Department of Defense Information Analysis Centers Webinar

Wednesday, April 15, 1200-1300 EDT

Power and Communication Systems Emulation

Presented by: Dr. Dan Bennett, Ph.D., Colonel, US Army (Retired)

National Renewable Energy Laboratory

Defense Systems Information Analysis Center

Cyber Security and Information Systems Information Analysis Center

Homeland Defense and Security Information Analysis Center

HDIAC, CSIAC, and DSIAC are sponsored by the Defense Technical Information Center (DTIC). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Technical Information Center.

NREL's Energy Security & Resilience Center

Colonel (Retired) Dan Bennett, Ph.D.
Senior Technical Advisor

Department of Defense Information Analysis Centers Webinar
April 15, 2020

Agenda

NREL’s Mission and the Grid of the Future

Critical Infrastructure Threats

Secure Cyber-Energy Systems Portfolio

4 Questions

NREL’s Mission and the Grid of the Future

Energy systems across the globe are changing.

NREL is advancing those future systems—and ensuring the safety, reliability, security, and resilience of those systems.

Grid security and reliability must keep pace

To manage, optimize, and secure the future grid, new technologies and control techniques will be required that don't currently exist.

NREL at a Glance

2,307

Employees,

plus more than

460

early-career researchers and visiting scientists

World-class

facilities, renowned technology experts

about 900

Partnerships

with industry, academia, and government

Campus

operates as a living laboratory

```
INFO: Network interface added:
10.0.0.204
INFO: Network interface added:
10.0.0.202
INFO: Network interface added:
10.0.0.203
ALERT: ET SCAN Potential SSH
Scan OUTBOUND
ALERT: ET SCAN Potential SSH
Scan OUTBOUND
ALERT: ET SCAN Potential SSH
Scan OUTBOUND
```

Transforming Energy through Science

NREL advances the science and engineering of **energy efficiency**, **sustainable transportation**, and **renewable power technologies** and provides the knowledge to **integrate and optimize energy systems.**

The integration and optimization of energy systems must account for vulnerabilities of technologies, systems, and operations, as well as costs associated with desired levels of security and resilience.

NREL’s Science Drives Innovation

Renewable Power

Solar

Wind

Water

Geothermal

Sustainable Transportation

Bioenergy

Vehicle Technologies

Hydrogen

Energy Efficiency

Buildings

Advanced Manufacturing

Government Energy Management

Energy Systems Integration

High-Performance Computing

Data and Visualizations

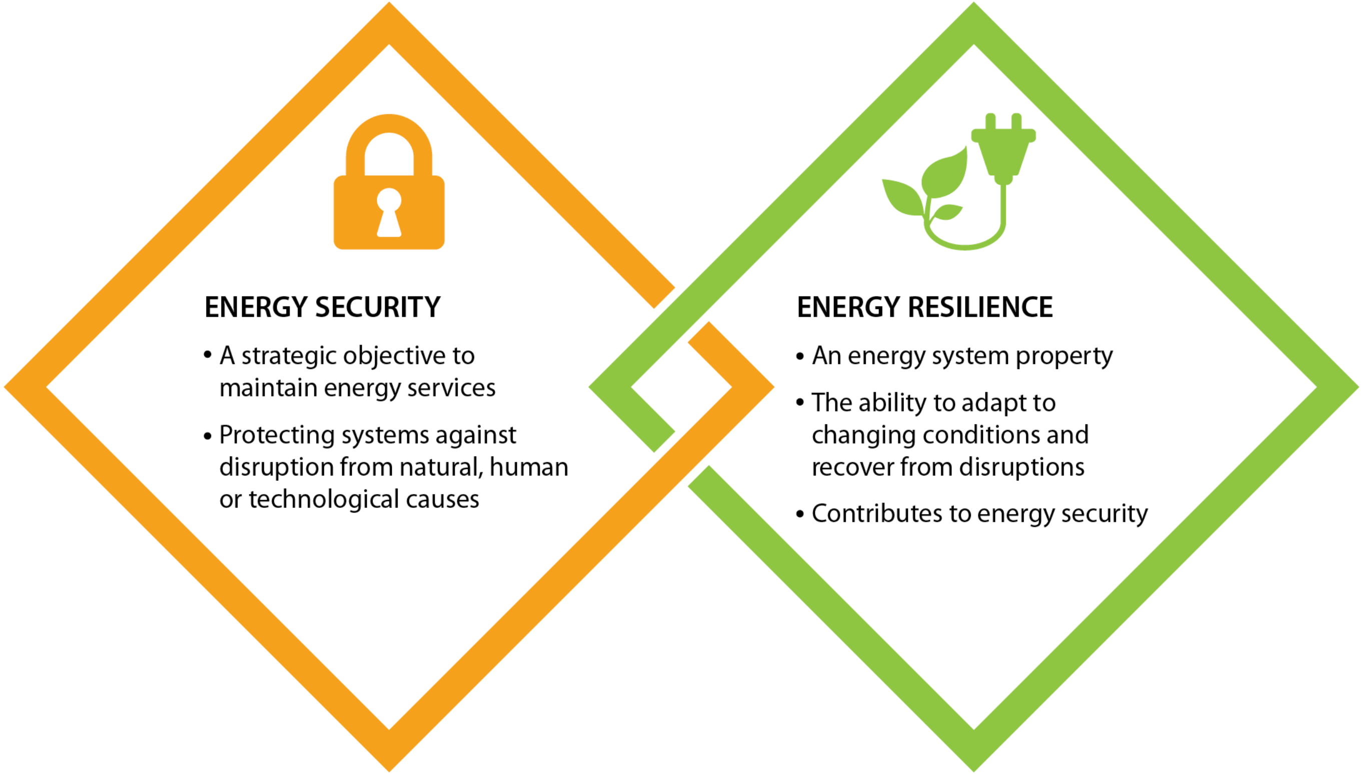
Cybersecurity

NREL's Energy Security & Resilience Program

The Energy Security & Resilience (ESR) program seeks to:

- Improve the current understanding of potential energy service disruption and their consequences
- Improve energy security under different scenarios, by continuing to provide energy services protecting energy systems from when human or natural disruptions occur
- Develop more resilient energy systems.

Energy Security & Resilience



ENERGY SECURITY

- A strategic objective to maintain energy services
- Protecting systems against disruption from natural, human or technological causes

ENERGY RESILIENCE

- An energy system property
- The ability to adapt to changing conditions and recover from disruptions
- Contributes to energy security

NREL Mission

NREL advances the science and engineering of energy efficiency, sustainable transportation, and renewable power technologies and provides the knowledge to integrate and optimize energy systems.

Research Capabilities

200+ power systems engineering and renewable generation **experts**

World-Class Operations

World-class electric grid research **facilities**

Record-setting models, maps, data sets, and **tools** for advanced grid analysis

Megatrends Driving Energy Security & Resilience Research

Electrification & Distributed Energy

Cyber threats

Cyber-Physical Systems Security

Vulnerability Analysis

Multilayer energy systems emulation and scenario analysis

Utility cybergovernance assessments

Mitigation Modeling

Cyber threat mitigation R&D

Modular encryption for distributed energy devices

Situational Awareness

Real threat identification and visualization

Consequence analysis of combined energy and communications systems

Stakeholder Engagement

Standards development for cybersecurity and renewable energy

New tools for cyber assessments and distributed energy systems

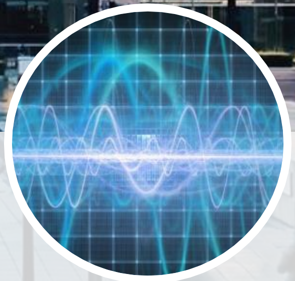
Critical Infrastructure Threats

Sources of Energy System Disruption

Natural Disasters

Space Weather

Physical Threats



Electromagnetic Pulse

Cyber Threats

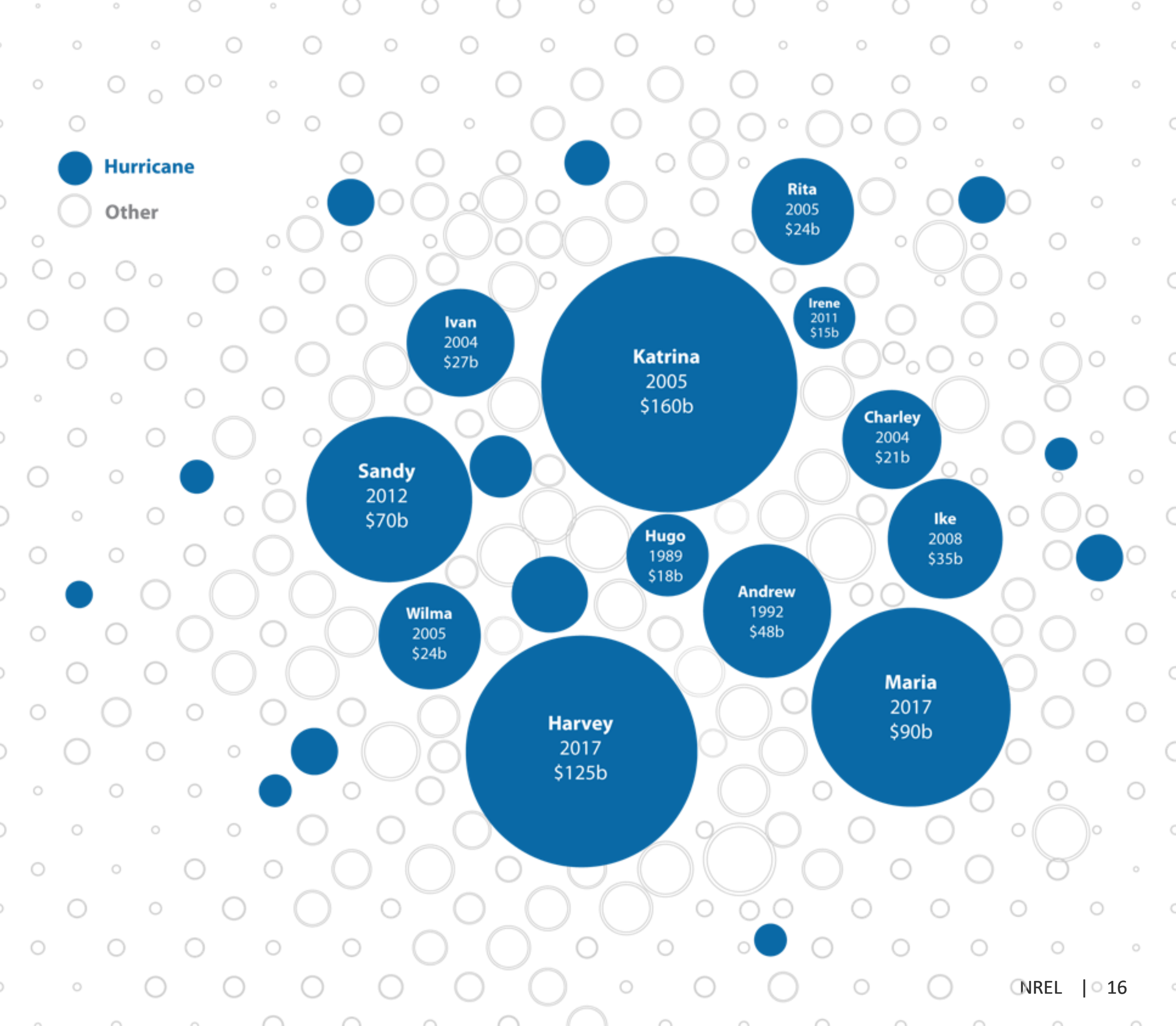
Natural Threats

Human Threats

Natural Disasters

Severe weather and other natural disasters can interrupt energy systems from multiple entry points, leading to cascading impacts on power systems, water systems, transportation systems, and businesses.

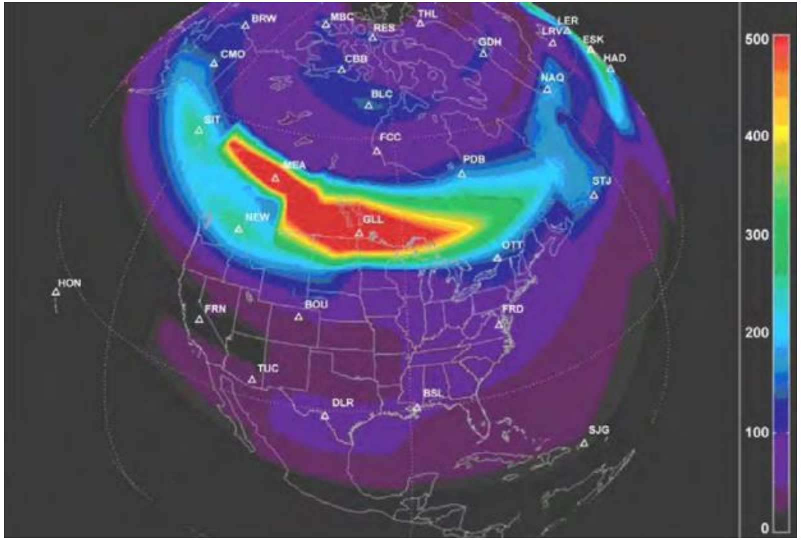
Billions of dollars are lost each year in the United States from power outages that cause interruptions to businesses, government, and infrastructure.



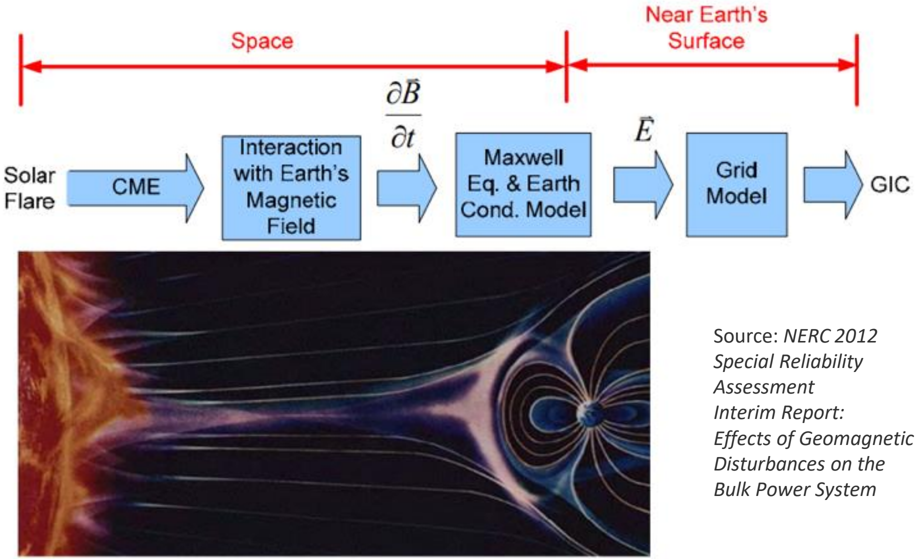
Source: *FiveThirtyEight*

Space Weather

Geomagnetic storms caused by solar coronal mass ejections can impact electric grid operations through strong induced currents.



Geomagnetic intensity, 1989 Hydro-Quebec Solar Storm


Space
Near Earth's Surface
Solar Flare
CME
Interaction with Earth's Magnetic Field
$\frac{\partial \vec{B}}{\partial t}$
Maxwell Eq. & Earth Cond. Model
$\vec{E}$
Grid Model
GIC

Source: *NERC 2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System*

Storm interaction with Earth and transmission lines

Risks from Geomagnetic Disturbance

- Damage to bulk power system assets, typically associated with transformers
- Loss of reactive power support, which could lead to voltage instability and power system collapse.

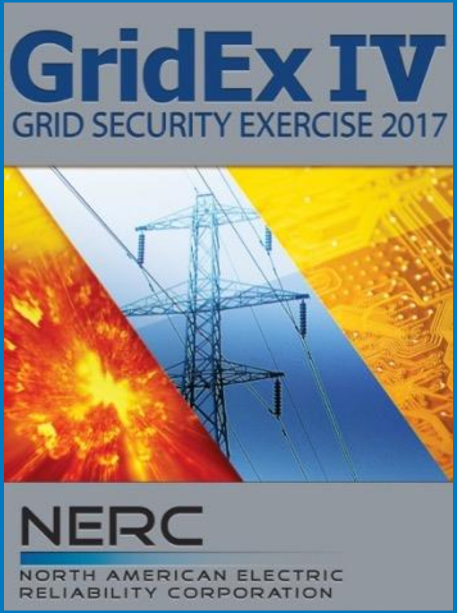
March 1989 Hydro-Quebec Solar Storm

- 9-hour outage
- 6 million people affected

Physical Threats

Physical threats to the power grid include component and system failures, dated infrastructure, human error, and deliberate attack.

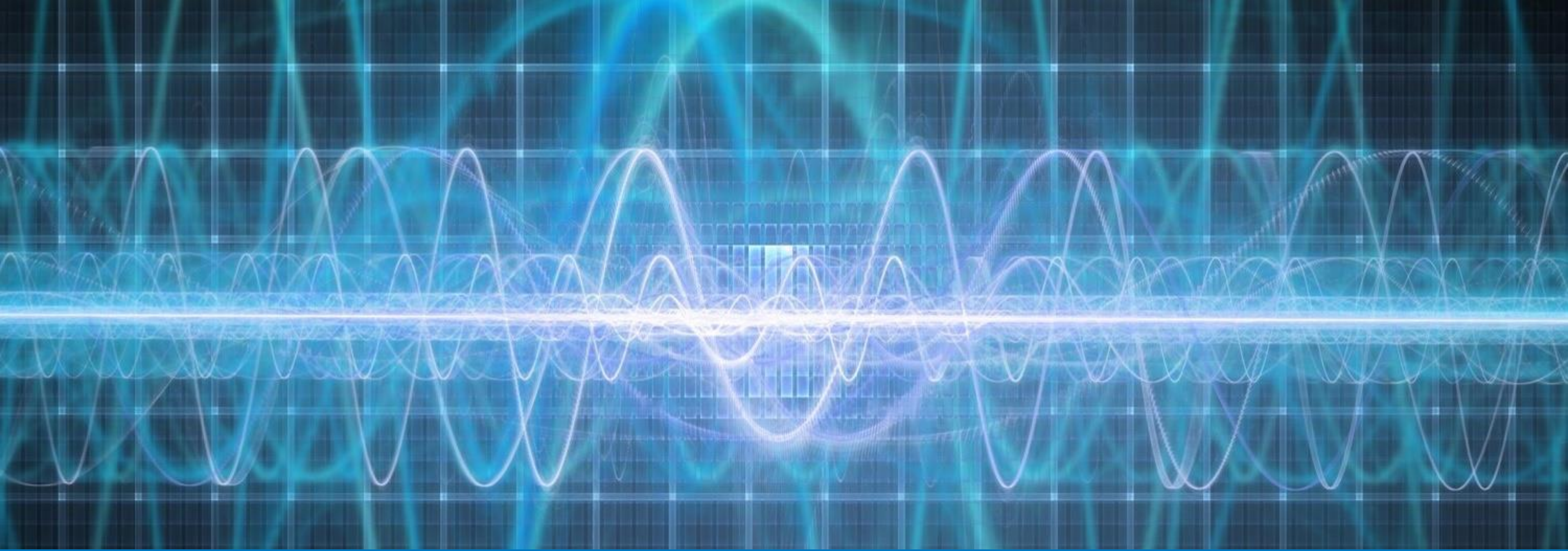
National Exercises Focus on Combined Cyber-Physical Attacks



GridEx is a biennial exercise designed to exercise national level response to a cyber/physical attack on the North American power grid and other critical infrastructures.

GridEx involves:

- Electric utilities
- Regional (local, state, provincial) and federal government agencies in law enforcement, first response, and intelligence community functions
- Critical infrastructure cross-sector partners (ISACs and other utilities)
- Supply chain stakeholder organizations

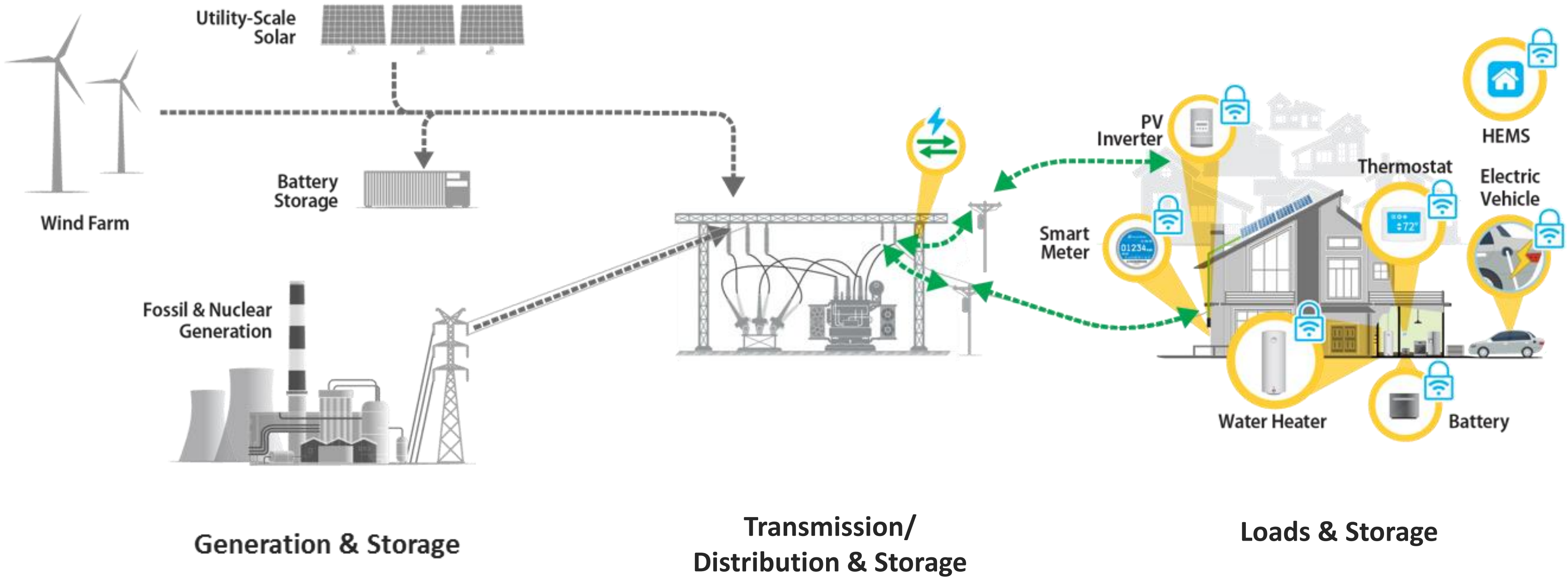


Electromagnetic Pulse (EMP)

EMP attacks can be caused by high-altitude nuclear explosions—and have the potential to interrupt all electrical services.

Cyber Threats

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.



Cost-competitive renewables are making up a larger share of the energy mix. The **grid edge** is transforming into a dynamic space where **networked, distributed energy generated,** stored, managed, and traded**.**

Cybersecurity for the Electric Sector: A growing need

- Advances in energy and information technologies are changing the way energy is produced, delivered, and used.
- Such advances could offer great benefits (choice, cost savings, business opportunities, etc.), but the vulnerabilities of these emerging energy systems are not yet well understood.
- Energy systems have always been subject to disruptions:
  - Accidents, component failures, natural disasters, human actions.
- Global trends are showing a growing reliance on energy-consuming technologies, intensifying weather events, and greater potential for large-scale cyberattacks.
- Energy systems are becoming more distributed and dependent on communications networks.

It is crucial to ensure the security and resilience of emerging energy systems for an evolving grid.

Secure Cyber-Energy Systems Select Initiatives

Event Log
INFO: Network interface added 10.0.0.204
INFO: Network interface added 10.0.0.202
INFO: Network interface added 10.0.0.203
ALERT: ET SCAN Potential SSH Scan OUTBOUND
ALERT: ET SCAN Potential SSH Scan OUTBOUND
ALERT: ET SCAN Potential SSH Scan OUTBOUND

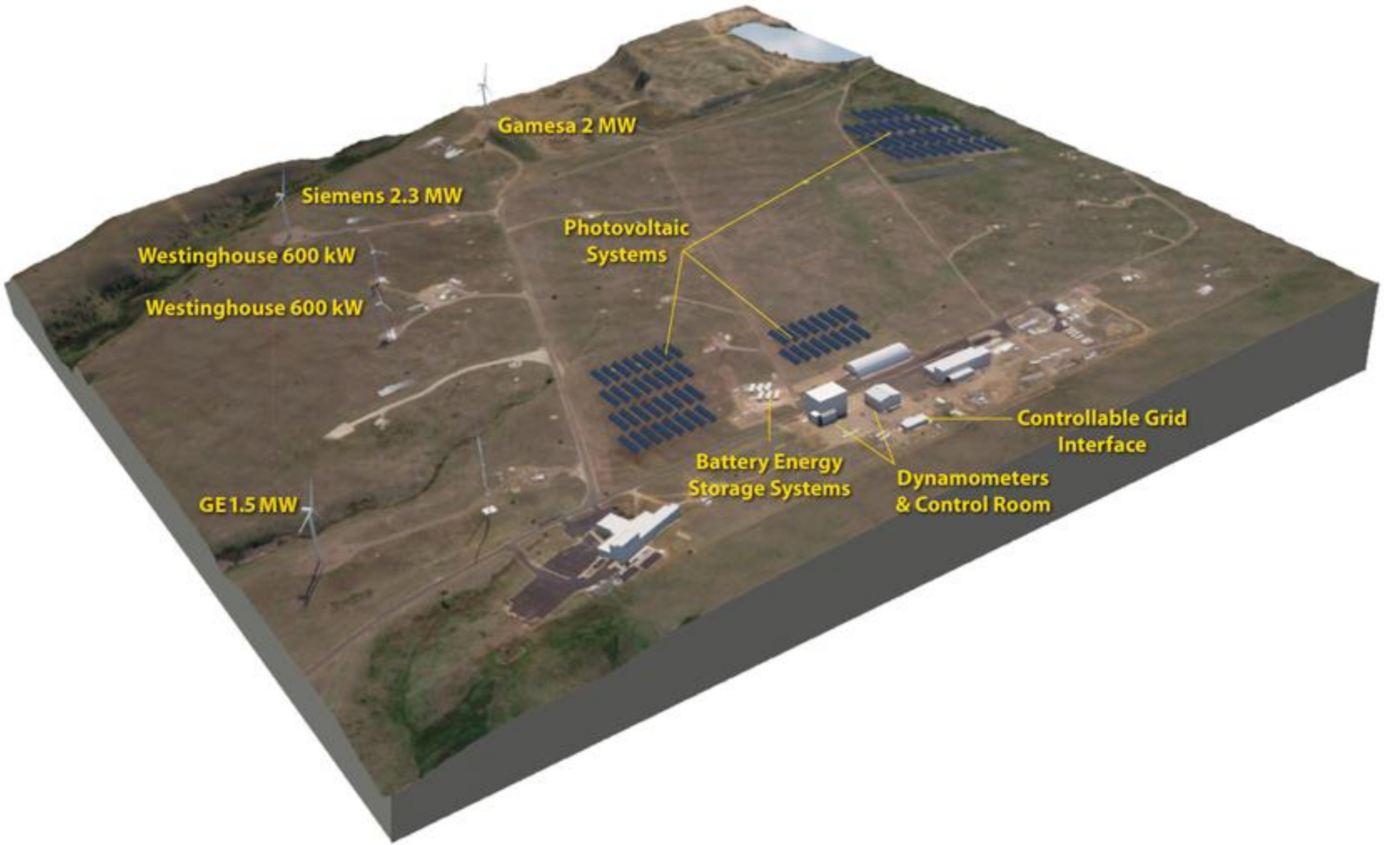
Secure Cyber-Energy Systems (SCyES)

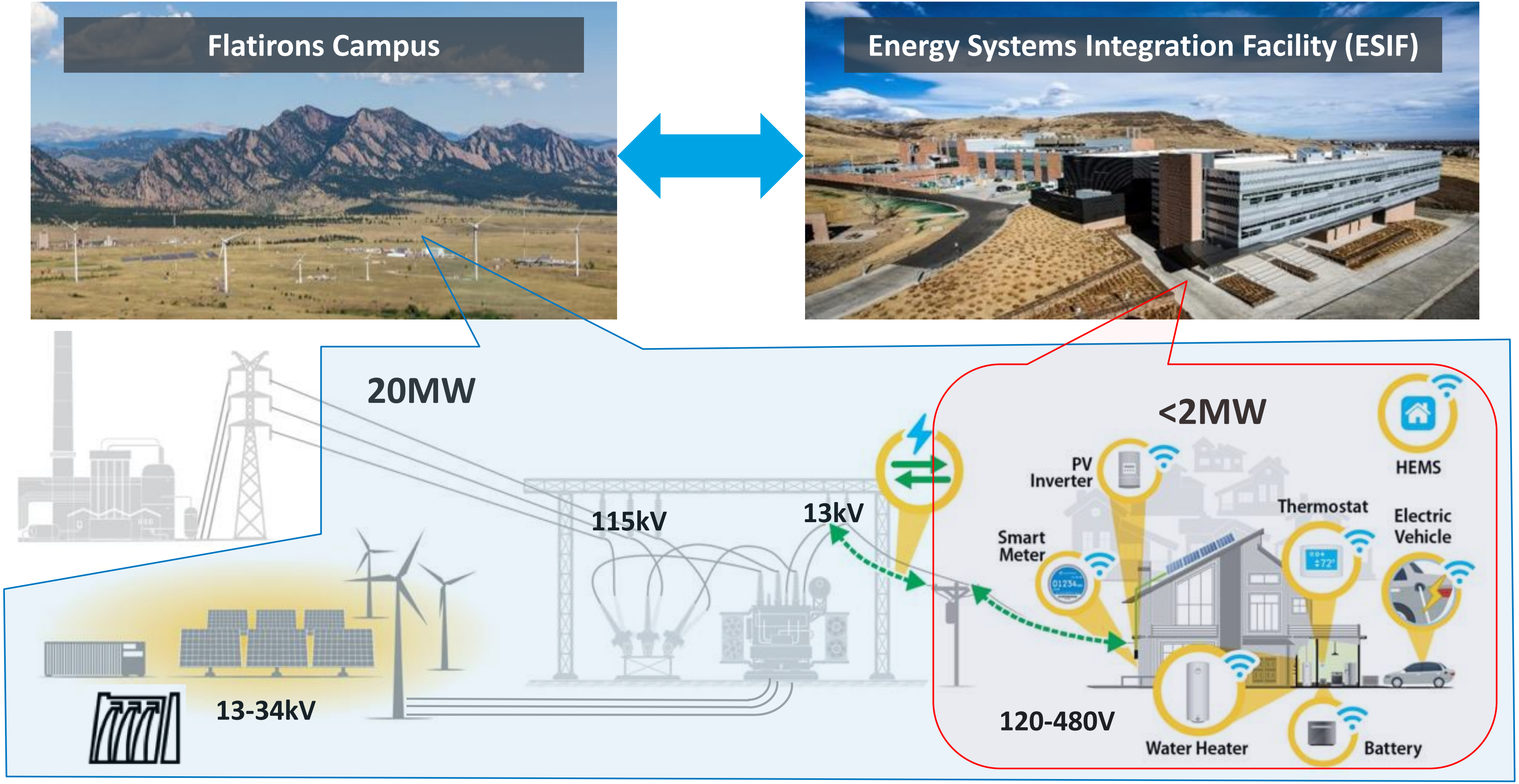
- The electric grid we rely on today was designed before utilities, grid operators, and customers considered cybersecurity as a potential threat to critical infrastructure.
- This is has led to a patching culture that can’t keep pace with the growth in cyber-related vulnerabilities.
- NREL is anticipating a future intelligent, distributed grid, exploring its performance to develop intrinsic security design principles—a grid that can operate autonomously, where millions of grid devices can automatically detect and respond to threats.

NREL’s Energy Systems Integration Facility

- Megawatt-scale power hardware-in-the-loop (PHIL) simulation
- Interconnectivity to external field sites
- Virtual utility operations center
- Research evaluation platform for smart grid communications and control
- Parallel alternating current and direct current power buses
- High-performance computing platform with petabyte-scale throughput
- Visualization environments to unveil engineering opportunities

Connection to NREL’s Flatirons Campus

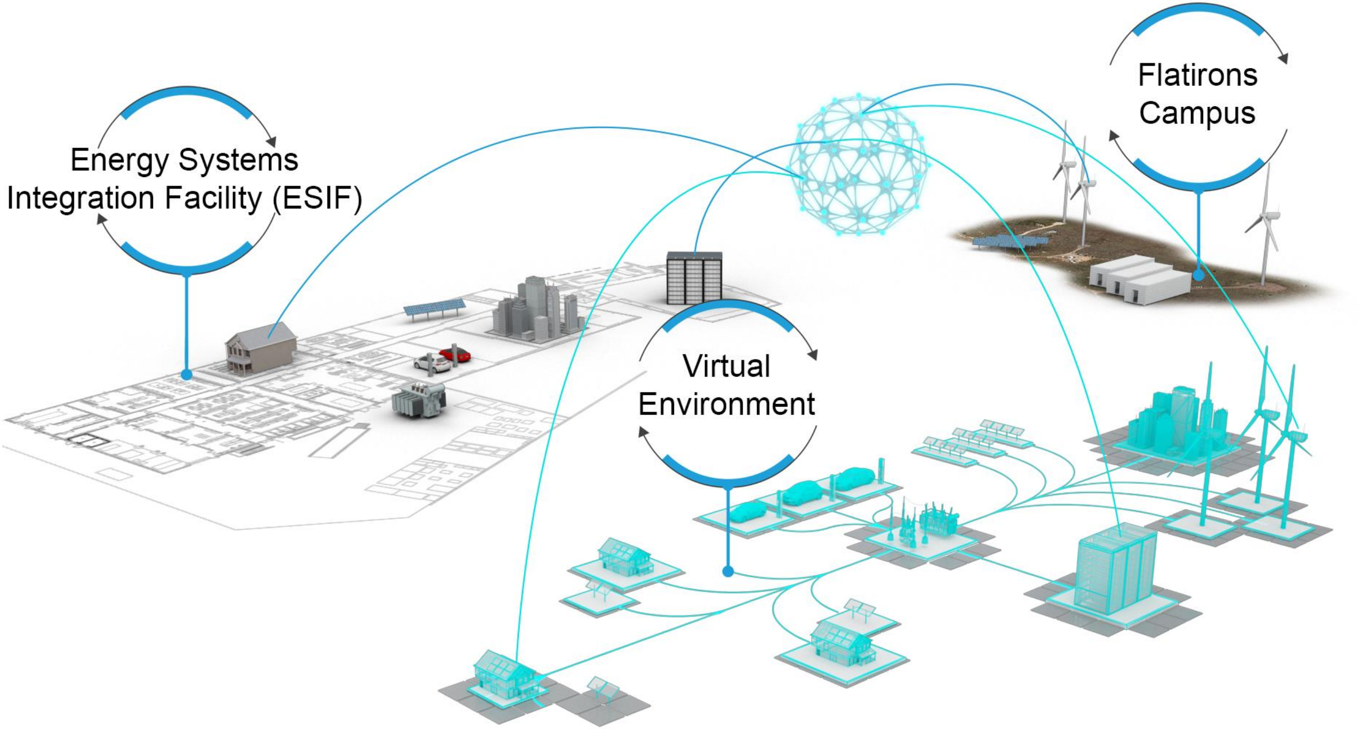




Bulk Generation, Storage, and MD/HD Mobility

Transmission/ Distribution & Storage

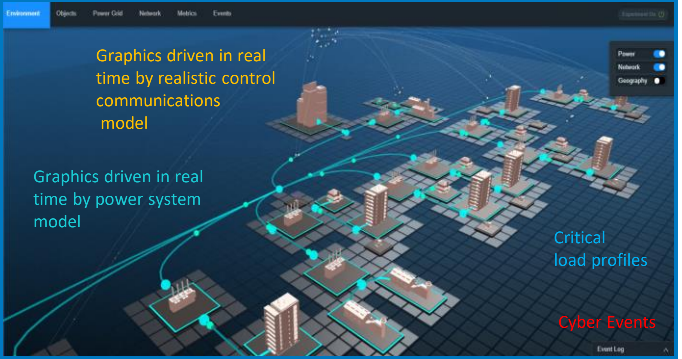
Distributed Generation, Storage, Loads, and LD Mobility



Cyber-Energy Emulation Platform (CEEP)

NREL's emulated, multilayer grid environment allows researchers to visualize and evaluate the interdependencies of power systems and network communication flows—and safely explore vulnerabilities and mitigation effectiveness.

Cyber-Energy Emulation Platform Capability & Applications


Environment
Objects
Power Grid
Network
Metrics
Events
Power
Network
Geography
Graphics driven in real time by realistic control communications model
Graphics driven in real time by power system model
Critical load profiles
Cyber Events
Event Log

Helps you to fully understand your infrastructure:

- Situational awareness
- Mapping
- Vulnerabilities
- Asset, change, patch, sensor management strategy
- Risk management, authority to operate processes.

Provides training, testing, exercising, and education:

- Attacking
- Defending
- Helping facilitate the integration/application of cloud, data science, machine learning, artificial intelligence capabilities to build efficiencies.

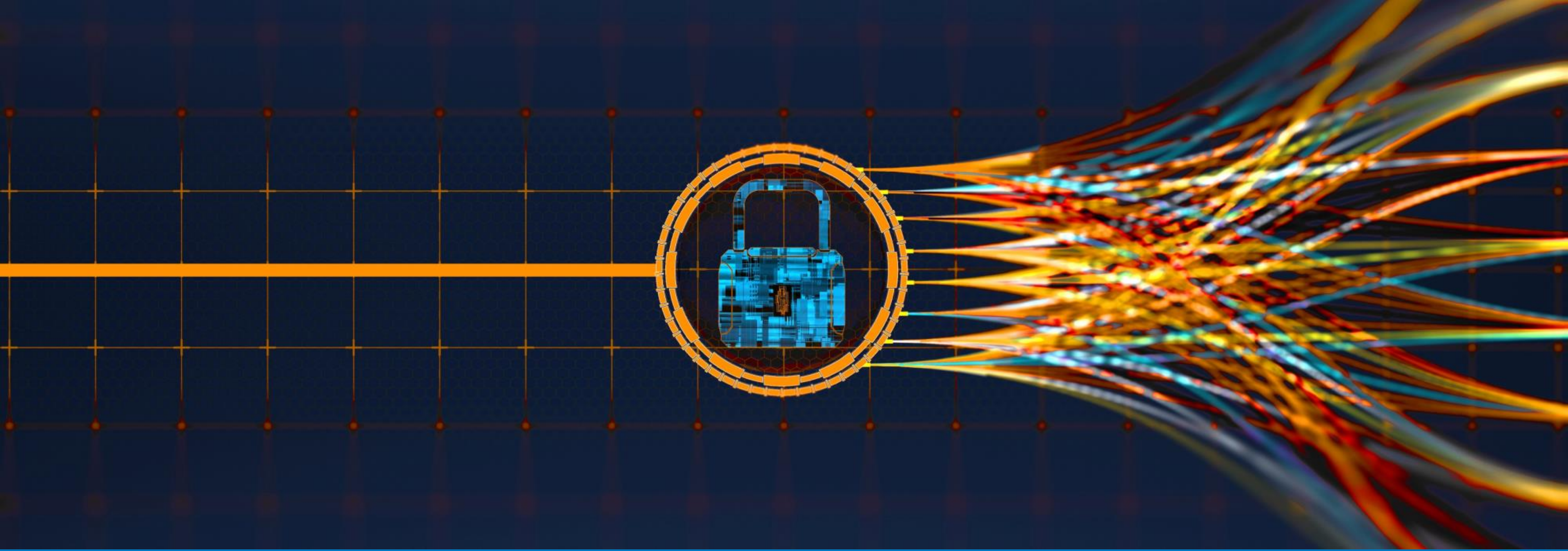
A tool to support resource prioritization for operations, planning, risk management, evaluation, training/exercising, and education.

Assessing PV Communications Systems Security Architecture

- NREL is providing technical expertise to Operant Solar to develop a combined WiFi and wireless mesh network gateway that connects distributed energy resources, such as residential solar sites, to the internet.
- NREL researchers will provide expert review of written security protocol and offer recommended test plans for the gateway once installed in the field.
- With NREL's technical expertise, Operant Solar will get ahead of security challenges for new networking approaches before they are deployed

Securing the Delivery of Command and Control Messages

- NREL is creating a Software Defined Network (SDN) test environment based on a blueprint and reference architecture that can be used for cyber experimentation.
- New cyber analytic algorithms will be created that integrate traditional NetFlow and new SDN information to provide enhanced situational awareness to energy delivery systems network operators.
- Uses a wide area network connection between NREL and PNNL to collect metrics.
- NREL is exploring the security objectives and potential benefits of SDN-enabled obfuscation and moving target defense for wide area communication.



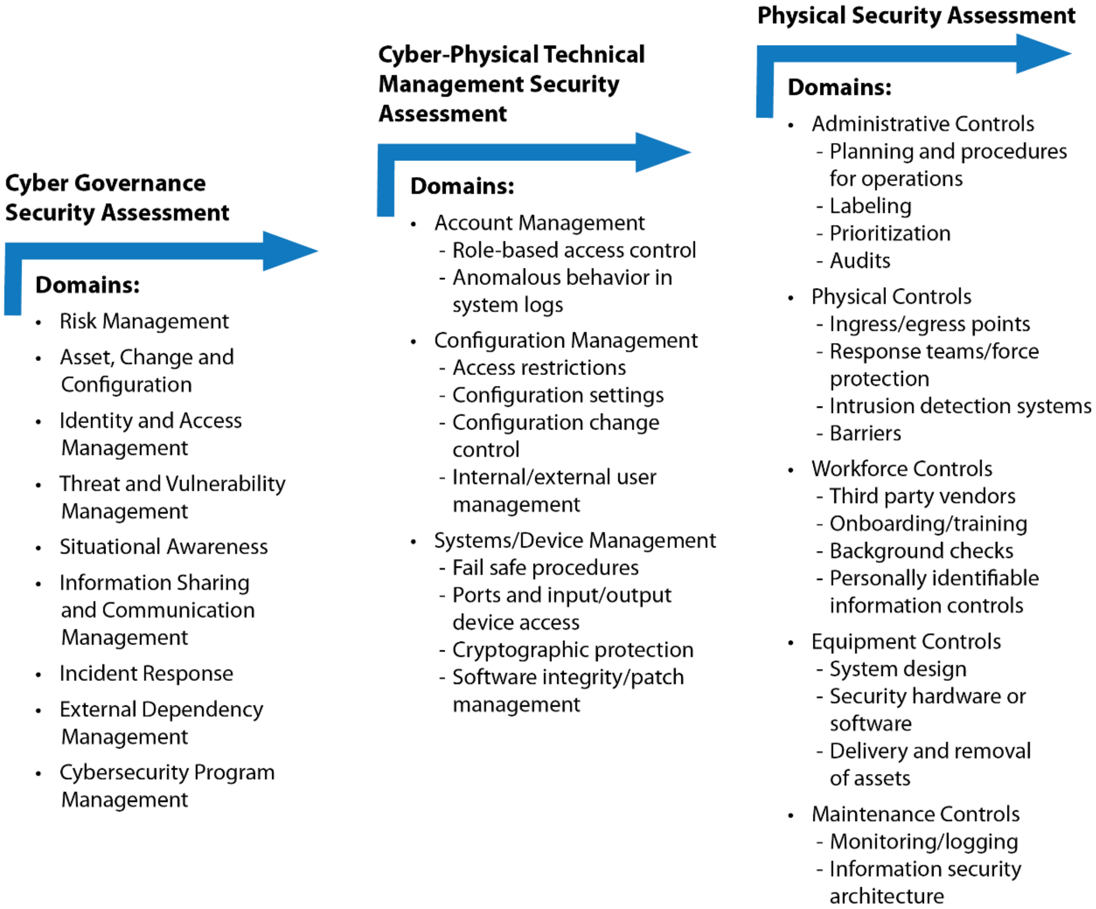
Distributed Energy Resources Cybersecurity Framework

NREL is developing the Distributed Energy Resources Cybersecurity Framework (DERCF) to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

Raising Cybersecurity Awareness

The DERCF 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.

Distributed Energy Resources Cybersecurity Framework



Cyber Governance Security Assessment

Domains:

- Risk Management
- Asset, Change and Configuration
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communication Management
- Incident Response
- External Dependency Management
- Cybersecurity Program Management

Cyber-Physical Technical Management Security Assessment

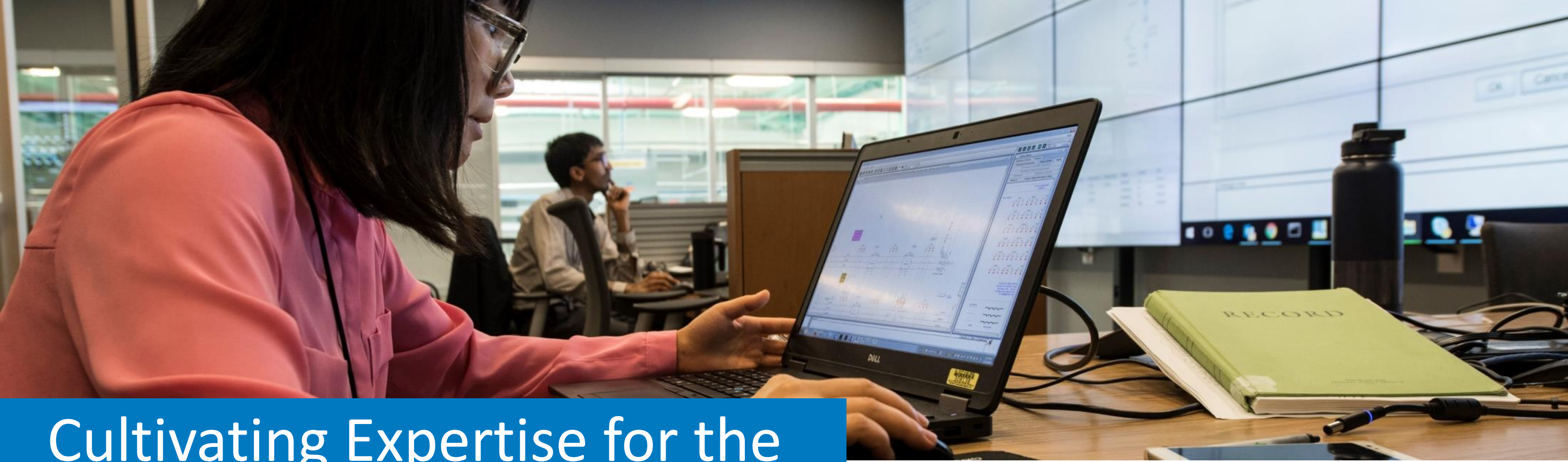
Domains:

- Account Management
  - Role-based access control
  - Anomalous behavior in system logs
- Configuration Management
  - Access restrictions
  - Configuration settings
  - Configuration change control
  - Internal/external user management
- Systems/Device Management
  - Fail safe procedures
  - Ports and input/output device access
  - Cryptographic protection
  - Software integrity/patch management

Physical Security Assessment

Domains:

- Administrative Controls
  - Planning and procedures for operations
  - Labeling
  - Prioritization
  - Audits
- Physical Controls
  - Ingress/egress points
  - Response teams/force protection
  - Intrusion detection systems
  - Barriers
- Workforce Controls
  - Third party vendors
  - Onboarding/training
  - Background checks
  - Personally identifiable information controls
- Equipment Controls
  - System design
  - Security hardware or software
  - Delivery and removal of assets
- Maintenance Controls
  - Monitoring/logging
  - Information security architecture

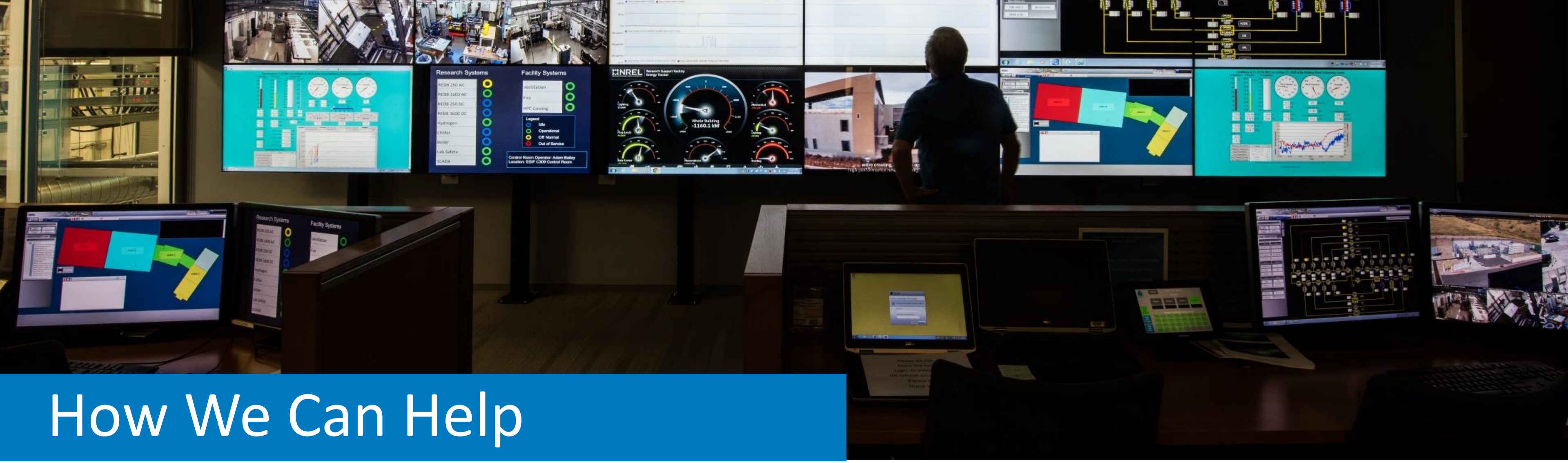


Cultivating Expertise for the Next Generation

- Energy system threat analysis
- Power systems engineering and operations
- Cyber-physical systems dynamics
- Cybersecurity for buildings, transportation, manufacturing, wind, water, solar power and electric grid applications
- Power systems engineering and operations

- Artificial intelligence, machine learning
- Intrusion detection, monitoring and event forensics
- Communications protocols and network architectures
- Complex adaptive system dynamics
- System analysts

- Urban planning analyst or resilience expert
- Behavioral scientists
- Economists
- Critical infrastructure experts
- Power systems engineering and operations



How We Can Help

NREL works to identify, anticipate, detect, protect against, and respond to today's biggest threats to the energy grid, primarily the renewable energy sector, offering a strong foundation of tools, expertise, and capabilities that support systems security and innovation, resilience science, and advanced visualization for decision support:

- Modeling and co-simulation (emulation)
- Cybersecurity evaluation
- Unique facilities
- Collaborations to advance resilience science.

Thank you

www.nrel.gov

NREL
Transforming ENERGY