EEI Edison Electric Institute

Power by Association℠

Keeping the Lights On

Industry Engagement in Resilience: Preparedness, Prevention, Response, and Recovery

The Problem
(Potential) Adversaries

- Script Kiddies
- _ Business Network
- Hacktivists
- Irregular Actors
- Disgruntled Insider
- Nation State/State Sponsored

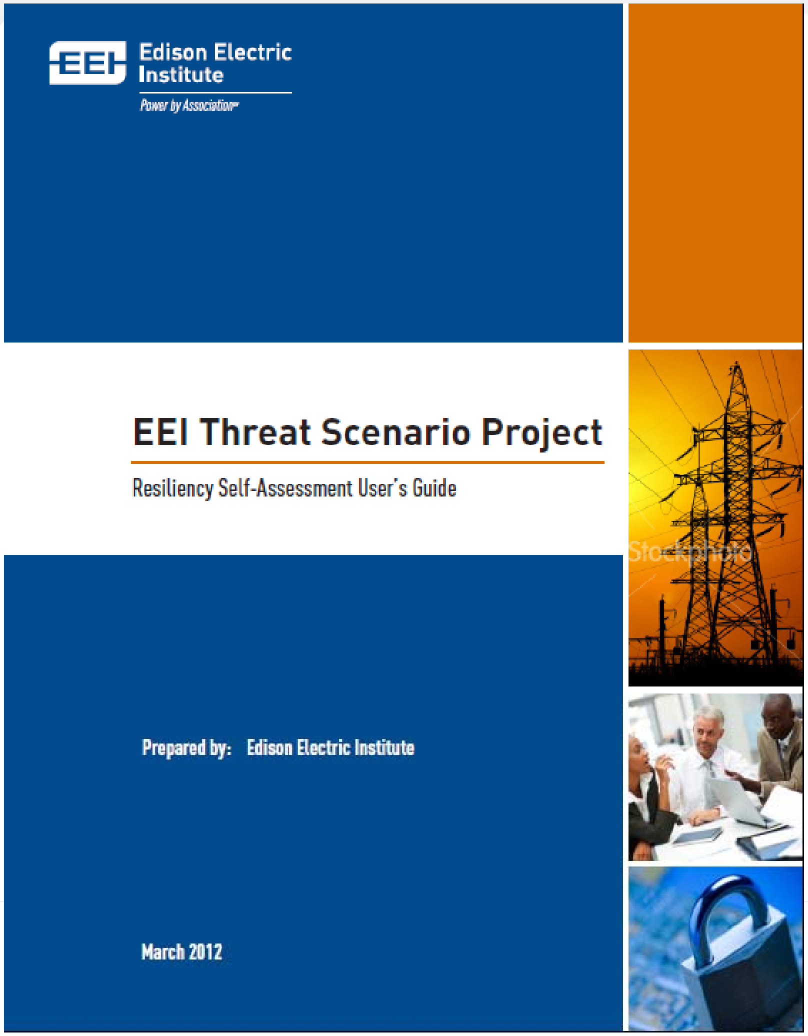
2012 (so far)

- Public statements about Stuxnet, Flame
- Major phishing attacks against oil and natural gas operators
- Military doctrine associated with cyber
- Attacks against NASA revealed
- Aramco / RasGas

Examples of Industry Response

- EEI
  Threat Scenario Project
- DOE C2M2

EEI Threat Scenario Project



Edison Electric Institute

Power by Association

EEI Threat Scenario Project

Resiliency Self-Assessment User's Guide

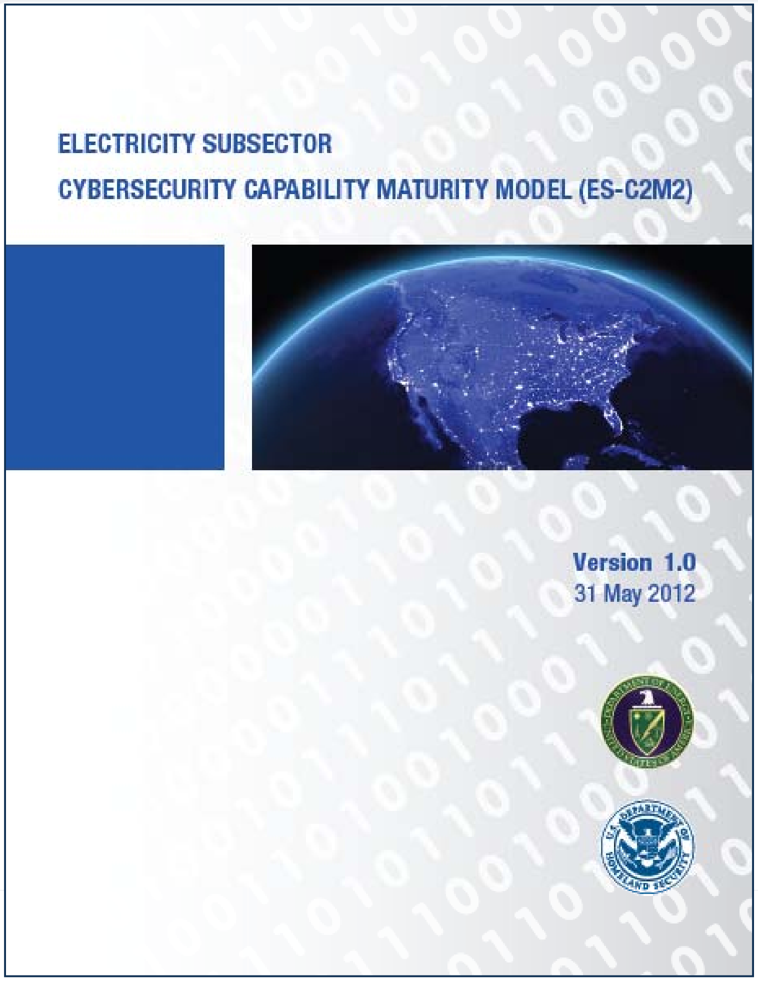
Prepared by: Edison Electric Institute

March 2012

Member companies worked with The Chertoff Group to develop mitigation actions for top industry threats

Conducted self-assessments based on threats and mitigation measures.

DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0
31 May 2012

Approximately 20 companies (Investor Owned Utilities, Coops and Munis) participated in the pilot.

Domains in maturity model in which companies are evaluated:

1. Asset, Change, and Configuration Management (ASSET)
2. Workforce Management (WORKFORCE)
3. Identity and Access Management (ACCESS)
4. Risk Management (RISK)
5. Supply Chain and External Dependencies Management (DEPENDENCIES)
6. Threat and Vulnerability Management (THREAT)
7. Event and Incident Response, Continuity of Operations (RESPONSE)
8. Situational Awareness (SITUATION)
9. Information Sharing and Communications (SHARING)
10. Cybersecurity Program Management (CYBER)

Utility, Asset Owner Operator Response

- Recognition of New Reality
- Different Threat Actors
- Marathon

- Corporate Culture Change

Responding

- CEO, Board of Directors Focus
- Engagement between operations and Physical/ IT/ Security organizations
- New engagement with Local/Federal law enforcement

Information Sharing

Responding

- Protection of Control / EMS /SCADA networks
- Sustainable, repeatable processes required
- Commitment to Protection

Thank You!

2012 Major Accomplishments

- NIST Smart Grid Framework 2.0 Published
- Recognized and used internationally
- SGIP Catalog of Standards
- Green Button now available to 15 million customers; 36 million by YE 2013
- SGIP 2.0 Launched
- NIST SG Program integrated into Engineering Laboratory
- Multi-year NIST SG measurement science research program plan developed
- Smart Grid Test Bed under development

Cybersecurity Needs for the Smart Grid

Bill Sanders

University of Illinois at Urbana-Champaign
www.tcipg.org
whs@illinois.edu

NIST SGAC Meeting
December 18, 2012

Coordinated Science Laboratory

Building Interdisciplinary Excellence with Societal Impact

- **Excellence in:**
  - Computing and Networks
  - Circuits, Electronics & Surface Science
  - Communications & Signal Processing
  - Decision & Control
  - Remote Sensing

- **Initiatives:**
  - Computer Vision
  - SRC Focus Center Research Program
  - Neuroengineering IGERT
  - Human-Machine Adversarial Network MURI

- **Statistics:**
  - 60 years as a premier national interdisciplinary research facility
  - 550 Researchers: 110 professors, 330 graduate students, 60 undergraduate students, & 50 professionals
  - Over $300M in active research projects as of Aug. 2012

- **Affiliated Institutes:**
  - ITI: Information Trust Institute
  - ADSC: Advanced Digital Sciences Center (Singapore)
  - PCI: Parallel Computing Institute

- **Major Centers:**
  - Illinois Center for Wireless Systems
  - NSF National Center for Professional and Research Ethics
  - NSF Science of Information Science and Technology Center
  - DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center
  - Boeing Trusted Software Center
  - HHS SHARPS Health Care IT Security Center
  - NSA Science of Security Center
  - Illinois Center for a Smarter Electric Grid

Outline

- Challenge, Vision, and Roadmap
- 4 Key Challenges
- TCIPG Vision and Research Focus
- Industry / Academic Interaction in Research

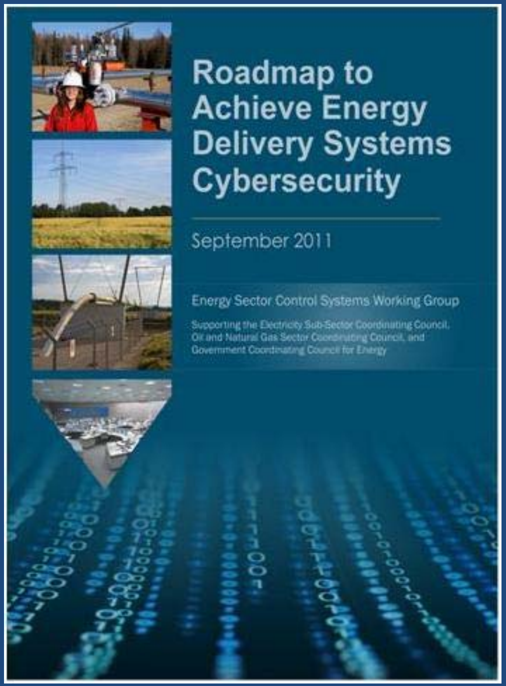
The Challenge: Providing Trustworthy Smart Grid Operation in Possibly Hostile Environments

- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Availability, Security, Safety, …
- Hostile Environment
  - 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)

Industry Roadmap – A Framework for Public-Private Collaboration



Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

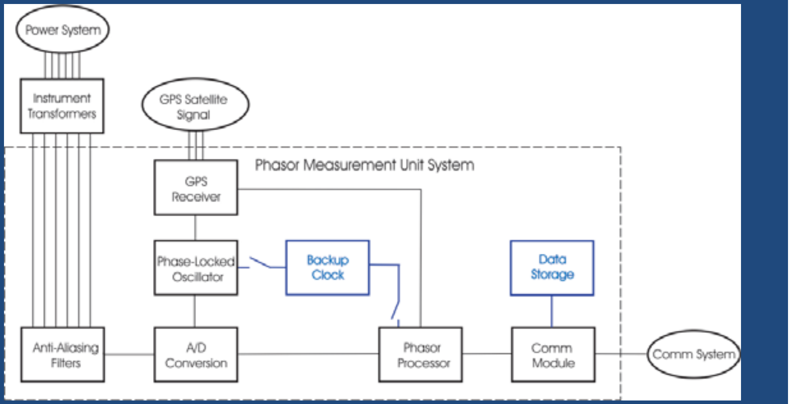
- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in 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.

Challenge 1: Trustworthy technologies for wide-area monitoring and control

- Smart Grid vision for the wide area (primarily transmission) is:
  - Vastly more sensing at high, synchronous rates (example: PMUs)
  - New applications that use these data to improve
    - Reliability
    - Efficiency
    - Ability to integrate renewables



- Achieving the vision requires secure and reliable communications between sensors, control devices, and monitoring and control applications all owned and operated by the many entities that make up the grid

Challenge 2: Trustworthy technologies for local area management, monitoring, and control

- Electric grid can be divided into three groups: the generation, the wires (T&D), and the demand. This challenge focuses on the demand and the nearby distribution
  - Generation must track load

- For a grid with more renewable, but less controllable generation (e.g., wind and solar PV), more load control will be needed
  - Distributed generation may be embedded in "demand"
  - New loads (electric vehicles) could drastically change demand profile

Challenge 3: Responding to and managing cyber events

- Combined cyber and physical attack detection, response to detected attacks, and recovery from attack consequences is essential to providing resilience
- Existing detection and response methods are *ad hoc*, at best, and rely on assumptions that may not hold
- Aim to detect and respond to cyber and physical events, providing resilience to partially successful attacks that may occur:
  - Making use of cyber and physical state information to detect attacks
  - Determine appropriate response actions in order to maintain continuous operation
  - Minimize recovery time when disruptions do occur

Challenge 4: Trust and Risk 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

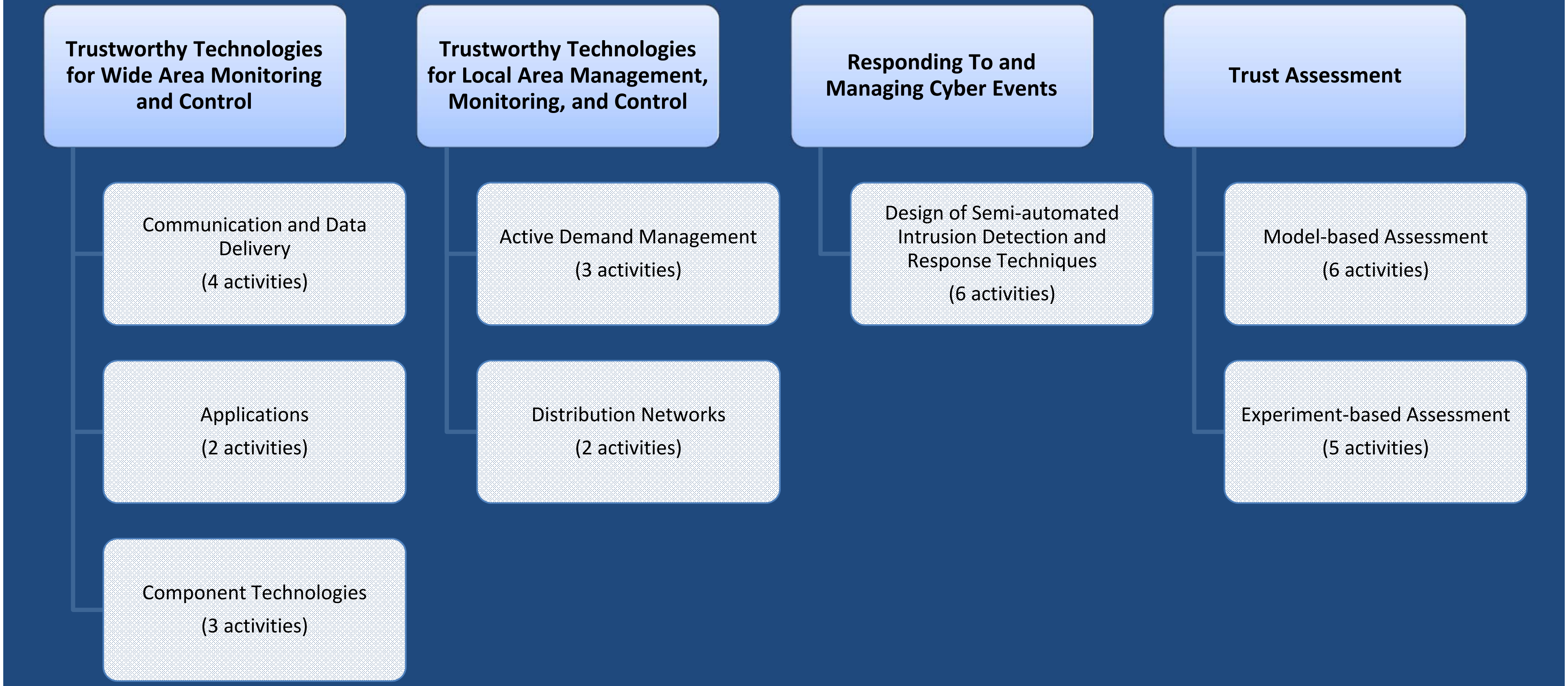
Research focus: Resilient and Secure Smart Grid Systems

- 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)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cybersecurity R&D Center, Office of Science and Technology
- Core to a suite of activities now going on at the partner schools
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 23 Faculty, 20 Technical Staff, 38 Graduate Students, 7 Ugrad Students, 1 Admin Staff worked on the project in FY 2012

TCIPG Technical Clusters and Threads



Trustworthy Technologies for Wide Area Monitoring and Control

- Communication and Data Delivery (4 activities)
- Applications (2 activities)
- Component Technologies (3 activities)

Trustworthy Technologies for Local Area Management, Monitoring, and Control

- Active Demand Management (3 activities)
- Distribution Networks (2 activities)

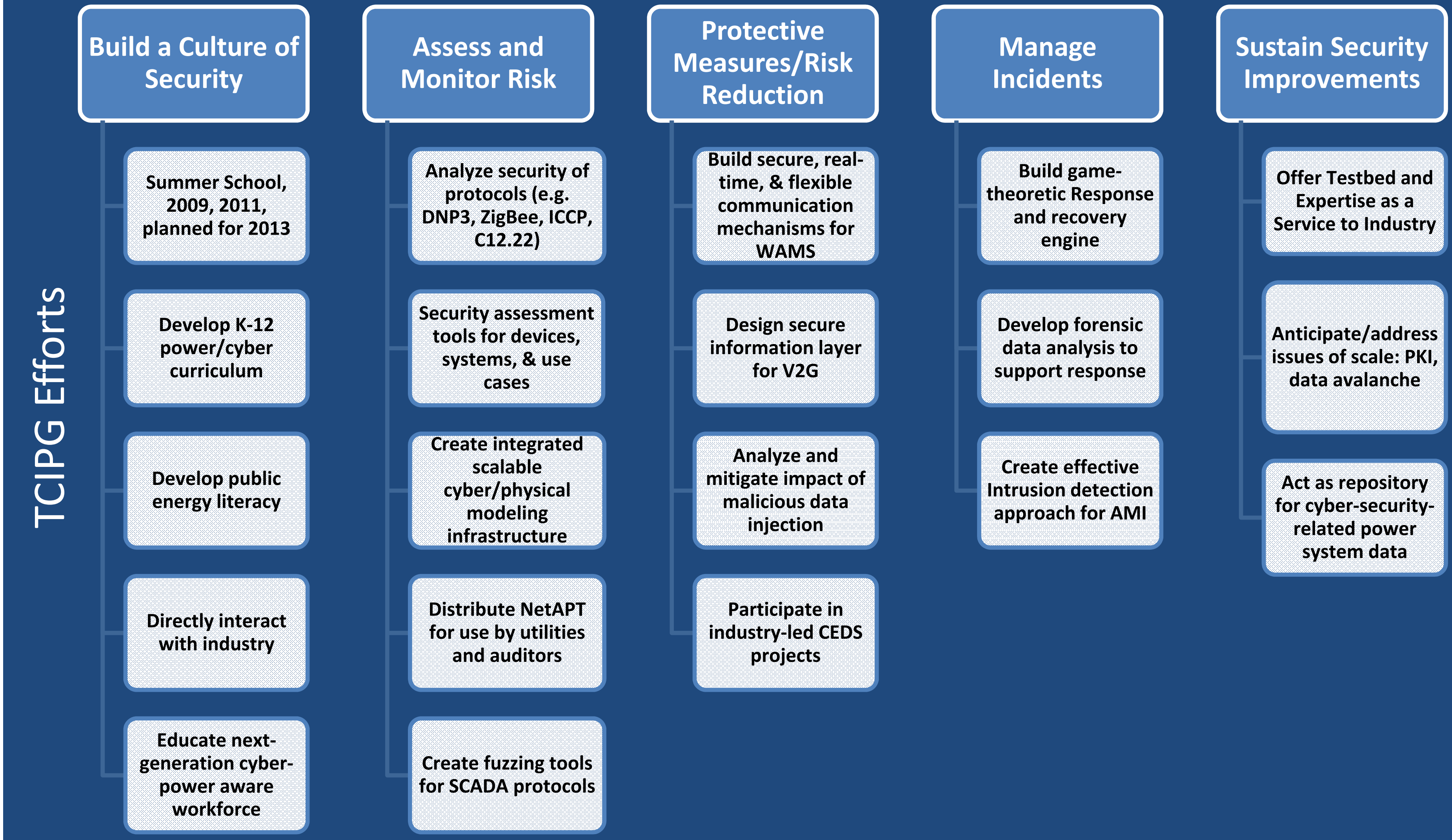
Responding To and Managing Cyber Events

- Design of Semi-automated Intrusion Detection and Response Techniques (6 activities)

Trust Assessment

- Model-based Assessment (6 activities)
- Experiment-based Assessment (5 activities)

TCIPG Impacts All Aspects of the Roadmap Framework



TCIPG Efforts

Build a Culture of Security
- Summer School, 2009, 2011, planned for 2013
- Develop K-12 power/cyber curriculum
- Develop public energy literacy
- Directly interact with industry
- Educate next-generation cyber-power aware workforce

Assess and Monitor Risk
- Analyze security of protocols (e.g. DNP3, ZigBee, ICCP, C12.22)
- Security assessment tools for devices, systems, & use cases
- Create integrated scalable cyber/physical modeling infrastructure
- Distribute NetAPT for use by utilities and auditors
- Create fuzzing tools for SCADA protocols

Protective Measures/Risk Reduction
- Build secure, real-time, & flexible communication mechanisms for WAMS
- Design secure information layer for V2G
- Analyze and mitigate impact of malicious data injection
- Participate in industry-led CEDS projects

Manage Incidents
- Build game-theoretic Response and recovery engine
- Develop forensic data analysis to support response
- Create effective Intrusion detection approach for AMI

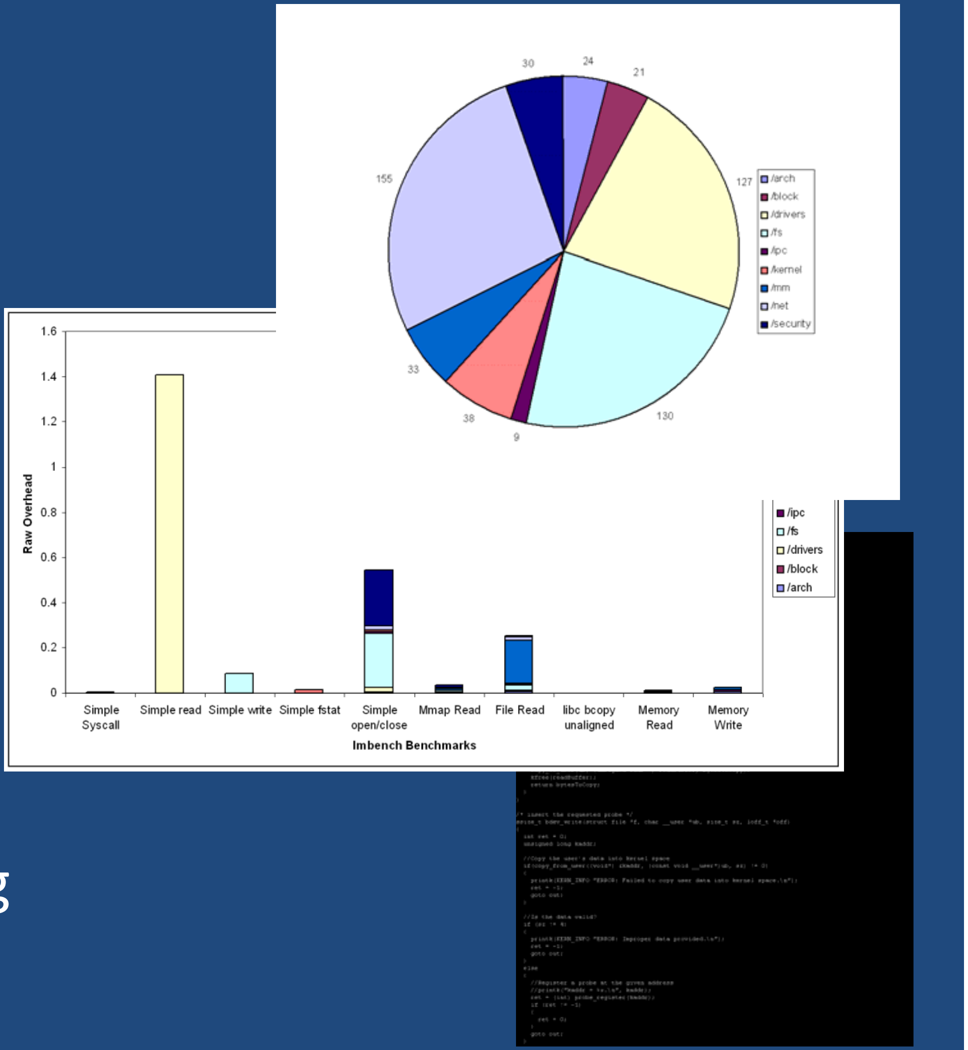
Sustain Security Improvements
- Offer Testbed and Expertise as a Service to Industry
- Anticipate/address issues of scale: PKI, data avalanche
- Act as repository for cyber-security-related power system data

Selected Accomplishments (Oct. 1, 2011 – Sep. 30, 2012)

- Autoscopy embedded system security transition to SEL
- NetAPT in use by utilities and regional entities. Commercialization grant from DHS.
- Advances in understanding and mitigating security issues with AMI and wide-area measurements
- Analysis tools to address the smart grid data avalanche, to efficiently quantify security policy in terms of high-level data structures
- Testbed enhancement now includes AMI and federation to DEFT framework

2012 Accomplishments: Autoscopy Jr.

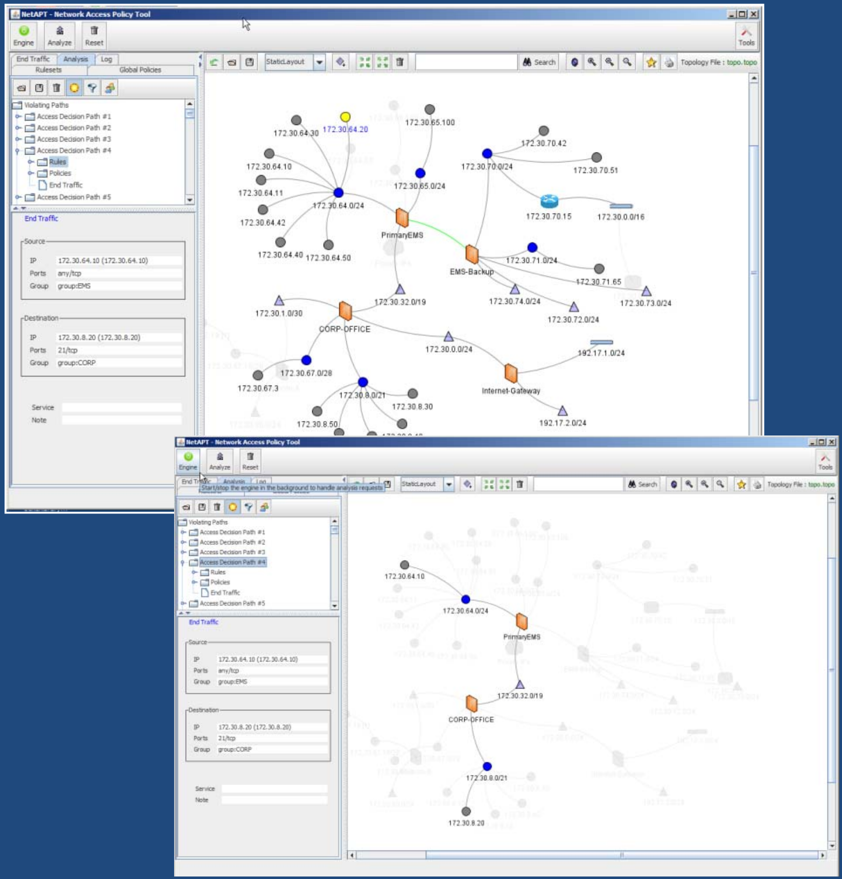
- Autoscopy Jr. is a practical, innovative approach to security in embedded systems
- Research largely completed in 2011
- Tech transfer to SEL
  - SEL has developed a flow-control system based on Autoscopy
  - Incorporated into SEL Exe-Guard project
  - Plans to include in upcoming product lines



```
  kfree(readBuffer);
  return bytesToCopy;
 }
}

/* insert the requested probe */
ssize_t bdev_write(struct file *f, char __user *ub, size_t sz, loff_t *off)
{
 int ret = 0;
 unsigned long kaddr;

 //Copy the user's data into kernel space
 if(copy_from_user((void*) &kaddr, (const void __user*)ub, sz) != 0)
 {
  printk(KERN_INFO "ERROR: Failed to copy user data into kernel space.\n");
  ret = -1;
  goto out;
 }

 //Is the data valid?
 if (sz != 4)
 {
  printk(KERN_INFO "ERROR: Improper data provided.\n");
  ret = -1;
  goto out;
 }
 else
 {
  //Register a probe at the given address
  //printk("kaddr = %x.\n", kaddr);
  ret = (int) probe_register(kaddr);
  if (ret != -1)
  {
   ret = 0;
  }
  goto out;
 }
```

2012 Accomplishments: NetAPT

- NetAPT identifies routable paths to network nodes, including critical cyber assets in energy delivery systems
- Mature TCIPG technology
  - Development continues to increase the number of firewalls supported
- More than 20 copies have been licensed to NERC auditors and utilities, including SERC, SPP, WECC, Ameren, PJM, and 3 Electric Cooperatives (AEIC, EIIEC, and Cornbelt Energy)
- Used as a NERC-CIP audit tool
- Commercialization grant from DHS



End Traffic

Source

IP 172.30.64.10 (172.30.64.10)

Ports any/tcp

Group group:EMS

Destination

IP 172.30.8.20 (172.30.8.20)

Ports 21/tcp

Group group:CORP

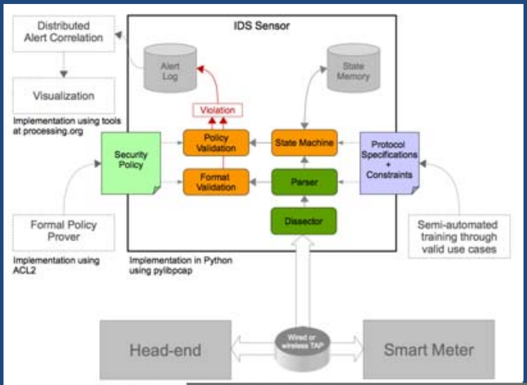
Service

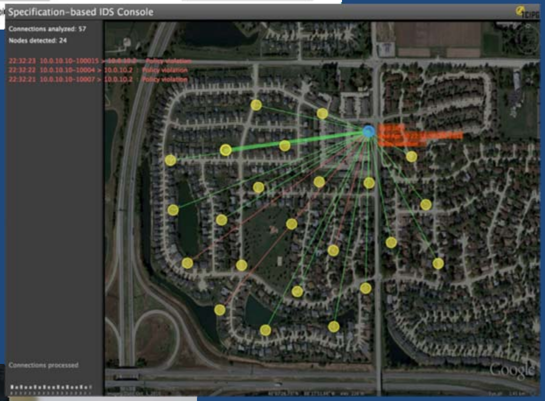
Note

Start/stop the engine in the background to handle analysis requests

2012 Accomplishments: AMI Security

- Specification-based IDS overcome shortcomings of signature-based IDS, and provide potential protection against zero-day attacks.
  - TCIPG's AMI-lyzer protects AMI systems using C12.22 and C12.19 protocols
  - Successfully deployed in TCIPG AMI testbed
  - Demonstration at EPRI Power Delivery and Utilization meeting
  - Working with FirstEnergy on a pilot deployment
- Hardware-based IDS for meters
  - 3 provisional patent applications


IDS Sensor
Distributed Alert Correlation
Visualization
Implementation using tools at processing.org
Alert Log
State Memory
Violation
Security Policy
Policy Validation
Format Validation
State Machine
Parser
Dissector
Protocol Specifications + Constraints
Formal Policy Prover
Implementation using ACL2
Implementation in Python using pylibpcap
Semi-automated training through valid use cases
Head-end
Wired or wireless TAP
Smart Meter
Simulation using Tabl



Connections analyzed: 57

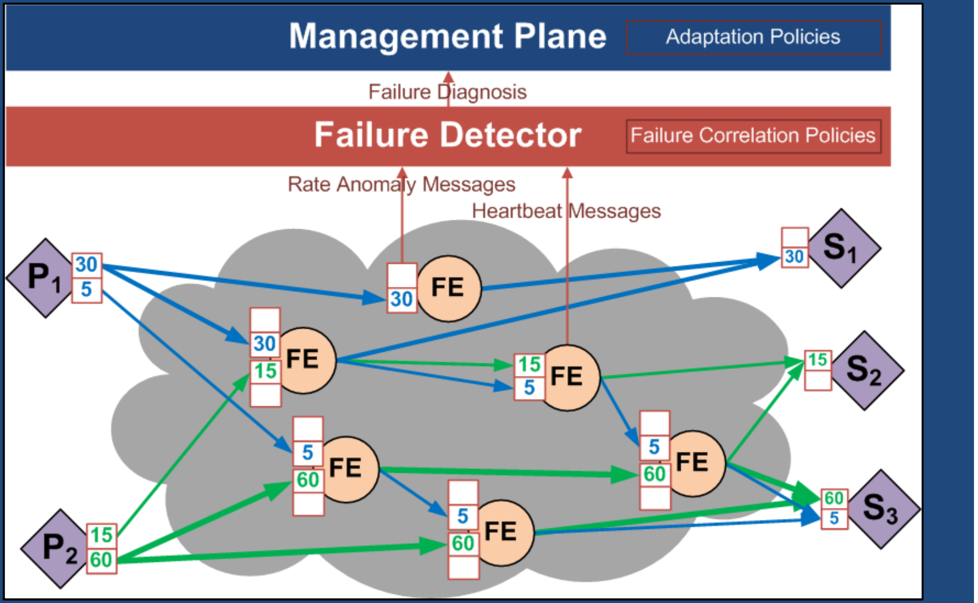
Nodes detected: 24

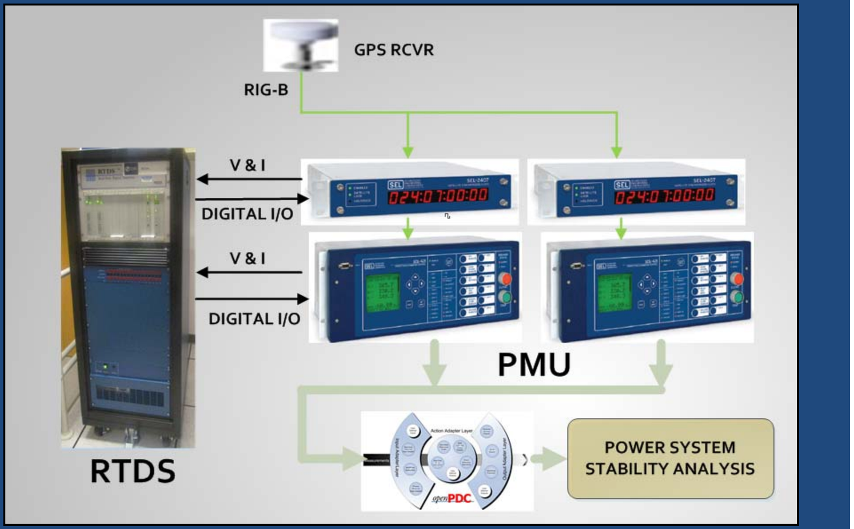
```
22:32:23  10.0.10.10-100015 > 10.0.10.2  : Policy violation
22:32:22  10.0.10.10-10004 > 10.0.10.2  : Policy violation
22:32:21  10.0.10.10-10007 > 10.0.10.2  : Policy violation
```

Connections processed

2012 Accomplishments: Wide-Area Measurement Infrastructures

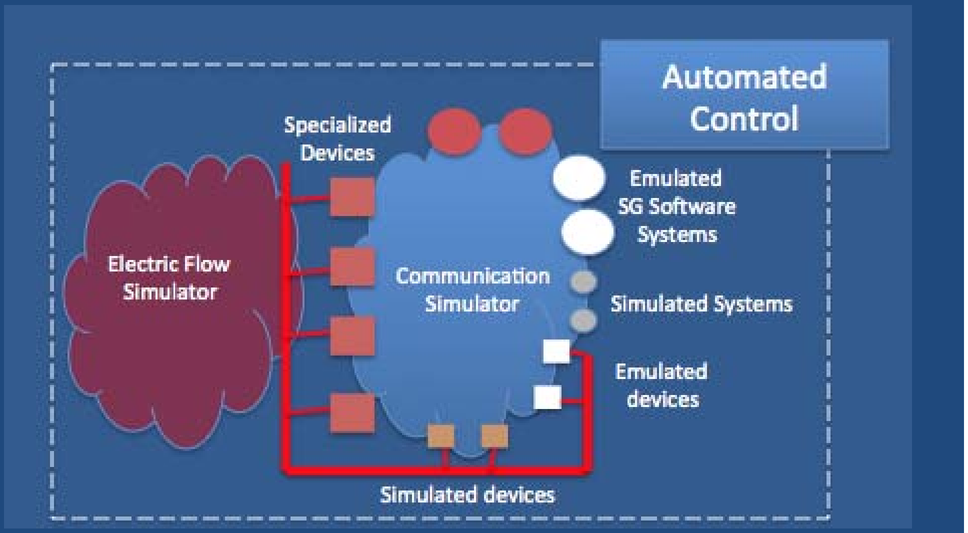
- GridStat Secure Middleware Communication Framework
  - Interaction with McAfee
  - GridStat Inc. spinoff
  - DEFT-DETER federation
- CONES: Converged Networks for SCADA
  - Transitioned to DOE-funded SIEGate (System Information Gateway) appliance with GPA
- Impacts of attacks against wide area measurement systems
  - GPS Spoofing
  - Malicious data injection into state estimation
  - Attack success assessment using graph centrality measures

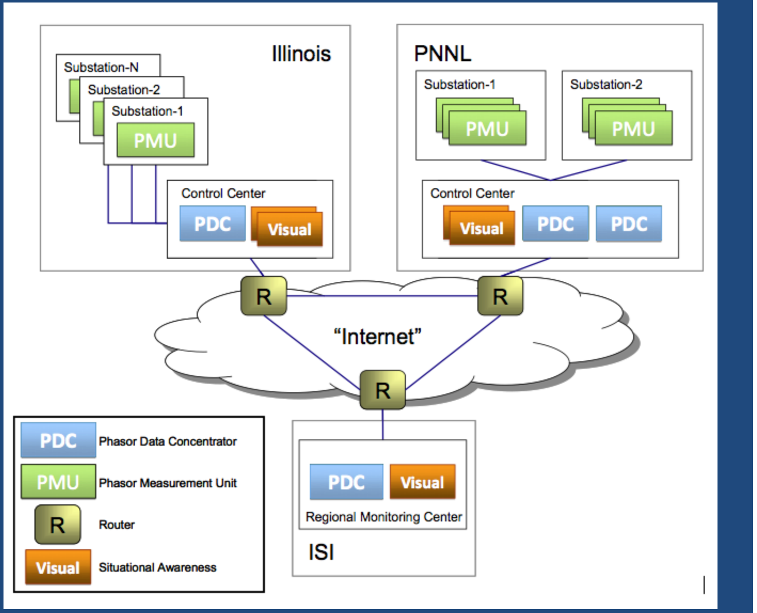




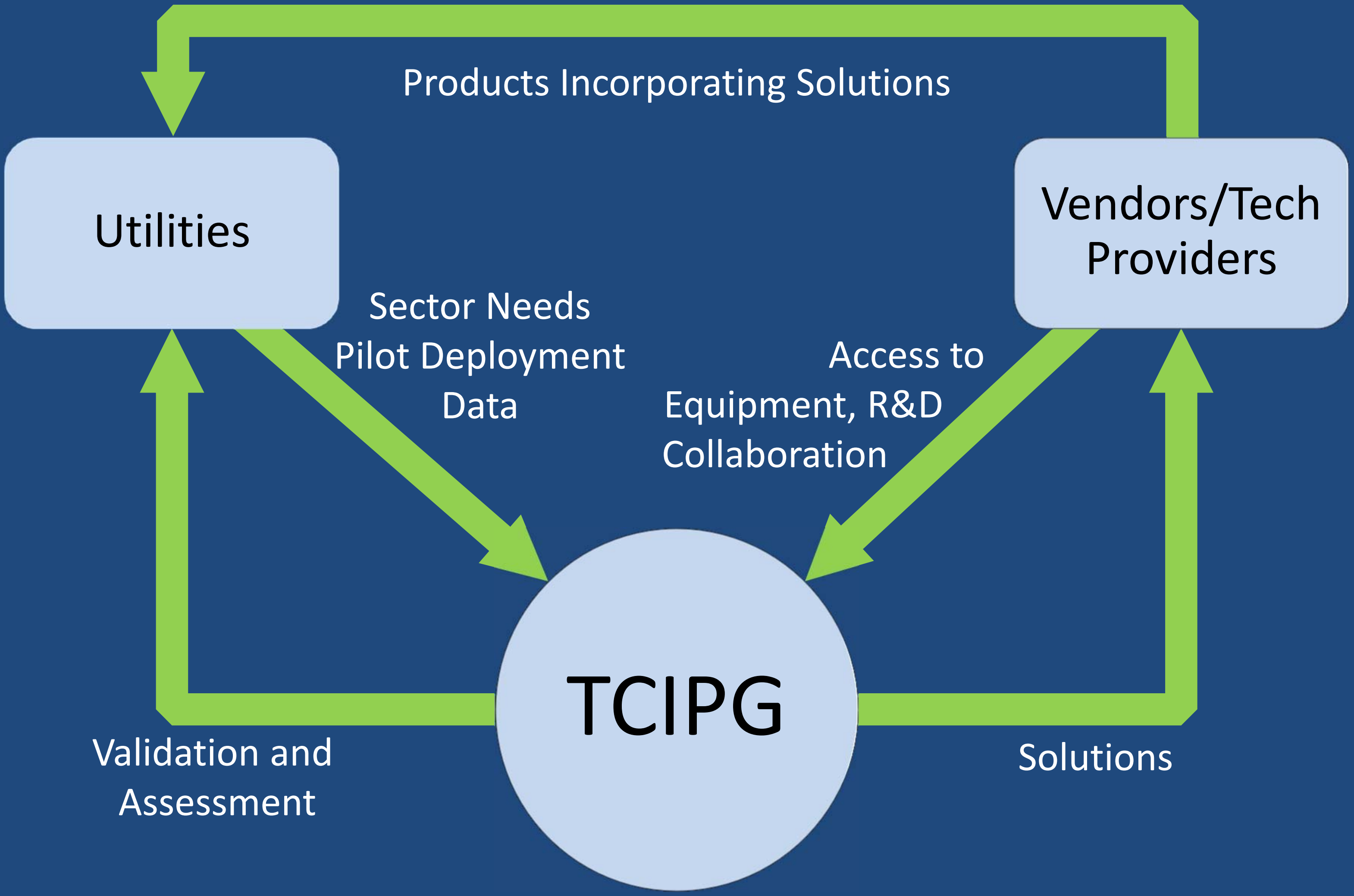
2012 Accomplishments: Testbed

- Implementation of the Itron AMI testbed
- New capabilities in experiment automation
- Expanded hardware-in-the-loop capability with RTDS
- Federation in the DEFT framework
- More detailed testbed presentation to follow

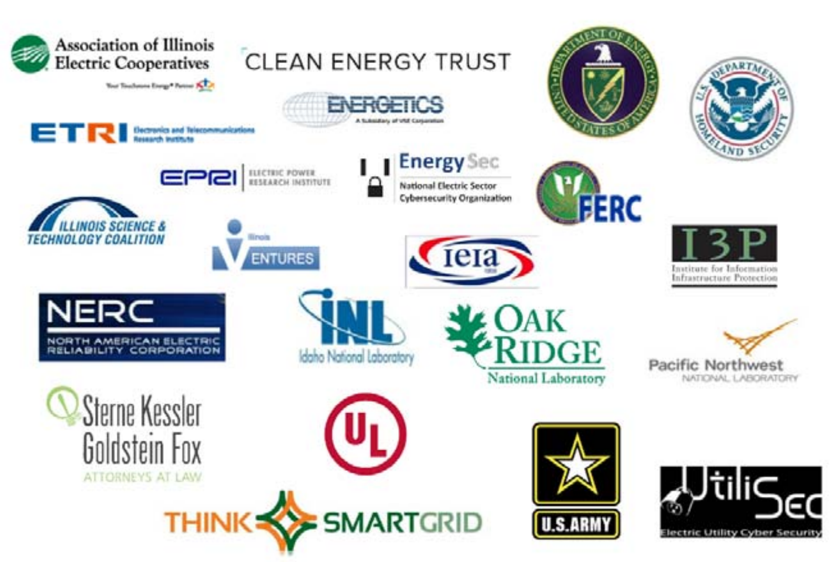


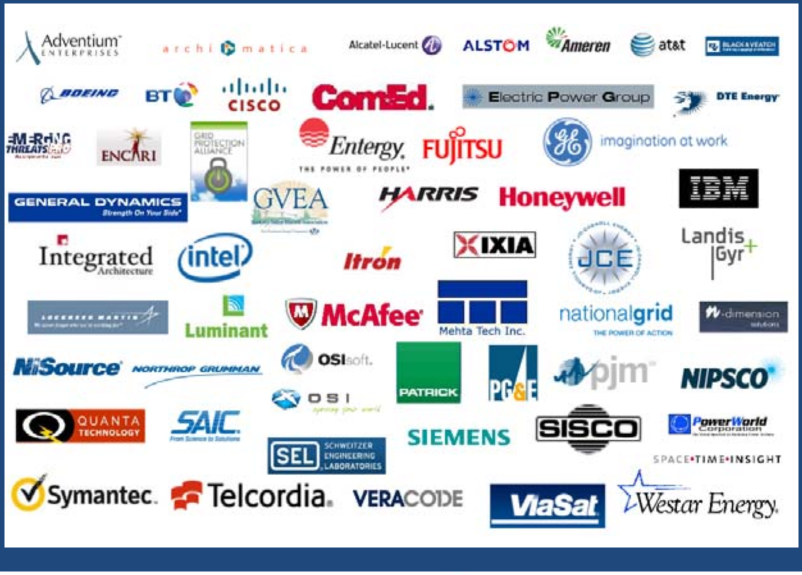


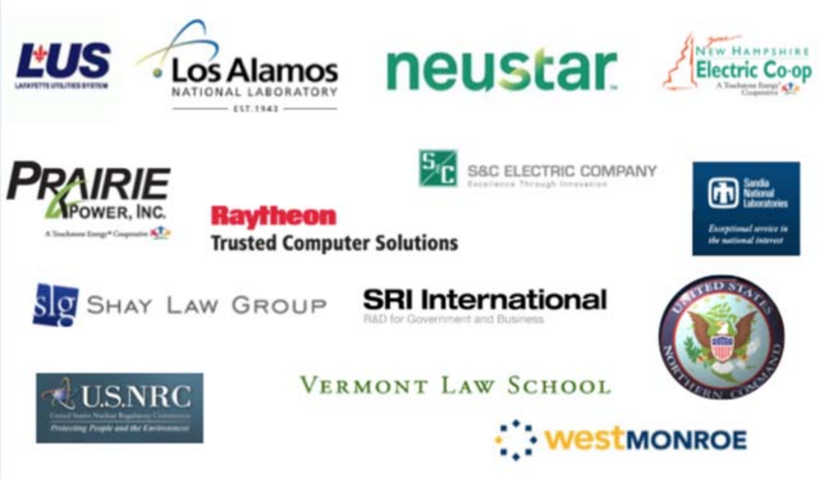
TCIPG as Catalyst for Accelerating Industry Innovation

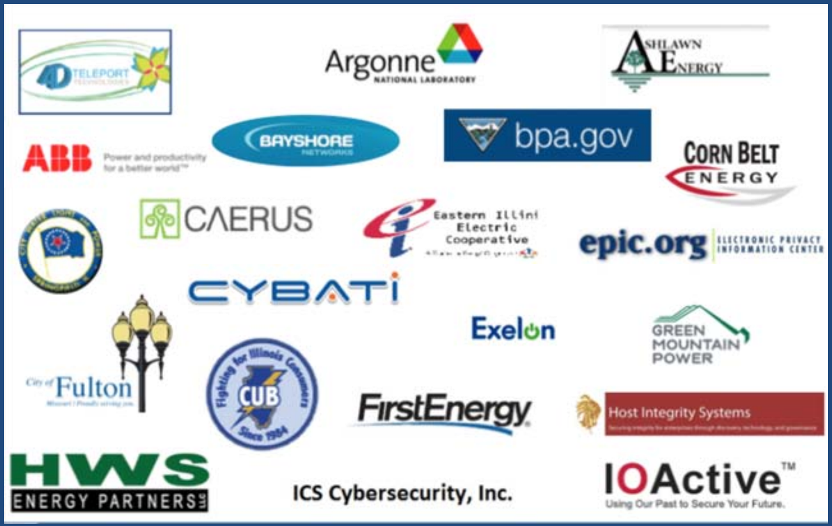


Industry Interaction: Vendors and Utilities that have participated in TCIPG Events


Association of Illinois Electric Cooperatives
CLEAN ENERGY TRUST
ENERGETICS
Department of Energy United States of America
U.S. Department of Homeland Security
ETRI Electronics and Telecommunications Research Institute
EPRI Electric Power Research Institute
EnergySec National Electric Sector Cybersecurity Organization
FERC
Illinois Science & Technology Coalition
Illinois Ventures
Ieia
I3P Institute for Information Infrastructure Protection
NERC North American Electric Reliability Corporation
INL Idaho National Laboratory
Oak Ridge National Laboratory
Pacific Northwest National Laboratory
Sterne Kessler Goldstein Fox Attorneys at Law
UL
U.S. Army
UtiliSec Electric Utility Cyber Security
THINK SMARTGRID

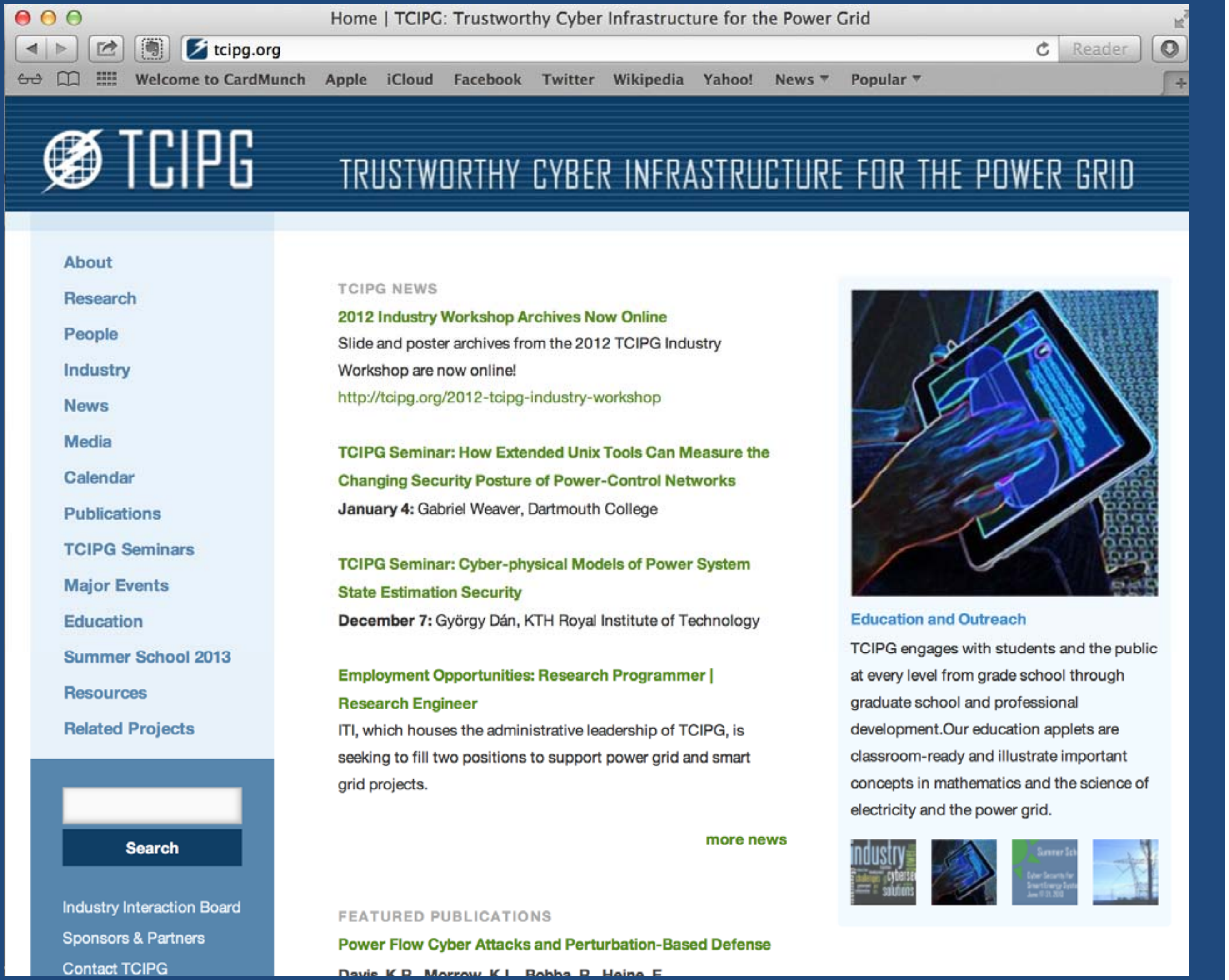



LUS Lafayette Utilities System
Los Alamos National Laboratory
neustar
New Hampshire Electric Co-op
Prairie Power, Inc.
S&C Electric Company
Raytheon Trusted Computer Solutions
Sandia National Laboratories
SLG Shay Law Group
SRI International
United States Northern Command
U.S.NRC
Vermont Law School
westMONROE



To Learn More

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our 2013 Summer School – June 17-21, 2013
- Attend Industry/Govt. Workshop Nov. 6-7, 2013



TCIPG NEWS

2012 Industry Workshop Archives Now Online
Slide and poster archives from the 2012 TCIPG Industry Workshop are now online!
http://tcipg.org/2012-tcipg-industry-workshop

TCIPG Seminar: How Extended Unix Tools Can Measure the Changing Security Posture of Power-Control Networks
January 4: Gabriel Weaver, Dartmouth College

TCIPG Seminar: Cyber-physical Models of Power System State Estimation Security
December 7: György Dán, KTH Royal Institute of Technology

Employment Opportunities: Research Programmer | Research Engineer
ITI, which houses the administrative leadership of TCIPG, is seeking to fill two positions to support power grid and smart grid projects.

more news

FEATURED PUBLICATIONS

Power Flow Cyber Attacks and Perturbation-Based Defense
Davis, K.R., Morrow, K.L., Bobba, R., Heine, E.

Education and Outreach
TCIPG engages with students and the public at every level from grade school through graduate school and professional development.Our education applets are classroom-ready and illustrate important concepts in mathematics and the science of electricity and the power grid.

SGIP

SMART GRID INTEROPERABILITY PANEL

The Next Generation

A Brief History

- Nov. 2009 – Formation of SGIP
- Jun. 2010 – Formation of SGFAC
- Dec. 2011 – SGFAC Report to NIST
- Dec. 2011 – NIST reports “curtailed funding” for SGIP in 2013
- Apr. 2012 – Draft of SGIP 2.0 Business Sustainment Plan
- May 2012 – Comments on Business Sustainment Plan from SGFAC
- Jul. 2012 – Business Sustainment Plan Finalized, SGIP 2.0 incorporated

Highlights of SGIP Business Sustainment Plan

- Support NIST responsibilities under EISA
- Coordination of interoperability standards development
- Identify the necessary testing and certification requirements
- Oversee the performance of these activities and maintain the momentum
- Educate industry stakeholders on interoperability
- Establish global interoperability alignment

Guiding Principles to Meet Our Mission

- Appropriate openness/digital and face-to-face engagement and collaboration
- Balance of interests/an equal seat at the table
- Aiming for consensus
- Harmonization and seamlessness of standards

SGIP Accomplishments

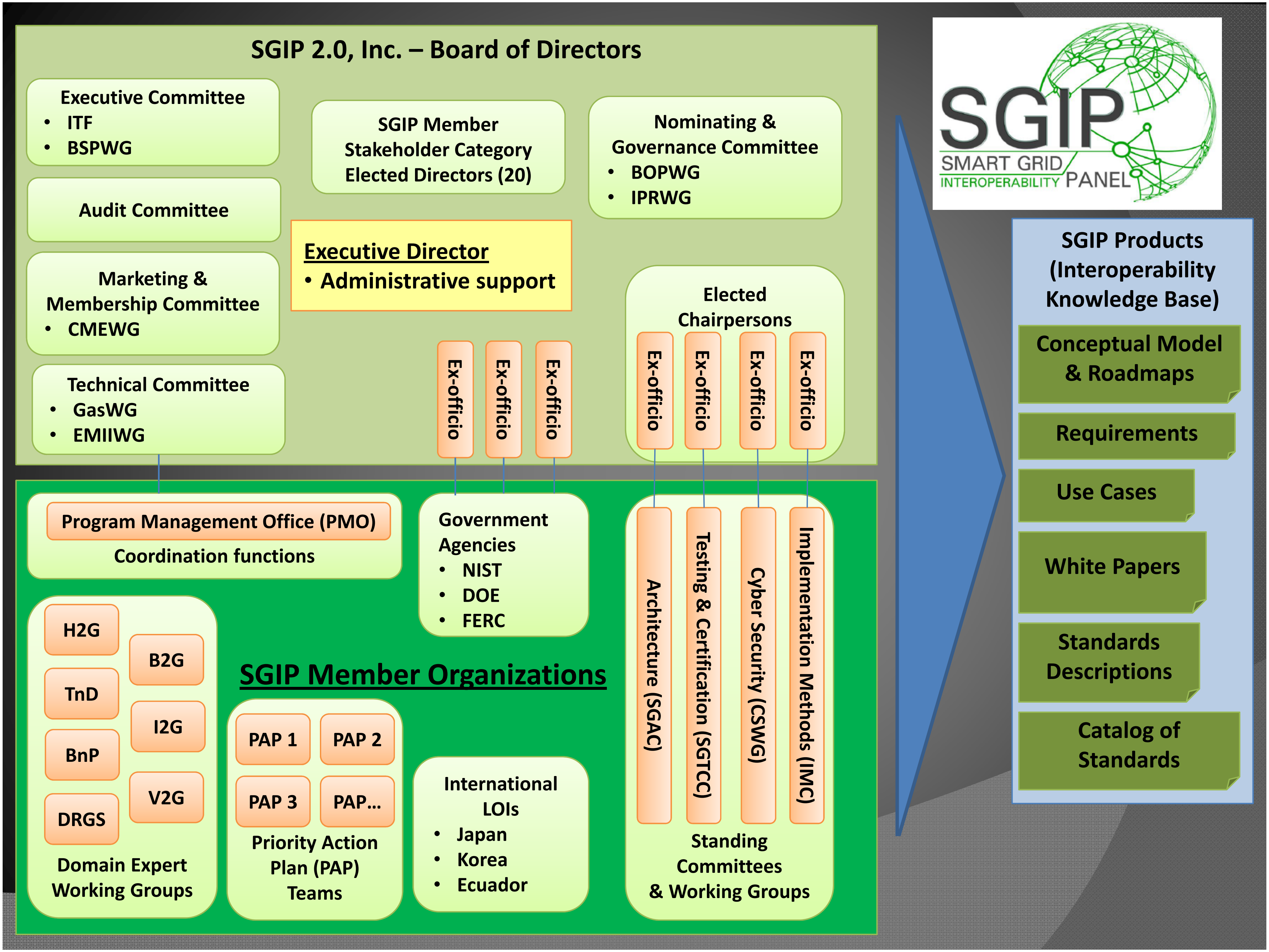
- Nearly 800 companies and organizations are members of SGIP
- Catalog of Standards
  - Hundreds of standards considered
  - 42 Included in the catalog
  - 14 currently being voted on
  - 82 in the review/evaluation queue
- International letters of intent have been signed with countries in Europe, Asia, and the Americas with many more to come

Organization and Structure

- Five Major Committees
  - Executive (XC) – Scott Ungerer
    - Manage the business of the Board
    - Business Operations, Budgeting, Staffing, Contractors, International Task Force
  - Technical (TC) – John Caskey
    - All technical activities
    - PAPs, DEWGs, Working Groups, PMO
  - Marketing & Membership (MMC) – George Bjelovuk
    - Membership & Recruiting
    - Face to Face Meetings, Sponsorship, CME Working Group

Organization and Structure

- Five Major Committees
  - Nominating & Governance (NGC) – David Forfia
    - Operating Procedures & Foundational Documents
    - Bylaws, IPR Policy, BoD Eligibility, Stakeholder Elections
  - Audit (AC) – Barry Haaser
    - Record-keeping
    - Procurement Policy, External Auditors
- Proposed Staffing
  - Executive Director
  - Supporting Staff



SGIP 2.0, Inc. – Board of Directors

Executive Committee
- ITF
- BSPWG

Audit Committee

Marketing & Membership Committee
- CMEWG

Technical Committee
- GasWG
- EMIIWG

SGIP Member Stakeholder Category Elected Directors (20)

Executive Director
- Administrative support

Nominating & Governance Committee
- BOPWG
- IPRWG

Elected Chairpersons

Ex-officio

Ex-officio

Ex-officio

Ex-officio

Ex-officio

Ex-officio

Ex-officio

Program Management Office (PMO)

Coordination functions

Government Agencies
- NIST
- DOE
- FERC

SGIP Member Organizations

H2G

B2G

TnD

I2G

BnP

V2G

DRGS

Domain Expert Working Groups

PAP 1

PAP 2

PAP 3

PAP…

Priority Action Plan (PAP) Teams

International LOIs
- Japan
- Korea
- Ecuador

Architecture (SGAC)

Testing & Certification (SGTCC)

Cyber Security (CSWG)

Implementation Methods (IMC)

Standing Committees & Working Groups

SGIP SMART GRID INTEROPERABILITY PANEL

SGIP Products (Interoperability Knowledge Base)

Conceptual Model & Roadmaps

Requirements

Use Cases

White Papers

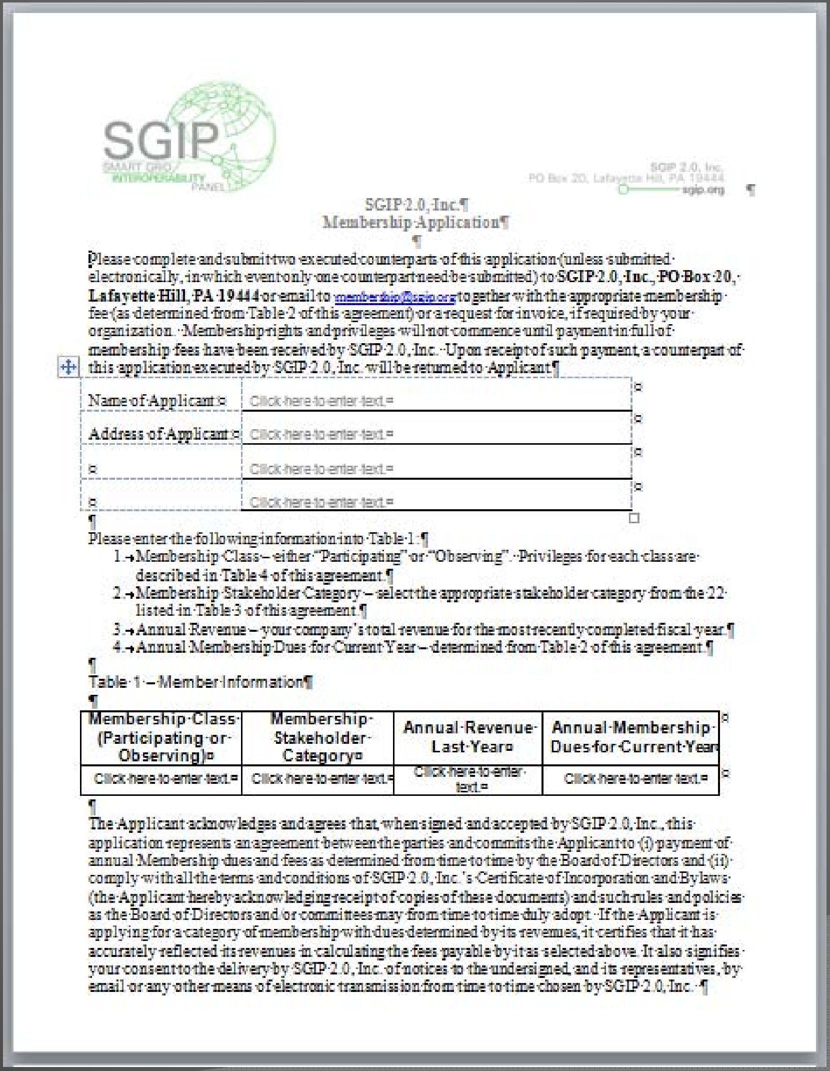
Standards Descriptions

Catalog of Standards

Membership Application

Downloadable at:

www.SGIP.org



SGIP
SMART GRID
INTEROPERABILITY
PANEL

SGIP 2.0, Inc.
PO Box 20, Lafayette Hill, PA 19444
sgip.org

SGIP 2.0, Inc.
Membership Application

Please complete and submit two executed counterparts of this application (unless submitted electronically, in which event only one counterpart need be submitted) to **SGIP 2.0, Inc., PO Box 20, Lafayette Hill, PA 19444** or email to membership@sgip.org together with the appropriate membership fee (as determined from Table 2 of this agreement) or a request for invoice, if required by your organization. Membership rights and privileges will not commence until payment in full of membership fees have been received by SGIP 2.0, Inc. Upon receipt of such payment, a counterpart of this application executed by SGIP 2.0, Inc. will be returned to Applicant.

Name of Applicant	Click here to enter text.
Address of Applicant	Click here to enter text.
	Click here to enter text.
	Click here to enter text.

Please enter the following information into Table 1:

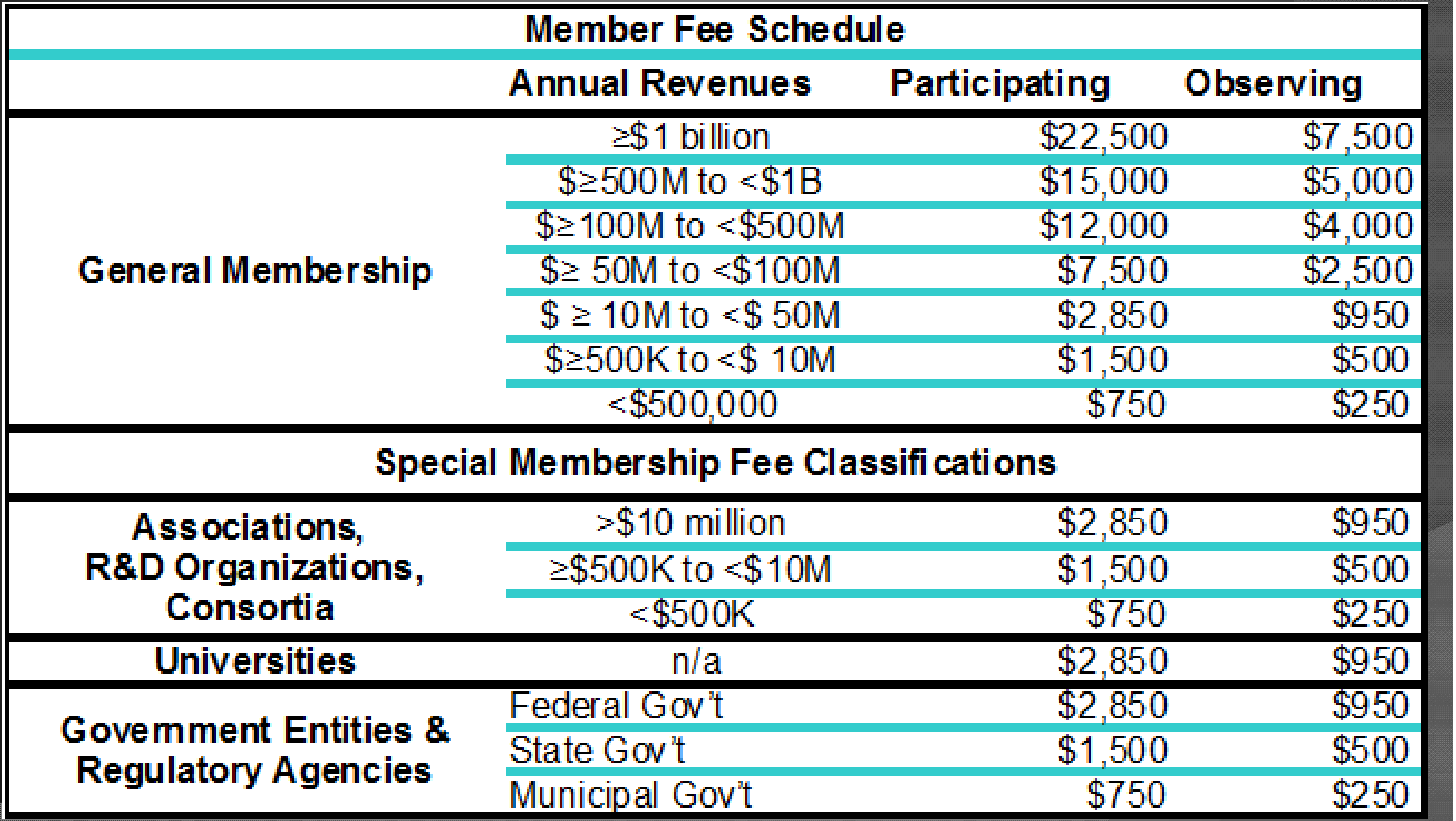
1. Membership Class – either "Participating" or "Observing". Privileges for each class are described in Table 4 of this agreement.
2. Membership Stakeholder Category – select the appropriate stakeholder category from the 22 listed in Table 3 of this agreement.
3. Annual Revenue – your company's total revenue for the most recently completed fiscal year.
4. Annual Membership Dues for Current Year – determined from Table 2 of this agreement.

Table 1 – Member Information

Membership Class (Participating or Observing)	Membership Stakeholder Category	Annual Revenue Last Year	Annual Membership Dues for Current Year
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

The Applicant acknowledges and agrees that, when signed and accepted by SGIP 2.0, Inc., this application represents an agreement between the parties and commits the Applicant to (i) payment of annual Membership dues and fees as determined from time to time by the Board of Directors and (ii) comply with all the terms and conditions of SGIP 2.0, Inc.'s Certificate of Incorporation and Bylaws (the Applicant hereby acknowledging receipt of copies of these documents) and such rules and policies as the Board of Directors and/or committees may from time to time duly adopt. If the Applicant is applying for a category of membership with dues determined by its revenues, it certifies that it has accurately reflected its revenues in calculating the fees payable by it as selected above. It also signifies your consent to the delivery by SGIP 2.0, Inc. of notices to the undersigned, and its representatives, by email or any other means of electronic transmission from time to time chosen by SGIP 2.0, Inc.

Membership Dues



Member Fee Schedule			
	Annual Revenues	Participating	Observing
General Membership	≥$1 billion	$22,500	$7,500
	$≥500M to <$1B	$15,000	$5,000
	$≥100M to <$500M	$12,000	$4,000
	$≥ 50M to <$100M	$7,500	$2,500
	$ ≥ 10M to <$ 50M	$2,850	$950
	$≥500K to <$ 10M	$1,500	$500
	<$500,000	$750	$250
Special Membership Fee Classifications			
Associations, R&D Organizations, Consortia	>$10 million	$2,850	$950
	≥$500K to <$10M	$1,500	$500
	<$500K	$750	$250
Universities	n/a	$2,850	$950
Government Entities & Regulatory Agencies	Federal Gov't	$2,850	$950
	State Gov't	$1,500	$500
	Municipal Gov't	$750	$250

Current Membership Stats

- 47 Member companies signed up and invoiced
  - 15 companies @ $22,500/year
  - $396,750 in dues commitment
  - ~$80,000 received
  - 4 applications in process
- Membership campaign in full swing
  - Ambassador Presentations
  - Additional digital meetings planned for 1Q 2013

Association of Home Appliance Manufacturers (AHAM)

Eaton Corporation

Grid2Home, Inc.

Home, Building & Utility Sytems

Kottage Industries LLC

Wedin Communications

Ameren Services

American Electric Power

Arizona Public Service Company

CenterPoint Energy Houston Electric

DTE Energy

FirstEnergy Service Company

Florida Power & Light Company

Hydro-Quebec

Portland General Electric Company

PPL Corporation

Southern California Edison

Southern Company Services, Inc.

Sacramento Municipal Utility District

National Rural Electric Cooperative Association (NRECA)

Buford Goff & Associates, Inc.

Clevest Solutions, Inc.

Systems Integration Specialists Company, Inc.

Tendril

Schneider Electric

Toshiba - Landis + Gyr

ZIV USA INC.

American Council of Independent Laboratories

Edison Electric Institute (EEI)

HomeGrid Forum

Japan Smart Community Alliance

Lakeview Consulting Group

Utilities Telecom Council, Inc. (UTC)

Electric Power Research Institute (EPRI)

Battelle Pacific Northwest Lab

National Institute of Standards and Technology (NIST)

SunSpec Alliance

Climate Talk Alliance

WiMAX Forum

Zigbee Alliance, Inc.

National Electrical Manufacturers Association (NEMA)

California Public Utilities Commission

New York State Department of Public Service

American Association for Laboratory Accreditation (A2LA)

Bonneville Power Administration

ISO New England

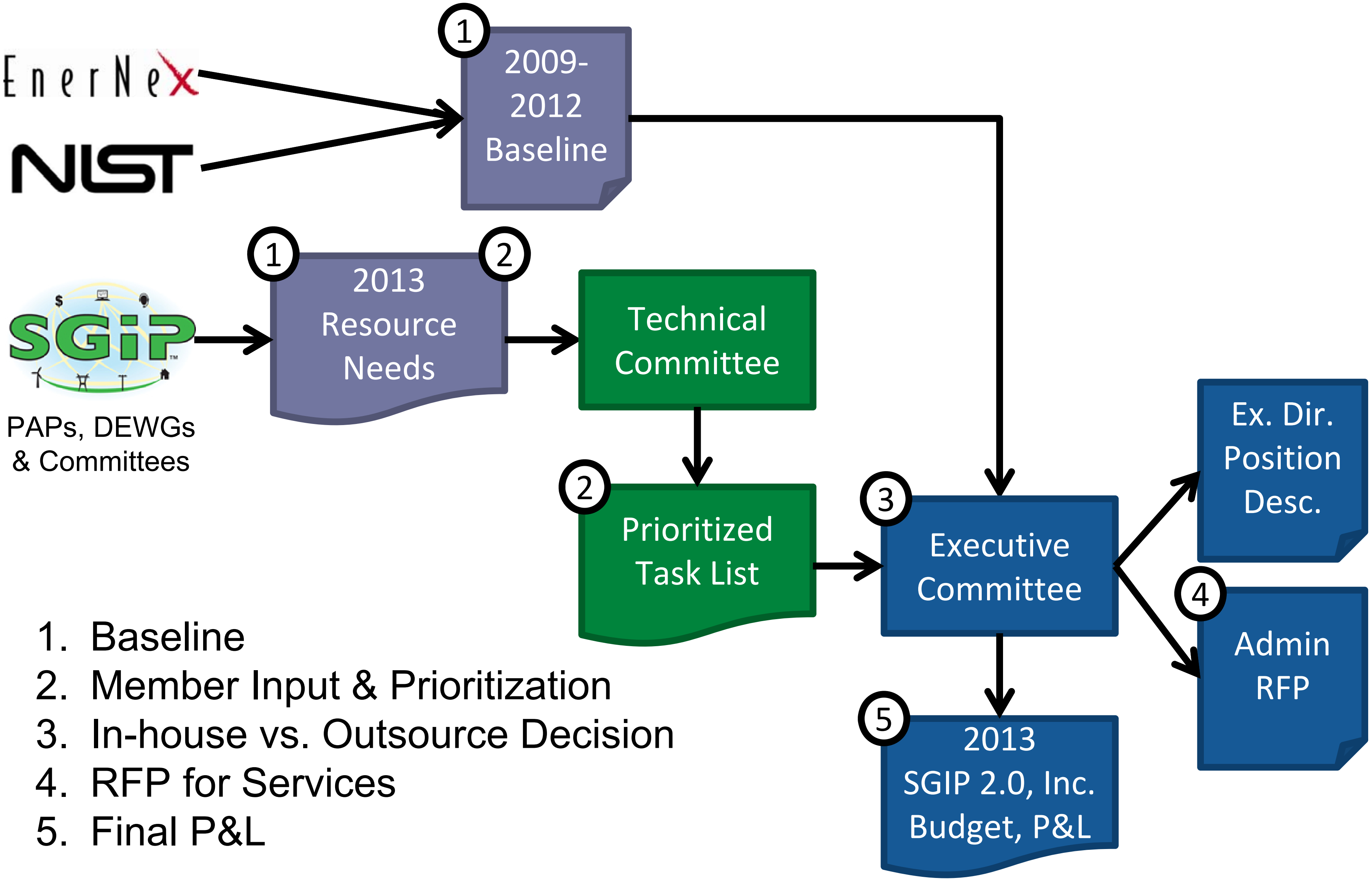
New York Independent System Operator, Inc.

PJM Interconnection

Transition Plan

- Ensure everything in SGIP is accounted for
- Track the major muscle movements
  - Foundational Documents (Bylaws, IPR, etc.)
  - Membership Campaign
  - Technical Working Priorities
  - Procurement Policy
  - Stakeholder BoD Elections
  - Budget and P&L
- Establish Basic business functionality
  - Staffing (Internal vs. Outsource)
  - IT/Website
  - Accounting
  - Membership Database
- Update External Relationships
  - NIST
  - International

SGIP 2.0 Budgeting Process

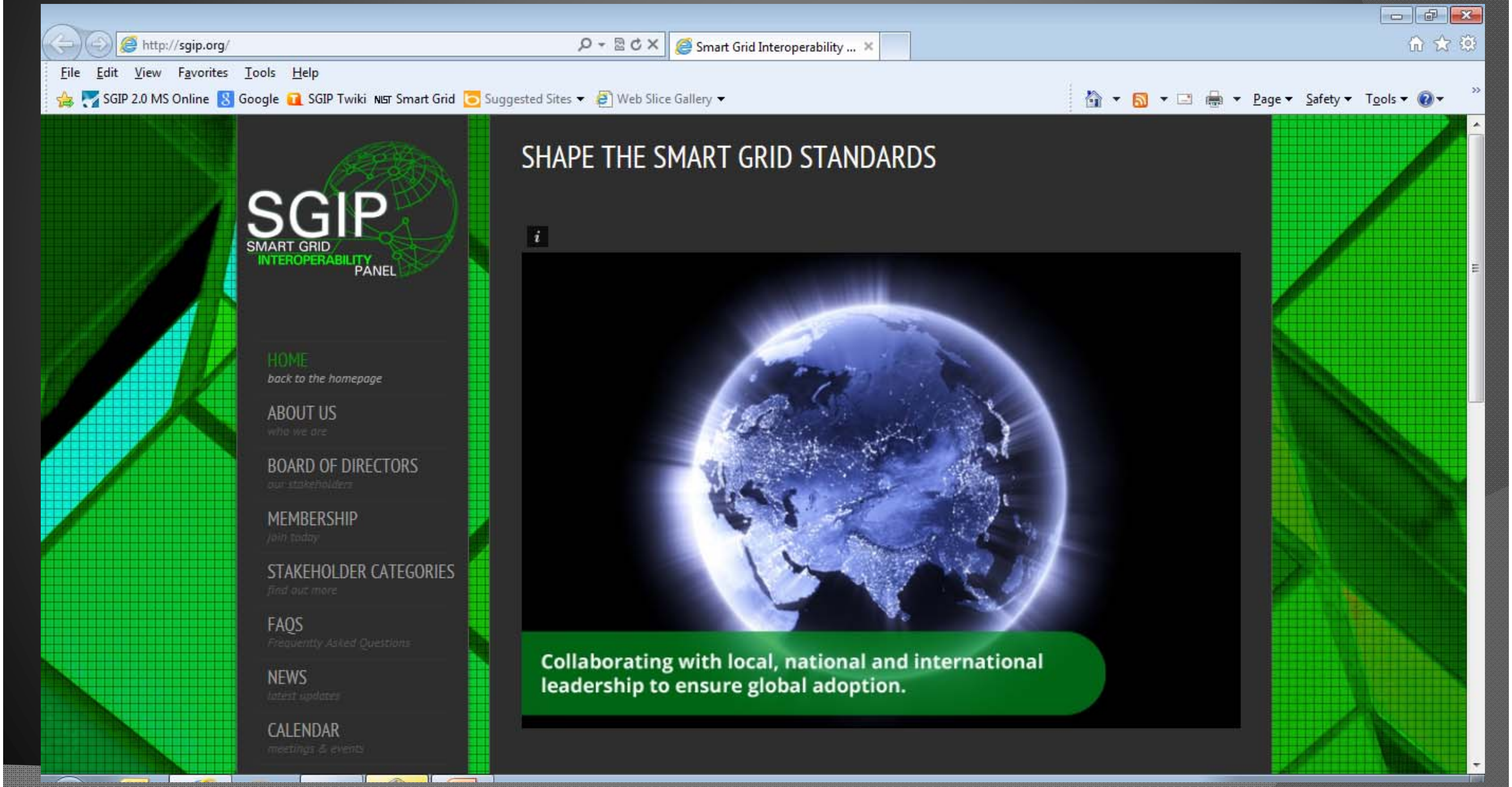


1. Baseline
2. Member Input & Prioritization
3. In-house vs. Outsource Decision
4. RFP for Services
5. Final P&L

Membership Campaign

- Bylaws and IPR Policy finalized on 10/10/12
- Membership packets sent on 10/12/12
  - Electronic copies to all 1,900 SGIP members
  - Hard copies mailed to member company “primary contacts”
  - 15 additional requests for packets received in first 24 hours
  - Minor tweaks being make to SGIP home page
  - Issues being worked in Nominating & Governance, and Membership & Marketing committees
    - Non-profit vs. not-for-profit
    - Member company acquisitions
- Stakeholder Ambassador Presentations

www.SGIP.org



SHAPE THE SMART GRID STANDARDS

Collaborating with local, national and international leadership to ensure global adoption.

SGIP

SMART GRID INTEROPERABILITY PANEL

The Next Generation

Questions?

NIST Actions Responding to Smart Grid Federal Advisory Committee Report Recommendations

George W. Arnold, Eng.Sc.D.

Director, Smart Grid and Cyber-Physical Systems Program Office, and

National Coordinator for Smart Grid Interoperability

Engineering Laboratory

December 18, 2012

National Institute of Standards and Technology
U.S. Department of Commerce

General Recommendations

FAC Recommendations	Actions
Prioritize, streamline, and leverage NIST Smart Grid activities • Need to prioritize and consolidate activities so that stakeholders can focus their participation	• NIST has developed and documented a multi-year SG Program Plan focused on five key program thrusts • SGIP 2.0 activities will be more focused and streamlined to align with funding
Need for consistent state regulatory support for Smart Grid standards development • Need to prioritize and consolidate activities so that stakeholders can focus their participation	• Strengthened NIST engagement with NARUC and state PUCs • Planned cooperative agreement to support state regulator engagement • Working with NARUC to identify commissioner for SGIP Board seat • PUC staffs engaged in SGIP working groups (Business and Policy DEWG, Cyber Security Working Group, and Implementation Methods Committee)

General Recommendations

FAC Recommendations	Actions
Need to continue the focus on transparency, roles, and responsibilities • Communicate clearer messages on SGIP process, the roles of federal and state agencies, and effects of standards on businesses and consumers	• Significant SGIP process improvements implemented • NIST / SGIP 2.0 MoU signed; defines roles and responsibilities • SGIP 2.0 marketing and membership committee has developed stakeholder group-specific business value propositions • New SGIP 2.0 Board Executive Committee driving more strategic member involvement
Consolidation of cybersecurity activities and research • Multiple organizations are working on cybersecurity activities and research and that is a challenge for industry to effectively participate and contribute	NIST-led SGIP Cybersecurity Working Group has strong collaborations with public and private sector partners: • The Cybersecurity Working Group (CSWG) has been reaching out and collaborating with Federal and State agencies, cybersecurity organizations, and SDOs through joint activities – DoE's Electricity Subsector Cybersecurity Capability Maturity Model – DoE's Risk Management Process (RMP) document – NESCOR – SEP 1.X Cybersecurity Mitigation Strategy whitepaper • Stakeholder outreach to regulators, others • Privacy - Third party data usage recommendations and "train the trainer" slides • SGIP Catalog of Standards – reviews/feedback on cybersecurity of standards NIST also participates in the DOE created NESCO/NESCOR activities to ensure coordination

General Recommendations Cont’d

FAC Recommendations	Actions
Urgent need for a communication plan and an education and outreach effort regarding importance of interoperability standards and research activities	• NIST sponsorship and strong presence in major technical industry conferences (GridWeek, Grid Interop, IEEE Innovative Smart Grid Technologies conference) • Regulatory outreach/education • Half-day class at Institute for Public Utilities “Grid School” • NIST led APEC Smart Grid Regulatory workshop • NIST engagement in Smart Grid Consumer Collaborative

Short- to Mid-term Challenges and Recommendations

FAC Recommendations	Actions
Reliability and implementation review of interoperability standards is critical • Propose a new Committee within the SGIP to focus on reliability considerations, implementation readiness, cyber impacts, stranded costs, and impacts on legacy systems	• NIST drove formation of new SGIP Implementation Methods Committee.
Prioritization of the standards, processes, and forums are necessary for greater utility and state participation • Enable effective participation by utility and state regulators given their limited resources	• SGIP 2.0 Technical Committee has been established and is prioritizing SGIP's work program for 2013

Short- to Mid-term Challenges and Recommendations - Continued

FAC Recommendations	Actions
Urgent need for a communication plan and an education and outreach effort for greater utility and state participation • Educate utility and state regulators the impact of standards and the risk of non-engagement and non-compliance to encourage their involvement	• See responses under "General Recommendations", above • SGIP 2.0 has developed business value propositions for each stakeholder category and is conducting outreach • EEI, NRECA and APPA provide strong support and outreach to utilities • Regular NIST conference calls with PUC staffs • NIST meetings with NARUC leadership • NIST-led ½ day class at "Grid School"
Need for regulatory certainty to ensure cost recovery of investments related to Smart Grid deployment	Aided by participation of PUC staffs in SGIP Business and Policy Domain Expert Working Group and the Implementation Methods Committee

Recommendations on Long-Term Evolution of the US Smart Grid Effort

FAC Recommendations	Actions
NIST will need to organize for its changing role by 2015 and beyond • Augment technological expertise • Greater support for state and federal regulators • Provide advice on cybersecurity issues	• Integration of NIST SG program into Engineering Lab • Development of multi-year SG Program Plan • Reallocation of extramural funding to intramural program and staff development • Strengthening NIST smart grid research focus • Planned cooperative research agreement on smart grid system modeling with leading university
Over the next five years, there will also be a need for interagency collaboration • Continue to collaborate with other federal agencies to support the EISA responsibilities • Collaborate with DHS on federal response to national cyber emergencies	• NIST will continue to collaborate with major Federal Agencies through the Federal Smart Grid Task Force • NIST co chairs the National Science and Technology Council Smart Grid Subcommittee • NIST provides guidance on topics such as continuation of operations and other recovery cyber-related guidelines. However, actual cyber emergencies are typically handled by either the US-CERT or the ICS-CERT.
NIST will need to reach out to industry to seek further input • Interact with industry in order to address the needs of the Smart Grid and take into account existing technologies in the standards process	• Continued SGIP involvement • Boulder workshop • NIST SG Federal Advisory Committee • Discussions with numerous individual stakeholders

Recommendation on NIST Smart Grid Research Activities

FAC Recommendations	Actions
Key Research Activities • Focus on interoperability, cybersecurity, testing and certification, metrics for interoperability, vulnerability, resilience, and other properties of complex systems • Smart Grid metrics to aid decision-making	Developed NIST Multi-year Program Plan addressing five thrusts • Systems-level cross-cutting Measurement Science for Smart Grid System Performance research • Measurement Science for Transmission and Distribution Grid Operations; • Measurement Science for Distributed Energy Resources and Microgrids, • Measurement Science for User-to-Grid Interoperation; • Smart Grid National Coordination function
Facilitator of Multi-Stakeholder Smart Grid Research Collaboration • Leverage the multi-stakeholder makeup of the SGIP to convene workshops on Smart Grid research that supports interoperability and other Smart Grid standards	NIST / RASEI Boulder workshop (August 2012) identified key research areas and gaps. Technical report due by December and High Level Opportunities document by 1Q '13.
Accreditation of Testing and Certification Laboratories • Develop processes and procedures to provide accreditation to independent laboratories • Look at lessons learned from other industries and how to adapt them to the Smart Grid	• SGIP workshop held with major test lab and certification Accreditation bodies • IPRM v2 completed • SGIP Testing and Certification processes include lessons learned form Health Care and Telecom

Recommendations on Long-Term Evolution of the US Smart Grid Effort

FAC Recommendations	Actions
Collaboration with Utilities and Private Sector • Collaborate on research into metrics for interoperability, cybersecurity, and other properties of the Smart Grid	• Technical and Opportunities report from the Boulder workshop will provide input for this activity
Continue Research in Electric Power Metrology • Metrology requirements for Smart Grid devices • Build on current electric power metrology for the Smart Grid • Measurements for new sensors and actuators • Identify new kinds of quantities to characterize Smart Grid system level behavior	Reallocated NIST SG funding to intramural research, including development of a Smart Grid Test Bed: • Will consist of 10 lab modules • First two sections will support Power Conditioning/Synchrophasor and cyber security research
Smart Grid Modeling • Create a framework for modeling the Smart Grid at the system level	NIST is pursuing collaboration with academia/national labs to assist in structuring and developing this project

NIST Smart Grid Program Thrusts

- Measurement Science for Smart Grid System Performance
  - Cybersecurity for Smart Grid Systems
  - Smart Grid Communication Networks
  - The Electromagnetic Compatibility of Smart Grid Devices and Systems
  - Smart Grid Testing and Certification
  - Smart Grid System Testbed Facility
- Measurement Science for Transmission and Distribution Grid Operations
  - Wide-area Monitoring and Control of Smart Grid
  - Advanced Metering in Smart Distribution Grids
- Measurement Science for Distributed Energy Resources and Microgrids
  - Power Conditioning Systems for Renewables and Storage
- Measurement Science for User-to-Grid Interoperation
  - Industrial Integration with Smart Grid
  - Building Integration with Smart Grid
- Smart Grid National Coordination
  - EISA Role