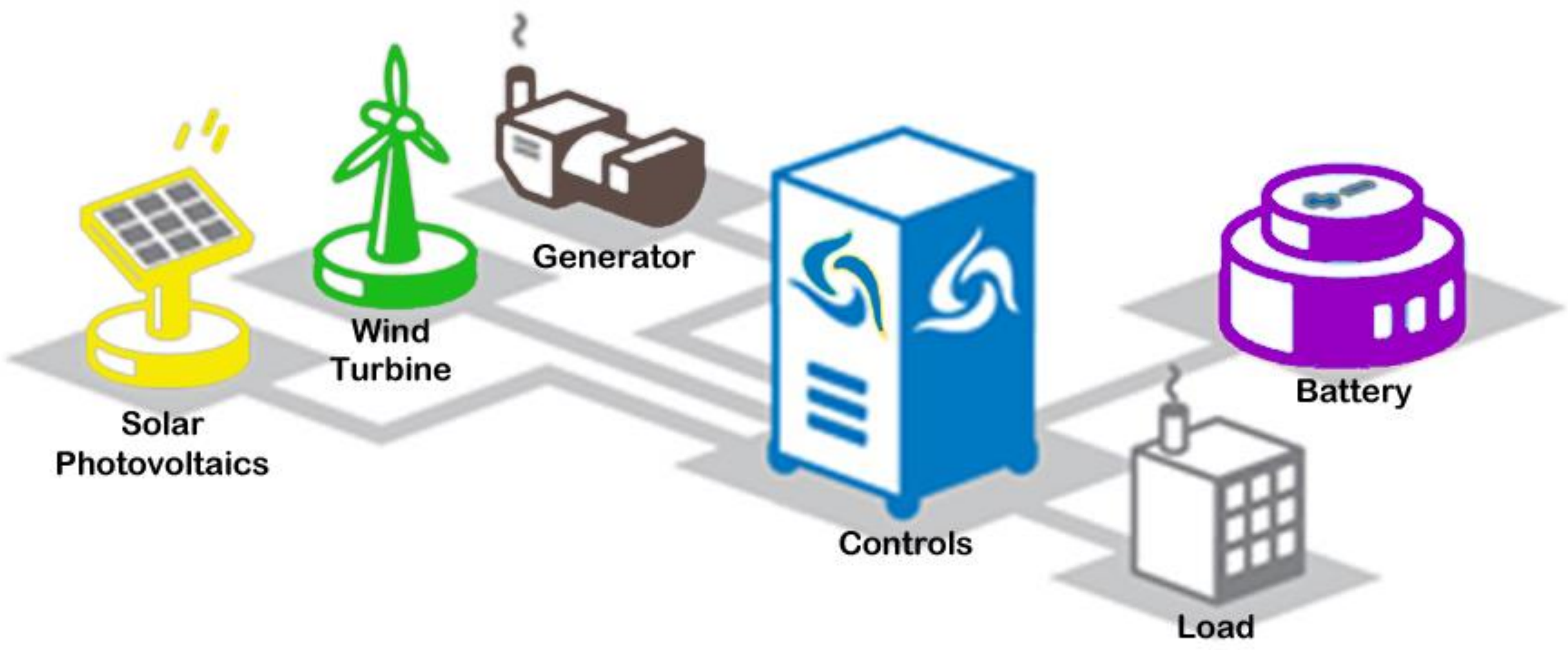
Secure, Dynamic Interoperability of Microgrid Assets

Hao Jan Liu, Al Valdes, and Hao Zhu

GOALS

- Establish a secure framework for interoperability of the following microgrid assets:
  - Storage.
  - Distributed energy resources (DERs).
  - Demand response.
  - Ancillary services from renewable energy assets.
- Develop robust control designs for dynamically managing microgrid heterogeneous components.
- Build an intelligent collaborative defense against malicious cyber attacks.
- Design an autonomous system with a secure dispatch mechanism.



FUNDAMENTAL CHALLENGES

- Interoperability of various components is presently ad hoc, with suboptimal and cyber-insecure operation and asset dispatch.
- Control strategies require high-quality communications under a secure framework.
- Microgrid controls are greatly challenged during an islanding event when the primary voltage source is lost.
- The inverter-based microgrid differs significantly from the traditional grid in terms of system modeling and operations. Thus, it gives rise to technical challenges with respect to:
  - Frequency and voltage control,
  - Islanding mode,
  - System protection.

RESEARCH PLAN

- Example microgrids, as well as distribution feeders, are modeled in OpenDSS via control function in MATLAB to demonstrate the effectiveness of the voltage control design.
- Measurements from monitoring devices are fed back to provide control inputs, e.g., reactive power support from DERs to regulate system voltages.
- We assume a centralized cyber infrastructure and communication networks and examine the response of a voltage control to cyber attacks, such as malicious data injections.
- Additional measurements from the microgrid are used to help identify potential cyber attack events through physical-cyber coupling of the network.
- The voltage control performances under malicious data injections and normal operation are compared to provide quantitative effects of cyber intrusion.

PRELIMINARY RESEARCH RESULTS

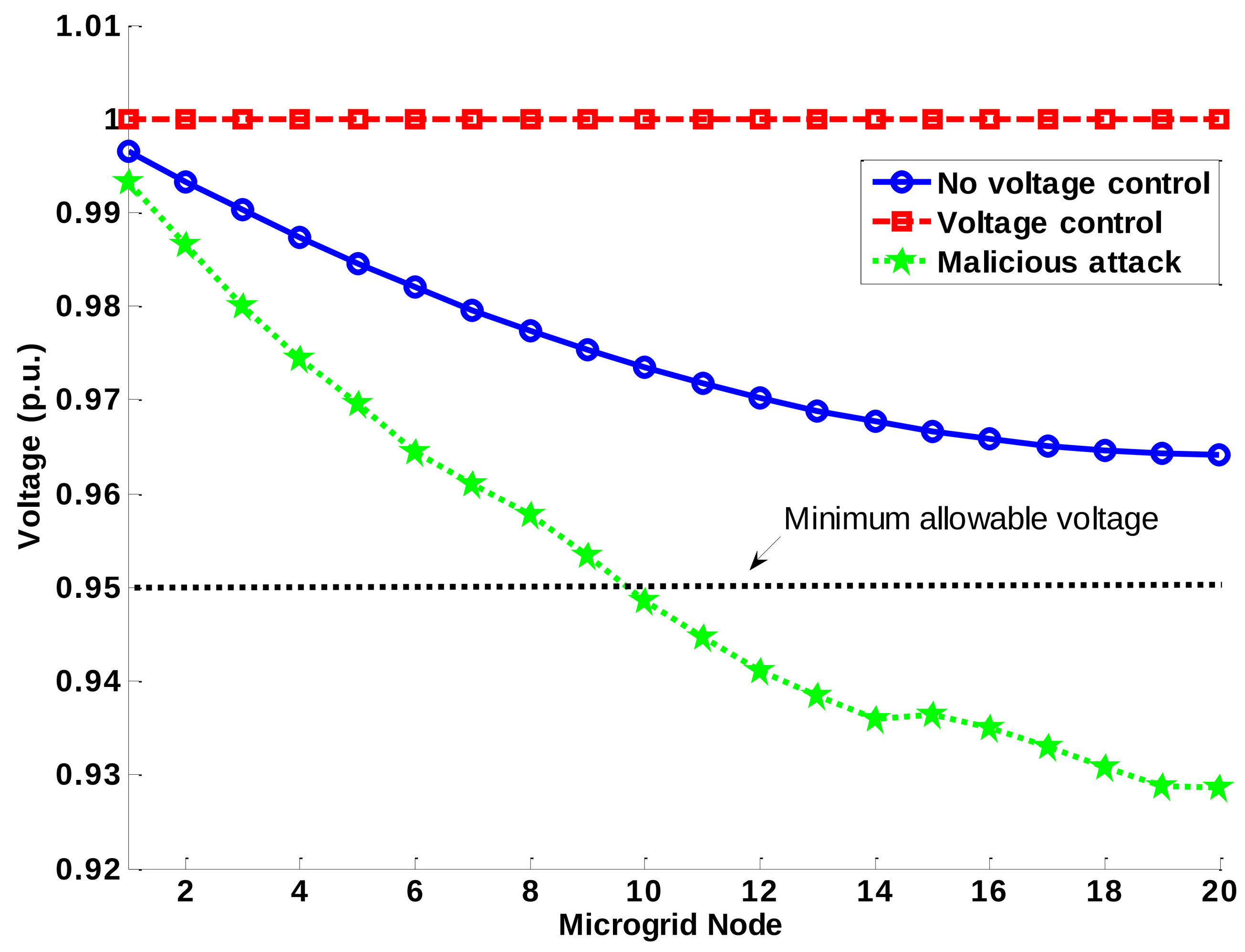
- Microgrid power flow is modeled as

$$-\mathbf{MP} = \mathbf{p}$$
$$-\mathbf{MQ} = \mathbf{q}$$
$$\mathbf{M}^T\mathbf{v} + \mathbf{m}_0 = \mathbf{D}_r\mathbf{P} + \mathbf{D}_x\mathbf{Q}$$

Malicious data attack

where **M** and $\mathbf{m_0}$ are from the graph incident matrix, **P** (**Q**) represents the real (reactive) power flow across lines, **p** (**q**) is the nodal real (reactive) power injection, and **v** is the nodal voltage.

- The goal is to keep the voltage at unity (1 p.u.).
- We assume that the line flow measurements are attacked via malicious data injections.
- The centralized controller requests the reactive power injection of each DER based on the malicious line flow measurements.



BROADER IMPACT

- Permit “plug and play” for microgrid assets.
- Improve system energy efficiency and reliability.
- Provide enabling technologies for grid independence to end-user sites.
- Mitigate economic impacts of power disruption.

INTERACTION WITH OTHER PROJECTS

- Industry interest in standard-based microgrid interoperability.
- The proposed activity involves hardware-in-the-loop simulation using the testbed currently used by UI and ABB on a current project examining collaborative cyber defense in IEC 61850 protection systems.

FUTURE EFFORTS

- Build a cyber-physical optimization framework that comprehends a collection of assets, their capabilities, and requirements.
- Design models for optimal operation and dynamic reconfiguration in response to cyber events or adverse conditions.
- Design tools for monitoring and control of microgrid to detect and prevent cyber intrusions.
- Develop robust control schemes in response to cyber intrusions to maintain reliable and economic microgrid operations.
- Rigorous testing using real and virtual components and RTDS models under a high-fidelity simulation environment, with the ability to inject cyber attacks.
- Conduct a field validation of the developed concepts.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY