


TCIP: Trustworthy Cyber Infrastructure for Power

Overview

Presented by: William H. Sanders

TCIP Industry Workshop, October 17, 2007

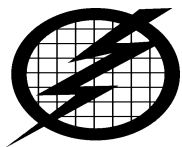
University of Illinois • Dartmouth College • Cornell University • Washington State University



TCIP Vision and Strategy

- Provide the fundamental science and technology to create the **cyber infrastructure** for an intelligent, adaptive power grid which
 - survives malicious adversaries
 - provides continuous delivery of power
 - supports dynamically varying trust requirements.
- By:
 - Creating the secure, reliable and trustworthy building blocks and architecture
 - Creating validation technology to quantify the amount of trust provided by proposed approach

University of Illinois • Dartmouth College • Cornell University • Washington State University



Fundamental Scientific Challenges

- **Enable advanced process control system capabilities**
 - In all power system components (e.g., IEDs, advanced meters, control center and ISO equipment, local- and wide-area networks)
 - Integrated with a sound architectural approach
 - While ensuring end-to-end security and timeliness
- **Maintain adaptive defensive capabilities and demonstrate operation through attack**
 - Model threats, attacks and consequences
 - Provide integrated assessment of physical and cyber health
 - Automate response to attacks
- **Provide quantitative and qualitative evaluation**
 - Experiment with physical and cyber system interactions
 - Study scalability of solutions (to the millions)
- **Develop workforce and influence societal progress**
 - Education and outreach
 - Demonstrate benefit to society

University of Illinois • Dartmouth College • Cornell University • Washington State University

TCIP Technical Approach

Address technical challenges motivated by domain specific problems in

By developing science in

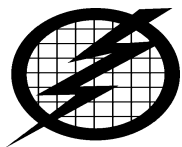
Ubiquitous exposed infrastructure → **Secure and Reliable Computing Base**






Real-time data monitoring and control → **Trustworthy infrastructure for data collection and control**

Wide area information coordination and information sharing → **Wide-Area Trustworthy Information Exchange**

Quantitative & Qualitative Evaluation

University of Illinois • Dartmouth College • Cornell University • Washington State University










TCIP's Unique Strengths

- **Making fundamental advances that will impact the power grid cyber infrastructure in the long (as well as short) time frame**
 - Forward-looking architecture
 - Innovative computing elements and protocols
 - Unique, accurate, scalable, evaluation methodology
- **Unique, holistic, integrated, approach driven by power grid needs**
 - Device-centric security
 - Robust, real-time, and secure protocols to support universal connection
 - Adaptive, partially automatic, response and recovery
 - Multi-level, hierarchical, simulation, emulation, and physical evaluation
- **Close interaction with more than 30 member industry advisory board**
 - Technology providers, asset owners, system operators
- **Integrated education approach**

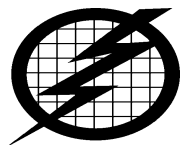
University of Illinois • Dartmouth College • Cornell University • Washington State University



Group Missions

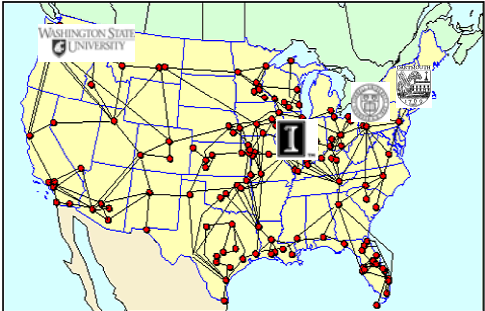
- **Secure & Reliable Computing Base**
 - To develop a secure and reliable computing base that provides low-overhead, robust protection against both accidental and malicious faults as the foundations of the power grid, and also provide foundations for system-wide security and reliability.
- **Trustworthy Communication & Control Protocols**
 - To design, implement, and integrate communications and control protocols that provide secure, reliable, and timely data collection and control
- **Quantitative & Qualitative Evaluation**
 - To provide evaluative methodologies and tools for modeling, simulation, emulation, and experimentation for security technology for the power grid.
- **Education**
 - To provide education, outreach and training at the K-12, undergraduate, and graduate levels and the public at large, and to prepare the next generation work force.

University of Illinois • Dartmouth College • Cornell University • Washington State University



TCIP Senior Investigators

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



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

University of Illinois • Dartmouth College • Cornell University • Washington State University

TCIP Graduate and Undergraduate Researchers

Graduate Students:

- Zahid Anwar (UIUC)
- Angel Aquino-Lugo (UIUC)
- John Kwang-Hyun Baek* (Dartmouth)
- Scott Bai (UIUC)
- Rasika Chakravarthy (WSU)
- Paul Dabrowski (UIUC)
- Matt Davis (UIUC)
- Shrut Kirti (Cornell)
- Peter Klemperer (UIUC)
- Yingyi Liang* (UIUC)
- Adam Lee* (UIUC)
- Michael LeMay* (UIUC)
- Christopher Masone* (Dartmouth)
- Mirko Montanari* (UIUC)
- Sunil Muthuswamy (WSU)
- Suvda Myagmar (UIUC)
- Hoang Nguyen (UIUC)
- Hamed Okhravi* (UIUC)
- Ashwin Ramaswamy (Dartmouth)
- Katherine Rogers (UIUC)
- Ravishankar Sathyam (UIUC)
- Sankalp Singh* (UIUC)
- Erik Solum (WSU)
- Frank Stratton (UIUC)
- Yang Tao (WSU)
- Zeb Tate (UIUC)
- Patrick Tsang* (Dartmouth)
- Yang Tao (WSU)
- Jianqing Zhang (UIUC)
- Saman Aliari Zonouz (UIUC)

Undergraduates:

- David Anderson (WSU)
- Katherine Coles (UIUC)
- Caroline Davis (UIUC)
- Alex Latham (Dartmouth)
- Loren Hoffman (WSU)
- Raoul Rivas (UIUC)
- Nathan Schubkegel (WSU)
- Evan Sparks (Dartmouth)
- Caroline Davis (UIUC)

Summer Interns:

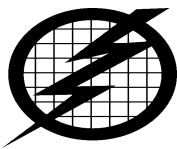
- Suhas Aggarwal (IIT)
- Tamal Das (IIT)

High School:

- Axel Hansen (Dartmouth)

*Not funded by TCIP, but working on TCIP

University of Illinois • Dartmouth College • Cornell University • Washington State University



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

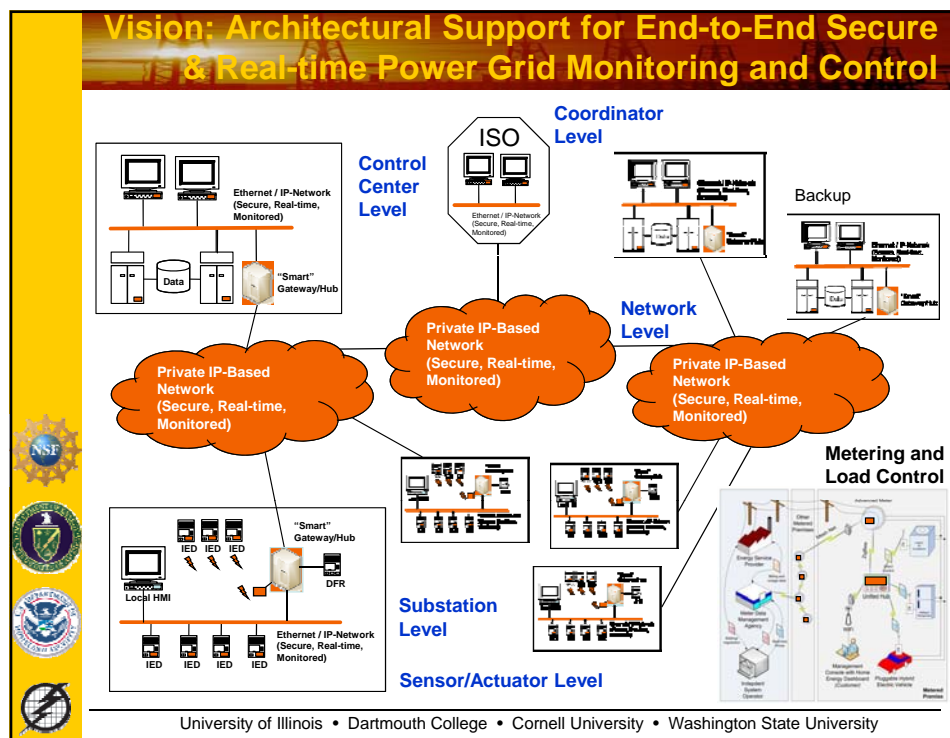
Independent System Operators

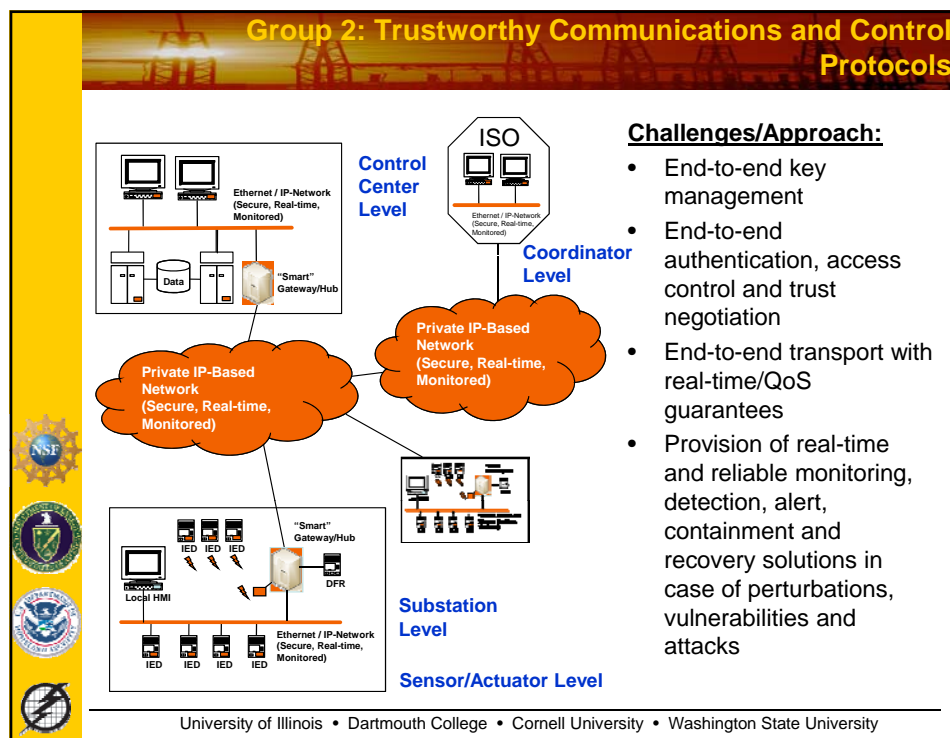
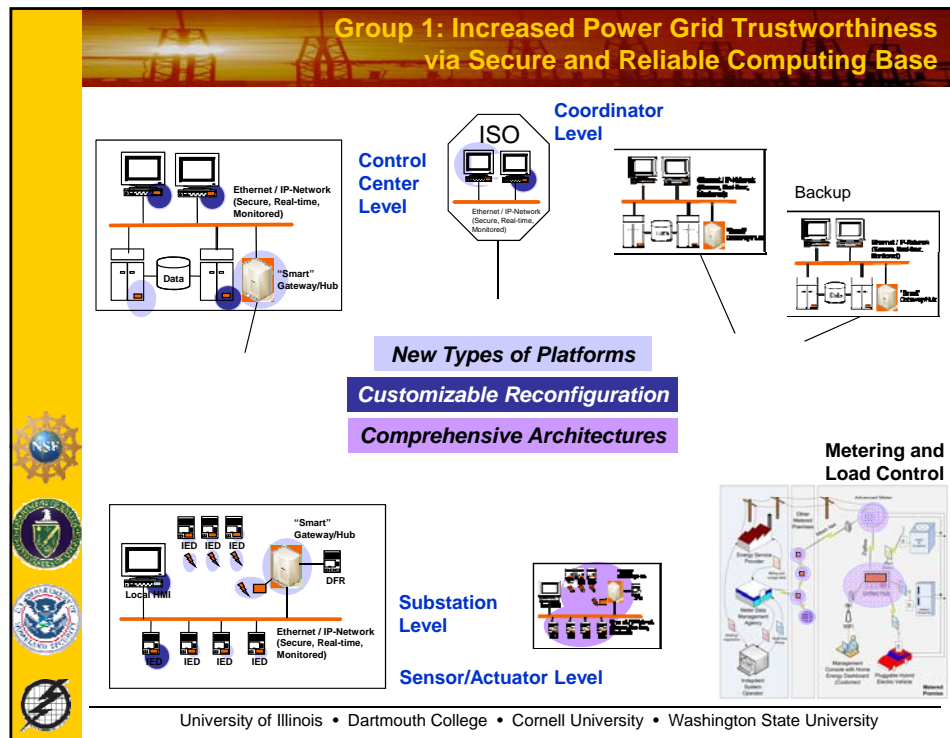
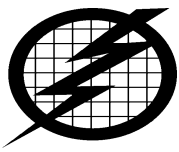
- CAISO** – ISO for CA
- MISO** – ISO for expanded Midwest
- PJM** – ISO for 7 states

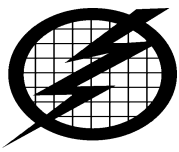
Technology Providers/Researchers

- 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
- NERC** – North American Electric Reliability Corp.
- OSI** – SCADA and EMS vendor for utilities
- OSisoft** – PCS Software 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 & OS Manufacturer

University of Illinois • Dartmouth College • Cornell University • Washington State University







Group 3: Quantitative & Qualitative Evaluation

Challenges/Approach:

- Developing tools and methodologies for evaluating next-generation power grid designs
- Developing tools and methodologies for evaluating existing system configurations with respect to best practice recommendations and global policies
- Studying the sensitivity of the power grid infrastructure to various kinds of cyber attacks

The diagram illustrates the evaluation framework. At the top, 'Algorithms' (Network modeling, High performance simulation, State sampling, Abstraction hierarchies, Policy checking) and 'Testing Methodologies' (Sensitivity analysis, Statistical sampling, Constrained exhaustive analysis, Hierarchy of experiments) feed into 'Tools' (RINSE, Powerworld, ASA, APT). These tools then feed into 'Testbed' (Simulators, ICD Emulators, SWS, relay, AUIS, Proof of concept) and 'Case Studies' (Latency analysis of secure hub, Communication analysis of distributed control agents, Security sensitivities of recovery action). The Testbed and Case Studies feed into a central 'RINSE' cloud, which is connected to various levels of the power grid: Control Center Level, ISO, Distribution Level, and Substation Level. The RINSE cloud is also connected to a 'PowerWorld' interface.

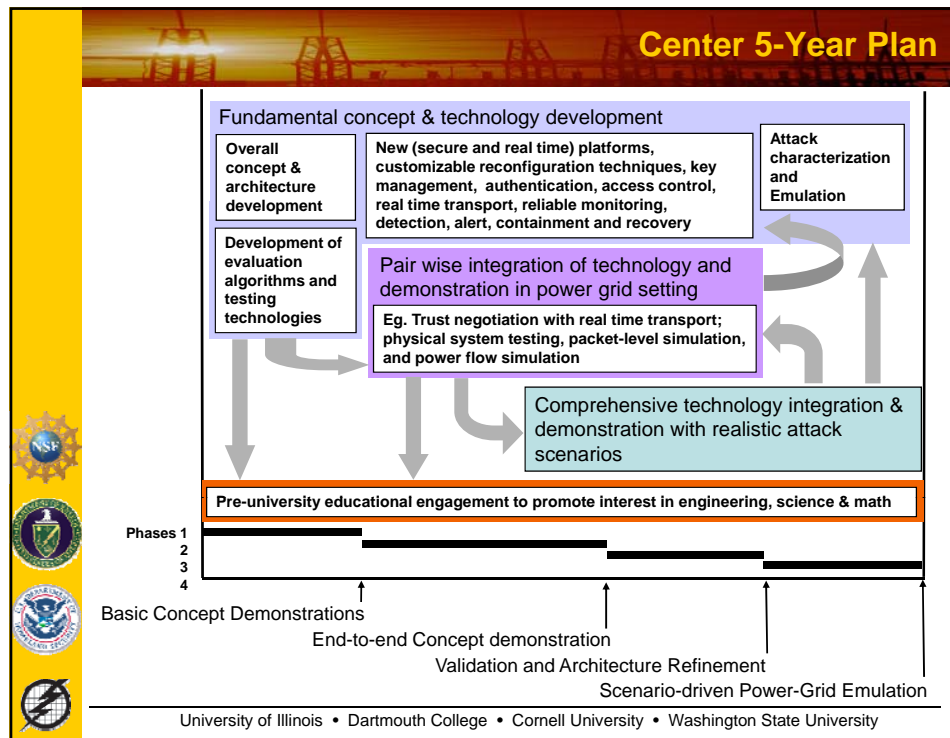
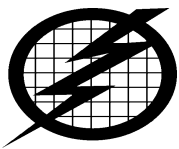
University of Illinois • Dartmouth College • Cornell University • Washington State University

Group 4: Education

- 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
- Undergraduate/graduate curriculum:
 - Provide research experiences to students

The images show educational materials, a group of students, and a computer screen displaying a power grid simulation. The materials include a 'New Power Grid' document and a 'Power Grid' diagram. The students are a group of young people standing together. The computer screen shows a detailed power grid simulation with various components and connections.

University of Illinois • Dartmouth College • Cornell University • Washington State University

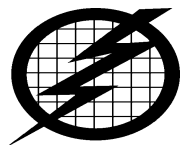


TCIP Annual Review Schedule, Oct. 15-16, 2007 (1)

Monday, October 15, 2007
301 Coordinated Science Laboratory (CSL)
1308 W Main Street, Urbana

- 7:45 a.m. – 8:15 a.m. Continental Breakfast
- 8:15 a.m. – 8:30 a.m. **Welcome, Introductions** (Linda Katehi, Provost, University of Illinois)
- 8:30 a.m. – 9:00 a.m. **Overview and Project Update** (Bill Sanders)
- 9:00 a.m. – 9:45 a.m. **Communication and Control Protocols** (Klara Nahrstedt)
- 9:45 a.m. – 10:00 a.m. Break
- 10:00 a.m. – 10:45 a.m. **Secure and Reliable Computing Base** (Sean Smith)
- 10:45 a.m. – 11:30 a.m. **Quantitative and Qualitative Evaluation** (David Nicol and Himanshu Khurana)
- 11:30 a.m. – 11:40 a.m. **Ilesanmi Adesida**, Dean, College of Engineering, University of Illinois
- 11:40 a.m. – 12:30 p.m. Lunch
- 12:30 p.m. – 1:30 p.m. **Student Poster Session**, 469 CSL
- 1:30 p.m. – 2:15 p.m. **Meeting with Graduate Students**, 369 CSL
- 2:15 p.m. – 2:25 p.m. *Return to 301 CSL*
- 2:25 p.m. – 2:45 p.m. **Education** (Molly Tracy, Zeb Tate and Jena Sebastik)
- 2:45 p.m. – 3:00 p.m. **Industrial Interactions** (Pete Sauer)
- 3:00 p.m. – 3:15 p.m. Break

University of Illinois • Dartmouth College • Cornell University • Washington State University



TCIP Annual Review Schedule, Oct. 15-16, 2007 (2)

- 3:15 p.m. – 5:00 p.m. **DEMO: Security, reliability, and trustworthiness capabilities for the Power Grid, 448 CSL**
- 5:00 p.m. – 6:00 p.m. **NSF Team Executive Session, 369 CSL**
- 6:00 p.m. – 6:30 p.m. **Meet with TCIP Director and Leads, 369 CSL**
- 6:00 p.m. Dinner
 - NSF Review Team, 369 CSL
 - TCIP Team, 301 CSL

Tuesday October 16, 2007

301 Coordinated Science Laboratory (CSL)
1308 W Main Street, Urbana



- 8:30 a.m. – 9:00 a.m. Continental Breakfast
- 9:00 a.m. – 9:30 a.m. **Response to Questions**
- 9:30 a.m. – 10:30 a.m. **NSF/DOE/DHS Feedback**
- 10:30 a.m. – 10:45 a.m. Break
- 10:45 a.m. – 11:30 a.m. **Future Government Initiatives in Security** (Karl Levitt, National Science Foundation)
- 11:30 a.m. – 1:00 p.m. Lunch

University of Illinois • Dartmouth College • Cornell University • Washington State University