NREL
Transforming ENERGY

Cybersecurity for the Future Electric Grid

At the Energy Systems Integration Facility, NREL analysts can visualize a virtual grid environment with connections to both emulated and real physical devices in the facility and at NREL's Flatirons Campus.

The U.S. energy grid is transforming.

With the introduction of smart devices and rise in distributed, networked energy systems, diligent focus on cybersecurity for an evolving grid is crucial.

The grid that we know today was designed for one-way, centralized power systems—and before utilities, grid operators, and customers could predict the potential for today's cyber vulnerabilities. Market trends show that we are moving to a more decentralized energy infrastructure, with growing levels of residential solar generation and other distributed energy resources.

As connectivity and distributed energy levels increase, so does the number of access points for potential cyber threats. With legacy systems that were not designed to protect against cyber vulnerabilities, the approach to securing the electric grid must change.

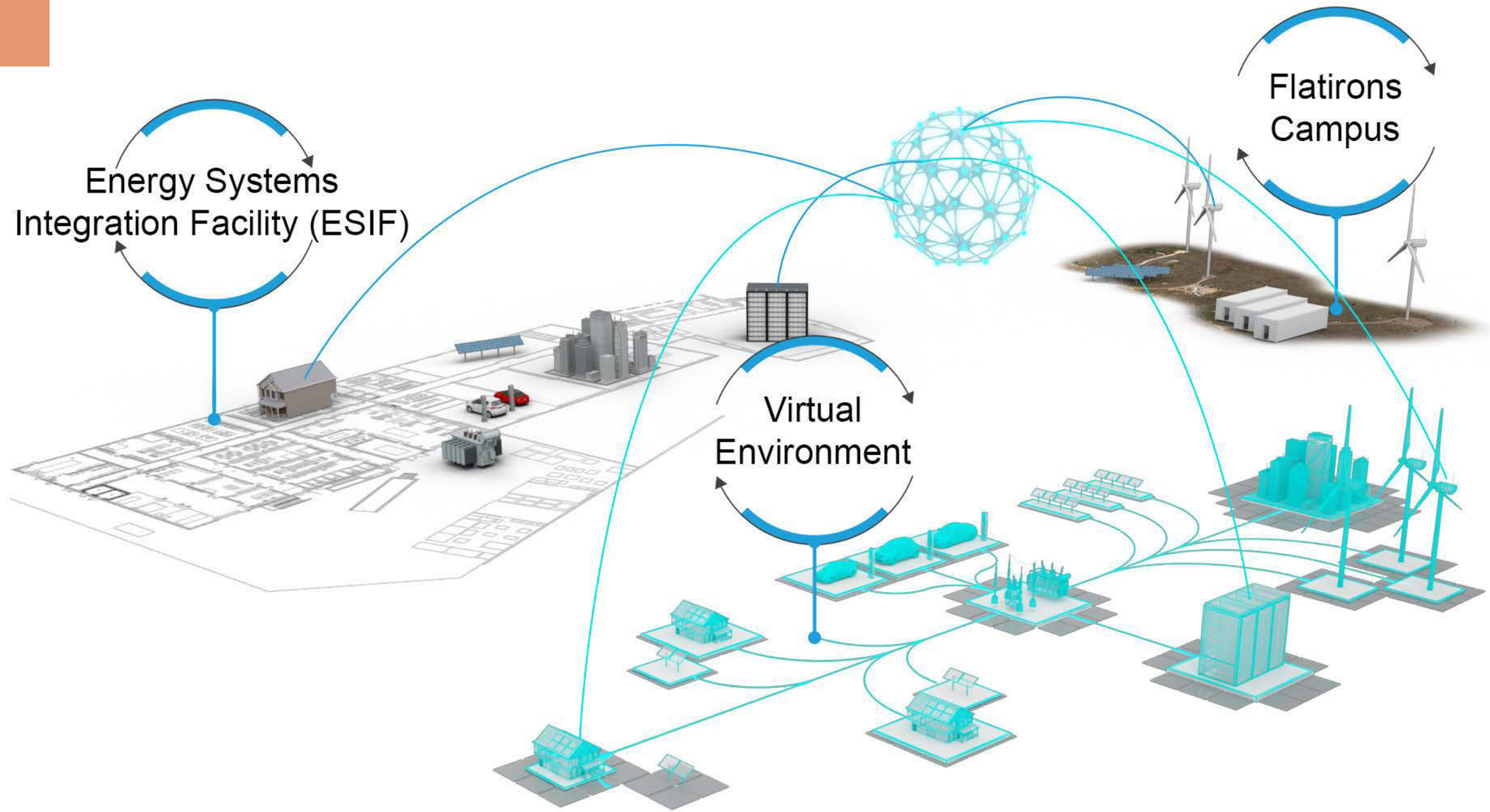
Unique Energy Systems Security Capabilities

The National Renewable Energy Laboratory (NREL) offers the ideal balance of expertise and infrastructure for cutting-edge research on cybersecurity and the future grid.

With one of the largest cadres of power systems researchers in the nation, NREL's expertise is growing with a cybersecurity team that's integrated with our research in distributed systems and emerging grid-tied technologies. The lab's 185,000 square-foot Energy Systems Integration Facility (ESIF) offers megawatt-scale power-hardware-in-the-loop simulation capabilities, high-performance computing and 3-D visualization, and integrated cybersecurity architectures.

Combined with the ability to remotely connect the ESIF to NREL's 305-acre Flatirons Campus—which offers utility-scale solar, wind, and storage research capabilities—researchers are performing distributed- and transmission-level cybersecurity evaluations across one large-scale, integrated testbed.

This unique infrastructure supports an emulated, multilayer grid environment, where analysts can assess the interdependencies between power systems and communications flows when cyber and physical threats occur. By evaluating the responses of interdependent and interconnected energy components in the emulated environment, NREL and industry partners can better understand how to improve the security, resilience, and blackstart recovery of today's critical energy infrastructure.



Cybersecurity R&D

Researchers at NREL are looking ahead to develop intrinsic security design principles for the future grid—one that can operate autonomously, with modern grid technologies to support high penetrations of wind, solar, and other distributed energy resources.

With a focus on understanding both human and natural threats to the grid, NREL's power systems engineers and cybersecurity researchers are working to mitigate threats to today's energy infrastructure and provide a pathway to a more secure and resilient future grid.

Projects at a Glance

Power and Communications Systems Emulation

Analysts are performing threat and consequence analysis in an emulated, multilayer grid environment at the ESIF, linking the multi-lab developed Hierarchical Engine for Large-scale Infrastructure Co-Simulation (HELICS) and Sandia National Laboratories' SCEPTRE platforms. This capability allows researchers to visualize and evaluate the interdependencies of power systems and network communication flows—and safely explore vulnerabilities and mitigation effectiveness.

Encryption for Distributed Energy

In collaboration with Sandia National Laboratories, the Public Service Company of New Mexico, and Yaskawa Solectria Solar, NREL is developing a low-cost module that provides optimized encryption for distributed energy resources and their operational technology networks. The module, called Module-OT, will help protect command-and-control messages over communications channels.

A New Framework for Cybersecurity

Built upon previous cybersecurity frameworks and with NREL's expertise in distributed energy systems, NREL is developing the Distributed Energy Resources Cybersecurity Framework (DERCF) to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems. The new framework will inform policies and controls for cyber governance, cyber-physical technical management, and physical security of distributed energy technologies at federal sites across the country.

Work with Us

Learn more about what we're doing to secure the future energy grid—and how to partner with our team of cybersecurity analysts at the ESIF. See www.nrel.gov/security-resilience

Contact

Jonathan White, NREL Cyber-Physical Security Group Manager, Energy Security and Resilience Center

Jonathan.White@nrel.gov | 303-384-7433

NREL

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/BR-5R00-73906 • May 2019