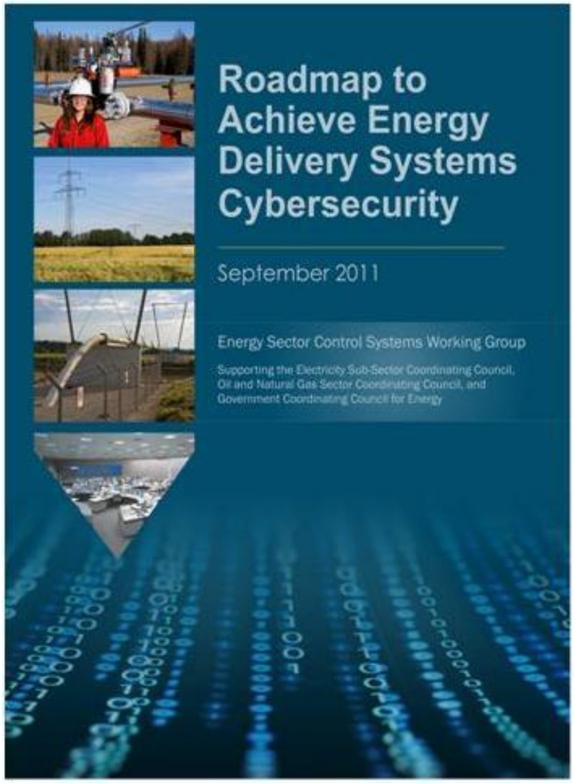
Cybersecurity for Energy Delivery Systems (CEDS) R&D

Following the Energy Sector's Roadmap



Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

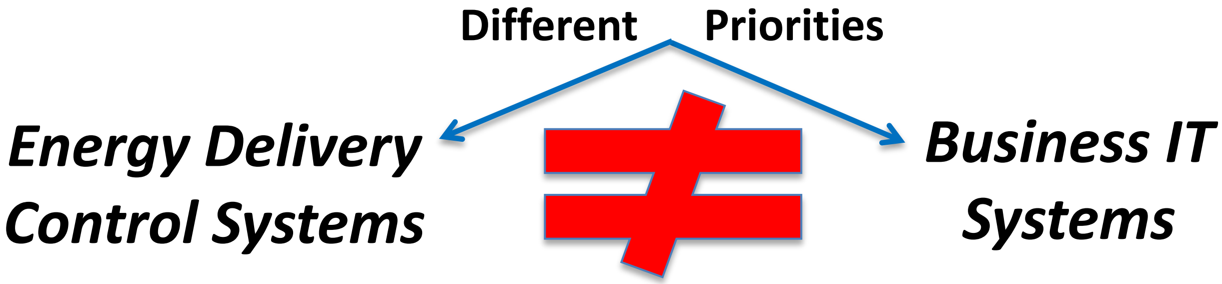
Energy Sector Control Systems Working Group

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

Carol Hawk
CEDS R&D Program Manager

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

Energy Sector Cybersecurity

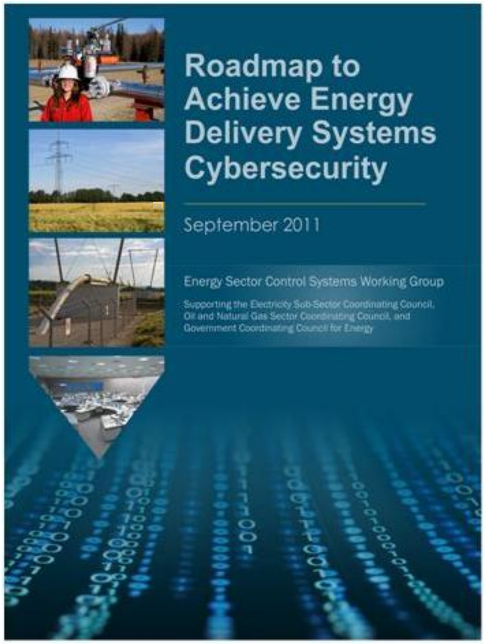


Different Priorities

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

- 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



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

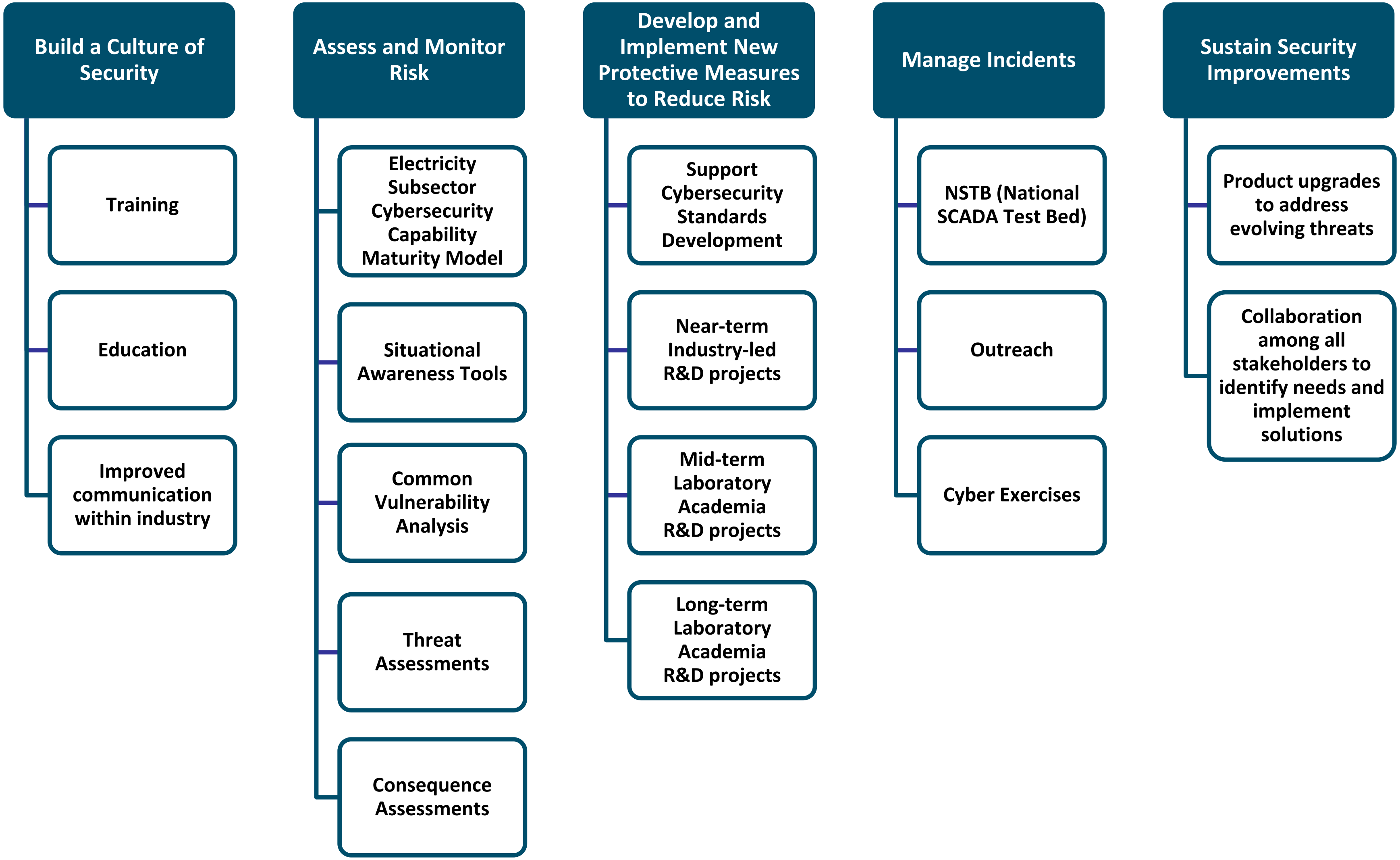
- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

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



Build a Culture of Security

- Training
- Education
- Improved communication within industry

Assess and Monitor Risk

- Electricity Subsector Cybersecurity Capability Maturity Model
- Situational Awareness Tools
- Common Vulnerability Analysis
- Threat Assessments
- Consequence Assessments

Develop and Implement New Protective Measures to Reduce Risk

- Support Cybersecurity Standards Development
- Near-term Industry-led R&D projects
- Mid-term Laboratory Academia R&D projects
- Long-term Laboratory Academia R&D projects

Manage Incidents

- NSTB (National SCADA Test Bed)
- Outreach
- Cyber Exercises

Sustain Security Improvements

- Product upgrades to address evolving threats
- Collaboration among all stakeholders to identify needs and implement solutions

CEDS Alignment with the Roadmap

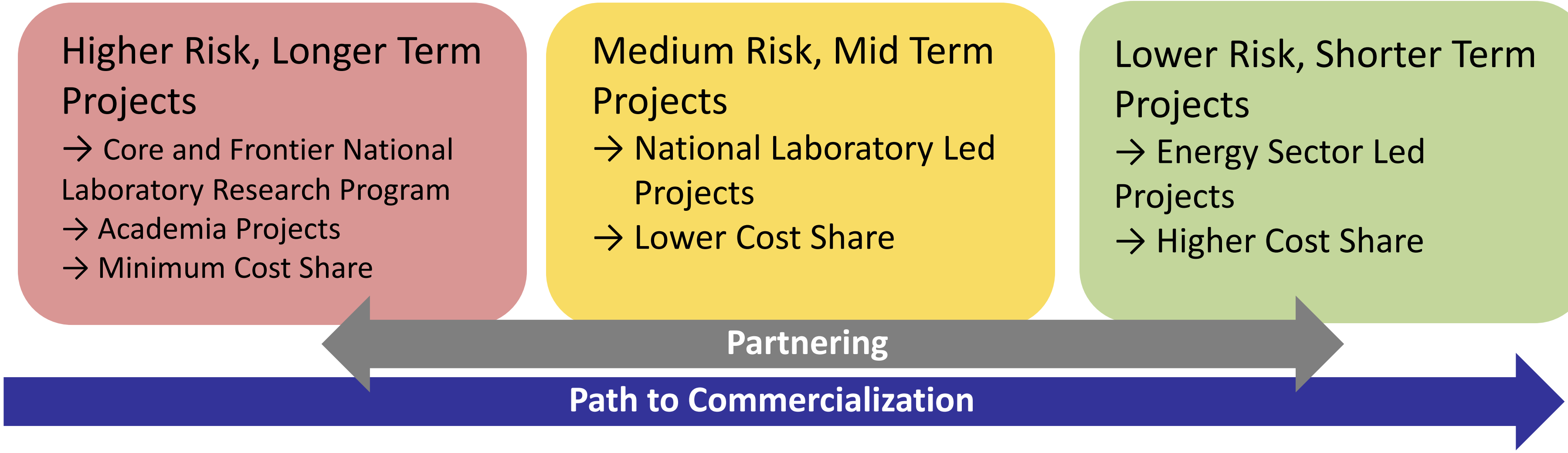
CEDS provides ***Federal funding*** to:

- 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



Higher Risk, Longer Term Projects

→ Core and Frontier National Laboratory Research Program

→ Academia Projects

→ Minimum Cost Share

Medium Risk, Mid Term Projects

→ National Laboratory Led Projects

→ Lower Cost Share

Lower Risk, Shorter Term Projects

→ Energy Sector Led Projects

→ Higher Cost Share

Partnering

Path to Commercialization

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

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

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

<u>Open Source Solution</u>

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

<u>Commercial Product</u>

Schweitzer Engineering Laboratories Ethernet Security Gateway SEL-3620 implements Lemnos

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

Project Lead

Project Partnerships

Project Title

Project: short description (summary)

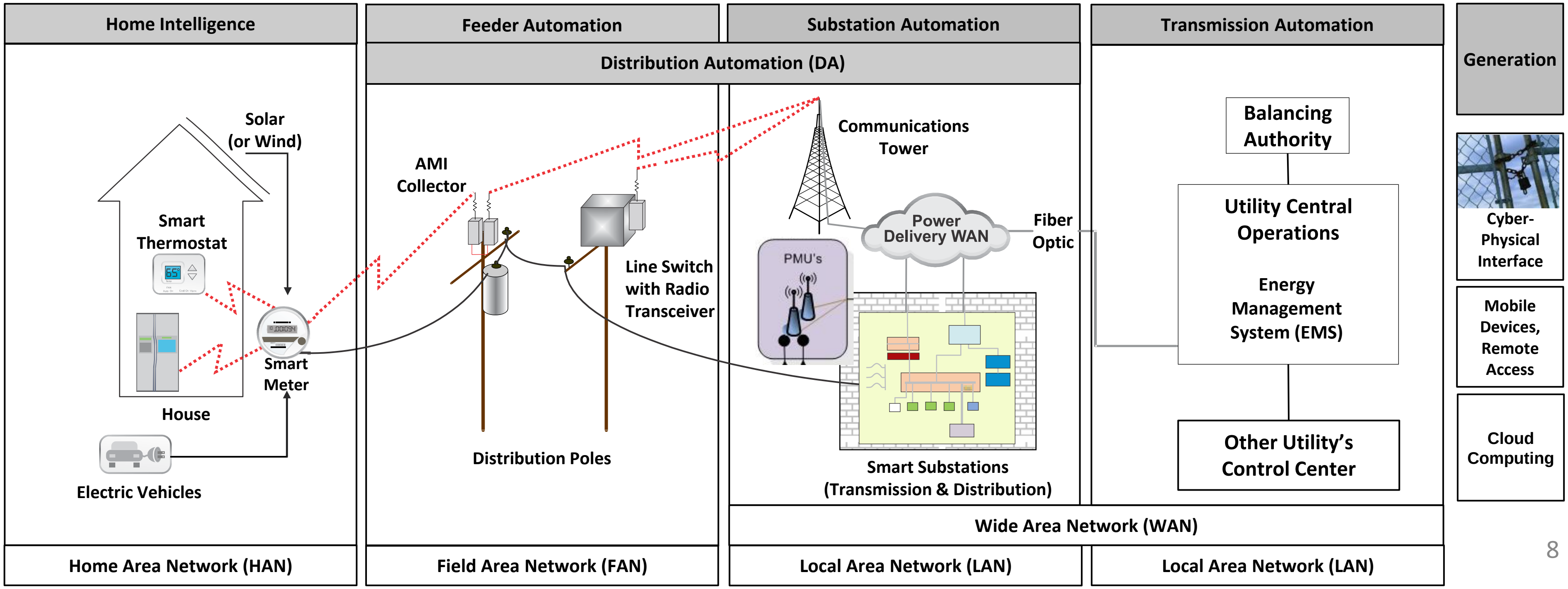
Cyber summary:

- 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)*



Home Intelligence

Feeder Automation

Substation Automation

Distribution Automation (DA)

Transmission Automation

Generation

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU's

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

Local Area Network (LAN)

Partners

Secure Information Exchange Gateway (SIEGate)

Flexible, real-time, reliable and secure information exchange for electric grid operations

- Consolidates data exchange to reduce the external attack surface and costs of maintaining multiple data exchange systems
- Provides a high-performance, low latency solution to securing data communication between control centers

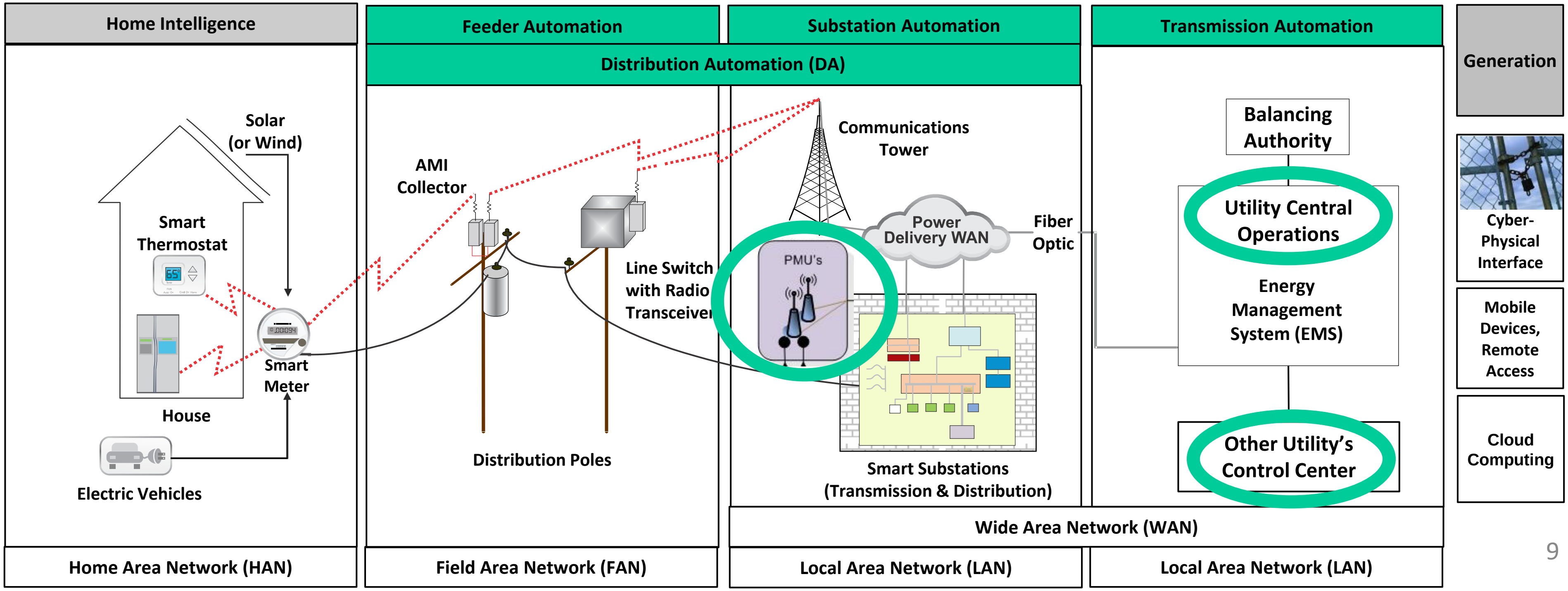
Builds upon the open source phasor gateway

- Provides a gateway for sharing increasingly high volumes of high-frequency, real-time data, such as phasor data, in a secure and timely manner with significantly greater functionality and cybersecurity capabilities
- Reduces cost and management overhead by maintaining and managing a single gateway

Current status/Project successes

- Pre-production version installed at several utilities
- Demonstrated capability to transfer large data streams between two major utilities

Addresses Roadmap Milestone: *3.3*



Home Intelligence

Feeder Automation

Substation Automation

Transmission Automation

Distribution Automation (DA)

Generation

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU's

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

Local Area Network (LAN)

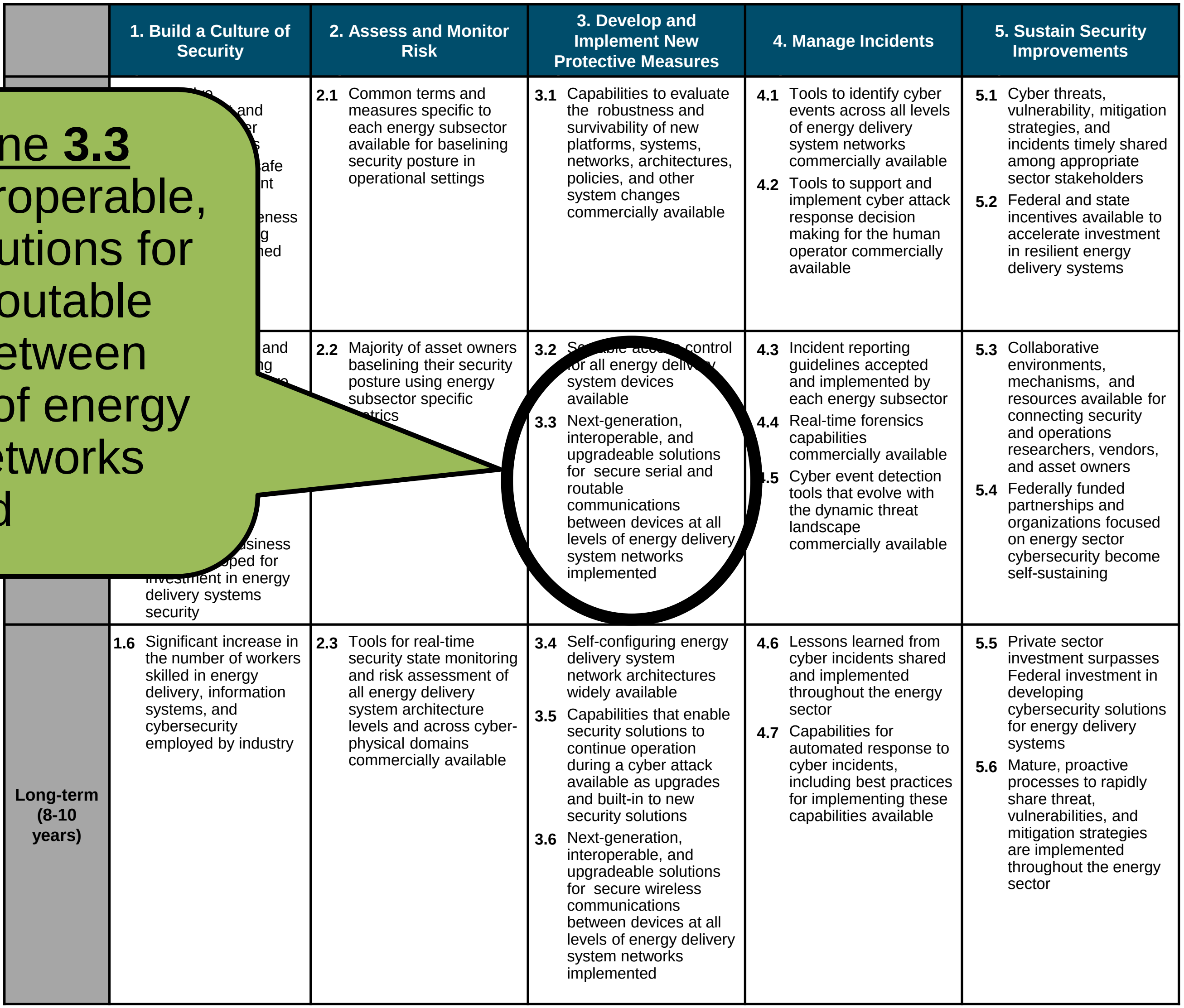
CEDS Alignment with the Roadmap

CEDS provides

To accelerate cybersecurity investment and adoption of resilient energy delivery systems

<u>Roadmap Milestone **3.3**</u>

Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented



	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
	[illegible] and [illegible] er [illegible] s [illegible] afe [illegible] nt [illegible] eness [illegible] g [illegible] ned	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
	[illegible] and [illegible] ng [illegible] siness [illegible] oped 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

SEL SCHWEITZER ENGINEERING LABORATORIES

Partners: Sandia National Laboratories, TVA

Padlock Security Gateway

Greater situational awareness and incident response capabilities for field devices

- Low power, low cost gateway with strong access control and password management
- Enhances cybersecurity of distribution automation system and communication field devices
- Builds upon Lemnos interoperability configuration profiles

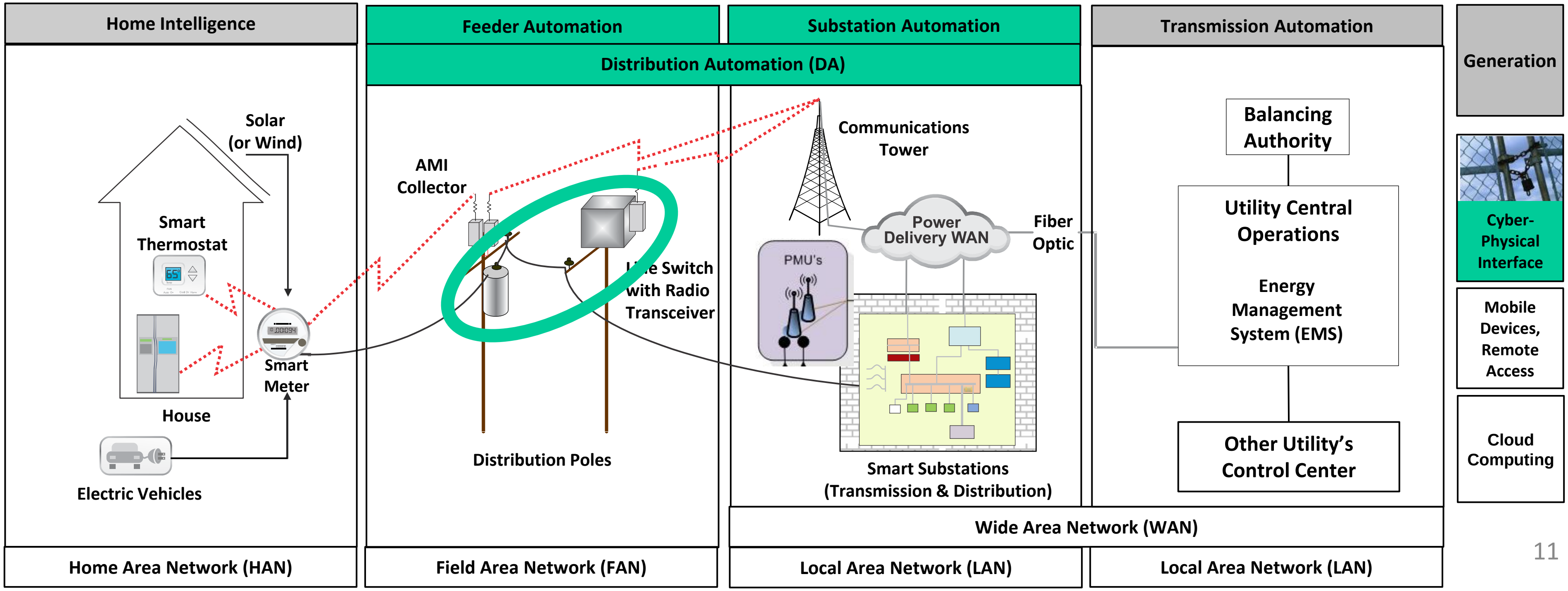
Bridges cyber and physical security

- Senses physical tampering to field devices and takes cyber actions to prevent escalation of intrusions
- Monitoring capabilities and near real-time logging of cyber and physical events

Current status/Project successes

- Accelerated release of hardware with security gateway features in 2012 due to consumer demand
- Thousands sold and protecting the Nation’s energy infrastructure today
- Sensing and notification of physical tampering firmware update coming in 2014

Addresses Roadmap Milestone: *3.2, 3.3, 4.1*



Home Intelligence

Feeder Automation

Substation Automation

Distribution Automation (DA)

Transmission Automation

Generation

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU’s

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility’s Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

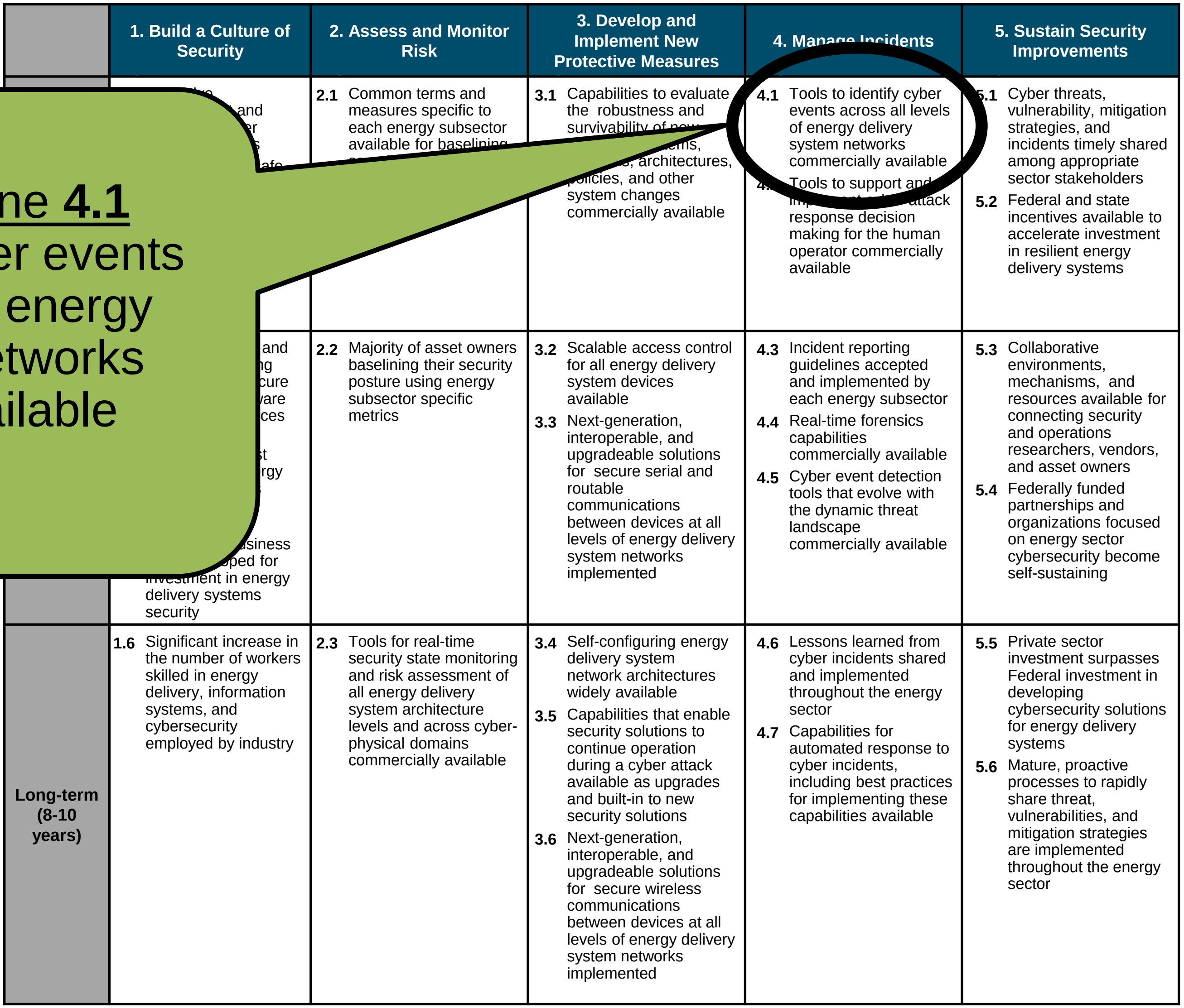
Local Area Network (LAN)

CEDS Alignment with the Roadmap

CEDS provides

<u>Roadmap Milestone **4.1**</u>
Tools to identify cyber events across all levels of energy delivery system networks commercially available

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
	...ive ...t and ...er ...s ...afe	**2.1** Common terms and measures specific to each energy subsector available for baselining	**3.1** Capabilities to evaluate the robustness and survivability of new ...ems, ...s, 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.** Tools to support and ... 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
	... and ...ng ...cure ...ware ...ces ...st ...rgy ...usiness ...oped 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

SEL SCHWEITZER ENGINEERING LABORATORIES

Partners

TVA

Sandia National Laboratories

Alliance Projects

Unified central control of both cyber and physical access to energy sector buildings and cyber assets

- Proximity card reader and controller that integrates with existing Lemnos and Padlock cybersecurity system and unifies trust management, logging and administrative activities for both physical and cyber security
- Uses Active Directory for system wide physical and cyber access for immediate change control and ease of administration
- Will implement Alliance in Lemnos conforming Secure Ethernet Gateway (SEL-3620) and Padlock (SEL-3622)

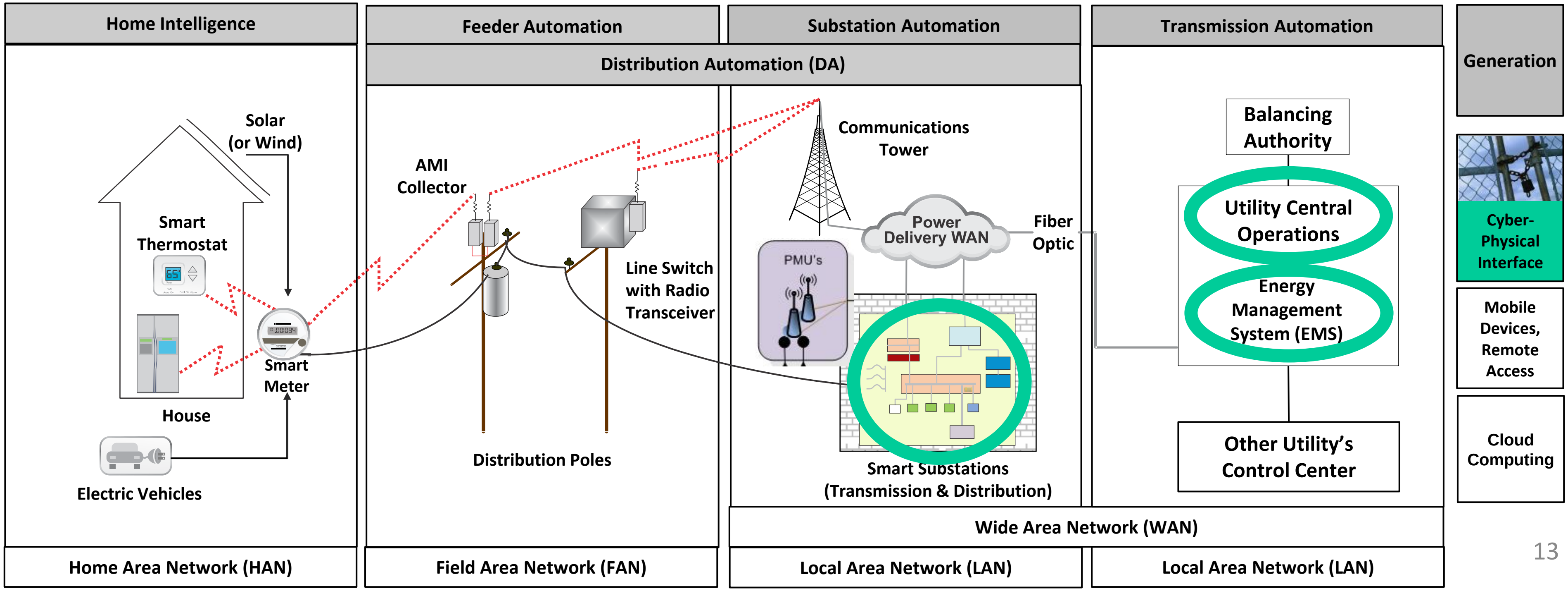
Single, unified cyber-physical trust management

- Unifies trust, logging and log management for physical and cyber access which facilitates compliance and incident response
- Enables operators to have better awareness of the system state; and the audit trail of who's where, when and what they are doing becomes clear with no additional administrative overhead
- Scale principle of least privileges to physical-cyber systems
- Lowers cost, simplifies training, eases and enhances reliability of access control administration
- The 2nd factor used in two-factor authentication for physical access is the same as cyber access, like your RSA token

Tailored trust: protect cyber-physical systems with physical-cybersecurity

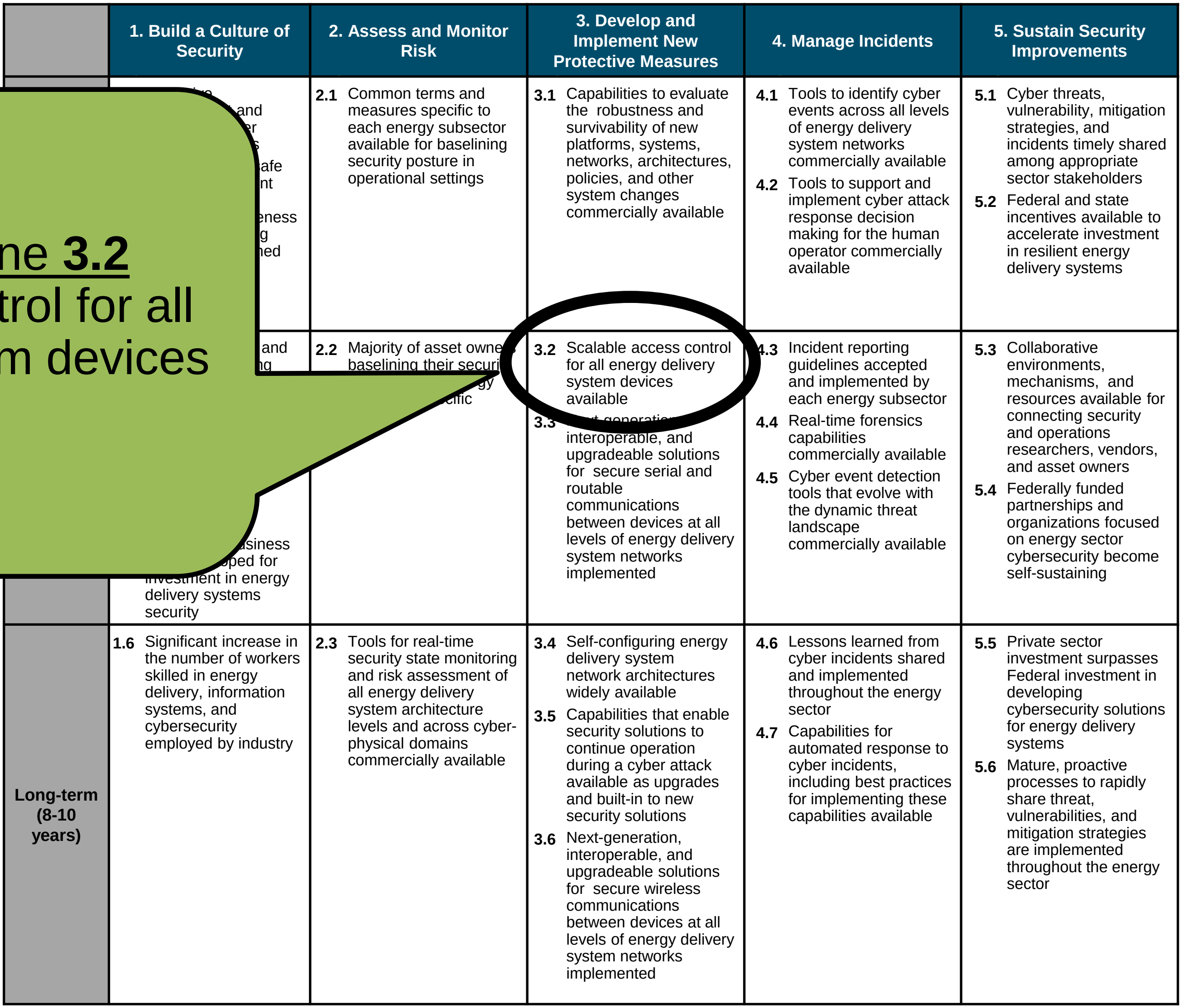
- Physical security that is aware of cybersecurity
- Cybersecurity that is aware of physical security
- High fidelity of cyber-physical access control – down to rack level

Addresses Roadmap Milestones: *3.2*



CEDS Alignment with the Roadmap

CEDS provides



	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
	and r s afe nt eness g ned	**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
	and ng siness oped for investment in energy delivery systems security	**2.2** Majority of asset owne baselining their securi gy cific	**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

<u>Roadmap Milestone **3.2**</u>
Scalable access control for all energy delivery system devices available

To accelerate cybersecurity investment and adoption of resilient energy delivery systems

APPLIED COMMUNICATION SCIENCES

Partners

SMUD SACRAMENTO MUNICIPAL UTILITY DISTRICT The Power To Do More.®

Cybersecurity Intrusion Detection and Monitoring for Field Area Networks

Smart Meter and Distribution Automation wireless communications security

- Anomaly and intrusion detection for advanced metering infrastructure and Distribution Automation wireless mesh networks
- Improves situational awareness , helps validate over-the-air security controls, mitigates supply chain cyber threats
- R&D advanced cyber intrusion detection analytics in the ACS SecureSmart managed security service for energy utilities

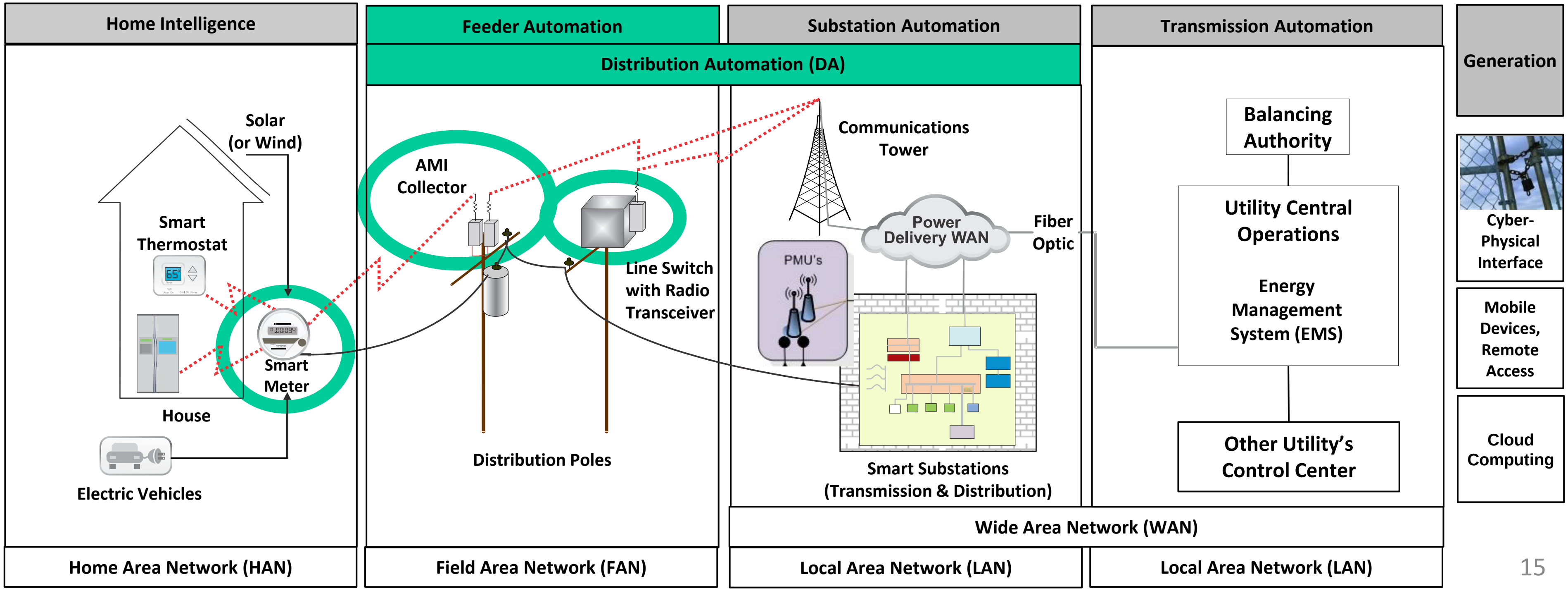
Visualize and analyze Smart Meter and Distribution Automation wireless communications

- Visibility beyond the wireless gateway into the self-forming mesh network
- Traffic analysis to characterize expected behavior of Smart Meter and Distribution Automation wireless mesh network traffic
- Traffic modeling, health indicators and operational baselines to detect departure from expected behavior
- Real-time monitoring of traffic flows and mesh network performance

Real-time Smart Meter and Distribution Automation anomaly and intrusion detection

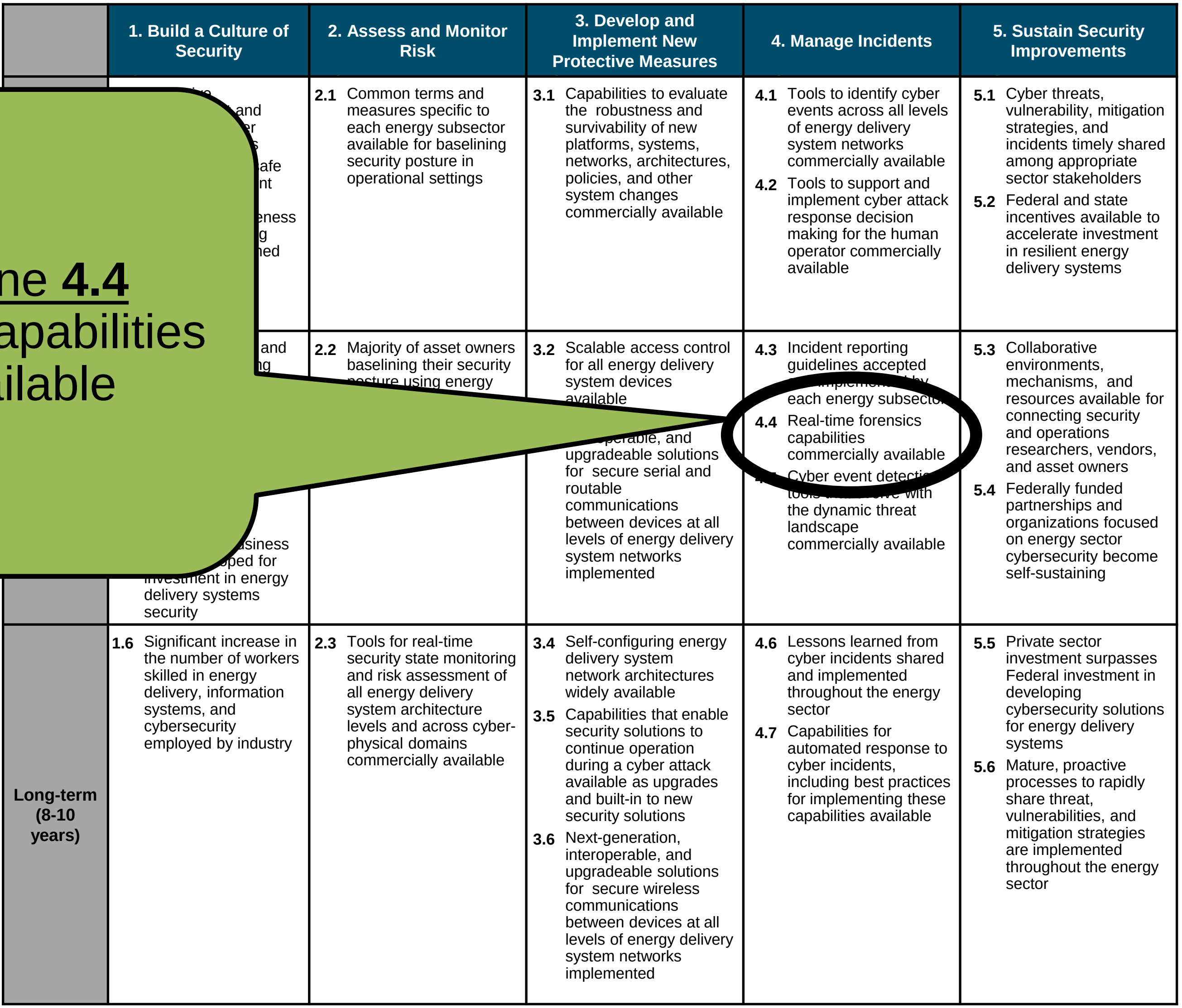
- Develop traffic analysis techniques to detect anomalies and malicious activity in Smart Meter and Distribution Automation wireless communications
- Abstract operationally meaningful network and node behavior from traffic analysis
- Find out how vulnerabilities in embedded hardware, firmware and software manifest in traffic analysis to detect exploitation attempts

Addresses Roadmap Milestones: *2.3, 3.6, 4.1, 4.2, 4.4, 4.5*



CEDS Alignment with the Roadmap

CEDS provides



	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
	ive t and er s afe nt eness g ned	**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
	and ng usiness oped for investment in energy delivery systems security	**2.2** Majority of asset owners baselining their security posture using energy	**3.2** Scalable access control for all energy delivery system devices available operable, 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 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

<u>Roadmap Milestone **4.4**</u>
Real-time forensics capabilities commercially available

To accelerate cybersecurity investment and adoption of resilient energy delivery systems

Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks

ABB Power and productivity for a better world™

Partners

TVA

ILLINOIS

Don't allow cyber activity that could jeopardize grid operations

- Protection and control devices, between and within substations, reach collaborative consensus to verify that a received input makes sense in the current operational state of the power grid
- R&D IEC 61850 distributed security extensions for collaborative defense, encourage vendor-neutral adoption and offer in firmware of ABB protection and control devices

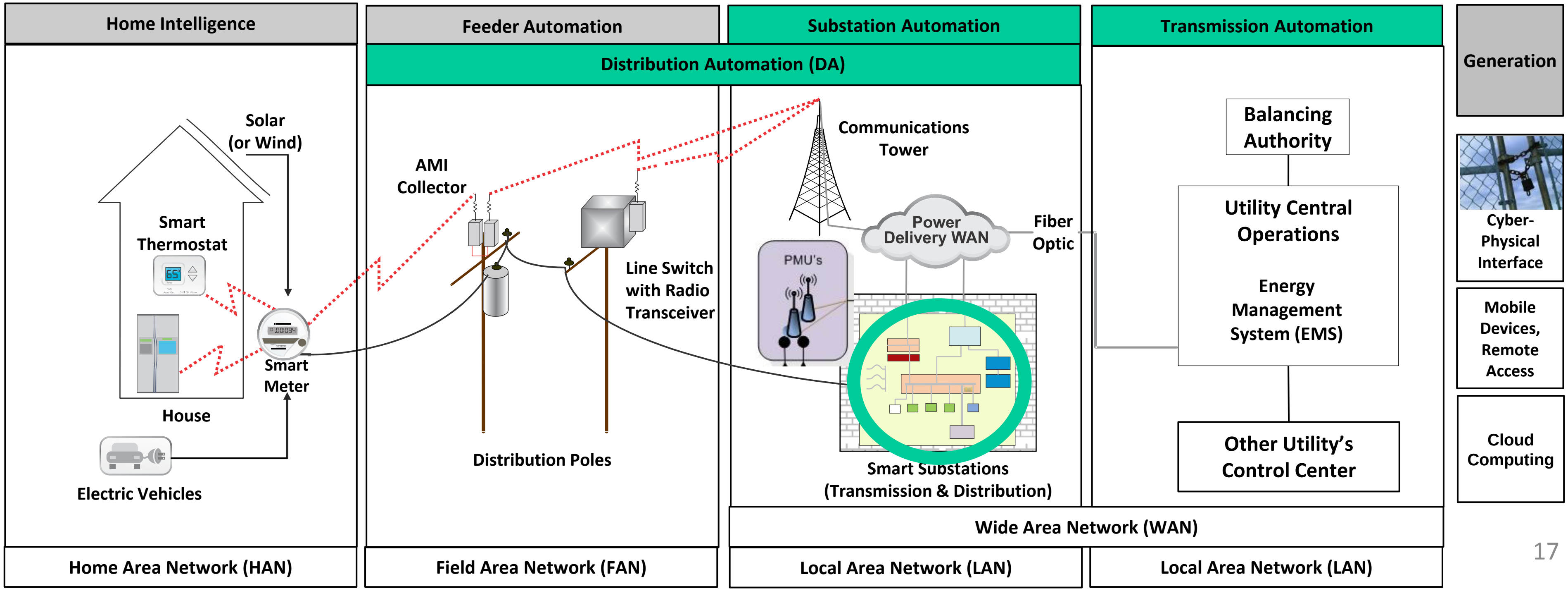
Real-time cybersecurity that is aware of power grid operations

- Detect malicious commands, even those that comply with expected syntax, protocol and device function, that if acted on could jeopardize power grid operations
- Detect insider attacks, spoofed power system data, malicious commands or configuration set points by anticipating their effect on power grid operations
- Block incorrect device function and report compromised device

Power grid devices work together to validate commands

- IEC 61850 distributed security extensions enable protection and control relays to collaboratively validate that inputs, configuration changes or power system data, make sense for reliable grid operations
- Fast, inter-device cross-checking framework completes collaborative validation as fast as the response time of the protection device so as to not impede protection and control function

Addresses Roadmap Milestones: *2.3, 3.5, 4.1, 4.2, 4.5, 4.7*



Home Intelligence

Feeder Automation

Substation Automation

Transmission Automation

Distribution Automation (DA)

Generation

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU's

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

Local Area Network (LAN)

CEDS Alignment with the Roadmap

CEDS provides

Roadmap Milestone 4.2
Tools to support and implement cyber attack response decision making for the human operator commercially available

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
	ive and er s afe	**2.1** Common terms and measures specific to each energy subsector available for baselining security posture in	**3.1** Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other ercially available	**4.1** Tools to identify cyber events across all levels of 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
	and ng cure vare ces st rgy siness oped 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

Georgia Institute of Technology

Partners: Southern Company; Virgin Islands Water and Power Authority; City of Burbank Water and Power; ACS Applied Control Solutions; 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

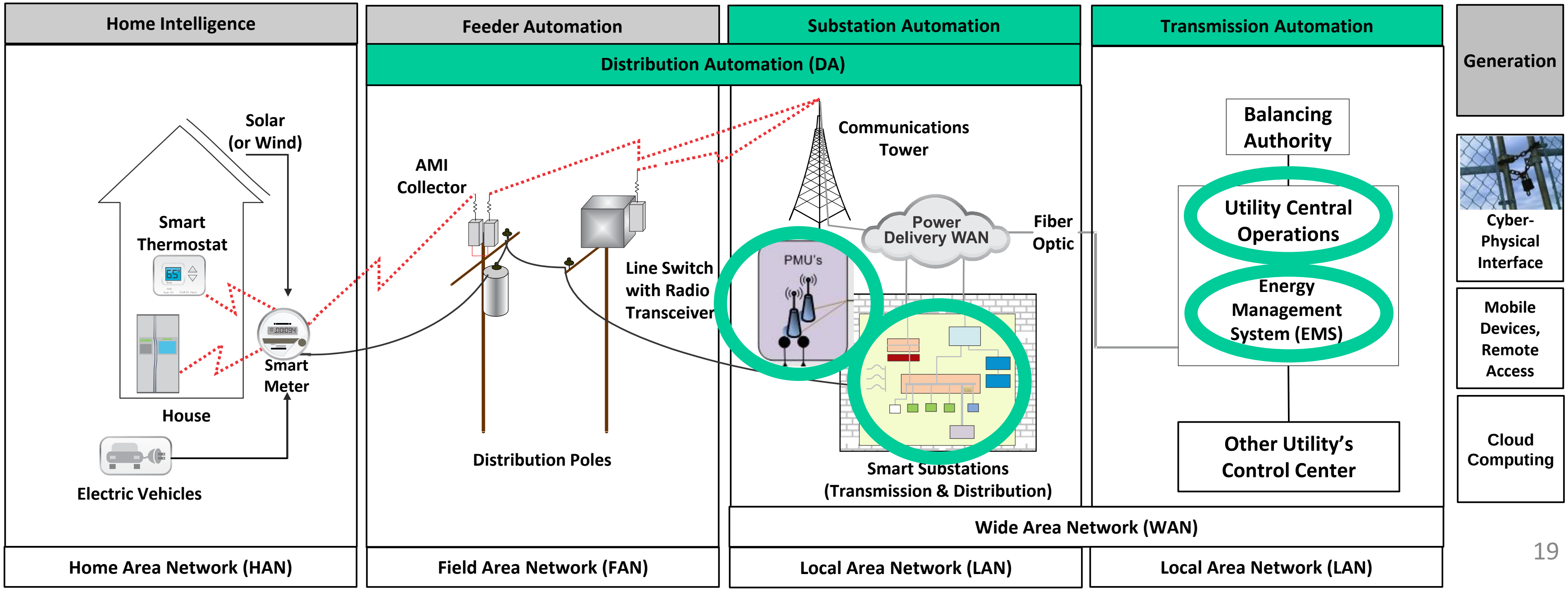
Real-time cybersecurity awareness for power grid operations

- 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*

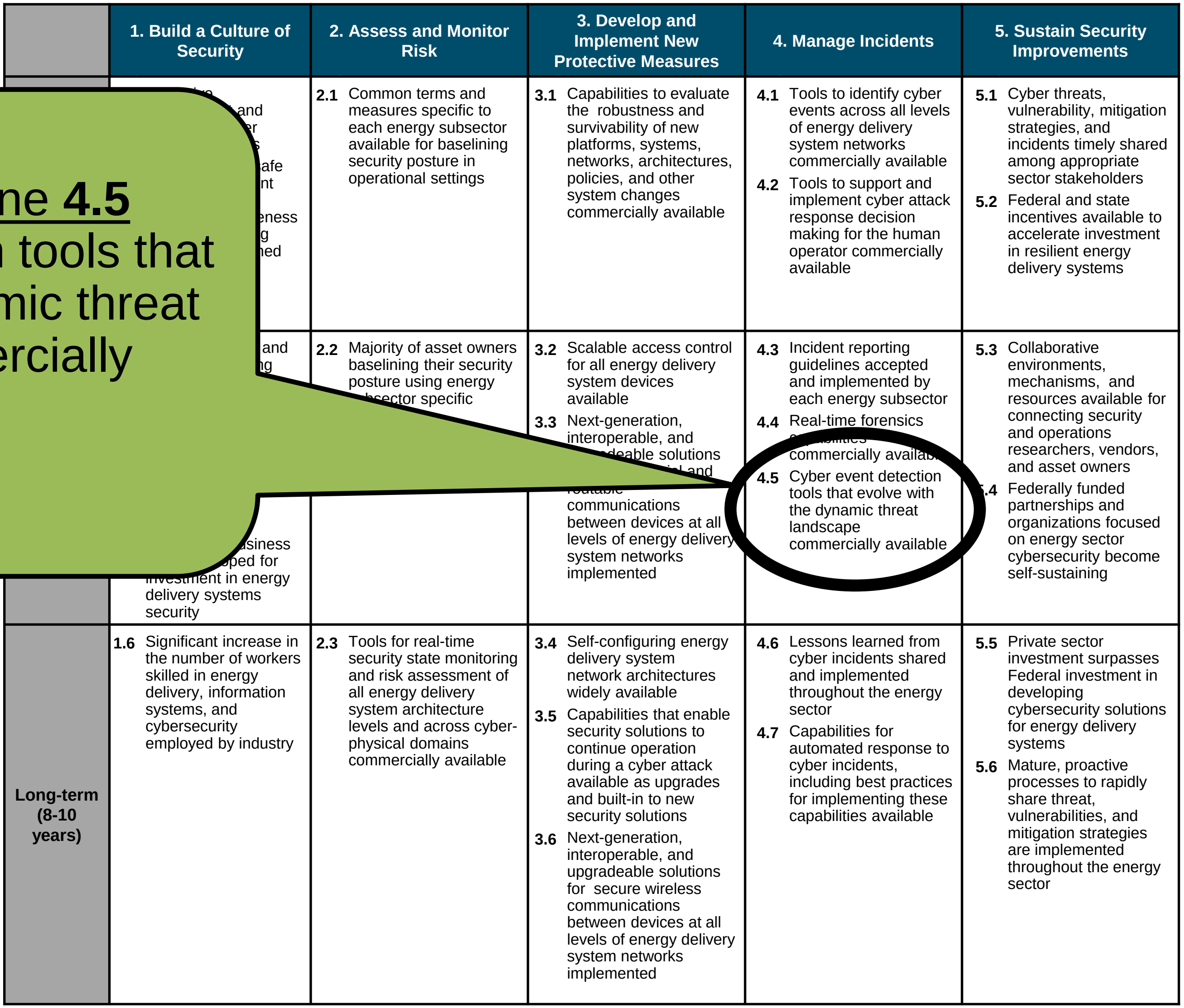


CEDS Alignment with the Roadmap

CEDS provides

Roadmap Milestone **4.5**
Cyber event detection tools that evolve with the dynamic threat landscape commercially available

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
	…and …er …s …afe …nt …eness …g …hed	**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
	…and …ng …siness …oped for investment in energy delivery systems security	**2.2** Majority of asset owners baselining their security posture using energy …bsector specific	**3.2** Scalable access control for all energy delivery system devices available **3.3** Next-generation, interoperable, and …deable solutions …ial 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 ca…bilities commercially availab… **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

Argonne NATIONAL LABORATORY

Partners

Pacific Northwest NATIONAL LABORATORY

ILLINOIS INSTITUTE OF TECHNOLOGY 1890

STATE

OPAL-RT

RTDS Technologies

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

Attack-resilient Wide-Area Monitoring, Protection, and Control (WAMPAC) framework

- Development of a self-healing Phasor Measurement Unit (PMU) network infrastructure through a risk mitigation model
- Development of bad data detection and attack-resiliency methods for the State Estimation (SE) algorithm
- Development of anomaly detection and attack-resilient control methods

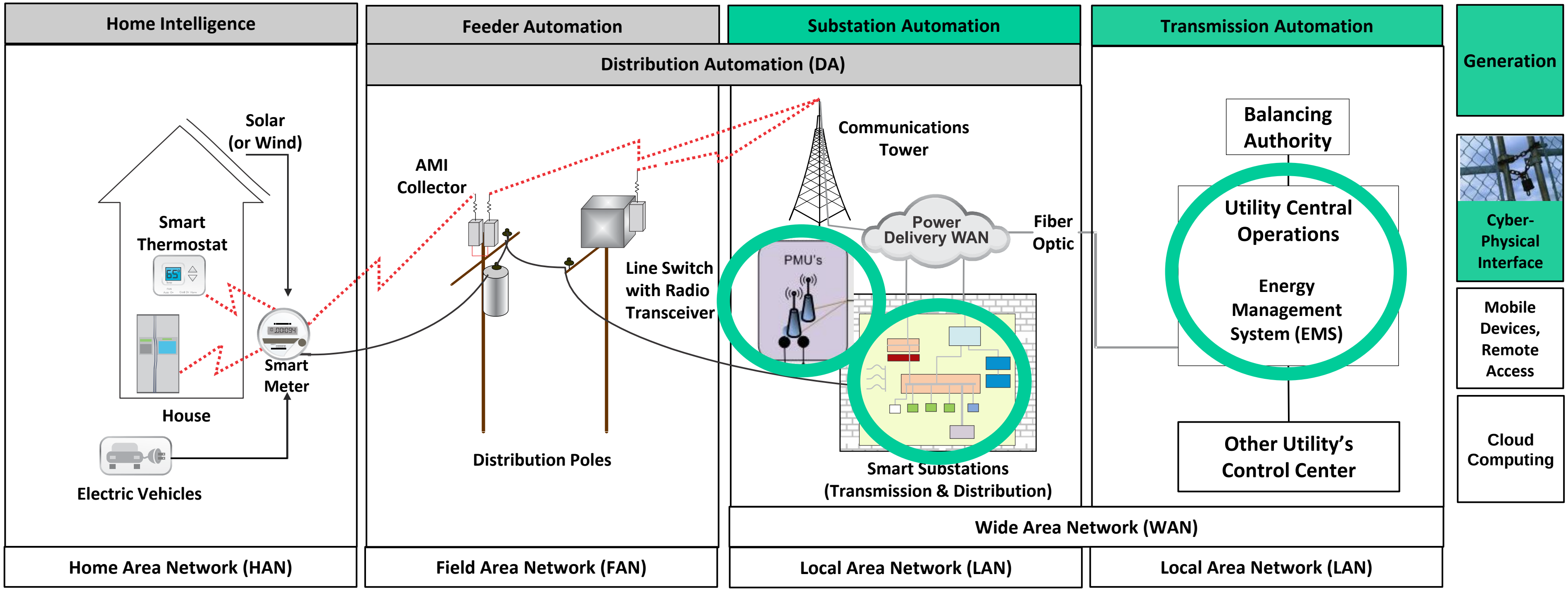
Mitigation and prevention of cyber attacks

- PMU risk mitigation model employs optimal response to cyber-attacks with the goal of preventing the propagation of the attacks and maintaining the observability of the power system
- SE algorithm encompasses stealthy attack vector formulations, attack impact analysis, and Moving Target Defense (MTD) strategies to mitigate sophisticated cyber-attacks

Comprehensive anomaly detection, control, and resilience methods

- Model-based control algorithms leveraging Cyber Physical System (CPS) properties
- Wide-area protection schemes that include the design of a hierarchical model-based MTD-inspired protection algorithm leveraging spatial-temporal properties of device/system operation
- Model-based anomaly detection methods for the Optimal Power Flow (OPF) algorithm though the use of Principal Component Analysis (PCA)

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



Home Intelligence

Feeder Automation

Substation Automation

Transmission Automation

Generation

Distribution Automation (DA)

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU's

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

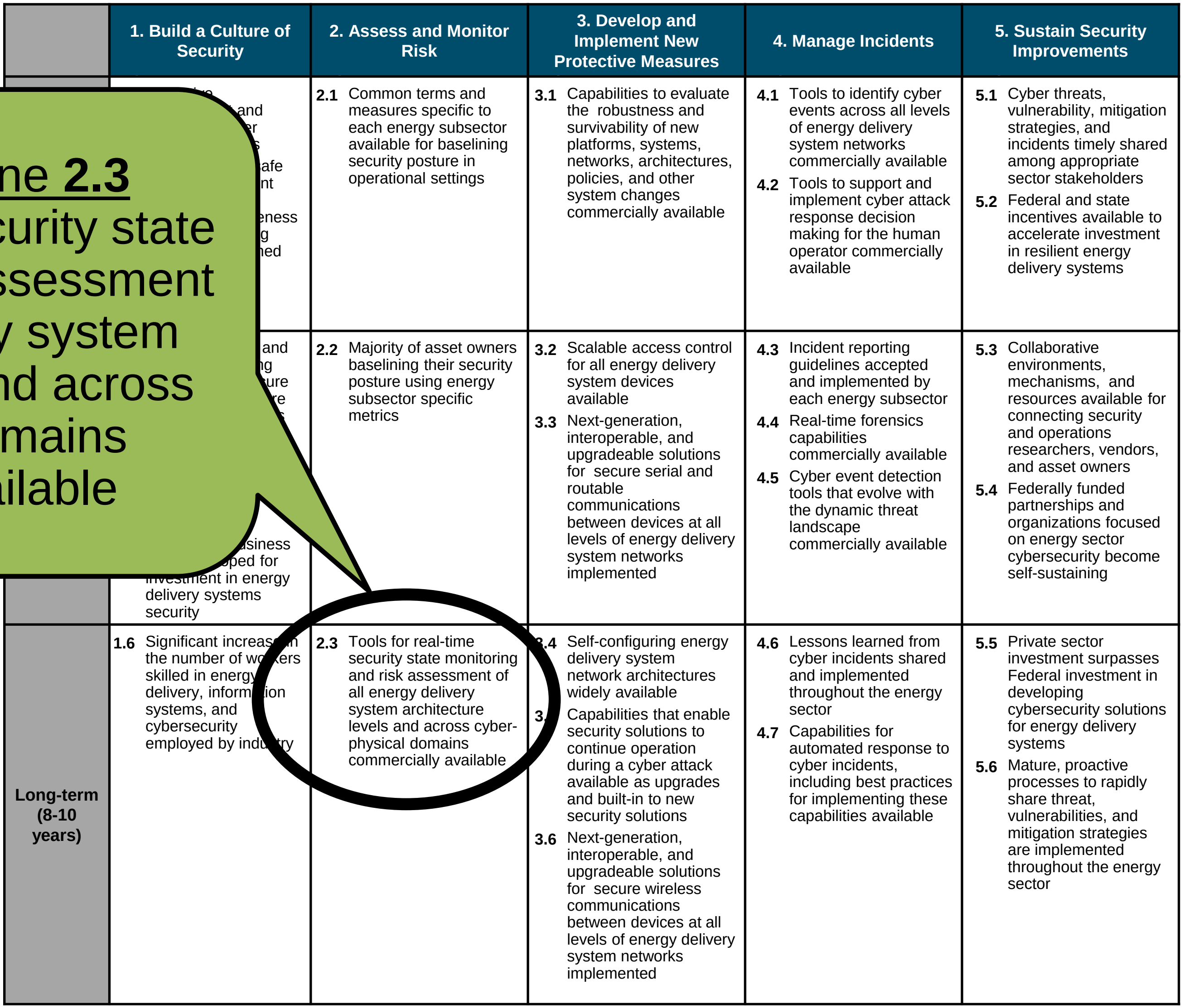
Local Area Network (LAN)

CEDS Alignment with the Roadmap

CEDS provides

<u>Roadmap Milestone **2.3**</u>
Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available

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
[illegible]	[illegible]	**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
[illegible]	[illegible] 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

Pacific Northwest NATIONAL LABORATORY

Partners

INL Idaho National Laboratory

PG&E

ALSTOM

Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals

Visualizations for efficient situational awareness and assessment

- Employ cognitive systems engineering methods to gain understanding of the work and data/information needs of cybersecurity professionals at utilities
- Integrate the necessary data and information from various systems that are relevant to a particular context
- Develop tools that present the information to operators in an intuitive and efficient fashion

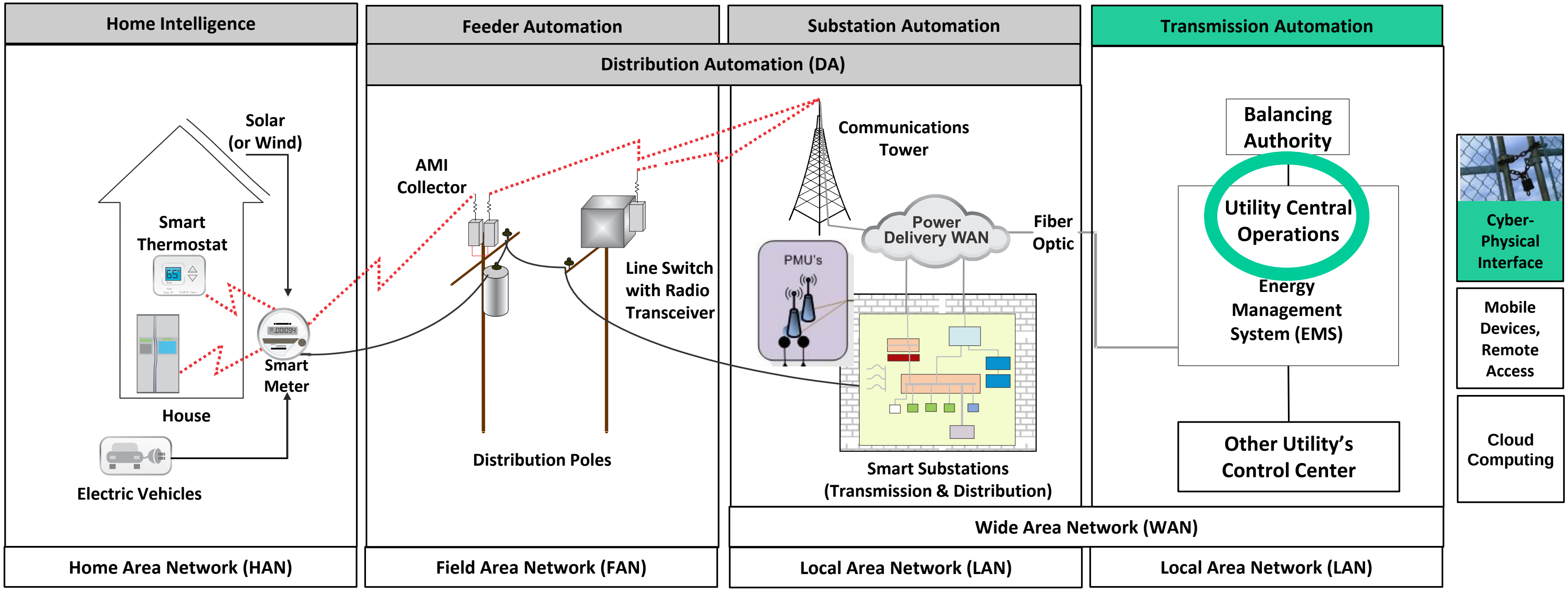
Visualization and decision support tools for faster response

- Reduces the cognitive demand on operators to enable enhanced, real-time awareness and problem solving capabilities
- Enables more effective coping with the increasing complexity of grid and cybersecurity operations
- Mitigates the impact of data overload on operator decision making by allowing operators to quickly focus attention on relevant contextual information

Extensible and integrated approach

- Allows other sources/inputs to be adapted based on local sources available
- Possibility for research results to be widely used by utilities, regardless of the vendors chosen in their existing systems
- Incorporates smart grid-wide set of inputs (e.g., communications, cybersecurity, power system) that may allow business processes to be fine-tuned to improve response time during incidents

***Addresses Roadmap Milestones:** 2.3, 5.3*



Home Intelligence

Feeder Automation

Substation Automation

Transmission Automation

Distribution Automation (DA)

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

PMU's

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

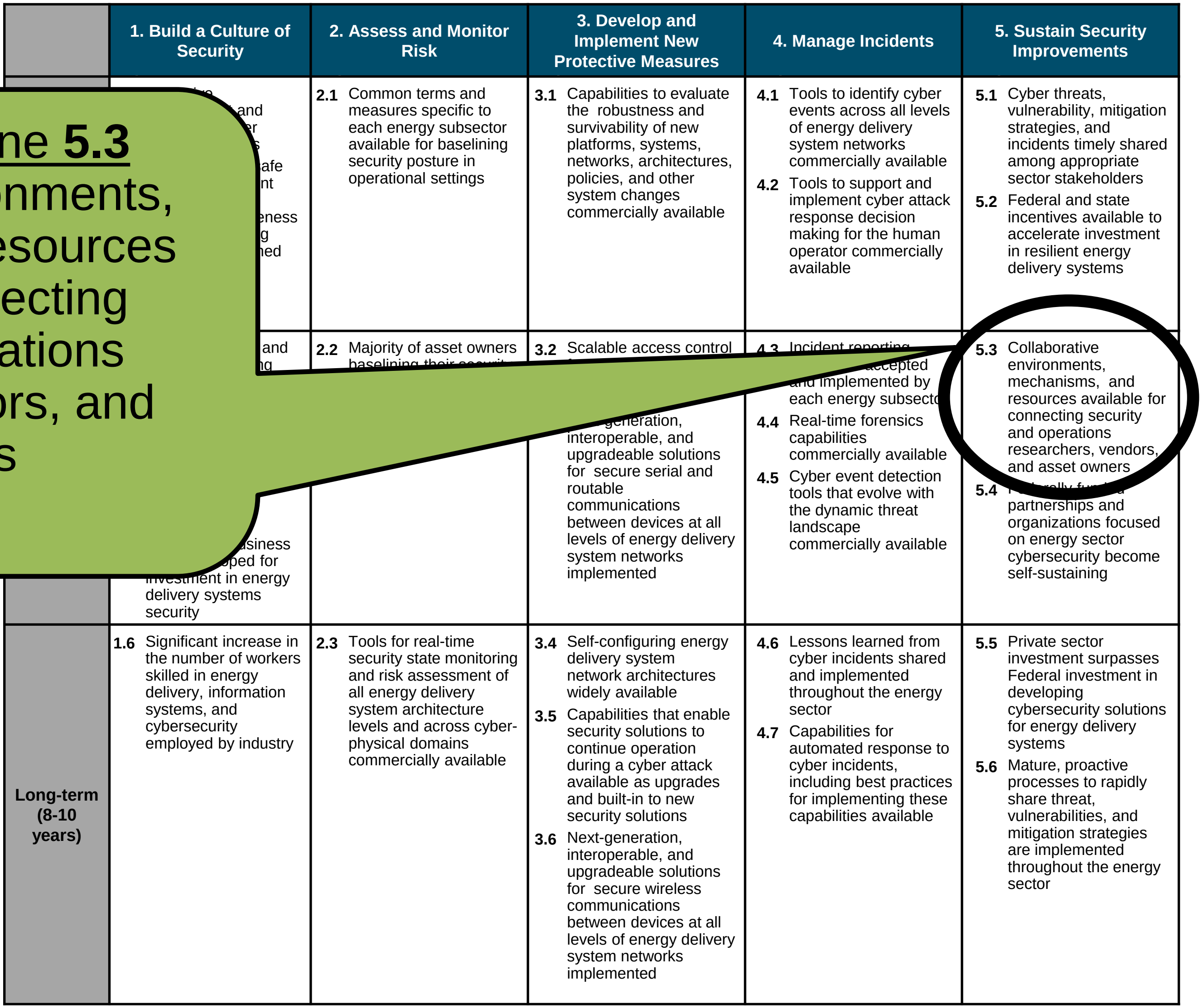
Local Area Network (LAN)

Local Area Network (LAN)

CEDS Alignment with the Roadmap

CEDS provides

<u>Roadmap Milestone **5.3**</u>
Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners



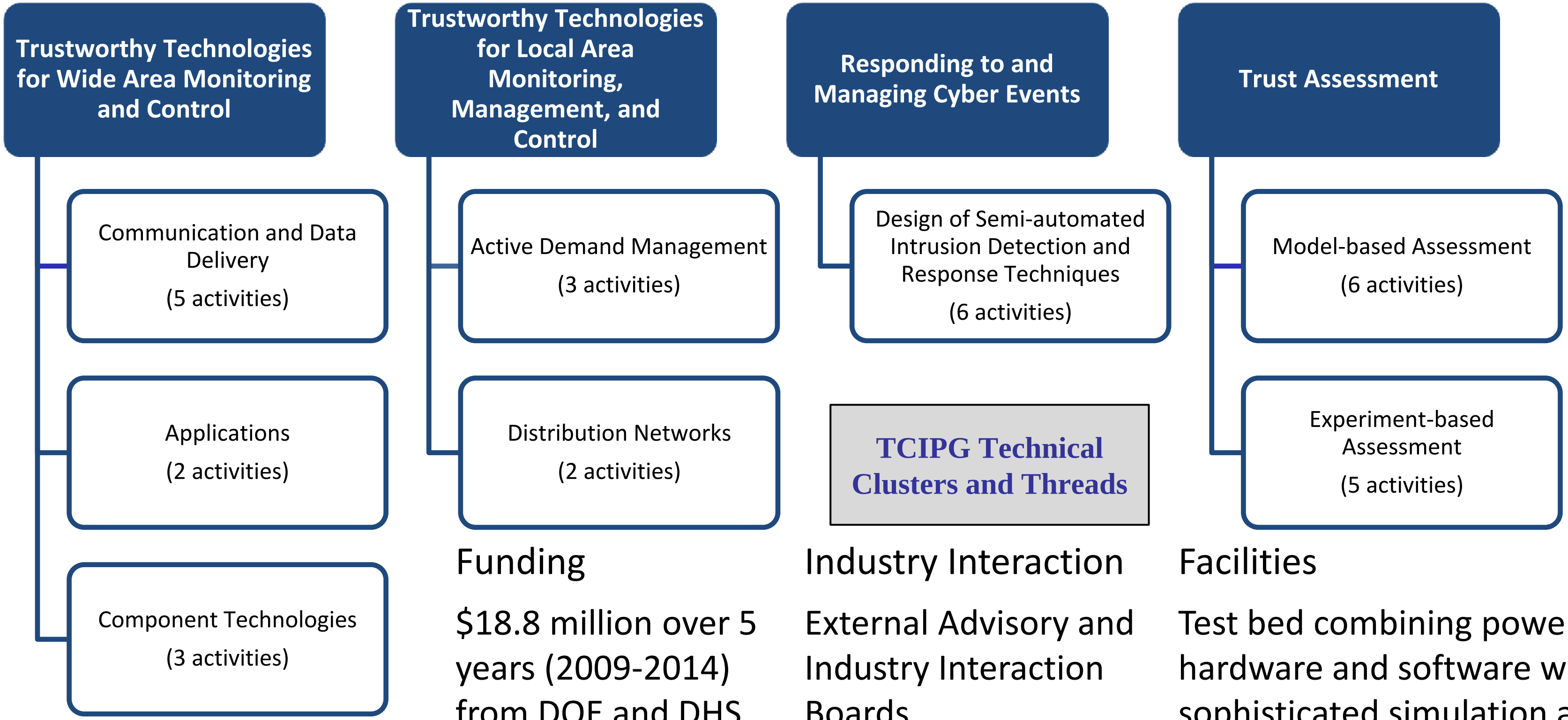
	1. Build a Culture of Security	2. Assess and Monitor Risk	3. Develop and Implement New Protective Measures	4. Manage Incidents	5. Sustain Security Improvements
[illegible]	[illegible] and [illegible] er [illegible] s [illegible] afe [illegible] nt [illegible] eness [illegible] g [illegible] ned	**2.1** 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
[illegible]	[illegible] and [illegible] ng [illegible] usiness [illegible] oped for investment in energy delivery systems security	**2.2** Majority of asset owners baselining their security [illegible]	**3.2** Scalable access control f [illegible] 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 [illegible] accepted and implemented by each energy subsecto **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

To accelerate cybersecurity investment and adoption of resilient energy delivery systems

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*



Trustworthy Technologies for Wide Area Monitoring and Control

- Communication and Data Delivery (5 activities)
- Applications (2 activities)
- Component Technologies (3 activities)

Trustworthy Technologies for Local Area Monitoring, Management, 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 Technical Clusters and Threads

Funding

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

Industry Interaction

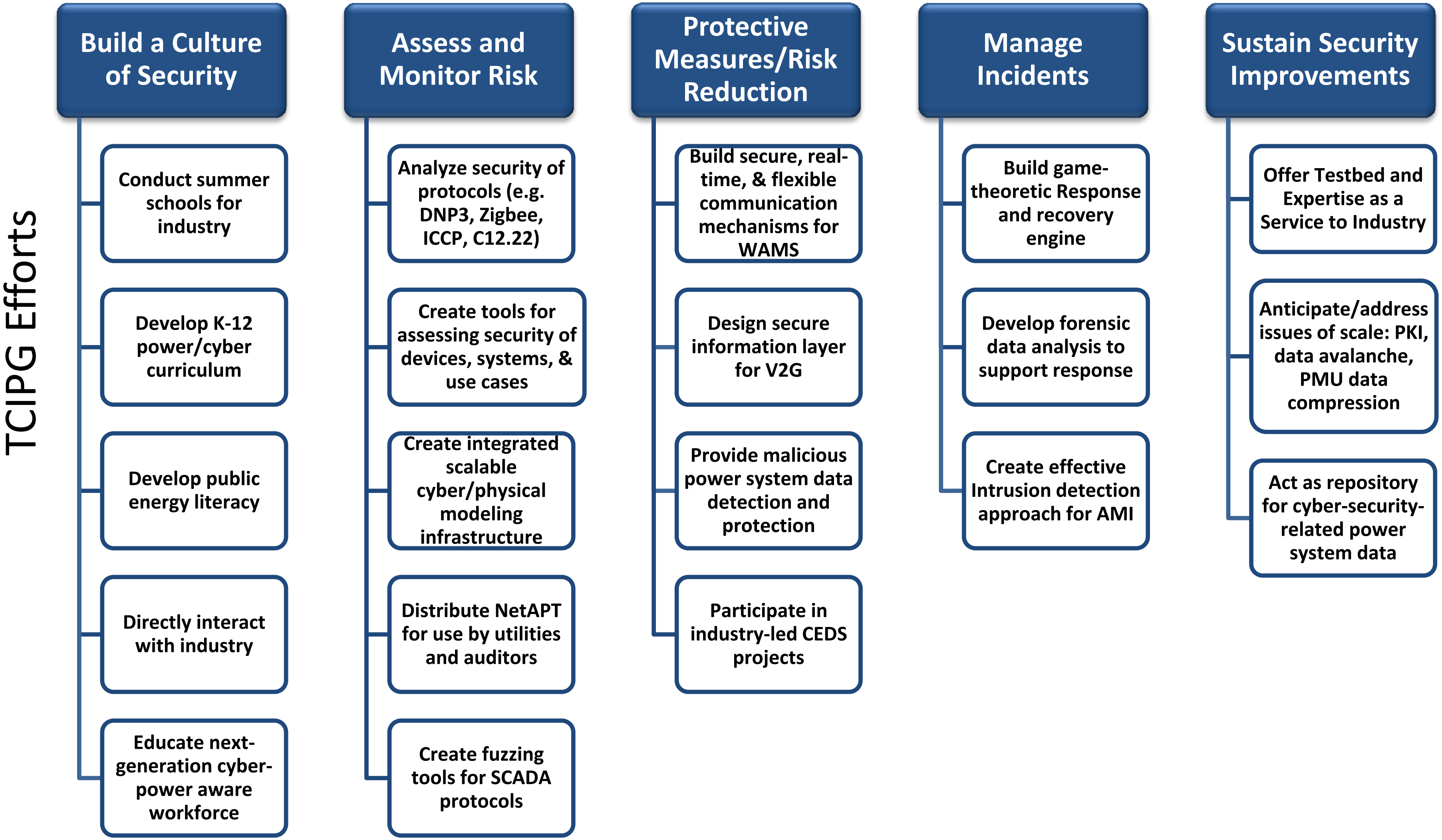
External Advisory and Industry Interaction Boards

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

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



TCIPG Efforts

Build a Culture of Security

- Conduct summer schools for industry
- 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)
- Create tools for assessing security of 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
- Provide malicious power system data detection and protection
- 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

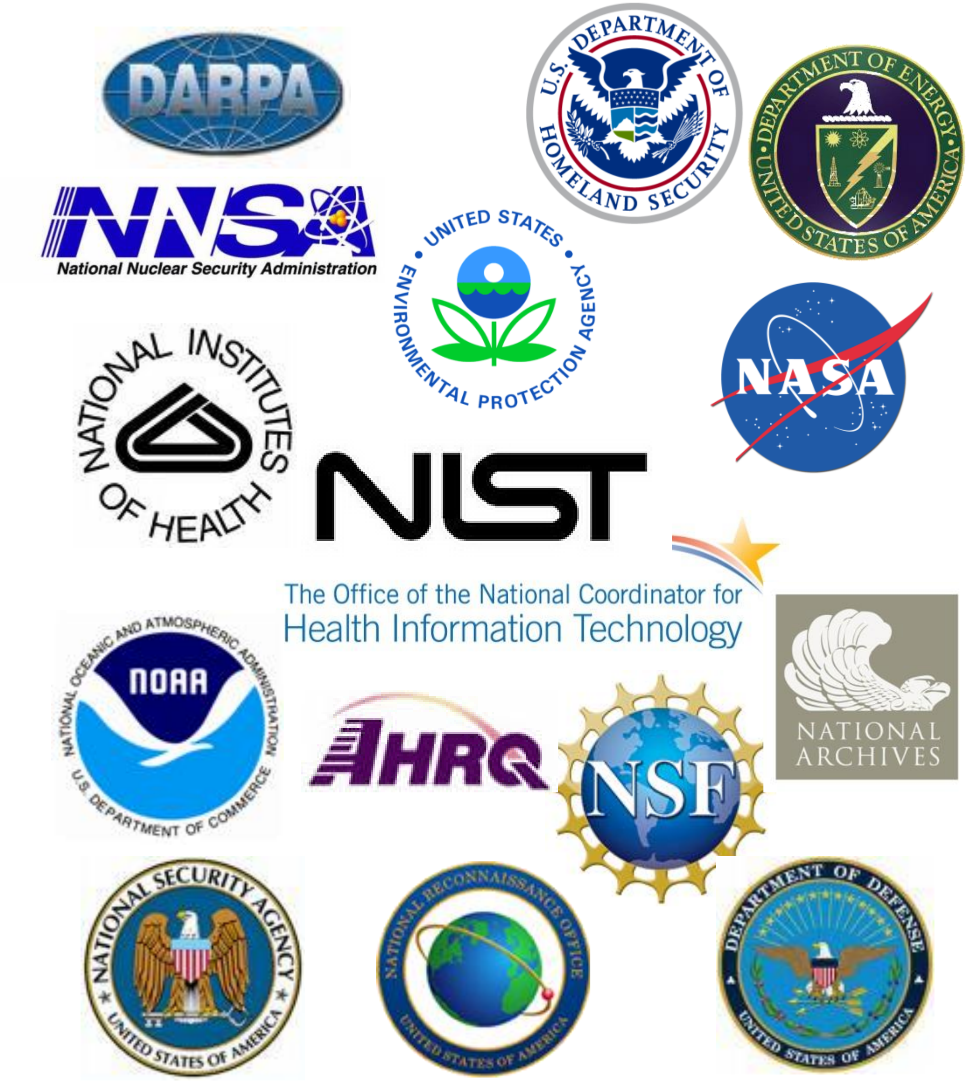
Sustain Security Improvements

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

Coordination with Other Federal Cybersecurity R&D Programs

NITRD

- 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)


DARPA
U.S. Department of Homeland Security
Department of Energy United States of America
NNSA National Nuclear Security Administration
United States Environmental Protection Agency
NASA
National Institutes of Health
NIST
The Office of the National Coordinator for Health Information Technology
National Oceanic and Atmospheric Administration NOAA U.S. Department of Commerce
AHRQ
NSF
National Archives
National Security Agency United States of America
National Reconnaissance Office United States of America
Department of Defense United States of America

CEDS Encourages R&D Collaboration

National Labs

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

Asset Owners/Operators

- Ameren
- Burbank Water and Power
- CenterPoint Energy
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- Idaho Falls Power
- National Rural Electric Cooperative Association
- Pacific Gas & Electric
- Peak RC
- PJM Interconnection
- Sacramento Municipal Utilities District
- San Diego Gas and Electric
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Cigital, Inc.
- EPRI
- Foxguard Solutions
- GE
- Grid Protection Alliance
- Honeywell
- ID Quantique
- NexDefense
- OSIsoft
- Schneider Electric
- SEL
- Siemens
- Telvent
- Utility Advisors
- Utility Integration Solutions
- ViaSat

Academia

- Carnegie Mellon University
- Georgia Institute of Technology
- University of Illinois
- UC Davis
- UC Berkeley
- University of Tennessee-Knoxville

Other

- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- Open Information Security Foundation

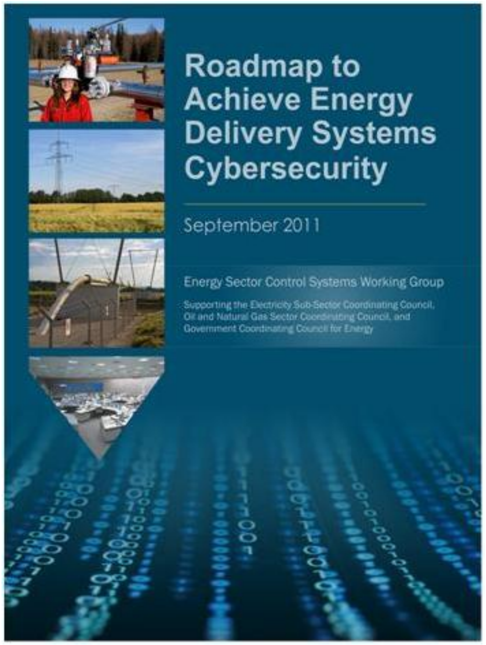
For More Information, Please Contact:

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



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

Visit:

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

www.controlsystemsroadmap.net