Challenges and Progress Toward a Resilient Electric Grid

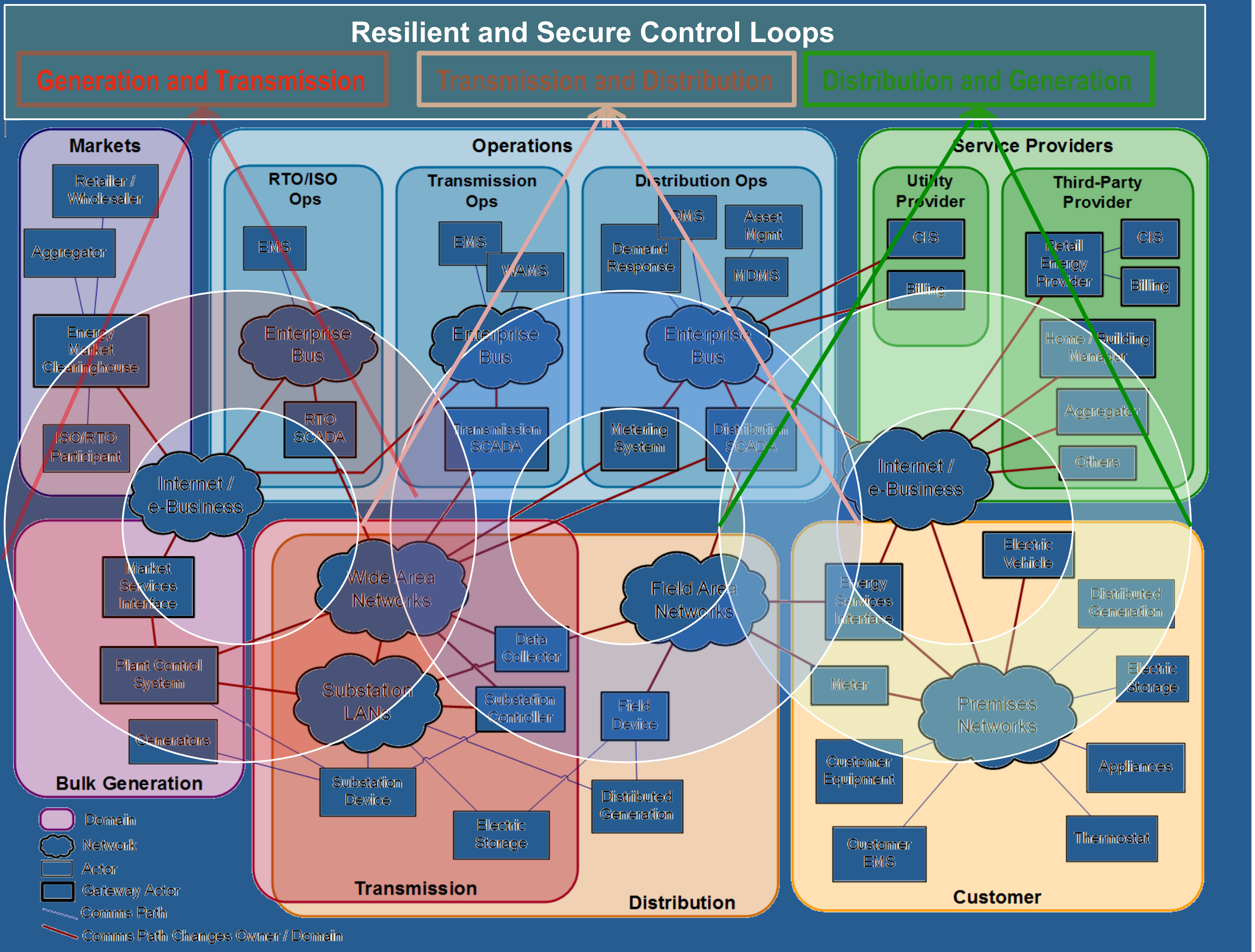
Bill Sanders

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

IFIP Working Group Meeting
January 21, 2013

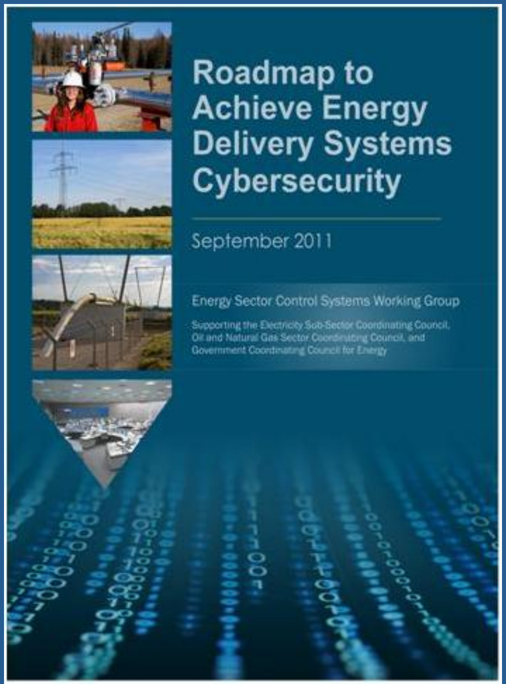
Infrastructure must provide control at multiple levels

- ✧**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.

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

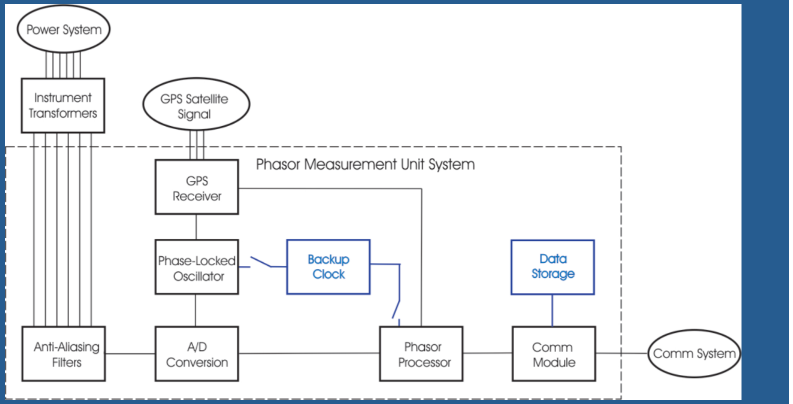
- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in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

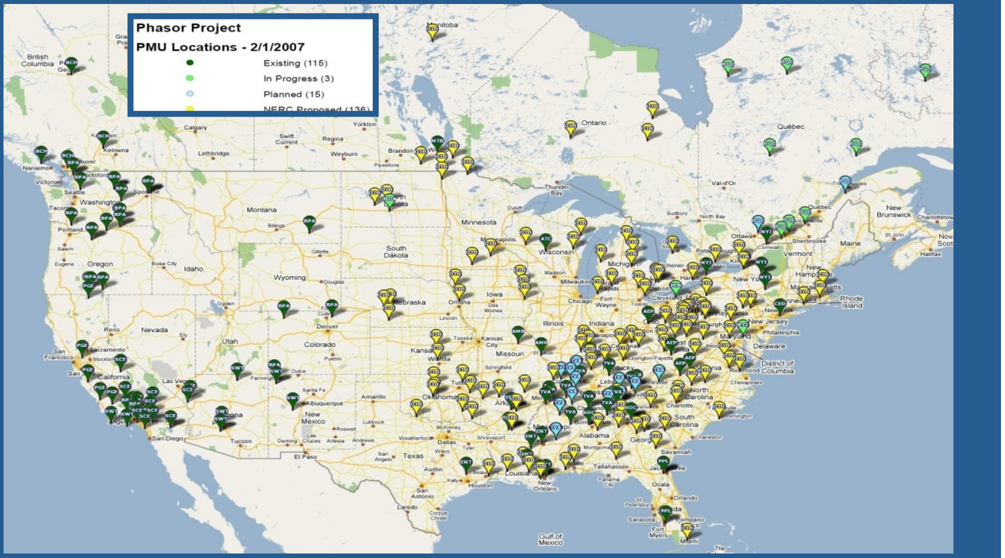
- Smart Grid vision for the wide area (primarily transmission) is:
  - Vastly more sensing at high, synchronous rates (example: PMUs)
  - New applications that use these data to improve
    - Reliability
    - Efficiency
    - Ability to integrate renewables

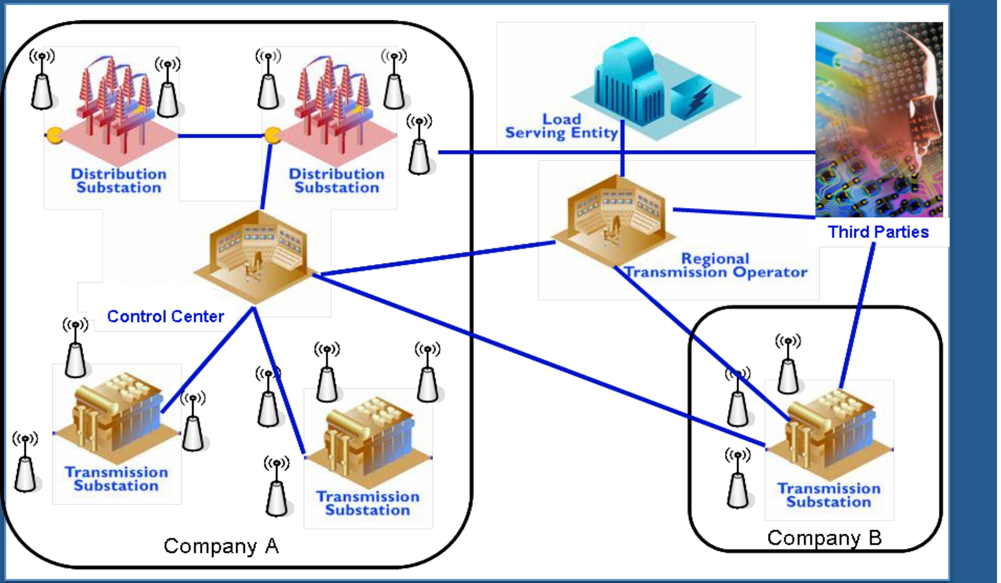


- Achieving the vision requires secure and reliable communications between sensors, control devices, and monitoring and control applications all owned and operated by the many entities that make up the grid

Power Grid of Tomorrow: North American SynchroPhasor Initiative

- Initiative, funded by DOE and industry, to investigate putting Phasor Measurement Units (PMUs) throughout physical power infrastructure
- Need significant changes in power cyber infrastructure to support PMUs.
- "Class A" service requires low latency, data integrity & availability ("no gaps")





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 & Research Focus

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

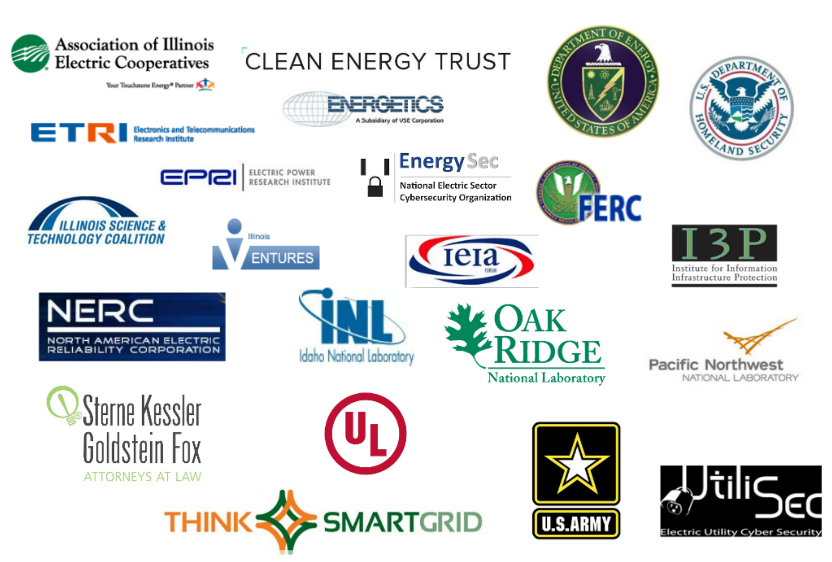
Research focus: Resilient and Secure Smart Grid Systems

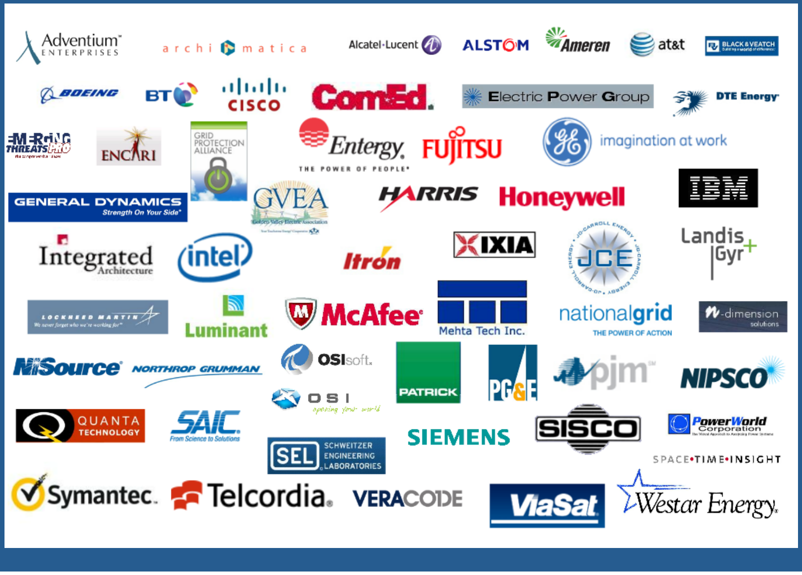
- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications
- Quantifying security and resilience

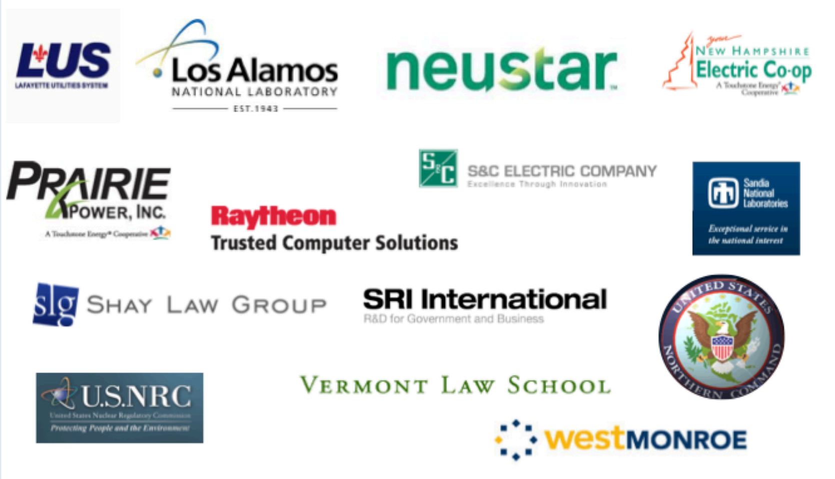
TCIPG Statistics

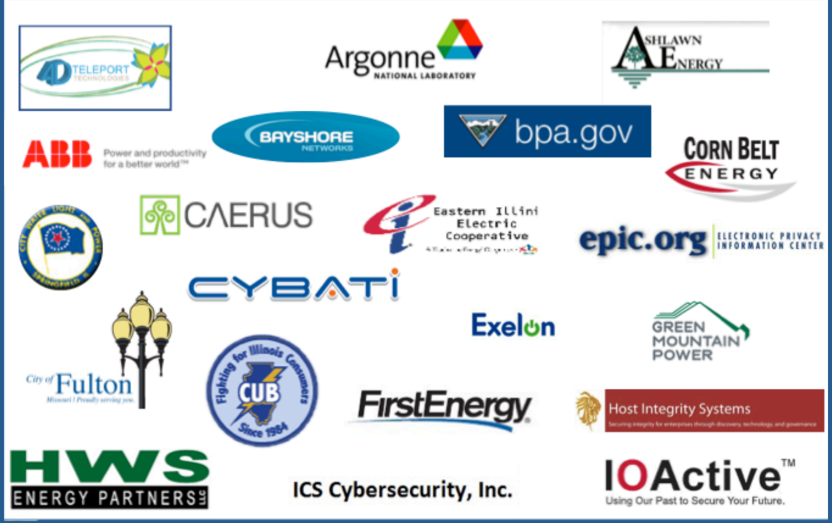
- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009 (including 20% cost share from partner schools)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 20 Faculty, 20 Senior Technical Staff, 37 Graduate Students, 5 Undergraduate Students, and 1 Admin

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

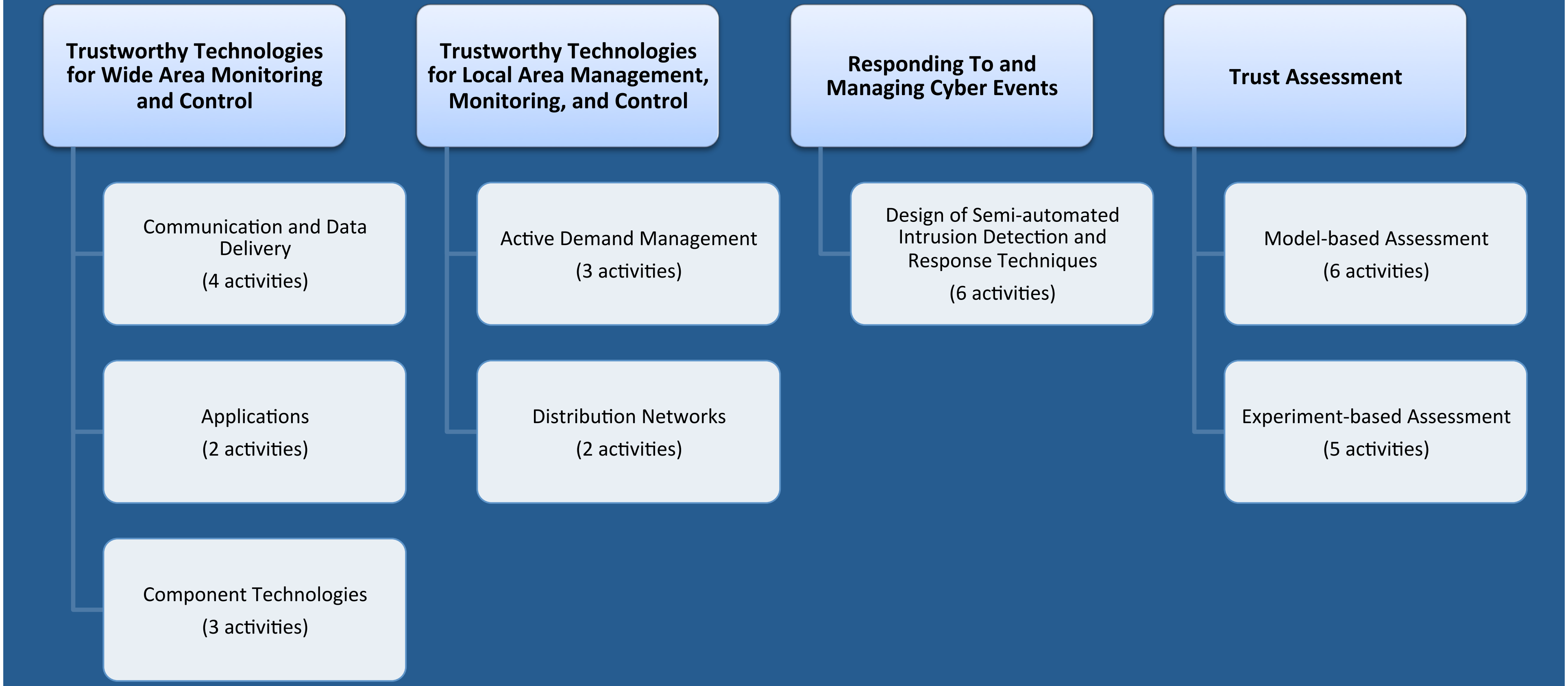

Association of Illinois Electric Cooperatives
Your Touchstone Energy Partner
CLEAN ENERGY TRUST
ENERGETICS
A Subsidiary of VSE Corporation
Department of Energy United States of America
U.S. Department of Homeland Security
ETRI Electronics and Telecommunications Research Institute
EPRI Electric Power 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
Think SmartGrid
UtiliSec
Electric Utility Cyber Security




LUS
Lafayette Utilities System
Los Alamos National Laboratory
Est. 1943
neustar
New Hampshire Electric Co-op
A Touchstone Energy Cooperative
Prairie Power, Inc.
A Touchstone Energy Cooperative
Raytheon
Trusted Computer Solutions
S&C Electric Company
Excellence Through Innovation
Sandia National Laboratories
Exceptional service in the national interest
slg Shay Law Group
SRI International
R&D for Government and Business
United States Northern Command
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment
Vermont Law School
westMonroe


4D Teleport Technologies
Argonne National Laboratory
Ashlawn Energy
ABB
Power and productivity for a better world
Bayshore Networks
bpa.gov
Corn Belt Energy
City Water Light and Power Springfield
Caerus
Eastern Illini Electric Cooperative
epic.org
Electronic Privacy Information Center
Cybati
Exelon
Green Mountain Power
City of Fulton
Missouri | Proudly serving you
CUB
Fighting for Illinois Consumers
Since 1984
FirstEnergy
Host Integrity Systems
HWS Energy Partners
ICS Cybersecurity, Inc.
IOActive
Using Our Past to Secure Your Future.

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)

2012 TCIPG Activities (1)

Trustworthy Technologies for Wide Area Monitoring and Control

Ongoing

- Cryptographic scalability in the smart grid
- Functional security enhancements for existing SCADA Systems
- GridStat middleware communication framework: Application requirements
- GridStat middleware communication framework: Management security and trust
- GridStat middleware communication framework: Systematic adaptation
- PMU-enhanced power system operations
- Real-time streaming data processing engine for embedded systems
- State-aware decentralized database system for smart grid

Completed

- CONES: Converged networks for SCADA
- Lossless compression of synchrophasor measurement unit archives
- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications

Trustworthy Technologies for Local Area Management, Monitoring, and Control

Ongoing

- Development of the information layer for the V2G framework implementation
- Password changing protocol
- Smart-grid-enabled distributed voltage support
- Trustworthy framework for mobile smart meters

Completed

- Coordinated island operation and resynchronization

2012 TCIPG Activities (2)

Responding To and Managing Cyber Events

Ongoing

- A game-theoretic response and recovery engine (RRE)
- Assessment and forensics for large-scale smart grid networks
- Hardware-based IDS for AMI devices
- Specification-based IDS for smart meters
- Usable management tools for the smarter grid's data avalanche

New Starts

- Specification-based IDS for the DNP3 protocol

Trust Assessment

Ongoing

- Analysis of impacts of smart grid resources on economics and reliability of electricity supply
- Automatic verification of network access control policy implementations
- Modeling methodologies for power grid control system evaluation
- Quantifying the impacts on reliability of coupling between power system cyber and physical components
- Security and robustness evaluation and enhancement of power system applications
- Synchrophasor data quality
- Test-bed driven assessment
- Trustworthiness enhancement tools for SCADA software and platforms
- Vulnerability assessment tool using model checking

Completed

- Tools for assessment and self-assessment of ZigBee networks
- Fuzz testing of proprietary SCADA/control network protocols

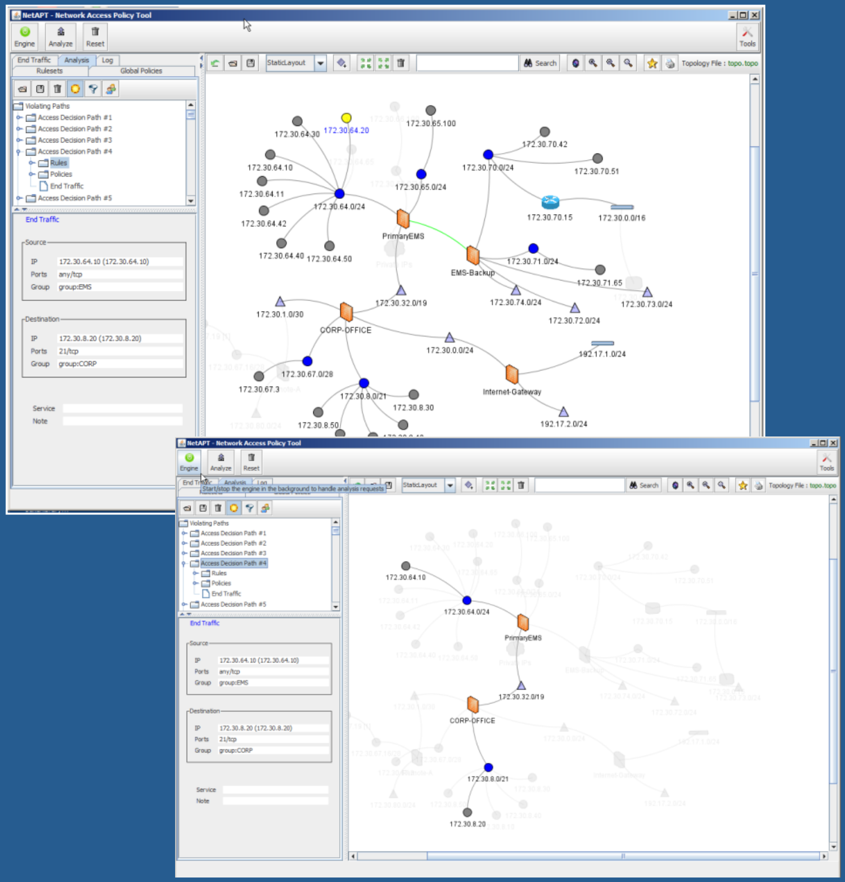
TCIPG Rack 1
TCIPG Rack 2
TCIPG Rack 3
TCIPG Rack 4
TCIPG Mu Dynamics
DELL
TRIPP-LITE
SEL

SEL-421
RTDS™
Real-Time Digital Simulator
RTDS Technologies
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 MANTENARLO
NO PINTE ENCIMA NI REMUEVA ESTA ETIQUETA
CENTRON
CL200 240V 3W TYPE C2SOD 30TA 1.0Kh
MARKETING SAMPLE
306 382 306
OpenWay
USA
CENTRON
CL200 240V 3W TYPE C2SOD 30TA 1.0Kh
MARKETING SAMPLE
306 382 289
OpenWay
USA

Selected 2012 Activities: 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 40 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



NetAPT - Network Access Policy Tool

Violating Paths
- Access Decision Path #1
- Access Decision Path #2
- Access Decision Path #3
- Access Decision Path #4
  - Rules
  - Policies
  - End Traffic
- Access Decision Path #5

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

StaticLayout

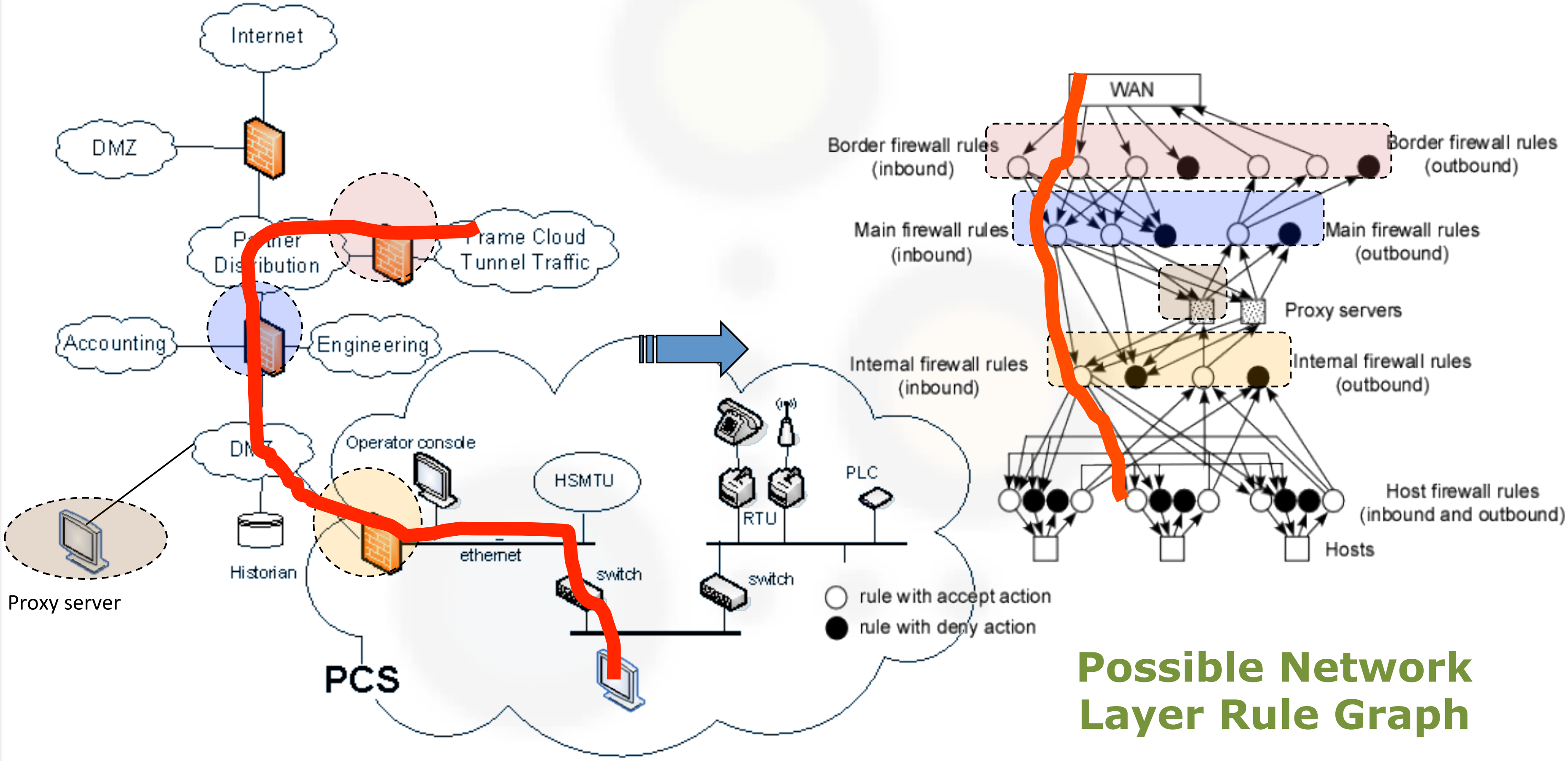
Topology File : topo.topo

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

Heart of Analysis : Rule Graph

Analysis based on identifying paths through "rule graph"

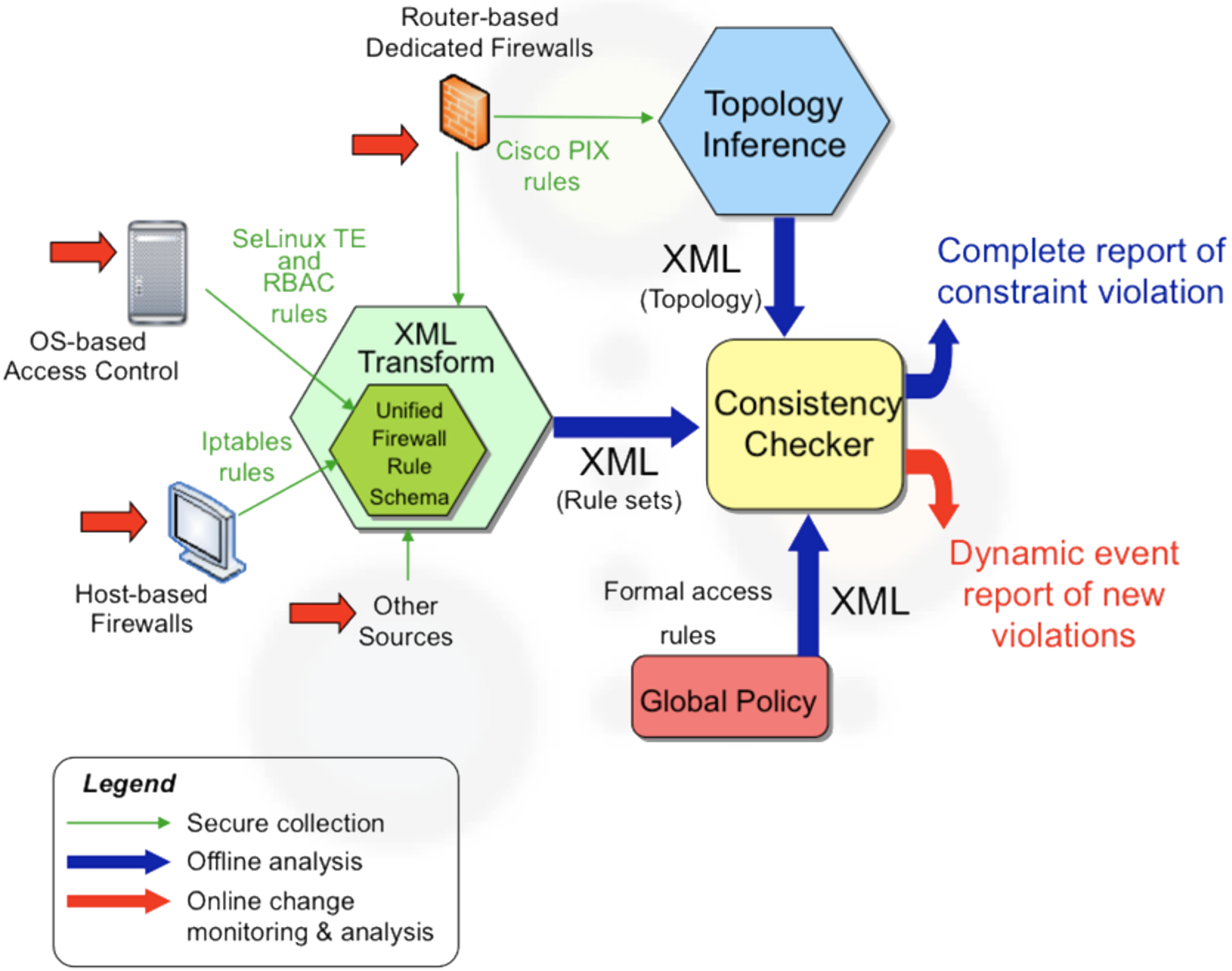
=> Each hop in path corresponds to "policy implementation"

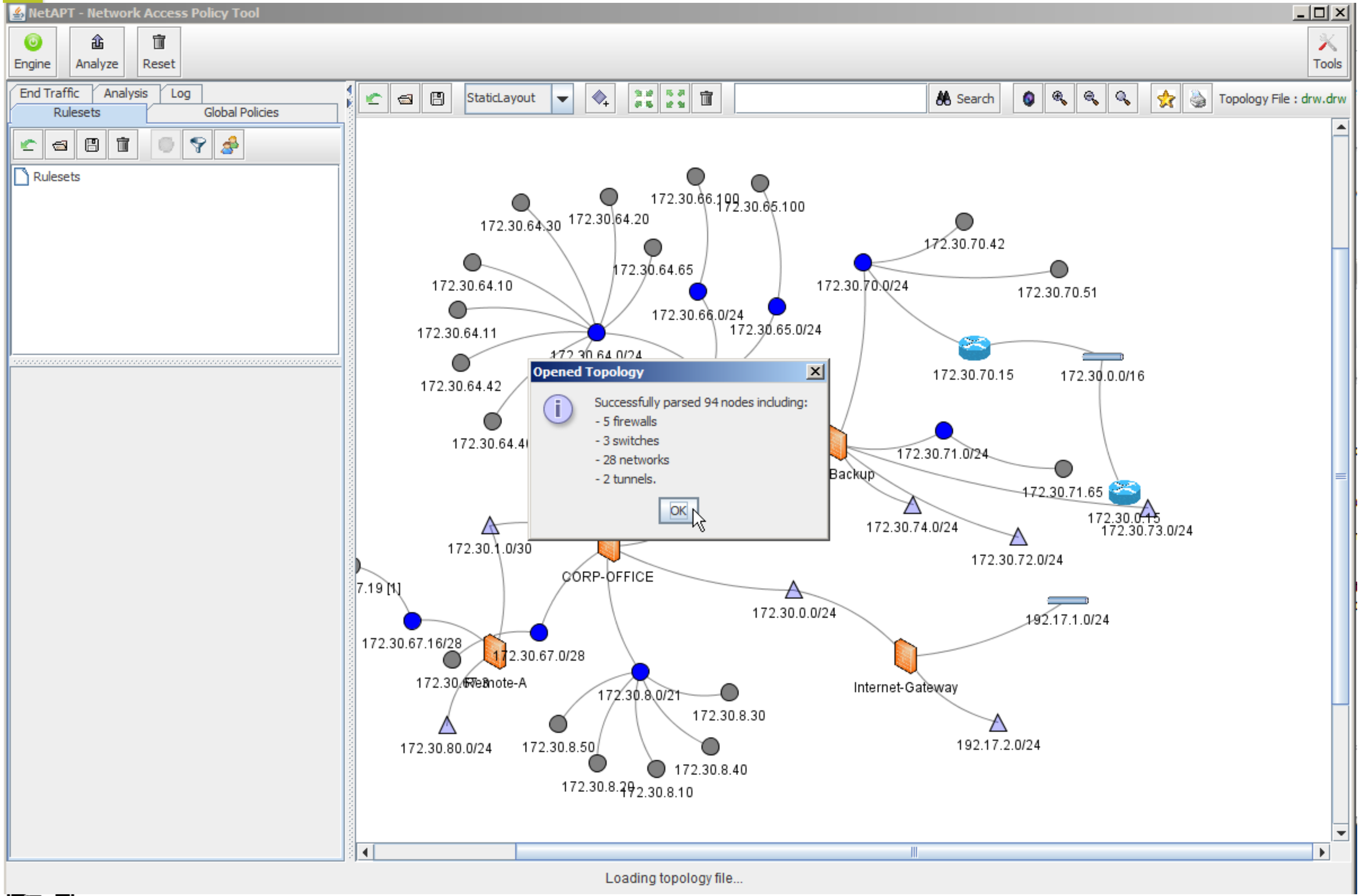

Internet
DMZ
Partner Distribution
Frame Cloud Tunnel Traffic
Accounting
Engineering
DMZ
Proxy server
Historian
Operator console
HSMTU
ethernet
switch
RTU
PLC
switch
PCS
WAN
Border firewall rules (inbound)
Border firewall rules (outbound)
Main firewall rules (inbound)
Main firewall rules (outbound)
Proxy servers
Internal firewall rules (inbound)
Internal firewall rules (outbound)
Host firewall rules (inbound and outbound)
Hosts
○ rule with accept action
● rule with deny action

Possible Network Layer Rule Graph

Network Architecture

Using NetAPT



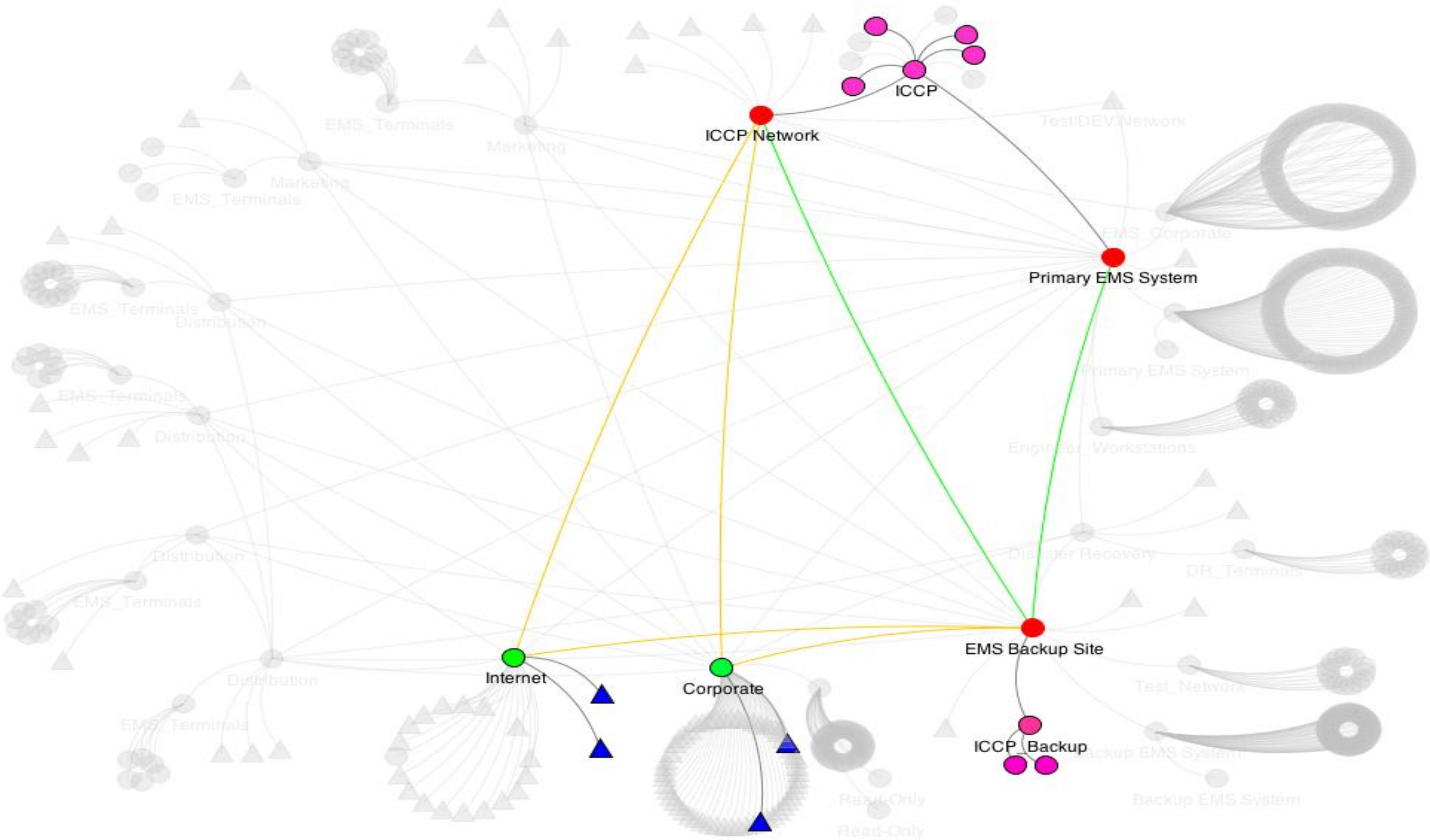


Opened Topology

Successfully parsed 94 nodes including:
- 5 firewalls
- 3 switches
- 28 networks
- 2 tunnels.

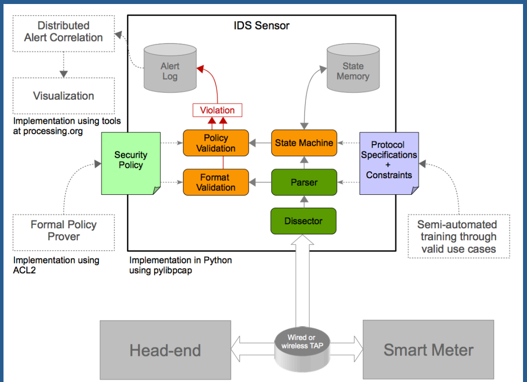
Loading topology file...

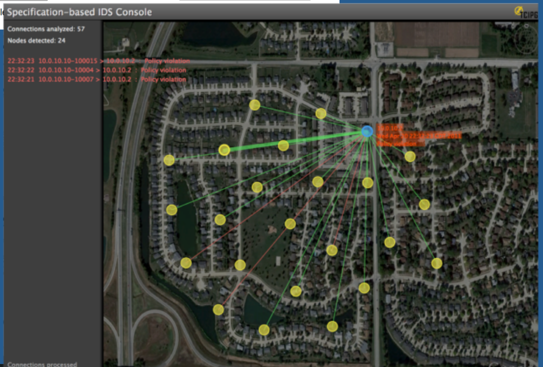
ICCP Traffic Highlighted



Selected 2012 Activities: 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


Distributed Alert Correlation
Visualization
Implementation using tools at processing.org
IDS Sensor
Alert Log
State Memory
Violation
Security Policy
Policy Validation
State Machine
Protocol Specifications + Constraints
Format Validation
Parser
Dissector
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



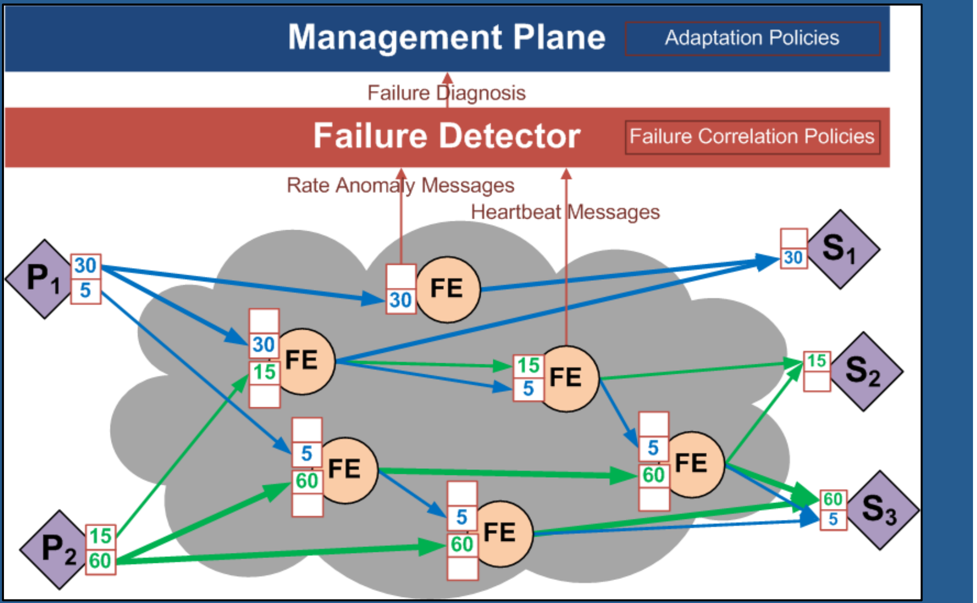
Connections analyzed: 57

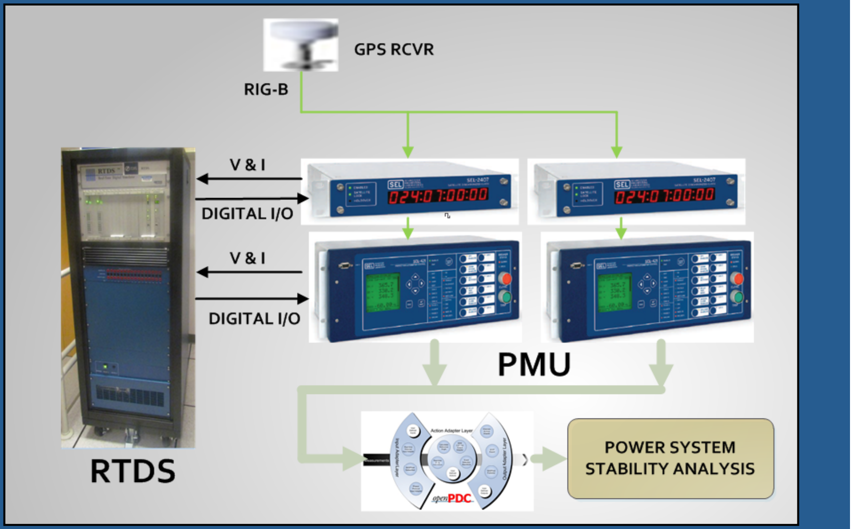
Nodes detected: 24

```
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
```

Selected 2012 Activities: Wide-Area Measurement Infrastructures

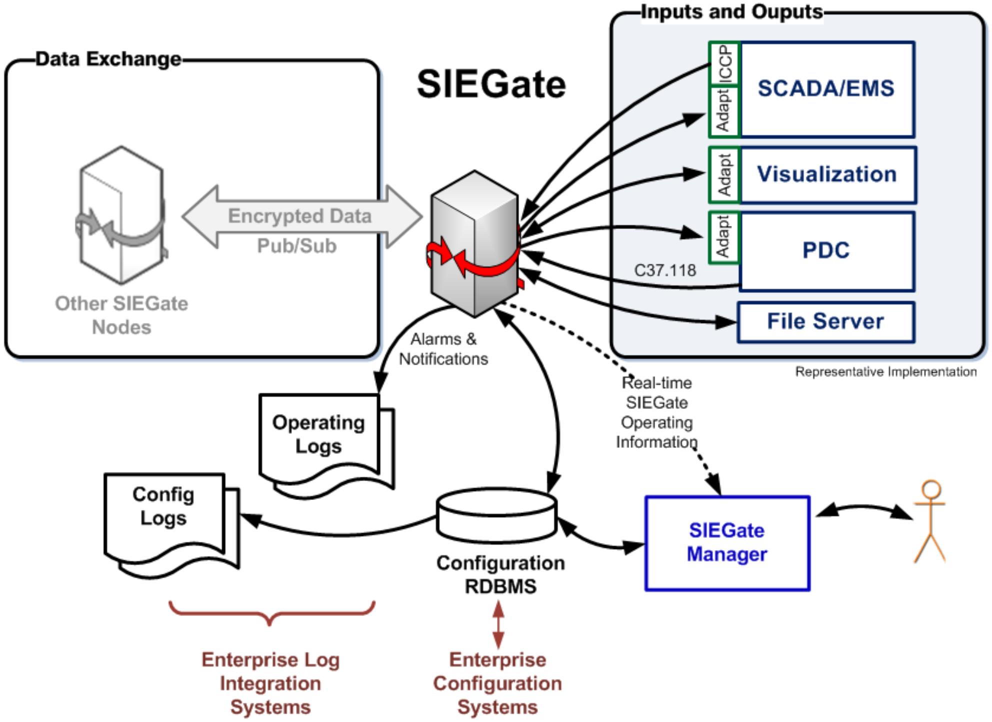
- GridStat Secure Middleware Communication Framework
  - Interaction with McAfee
  - GridStat Inc. spinoff
  - DEFT-DETER federation
- CONES: Converged Networks for SCADA
  - Transitioned to DOE-funded SIEGate (System Information Gateway) appliance with GPA
- Impacts of attacks against wide area measurement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





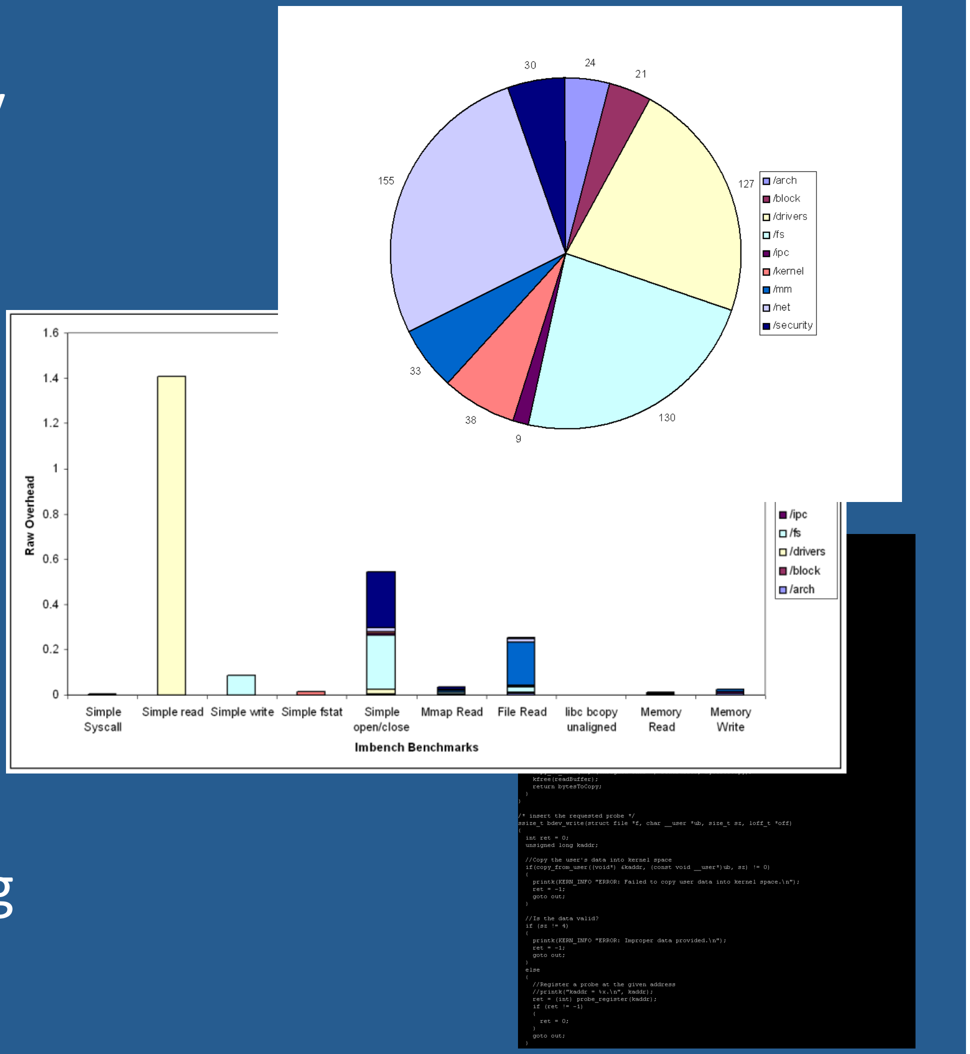
SIEGate: Technical Design Challenges

- **Performance given system complexity**
  - Support multiple data types efficiently and securely
  - Support multiple priorities
  - Minimize latency and maximize throughput
- **High availability assurance**
  - Horizontal and vertical scalability
  - SIEGate stability and reliability
  - Graceful performance degradation
- **Security assurance**
  - Maximize security performance
  - Minimize security breach impact
  - Configurable security levels
  - Security versus simplicity/usability tradeoff



Selected 2012 Activities: Autoscopy Jr.

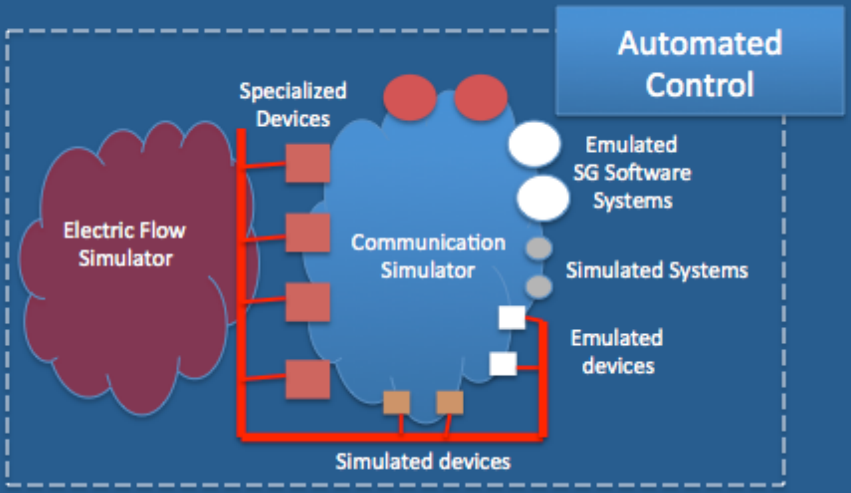
- Autoscopy Jr. is a practical, innovative approach to security in embedded systems
- Research largely completed in 2011
- Tech transfer to SEL
  - SEL has developed a flow-control system based on Autoscopy
  - Incorporated into SEL Exe-Guard project
  - Plans to include in upcoming product lines

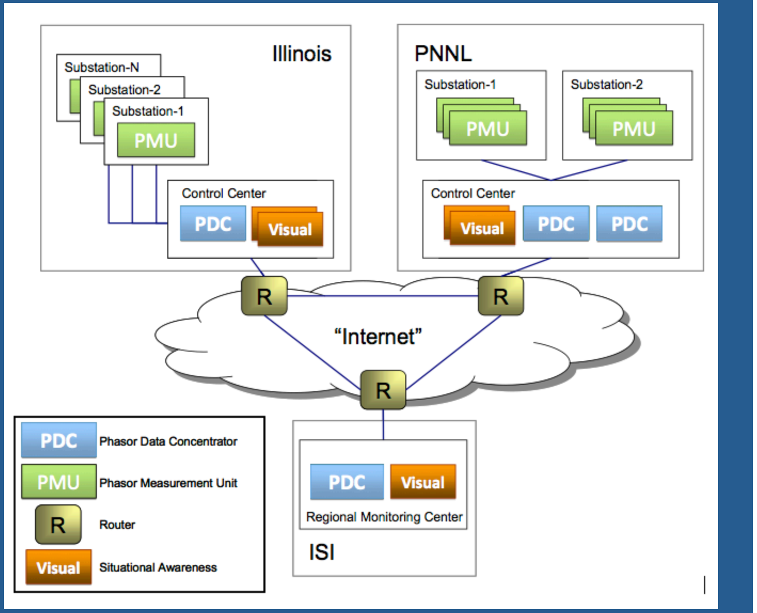


```
    kfree(readBuffer);
    return bytesToCopy;
  }
}

/* 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;
  }
```

Selected 2012 Activities: Testbed

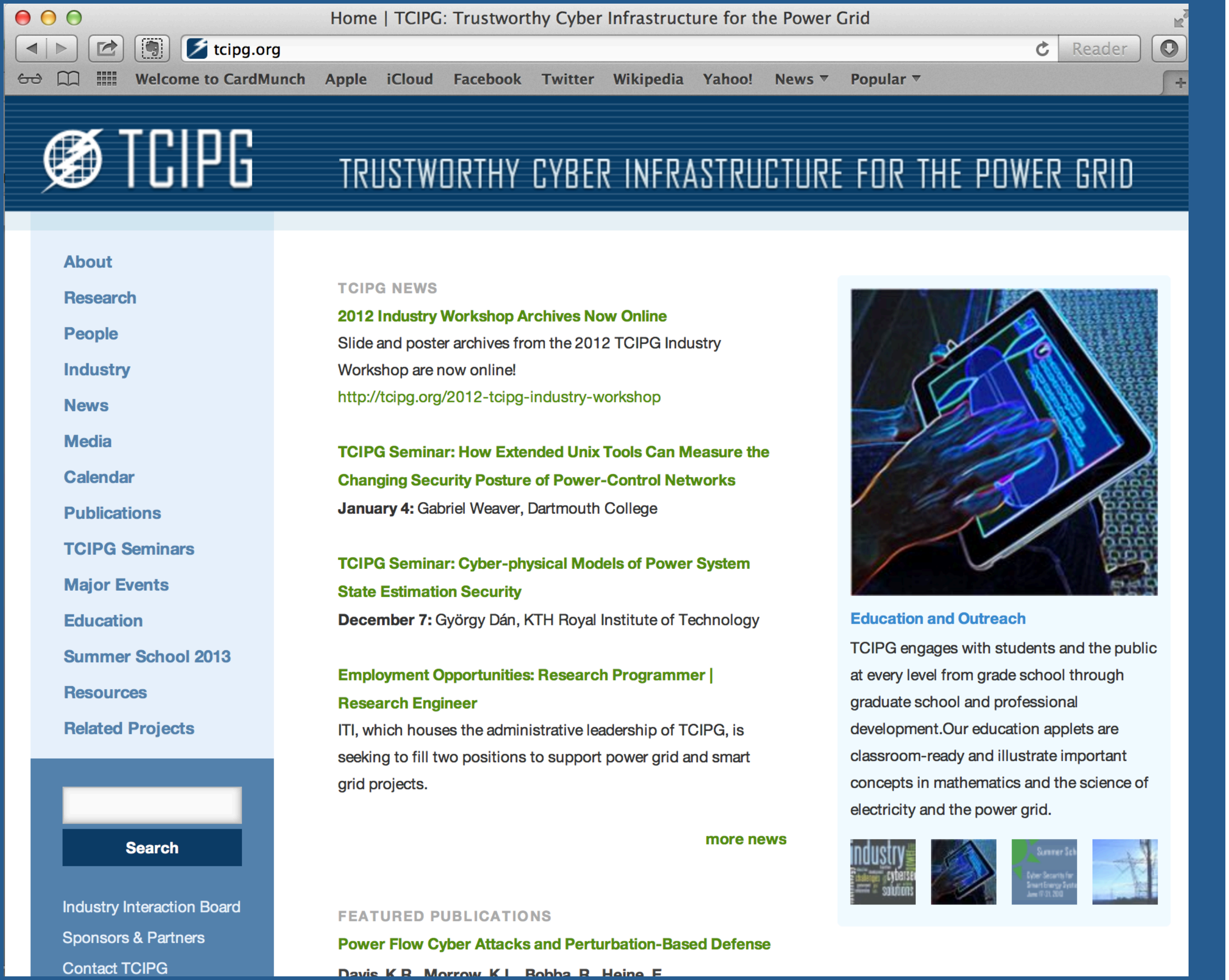
- Implementation of the Itron AMI testbed
- New capabilities in experiment automation
- Expanded hardware-in-the-loop capability with RTDS
- Federation in the DEFT framework
- More detailed testbed presentation to follow





To Get More Information

- www.tcipg.org
- 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.