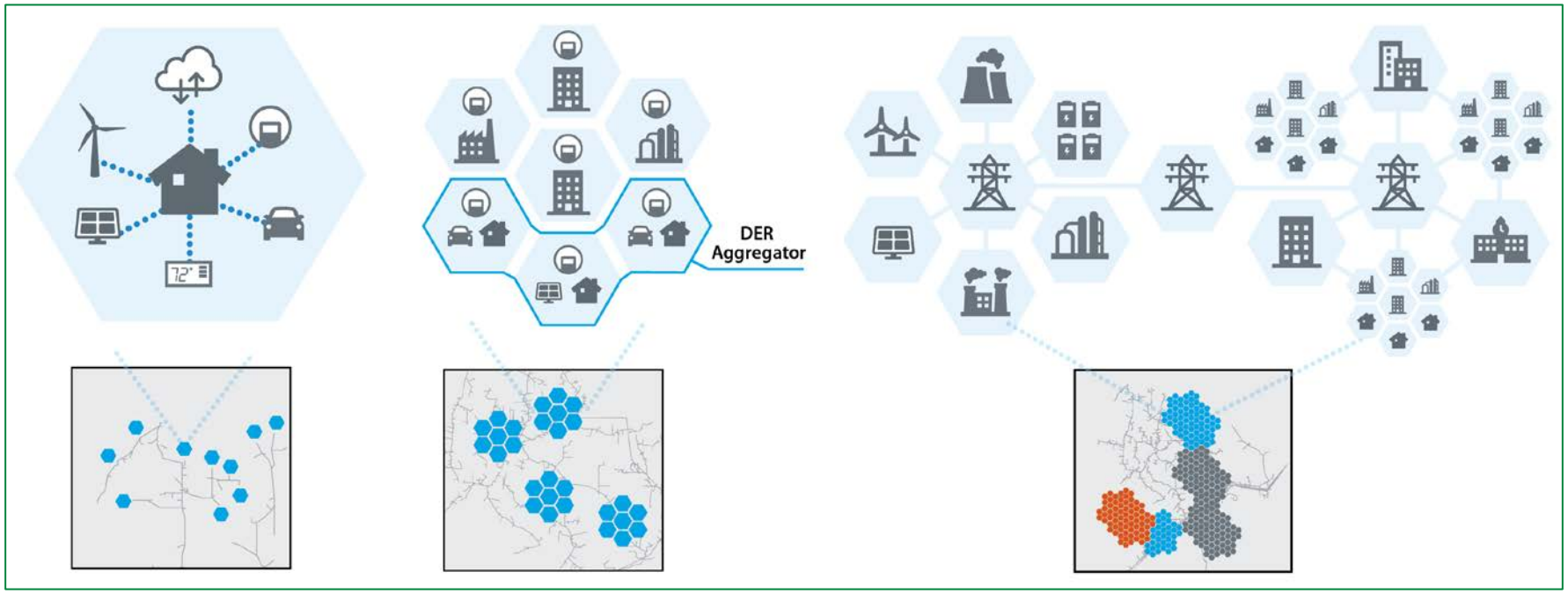
Cyber-resilient design methodology for microgrids

Venkatesh Venkataramanan, NREL

Team: Richard Macwan, Michael Abdelmalak, Shuva Paul

Future grid challenges

Features of future microgrid		Cyber-resilience challenges
Distributed (authority)	→	Distributed attack surface
Interconnected (communications)	→	Multiple attack entry points
Hierarchal and coordinated (design and operation)	→	Cascading impacts and failures
Autonomy (control and operation)	→	Autonomous decision making



Cyber-resilient design

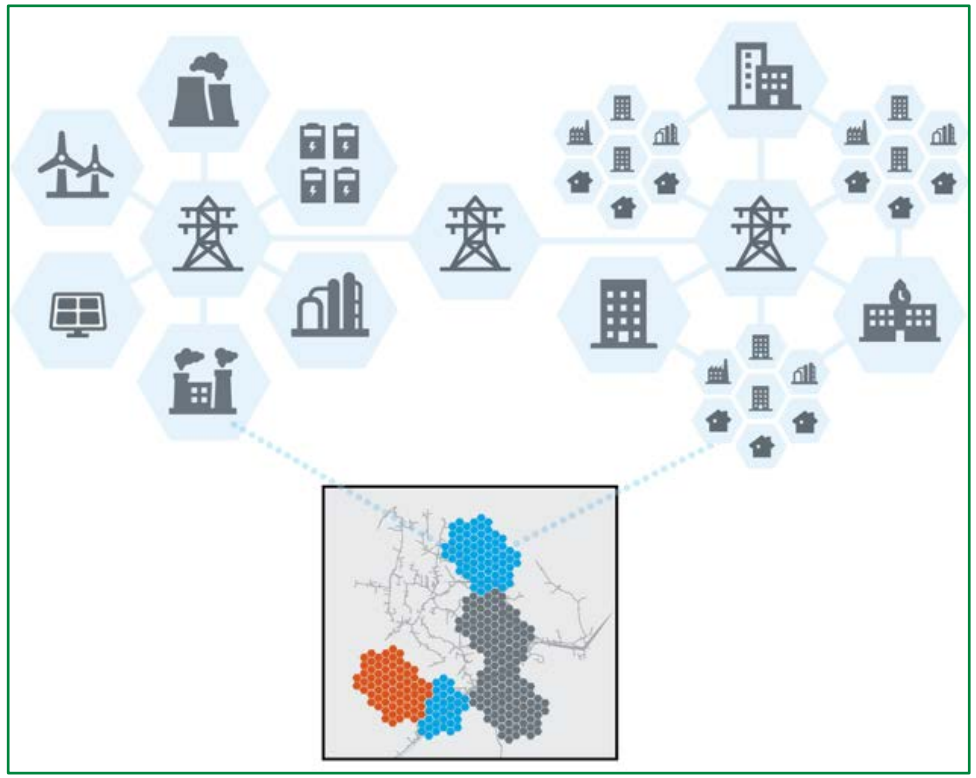
Challenge:

How to ***prepare, defend, and adapt*** the system against cyberattack in an environment with a ***highly distributed attack surface*** and ***possibility of cascading failures*** due to a cyberattack?

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.



How are things changing?

Emerging features of future microgrid

Increasing unpredictability

Highly distributed generation

Increasing grid-edge devices and intelligence

Hierarchal and coordinated design and operation

Emerging cyber-resilience challenges

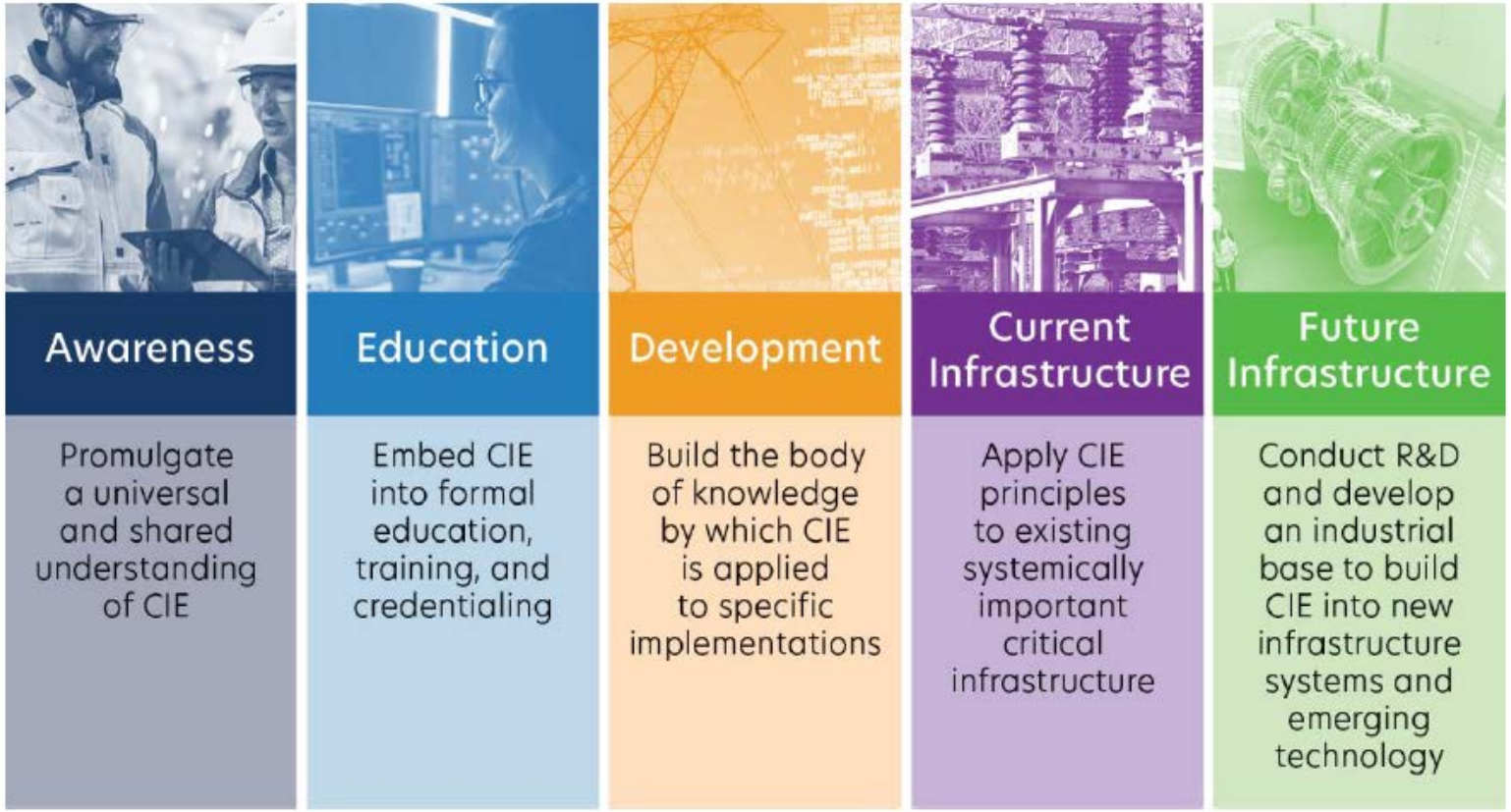
Distributed attack surface

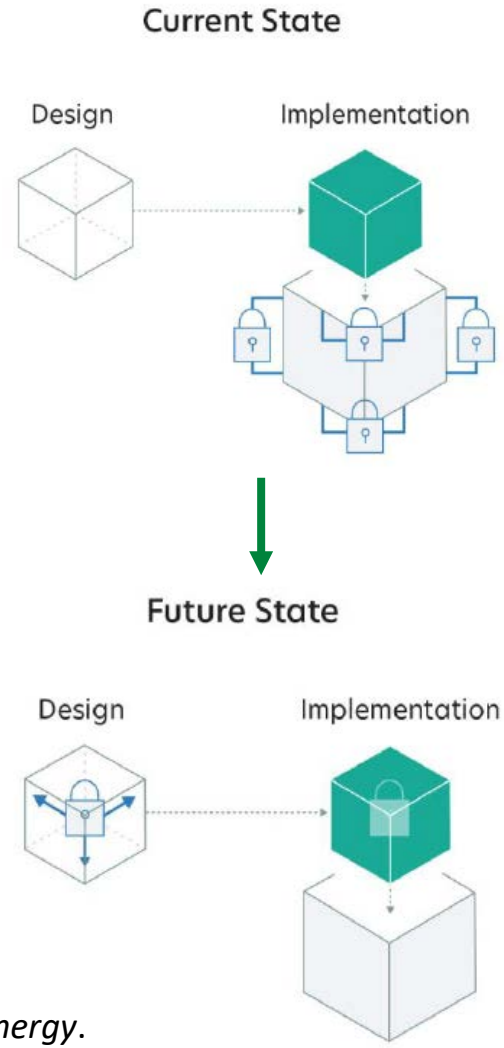
Cascading impacts and failures

Increasing interdependence

Related efforts

Cyber-Informed Engineering (CIE)





U.S. Department of Energy. 2022. *National Cyber-Informed Engineering Strategy from the U.S. Department of Energy*. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

Related efforts

MITRE Cyber Resiliency Design Principles

- Presents a representative set of cyber-resilience design principles
- Design framework: Goals → Objectives → Techniques
- Design principles classified under two main categories:
  1. Strategic principles (e.g., focus on common critical assets, expect adversaries to evolve)
  2. Structural principles (e.g., limit need for trust, maintain redundancy, determine on-going trustworthiness)

- Proposes a framework for implementation by stakeholders and correlates principles to risk management strategy.

Bodeau, Deborah J., and Richard D. Graubart. 2017. “Cyber Resiliency Design Principles.” The MITRE Corporation. https://www.mitre.org/publications/technical-papers/cyber-resiliency-design-principles.

Challenges

- Need a defined strategy that translates “big picture” ideas to actual, defined steps for design
- Need to translate design goals into actual metrics, which will be used to execute the design
- Need to identify the best way to model and characterize cyber-physical systems (CPS) to align with design principles.

CPS Models

An overview

Differences between cyber and physical system

	Nature of system	Time behavior	Mathematical model	System state	System operation	Branch model	Components	Condition	Contingency	Event behavior
Cyber	Static	Discrete	Difference equations	Information flow	Information technology (IT)	Information flow model	Communication networks, computing devices, control systems, etc.	Interdependent operation balance among all functions	Cyberattacks, communication latency, malicious failures, etc.	Synchronous
Physical	Dynamic	Continuous	Differential-algebraic equations	Energy flow	Operation technology (OT)	Power grid model	Generators, transformers, lines, protective relays, circuit breakers, loads, etc.	System operation constraints: load balance, transmission limits, etc.	Line faults, generator outage, vegetation, etc.	Asynchronous

- Cyber and physical systems have very different characteristics, which make integrated modeling and designing challenging.
- The right modeling method needs to be chosen for microgrids to ensure accurate representation of interdependent, and intra-dependent interactions.

Overview of CPS modeling approaches

Modeling techniques that are suitable for modeling cyber-physical microgrids include:

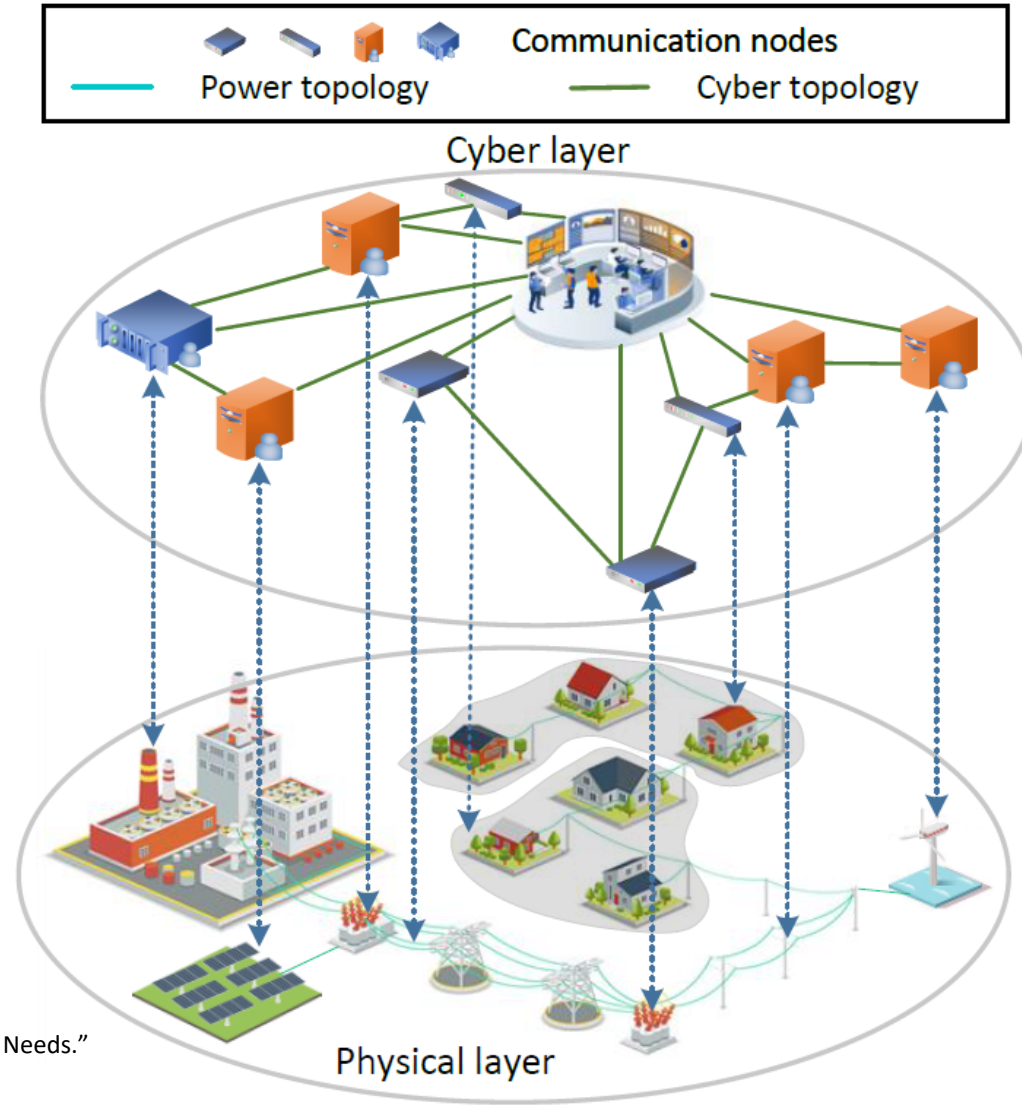
1. Graph theoretical methods
2. Complex network methods
3. System and control-based methods
4. Other modeling techniques.

Modeling evaluation criteria:

1. Accuracy
2. Scalability
3. Fidelity
4. Ability to model distributed systems
5. Ability to model system dynamics.

Mapping from physical to communication

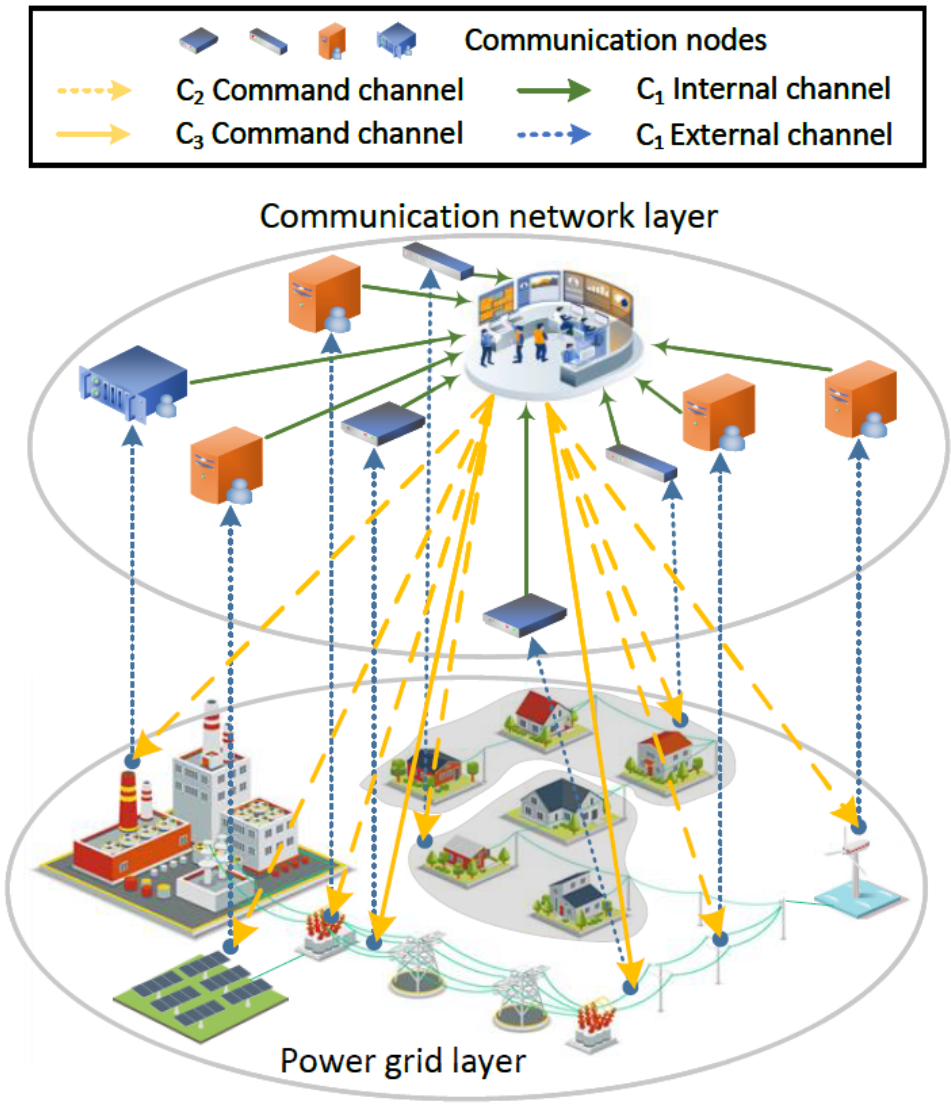
- It is important to distinguish communication and computation capabilities.
- “Cyber” capabilities are often used to mean either or both of these capabilities.
- Computation capabilities are often mapped in a one-to-one fashion—each computation node maps to a physical node.
- Computation capabilities play an important role in designing controls and coordination methods—does the microgrid need a central, decentralized, or distributed solution mechanism? (Refer to [1] for additional details.)



[1] Patari, Niloy, Venkatesh Venkataramanan, Anurag Srivastava, Daniel K Molzahn, Na Li, and Anuradha Annaswamy. 2021. “Distributed Optimization in Distribution Systems: Use Cases, Limitations, and Research Needs.” *IEEE Transactions on Power Systems*. https://doi.org/10.1109/TPWRS.2021.3132348.

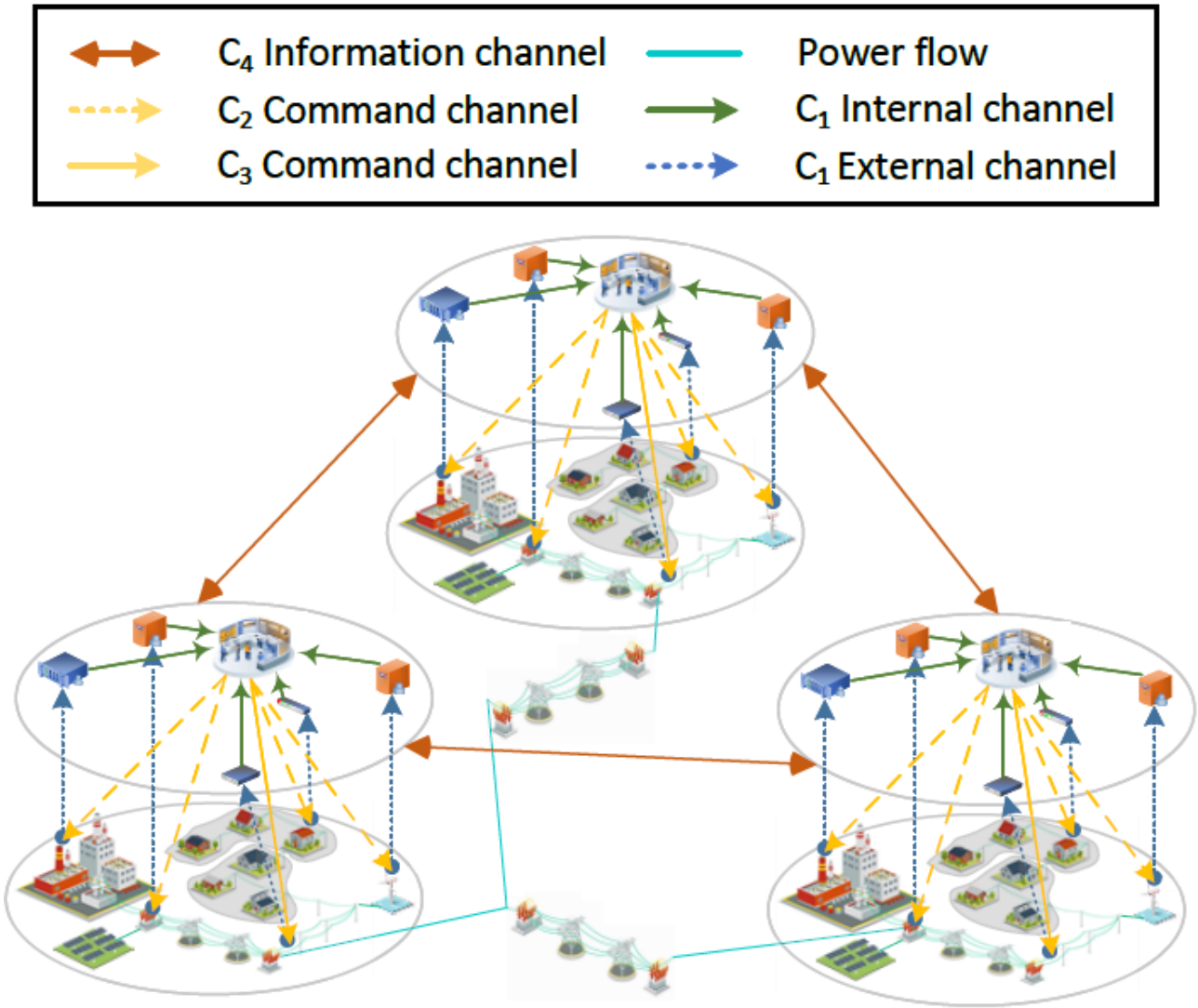
Mapping from physical to communication systems

- Communication systems dictate how IT and OT systems are configured.
- Microgrid architectures rely on simple communication models such as point-to-point.
- Diversity in protocols, ownerships, and communication media are challenges for system design.



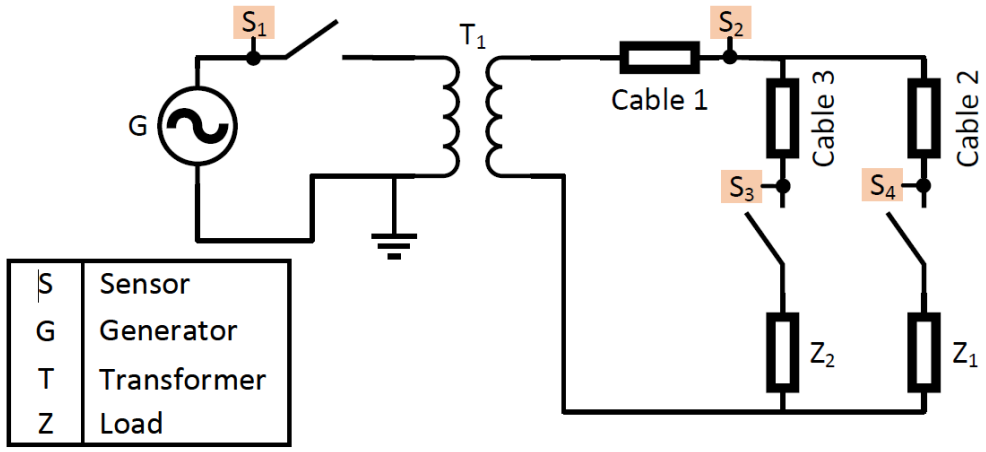
A multi-system design problem

- Co-design of power, communication, and cyber systems involves studying the impacts of one system on the other.
- Needs detailed understanding of failure and risk models to evaluate impact of failures and attacks.
- Resilience in design needs to be fundamental and an overarching principle in making decisions on all three layers.

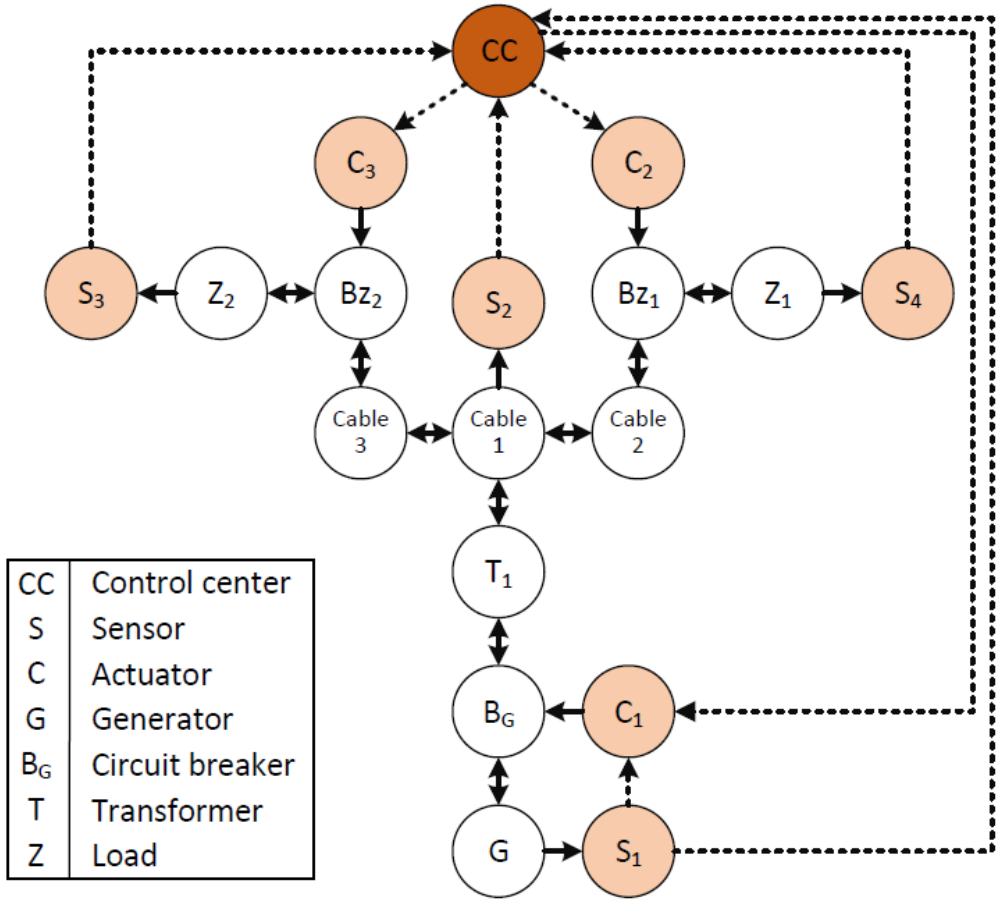


Interconnection modeling

Components-based approach



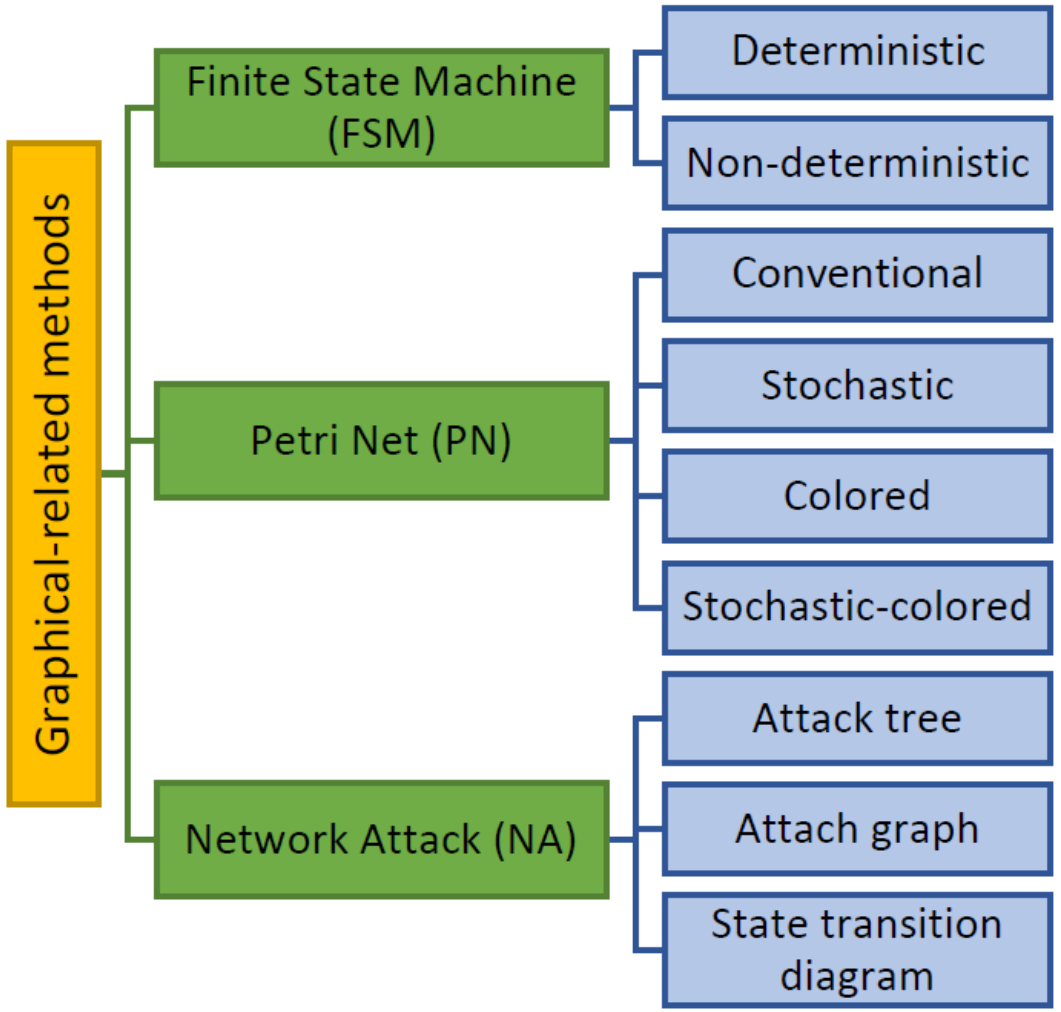
- Components are derived from physics, and physical system changes are represented by transitions.
- Provides highest fidelity in characterizing system behavior, as models have been studied and validated over a long time.



Interaction modeling

Graphical techniques

- Graphical techniques are among the most prominent techniques for creating accurate CPS models.
- There are multiple methods that leverage graphical techniques, including simple bijective relationships to more complex techniques.
- Active research is also being carried out using newer techniques such as graph neural networks.
- Graphical adjacent techniques are also used in designing security mechanisms, such as attack trees and failure models.



Interdependent modeling

System modeling techniques

A wide range of theoretical modeling techniques have been used to model microgrids:

- Dynamic modeling method (classical state-space and DAE models)
- Multi-agent system approach
- Network control system approach
- Correlation matrix approach
- Probabilistic approach
- Cellular automata.

$$\dot{x_G} = \begin{bmatrix} -D_G/J_G & 1/J_G & e_T/J_G \\ 0 & -1/T_u & K_t/T_u \\ -1/T_g & 0 & -r/T_g \end{bmatrix} x_G + \begin{bmatrix} 0 \\ 0 \\ 1/T_g \end{bmatrix} u_G + \begin{bmatrix} -1/J_G \\ 0 \\ 0 \end{bmatrix} P_G$$

$$x_G = \begin{bmatrix} \omega_G & P_T & a \end{bmatrix}^T$$

Cyber-physical generator (DER) models

$$x_{L,k} = \begin{bmatrix} 1 - \Delta T D_l/J_L & -\Delta T E_L/J_L \\ 0 & \phi_L \end{bmatrix} x_{L,k-1} + \begin{bmatrix} -\Delta T/J_L \\ 0 \end{bmatrix} P_{L,k-1} + \begin{bmatrix} 0 \\ E_L^T \end{bmatrix} \omega_L$$

$$x_{L,k} = \begin{bmatrix} \omega_{L,k} & \mathbf{L}_k^T \end{bmatrix}^T$$

Cyber-physical load models

Lessons learned

Comparing different modeling approaches

Method	Accuracy	Scalability	Fidelity	Distributed	Dynamical
Graph theory and complex network	High	High	Low	High	Low
FSM, Petri net, and network attack	High	Low	High	Low	High
Control-based	High	Low	Low for cyber, High for power	High	High
Correlation matrix	High	High	Low	Low	High
Probabilistic	Low	Low	Low	–	Low
Variable structure	Low	Low	Low	–	–
Cellular automata	Low	Low	High	–	Low

Challenges (revisited)

- Need a defined strategy that translates “big picture” ideas to actual, defined steps for design
- Need to translate design goals into actual metrics, which will be used to execute the design
- Need to identify the best way to model and characterize systems to align with design principles.

Resilience by design

Proposed framework

Definitions

1. **Design philosophies**: This will dictate the ***overall goal*** of the design, and the design philosophies could include broad goals such as resilience, cost optimization, security of systems, or decarbonization. These philosophies are ***not mutually exclusive, and multiple philosophies can coexist*** in a design. For example, a military installation could prioritize security highest while still considering decarbonization goals.
2. **Design aspects**: These are ***design choices*** that the system designer has to make irrespective of the design philosophy chosen. For example, various design aspects such as topological, diversity, redundancy and margin, and partitioning of assets are considered.
3. **Design metrics**: Based on the design aspects, the best ***metric to track a particular aspect*** is chosen. This metric will be determined based on the suitability of the metric to evaluate resilience and its ability to track performance across time and multiple installations.

A design approach to resilience

Design philosophies (Resilience, Cost, Security, Decarbonization, …)

W_1
W_2
W_3
…
W_k
Weights

Design Aspects:

1. Structural/topology
2. Diversity in ownership
3. Diversity in devices
4. Vulnerabilities
5. Carbon emissions
6. Layering and partitioning
7. Security mechanisms
8. Observability and controllability
9. Deployment of control algorithms
10. Redundancy and margin.

Design Metrics (M):

1. Algebraic connectivity
2. Third party ownership %
3. # of vendors
4. Min. CVSS* / # of vulnerabilities
5. Emission amount
6. Firewall rules
7. Security score
8. Controllability manifold metric
9. Centralized vs. distributed
10. Reserve capacity.

***CVSS – Common Vulnerability Scoring System**

Challenges (revisited)

- Need a defined strategy that translates “big picture” ideas to actual, defined steps for design
- Need to translate design goals into actual metrics, which will be used to execute the design
- Need to identify the best way to model and characterize systems to align with design principles.

Operational resilience

Future work

Adaptive resilience

Evolution of baked-in resilience

- When resilience becomes a characteristic of the system, and design choices are made considering resilience, operation becomes easier.
- However, considering that system operation is dynamic, and that adversaries are always evolving, resilience targets need to be ***dynamic and adaptive***.
- Need to formulate methods for changing the definition of resilience according to the situation—an adaptive resilience metric.
- Various approaches are being considered in literature: data-driven methods, system methods such as reinforcement learning, and human-driven performance adaptation.

Thank you!

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by 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.

Team: Richard Macwan, Michael Abdelmalak, Shuva Paul

NREL/PR-5000-83482

NREL
Transforming ENERGY