Strengthening Our Grid Against Tomorrow's Threats

Energy is changing. Are we ready? The National Renewable Energy Laboratory (NREL) offers unique research capabilities to help innovators and partners prepare for an energy future with increased connectivity, diversity, and uncertainty.

New Trends, New Threats, Security-by-Design Solutions

Security is paramount for the energy sector—whether for a device manufacturer, power provider, industrial operator, or customer at home.

Cybersecurity takes on new significance in energy systems that are becoming more integrated with renewable and increasingly distributed technologies, connected by digital communications and advanced controls, and faced with new threats by malicious actors that are becoming more sophisticated. These trends are all on the rise and open the energy sector to vulnerabilities that underlie the critical need for cybersecurity innovation that will strengthen our grid against tomorrow's threats.
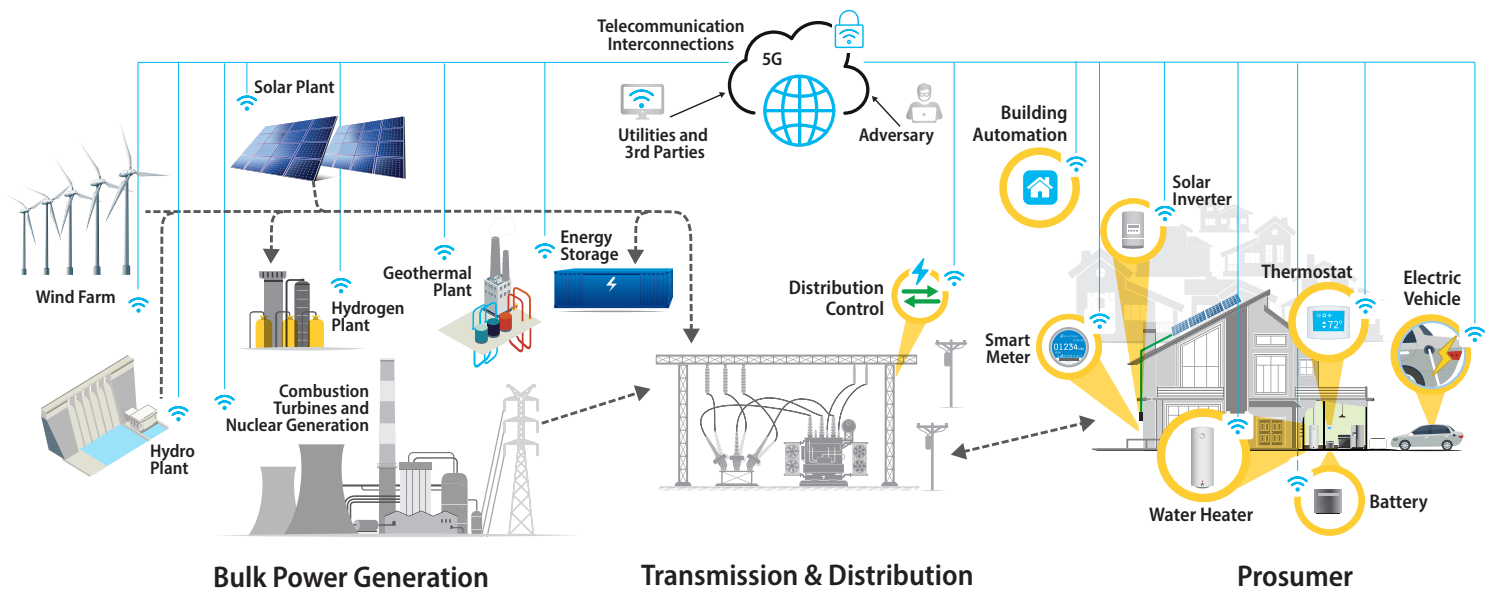
To continue building clean, efficient, and reliable energy infrastructure, industry needs advanced tools that can address future energy security and adopt security-by-design solutions.

Replicating Energy Systems to Derisk Cybersecurity Deployments

Enacting cybersecurity solutions requires a leap from laboratory validations to actual implementation. But NREL can make that leap far less difficult by bringing real systems into the lab. As part of NREL's Advanced Research on Integrated Energy Systems (ARIES) platform, NREL's cyber range provides vast connectivity between hardware across NREL's Energy Systems Integration Facility, Flatirons Campus, and an advanced emulation environment.

These integrated capabilities allow users to witness how devices and operations respond in real time to future cybersecurity threat scenarios. Companies and utilities can validate the cybersecurity of new technologies within a highly realistic, virtual operational environment and identify potential risks before they are deployed on real systems. The cyber range is being applied in several wide-reaching collaborations, including the exploration of 5G and advanced communications, the cybersecurity of extreme-fast-charging electric vehicle infrastructure, and employing artificial intelligence response to identify and classify power grid anomalies.

Telecommunication Interconnections

5G

Utilities and 3rd Parties

Adversary

Solar Plant

Building Automation

Solar Inverter

Thermostat

Electric Vehicle

Wind Farm

Hydrogen Plant

Geothermal Plant

Energy Storage

Distribution Control

Smart Meter

Hydro Plant

Combustion Turbines and Nuclear Generation

Water Heater

Battery

Bulk Power Generation   **Transmission & Distribution**   **Prosumer**

Research for Secure Energy Transitions

NREL is a leader in cybersecurity research for future energy systems. With distributed energy expertise, broad technical capabilities, and access to highly advanced energy evaluation platforms, NREL has worked alongside partners from utilities, cyber solution providers, and government agencies to demonstrate forward-thinking approaches to energy security. NREL's work in cybersecurity research falls into three focus areas:

Technology innovation—NREL is involved in foundational research and development that integrates cybersecurity into the design of energy devices. Past and ongoing projects include a plug-and-play encryption technology for distributed energy resources, an artificial intelligence solution for situational awareness, and blockchain methods for energy security management. NREL's innovations have been used in broad applications, such as electric vehicle charging and 5G communications networks.

Market and planning support—Government agencies and policymakers are often at the forefront of difficult cybersecurity decisions for energy systems. NREL uses a variety of custom tools, such as its Distributed Energy Resource Cybersecurity Framework, to help energy decision makers of any type assess and improve their cybersecurity posture. In addition to decision support, NREL convenes consortiums and multisector stakeholder groups, such as the Wind Cybersecurity Consortium, to advance standards and share best practices.

Deployment strategies—When it comes to putting security-by-design theories into practice, no two energy systems are the same. That fact is underlined by differences in operations, staff experience, and system hardware. To help businesses and organizations confidently deploy their unique cybersecurity solutions, NREL houses one of the world's most advanced, integrated research platforms for cyber-energy evaluation. NREL's cyber range can replicate cyber and physical characteristics of any system at real power, and it has been used to train, teach, and analyze organizations for cybersecurity deployment.

Work With Us

NREL offers unique capabilities and expertise for achieving future energy cybersecurity—and many ways to partner across the energy sector.

To learn more about our research or opportunities for partnerships, visit **www.nrel.gov/security-resilience/work-with-us.html.**