NREL
NATIONAL RENEWABLE ENERGY LABORATORY





Grid Evolution & Attack Evolution

Maurice Martin
Senior Technology Lead, PSEC Security & Resilience
April 1, 2018

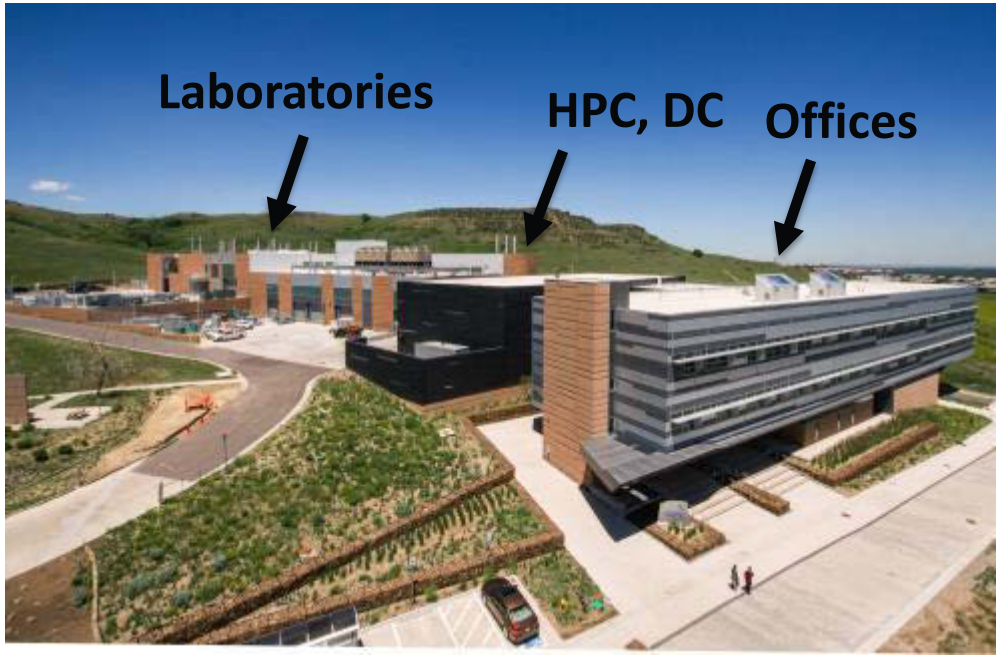
NREL/PR-5D00-71222

NREL—Golden, Colorado, Campus

NREL, 26954

Energy Systems Integration Facility

Energy Systems Integration Facility



NREL, 30433

Addressing the challenges of large-scale integration of clean energy technologies into the energy systems infrastructure

http://www.nrel.gov/esif/

- NREL's largest R&D facility (182,500 ft^2 /20,000 m^2)
- Space for approximately 200 NREL staff and research partners
- Petascale High-Performance Computer (HPC) and Data Center supports all research at NREL
- Labs focus on R&D of integrated energy systems:
  - Electricity
  - Fuels
  - Transportation
  - Buildings and campus.
- Integrated electrical, thermal, fuel, and data infrastructure.

NREL's Cybersecurity Research and Development Strategy

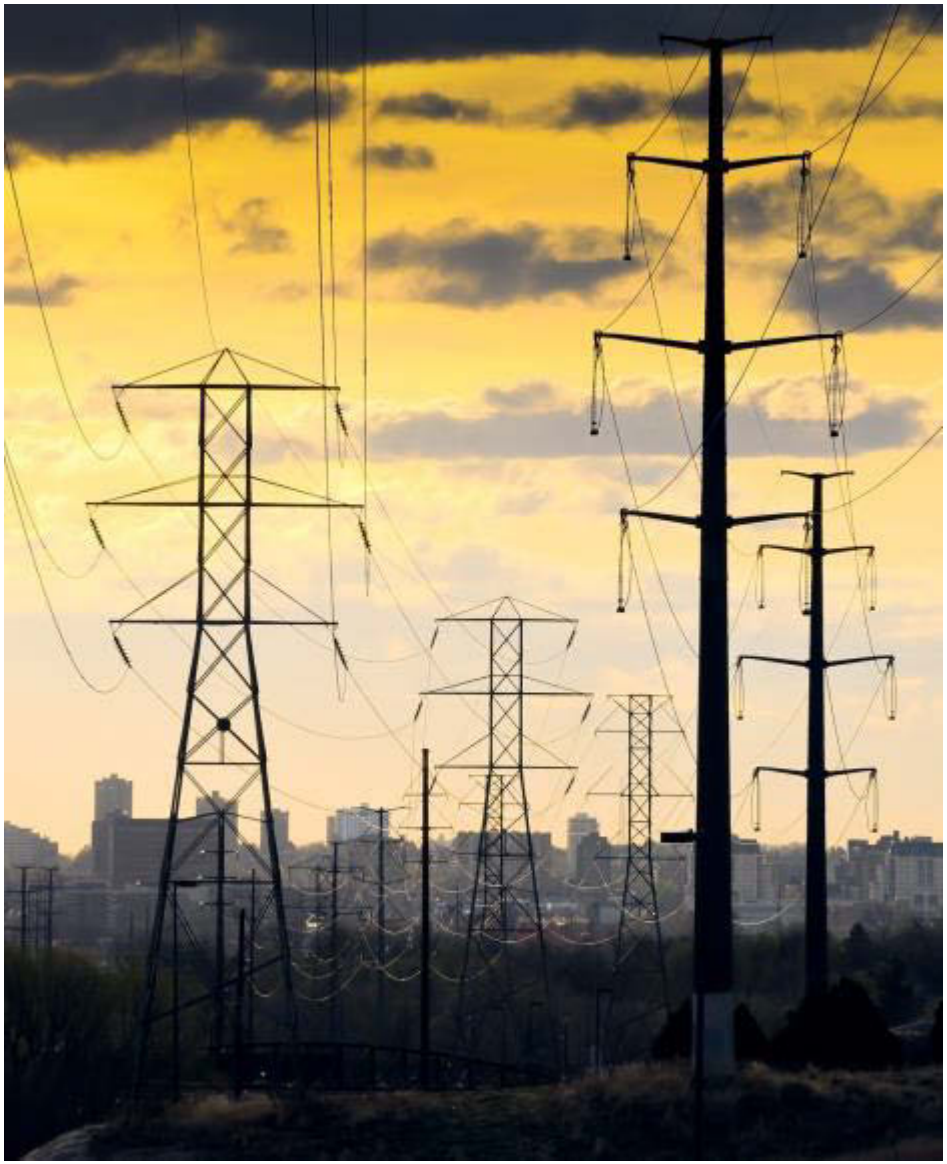
- Assist public and private sector clients in implementing the National Institute of Standards Technology's (NIST's) Cybersecurity Framework and the U.S. Department of Energy (DOE's) Cybersecurity Capability Maturity Model (C2M2) through strategic partnership projects (electric, water, oil and gas, and other sectors).

- Identify research-and-development (R&D) gaps in cybersecurity and resilience in the public and private sector via strategic partnerships.

- Inform DOE, NIST, the U.S. Department of Defense, Advanced Research Projects Agency-Energy (ARPA-E), state and local governments, and regulatory bodies of empirically verified cybersecurity and resilience R&D gaps identified via client engagements.

- Research the gaps through funded R&D projects in partnership with academia, industry, and other national laboratories.

Cyber-Challenge With Distributed Generation



NREL, 18979

CHALLENGE:

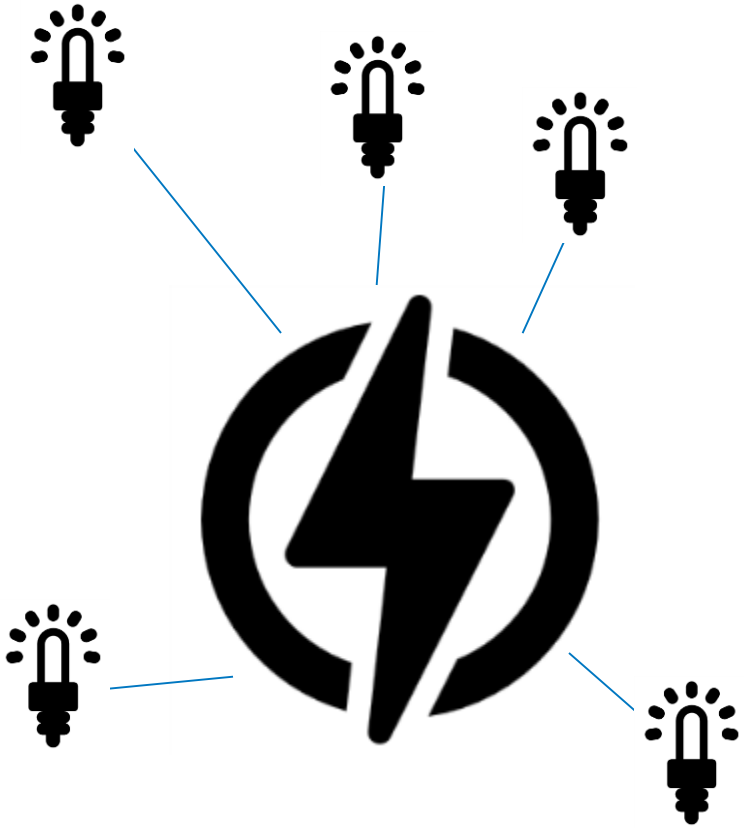
Distributed intelligence creates new cybersecurity vulnerabilities on the electric grid.

SOLUTION:

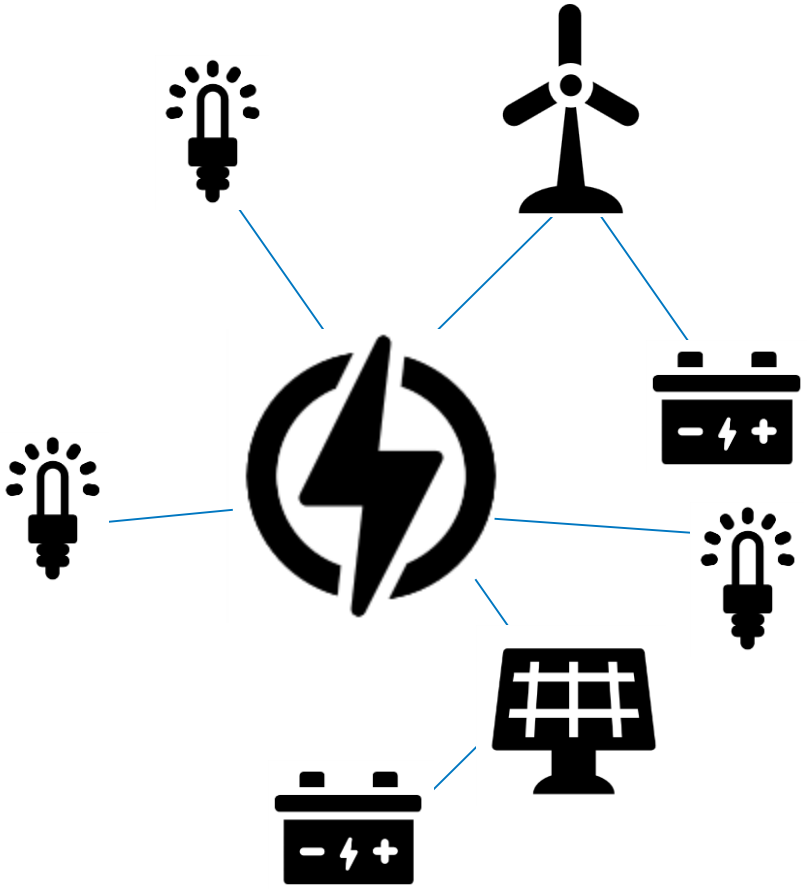
A new, disruptive approach to system security based on nine layers.

Evolution of the Grid

Past: A fortress



Present: A network

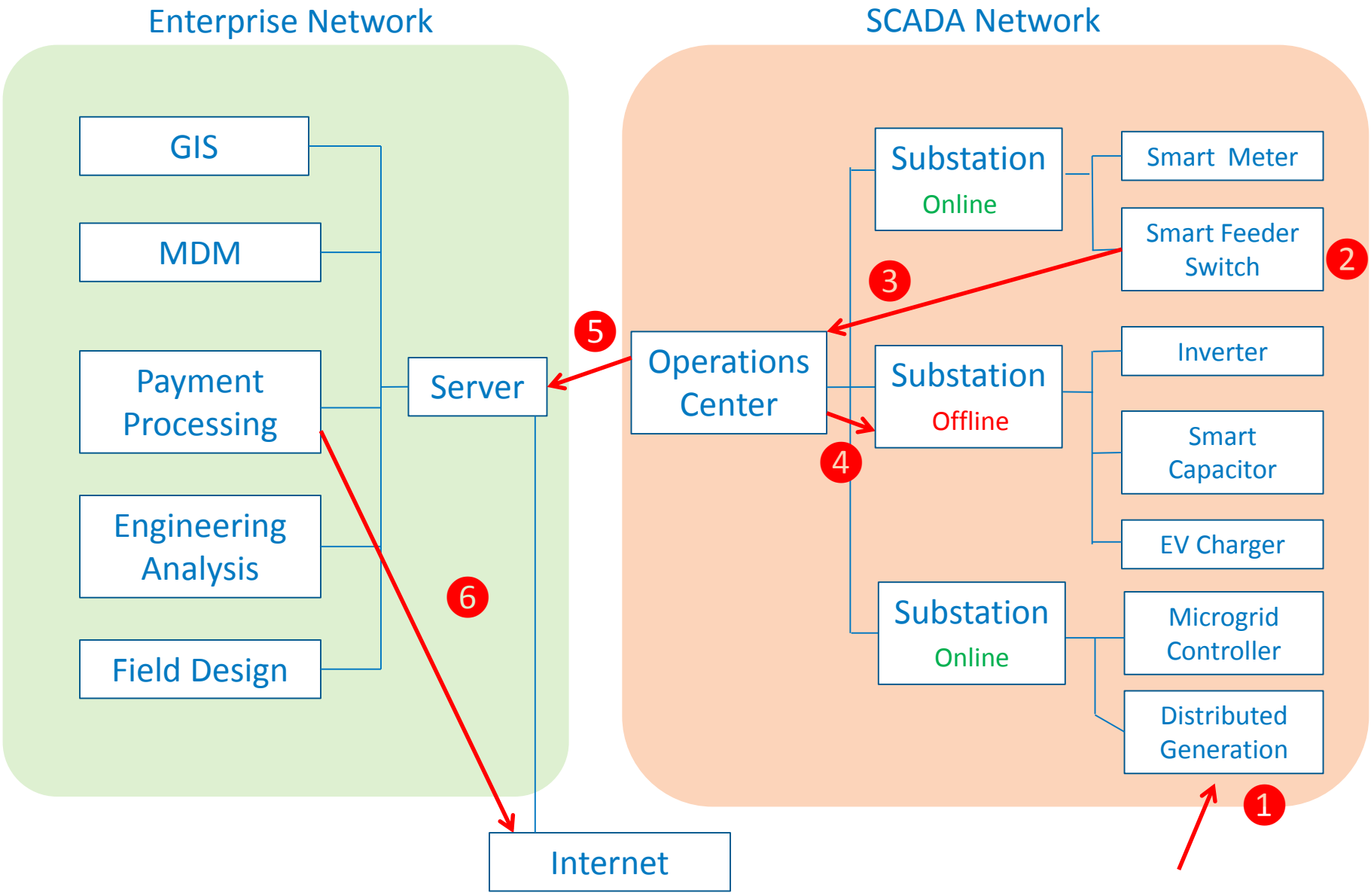


Utility Infrastructure: A Communications and Security Challenge

- Power generation SCADA
- Transmission energy management system (EMS)
- Distribution SCADA
- Advanced metering infrastructure
- Home area networks
- Electric vehicle (EV) charging
- Energy storage
- Photovoltaics (PV)
- Wind energy.

Source: iStock

Distribution Utility Attack



Common Practice in Security: Protocol and End Point Focused

Approach: Lock down everything.

- Encrypt all communications.
- Enforce protocol-level security.
- Monitor advanced authentication at the end-device level.

Limitations:

- Reactive—hackers are always ahead of an organization's cybersecurity capabilities (i.e., standard security processes are too slow).
- There is too much overhead (e.g., memory, processing, networking).
- Required upgrades of legacy equipment are costly.

NREL R&D Approach: Systemic Security

Approach: Limit damage that can be done from the start.

- Adhere to cyber hygiene (e.g., sound network design principles and cybersecurity management best practices).
- Use third-party, off-the-shelf technologies selectively for in-line blocking and context-based intrusion detection to maximize situational awareness and provide systemic cyber protection.
- Ensure that the strategy is compatible with legacy and modern equipment on Day 1 (so that no upgrades are required to function).
- Ensure that the strategy is modular and scalable.
- Ensure that the strategy does not depend on cybersecurity controls at the end-device or protocol level.

Limitations:

- Legacy end devices in the field are still vulnerable to tampering (limited authentication available).

ESIF Laboratories

Rooftop PV and Wind

Energy Storage Lab
Residential, Community and Grid Battery Storage, Flywheels and Thermal

Systems Performance Lab with Cyber
Buildings and Loads

HPC and Data Center

NREL, 24614

Energy Systems Integration Lab
Fuel Cells, Electrolyzers

Power Systems Integration Lab
Grid Simulators, Microgrids

Outdoor Test Areas
EVs, Power Transformers

NREL, 28836

Auxiliary Control Room
Advanced Distribution Management System Test Bed

NREL, 40902

Unique Value Proposition for CPSS&R

- **Deep expertise** in:
  - Power systems Supervisory Control and Data Acquisition (SCADA)
  - Cybersecurity
  - Networking
  - Distributed energy resources (DERs).

- **Advanced research capabilities** at the Energy Systems Integration Facility's (ESIF's) Systems Performance Laboratory, including:
  - Complete test bed with modular power systems, communications, and cybersecurity capabilities
  - Vendor and technology agnostic perspective
  - Ability to pen test at interface, component, or systems level.

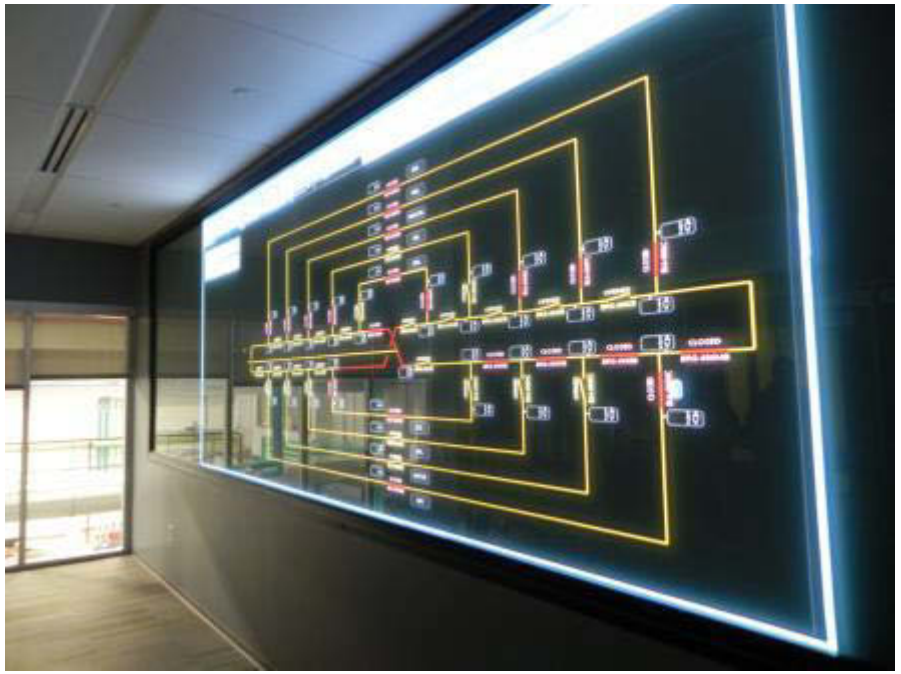
- **Flexibility** to expand to water, oil and gas, and thermal systems testing for cybersecurity and resilience.

NREL, 35452

NREL, 35445

CPSS&R Cyber Testbed Power Systems Use Cases

- Develop **five use cases** utilizing distribution management system (DMS) applications:
  - Auto-sectionalizing and restoration
  - Volt/volt-ampere reactive optimization
  - Demand response with EV charging
  - PV smoothing with storage
  - Frequency regulation with storage.



NREL, 24927

- Build the distribution system testbed with a DMS, enterprise SCADA, substation automation platform, intelligent electronic devices (Remote Terminal Units, Programmable Logical Controllers, and field sensors), energy storage, electric vehicles, and simulated grid with capacitor banks and smart switches.

Cybersecurity Test Bed Network View

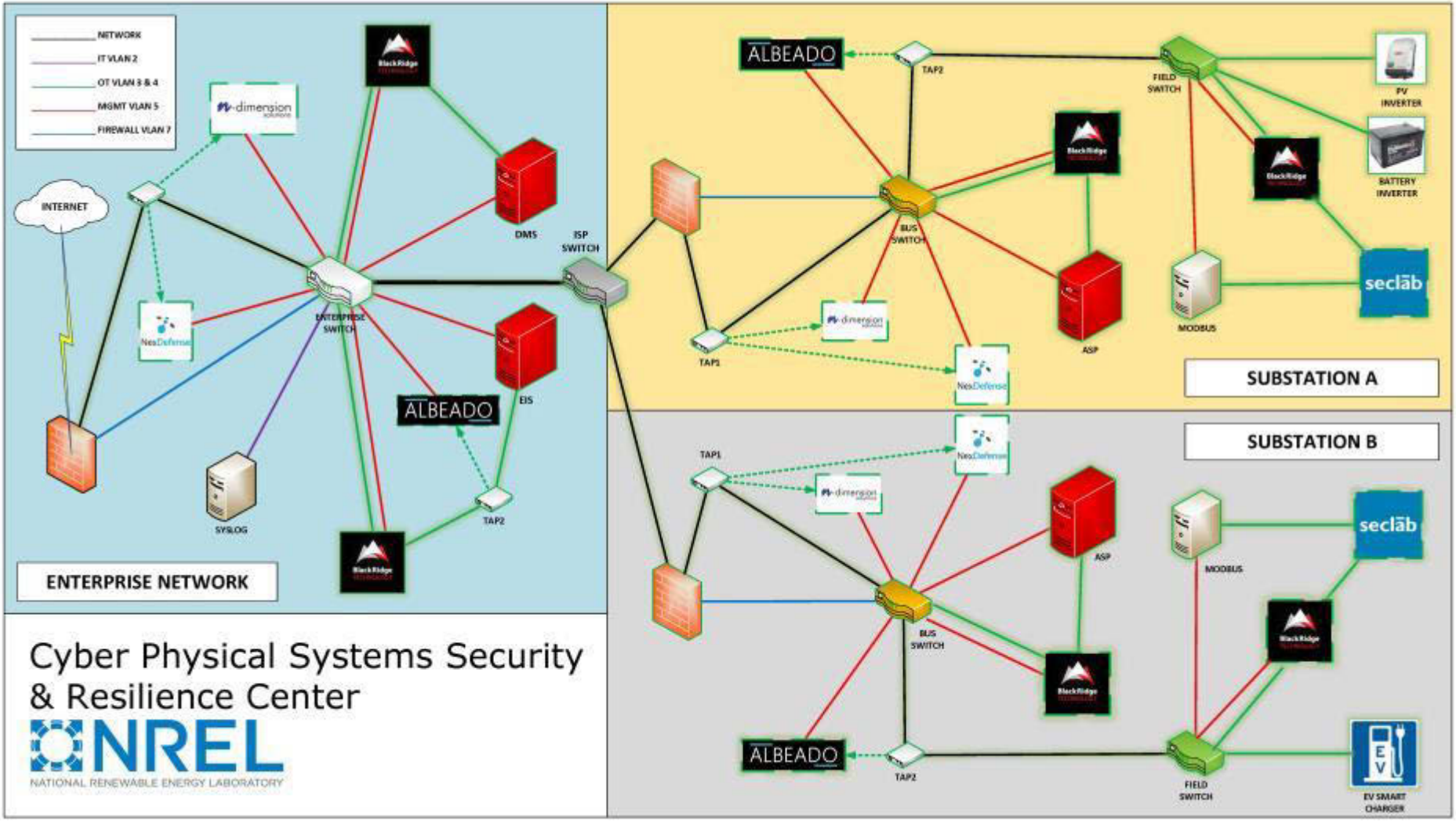


Diagram created by NREL, July 2017

Cybersecurity Test Bed Power Systems View

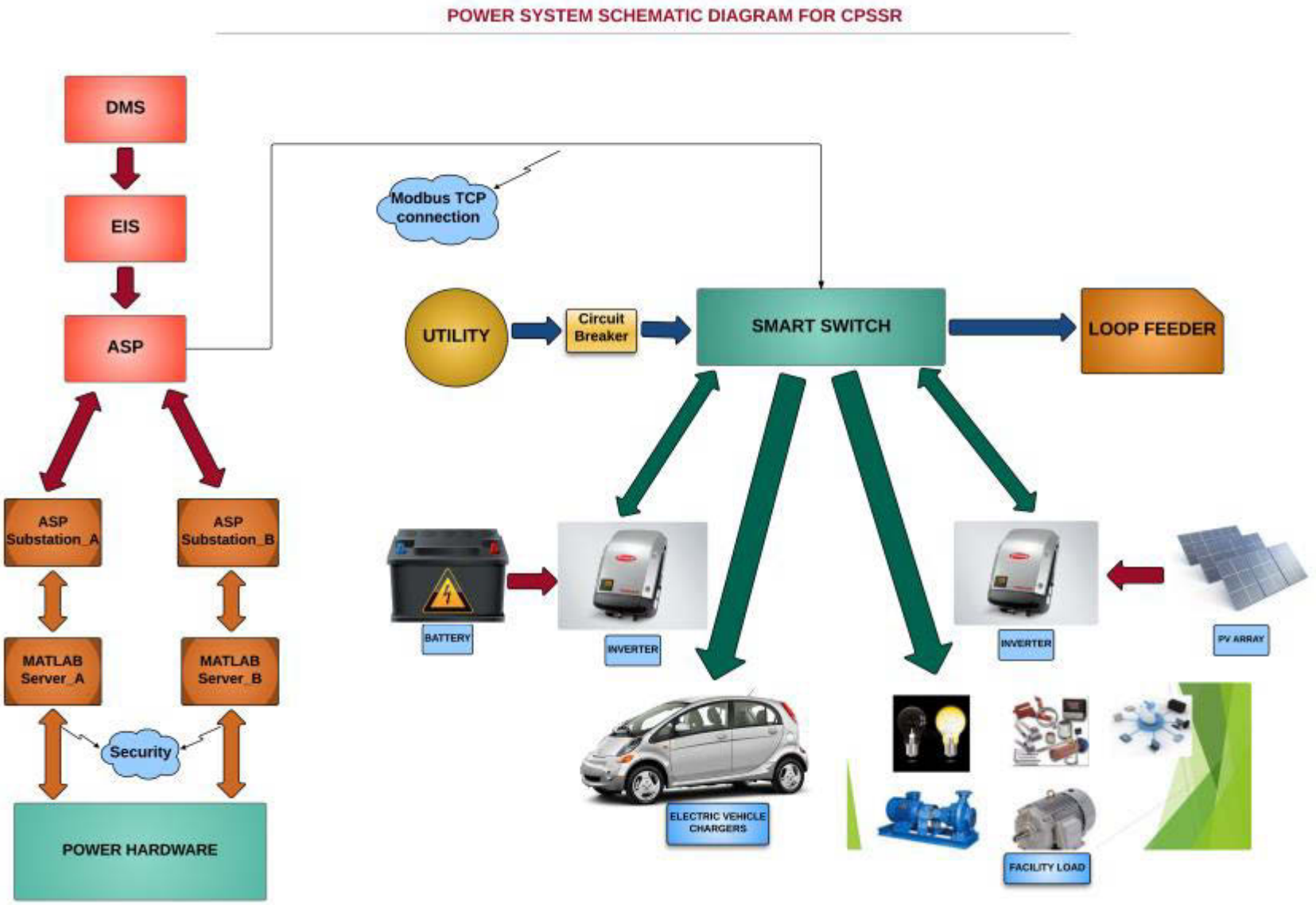


Diagram created by NREL

9-Layer Security Architecture - Testbed Technologies

security application / layer	SecLab Denelis	BlackRidge TAC	Cisco Firewall + Switches	NexDefense Integrity	N-Dimension N-Sentinel	Albeado PRISM
GWAC 5-6 Business						
GWAC 4 Semantic						
OSI 7 Application						
OSI 6 Presentation						
OSI 5 Session						
OSI 4 Transport						
OSI 3 Network						
OSI 2 Data Link						
OSI 1 Physical						

Diagram updated by NREL in July 2017

NREL's 10-Step Systems Engineering Approach to Security

1. Assess cyber-governance (security controls in place, prioritized action items for gaps in security controls) **(identify and protect**).

2. Implement technical plan to address gaps from cyber-governance assessment **(protect)**.

3. Perform due diligence on cutting-edge cybersecurity technologies for energy systems, including functional and integration testing **(identify and protect)**.

4. Develop procurement language for secure, reliable, and resilient SCADA systems **(protect)**.

5. Review utility SCADA cybersecurity architecture and benchmark against NREL nine-layer cybersecurity model, including vulnerability assessment and risk mitigation **(identify, protect, monitor, and respond)**.

NREL's 10-Step Systems Engineering Approach to Security

6. Scan software code and binary executables to identify malware and cyber risks as well as techniques for mitigation **(identify and protect).**

7. Test data fuzz of SCADA systems with risk mitigations **(identify and protect).**

8. Pen-test SCADA systems in NREL's cybersecurity test bed to identify residual cyber risks and provide mitigations **(monitor, respond, and recover).**

9. Develop and analyze failure scenarios with mitigations **(recover).**

10. Provide training on cybersecurity awareness for corporate staff and information technology/operation technology audiences to reduce cyber risks from social engineering and phishing schemes from advanced persistent threats **(identify, protect, monitor, respond, and recover).**

Contact Information:
Maurice.Martin@nrel.gov
(303) 384-7592

www.nrel.gov

NREL
NATIONAL RENEWABLE ENERGY LABORATORY