



Cybersecurity for Distributed Wind: MIRACL Advisory Board Meeting 2022

October 2022

Changing the World's Energy Future

Megan Jordan Culler



INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Cybersecurity for Distributed Wind: MIRACL Advisory Board Meeting 2022

Megan Jordan Culler

October 2022

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**



October 27, 2022

Megan Culler
Power Engineer

Cybersecurity for Distributed Wind

MIRACL Advisory Board Meeting 2022

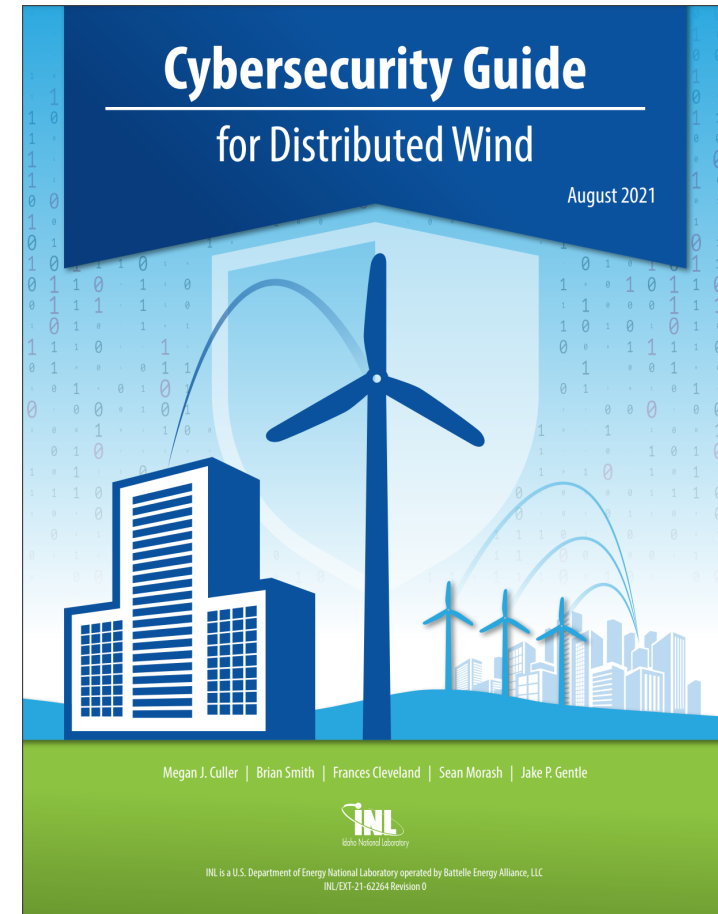
Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy



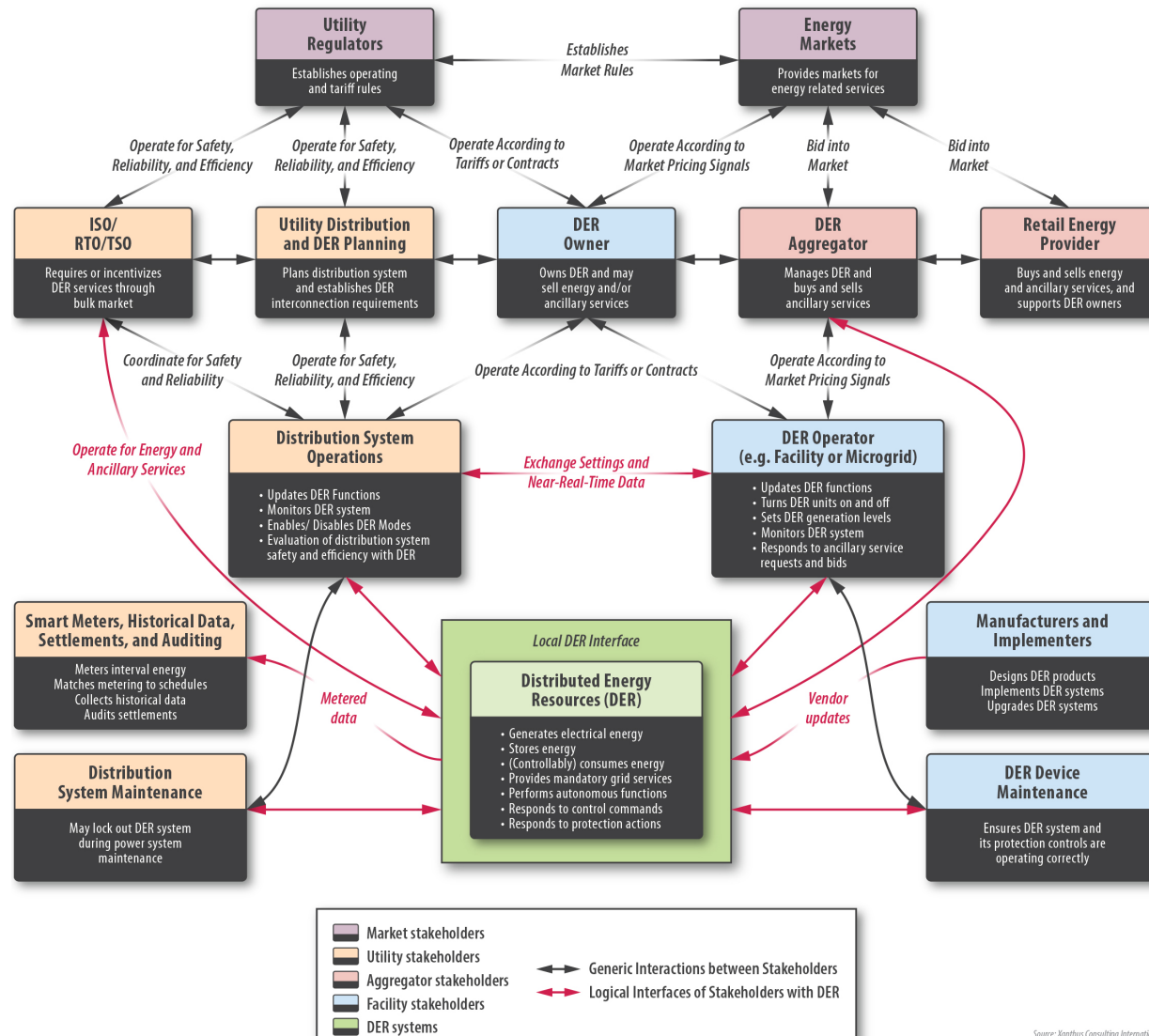
INL/MIS-22-69652

Cybersecurity Guide for Distributed Wind

- Establishing a common architecture
- Need for cybersecurity for distributed wind
- Challenges of securing distributed wind
- Cyber risk management architecture
- Recommendations & stakeholder roles

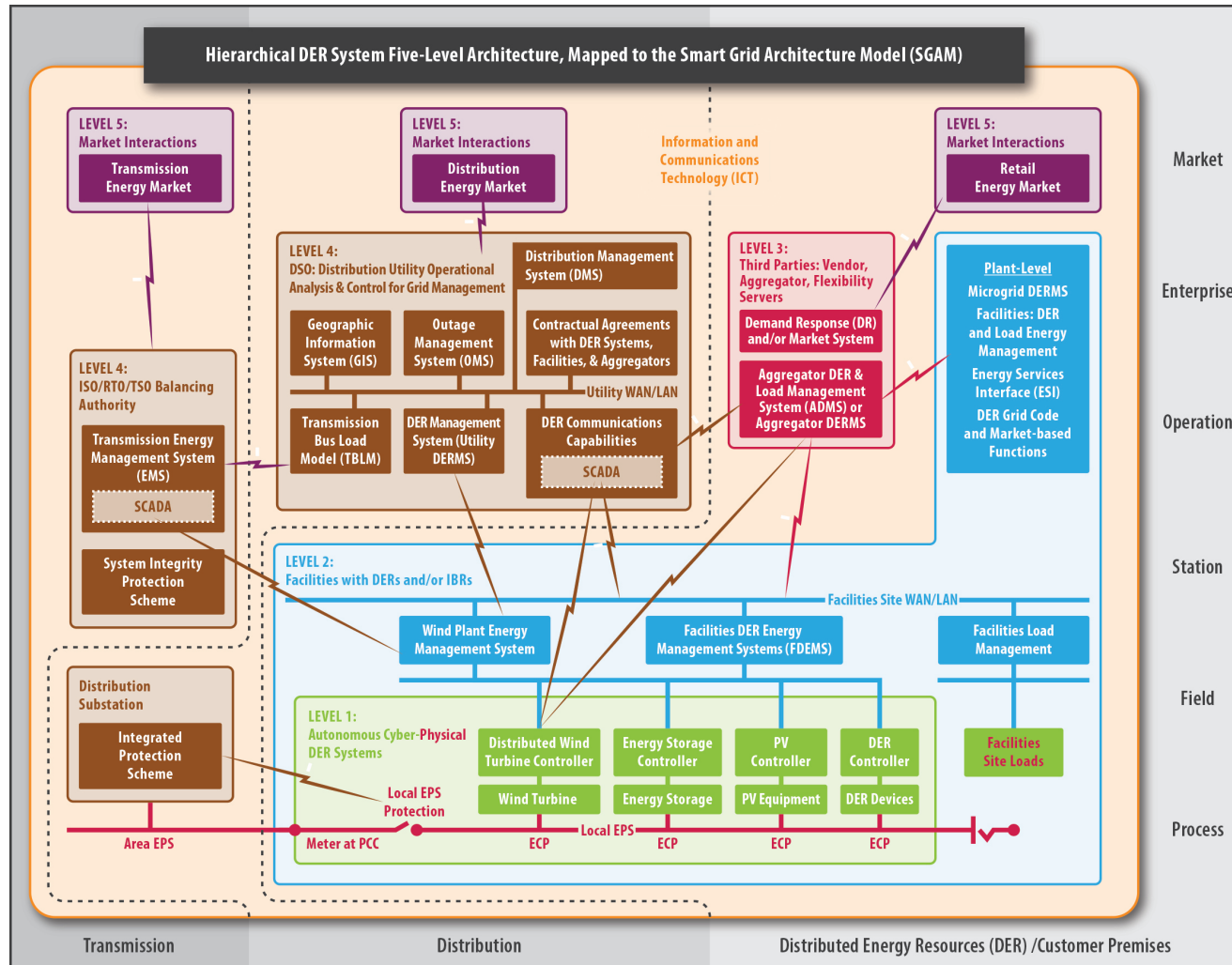


Distributed Wind Reference Architecture Stakeholders



- Who has a role in distributed wind cybersecurity?

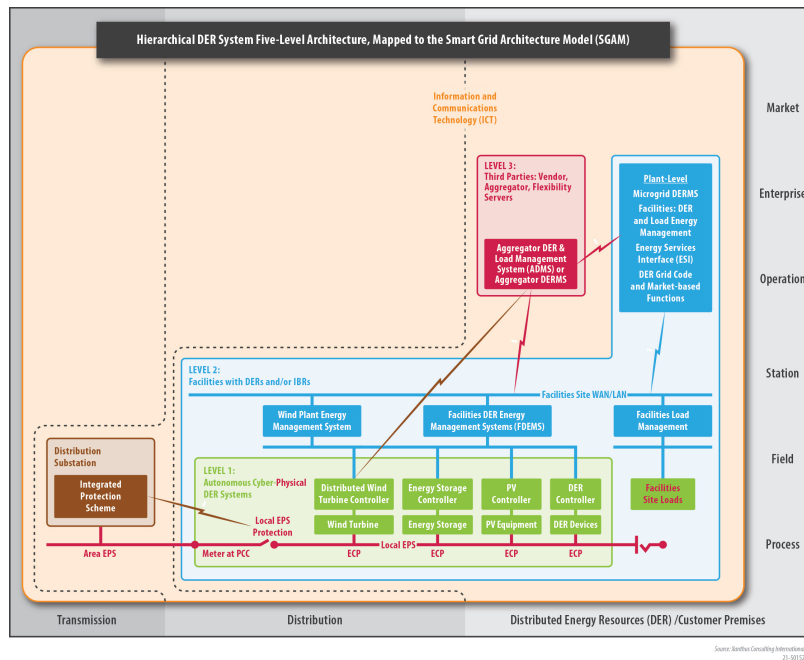
Distributed Wind Reference Architecture Overall Architecture



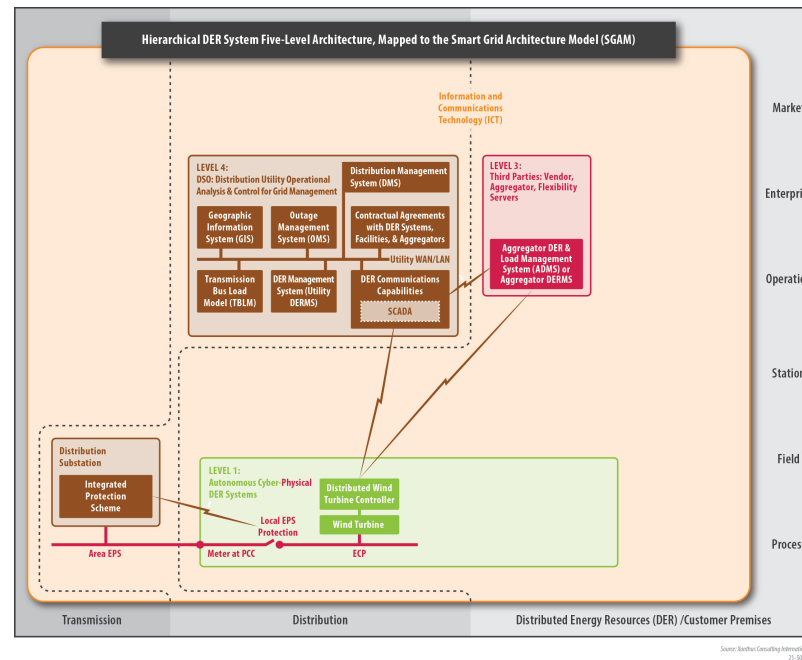
- What is the system that we are protecting?

Distributed Wind Reference Architecture Customized Architectures

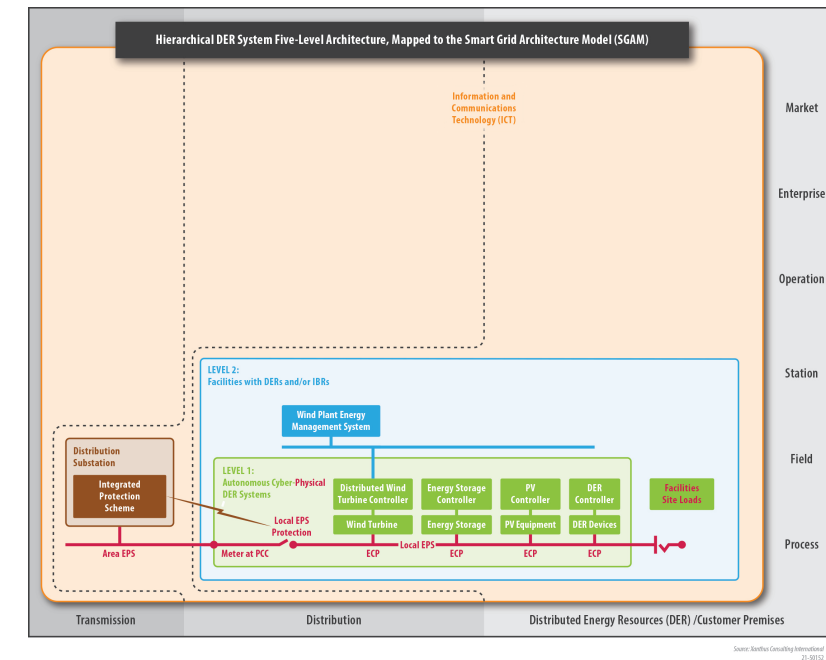
- How does this system change based on the configuration of assets?



Microgrid



Aggregator managed



Behind-the-meter



The Need for Distributed Wind cybersecurity

Academic Exercises in Exploiting Distributed Wind

- Attacks against SCADA system for unauthorized control
- Attacks targeting turbine damage, wind plant disruptions, substation disruption and damage
- Worms to propagate within a turbine or throughout a wind plant network
- Vulnerabilities in specific turbine systems
 - Cross-site request forgery to change default user password
 - HMI vulnerability providing access to credentials in plain text
- Vulnerabilities exploited to exceed turbine limits
- Pass false measurement data between turbines and SCADA using a man-in-the-middle attack

Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018.

DOI:10.1109/iecon.2018.8591200

Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." *International Journal of Critical Infrastructure Protection* 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.

ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." Last modified August 27, 2018. [Online]. <https://ics-cert.us-cert.gov/advisories/ICSA-15-076-01>

Yan, Jie, Chen-Ching Liu, and Manimaran Govindarasu. "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis." Paper presented at the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, Arizona, March 2011.

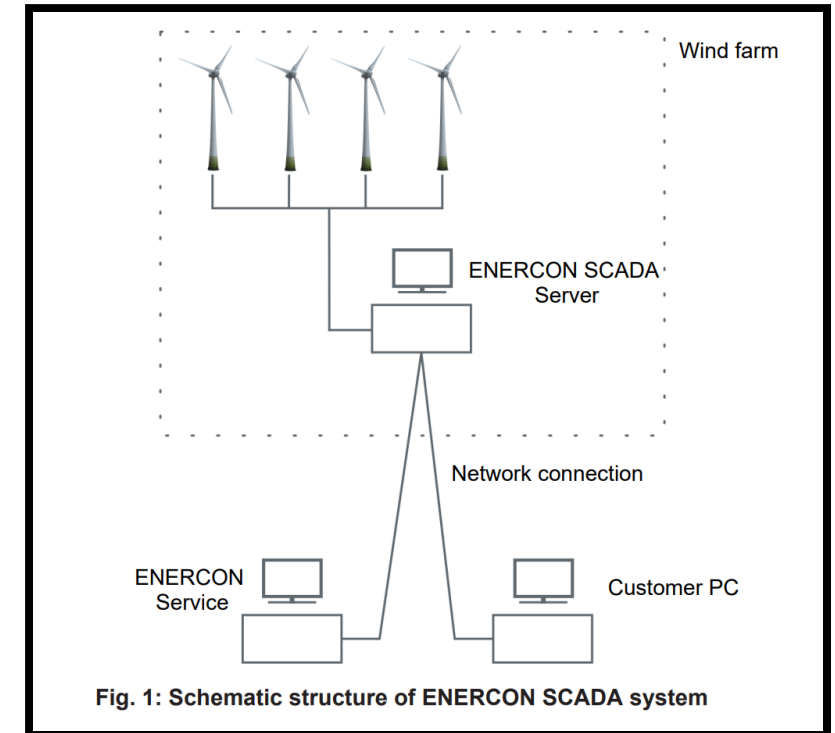
Real-world Events

- 2014: Russian-linked hackers remotely accessed and manipulated wind turbines' automatic voltage regulator settings (limited reach)
- 2018: Technician downloaded malware by mistake on a laptop. Later, when plugged into wind plant, turbines stopped working one-by-one
- 2018: Workstations infected with cryptojacking malware, slowing down wind network
- March 2019: Firewall vulnerability led to DoS that disrupted view into solar and wind generation sites



Real World Events Cont.

- Nov. 19, 2021: Vestas hit by ransomware
- Feb. 24, 2022: Enercon wind turbines in Germany lose remote monitoring connection due to SATCOM attack
- March 31, 2022: Nordex Group, major wind turbine manufacturer, hit by Conti ransomware
- April 11, 2022: Deutsche Windtechnik, wind turbine maintenance company, hit by cyber attack



Challenges to Securing Distributed Wind Systems



Risk Management Architecture

$$\text{Risk} = \text{Likelihood} \times \text{Consequence}$$

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

$$\text{Risk} = \text{Threat} - M_T \times \text{Vulnerability} - M_V \times \text{Consequence} - M_C$$

- Risk management comes from mitigating each element individually
- Cyber resilience measures can apply to any element

Risk Management Architecture: Threats

Threat

=

Intent

X

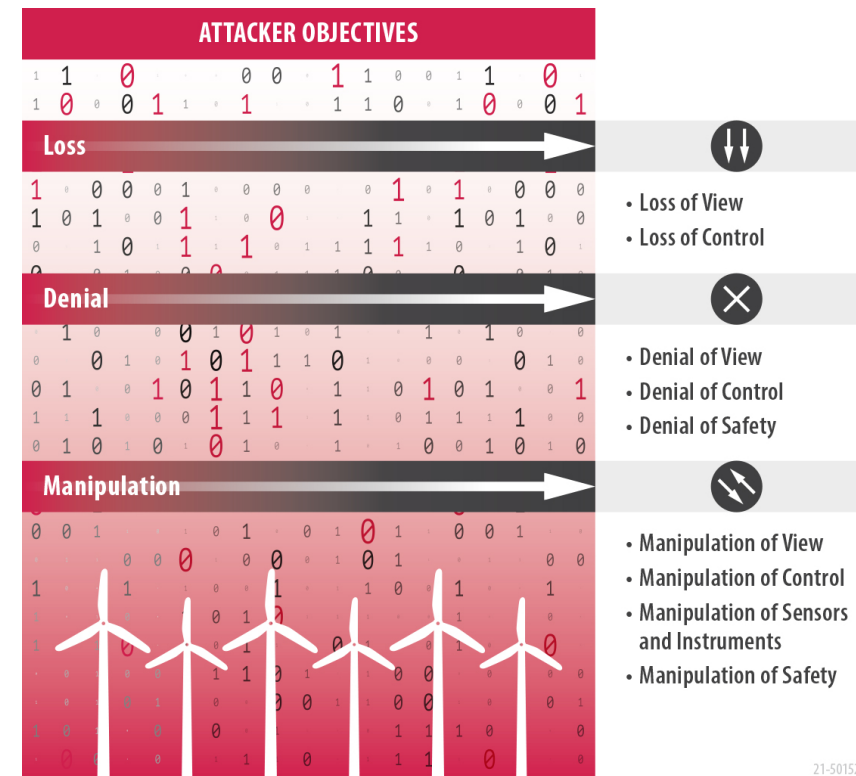
Capability

X

Opportunity

- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

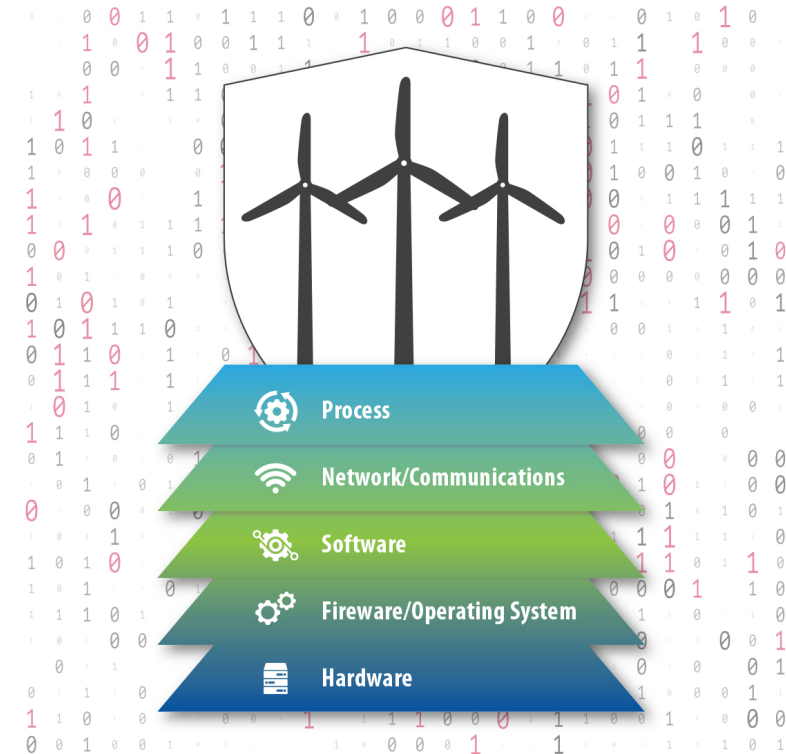
Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	AWEA technician
Organized group	Russian cybercrime
Hostile nation-state or terrorist	Nation-state sponsored APT



21-50152

Risk Management Architecture: Vulnerabilities

- **Vulnerability:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- May be a flaw in either design or implementation
- Can occur at any layer of the system
- Distributed wind examples:
 - Worms propagating malicious commands through flat wind network
 - XZERES 442SR CSFR
 - NovaWind Turbine HMI vulnerability



Risk Management Architecture: Consequences

POTENTIAL IMPACT BY STAKEHOLDER			
Event	Utility (Non-Operator)	Operator (Facility/Aggregator/Utility)	Manufacturer, Integrator, or Installer
Loss of View		<ul style="list-style-type: none"> • Loss of revenue 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Loss of Control	<ul style="list-style-type: none"> • Energy imbalance 	<ul style="list-style-type: none"> • Propagated failures • Injury • Equipment damage 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Denial of View		<ul style="list-style-type: none"> • Improper operation 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Denial of Control		<ul style="list-style-type: none"> • Improper operation 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Denial of Safety	<ul style="list-style-type: none"> • Injury 	<ul style="list-style-type: none"> • Injury 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Manipulation of View	<ul style="list-style-type: none"> • Improper control decision 	<ul style="list-style-type: none"> • Improper control decision 	<ul style="list-style-type: none"> • Reduce reputation • Financial liability
Manipulation of Control	<ul style="list-style-type: none"> • Additional energy resources • Injury 	<ul style="list-style-type: none"> • Loss of reliable operation • Activation of critical load algorithm • Loss of required generation • Failure to meet contractual obligations 	<ul style="list-style-type: none"> • Reduce reputation • Technical investigation • Financial liability
Manipulation of Sensors and Instruments	<ul style="list-style-type: none"> • Energy imbalance • Failure of regulatory compliance 	<ul style="list-style-type: none"> • Improper operation • Severe mechanical damages • Loss of revenue resource • Increased operation and maintenance costs 	<ul style="list-style-type: none"> • Reduce reputation • Increase after-sale expenses • Potential product call-back • Financial liability
Manipulation of Safety	<ul style="list-style-type: none"> • Extended restoration time • Failure of regulatory compliance 	<ul style="list-style-type: none"> • Injury or death • Loss of intellectual property • Technical investigation 	<ul style="list-style-type: none"> • Devalue brand name • Reduce market share • Decommission the product from the market • Financial liability

Mitigations: Cyber resilience by design

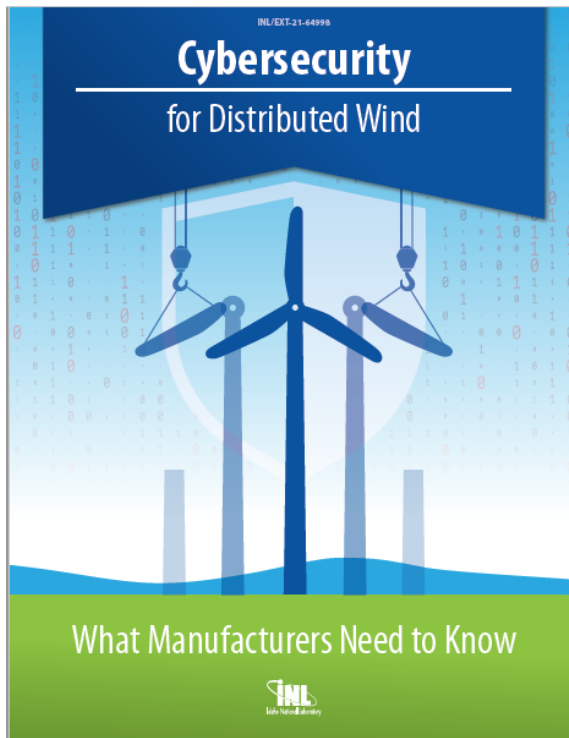
- Recommendations to align with IEEE 1547.3, Section 5
 - Risk assessment and management
 - Communication and network engineering
 - Access control
 - Security management
 - Coping with and recovering from security events
- Relevant standards

Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments			
Area (Focus)	Organizational (What)	Technical (How)	Process towards Compliance
General IT Security Reflecting Business Requirements	ISO/IEC 27001 Security Requirements ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment	<u>Internet Standards</u> Directory svcs X500 IPSec RFC 1827 LDAP RFC 4511 TLS RFC 5246 PKI, X509 SNMP RFC 3418 OCSP RFC 6960 Syslog RFC 5424 GDOI RFC 6407 OAuth RFC 6749 EST RFC 7030 Cloud Services SCEP ... XML ...	ISO/IEC 27001 Certification (ISO/IEC 27002/27019) ISO 22301 Business Continuity Cybersecurity Capability Maturity Model (C2M2) (for determining the degree of compliance)
Energy Systems Operational Environments (Organizational and Procedural Security Controls)	NIST Cyber Security Framework ISO/IEC 27002, 27019 Security Controls NISTIR 7628 Smart Grid Security Controls NERC CIPs Security Regulations for Bulk Power IEC 62443-2-3, 2-4, & 4-1 Security Programs	<u>IEC 62351</u> IEC 62351-3 to -6 Security for Protocols IEC 62351-7 Network & Sys Mgmt (SNMP) IEC 62351-8 Access Control (RBAC) IEC 62351-9 Key Management IEC 62351-10 Security Architecture IEC 62351-11 Security for XML Files IEC 62351-12 Cybersecurity for DER IEC 62351-14 Security Logging IEC/TR 62351-90-2 Deep Packet Inspection	IEC 62443-3-3 System Security Controls IEEE 1547.3 Guide and Recommendations for Cybersecurity for DER IEC 62443-4-2 Security for Products
Energy Systems Operational Technologies (Technical Security Controls and Techniques)	IEC 62443-3-3 System Security Controls IEEE 1547.3 Guide and Recommendations for Cybersecurity for DER IEC 62443-4-2 Security for Products	IEEE 1686 Security for IEDs IEC 62325-503 Energy Market Security	IEC 62443-3-3 System Security Controls IEEE 1547.3 Guide and Recommendations for Cybersecurity for DER IEC 62443-4-2 Security for Products

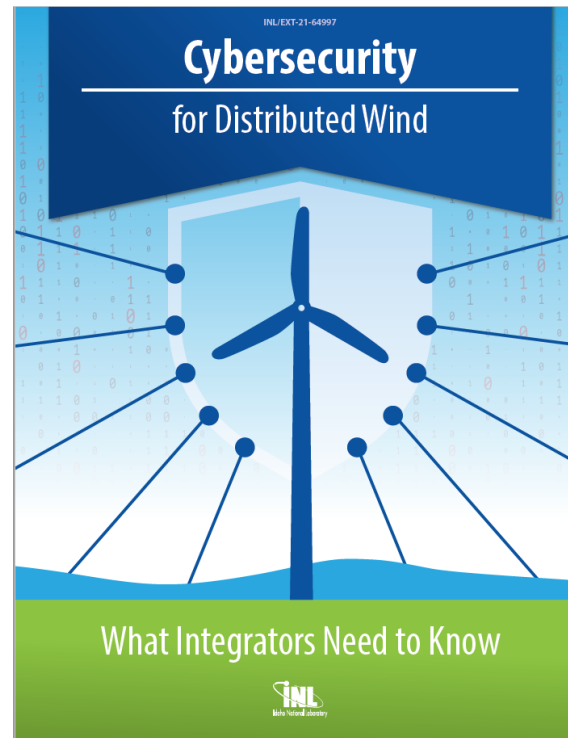
Source: Xanthus Consulting International
21-50152

Mitigations: Cyber Resilience by Design

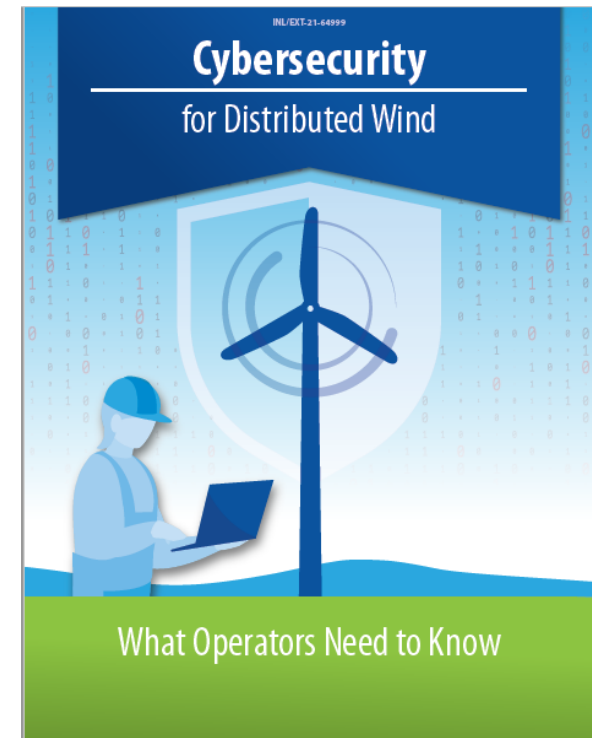
- Stakeholder roles and responsibilities



Manufacturers



Integrators



Operators



Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

WWW.INL.GOV