INTRODUCTORY NOTE

IEA WIND TASK 11 TOPICAL EXPERT MEETING #116

ON

CYBERSECURITY FOR WIND ENERGY SYSTEMS

14 October 2025

Jake Gentle – Idaho National Laboratory

Megan Egan – Idaho National Laboratory

Juan Felipe Gallego Calderon – Idaho National Laboratory

…

A. VALUE FOR IEA WIND TCP

BACKGROUND

Critical infrastructure is facing ever evolving threats and risks in cyberspace and wind energy sector is no exception. A rising number of cyber events impacting wind energy organizations and wind energy systems demonstrate that cyber adversaries are increasingly targeting the sector. Whether intentional or unintentional, wind energy systems are being affected by these attacks. In 2022 alone, multiple cyberattacks and intrusions targeted the wind energy sector, including ransomware attacks on Nordex and Deutsche Windtechnik control centers, a wiper attack that disabled SATCOM modems serving ENERCON wind turbines, and an espionage campaign against companies operating in the South China Sea.[1]

The low cost, reliable generation of electrical energy from wind relies heavily upon automation and control systems, arguably more so than traditional thermal generation. However, these systems also serve as prime targets of malicious cyberattacks. As the share of power generation from wind assets increases, and moves offshore, these systems become increasingly dependent on digitalized services. This shift also makes them more vulnerable to complex and frequent cyber threats. Therefore, understanding and addressing cybersecurity challenges in wind energy technology is more important than ever, especially as the industry grows in value and becomes an even more attractive target for cyberattacks.

[1] U.S. Department of Energy, Wind Energy Technologies Office. "Protecting Wind Energy Systems From Cyberattacks." May 21, 2024. https://www.energy.gov/eere/wind/articles/protecting-wind-energy-systems-cyberattacks.

Cybersecurity is a global issue and this TEM, proposed by the United States, aims to bring together experts from wind energy-producing countries and stakeholders in the wind energy industry. The goal is to identify and prioritize the most pressing cybersecurity concerns and challenges within the wind energy sector by October 2025.

MOTIVATION

The wind energy sector is deploying increasingly large and complex installations offshore turbines, which come with their own set of cybersecurity challenges. This is an opportune moment to explore global solutions for scaling cybersecurity protections, mitigations, and best practices. Key challenges include integrating cybersecurity into existing plants and assets, incorporating security-by-design into future infrastructure, and understanding cyber-physical consequences of cyber threats as the sector becomes an attractive target for attacks.

The reputational damage that cyberattacks can inflict on global companies and technologies make this an international issue. It is essential to gather inputs from global experts who can share diverse perspectives on both wind energy deployments and cybersecurity threats. Their collective input is critical in identifying and prioritizing innovative solutions.

This TEM complements the ongoing IEA Wind Task 43 on Wind Energy Digitalization.[2] As identified by U.S. National Laboratories' collaboration wind energy digitalization roadmap, cybersecurity must be part of the broader transformation to digital ecosystem transformation to a Wind Energy Industry 4.0.[3] IEA Task 43 focuses on data standardization, sharing, and management and the cybersecurity TEM can help inform critical Task 43 deliverables, such as providing Task 43's roadmap with cybersecurity risks as fundamental barriers to digitalization benefits. Outside of Task 43, this TEM will help the IEA assess whether a new task is needed to address sector-specific cybersecurity challenges. The outcomes of this meeting will also inform ongoing work with the IEA on digitalization, control systems, optimization, and technology development, particularly concerning data schemas related to cybersecurity and the expansion of wind energy-specific ontologies.

---

[2] IEA Wind. "Wind Energy Digitalization, IEA Wind Task 43." https://iea-wind.org/task43/

[3] McKinsey & Company. "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?". August 17, 2022. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir.

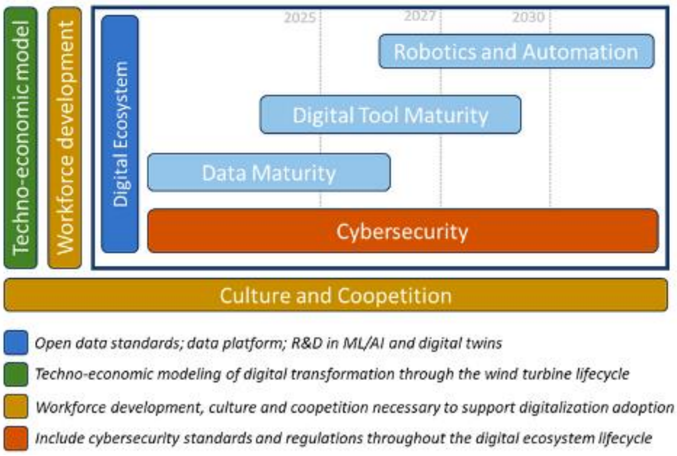

Figure 1. Key activities to achieve Wind Industry 4.0.

ADDED VALUE OF COLLABORATION

International collaboration on this topic is critical due to the global nature of the wind energy ecosystem. This includes the design and manufacturing of turbines, cross-border remote monitoring and maintenance capabilities, and the risk that vulnerabilities in one country's wind infrastructure can impact others. For example, the 2022 cyber espionage campaign targeting wind energy assets in the South China Sea affected European and other global companies involved in the manufacturing, maintenance, and installation.[4]

Although cybersecurity research and development for wind energy is currently funded at the national level—such as at the U.S. Department of Energy's Renewable Energy and Storage Cybersecurity (RESCue)—this TEM offers a unique opportunity for an international gathering of experts. These experts bring valuable insights from their engagement with industry representatives and other sectors. For example, RESCue's work on hybrid energy systems, including wind, solar, and energy storage, could be expanded upon through international collaborations. Sharing lessons from national efforts will help identify pathways to robust cybersecurity defences and inform international collaboration at the IEA TEM on cybersecurity.

ALIGNMENT WITH IEA WIND STRATEGY

This topic aligns with the IEA Wind's strategic objectives to maximize the value and competitiveness of wind energy. Cyberattacks on wind assets can undermine confidence in the industry and have already been shown to increase costs for asset owners, operators, and customers. As IEA Wind seeks to digitize and accelerate technology development, it is essential to integrate cybersecurity measures alongside these initiatives to reduce risks and enhance resilience.

Cybersecurity is a cross-cutting issue that affects multiple IEA wind research areas—primarily turbines, plants and grid connectivity. Effective protections and mitigations must be applied across all levels of technology deployment, considering the broader

---

[4] M. Raggi and S. Scenarelli, Proofpoint, "Rising Tide: Chasing the Currents of Espionage in the South China Sea." August 30, 2022. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.

architecture. Cybersecurity is also a key drive innovation in secure-by-design deployments and cyber-informed engineering[5] within the sector.

B. MEETING FORMAT AND GOALS

OBJECTIVES

The primary objective of this TEM is to accelerate the implementation of effective and innovative cybersecurity measures within the wind energy sector. The meeting will serve as a forum to:

- Review the current state of the industry.
- Discuss the challenges hindering the adoption of cybersecurity measures.
- Establish consensus on best practices where cybersecurity has already been successfully implemented.
- Identify immediate opportunities for applying cybersecurity solutions to address the sector's challenges.

Additionally, the TEM will assess whether cybersecurity should be integrated into existing tasks, or if a new dedicated task is needed

SPECIFIC OUTCOMES

The TEM will work toward several outcomes, which may be compiled into one comprehensive deliverable on identified challenges and opportunities or published separately as more focused reports. These outcomes include:

- Developing a global understanding of cyber threats to wind energy sector.
- Gathering top cybersecurity concerns and needs from the global wind energy industry.
- Assessing component criticality in representative wind systems to identify priorities for cybersecurity.
- Developing cyber-informed engineering guidance for wind system design, based on the insights gained from the other outcomes.

If the group determines that cybersecurity inputs should be integrated into existing IEA Wind Tasks or if a new task is needed, proposals or guidance on key questions and challenges will be developed.

INTENDED PARTICIPATION

Intended participants from this TEM include a global representation from academia, wind industry, regulatory, and third-party services involved in cybersecurity for wind energy.

Country	Institutions	Number of Experts
Belgium	WindEurope	2

[5] U.S. Department of Energy. "Cyber-Informed Engineering." https://www.energy.gov/ceser/cyber-informed-engineering.

Canada	Concordia University	1
China	Nanjing University of Aeronautics and Astronautics	2
Denmark	Opoura Ørsted PEAK Wind Siemens Gamesa Renewable Energy Vestas	6
Finland	Tampere University	1
Lithuania	EPSO-G Ignitis	3
Netherlands	Senkron Digital TU Delft	4
Norway	DNV Cyber	2
Spain	EDP Renováveis	2
United Kingdom	Alan Turing Institute CFP Energy Cyber Energia University of Plymouth	6
United States	Department of Energy, Wind Energy Technologies Office GE Vernova Idaho National Laboratory National Renewable Energy Laboratory Old Dominion University Sandia National Laboratory Siemens Energy UL Solutions University of Tulsa	14

TENTATIVE PROGRAM

The in-person meeting will take place Tuesday, October 14, 2025. It will be co-located with the NAWEA WindTech conference in Dallas, Texas, United States. The meeting will also have a virtual option to increase opportunities for participation.

Cybersecurity Collaboration Program Agenda

Time	Tentative Content
Morning Session	**Laying the Groundwork**
8:30 AM–9:00 AM	**Registration & Networking Breakfast** *Welcome coffee and light refreshments, opportunity for informal networking.*
9:00 AM–9:30 AM	**Welcome & Program Overview** *Introduction to the objectives of the program, key outcomes expected, and overview of the day's agenda.*

9:30 AM–10:00 AM	**Cyber Threat Landscape: Current & Emerging Risks** *Setting the stage with a comprehensive briefing on the current cyber threat landscape. Overview of challenges facing industries, governments, and academia.*
10:00 AM–11:15 AM	**Expert Presentations on Current Work** • Academia/Research Perspective – Latest trends, challenges, and cutting-edge research in cybersecurity. • Industry Perspective – Real-world application, lessons learned, and current initiatives addressing cybersecurity issues. • Government & Regulatory Perspective – Policy, regulation, and the role of government in cybersecurity defense and strategy.
11:15 AM–12:00 PM	**Open Discussion: Current Activities and Key Gaps** *Facilitated discussion on the current cybersecurity efforts, challenges, and potential gaps in research, industry practices, and government policies. Begin identifying areas of critical need.*
12:00 PM–12:30 PM	**Networking Lunch Break** *Relaxed break to facilitate informal discussions and networking among participants.*
Afternoon Session	**Exploring Solutions and Building Collaboration**
12:30 PM–2:00 PM	**Breakout Sessions: Identifying Current Challenges & Gaps** *Participants break into smaller groups to discuss specific challenges within their domain (research, industry, government) and identify key gaps in current cybersecurity efforts.* *Focus Areas:* • Technical and operational challenges • Collaboration gaps across sectors • Opportunities for improved policy and regulation
2:00 PM–2:30 PM	**Breakout Session Report-Back & Group Discussion** *Each group presents their findings, focusing on key challenges and identified gaps. Facilitated discussion to synthesize insights and highlight common themes across sectors.*
2:30 PM–3:30 PM	**Pathways to Address Challenges & Gaps: Future Collaboration** *Facilitated discussion on actionable pathways to address identified challenges and gaps. Explore ideas for future research, cross-sector collaboration, and cyber-informed engineering guidance. Identify potential projects or initiatives for collaborative action.*
3:30 PM–4:00 PM	**Closing Remarks & Next Steps** *Summarize key takeaways from the day's discussions, outline next steps for collaboration, and set expectations for follow-up actions.*
3:45 PM–4:00 PM	**Networking & Farewell** *Informal networking opportunity to continue conversations and foster ongoing connections.*