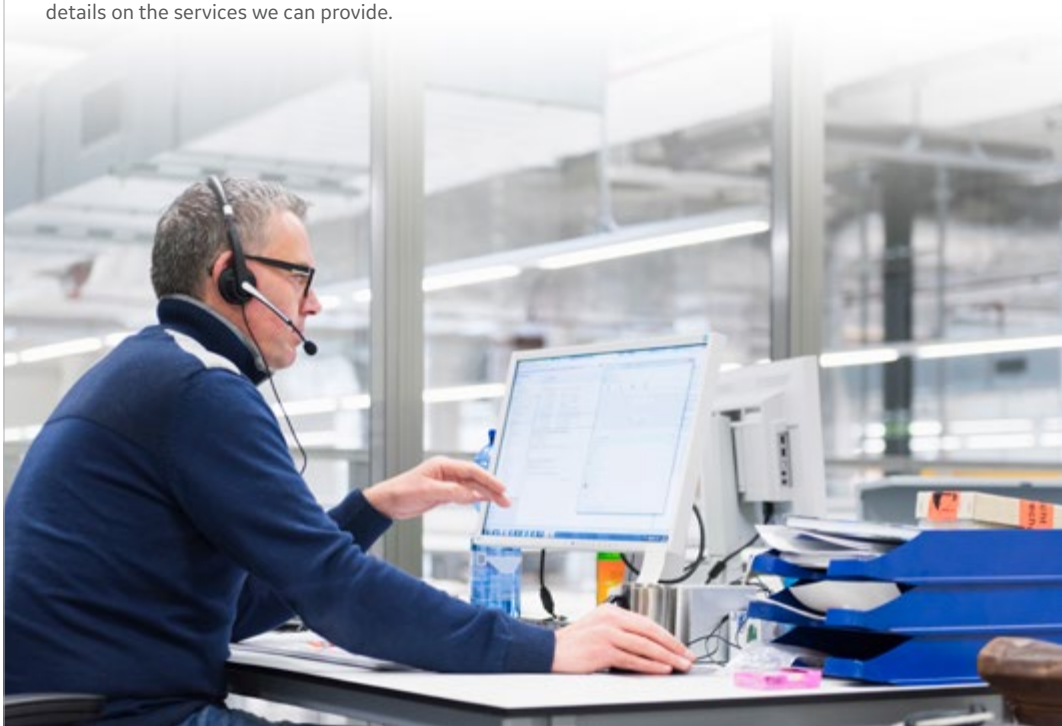
Avoid disruption and downtime by having expert engineers deliver proactive maintenance and well-executed project management.

OVERVIEW

Introducing Professional Services in Cyber Security from GE

Your GE HMIs are critical to your organization; they support essential plant operations around the clock and throughout the year. These HMIs represent a vital component of a GE controls network that includes controls, switches, and other network equipment. Consequently, ensuring HMIs remain operational and secure is a vital mandate. However, only individuals with expertise in both plant operations and cyber security can effectively manage these efforts. This unique combination of expertise can be in short supply internally, and it can be difficult to find within the broader service provider marketplace.

GE's Digital Energy offers a complete range of services to help support your GE HMI implementations and investments. We can provide the specific services you need, when you need them. Our team of experts can deliver services on a one-time or recurring basis, and we can customize our offerings to meet your organization's specific objectives and OT environments. The following sections offer more details on the services we can provide.



Professional OT Cyber Security Services
Cyber Security Solutions

Expert Services that Strengthen Security and Resilience

Hardware Maintenance Services

Your Challenges

Routine maintenance on your HMI hardware is a wise investment. It can help prevent issues and extend the usability of your systems. However, with lean internal teams, it can be difficult to find staff that have the time and expertise needed to perform this maintenance, and to ensure they carry out this work on an ongoing, consistent basis.

Our Solution

On a one-time or recurring basis, we can provide the comprehensive maintenance your HMIs need. As part of our services, we handle a range of efforts:

- Thorough cleaning of a system's internal components to remove any contaminants.
- Complete system diagnostics and remediation of any issues detected.
- Disk defragmentation to improve system performance.
- Inspection of system components, including cooling fans, power supplies, keyboards, air filters, and more.
- Replacement of any faulty components, as needed.

BUSINESS CHALLENGES

Once a day, the energy sector faces a cyber attack that hasn't been seen before.[1]

46% of all cyber attacks in the OT environment go undetected.[2]

$3.92 million: Average total cost of a data breach.[3]

On-site Patch Deployment Services

Your Challenges

Cyberattacks are a constant threat for today's power generators. At any time, attackers may try to exploit software vulnerabilities to gain system access and achieve their nefarious objectives. It is therefore critical to address any vulnerabilities that rogue actors can exploit. This includes installing security patches.

For many power generators, it is a struggle for staff to keep pace with day-to-day demands, leaving precious little time to handle these critical, yet time-consuming patching efforts. Further, these efforts don't just take a lot of time, they require a lot of expertise. To manage patching effectively, staff need current security expertise on evolving threats and vulnerabilities. They also have to know how to implement patches in the safest, most efficient manner, while ensuring functionality and ongoing operations aren't jeopardized. Given these requirements, critical patching efforts continue to be relegated to the back burner, meaning the backlog of open vulnerabilities continues to grow.

Our Solution

GE's Digital Energy team can deliver complete, end-to-end patching services. Our services include comprehensive project management. We will work with your on-site staff and resources to establish a plan for how to sequence patching of HMIs. As part of this plan, we'll develop a detailed schedule for modifications and sequencing, so that we can promote speed and efficiency, while avoiding any potential disruptions. Our team will identify which HMIs can be modified in parallel and those that must be worked on in isolation. We'll make sure that, while one HMI is modified, other resources will be in place so that critical plant operations continue to function.

In building the schedule, we'll account for dependencies. For example, we'll factor in timeframes that are needed for gaining the permissions required for working on different HMIs, so we can reduce the time spent waiting for resources to become available. Our team will also identify the personnel that will be needed to assist us, for example, engineers who will need to provide us with system access or validate functionality. We'll then align plans and schedules with the availability of these resources. Throughout the project, GE's team will review progress with site personnel, and make modifications to the plan if needed.

Following is an overview of how the patch installation is managed:

- Prior to making any changes, we will reboot the HMI and verify the system functions correctly after reboot. If so, we will then back up the HMI.
- Before installation begins, we'll create patch collections, verify signatures of all patches, and validate the integrity of the patch collection.
- Next, we will install security patches.
- After changes are made, we'll work with site engineers to test the patched systems and validate they are functioning properly.
- If the HMI is not functioning correctly, we can revert to the original backup. If the system is functioning properly, we will make a new backup of the updated system.

At the conclusion of the installation, we will provide your staff with documentation that specifies which changes were made to the HMI. If any planned changes weren't executed, our documentation will detail the reasons for the exclusion. Finally, we can provide any necessary training to help staff continue to safely operate systems after the engagement.

Professional OT Cyber Security Services
Cyber Security Solutions

Expert Services that Strengthen Security and Resilience

Hardening Services

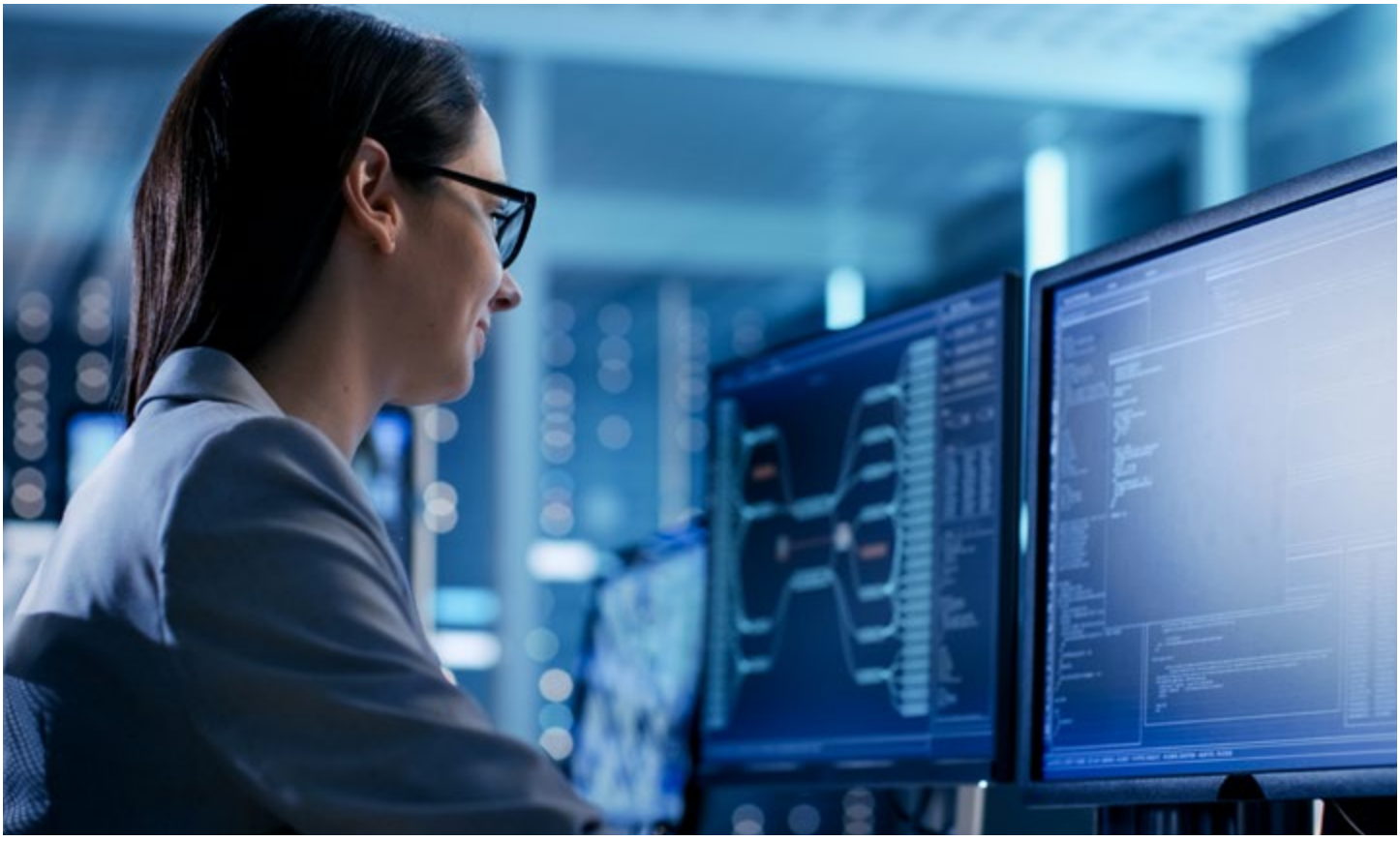
Your Challenges

For any number of reasons, HMIs may be unnecessarily exposed to unauthorized access. Misconfigurations, unapproved credentials and access methods, and even the age of a system can play a role in an HMI being vulnerable. However, within many organizations, it is challenging to address these vulnerabilities. Constantly juggling competing priorities and demands, internal staff struggle to find the time needed to do proactive diagnosis and remediation. As a result, vulnerabilities are often left unaddressed.

Our Solution

GE's experts can do a comprehensive examination of your HMIs and carry out a thorough hardening to strengthen system security. Our system hardening approaches are based on the Security Technical Implementation Guide (STIG) and GE Power standards. We'll manage the entire project. Our team will work with your internal staff to establish and document a plan, specifying all the tasks and activities we'll be carrying out over the course of the engagement. Our team can provide comprehensive hardening services and approaches, offering coverage of the following areas:

- **Applications.** We will work with your staff to identify which applications are approved, and remove any unapproved applications.
- **Media ports.** We'll lock down unused media ports, such as USB ports, using port blockers and other software or configuration techniques.
- **Settings.** Our team will change settings that unnecessarily leave a system exposed to various malware attacks. For example, if a compromised DVD is inserted into a system with auto-play enabled, the machine may be exposed to a malicious code injection. By disabling auto-play, we can help protect systems against this threat. We can also eliminate a potential attack vector by disabling IPv6 services. (GE control systems only use IPv4, so there is no need for IPv6 services to be enabled.) Our team can also implement any recommendations that have been specified in GE Cyber Security Technical Information Letters.
- **Passwords and access controls.** GE's teams can institute a range of changes to help safeguard system access. For example, we'll disable automatic login, so user authentication is required for each session. We'll set BIOS passwords to help prevent unauthorized BIOS configuration changes. Our team will also work with your staff to identify and disable any unapproved accounts and network shares. We can also join the HMI with an optional Active Directory domain, which can be furnished by GE. Through this effort, we can help establish and enforce access policies. We can help apply password expiration and complexity policies. In addition, we can identify well-known, commonly used privileged accounts, and either disable or rename them. For example, instead of using easily guessed account names like "admin", we will assign unique, site-specific account names.
- **Antivirus.** Our team can install antivirus software along with the most recent antivirus signatures. Through our services, we can also do a full antivirus scan in order to detect and remove any viruses.



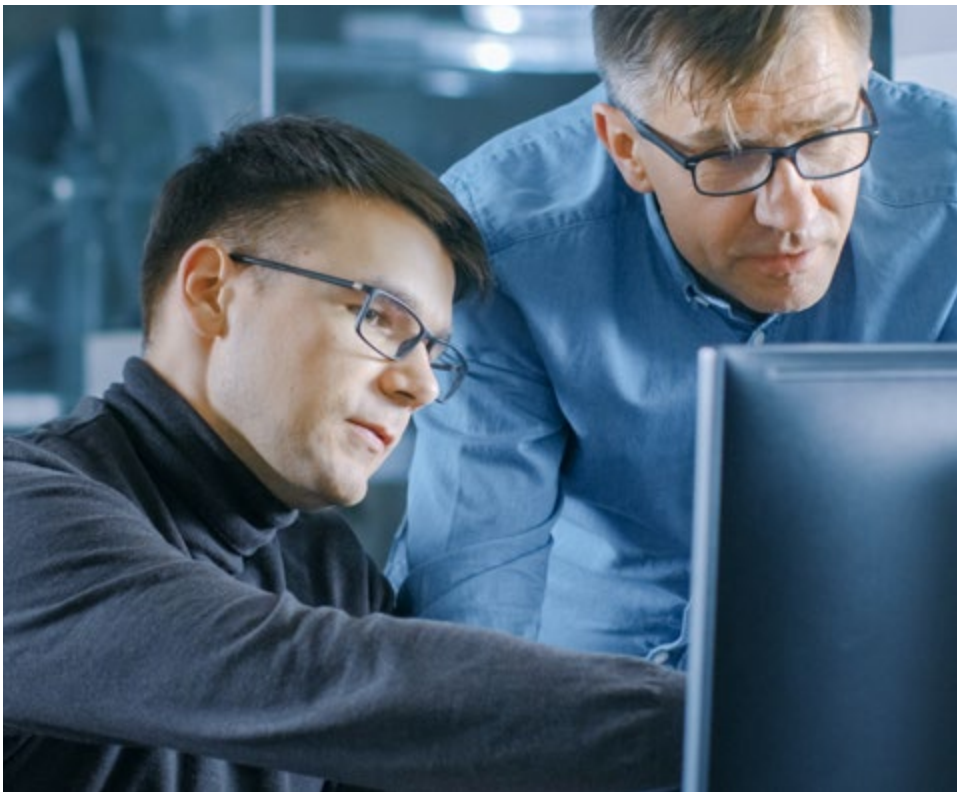
Professional OT Cyber Security Services
Cyber Security Solutions

Expert Services that Strengthen Security and Resilience

Benefits

By working with GE's professional services team, your organization can realize a number of benefits:

- **Boost staff efficiency.** By offloading ongoing efforts like maintenance, patching, and hardening, we can help your staff free up time to focus on their other responsibilities and priorities.
- **Extend HMI investments.** By doing proactive, preventative maintenance, your organization can avoid issues and prolong the usage of your existing HMIs.
- **Mitigate risk.** By more consistently and comprehensively employing patches, our services can help your organization mitigate exposure to cyberattacks.
- **Avoid disruption and downtime.** Our expert engineers can work with your teams to establish plans that help critical plant operations remain functional while services are delivered. Through our proactive maintenance services, your organization can take steps to avoid system issues and the cost and disruption associated with urgent repairs.



How to Get Started

To learn more and sign up, please contact your local GE's Digital Energy or GE's Power Services Account Executive or call 770-722-2552.

Sources

1 S&P Global, "Feature: Energy industry faces unprecedented cyber threats almost daily," July 19, 2018, www.spglobal.com/platts/en/market-insights/latest-news/electric-power/071918-feature-energy-industry-faces-unprecedented-cyber-threats-almost-daily.

2 Ponemon Institute LLC, "The State of Cybersecurity in the Oil & Gas Industry: United States," February 2017, www.crc-ics.net/documents/CRC-ICS-2017_Pokemon%20Report-Cyber_Readiness_US_Oil__Gas_2017.pdf.

3 Ponemon Institute, sponsored by IBM Security, "2019 Cost of a Data Breach Report," July 2019, www.ibm.com/security/data-breach.

Contact Us
ge.com/digital/sales-contact-me