Building Resilience into the Smart Grid

Bill Sanders

University of Illinois at Urbana-Champaign
www.tcipg.org
whs@illinois.edu

Great Lakes Symposium
September 25, 2013

Outline

- Challenge, Vision, and Roadmap
- 4 Key Challenges
- TCIPG Vision and Research Focus
- Industry / Academic Interaction in Research

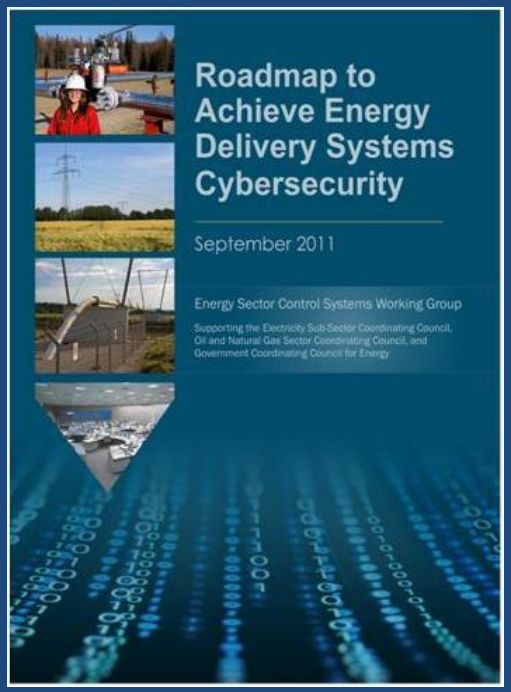
The Challenge: Providing Trustworthy Smart Grid Operation in Possibly Hostile Environments

- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Availability, Security, Safety, …
- Hostile Environment
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.

Trustworthiness through Cyber-Physical Resiliency

- Physical infrastructure has been engineered for resiliency ("n-1"), *but*
- Cyber infrastructure must also be made resilient:
  - Protect the best you can (using classical cyber security methods optimized for grid characteristics), but
  - Detect and Respond when intrusions succeed
- *Resiliency of overall infrastructure dependent on both cyber and physical components*
- Approaches must be developed that make use of sound mathematical techniques whose quality can be proven (need a *science* of cyber-physical resilience)

Industry Roadmap – A Framework for Public-Private Collaboration



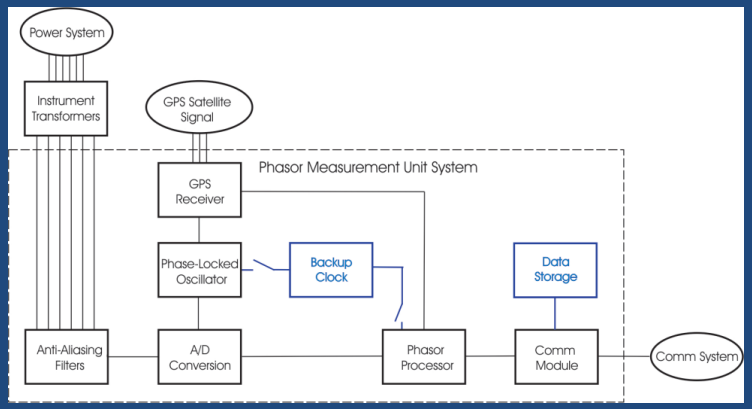
- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Challenge 1: Trustworthy technologies for wide-area monitoring and control

- Smart Grid vision for the wide area (primarily transmission) is:
  - Vastly more sensing at high, synchronous rates (example: PMUs)
  - New applications that use these data to improve
    - Reliability
    - Efficiency
    - Ability to integrate renewables



- Achieving the vision requires secure and reliable communications between sensors, control devices, and monitoring and control applications all owned and operated by the many entities that make up the grid

Challenge 2: Trustworthy technologies for local area management, monitoring, and control

- Electric grid can be divided into three groups: the generation, the wires (T&D), and the demand. This challenge focuses on the demand and the nearby distribution
  - Generation must track load
- For a grid with more renewable, but less controllable generation (e.g., wind and solar PV), more load control will be needed

  - Distributed generation may be embedded in “demand”
  - New loads (electric vehicles) could drastically change demand profile

Challenge 3: Responding to and managing cyber events

- Combined cyber and physical attack detection, response to detected attacks, and recovery from attack consequences is essential to providing resilience
- Existing detection and response methods are *ad hoc*, at best, and rely on assumptions that may not hold
- Aim to detect and respond to cyber and physical events, providing resilience to partially successful attacks that may occur:
  - Making use of cyber and physical state information to detect attacks
  - Determine appropriate response actions in order to maintain continuous operation
  - Minimize recovery time when disruptions do occur

Challenge 4: Trust and Risk Assessment

- Define appropriate security metrics
  - Integrated at multiple levels
  - Applied throughout system lifecycle
  - Be both “process” and “product” oriented
- Determine methods for estimating metrics
  - To choose appropriate architectural configuration
  - To test implementation flaws, e.g., fuzzing, firewall rule analysis
  - Can be applied in cost effective manner *before* an audit
- Which link technical and business concerns

Smart Grid Security Efforts @ Illinois

TCIPG: Trustworthy Cyber Infrastructure for the Power Grid

- Drive the design of an resilient cyber infrastructure electric power which operates through attacks
- $18.8 M over five year, started Oct. 1, 2010
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

Smart Grid Subprogram

~$15M effort / 5 years

Projects in Microgrids, DERs, and HANs

Korean National Smart Grid TestBed on Jeju Island.

MOU concerning tesbed and cyber security research

CACAIS

Testbed

Products tested & validated in CACAIS testbed: $1.2M FY10 funding from ONR

Illinois Center for a Smarter Electric Grid

Validation & Compliance Services

- $4.0 M funding from State
- Test bed & lab equipped with HW/SW to perform validation of Smart Grid systems
- Critical Infrastructure Protection (CIP): pre-audit check for compliance to NERC standards
- Prepare for NERC reliability compliance audits

4 DOE Office of Electricity Security Projects with:

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Entergy THE POWER OF PEOPLE

GRID PROTECTION ALLIANCE

DTE Energy

Telcordia

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest NATIONAL LABORATORY

pjm

GRID PROTECTION ALLIANCE

ALSTOM

Honeywell

INL

TCIPG Vision and Research Focus

Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today's and tomorrow's power grid, so that it operates through attacks

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience

TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009 ($3.8M cost share)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cybersecurity R&D Center, Office of Science and Technology
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 23 Faculty, 20 Technical Staff, 38 Graduate Students, 7 Ugrad Students, 1 Admin Staff worked on the project in FY 2012

TCIPG Technical Clusters and Threads

Trustworthy Technologies for Wide Area Monitoring and Control

- Communication and Data Delivery (4 activities)
- Applications (2 activities)
- Component Technologies (3 activities)

Trustworthy Technologies for Local Area Management, Monitoring, and Control

- Active Demand Management (3 activities)
- Distribution Networks (2 activities)

Responding To and Managing Cyber Events

- Design of Semi-automated Intrusion Detection and Response Techniques (6 activities)

Trust Assessment

- Model-based Assessment (6 activities)
- Experiment-based Assessment (5 activities)

TCIPG Activities (1)

Trustworthy Technologies for Wide Area Monitoring and Control

Ongoing

- 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

Completed

- CONES: Converged networks for SCADA
- Lossless compression of synchrophasor measurement unit archives
- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications

Trustworthy Technologies for Local Area Management, Monitoring, and Control

Ongoing

- 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

Completed

- Coordinated island operation and resynchronization

TCIPG Activities (2)

Responding To and Managing Cyber Events

Ongoing

- A game-theoretic response and recovery engine (RRE)
- Assessment and forensics for large-scale smart grid networks
- Hardware-based IDS for AMI devices
- Specification-based IDS for smart meters
- Usable management tools for the smarter grid's data avalanche

New Starts

- Specification-based IDS for the DNP3 protocol

Trust Assessment

Ongoing

- Analysis of impacts of smart grid resources on economics and reliability of electricity supply
- Automatic verification of network access control policy implementations
- Modeling methodologies for power grid control system evaluation
- 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
- Test-bed driven assessment
- Trustworthiness enhancement tools for SCADA software and platforms
- Vulnerability assessment tool using model checking

Completed

- Tools for assessment and self-assessment of ZigBee networks
- Fuzz testing of proprietary SCADA/control network protocols

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

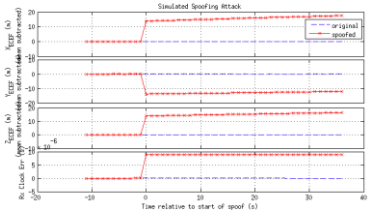
- Continued partnership with FirstEnergy to test prototype in a large AMI testbed
- Continued collaboration with EPRI to implement failure-driven security policy for AMI
- Presentation of Amilyzer during TCIPG Summer School

Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

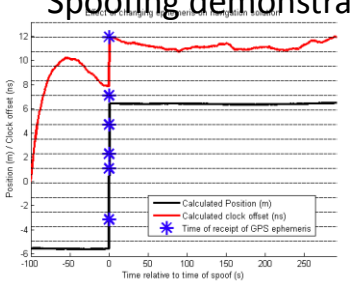
Objectives

- Develop a hardware-based testbed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.
- Demonstrate the feasibility of an attack using this hardware setup.
- Investigate possible detection and mitigation schemes to harden PMUs to GPS spoofing attacks.

Spoofing simulation



Spoofing demonstration



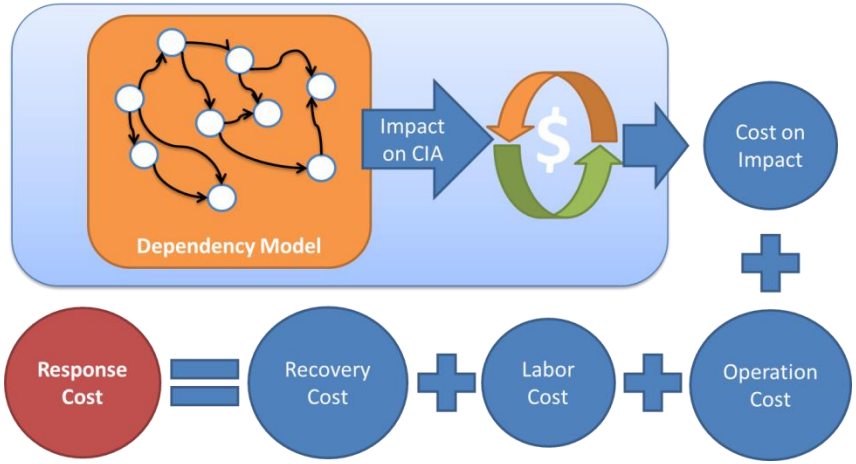
Recent Achievements

- We have conducted a survey of the use of GPS in the power sector and written a preliminary document giving an overview of the current state-of-the-art in GPS spoofing attacks and mitigation schemes.
- We have assembled the necessary hardware to build a GPS simulator through which we will test various GPS spoofing attacks.

A Game-Theoretic Intrusion Response and Recovery Engine

Objectives

- Reactive response against adversarial attacks that uses knowledge about the power grid's current security-state and its security level.
- Design a modular distributed self-stabilizing response and recovery engine
- Verify safety of the automated system

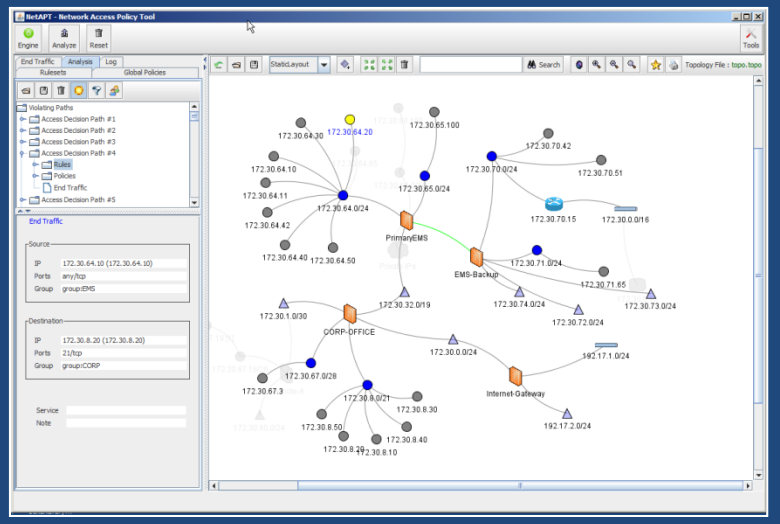


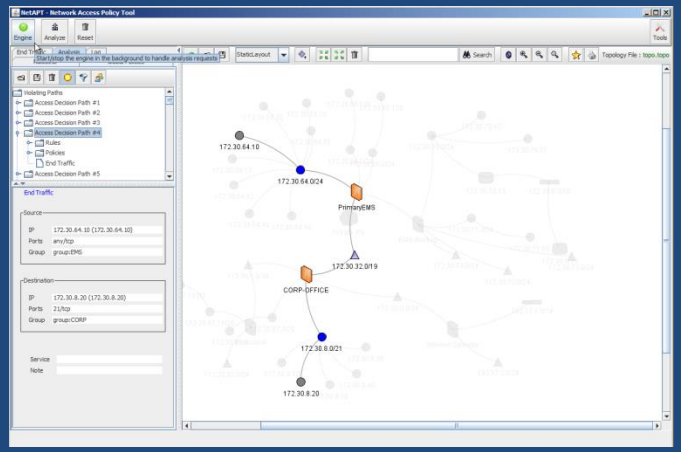
Recent Achievements

- Started an SEL affiliated project to study the use of Software-Defined Networks (SDN) to implement intrusion responses
- Utilized an OpenFlow switch to detect DNP3 attacks using SNORT and respond accordingly

NP-View NERC CIP Security Assessment

- NP-View identifies routable paths to network nodes, including critical cyber assets in energy delivery systems
- Mature TCIPG technology
  - Development continues to increase the number of firewalls supported
- More than 40 copies have been licensed to NERC auditors and utilities, including SERC, SPP, WECC, Ameren, PJM, and 3 Electric Cooperatives (AEIC, EIIEC, and Cornbelt Energy)
- Used as a NERC-CIP audit tool
- Commercialization grant from DHS





Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks

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

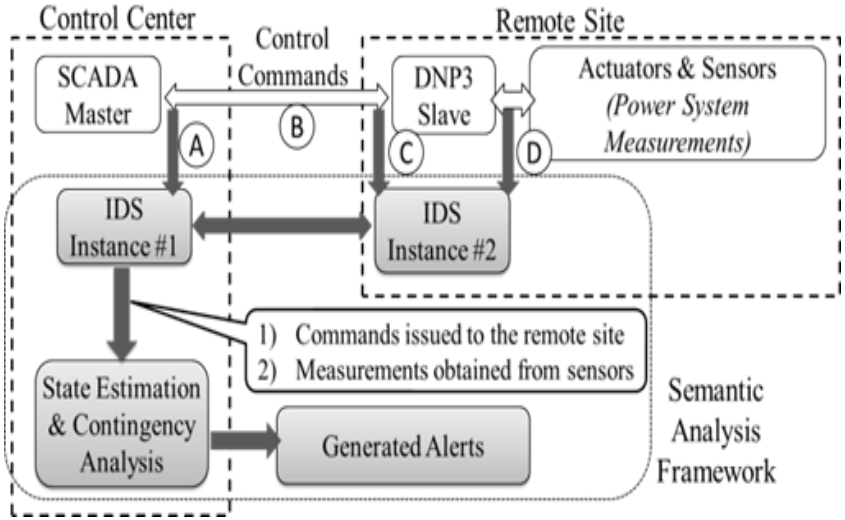
Recent Achievements

- Released KillerBee support for Zigduino (popular Arduino-based digital radio from AVR) under GoodFET drivers; also, released updated GoodFET drivers for Zigduino.
- Both of the above are released under the BSD license to the projects SVN repository (http://goodfet.sourceforge.net/)
- River Loop and contributors added tools to KillerBee, zbkey and soon zbHAtoggle
- River Loop upgraded KillerBee to support pyUSB1.0 to allow it to coexist with Ubertooth, a popular Bluetooth sniffing hardware platform.
- APImote v2 is finally in production; initial run is being assembled.

Specification-based IDS for DNP3 Protocol

Objectives

- Propose and experimentally evaluate a framework based on distributed Bro IDS instances to detect attacks that penetrate power system by means of maliciously crafted control commands sent to power substations
- Combine system knowledge on cyber and physical infrastructure in power grid to proactively estimate consequences of control commands and thus, to reveal attacker's malicious intentions
- Augment Bro IDS with power flow assessment tools to perform run-time contingency analysis



Semantic Analysis Framework

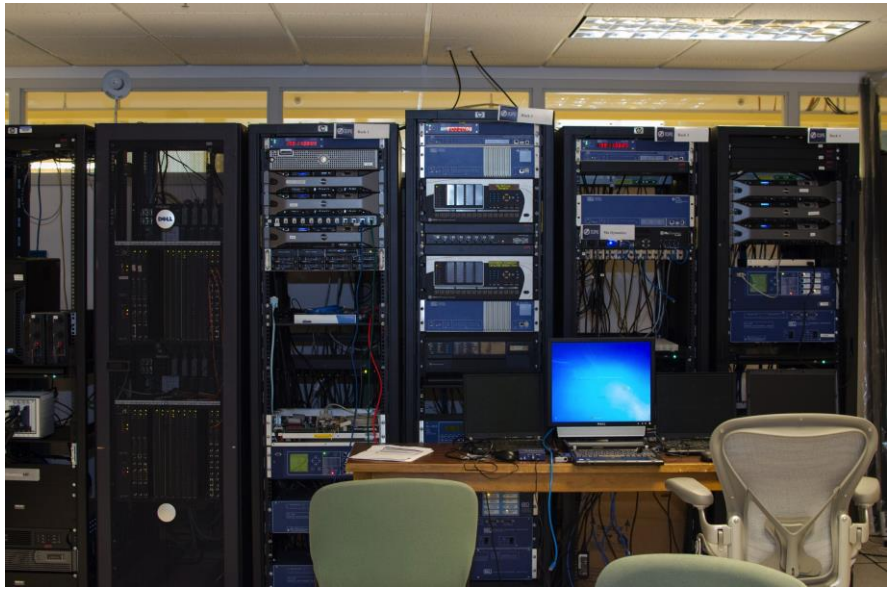
Recent Achievements

- Further code optimization on the implemented DNP3 analyzer
- Combine Bro-IDS with power flow analysis toolbox to provide run-time contingency analysis to enable detection of legitimate but maliciously crafted control commands sent to power substations
- Evaluate the approach on the IEEE 30-bus system
- Further research on how to perform preemptive responses on attacks so to prevent potential physical damages to the system

Testbed Development

Objectives

- Extend and augment testbed facilities to support TCIPG research through existing and new capabilities
- Increase automation of experiment configuration for cyber-physical systems
- Operate as a pipeline for technology advancement and transition



Recent Achievements

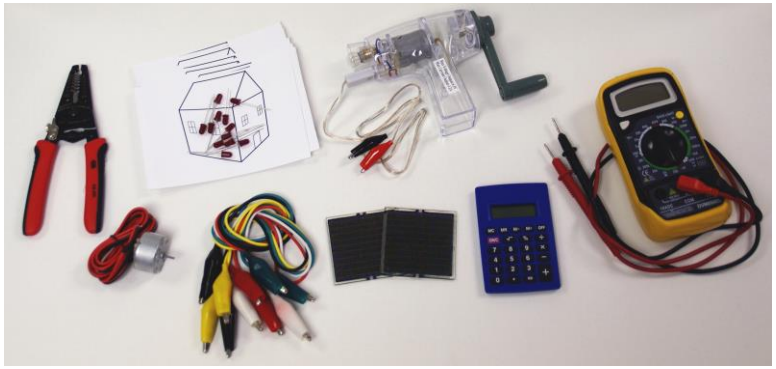
- Created SCADA Security Assessment Lab (mini and primary portable)
- Increased automation and integration
- Exploring options for external testbed facility use
- Building more relationships for engaging with TCIPG research in the testbed
- Increasing engagement with Utilities, Vendors, and other testbeds


SEL-421
SEL
RTDS ™
Real-Time Digital Simulator
RTDS Technologies
DIGITAL CHANNELS
GROUND
DIGITAL OUT


DANGER / PELIGRO
HAZARD OF ELECTRICAL SHOCK OR BURN
SERVICE BY UTILITY AUTHORIZED PERSONNEL ONLY
DO NOT PAINT OVER OR REMOVE THIS LABEL
PELIGRO DE DESCARGA ELECTRICA O QUEMADURA
SOLAMENTE PERSONAS AUTORIZADAS DE LA COMPANIA ELECTRICA PUEDEN MANTENERLO
NO PINTE ENCIMA NI REMUEVA ESTA ETIQUETA
CL200 240V 3W TYPE C2SQD 30TA 1.0Kh
MARKETING SAMPLE
306 382 306
306 382 289
OpenWay

Education and Engagement

Objectives

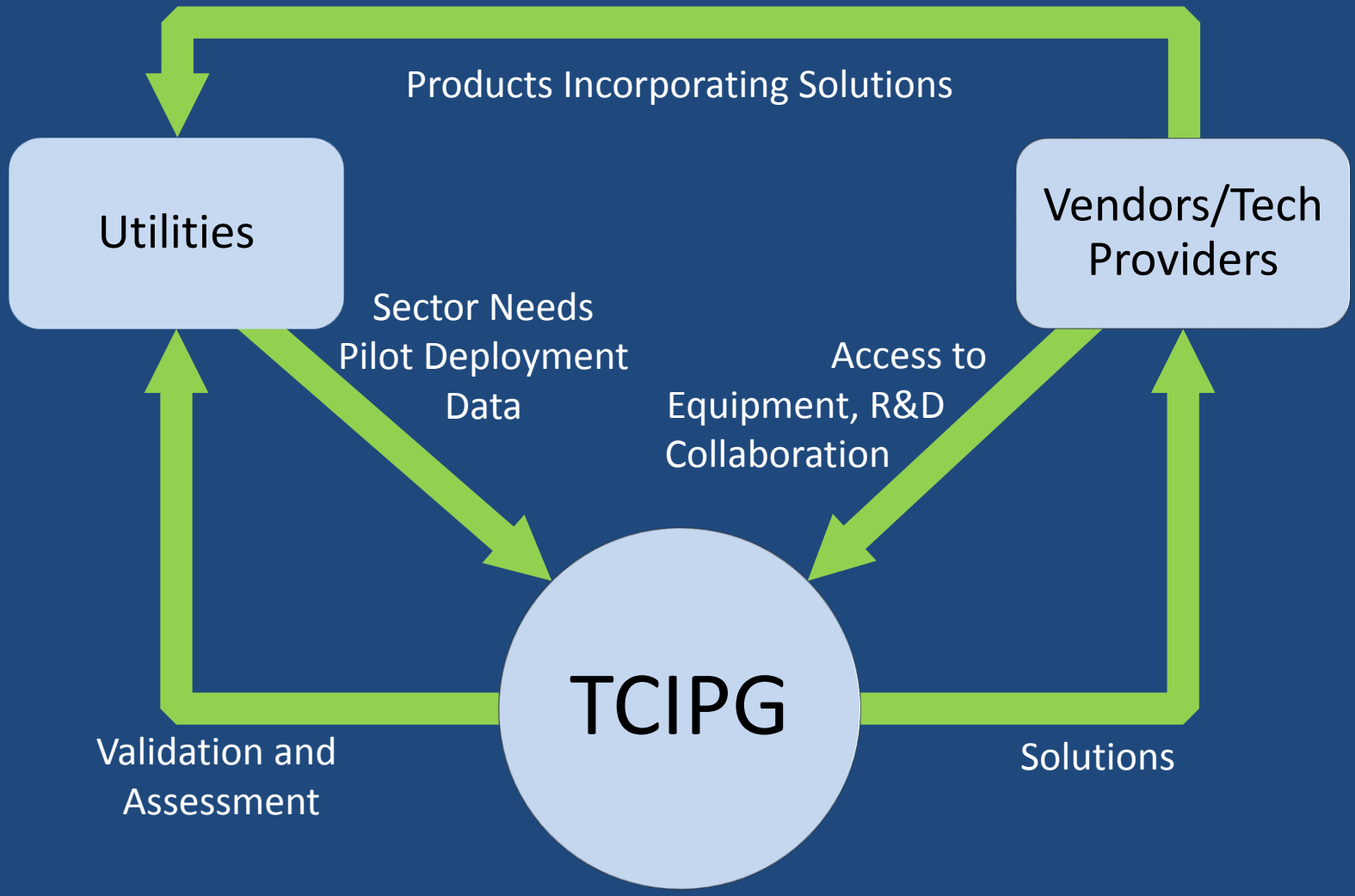


- Link researchers, educators, consumers, and students
- Connect with schools and national curriculum endeavors
- Develop interactive lessons and activities available on the web and for touch tablet devices
- Create interest in STEM disciplines and careers
- Illustrate issues necessary for consumer acceptance and use of smart grid technologies

Recent Achievements and Events

- TCIPG Education has launched a new website, Exploring Solar The site offers materials for teaching and learning about solar power. The resources and activities are designed to offer insights into the advantages and limitations of PV panels and to generate discussion about how solar power may become a part of the world's energy mix.
- TCIPG Educational materials were showcased at the following events:
  - DHS's Kids Day at S&T in Washington D.C., April 25, 2013
  - IRISE Engineering Design for middle school students campus field trip, May 3
  - TCIPG Summer School in St. Charles, IL, June 17, 2013
  - ASEE 10th Annual K-12 Workshop on Engineering Education at The Georgia World Congress Center in Atlanta, Georgia, June 22, 2013

TCIPG as Catalyst for Accelerating Industry Innovation



Industry Interaction: Vendors and Utilities that have participated in TCIPG Events

Webinars on Technologies for a Resilient Power Grid

Monthly seminars are presented live and webcast to academic, government, and industry stakeholders in power grid resiliency. Seminars are presented at 1PM/CT.

Friday, September 6, 2013
Presenter: Robin Berthier,
Information Trust Institute and
Network Perception

Friday, October 4, 2013
Presenter: Daniel Thanos
Chief Cyber Security Architect
GE Digital Energy

Friday, November 1, 2013
Presenter: Anna Scaglione
Professor, UC Davis

Friday, December 6, 2013
Presenter: TBD

Industry Workshop and Annual Review

iHotel and Conference Center
November 6-7, 2013

- Dinner Reception, Tuesday 11/5
- Wednesday Agenda
  - Research Presentations
  - Industry Panels
  - Poster Session/Dinner Reception
- Thursday Agenda
  - More Sessions until lunch
  - Private annual review at CSL to follow after lunch

Annual Industry Workshop – Industry Panels

- **Supply Chain Cybersecurity for Energy Delivery Systems**
  - Nadya Bartol, Utilities Telecom Council
  - Ido Dubrawsky, Itron
  - Dennis Gammel, Schweitzer Engineering Laboratories
  - Jessica Smith, PNNL
- **Implications of Cloud Computing on the Security of Grid Systems**
  - Art Anderson, PG&E
  - Alvaro Cardenas, UT Dallas
  - William Hadala, iWire365
  - Craig Miller, NRECA

Annual Industry Workshop – Industry Panels

- **Managed Security Services for the Electric Sector**
  - Phil Craig, PNNL
  - Bill Menter (or Phil Mar), ViaSat
  - William Souza, PJM
  - TBD, McAfee
- **Executive/Legislative Actions Affecting Energy Delivery Systems Cybersecurity**
  - Joe Bucciero, Corporate Risk Solutions
  - Don Harris, Sargent & Lundy
  - Scott Mix, NERC

Summary

- TCIPG is addressing a complex, multifaceted mission
- TCIPG is a world-leading research center, but uniquely positioned with relationships to industry
  - Identifying and taking on important hard problems
  - Unique balance of long view of grid cyber security, with emphasis on practical solutions
  - Working to get solutions adopted
- TCIPG is an important research nucleus, enabling additional valuable industry/academic collaboration

To Learn More

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Pete Sauer
- psauer@illinois.edu
- Tim Yardley
- yardley@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our Industry Workshop Nov. 6-7, 2013