PROTECTING ASSETS AGAINST NEW THREATS

Even on wind-farm projects today, the implications of a drone attack onshore or offshore are not always incorporated into risk assessments. (Courtesy: Shutterstock)

Wind-farm physical security is critical in a cyber-focused world.

By NELSON DURAN

In today's technology-driven world, where cyber threats dominate headlines and organizations invest significant resources in safeguarding their OT and IT infrastructure from digital threat vectors, the importance of the physical security of a wind-power farm can sometimes be overlooked. However, it remains an essential component of a wind operator's enterprise risk mitigation.

PGE plans to build offshore wind farms with a total capacity of 6.5 GW by 2040, while Orlen has a license to build a farm with a capacity of up to 1.2 GW, the construction of which would be completed in 2026. Depending on the investor, they will be from 23 to 80 kilometers from the shore, which is often beyond the line of the radar or optical horizon. The location of these facilities, which could result in extended response times for the services responsible for the security of the state, means they could become the target of terrorist acts once they become operational. The wide range of possible activities and the complexity of the maritime environment makes offshore critical infrastructure, such as offshore farms, extremely difficult to protect and secure from potential destabilizing attacks.

Indeed, earlier this year, the Dutch government warned of potential targeting of offshore wind for sabotage, amid mounting concern over the security of renewable energy assets.

Like many industrial assets, wind farms are designed first and foremost for functionality. A comprehensive security strategy should therefore prioritize and address both cyber and physical vulnerabilities. After all, a malicious actor in either area can cause significant undesirable outcomes (e.g., compromised employee health and safety, damage to wind-turbine equipment, lost production time, etc.).

OLD THREATS, NEW TECHNOLOGY

Despite advancements in technology, some hazards will continue to exist. Insider threats, for example, always pose a significant risk to wind-farm operations. Typically, these types of attacks are orchestrated by individuals (e.g., employees, contractors, trusted partners, etc.) who have authorized access to systems, data, or facilities but misuse that access for malicious purposes. The threat they present can range from accidental breaches due to negligence or lack of awareness, to deliberate acts of sabotage, espionage, or data theft.

Insider threats can be particularly challenging to detect and mitigate because the individuals often have legitimate access and can exploit their privileges without raising suspicion. Some of the best prevention methods for this type of risk are implementing robust access controls, regular monitoring, and employee awareness programs. Promoting a culture of security and vigilance can minimize the potential impact of insider threats, and valuable assets such as sensitive information can be better safeguarded.

Vandalism, theft, and flammable substances are also an ever-present risk to onshore facilities. In recent years, many organizations across the renewables sector have upgraded their assets to include the latest digital monitoring equipment, promoting the rapid uptake of industrial cybersecurity measures. However, this doesn't eliminate the risk of physical attempts at vandalism, theft, or purposeful releases, nor does it negate the need to defend against such attempts. Organizations operating in the wind industry should remain vigilant of these threats, even in a cyber-focused world.

EVOLVING PHYSICAL THREATS

Cyberattacks are typically the first thing that come to mind when discussing the impact of increased digitalization on power plants and wind-farm security. However, physical attack vectors have also evolved with technology.

One prominent physical attack vector example involves the use of unmanned aerial vehicles (UAVs) or drones. Several high-profile drone attacks on critical infrastructure outside the U.S. have raised questions about how facilities can protect against aerial attacks. While most of these incidents originate from nation-states or designated terrorist groups with military-grade UAVs, access to recreational drones is now ubiquitous.

Whether operating within the bounds of the plant incidentally or with malicious intent, even the most unsophisticated of UAVs can easily penetrate traditional physical security measures (e.g., fences, gates, perimeter cameras, etc.). Most enterprises did not have to consider this when their plant was originally built, thus potentially leaving them exposed to such modern-day threats. Even on wind-farm projects today, the implications of a drone attack onshore or offshore are not always incorporated into risk assessments. Part of this is attributable to the perception that nothing can proactively be done to prevent such an occurrence from happening. However, this is only true in some cases, as certain critical areas of a wind farm and its facility can be hardened.

By incorporating the threat into a risk assessment, personnel will be forced to think about reactive measures if an event does occur, which is important to help minimize its impact and better preserve safety after the fact.

Embracing the concept of "Security-By-Design," which prioritizes integrating security features into the wind farm and its land-based power facility during its development, is also important. By addressing physical threats as early as possible with the same rigor and focus as those in the digital space, wind-farm operators and utility providers can enhance their overall security posture, mitigate threats, and help ensure business continuity. Requirements should be mapped to relevant standards that are applicable to generating assets operational requirements — for example, ISA 62443, NERC CIP, EPCIP, etc.

THREAT, VULNERABILITY, AND RISK ASSESSMENTS

To help better ensure that all physical security risks are addressed, it is beneficial for organizations to perform ei-

Like many industrial assets, wind farms are designed first and foremost for functionality. A comprehensive security strategy should therefore prioritize and address both cyber and physical vulnerabilities. (Courtesy: Shutterstock)

ther Security Vulnerability Assessments (SVAs), Threat and Vulnerability Risk Assessments (TVRAs), or both. Each constitutes a comprehensive approach to risk mitigation and can help wind-farm facilities develop an effective physical security strategy by:

- **Better understanding the unique threats they face:** When conducting a threat assessment, wind-farm operators can start by identifying potential adversaries, their intent, and capability, then review tactics from past attacks at similar locations to estimate the threat to the organization.
- **Assessing vulnerability:** Understanding the threat is essential, but the ability to deter attack onshore or offshore is amplified by understanding vulnerability. Vulnerability can be considered as the psychological, sociological, or physical characteristics that leave an asset – such as a wind turbine – unprotected or exploitable for attack. Typically, the emphasis is on physical security vulnerabilities, but the human factor can make or break security efforts. Thinking, "It will never happen here," or, "It will never happen to us," can add to vulnerability.
- **Quantifying risk:** Risk is defined in the basic form as "R = L x C," where R is risk, L is the likelihood of the event occurring, and C is its consequence. When it comes to performing risk calculations, most organizations operating across the renewable energy industry focus heavily on the consequence term of the equation without measuring it against its associated likelihood. This makes it difficult to accurately prioritize risks and efficiently allocate resources toward mitigation measures. It also shifts the focus away from identifying critical vulnerabilities in wind-farm infrastructure and can leave onshore or offshore operations unprotected from "low probability" events. To develop a complete risk profile, both the consequence and likelihood terms of the risk equation should be thoroughly evaluated.

After quantifying the risk, organizations can begin to take preventative action by physically hardening wind-farm infrastructure, such as using perimeter protection, blast analysis and design, facade strengthening, disproportionate collapse mitigation, local hardening of security command centers, and more. Another important step is security systems evaluation and design (i.e., intrusion detection, monitoring and surveillance, access control systems, security policies and procedures, redundancy evaluations, etc.), along with the implementation of dependency mitigation measures related to emergency backup power, spare parts, supply chains, emergency response, and so on.

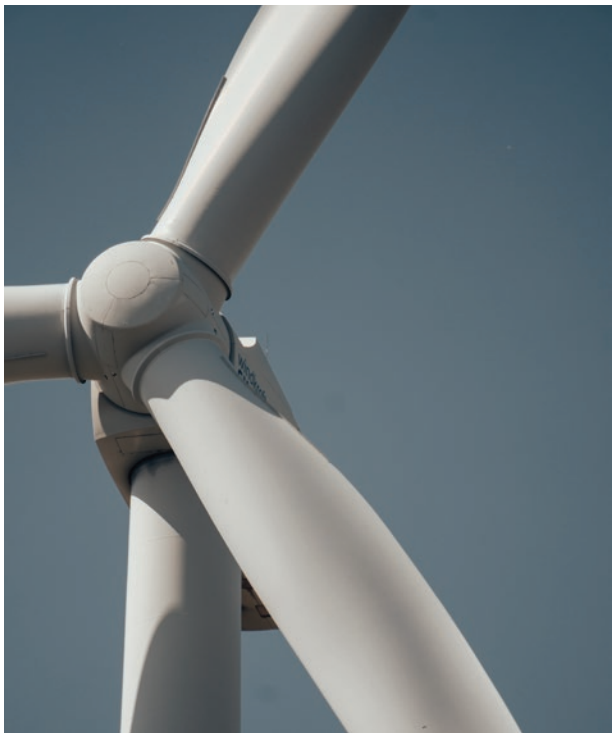
AD INDEX

CONCLUSION: AN INVESTMENT, NOT A COST

Adversaries will continually seek the weakest link in their target's security. Therefore, a balanced and well-thought-out security profile that includes both cybersecurity and physical security can be vital for effective wind-farm facility protection and safety.

In the ever-evolving landscape of cybersecurity threats, physical security continues to play an indispensable role in protecting organizations operating across the renewables industry. While cybersecurity measures are vital and growing in importance, they should be accompanied by robust physical security measures to provide comprehensive protection.

In both the physical and cyber worlds, security should not be viewed as a cost but as an investment to improve the overall safety of a wind-farm facility. As wind energy continues to develop into an important sector, contributing to more of the energy mix, organizations should remember that one of the primary goals of any security measure is to preserve the safe, reliable operation of its physical infrastructure.



ABOUT THE AUTHOR

As the director of Operations for the Protected Design Group within ABS Group, Nelson Duran heads up a highly talented team that spans the world, helping customers mitigate the threat potential of both man made and natural disasters.