Multi-layered Resilient Microgrid Networks: Final Technical Report

Principal Investigator: Dmitry Ishchenko
ABB Power Grids Research.

US Corporate Research Center
Raleigh, NC 27606, USA

Project Participants:
University of Illinois at Urbana-Champaign
Duke Energy

December 2019

DOE CEDS
Award Number DE-OE0000831
Final Project Report OSTI ID:1786363

Acknowledgment: The work described here was performed with funding from the Department of Energy (DOE) under Cooperative Agreement DE-OE0000831. The views expressed are those of the authors. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

TABLE OF CONTENTS

SUMMARY

Distribution grid resilience, especially when the grid is under high penetration of Distributed Energy Resources (DER), e.g. PV and energy storage, is essential to ensure the quality of electric power services. The resiliency aspect is particularly important for critical loads that typically include hospitals, police/fire stations, and national security facilities. Networks of multiple interconnected reconfigurable microgrids help to increase renewable energy penetration and may be used as basic building blocks for implementing future resilient power grids. However, this integration requires additional layers of communications, both horizontal and vertical, which may substantially increase the potential cyber attack surfaces as well as escalate risks for wide-spread malfunctions of automation systems.

The Mulit-layered Resilient Microgrid Networks project is an industry-academic collaboration between ABB, Duke Energy and the University of Illinois at Urbana-Champaign (UIUC) that has developed and demonstrated a cyber-physical resilient control and communication architecture for deployment of multiple microgrid networks, as well as retrofitting the existing distribution grids by increasing DER penetration levels.

1 INTRODUCTION

Microgrids are increasingly adopted as an integral component of electric power grids as a framework to integrate DER. The present focus in microgrids research and development is associated with addressing the operational challenges of DER and energy efficiency resources (such as CHP) integration, including support for seamless transitions from grid-connected mode to islanded and back without blackouts, and ensuring safety for the public and utility personnel in all modes and during transitions. Additionally, microgrids are often seen as a way of providing enhanced grid resilience services, particularly considering the aftermath of natural events such as hurricanes and storms.

Operational optimization of multiple microgrids is often considered to be the next step in microgrid technology evolution. It is anticipated that multiple microgrids with significant renewable energy penetration will be used to implement future resilient power grids, such as grids in Smart Cities. However, this integration requires additional layers of communications, both horizontal and vertical, which may substantially increase the potential cyber-attack surfaces as well as risks of wide-spread malfunctions of automation systems.

Traditional approaches to power system control algorithm design decouple power systems/control and communications/IT domains, and this decoupling often affects the algorithm performance and accuracy. We have researched, conceptualized, and demonstrated a comprehensive cyber-physical multi-microgrid system design that incorporates a multiple-layer power system control, communication and operation architecture using the overall system resiliency and safety as key operational constraints. The system provides the framework for integrating distributed generation and storage in multiple microgrids and is resilient to false data injection cyber-attacks.

The work conducted in this project has been focused on networked microgrids secure control and communications architecture using IEC 61850 and OpenFMB for improved interoperability. We have also researched, developed and implemented the first principle-based attack mitigation strategies that go beyond the traditional IT measures and utilize the inherent physical properties of energy delivery systems to overcome barriers to DER integration from the perspective of availability, security, and stability. Such strategies are essential to realize the potential benefits of large-scale DER integration and networked microgrids. The use cases presented in this report are secure distributed state estimation, secure secondary frequency control, and secure microgrid interoperability to supply critical loads. The proposed concepts have been validated through real-time hardware-in-the-loop testing and demonstration at Duke Energy's Mt. Holly microgrid laboratory.

This report presents a summary of the methodology developed, the implementation and demonstrations performed as part of technology transfer phase of the project. For more details please refer to the previously submitted technical and milestone reports.

2 PROJECT OBJECTIVES

The project targeted to develop an architecture with various layers in the communication and control network to monitor and control a multi-microgrid system, detect and respond to varying load requirements, monitor adverse events, and identify indications of cyber-attack or compromise. The system should support an ecosystem of cooperating but autonomous microgrids to enable flexible response to a natural disaster or cyber event by maintaining critical loads. The architecture enables information exchange between microgrids at varying degrees of granularity across points of cyber and physical coupling.

The project has developed a secure and layered communication architecture and functions to integrate multiple microgrids into a modern advanced Distribution Management System (DMS). A threat analysis has been performed to understand potential impacts to microgrid operations and identify accompanying mitigation strategies. We have employed distributed state estimation (DSE) principles to detect and defend against attacks by forecasting the impact of a pending control action, assessing if an action is a legitimate control command or adversarial command, and ignoring or overriding commands, as appropriate. DSE will be implemented as part of each microgrid's energy management controller to optimize microgrid performance, resilience, and interactions between multiple microgrids.

The project has developed robust control for stable transient operation that has the capability to consider various attack scenarios and defend against such attacks.

The following sections provide a brief description for the algorithms and methodologies developed in the project.

All project goals have been achieved as demonstrated in the final project demonstration at Duke Energy Mt. Holly microgrid laboratory.

3 CONTROL AND COMMUNICATION ARCHITECTURE

The conceptual diagram for a multi-microgrid system that enables coordinated control through aggregation and integration of multiple microgrids and provides an interface into utility Distribution Management Systems (DMS)/ DER Management System (DERMS) built on top of open standards is shown in Figure 1.

The example system shown in consists of two Medium Voltage microgrids connected to two distribution substations in normally open loop configuration. Note that for simplicity the DER step-up transformers and protection relays are not shown in this figure. Each DER asset in a microgrid is controlled by a supervisory controller used to implement the distributed microgrid control system functionality referred to as e-mesh Control, which is resilient to failure of a single DER/controller. The e-mesh Control distributed control system implements the core individual microgrid management functions including DER dispatch, power sharing, intermittency and spinning reserve support, load management, and protection coordination, as well as the other microgrid requirements. In this setup the e-mesh component controllers of Figure1 are polling the primary DER controllers with Modbus, run their respective control algorithms and share the information with each other via fast peer-to-peer communications using IEC 61850 GOOSE messaging. The e-mesh SCADA supervisory system is used for data logging, HMI and interface to the utility.

For intra-microgrid communications the individual microgrid control systems exchange information with the neighboring microgrid control system through secure 4G LTE wireless gateways with VPN capability using OpenFMB with Data Distribution Service (DDS) publisher-subscriber mechanism [4].

The individual microgrid communication networks can be dynamically partitioned as needed by using the Software Defined Networking (SDN) technology. In case of an electrically connected microgrid clusters the microgrids may operate on the same communications subnetwork, otherwise they will be operated on different subnetworks with the ability to re-compose the communication network as needed to accommodate for instance distribution network reconfiguration. This architecture adopts the IEC Technical Committee 57 Working Group 17 DER integration architecture and implements OpenFMB extensions for Microgrid-to-Microgrid communications.

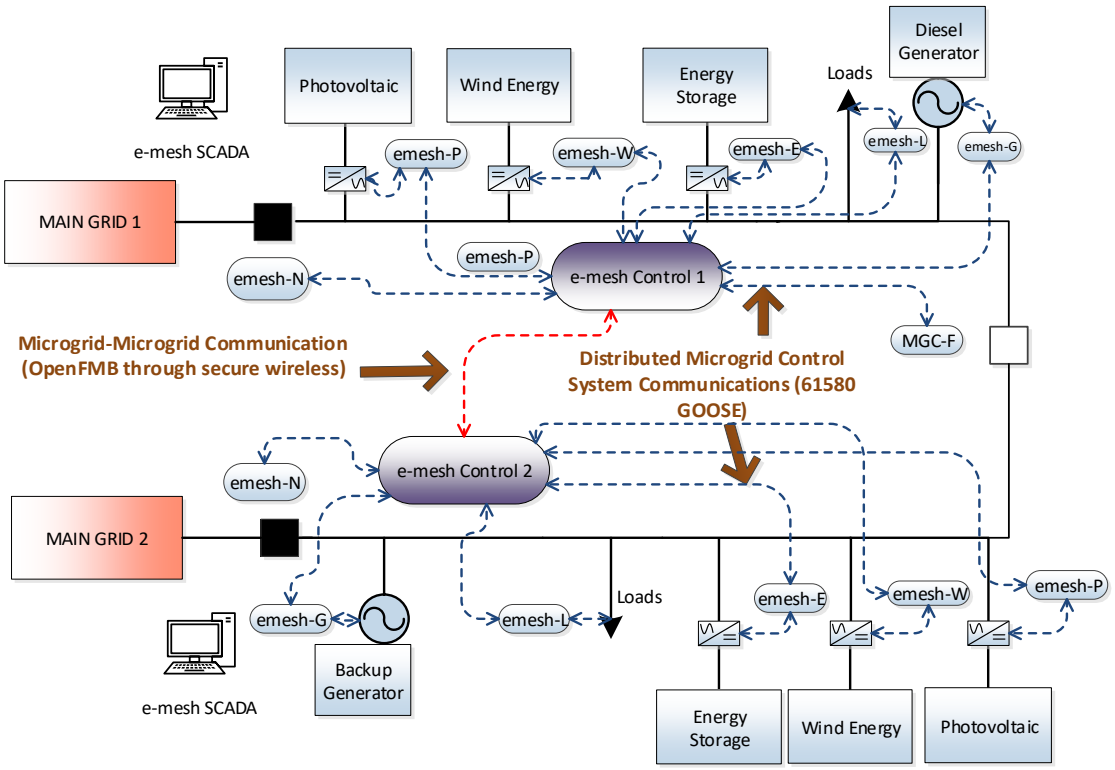


Figure 1 – Multi-layered Resilient Microgrid Network.

Secure microgrid-to-microgrid communications are required to enable microgrid self-healing functions for increased system resiliency, as well as implement compromised agent isolation functionalities. In terms of the information models, the individual microgrid controllers implement the semantic models of IEC 61850 and OpenFMB, which are based on the IEC 61850 and Common Information Model data semantics. Mapping of IEC 61850 GOOSE messages to OpenFMB/DDS for microgrid-to-microgrid communications is performed with the IEC 61850 GOOSE-to-OpenFMB adapter developed by Duke Energy, or alternatively directly at the application layer.

Building on top of OpenFMB/DDS allows for implementation of the advanced multi-microgrid use cases. For instance, in case of an internal fault in one of the microgrids the distributed microgrid control system can identify the fault location, isolate the faulted segment, and reconfigure the system as needed to minimize the outage effect including both physical and cyber networks. Additionally, in case one microgrid is compromised by a cyber-attack, the system will be able to identify the intrusion and isolate the compromised microgrid from the rest of the network.

4 IEC 61850 AND OPENFMB MODELING

The manufacturers of DER devices traditionally have applied traditional point-based utility communications protocols, e.g. Sunspec Modbus, IEC 60870-5-104 or DNP3. However,

as utilities, aggregators, and other energy service providers start to manage large number of DER devices interconnected with the power grid, different communication technologies may present major technical difficulties, associated with implementation and maintenance costs. Additionally, point based protocols do not include any semantic information, making integration of products from multiple vendors more difficult. Consequently, the need to have a standard that defines semantics-based communication and control interfaces for all DER devices led to the development of the IEC 61850-7-420 standard [1]. This standard defines new IEC 61850 information models that can be used in the exchange of information among controllers of distributed energy resources.

The IEC 61850 semantic model uses the concepts of logical nodes, which are essentially container classes that hold the data relating to one device or function. The semantic models representing DER include Logical Nodes for generation, storage and loads. Generation devices are further classified as photovoltaics, combined heat and power (CHP), reciprocating engines, and fuel cells. The Logical Nodes related to energy storage systems are defined in detail in IEC 61850-90-9 [5]. The IEC 61850-7-420 information model utilizes UML modeling approach and builds on top of the existing IEC 61850-7-4 logical nodes where possible, and also defines DER specific logical nodes as required for the new use cases. This also provides a convenient mechanism for asset self-description through standard data objects, e.g. state of charge of the battery, capability curves and ramp rates of the generators. Figure 2 shows the abstract DER Logical Node class for a DER system. More details can be found in [1].

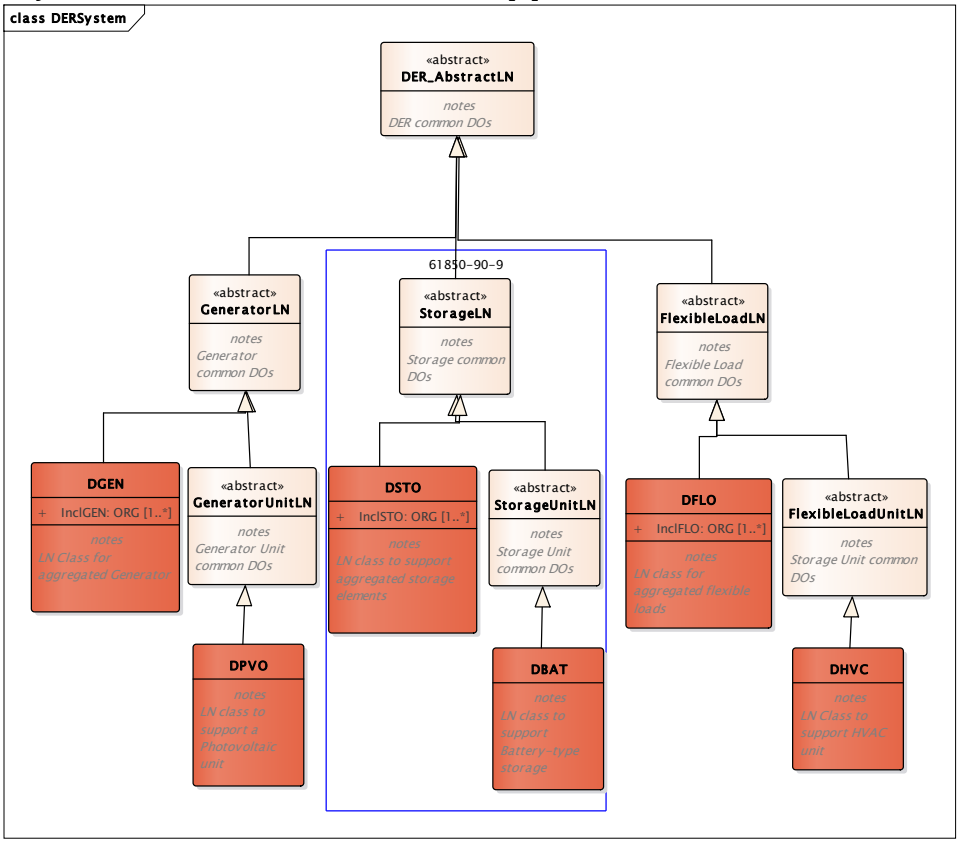


Figure 2 – DER Abstract Logical Node Class [1].

While the semantic models for core power system functions as well as DER extensions are offered by IEC 61850 [1], the OpenFMB [3] framework offers an attractive way to enable peer-to-peer field interoperability particularly when interconnecting heterogeneous communication networks. OpenFMB is an architectural framework for distributed intelligent nodes interacting with each other through loosely coupled, publisher-subscriber messaging for field devices and grid edge systems. OpenFMB Node architecture shown in Figure 3 is composed of the application/adapter, interface, and a middleware layer. OpenFMB Applications support grid functions by analyzing data and requesting appropriate actions as needed in the specific use case. OpenFMB Adapters interface the field message bus with end devices and provide uni-directional or bi-directional exchange of information between data profiles and other protocols and conventional formats, e.g. DNP3, Modbus, IEC 61850 GOOSE, C12, XMPP, or others.

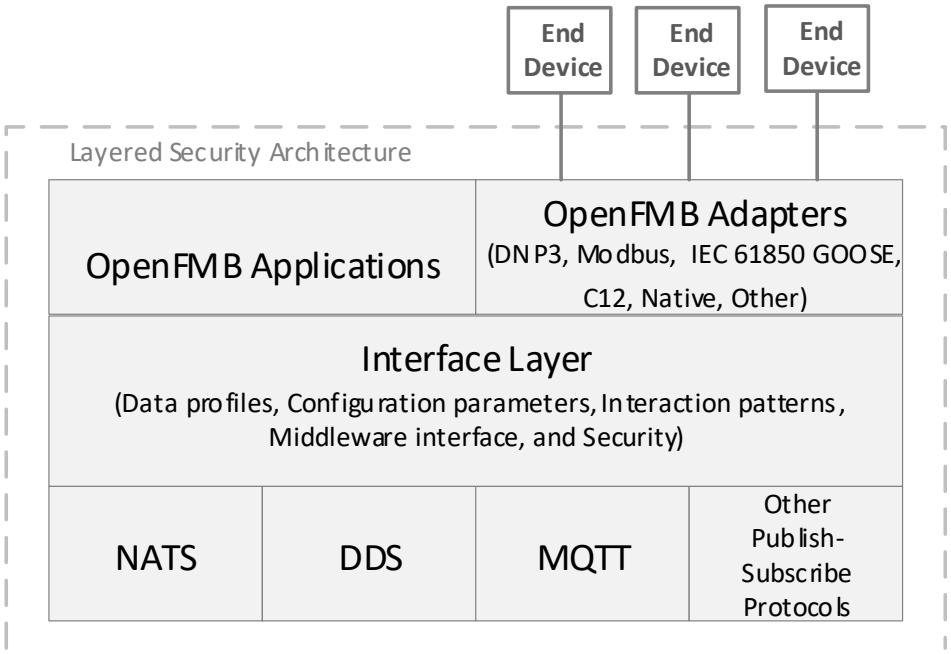


Figure 3 – OpenFMB Operational Logical Architecture[3].

The OpenFMB data model is built on top of the semantic models of IEC 61850 and the IEC 61968/61970 Common Information Model (CIM) components. For instance, Figure 4 shows the OpenFMB profile for discrete breaker control. It is built with the standard IEC 61850 XCBR circuit breaker logical node with the attached master resource identifier (mRID) tags that allow to create unique identifiers for each object.

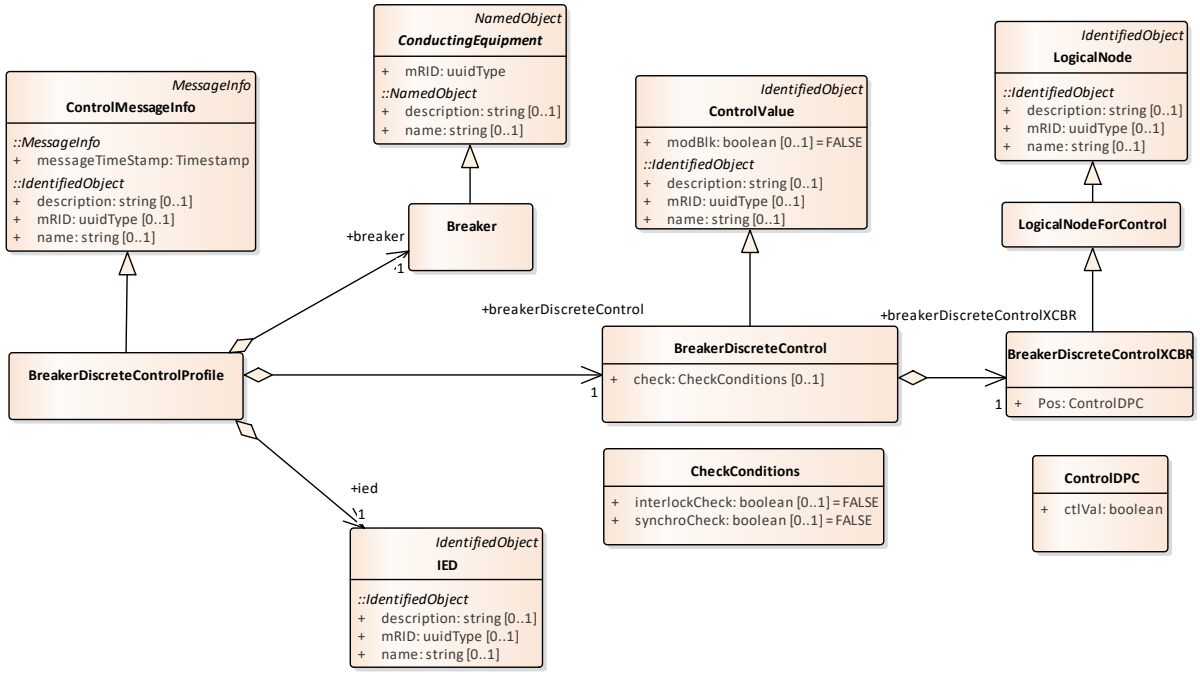


Figure 4 – OpenFMB Breaker Discrete Control Profile.

It also inherits ConductingEquipment class from CIM that allows the breaker status information to be associated with a specific piece of equipment in the system. This capability is very important for mapping the IEC 61850 field data to network topology, particularly for multi-microgrid management functionality when the network topology changes dynamically, as with self-healing, reconfiguration and other use cases supporting resiliency.

All project use cases have been developed, implemented and demonstrated within this framework as described in the following sections.

5 SECURE DISTRIBUTED STATE ESTIMATION

Distributed State Estimation is the key feature of the proposed microgrid networks control system architecture. In this concept each microgrid has detailed view of its own state and estimates of neighboring microgrid states. The cyber-resilient distributed algorithm with built-in anomaly detection engine uses the adaptive diffusion strategy and is designed so that a compromised agent (in this case a microgrid) will be collectively detected by the rest of the microgrids. The developed control algorithms can also be used to isolate the individual components within microgrids, as well as severe the electrical connection to fully isolate compromised part of the system both from cyber and physical perspectives.

The secure distributed state estimation implements a distributed bi-level algorithm to achieve global state of the networked microgrids, while respecting local information policy and privacy. In this context respecting privacy refers to each microgrid knowing only its own measurements.

The implementation can be summarized as follows with more details provided in [6]:

- The first step is to calculate the local estimates in each microgrid. This is done with the weighted least square method using conventional measurements.
- Second, each microgrid initializes the global estimate vector that corresponds to the total number of stats in the entire network and includes the information regarding the local states estimated in step one.
- Peer-to-peer communication is established as per publish/subscribe topology.
- Peer neighboring microgrids apply diffusion strategy based on iterative publisher-subscriber information exchange.
- Distributed state estimation algorithm runs collaboratively until an acceptable precision of convergence is achieved.
- If any threat is detected while converging, the agents switch to malicious node detection and isolation process.

Under normal operating conditions, the communication among microgrid agents is defined to use optimal and fixed trust policy. Normally the assigned weights are directly related to the connection degree of the agents. To detect and isolate the misbehaving node, the agents must switch to the adaptive combination policy, which allows the agent to adapt their combination coefficients in order to exclude misbehaving nodes from the network.

The adaptive trust policy developed in secure distributed state estimation algorithm is a modification of the optimal policy and has the ability of networks to detect a misbehaving node by creating on-the-fly network clusters. Fundamentally, the agents cut links of the neighbors if trust index falls behind a predefined threshold.

Although the adaptive combination policy provides the ability to detect misbehaving nodes, convergence precision may not be sufficient as achieved by the optimal policy. It is imperative to balance trade-off between two conditions: (1) optimal combination policy; and (2) fully adaptive policy. To overcome this problem, we have implemented an adaptive solution which enables a switching mechanism between optimal and adaptive policies.

6 SECURE MICROGRID INTEROPERABILITY

UIUC examined a use case consisting of two microgrids connected by a normally open tie line. Within the first microgrid, there is a main microgrid bus with several DER and loads, and a critical load bus with a DER and a critical load (for simplicity, microgrid 2 has similar topology, but this is not required). This is shown in Figure 5, which may be considered a simplified variant of the system in Figure 1 above.

The operation of the use case begins with a detection of a possible attack on the voltage measurement at the energy storage system (ESS) on the critical load bus of microgrid 1. The detection may be via a Kirchhoff-law distributed agreement algorithm developed in [7] or via reachability analysis that uses sampling from off-line simulated trajectories based on dynamical system analysis and determines that an adverse state is “reachable” with unacceptably high probability [8]. Detection is shown as step 2 in the figure. This leads to tripping of the ESS, which may lead to instability if the remaining generation cannot supply the loads.

At this point, the e-mesh controller in the first microgrid signals its peer in the second microgrid over the communication link, and the two agree to close the normally-open tie line. At present, this is done as a request from e-mesh 1 to e-mesh 2. The future implementation will invoke a secure distributed algorithm similar to the distributed state estimation which will result in secure agreement between the two e-mesh controllers that the tie line should close. The tie line beaker is shown as red in the figure to indicate that it has been closed.

Closing the tie line provides power to the critical load in microgrid 1, but the frequency will be unstable. Therefore, a secondary distributed stabilization algorithm is executed to restore stability of the entire system, which is now electrically connected. The algorithm uses alternating direction method of multipliers (ADMM) to compute per-unit power injections at each DER controller in order to stabilize frequency. Since the system may be under cyber attack and some DER may report malicious measurements, there is a "round robin" (RR) procedure whereby the DER agree on a consensus variable (the power injection, expressed per-unit) via polling the DER in each round. We have shown that the malicious DER is identified in a single round. The entire algorithm is referred to as "RR-ADMM" [9], [10].

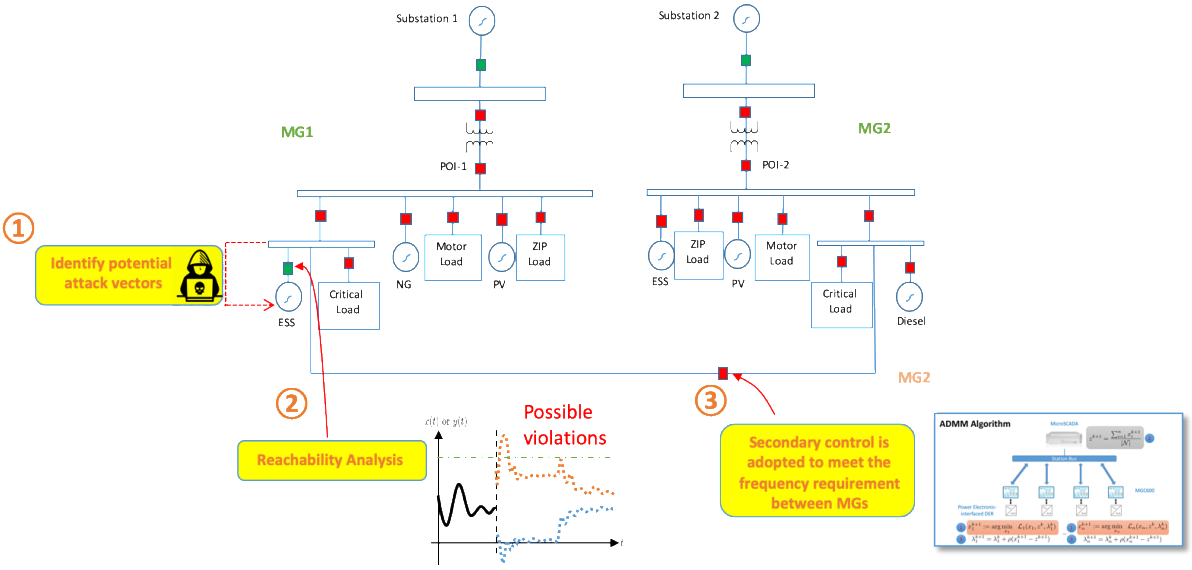


Figure 5 – Secure Microgrid Interoperability

Communications within each microgrid use IEC 61850 GOOSE messages. Communications between e-mesh controllers is over OpenFMB-DDS over a SDN infrastructure. When fully implemented, the SDN functionality will permit isolation of malicious nodes from the communication framework.

7 TESTING AND DEMONSTRATION

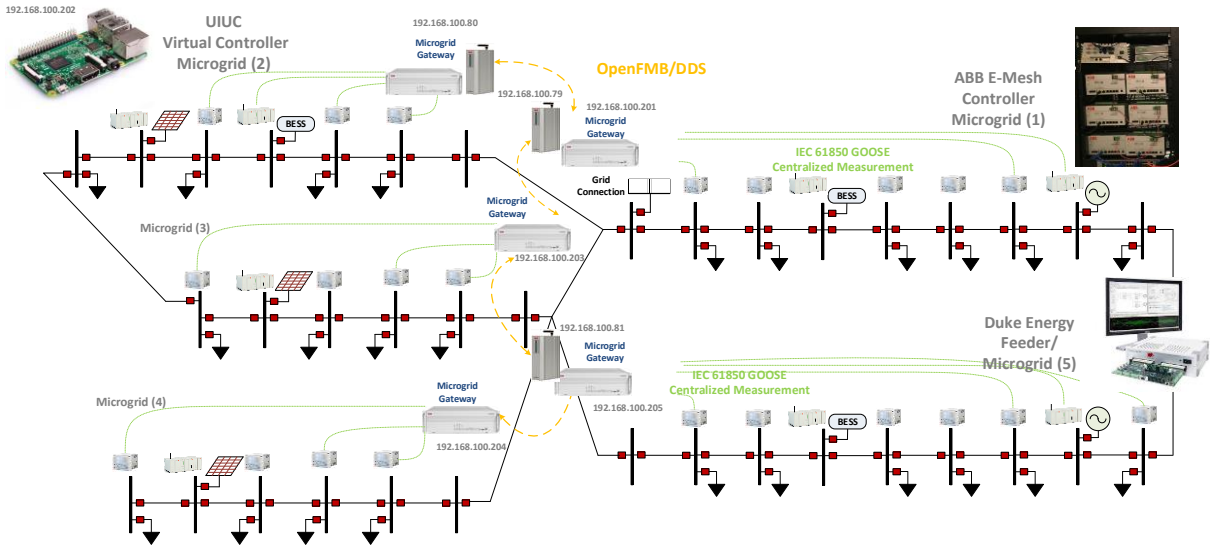
For implementation, testing and demonstration of the microgrid-to-microgrid interoperability and secure distributed state estimation functions, a system consisting of five medium voltage microgrids was created, as shown in Figure 5. In this network the

distributed microgrid control system with fully implemented e-mesh Control and SCADA functionality with a simplified power system dynamics simulator was connected through 4G LTE wireless gateway to Duke Energy's medium voltage feeder microgrid model. This model was running on Typhoon real-time digital simulation platform with integrated energy storage controller board. Another microgrid was represented as a virtual controller at the University of Illinois laboratory in Urbana-Champaign, IL. As mentioned previously mentioned the internal microgrid communications were done with IEC 61850 GOOSE, while microgrid-to microgrid communications were done with OpenFMB DDS publisher-subscriber mechanism with the data profiles for distributed state estimation created in the OpenFMB format.

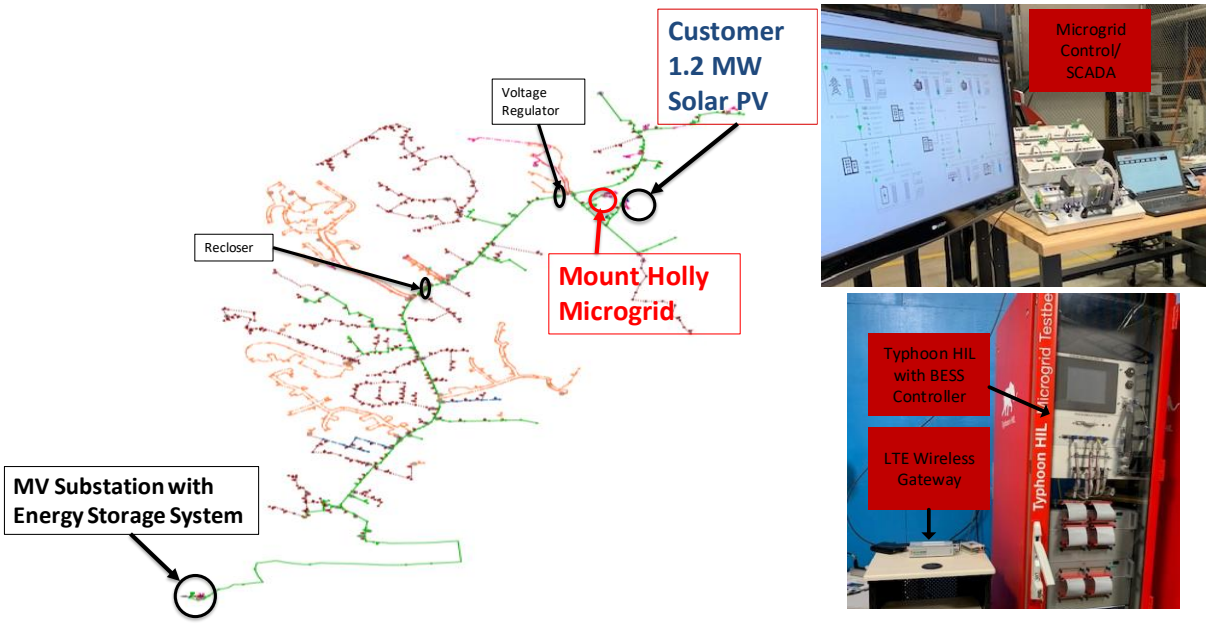
The description of the test cases implemented, and the logic steps performed for each case is provided in Figure 7. The figure shows voltage magnitude and angle for one of the buses in Microgrid 1 of Figure 6. The DSE algorithm is designed to run continuously with one-minute interval.

After the initialization under the normal operating conditions the algorithm successfully converges. In the second iteration, a false data injection attack is on state estimation values by Microgrid 4 is performed by adding the 10% bias to its published state. Once the attack is initiated the individual agent estimates begin to deviate from each other. As soon as the cumulative error goes beyond a pre-determined threshold, the misbehaving node detection mechanism is activated and the agents are switched to the adaptive trust policy, which then detects and isolates the attack.

The rest of the agents collaboratively detect the intrusion and isolate the misbehaving agent. After that round 3 runs by excluding the misbehaving agent node, which has only 4 microgrids in this case. Then rest of the rounds, all agent reunion again and the DSE operation continues to run.



a) Five Microgrid Network



b) Duke Energy MV Feeder HIL integration through wireless gateway

Figure 6 – Demonstration Setup.

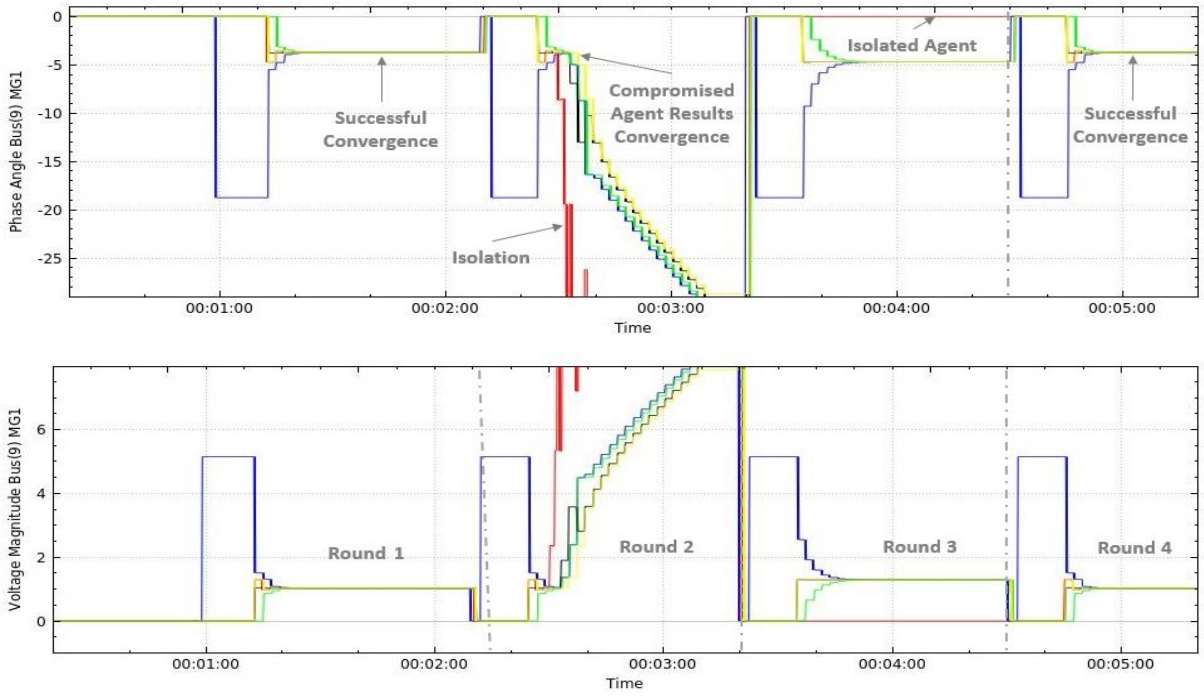


Figure 7 – Real-time demonstration results.

8 PROJECST OUTPUTS

A. Papers

D. Ishchenko, A. Kondabathini, M. Cintuglu A. Brissette, A. Valdes, R. Macwan, H.J. Liu, S. Laval and D. Lawrence “Cyber-physical Resilient Interoperable Microgrid Networks,” accepted for publication at CIGRE Symposium, Paris, France, September 2020. OSTI ID:1797435

M. Cintuglu and D. Ishchenko “Secure Distributed State Estimation for Networked Microgrids,” *IEEE Internet of Things Journal*, Vol. 6 Issue 5, October 2019. OSTI ID:1797440

A. Kondabathini, D. Ishchenko, M. Fillippone, and A. Brissette “Implementation and Evaluation of IEC 61850-based Distributed Control System for Microgrid Applications, 2019 PACWorld Americas Conference, Raleigh, August 2019. OSTI ID:1797441

D. Ishchenko, A. Kondabathini, J. Hong, A. Brissette and M. Cintuglu, “Nested Microgrids for Increased Grid Resiliency,” 2018 PACWorld Americas Conference, Raleigh, August 2018. OSTI ID:1797442

H.J. Liu, L.Y Lu, Z. Wu, and A. Valdes “Distributed Optimization Approach for Frequency Control with Emulated Virtual Inertia in Islanded Microgrids,” 2018 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Singapore, May 2018.

H. J. Liu, H. Choi, P. Buason, and A. Valdes. “Probabilistic Bounds on the Impact of Potential Data Integrity Attacks in Microgrids,” Hawaii International Conference on System Sciences (HICSS 2018), January 2018.

H. J. Liu, M. Backes, R. Macwan, and A. Valdes, “Coordination of DERs in microgrids with cybersecure resilient decentralized secondary frequency control,” in *Proc. Hawaii International Conference on System Sciences*, 2018. [Online]. Available: http://hdl.handle.net/10125/50226

B. Demonstrations

The project team made several demonstrations as part of technology transfer phase at the following events:

- Innovative Smart Grid Technologies Conference, Washington DC February 2019.
- Microgrid 2019 Conference, San Diego, CA May 2019.
- CREDC Summer School, St. Charles, IL, June 2019.
- OpenFMB PlugFest, Charlotte NC, September 2019.
- Final project demonstration, Mt. Holly, NC, October 2019.

C. Patent Applications

M. Cintuglu, and D. Ishchenko “Security of Distributed State Estimation for Networked Microgrids,” Application No. 16/142,103, Filed on September 26, 2018. S-149,148

J. Hong, D. Ishchenko, and R. Nuqui “Cyber attack resilient layered state estimation and secured control for multi-microgrids operation,” Application No. 16/147,979, Filed on October 1, 2018. S-149,146

D. Networks/Collaborations Fostered

The project use cases have been presented at several OpenFMB Users Group meetings and the project team participated in OpenFMB Plugfest in Charlotte, NC in September 2019.

9 CONCLUSIONS

Microgrid networks are targeted to simplify utility operation by bringing the grid management intelligence closer to the grid edge and enhance overall grid resilience by extending the duration of electrical service to critical loads during extreme event outages.

The project has developed introduced the architectural framework for integrating individual microgrids into microgrid networks. Communication architecture has been designed based on open industry standards IEC 61850 and OpenFMB.

The first-principle based false data injection detection mechanisms developed in controller hardware-in-the-loop testing environment through wireless communications confirm the feasibility of the proposed approach and complement the traditional IT-based intrusion detection systems.

Major project use cases have been implemented with ABB e-mesh microgrid control and SCADA systems and demonstrated in the utility environment at Duke Energy Mount Holly microgrid test facility.

BIBLIOGRAPHY

[1] IEC 61850-7-420: Communication Networks and Systems for Power Utility Automation – Basic Communication Structure – Distributed Energy Resources Logical Nodes, Edition 2.0 (Draft), 2018.

[2] IEC 61970-301, Energy management system application program interface (EMS-API) –Part 301: Common information model (CIM) base, 2016.

[3] Open Field Message Bus (OpenFMB), NAESB Standard, November 22, 2019.

[4] Data Distribution Service Specification http://www.omg.org/spec/DDS/1.4/PDF

[5] IEC 61850-90-9: Communication Networks and Systems for Power Utility Automation – Use of IEC 61850 for Electrical Energy Storage Systems, Edition 1.0 (Draft), 2018.

[6] M. Cintuglu and D. Ishchenko “Secure Distributed State Estimation for Networked Microgrids,” *IEEE Internet of Things Journal*, Vol. 6 Issue 5, October 2019.

[7] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ishchenko, “Collaborative defense against data injection attack in IEC 61850 based smart substations,” in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2016.

[8] H. J. Liu, H. Choi, P. Buason, and A. Valdes. “Probabilistic Bounds on the Impact of Potential Data Integrity Attacks in Microgrids,” Hawaii International Conference on System Sciences (HICSS 2018), January 2018.

[9] H. J. Liu, W. Shi, and H. Zhu, “Distributed voltage control in distribution networks: Online and robust implementations,” *IEEE Trans. Smart Grid*, 2016, (Early Access).

[10] H. J. Liu, M. Backes, R. Macwan, and A. Valdes, “Coordination of DERs in microgrids with cybersecure resilient decentralized secondary frequency control,” in *Proc. Hawaii International Conference on System Sciences*, 2018. [Online]. Available: http://hdl.handle.net/10125/50226