Trustworthy Cyber Infrastructure for Power (TCIP)

tcip.iti.uiuc.edu

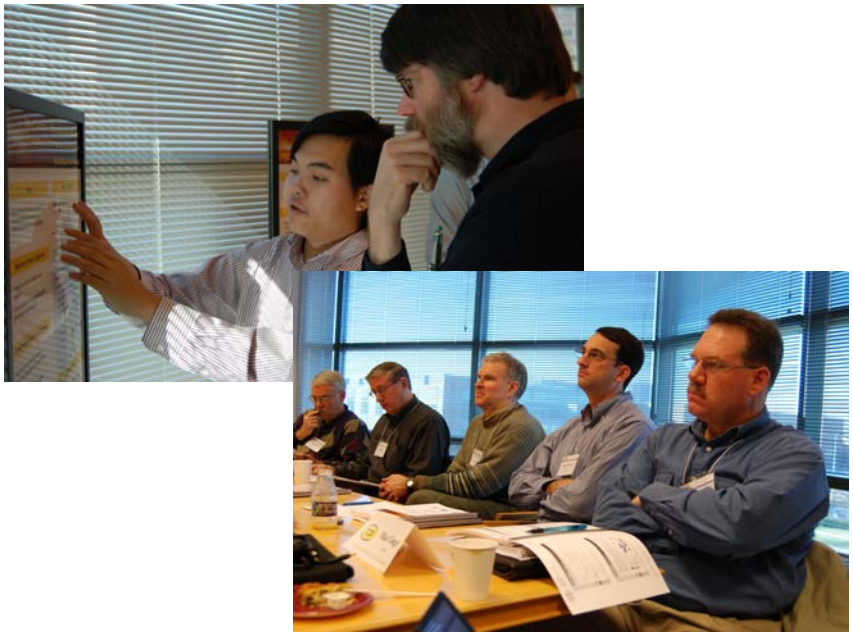
Himanshu Khurana
University of Illinois

NASPI Meeting, Scottsdale AZ
February 4-5, 2009

Scale of effort

- $1.5 M per year for 5 years
- Funded by National Science Foundation CISE and ENG programs
  - With additional support from Department Of Energy, Department of Homeland Security
- 4 universities, 20 senior investigators. 30 Graduate students
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - Cornell University
  - Dartmouth University
- Industry advisory board (35+)

Industrial Partnerships – Spanning Stakeholders



Electrical Power Asset Owners

Ameren – Utility in Mo. and IL
Entergy – Utility in South
Exelon – Utility – Midwest & East
ITC – Transmission company
TVA – Largest public power company

Independent System Operators

CAISO – ISO for CA
MISO – ISO for expanded Midwest
PJM – ISO for 7 states

Technology Providers/Researchers

Argonne Nat'l Lab – Security research
ABB – Industrial manufacturer and supplier
Siemens – Industrial manufacturer and supplier
Areva – SCADA and EMS vendor
Cisco Systems – CIP Researchers
Cyber Defense Agency – Security Assessment
Electric Power Group – PCS Software
EPRI – Electric Power Research Institute
GE – Communication and computing requirements for the power grid
Gehrs Consulting – Power System Consulting
Honeywell – Industrial control system provider
Idaho Nat'l Lab – National SCADA testbed
InStep Software – Equipment Provider
KEMA – Consultants for power systems
Lawrence Livermore Nat'l Lab – Security Research
N-Dimension – Process Control Security Provider
NERC – North American Reliability Corp.
OSI – SCADA and EMS vendor for utilities
OSIsoft – Equipment Provider
PNNL – National lab doing security research
PowerWorld Corp – Analysis and visualization
S&C Electric – Switchgear Manufacturer
Sandia National Lab – SCADA research
Schweitzer – Manufacturer of protection devices
Siemens – Industrial control system provider
SISCO – Power system automation Software
Starthis – Automation Middleware
Sun – Computer Manufacturer

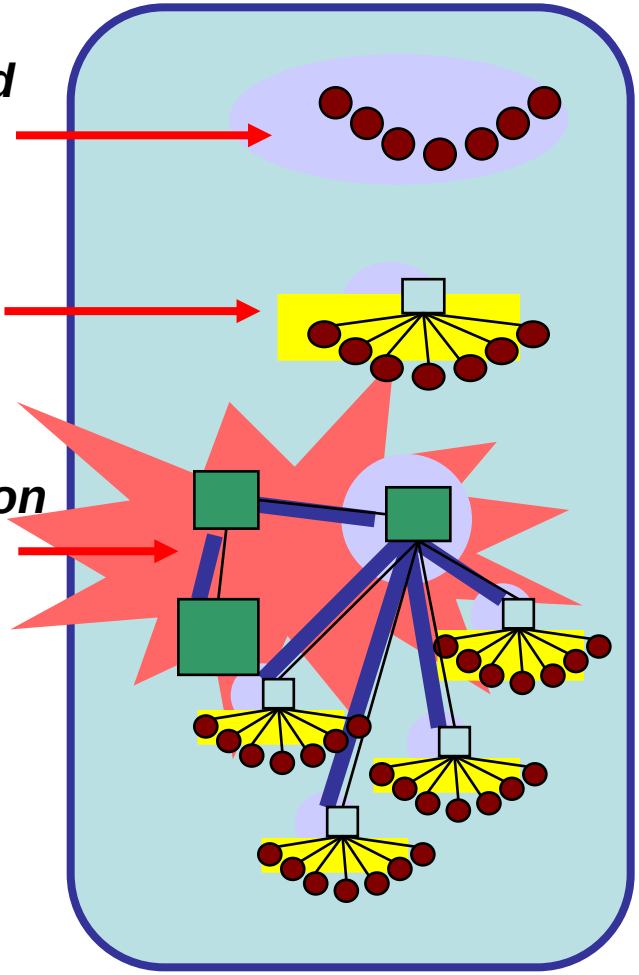
TCIP Overview

Address technical challenges motivated by domain specific problems in

Ubiquitous exposed infrastructure

Real-time data monitoring and control

Wide area information coordination and information sharing



By developing science and technology in

Secure and Reliable Computing Base

Communication and Control Protocols

Quantitative & Qualitative Evaluation

Education

TCIP Vision and Strategy

- Drive the design of *an adaptive, resilient, and trustworthy cyber infrastructure for electric power*, which *operates through attacks* by:
  - Protecting the cyber infrastructure
  - Making use of cyber and physical state information to detect and respond to attacks
  - Supporting greatly increased throughput and timeliness requirements
- Support the provisioning of a new power grid that
  - Enables advanced energy applications
    - high-speed monitoring and asset control, advanced metering, diagnostics & maintenance

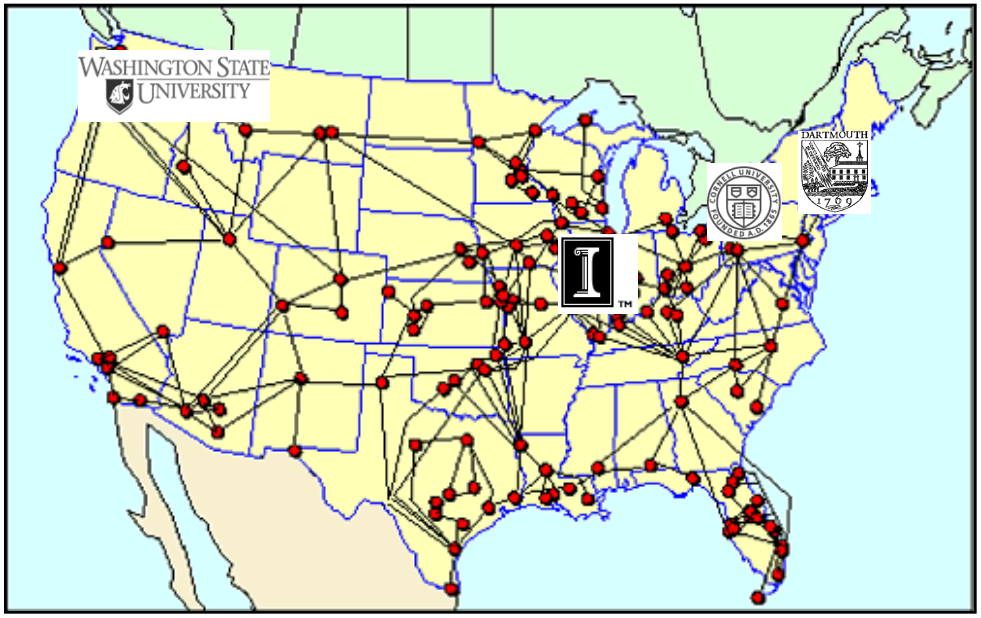
Related Efforts

- Roadmap to Secure Control Systems:
  - energetics.com/csroadmap
  - 97 Projects currently documented (including 10 TCIP projects)
- Government/National Lab efforts include:
  - DOE-funded National SCADA Testbed (inl.gov/scada)
  - DHS Control Systems Security Program (us-cert.gov/control_systems)
  - NIST Process Control Security Requirements Forum (isd.mel.nist.gov/projects/processcontrol)
- Efforts with Industry engagement
  - DHS-funded I3P Process Control System Research (thei3p.org/projects/pcs.html)
  - Process Control Systems Forum (pcsforum.org)
- More generic longer-term research also exists, e.g.,
  - Berkeley TRUST NSF S&T Center

⇒ TCIP is unique in its focus on long-term issues specific to power grid security, and more broadly, trust.

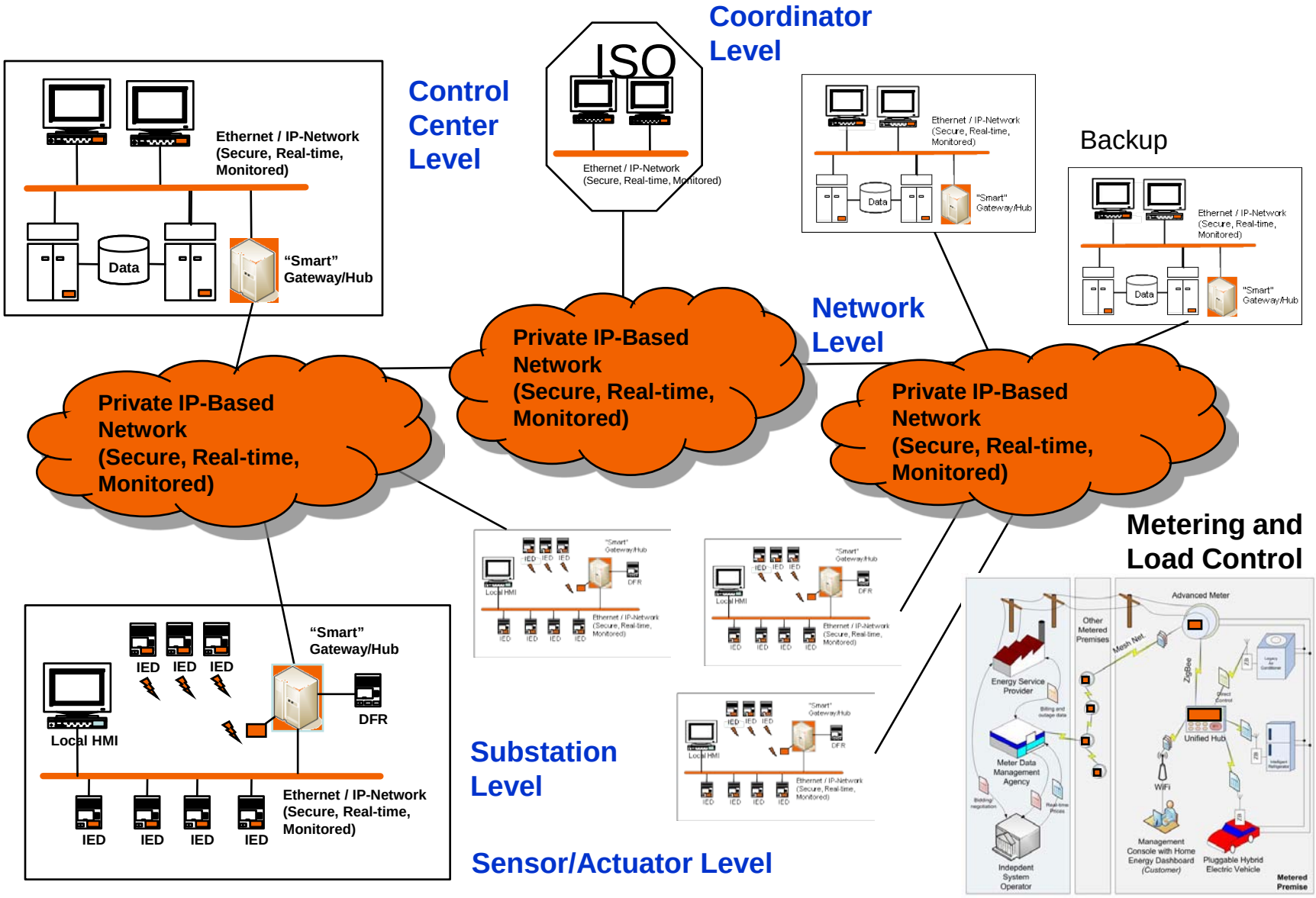
TCIP Senior Investigators

- Secure & Reliable Base
  - Bratus, Gross, Gunter, Iyer, Kalbarczyk Nakka, Sauer and Smith
- Communication & Control Protocols
  - Bakken, Bose, Bobba, Hauser, Khurana, Minami, Nahrstedt, Sanders, Scaglione, Thomas, Wang, Welch, Winslett
- Quantitative & Qualitative Evaluation
  - Campbell, Gunter, Khurana, Nicol, Overbye, Sanders, Yardley
- Education
  - Overbye, Reese, Sebestik, Tracy



- Partner Institutions
  - Cornell
  - Dartmouth
  - University of Illinois
  - Washington State University

Vision: *Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure*



TCIP Impact Vehicles

- **Research papers**
- **Tools: hardware and software prototypes**

• **Designs** of protection, detection and response mechanisms
• **Taxonomies** for a common understanding of designs
• **Architectures** that integrate designed components
• **Evaluation/measurements** that assess impact of attacks and benefits of designs/architectures

• **Over 80 papers already published**

TCIP Impact Vehicles

- Research papers
- **Tools: hardware and software prototypes**

- **17 tools developed or enhanced**

- **Trustworthy Computational Base**
  - Penetration testing (LZFuzz), secure co-processors (CeSium, Faerieplay, RSE), encryption (YASIR), AMI/demand-response (AVR PCT, jXBee)
- **Trustworthy Communication and Control Protocols**
  - Reliable and real-time communication (GridStat, iDSRT), trust negotiation (TrustBuilder), encryption (SMOCK), key management (DNSCert), attributed-enhanced email (ABUSE)
- **Qualitative and Quantitative Evaluation**
  - Access policy enforcement (APT), power flow simulation (PowerWorld), network simulation (RINSE), security assessment (ASSESS)
- **Education applets**

TCIP Impact Vehicles

- Research papers
- Tools: hardware and software prototypes
- **Interactions with Industry Advisory Board**

- Four industry workshops
  - 20 - 25 industry participants per workshop
- Day-long visits with formal seminars and discussions
  - Ameren, Applied Control Solutions, EPRI, Gehrs Consulting, GE, NERC, PNNL, SISCO
- Visits to industry
  - Ameren, Areva, Entergy, MISO, OSII, PJM, PowerWorld, TVA
- Donations for TCIP test-bed
  - > 1 million dollars worth of hardware, software
- TCIP Summer School (June 2008)
  - 12 IAB speakers

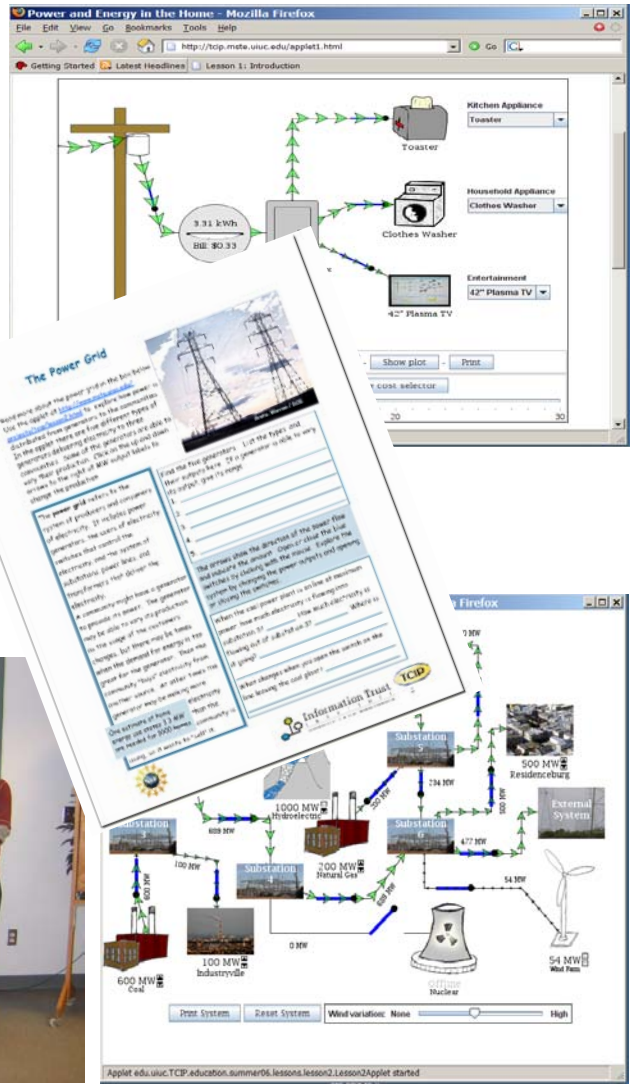
TCIP Impact Vehicles

- Research papers
- Tools: hardware and software prototypes
- Interactions with Industry Advisory Board
- **Participation in major initiatives**

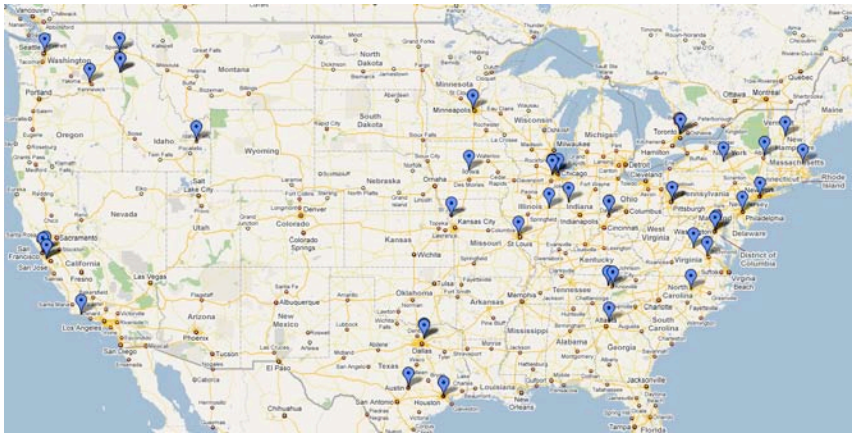
- North American Synchrophasor Inititative (NASPI)
- Automated Metering Infrastructure Security (AMI-SEC)
- EPRI Power and Delivery
- Roadmap to Secure Control Systems
  - 10 projects in roadmap
  - Presentations at May'08 workshop

TCIP Education Activities; tcip.mste.uiuc.edu

- TCIP Researchers, in partnership with math/science education specialists:
- Pre-university engagement:
  - Develop pedagogically and technologically sound math and science curriculum materials
  - Utilize these materials to connect with middle and high school teachers and students
- Provide research experiences to students



- **Program Highlights**
  - Lectures and discussions on a range of security issues facing control systems
  - Interactive agenda
  - Opportunities to learn about and influence long-term research problems
- **Who attended**
  - 86 researchers and practitioners from industry, national laboratories and academia
- **Who presented**
  - 16 expert lecturers from Industry (8), National Labs (3), Government (2) and Academia (3)



Link: http://www.iti.uiuc.edu/events/SummerSchool2008.html

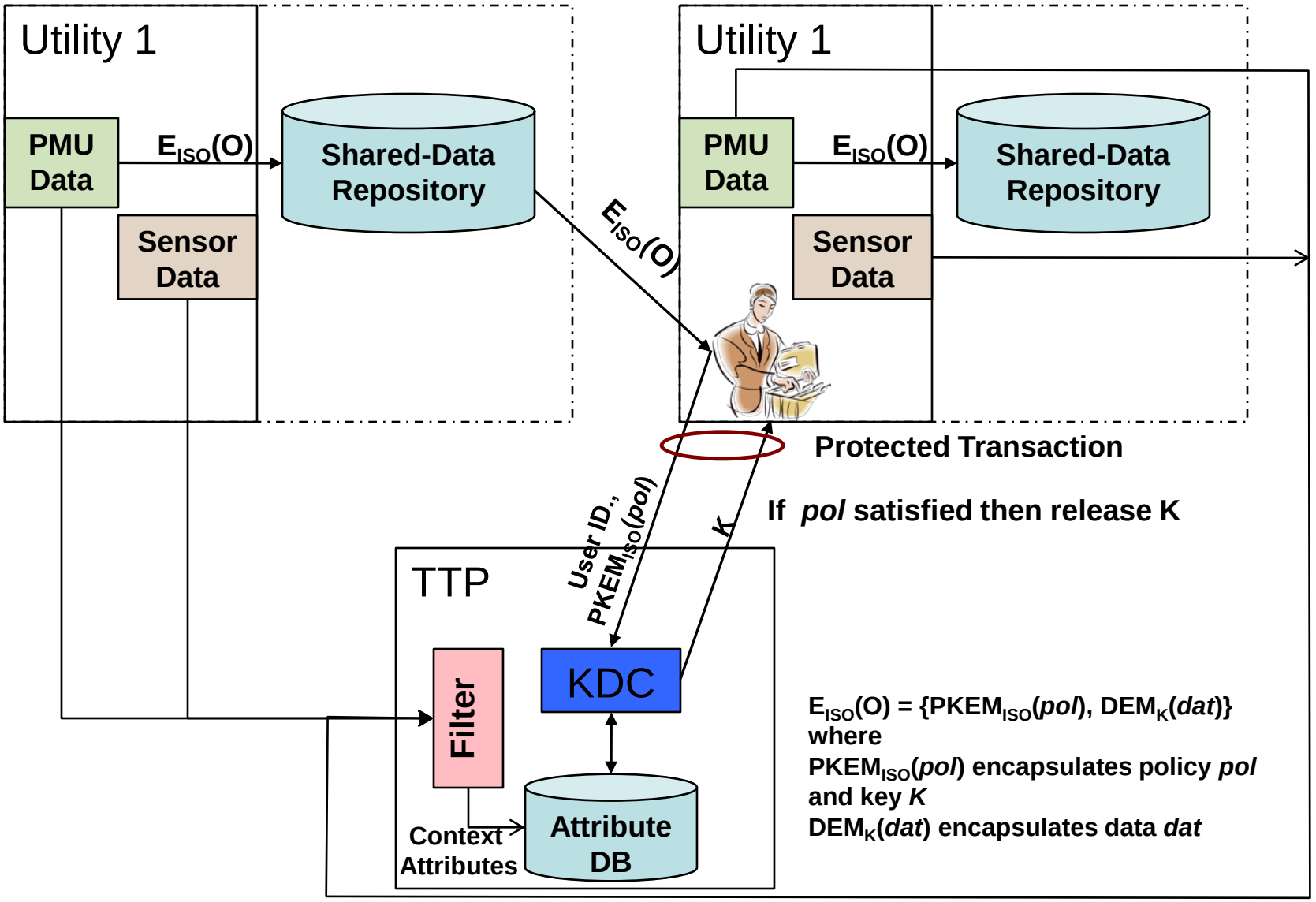
- **Sponsors**
  - DOE, NSF, DHS
  - PJM, OSI

PMU focused TCIP Research Efforts

Project 1: Secure Policy-based PMU Data Sharing (Rakesh Bobba, Himanshu Khurana; Illinois)

- Multi-recipient data sharing
  - Recipients not known at the time of data creation
  - Data sharing based on policy
- Flexible Policy Specification
  - Role, attribute and context based
  - Policy satisfiability may not be verifiable by data owner
    - Grant Access if (Reliability Engineer in *Utility X*) AND (*Utility X* in ISO B) AND (Overloaded Tie Line between *Utility X* and Utility A) AND ((Below Critical Reactive Power Reserves in *Utility X*) OR (Reactive Limiters active in *Utility X*))
- Data sharing on open networks
- Policy and data secrecy
- Efficiency and compatibility
- Security
  - against active adversaries

Project 1: Proposed Architecture

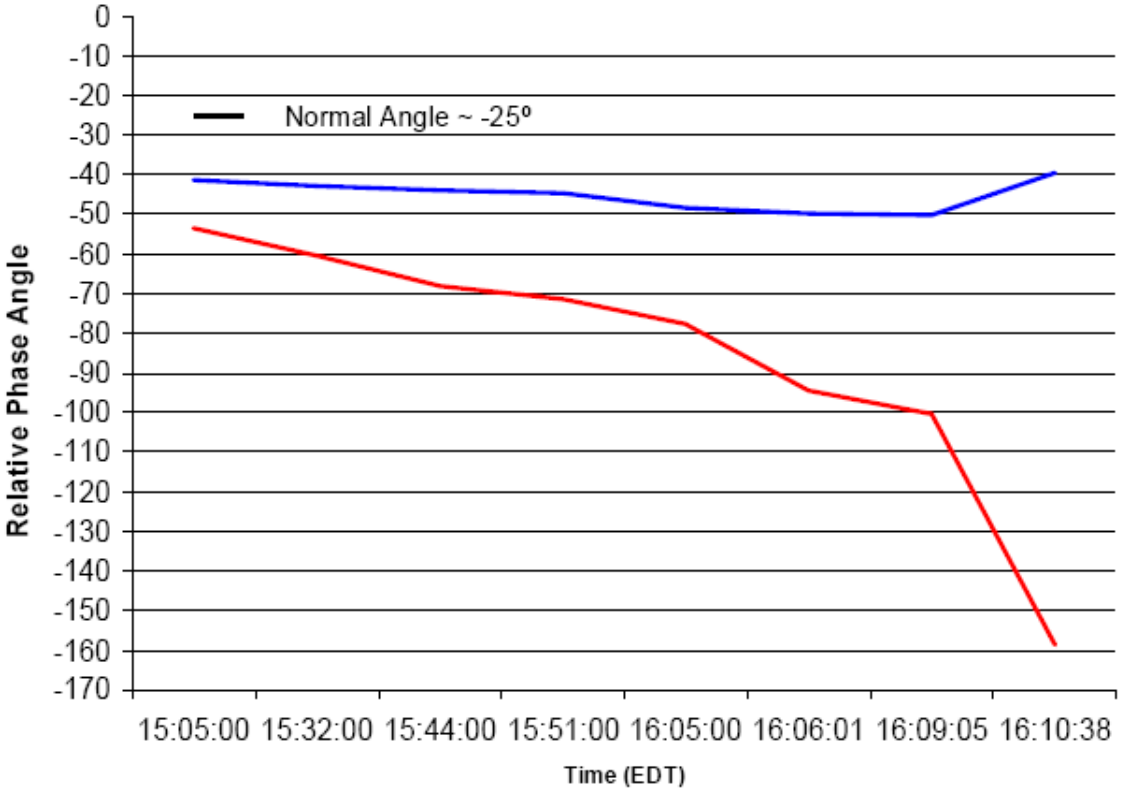


Recent PMU-related research at WSU
(Dave Bakken, Anjan Bose, Carl Hauser)

- GridStat lessons learned -> NASPI-net (Bakken)
  - Example: QoS management capabilities
  - Synchronized rate filtering – network delivers a synchronized subset of measured values
- C37.118 GridStat publisher (Hoffman)
  - Matching the GridStat pub-sub model to the PMU data stream standard
- Two-level PMU-based linear state estimator (Bose and Yang)
  - Fast system-level computation based on distributed computation of individual substation states
- Authentication protocols for long-lived field devices and infrastructures (Mudumbai and Hauser)
  - How can a data delivery service for devices deployed in remote locations evolve with cyber-security developments over several decades
- Assessment of GridStat security (WSU Team, PNL, INL – not TCIP funded but complementary to TCIP work)
  - Identified specific issues in the code
  - Generated ideas for addressing known shortcomings in management plane security
  - Suggested new research topics in area of platform security

Project 3: Interpretation of Phase Angles Difference (Tom Overbye, Matt Davis; Illinois)

A Motivating Example from 8/14/03



Slide at left indicates that during the 8/14/03 event there was a significant angle separation between Cleveland and Western MI. But it also raises some interesting research questions

Slide source: Robert Cummings (NERC) November 29, 2007 PMU Overview and Update Presentation

Project 3: Ongoing Research Work

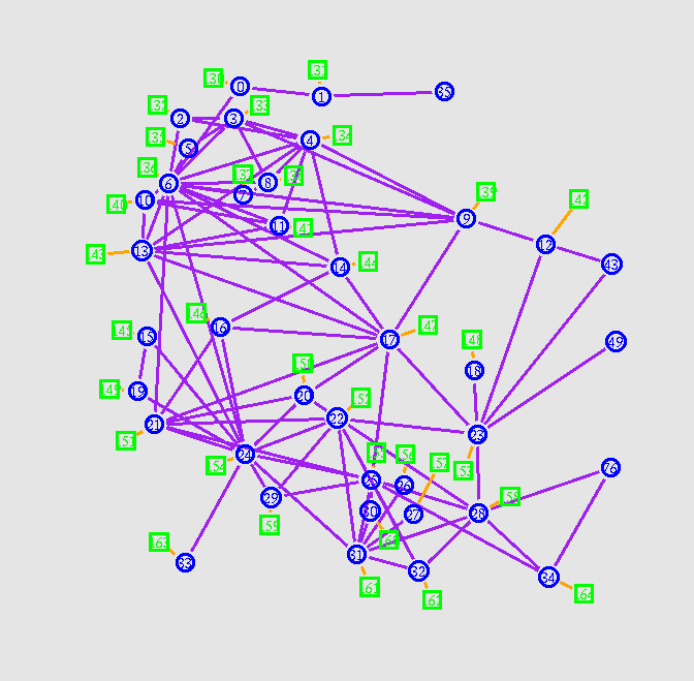
- In the Eastern Interconnect the significance of individual bus angles or bus angle differences across different regions is not fully understood.
- We are exploring theoretical and practical issues associated with the interpretation of phase angle differences.
- Useful input data would be a set of state estimator cases to give actual operating conditions coupled with associated PMU measurements.
- Results would (hopefully) be interpretations and visualizations of this data

Project 4: Modeling NASPInet Data Flows (R.Hasan, R.Bobba, H.Khurana; Illinois)

- **Motivation**: How can we design and implement a scalable PMU data sharing NASPInet?
  - what kind of bandwidth is needed for NASPInet?
  - how do latency constraints affect bandwidth provisioning and security guarantees?
  - will it scale to multiple applications (current/future) using data from thousands of PMUs?
- **Goal**: To build a modeling framework that will analyze and validate network and storage architectures as well as security technologies suitable for PMU data sharing in a scalable manner

Project 4 Study: WECC Point-to-Point

- WECC topology
  - 35 PGWs, 1 PDC per PGW, 100 – 250 PMUs per PDC/PGW
- Point-to-point communication links
  - 56 Kbps PMU-PDC link, 4.6 – 9.3 MBPS PGW-PGW links,
- Standard security mechanisms
  - hop-by-hop auth. (MAC/Signatures)
- Distributed storage
  - everybody stores all data
- **Results**
  - Data for 200PMUs/PGW, 7.72Mbps PWG-PGW link



- Authentication adds ~ 3ms additional (20 byte tx time)
- Signatures feasible when aligning at source
- Storage – Each BA generating 768000 bytes/sec ~ 22TB/year

TCIP Summary

- **Vision**
  - Design of an adaptive, resilient, and trustworthy cyber infrastructure for electric power
- **Approach**
  - Unique, holistic, technological approach
  - Academic, Government, Industry partnership
- **Execution**
  - Maintaining long term focus, but developing capabilities that can be used in today's grid
- **New Partnerships for Transition**
  - Engaging Industry and National Lab partners to take TCIP technologies to the next level

- **More information: tcip.iti.uiuc.edu; hkhurana@illinois.edu**

Questions?

- Contact
  - Himanshu Khurana (hkhurana@illinois.edu)