CREDC

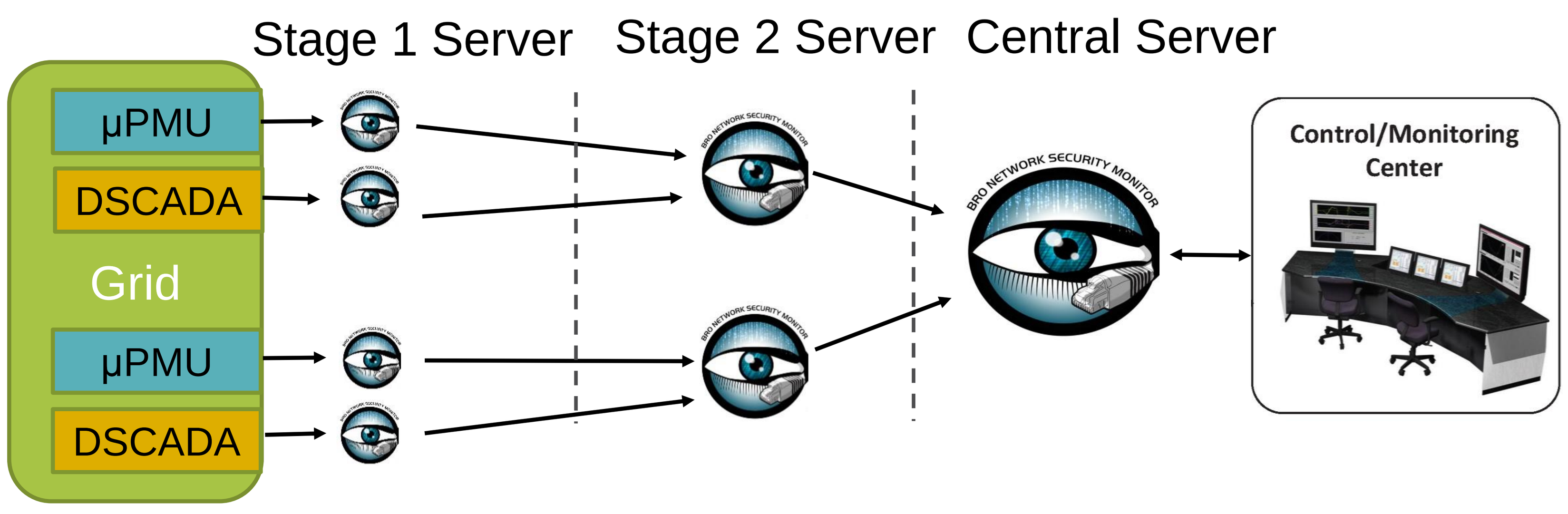
Supporting Security with Advanced Multimodal Grid Data Analytics

Micro Synchrophasor-Based Intrusion Detection in Automated Distribution Systems

M. Jamei (ASU), R. Gentz (ASU), A. Scaglione (ASU), S. Peisert (LBNL), E. Stewart (LBNL), C. McParland (LBNL), C. Roberts (LBNL), A. McEachern (PSL)

GOALS

- Combine high resolution µPMU data & sniffed SCADA for Intrusion Detection.

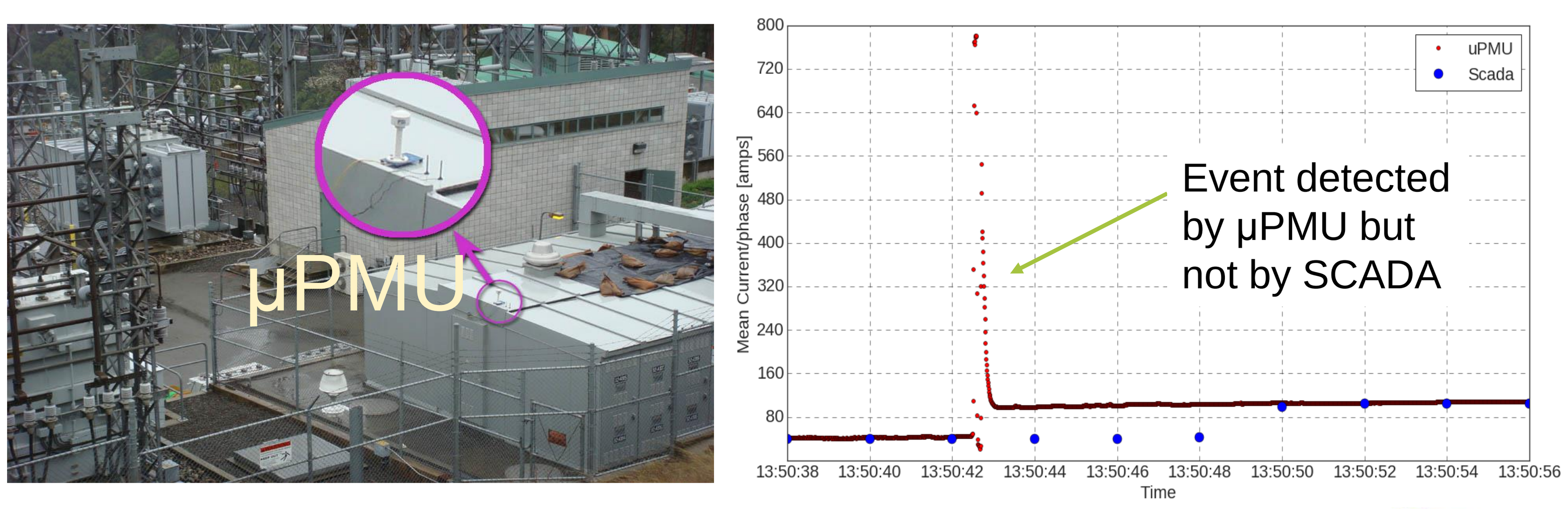


CURRENT SECURITY CHALLENGES

- Firewall, authentication, cryptographic algorithms, Intrusion Detection System (IDS), … are insufficient.
- Solutions are divorced from the knowledge of the physics of the system, safe operations and limits, and its current physical operating point.
- Extending the IDS notion in previous works by checking the compliance of sniffed SCADA data with cyber-physical rules.
- Previous IDS is blind to some sophisticated attacks.

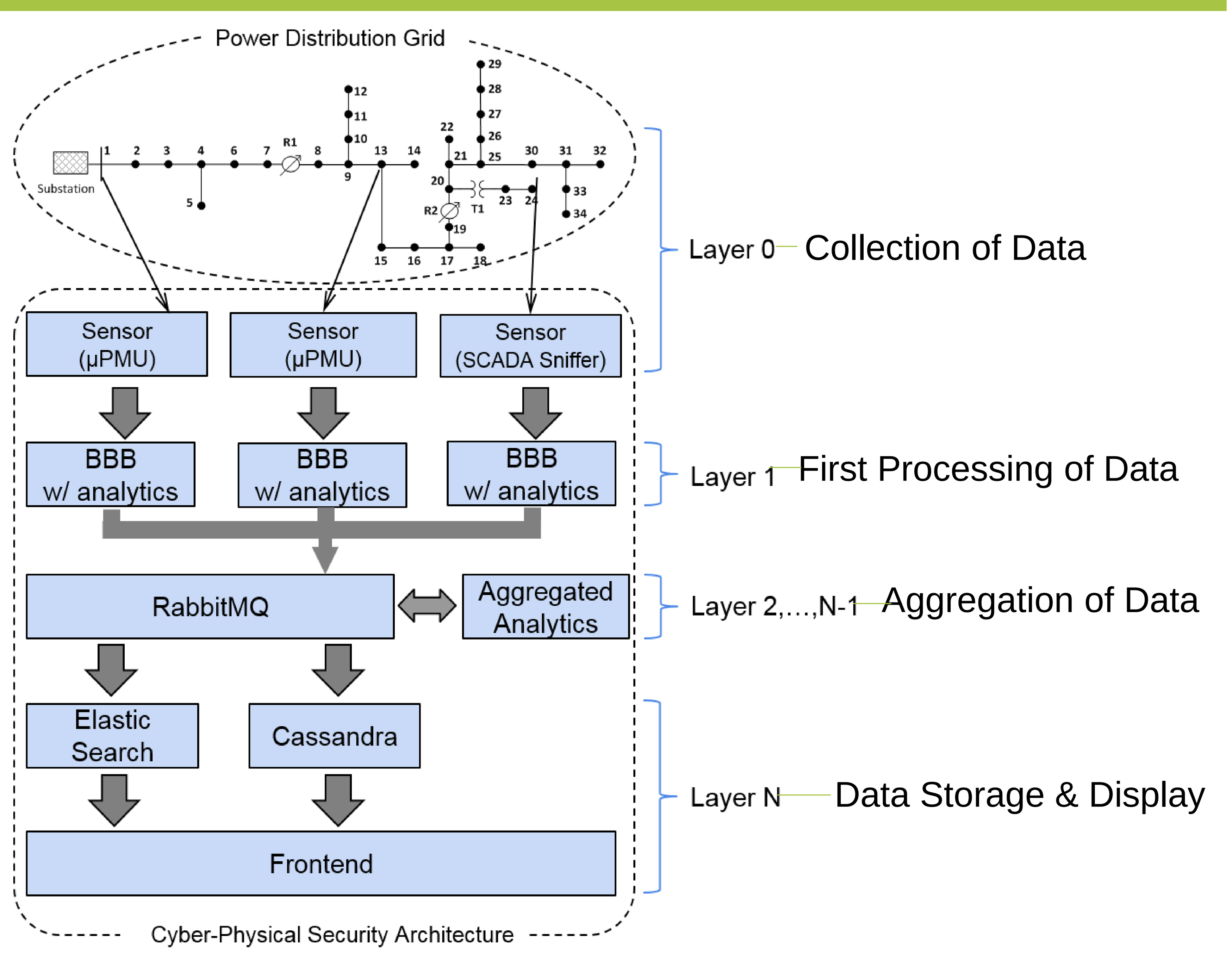
MICRO-PMU DATA (A GAME CHANGER)

- Situational awareness through µPMU devices.
- Significantly more information vs event triggered SCADA data.



- Many cyber-attacks leave footprints in the µPMU data.
- Detected µPMU anomalies + knowledge of grid operation security status hypothesis testing.

GRID SECURITY SYSTEM ARCHITECTURE



BeagleBoneBlack (BBB) minicomputer next to each sensor:
Hosting Stage one data-driven processing and traffic priorities

RabbitMQ as universal messaging system for data aggregation:
Hosting Stage i (i>1) data-driven processing

Elastic search as database for search – All elements are searchable fast

Cassandra as Database for archiving – Data stored in Protobuf format; 8x data reduction vs CSV format.

ANOMALY DETECTION ALGORITHMS

What happens at Stage-1 Servers (field level):

–Next to each local sensor.
–Agnostic about the grid interconnection (for scalability).
–Detect anomalies and put them in the priority to send to the next stage.
–Robust w.r.t data injection attacks that happen at the network level.

What happens at Stage-i (i>1) Servers:

–µPMU data and SCADA traffic captured and analyzed with Bro are available (possibly augmented by the output of DMS apps).
–Know the grid interconnection.
–Detect anomalies by correlating the available data.

Current Focus: Detecting anomalies using merely µPMU data.
Future Direction: Discriminating between malicious and non-malicious events detected by µPMUs using sniffed SCADA.

Stage-1 Anomaly Detection Rules:

– *Voltage Magnitude Change,*
– *Current Magnitude, Active and Reactive Power Fast Changes,*
– *Instantaneous Frequency Drift Fast Changes,*
– *Thevenin Source Impedance Fast Changes,*
– *Validity of Quasi Steady-State Regime,*
During transient:
quasi steady-state regime is not valid → signature of anomaly.

$$\mathbf{i}_{ij}[k] = \overline{\boldsymbol{Y}}_{ij}(f_0,\beta_k)\mathbf{v}_i[k] - \boldsymbol{Y}_{ij}(f_0,\beta_k)\mathbf{v}_j[k]$$

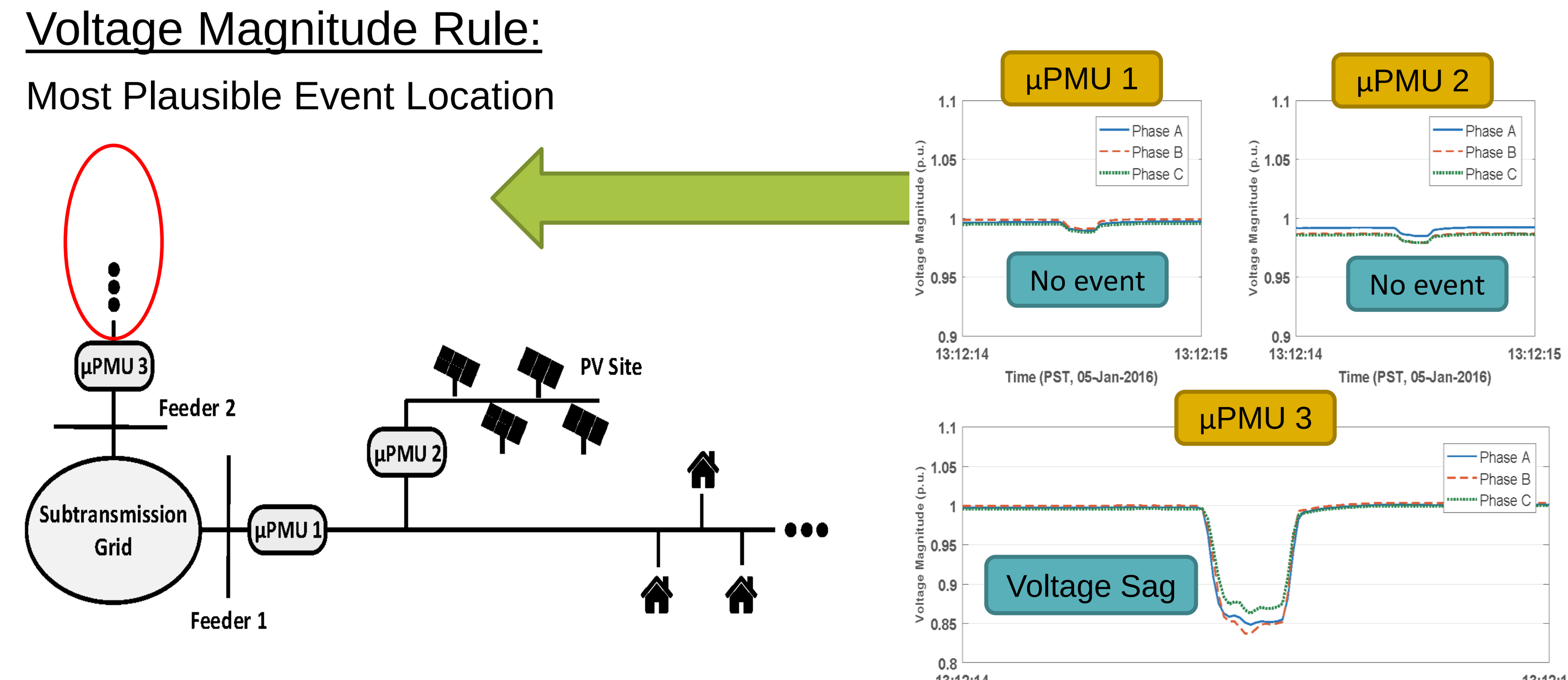
Stage-i (i>1) Anomaly Detection Rules:

– *Extension of quasi steady-state invalidity using small number of µPMUs.*

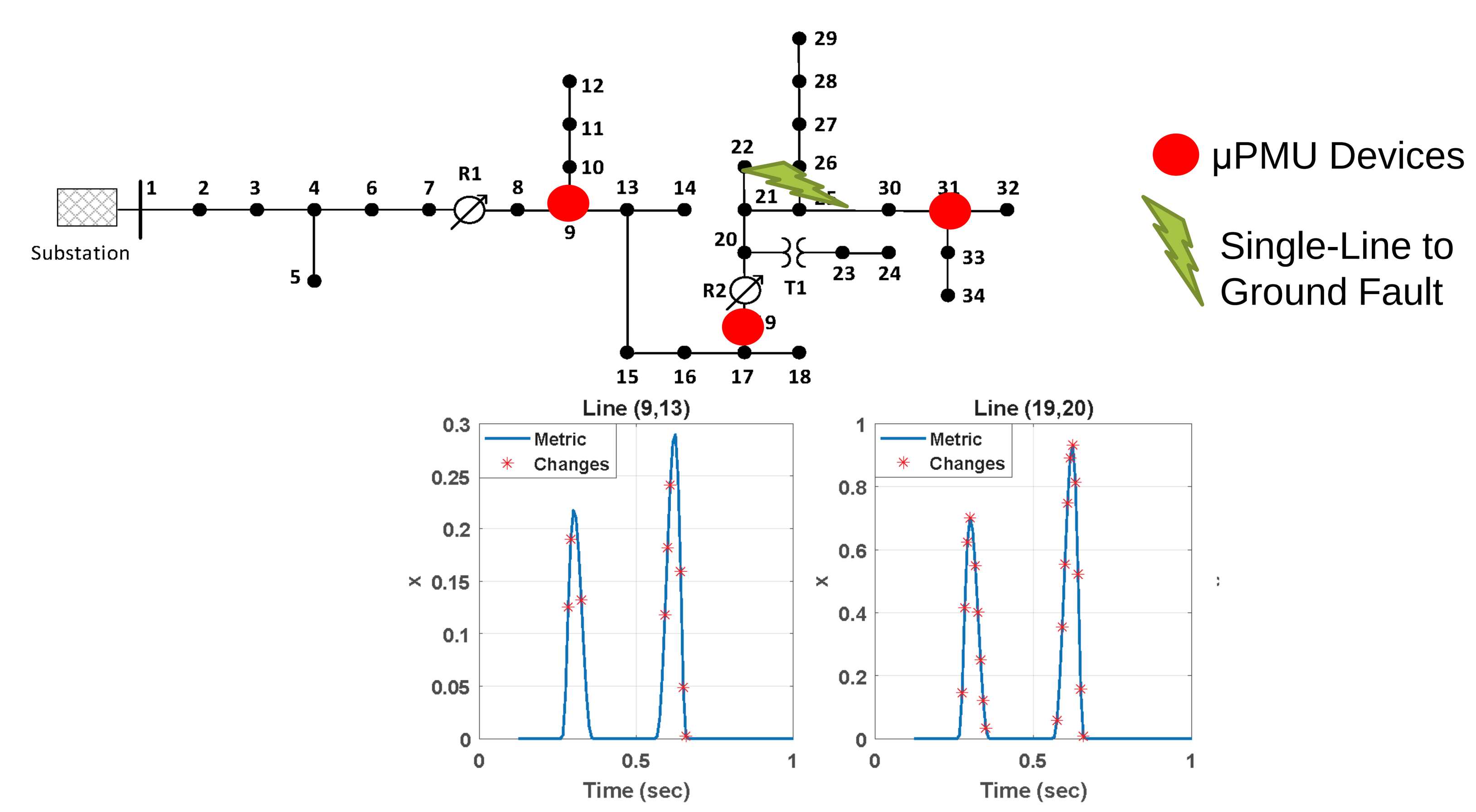
NUMERICAL RESULTS

Voltage Magnitude Rule:

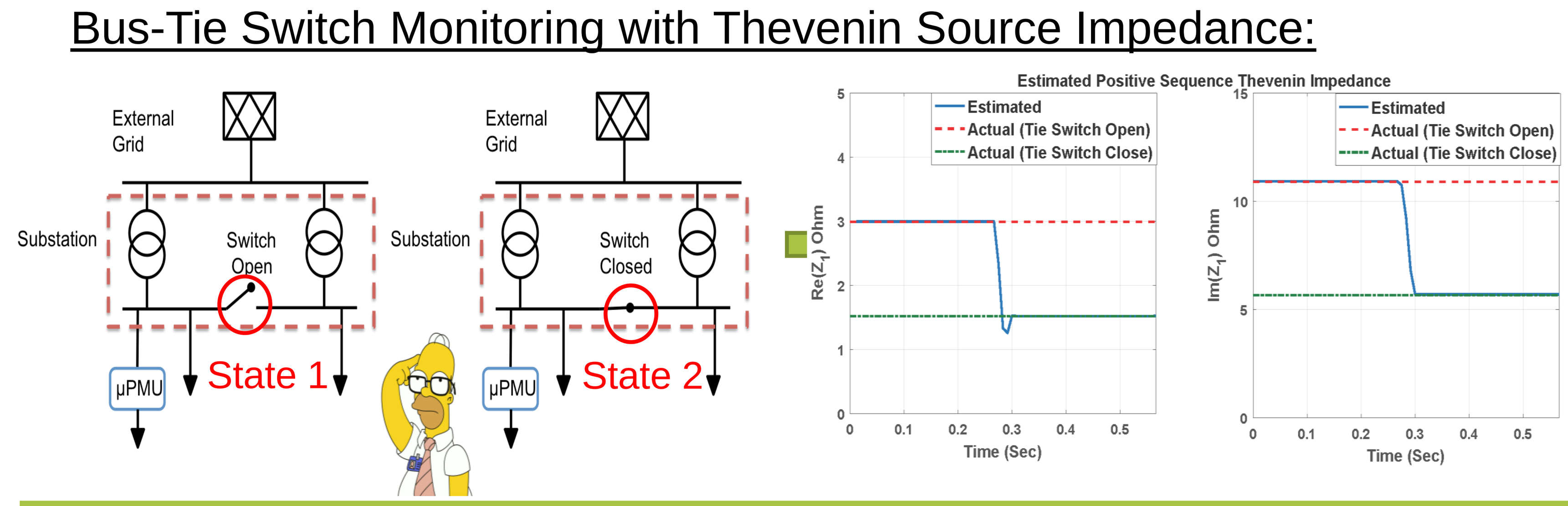
Most Plausible Event Location



Quasi Steady-State Regime Validity:



Bus-Tie Switch Monitoring with Thevenin Source Impedance:



INTERACTION WITH OTHER PROJECTS

This activity has been in close collaboration with LBNL under another CEDS-funded project. The real data are provided for us thanks to an ongoing ARPA-E funded project.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY