U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Multi-layered Resilient Microgrid Networks

ABB Inc.

Dmitry Ishchenko

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

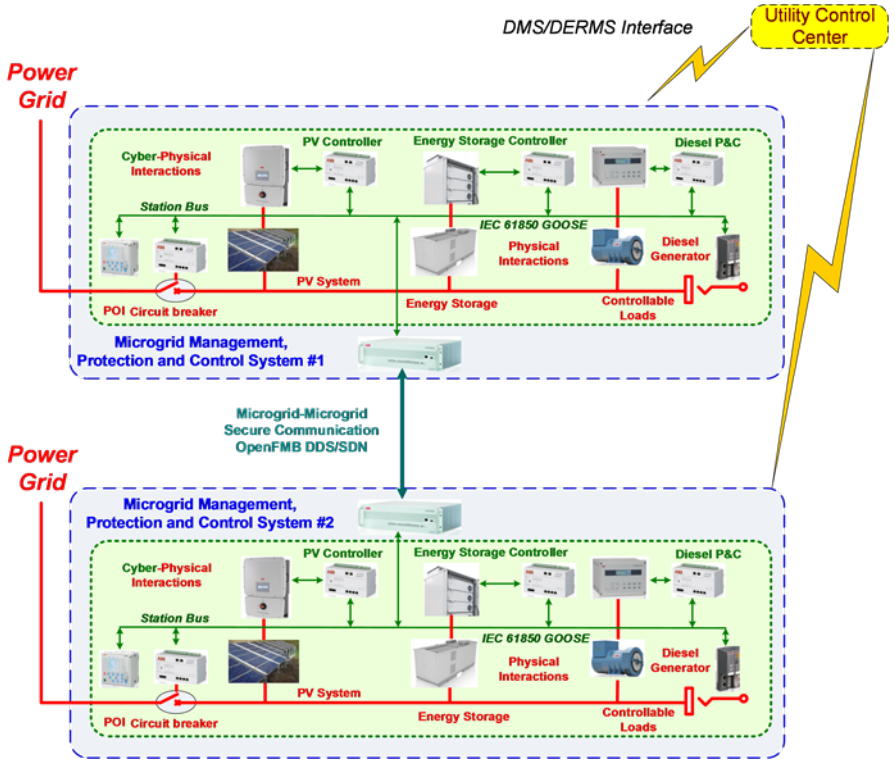
Summary: Multi-layered Resilient Microgrid Networks

Objective

- Research, develop, and demonstrate cyber-physical resilient control and protection architecture for a multi-microgrid power system

Schedule

- 10/2016-10/2019
  - Threat analysis - Done
  - Control and communication architectures design and lab-scale implementation - Done
- Capability: Cyber secure communication and control platform supporting a heterogeneous ecosystem of microgrids, with connections to both utility and peer microgrids



Total Value of Award:	**$ 3,098,964**
Funds Expended to Date:	**52.1%**
Performer:	**ABB Inc.**
Partners:	**University of Illinois, Duke Energy**

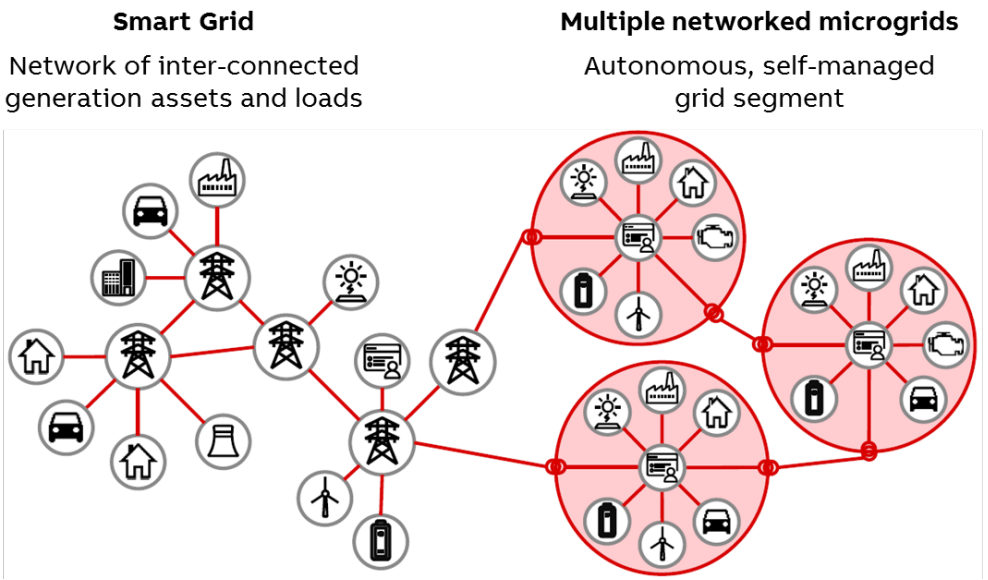
Advancing the State of the Art (SOA)

- **SOA solutions are mostly associated with addressing the operational and security challenges of a single microgrid**
- **Our approach extends microgrid P&C and communications to multi-microgrid networks to incorporate an added layer of intelligence at the grid edge**
- **Enable higher DER penetration levels and increased grid resiliency through improved DER asset utilization**
- **We are building on top of open standards (IEC 61850, CIM and OpenFMB) to ensure industry acceptance**

Advancing the State of the Art (SOA)

- **First principle based cyber threat detection and mitigation mechanisms**
- **Respect local microgrid information privacy to address varying microgrid ownership models**
- **Major project use cases and OpenFMB/GOOSE adapters contributed to the community**
- **Leveraging DER assets in multiple microgrids in a coordinated manner helps to increase power grid reliability, resiliency and power quality**

From local benefit to grid support



Challenges to Success

Maintaining local microgrid privacy

- Only exchange state estimates with the neighbor microgrids as opposed to full network model/topology

Heterogeneous communication networks currently deployed

- Flattening communication profiles with OpenFMB/SDN extensions

Algorithm performance must be fast

- Leveraging peer-to-peer publisher subscriber model minimizing the overhead and implementing QoS for various performance classes

Progress to Date

Major Accomplishments

- Derived control and communications architecture based on open industry standards (IEC 61850/CIM/OpenFMB)
- Implemented lab-scale proof of concept prototype for major project use cases
- Control and power real-time hardware in the loop implementation
- Federated real-time co-simulation testbed to support multi-microgrid use cases

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge?
  - Asset owners
  - Utilities
  - Vendors
- What are your plans to gain industry acceptance?
  - Field demonstration with Duke Energy support
  - Providing inputs to IEC/IEEE/OpenFMB Users Groups
  - Information models supporting project use cases released to the community

Next Steps for this Project

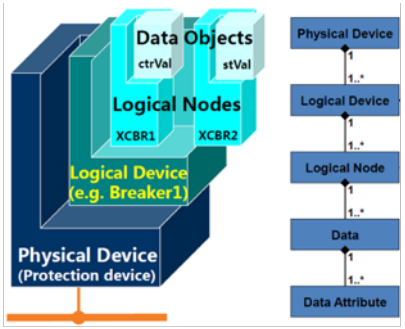
Approach for the next year or to the end of project

- Field demonstration with algorithm tuning as needed in the second quarter of 2019

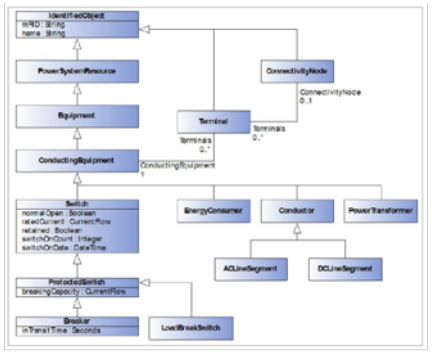
- Dissemination of results through IEEE/IEC/UCAIuG

Ontology Based Threat Modeling

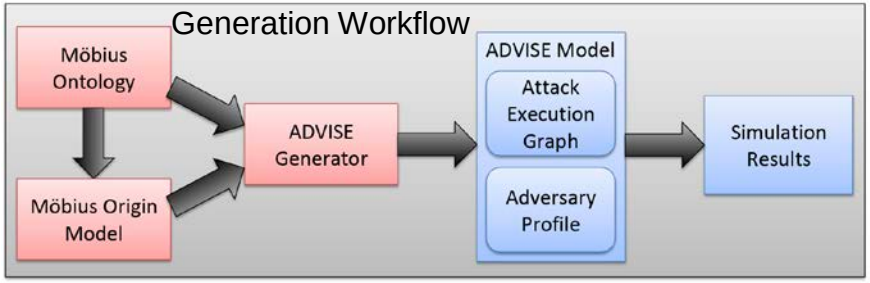
- Ontology defined based on the IEC 61850/CIM/OpenFMB Model
- Extend adversary modeling framework ADVISE to comprehend cyber-physical aspects
- Automatic generation of attack execution graphs from block diagram system definition (Mobius Origin Model)
- Identify critical components (those on multiple critical attack paths)
- Can be a basis for mitigation strategy

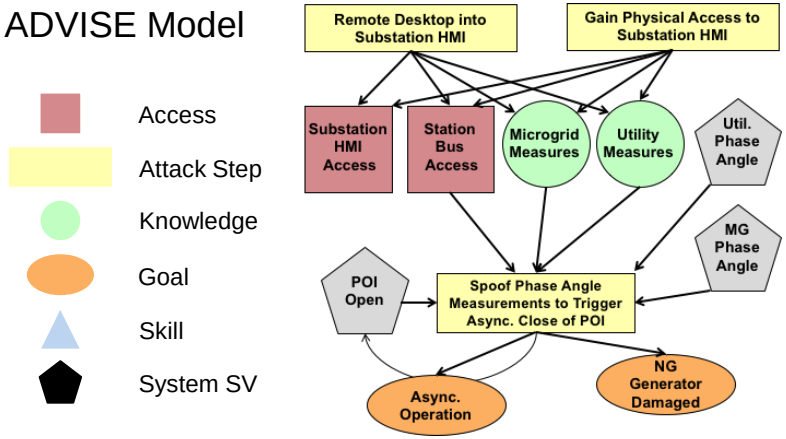


IEC 61850: Object model for devices and functions, Spec for inter-device communications, Extensions for DER



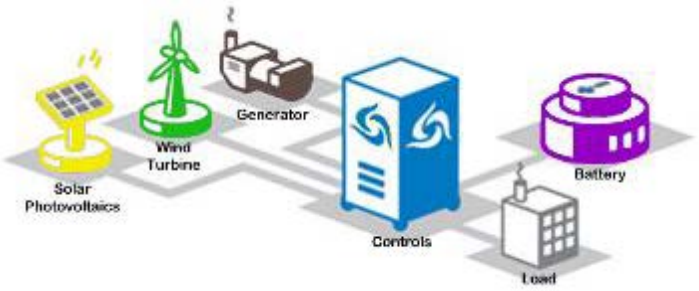
Common Information Model Primer, EPRI 2015 Technical Report

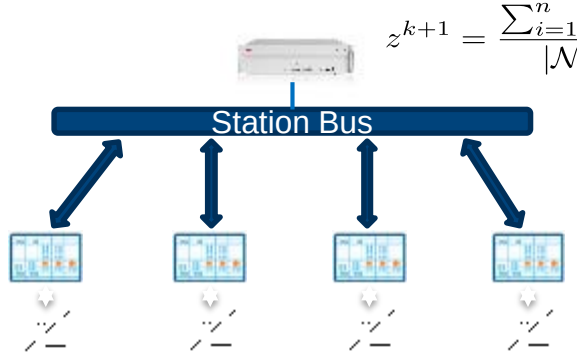




Frequency Control and Reachability Analysis

- Challenges in maintaining microgrid frequency stability
  - Scarce generation resources
  - Varying renewable energy generation
  - Low physical inertia for frequency damping
  - Solution: distributed secondary frequency control based on local measurements, robust against link failure and attack



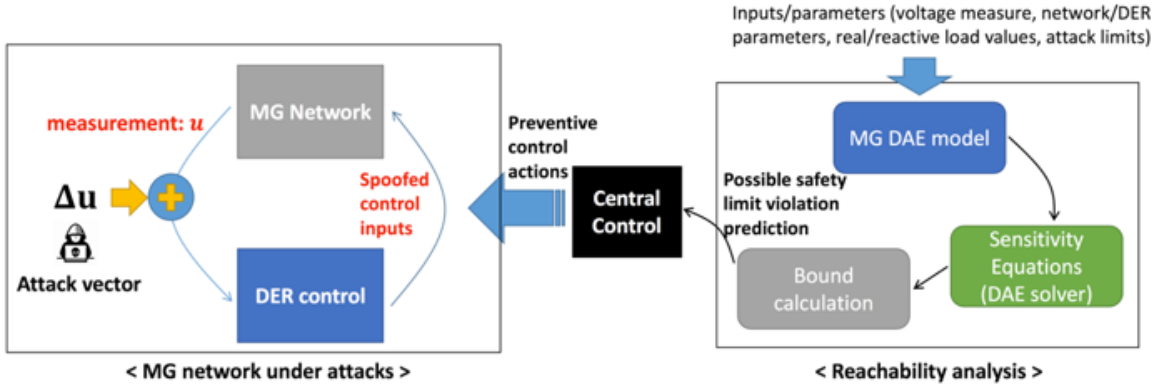


$$z^{k+1} = \frac{\sum_{i=1}^{n} x_i^{k+1}}{|\mathcal{N}_D|} \quad (2)$$

$$x_i^{k+1} = \frac{\rho z^k + D_i c_i^k - \lambda_i^k}{D_i + \rho} \quad (1)$$

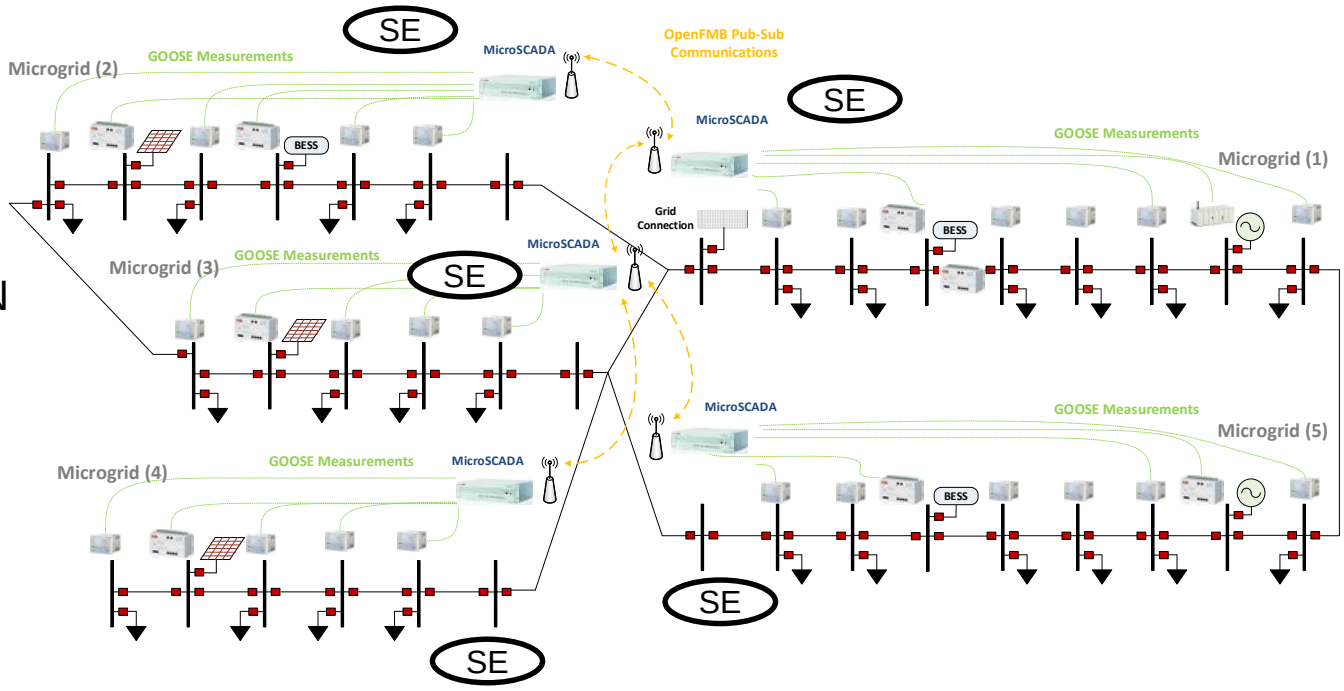
$$\lambda_i^{k+1} = \lambda_i^k + \rho(x_i^{k+1} - z^{k+1}) \quad (3)$$

- Reachability Analysis
  - Find envelope on the solution trajectories for all possible parameter/input variations due to spoofed measurement/control



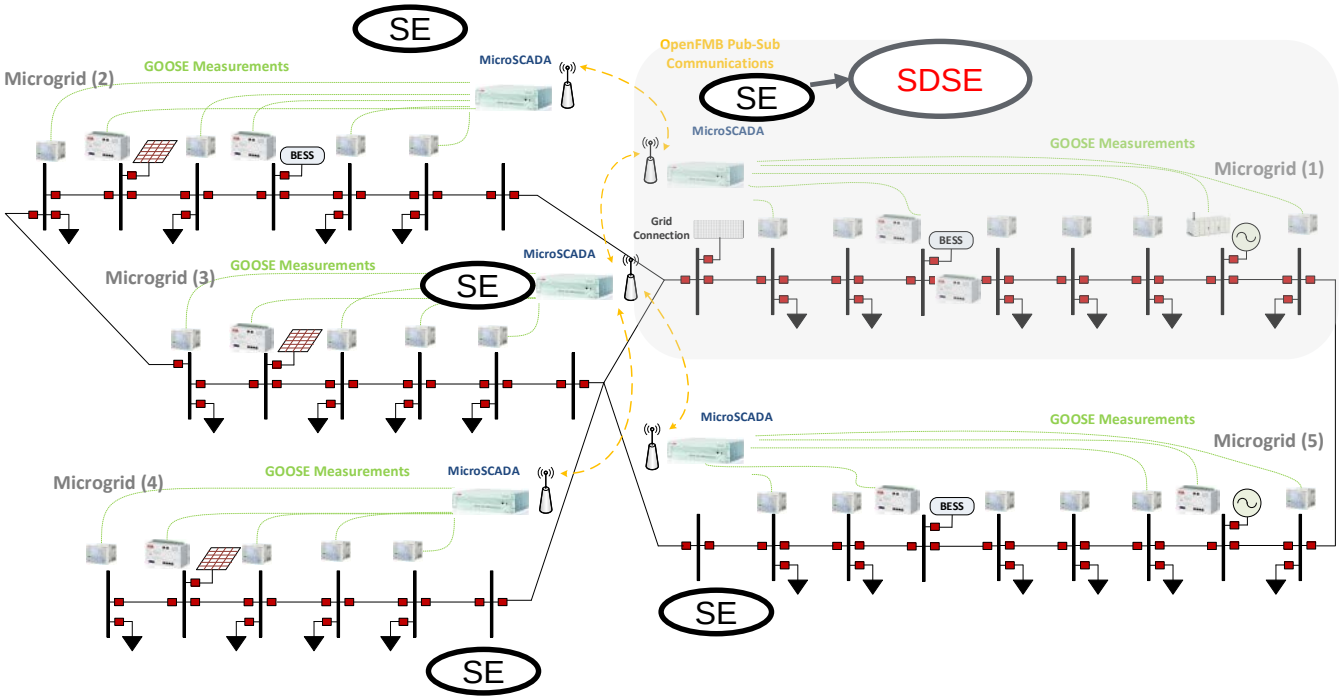
Secure Distributed State Estimation

- Communications within microgrid: IEC 61850 GOOSE
- Microgrid-to-microgrid communication with OpenFMB/DDS with SDN extension
- Supervisory microgrid controller (MicroSCADA/COM600) implements
  - Secure Distributed SE
- State estimation as input into Microgrid EMS and other functions



Secure Distributed State Estimation

- Secure DSE detects cyber issue in Microgrid 1
- Isolate Microgrid 1 from the rest of the system with SDN and (optionally) physically disconnect



U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Thank You!

Questions?