Cybersecurity Design Considerations for Offshore Wind Energy Facilities Based on IEC 62443

Jason Dearien and Sagar Dayabhai
Schweitzer Engineering Laboratories, Inc.

Presented at the
CIGRE Paris Session 2026
Study Committee D2 Information Systems,
Telecommunications & Cybersecurity
Paris, France
August 23–28, 2026

Cybersecurity Design Considerations for Offshore Wind Energy Facilities Based on IEC 62443

Jason Dearien and Sagar Dayabhai, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Offshore wind energy facilities are deployed as part of national energy transition strategies, introducing complex protection, automation, and control (PAC) systems distributed across offshore and onshore environments. These systems rely on extensive digital communication and remote connectivity, which significantly expand the cybersecurity attack surface and introduce new operational risks. In offshore environments, limited physical access, high availability requirements, and reliance on wide-area communications necessitate a cybersecurity approach that is embedded into system design rather than applied retrospectively.**

This paper presents a cybersecurity design approach for offshore wind energy facilities based on the principles of the IEC 62443 standard series. The proposed methodology focuses on architectural decisions that balance cybersecurity, availability, and deterministic performance, with particular emphasis on the application of zones and conduits, risk-based assignment of target security levels, and defense-in-depth.

Key design considerations include redundancy and availability strategies, secure remote access, demilitarized zone (DMZ) design, and system hardening, all tailored to the practical constraints of offshore deployment. The design approach presented aims to assist utilities and developers in engineering cybersecure offshore wind energy facilities that support long-term reliability, regulatory compliance, and secure integration with modern power systems.

***Keywords*—IEC 62443, PAC, IEC 61850, OT-SDN**

I. Introduction

With energy security becoming critical, nations are prioritizing domestic renewable sources to reduce dependence on external supply and enhance energy sovereignty. Wind power offers a resilient and sustainable solution, positioning itself as a cornerstone for global industrial growth [1]. Offshore wind has become a key technology in the energy landscape of today. Globally, more than 80 GW of offshore wind capacity is already operational and supplying power to approximately 70 million households, driving economic growth [1]. The Asia Pacific region currently holds the largest global share of offshore wind installations, with China leading with roughly half of the global offshore wind market share. Europe ranks second, with the UK being the second largest installer of offshore wind [1]. An additional 48 GW is under construction, and projections indicate continued expansion. The International Energy Agency estimates more than 280 GW of installed capacity by 2030 [1].

The rapid growth of offshore wind energy facilities has been accompanied by increasing system complexity and digitalization. Modern offshore wind farms rely on geographically distributed PAC and communications systems that interconnect wind turbines, offshore substations, and onshore control centers. These systems depend on high levels of automation and remote connectivity to support continuous operation, monitoring, and maintenance. Once in place, this architecture is leveraged to support efficient operation, monitoring, and expansion, but it simultaneously increases cyber exposure.

Compared to many traditional onshore generation facilities, offshore wind energy facilities are inherently more exposed to cyber risk due to their distributed topology, reliance on remote access, and dependence on WAN communications. Multiple interconnected systems, often separated by long distances and harsh environmental conditions, create additional potential access points for cyber threats. As offshore wind continues to scale in size and complexity, cybersecurity must therefore be addressed as a fundamental design consideration integrated alongside safety, availability, and operational performance rather than treated as a standalone or retrospective concern. The remote and exposed nature of offshore installations further increases susceptibility to both cyber and physical threats, reinforcing the need for resilient system-level security architectures.

This paper focuses primarily on system-level cybersecurity design and architecture in line with IEC 62443-3-2 and IEC 62443-3-3. Device-level security aspects aligned with IEC 62443-4-2 are referenced only where necessary to support system-level design decisions.

II. System Requirements and Objectives

Offshore wind energy facilities rely on integrated PAC systems to achieve several operational and security objectives. These systems must support reliable and continuous power generation while operating in remote, harsh environments with limited physical access and high logistical costs. As a result, system design is primarily driven by availability, safety, and correct and dependable operation of PAC functions. These requirements represent some of the most critical system-level objectives that directly influence availability, safety, and recoverability of offshore wind energy facilities:

- Ensure efficient and reliable plant operation to maximize energy output and revenue.
- Support long-term operations, maintenance, and lifecycle management of offshore assets.
- Achieve secure and reliable grid integration with system operators.
- Maximize fault-tolerant operation across offshore assets to minimize downtime and enable rapid

recovery following unforeseen outages or disturbances.
- Secure local networking infrastructure to support onsite administration.
- Enable secure remote access for stakeholders to monitor, manage, and maintain operations while ensuring autonomous local functionality.

Meeting these objectives requires extensive use of digital communications networks, remote access mechanisms, and system integration across both IT and operational technology (OT) domains. While essential for offshore operation, these capabilities expand the potential cyberattack surface.

To mitigate this expansion, cybersecurity must be addressed in a manner that is aligned with operational priorities and the physical, operational, and technical constraints inherent to offshore wind energy facilities. Cybersecurity must be integrated into secure-by-design system architecture and lifecycle processes, rather than added retrospectively or implemented independently of system design and operation. A structured, risk-based approach based on the principles of IEC 62443, complemented by applicable regulatory frameworks such as the European Union directive EU 2022/2555 (NIS2), provides a suitable foundation for achieving this integration.

III. Challenges

The remote offshore location, the scale and distribution of assets, and the increasing reliance on digital connectivity to support operation and maintenance present several technical, operational, and cybersecurity challenges when trying to meet the operation and system objectives of the offshore wind energy facilities in a cost-effective and reliable manner.

The variable nature of wind resources results in intermittent power generation, placing a strong emphasis on maximizing availability to maintain energy output and economic viability [2]. Unplanned outages directly reduce generation capacity and revenue potential, while recovery activities are often delayed by limited access, weather dependency, and the need for special logistics and personnel. As a result, offshore wind energy facilities depend heavily on advanced PAC systems to support rapid fault detection, accurate monitoring and precise time, prompt alarming, and effective disturbance recording and analysis.

Remote connectivity and access is therefore essential for diagnosis, system restoration, and ongoing operational support. However, this introduces significant cybersecurity risk as, in some cases, some of this infrastructure is shared across public infrastructure. Communication constraints associated with offshore locations further complicate this challenge, requiring high-bandwidth and low-latency links to support PAC systems and monitoring functions.

In addition, the convergence of IT and OT systems is necessary to enable integration with external networks, grid operators, and enterprise business systems. While this convergence improves situational awareness, decision-making, and operational efficiency, it also increases system dependencies and expands the potential attack surface. Threat actors frequently leverage IT-based attack techniques, tools, and initial access vectors to pivot toward OT environments. Managing this convergence securely is therefore critical to ensuring that operational benefits are realized without compromising system availability and safety of the PAC systems.

These challenges highlight the need for a structured cybersecurity approach that addresses both technical and operational risks in a coordinated manner. A framework based on the principles of IEC 62443, including defense-in-depth, zone and conduit segmentation, and risk-based security level assignment, provides a suitable foundation for managing cybersecurity in offshore wind energy facilities while accommodating their unique operational constraints.

IV. IEC 62443 Design

Offshore wind farms are recognized as critical infrastructure under NIS2 (EU 2022/2555), which imposes stringent cybersecurity requirements on operators of essential services [3]. These requirements include the implementation of appropriate technical and organizational measures for risk management, incident handling and reporting, and supply chain security.

The IEC 62443 standard series provides a structured, risk-based framework that supports alignment with these regulatory requirements. By applying IEC 62443 principles at the system architecture level, offshore wind operators can support cybersecurity governance, resilience, and risk mitigation requirements in a consistent and auditable manner [3]. Concepts such as security zoning, controlled communication pathways, and defense-in-depth enable cybersecurity controls to be implemented proportionally across geographically distributed systems in the offshore wind energy facility and remote operational environments.

A key element of applying IEC 62443 is the determination of the appropriate target security levels (SL-T) for different parts of the system [4]. The required security level for any given zone is not uniform across an offshore wind energy facility and depends on multiple factors, including the outcome of the cybersecurity risk assessment for that system, the criticality of the function and system, the applicable regulatory obligations, and the potential operational impact of security controls on system performance and functionality. In offshore wind energy facilities, where continuous operation and timely response to disturbances or emergency conditions are essential, cybersecurity mechanisms must be carefully selected to avoid introducing latency, instability, or unintended denial-of-service conditions that could compromise safety or availability.

Security Levels are typically assigned based on the criticality and role, connectivity, and potential system-wide impact of each zone. Zones performing time-critical local control functions may target SL-T 2, while zones with supervisory or system-wide control responsibilities commonly target SL-T 3. In offshore wind energy facilities, this often results in wind turbine and offshore substation zones targeting SL-T 2, whereas onshore control and wide-area communication environments typically target SL-T 3. In some regulatory

contexts, security levels may be defined per foundational requirement (FR), resulting in differentiated SL-T values across FRs rather than a single uniform target.

IEC 62443 supports the use of compensating countermeasures, allowing security functions to be implemented at the system or architectural level when individual components cannot meet specific target requirements [2].This risk-based and architecture-driven application of IEC 62443 principles provides a foundation for designing secure offshore wind communications networks as discussed in the following sections.

A. Communications Network

Offshore wind energy facilities comprise multiple systems and networks that must interoperate across geographically distributed offshore and onshore environments. The communications network must therefore support traffic with different criticalities and performance requirements. Time-critical PAC communications based on the IEC 61850 series GOOSE messages associated with substation protection and park control must meet strict latency and performance metrics while non-real-time operational traffic is accommodated concurrently on shared network links.

In many practical installations, networks supporting PAC functions and wind turbine systems are segregated from other operational networks. This is achieved using Virtual Local Area Networks (VLANs), controlled routing, traffic prioritization mechanisms, and firewalls that inspect and manage traffic between network segments and between offshore and onshore environments. This separation reflects the multivendor nature of offshore wind installations and the need to tightly control access to mission-critical OT systems.

The communications architecture is developed in accordance with IEC 62443-3-2 by defining zones, conduits, and associated security requirements at the system level [4]. This architecture aligns with the principles of IEC 62443 by enforcing defined trust boundaries and restricting communications paths. Defense-in-depth is realized through multiple, independently managed firewalls at key network boundaries, ensuring that failures or misconfigurations at a single point do not compromise the wider system. The resulting architecture depicted in Figure 1 provides a controlled and resilient foundation for offshore wind operations.

The communications architecture illustrated in Figure 1 concentrates on turbine, offshore substation, and onshore control center systems, as these constitute the most time-critical and safety-relevant components of offshore wind energy facilities. While additional systems such as fire detection, security, and auxiliary services are not shown in detail, the same segmentation and security principles apply to their integration.

These architectural mechanisms form the basis for applying the IEC 62443 zone and conduit model to formally define security zones, classify communications paths, and assign appropriate security requirements across the communications network. The following section examines the application of zones and conduits within offshore wind energy facilities.

B. Zone and Conduit Model

The communications architecture described in the previous section applies the IEC 62443 zone and conduit model to structure and control data exchange within offshore wind energy facilities. Systems are grouped into zones based on operational role and function, location, and required level of security, with conduits defining the permitted communication paths between them [5].

In offshore wind energy facilities, zones are primarily defined by the separation between offshore and onshore environments and by grouping systems that perform similar PAC functions with comparable real-time and security requirements. As illustrated in Figure 2, the PAC systems in the offshore side of the wind energy facility form distinct zones for the substation and wind turbine network, separated from the onshore control and supervisory systems and WAN communications. The communications network, comprising redundant fiber and microwave links, is treated as a separate zone to reflect its exposure and operational characteristics.

SL-Ts are assigned per zone based on risk assessment outcomes and may vary by FR rather than being uniformly applied across all requirements. Communication between zones is restricted to defined conduits that are explicitly engineered and protected. These conduits are implemented using firewalls and explicitly routed interzone links with additional controls, such as encrypted tunnels and DMZs where communication traverses offshore, onshore, and external networks. Communication to these external networks is only permitted through managed interfaces located within DMZs.

By applying zones and conduits in this manner, communication between offshore, onshore, and external networks is restricted to explicitly defined communication paths, ensuring that network faults, system misconfigurations, or security events are contained within their respective zones and do not directly impact PAC functions elsewhere in the facility. This structured approach provides a practical foundation for assigning security levels to individual zones and for introducing more granular segmentation mechanisms and zero-trust networking, as discussed in subsequent sections.

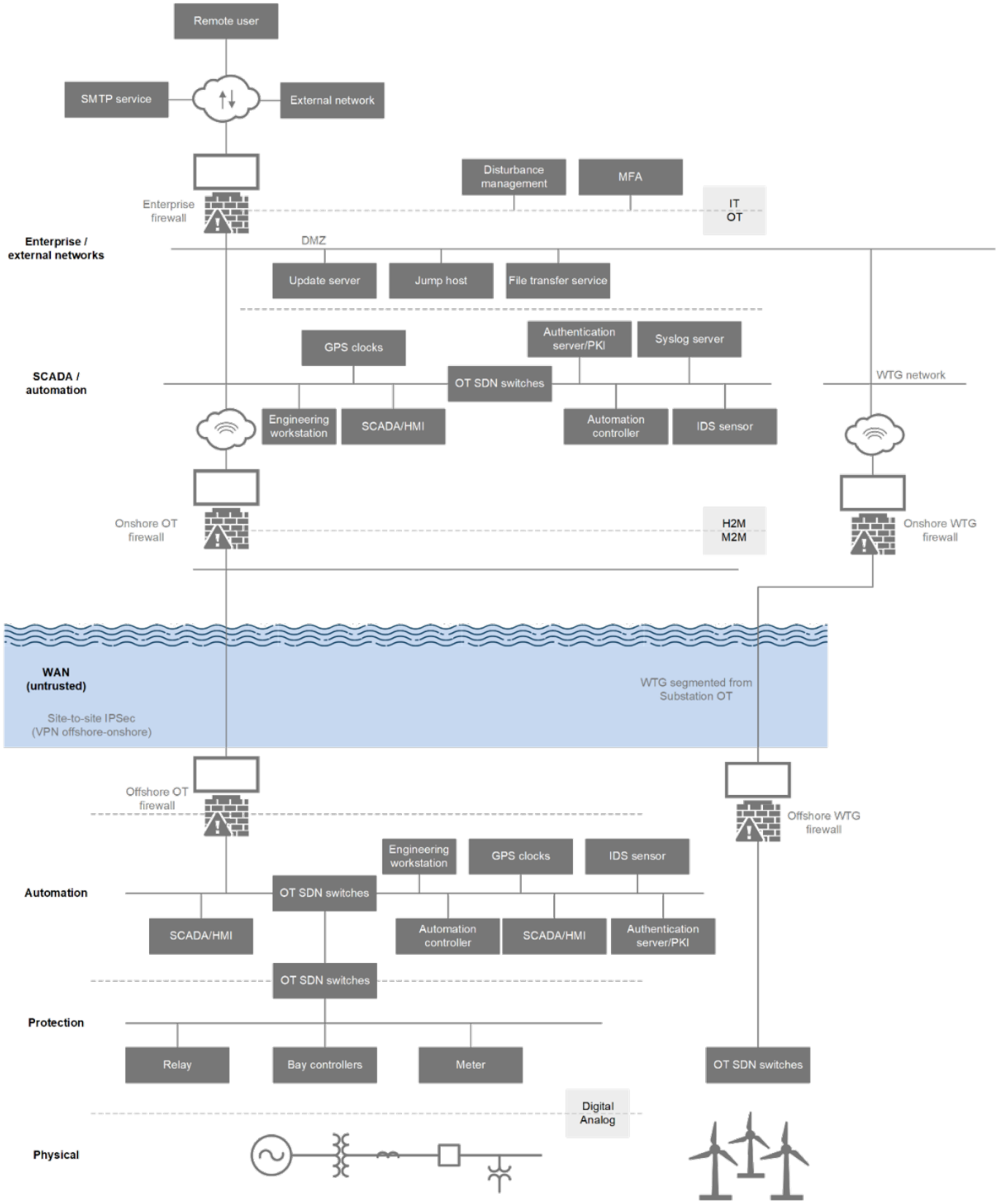

Figure 1 - Typical Network Architecture of Offshore Wind Energy Facilities

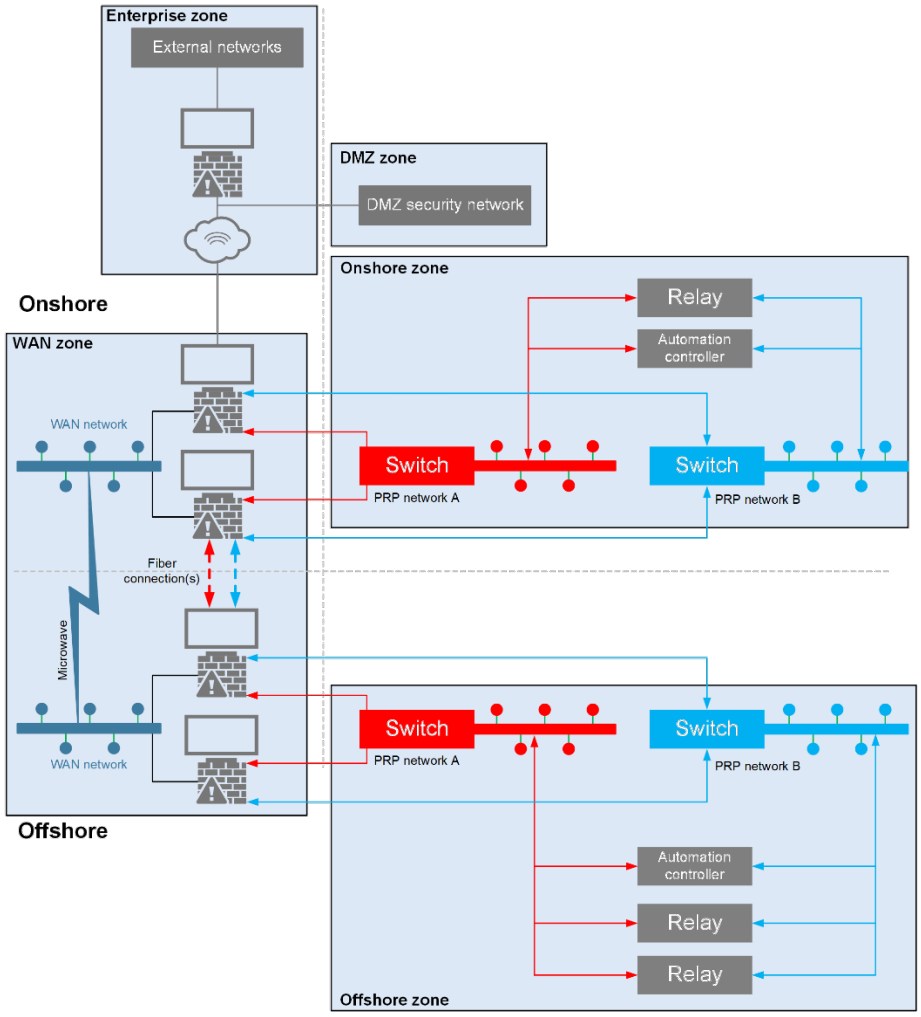

Figure 2 - Zone and Conduit Model

V. CYBERSECURITY DESIGN

Building on the communications architecture and zone and conduit model, this section examines key cybersecurity design considerations for offshore wind energy facilities. The focus is on practical system-level design decisions that directly influence availability, resilience, and recoverability in offshore environments.

A. System Redundancy

Redundancy and availability mechanisms in offshore wind energy facilities are selected based on the consequences of communication loss, including impacts on safety, generation availability, and the ability to recover without offshore intervention. Given the logistical challenges and high cost of offshore access, network designs should prioritize continued operation or rapid autonomous recovery under fault conditions.

Where substation PAC functions require uninterrupted and deterministic communication to maintain safe operation, fault-tolerant designs are applied. These systems are typically based on IEC 61850 and employ the use of Parallel Redundancy Protocol (PRP).

Other OT networks within offshore wind energy facilities typically adopt high availability designs rather than strict fault tolerance wherever appropriate and applicable. These designs rely on redundant network devices, cabling, and topologies (e.g., ring-based architectures) to enable rapid recovery following a device, link, or switch failure. In offshore wind energy facility, redundancy is implemented by duplicating critical systems across offshore and onshore locations. This replication ensures that the loss of a single site or subsystem does not result in a loss of visibility, supervisory control, or the ability to manage and recover the PAC systems.

Communication between offshore and onshore sites is further protected through physically diverse wide-area communications links, commonly combining subsea fiber-optic cables with alternative technologies, such as microwave links. This physical diversity improves resilience against cable damage, environmental conditions, and external disruptions while maintaining the connectivity required for PAC across the wind farm.

An additional practical consideration in offshore wind facilities is the selection of next-generation firewalls capable of supporting these redundancy requirements. Firewalls deployed at offshore and onshore electrical security perimeters must provide sufficient processing performance for deep packet inspection and encryption while operating on industrial-hardened computing platforms suitable for harsh environments which also support PRP. In addition to security enforcement,

the firewalls are responsible for monitoring the availability of the primary fiber-optic link and automatically failover traffic to the microwave link in the event of a failure, as illustrated in Figure 2.

B. Access Control

Access control in offshore wind energy facilities is enforced at the onshore DMZ and offshore-onshore WAN firewalls and on individual OT systems. The onshore-offshore WAN firewalls restrict which connections are permitted into PAC networks, while user access to IEDs is controlled using directory-based authentication and group-based permission mapping either directly to the IED or via proxy gateways.

In a typical implementation, centralized authentication is provided using directory services, such as Microsoft Active Directory Domain Services, with redundant domain controllers deployed at offshore and onshore sites, respectively. This ensures that authentication remains available during various loss-of-communication situations. Human access is governed through directory-based authentication and role- or group-based authorization, while machine-to-machine communications rely on certificate-based authentication and explicitly defined conduits between zones.

To support certificate-based authentication and encrypted communications within and between OT zones, a dedicated public key infrastructure is deployed within the wind energy facility. This typically includes a locally managed root certificate authority (CA) acting as the trust anchor, with separate intermediary CAs for each electrical security perimeter (i.e., onshore and offshore environments).

C. Secure Remote Access

Secure remote access is required to support offshore wind energy facility operations, maintenance, diagnostics, and manufacturer support while traversing untrusted networks. The remote access is therefore designed to provide controlled connectivity without exposing PAC systems directly to external networks.

Client-to-site VPN access is terminated at the enterprise firewall using enterprise-managed user accounts with multifactor authentication, as shown in Figure 1. VPN users are restricted to a dedicated access role that permits connectivity only to the onshore OT DMZ. Direct VPN access to onshore or offshore OT networks is not permitted.

Within the OT environment, authentication and authorization are performed independently of enterprise identity systems. Users authenticate to a jump host located in the onshore OT DMZ using OT-managed credentials. From this jump host, authorized sessions are initiated to onshore and offshore engineering workstations and SCADA servers through the onshore OT firewall.

When accessing the offshore engineering workstations and SCADA servers, site-to-site VPN tunnels are used to secure communications traversing the offshore-onshore WAN, ensuring that OT traffic between offshore and onshore environments is encrypted and authenticated over the untrusted WAN communications infrastructure. Enterprise-managed identity and multifactor authentication are used exclusively to control client-to-site VPN access at the enterprise firewall, while authentication and authorization within the OT environment are enforced using OT Active Directory and group-based access control. This ensures that enterprise identity systems do not extend trust into the OT networks and that access to PAC systems is governed entirely by OT-managed security controls.

D. DMZ Design

DMZs are used to host systems that require controlled interaction between enterprise and/or external and OT networks without exposing PAC systems directly to untrusted environments. In offshore wind energy facilities, the DMZ is implemented as a security zone located between the enterprise network and the onshore OT network, provisioned by dedicated firewalls as shown in Figure 1 and Figure 2.

Systems deployed within the DMZ are limited to the jump host for remote access, update and patch management server, log forwarders, and file transfer server. These systems are configured to initiate or relay communications in a controlled manner. Firewall policies strictly constrain permitted protocols, source addresses, and destinations, ensuring that OT systems are reachable only from explicitly authorized DMZ hosts. The DMZ is designed to be isolatable under fault or incident conditions. This containment capability limits the propagation of any malicious traffic and supports incident response while maintaining plant availability.

E. System Hardening

System hardening measures are applied to reduce the attack surface of OT assets at the component level where required to support system-level security objectives while preserving deterministic behavior and operational availability. In offshore wind energy facilities, application control is implemented using allowlisting techniques that permit only authorized applications and binaries. Allowlisting is complemented by endpoint protection and host-based intrusion detection systems (HIDS) to monitor authorized applications for malicious behavior, protect memory and file systems, and detect compromise within permitted software. Operating systems are hardened using established configuration baselines, such as Center for Internet Security (CIS) benchmarks, with a minimum of Level 2 applied where operationally feasible.

VI. Zero-Trust Enablers

The communications architecture described in the previous sections is based on established industrial networking practices, including VLAN-based segmentation, routed communication between zones, and firewall-enforced conduits. These approaches can become increasingly complex to manage as offshore wind energy facilities scale in size from a security, management and configuration perspective. Zero-trust networking, implemented through SDN, provides an alternative architectural approach that enables granular control of communications while reducing configuration complexity and improving visibility.

SDN is the foundation of zero-trust network implementations as noted by the NSA [6]. SDN provides deny-by-default network capabilities, which is a recommended enhancement in the IEC 62443 standard [2]. The standard also requires logical separation of both control vs. noncontrol networks and critical control vs. noncritical control networks. The standard also has recommended enhancements to provide physical isolation of control and non-control (critical or otherwise) networks [2]. SDN also acts as a compensating system-level control, enabling security objectives to be met even when individual field devices lack native support for advanced security functions. OT-SDN satisfies these requirements by giving the network designer complete control over all the communication circuits in the LAN.

With OT-SDN the granular control of each communication circuit between any two devices will be independently defined (using TCP/IP Layer 4 match criteria) so only designed communications are allowed, including the directionality of the initiating request. This circuit independence is also what provides the required logical segregation between control and/or noncontrol and critical and/or noncritical communications. Each circuit is independent from every other circuit, even if the source and destination device are the same. Two devices may be having both critical and noncritical conversations and they will be logically independent. The traffic that goes through these independent circuits can also be uniquely prioritized (without the need for VLAN tagging) and physically segregated onto different network cables and/or switches if desired.

In addition to applying SDN within the OT LAN, similar principles can be extended to the offshore-onshore WAN. Offshore wind facilities typically rely on a primary fiber-optic link with a secondary microwave link for resilience as shown in Figure 2.

A. Simplified and Superior Microsegmentation

In the onshore and offshore OT network, there will be many independent control systems that are often installed, maintained, and/or operated by different groups. In a zero-trust LAN, these disparate systems should be isolated from each other so cross-communication is not possible. Traditional IT network practices would use port-based VLANs and restrictive IPs and/or subnets to enforce this separation. This practice requires careful planning and configuration but when implemented it does not control and/or restrict any of the communications between devices in a single system, just between different systems. By implementing OT-SDN on the LAN, then extreme microsegmentation is accomplished without the need for restrictive IPs and/or subnets, or port-based VLANs, so configuration is simplified. Only devices that need to communicate are allowed to communicate, and if devices in different systems need to share data, they can do so easily without the need for VLANs and routers.

B. Diagnostics, Monitoring, and Detection

With OT-SDN, each of the independently defined communication circuits records traffic statistics for each circuit. These statistics can be monitored to give visibility to the health of the control system. Most machine-to-machine (M2M) communications are very regular so statistics on a circuit should be very consistent. If the statistics stop increasing, that may be an indication of a problem and if the counters increase significantly, it may be an indicator of compromise. Human to Machine (H2M) communications could also be monitored to look for odd behavior, like remote sessions to jump hosts or access to IEDs being used in the middle of the night when no one should be working.

OT-SDN allows a copy of the traffic from any of these circuits to be sent to the local Intrusion Detection Sensor (IDS), located at the onshore and offshore OT network, without any per-switch sensor infrastructure. The network designer can decide which circuits should be mirrored to the IDS and which ones are not necessary. It could be that some M2M communications are not required to be monitored but all H2M communications should be.

Because of the deny-by-default nature of OT-SDN, erroneous traffic is automatically quarantined and easily reported. Any Ethernet packet that enters a switch that does not have a designed circuit to move it across the network will be, by default, dropped and not traverse the network at all. It is also for these packets to be sent to the local IDS for detection.

VII. Conclusion

This paper has presented a system-level cybersecurity design approach for offshore wind energy facilities based on IEC 62443 principles, with a focus on practical architectural decisions that balance cybersecurity, availability, and operational constraints. Offshore wind environments introduce unique challenges, including geographical separation, limited physical access, high availability requirements, and reliance on wide-area communications, all of which must be addressed as part of the cybersecurity design rather than as afterthoughts.

By applying IEC 62443 concepts, such as zones and conduits, target security levels, defense-in-depth, and compensating system-level controls, the proposed architecture enables secure integration of PAC systems across offshore and onshore environments. The paper has shown how established industrial networking practices can be combined with secure remote access, robust access control, redundancy strategies, and system hardening measures to achieve resilient operation without compromising deterministic performance.

The discussion further highlights how emerging approaches, including SDN and zero-trust principles, can enhance visibility, segmentation, and policy enforcement in complex offshore wind environments, particularly where traditional device-level security capabilities are limited. Together, these design considerations provide a practical foundation for utilities and developers to engineer cybersecure offshore wind energy facilities that support long-term reliability, regulatory compliance, and secure integration with modern power systems.

VIII. REFERENCES

[1] R. Williams, F. Zhao, N. Melkonyan, M. Hutchinson, and J. Cheong, "Global Offshore Wind Report 2025," Global Wind Energy Council, Lisbon, Portugal, 2025.

[2] IEC-62443-3-3, *Industrial Communication Networks – Network and System Security* – Part 3-3: System Security Requirements and Security Levels, 2013.

[3] Official Journal of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council," *On Measures for a High Common Level of Cybersecurity across the Union*, December 2022. Available: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[4] IEC 62443-3-2, *Security for Industrial Automation and Control Systems* – Part 3-2: Security Risk Assessment for System Design, 2020.

[5] IEC 62443-4-2, *Security for Industrial Automation and Control Systems* – Part 4-2: Technical Security Requirements for IACS Components, 2019.

[6] National Security Agency, "Cybersecurity Information Sheet," *Advancing Zero Trust Maturity Throughout the Network and Environment Pillar*, March 2024. Available: media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF.

[7] S. Dayabhai and P. Diamandis, "Implementation of Smart-Grid Technologies for Automation & Control in a Grid Connected Wind Energy Facility in South Africa," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2015.

Previously presented at the CIGRE Paris Session 2026,
Paris, France
20260410 • TP7253-01