

Cybersecurity for Wind Offshore

White paper

siemens-energy.com/wind-offshore-controls

SIEMENS energy



3 Overview

4 The Cybersecurity Challenge for Wind

5 The Secure By Design Opportunity

6 The Secure By Design Approach

8 Securing Integrated Wind Systems

9 Setting the New Standard for Unified Cybersecurity

11 Conclusion

Overview

Wind power continues to grow rapidly as governments and consumers demand more clean energy. As this efficient, cost-effective renewable power source becomes an ever-larger share of power production, wind farm developers, owners, and operators need to ensure that these facilities provide reliable energy delivery throughout their life cycle. This responsibility calls for cybersecurity strategies adapted to the technical and physical realities intrinsic to wind farms, their often remote, distributed nature, and the complexity of the digital systems and subsystems that must work together to manage turbines individually, as a wind farm, and as a growing contributor to regional and national electricity supplies.

Wind power requires digital management. Variable inputs from wind and wave conditions require active management to maximize power production and synchronize outputs with regional electric grids. The considerable cost of site visits for maintenance make remote management and diagnostic tools essential for minimizing operating costs. Typical wind farms include digital management systems for orienting turbines, monitoring environmental conditions, managing power flows, and several other critical workflows. These systems require cyber defenses both individually and as an integrated system.

Growth in wind power comes with growing risks. As a larger share of power production, wind becomes a more attractive target for cyber attacks. Critical infrastructure operators in the energy sector face frequent, sophisticated attacks from criminal organizations and geopolitical rivals seeking to extract profit or sow seeds for future disruption of rival economies. Building more wind power multiplies the number of networks and devices that could provide attack pathways if left undefended, or unstable interactions if improperly configured. Expanding the number of employees and contractors working on wind likewise increases the chance of a cyber incident from a disaffected employee or a failure to follow correct protocols.

Cyber incidents that disrupt wind farms pose clear financial risks. Immediate risks include lost production, potential power outages, incident recovery costs, and potentially replacement costs in the event of physical damage. Less obvious but also at stake are reputational risks including lost investor confidence, legal action, and increased regulatory scrutiny and future compliance costs.

Risks that could be considered negligible when wind power was a small portion of overall energy production can no longer be ignored. Wind farm developers, owners, and operators share an interest in cybersecurity risk management strategies that account for the full life cycle of these assets. To ensure secure reliable renewable power delivery, wind farms should be built and operated with a secure by design approach, with systems-level integration in mind, and with the understanding that the threat environment will continue to evolve long after construction is complete.



The Cybersecurity Challenge for Wind

The challenge for wind power is twofold: wind farms must comply with strict cybersecurity regulations, and must in practice provide adequate defenses to a complex set of systems in a harsh, remote real-world environment.

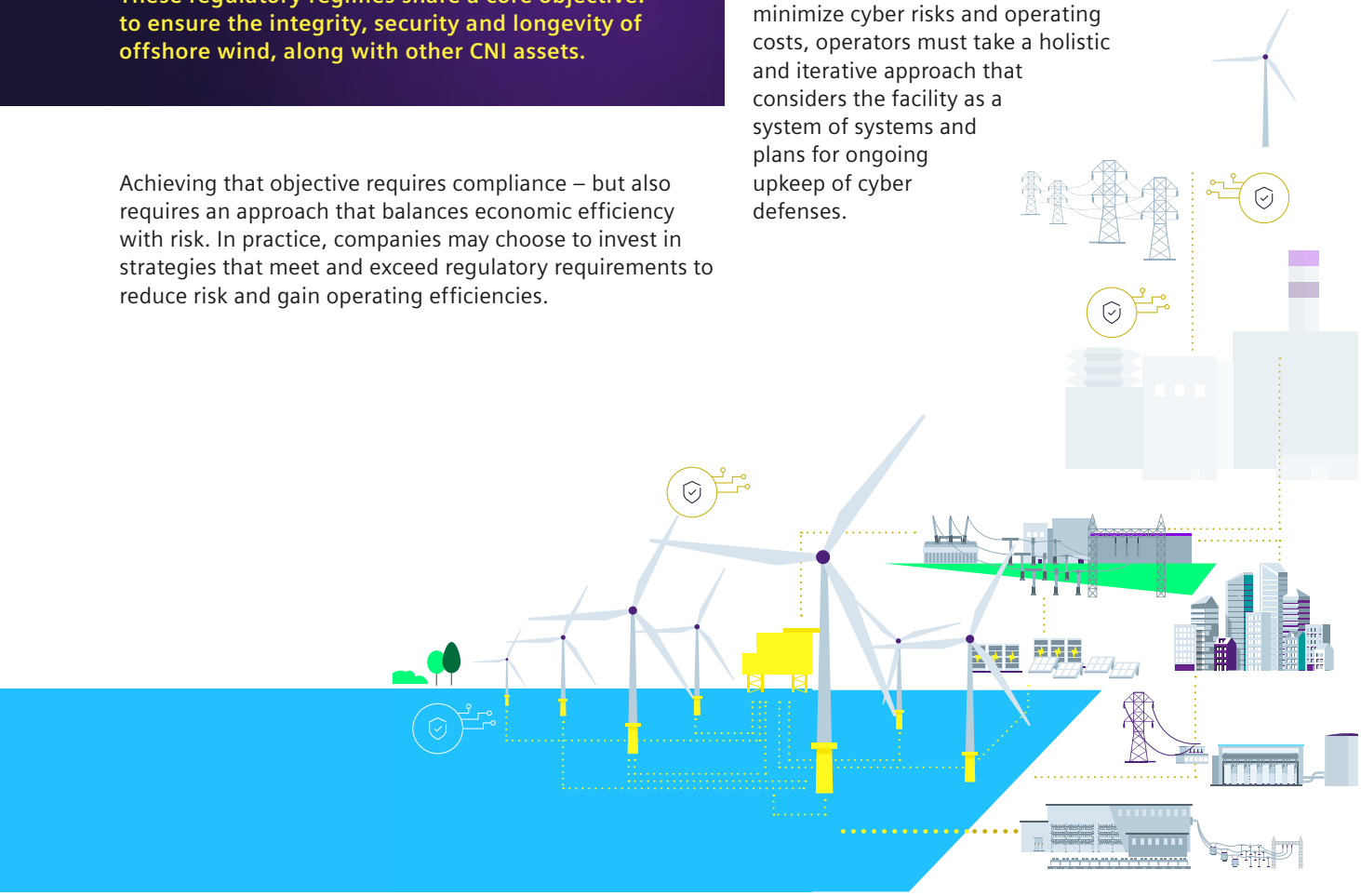
Wind farms face tough cybersecurity standards. This is in part a reflection of wind power's economic success, now providing a non-negligible portion of power to regional and national economies. Legislators correctly discern that disruptions to wind power production could lead to high-consequence power outages, and include wind as part of Critical National Infrastructure (CNI). Standards such as the Network and Information Security (NIS) Directive, NIS 2022/2555, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), KRITIS in Germany, and VGB PowerTech standards apply to wind power. The EU has also implemented cybersecurity measures and surveillance standards for offshore wind, as part of critical infrastructure, along with the new EU Maritime Security Strategy (EUMSS) and Action Plan.

These regulatory regimes share a core objective: to ensure the integrity, security and longevity of offshore wind, along with other CNI assets.

Achieving that objective requires compliance – but also requires an approach that balances economic efficiency with risk. In practice, companies may choose to invest in strategies that meet and exceed regulatory requirements to reduce risk and gain operating efficiencies.

Wind farms differ from other forms of power production in ways that make cybersecurity both more important and more challenging. Conventional power plants are centralized and possible to secure physically; wind farms occupy physical footprintso of the size of large villages, and may be located up to 150 kms offshore. Operators at conventional plants control inputs; wind power must respond to environmental conditions. Conventional power plants have staff on site on a daily basis; bringing staff to offshore wind facilities is costly. Solving these challenges calls for a complex set of subsystems working together as a unified whole.

Current process-based approaches often used in wind infrastructure require that each primary technology supply its own separate control system. In this model, suppliers shoulder the responsibility for delivering on performance guarantees and complying with national and regional cybersecurity standards. This approach is no longer fit for purpose. Faced with a dynamic threat environment, static defenses degrade rapidly and will leave assets vulnerable until patched. Subsystem defenses designed without interoperability leave blind spots for analysts, or require retrofits. To minimize cyber risks and operating costs, operators must take a holistic and iterative approach that considers the facility as a system of systems and plans for ongoing upkeep of cyber defenses.



The Secure By Design Opportunity

Cybersecurity is a risk management journey with compliance milestones. Securing any piece of energy infrastructure will require ongoing attention and effort to keep ahead of evolving threats, maintain subsystems that degrade at different rates, and meet regional compliance requirements.

A **secure by design approach** to developing and operating wind farms is **more effective and less expensive**. Instead of treating cybersecurity as an afterthought, wind power developers, owners, and operators work together to ensure that cybersecurity is considered as a design factor from its earliest design to its ongoing operation. A secure by design approach ensures that the **site architecture will enable integrated, unified defenses, will provide for maintenance and upgrades like software patches, updates, and cybersecurity monitoring.**

Design choices affect the operating costs associated with cybersecurity. For example, standardizing equipment and configurations across the wind farm simplifies cybersecurity monitoring. Understanding which assets will need differing levels of monitoring can make networks easier to secure appropriately. Planning for ongoing monitoring of unified data streams can enable outsourcing for cybersecurity monitoring services.

At each phase in the life cycle, it should be clear who bears responsibility for cybersecurity. Assigning responsibility for securing subcomponents without assigning responsibility for securing the whole system will lead to fragmentation, blind spots, incompatibility, vulnerabilities, and future expense. The designated person who will bear responsibility for integrated, site-wide cyber defenses should be known and involved in design decisions from the earliest phases of design. Likewise, there should be a clear chain of command for cyber defenses once the site is operational.

Secure by design approaches set wind farms up for success, **facilitating the clear accountability, site architecture, continuous monitoring, evaluation, and updates to cybersecurity** that defenses will need to remain effective and compliant.

"Security by design" is a philosophy that prioritizes cyber security in the early stages of a new build project's lifecycle and encourages owners and providers to think, buy and design cyber security – as part of the functionality.



The Secure By Design Approach

Siemens Energy partners with wind farm developers, owners, and operators to guide the cybersecurity journey. As an original equipment manufacturer, Siemens Energy has a **deep understanding of the engineering requirements for offshore wind, as well as the regional regulatory environments in the EU and around the world**. Siemens Energy has invested in developing purpose-built cybersecurity solutions and services for operational technologies (OT), applying secure by design principles to manage risk, streamline compliance, and mature cyber security for energy infrastructure.

Siemens Energy's combination of **global presence, engineering know-how, and cybersecurity experience** means that we are able to guide clients to **affordable, effective solutions** for their site's specific needs. We have the technical capacity to serve as the **integrator of the many complex subsystems** needed to securely operate a wind farm. Siemens Energy follows a certified approach to **Secure by Design and lifecycle management pre-process,** like ISO 27001 and IEC 62443-4-1. We offer a cyber-informed engineering (CIE) focus on reducing risk.

Just as important as the technical competence, we understand that the **profit engine of a wind farm depends on maximizing uptime**. We understand how to deploy and update cybersecurity systems with **minimal disruption to power production**. We build cybersecurity to protect assets against low-probability, high-consequence cyber incidents, and have invested in technologies designed to enable operators to quickly contain and recover from cyber incidents that do occur. For wind farms in particular, the ability to remotely and quickly determine which equipment has and has not been affected by a cyber incident can be a major factor in the cost of recovery after a cyber incident.



Benefits of Siemens Energy's Offshore Security Solution



Manufacturer-Agnostic:

Siemens Energy can integrate equipment across manufacturers and machine languages to create a unified, holistic cybersecurity environment

Regulatory Expertise:

Siemens Energy has long experience with OT cybersecurity regulations in markets around the globe

AI-driven Automation:

Siemens Energy's proprietary machine learning engine assists in analyzing huge data volumes with machine-like speed

Engineering Excellence:

Siemens Energy brings a long heritage as an original equipment manufacturer to our OT cyber-security approach

Evergreen Security Approach:

Cybersecurity at the core from commissioning to end of life

Securing Integrated Wind Systems

Omnivise T3000 enables secure integration and automation for the many complex subsystems that comprise a wind farm. Siemens Energy's Omnivise T3000 is a comprehensive solution that manages the control and automation functionalities across various parts of an offshore wind farm. It can manage control functionalities, substation automation functionalities, and SCADA functionalities. As a reliable partner, we're supporting energy producers worldwide in advancing the energy revolution in almost 4,000 projects worldwide.

Siemens Energy and Omnivise T3000 help standardize operations. Siemens Energy has selected strategic partners and suppliers that meet cybersecurity standards. Omnivise T3000 includes powerful vulnerability management, architecture mapping, and network intrusion detection powered by Tenable. We use systems like Radius, Diameter, or TACACS+ to manage authentication, authorization, and accounting solutions. Together, these capabilities help defenders determine not just whether systems are open to attack, but also whether trusted insiders or known devices have been hijacked.

Omnivise T3000 enables operators to easily remain in compliance with standards like IEC 62443 while implementing architecture that meets the needs of large-scale wind power. Typical wind power worksites call for three main layers: operation, engineering and cybersecurity. Omnivise T3000 provides security appropriate to the assets in each network zone, and can provide Virtual LAN (VLAN) connections that meet the network segregation requirements.

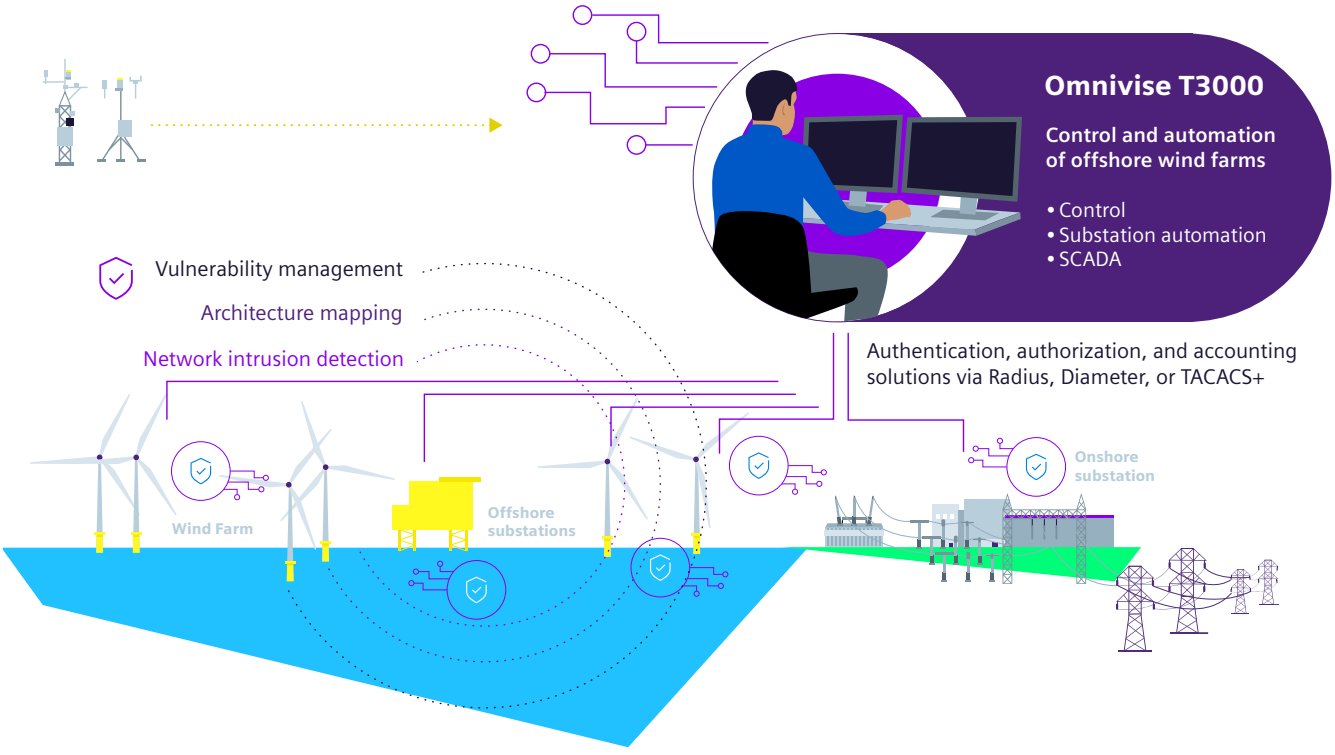
Siemens Energy has developed integration and serviceability concepts for each piece of equipment, encompassing life cycle management and cybersecurity integration. This strategy allows Siemens Energy not only to integrate such equipment into projects but also provide servicing for assets during and beyond the warranty period.

Siemens Energy's standardization and existing partnerships enable a wind farm developers, owners, and operators to enjoy a smoother experience. Devices across the wind farm integrate seamlessly. Unified Human-Machine Interfaces (HMI) reduce the need for operators to learn several interface formats for maintenance. Cybersecurity management becomes easier, with more comprehensive visibility into monitored systems and streamlined patch and vulnerability management.

Comprehensive Control & Automation Functionality

Advanced Embedded Security Controls

Scalable Industrial Control System Architecture



Setting the New Standard for Unified Cybersecurity

Siemens Energy recommends that wind farms incorporate a Unified Cyber Monitoring Center (UCMC). Designing with a UCMC in mind from the earliest stages helps align many decisions about how various hosted functionalities will be deployed across the whole of the wind farm.

Establishing a UCMC ensures that the correct technical capabilities – both in terms of equipment and personnel – exist in a centralized, systematic way, and are available to advise and act on the decisions of the person accountable for cybersecurity.

Over the course of a wind farms 25–35 year life span, a UCMC also serves as part of a cyber serviceability plan.

Cyber serviceability accounts for the fact that over decades of operation, a wind farm will almost certainly see new cyber threats emerge, new regulations come into effect, and current software become obsolete. Adapting and updating cybersecurity solutions and software is easier when the equipment, software and personnel are centralized and systematically tracked, instead of fragmented and scattered across the wind farm.



Siemens Energy's Offshore Security Approach Gives Wind Operators the Tools to Programmatically Combat Cyber Risk



Foundational Security Excellence

1. **Software Updates:** managing patterns for updating software.
2. **Patch Administration:** handling and implementing required software updates and patches to address known vulnerabilities.
3. **Firewall Administration:** managing the function and configuration of firewalls to prevent unauthorized network access.
4. **Endpoint Security:** managing the security of all endpoints, such as computers and other devices connected to the network.
5. **Unified DMZ:** a dedicated DMZ zone enables access to the equipment installed in the Wind Park from outside.
6. **Data Diode for Data Extraction:** using a data diode to extract data to the IT environment.
7. **Encrypted Communication to IEDs:** ensuring secure communication to Intelligent Electronic Devices (IEDs).



Realtime Visibility & Context

1. **Vulnerability Evaluation:** consistently evaluating the network and systems for potential weak spots and suggesting corrective actions.
2. **Network Surveillance:** providing constant scrutiny of network activities to identify any abnormal behavior or traffic patterns.
3. **Log Administration:** gathering and scrutinizing log data from multiple sources for audit, compliance, and forensic purposes.
4. **Access Supervision:** handling access control to different parts of the network and systems, ensuring that users only have the necessary access for their tasks, and two-factor authentication is appropriately implemented.
5. **Intrusion Identification and Mitigation:** employing IDS / IPS systems to spot and counter potential cyber incidents.
6. **Threat Identification:** continuously monitoring network traffic and system activities to detect potential threats or harmful activities.



Preparedness & Resilience

1. **Disaster Recovery Strategy:** formulating and executing plans for restoring operations in the event of a significant incident or disaster.
2. **Incident Management:** If a security incident is detected, triggering appropriate response actions to reduce the impact, which may include isolating affected systems or shutting down certain operations.

Conclusion

Wind farms and offshore wind provide a growing share of power to major economies. With that growth comes an increased need to responsibly manage the cyber risks associated with these large, complex, facilities and their harsh remote environments. Because digital devices sit at the heart of wind farms and must integrate their many subsystems, cyber defenses must be strong and comprehensive.

Current approaches to cybersecurity for offshore wind focus on process-based compliance, and insufficiently address the risk that vulnerabilities will arise in the integration of subsystems and the absence of clear accountability for securing the overall wind farm. Companies that take a secure by design approach and consider the complete life cycle of their assets stand to gain a competitive advantage by reducing operating costs while improving security and performance.

Secure by design decision making and strict regulatory environments should lead wind farm developers, owners, and operators to invest in unified cyber management centers as a means to streamline compliance and cyber serviceability.

With its deep knowledge of engineering requirements, regional regulatory environments, and cybersecurity, Siemens Energy is a valuable partner for wind farm developers, owners and operators seeking assistance in securing wind assets across their life cycle.



Published by

Siemens Energy Global GmbH & Co. KG
Gas Services
Siemenspromenade 9
91058 Erlangen, Germany

Siemens Energy Inc.
4400 Alafaya Trail
Orlando, FL 32826, USA

For more information, please visit our website:
siemens-energy.com/wind-offshore-controls

© Siemens Energy, 2024

Subject to changes and errors. The information given in this document only contains general descriptions and/ or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.
All product designations trademarks or products of Siemens Energy Global GmbH & Co. KG or other companies whose use by third parties for their own purposes could violate the rights of the owners.

Siemens Energy is a trademark licensed by Siemens AG.