Photo by Werner Slocum, NREL 62543

The NREL Cyber Range

A one-of-a-kind environment for experiencing energy system cybersecurity with real technologies and operations.

With the National Renewable Energy Laboratory's (NREL's) cyber range, researchers can replicate cybersecurity scenarios as they would occur on real, complex energy systems. With supercomputing and advanced emulation capabilities, the cyber range allows users to build digital twins of real systems and connect the emulated environment to actual physical devices throughout NREL's laboratories. The space offers unlimited potential to test the frontier of energy systems security.

The NREL cyber range combines accurate energy system models, advanced controls, and tomorrow's energy infrastructure to construct a flexible environment that matches the sophistication of future threats and defenses. At NREL, researchers and partners can safely explore energy disruption scenarios with the fidelity needed to represent future distributed energy systems—from individual devices to utility power grids, cities, military bases, and more.

The Threat Landscape

In 2016, malware struck an electric transmission station in Ukraine, sending automated commands that blacked out a portion of the capital city, Kiev. The incident was one of several that proves malicious actors have advanced methods for disrupting power systems.

Cyberattackers will change their strategies and develop new tools, meaning risk analysis and planning must continuously evolve and adapt to match this. NREL's cyber range allows researchers to anticipate, prepare for, and adapt to changing conditions and power system threats, including natural events, such as extreme weather, wildfires, or solar events; technological factors, such as system or component failures and aging infrastructure; and human-caused disruptions, including accidents, physical attacks, and cyberattacks.

Advanced Research Capabilities

Hardware-in-the-loop: NREL's cyber range integrates a variety of energy devices at the Energy Systems Integration Facility (ESIF)—including electric vehicles, connected buildings, batteries, and utility distribution components—and connects remotely to the 305-acre Flatirons Campus, where NREL houses wind turbines, solar arrays, megawatt-scale battery systems, and power grid infrastructure.

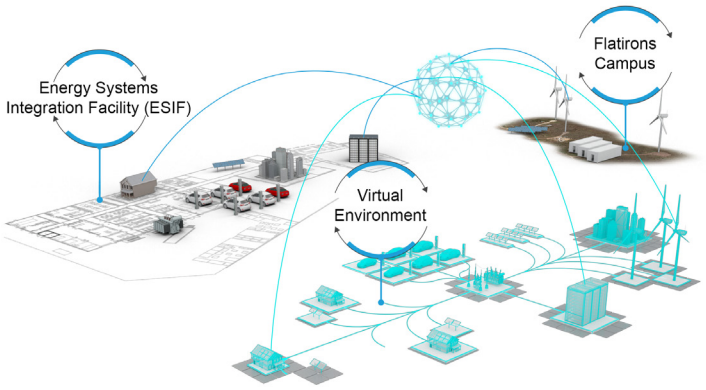
At-scale simulation: With connection to up to 20 MW of energy systems hardware, the cyber range provides one of the most advanced simulation environments for evaluating emerging threats, natural hazards, and the impacts of energy disruption.

Emulation: Real systems can be emulated by designing a digital twin of energy assets, connections, and communications, all within a state-of-the-art, scalable platform that supports the fast deployment of high-fidelity system models. Virtualization, container orchestration, and software-defined networking are just a few of the techniques that enable this capability.

Visualization: Interactive visualizations deliver real-time intelligence about data for a given scenario. Presentations can be projected onto a large-format video wall for picturing data in 3D and for capturing experiments at a glance to understand dynamic, system-level interactions.

System-Level Security

The cyber range is part of a larger NREL-developed platform called Advanced Research on Integrated Energy Systems (ARIES). ARIES brings together the physical devices at the ESIF with the utility-scale hardware at NREL's Flatirons Campus in the emulated world of the cyber range, allowing for hardware-, controller-, and human-in-the-loop studies. This capability helps close the system-level security gaps that emerge from distinct hardware and software becoming integrated, reducing overall vulnerabilities in energy systems that are evolving.



Research Applications

NREL is establishing a niche in cybersecurity research for renewable energy systems with tools like the cyber range to stay ahead of emerging threats. With the ability to emulate an unlimited number of digital clones, researchers can build virtual grids connecting to potentially thousands of devices on-site. The emulations support proactive defense and automated response, improved situational awareness, and telecommunications innovation.

The cyber range delivers market impact by helping researchers develop secure approaches for new grid technologies earlier in the design phase so that cybersecurity becomes a more integral part of our overall energy system.

Clean Energy Cybersecurity Accelerator

Cyber technology companies come to NREL to develop new products using the collective expertise and guidance of public and private sector advisors. Their novel solutions are validated on the cyber range to accelerate market readiness and deployment. Operating in cycles from 3 to 12 months, the accelerator is designed to outpace the speed of emerging threats.

5G and Advanced Communications

5G technologies can mitigate cyberattacks in ways that couldn't be done before. For example, a network architecture evaluation by NREL serves as a proof of concept that network slicing can be used in grid monitoring and controls to rapidly respond to an attack and maintain critical functions and services. The cyber range is being leveraged to explore future applications.

Electric Vehicle Charging Stations

Employing NREL's hardware-in-the-loop simulation capabilities, researchers evaluated a 50-kW fast-charge station under scenarios that could result in high-consequence attacks to the power grid from the integration of fast-charging stations. The cyber range can explore attackers' strategies within the communications infrastructure and evaluate potential response mechanisms.

Types of questions the cyber range can answer:

- **How will a new technology change the cybersecurity of an energy system?**
- **Can I secure this system against the latest known vulnerabilities?**
- **How will a network redesign or patch installation affect the system?**
- **What system-level security gaps will arise in the near future?**
- **Are my system defenses capable of responding to and recovering rapidly from disruptions?**

Want to learn more?

Get in touch by contacting us at:
NREL.Cybersecurity.Program.Office@nrel.gov

NREL Transforming ENERGY

National Renewable Energy Laboratory
15013 Denver West Parkway, Golden, CO 80401
303-275-3000 • www.nrel.gov

NREL prints on paper that contains recycled content.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency and Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

NREL/FS-5R00-81619 • January 2021