Cyber Resilient Design and Controls for Energy Systems

September 20, 2022

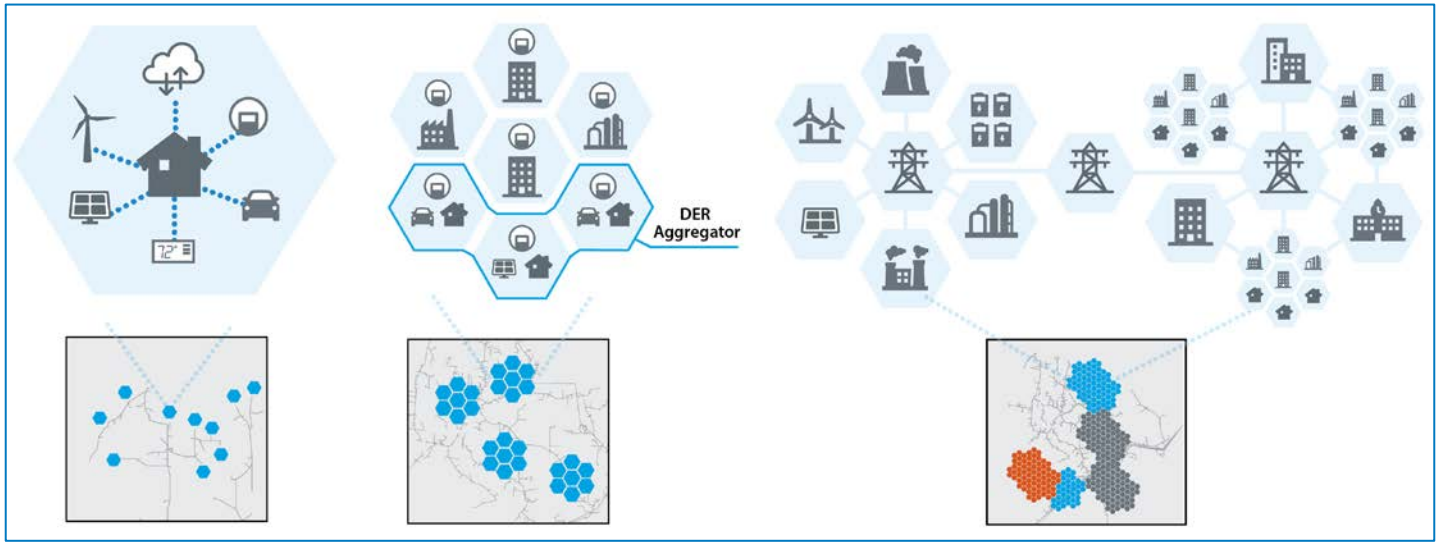
Richard Macwan

Senior Researcher Power System Cybersecurity

Cybersecurity Science and Simulation Group

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



Challenges of Cyber-Resilience

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

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

Cyber Resilient Design

Cyber-Resilient Design

Emerging Features of future grid
Highly Distributed
Hierarchal and Coordinated Design and Operation

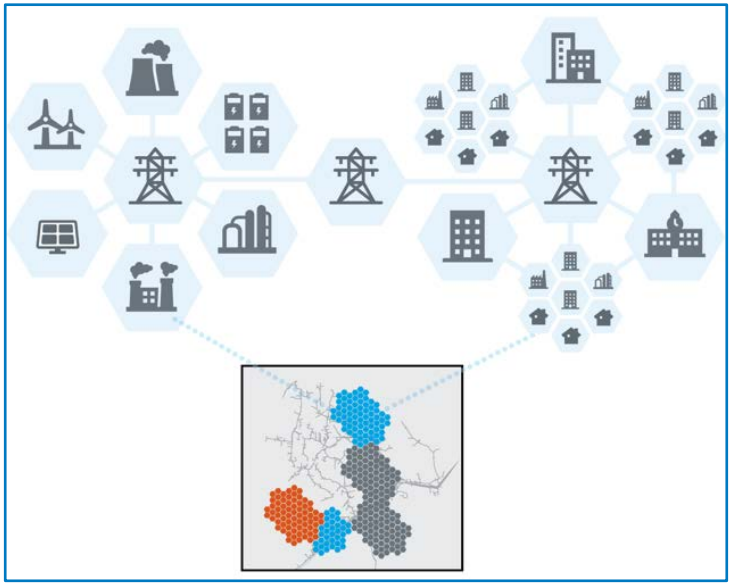
Emerging Cyber-Resilience challenges
Distributed attack surface

Challenge:

How to ***prepare, defend, and adapt*** the system against cyber-attack in an environment with a ***highly distributed and dynamic attack surface***?

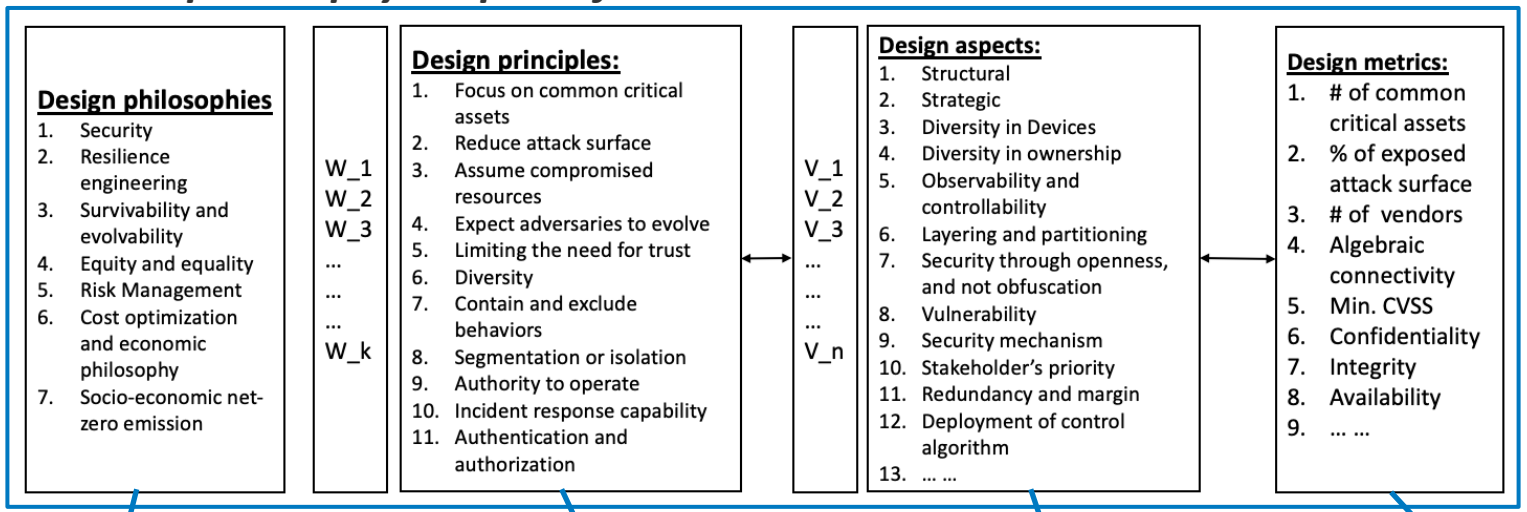
Approach:

- **Cyber-Resilience by Design**
  - Quantifying the impact of the network design and topology on the cyber-resilient operation of the system
  - Algorithms and methods to search for network design and topology for enhancing cyber-resilient operation



Cyber Resilient Design: Philosophy to Metrics

- Cyber Resilience by design implementation framework:
  - ***From philosophy to quantifiable metrics***



not mutually exclusive, and multiple philosophies can coexist

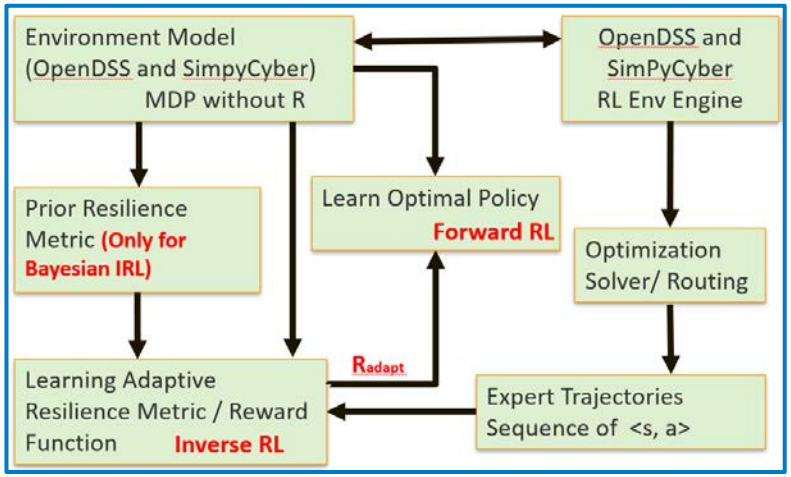
translate the broad design goals into specific principles

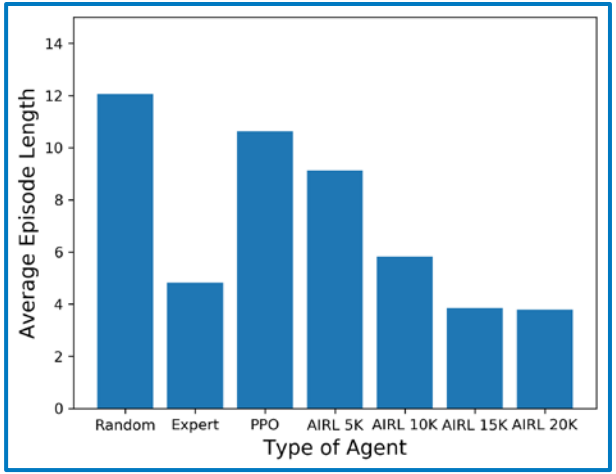
design choices, irrespective of the design philosophy

metric to quantify a design aspect

Adaptive Resilience Metrics

- **Challenge:**
  - How to prioritize resilience metric given the dynamic state of the system?
  - Static metrics trigger sub-optimal defense strategies
- **Approach:**
  - Learn ***Adaptive Resilience Metrics (Reward) using Adversarial IRL*** based on *States* and *Actions* on CPS
  - These Adaptive Resilience Metrics can be used to improve upon current optimal response policies





Single line outages from a set of 7 transmission lines and 14 critical loads in the IEEE 123 distribution feeder.

Cyber Resilient Controls

Major Accomplishments

Cyber-Resilient Controls

Emerging Features of Future Grid
Hierarchal and coordinated design and operation

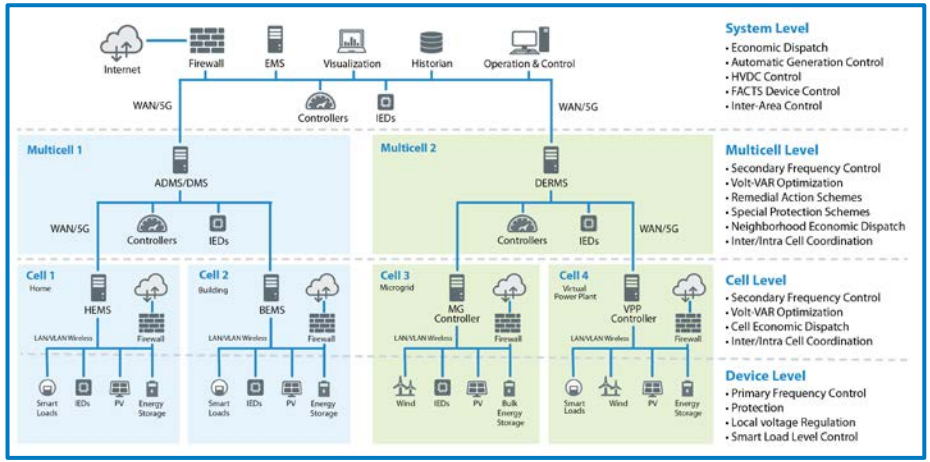
Emerging Cyber-Resilience Challenges
Cascading impacts and failures

Challenge:

- How does an ***attack at the cyber layer translate into a cascading impact on the physical layer***?
- How to ***inject cyber security and resilience into the control layer*** of the system?

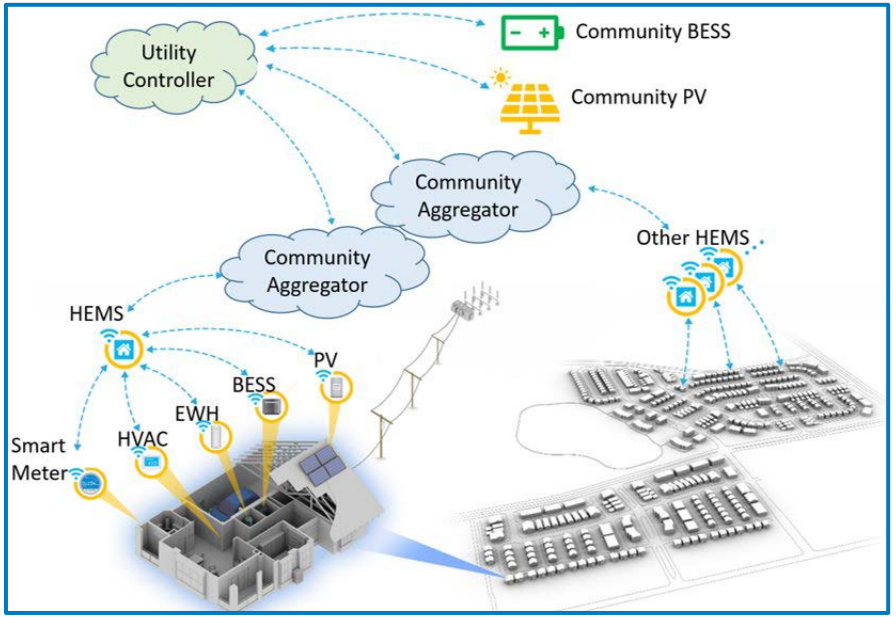
Approach:

- Identify and analyze control architecture cyber vulnerabilities
- Secure communication for power grid control
- Cyber attack detection and mitigation at control layer



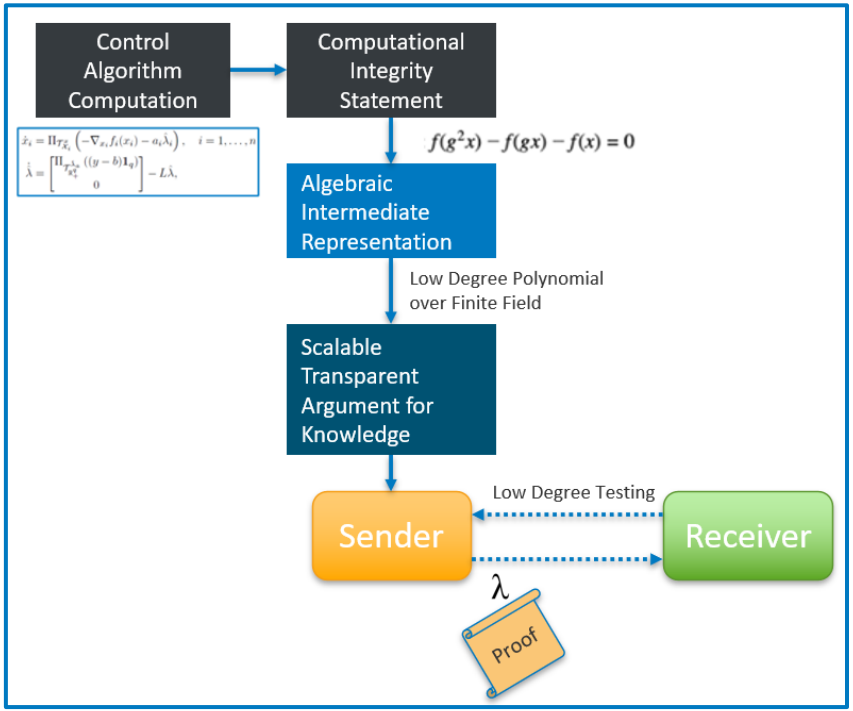
Cyber Attacks: Cyber layer to Physical layer

- ***3 Key of AES and AUMC Control Algorithms selected***
  - Centralized vs Distributed
  - Time scales (ms, s, mins, hours)
  - Level of control (Grid, BTM)
- ***Vulnerability analysis*** for each of the control algorithms
  - Cyber attack to physical impact
- ***Identification of high impact attack scenarios*** for each of the control algorithms



Zero Knowledge Proof for Secure Communication

- ***Proof of computational integrity for the grid control approaches*** leveraging zero-knowledge proofs
  - Zero knowledge - Succinct Transparent Arguments of Knowledge (zk-STARK)
  - Computational Integrity instead of data integrity
  - Transparency: Trust towards none, integrity for all
  - Scalable and efficient
  - Post-quantum secure (Plausibly!)
- Failure to provide successful proof is easy attack detection



Thank You!

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.

NREL/PR-5R00-83978