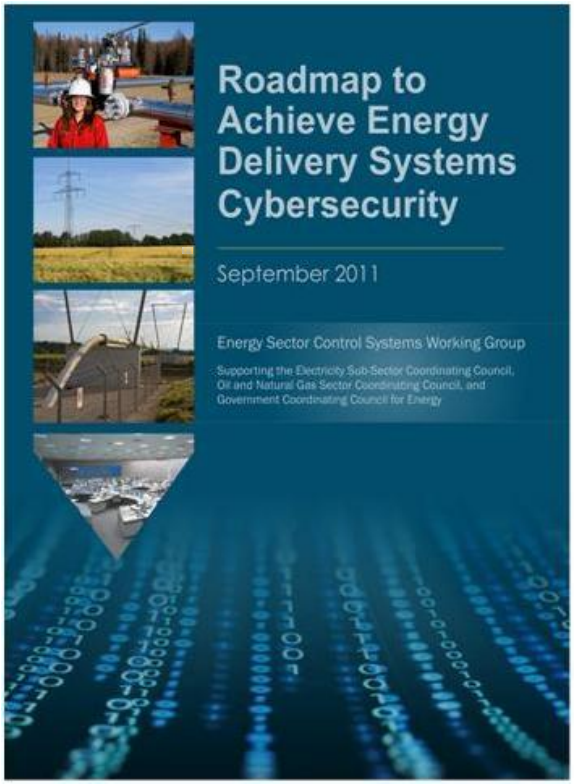
Cybersecurity for Energy Delivery Systems (CEDS) R&D

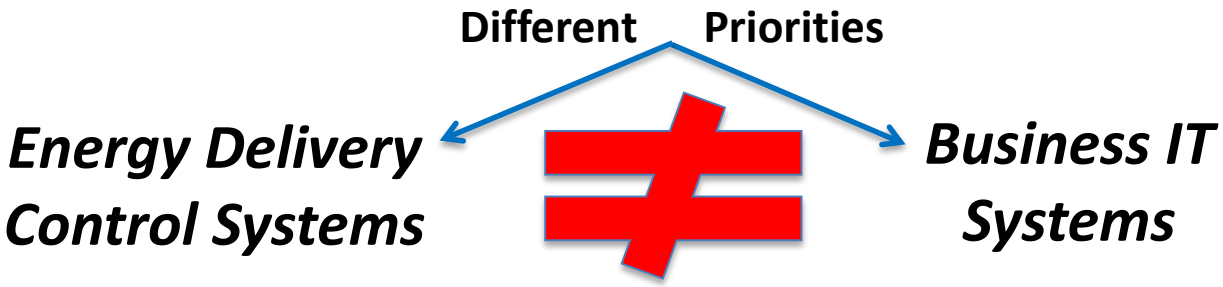
Following the Energy Sector's Roadmap



Carol Hawk
CEDS R&D Program Manager

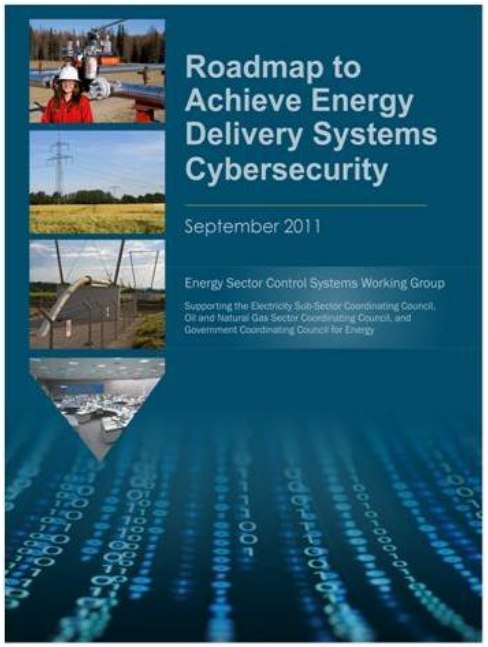
U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

Energy Sector Cybersecurity



- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- EDS components are widely dispersed over wide 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

Roadmap – Framework for Collaboration



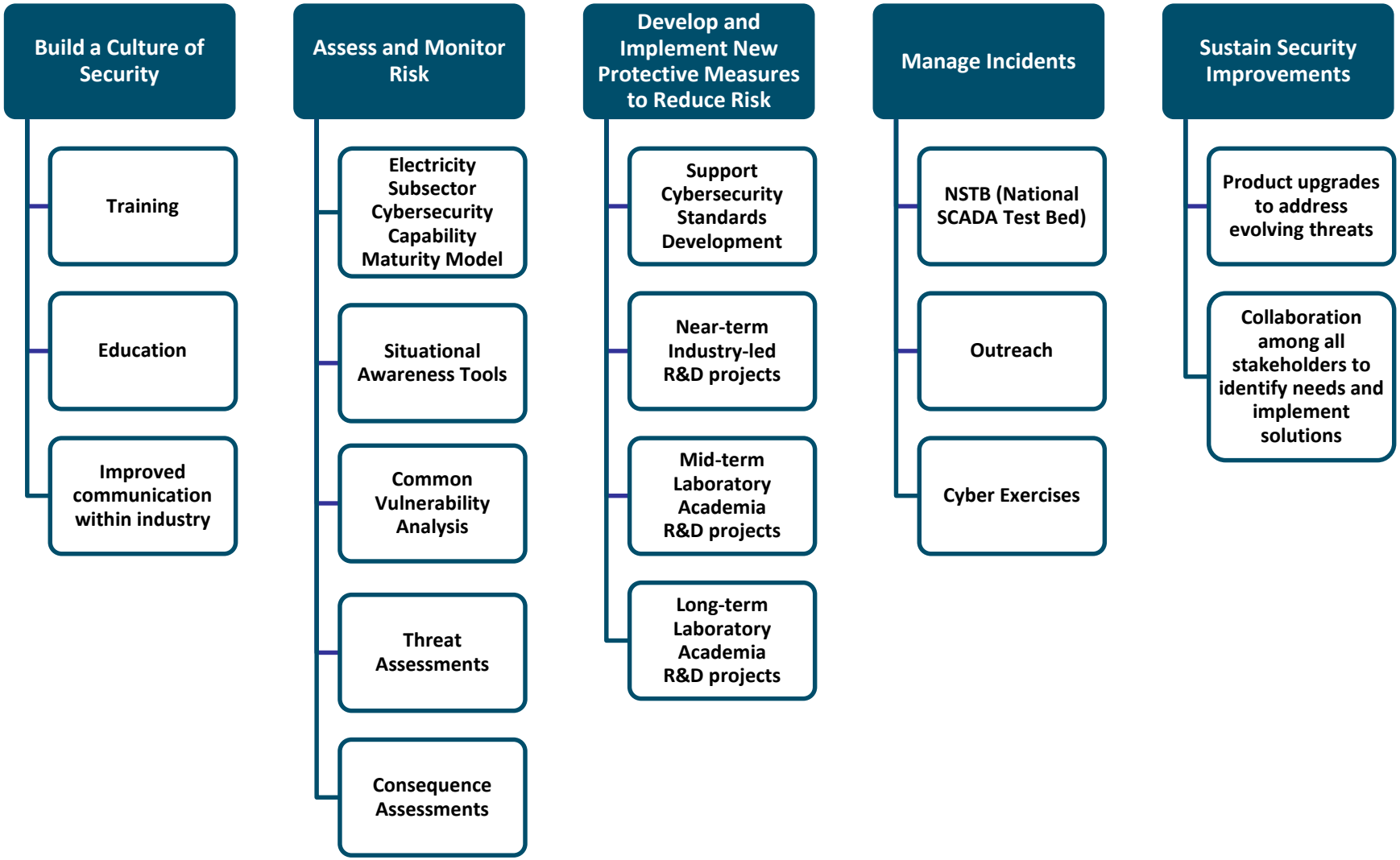
- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

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

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

	1. Build a Culture of Security	2. Assess and Monitor Risk	3. Develop and Implement New Protective Measures	4. Manage Incidents	5. Sustain Security Improvements
Near-term (0–3 yrs)	**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 resilient energy delivery systems
Mid-term (4-7 years)	**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 (8-10 years)	**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

CEDS Program Structure

The CEDS program emphasizes collaboration among the government, industry, universities, national laboratories, and end users to advance research and development in cybersecurity that is tailored to the unique performance requirements, design and operational environment of energy delivery systems. The aim of the program is to reduce the risk of energy disruptions due to cyber incidents as well as survive an intentional cyber assault with no loss of critical function. This program has resulted in increased security of energy delivery systems around the country.

Collaboration Transitions R&D to Practice

Prototype Development

Commercial prototype and open source configuration profile for interoperable secure routable energy sector communications

EnerNex Corporation, Sandia National Laboratories, Schweitzer Engineering Laboratories, Tennessee Valley Authority, 7 Network Security Vendors

Field Demonstration

Lemnos has become a broad industry partnership for secure, interoperable communications

Increasing numbers of energy delivery system vendors have demonstrated Lemnos, today at least ten

Applied Research

Open Process Control System (PCS) Security Architecture for Interoperable Design, known as OPSAID provides vendors of supervisory control and data acquisition/energy management systems (SCADA/EMS) with the capability to retrofit secure communications for legacy devices, and to design-in interoperable security for future energy delivery control systems

Sandia National Laboratories

CEDS projects engage national labs, vendors, asset owners, and academia throughout the project lifecycle to deliver relevant projects with clear commercialization paths.

Open Source Solution

Broad energy sector partnership uses Lemnos interoperable, secure routable energy sector communications

Commercial Product

Schweitzer Engineering Laboratories Ethernet Security Gateway SEL-3620 implements Lemnos

CEDS R&D Transitioned to Practice

- **Amilyzer:** Monitors AMI traffic, helping to ensure that smart meters are running in a secure state ***(TCIPG)***
- **Electric Sector Failure Scenarios:** Utilities can leverage these scenarios for conducting risk assessments and identifying common mitigations ***(NESCOR)***
- **NP-View/Network Access Policy Tool (NetAPT):** Automated and comprehensive security policy analysis of firewall configurations ***(TCIPG)***
- **Padlock and Exe-Guard:** Built on success of Lemnos Security Profiles to enhance the cyber/physical security of distribution automation systems and communication field devices, and prevent unexpected cyber activity ***(SEL)***
- **Secure Information Exchange Gateway:** Security gateway for secure information exchange at control centers ***(GPA)***
- **Sophia:** Provides real-time visualization of inter-device communications between control system components connected via IP-based networks ***(INL)***

Project Lead

Project Partnerships

Project Title

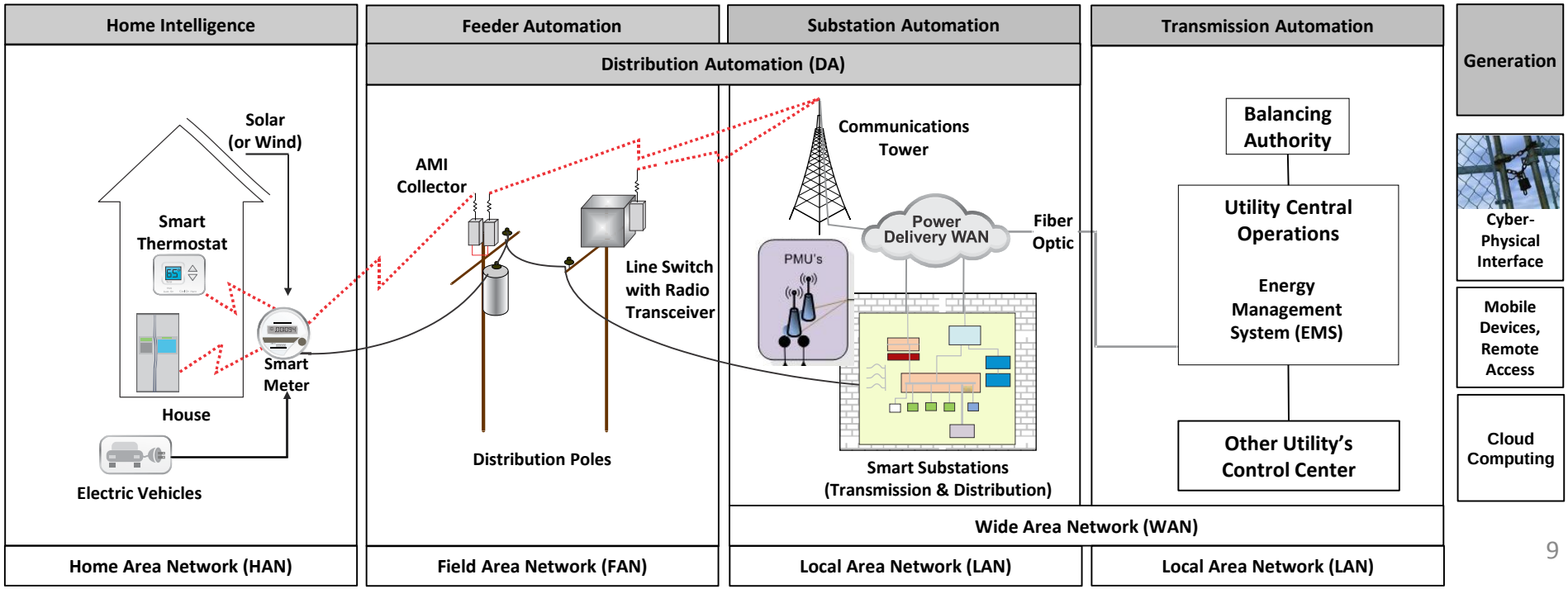
Project: short description (summary)

Cyber summary:
- Supporting technical information/approach
- *How to get there*

Priority aspect(s) of the project

Benefits to the energy sector, asset owner

Addresses Roadmap Milestones: *(milestone numbers from slide 5)*



Partners

Cybersecurity Procurement Language for Energy Delivery Systems

Cybersecurity procurement language tailored to the specific needs of the energy sector

- Helps address evolving challenges, including advancing cybersecurity threats, new technologies, and more stringent regulatory requirements
- Helps asset owners, operators, and suppliers communicate expectations and requirements in a clear and repeatable manner
- Promotes cybersecurity throughout the product lifecycle, including the design, supply chain selection, manufacture, shipment, installation, and maintenance phases of the product.

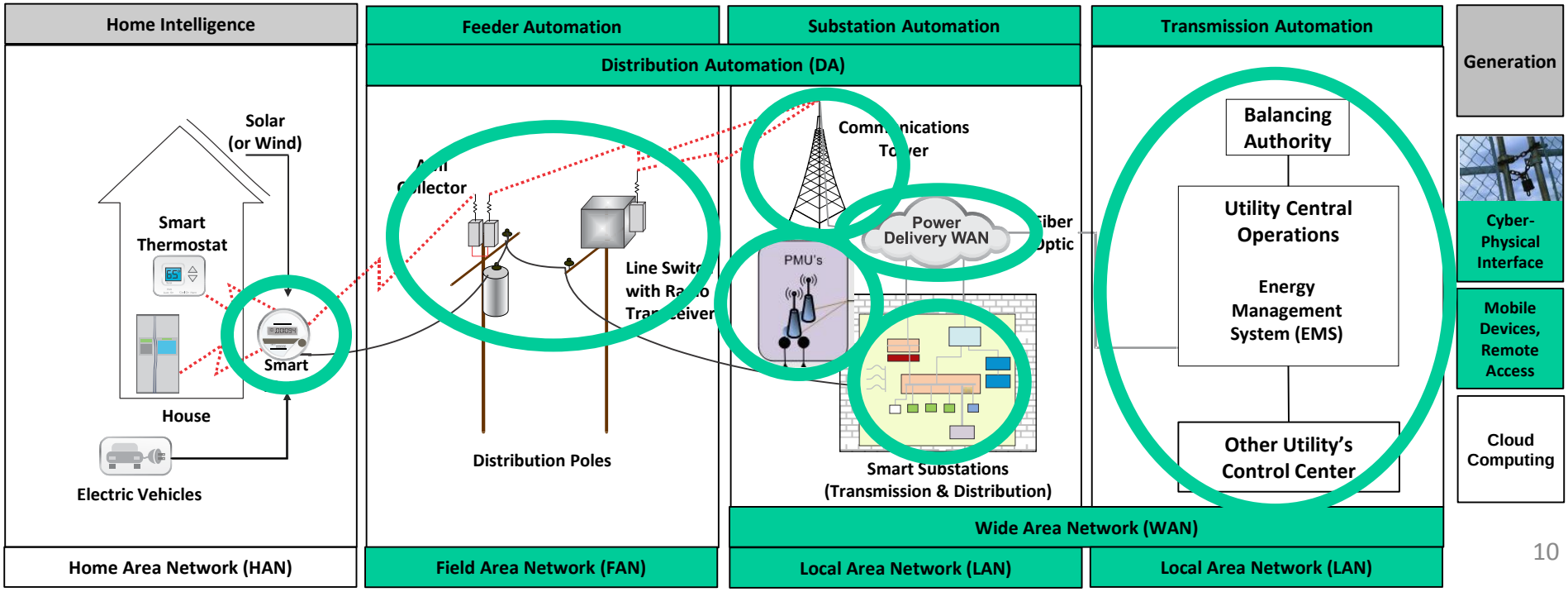
Baseline cybersecurity procurement language

- Provides a menu of cybersecurity considerations that can be tailored for specific procurement contracts
- Sample language can be used to help inform the Request For Information/Proposal process
- Recommended language can help improve the security and transparency of the supplier and/or integrator's supply chain practices

Current status/Project successes

- A successful partnership of government, national laboratory, and a broad range of Energy Sector stakeholders on the document writing team.
- Two drafts have undergone Energy Sector stakeholder review (November 2013, February 2014) – including asset owners, operators, and suppliers.
- Final version released in April 2014

Addresses Roadmap Milestones: *1.2, 1.3, 1.5*



National Rural Electric Cooperative Association
A Touchstone Energy® Cooperative

Cooperative Research Network

Partners: Honeywell, Cigital, NRECA cooperatives, Carnegie Mellon University, Pacific Northwest National Laboratory

Energy Sector Security Appliances in a System for Intelligent, Learning Network Configuration Management and Monitoring (Essence)

Stronger, easier to manage operational and back office network security for electric cooperatives

- Make it easier for small electric cooperatives with limited IT resources to securely define, configure, manage and monitor utility operational networks
- Secure the ongoing migration of utility IT and operational systems to virtualization and cloud managed services
- R&D for a software defined network (SDN) that automates secure operational network management to reduce effort and risk associated with manual processes

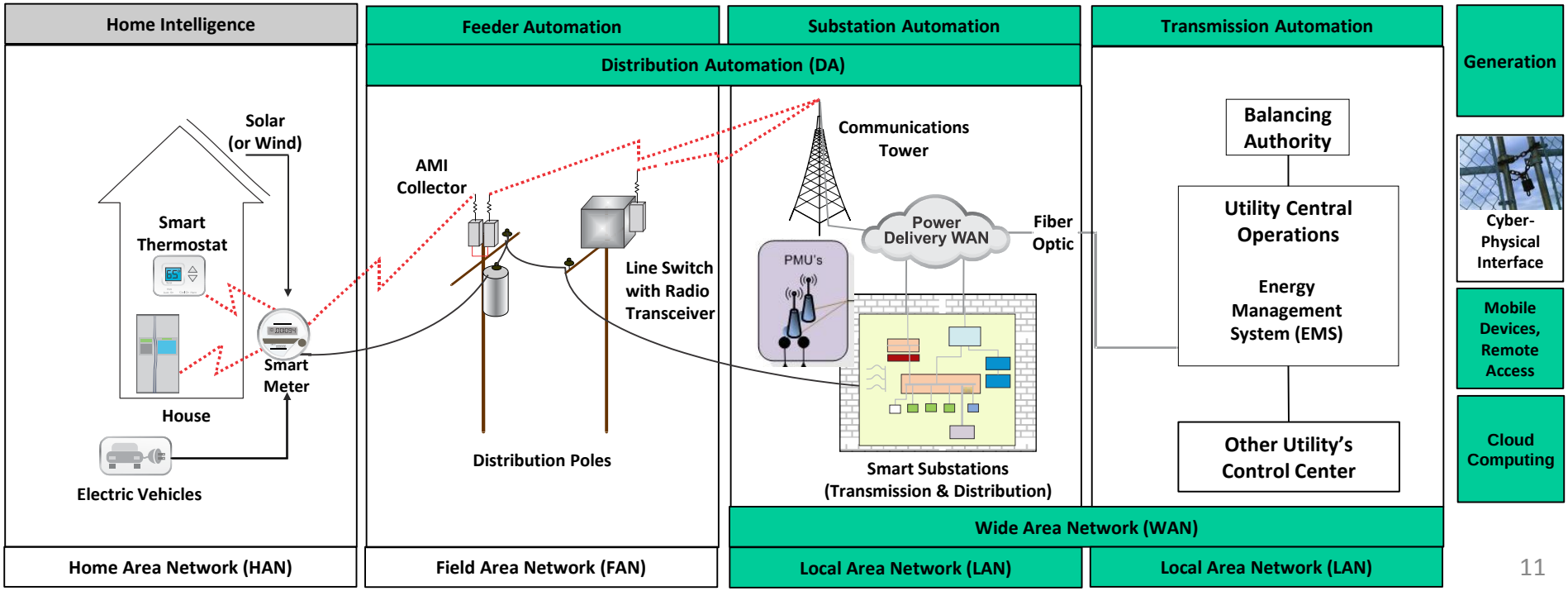
Easier, more reliable development and enforcement of utility's security policy

- SDN maps a network, analyzes network traffic and learns expected traffic flow to better inform human operators
- Defines, implements and enforces high-granularity security policy
- Updates utility's security policy as business needs and cyber-threats evolve
- Ensures operational network configuration changes conform to utility's security policy
- Simplifies security reporting and compliance tasks for utility operational networks

Real-time cybersecurity that is aware of power grid operations

- Power grid operations-aware filtering rules detect and prevent malicious operational network traffic using utility protocols (e.g., Multispeak, DNP3)
- Dynamic network access control policies that invoke graceful degradation tailored to the role of the person or cyber device for which trust has decreased

Addresses Roadmap Milestones: *2.3, 3.3, 3.4, 3.5 , 4.1, 4.2, 4.5*



Secure Policy-Based Configuration Framework (PBCONF)

Partners: SEL Schweitzer Engineering Laboratories; Ameren Focused Energy. For Life.; Illinois

Reduce risk of cyber attacks that exploit incorrect or inconsistent energy delivery device security

- Interoperable, common framework for secure remote configuration of a utility's energy delivery devices
- Framework supports centralized and distributed peer based configuration for consistency, scalability and resiliency
- Framework will be released as open source code with modules: user GUI, open ontology that can be used to describe utility's security policy, secure brokered remote access method, API for vendor's to use to describe device-specific configuration
- Vendor device-specific configuration modules do not need to be open source, to protect intellectual property

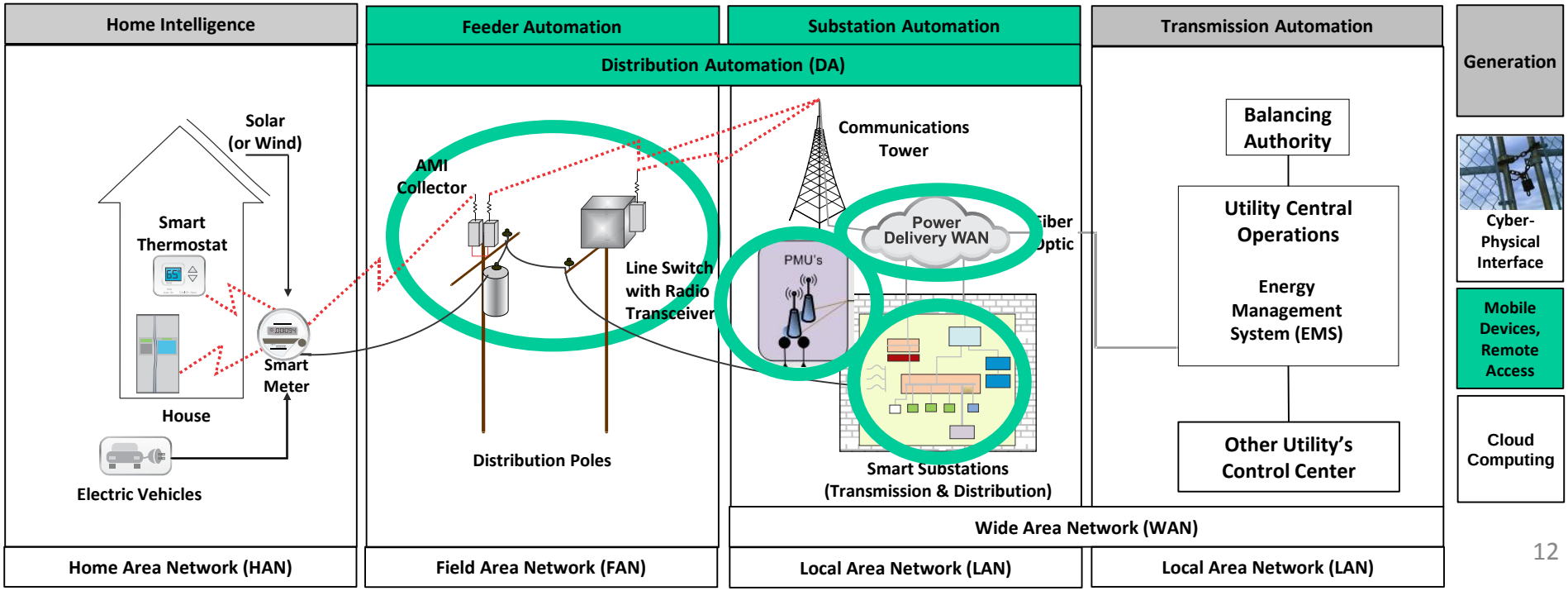
Utility-wide uniform single view and secure remote configuration of energy delivery devices, modern or legacy, of any vendor

- Centralized management supports uniform, consistent implementation of security policy and saves resources by reducing the need to visit and independently configure individual devices
- Vendor translation modules map device-specific security configuration to utility's security policy

Easier, more reliable implementation of utility's remote access security policy

- Automates conformance to, reports deviations from and enables consistent implementation of remote access security policy
- Verifies, audits and logs security configuration changes

Addresses Roadmap Milestones: *3.2, 3.3*



FOXGUARD SOLUTIONS®

Partners

Patch and Update Management Program for Energy Delivery Systems

Reduce the risk that a known vulnerability could be exploited on an energy delivery control system

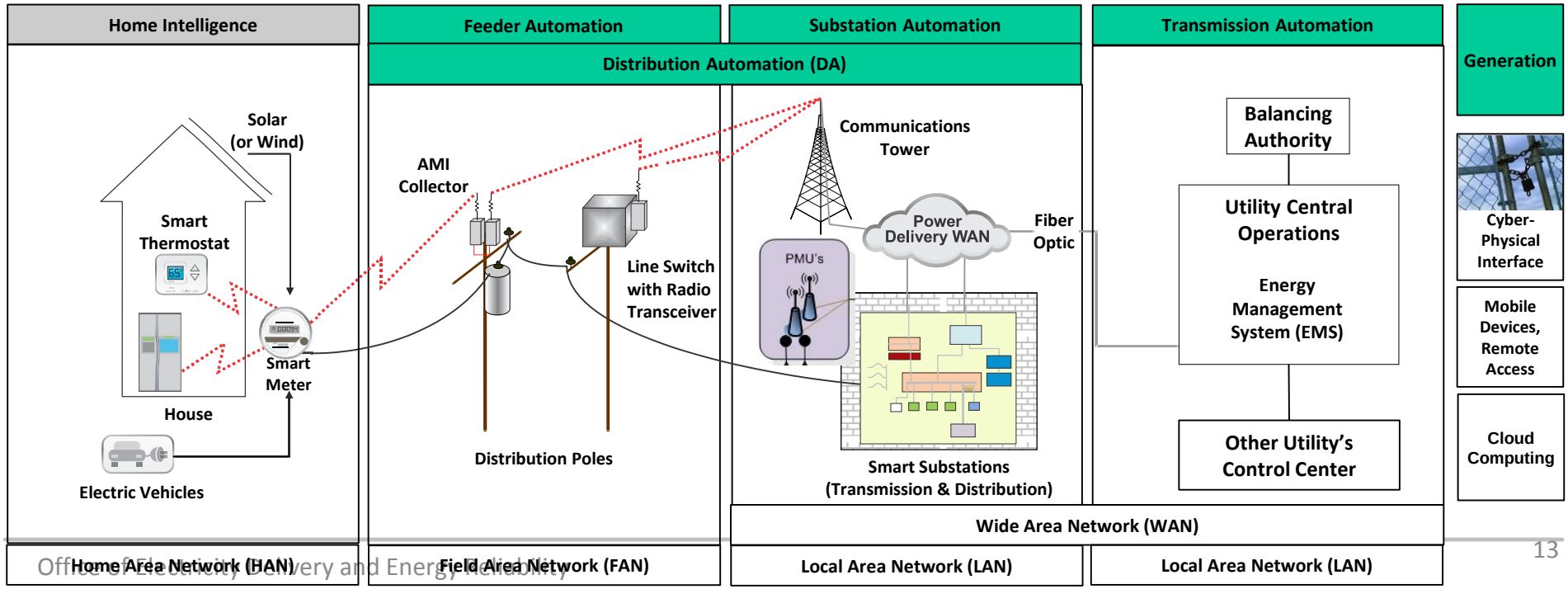
Patch and update managed service for the energy sector so the utility can more easily:

- Locate patch and update information for all delivery control systems
- Collaborate with asset owners who have similar delivery control systems
- Create and manage a patch and update program
- Validate patch or update performance so nothing unexpected happens when patch or update is deployed
- Centrally manage patch and update identification, verification and deployment
- For devices of any vendor, legacy or modern
- For energy delivery control system software, operating systems, third-party software, and device firmware
- Scan energy delivery control system to identify devices that need patches or updates
- Share hash value information for each patch and update through crowd sourcing

Reduce the risk that the patch or update itself could cause system down-time

- Work with asset owner to develop patch and update validation program, could perform patch and update performance validation using test facilities of asset owner, FoxGuard Solutions or third-party location

Addresses Roadmap Milestones: *1.3, 3.1, 5.1, 5.3*



Georgia Institute of Technology

Partners

SOUTHERN COMPANY

Virgin Islands Water and Power Authority

City of Burbank Water and Power Since 1913

ACS APPLIEDCONTROLSolutions

OISF Open Information Security Foundation

Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)

Predict in real-time how a cyber attack might disrupt energy delivery, and dynamically protect

- Faster than real-time simultaneously simulate physical power grid operations and cyber control systems
- Predict vulnerable cyber-physical states with substation-level distributed state estimation
- Generate dynamic protective rules at the local substation-level and global central control system-level
- Communicate protective rules to security sensors at the substation and central control system levels to evaluate cyber control messages in a dynamic security context

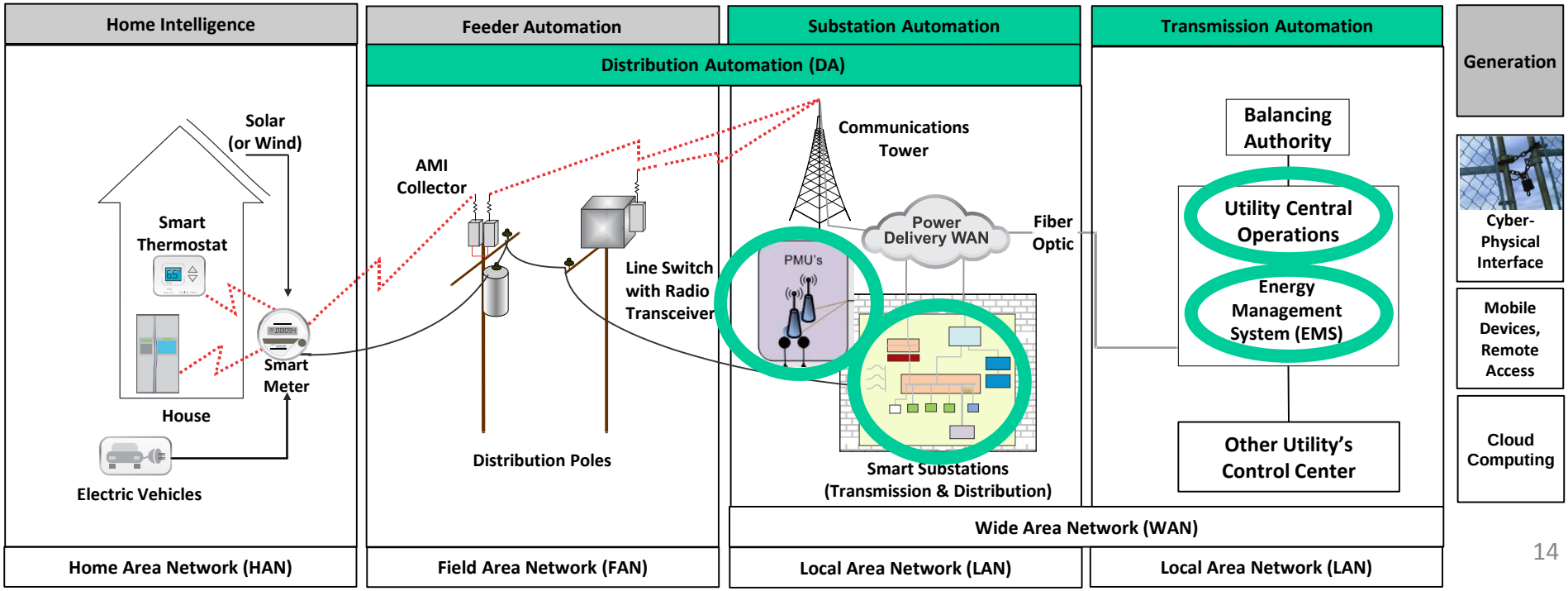
Real-time cybersecurity awareness for power grid operations

- Cyber intrusion detection and prevention that dynamically evolves with power grid operations
- Identification of cyber control actions that could alter power system components outside of dynamically varying allowed ranges
- Detection of malicious activity that plays by the rules, using allowed cyber activity, but in the wrong operational context

Cyber-physical contingency analysis

- Cyber-physical security state estimation for intrusion detection, control command validation, and control command assessment in terms of the cyber control layer and power grid operations
- Must be faster than control speed actions to not impede energy delivery control functions

Addresses Roadmap Milestones: *2.3, 3.4, 3.5, 4.1, 4.2, 4.5*



2014 Research Call National Lab R&D

Sandia National Laboratories

Artificial Diversity and Defense Security (ADDSec)

Research the transition of Software Defined Networks (SDN) from Ethernet networks into Wide Area Networks (WANs) and then focus on developing a moving-target security architecture that can be applied to existing and future control systems.

Partners: SEL Schweitzer Engineering Laboratories; Washington Gas Energy Systems; Lawrence Livermore National Laboratory; Chevron; GRIMM

OAK RIDGE National Laboratory

Timing Authentication Secured by Quantum Correlations

Leverages commercial wireless communication and Quantum Key Distribution (QKD) systems to establish a ground based wireless authenticated precise timing distribution system. Will develop and demonstrate a system of ground-based authenticated precise timing and communications beacons featuring security that is enhanced by the fundamental laws of physics.

Partners: PG&E; The University of Texas at Austin; Sandia National Laboratories; ubitekk

---

Argonne NATIONAL LABORATORY

A Resilient Self--Healing Cyber Security Framework for Power Grid

Develop an attack-resilient Wide Area Monitoring Protection and Control (WAMPAC) framework, with associated computational algorithms and software tools, to prevent and mitigate cyber-attacks and improve resilience of the bulk power system.

Partners: Pacific Northwest National Laboratory; RTDS Technologies; Iowa State; Illinois Institute of Technology; OPAL-RT

Pacific Northwest NATIONAL LABORATORY

Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity

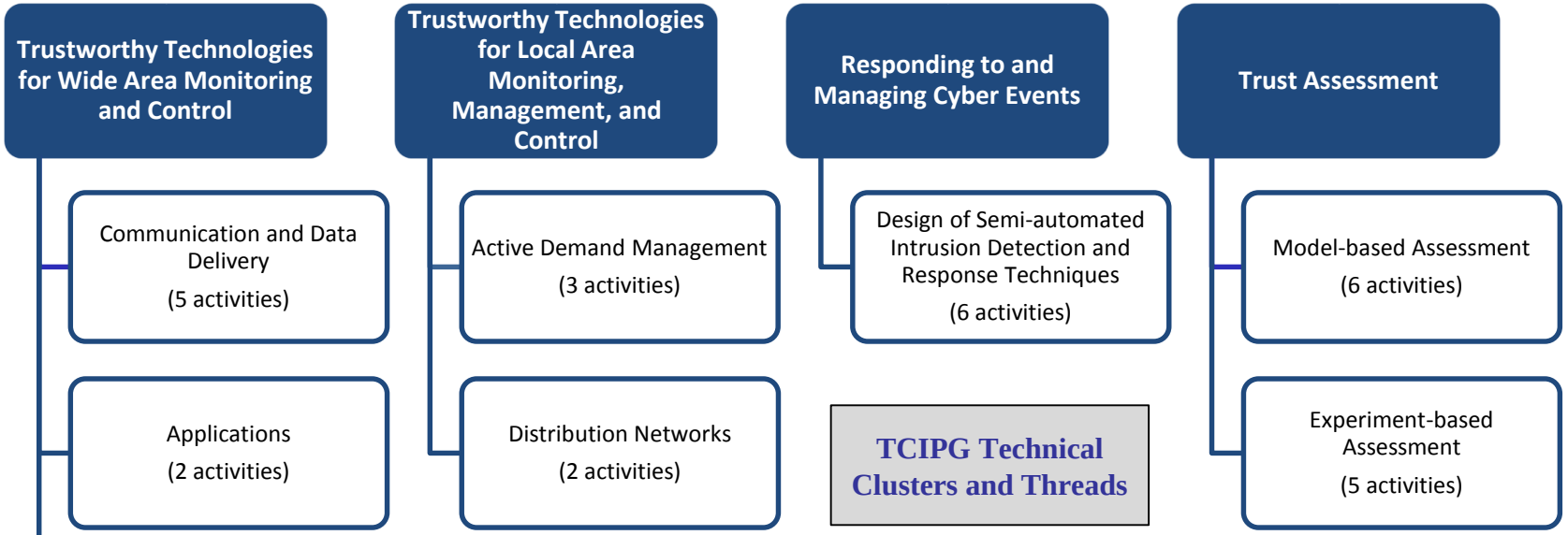
Conduct a cognitive systems engineering assessment of operator workflow, the data and information associated with the work, and the decisions, actions, and goals of operators to develop visualizations that power system operators can use to improve situational awareness during unfolding events.

Partners: INL Idaho National Laboratory; PG&E; ALSTOM

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

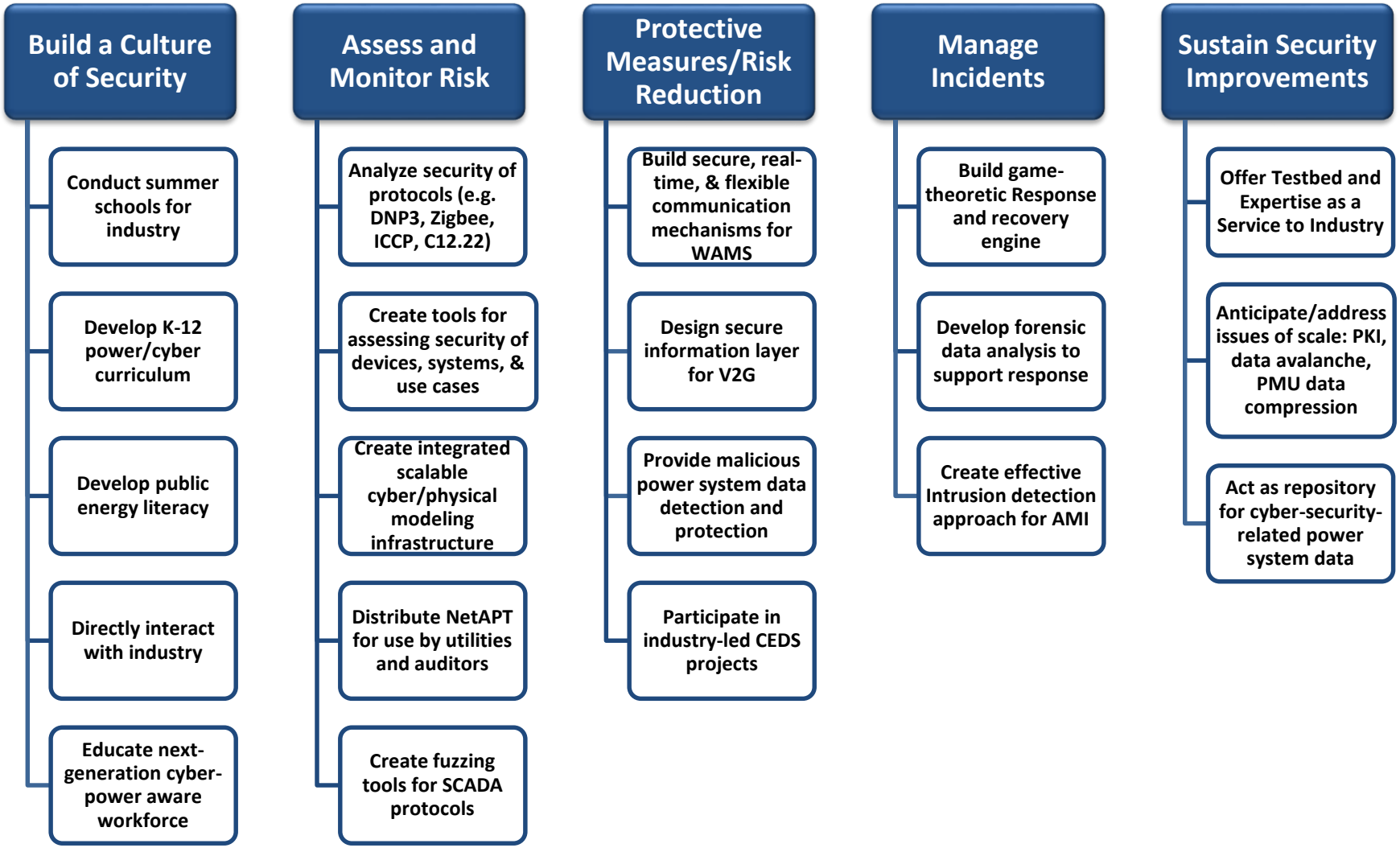
Facilities

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

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

TCIPG Impacts all aspects of the *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*

TCIPG Efforts



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)

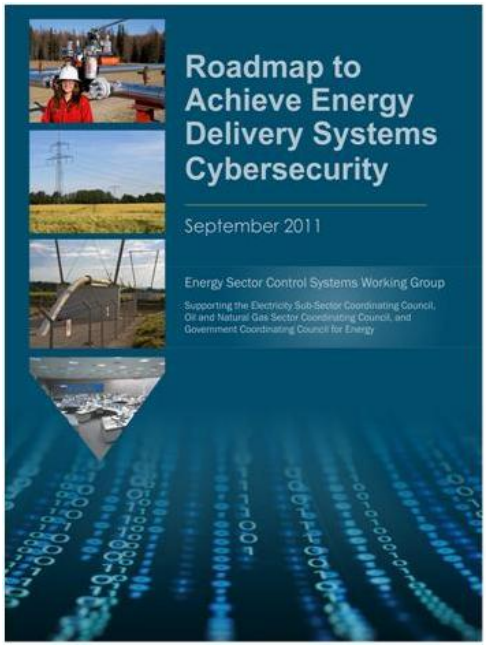
For More Information, Please Contact:

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

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

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

David Howard
David.Howard@hq.doe.gov
202-586-6460



Visit:

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

www.controlsystemsroadmap.net