TCIPG

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG

CYBERSECURITY & PRIVACY FOR THE SMART GRID: CHALLENGES AND OPPORTUNITIES

FEBRUARY 10, 2015

BILL SANDERS

GUIRR: CROSS-SECTOR IMPACT OF THE SMART GRID
NATIONAL ACADEMY OF SCIENCES

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

THE CHALLENGE: PROVIDING TRUSTWORTHY GRID OPERATION IN POSSIBLY HOSTILE ENVIRONMENTS

- Trustworthy
  - A system which does what it 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)

- **Multiparty interactions with partial & changing trust requirements**
- **Regulatory limits on information sharing**

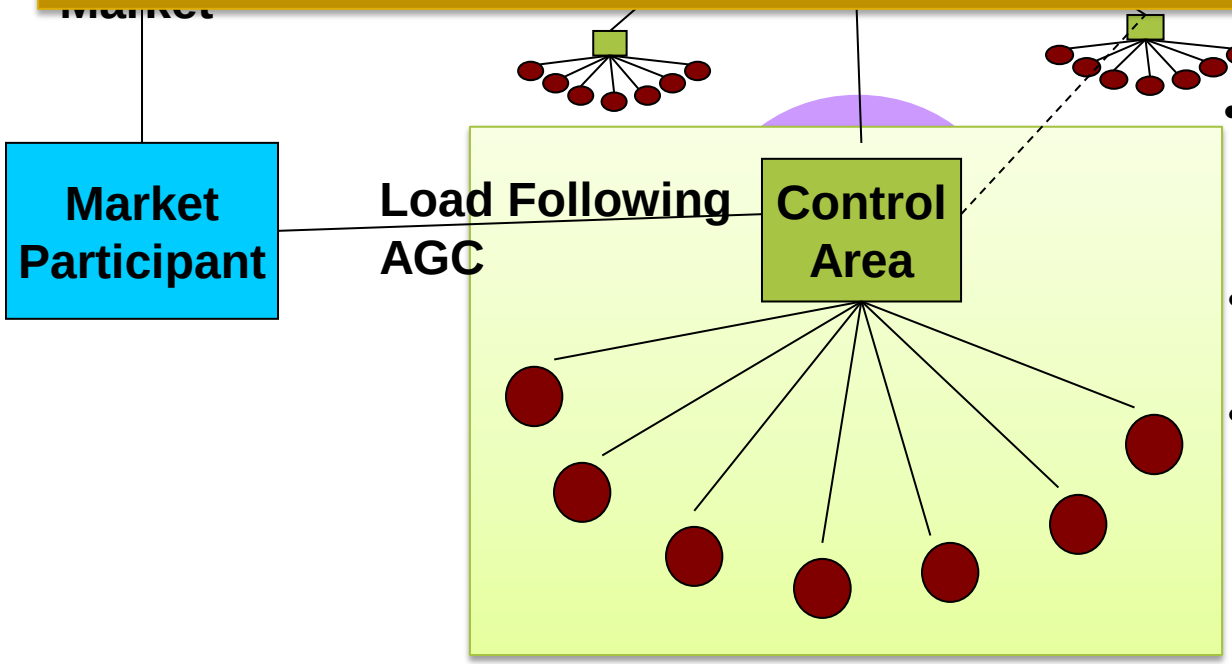
Other Coordinators

Market

Coordinator

Cross Cutting Issues

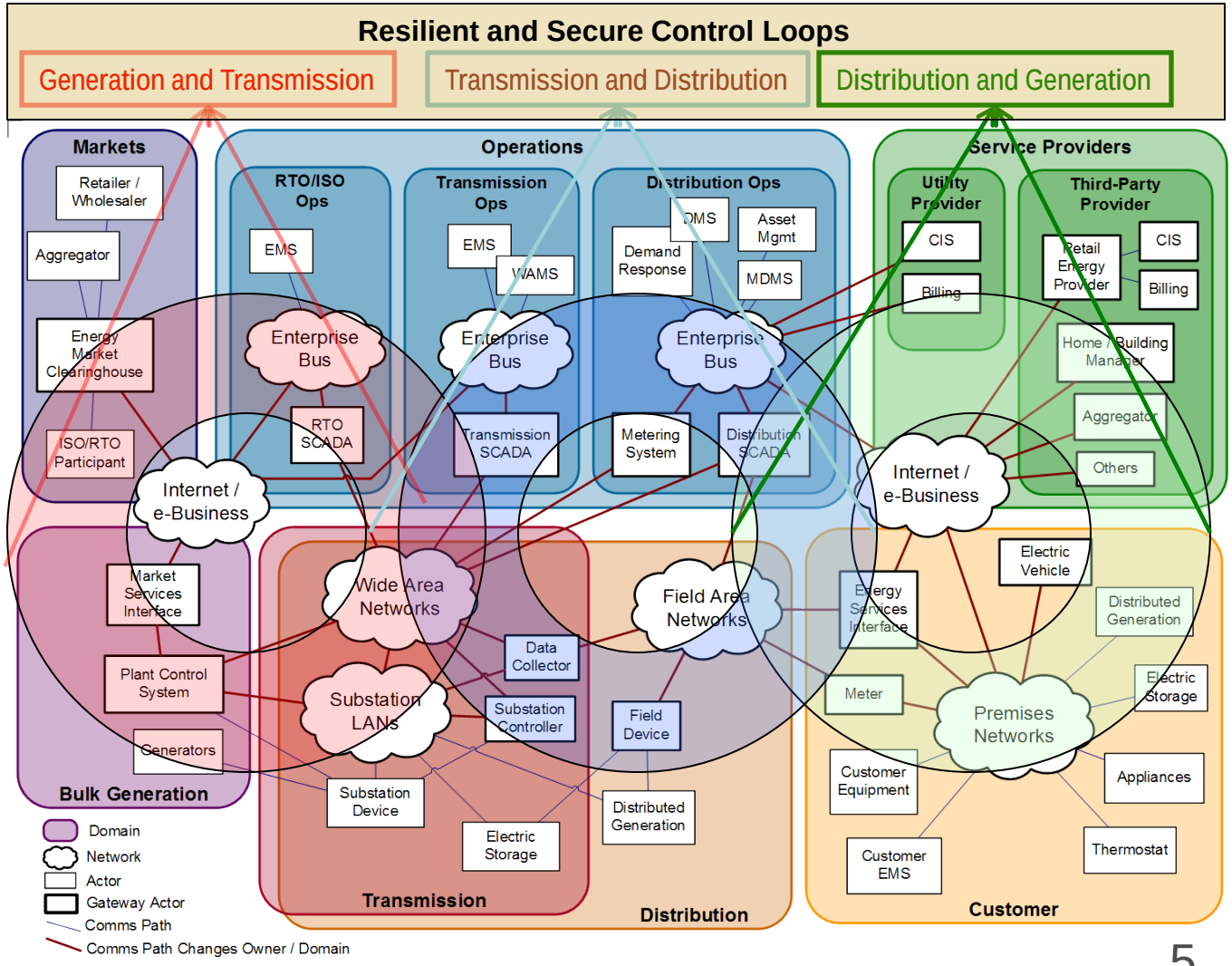
- **Large-scale, rapid propagation of effects**
- **Need for adaptive operation**
- **Need to have confidence in trustworthiness of resulting approach**



- Need to create secure and reliable computing base
- Support large # of devices
- Timeliness, security, and reliability required of data and control information

INFRASTRUCTURE MUST PROVIDE CONTROL AT MULTIPLE LEVELS

- **Multi-layer Control Loops**
- *Multi-domain Control Loops*
  - Demand Response
  - Wide-area Real-time control
  - Distributed Electric Storage
  - Distributed Generation
- *Intra-domain Control Loops*
  - Home controls for smart heating, cooling, appliances
  - Home controls for distributed generation
  - Utility distribution Automation
- **Resilient and Secure Control**
  - *Secure and real-time communication substrate*
  - Integrity, authentication, confidentiality
  - Trust and key management
  - End-to-end Quality of Service
  - *Automated attack response systems*
  - *Risk and security assessment*
  - Model-based, quantitative validation tools

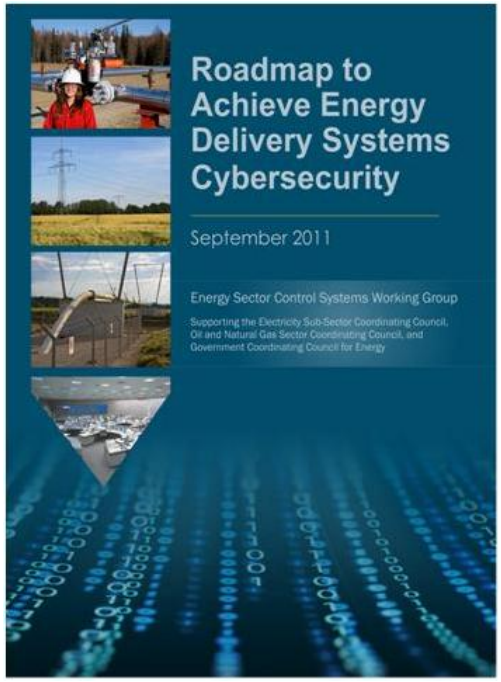


Note: the underlying Smart Grid Architecture has been developed by EPRI/NIST.

POWER GRID CYBER SECURITY GUIDANCE

- Roadmap to Achieve Energy Delivery Systems Cybersecurity – 2006, 2011
- FERC/NERC: Cybersecurity Standards – 2008 to present
- NISTIR 7628: Guidelines for Smart Grid Cybersecurity, 2009 to present
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) – 2012 to present

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.

FERC/NERC CYBER SECURITY STANDARDS FOR THE BULK ELECTRIC POWER GRID

- Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards
- FERC designated NERC as the ERO in 2006
- NERC worked with electric power industry experts to develop the NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009
- Standards approved by FERC in 2008, making them mandatory for owners and operators of the bulk electric system
- NERC standards continue to evolve, as the threat environment evolves, and more is known about critical infrastructure protection

CLASSICAL (PHYSICAL) ATTACK APPROACHES

- Physical attacks on lines, buses and other equipment can be locally effective:
  - "low tech" attacks may be easy, and are also difficult to defend against
  - Requires physical proximity of attacker
  - Particularly effective if multiple facilities are attacked in a coordinated manner
- But coordination may be much easier in a cyber attack

J.D. Konopka (a.k.a. Dr. Chaos) Alleged to have caused $800K in damage in disrupting power in 13 Wisconsin counties, directing teenaged accomplices to throw barbed wire into power stations. (From Milwaukee Journal Sentinel)
http://www.jsonline.com/news/Metro/may02/41693.asp

POTENTIAL TRANSMISSION-SIDE CYBER ATTACK STRATEGIES

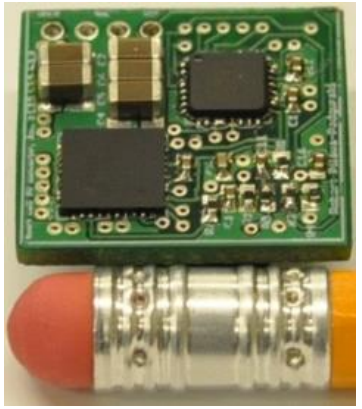
- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Malicious fuzzing of power system components
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

CHALLENGE #1: WIDE AREA TRUSTWORTHY OPERATION

- Physical consequences of cyber events in existing and evolving applications
- Scale
  - Number of devices
  - Number of business entities
  - Distance/area/fraction of grid encompassed
  - Large attack surface
- Real-time
  - Someday, wide-area controls expected to stabilize the grid after cyber or physical contingencies
- Achieving resilience through redundancy
- Analyzing *risks*, not just vulnerabilities

CHALLENGE #2: LOCAL AREA TRUSTWORTHY OPERATION

- Leveraging a much more dynamic load
  - New loads including PHEVs, and distributed resources such as PV, represent challenges and opportunities
  - Smart meters provide enhanced understanding and, potentially, control of the load, but also more cyber issues



- Making the distribution system smarter
  - More information for better safety and reliability
  - More cyber-enabled, distributed devices
  - Communication and control issues

CHALLENGE #3: PROVIDING GRID RESILIENCY

- Detection of suspicious events
  - Profusion of potential attack points
    - Many embedded and legacy systems, difficult to harden
  - Direct detection via cyber traffic analysis
  - Detection informed by physical system state
- Making sense of potential “event avalanche”
  - Situational awareness
  - Again, comprehend the cyber and physical state
- Response
  - Carefully consider consequence of response
  - Ultimately, operate through cyber attack or failure

CHALLENGE 4: TRUST 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

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

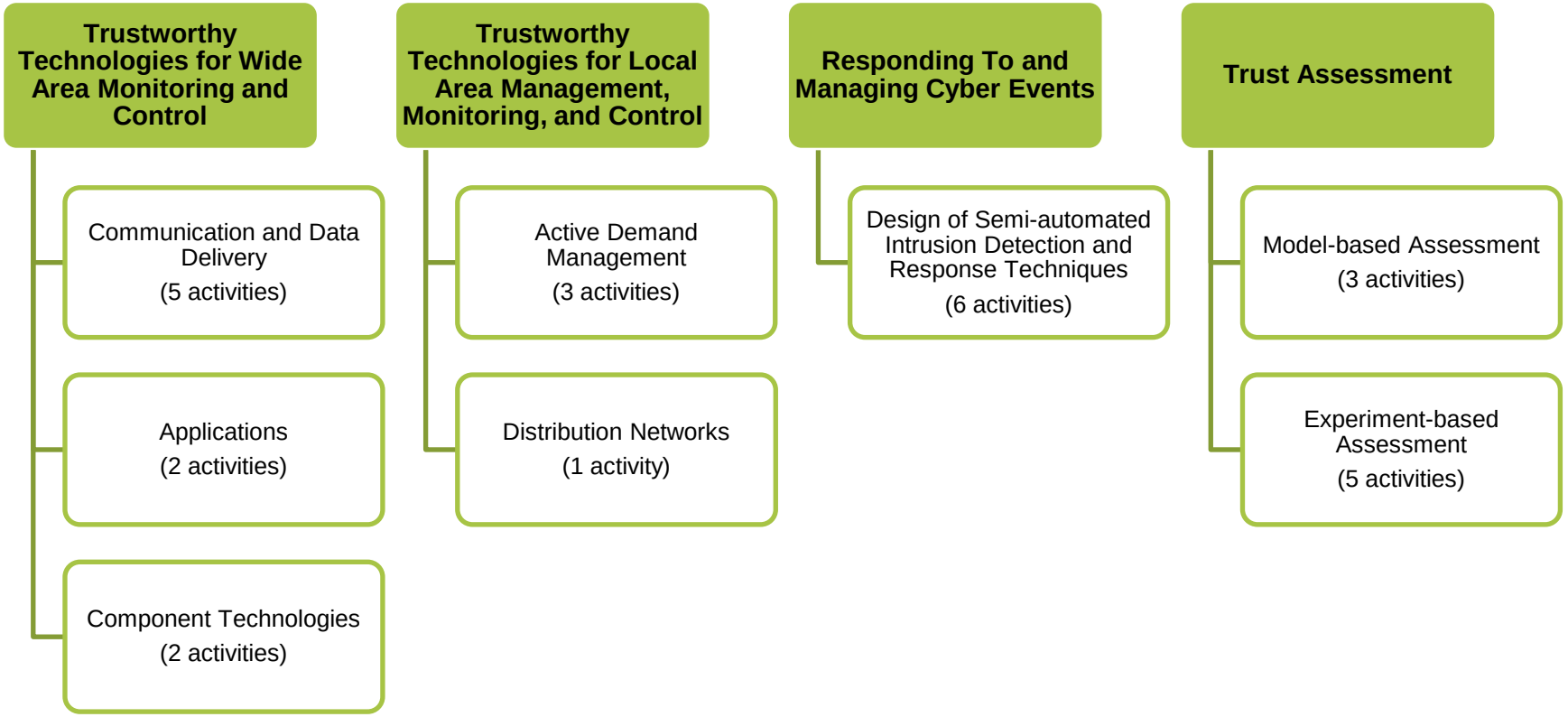
Research focus: Resilient and Secure Smart Grid Systems

- 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

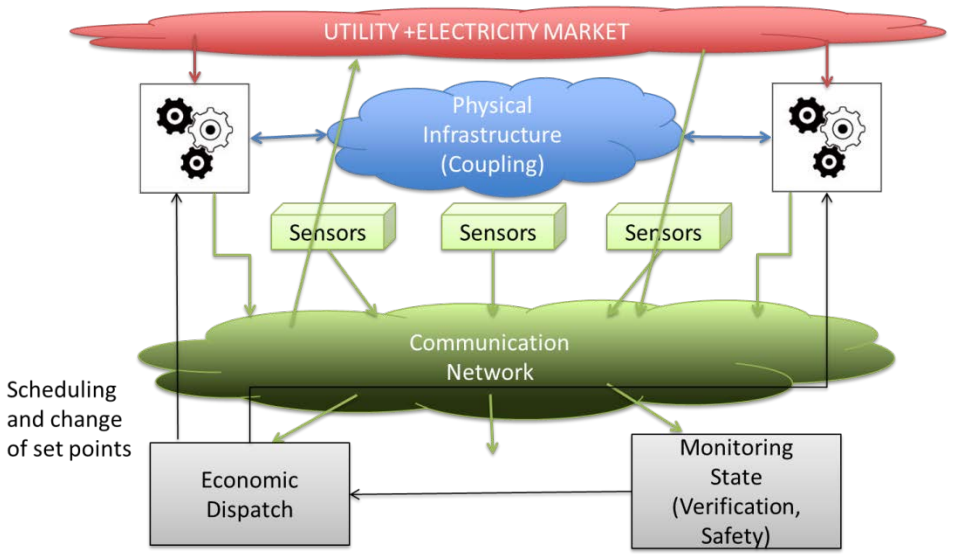
- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009 ($3.8M cost share)
- No-cost extension to Aug. 30, 2015
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cybersecurity R&D Center, Office of Science and Technology
- 4 Universities
  - Dartmouth College
  - University of California at Davis
  - University of Illinois at Urbana-Champaign
  - Washington State University
- 20+ Faculty, 15+ Technical Staff, 40+ Students and 3 Admin Staff contributed to the project in FY 2014

TCIPG TECHNICAL CLUSTERS AND THREADS



CLUSTER 1: TRUSTWORTHY TECHNOLOGIES FOR WIDE-AREA MONITORING AND CONTROL

- Applications of wide-area data, primarily in the transmission system
- Cyber infrastructure architecture to support those applications
- Securing data in transit
- Security and resilience of subsystems that collect, communicate and process data



CLUSTER 2: TRUSTWORTHY TECHNOLOGIES FOR LOCAL-AREA MANAGEMENT, MONITORING, AND CONTROL

- Key driver is adding more renewable, but less controllable generation
  will require more end
  user participation

- Cyber security concerns
  for both end users and the distribution system
- End Users (Load)
  - Requiring more communication and control
  - Increasing use of distributed generation resources
- Distribution Systems
  - New technologies an sensing promise better reliability

CLUSTER 3: RESPONDING TO AND MANAGING CYBER EVENTS

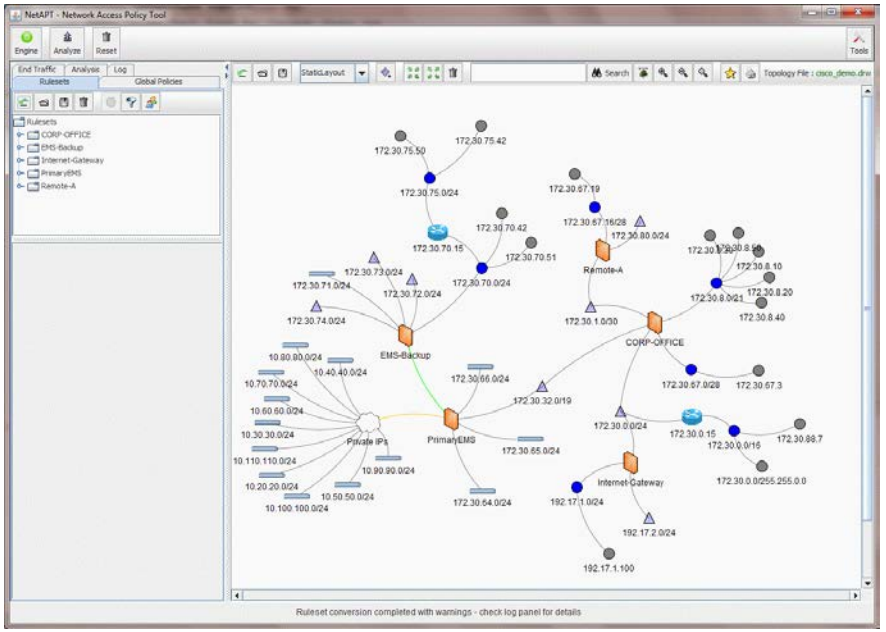
- Attack detection
  - Based on formal analysis of protocol
  - Leveraging special properties of grid systems
- Situational understanding of the security state as it impacts the physical state
- Cyber-physical aware response
- Operate through attack
- Post-event analysis
- Deploy solutions

CLUSTER 4: TRUST ASSESSMENT

- Create methods and tools that use simulation, modeling, and experimentation to support quantitative trust assessment of
  - power grid devices, hardware/software architectures, protocols, and applications
  - measurement data representing power system state
  - monitoring and protection mechanisms/algorithms used to provide power grid resiliency

EXAMPLE TECHNOLOGY TRANSFER: NETWORK PERCEPTION, INC.

- Based on NetAPT technology developed under TCIPG
  - Static analysis of firewall rulesets
  - Tuned to utility systems, where identifying routable paths to critical cyber assets is an increasingly important problem
- Pilot deployment at major IOUs as technology matured
  - Demonstrated usefulness in NERC CIPS audits
- Used in security assessment of rural electric cooperative utility networks
- Transition of NetAPT from an academic project to a commercial product has been supported at UIUC by a one-year grant from DHS S&T



Network Perception is now a technology startup

ENGAGEMENT AND PUBLIC LEARNING

Parents and children learn together

Publicize the importance of knowing about electricity production and delivery

Illustrate challenges, trade-offs and decisions that will come with the modernization of the electric grid

Communicate the importance of consumers as a smarter grid becomes a reality

Power and Energy applets

- 32,000 visits in the past year
- 1000 CD's distributed

Tesla Town for the iPad and Android

- 5500 iTunes downloads
- Available in Google play store

Lesson plans

Posters

Trading cards

Hands-on kits

HANDS-ON SCADA SECURITY ASSESSMENT TRAINING

A utility-like virtual environment

- Includes typical security flaws
- Provides an introductory demonstration of assessment techniques within a SCADA environment

2015 TCIPG SUMMER SCHOOL

- Plan: Leverage the emerging Smart Grid Cybersecurity Curriculum
- Will include hands-on training
- Scheduled for June 15-19, 2015, reception June 14
- Venue will be the Q Center near Chicago, IL

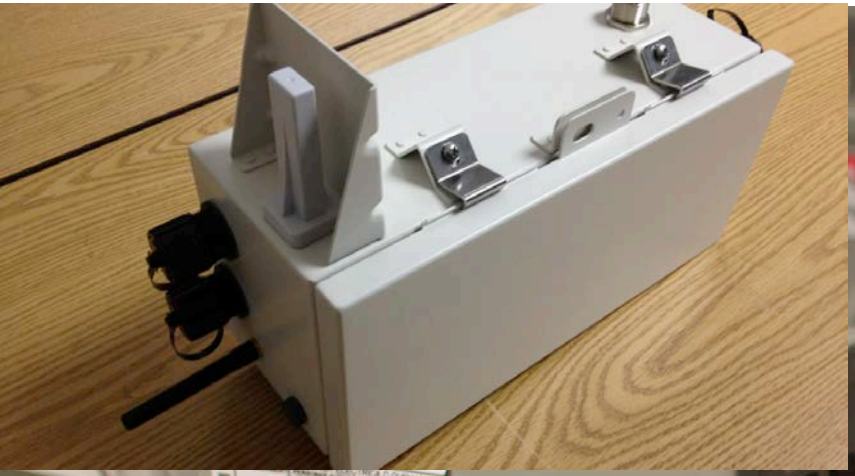
2015 Summer School
June 15-19, 2015
Reception: June 14

TCIPG TESTBED

- A lab-contained but true-to-reality implementation of critical infrastructure
- Leverages over $6.5 million worth of hardware and software (much of which is donated)
- Brings together power system equipment, emulation, and simulation
  - Supports cutting-edge research on grid topics from generation to consumption
- Automated for efficient and effective provisioning of power and cyber assets per experiment
- Used for internal TCIPG research, collaboration with national labs, and projects with industry

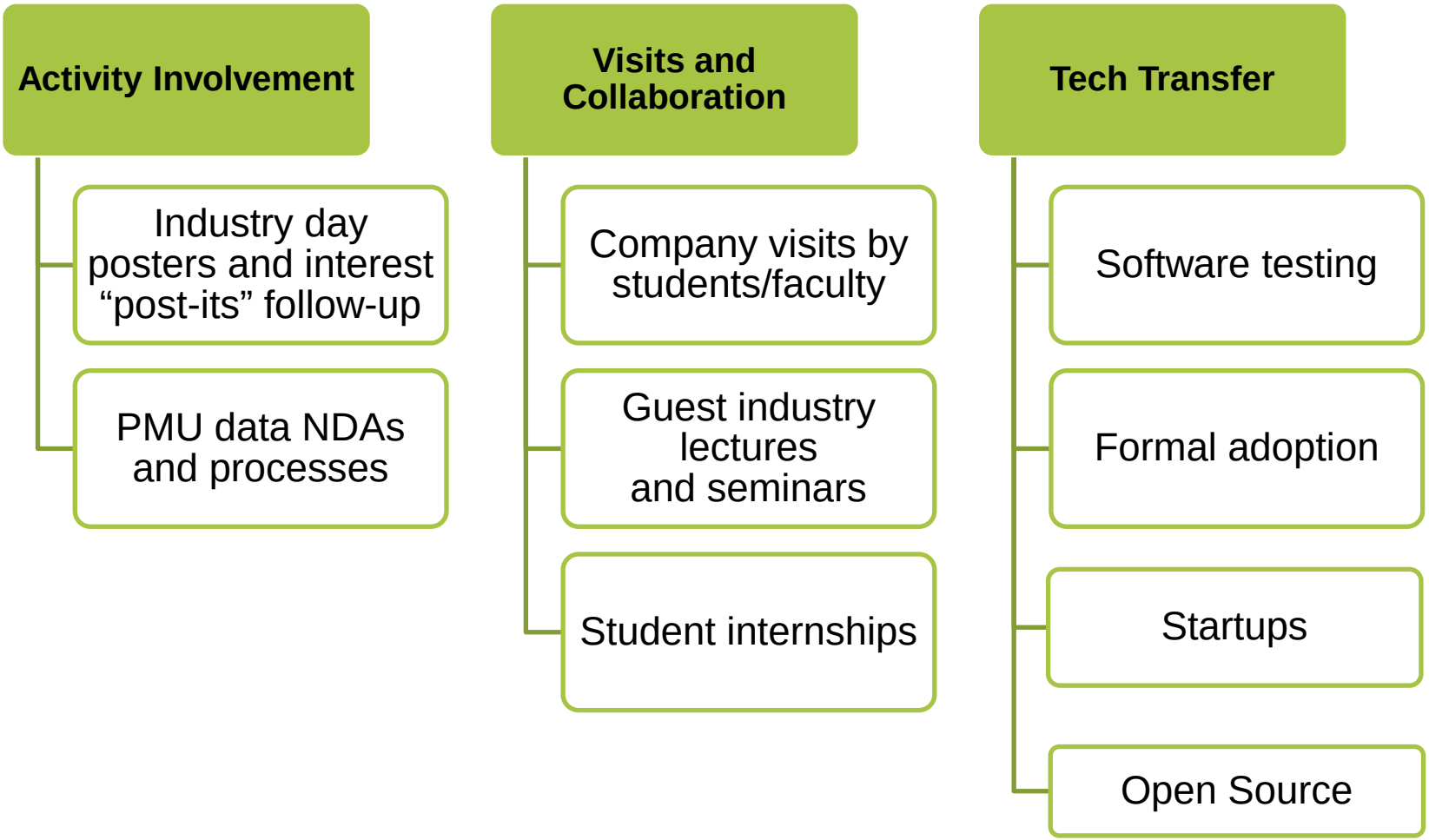

TCIPG Rack 1
TCIPG Rack 2
TCIPG Rack 3
TCIPG Rack 4
Mu Dynamics
DELL


SEL-421
SEL
RTDS ™
Real-Time Digital Simulator
RTDS Technologies
GTWIP
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 C2S0D 30TA 1.0Kh
MARKETING SAMPLE
306 382 306
OpenWay
CL200 240V 3W TYPE C2S0D 30TA 1.0Kh
MARKETING SAMPLE
306 382 289
OpenWay

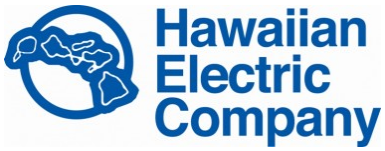
CROSS-CUTTING EFFORT: INDUSTRY INTERACTION AND TECHNOLOGY TRANSITION



INDUSTRY INTERACTION: VENDORS AND UTILITIES THAT HAVE PARTICIPATED IN TCIPG EVENTS (2010-2011)

INDUSTRY INTERACTION: OTHER ORGANIZATIONS THAT HAVE PARTICIPATED IN TCIPG EVENTS (2010-2011)

NEW PARTICIPANTS FOR 2012-2013 (1)



NEW PARTICIPANTS FOR 2012-2013 (2)

Host Integrity Systems
Securing integrity for enterprises through discovery, technology, and governance

HWS ENERGY PARTNERS LLC

ICS Cybersecurity, Inc.

Fighting for Illinois Consumers CUB Since 1984

Illinois Commerce Commission ICC

IOActive™
Using Our Past to Secure Your Future.

LUS
LAFAYETTE UTILITIES SYSTEM

Los Alamos
NATIONAL LABORATORY
EST. 1943

neustar

your NEW HAMPSHIRE Electric Co-op
A Touchstone Energy® Cooperative

OFFIS

PNM Resources

PRAIRIE POWER INC.

Raytheon

RIVER LOOP SECURITY

Sandia National Laboratories

S&C ELECTRIC COMPANY
Excellence Through Innovation

Schneider Electric

Sega®

SOUTHERN CALIFORNIA EDISON
An *EDISON INTERNATIONAL* Company

SRI International
R&D for Government and Business

U.S.NRC

SHAY KEPPLE PHILLIPS LTD
ATTORNEYS AT LAW

TECO
TAMPA ELECTRIC

TIAA CREF

United States Northern Command

THE WHITE HOUSE
WASHINGTON

VERMONT LAW SCHOOL

westMONROE PARTNERS

wurldtech™

SUMMARY

- Assuring grid resilience demands a complex, multifaceted mission
- TCIPG is a world-leading research center that is 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
- Many challenges remain – but the progress has been dramatic over the last decade – and the future is bright if industry, government, and academia work together.

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our TCIPG Summer School June 2015