Cybersecurity and Wind Farms
What does cybersecurity really mean?

Security is the process of maintaining three primary attributes:

- **Availability** ensures that the system is reliably available for its intended purpose
- **Integrity** ensures that data is what it is supposed to be, and control is maintained
- **Confidentiality** ensures that only the people you want to see your data can see it

**Note:**

IT = Information Technology (i.e., data processing)
OT = Operational Technology (i.e., control systems)
Overview:
Researchers cut lock to break into turbine tower and exploit control network to pivot into SCADA servers, resulting in full control of entire wind farm. Wired article precedes well attended BlackHat talk on hacking wind farms. Turbine manufacturer was not revealed.
Malware comes in many forms

**RANSOMWARE** – at least it tells you it’s there...

All your files have been encrypted!
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.

**RATs** give hackers remote control
Trojans can be modular frameworks allowing attackers to customize reconnaissance and further penetration.

**CRYPTOMINING** is stealthy but disruptive
With DNS access, attackers can exfiltrate data, including Bitcoin from stolen CPU power.
There is no shortage of motivated actors

**Nation State**
- Well funded & state sponsored
- To further economic, political, or military initiatives
- In preparation for warfare

**Cyber Crime**
- Organized crime establishing crime as a service
- Theft of credentials & personal information
- To monetize through fraud

**Insider**
- Authorized employees or contractors
- Theft of company information/trade secrets
- For personal gain or correct perceived social injustice

**Hacktivism**
- Individuals supporting or sponsoring a “political movement”
- Theft of company information/public disclosure
- To conduct political or social protest
How do they get in?

- Insecure protocols exposed to the Internet
- Vulnerable software not updated or patched
- Simple passwords, unchanged default passwords
- Infected files copied from USB or network shares
- Improper use of SCADA equipment (email, web)
- Unmonitored or unaudited security events

Searching for and penetrating targets is now automated at global scale!

A ‘hacker’ is malicious software... without a deadline.
Software uses “service ports” to listen for commands from over the network. If software listening on a network has a vulnerability, it can be exploited by any network node that reaches it.

Ports can be mapped from LAN to WAN...

Software should be kept updated and configured to manufacturer recommendations to avoid exploitation.
Securing remote connections is critical

Asset operator connections should:

- Use IPSec VPN tunnels to avoid exposure to the public Internet
- Configure routers to disable ports not in use
- Use Access Control Lists (ACLs) to restrict traffic to specific IP addresses (i.e. hide from public search engines)
- Utilize a firewall with proper rule sets to whitelist or blacklist IP addresses (and country domains) and trigger event alerts
- Employ monitoring to alert on attacks as close to real time as possible
Confidential. Not to be copied, distributed, or reproduced without prior approval.

Exploiting the Internet

What we can learn from a public search engine:
- Software displays ‘banners’ in response to queries
- Vuln databases can be searched with versions
- Location triangulation is possible

Why use VPNs and ACLs?

Outdated firmware

Fingerprint of Sierra Wireless cell modem

Old embedded Linux

Some obsolete crypto (can negotiate fallback?)

What else?
Here is the interface to that Sierra Wireless modem, found on an adjacent public IP address, and accessed using the default password.

These interfaces have been found in the field with another open TCP port known to be a Remote Access Trojan (RAT).

With the RAT installed, the device behaves normally, but allows attackers to spy on the network traffic.

Your best defense is a regular assessment of your security posture.
Secure design was optional, cybersecurity regulation nonexistent
Standardizing network segmentation

Segmentation isolates malware from spreading

- Control system networks intended to be isolated from customer Enterprise networks, using only appropriate gateway protocols routed to customer networks.
- Core firewalls are used to direct network traffic, prevent unauthorized use, optimize bandwidth and latency within segments.
- Unhardened systems such as printers, VOIP phone systems, etc. are not intended to reside in control system environments.
- Align with standards such as ISA/IEC 62443 for network segmentation and hardening.
Security management applied to the wind farm
Summary

- Cybersecurity risks in wind farms are no different than other critical infrastructure!
- To mitigate risks, a strong security program and preventative measures are needed.
- Proactive security management is a significant defense against production loss.
Thank you

Q&A