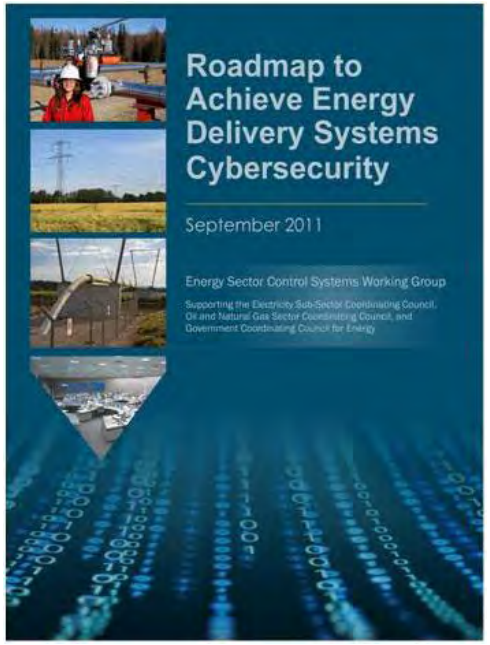
Working Together to Achieve the Energy Sector's Roadmap Vision



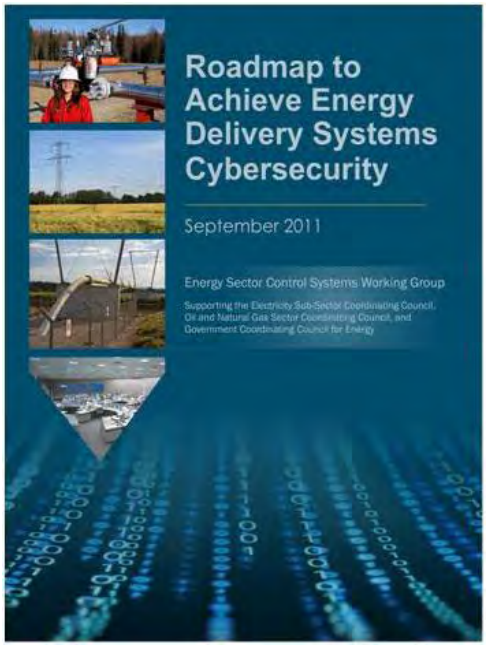
Cybersecurity for Energy Delivery Systems (CEDS)

NASEO

November 12, 2012

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

Roadmap – Framework for Collaboration



- ***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.

For more information go to: www.controlsystemsroadmap.net

R&D Portfolio Strategy

Roadmap prioritizes R&D near, mid, and long term focus

Higher Risk, Longer Term Projects
→ Core NSTB Program
→ Academia Projects
→ Minimum Cost Share

Medium Risk, Mid Term Projects
→ National Laboratory Led Projects
→ Lower Cost Share

Lower Risk, Short Term Projects
→ Industry Led Projects
→ Higher Cost Share

Partnering

Path to Commercialization

Training, Education, Standards Development, and Other Outreach Activities

Academic Program

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

- Cornell University
- Dartmouth College
- University of California, Davis
- University of Illinois
- Washington State University

Software Engineering Institute (SEI)

National Lab Program

- Argonne National Laboratory
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- Lawrence Berkeley National Laboratory

Industry-led Projects

- Grid Protection Alliance
- Honeywell
- Schweitzer Engineering Laboratories, Inc.
- Siemens Energy, Inc.
- Sypris
- Telcordia

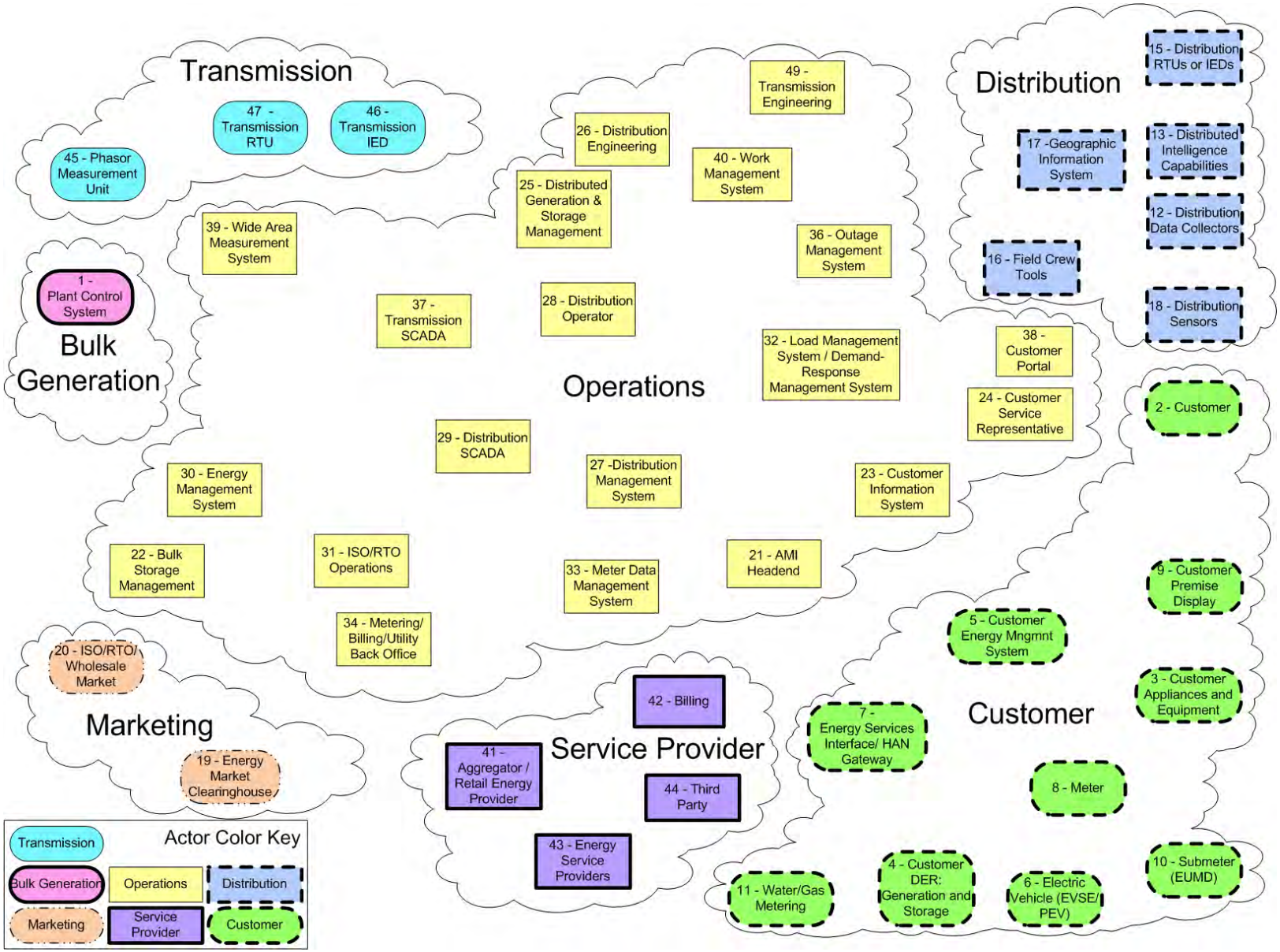


Figure 2-2 Composite High-level View of the Actors within Each of the Smart Grid Domains

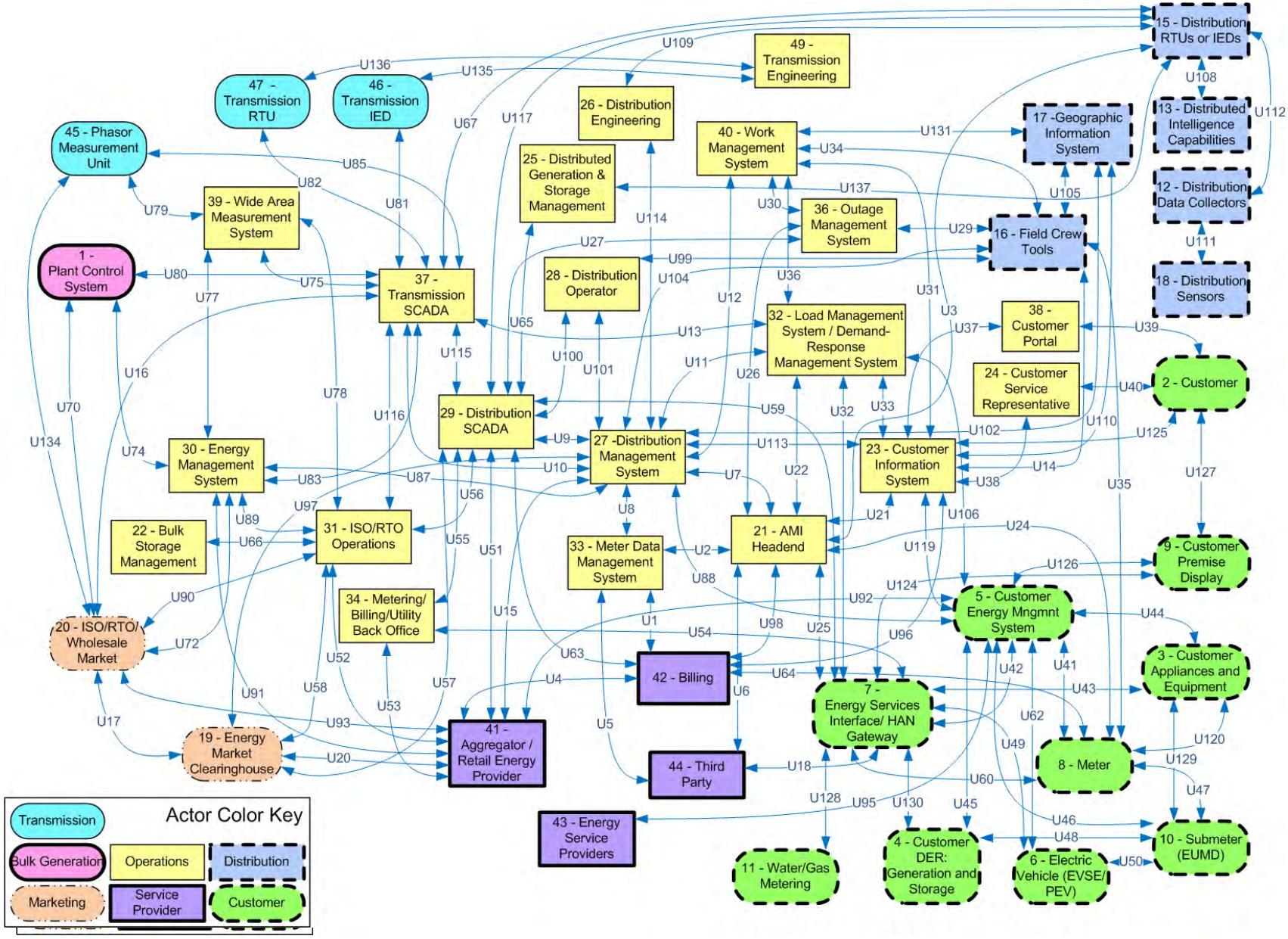


Figure 2-3 Logical Reference Model

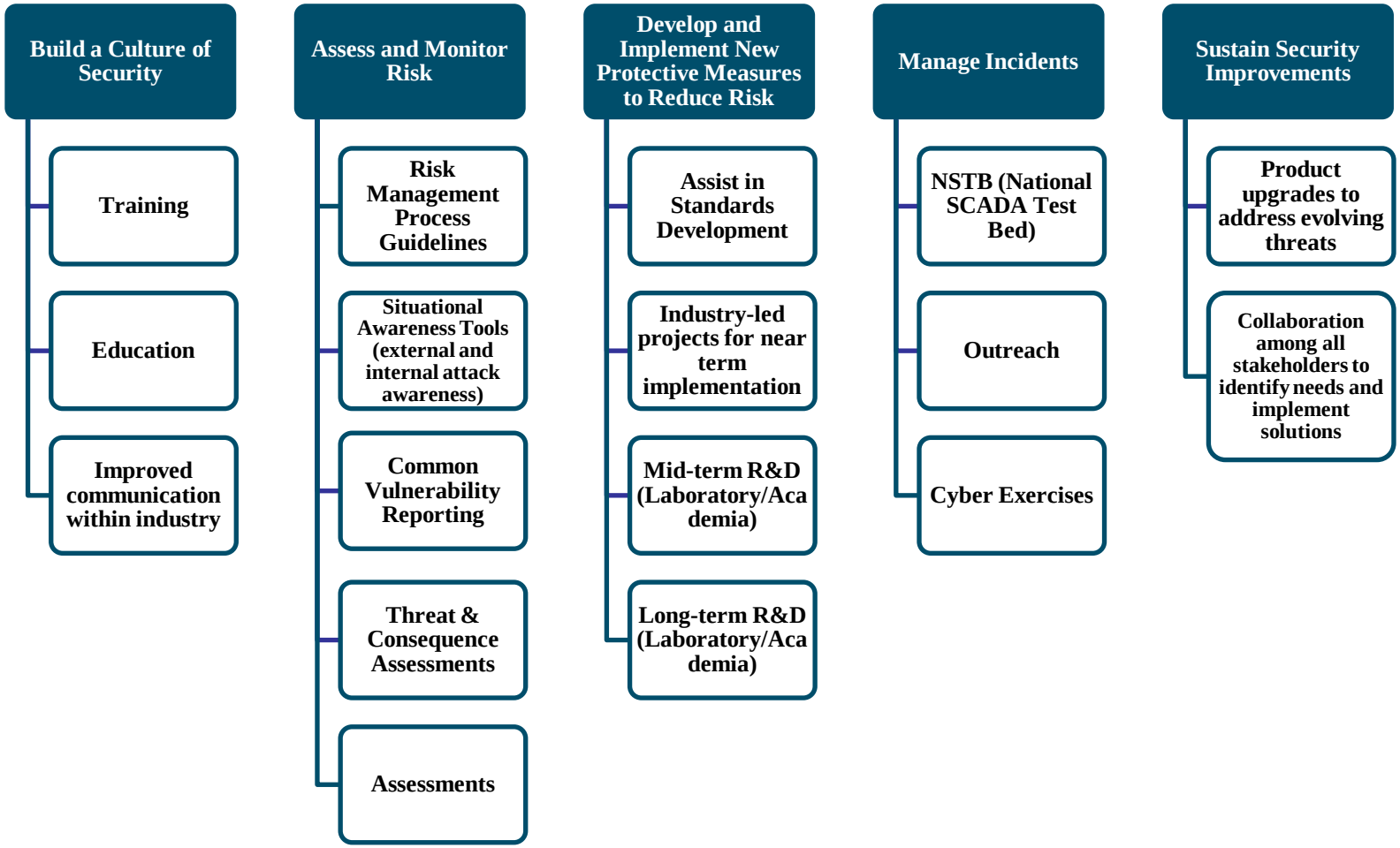
Reading Group Questions

1. How effective is the document in laying out a "strategy" for achieving Electric Power Energy Delivery Systems Cyber Security? The argument supporting your conclusion?

2. Who is responsible for realizing "cyber-secure" Electric Power Energy Delivery Systems? Again support your conclusion

3. What needs to be done in U.S. Universities to support providing "cyber-secure" Electric Power Energy Delivery Systems in the mid- and long-terms?

DOE Activities Align with the Roadmap



CEDS Alignment with the Roadmap

CEDS provides ***Federal funding*** to:

- National Laboratories
- Academia
- Solution providers

To accelerate cybersecurity investment and adoption of resilient energy delivery systems

Strategies	1. Build a Culture of Security	2. Assess and Monitor Risk	3. Develop and Implement New Protective Measures to Reduce Risk	4. Manage Incidents	5. Sustain Security Improvements
Near-term Milestones (0–3 years) By 2013	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (4–7 years) By 2017	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (8–10 years) By 2020	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector

NetAPT/Sophia

Automated Visualization and Monitoring Technologies Strengthen Network Access Control

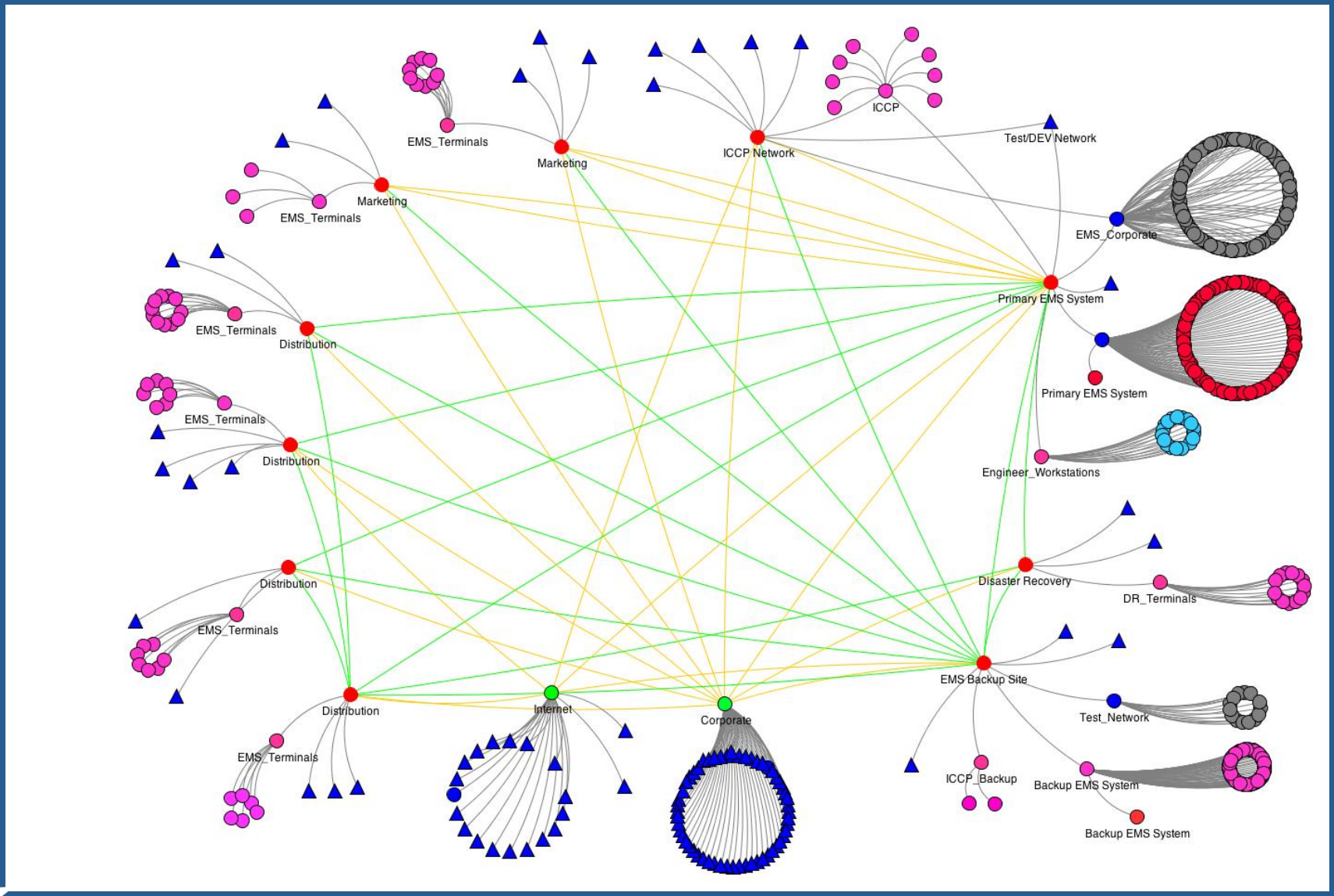
- ***NetAPT captures network firewall configuration information and develops a network topology*** to aid with vulnerability assessments and prepare for NERC CIP audits
- ***NetAPT Compares user defined global access policy to existing configuration and Sophia's real-time observations to identify unexpected communication behavior*** to help operators reduce cybersecurity risk
- ***Sophia provides thorough, real-time, and historical view of communications between control system components connected via IP-based networks, and alerts them when unusual activity may present a security concern***

Project Successes:

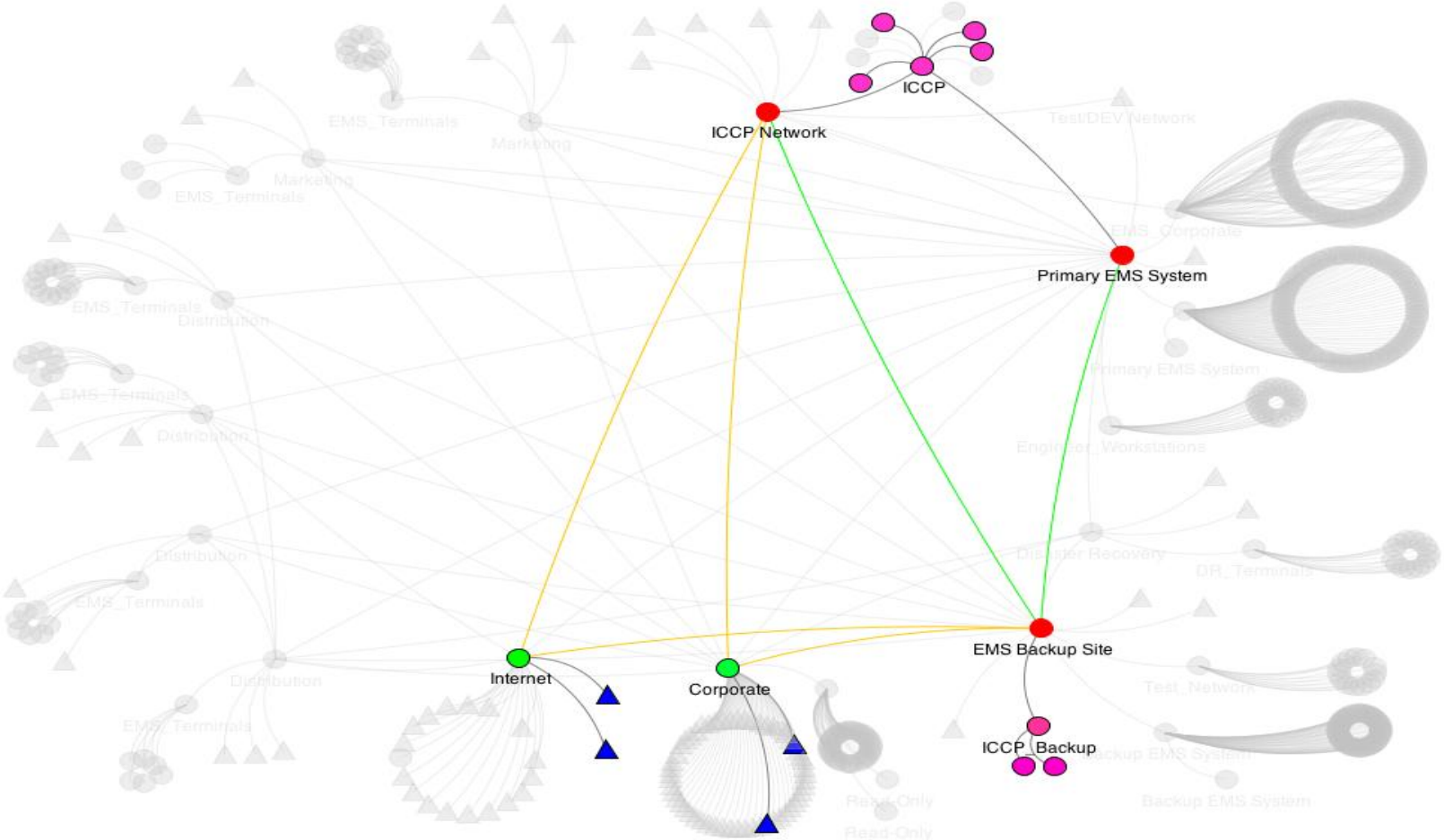
- More than 20 copies of NetAPT have been licensed; a company has formed to commercialize it
- TCIPG's industry partners are now using NetAPT for vulnerability assessments and compliance audits
- Sophia was beta tested by 29 industry participants and is moving toward commercialization

TCIPG: University of Illinois, Idaho National Laboratory, Idaho Falls Power

Network Map


ICCP
EMS_Terminals
Marketing
ICCP Network
Test/DEV Network
Marketing
EMS_Terminals
EMS_Corporate
Primary EMS System
EMS_Terminals
Distribution
Primary EMS System
EMS_Terminals
Distribution
Engineer_Workstations
Distribution
Disaster Recovery
DR_Terminals
EMS_Terminals
EMS Backup Site
Distribution
Internet
Corporate
Test_Network
EMS_Terminals
ICCP_Backup
Backup EMS System
Backup EMS System

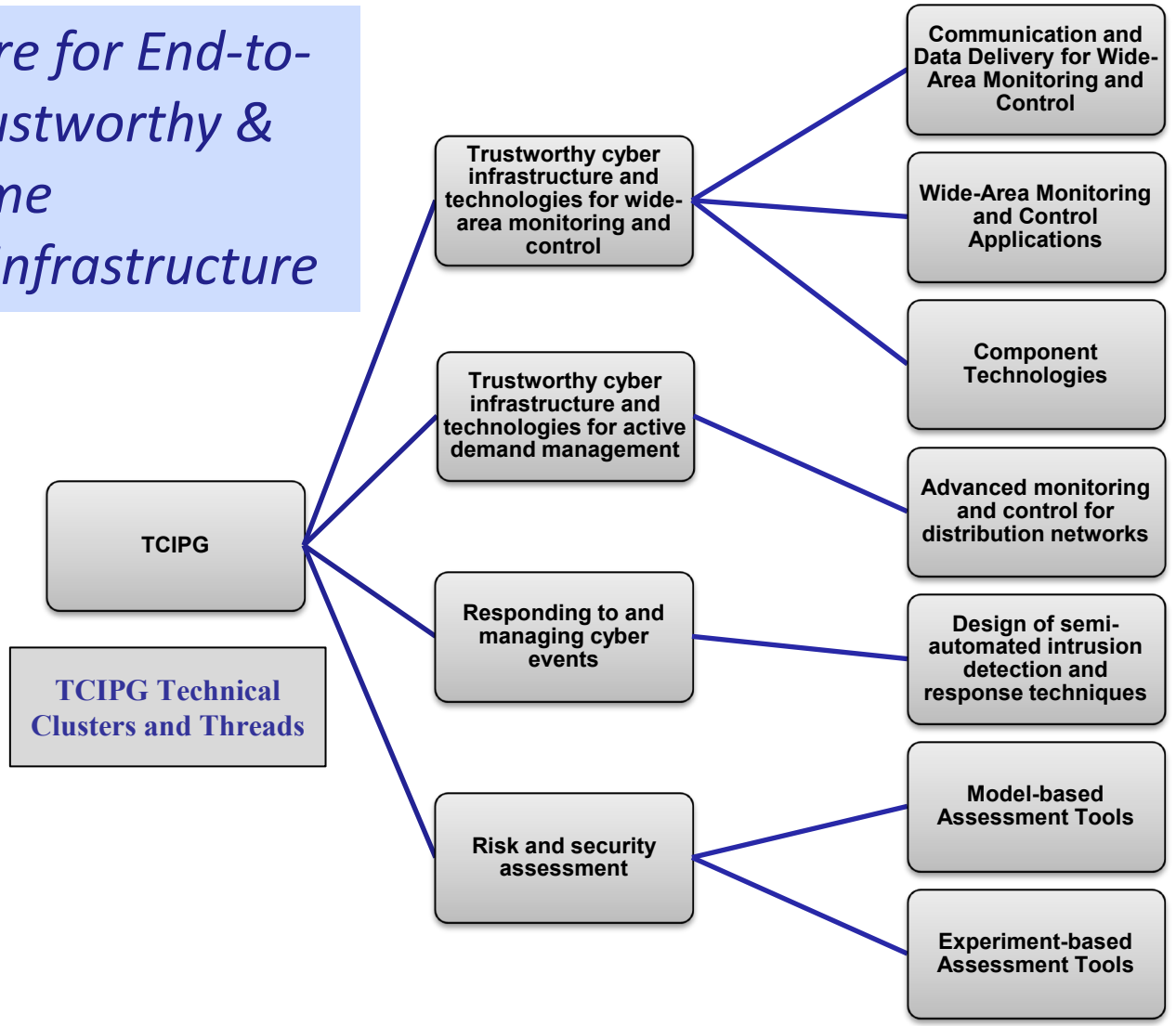
ICCP Traffic Highlighted



Trustworthy Cyber Infrastructure for the Power Grid

(TCIPG, University-Led Collaboration)

Vision: *Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure*



Funding

$18.8 million over 5 years (2009-2014, 20% cost match)

from DOE and DHS

Facilities

Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

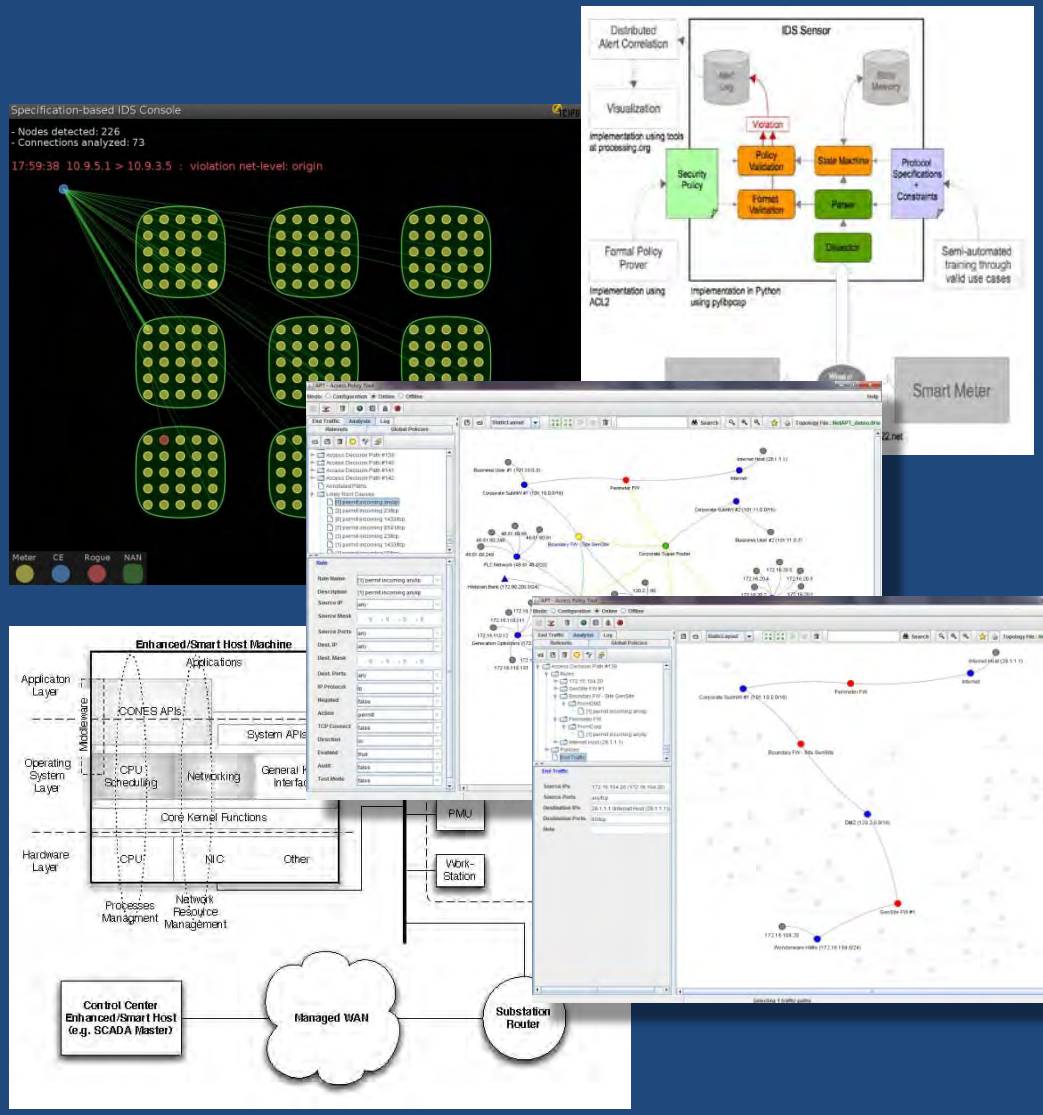
TCIPG IMPACTS ALL ASPECTS OF THE *2011 ROADMAP TO ACHIEVE ENERGY DELIVERY SYSTEMS CYBERSECURITY*

TCIPG Efforts

Build a Culture of Security	Assess and Monitor Risk	Protective Measures/Risk Reduction	Manage Incidents	Sustain Security Improvements
Conduct summer schools for industry	Analyze security of protocols (e.g. DNP3, Zigbee, ICCP, C12.22)	Build secure, real-time, & flexible communication mechanisms for WAMS	Build game-theoretic Response and recovery engine	Offer Testbed and Expertise as a Service to Industry
Develop K-12 power/cyber curriculum	Create tools for assessing security of devices, systems, & use cases	Design secure information layer for V2G	Develop forensic data analysis to support response	Anticipate/address issues of scale: PKI, data avalanche, PMU data compression
Develop public energy literacy	Create integrated scalable cyber/physical modeling infrastructure	Provide malicious power system data detection and protection	Create effective Intrusion detection approach for AMI	Act as repository for cyber-security-related power system data
Directly interact with industry	Distribute NetAPT for use by utilities and auditors	Participate in industry-led CEDS projects		
Educate next-generation cyber-power aware workforce	Create fuzzing tools for SCADA protocols			

Selected TCIPG accomplishments transitioning to the energy sector

- **Autoscopy Jr.:** Lightweight kernel-based intrusion detection system
- **Specification-based IDS for AMI**
- Security specification development and review for industry
- NetAPT creates passive map of control system network paths
- LZ-Fuzz has been used in a power environment to test ICCP connections
- CONES: Converged Networks for SCADA algorithms formed basis of DOE-funded SIEGate (System Information Gateway) appliance



Industry-Led Projects

1. **Watchdog** – Develop a Managed Switch for the control system local area network (LAN) that uses whitelist filtering and performs deep packet inspection→**Schweitzer Engineering Laboratories**, *CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory*

2. **Whitelist Anti-Virus for Control Systems** - Develop a whitelist anti-virus solution for control systems integrated with substation-hardened computers and communication processor→**Schweitzer Engineering Laboratories**, *Dominion Virginia Power, Sandia National Laboratories*

3. **Security Core Component** - Develop a near-real-time cyber and physical security situational awareness capability for the control system environment→**Siemens Energy Automation**, *Sacramento Municipal Utilities District, Pacific Northwest National Laboratory.*

4. **Role Based Access Control -Driven (RBAC) Least Privilege Architecture for Control Systems** - Develop a least-privilege architecture for control systems that is driven by role-based access control (RBAC)→**Honeywell International**, *University of Illinois, Idaho National Laboratory*

Industry-Led Projects

5. **Tools and Methods for Hardening Communication Security of Energy Delivery System** - Research vulnerabilities in energy sector communication protocols and develop mitigations that harden these protocols against cyber attack while enforcing proper communications→**Ericsson**, *University of Illinois, Electric Power Research Institute, DTE Energy.*

6. **SIEGate** - Develop a Secure Information Exchange Gateway (SIEGate) that provides secure communication of data between control centers→**Grid Protection Alliance**, *University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D.*

7. **Centralized Cryptographic Key Management** - Develop a cryptographic key management capability scaled to secure communications for the millions of smart meters within the smart grid advanced metering infrastructure→**Sypris Electronics**, *Purdue University Center for Education and Research in Information Assurance and Security, Oak Ridge National Laboratory, Electric Power Research Institute*

8. **Padlock** - Develop a low-power, small-size dongle (or plug-in device) that provides strong authentication, logging, alarming, and secure communications for intelligent electronic devices (IED) in the field operating at the distribution level→**Schweitzer Engineering Laboratories**, *Tennessee Valley Authority, Sandia National Laboratories*

National Laboratory-Led Projects

1. **High-Level (4th Gen) Language Microcontroller Implementation**—limits direct access to device memory and hardens microcontrollers against low-level cyber attacks→ **Idaho National Laboratory**, *Siemens Corporate Research*

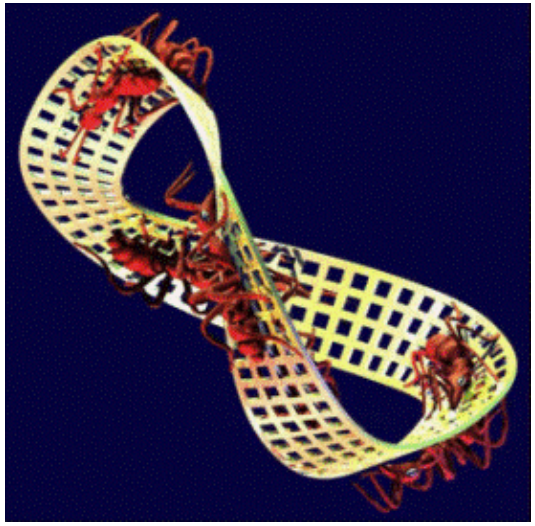
2. **Control Systems Situational Awareness Technology Interoperable Tool Suite**—a situational awareness tool suite for control systems that will show network communications, collect wireless mesh network data message routes, report unexpected behavior, monitor system health, distinguish between component failure and cybersecurity incidents, perform data fusion and determine global effects for local firewall rules→ **Idaho National Laboratory**, *Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho*

3. **Automated Vulnerability Detection for Compiles Smart Grid Software**—automated vulnerability detection for static analysis of compiled software and device firmware→ **Oak Ridge National Laboratory**, *Software Engineering Institute, University of Southern Florida, EnerNex Corporation*

National Laboratory-Led Projects

4. **Next Generation Secure, Scaleable Communication Nework for the Smart Grid**—a secure, scalable communication network for the smart grid using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming→ **Oak Ridge National Laboratory**, *Pacific Northwest National Laboratory, Virginia Tech, OPUS Consulting, Kenexis Consulting.*

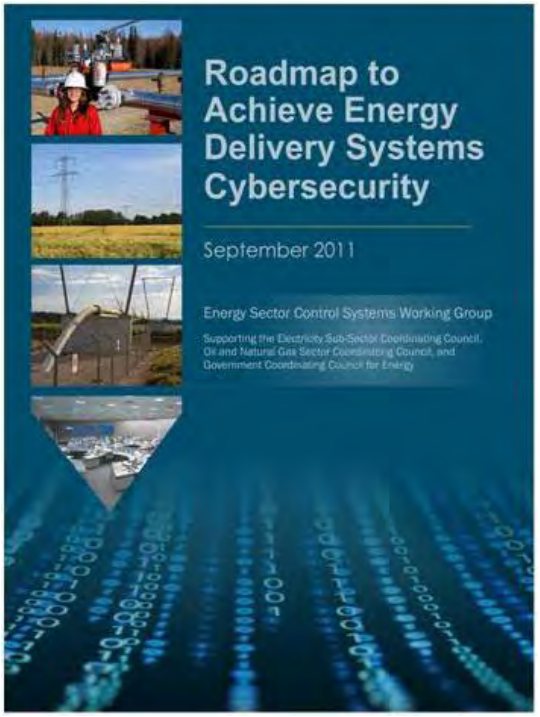
5. **Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector**—bio-inspired technologies using lightweight, mobile agents (Digital Ants) across multiple organizational boundaries found in smart grid architectures to correlate activities, produce emergent behavior, and draw attention to anomalous conditions → **Pacific Northwest National Laboratory**, *Wake Forest University, University of California-Davis, Argonne National Laboratory, SRI International*.



Cybersecurity for Energy Delivery Systems (CEDS R&D)

Carol Hawk
Carol.Hawk@hq.doe.gov
202-586-3247

Diane Hooie
Diane.Hooie@netl.doe.gov
304-285-4524



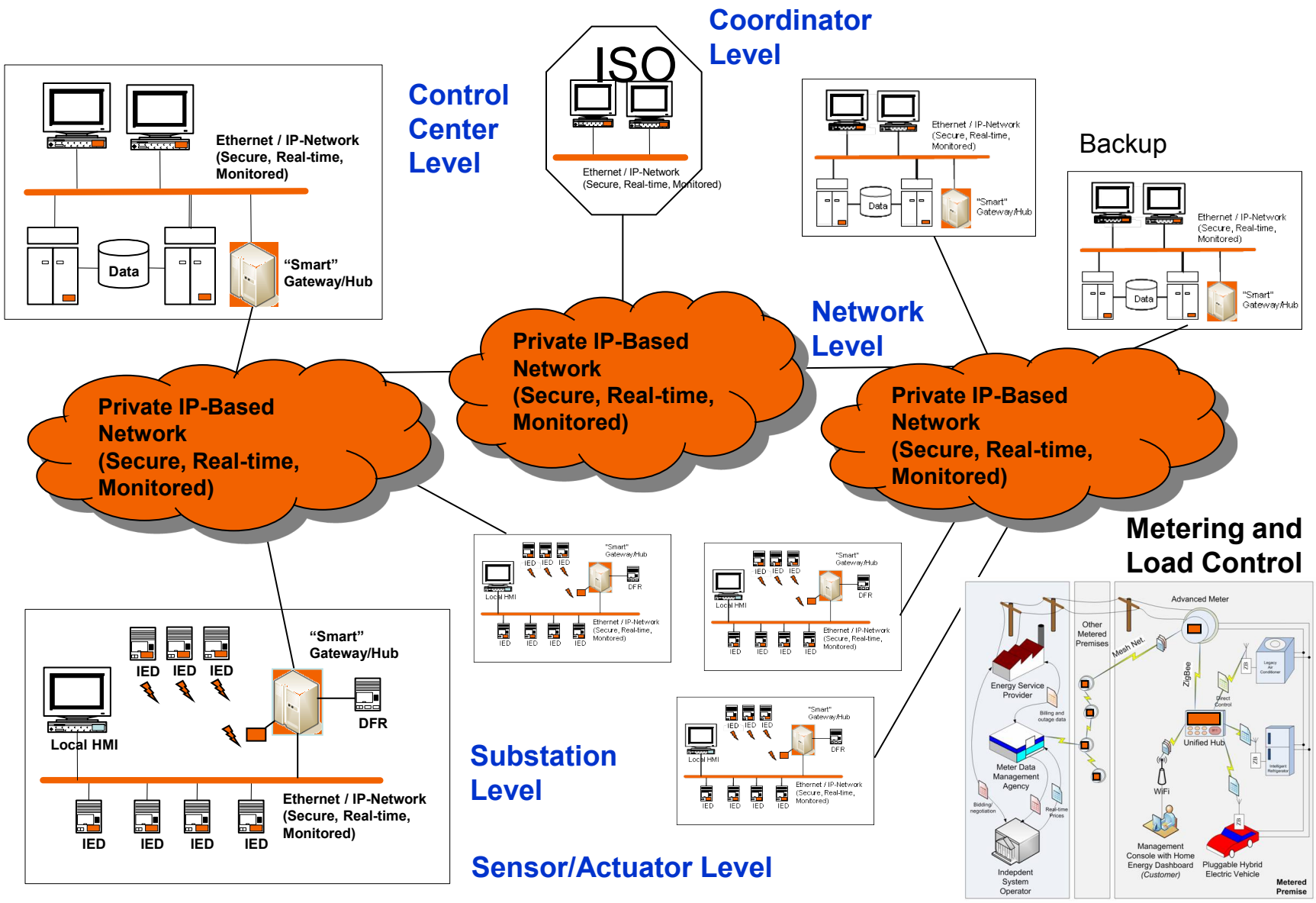
Visit:

http://energy.gov/oe/technology-development/control-systems-security

www.controlsystemsroadmap.net

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

Vision: *Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure*



1.2 SCOPE AND DEFINITIONS

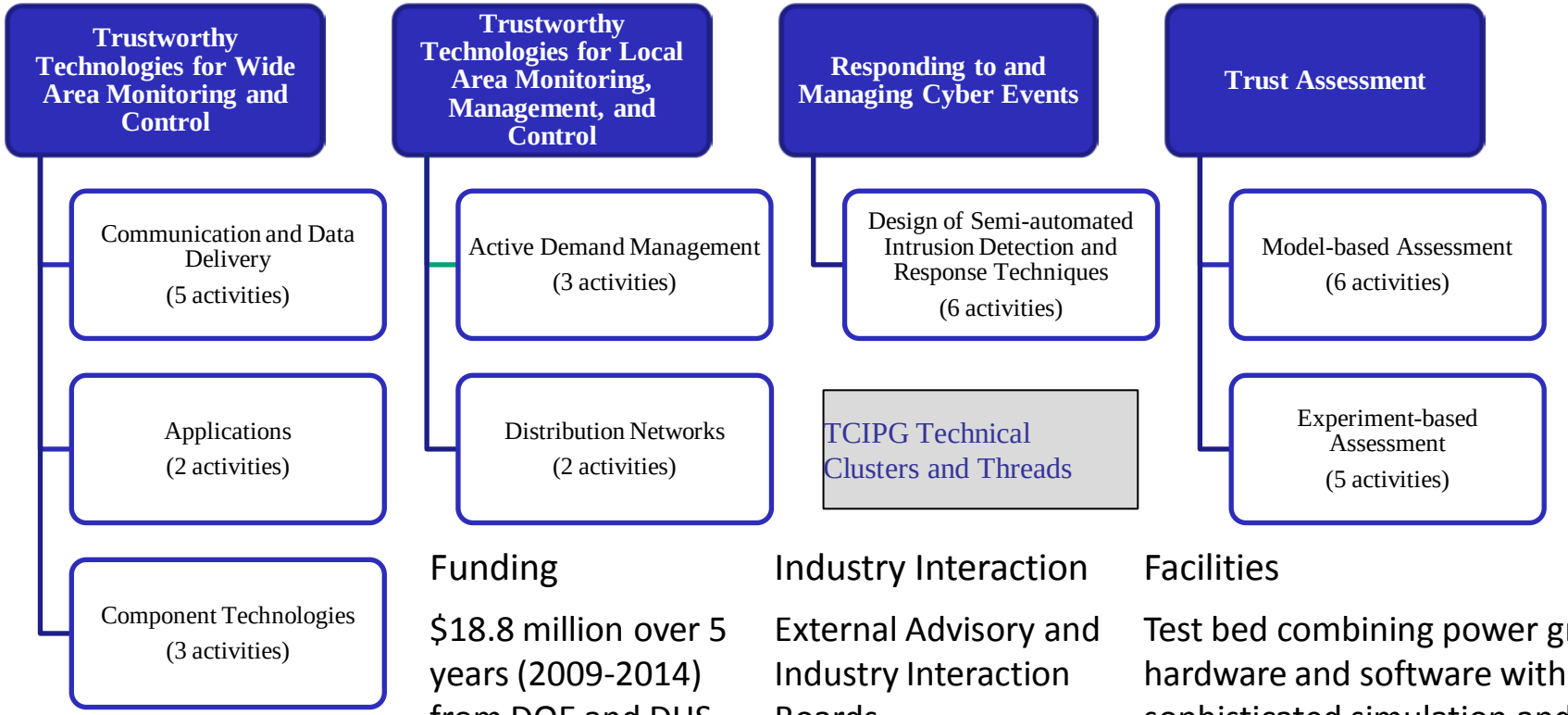
The following definition of cyber infrastructure from the National Infrastructure Protection Plan (NIPP) is included to ensure a common understanding.

> **Cyber Infrastructure**: Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

Trustworthy Cyber Infrastructure for the Power Grid

(TCIPG, University-Led Collaboration; www.tcipg.org)

Vision: *Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure*



Funding

$18.8 million over 5 years (2009-2014) from DOE and DHS (20% cost share)

Industry Interaction

External Advisory and Industry Interaction Boards

Facilities

Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

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

Energy sector cybersecurity protections must respect the operational environment

Energy Delivery Control Systems  ***Business IT Systems***

- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- Energy delivery control system components may have limited computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities
- Energy delivery control system components are widely dispersed over extensive geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

Lemnos Interoperable Configuration Profiles

Configuration Profiles Improve Electricity Delivery Systems Security and Interoperability

- ***Secure channels for routable data communications*** through Internet Protocol Security (IPSec) virtual private networks (VPNs)
- ***Secure web communications and terminal connection*** using the Transport Layer Security (TLS) cryptographic protocol to provide communication security over the Internet and Secure Shell (SSH) for public-key cryptography to authenticate a remote terminal user
- ***Centralized Certificate Revocation*** using the Online Certificate Status Protocol (OCSP) to obtain the revocation status of a digital certificate
- ***Central authentication and authorization*** using the Lightweight Directory Access Protocol (LDAP) for accessing and maintaining distributed directory information services over an IP network
- ***Central log collection*** using Syslog for notification, traceability, and trouble shooting

Project Successes:

- More than 10 security device vendors are using Lemnos profiles in product development
- Interoperability demonstrated in the SEL-3620 Ethernet Security Gateway, now commercially available
- Multiple DOE CEDS projects now using Lemnos

EnerNex Corporation, *Sandia National Laboratories, Schweitzer Engineering Laboratories, Tennessee Valley Authority*

SIEGate

Appliance secures reliability and market data among grid operating entities

- ***Lower risk by building upon the open source phasor gateway***
- ***Create an extensible platform***
- ***Design security throughout***
- ***Balance real-time and security needs***
- ***Conduct thorough bench tests to identify and fix security defects***

Project Successes:

- Field trials are under way
- Design Document complete
- Commercial release Dec 2013

- ***Grid Protection Alliance; University of Illinois,*** Pacific Northwest National Laboratory, Alstom Grid, and PJM Interconnection

Padlock Project

Security Gateway Strengthens Field Device Security

- ***Secure channels for routable data communications (Lemnos)***
- ***Secure web communications and terminal connection (Lemnos)***
- ***Centralized Certificate Revocation (Lemnos)***
- ***Central authentication and authorization (Lemnos)***
- ***Central log collection (Lemnos)***
- ***Connects to serial or Ethernet field device ports***
- ***Proxy host services*** so that users do not connect directly to critical cyber assets
- ***Password enforcement and management of complex passwords***
- ***Physical tampering notification*** will alert operators of a potential problem with the field device

Project Successes:

- Accelerated commercial release to meet customer demand
- Product shipping daily, many to installations where such security controls aren't required by regulation

Schweitzer Engineering Laboratories, *Tennessee Valley Authority, Sandia National Laboratories*

Watchdog Project

Managed Switch Provides Substation Intrusion Protection

- ***Secure terminal connection (Lemnos)***
- ***Central authentication and authorization (Lemnos)***
- ***Central log collection (Lemnos)***
- ***Integrated with a network switch***, which controls all traffic paths for equipment on the local area network (LAN)
- ***Deep packet inspection*** using a white list approach to monitor network traffic down to the application layer for unusual or threatening traffic behavior
- ***Network access control*** quarantines devices that are not authorized to join the network or exhibit unusual or threatening behavior

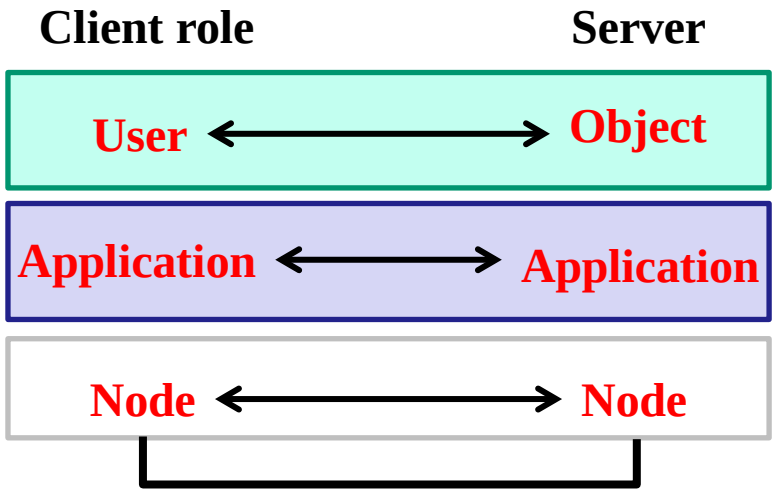
Project Successes:

- Field trials are under way
- Commercial release as the SEL-2730S is expected in May 2014

Schweitzer Engineering Laboratories, *CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory*

RBAC Driven Least Privilege Architecture for Control Systems

- ***Integrated and scalable RBAC for oil and gas controls which addresses nodes, applications and users.***
- ***Policy model providing a common view and optimized for the control system environment***
- ***Architecture and implementation of layered enforcement model***
- ***Evaluate and demonstrate***

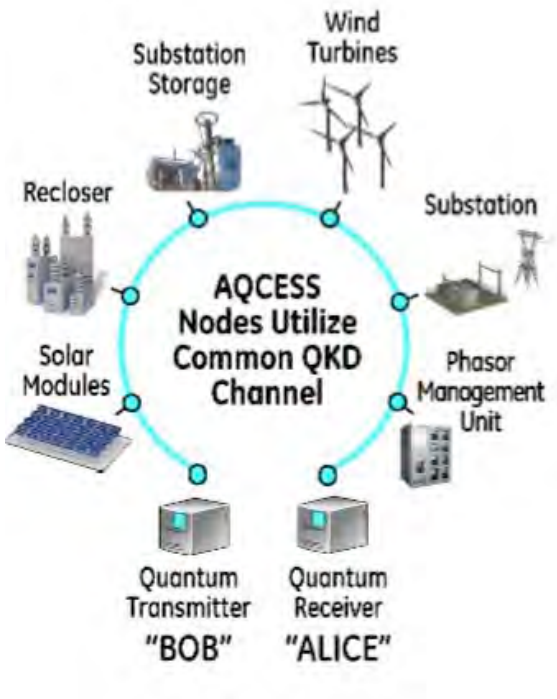


- ***Honeywell Labs, Honeywell Process Solutions****, U of I Information Trust Institute, Idaho National Lab*

Practical Quantum Security

Practical Quantum Security for Grid Automation

- Develop a quantum key distribution (QKD) encryption solution for grid automation components that allows multiple clients to communicate over a single encrypted channel
  - *Unbreakable encryption solution: QKD communications can only be intercepted by violating the known laws of physics*
- Demonstrate AQCESS (Accessible QKD for Cost-Effective Secret Sharing) nodes
  - AQCESS nodes are quantum modulators that modulate the quantum signal being propagated in a commercial QKD channel
  - Multiple AQCESS nodes can utilize the same common QKD channel, allowing any one node to communicate with any other node on the channel
- Integrate AQCESS nodes into commercial grid products



Project Team: ***Oak Ridge National Laboratory***, *General Electric, ID Quantique*

Transition of Energy Sector Protocols

Transition of Energy Sector Legacy Protocols to Support Secure Remote Access

- Objective is to transition legacy protocols towards modern security architectures
- Develop provably secure subsets of legacy protocols
  - Use a language-theoretic view of protocols as a means for classifying protocol complexity and security
  - Generate usage-base subsets of legacy protocols, which are provably more secure than full protocol implementations
- Adapt modern communication technologies to legacy protocols
  - Adapt modern transport (e.g., ZeroMQ) and serialization (e.g., Google Protocol Buffers) technologies to existing energy sector protocols

Project Team: ***Idaho National Laboratory****, New Mexico Institute of Mining and Technology, University of Idaho, Idaho Falls Power, Alberta Electric Systems Operators, UtiliSec, Pacific Northwest National Laboratory*

3 New Laboratory-Led Projects from 2012

Results of the Fiscal Year 2012 National Laboratory Call

1. **Practical Quantum Security for Grid Automation** – Oak Ridge National Laboratory is developing and demonstrating an enhanced quantum key distribution encryption solution for grid automation components.
2. **Supply Chain Integration for Integrity (SCI-FI)** – Pacific Northwest National Laboratory is developing tools and techniques to discover supply chain compromises prior to commissioning and during the service of digital software, firmware, and hardware assets.
3. **Transition of Energy Sector Legacy Protocols to Support Secure Remote Access** – Idaho National Laboratory is transitioning energy delivery systems communications protocols toward modern security architectures

Coordination with Other Federal Cybersecurity R&D Programs

- Primary mechanism for U.S. Government, unclassified Networking and IT R&D (NITRD) coordination
- Supports Networking and Information Technology policy making in the White House Office of Science and Technology Policy (OSTP)

AHRQ, Archives, DARPA, DOD, DOE/OE, DOE/NNSA, DOE/SC, DHS, EPA, HHS/ONC, NASA, NIH, NIST, NOAA, NSA, NSF

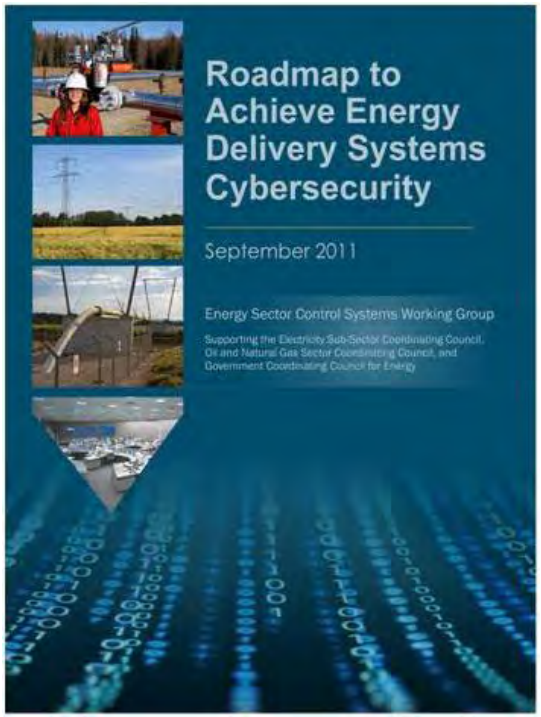
Supply Chain Integration for Integrity (SCI-FI)

Supply Chain Integration for Integrity

- Objective is to develop a suite of open source tools and technologies to detect compromise of energy delivery systems supply chain integrity for utilities, vendors, and chipset manufacturers
- Static discovery - detect compromise of digital assets before commissioning into service
- Dynamic discovery – detect compromise of digital assets during service
- Integrated, inter-disciplinary approach with focus on electricity delivery system:
  - Policy and architecture for built-in supply chain integrity of trusted components
  - Software, firmware, and hardware assets

Project Team: ***Pacific Northwest National Laboratory****, Oak Ridge National Laboratory, Lawrence Livermore National Laboratory, Pacific Gas and Electric, and Digital Management, Inc.*

CEDS Focuses on the Roadmap Vision



- CEDS aligns its R&D efforts with the strategies, milestones, and goals identified in the Energy Sector-led Roadmap
- Encourages partnering among national labs, academia, solution providers, asset owners/operators, and Federal agencies to overcome the energy sector cybersecurity challenges
- Uses its funding and partnerships to accelerate the development and adoption of advanced energy delivery systems cybersecurity solutions