TCIPG Highlights

Bill Sanders
on behalf of the TCIPG Team

July 20, 2011

NITRD TTS: Solutions for Smart Grid Workshop

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

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, 2009
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

Ilinois's Singapore Adv. Digital Sciences Center Smart Grid Subprogram

~$15M effort / 5 years

Projects in Microgrids, DERs, and HANs

Korean National Smart Grid TestBed on Jeju Island.

Project concerning tesbed and cyber security research DDOS)

CACAIS Testbed

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

Illinois Center for a Smarter Electric Grid

Validation & Compliance Services

- $2.5M, YR1 DCEO funding
- 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 & Research Focus

Vision: Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, which 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
- 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

TCIPG External Advisory Board

- Marija Ilic (CMU)
- Jeff Katz (IBM)
- Himanshu Khurana (Honeywell)
- Scott Mix (NERC)
- Paul Myrda (EPRI)
- David Norton (FERC)
- Mahendra Patel (PJM)
- Dave Whitehead (SEL)

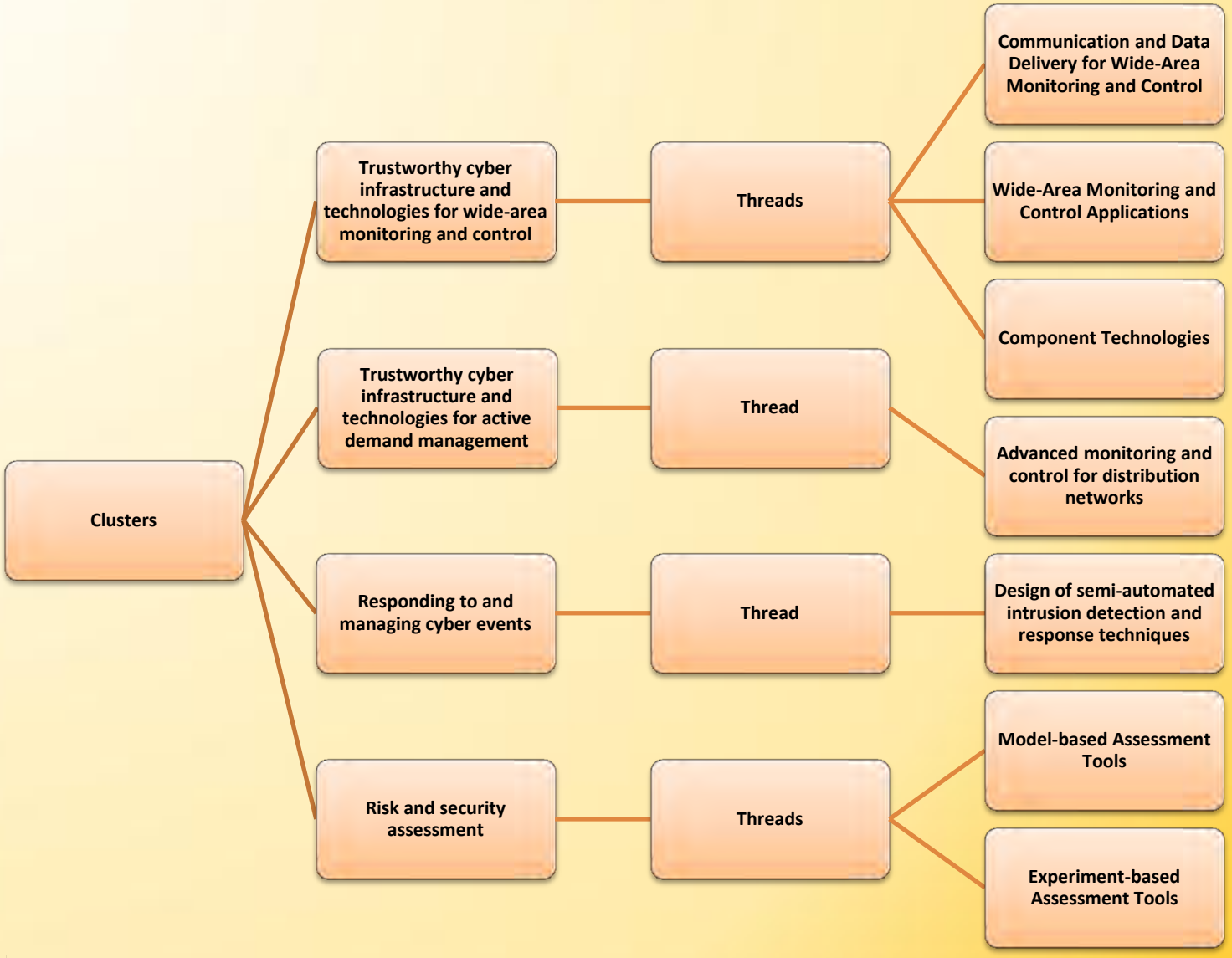
TCIPG Industry Interaction Board

ADSC
Association of Illinois Electric Cooperatives
Alcatel-Lucent
ALSTOM
Ameren
at&t
BOEING
BT
Center for Community Adaptation
CLEAN ENERGY TRUST
CHAMPAIGN COUNTY ILLINOIS EDC
ComEd.
DTE Energy
ENCARI
ENERGETICS A Subsidiary of VSE Corporation
EnergySec™
Entergy THE POWER OF PEOPLE
Electric Power Group
EPRI ELECTRIC POWER RESEARCH INSTITUTE
FUJITSU
imagination at work
GENERAL DYNAMICS Strength On Your Side
GRID PROTECTION ALLIANCE
HARRIS
Honeywell
IBM
ILLINOIS SCIENCE & TECHNOLOGY COALITION
Illinois VENTURES
Integrated Architecture
intel
IEIA
KTH VETENSKAP OCH KONST
LOCKHEED MARTIN We never forget who we're working for
Luminant
McAfee
Mehta Tech Inc.
nationalgrid THE POWER OF ACTION
n-dimension solutions
NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
NORTHROP GRUMMAN
OSIsoft.
PATRICK
pjm
PowerWorld Corporation
ETRI Electronics and Telecommunications Research Institute
QUANTA TECHNOLOGY
SAIC From Science to Solutions
SIEMENS
Telcordia
SPACE•TIME•INSIGHT
SEL SCHWEITZER ENGINEERING LABORATORIES

TCIPG Clusters and Cross-Cutting Efforts

- Clusters integrate work in specific technical areas over the life of the project:
  - Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
  - Trustworthy cyber infrastructure and technologies for active demand management
  - Responding to and managing cyber events
  - Risk and security assessment
- Cross-Cutting Efforts address issues that cross technical clusters:
  - Education and workforce development
  - Testbed and evaluation methodologies
  - Industry interactions and technology transition

TCIPG Technical Clusters and Threads



Cluster: Trustworthy Cyber Infrastructure and Technologies for Wide-Area Monitoring and Control

Communication and Data Delivery for Wide-Area Monitoring and Control

- Converged Power Grid Cyber Networks*
- Cooperative Congestion Control in Power Grid Communication Networks*
- GridStat Middleware Communication Framework: Management Security and Trust*†
- Decentralized Sensor Networking Models and Primitives for the Smart Grid*
- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications*

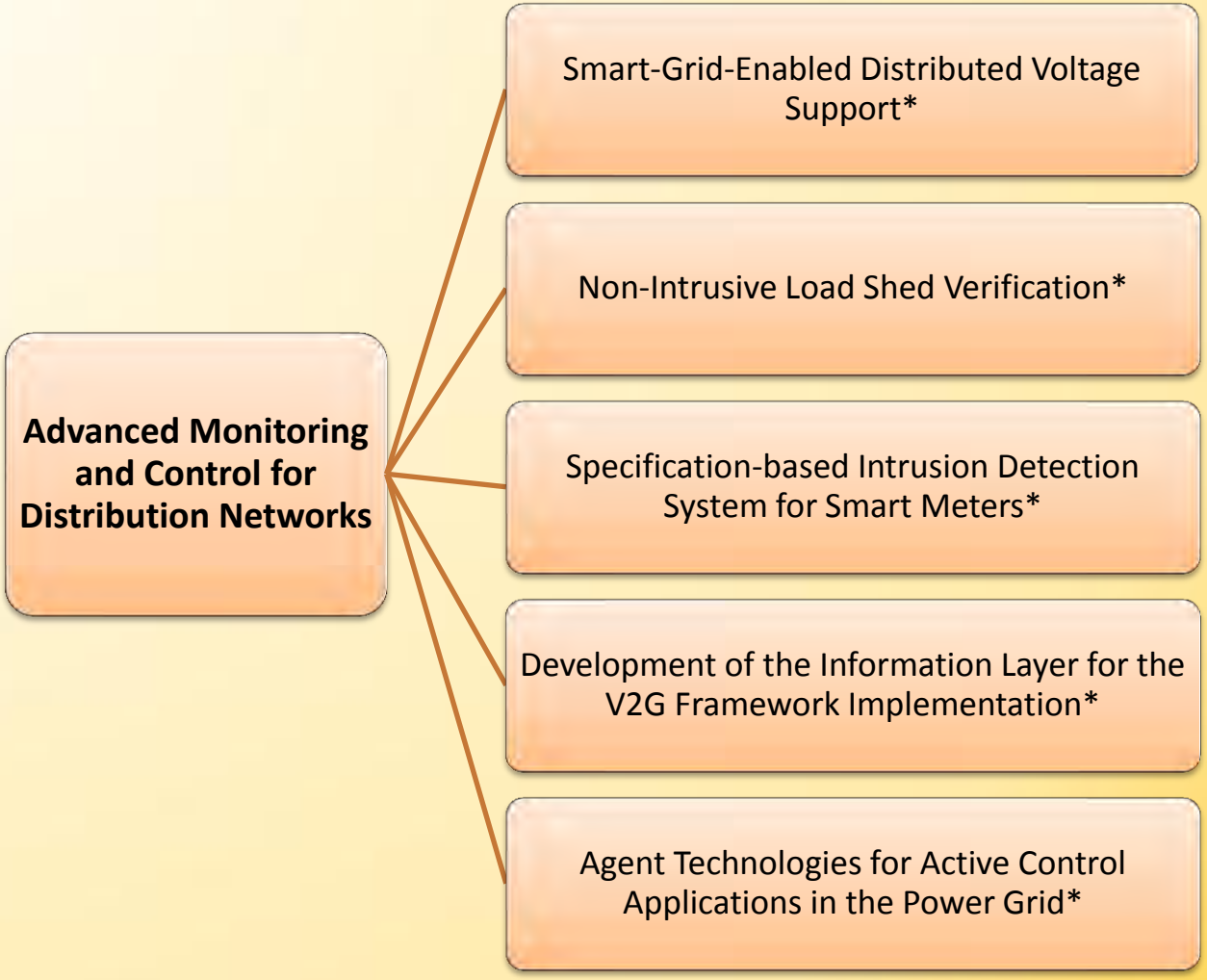
Wide-Area Monitoring and Control Applications

- Direct Application of PMU Values into Power Flow Software*
- GridStat Middleware Communication Framework: Application Requirements†

Component Technologies

- Lossless Compression of Synchrophasor Measurement Data Archives*
- Real-time Streaming Data Processing Engine for Embedded Systems*

Cluster: Trustworthy Cyber Infrastructure and Technologies for Active Demand Management



Cluster: Responding to and Managing Cyber Events

Design of Semi-Automated Intrusion Detection and Response Techniques

- A Game-Theoretic Response and Recovery Engine*
- Assessment and Forensics for Large-Scale Smart Grid Networks*
- Coordinating Black Start Operations Using Synchrophasors*

Cluster: Risk and Security Assessment

Model-based Assessment Tools

- Automatic Verification of Network Access Control Policy Implementations*
- Modeling Methodologies for Power Grid Control System Evaluation*
- Vulnerability Assessment Tool Using Model Checking*
- Analysis of Impacts of Smart Grid Resources on Economics and Reliability of Electricity Supply*
- Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components*
- Security and Robustness Power Evaluation and Enhancement of Power System Applications*

Experiment-based Assessment Tools

- Testbed-Driven Assessment: Experimental Validation of System Security and Reliability*
- Tools for Assessment and Self-assessment of ZigBee Networks*
- Fuzz-testing of Proprietary SCADA/Control Network Protocols*
- Trustworthiness Enhancement Tools for SCADA Software and Platforms*

Smart Grid Testbed Facilities Overview

- Multiple funding sources (NSF, DHS, DOE, State of Illinois, Office of Naval Research)
- Six years of enabling research for smart grid efforts (e.g., TCIP, TCIPG)
- Directed focus of supporting research in the power grid

Smart Grid Testbed Facilities
Current "State"

- Extensive end-to-end power hardware and software
  - 6 years of support and millions in equipment (purchased and donated)
  - Local expertise on a wide variety of real systems
- Encompassing Simulation and Emulation capabilities
  - Power, Network, and co-simulation
  - Protocols, Transport mediums
- Flexible framework being implemented and advancing towards tailored operating constraints

Smart Grid Testbed Facilities
Current Operating Model

- Advanced Academic Research
  - TCIPG (DOE, DHS)
  - CACAIS (ONR)
  - ICSEG (State of Illinois)
- Leveraged as a resource for various other smart grid projects at Illinois

Smart Grid Testbed Facilities
Near Term Direction

- Tailored environment to support external interaction
- Automated isolation and integration with a wide variety of resources
- Leveraging of the extensive work done under TCIPG and assist pipelining promising work into Industry

- Operating Model: Open for collaborative research

Smart Grid Testbed Facilities
Future Direction

- Fully automated isolation and customizable environment to time-share access to all resources in a repeatable and flexible manner
- Provide advanced cross-cutting expertise, talented resource pool, and uniquely available resources for wide use and to cooperatively engage in advanced research, support of industry agenda, and accelerated transition to practice
- Critical Infrastructure … beyond the smart grid

- Operating Model: Open for facility driven use, sponsored research, or technical testing

TCIPG Webcasts: Technologies for a Resilient Power Grid

- Present topics on research, development, and design of a secure and resilient power grid
- Webcasts are open to the public and attract a broad audience from industry, academia, and government
- Webcast first Friday of each month at 1:00 p.m. CT

CALL FOR SPEAKERS

TCIPG Seminar Series: Technologies for a Resilient Power Grid
beginning Fall 2010

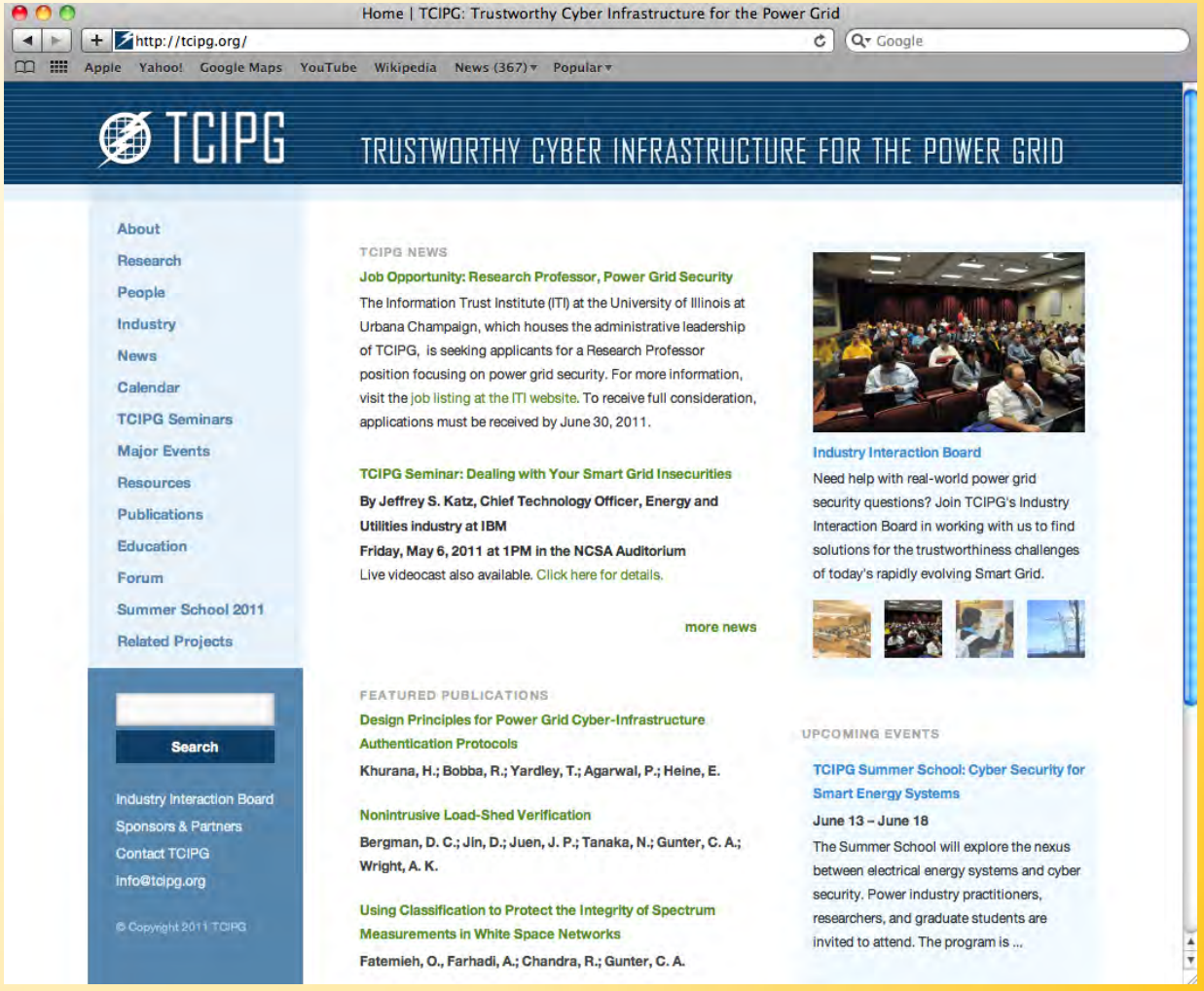
The new TCIPG Seminar Series on Technologies for a Resilient Power Grid seeks speakers to present topics in the broad area of research, development, and design for secure and resilient systems related to the power grid. The scope includes all power grid systems, from traditional systems involved in generation, transmission, and distribution to emerging systems dealing with distributed generation, renewable integration, and demand-response. The seminars will be held on the campus of the University of Illinois at Urbana-Champaign, normally on the first Friday of every month at 1:00 p.m. Central Time, and streamed live on the Web. The seminars will be open to the public and are expected to attract a broad audience from industry, academia, and government. TCIPG will cover speakers' travel costs.

If you are interested in appearing as a speaker in the series, please contact TCIPG principal scientist Himanshu Khurana at hkhurana@iti.illinois.edu.

The new seminar series is presented by the TCIPG Center (Trustworthy Cyber Infrastructure for the Power Grid), whose partner institutions are the University of Illinois at Urbana-Champaign, Cornell University, Dartmouth College, the University of California at Davis, and Washington State University. The TCIPG Center, which is a successor to the earlier NSF-funded TCIP Center, was founded in 2009 by the U.S. Department of Energy with additional support from the U.S. Department of Homeland Security. It is housed in the University of Illinois Information Trust Institute.

The TCIPG Center's work involves the development and integration of information technologies with the key properties of real-time availability, integrity, authentication, and confidentiality needed to build a more resilient power grid. Its objectives are to develop and evaluate technologies needed for realizing select Smart Grid applications, such as wide-area monitoring and control, demand response with controllable load, and plug-in hybrid electric vehicles. Ultimately, TCIPG research is expected to result in a secure and real-time communication system, an automated attack response system, and risk assessment and security validation techniques.

www.tcipg.org

To Learn More

- www.tcipg.org
- info@tcipg.org
- Request to be on our mailing list