Cyber-Resilient Distributed Autonomous Energy Grid

May 10, 2022

Richard Macwan

Senior Researcher Power System Cybersecurity

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

Defining Cyber-Resilience

- The ability of the system to ***prepare, anticipate, defend, withstand, recover,*** and ***adapt*** from an adverse cyber event on the system.

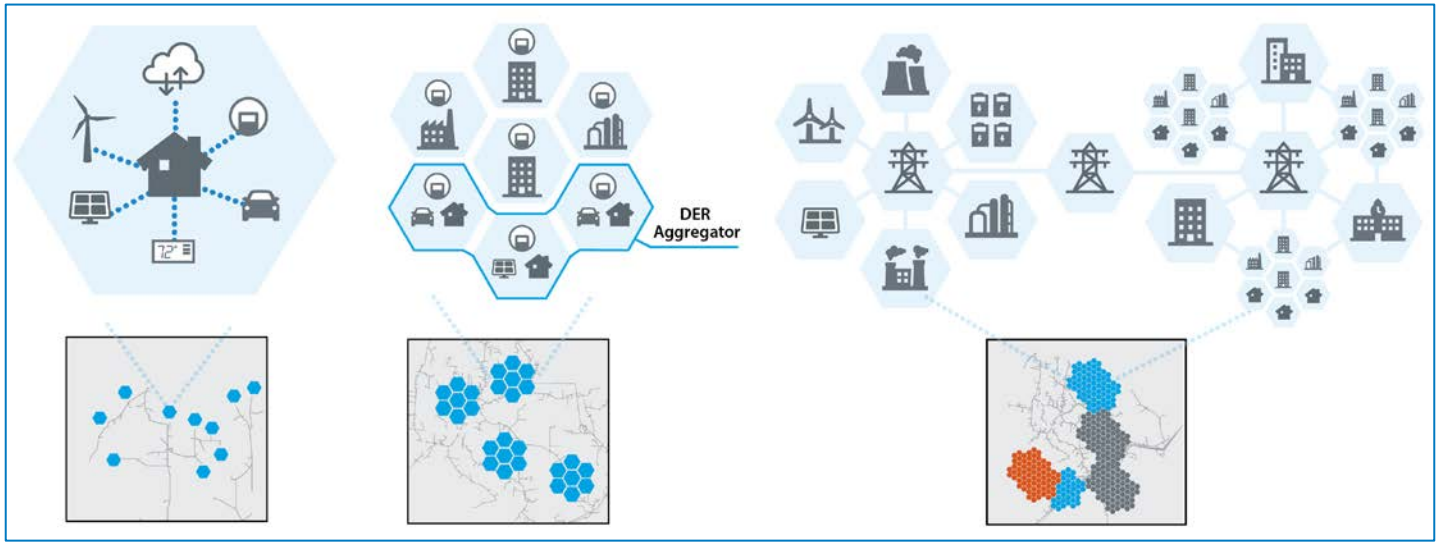
Cyber-Resilience Definitions*

Context	Term	Definition
National Security	Resilience	"The ability to ***adapt*** to changing conditions and ***prepare*** for, ***withstand,*** and rapidly ***recover*** from disruption." [WH 2010]
Critical Infrastructure	Infrastructure resilience	"Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to ***anticipate, absorb, adapt*** to, and/or rapidly ***recover*** from a potentially disruptive event." [NIAC 2010]
Critical Infrastructure Security and Resilience	Resilience	"…the ability to ***prepare*** for and ***adapt*** to changing conditions and ***withstand*** and ***recover*** rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [WH 2013]
DoD Cybersecurity	Operational resilience	"The ability of systems to ***resist, absorb,*** and ***recover*** from or ***adapt*** to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions." [DoD 2014]

* "Cyber Resiliency FAQ" MITRE, Available online: https://www.mitre.org/sites/default/files/PR_17-1434.pdf

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



Research Approach

Cyber-Resilient Design

Emerging Features of Future Grid
Highly distributed

Emerging Cyber-Resilience challenges
Distributed attack surface

Approach:

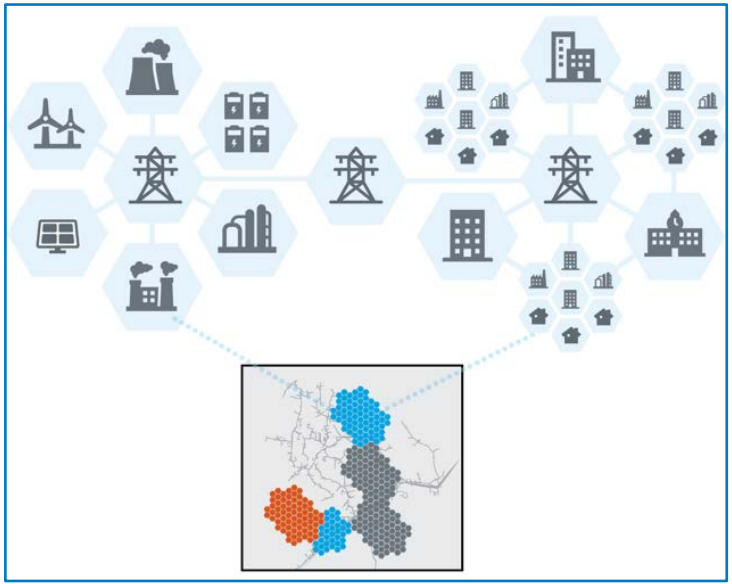
- Development of ***novel cyber-resilience metrics for cyber-physical systems***
  - Highly distributed and autonomous
- Development of ***novel Graph Neural Net approach*** to analyze and search for a more resilient cyber-physical topology

Innovation:

- Mathematical quantification of the impact of system topology on resilient operation of a distributed and autonomous grid
- Novel graph embedding techniques for combined cyber-physical networks

Impact:

- Bake-in security the design instead of bolt-on security
- Leverage topology for developing cyber attack response
- Determine future security investments



Cyber-Resilient Controls

Approach:

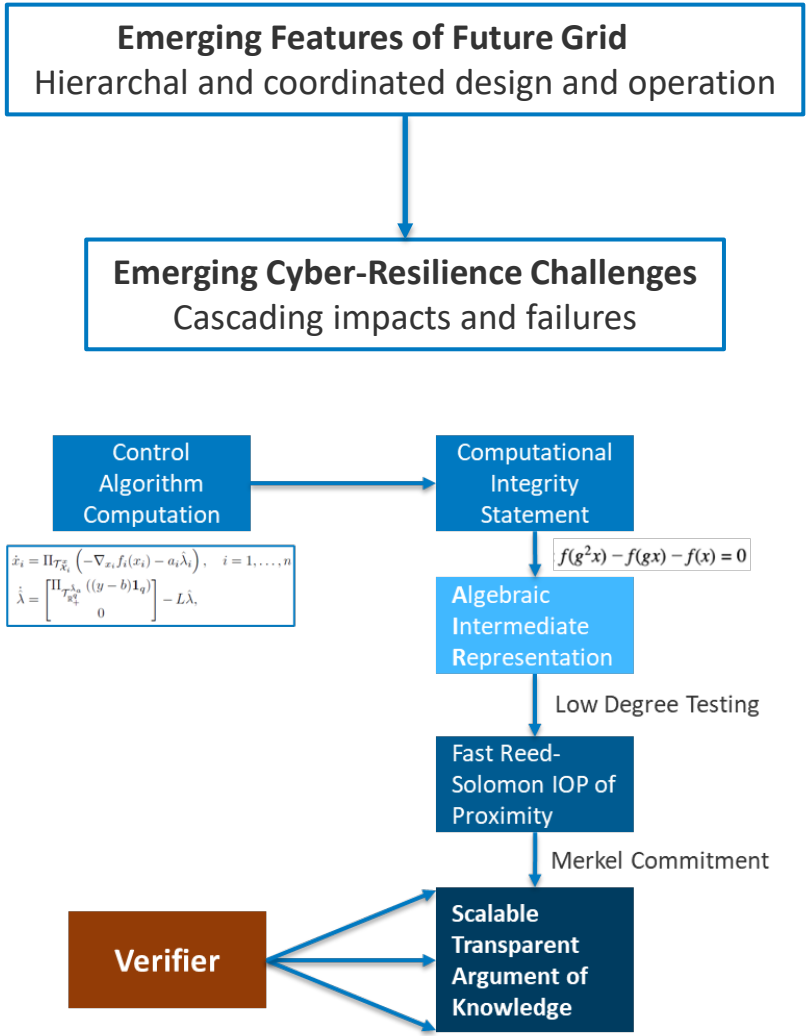
- ***Proof of computational integrity for the grid control approaches*** leveraging zero-knowledge proofs
  - Zero knowledge - Succinct Transparent Arguments of Knowledge (zk-STARK)

Innovation:

- Computational integrity versus just data integrity
- Transparency: Trust towards none, integrity for all
- Scalable and efficient
- Post-quantum secure (plausibly!)

Impact:

- Attack resilient control schemes
- Not reliant on novel encryption or access control schemes
- Forms a last line of defense



Zero Trust Architecture for Autonomous Grid

Emerging Features of Future Grid
Highly interconnected

Emerging Cyber-Resilience Challenges
Multiple attack entry points

Approach:

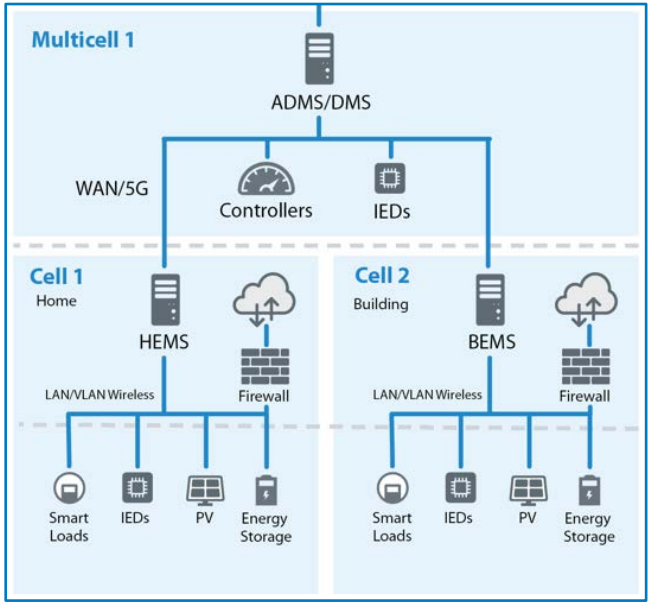
- ***Formally verifiable approach to developing zero trust architecture for operational technology (OT) systems***
  - Formal specification language for a cyber physical system
  - Physics informed machine learning for verification of data flow

Innovation:

- Bringing formal methods approaches to OT security
- Formal proof of minimum protect surface for OT system
  - Adequate, consistent, unambiguous, and complete

Impact:

- Move the challenge from inherent trust in the system to a quantifiable confidence.



Autonomy for Cyber-Resilience

Emerging Features of future grid
Autonomous Control and Operation

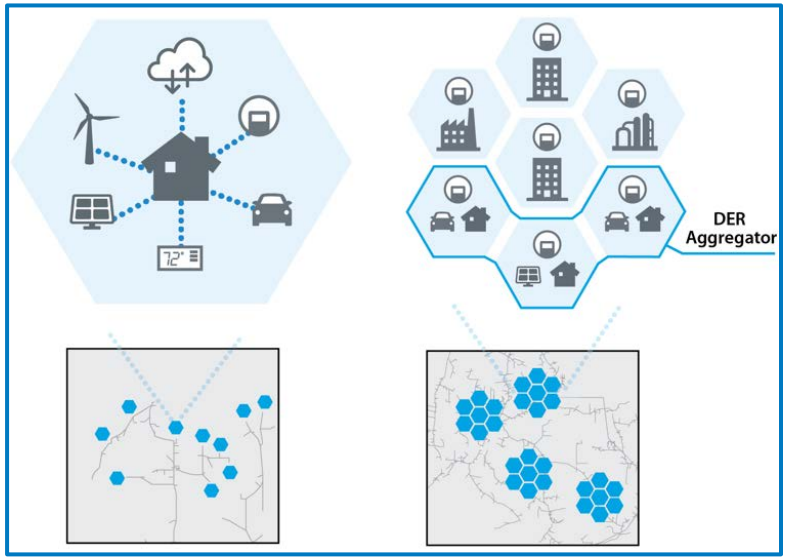
Emerging Cyber-Resilience challenges
Autonomous Decision Making

Challenge:

How to perform ***autonomous decision making*** in an environment that is governed by ***autonomous controls*** to ***withstand and recover*** after a cyber attack?

Approach:

- **Autonomous Decision Making = Autonomous Response in light of cyber threat intelligence**
  - Develop self-healing and self-optimizing techniques for communication systems for autonomous response to withstand and recover from a cyber-attack
  - Develop novel techniques for cyber deception and decoy in real-time OT environments that can help gather cyber-threat information



Areas of Research:

Graph Theory

Optimization Theory

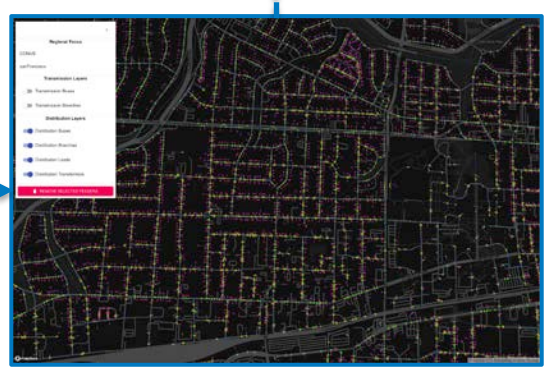
Complex System Theory

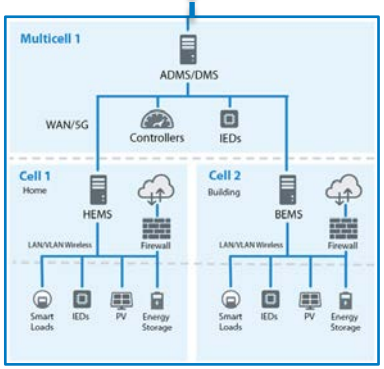
Game Theory

AI/ML Based Approach

NREL Cyber Range

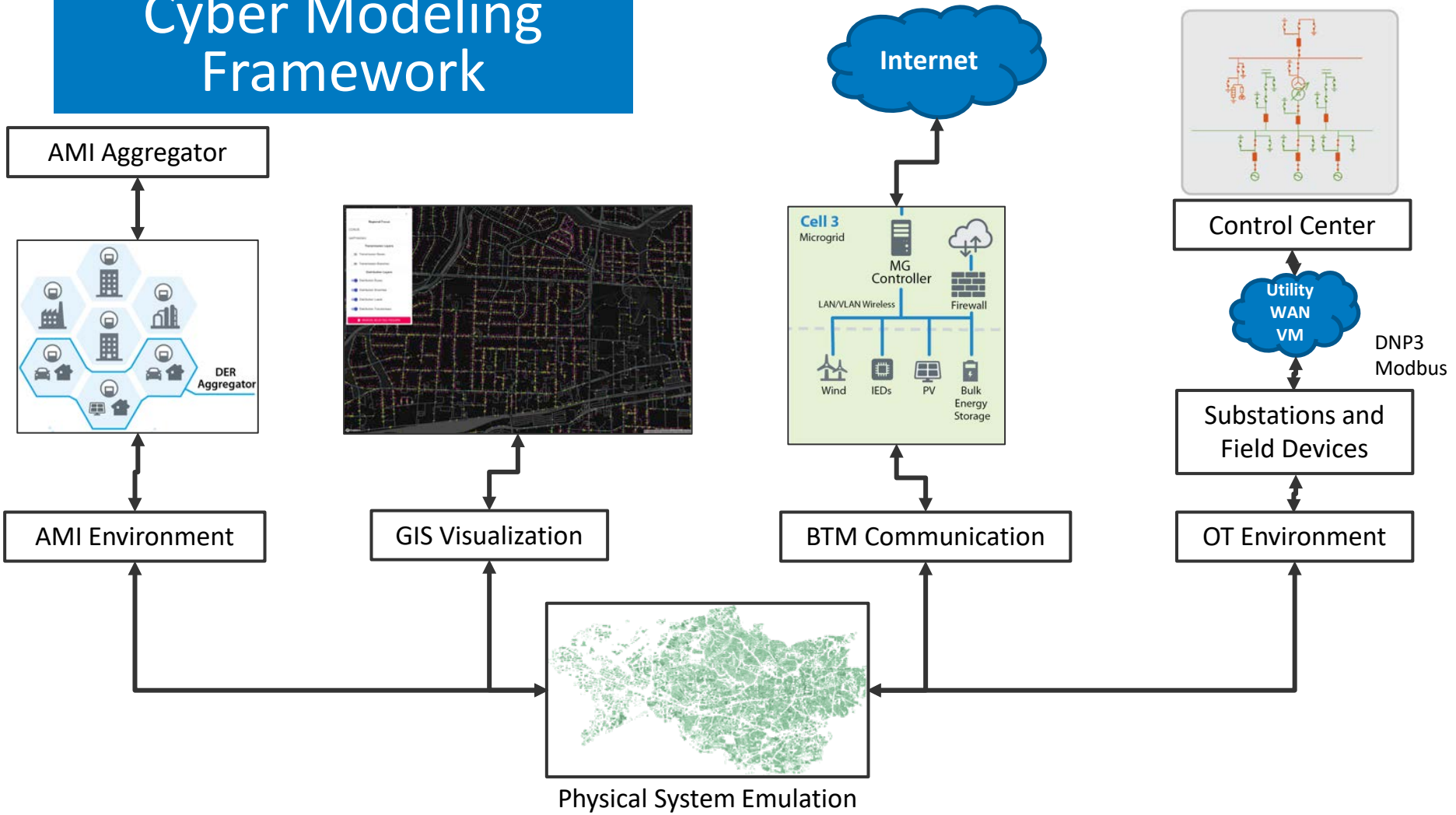
In minutes instead of Months.





- **Scale + Complexity**
- Dynamic orchestration
- Protocol Fidelity
- AMI Network emulation
- GIS visualization
- Policies and Procedures

Cyber Modeling Framework



Summary

- ***Enhance secure and resilient integration of renewable energy resources at scale***
  - 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

Acknowledgement

NREL/PR-5R00-82942

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. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.