# TCIPG Overview

Bill Sanders
on behalf of the TCIPG Team

November 7, 2011

# Welcome to the TCIPG 2011 Industry Workshop

- Who is here?
  - TCIPG researchers and students
  - representatives of industry: utilities, vendors, national labs, ...
  - our sponsors and external advisory board
- Why have an annual industry workshop?
  - For TCIPG and sponsors:
    - to have impact
    - to communicate our results
    - to help choose our research well
  - For industry:
    - to discover and explore TCIPG research
    - to influence future directions
    - to form productive collaborations that can profitably shape the evolving Smart Grid

# Welcome to the TCIPG 2011 Industry Workshop, cont.

- What happens during the Industry Workshop?
  - sharing TCIPG research results and directions
  - listening and learning about industry's perspective
- Purpose of this talk?
  - introduce TCIPG – provide context for navigating the next day and a half: who we are, what we do, and why we do it
  - invite your active participation in workshop and in the longer term as well

# 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
  - Malicious Attacks
  - Accidental Failures
  - Design Flaws
- Cyber Physical
  - Must make the whole system trustworthy, including physical components, cyber components, and their interactions

# A Brief History …

- SCADA systems were designed without specific attention to security
  - Security improvements were achieved by application of standard cyber security practices
- As cyber component of grid grew (and became “smart”) standard security practices were not sufficient
  - Security was “bolted-on” or “built-in” to many vendor products, but was largely limited to prevention
  - Cyber security solutions were specialized to the grid to deal with issues related to scale, embedded and exposed nature, cost, and importance of availability
  - But not all attacks can be prevented, so gaps still remained, and resilience approaches are needed …

# and a Prediction …

- In the envisioned grid of the future,
  - Generation, transmission, and distribution will become co-mingled
  - Islanding, reintegration, and microgrids will become the norm
  - Consumer end devices and ubiquitous sensors/actuators throughout the grid will produce/require an “avalanche” of data
  - Many of these devices/sensors will be outside the administrative and physical control of the utilities that rely on them
  - Energy markets could become as complex (and as risky) as derivative-based financial markets of today
  - Distributed stability maintenance will be the only option
  - Fundamentally new approaches to cyber security and resilience (both cyber and power system) will be required

# TCIPG Vision & Research Focus

**Vision**: Drive 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

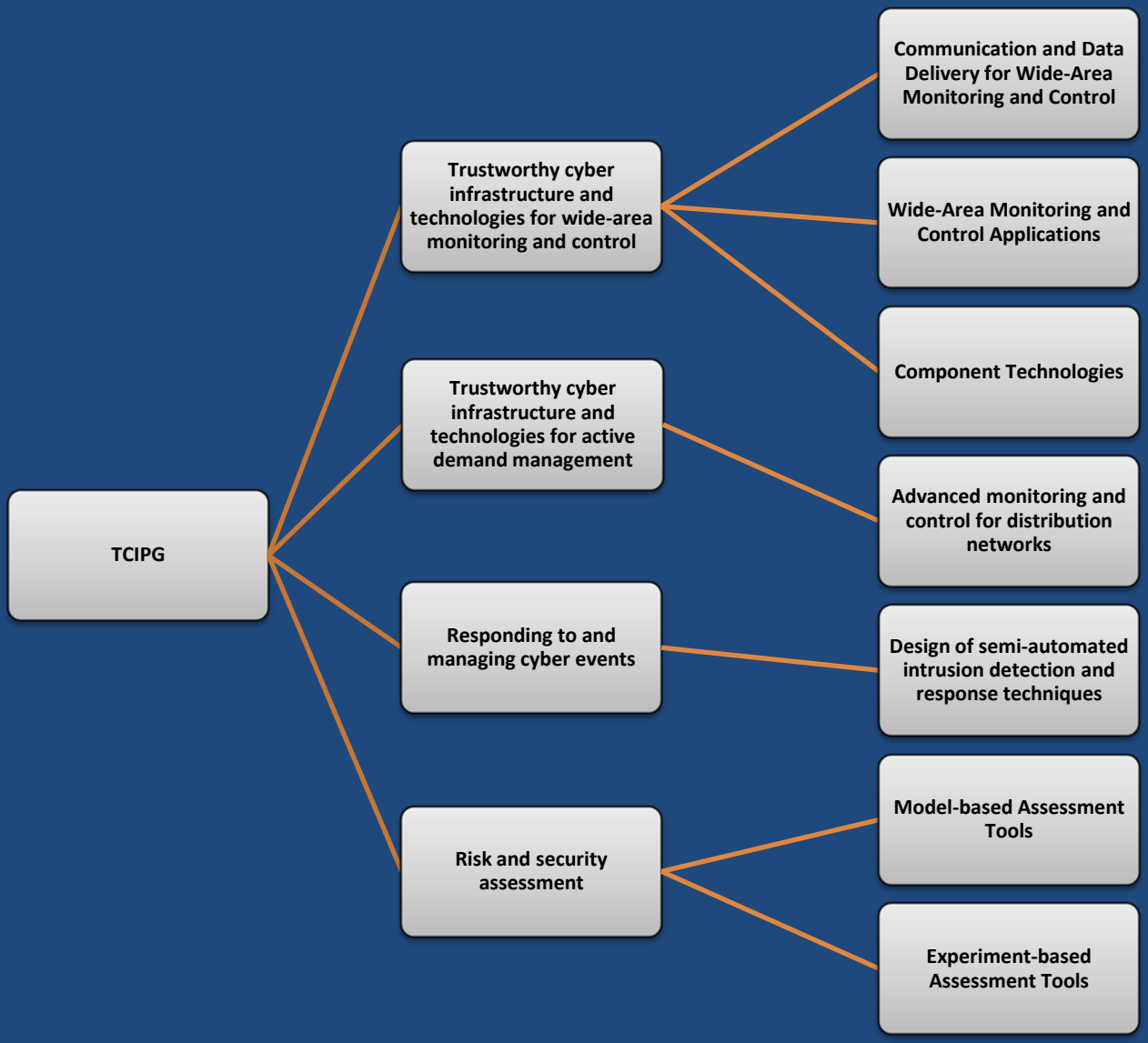
# TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 20 Faculty, 20 Senior Technical Staff, 37 Graduate Students, 5 Undergraduate Students, and 1 Admin

# TCIPG's Multifaceted Mission

- Identify and address critical security and resiliency needs at the cyber-physical junction in the evolving power grid
  - Meet the challenge of rapid evolution and mixed legacy environment
  - Address the proliferation of devices, demand response, DG integration, HAN…
  - Emphasis on trust and resiliency
- Engage Industry (utility, control system vendors, technology providers)
  - Ensure relevance of research
  - Foster technology transfer
- Research Excellence
  - Balance long-range basic research with the need to develop practical solutions in the near term
  - Publications and conference presentations
  - TCIPG is the "go to" academic center
- Education
  - Develop university students who will be experts in the field
  - Outreach to K-12 students and the public

# TCIPG Technical Clusters and Threads



# Cross-Cutting Efforts

Cross-Cutting Efforts address issues that cross technical clusters:

- Education and workforce development
- Testbed and evaluation methodologies
- Industry interactions and technology transition

# TCIPG Impacts all aspects of the *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*

TCIPG Efforts

| Build a Culture of Security | Assess and Monitor Risk | Protective Measures/Risk Reduction | Manage Incidents | Sustain Security Improvements |
|---|---|---|---|---|
| Conduct summer schools for industry | Analyze security of protocols (e.g. DNP3, Zigbee, ICCP, C12.22) | Build secure, real-time, & flexible communication mechanisms for WAMS | Build game-theoretic response and recovery engine | Offer testbed and expertise as a Service to Industry |
| Develop K-12 power/cyber curriculum | Create tools for assessing security of devices, systems, & use cases | Design secure information layer for V2G | Develop forensic data analysis to support response | Anticipate/address issues of scale: PKI, data avalanche, PMU data compression |
| Develop public energy literacy | Create integrated scalable cyber/physical modeling infrastructure | Provide malicious power system data detection and protection | Create effective Intrusion detection approach for AMI | Act as repository for cyber-security-related power system data |
| Directly interact with industry | Distribute NetAPT for use by utilities and auditors | Participate in industry-led CEDS projects | | |
| Educate next-generation cyber-power aware workforce | Create fuzzing tools for SCADA protocols | | | |

# TCIPG Anticipates and Responds to Sector Critical Needs

| Critical Need | TCIPG Efforts |
|---|---|
| Proliferation of nodes outside physical security perimeter | • Specification-based AMI IDS<br>• AMI security review<br>• Scalable PKI for smart grid<br>• TCIPG password change protocol |
| Threats to critical measurements | • Analysis of PMU attacks via GPS spoofing<br>• PMU data quality assessment<br>• Grid state estimation: Malicious data detection<br>• PMU integration: Mixed power flow analysis |
| Trustworthy electric vehicle information layer | • Mobile smart meters<br>• Secure V2G information framework |
| Secure and stable Integration of renewables/DG | • Distributed voltage support<br>• Distributed reactive power |
| Secure smart grid communications | • CONES, GridStat |
| Characterize routable paths to critical assets | • NetAPT |
| Secure and resilient demand response | • AMI activities noted previously<br>• Smart grid economic analysis |
| HAN Security | • Zigbee vulnerability assessment |

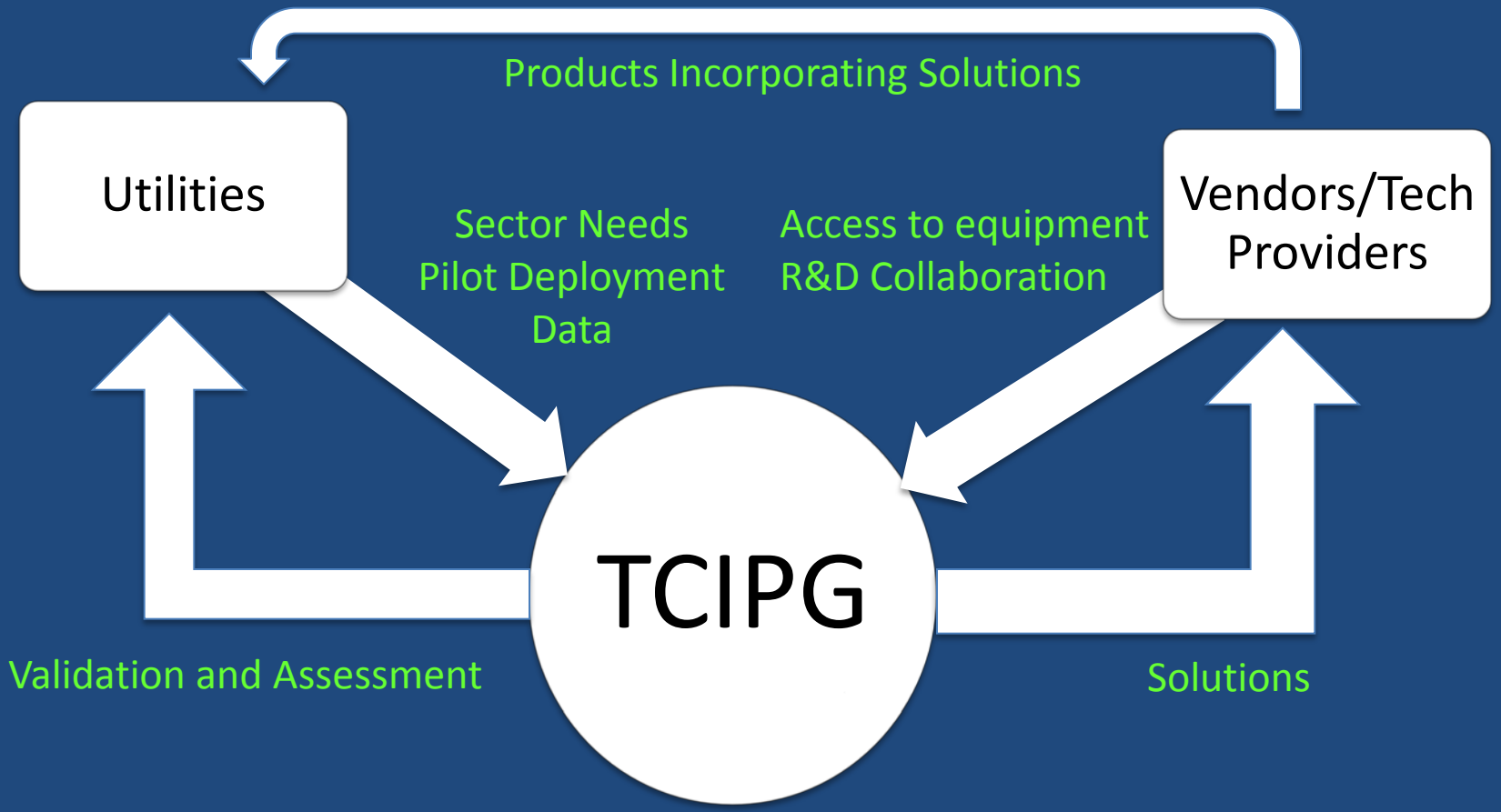
# TCIPG Industry Interaction and Collaboration

- TCIPG emphasizes industry validation of research
- TCIPG is actively working with utilities and technology providers to anticipate and define sector's critical needs
- TCIPG is the "go to" center for academic/industry collaboration on smart grid security, and now benefits from *industry-initiated* outreach
- In addition to industry, TCIPG collaborates with the National Laboratories, NIST, NASPI, EPRI, and others

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

# Industry Interaction: Other organizations that have participated in TCIPG Events

# TCIPG as Catalyst for Accelerating Industry Innovation



# TCIPG as Catalyst for Industry

- TCIPG capabilities and technologies are getting into the field, e.g.,
  - NetAPT
  - LZ Fuzz
  - CONES
  - Autoscopy Jr.
  - Vulnerability assessment
- TCIPG develops expertise that enables deeper engagement with the sector under DOE Industry-led projects
  - SIEGate (GPA)
  - Telcordia
  - Honeywell
  - Entergy SGIG
- Synergistic Industry funding on related projects
  - EPRI
  - Fujitsu
  - GE
  - Lockheed Martin
  - Northrup Grumman
  - SEL
- TCIPG opens door to opportunities
  - Emerging microgrid collaborations
  - Microgrid as on-grid/near-grid testbed for TCIPG and possibly other DOE portfolio performers

# TCIPG as a Connection to other Research

- TCIPG has leveraged other work in security and power systems at the member institutions
- TCIPG in turn provides expertise and capability synergistic with research directions

- Illinois Center for a Smarter Electric Grid (ICSEG)
  - Demonstration/validation of smart grid technologies
  - Validation services for utilities
- Center for Assured Critical Application and Infrastructure Security (CACAIS)
  - Evaluation of emerging security technologies
- Advanced Digital Sciences Center (ADSC – Illinois/Singapore)
  - AMI security collaboration with EMA
- DOE ARPA-E GENI Project (WSU)
  - GridControl: A Software Platform to Support the Smart Grid
- NSF GENI Program (WSU)
  - EAGER: GridStat at Scale using GENI
- DOE Workforce Development (WSU)
  - Workforce Training for the Electric Power Sector
- Power Grid Reliability and Security (GridSim), DOE (WSU)

# How can you get involved?

- Provide feedback on the research activities and directions that you will hear in the cluster and cross-cutting area talks
- Actively participate in the panel sessions, providing (together with the panelists) answers to the questions the panel's pose
- Engage deeply with TCIPG researchers in the poster session, indicating (with the stickers provided) which activities that you would like to engage with after the workshop
- Alert us to any gaps you see in our research program and suggest new activities that we should start

# 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
  - Uniquely balancing a 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