Stacy Prowell

Oak Ridge National Laboratory

Core and Frontier

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: Core and Frontier

- **Objective**
  - Build capabilities and collaborations to enable ORNL to effectively contribute to improving the cybersecurity of energy sector.
- **Technical Approach**
  - Establish and grow partnerships.
  - Focus on the edge of the grid.
  - Build capabilities through internal integration.

- **Total Value of Award:** $397K
- **% Funds expended to date:** 55%
- **Performer:** ORNL
- **Partners:** Multiple

Projects

- **CURENT**
- **RTDS**
- **Outreach**
- **GridSQuaRe**

Jason M. Carter
Tom Swain
Oak Ridge National Laboratory

CURENT
Center for Ultra-Wide-Area Resilient Electric Energy Transmission Networks

Cybersecurity for Energy Delivery Systems Peer Review
August 5-6, 2014

Summary: CURENT

- **Objective**
  - Develop a collaborative effort with CURENT to enhance security within future wide-area energy delivery system architectures.
- **Schedule**
  - CY2014
  - Identify CURENT-relevant cyber focus areas
  - A written assessment and a plan to address identified critical challenges

CURENT
CENTER FOR ULTRA-WIDE-AREA RESILIENT ELECTRIC ENERGY TRANSMISSION NETWORKS

- **Total Value of Award:** $75K
- **% Funds expended to date:** 25% (50%)
- **Performer:** ORNL
- **Partners:** UT CURENT

Major Accomplishments

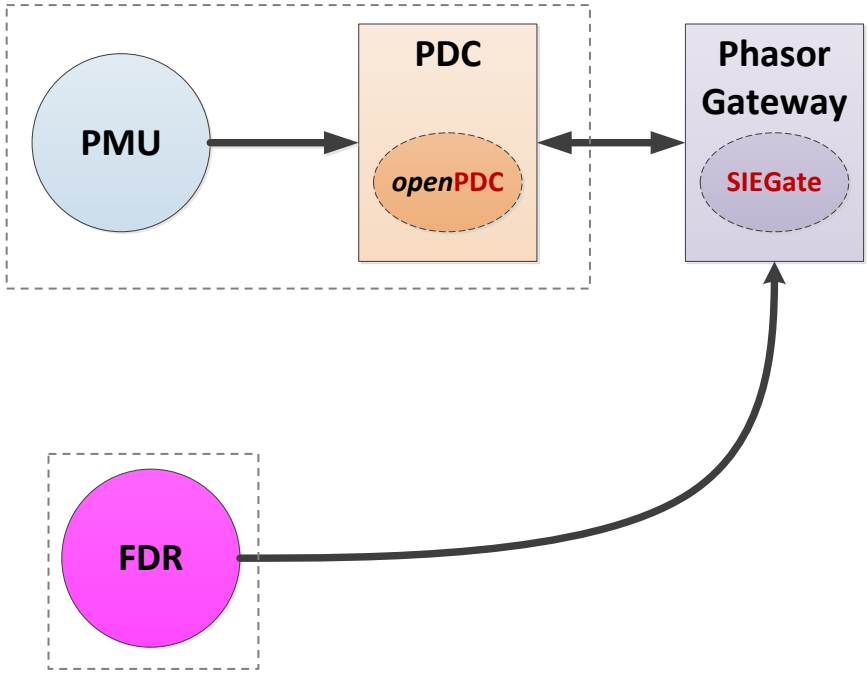
- **Comprehensive review of relevant energy delivery system security research.**
- **Identified gaps in cyber security research pertaining to the CURENT project.**
- **Identified two major CURENT-relevant focus areas that can be simulated on UT CURENT and ORNL simulators.**
- **Developed a detailed research plan; coordinated future research with UT CURENT staff.**

Next Steps for this Project

- **Approach for the next year or to the end of project**
  - Finalize an assessment of specific risks to the wide-area architectures CURENT is exploring.
  - Develop strategies to integrate identified security research into the Large Scale Testbed (LTB).

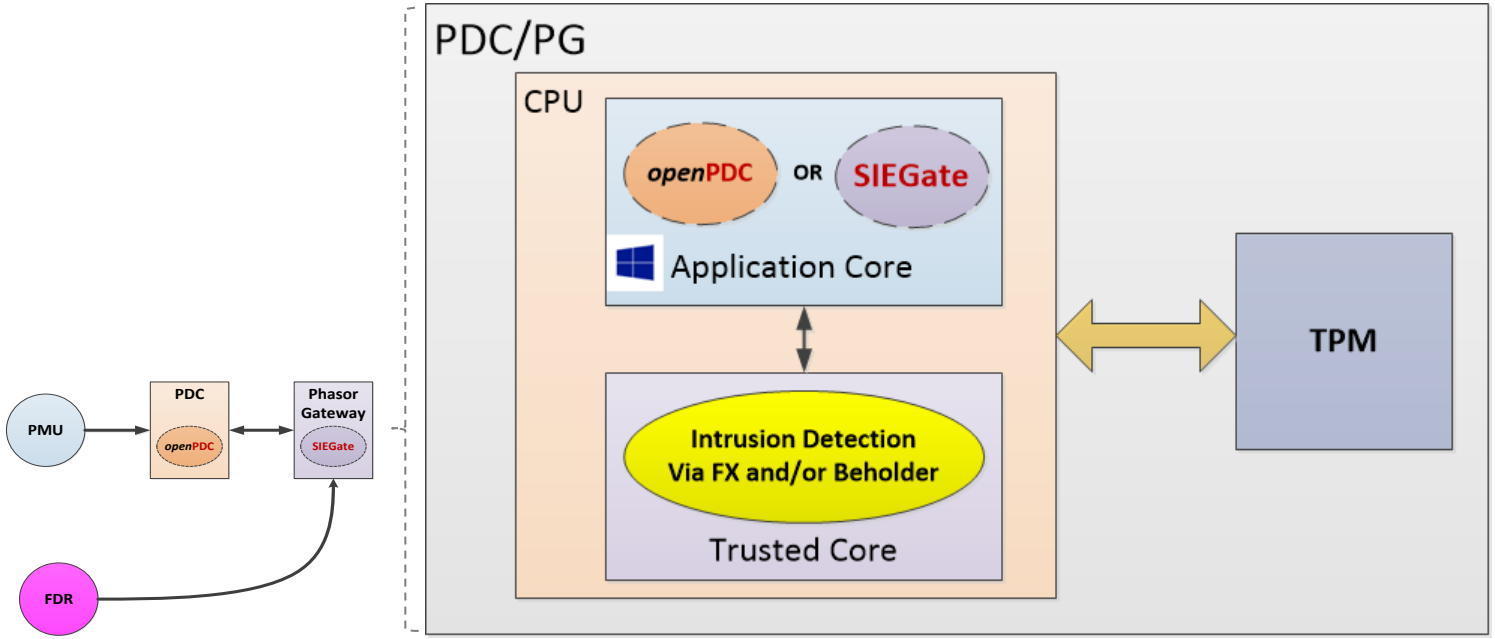
Critical Components

- **Critical CURENT components**
  - Phasor Measurement Units (PMU)
  - Phasor Data Concentrators (PDC)
    - Open software architecture
  - Phasor Gateways (PG)
  - Frequency Disturbance Recorders (FDR)



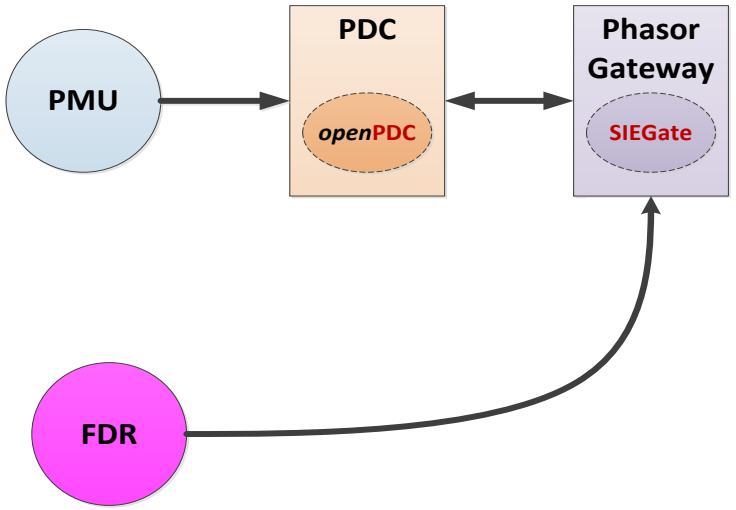
Measurement-Based Intrusion Defense

- Apply existing tools and guidelines to integrated Windows platforms
- Exploit Trusted Platform features inherent in the hardware
- Implement Real-Time Execution Monitoring



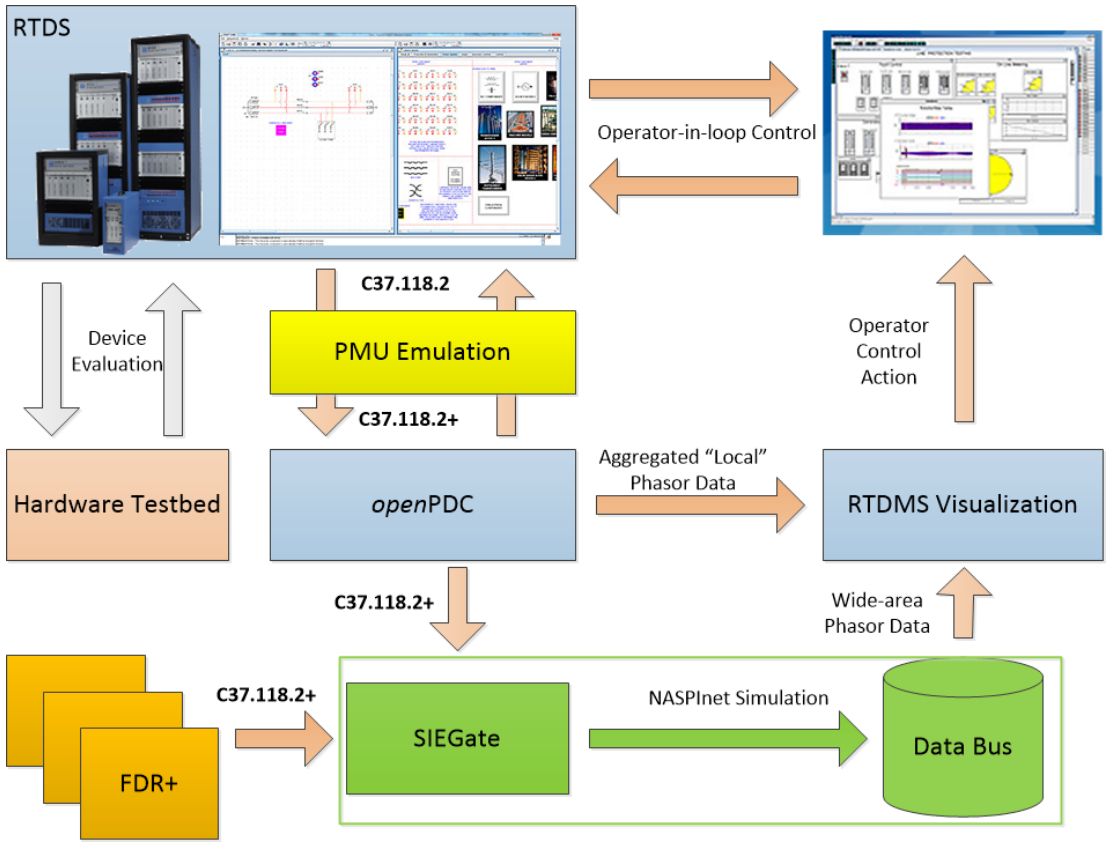
Measurement-Based Communication Security

- **Methods to provide authentication and message integrity to C37.118.2 packets**
  - Adaptation of TV-OTS
- **Secure integration of NASPInet**



Our Vision for CURENT Collaboration

- **Use the LTB to investigate new security research.**
  - Intrusion Defense
  - Communication Security
- **Examine security for C37.118.2 comms**
  - PMU Emulation
- **NASPInet Integration**
  - Prototype secure FDR integration
- **Advance proof of concept through simulation.**



Marcus Young

Oak Ridge National Laboratory

RTDS-based Testing Framework

Cybersecurity for Energy Delivery Systems Peer Review

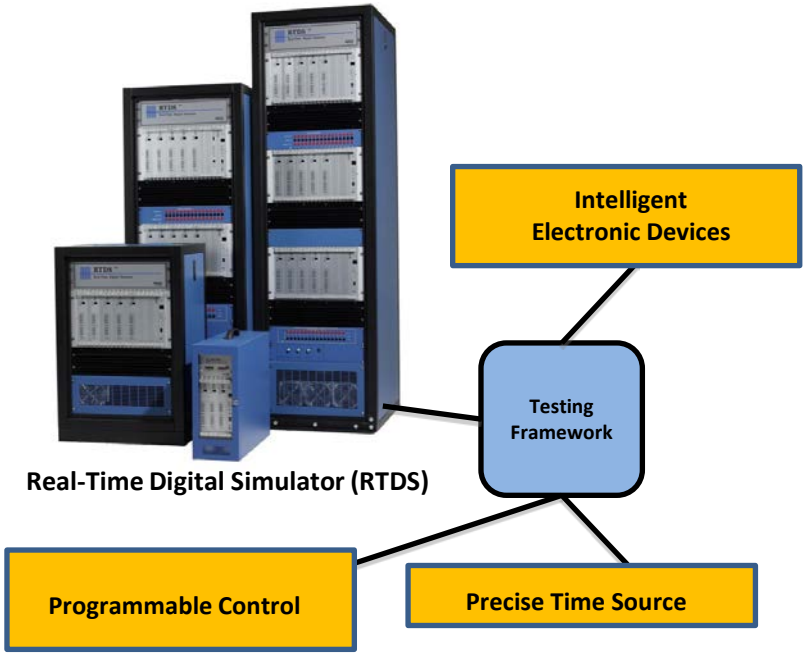
August 5-6, 2014

Summary: RTDS-based Testing Framework

- **Objective**

  Create an experimentation platform for better analysis and understanding of power systems.

- **Schedule**
  - 10/2012 to 12/2014
  - Problem statement and scenarios/test cases delivered. Advisory team formed and equipment configuration complete
  - Provides a capability and a evaluate impacts of compromised systems on electric power grids



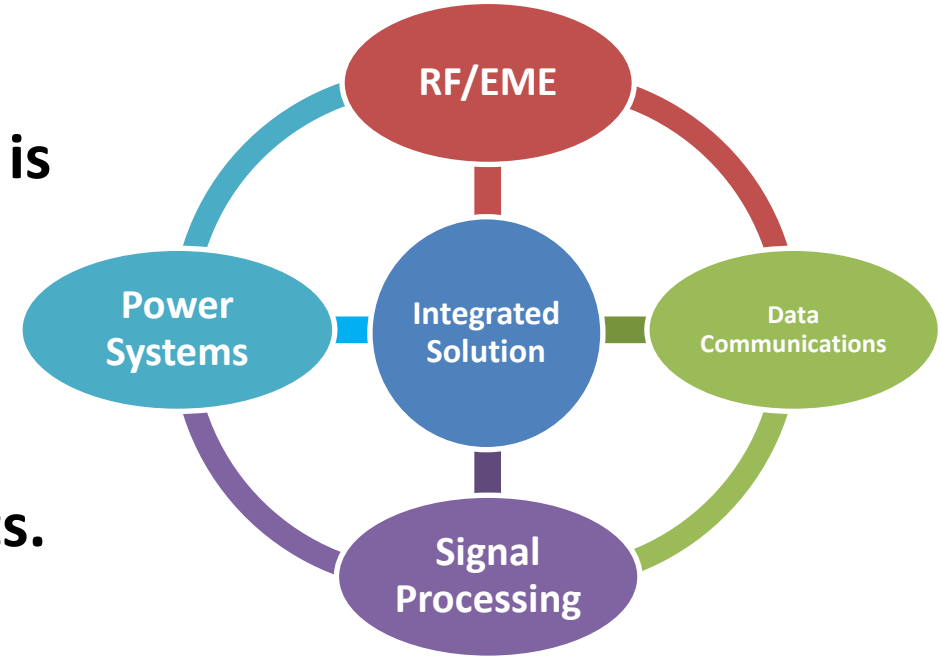
- **Total Value of Award:** $137K
- **% Funds expended to date:** 19%
- **Performer:** ORNL
- **Partners:** PNNL

OAK RIDGE National Laboratory

Pacific Northwest NATIONAL LABORATORY

Advancing the State of the Art (SOA)

- **Power systems are becoming increasingly dependant on precise time sources and packet-based communications.**
- **Focus is often on vulnerabilities rather than power system impacts.**
- **The RTDS-based framework is an integrated approach.**
- **Understanding impacts will help engineers to develop solutions to mitigate impacts.**

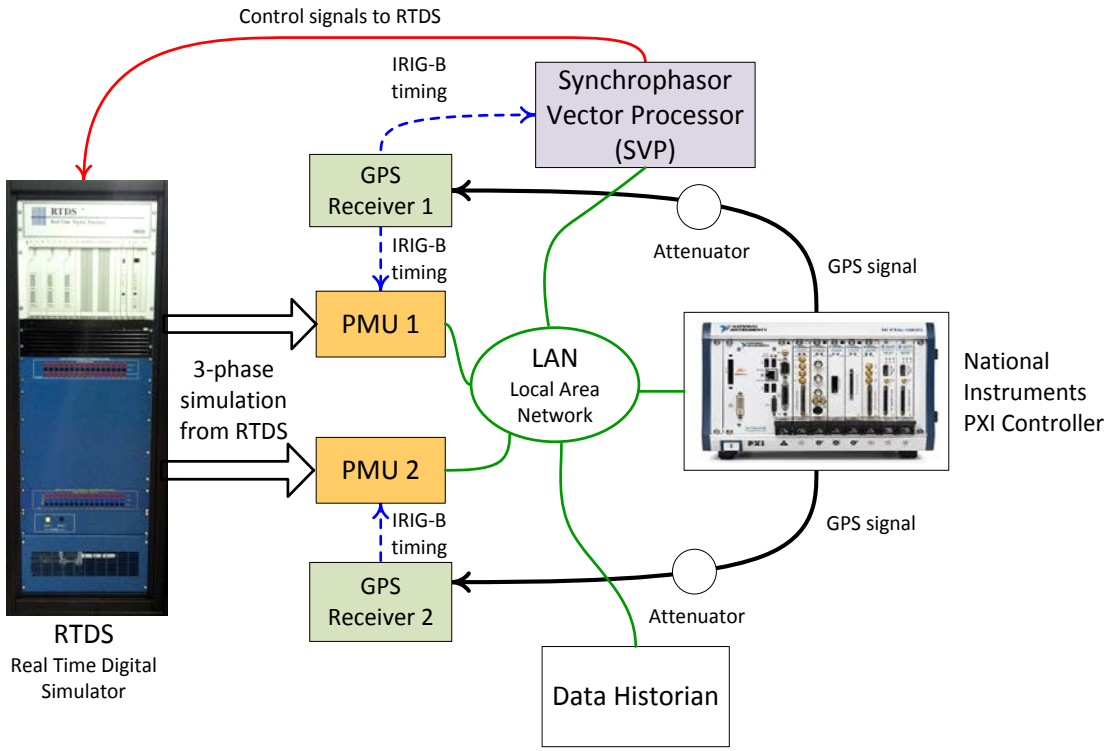


Advancing the State of the Art (SOA)

- **The framework can support tests for large range of vulnerabilities and is scalable from small to large systems.**

- **Key components:**

  - RTDS (Power system models and controls)
  - Intelligent electronic devices (relays, PMUs, etc.)
  - Precise time sources (e.g. GPS)
  - Communications (packet-based)
  - Customizable control equipment (SVP and PXI)

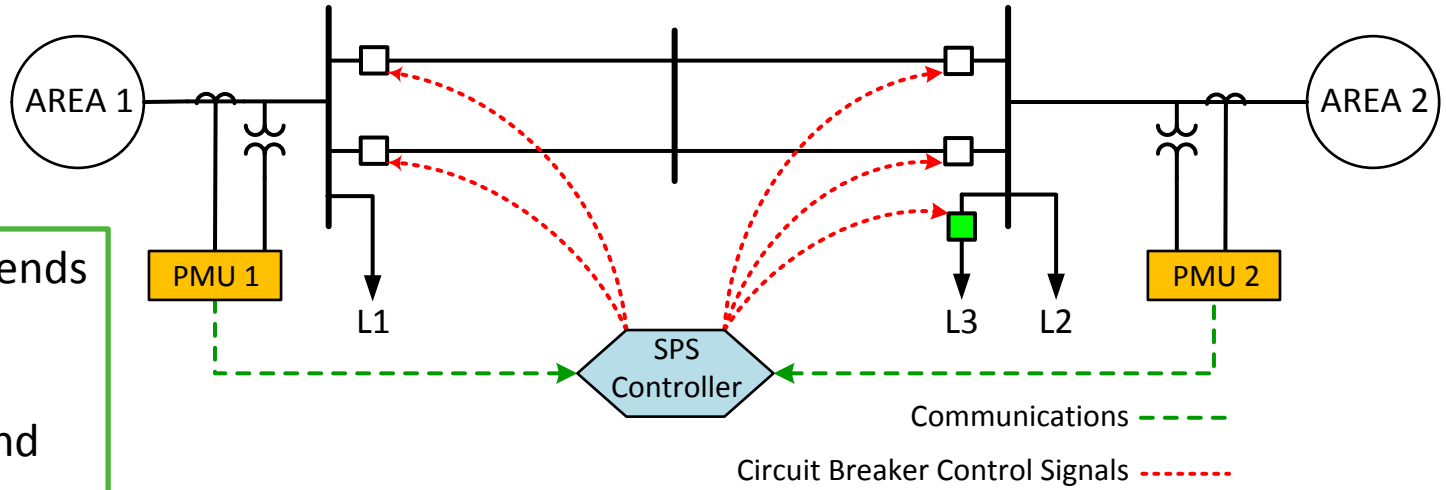


Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Targeted end user is the power utility and power system research entities. Both are trending towards obtaining the capabilities to execute this framework.
  - What are your plans to gain industry acceptance?
    - The project team has assembled an advisory team to guide the research.
    - The advisory team consists of two utilities, a university research center, and a vendor.

Demonstration: Simple Special Protection Scheme

- **Two area power system simulated in RTDS with hardware-based Special Protection Scheme (SPS)**
  - 4 generators (two in each area) with AGC and exciter controls
  - Normally, power is exported from Area 1 to Area 2 over the inter-tie
  - SPS Controller detects angular separation between areas via PMUs and executes a predetermined protection function if separation surpasses the threshold (e.g. reduces Area 2 load by opening breaker on L3).



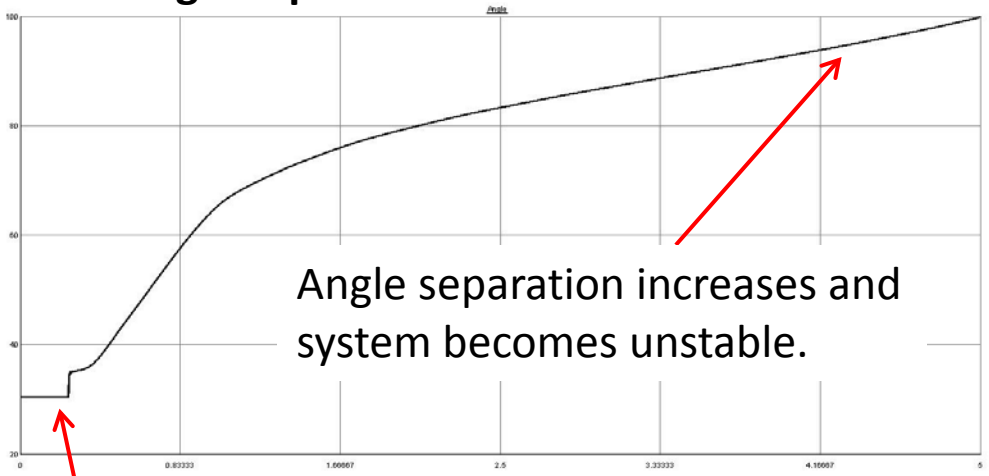
System control depends on precise timing, packet-based communications, and centralized controller.

Scenario: Loss of a Line

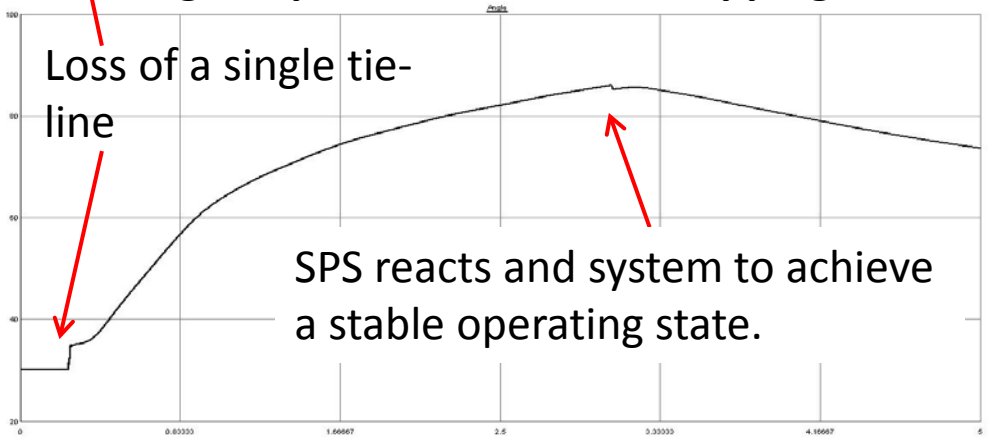
- One tie-line path is lost (e.g. fault)
- Stability of the system is impacted by loss of the line.
- SPS detects the angular separation between areas and reduces the load in Area 2 to achieve stable operation.
- A similar SPS is used in Guatemala.

While a simple example, this scenario depends on cyber elements. What impacts would spoofed GPS or communications hacks have on SPS?

Angle separation without SPS action



Angle separation with SPS dropping L3



Peter Fuhr

Oak Ridge National Laboratory

Outreach

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: Outreach

- **Objective**
  - Inform and provide guidance to the energy delivery utilities, industrial and factory automation companies, and associated suppliers and system integrators of trends and improvements in cybersecurity associated with their needs.
- **CEDS Outreach Presentations**
  - 19 presentations (including):
    - ISA Power Industry Forum
    - Emerge Alliance Workshop
    - IEEE Instrumentation & Measurement Society
    - SCADA 2014
    - EPRI Fleetwide Monitoring IG

Outreach to Partners/Interested Parties

- Electric Utilities (including)
  - TVA, Ameren UE, SoCal Edison, PG&E, ISO-New England, Duke Energy, Southern Companies, Arizona Public Service, Otter Tail Power
- Organizations (including)
  - National Rural Electric Cooperative Association, USDA, Bell Labs' GreenTouch, Society of Petro. Eng.
- Oil&Gas (including)
  - Koch Pipelines, Pioneer Natural Resources, Transocean, Shell, BP
- Suppliers (T&D and networking gear, including)
  - ABB, Siemens, Honeywell, Cisco, Motorola, GE, Eaton, Emerson, Invensys, Yokogawa

Next Steps for this Project

- **Approach for the next year or to the end of project**
- **A key impact of the OutReach effort involves the "cross-purposing" of cybersecure sensors, systems and network architectures developed for - and being deployed in - the electric utility sector into the oil and gas arena, in general, and in hydraulic fracturing operations in particular.**

- **As expressed by Jason Kennedy, Pioneer Natural Resources (largest domestic fracking company in the USA), *"we are quite aware of the potential for cybersecurity vulnerabilities in our energy delivery systems. ORNL made us aware of the CEDS efforts related to secure wireless in the electric utilities, ideas and architectures that we began implementing immediately".***
- **2015 Next steps: Continue to inform and provide guidance to the energy delivery utilities, industrial and factory automation companies, and associated suppliers and system integrators of trends and improvements in cybersecurity associated with their needs.**

Warren Grice

Oak Ridge National Laboratory

GridSQuaRe

Grid Security with Quantum Architectures & Resources

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary

- **Quantum Key Distribution**
  - Protocol is *provably secure*; COTS equipment expensive
  - **Has not been applied to Grid-related applications**
- **Evaluated QKD against NISTIR-7628 Use Cases**
  - Explored limitations of classical cryptography & PKI
  - **Where can QKD be deployed effectively?**
  - *Report completed Q3 FY14*
- **Follow-on Funding in Lab Calls**
  - **Practical Quantum Security** project
  - Transitioning Grid-centric QKD solutions to industry

First study of its kind – defining the state of the art

Summary – Questions?

- **CURENT**
- **RTDS**
- **Outreach**
- **GridSQuaRe**