Digital Wind Cyber Security from GE Renewable Energy

BUSINESS CHALLENGES

The impact of a cyber attack to power generation operations has the potential to be catastrophic to the renewables industry as well as employee and public well-being. More and more, utilities are a growing target for cyber criminals keen on making political statements or simply as criminal misdeeds. Government organizations, such as the Department of Homeland Security, continue to advise power executives to take proactive steps to protect physical assets, software systems and network components of their operating environment.

Additionally, as the renewable energy industry has become a more challenging operating environment, leaders are forced to be creative in business planning, and the associated risk management to that business plan. As part of an enhanced risk management program, forward thinking energy industry leaders are putting the right programs in place to assess their vulnerabilities, to protect their systems and proactively defend their environments. However, the challenge is significant. The nature of security attacks are ever-evolving and require continuous vigilance to combat. Due to the specific nature of attacks on operating technologies, such as Supervisory Control and Data Acquisition (SCADA), unique programs are required above the standard IT security protocols to truly protect the power operating environment.

What's needed is a partner who understands the security profile of an operating environment and understands emerging cyber security regulatory requirements, who has a focus on industrial software and technology, offers a comprehensive strategy and software portfolio, and is backed by global security expertise. GE has been serving the energy industry for decades in every region in the world and offers a comprehensive set of cyber solutions, built on experience and the Industrial Internet platform, Predix. Together with our customers we are dedicated to protecting the global energy infrastructure from those who would compromise power generation, public safety and the financial health of our customers.

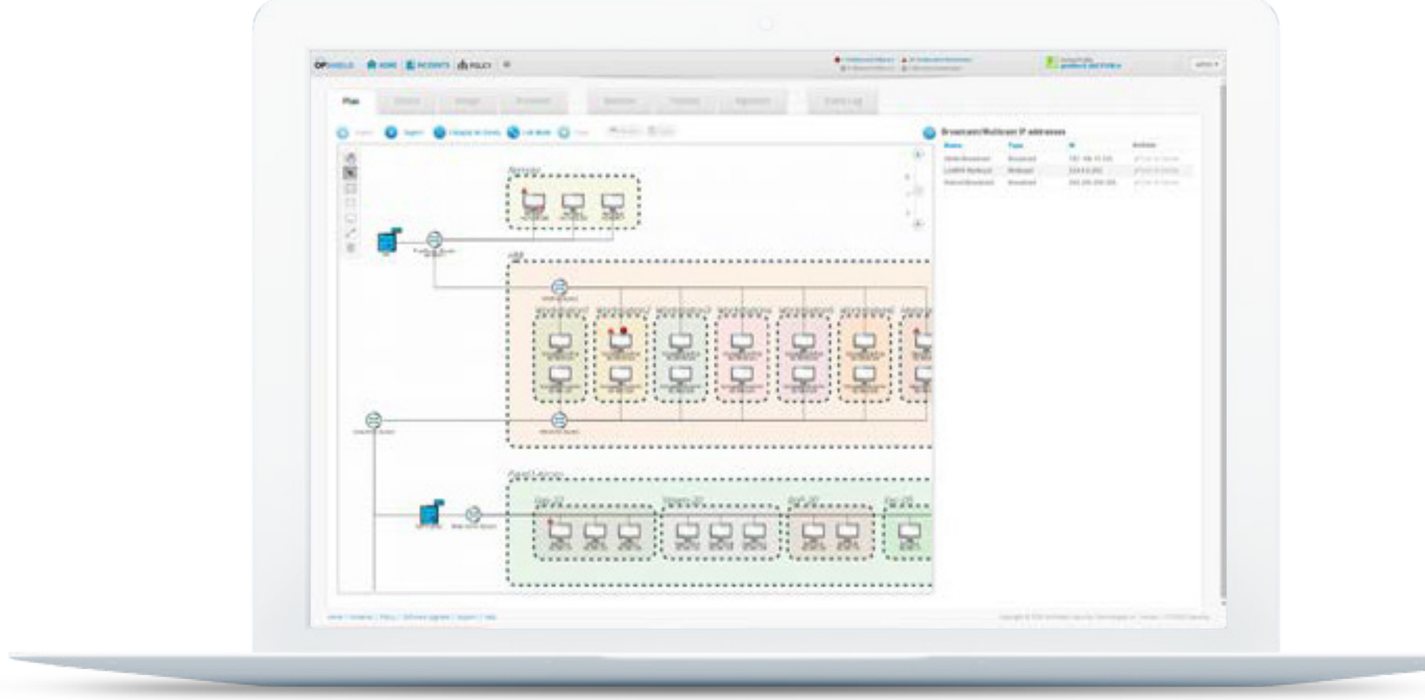
225K

people lost power in the Ukraine due to a cyber attack (December 2015)

$243 BILLION

impact to the US economy of an electricity blackout across 15 US states affecting 93 million people

Source: Lloyds Emerging Risk Report, 2015



THE PATH FOR MAXIMUM CYBER PROTECTION

It is important to understand the steps required to implement a security strategy. The easiest way to identify and initiate these steps is to review a security maturity model, with clear actions outlined for the Renewables business environment:

CONCERNED → **COMPLIANT** → **CONFIDENT**

CONCERNED

For customers concerned about their security posture, we start with an assessment to identify immediate security issues that can impact operations, even if the environment is thought to be “air gapped.” Common findings from expert assessments include unapproved wireless access points or unsafe software — vulnerabilities that attackers can easily exploit. Many of these issues can be fixed quickly and simply to reduce cyber threat risk.

COMPLIANT

We can also assist customers with understanding cyber security regulations. Implement defensive layers to comply with standards and strengthen the security posture. Lower the risk of security exploits by using technical solutions, such as purpose-built industrial control security equipment. Set up automation and patch management tools to simplify and expedite security administration. Implement Cyber incident response plan to inform internal resources on what to look for and how to respond to cyber activities.

CONFIDENT

Asset security monitoring, personnel training and ongoing incident response. Regular assessments and security health checks can monitor dynamic environments. Centralizing security management operations can significantly reduces system downtime, potential asset damages and production risks.

Across all stages, it is critical to maintain a constant vigilance to ensure basic security hygiene and the enforcement of cyber security policies.

SOLUTION DESCRIPTION

GE Renewable Energy Digital Solutions work at any stage of security maturity to bring greater control, less risk and increased reliability to a power generation business. Depending on the situation, there are impactful people, process and technology actions that can be instituted. GE's Digital Cyber Security Solutions include:

Security Assessment Services

Security and assessment testing for operational technology (OT) is a specific and demanding discipline. It requires an industrial mindset, in-depth OT cyber security knowledge and the ability to apply best practices to industrial process environments. GE's security and test professionals can help power companies plan, design, and build operational resilience into people, processes and technology.

Cyber Security Assessment is an in-depth, comprehensive evaluation of the operational site facility based on industry standards and best practices, resulting in an individualized report with prioritized mitigation recommendations and strategies. The assessment consists of:

- **Site Security Health Check:** Rapid overview of the operational site facility providing a baseline of cyber strategy, with recommendations on further analysis as well as economic justifications for remediation.
- **Site Security Assessment:** Deliver comprehensive, in-depth facility evaluation to understand the security posture of the processes, architecture, and technology. Identify security weaknesses, prioritize areas of improvement and align security practices to industry standards with a comprehensive, in-depth facility evaluation.
- **NERC CIP Cyber Vulnerability Assessment:** In-depth evaluation for electric utilities following the requirements prescribed by NERC CIP. The report includes mitigation plans aligned to NERC CIP as well as other industry best practices.
- **IEC Security Practices Certification:** Provides certification for system supplier compliance with industry standard security best practices (IEC62443-2-4), covering areas such as hardening, anti-malware, patch management, network, and data security.

Glossary of Key Terms

FSA: Full Service Agreement	SIEM: Security Information and Event Management
DMZ: Demilitarized Zone	VLAN: Virtual Local Area Network

OpShield

A purpose-built intrusion detection and intrusion protection security solution designed to protect critical infrastructure, control systems, and operational technology (OT) assets. OpShield monitors and blocks malicious activity and minimizes disruptions to enable highly available operations and secure productivity.

OpShield is purpose-built to protect industrial and SCADA operations, offering comprehensive security, simplicity, and visibility. This network security solution monitors and blocks malicious activity and attacks to ensure highly available industrial operations for maximum uptime and secure productivity.

- **Inspects and Controls:** Industry leading threat signatures and granular control over protocol commands
- **Virtual Zoning:** Create logical security policy zones without physically rewiring the network (VLAN)
- **Graphical Network Topology (real-time):** Real time graphical representation of the controls network. Includes unknown device discovery and alerting and SIEM integration
- **Intrusion Protection System/Intrusion Detection System (IPS/IDS):** Accurately detects and protects cyber attacks to the industrial network. By leveraging Wurldtech's* OT and IT signature set, OpShield offers specific and customized, industrial protection for **SCADA systems and industrial networks.** Purpose built for industrial control systems, the inspection engine supports most existing industrial protocols, with the flexibility to easily support emerging proprietary protocols.
- **Centralized Management:** A single graphical interface to build and deploy security policy and protection profiles. It also offers a network-wide view of alerts and attacks on the industrial network

SecurityST

GE's SecurityST provides an integral defense-in-depth solution for turbine, plant and generator controls environments. Employing multiple defensive services and technologies, it supports the reliability, availability, integrity and maintainability of a plant's critical control system and related networks. The SecurityST solution is designed to support wind farm operators' compliance to cyber security regulations, standards, and guidelines such as, NERC CIP and IEC

- **Role Based Access Control:** Enforces best practice of every user having a unique user name and password
- **Password Management:** Enforces policies for password strength, life, and reuse restrictions
- **Security Information and Event Management:** Provides centralized function with real-time visual security status dashboard and events display
- **Patch Update Service:** Monthly subscription service provides vendor approved software security patches
- **Endpoint Protection:** Every Windows®-based system is continuously monitored for viruses, spyware, rootkits, Trojans, and adware
- **Backup and Recovery:** Backup functionality for typical and disaster recovery processes

Cyber Security Training

A comprehensive portfolio of security training courses for critical infrastructure to increase staff knowledge and awareness.

Training content is developed and delivered by GE's security experts, who regularly analyze and implement real-world security solutions at operating facilities.

Security Monitoring Service**

Remote monitoring and diagnostics of OT control environment security events. Activities are examined on network, SCADA and host environments; User and systems accounts are monitored for malicious or compromising events.

* GE acquired Wurldtech Security Technologies in 2014.
** Scheduled for General Availability release in late 2017

CUSTOMER BENEFITS

Overall Cyber Security Solution Benefits

- Reduced risk from cyber attack on key assets, SCADA systems, and operational network infrastructure
- Proactive identification of critical vulnerabilities and security events
- Improved operational reliability and reduced risk in business continuity
- Support regulatory compliance globally, such as NERC CIP in North America, with ability to demonstrate security actions and activities

OpShield Benefits

- Protects industrial OT system with strong perimeter and field defense
- Inspects and protects control system network protocols with industry's leading threat intelligence
- Introduces breakthrough drag-and-drop virtual zoning for segmentation without network disruption
- Displays graphical network-wide industrial security view and integrates with SIEM tools
- Simplifies security administration with easy to use graphical interfaces

SecurityST Benefits

- Maintains consistent operations of plant's critical controls and related systems
- Identifies cyber threats to control systems from external or internal sources
- Provides secured backup and recovery capabilities
- Provides enhanced protection against execution of unauthorized code
- Supports plant management's compliance to cyber security regulations, standards and guidelines

Cyber Security Training Benefits

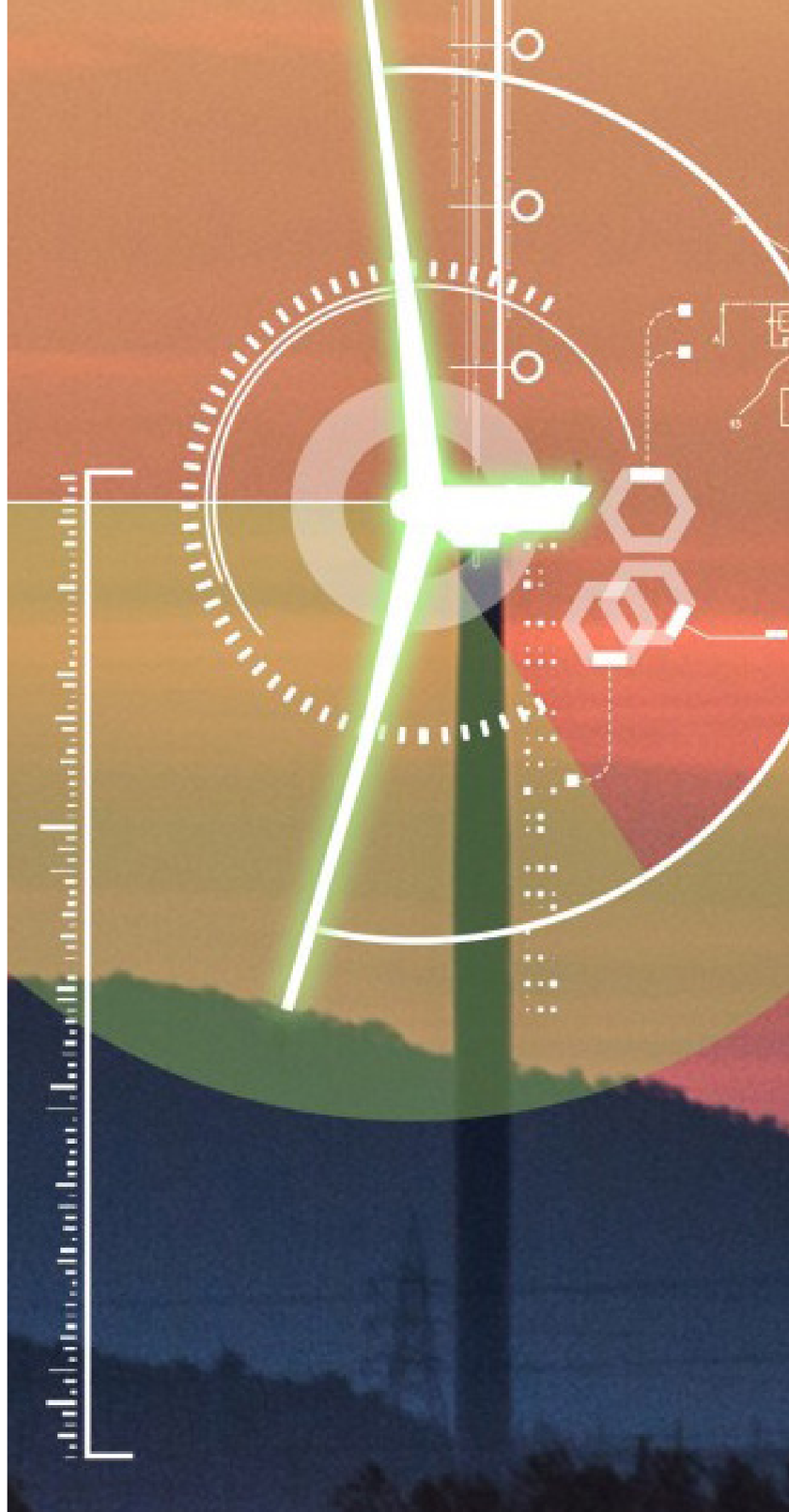
- Arms personnel to be the front line in the battle against cyber attacks
- Achieve compliance requirements for training and preparedness
- Protect against employee attrition by educating a broader set of talent
- Proactively stop cyber attacks with a well developed staff, ready to identify and act on suspicious events

$29K

avoided from a day of downtime at a 50 MW wind farm

$1MM

— max penalty per day per NERC CIP violation



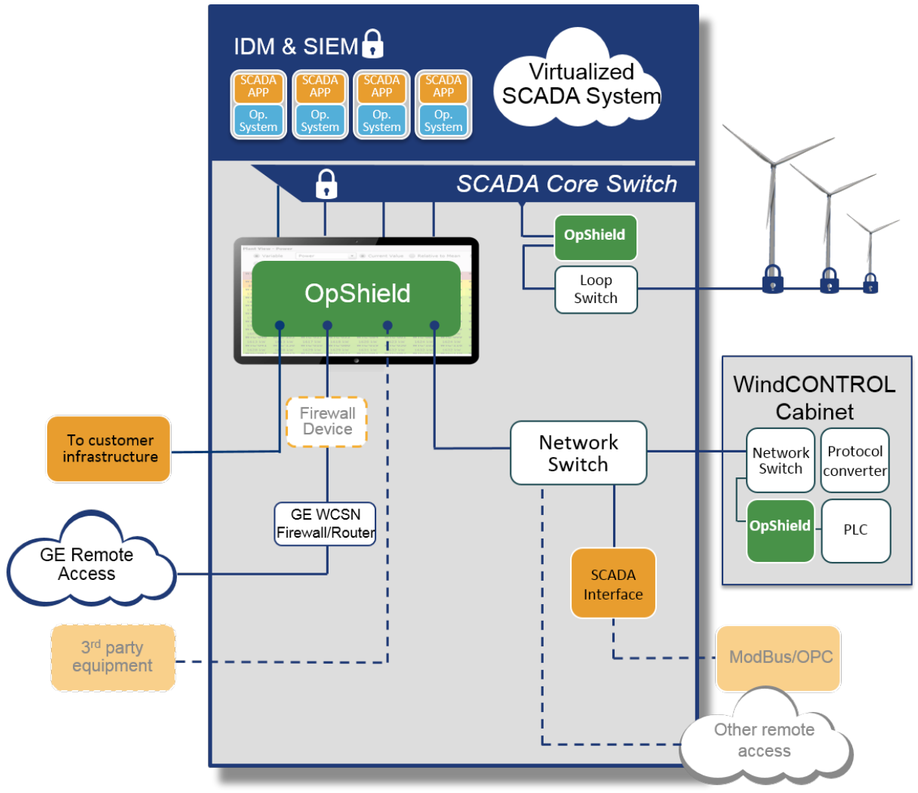
A WELL DEFINED AND PROTECTED OPERATIONS ENVIRONMENT

IT systems are typically fortified at the edge of the Internet with firewalls, proxy servers and intrusion detection services. However, within the corporate environment, sub-networks exist with much looser security barriers, due to the system and data sharing requirements between departments. The OT environment requires a much stronger vigor to protect against attacks that might come from the Internet:

- The wind farm SCADA should exist within it's own network environment, with no direct access to the Internet allowed from that network.
- The SCADA network should be separated from the rest of the corporate network via technologies (i.e. firewall, DMZ) that limit traffic allowed between the two to only that with special designation.
- User access to the OT network environment should be controlled and examined frequently to ensure that only those that require access are allowed access.
- Access lists should be reviewed at regular intervals by senior management — extraneous access and departed employees should be removed immediately.
- Traffic within the SCADA "network" needs to be monitored closely with sophisticated intrusion detection capabilities to identify any suspicious activities.

NERC CIP Compliance

Many U.S. electric utilities are now federally mandated to comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards that dictate industrial security and remediation technology, including required compliance, by July 1, 2016. GE's products and services assist power generation customers in meeting CIP mandatory standards and reduce the likelihood of a compliance event. An event would result in a fine of $1MM per day.



Cyber Security Solution Applicability

Regulatory Cyber Asset Integration Solution Results in Compliance and Avoided Penalties

MidAmerican ENERGY
OBSESSIVELY, RELENTLESSLY *AT YOUR SERVICE*®

Established wind businesses have sophisticated challenges. NERC CIP compliance of back-office is a critical need that must be in place while maintaining seamless connectivity and FSA.

The solution was GE Renewable Energy's Digital Wind Cyber Security. The team implemented security solution to the customer's remote operating center, built secure communication channels, and established secure processes for services.

As a result of the integration, the remote monitoring center is NERC CIP Compliant, penalties were avoided, secure access for FSA is in place and maintained.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.renew.ge/digitalwind