PIs: Sean Peisert, Chuck McParland, Anna Scaglione, & Emma Stewart

Lawrence Berkeley National Laboratory

Supporting Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Summary: Cyber Detection using µPMU and SCADA Data

Objective

- Use µPMUs and SCADA in distribution grid to measure physical/electrical power system parameters and detect cyber attacks against substation equipment.

Schedule

- Start: Early 2015 → End: 5/31/18
- Key Deliverables
  - Cyber attack scenarios — 6/15/15
  - Requirement Docs — 12/2/15
  - µPMU placement rpt — 11/15/16
  - Algorithm design and selection — 12/15/16
  - Pilot site deployment rpt. — 5/18/18

- **Key capability from this effort:** using 1-2 µPMUS per distribution feeder, can give a more reliable, robust, scalable, and cost-effective means of detecting key classes of cyber-attacks against the power distribution grid than traditional approaches

Performer:	LBNL
Partners:	ASU, EnerNex, EPRI, PSL
Federal Cost:	$1,200,000
Cost Share:	
Total Value of Award:	$1,200,000
Funds Expended to Date:	42%

Advancing the State of the Art (SOA)

Key Insights:

- Cybersecurity for energy delivery systems often treats those systems like traditional IT components and often doesn't consider the condition of power-grid elements, and the effects of that condition on the grid.
- Grid security is different than IT security: isolation is ***not*** the goal
  - A cyber attack against the grid is a ***physical*** phenomenon
  - Cybersecurity of power grid systems can ***leverage physics***

What are we doing?

- Use a separate sensor network to independently view grid operations
- Compare signatures of physical measurements and communication between devices that control the grid to detect cyber attacks and physical events
- Example: Physical outage at LBNL detected 120 seconds prior to event

Why does it matter?

- 1-2 sensors per distribution feeder, can give a more ***reliable***, ***robust***, ***scalable***, and ***cost-effective means*** of ***detecting key classes of cyber-attacks against the power distribution grid*** than traditional approaches

Advancing the State of the Art (SOA)

- Use ***both*** physical (µPMU) sensors in distribution grid to measure physical/electrical power system parameters and SCADA traffic.
- Develop data-driven models to identify key classes of cyber attacks, physical events, and equipment malfunction .
- Compare ***physical state from µPMUs with view of network (SCADA) commands***, and correlate equipment operation (or lack of operation)
- Use statistical and machine learning algorithms to:
  - identify “normal,” ”abnormal,” or malicious operation,
  - determine if operation is “safe” or “unsafe,”
  - identify and distinguish key classes of cyber attacks from equipment malfunctions or natural disasters.
- µPMUs are:
  - a scalable, cost-effective solution already being deployed by major utilities to analyze natural faults.
  - a separate network of sensors. When compared against SCADA data, µPMUs provide an ***independent*** view of distribution system operations, making detection of certain classes of cyber attacks more reliable.
- Our technique is based on ***physics***, not guesswork about what new cyber malware might be developed by motivated attackers:
  - much harder to spoof
  - more accurately identify the effect of the attack, not just that something is anomalous
  - “physical” aspect of the grid become an asset, not just a liability
- Partnered with numerous vendor and utility organizations to implement, experimentally validate system, and transition to practice.

Challenges to Success

Loss of Key Partner (Erich Gunther, EnerNex)

- Solutions: redistributed some work to LBNL and ASU, brought on additional power expertise from EnerNex

Challenge 2

- ARPA-E project that we are leveraging μPMU data from replaced of one utility with another as utility partner
  - Our CEDS project needed an additional NDA with new utility. This is now complete.

Challenge 3

- This project requires multiple personnel with power expertise and multiple personnel with cyber security expertise
  - Explaining the application of and solution to the project is an ongoing process requiring both sides of the project team to continue to develop a languages to explain to both sides.

Progress to Date

Major Accomplishments

- Identify substation cyber attack scenarios suitable for detection using our methodology and enumerate specific data signatures used for attack detection.
- Create simulated data streams that exhibit attack signatures.
- Through analysis of simulated behavior, determine ability to detect above signatures in multiple operating scenarios.
- Implement streaming data collection, storage, and analysis system and obtain and store µPMU data from RPU and Southern Co.
  - Identify optimal µPMU placement parameters.
  - Initial analysis algorithm design and selection.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Targeted end user for the technology is Asset Owners.
  - Several µPMUs installed at Riverside Public Utilities and Southern Company. Successful validation will encourage larger scale adoption directly at those utilities.
    - µPMUs installed directly at RPU and Alabama Power / Southern Co. as part of ARPA-E project.
    - As a by-product of the integration of the sensors and validation of SCADA data the utility will be enabled to have better management of load
  - Working with Power Standards Lab, which manufactures the µPMUs, and EnerNex and EPRI, which consult to and advise utilities.
    - EPRI and EnerNex help ensure we are working with known and realistic threat vectors, and attack analysis techniques that will be acceptable to utilities.
- Interfacing our data collection / analysis architecture with ADMS and GMLC working groups on applications of sensing and measurement technology

Next Steps for this Project

General Approach

- Implement µPMU and SCADA collection, analysis, and reporting capabilities in live system and do on-going tests with live data.

Remaining Milestones & Deliverables

- Successful operation of Bro pilot deployment at LBNL — 8/15/17
- Integration of Bro framework with OSIsoft and circuit simulation tools. — 8/16/17
- Successful demonstration of modeling framework development and data collection from LBNL network — 12/15/17
- Report on pilot site deployments — 5/18/18

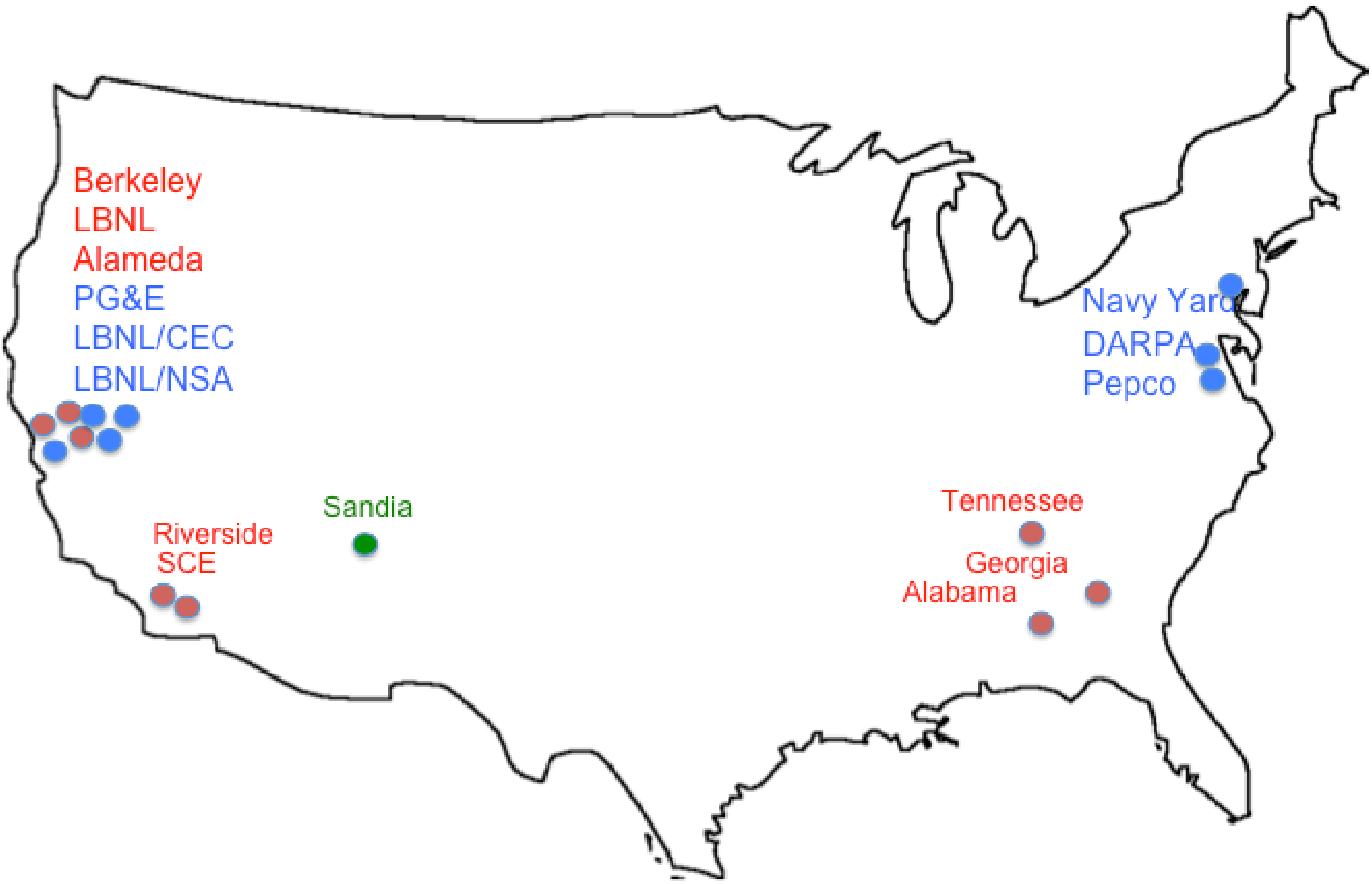
Additional Slides

Maximum of five additional slides

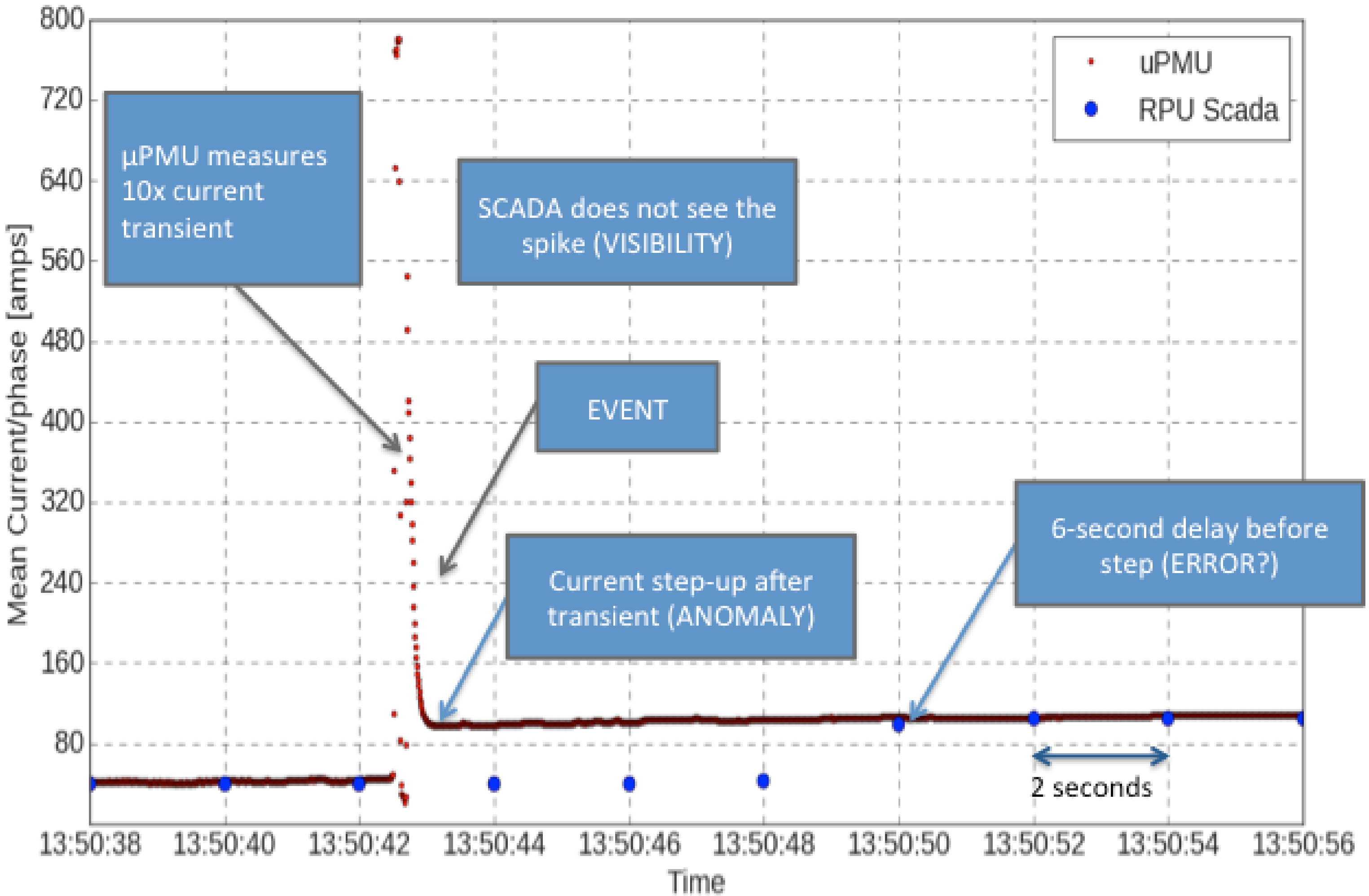
Remaining slides should provide additional information that supports the template slides, with a strong focus on:

- The technical aspects of the project
- The feasibility that this technology/knowledge will become a valuable, widely-accepted cybersecurity solution for energy delivery systems

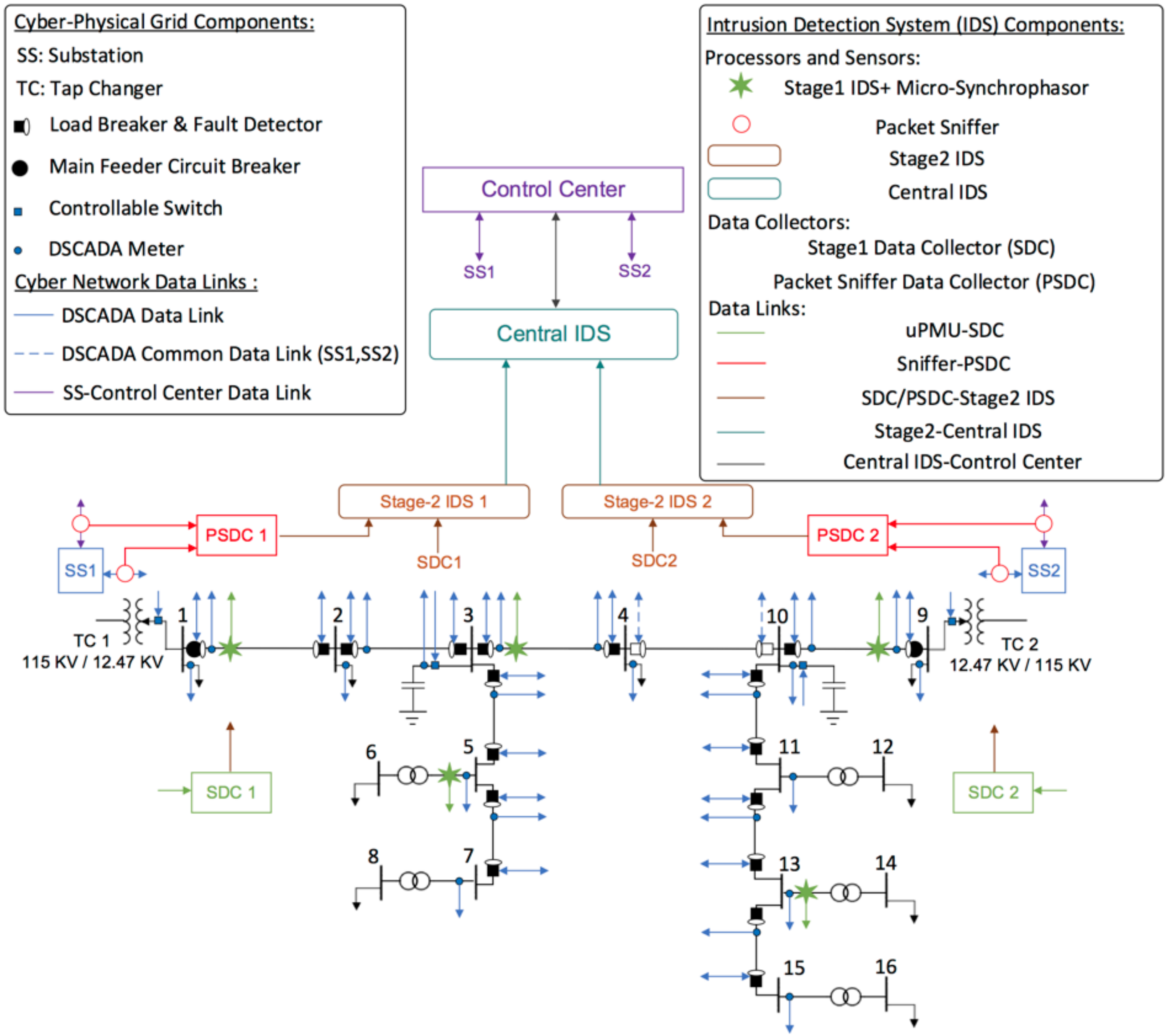
Current Locations of μPMUs



Comparison of traditional and μPMU data at Riverside Public Utility



μPMU and SCADA Architecture



Status

- **Current CEDS Power Grid Cybersecurity R&D project is $400k/yr for 3 years**
  - Currently a little less than halfway through.
- Separate project (LBNL not involved) funded by DARPA RADICS, also uses the PSL µPMU to detect cyber attacks against the grid
  - Focuses on military base grids, rather than commercial grids.
- **µPMU technology and the applications developed through ARPA-E are being transitioned to various OE & EERE Projects**
  - ARPA-E project received plus-up for continuing integration with Advanced Distribution Management Systems and Distributed Energy Resources pilots at Riverside Public Utility
  - µPMUs can be deployed immediately with commercially-available instruments

Status and Possible Future Steps

- Finish project (additional 1.5 years)
- Current CEDS Power Grid Cybersecurity R&D project is $400k/yr for 3 years
  - Currently a little less than halfway through.

- Separate project (LBNL not involved) funded by DARPA RADICS, also uses the PSL µPMU to detect cyber attacks against the grid
  - Focuses on military base grids, rather than commercial grids.
- µPMU technology and the applications developed through ARPA-E are being transitioned to various OE & EERE Projects
  - ARPA-E project received plus-up for continuing integration with Advanced Distribution Management Systems and Distributed Energy Resources pilots at Riverside Public Utility
- µPMUs can be deployed immediately with commercially-available instruments

Possible Future Steps:

- Accelerate and implement wider-scale R&D and validation, continued emphasis on practical outcomes. Cost: $3M
- Broad test deployment across most major U.S. utils within a year. Cost: $30M
  - Top 500 substations @ ~$50k per substation for instrumentation & installation
  - Communication costs, system management. Cost $5M