Bill Sanders

(on behalf of entire TCIPG team)

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

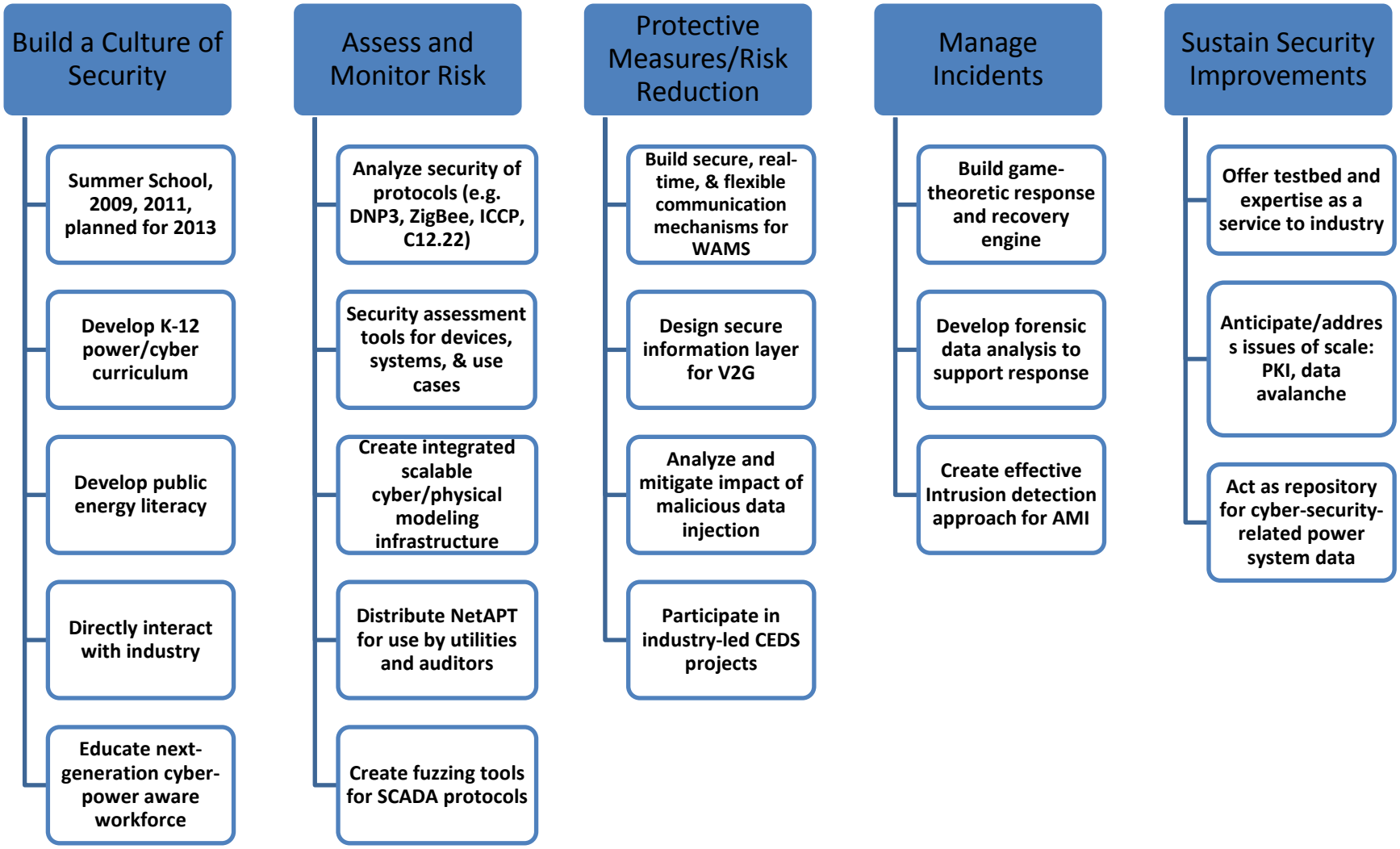
TCIPG Summary

- **Objectives**
  - Identify and address critical security and resiliency needs at the cyber-physical junction in the evolving power grid
  - Engage Industry (utility, control system vendors, technology providers)
  - Research Excellence
  - Education
- **Technical Approach**
  - Identify and take on important & hard problems
  - Unique balance of long view of grid cyber security, with emphasis on practical solutions
  - Work to get solutions adopted

TCIPG

- **Schedule:** Sept 30, 2009 – Aug. 30, 2015 (w/anticipated no cost extension)
- **Total Value of Award:** $18M
- **% Funds Expended to Date:** ~79%
- **Performers:** University of Illinois t Urbana-Champaign, Dartmouth College, Cornell University, University of California Davis, Washington State University
- **Partners:** 9-Member External Advisory Board (EAB) from utilities and industry, as well as large Industry Interaction Board

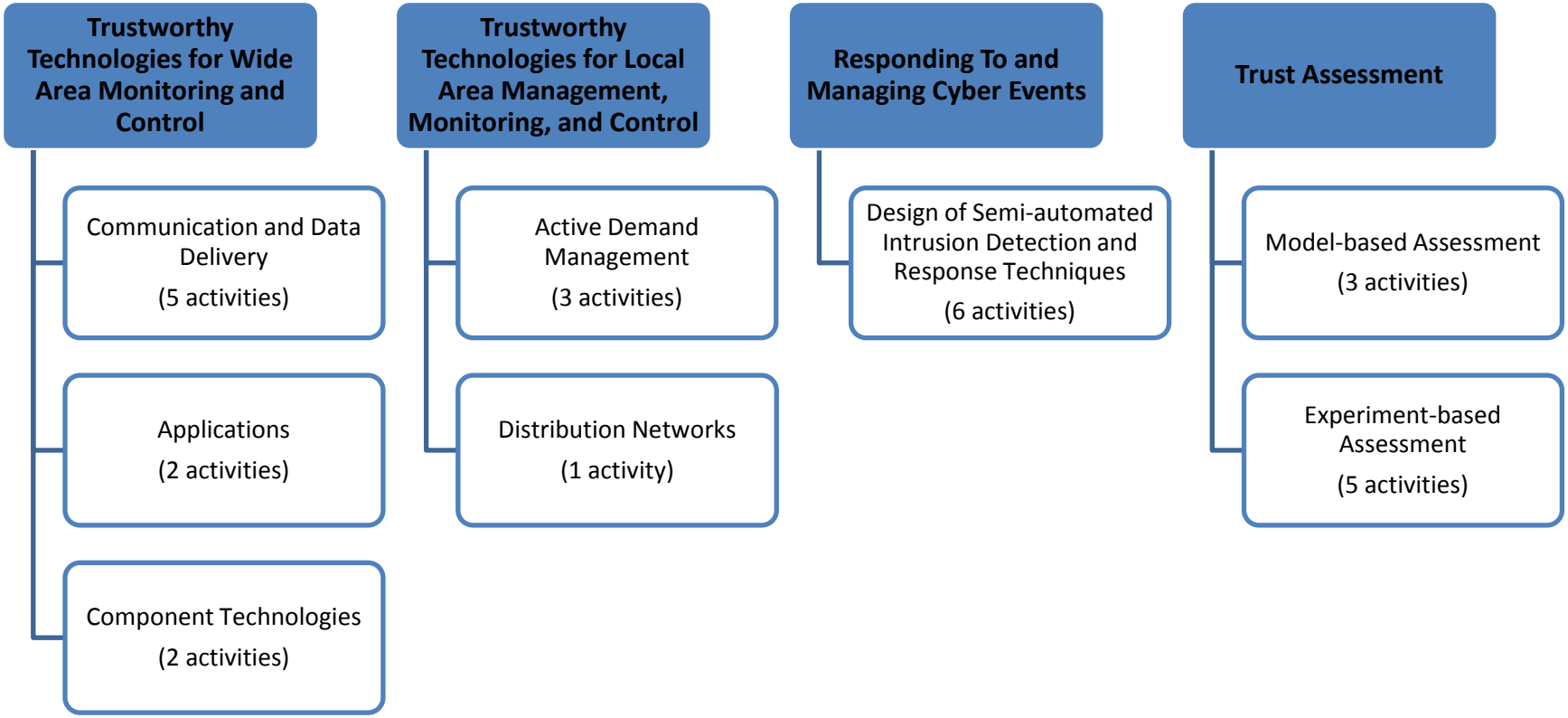
TCIPG Impacts All Aspects of the Roadmap Framework



Technical Approach and Feasibility

- **Approach**
  - TCIPG is a multi-university R&D center
  - Research is organized into four topical *Clusters*, each of which contain a number of *Activities* (28 total)
  - Cross-cutting efforts address Industry Interaction, Education/Outreach, and Testbed
  - Close collaboration with Industry and National Labs
- **Metrics for Success**
  - Impact in the sector in the form of technology and knowledge transfer
  - Collaboration with National Labs; industry; and groups such as IEEE PES, NASPI, GPA, EPRI, and others
  - Publications
  - Workforce development: Graduates placed in industry and academia

TCIPG Technical Clusters and Threads



TCIPG Activities (1)
Trustworthy Technologies for Wide Area Monitoring and Control

Current Efforts

- Cryptographic scalability in the smart grid
- Functional security enhancements for existing SCADA Systems
- GridStat middleware communication framework: Application requirements
- GridStat middleware communication framework: Management security and trust
- GridStat middleware communication framework: Systematic adaptation
- PMU-enhanced power system operations
- Real-time streaming data processing engine for embedded systems
- State-aware decentralized database system for smart grid
- Trustworthy Time Synchronous Measurement Systems

Past Efforts

- CONES: Converged networks for SCADA
- Cooperative Congestion Control in Power Grid Communication Networks
- Decentralized Sensor Networking Models and Primitives for Smart Grid
- Lossless compression of synchrophasor measurement unit archives
- PMU Integration into Power Flow Software
- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications

GridStat Middleware Communication Framework: Management Security and Trust

OBJECTIVES

- Through algorithmic improvements, reduce the latency and increase the security of multi-cast message authentication protocols
  - Current focus: Time-Valid One Time Signature protocol (TV-OTS)
  - Systematically evaluate and reduce cost of all TV-OTS components towards creating viable, low-latency message authentication for sensor data streams
  - Determine operating parameters for TV-OTS that provide both security and good performance
- Create theoretical and practical foundations for trust decision making regarding information sharing and use in the power grid
  - Formal foundation based on modal logic and probabilistic reasoning: proofs of soundness and relative completeness
  - Figure out how to instantiate trust models using data about/from the grid so that trust information improves decision making
  - Improve understanding of risks of cyber-attacks by taking into account probabilistic assessment of both cyber vulnerability and physical consequences
  - Use framework to assess risk of bad data injection attack on PMU data streams

RECENT ACHIEVEMENTS

- Evaluation various of transport-layer vulnerabilities for PMU data streams
  - Attacker effort required for bad data injection or denial of service when using network layer bindings proposed in C37.118-2 standard
  - Influence of operating system and firewall side-channel exposure of TCP sequence number information
- Initial work on replacement protocols not having these susceptibilities

Transport-layer issues for PMU data streams:

- TCP
  - Sequence number predictability due to constant rate, precisely timed output; possible side channels from firewalls and OS error monitoring
  - TCP Veto in which injected data prevents the application layer from getting correct data even if the application can determine the injected data is incorrect
  - Effect of TCP Veto on TCP streams using TLS (does the “veto” become permanent
- UDP
  - Bad data injection
  - How much does DTLS (Datagram TLS) help?
- What are the consequences (good and bad) of using IPSec or other VPN techniques instead of transport-layer security techniques

TCIPG Activities (2)
Trustworthy Technologies for Local Area Management, Monitoring, and Control

Current Efforts

- Development of the information layer for the V2G framework implementation
- Password changing protocol
- Smart-grid-enabled distributed voltage support
- Trustworthy framework for mobile smart meters

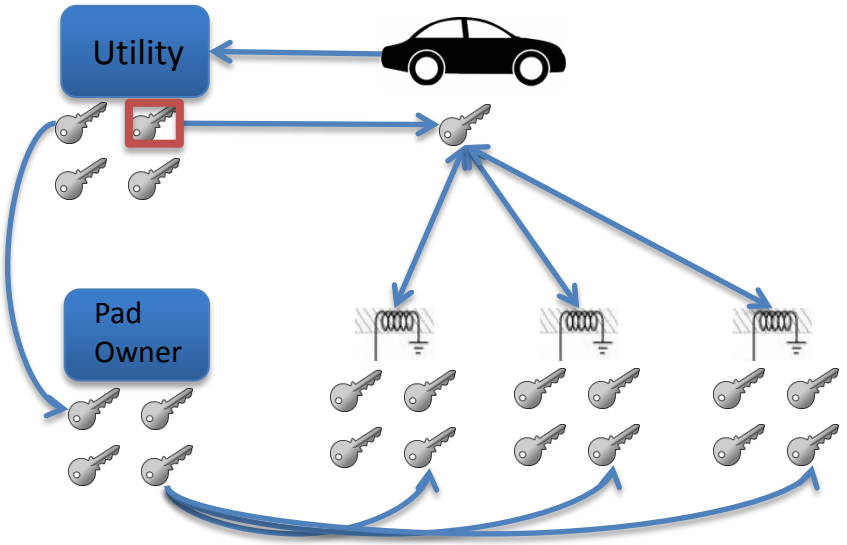
Past Efforts

- Agent Technologies for Active Control Applications in the Power Grid
- Coordinated island operation and resynchronization
- Non-Intrusive Load Shed Verification
- SCADA Secure Wireless Networks

Example Activity:
Trustworthy Framework for Mobile Smart Meters

OBJECTIVES

- Mobile Smart Meters as on-board units of electric vehicle
- Secure data transmission between mobile smart meter and charging station/charging pad
- Fast authentication for dynamic wireless charging of EV



RECENT ACHIEVEMENTS

- We have developed a key pre-distribution based approach for EV-charging pad authentication that supports roaming service and preserves EV's location privacy
- Paper submitted to SmartGridComm'14
- As future work we will implement the protocol on portable computing device such as RaspberryPi and evaluate its performance in practice

TCIPG Activities (3)
Responding To and Managing Cyber Events

Current Efforts

- A game-theoretic response and recovery engine (RRE)
- Assessment and forensics for large-scale smart grid networks
- Detection/Interdiction of Malware Carried by Application-Layer AMI Protocols
- Intrusion Detection for Smart Grid Components by Leveraging of Real-Time Properties
- Specification-based IDS for smart meters
- Specification-based IDS for the DNP3 protocol

Past Efforts

- Coordinating Black Start Operations Using Synchrophasors
- Hardware-based IDS for AMI devices
- Usable management tools for the smarter grid's data avalanche

Example Activity: Specification-based IDS for Smart Meters

OBJECTIVES

- Design an efficient monitoring architecture to detect and potentially prevent intrusions targeting or originating from an Advanced Metering Infrastructure (AMI)
- Implement a prototype of this monitoring solution and validate its accuracy and applicability

RECENT ACHIEVEMENTS

- Continued partnership with FirstEnergy to test prototype in a 36,000-meter AMI
  - Developed and tested a Web interface to enable operators to customize intrusion detection signatures
- Continued collaboration with EPRI to implement failure-driven security policy for AMI
- Initiated collaboration with Fujitsu, UT Dallas, Honeywell, and Sandia to address the challenge of encrypted traffic

TCIPG Activities (4)
Trust Assessment

Current Efforts

- 802.15.4/ZigBee Security Tools
- Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components
- Security and Robustness Evaluation and Enhancement of Power System Applications
- Synchrophasor Data Quality
- Tamper-Event Detection Using Distributed SCADA Hardware
- Testbed-Driven Assessment: Experimental Validation of System Security and Reliability
- Trustworthiness Enhancement Tools for SCADA Software and Platforms
- Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

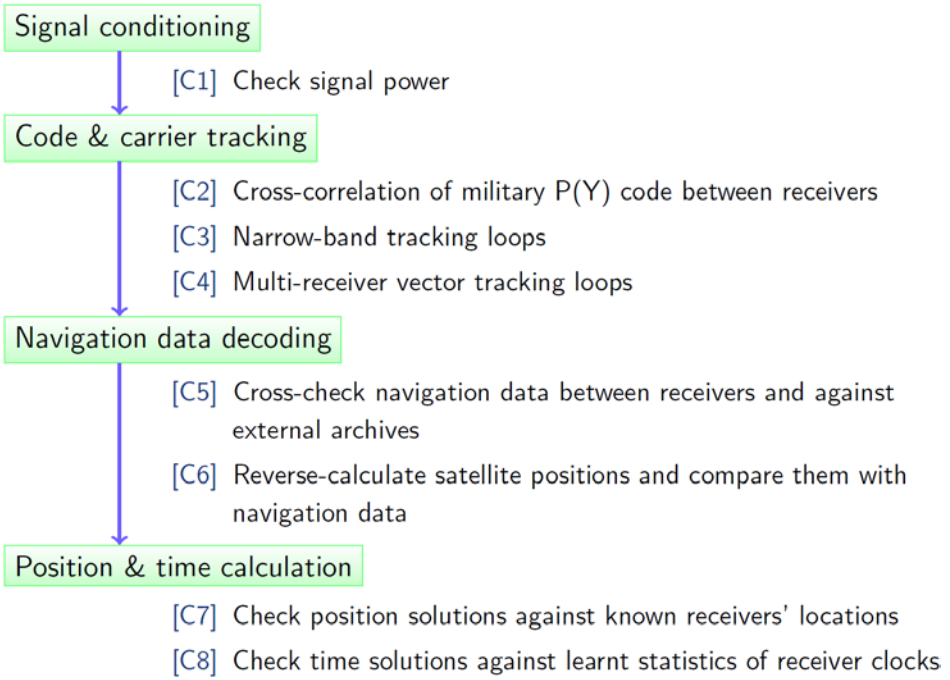
Past Efforts

- Automatic Verification of Network Access Control Policy Implementations
- Fuzz-testing of Proprietary SCADA/Control Network Protocols
- Modeling Methodologies for Power Grid Control System Evaluation
- Smart Grid: Economics and Reliability
- Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks
- Vulnerability Assessment Tool Using Model Checking

Example Activity:
Understanding and Mitigating the effects of GPS Vulnerabilities

OBJECTIVES

- Understand the timing and synchronization needs in power system applications.
- Investigate possible detection and mitigation schemes to harden PMUs against spoofing, jamming, and receiver errors.
- Develop a hardware-based testbed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.
- Develop a trustworthy GNSS-based timing source that is more spoofing-resilient than current GPS-based clocks.



Proposed multi-layer multi-receiver architecture for reliable GPS-based timing for power system applications.

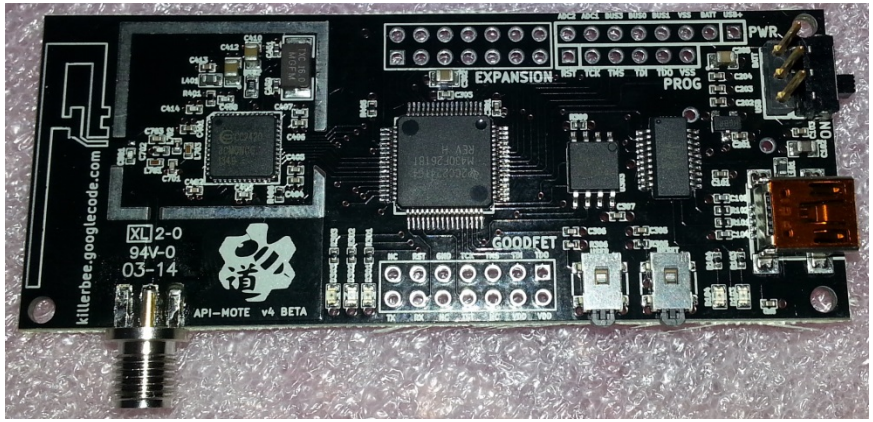
RECENT ACHIEVEMENTS

- Created eight countermeasures to harden GPS-based timing for PMUs
- Theoretical analysis and experiments on [C2].
- Submitted an abstract to ION GNSS+ 2014 conference

Example Activity: 802.15.4/ZigBee Security Tools

OBJECTIVES

- Production of a cheap, easy-to-configure 802.15.4 radio peripheral
- Full support for popular 802.15.4 platforms accessible to SCADA asset owners
- Kismet-like GUI familiar to users of "wardriving" Wi-Fi auditing tools

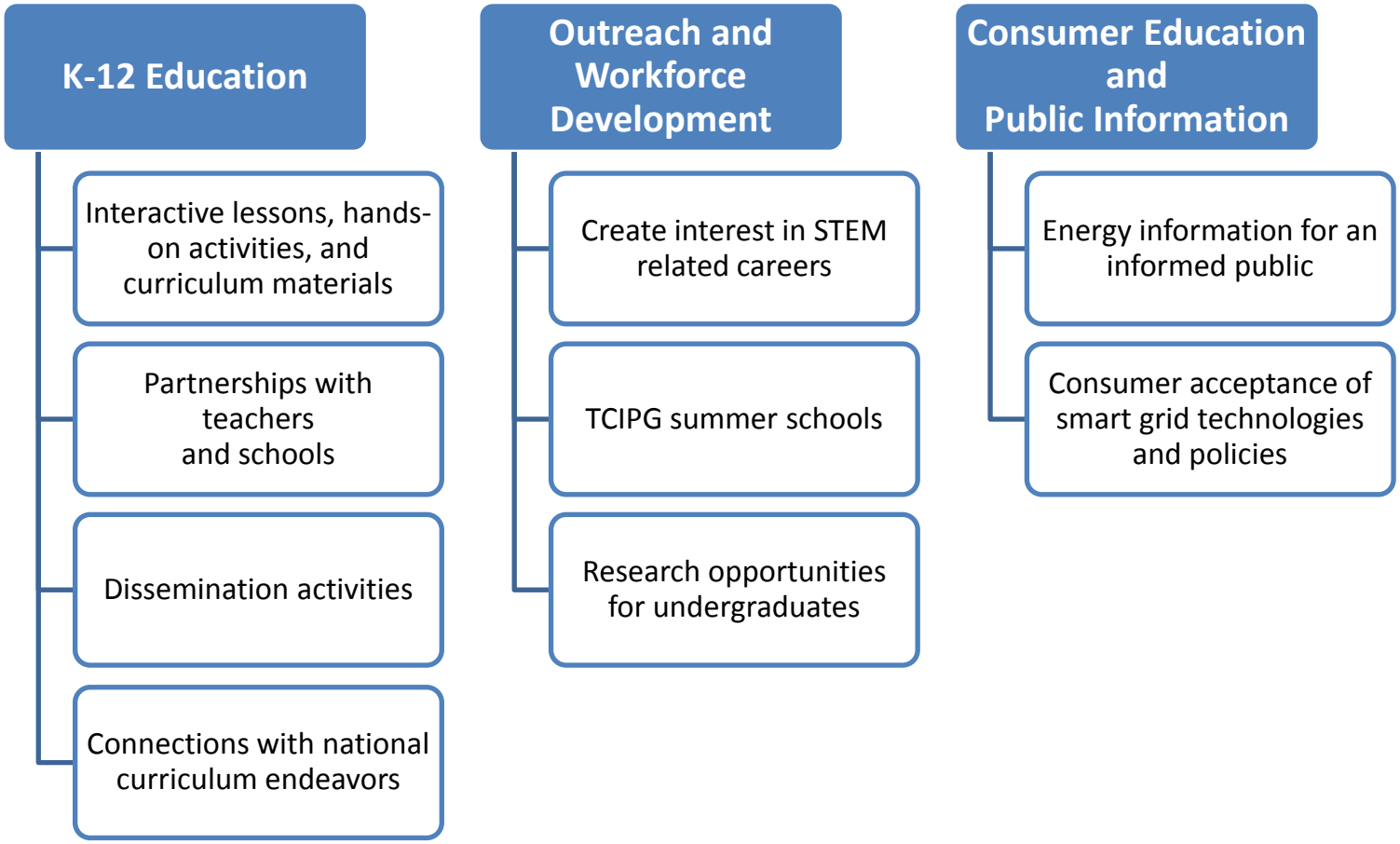


RIVER LOOP SECURITY

RECENT ACHIEVEMENTS

- APImote v4 open source design donated by River Loop produced, released at Troopers.de industry conference & distributed to security industry researchers.
- Fingerprinting results & techniques for 802.15.4 digital radios confirmed, submitted to ACM WiSec & published in Dartmouth TR2014-746
- WIDS/WIPS evasion techniques utilizing PHY-level frame crafting confirmed, described in updated Dartmouth TR2014-749

Cross-Cutting Effort: Education and Engagement



Education and Engagement

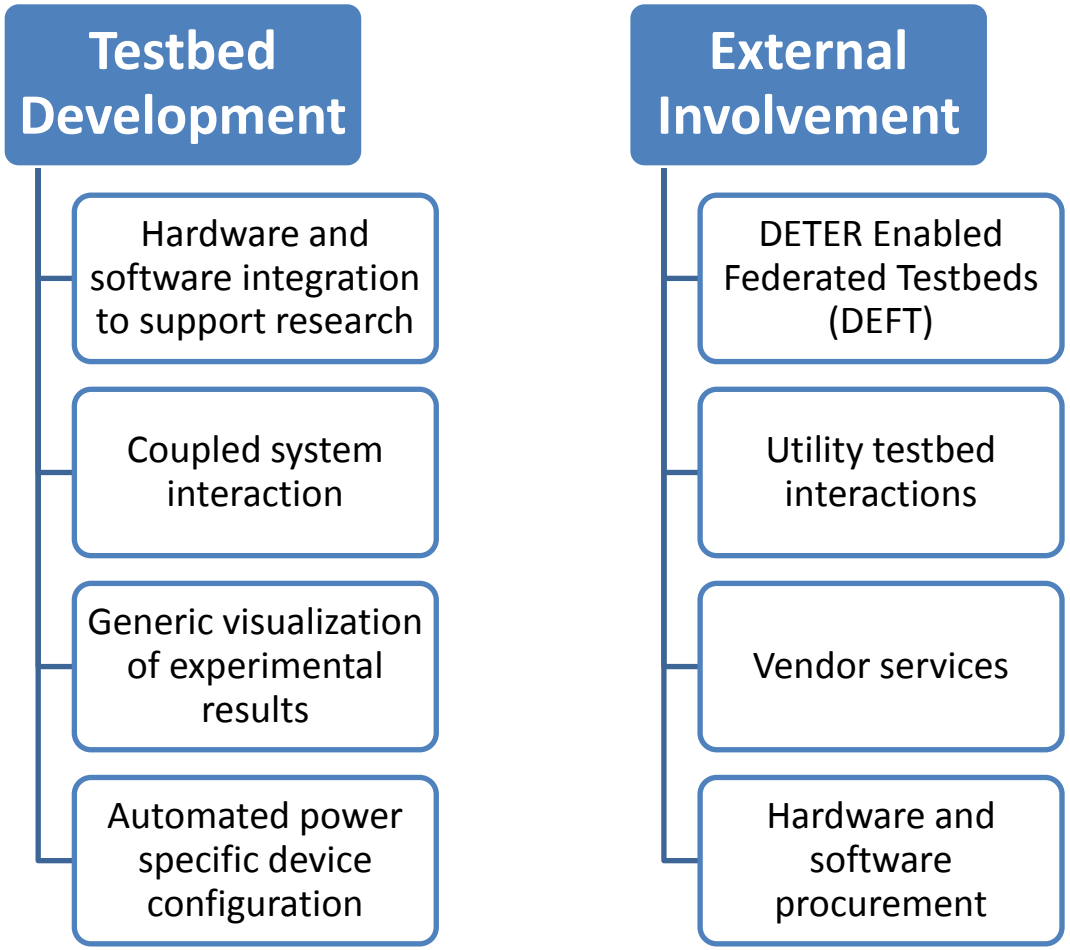
OBJECTIVES

- Create curriculum to connect researchers, educators, consumers, and students
- Develop hands-on and virtual activities
- Partner with national curriculum endeavors, teachers, and schools
- Create interest in STEM careers
- Participate in professional conferences and community events

RECENT ACHIEVEMENTS

- Established a TCIPG MinecraftEdu server that invites players into a smart grid world Students at Urbana Middle School will begin exploring this world in early April
- Work continues on Charge On, a electric grid strategy game for IOS 7 devices
- TCIPG Education participated in the 2014 Illinois Public Engagement Symposium on March 11 and in Agora Days 2014 at University of Illinois Laboratory High School

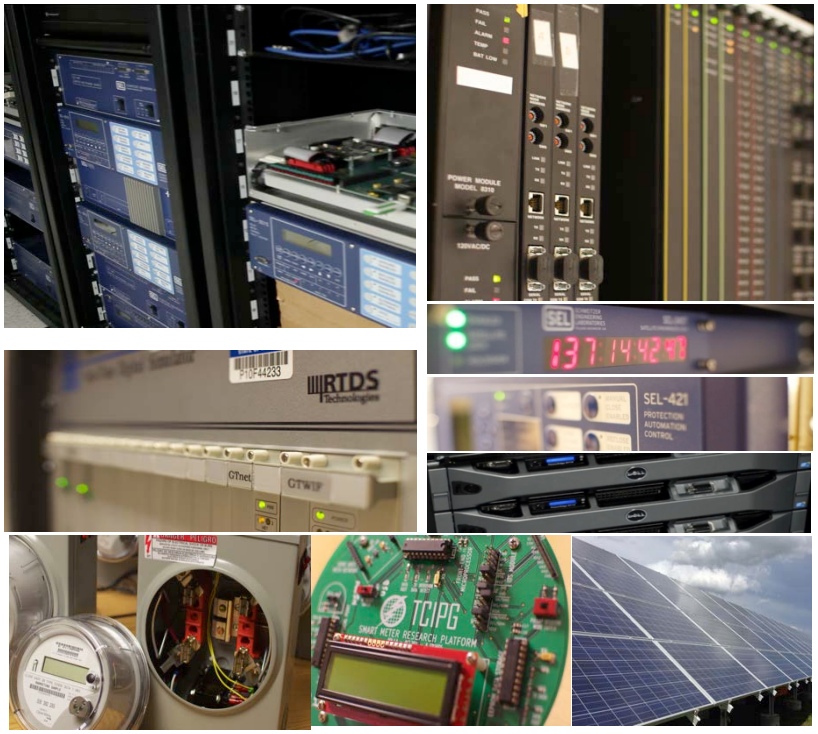
Cross-Cutting Effort: Testbed Initiatives



Testbed Overview

OBJECTIVES

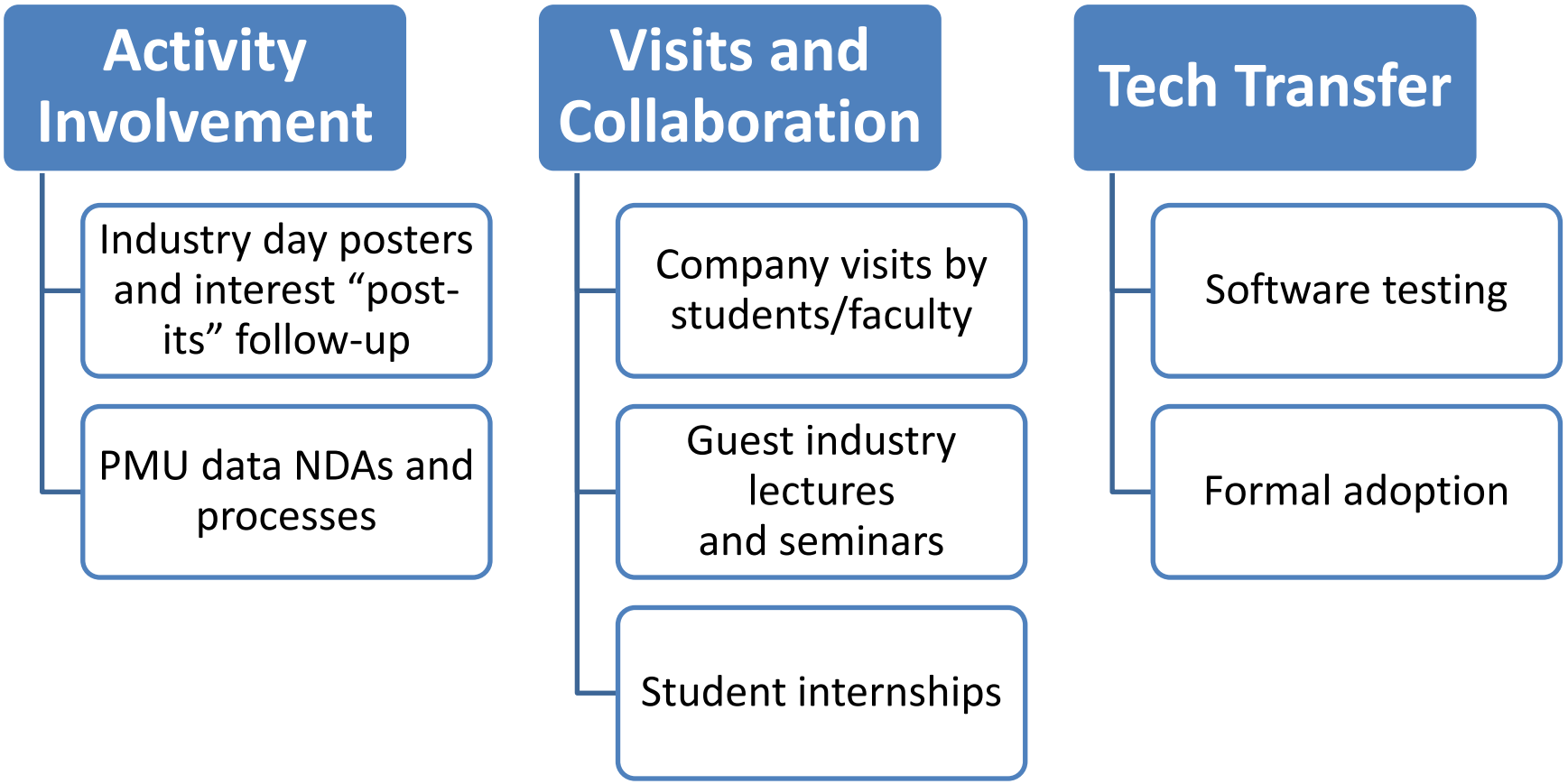
- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities
- Provide foundational support for TCIPG projects
- Analyze research through varying fidelities and scales
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems



RECENT ACHIEVEMENTS

- Brought in additional backup and disaster recovery options for the lab.
- Started new training/education based activity leveraging testbed prior work.
- Positioning testbed activities and resources for transition to practice.

Cross-Cutting Effort: Industry Interaction and Technology Transition



Industry Interaction & Tech Transfer (Jan. – Mar. 2014)

- FERC Commissioner, Tony Clark, visited the UC Davis TCIPG team in January. His visit included tours of UC Davis labs and a video conference meeting with TCIPG Illinois researchers.
- UC Davis continues to collaborate with researchers at LBNL.
- The IDS for SGC team is working with a utility partner for analyzing real network traces; a power system vendor who may provide a system and code with real-time properties for managing control systems.
- The IDS for SGC team continues to work with researchers from Qualcomm.
- The IDS for DNP3 team is working with engineers from Ameren to test the DNP3 analyzer in Bro towards network traffic collected from real substations.
- TCIPG was invited to attend and present at a UNITE Security Directors Meeting. The group is comprised of security directors representing 20 of the largest electric utilities.

Industry Interaction & Tech Transfer (Jan. – Mar. 2014)

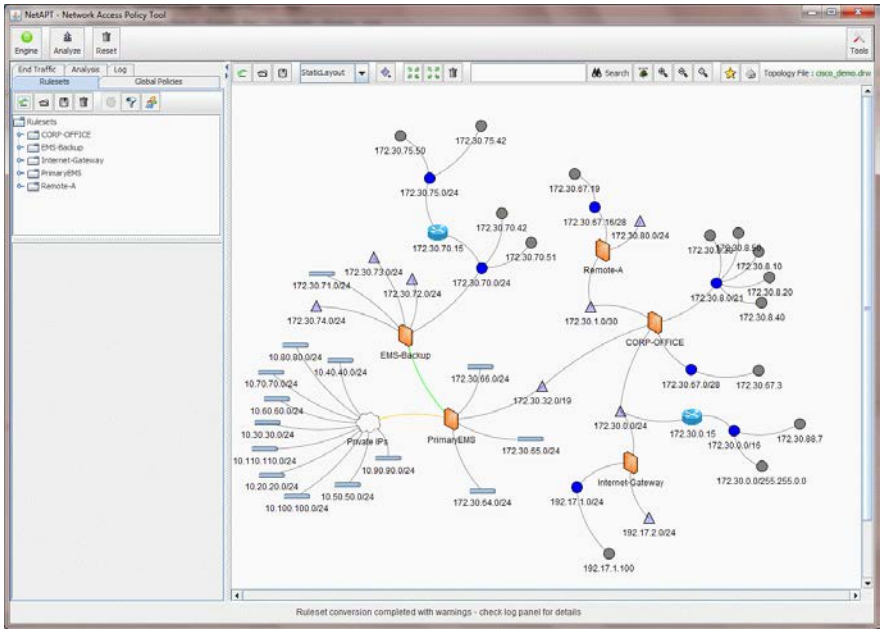
- The Robust Power Applications team is working with a major technology company to define a security model for power system applications in the cloud.
- The Synchrophasor Data Quality team continues to work with ATC to investigate synchrophasor data quality using ATC data from 90+ PMUs.
- The Synchrophasor Data Quality team continues collaboration with PNNL to leverage the SitAAR analysis tool in its research efforts.
- Ryan Bradetch of SEL is serving on Jason Reeves' thesis committee. Ryan also visited Dartmouth to discuss future collaboration with tamper-event detection research.

Industry Interaction & Tech Transfer (Jan. – Mar. 2014)

- The ELFbac prototype is undergoing a private code review.
- We have a patent pending for “Robust and Secure Timing Device Based on Multiple Cooperative GNSS Receivers,” resulting from our initial disclosure that was filed with the Office of Technology Management in October 2013.
- We emailed our industry friends asking for concerns and topics for which TCIPG Education could provide informational posters or short videos that could improve work place security. Based on this feedback our first project is to produce a series of posters related to password safety.

Example Technology Transfer: Network Perception, Inc.

- Based on NetAPT technology developed under TCIPG
  - Static analysis of firewall rulesets
  - Tuned to utility systems, where identifying routable paths to critical cyber assets is an increasingly important problem
- Pilot deployment at major IOUs as technology matured
  - Demonstrated usefulness in NERC CIPS audits
- Used in security assessment of rural electric cooperative utility networks
- Transition of NetAPT from an academic project to a commercial product has been supported at UIUC by a one-year grant from DHS S&T



Network Perception is now a technology startup

2014 Industry Workshop

- **November 12-13, 2014 (Reception Nov. 11)**
  iHotel and Conference Center
- **Email us to request an invitation**
- **Industry Panel Topics**
  - Challenges of Cybersecurity Economics in Distribution Systems
  - Security of Cloud Computing for the Power Grid
  - Case Studies of Cybersecurity in Smart Grid Deployments
  - Cybersecurity for Smart Buildings and Microgrids

2014 Industry Workshop

Confirmed Industry Panelists

- **Challenges of Cybersecurity Economics in Distribution Systems**
  - Mark Browning, Exelon
  - Steve Dougherty, IBM
  - Robert Kolasky, DHS
  - Carolene Mays, Indiana Utility Regulatory Commission
- **Security of Cloud Computing for the Power Grid**
  - Jeff Katz, IBM
  - Xiaochuan Lu, ISO New England, Inc.
  - Craig Miller, NRECA
  - David Norton, FERC
- **Case Studies of Cybersecurity in Smart Grid Deployments**
  - Phil Craig, PNNL
  - James Sample, PG&E
  - David Scott, Accenture
  - TBA, SCE
- **Cybersecurity for Smart Buildings and Microgrids**
  - Jonathan Butts, USAF Research Lab
  - Lisa Kaiser, DHS (formerly ICS-CERT, now FRC)
  - Himanshu Khurana, Honeywell
  - Billy Rios, Qualys

To Learn More

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Request to be on our mailing list
- Attend our Industry-Govt. Workshop Nov. 12-13, 2014
- Attend Monthly Public Webinars
- Attend our TCIPG Summer School June 2015