Cyber Resilience for Wind Installations

A tailored approach to evaluating and implementing benefit-based cybersecurity technologies for wind power plants

Cyber Resilience for Wind Installations

Recent research and development (R&D) have provided insights into cybersecurity strategies and business cases for cybersecurity investments. These findings will help renewable sector entities tailor an approach to evaluating and implementing cybersecurity technologies for wind power plants.

A Cyber Resilient Reference Architecture

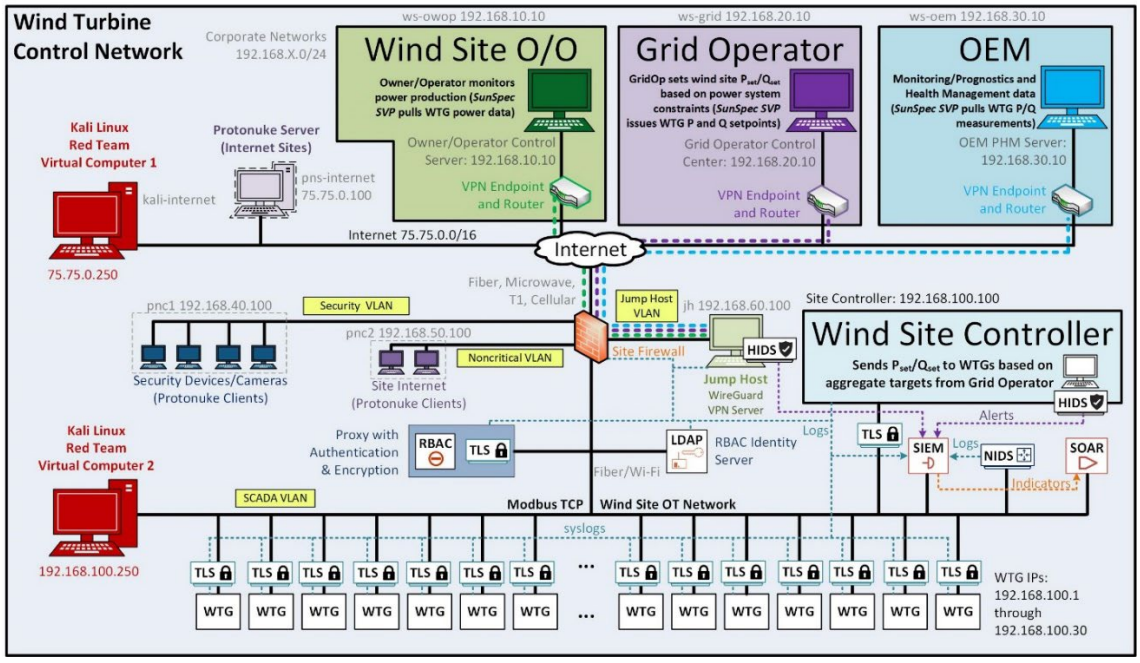
The integration of secure technologies will underpin next generation resilient designs for energy applications, informed by R&D, and implemented by industry. We used this Survey to better understand R&D gaps, assess current state, and help the renewable industry improve informed architecture design. A security architecture includes several functional elements:

- Prevent: Block adversaries with access control, encryption, secure perimeters, and zero trust architectures
- Detect: Monitoring of network traffic and endpoint operations to recognize undesirable traffic
- Analyze: Methods, including machine learning, to baseline normal behaviors and recognize abnormal
- Decide/Visualize: Presentation of information to cyber defenders for quick recognition and response
- Mitigate/Recover: Methods to stop a cyber-attack and reverse any negative affects
- Share: Securely providing of indicators of compromise to support the defense of other organizations

While there is no one-to-one mapping, security architecture functional elements are implemented using the following security tools:

- Prevent: Encryption, Firewalls, Data Diodes, Identity and Access Management (IAM) tools
- Detect & Analyze: Host/Network-based Intrusion Detection Systems (HIDS/NIDS) and Endpoint Detection and Response (EDR)
- Decide/Visualize: Security Information and Event Management (SIEM)
- Mitigate/Recover: Security Orchestration, Automation, and Response (SOAR)
- Share: Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Intelligence Information (TAXII)

An example wind site architecture with these capabilities is shown below.



Wind Architecture Cybersecurity Reference Architecture

National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

INL/SNL WIND CYBERSECURITY INNOVATION SHEET

Investing for Cyber Resilience

In support of a Department of Energy (DOE) Wind Energy Technologies Office (WETO) project, the team built a high-fidelity implementation of wind turbine generators, site control systems, and communication architectures, which established the physical and cyber benefits to incorporating cybersecurity technologies in wind sites. The relative benefits vs cost for six technologies are provided below and include labor as Full-Time Equivalents (FTEs). Costs and benefits are based upon polled large businesses unless otherwise noted.

Hardening Technology	Purchase Cost[1] ($M/yr)	Maintenance Cost[1] ($M/yr)	Labor (FTE/yr)	Cost of Breach[2] ($M/yr)	Payback Period (Yrs)
Encryption	0.225[4]	0	0	4.82	< 1 Yr
Access Control	0.005 – 0.025[3]	0.005 – 0.010[3]	0.25-0.5[3]		
SIEM	0.025 – 1.500	0.025 – 0 .500	1 – 2		
NIDS	0.050 – 0.500	0.050 – 0.500	0.5 – 1		
HIDS/EDR	0.000[5]	0.025 – 1.000	0.5 – 1		
SOAR	0.000[5]	0.100 – 0.500	1 – 2		

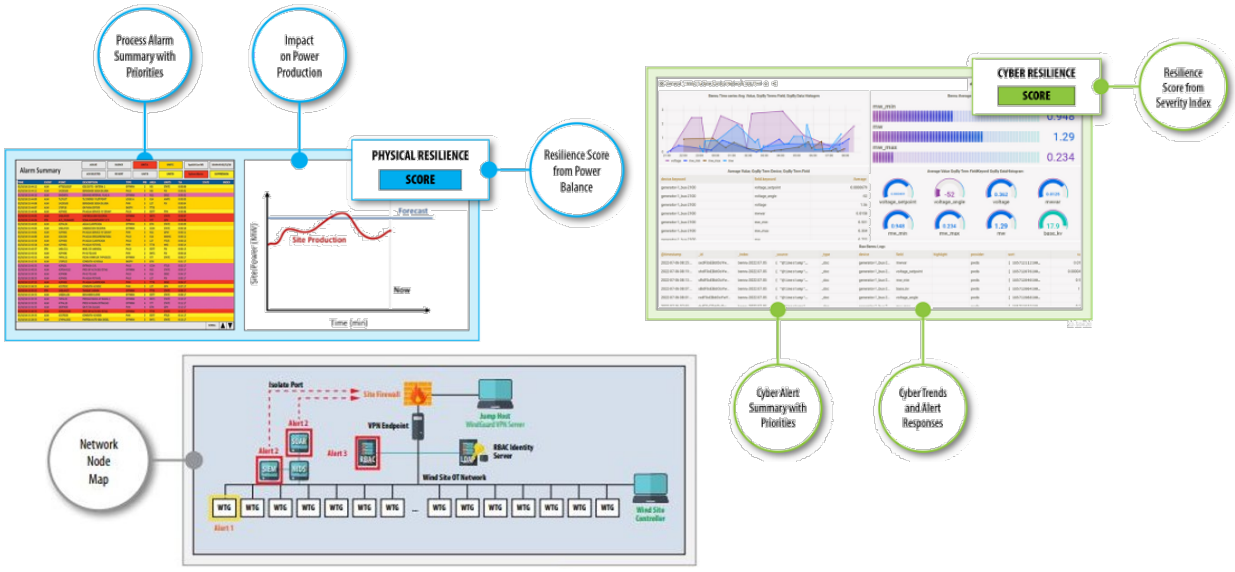
Jake Gentle
208-526-1753
jake.gentle@inl.gov

Jay Johnson
505-284-9586
jjohns2@sandia.gov

Two representative remote and local cyberattacks were performed on wind sites with different cybersecurity technologies. In each test envionment, (a) a remote attack used compromised virtual private network credentials from a phishing attack to pivot through the wind network and change turbine setpoints, and (b) a local attacker cut the lock on a tower and connected to the local network to issue turbine setpoints. Based on the attack sequences, cyber and physical resilience metrics were calculated for each test topology in the table below. Cyber resilience measured the ability to defend the system and recognize attacks earlier. Physical resilience measured the ability to maintain power generation despite attack. Encryption prevented the attacker from communicating directly with the turbines (Test 2), and the NIDS/HIDS recognized the attacks and provided defenders with SIEM alerts (Tests 3 & 4) or SOAR playbooks the data to execute a rapid response (Tests 5).

Test \ Tech	Cyber Attack	Encryption	Access Control	SIEM	HIDS	NIDS	SOAR	Cyber Resilience	Physical Resilience
1	Remote	Baseline						38.5%	46.4%
	Local							61.5%	17.2%
2	Remote	X	X					46.2%	100%
	Local							69.2%	100%
3	Remote			X		X		84.6%	100%
	Local							92.3%	100%
4	Remote	X		X	X			53.8%	100%
	Local							84.6%	100%
5	Remote			X	X	X	X	84.6%	100%
	Local							92.3%	100%

Cyber technologies reduce risks to wind asset owners and operators. Cyber risk in these experiments focused on the impact of two threat actors on a wind farm. By adding security technologies, attacks were successfully mitigated—demonstrating operational resilience and a return on investment (ROI) for integrating cybersecurity technologies within the renewable sector.



Cyber-Physical Evaluation Dashboard Elements

[1] Relative subscription and maintenance cost only for commercial tools.

[2] Critical Infrastructure, Cost of a Data Breach Report, IBM Security, 2022.

[3] Assuming an on-site LDAP or Active Directory Domain Controller for network access controls with regular maintenance and updates to the users, objects, and associated permissions. Control system devices may include access control features with network security services.

[4] Point to point for 30 pairs. Some vendors offer integrated solutions.

[5] No upfront software cost but there are maintenance/license costs.