INL/CON-25-82636-Revision-0

Threat Landscape for BESS and IBR

January 2025

Megan Jordan Culler

Changing the World's Energy Future

Idaho National Laboratory

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

INL/CON-25-82636-Revision-0

Threat Landscape for BESS and IBR

Megan Jordan Culler

January 2025

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

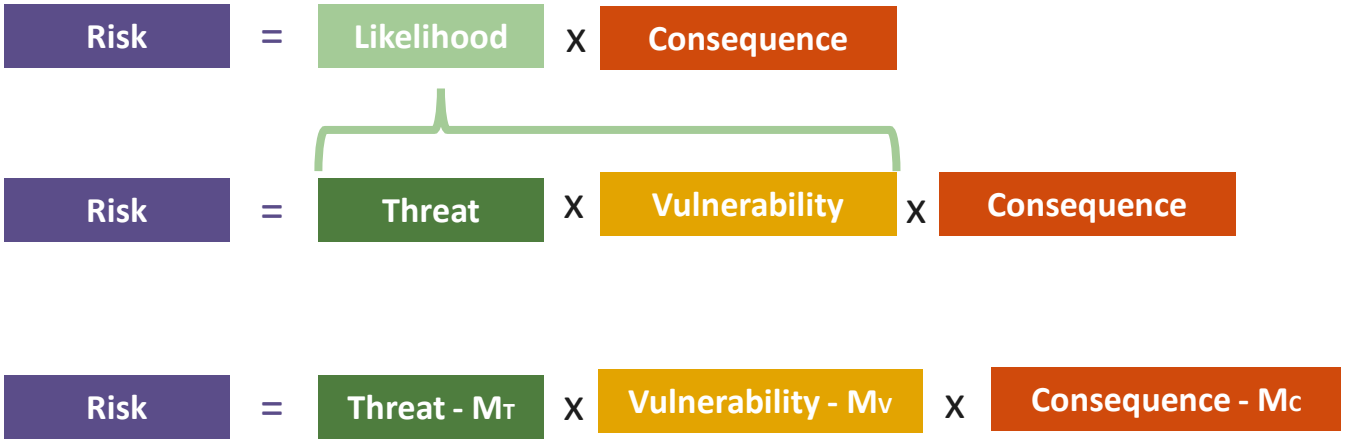
Threat Landscape for BESS and IBR

Megan Culler
Idaho National Laboratory

IEEE PES GRID EDGE TECHNOLOGIES CONFERENCE & EXPOSITION

INL/CON-25-82636

Cyber Risk Management Architecture



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

Threats

Cyber Risk Management Architecture

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	Technician accidentally deploys malware at wind plant
Organized group	Russian cybercrime or ransomware gangs
Hostile nation-state or terrorist	Nation-state sponsored APT

Attack Vectors

Physical Access

- Physical access to IBR plants or consumer IBR systems
  - Takes time to respond to intrusions

Image: Elgin Power Solutions
https://www.elginpowersolutions.com/substations/bess

Image: Copa Data
https://www.copadata.com/en/newsroom/tech-for-bess-essential-technology-for-smart-grids/

Cyber Access

- Vulnerable web APIs
- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network

Transient Access

- Authorized external devices
- Infected technician equipment

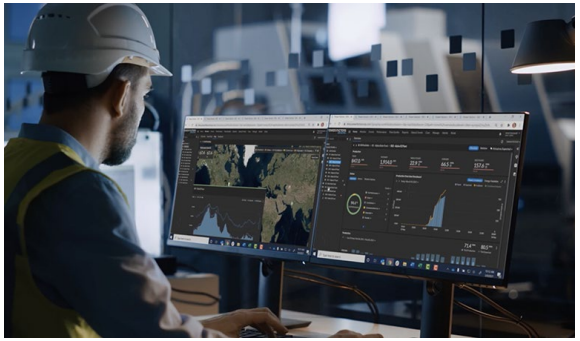


Image: Solar Power World
https://www.solarpowerworldonline.com/2024/04/qa-with-power-factors-on-large-scale-battery-om-considerations/

Exposure

What opportunity do adversaries have to reach a target system?

- Cyble researchers scanned the web for solar PV devices and found over 134,000 products from various vendors accessible
  - Note: exposed assets may not be vulnerable or misconfigured, but some interfaces did allow unauthenticated access
- Solar monitoring and management API exposes many entry points for various manufacturer integration; researchers generated authrorization tokens for any vendors & other breaches of data privacy (related issues with Deye batteries)
  - Solarman claims to be responsible for 195 GW of capacity across 2M+ plants involving 10M+ devices in 190+ countries and territories

Takeaways for IBRs:

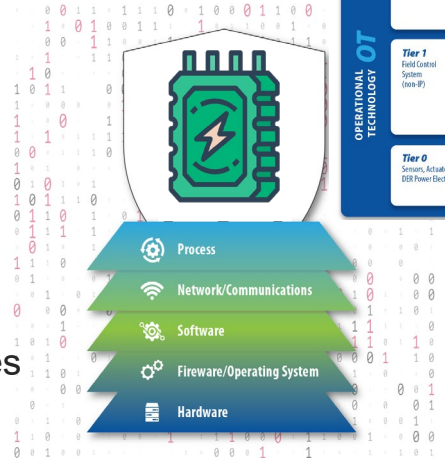
- Make sure operational systems are not exposed to public internet – use private subnets, VPNs, and firewalls.
- Use available tools to check against exposure (war driving sites, Shodan, etc.)
- Require passwords for access to web portals.

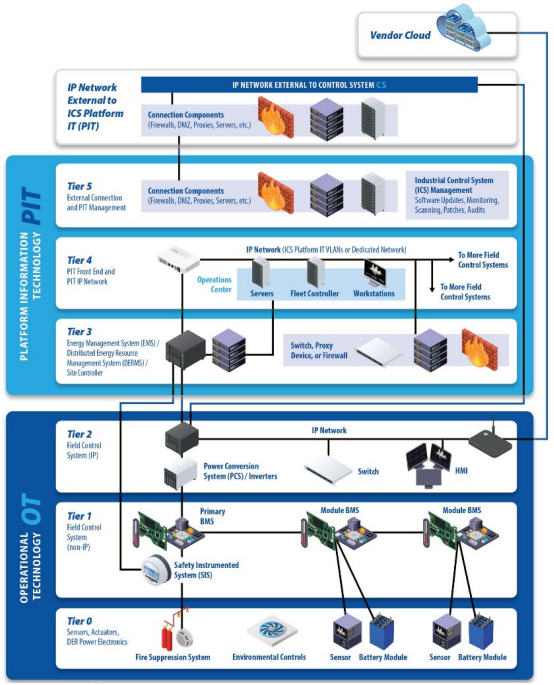
https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/

Vulnerabilities

Cyber Risk Management Architecture

- **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
- Renewable examples:
  - XZERES 442SR CSFR (ICSA-15-076-01)
  - Schneider Electric NICs, cooling, and BMS exposure vulnerability
  - CONTEC, SMA, Enphase web vulnerabilities





Trends in IBR Vulnerabilities

- Weak credentials
  - Weak requirements
  - Hard-coded credentials
  - Passwords derived from available information
  - Plaintext storage
  - Weak encryption or authentication
- Web page vulnerabilities allowing arbitrary code execution
- Web page vulnerabilities allow unauthorized access to data, private web pages, and sensitive files
- Root privilege escalation
- Cross-site scripting vulnerabilities
- Web apps were the most targeted service type followed by remote management protocols

Takeaways for IBRs

- Make sure the fix is really a fix
- Best practices for storing sensitive information (i.e., passwords)
- Web portal security

Consequences

Cyber Risk Management Architecture

- Asset health and damage
- Loss of remote monitoring
- Power system stability

Image: AMTEK Land
https://www.ametek-land.com/industries/powergeneration/fire-prevention

Image: Tesla Megapack on fire at Victorian Big Battery Australia; from Fire Rescue Victoria

Critical failures can lead to severe physical damage.

- Ancillary services
- Power dispatch
- Reputational damage

Recent Renewable Energy Cyber Attacks

2018: Malware on wind plant (U.S.)
Mar. 2019: sPower DoS (U.S.)
2020: PoetRAT campaign (Azerbaijan)
Nov. 2021: Vestas Ransomware
Feb. 2022: Enercon GmbH DoS (Germany)
Apr. 2022: Nordex SE Ransomware
Apr. 2022: Deutsche Windtechnik AG Ransomware (Germany)
Sept. 2022: Canadian Solar Ransomware (Canada)
2022: Chinese reconasissance activities on wind installations
Mar. 2023: Mirai botnet exposure using SolarView devices
May 2023: Coordinated attack on Danish utilities (Denmark)
Aug. 2023: Energy One data breach (Australia)
Jan. 2024: Schneider Electric Sustainability Business ransomware (France)
Feb. 2024: Compromise of EV charging management platform (Lithuania)
May 2024: Bank fraud using SolarView vulnerabilities (Japan)
Sept. 2024: Alleged attack on solar monitoring platforms (Lithuania)

sPower Denial-of-Service

March 15, 2019

- Utah-based independent power producer sPower
- Known vulnerability exploited in Cisco firewall
  - Forced firewalls to reboot repeatedly
  - 5-minute interruptions occurred repeatedly over 12-hour period
- Disabled communication to generation sites
  - Loss of view to field equipment and generation sites
- Did not affect power generation
  - Thought to be a test or scan
  - Adversaries may not have known what they were affecting

https://cyberscoop.com/spower-power-grid-cyberattack-foia/

Takeaways for renewables:

- Effective patch management strategies key
- Limit exposure of internet facing devices
- Note prevalence of IT infrastructure in the OT environment

S·POWER
An AES and AIMCo Company

Ransomware Attacks

- Vestas (November 2021)
  - Cyber incident reported (Group using Lockbit 2.0 took credit)
  - IT systems shut down across multiple business units
  - Data stolen, some personal data publicly released
  - Ransom not paid (“failed in attempt to extort”)
- Nordex SE (April 2022)
  - Conti ransomware
  - IT systems and remote access to managed turbines shut down
- Deutsche Windtecnik AG (April 2022)
  - Controlled shut down of remote monitoring for turbines
  - Regular activity restored within 3 days
  - Evidence found of Conti ransomware on IT systems
- Canadian Solar (September 2022)
  - Lockbit 3.0 ransomware
  - $20k to return data; $20k to destroy data; $10k/day to extend deadline

Takeaways for renewables:

- Track reliance on third-party services and OEM access
- Ransomware continues to be prevalent, and indirectly impacts OT

https://informationsecuritybuzz.com/canadian-solar-has-been-hacked-by-lockbit-3-0-ransomware/
https://www.vestas.com/en/media/company-news/2021/third-update-on-cyber-incident-c3466518
https://cybernews.com/news/deutsche-windtechnik-hit-with-a-cyberattack-a-third-on-germanys-wind-energy-sector/
https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/

Mirai botnet exposure

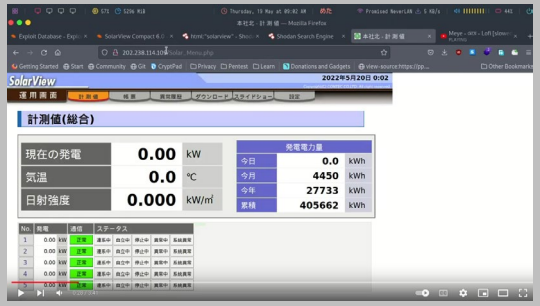
March 2023

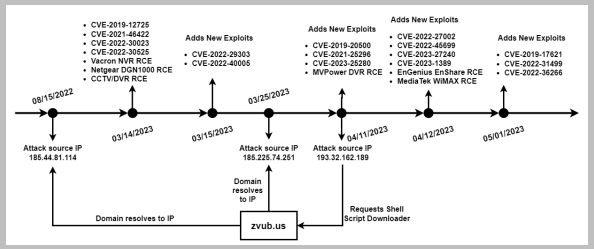
- Palo Alto Networks Unit 42 describes threat actor activity leveraging IoT vulnerabilities to spread a variant of Mirai botnet
- Contec SolarView vulnerabilities included, but not the only ones
- After adding solar devices to botnet, used to execute additional attacks, including DoS
- Shodan indexed 600 accessible SolarView systems
- Less that 1/3 of internet-facing SolarView systems appeared to be patched against the CVE.
- Exploits posted to blogs, YouTube videos, Exploit-dB database

https://vulncheck.com/blog/solarview-exploitation
https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits/

Takeaways for renewables:

- Apply patches as soon as possible
- Ensure devices not on public internet





Campaign affecting multiple U.S. water facilities

November 2023

- CISA alert released detailing active exploitation of Unitronics PLCs in multiple sectors, including water and wastewater systems
- Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated actors
- Compromised devices that used default credentials
  - Forescout research indicated >1,800 Unitronics PLCs exposed to the internet worldwide
- Impact:
  - Municipal water authority in Aliquippa, PA confirmed that a booster station was hacked, but no risk to water supply
  - Attack triggered an alarm, which caused operators to take over manual control of the station
  - Defaced HMI

https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

Takeaways for renewables:

- Renewables or particular vendors may be targeted for various affiliations

Exploitation of Contec SolarView vulnerabilities in bank attacks (May 2024)

May 2024

- Japanese media Sankei Shimbun reported 800 SolarView compact devices hijacked in Japan
- Exploited systems unpatched for same 2022 CVE
- No operational impact to systems
- Used the devices to steal bank accounts and commit bank fraud for financial gain

https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html

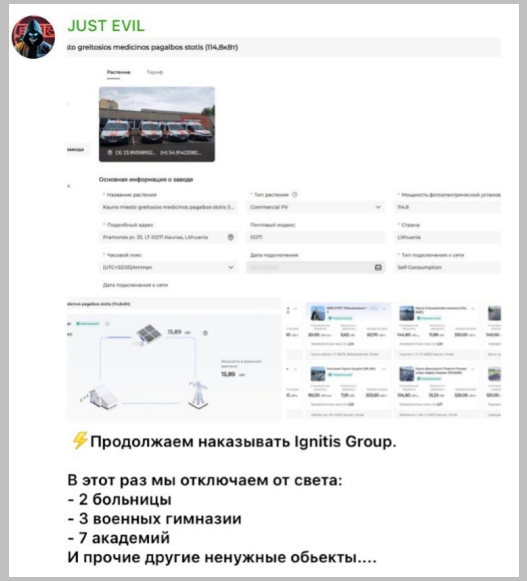
Takeaways for renewables:

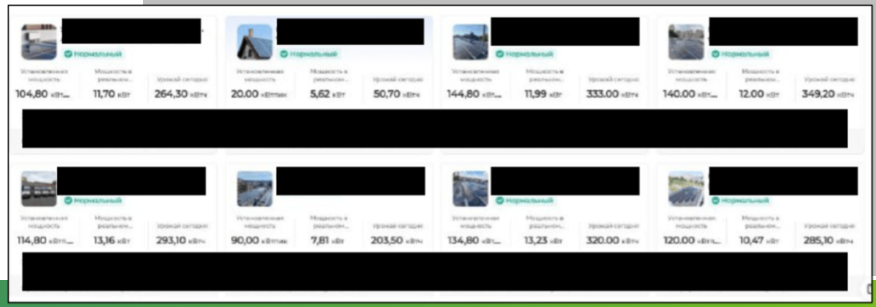
- Apply patches!
- Proof-of-concept code can make exploits easy for different threat actors.

Alleged Attack on Lithuanian Solar Monitoring Systems

September 2024

- Pro-Russian hacktivist group Just Evil claimed to compromise PV monitoring solution used by the state-owned energy holding company Ignitis Group
- Claimed to access power monitoring dashboard of 22 Ignitis clients, including hospitals and military academies.
- Believed that compromised credentials provided initial access.
- Same group compromised EV charging control panel in February, demanded ransom.
- No operational impact from this incident, no ransom reported.





https://cyble.com/blog/solar-monitoring-solutions-in-hacktivists-crosshairs/

Trends

- Notable increase in attacks targeting IBR installations at large
- No strong evidence that renewables being targeted because their renewables or for operational impact
  - Active exploitation of vulnerabilities just uses devices for computing power for other attacks
- Ransomware and data breaches continue to be some of most common attacks.
- Operational impact seen most as denial-of-service.
  - Level of impact depends on stakeholder affected and criticality of assets.
- Attacks targeting third parties (OEMs, maintenance, etc.)
- APT activity detected before OT attack executed

THANK YOU

Megan Culler

megan.culler@inl.gov

https://inl.gov/national-security/csdet/

IEEE PES GRID EDGE TECHNOLOGIES CONFERENCE & EXPOSITION