HITACHI
Inspire the Next

Three key considerations for the next generation of offshore wind parks.

Hybrid communications, cybersecurity and the future of offshore wind

Hitachi Energy

It’s no secret that offshore wind is experiencing unprecedented growth and opportunity.

Rapidly increasing global interest in offshore wind is coupled with accelerated adoption of technologies being driven by the macro trend of digitalization. This dynamic is compressing timelines and underscoring the need for project developers to keep abreast of the latest trends and technologies that can be applied to offshore wind parks.

To help developers understand options that can affect the path to reliable and profitable system performance, this paper looks at three technologies that are shaping the conversation:

1. Digital substations
2. Cybersecurity
3. Hybrid communications networks

1 The advantages of digital substations for offshore wind parks

The offshore wind industry's main contribution to the energy transition during last several years has been reducing global CO_2 emissions while maintaining profitably and reducing wind energy's physical footprint and impact on nature. Now it is time to green the heart of offshore wind parks – their substations!

Digital substations are "offshore wind substations"
With all the ecological benefits of offshore wind, the industry's real triumph over its earlier day has been making offshore wind economically viable including successful "zero-subsidy" projects in the Netherlands and Germany.

However, innovation in offshore wind substations has been limited. Already under pressure to guarantee maximum reliability and avoid downtime of its mission-critical generation assets, offshore wind substations must also cope with rapidly changing technologies. These substations must be able to live up to rapid developments on the power generation side, i.e. ever-increasing wind turbine MW ratings (from 0.45 to 15 MW), kV outputs (from 20 to 66 kV) and wind turbine environmental envelopes. In addition to coping with continual technological change, offshore wind substations also need to contribute to overall project success by helping to decrease footprint, CAPEX and OPEX, which reduces total cost of ownership (TCO) and levelized cost of energy (LCOE).

To accomplish this, the industry needs to embrace the next level in offshore wind substations: digital substations. Leveraging over a decade of innovation from onshore substation technology, digital substations have proven their ability to perform in conditions that make them more relevant and impactful in offshore environments and they possess the characteristics to be the industry's next step in greening offshore wind profitably. Wind parks that adopt digital substations will realize several advantages because they are:

- **Safer.** Digital substations help reduce the risk of electrical shocks during testing and commissioning by replacing conventional current and voltage transformers (CTs and VTs) with sensors, or low-power instrument transformers (LPITs) that share their measurement digitally over fiber optic to ensure galvanic separation and with superior testing feature of IEC 61850.
- **Greener.** Digital substations reduce risks of erosion, weight and space by replacing copper cables with fiber-optic cables.
- **Faster.** Modular design of digital substations reduces installation time and onsite testing and commissioning time with pre-manufacture and pre-tested fully digital equipped modules for increased project revenues.
- **Future-ready.** As their name implies, digital substations are at the forefront of system digitalization and enable a whole new level of substation condition monitoring and controls and protection in un-manned offshore wind substation environments.

Reducing the risk of electrical shock.
Replacing CTs and VTs with NCITs makes commissioning and servicing faster, thereby reducing the exposure of personnel to time spent in hazardous environments in an already challenging offshore wind environment. By significantly reducing the time required for commissioning, the risk of electrical shock is dramatically reduced, contributing to the “safety first” culture in offshore wind. All digital interfaces coming from the sensor to the control and protection IED can be simulated and used for testing without requiring the service technicians to enter hazardous environments. Testing of new parameters can even been done from remote without being on the offshore platform.

Reducing space, weight and corrosion risks.
Using fiber-optic communication infrastructure rather than copper cables is a primary advantage of digital substations over traditional substations. In digital offshore wind substations, fiber optics are used not only in the station and bay levels, but all the way through to the process bus in the substations’ protection relay panels. Compared to classical substations, digital substations reduce the amount of copper cable used by up to 80% and reduce relay house space by up to 60%.

For offshore wind parks, corrosion is always a concern. Trends in substation design – such as optimization of housing philosophies for cost savings or for potential reduction of mantling in floating applications – makes offshore wind substations even more vulnerable to corrosion. Fiber-optic cables match these trends much better than copper cables because they are far more resistant to the corrosiveness of humidity and salt.

Protecting offshore wind revenues.
Implementing digital substations that use fiber-optics instead of copper cable and replacing CTs and VTs by NCITs paves the way for modular digital substations in which GIS and electrical protection are merged into one cabinet, eliminating the need for protection panels. Depending on the project size, this can reduce the number of protection panels required by 40 or more. In addition to capital cost savings, this also speeds installation time and reduces space and weight to protect offshore wind revenues.

- Installation time reduction of up to 40%, minimizing the splicing and testing works required for copper cable connections splicing
- Time spent on site for testing can be reduced by combining modular and digital substation technology in the form of integrated GIS applications (IGAs). In a recent offshore wind project Hitachi Energy identified up to three months of time savings for the substation part of the project by benefiting from in-factory-testing vs. on-site testing being enabled through digital IGAs. This savings would not be possible on a conventional substation project.

Moving from failure-based to predictive maintenance in offshore wind substations.
Some form of predictive maintenance has been a reality in wind turbine generators (WTGs) for years. However, most offshore substations are still maintained through regular, time-based inspections independent of the likelihood of failures and, once failures do happen, through reactive maintenance. This approach is both outdated and costly.

Offshore-wind-specialized O&M engineers and site trips are particularly costly and offshore wind vessel costs can exceed US$100K per day. These costs alone are reasons to limit regular inspections, reactive repairs and major replacements.

Digital substations provide an alternative approach. Through advanced SCADA solutions and mission-critical, cyber-secure private wired and wireless communication infrastructure, digital substations can deliver the type of reliable and real-time transmission of sensor data on par with offshore WTGs. When combined with asset performance management (APM) software, digital substations become “smart digital substations.” These solutions can change the maintenance model to be more predictive – and even prognostic – which greatly reduces O&M costs. Due to the mission-critical nature of these workloads, data storage and processing for smart digital substations is performed in the latest, cyber-secure cloud environments.

In onshore digital substations, Hitachi Energy has proven a +10% reduction in asset running costs for transmission substations and expect the savings to be even greater in offshore wind parks where O&M costs are particularly high.

Exceeding typical wind power availability rates
Introducing new solutions to sites with challenging environmental conditions can make some uneasy – and they shy away from introducing digital substations into offshore wind parks for this reason. While it may seem counterintuitive, the new technologies in digital substations deliver distinct advantages that improve reliability over time: they have fewer parts and use less material – especially copper, which is vulnerable to salty and humid conditions.

In fact, one of the world’s largest solar PV plants, ENEL Green Power’s Brazilian 475 MW São Gonçalo project, relies on a fully digital substation for its 500 kV transmission grid connection. The project, located in a hot and humid climate, has experienced zero downtime since its inauguration in January 2020, exceeding the TSO’s requirement of 99.9% uptime since its successful commissioning.

For offshore wind operators that want to take the next step to contractually ensure real performance guarantees, time-based availability warrantees are now offered for digital substations, in addition to WTGs.

A proven track record for a sustainable future
Since installing its first digital substation in 2009, Hitachi Energy, including its predecessor companies ABB and Hitachi ABB PowerGrids, has installed more than 35 digital substations globally that have consistently exceeded the asset uptime of wind or PV generation. Given their many proven advantages, digital substations – and their smart, APM-driven variations – are poised to become the green heart of offshore wind parks everywhere. Learn how Hitachi Energy can help you here.

2 Offshore wind challenges: navigating the cybersecurity threats

Offshore wind as a percentage of the energy mix has grown steadily in recent years. So have cyberattack on power generation companies.

Offshore wind is quickly becoming a mission-critical power source for nations and regions, and governments are setting ambitious new targets for integrating offshore wind into the energy mix. As a result of the industry's rapid growth and increased relevance, safety of people, reliability of power supply, cybersecurity has never been as important for offshore wind developers as they are now. The offshore wind industry digitalization helps interconnect multiple networks, OT systems and locations, increasing overall operational efficiencies, but also introduces cybersecurity concerns previously understood only to office or enterprise IT systems, potentially exposing offshore wind assets vulnerable to cyber attacks. Building a defense in depth cybersecurity architecture is paramount to minimize and manage risk of cyber attacks.

Challenges for organizations starting their cybersecurity journey
Moving into the digital era with confidence requires automated, evolving and resilient cybersecurity solutions that can overcome significant challenges:

- **Regulation**. Understanding cybersecurity regulations and requirements to ensure operational technology (OT) control systems are secure.
- **Emerging technologies**. Introducing new digital technologies creates fear of exposing OT systems to cyber threats.
- **Security culture alignment**. Bringing IT and OT security cultures together means bridging differing objectives and organizational structures. The complexity of human aspect is often underestimated and is very important to manage.
- **Barriers to adoption**. Embracing cybersecurity as an enabler to advanced monitoring and control systems requires a deliberate, sustained education and awareness effort to facilitate organizational adoption.
- **Industry standards**. Industry standards are your friend. Understanding these best practices establishes your blueprint for maturing a cyber posture that supports the utility's digital transformation.

Why should you care about cybersecurity in OT systems?

Cyberattacks usually make news in consumer incidents when many people are affected by identity theft or other security breaches. However, attacks on public utilities have been increasing constantly over the past 10 years and pose a tangible threat to power system integrity. The December 2015 'Sandworm' incident in the Ukraine which targeted utility OT systems highlights the danger. That attack was initiated through a phishing email that switched off 30 substations (seven 110kv substations and twenty-three 35kv substations) and left about 230,000 people without electricity for up to 6 hours. The longer term effect was that the attack allowed adversaries surveil the OT system for months. The attack was initiated with BlackEnergy Trojan malware to access the network, surveil the grid operations gaining system knowledge for months before accessing the operator's machines to take control of the system initiating the attack on the grid. To delay recovering, the adversaries deployed denial-of-service attack against the utility's communications system and utilized KillDisk data destruction malware on substation cyber assets in an attempt to make it difficult to recover from the cyber attack.

Attacks on the utility supply chain are also a growing concern as another threat where adversaries attempt to compromise the utility's OT systems. In 2020, the SolarWinds' hack was the subject of a software supply chain cyberattack where the adversaries inserted malware into their Orion® software update that was distributed to their clients and went undetected for months. The fact that the company's software distributed trojanized updates that were digitally signed with a legitimate certificate. These type of supply chain threats were previously unanticipated by many organizations in the public sector. Power producers with distributed assets such as offshore wind farms need to understand these aspects of cyber risk because it is challenging to anticipate and protect against through the multiple tiers in the supply chain.

Embracing standards and recommended practices
Industry best practices, together with governmental policies and regulations, are essential to guide asset owners through the digitalization journey while building a framework to protect your infrastructure from cyber attacks. Some of the key standards are:

- IEEE 1686 Standard for Intelligent Electronic Devices Cybersecurity Capabilities
- IEEE C37.240 Cybersecurity Requirements for Substation Automation, Protection, and Control
- IEC 62351 Standards for Securing Power System Communications
- IEC 62443 comprehensive cybersecurity framework for control system security rooted from ISA99
- ACP (formerly AWEA) Offshore wind Compliance Recommended Practices (OCRP) cites three of the above cybersecurity standards.

How to start thinking about cybersecurity
Most power generation companies have some understanding of cybersecurity and the implications of being exposed and vulnerable. Many companies have limited resources to address the cybersecurity challenges so knowing where to start or improving your maturity and capability is very important. In the current climate, an organization should focus on cyber hygiene, following best practices to improve cybersecurity posture introducing risk assessment to understand threats to your system, develop risk mitigation and risk management plans and commence process improvement for elevate organizational maturity as main objectives. Awareness and education are paramount to building a cyber-aware culture throughout the organization.

Companies can start their cyber hygiene program by assessing their cyber maturity level and identifying the incremental steps to improve it. Turning to standards that are policy, procedure, practice and personnel related, can help you with this journey. Standards like IEC 62443-2-4 is a good example because it defines the security capabilities for system integrators. The US National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) and Cybersecurity Capability Maturity Model (C2M2), are also a good references, as it provides guidance on an organization's implementation and management of cybersecurity practices.

How Hitachi Energy can keep your systems secure
With more than 16 GW of offshore wind solutions executed, contracted, and in preparation, Hitachi Energy understands the issues that create risk for utilities, IPPs and other power generation companies. Our products and systems are rigorously tested in our system verification center (SVC) and Cybersecurity Assurance Center (CSAC) to ensure they comply with the most stringent industry standards and follow the 'defense-in-depth' approach in which a series of defensive mechanisms are layered to protect cyber assets if an attack occurs.

All of Hitachi Energy's software, substation automation, and communication systems are designed and configured according to best practices and provide a broad range of cybersecurity measures, which are grouped into three main categories as described below.

Hitachi Energy's cybersecurity measures

1 Monitor

Monitoring features provided real-time security and monitor the health and activity of assets across grid automation system, incuding networks and applications.

2 Manage

Managing features help users manage critical activity including configurations, changes and patches across grid automation systems.

3 Protect

Protecting features defend grid automation systems against unauthorized access, attacks, exploits and malware that compromise system availability, performance, security and compliance.

To ensure that all security measures of the design are properly implemented all our Hitachi Energy operation units that integrate and deliver system and services have been certified to IEC 62443-2-4 and ISO 27001. By that we can be a reliable partner for mission critical infrastructure operators to put their system in service and to keep the security sustained over the entire life cycle of the asset.

Offshore wind industry cybersecurity and resiliency must be improved to protect its critical assets from growing cyber attacks. Owners, operators and other industry stakeholders need to start adopting cybersecurity strategies that best meet their individualized needs, while following industry best practices, regulations and standards. Hitachi Energy can help you in this journey. Learn more

3 Why hybrid wireless is the best option for offshore wind communications

Traditionally, offshore wind turbine generators (WTGs) communicate between each other and to the offshore substations via fiber that is used for teleprotection and data transmission. However, fiber has several shortcomings – such as splicing and scalability – that can challenges as the number of applications grow. Some of those challenges can be overcome by using a hybrid approach.

Wind park operators can strive to take advantage of several communications technologies as a single "hybrid" network. Hybrid network solutions, leverage large scale highly reliable wireless and wired technologies, to provide resilient, flexible, futureproof and economical communications infrastructure designed to serving power generation applications with varying requirements. A hybrid device can provide connectivity over several different technologies simultaneously or by using a fallback mechanism. Hybrid networks solve several key communications system challenges for wind park operators:

Device and application scaling

Offshore wind substations are typically unmanned and deploying human workforce to them is expensive. For example, commissioning vessels and staff can cost more than US$100,000 per day. For this reason, most operators seek to keep human presence in offshore wind farms to the absolute minimum. As wind generation technology evolves, the ability to optimize processes and operations means that more and more devices must exchange information. In the past, wind farms had tens or maybe hundreds of connected devices. With the proliferation of IoT-connected equipment and sensors, operators will need to be able to accommodate thousands – and maybe even hundreds of thousands – of devices in the not-so-distant future. Communications systems being designed today will need to support data transmission from a broad range of WTG equipment, digital substations and all auxiliaries, CCTV, field worker mobile devices, as well as applications to support geofencing for safety and security. Hybrid network architectures can provide a future proof device scale to large offshore wind operators.

From an application perspective, traditional substation control and monitoring, or line and differential protection, still dominate the landscape in offshore wind communication applications. However, the need for operational optimization and efficiency is driving a strong application growth to support machine-to-machine communication as well as people-to-internet and people-to-people communications. In the past, offshore wind projects have deployed one application per network, over time resulting in layers upon layers of standalone networks.

An example of how this occurs is when WTG-to-offshore substation fiberoptic networks are built. Developers typically rely on WTG equipment OEMs (each with separate systems) to ensure liability for network performance to remain responsibility of the WTG warranty holders. While this could be the result of an extension of the offshore substation network that offers synergies and minimizes the number of sub-suppliers, this practice tends to proliferate, rather than consolidate, network functionality. On the other hand, today wind park operators consider 4G/5G networks for people only communications. Since this approach often requires usage of expensive and scarce licensed spectrum, not exploring wider application connectivity can result in a poor investment harvesting.

Another example of how communications systems become layered occurs when integrating CCTV on offshore wind substations. In most instances, IP networks sourced from the CCTV supplier and only serving the CCTV integration are connected to form their own network. Once again, the usage of vastly capable networks for a single application bypasses an opportunity to leverage the investment by integrating both CCTV and other auxiliary communication applications into one reliable network.

Over time, the "one application/ one network" approach, may not only result in over-dimensioned and underutilized investment but also in significant complexity. Specifically, dispersed and individualized network management becomes costly over time and leads to long troubleshooting lead times. This is particularly evident when interworking components from different vendors experience an issue.

Nowadays, traditional generation and substation applications are accompanied by a new generation of sensing devices, inspection drones, mobile and smart workers, real-time safety and security, process optimization applications. These use cases each have a different set of requirements including latency, bandwidth, volume, density, reliability, and mobility. There is no one size fits all, certain technologies are undoubtedly more suitable than others scenario to scenario. With a hybrid architecture however the need to choose and overlay is significantly reduced. Multi technology hybrid networks significantly reduce the number of networks components, as well as complexity without jeopardizing service integrity.

Reduction of fiber splicing

Today's wind park to offshore substation machine communications and communications within substations predominantly take place over fiber since the communications medium is laid alongside power cables, offering synergies in the commissioning phase. While fiber is very reliable, it can be costly to deploy and scale. This challenge will be further exasperated as the number of devices and application within the wind park and substation increase. Mission critical grade wireless communications reduce the commissioning lead-time, by providing splicing-free connectivity to a growing number of devices and applications.

A robust system can switch WAN backhaul interfaces and media either by configuration or condition detection fallback, without any impact to connected clients. In some cases, operators may want to use fiber infrastructure for operationally critical applications such as line and differential protection and wireless communication for non-operationally critical applications such as condition monitoring. In these cases, hybrid devices can significantly reduce the splicing scope, by aggregating many clients to a single device, capable of switching multiple media or separating concurrent traffic across multiple media. Alternatively for some applications, splicing can be omitted altogether if operators choose to implement a mission-critical broadband mesh or 4G/5G WAN backhaul options.

Reduction of commissioning lead time

During the commissioning phase, wireless technologies offer a fast, temporary communications set up for most applications. Temporary wireless communications for the commissioning phase may not represent the final topology and configuration; however, this approach can provide a fundamental building block, addressing scalability challenges as well as providing redundancy to fiber over the 25-year lifetime of the park. A hybrid network certified for high voltage mission critical applications allows wind park operators to build incrementally, not interchangeably which reduces not only commissioning lead time but also risk. Once the permanent backhauling is in place, operators may choose to follow the traditional fiber approach or remain on wireless backhauling options for certain application – without any client connectivity interruptions.

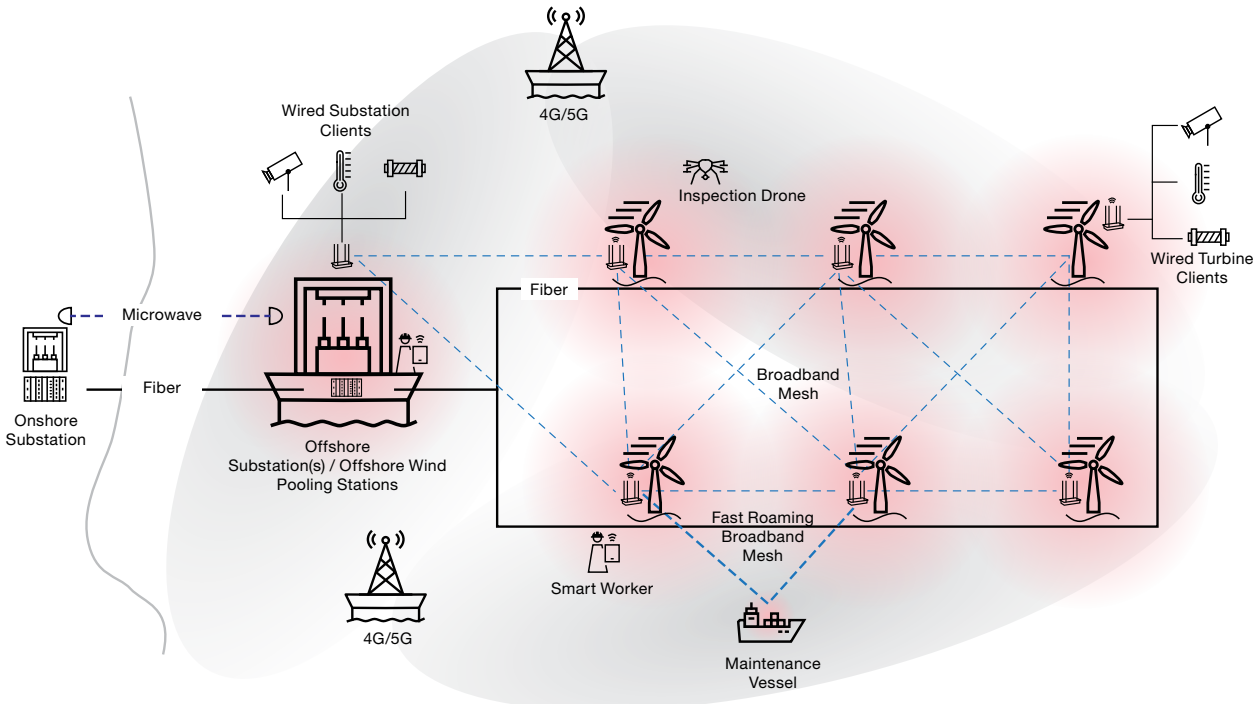
Network responsiveness and data exchange optimization

Traditional communication devices' primary purpose was to send and receive data. Hybrid networks take communication a step further and may include edge computing capability. Including an application intelligence platform at the edge enables rapid decision making throughout the generation process and conserves costly network bandwidth. When combined with a capable analytics platform data from these systems, operators benefit from application specific business analysis with algorithms especially designed for generation and transmission use cases. Application execution at the edge, prepares wind park operators for the growing landscape of clients, devices, applications and ultimately complexity in optimizing wind generation operations.

Multi-use capabilities

Wireless networks support multiple applications and user groups. The same physical infrastructure can be leveraged for applications such as substation automation (SA), outage management systems (OMS), SCADA, mobile workforce, and substation security. Supporting multiple current and future applications typically requires high throughput and capacity, as well as low latency. Hybrid wired/wireless networks multiple technologies and media to support gigabit per second (Gbps) throughput and have latency low enough to satisfy most latency-sensitive applications. They enable creation of multiple virtual networks spanning different physical segments, each with their own IP address space, quality of service (QoS) and security policies, completely segregating the traffic of different applications and user groups and enabling prioritization and reliable delivery of critical traffic. Most importantly, hybrid networks provide an economic solution addressing both scalability and reliability challenges operators face today and will encounter tomorrow.

Hybrid communications architecture



A note on cybersecurity

While cybersecurity is a primary concern for any communications system, it is important for wind park operators to make sure the devices they select are hardened using a combination of technical and procedural measures that meet cybersecurity standards such as IEC 62443-2-4 and NERC-CIP. Network security is extremely critical in securing the communication link, network devices that carry the communication data as well as the assets generating it. The goal of network security is to provide confidentiality, integrity and authenticity and ensure operational continuity.

- **Confidentiality** keeps transmitted data and data at rest secret from unintended listeners on the network.
- **Integrity** ensures that the received data is the data that was actually sent and has not been tampered with during the transmission.
- **Authenticity** provides the identity of the source and the destination endpoints to ensure that they are the intended entities in the communication channel.
- **Operational continuity** is the result of the above, ensuring the wind park operation is not interrupted by malicious intruders.

While cybersecurity is often looked at as a set of features and algorithms, true industrial security spans from the way infrastructure is designed, manufactured, and documented, through to its operation and ultimately to its disposal. Cybersecurity is much more than a product feature; it is fundamental throughout the system and every process within it.

Wireless communications are a cost-efficient and practical approach throughout the windfarm lifecycle. The advantages they bring to scaling, responsiveness and costs related to commissioning and fiber splicing are significant. By taking a hybrid approach to wind park communications, operators can develop multi-use networks that can provide edge computing and other capabilities to help future-proof the systems.

Hitachi Energy offers robust, cost-effective, end-to-end communication solutions for offshore wind applications, meeting the challenges of some of the harshest operating conditions. Hitachi Energy's industrial graded communication networks and can be used to build a highly reliable, secure, manageable, and scalable foundation that meet performance and capacity requirements. Our wireless products seamlessly integrate into an enterprise-class network management platform to provide full network observability, operational simplicity, and troubleshooting. Get to know more here.

Hitachi Energy
Brown-Boveri Strasse 5
8050 Zurich
Switzerland

4CAE001148