U.S. DEPARTMENT OF ENERGY

OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

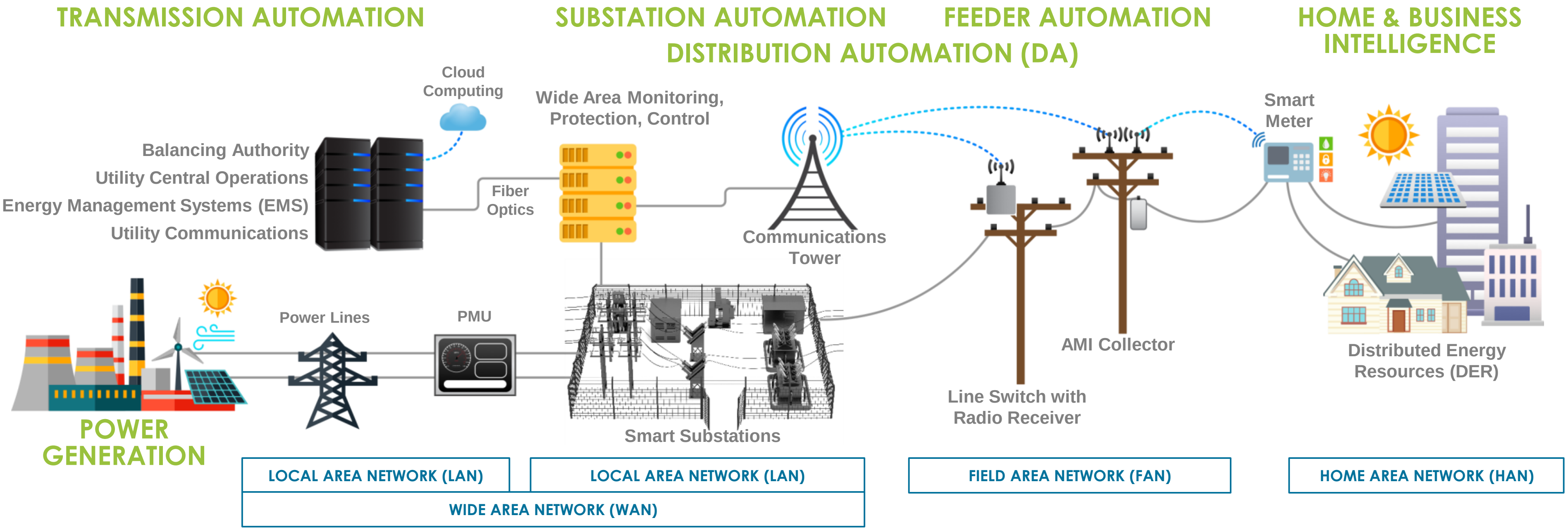
Cybersecurity for Energy Delivery Systems (CEDS) Division Overview

Carol Hawk

Acting Deputy Assistant Secretary

March 4, 2019

Electricity Delivery Infrastructure



TRANSMISSION AUTOMATION

SUBSTATION AUTOMATION

FEEDER AUTOMATION

DISTRIBUTION AUTOMATION (DA)

HOME & BUSINESS INTELLIGENCE

Cloud Computing

Wide Area Monitoring, Protection, Control

Balancing Authority
Utility Central Operations
Energy Management Systems (EMS)
Utility Communications

Fiber Optics

Communications Tower

Smart Meter

AMI Collector

Line Switch with Radio Receiver

Distributed Energy Resources (DER)

POWER GENERATION

Power Lines

PMU

Smart Substations

LOCAL AREA NETWORK (LAN)

LOCAL AREA NETWORK (LAN)

WIDE AREA NETWORK (WAN)

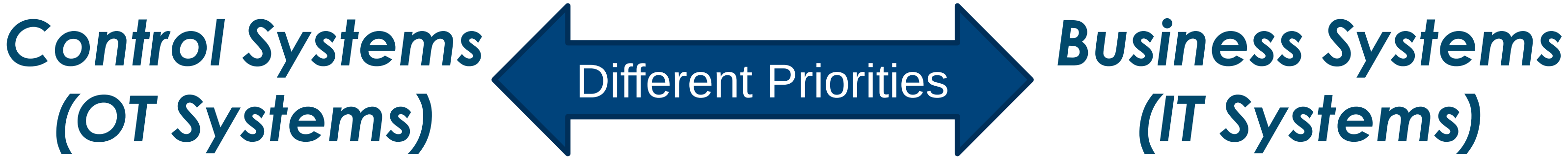
FIELD AREA NETWORK (FAN)

HOME AREA NETWORK (HAN)

Operational Technology (OT) and Information Technology (IT)

Energy delivery control systems are OT:

- Computers and networks that manage, monitor, protect and control energy delivery
- Cyber-attack can disrupt power, damage physical equipment, jeopardize public safety, economic prosperity and national security



Control Systems (OT Systems)

Different Priorities

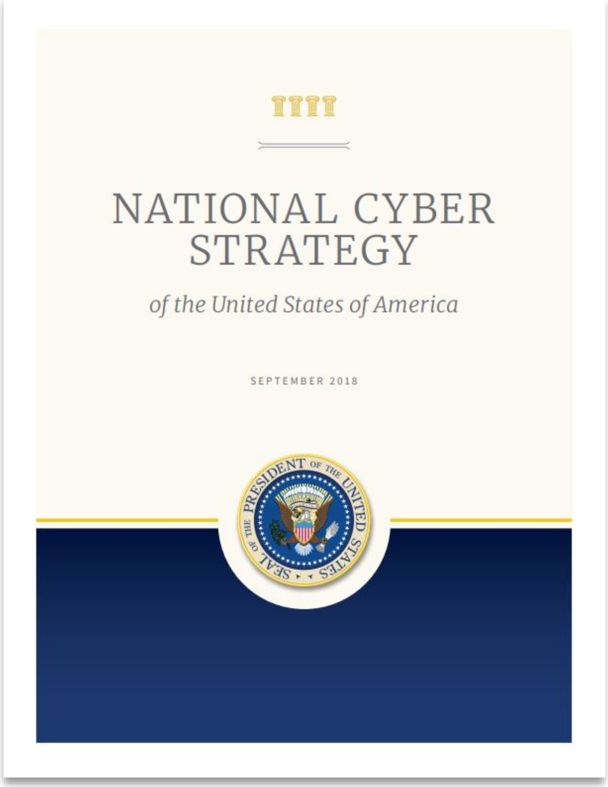
Business Systems (IT Systems)

Energy delivery cybersecurity OT solutions must be tailored to support operations

- No down time for system fixes – power systems must operate 24/7 with high reliability and high availability
- Components are distributed over wide geographical regions, publicly accessible subject to tampering
- Legacy equipment and protocols not designed to support cybersecurity measures
- Latency is often unacceptable – cyber solutions cannot slow system operations
- Active scanning of network can interfere with equipment operations
- Real-time emergency response capability is necessary
- Patches/upgrades require rigorous, prolonged testing

Physics Rules OT

National Cyber Strategy



NATIONAL CYBER STRATEGY

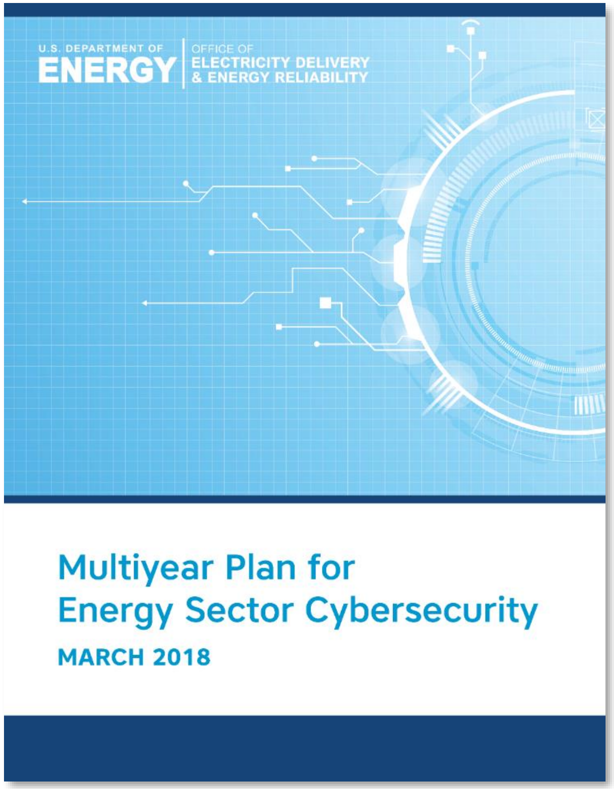
of the United States of America

SEPTEMBER 2018

- First fully articulated national cyber strategy **in 15 years.**
- Outlines actions to

1. **Defend the homeland** by protecting networks, systems, functions, and data
2. **Promote American prosperity** by nurturing a secure, thriving digital economy and fostering strong domestic innovation
3. **Preserve peace and security** by strengthening the United States' ability— in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes
4. **Expand American influence abroad** to extend the key tenets of an open, interoperable, reliable, and secure Internet.

DOE CESER Multiyear Plan for Energy Sector Cybersecurity



U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

MARCH 2018

- **DOE's strategy** for partnering with industry to protect U.S. energy system from cyber risks
- **Guided by direct industry input** on cybersecurity needs and priorities – complements the Energy Sector Roadmap
- **Market-based approach** encourages investment and cost-sharing of promising technologies and practices
- **Establishes goals, objectives, and activities** to improve both near- and long-term energy cybersecurity

DOE Vision

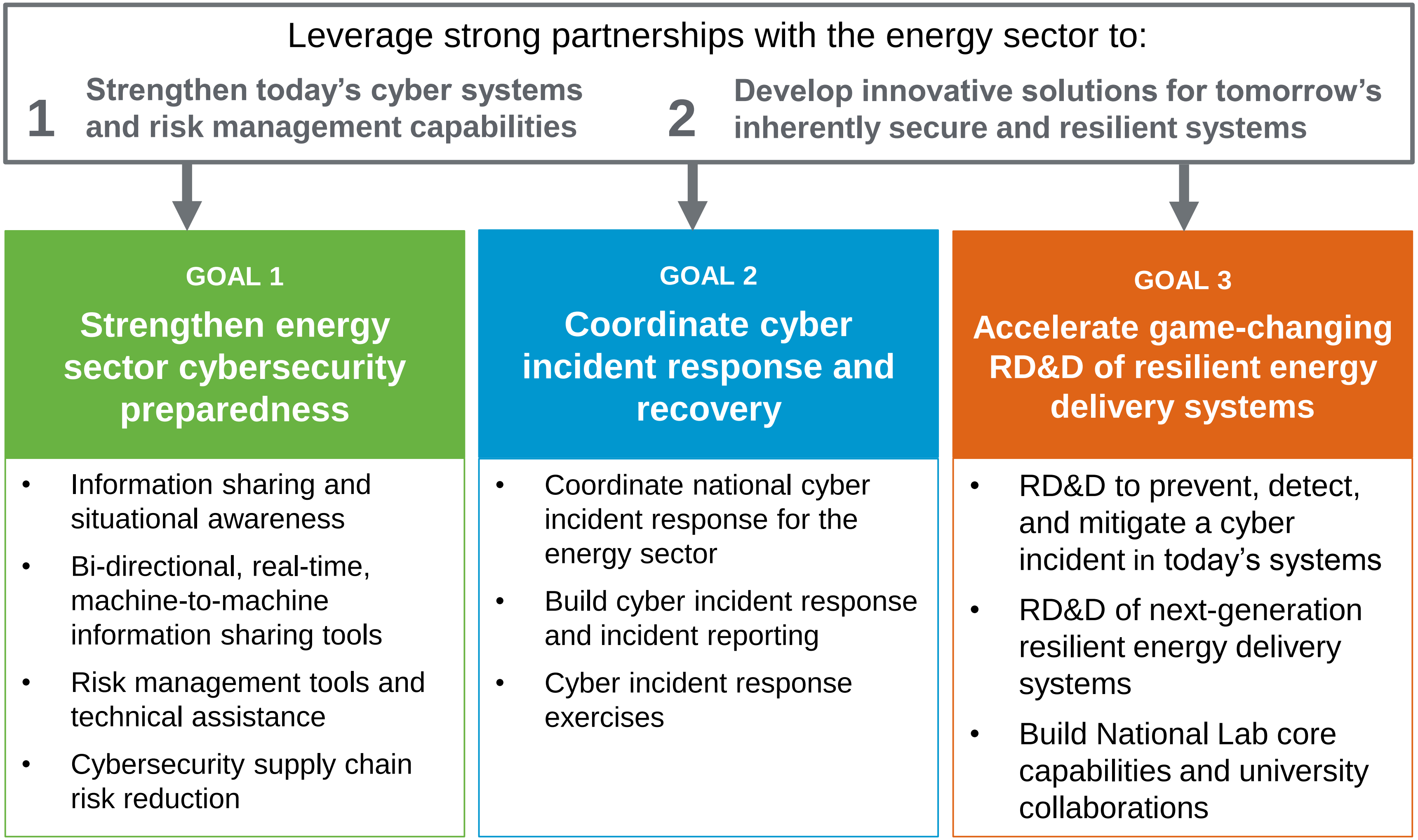
Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions

Strategy for a resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover	Manual	OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Bold = CESER-funded projects in this area

DOE’s Strategy for Energy Sector Cybersecurity



Leverage strong partnerships with the energy sector to:

1 **Strengthen today’s cyber systems and risk management capabilities**

2 **Develop innovative solutions for tomorrow’s inherently secure and resilient systems**

GOAL 1

Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2

Coordinate cyber incident response and recovery

- Coordinate national cyber incident response for the energy sector
- Build cyber incident response and incident reporting
- Cyber incident response exercises

GOAL 3

Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today’s systems
- RD&D of next-generation resilient energy delivery systems
- Build National Lab core capabilities and university collaborations

140+ Partners Participating in CEDS R&D

Asset Owners/Operators

- Ameren
- Arkansas Electric Cooperatives Corporation
- Avista
- Burbank Water and Power
- BPA
- CenterPoint Energy
- Chevron
- ComEd
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- FirstEnergy
- FP&L
- HECO
- Idaho Falls Power
- Inland Empire Energy
- NIPSCO
- Omaha Public Power District
- Orange & Rockland Utility
- Pacific Gas & Electric
- PacifiCorp
- Peak RC
- PJM Interconnection
- Rochester Public Utilities
- Sacramento Municipal Utilities District
- San Diego Gas and Electric
- Sempra
- Snohomish PUD
- Southern Company
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority
- WAPA
- Westar Energy
- WGES

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Cybati
- Eaton
- Enernex
- EPRI
- FoxGuard Solutions
- GE
- Grid Protection Alliance
- Grimm
- Honeywell
- ID Quantique
- Intel
- NexDefense
- OPAL-RT
- Open Information Security Foundation
- OSIsoft
- Parsons
- Power Standards Laboratory
- Qubitekk
- RTDS Technologies Inc.
- Schneider Electric
- SEL
- Siemens
- TDi Technologies
- Telvent
- Tenable Network Security
- Utility Advisors
- Utility Integration Solutions
- UTRC
- Veracity
- ViaSat

Academia

- Arizona State University
- Carnegie Mellon University
- Dartmouth College
- Florida International University
- Georgia Institute of Technology
- Illinois Institute of Technology
- Iowa State University
- Lehigh University
- Massachusetts Institute of Technology
- Oregon State University
- Rutgers University
- Tennessee State University
- Texas A&M EES
- University of Arkansas
- University of Arkansas-Little Rock
- University of Buffalo - SUNY
- University of Illinois
- UC Davis
- UC Berkeley
- University of Houston
- University of Tennessee-Knoxville
- University of Texas at Austin
- Washington State

National Labs

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

Other

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

CEDS R&D Reach and Impact

- **Funds earlier, high-risk/high-reward R&D** in areas critical for national security where a business case cannot readily be established by a private-sector company
- **Builds R&D pipeline through partnerships** with energy sector utilities, vendors and service providers, universities, and national laboratories

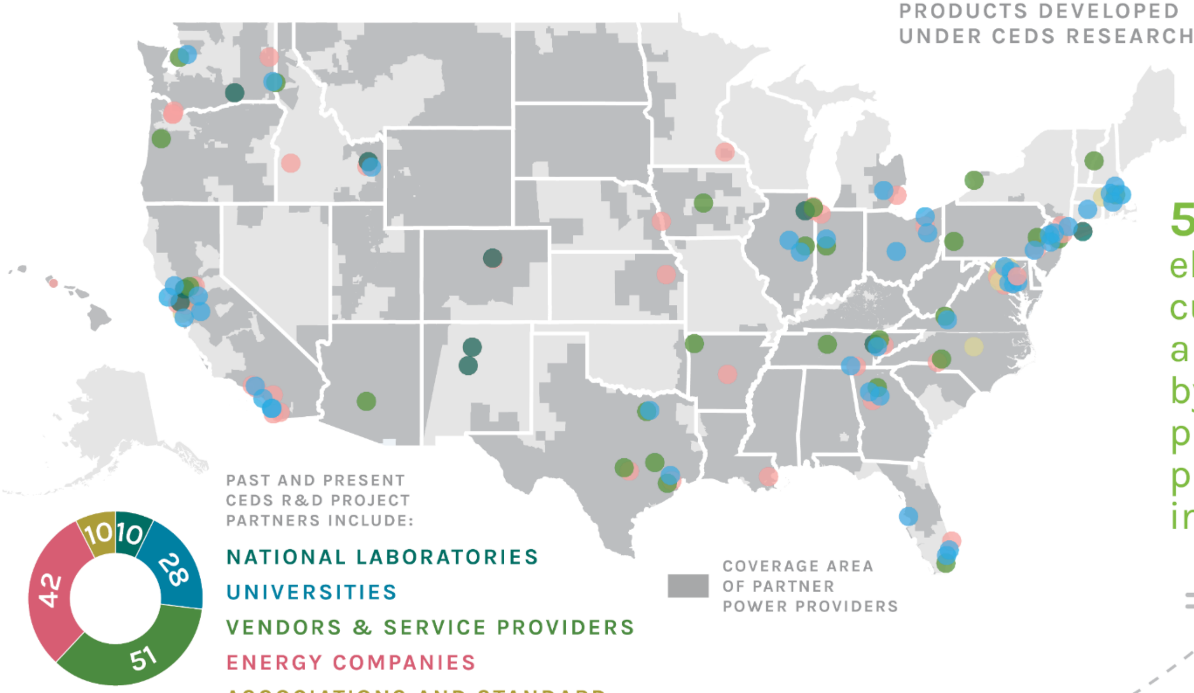
CEDS delivered more than **47** products, tools, and technologies

SINCE 2010 TO REDUCE ENERGY SECTOR CYBER RISK

More than **1,500** utilities in all **50** states

HAVE PURCHASED PRODUCTS DEVELOPED UNDER CEDS RESEARCH

57% of U.S. electricity customers are served by power providers participating in CEDS R&D



PAST AND PRESENT CEDS R&D PROJECT PARTNERS INCLUDE:

NATIONAL LABORATORIES

UNIVERSITIES

VENDORS & SERVICE PROVIDERS

ENERGY COMPANIES

ASSOCIATIONS AND STANDARD ORGANIZATIONS

▨ COVERAGE AREA OF PARTNER POWER PROVIDERS

More than 140 partners have participated

IN COMPETITIVELY FUNDED PROJECTS

All CEDS projects included an energy sector partner

TO DRIVE REAL-WORLD SOLUTIONS

MYP GOAL 3: Accelerate Game-Changing RD&D of Resilient Energy Delivery Systems

PRIORITIES AND PATHWAYS

Research, develop, and demonstrate tools and technologies to:

1. **Prevent, detect, and mitigate cyber incidents in *today's energy delivery systems***
   - Decrease the cyber attack surface and block attempted misuse
   - Decrease the risk of malicious components inserted in the supply chain
   - Enable real-time, continuous cyber situational awareness
   - Automatically detect attempts to execute a function that could de-stabilize the system when the command is issued
   - Characterize cyber incident consequences and automate responses
2. **Change the game so that *tomorrow's resilient energy delivery systems* can survive a cyber incident**
   - Anticipate future grid scenarios and design cybersecurity into systems from the start
   - Enable power systems to automatically detect and reject a cyber attack, refusing any commands/actions that do not support grid stability
   - Build strategic partnerships and core capabilities in National Labs

Example Outcomes for Securing *Today's* Energy Delivery Systems

EXAMPLE OUTCOMES

Tools and technologies to *prevent* cyber attacks:

- → Quantum key distribution to securely exchange data using cryptographic keys while detecting attempted eavesdropping
- → Algorithms that continuously and autonomously assess and reduce the cyber attack surface

Tools and technologies to *detect* cyber attacks:

- → Rapid anomaly identification that may indicate a compromise in utility control communications
- → Tools to detect spoofing or compromise of the precise GPS time signals used for synchrophasor data

Tools and technologies to *mitigate* cyber attacks:

- → Ability for high-voltage DC systems to detect when commands could destabilize the grid and reject the command or take a different action

Example Outcomes for *Tomorrow's* Resilient Energy Delivery Systems

EXAMPLE OUTCOMES

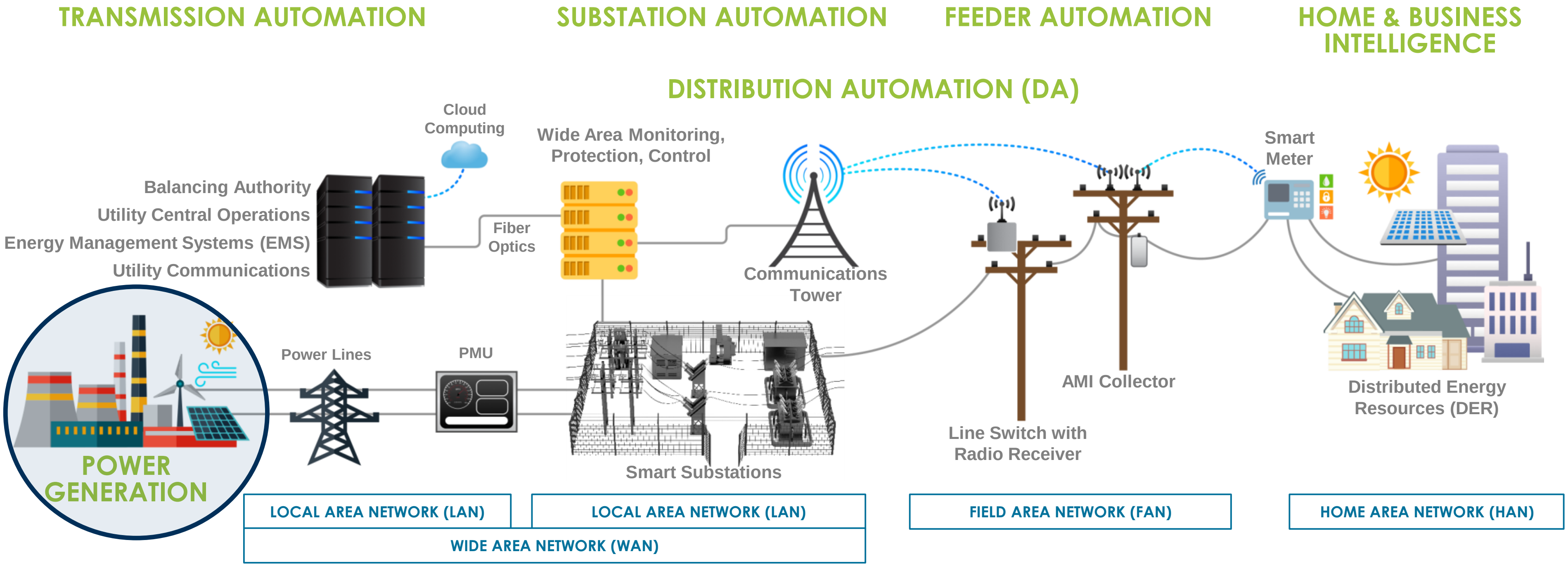
Tools and technologies to anticipate future grid scenarios, design in cybersecurity, and enable power systems to automatically recognize and reject a cyber attack:

- → Architectures that secure the cyber interaction of grid-edge devices and data streams in the cloud
- → Resilient building energy management systems that can switch to a more secure platform during a potential cyber incident
- → A cyber-physical control and protection architecture for multi-microgrid systems that enable stable grid performance during a cyber attack using electrical islands
- → Resilient operational networking technology that automates cyber incident responses

Build strategic core capabilities at 10 National Laboratories and build multi-university collaborations dedicated to advancing EDS cybersecurity

Redesign the architecture, adapt to survive

GE Cyber-Attack Detection and Accommodation for power plants



Redesign the architecture, adapt to survive

GE Cyber-Attack Detection and Accommodation for power plants

MYP objective:

Characterize cyber incident consequences and automate responses

We are …

developing a new method of Cyber-attack Detection and Accommodation (ADA) framework to control how a power plant communicates and stops unauthorized attacks on a power plant protection.

So what?

Power plants ride through a cyber-attack while continuing to provide power.

PROJECT LEAD

GE Global Research

PARTNERS

GE Power

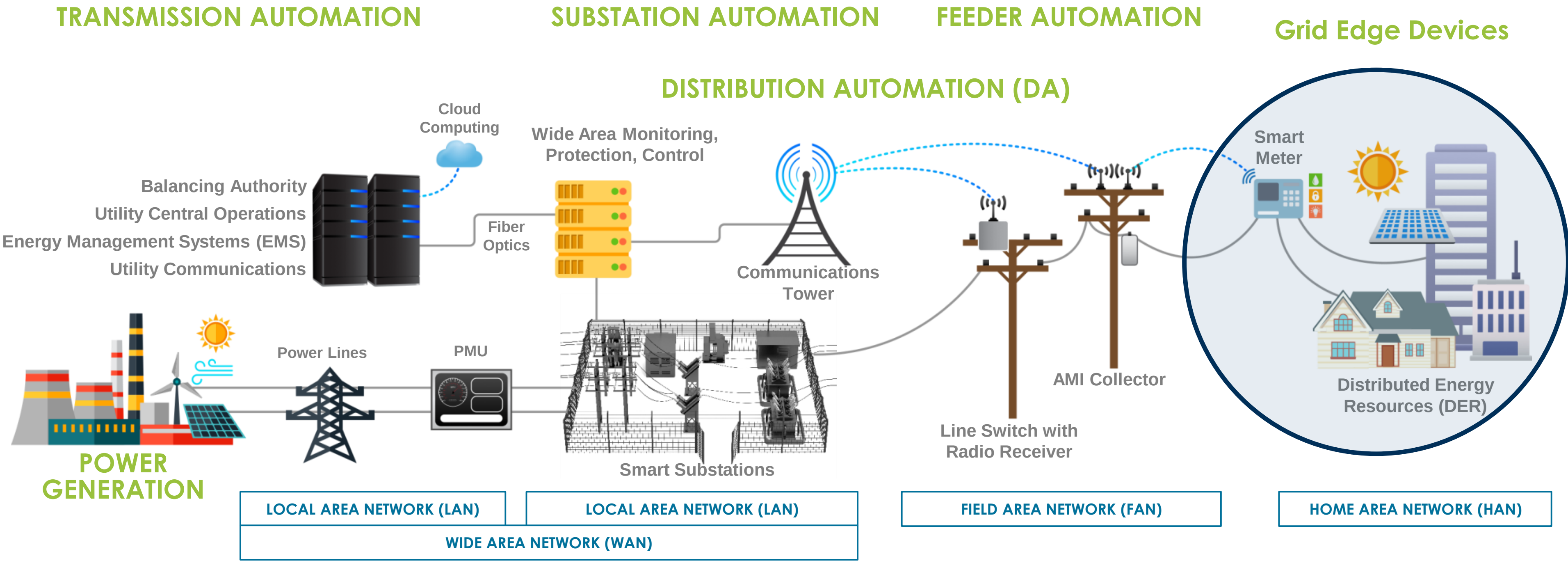
Inland Empire Energy Center

CURRENT ACCOMPLISHMENTS

- Successfully demonstrated ***detection*** capability using GE Power Plant model and real-time sensor data sets. (0.0006% FPR)
- Identified and validated attack ***localization*** (sensor and nodes) (0.28% FPR)
- Exercised ***neutralization*** logic demonstrating system accommodation to adapt and stay operational

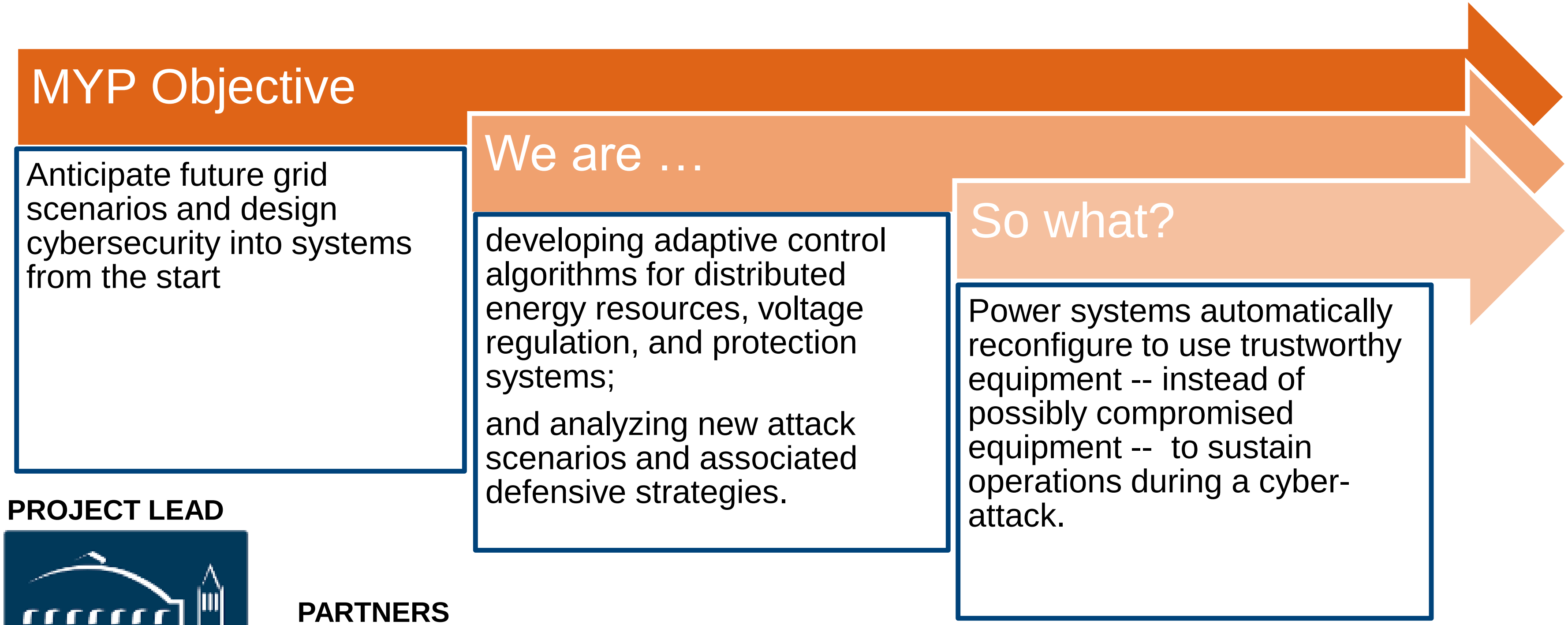
Redesign the architecture, adapt to survive

Adaptive Control of Electric Grid Components for Cyber-Resiliency



Redesign the architecture, adapt to survive

Adaptive Control of Electric Grid Components for Cyber-Resiliency



MYP Objective

Anticipate future grid scenarios and design cybersecurity into systems from the start

We are …

developing adaptive control algorithms for distributed energy resources, voltage regulation, and protection systems;

and analyzing new attack scenarios and associated defensive strategies.

So what?

Power systems automatically reconfigure to use trustworthy equipment -- instead of possibly compromised equipment -- to sustain operations during a cyber-attack.

PROJECT LEAD

BERKELEY LAB

PARTNERS

OSIsoft. SUNSPEC ALLIANCE

solaredge PSL

HDPV ALLIANCE ASU Arizona State University

NRECA SMUD

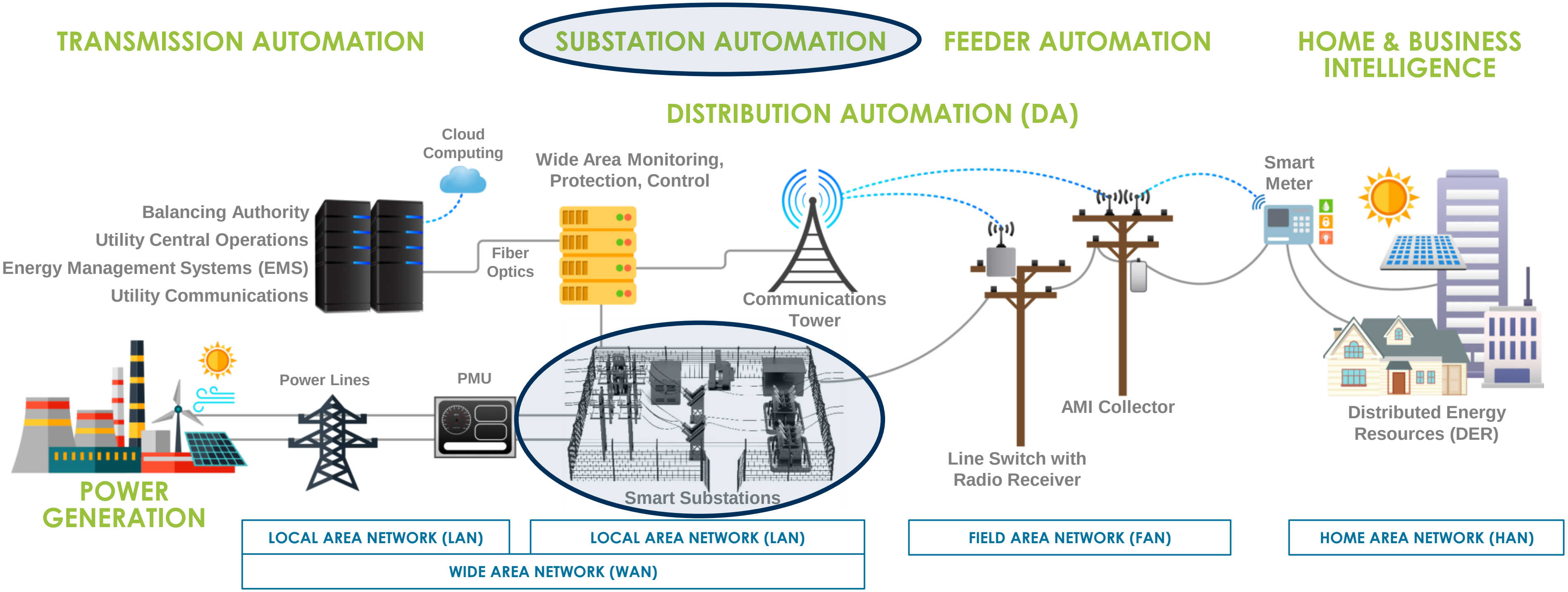
EPRI SIEMENS

CURRENT ACCOMPLISHMENTS

Developing reinforcement learning-based defensive algorithms determine the settings of DER smart inverters and utility voltage and protection systems needed to mitigate certain cyber-physical attacks.

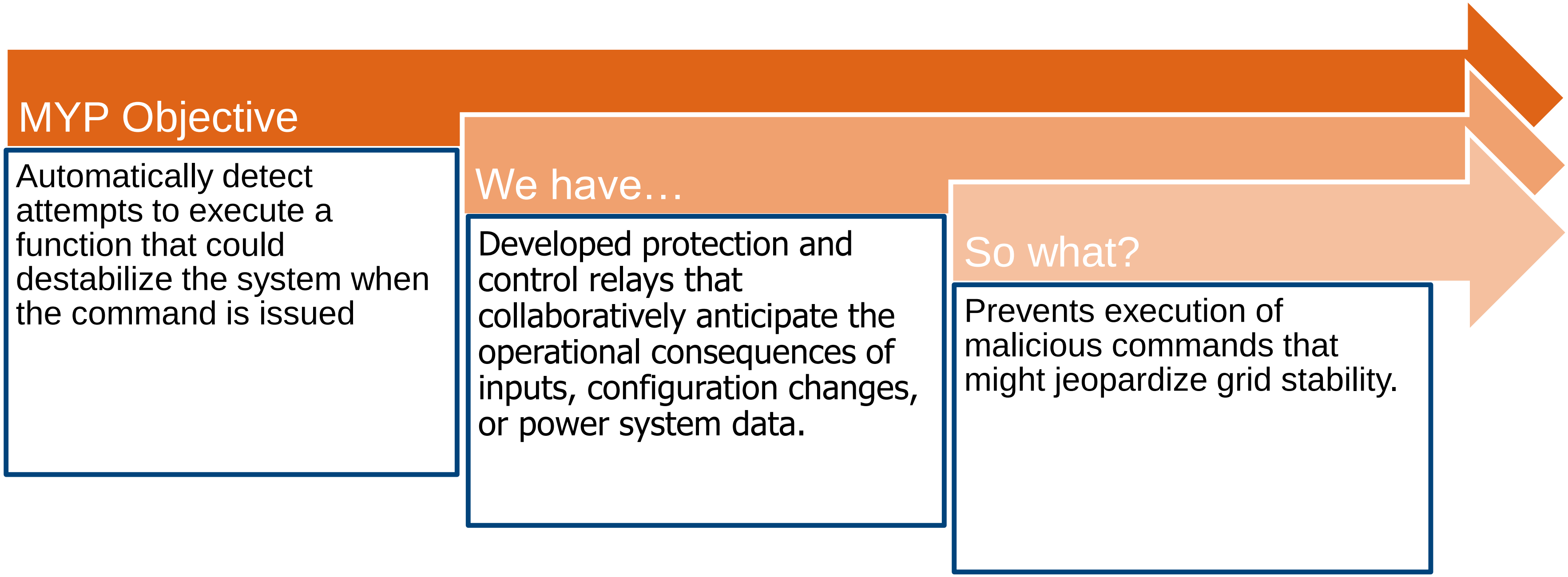
Redesign the architecture, adapt to survive

ABB Collaborative Defense (CODEF) for protection and control equipment



Redesign the architecture, adapt to survive

ABB Collaborative Defense (CODEF) for protection and control equipment



MYP Objective

Automatically detect attempts to execute a function that could destabilize the system when the command is issued

We have…

Developed protection and control relays that collaboratively anticipate the operational consequences of inputs, configuration changes, or power system data.

So what?

Prevents execution of malicious commands that might jeopardize grid stability.

PROJECT LEAD

ABB

PARTNERS

Bonneville POWER ADMINISTRATION

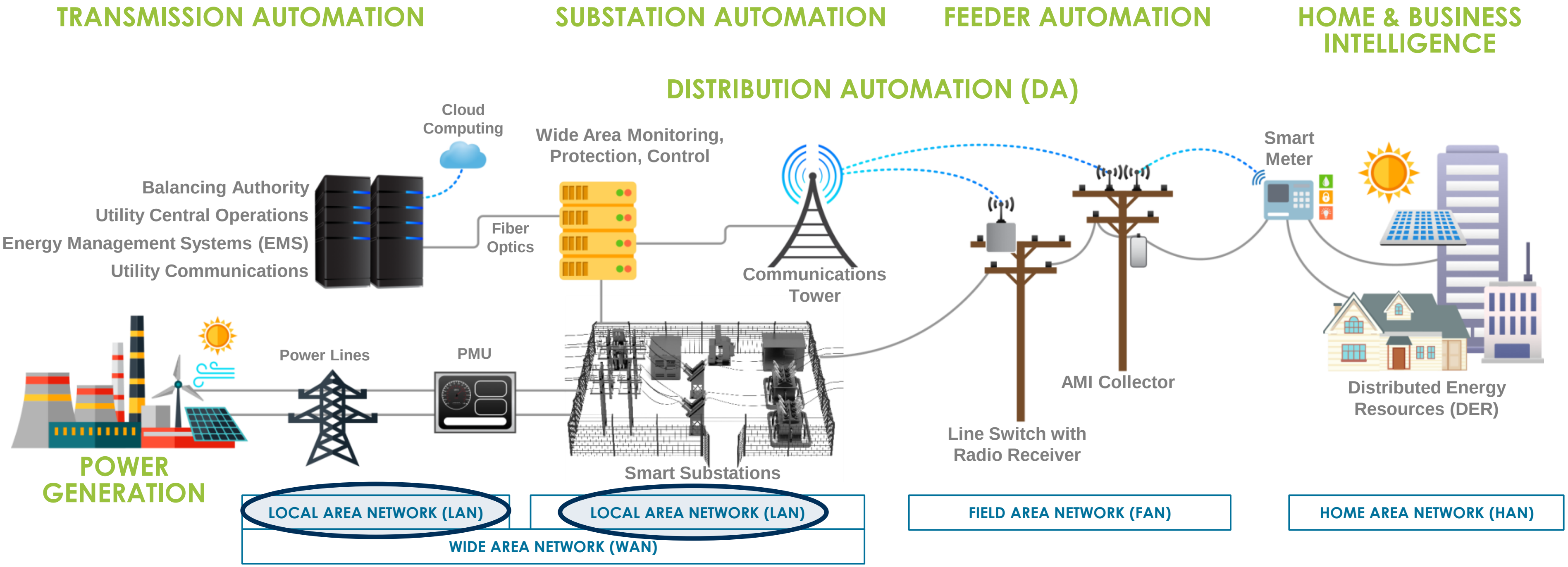
ILLINOIS

CURRENT ACCOMPLISHMENTS

- Demonstrated in a quasi field environment utilizing the substation automation protocol IEC 61850-enabled ABB protection relays configured with actual BPA high voltage line and transformer protection settings.
- Demonstrated attack detection on intelligent electronic device (IED) configurations and prevention of malicious command execution.

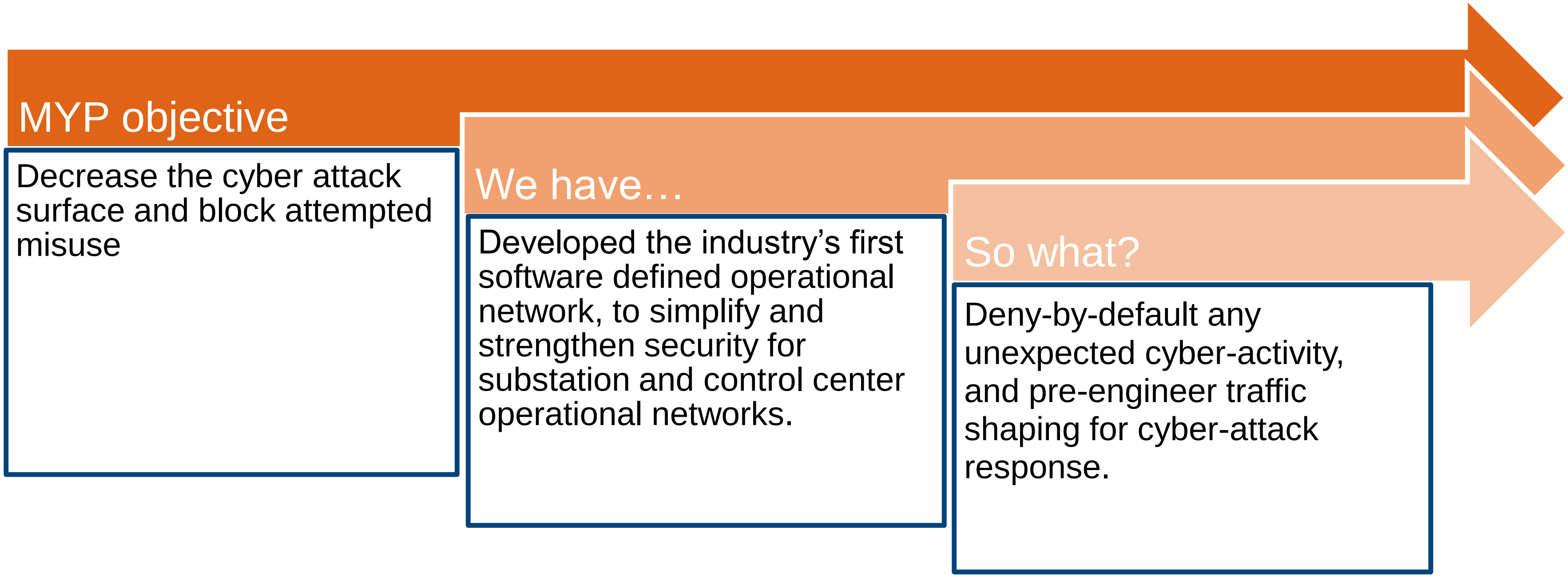
Redesign the architecture, adapt to survive

Software Defined Networking (SDN) and Chess Master Project



Redesign the architecture, adapt to survive

Software Defined Networking (SDN) and Chess Master Project



MYP objective

Decrease the cyber attack surface and block attempted misuse

We have…

Developed the industry’s first software defined operational network, to simplify and strengthen security for substation and control center operational networks.

So what?

Deny-by-default any unexpected cyber-activity, and pre-engineer traffic shaping for cyber-attack response.

PROJECT LEAD

SEL SCHWEITZER ENGINEERING LABORATORIES

PARTNERS

Pacific Northwest NATIONAL LABORATORY

VERACITY Industrial Network Security

Ameren

CURRENT ACCOMPLISHMENTS

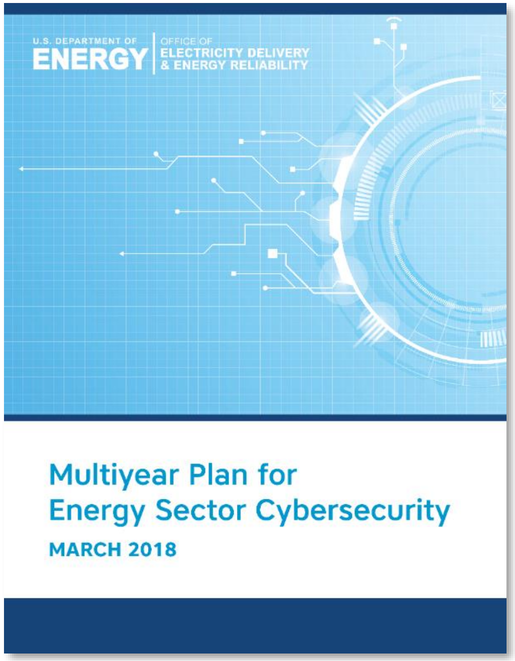
- Commercial product released the SEL-2740S (SDN Switch) and SEL-5056 in the industry’s first commercial industrial flow controller
- Completed the API between Flow Controller and security state monitoring
- Demonstrated the integrated threat management platform to engineer networks and define how the networks will react to events like link loss or unauthorized packets at 2018 DistribuTECH

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)

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
NOAA
National Oceanic and Atmospheric Administration
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
U.S. DEPARTMENT OF ENERGY
OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

For More Information, Please Contact:



U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for
Energy Sector Cybersecurity

MARCH 2018

Dr. Carol Hawk
Acting Deputy Assistant Secretary
Cybersecurity for Energy Delivery Systems (CEDS) Division
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

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

Visit: https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response