INL/MIS-22-69652-Revision-0

Cybersecurity for Distributed Wind: MIRACL Advisory Board Meeting 2022

October 2022

Megan Jordan Culler

Changing the World's Energy Future

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

INL/MIS-22-69652-Revision-0

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

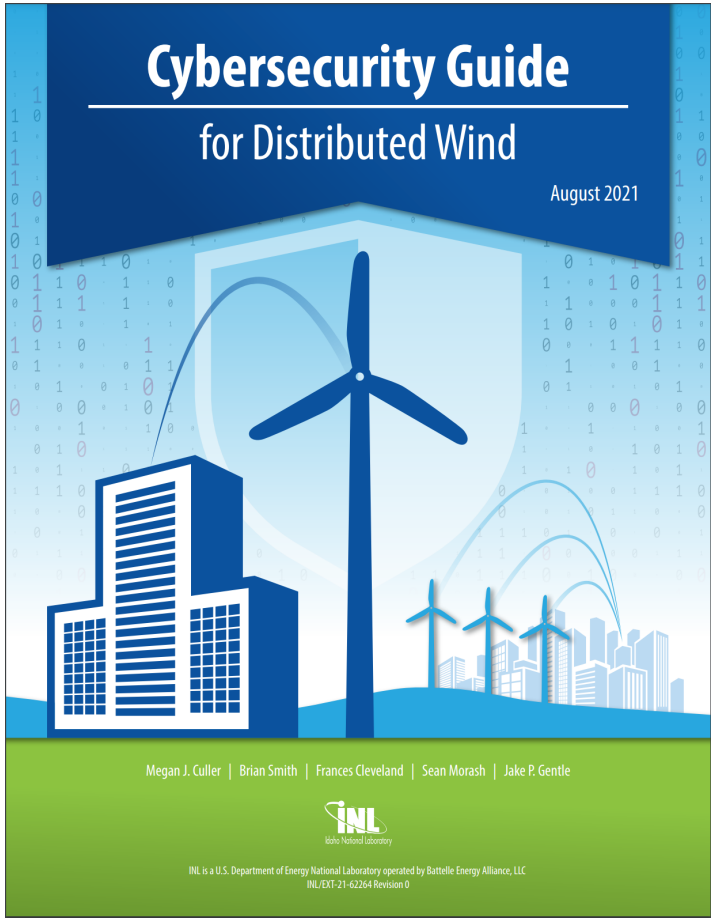
Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

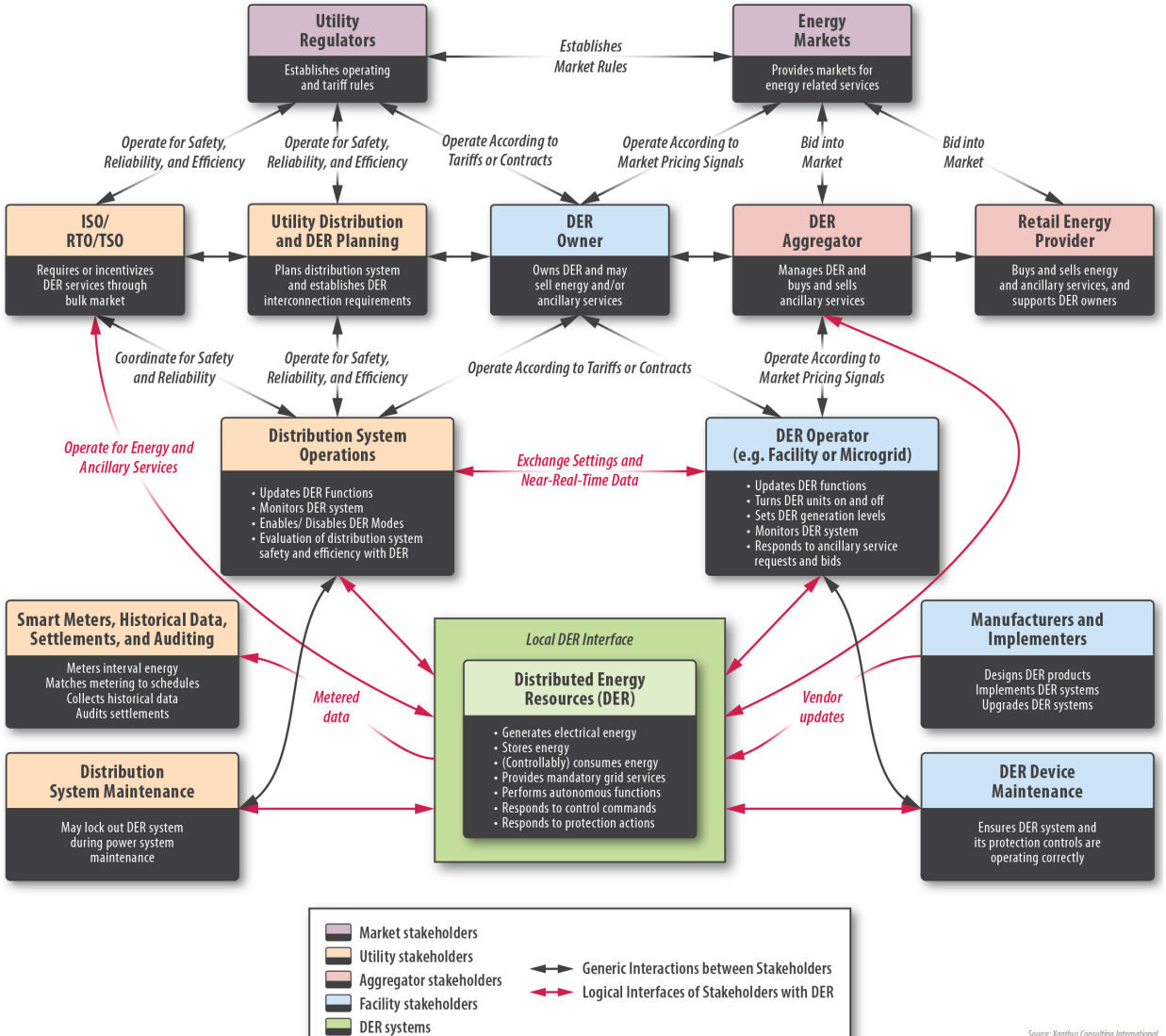
INL/MIS-22-69652

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

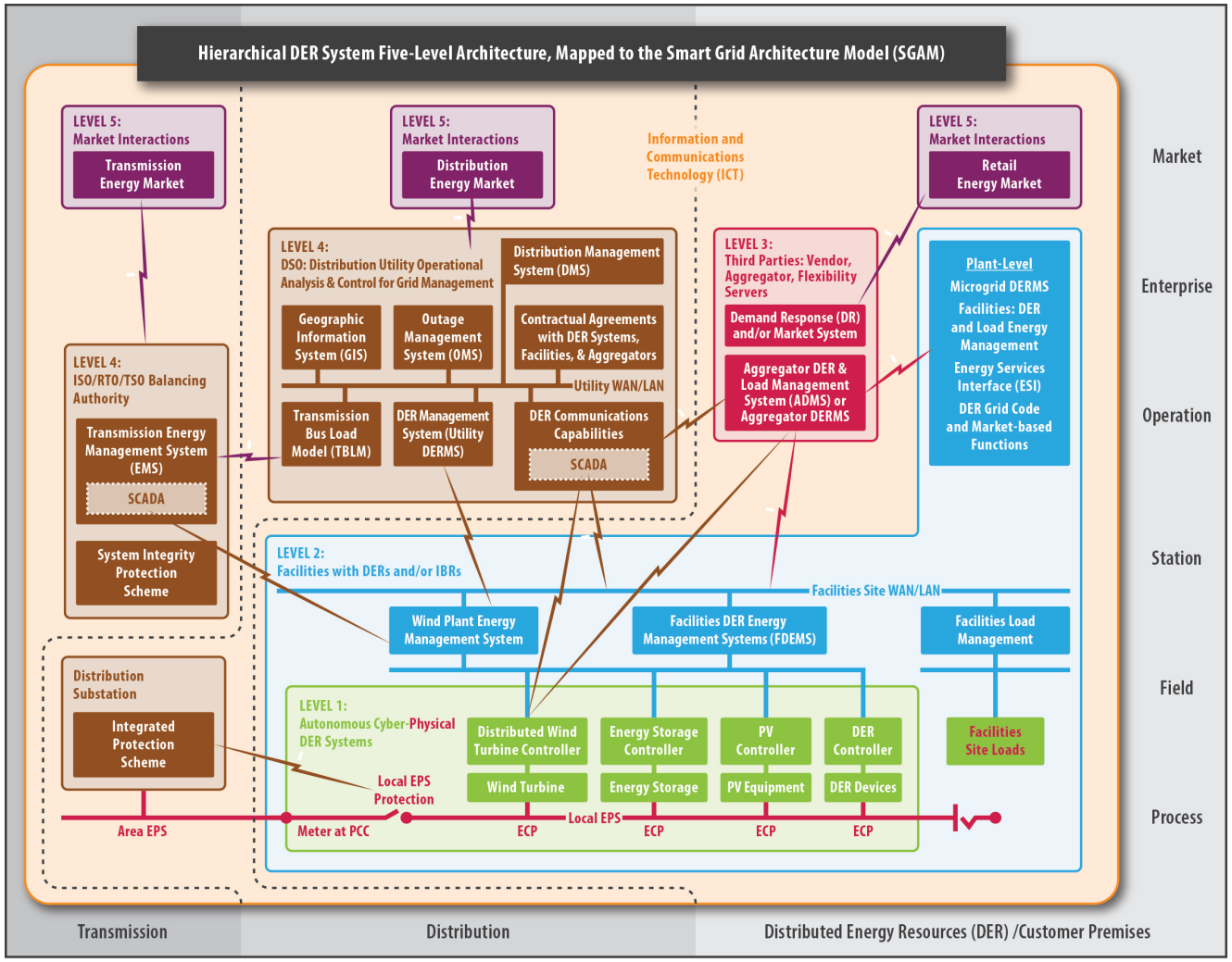


Distributed Wind Reference Architecture Stakeholders



- Who has a role in distributed wind cybersecurity?

Distributed Wind Reference Architecture
Overall Architecture

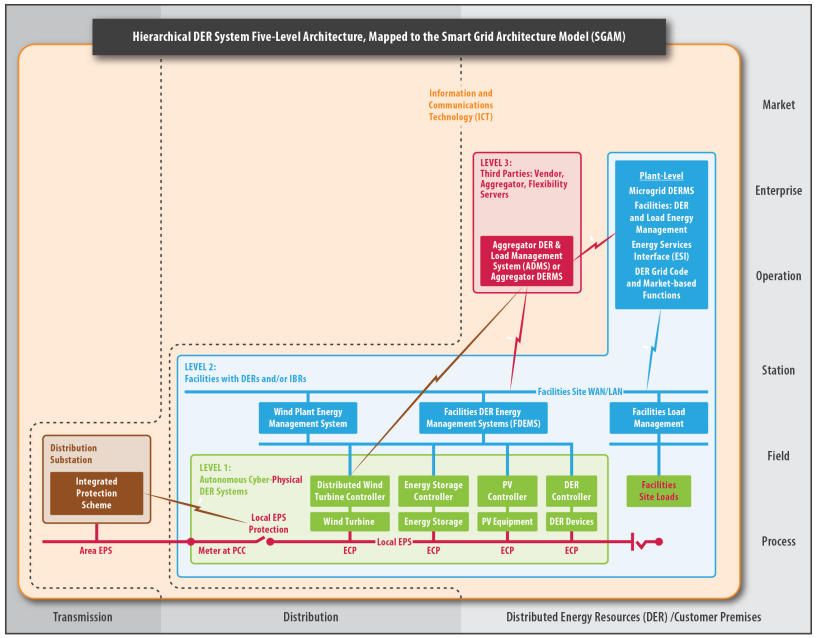


Source: Xanthus Consulting International
21-50152

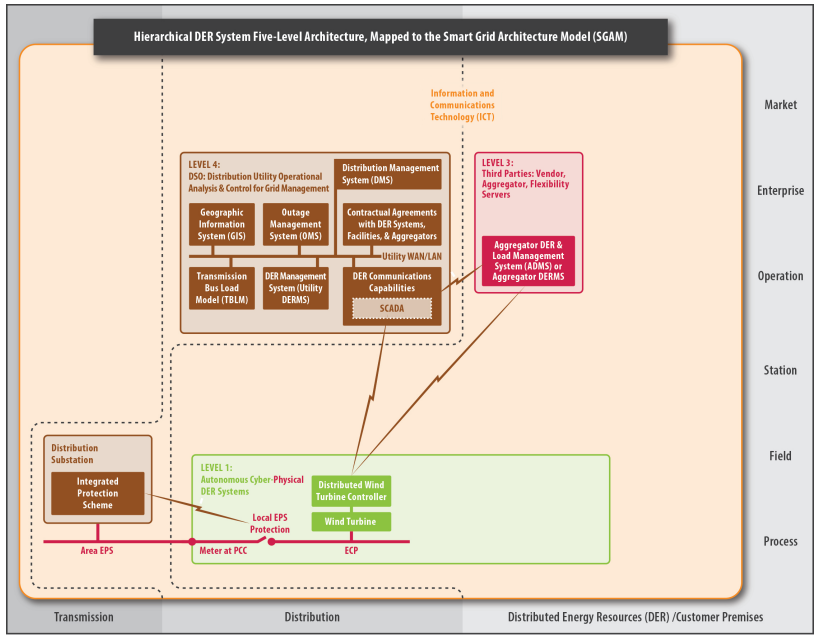
- What is the system that we are protecting?

Distributed Wind Reference Architecture
Customized Architectures

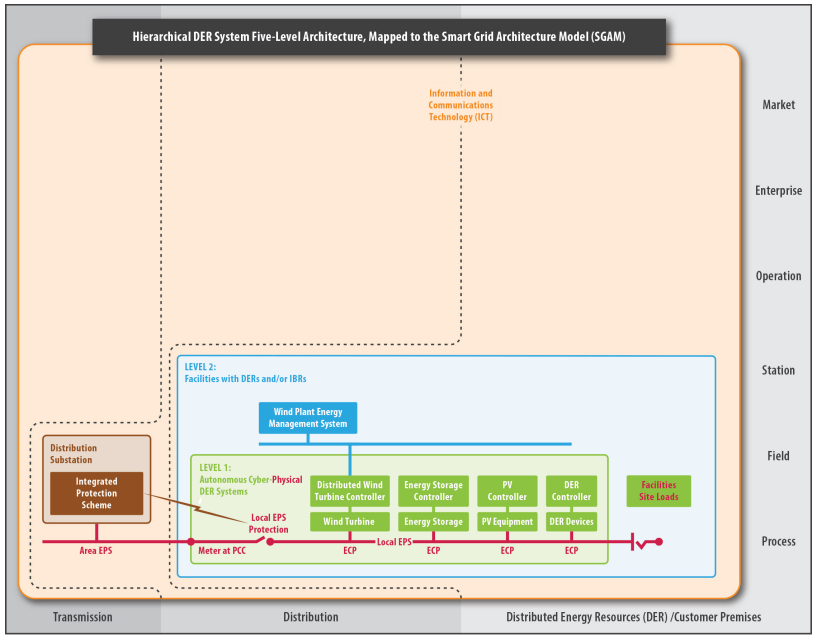
- How does this system change based on the configuration of assets?



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."

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

https://www.mita-teknik.com/products-solutions/wind/wind-turbine-control/turbine-control/

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

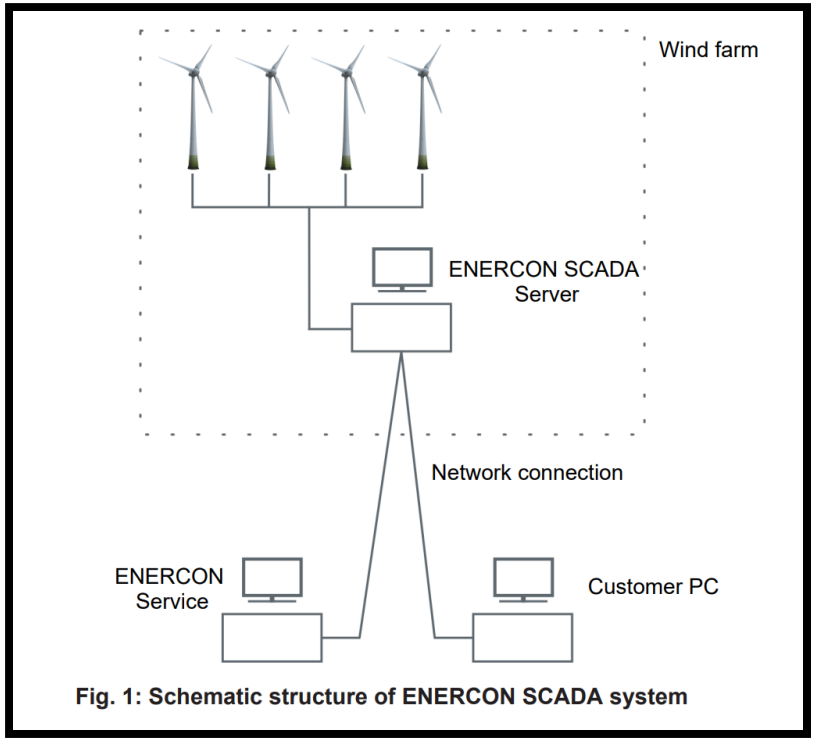


Fig. 1: Schematic structure of ENERCON SCADA system

Challenges to Securing Distributed Wind Systems

Risk Management Architecture

Risk = **Likelihood** x **Consequence**

Risk = **Threat** x **Vulnerability** x **Consequence**

Risk = **Threat - M_T** x **Vulnerability - M_V** x **Consequence - M_C**

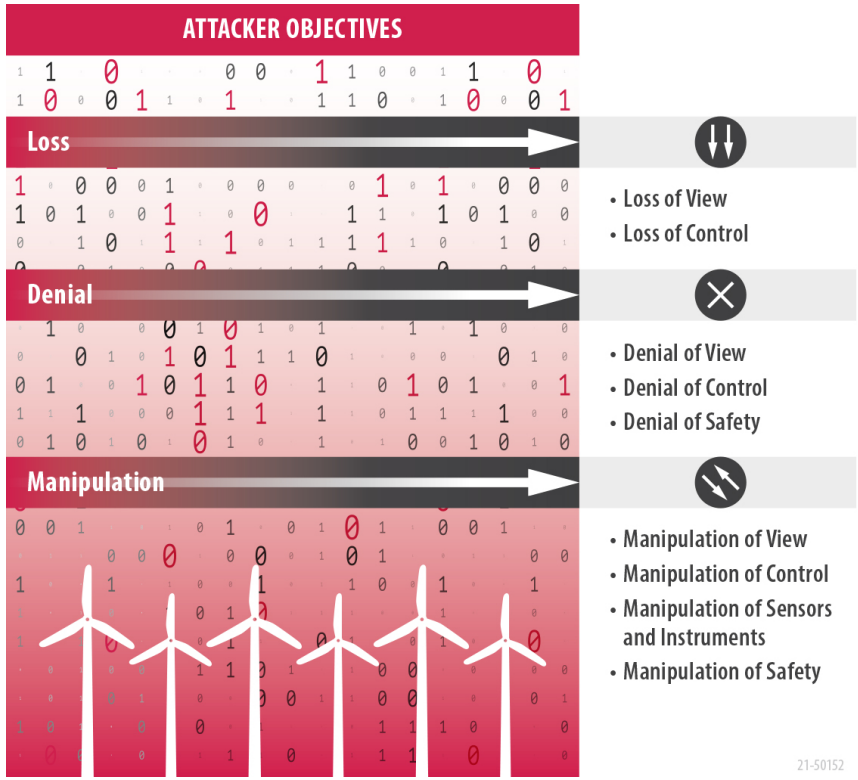
- Risk management comes from mitigating each element individually
- Cyber resilience measures can apply to any element

Risk Management Architecture: Threats

Threat = **Intent** x **Capability** x **Opportunity**

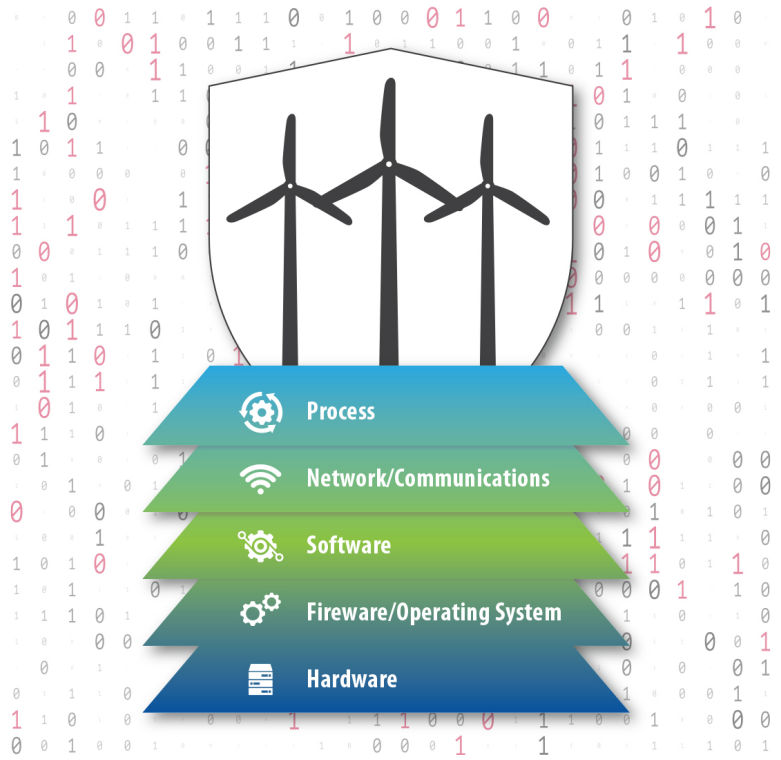
- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

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



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

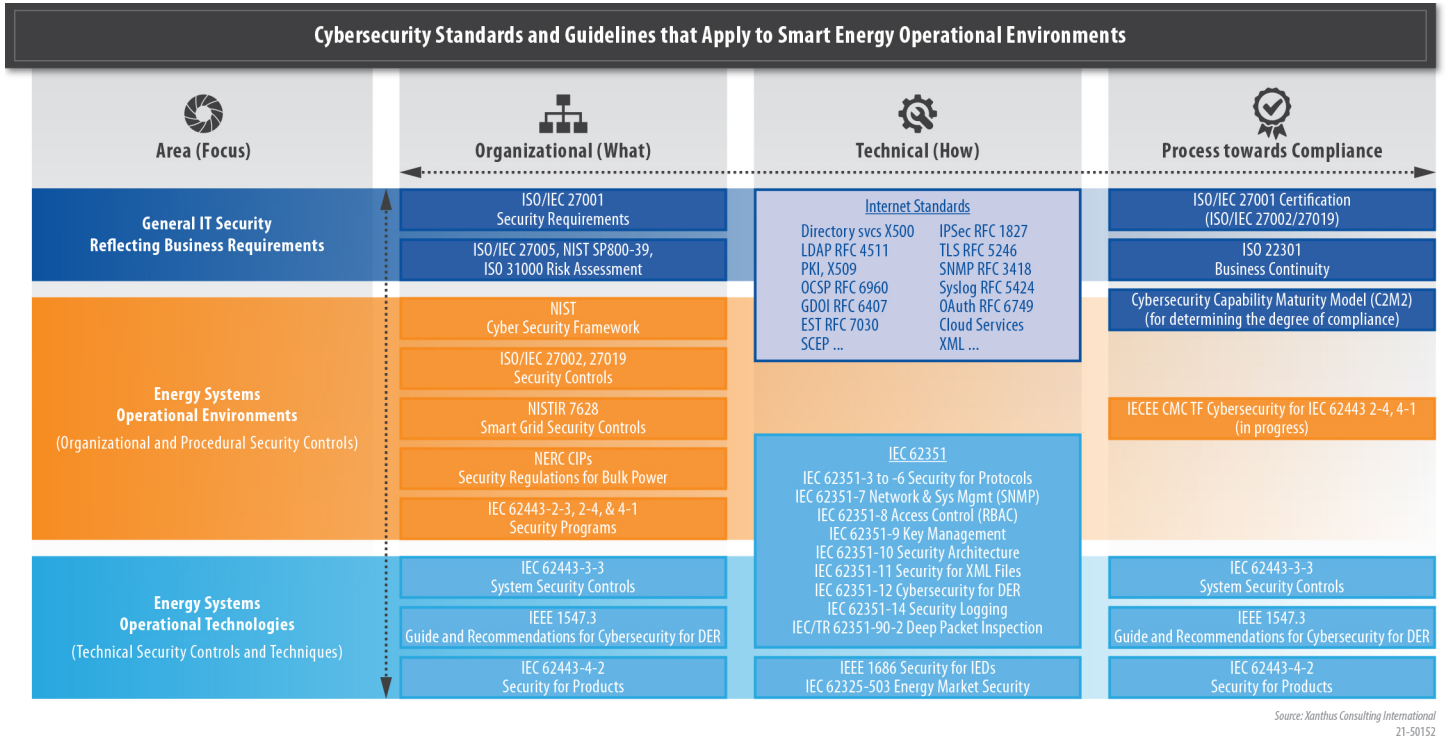


Risk Management Architecture: Consequences

POTENTIAL IMPACT BY STAKEHOLDER			
Event	**Utility (Non-Operator)**	**Operator (Facility/Aggregator/Utility)**	**Manufacturer, Integrator, or Installer**
Loss of View		• Loss of revenue	• Reduce reputation • Financial liability
Loss of Control	• Energy imbalance	• Propagated failures • Injury • Equipment damage	• Reduce reputation • Financial liability
Denial of View		• Improper operation	• Reduce reputation • Financial liability
Denial of Control		• Improper operation	• Reduce reputation • Financial liability
Denial of Safety	• Injury	• Injury	• Reduce reputation • Financial liability
Manipulation of View	• Improper control decision	• Improper control decision	• Reduce reputation • Financial liability
Manipulation of Control	• Additional energy resources • Injury	• Loss of reliable operation • Activation of critical load algorithm • Loss of required generation • Failure to meet contractual obligations	• Reduce reputation • Technical investigation • Financial liability
Manipulation of Sensors and Instruments	• Energy imbalance • Failure of regulatory compliance	• Improper operation • Severe mechanical damages • Loss of revenue resource • Increased operation and maintenance costs	• Reduce reputation • Increase after-sale expenses • Potential product call-back • Financial liability
Manipulation of Safety	• Extended restoration time • Failure of regulatory compliance	• Injury or death • Loss of intellectual property • Technical investigation	• Devalue brand name • Reduce market share • Decommission the product from the market • Financial liability

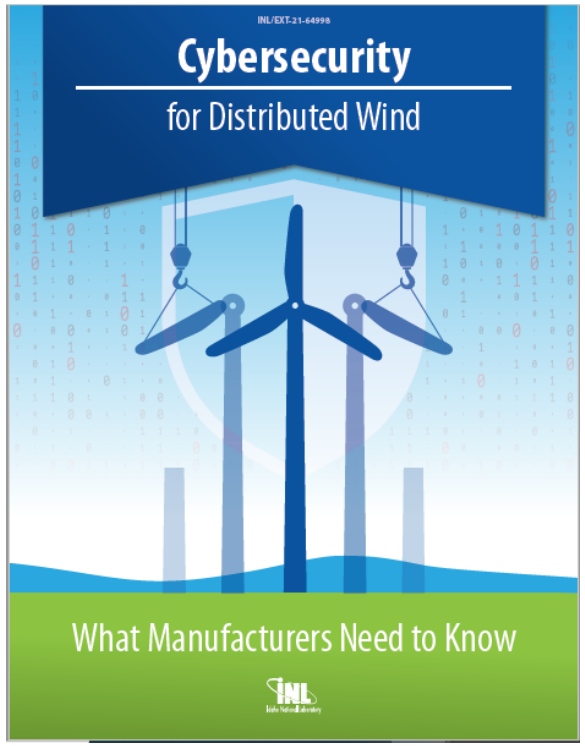
Mitigations: Cyber resilience by design

- 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

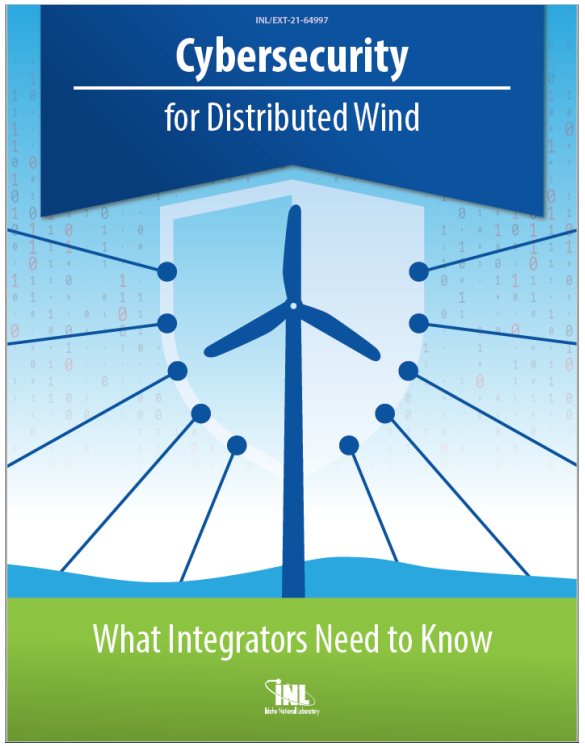


Mitigations: Cyber Resilience by Design

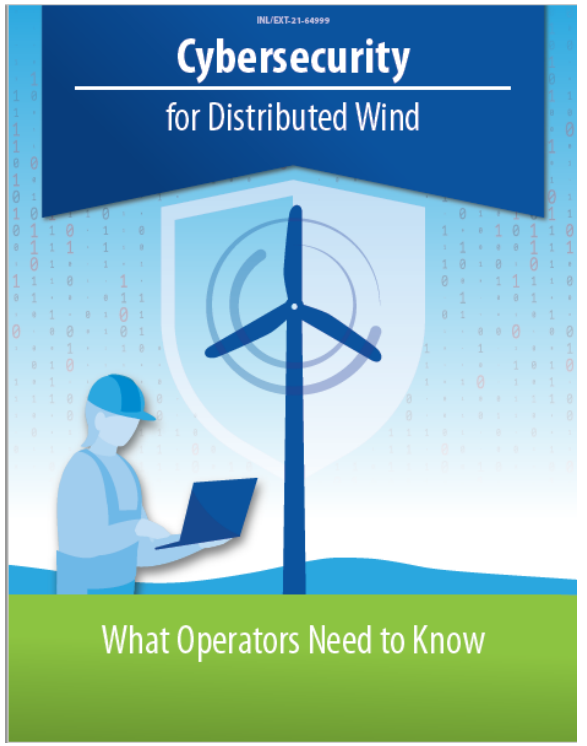
- Stakeholder roles and responsibilities



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.