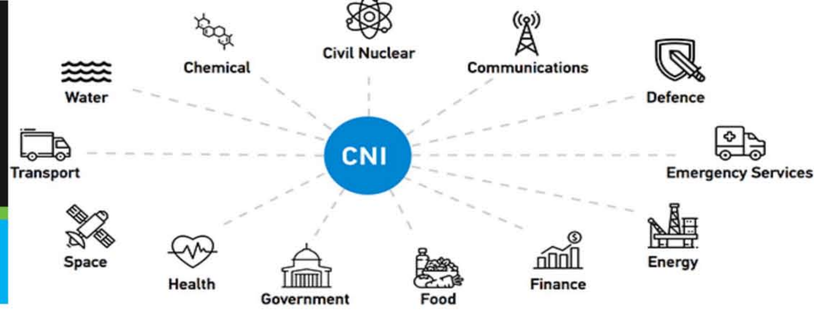
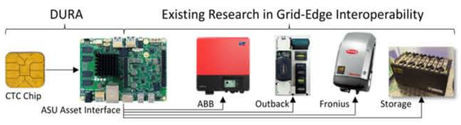
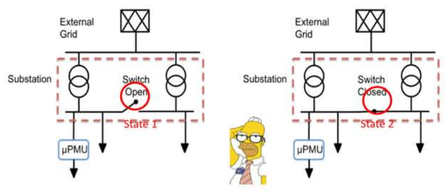
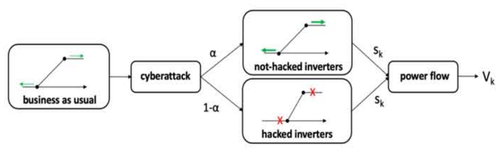
Cybersecurity of Operational Technology in Electric Grids

Shammya Saha[1], Raksha Ramakrishna[1], Teklemariam Tesfay[1], Gary Morris[2], Anna Scaglione[1], Nathan Johnson[2]
[1]School of Electrical, Computer and Energy Engineering, Arizona State University, [2]The Polytechnic School, Arizona State University

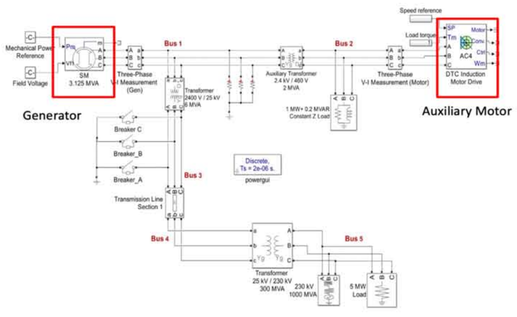


Motivation

Area of Work	Description
PREVENTION *Stopping cyber attacks from happening*	
DETECTION *Identifying if/when cyber attacks occur*	
MITIGATION *Reducing impact of cyber attacks*	

Identity Threat Vectors to Power Generation and Distribution Infrastructure

- Assessed susceptibility of power plants to threats on exterior electrical lines
- Identified threat vectors from distributed energy resources and IoT
- Identified methods to attack and shutdown power plants from power disturbances created over 100+ km away

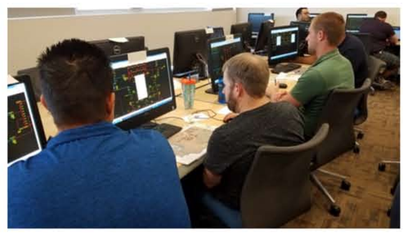


Quantified severity of attack impact on electrical motors and drives

Publication: Saha S. and Johnson NG. Point-On-Wave Analysis of Three-Phase Induction Motor Drive Under Fault External to Power Plant. 2018 IEEE PES General Meeting.

Train Veterans and Navy Personnel

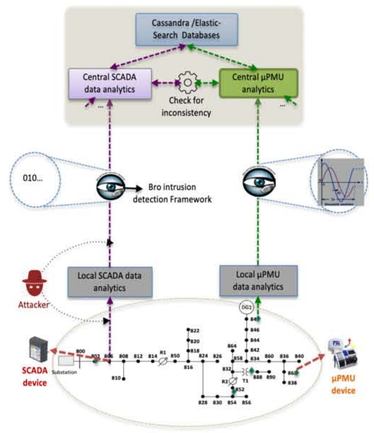
- Developed grid cyber security training modules focused on operational technology (e.g., motorized breaker) and informational technology (e.g., router)
- Trained 28 Veterans (over two workshops) in grid cybersecurity (right) with a focus on operational technology
- Took 3rd place in Western Regional Collegiate Cyber Defense Competition (left) with a focus on protecting information technology from attack



Methods for Intrusion Detection in Electrical Distribution Infrastructure

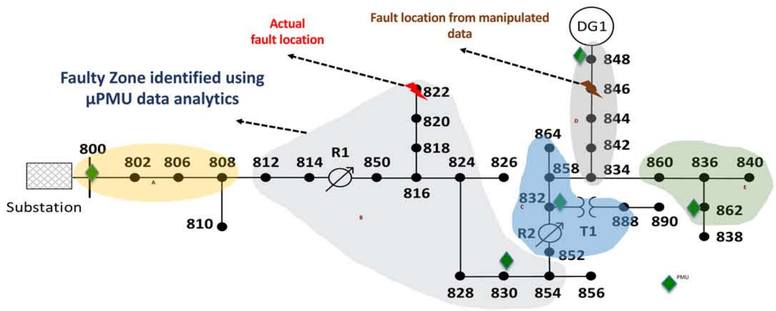
- Identified weaknesses and system behaviors in DoD cyber infrastructures
- Created sniffers and automated warning/correction algorithms
- Developed and tested intrusion detection algorithms that compared measured operational data (from SCADA device) to modeled operational data (with data from micro phasor measurement unit, μPMU device)

Publication: Jamei M., Scaglione A., and Peisert S. "Low-Resolution Fault Localization Using Phasor Measurement Units with Community Detection" IEEE SmartGridcomm 2018.



Cyber Vulnerabilities in Navy Installation and Electric Utility Infrastructure

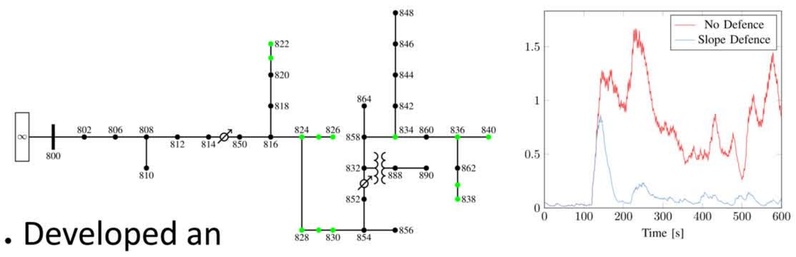
- Completed work in localizing faults in under-sampled grid regime when there is loss of resolution. Investigated the dependency on the network properties and introduce notion of cluster level fault localization



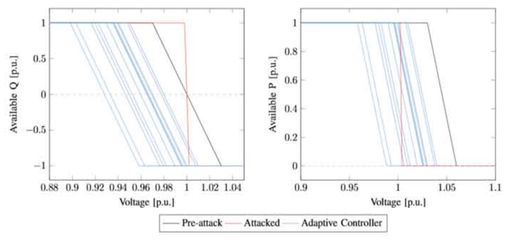
- Identified optimum sensor placement for fault localization for maximum possible resolution

Publication: Jamei M., Ramakrishna R., Tesfay T., Gentz R., Roberts C., Scaglione A., Peisert S. "Phasor Measurement Units Optimal Placement and Performance Limits for Fault Localization" JSAC SI Communications and Data Analytics in Smart Grid.

Adaptive Controller Design for Smart Inverter Stability during Cyber-Attacks

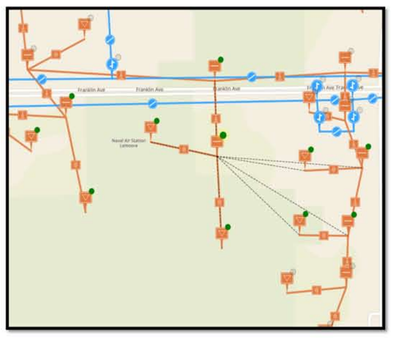


- Developed an adaptive controller that adjusts inverter operating curves based on local measurements

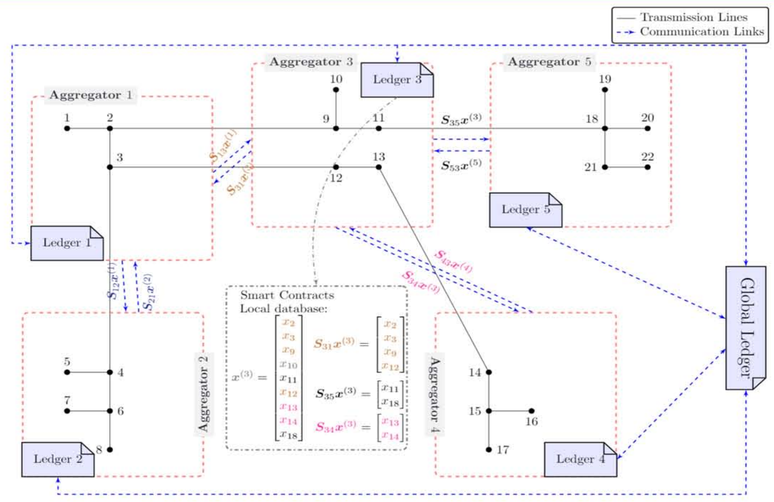


An Interactive Decision Support Tool to Evaluate Cyber Attacks

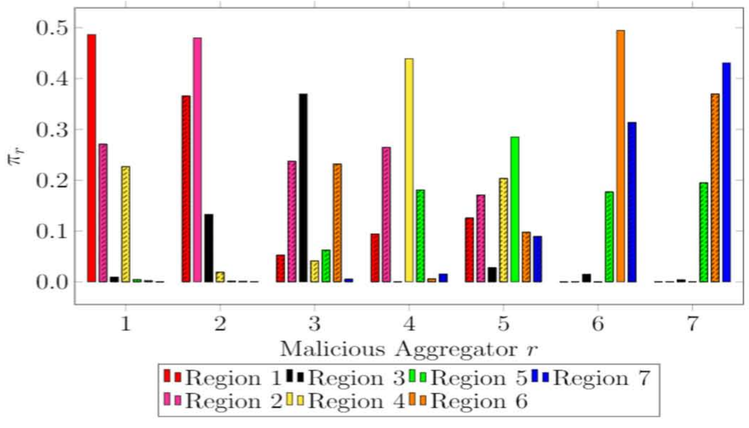
- Created visualization of operational technology in grid network and indicators of cyber attack for real-time threat identification and mitigation
- Tracked communication pathways from remote terminal units (attack entry points) to substations and higher-level grid infrastructure (shown below for NAS Lemoore)
- Represented Remote Terminal Units (RTUs) commonly used to connect physical assets to the digital realm (SCADA)



Blockchain for Distributed Security of Grid-Edge Devices



- Work in progress to develop a Blockchain based distributed architecture for Transactive Energy
- The proposed architecture resolves scalability issues, uses cryptographic features (software and hardware based) in conjunction with developed state verification algorithms to detect false data injection (FDI) attacks



Publication: Ravi N., Saha S., Scaglione A., and Johnson N. "Keeping Them Honest: a Trustless Multi-Agent Algorithm to Validate Transactions Cleared on Blockchain using Physical Sensors" submitted to ACC 2020.

Acknowledgements

Ira A. Fulton Schools of Engineering, Arizona State University
BLOCKFRAME
BERKELEY LAB
Department of the Navy, ONR, Science & Technology

Contact: Nathan Johnson, nathanjohnson@asu.edu, 1-480-727-5271