Cybersecurity and Artificial Intelligence (AI)

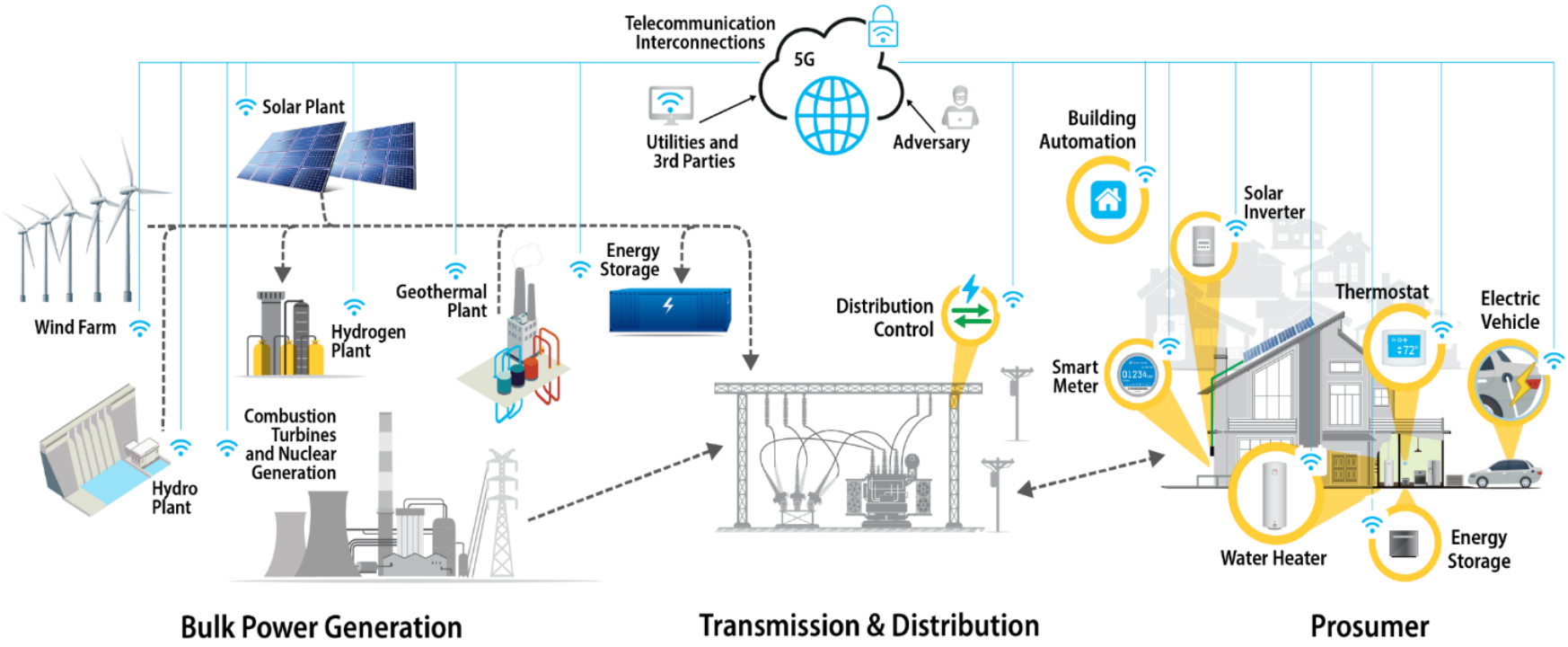
Maurice Martin
NREL
Sep. 9, 2025

Photo by Josh Bauer, NREL 61725

This presentation was produced when the laboratory operated as the National Renewable Energy Laboratory (NREL). The laboratory is now the National Laboratory of the Rockies (NLR).

Coast to Coast

The **17** national laboratories have served as the leading institutions for scientific innovation in the United States for more than 90 years.



Modern Power Grid Operations Requires Advanced Analytics

Examples of <u>current</u> AI applications:

- Load forecasting
- Weather/renewable generation prediction
- Cyber anomaly detection
- Fault detection, asset monitoring, etc.

The Rate of Change is Increasing

More operational change in the next **10 years** than we've seen in the last **100 years**.

Utilities are now **data companies** as much as they are **energy delivery companies.**

OUTAGE PREDICTIONS

Direct resources to at-risk areas.

Example: Énergie NB Power has leveraged machine learning to speed restoration and save millions annually.

PERFORMANCE OPTIMIZATION

Maximize Efficiency.

Example: Xcel Energy analyzes wind variability to optimize renewables, saving millions by reducing fossil-file ramp-ups.

IMPROVED VEGETATION MANAGEMENT

Prioritize trimming activities

Example: National Grid decreased customer interruptions by 38%, saving millions.

Source: https://www.utilitydive.com/spons/analytics-and-ai-for-utilities-unlocking-efficiency-and-reliability/758825/

Examples of Emerging Energy Applications for AI

On the AI horizon…

Any digital system can be compromised through cyberattack.

Even AI.

With sufficient resources, skills, and motivation, attackers will succeed.

If compromised by cyberattack…

Security **WITH** AI	Security **OF** AI	Security **FROM** AI
SOLUTION		
Employ AI for **detection, prediction, and autonomous response** in power grid environments.	Ensure AI systems used in grid operations are **robust, interpretable, and verifiable**.	**Understand and address risks from malicious use of AI** that target the energy sector.

AI & Cybersecurity

The energy sector **will** continue adopting AI, securely or not.

Can we enjoy its benefits while maintaining an acceptable level of cyber risk?

Yes, if we proactively prevent the worst possible consequences of cyberattack.

- Start during design and implementation.

- Take “doomsday scenarios” off the table.

- Address less severe consequences through continuous improvement.

Cyber-Informed Engineering

Cyber-Informed Engineering (CIE): Designing Out Worst-Case Cyberattacks

CIE Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

Cyber-Informed Engineering Program Activities

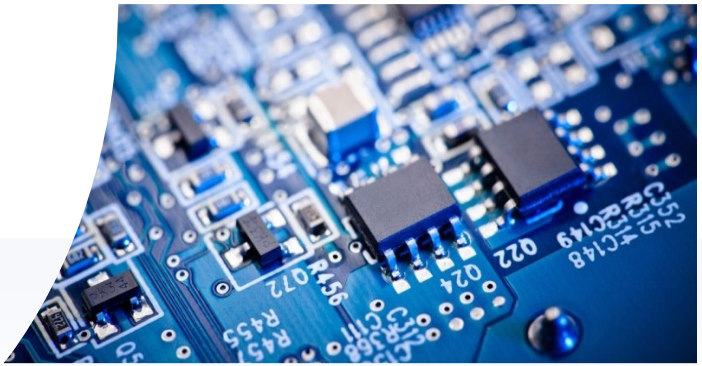
- Sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response

- Performed by:
  - Idaho National Laboratory (INL)
  - National Renewable Energy Laboratory (NREL)

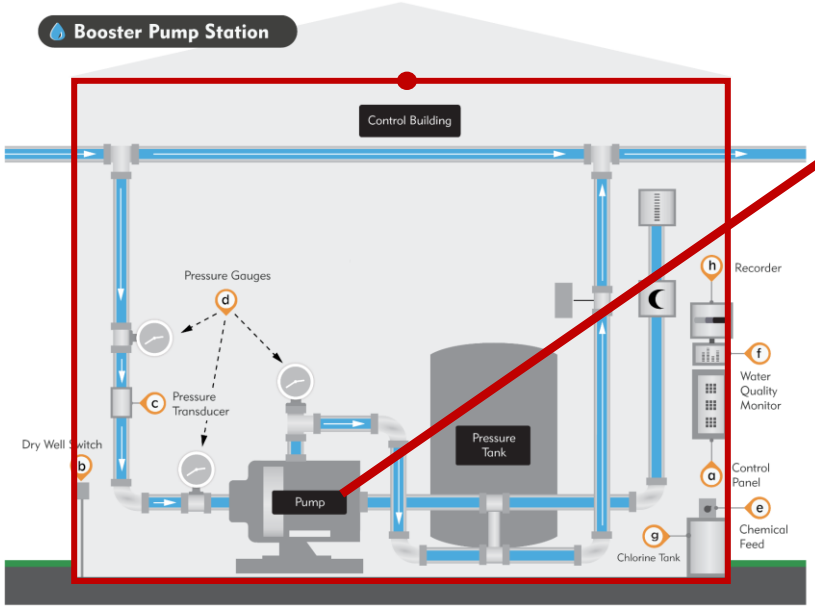
- The project benefits from the voluntary participation of:
  - Utilities
  - Vendors
  - Academia
  - Other industry stakeholders.

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attacks.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation life cycle rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to create a **culture of security** that is aligned with the existing industry safety culture.



Water Booster Pump Station



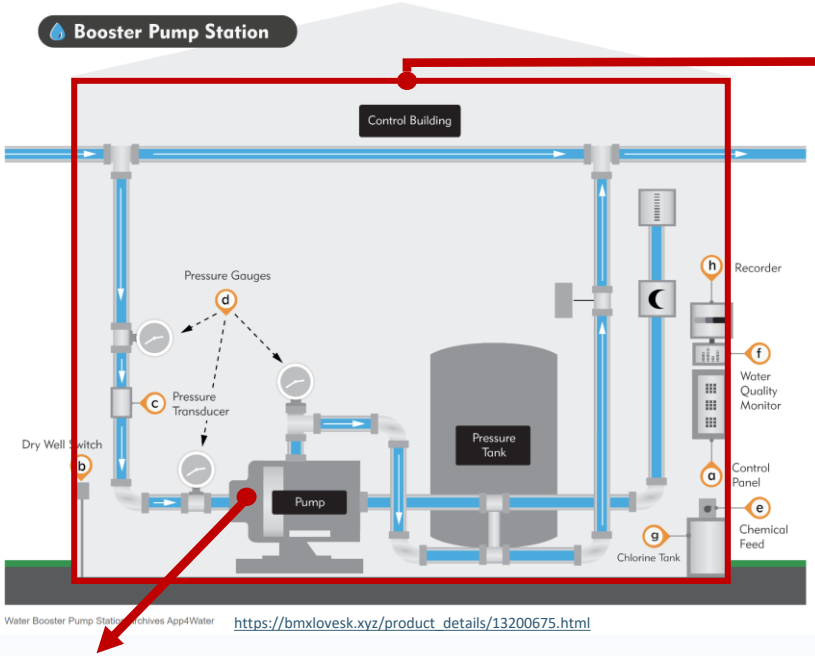
Water Booster Pump Station Archives App4Water https://bmxlovesk.xyz/product_details/13200675.html

Cloud-based monitoring and control

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

Water Booster Pump Station



Cloud-based monitoring and control

Mechanical time delay relay

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

Cyber-Informed Engineering

For more information

Maurice.Martin@NREL.gov

https://www.nrel.gov/security-resilience/cyber-informed-engineering

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Thank You

www.nrel.gov

This work was authored by the National Laboratory of the Rockies for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Photo from Getty-181828180

NLR/PR-5T00-96913

NREL