NREL
Transforming ENERGY

Cyber-Resilient Distributed Autonomous Energy Grid

DARPA AMP Meeting: January 24, 2023

Richard Macwan & Yakoub Nemouchi

Senior Researcher

Cybersecurity Science and Simulation Group

Cyber-Resilient Distributed Autonomous Energy Grid

Research Aim:

*Develop an **integrated framework for cyber-resilience** in the design and operation of a distributed autonomous energy grid.*

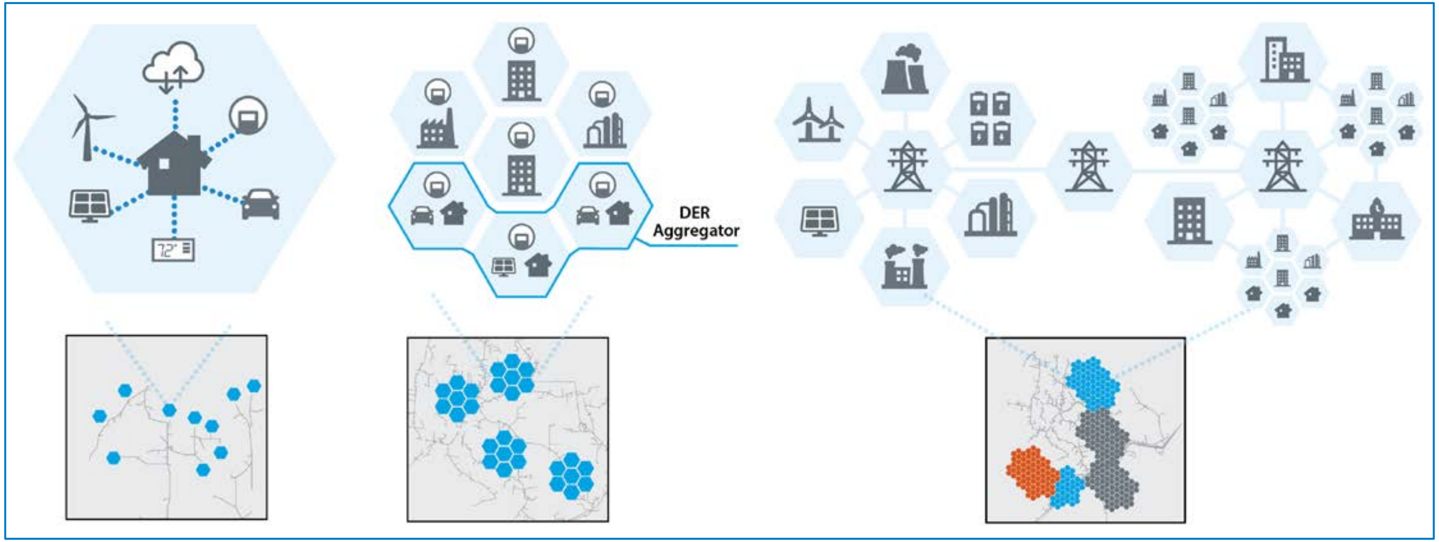
Research Approach:

Advancements in fundamental science and engineering approaches in the field of:

- Cyber-resilient design and control
- Zero trust architecture for autonomous grid
- Autonomy to enhance cyber-resilience

Future Grid Challenges

Features of future grid		**Cyber-Resilience challenges**
Distributed (Authority)	→	Distributed attack surface
Interconnected (Communications)	→	Multiple attack entry points
Hierarchal and Coordinated (Design & Operation)	→	Cascading impacts and failures
Autonomy (Control and Operation)	→	Autonomous Decision Making



Cyber-Resilience For Future Grid

- Cybersecurity can be a subset of Cyber-Resilience
- Cyber Resilience is a ***dynamic and ongoing*** process
- Cyber-Resilience needs ***novel solutions at every layer*** of the system

State of Patching in OT Security

- Devices life cycle 25-30 years.
- Lack of patch management tools for OT environments.
- Impact on time, cost, and manpower.
- Prevalence of legacy devices in terms of:
  - Operating Systems
  - Hardware Architecture
  - Applications
- “Don’t fix what is working” mindset (domino effect on the 16 CIKR)
- Heavy reliance on the IT-OT airgap

Evolving Challenges

- Dramatic increase in the number of devices
- Increased heterogeneity of devices and applications
- Unfettered supply chains
  - Hardware and Software
- IT-OT Convergence (The concept of airgap is not true anymore)
- Lack of means for prioritization for patching
- Lack of assurance on post patching state of operation

Use Case 1: Legacy Device Maintenance

- **Scenario:**
  - Prevalence of legacy devices with outdated hardware and software with known vulnerabilities controlling critical assets
  - Lack of vendor support or Vendor gone out of business
- **Challenge:**
  - Patch acquisition (down time, implementing the patch, buying a patch?)
  - Patch management (validating the patch, compliance to NREL's regulations, etc.)
  - Patch deployment
  - Assurance of post-patching critical system operation

Use Case 2:
Security Architecture Assurance

- **Scenario:**
  - New paradigms such as Zero Trust Architecture needed for secure energy system evolution
  - Implementing ZTA considering multi-stakeholder environment
- **Challenge:**
  - Patching for feature modification/enhancement to meet new security architecture requirements
  - Providing enhancements for enabling security by design
  - Enabling dynamic onboarding of new devices and applications

Use Case 3: Patching at Scale

- **Scenario:**
  - Rapid integration of large number of heterogenous DER devices and applications
    - Scale in variety of features in a single device
    - Scale in number of heterogenous devices
  - Diverse set of vendors: hardware and software
- **Challenge:**
  - Assured patching for heterogenous vendor devices to meet a given security requirement
  - Assured patching across applications and protocols on a device to meet a given security requirement

Use Case 4: Patching to Enable Rapid Recovery

- **Scenario:**
  - Large scale blackout on the power grid due to a cyber attack
  - Need for rapid recovery of energy supply to critical assets
  - Energy recovery without verifiable cyber recovery is useless
- **Challenge:**
  - Rapid cyber system recovery requires threat characterization and attribution (DARPA RADICS)
  - Targeted patching in a dynamic and contested environment
  - Security patching and feature modification to enable rapid recovery

Research Opportunities

- **Prioritization**
  - How to prioritize what to patch and when to patch?
- **Scale**
  - How to develop tools and methods to enable patching of heterogenous devices and applications?
- **Mission Assurance**
  - How to provide assured targeted patching for feature enhancements and security while providing mission assurance?
- **Assured Compliance**
  - How to enable bottom-up verification for devices and applications for verifiable security standard compliance?
- **Autonomy for Cyber-Resilience**
  - How to develop tools and techniques to enable autonomous detection and patching to enhance system cyber-resilience?

Formal methods strategy

Verified requirements

- Top-down verification
- System-level verification
- Refinement and instantiation
- Code generation

Crown jewels protection

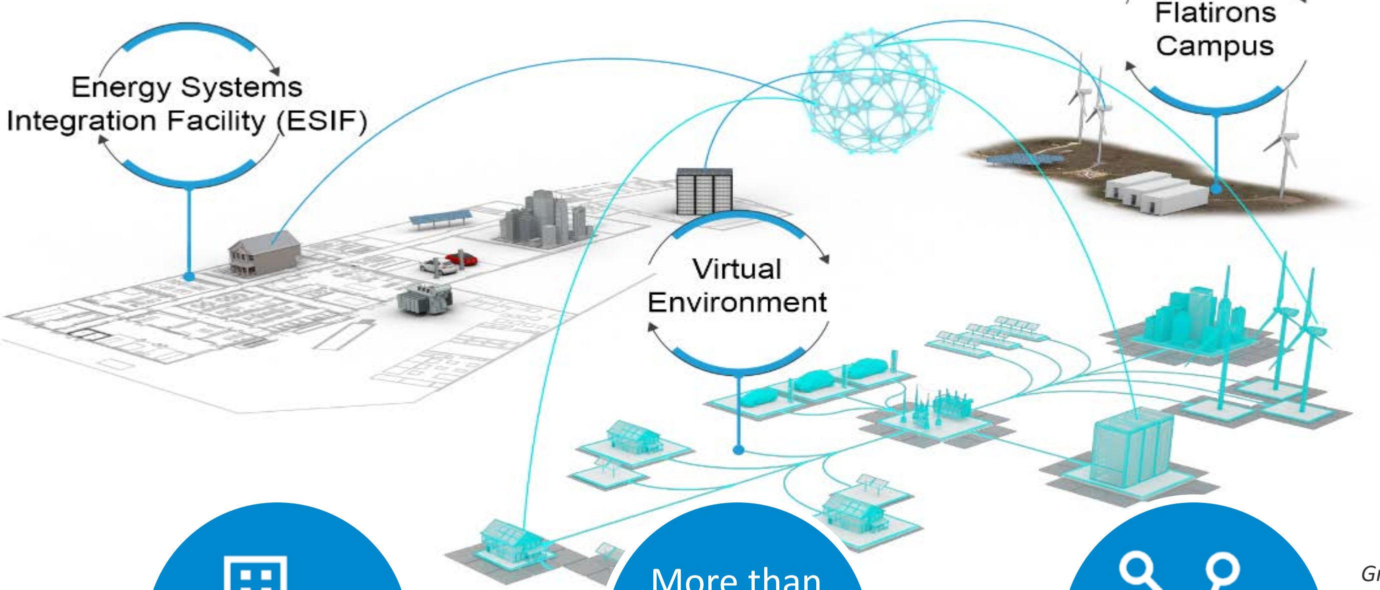
- Bottom-up verification.
- Verification based on attacker models.
- Low-level code verification.

Verified Compliance

- Crafting artifacts for High level certification.
- Document modeling.
- Assurance case Arguments (GSN, SACM, CAE).

NREL Capabilities

ARIES: Advanced Research in Integrated Energy Systems



Graphic by NREL

2,926

Workforce, including

219 postdoctoral researchers

60 graduate students

81 undergraduate students

World-class

facilities, renowned technology experts

More than **900**

Partnerships

with industry, academia, and government

Campus

operates as a living laboratory

Summary

- ***Secure and resilient integration of renewable energy resources at scale***
  - The use of formal methods for OT security and resilience.
  - Advance the state of the art of formal methods to be applied to energy systems
  - Advance the science of cyber-resilient OT system design
  - Secure and resilient grid control schemas
  - Move OT security from implicit trust to explicit verification
  - Enable autonomy and deception to stay ahead of the threat curve

NREL/PR-5R00-85142

This work was authored by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported by the Laboratory Directed Research and Development (LDRD) Program at NREL. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government.