Wattch
404-649-0458
team@wattch.io

Are your energy assets secure?

When it comes to securing energy projects, there is no silver bullet. Good security is the result of hundreds of small decisions.

However there are practices and pitfalls you can look for as you select hardware and software for your projects.

1 Why good security practices matter

In the headlines

European wind-energy sector hit in wave of hacks

Wall Street Journal
April 25, 2022

Dutch agency investigates cybersecurity of PV inverters after hack

PVmagazine
September 6, 2022

Poor security practcites can lead to...

- **Lost revenue**
- **Device damage**
- **Grid instability**
- **National security threats**

2 Having a security-first mindset

Security can be compromised in subtle and insidious ways, so it is important to consider security in every decision, large or small.

Malicious actors can exploit small vulnerabilities that are difficult to identify until after the fact.

These actors steal, delete or write fake data, which can trigger or suspend control loops, as well as control assets directly.

To help prevent security breaches, select partners committed to protecting your data both at the edge and in the cloud.

3 Best practices and pitfalls

Look for...

Secure websites (HTTPS)
- Prevents DNS spoofing
- Prevents hijacking and snooping
- Secures traffic to site

Mutual authentication
- Ensures security of server
- Prevents unauthorized data access and posting
- Ensures uncorrupted reporting, billing metrics, and control loops

Multi-factor authentication
- Prevents unauthorized access in the event of leaked passwords

Encrypted credential storage
- Ensures credential safety in the event of unauthorized access

Data encryption at rest and in transit
- Ensures data safety in the event of unauthorized access

Different credentials per edge device
- Ensures fleet safety in the event that a single device is compromised
- Enables easy deactivation after a breach

Secure remote firmware upgrades
- Ensures that security patches can be applied without a site visit

Customizable permissions
- Limits scope of damage for compromise of individual accounts
- Prevents damaging changes made by less-trusted actors

Audit logging
- Provides a paper trail to determine who accessed which resources or made which changes

Avoid...

Public IP addresses
- Necessitates strict firewall rules to prevent access to OS processes that impact the entire system

Shared accounts and passwords
- Requires unnecessary storage and transmission of credentials
- Easier to leak, harder to update

Outdated technology
- Increases risk of unpatched security vulnerabilities
- Increases the available time for hackers to exploit vulnerabilities

Custom security practices
- Publicly-defined security standards have been battle-tested by millions of people over many years
- Customized, in-house standards often have more vulnerabilities

Cloud platforms and edge devices that don't require authentication by default

4 Evolving security standards

Commercial Scale

IEEE 1547.3-2007

IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems

IEEE 2030.5-2018

IEEE Standard for Smart Energy Profile Application Protocol

Utility Scale

NERC/CIP (Critical Infrastructure Protection) Standards 002-014

6 Get involved

SunSpec / Sandia
DER Cybersecurity Work Group
https://sunspec.org/cybersecurity-work-group/