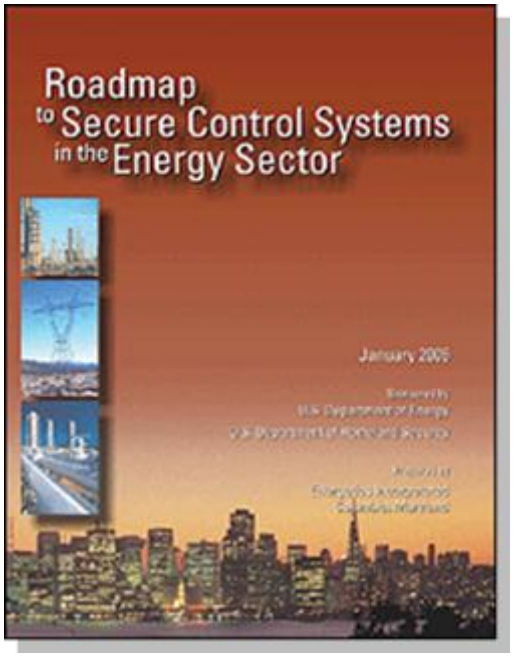
U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Working to Achieve Cybersecurity in the Energy Sector

"Cybersecurity for Energy Delivery Systems (CEDS)"

Roadmap – Framework for Public-Private Collaboration

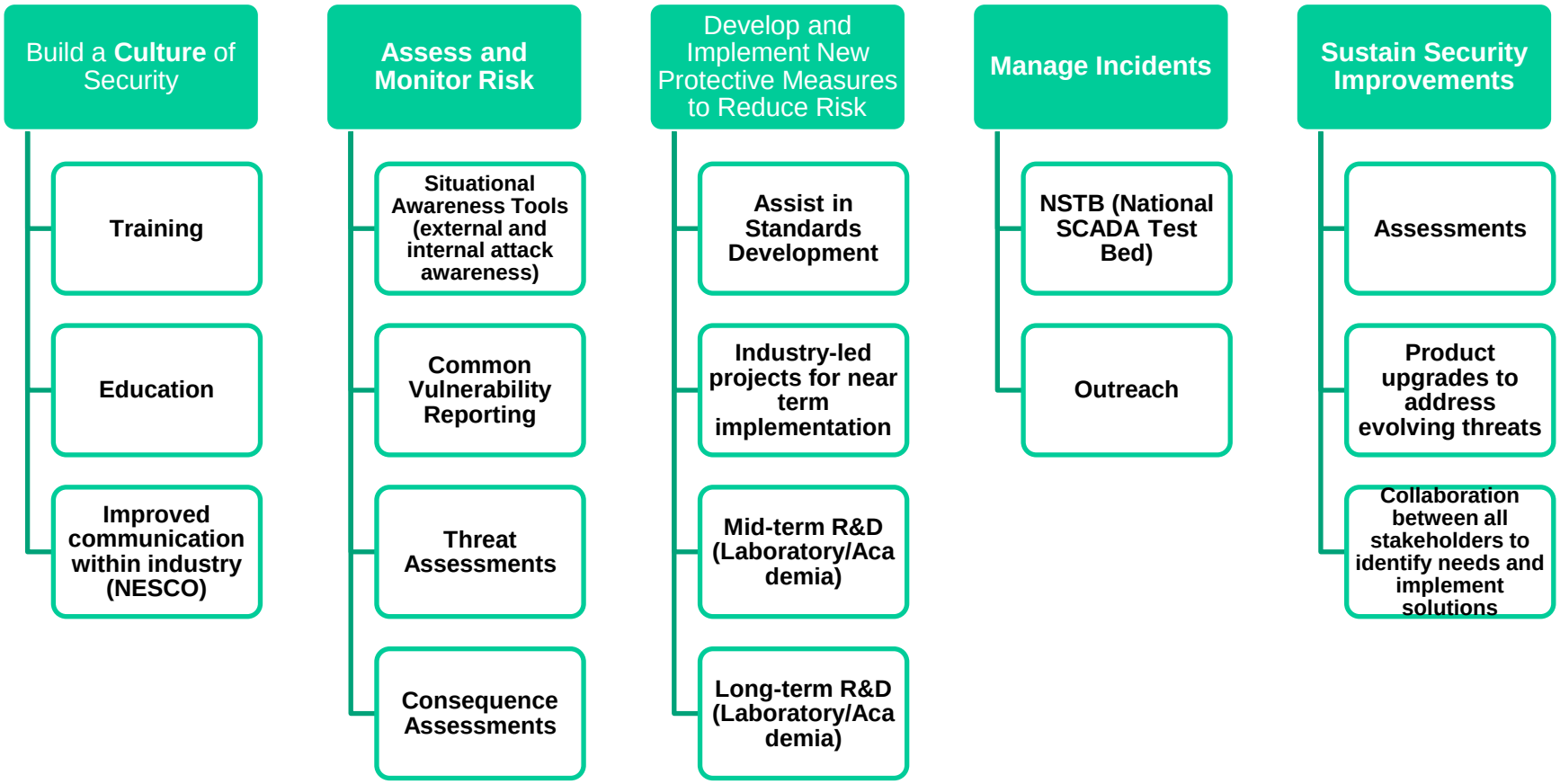


- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in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

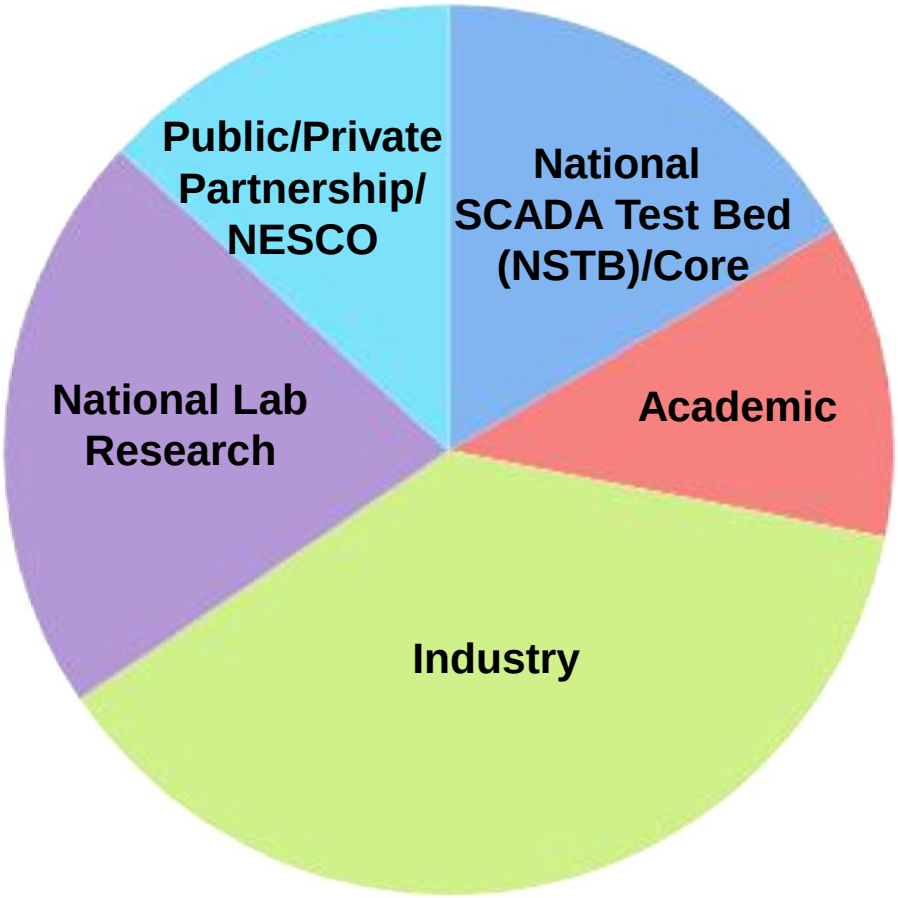
Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to ***survive*** an intentional cyber assault with no loss of critical function.

Strategic Framework



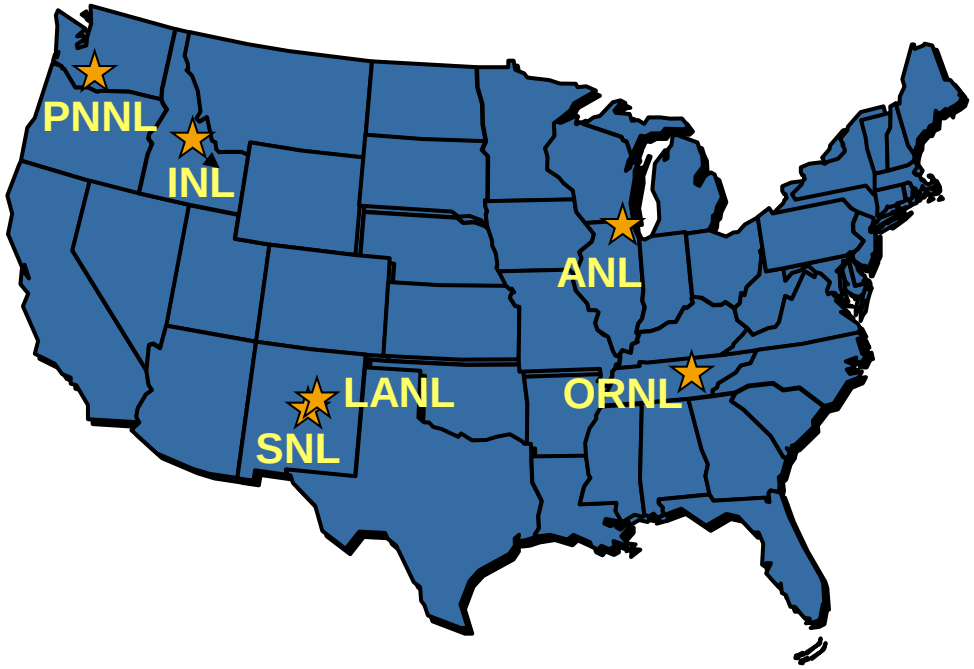
Cybersecurity for Energy Delivery Systems (CEDS) Program—5 Key Areas



DOE National SCADA Test Bed (NSTB) Program

DOE multi-laboratory program *…established 2003*

Supports industry and government efforts to enhance cyber security of control systems in energy sector



"..the only reliable way to measure security is to examine how it fails"

Bruce Schneier, Beyond Fear

Key Program Elements

- Cyber security assessments and recommended mitigations for energy control systems
- Integrated risk analysis
- Secure next generation control systems technology R&D
- Public-private partnership, outreach, and awareness

17 NSTB Facilities From 6 National Labs

IDAHO Critical Infrastructure Test Range
- SCADA/Control System Test Bed
- Cyber Security Test Bed
- Wireless Test Bed
- Powergrid Test Bed
- Modeling and Simulation Test Bed
- Control Systems Analysis Center

SANDIA Center for SCADA Security
- Distributed Energy Technology Laboratory (DETL)
- Network Laboratory
- Cryptographic Research Facility
- Red Team Facility
- Advanced Information Systems Laboratory

PACIFIC NORTHWEST Electricity Infrastructure Operations Center
- SCADA Laboratory
- National Visualization and Analytics Center
- Critical Infrastructure Protection Analysis Laboratory

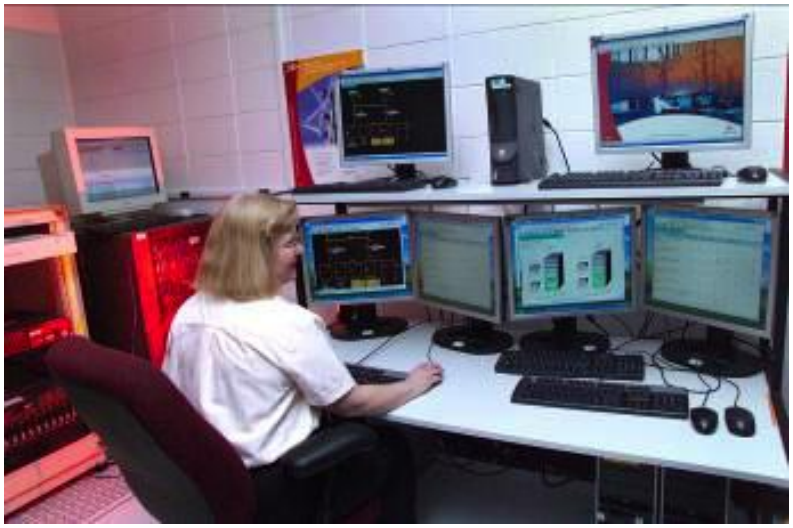
OAK RIDGE Cyber Security Program
- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

ARGONNE Infrastructure Assurance Center

LOS ALAMOS Cybersecurity Program

DOE National SCADA Test Bed (NSTB)
System Vulnerability Assessments - SCADA/EMS

- **Completed assessments of 38 vendor control systems and associated components on-site at utility field installations and at the INL SCADA Test Bed facility**



Detroit Edison
A DTE Energy Company

AREVA

SIEMENS

TELVENT

GE Energy

TELTONE®

ABB

AMERICAN TRANSMISSION COMPANY

OSIsoft.

OSI
opening your world

SUCCESS STORY:
2008 First DOE-Awarded Industry Projects

- **Hallmark Project**
  - **Secure serial communication links**
- **Cyber Security Audit and Attack Detection Toolkit**
  - **Baseline optimal security configuration**
- **Lemnos Interoperable Security Program**
  - **Interoperable configuration profiles and testing procedures**

Key Milestones:

Next Generation Control Systems

System Vulnerability Assessments

Partnership and Outreach

The Hallmark Project
Schweitzer Engineering Laboratories, Inc.

Outcomes:

- Develop solutions that can be applied to existing control systems and designed into new control systems to mitigate network vulnerabilities
- Provide data integrity ("cryptographic security") in open protocol environment through message authentication
- Commercial Prototype

Participants:

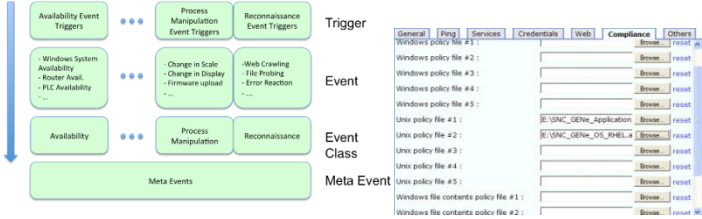
- CenterPoint Energy
- Pacific Northwest National Laboratories (PNNL)
- "Early Adopters"

Success Stories:

- **SSCP Technology Transfer Completed**
  - Provides message integrity by marking original SCADA messages with a unique identifier and authenticator
  - Receiving devices will validate before enacting commands
- **Cryptographic Daughter Card**
  - Electronic hardware card that runs the SSCP protocol
- **Link Module**
  - Hardware and firmware platform
  - Provides the interface between the control system network and the CDC with SSCP
- **Easily incorporated into all legacy, and new control system designs**
- **Enables uniform energy infrastructure improvements without dependency on protocols or configurations.**
- **Prototypes delivered and being tested**
- **Listed in Catalog!**

Cyber Security Audit and Attack Detection Toolkit

Digital Bond, Inc.



Outcomes:

- Leverage existing tools
- Identify vulnerable configurations in control system devices and applications
- Aggregate and correlate control system data
- Project results will be available directly from the vendor and via Digital Bond's subscriber site

Participants:

- OSISoft
- Tenable Network Security
- Various Asset Owners

Success Stories:

- **Bandolier Project – Optimizing Security Configurations of Control System Workstations and Servers Without Installing Software or Adversely Impacting the System**
  - Leveraged compliance plug-in of the Nessus Vulnerability Scanner
  - Developed audit files for Siemens, Telvent, ABB, Matrikon, Emerson, AREVA, and SNC systems
  - Audits check all of the security parameters for a particular control system component and provide user with a list of the non-optimal parameters and identify the optimal settings.
- **Portaledge Project – Aggregating and Correlating Control System Data**
  - Leverages OSIsoft's PI Server
  - Gathers and correlates control systems data, including security event data, to identify a sequence or "recipe" of events that could indicate a specific attack goal or achievement
- **Available as subscriber content on website**
  - **Over 200 organizations subscribing**

LEMNOS Interoperable Security Program
EnerNex, Corp.

Outcomes:

- Commercial Prototype
- Open Source Design
- Plugfest

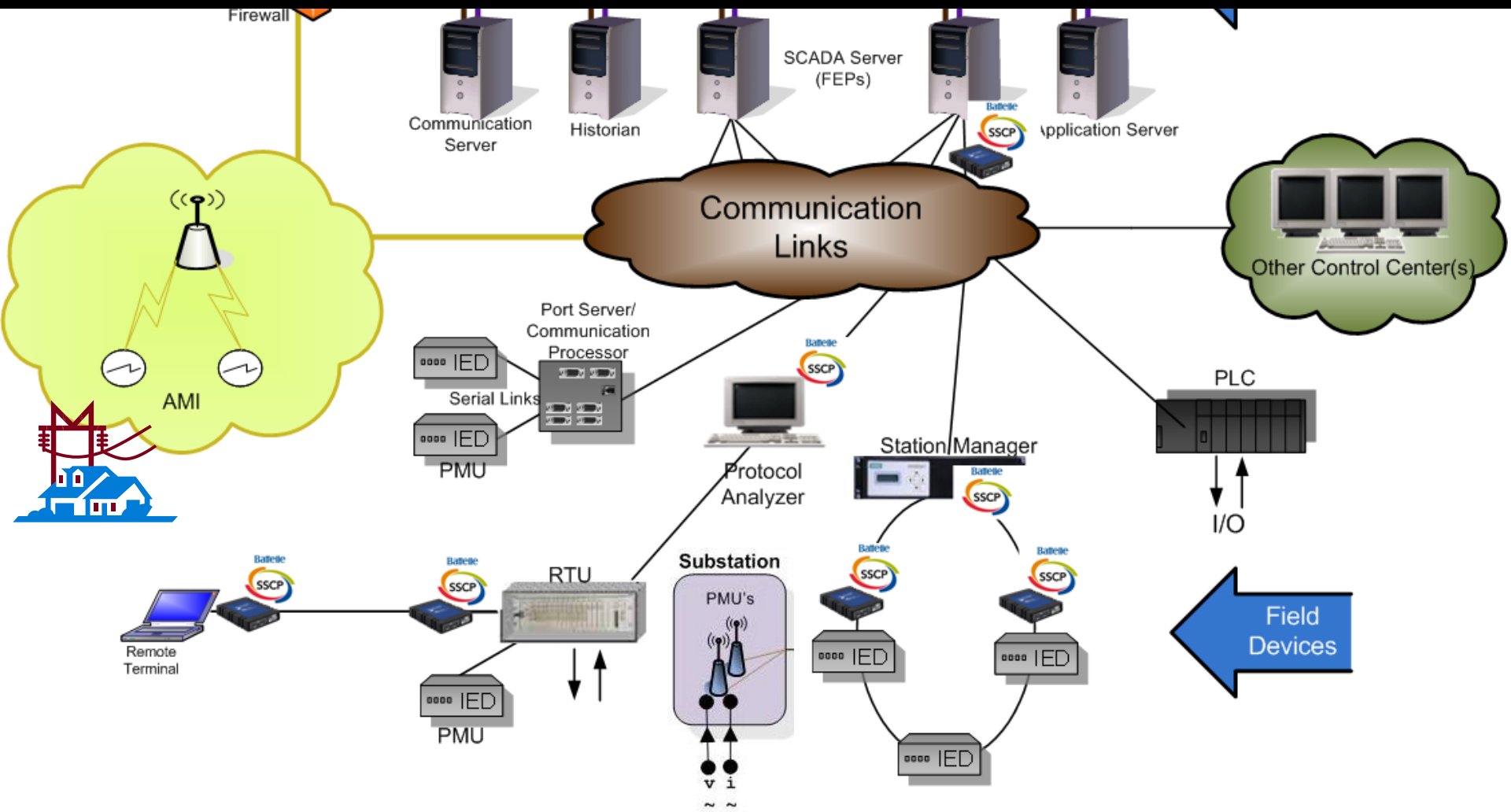
Participants:

- Sandia National Laboratories
- Schweitzer Engineering Laboratories
- Tennessee Valley Authority
- 7 Network Security Vendors

Success Stories:

- **Reference Taxonomy Completed**
  - Vocabulary and set of metrics
  - Describe functionality within the network security domain
  - Available to developers, vendors, and asset owners.
- **Designed, built, and tested a prototype of the SEL-3620 Ethernet Security Gateway**
  - Interoperable
  - Capable of operating with existing IT and control systems
  - Uses intuitive, menu-driven web-based interface to create an Internet Protocol Security (IPsec) virtual private network (VPN).
- **Demonstrated Interoperability**
  - DistribuTech (March 2010, Tampa)

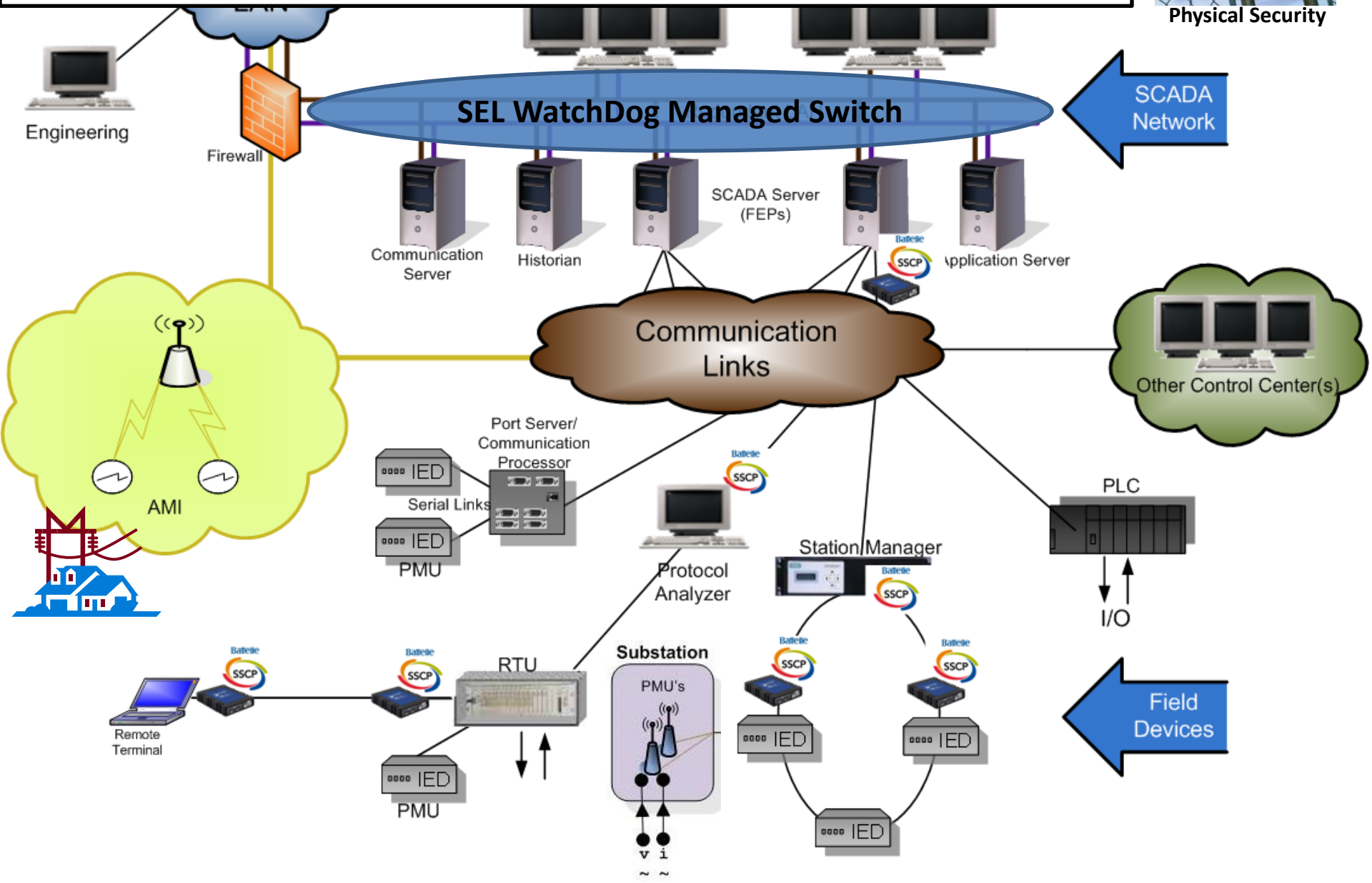
The 2010 DOE Cybersecurity for Energy Delivery Systems Program Industry-Led & National Laboratory-led Projects



Research, develop and commercialize a managed switch for the control system local area network (LAN) that uses whitelist filtering and performs deep packet inspection

Project Lead: Schweitzer Engineering Laboratories (SEL)
Partners: CenterPoint Energy Houston Electric, Pacific Northwest National Laboratories (PNNL)

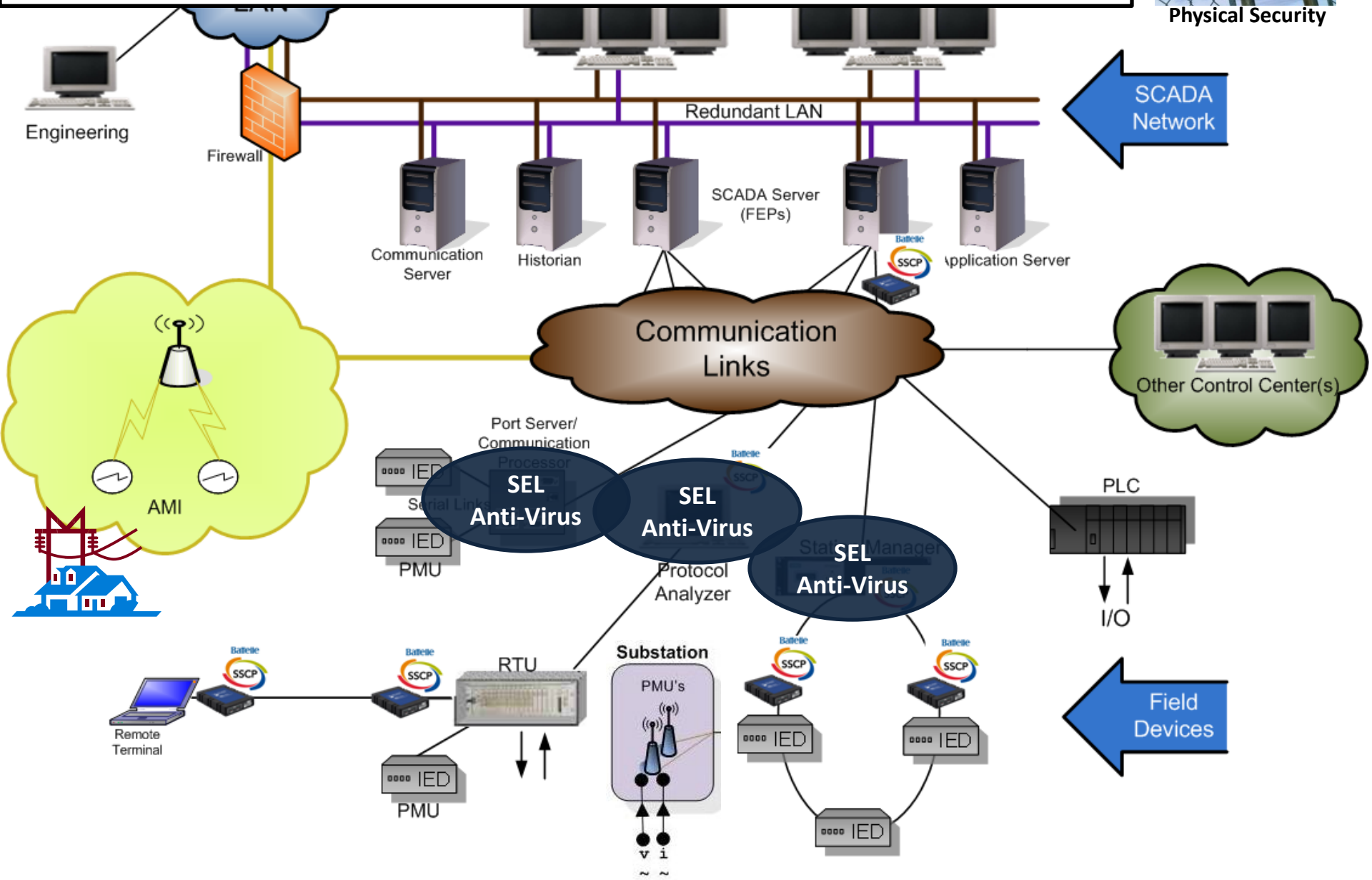
Physical Security



Research, develop and commercialize a whitelist antivirus for control systems solution to be integrated with Schweitzer Engineering Laboratories substation-hardened computers and communication processor

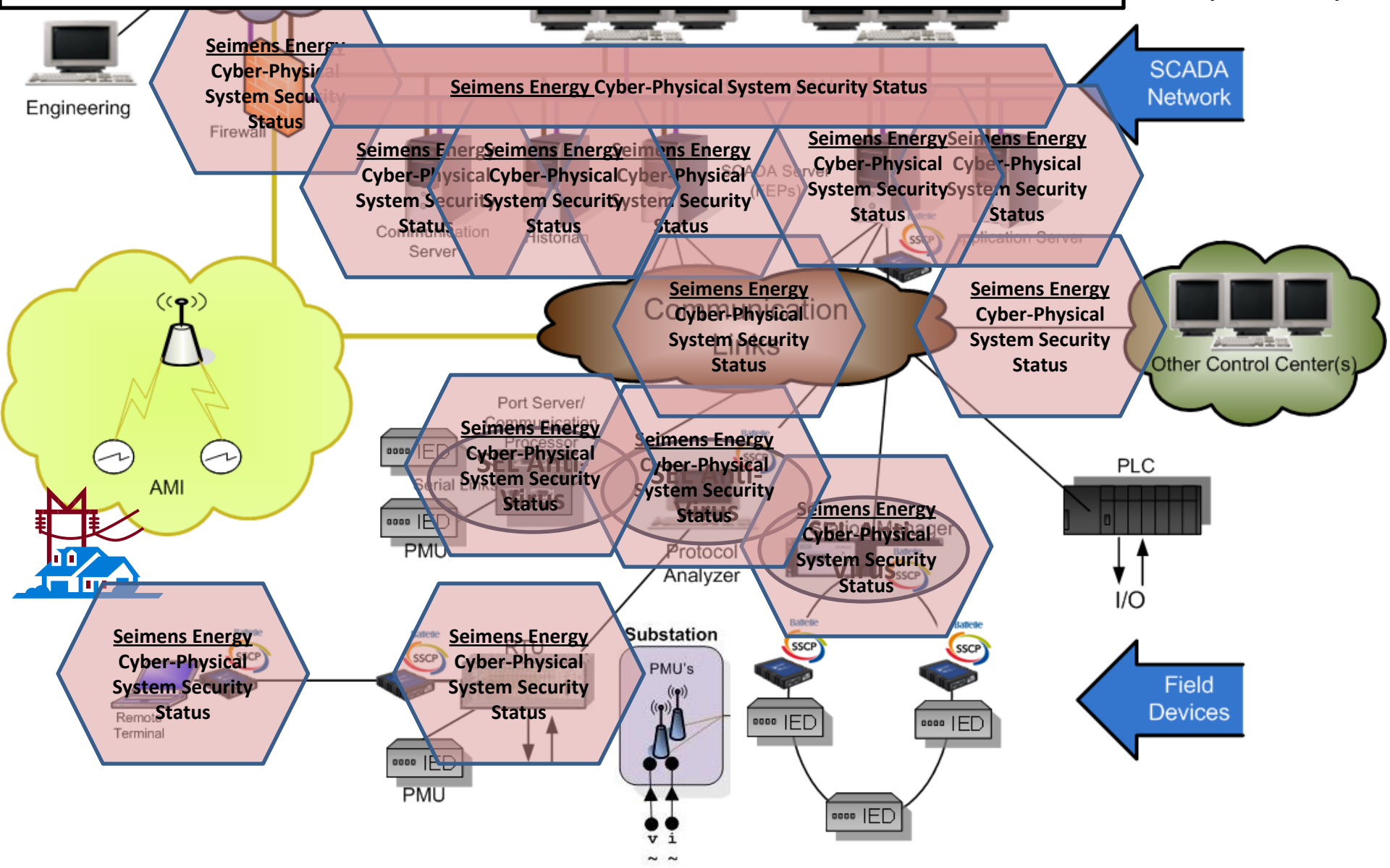
Project Lead: Schweitzer Engineering Laboratories (SEL)
Partners: Dominion Virginia Power (DVP), Sandia National Laboratories (SNL)

Physical Security



Develop and demonstrate a near-real-time cyber and physical security situational awareness capability for the control system environment

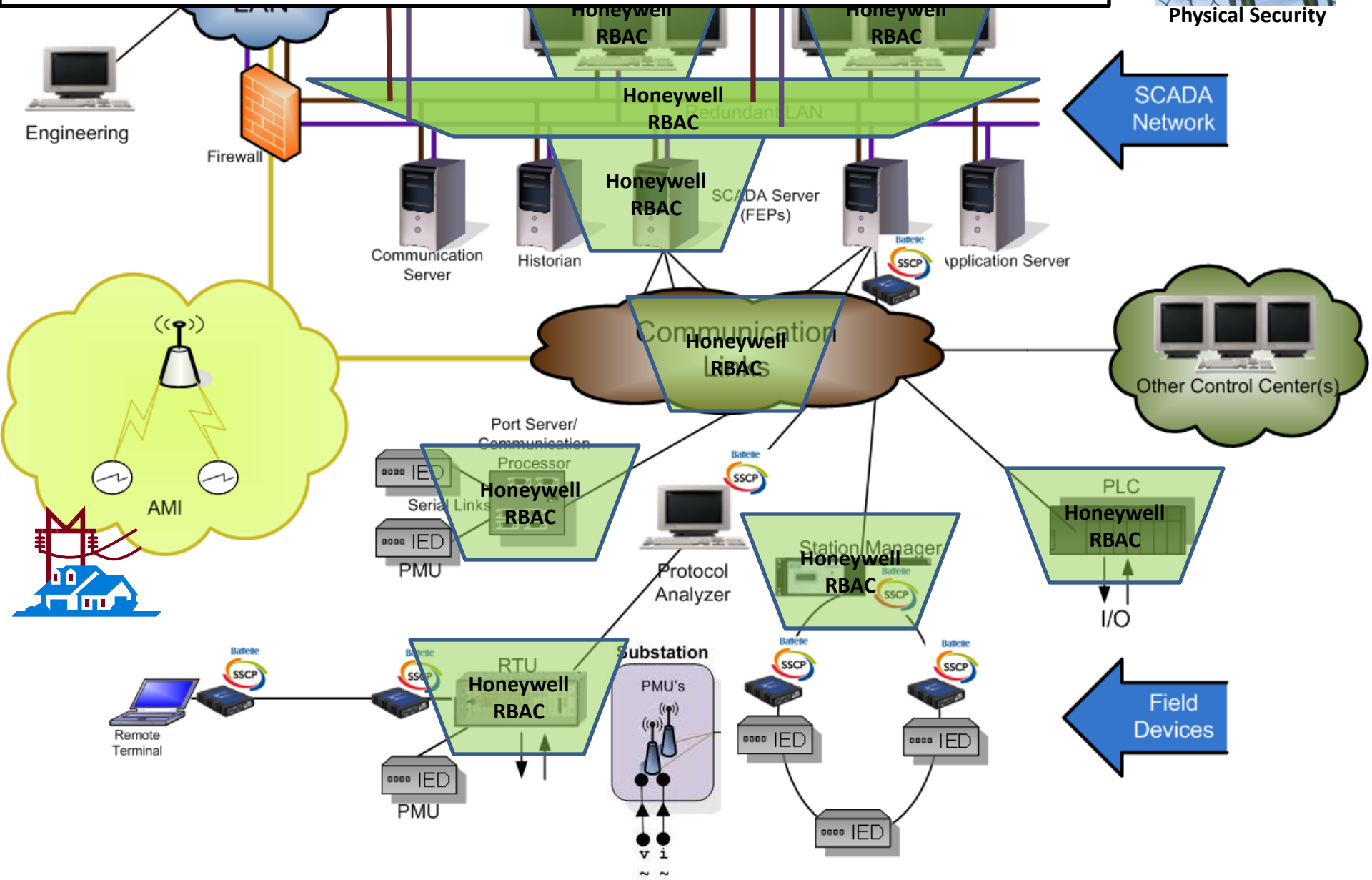
Project Lead: Siemens Energy, Inc.
Partners: Sacramento Municipal Utilities District, Pacific Northwest National Laboratories
Advisors: CenterPoint Energy, Omaha Public Power District, New York Power Authority



Research, develop and commercialize a role-based access control (RBAC) –driven, least privilege architecture for control systems

Project Lead: Honeywell International, Inc.
Partners: University of Illinois, Idaho National Laboratory

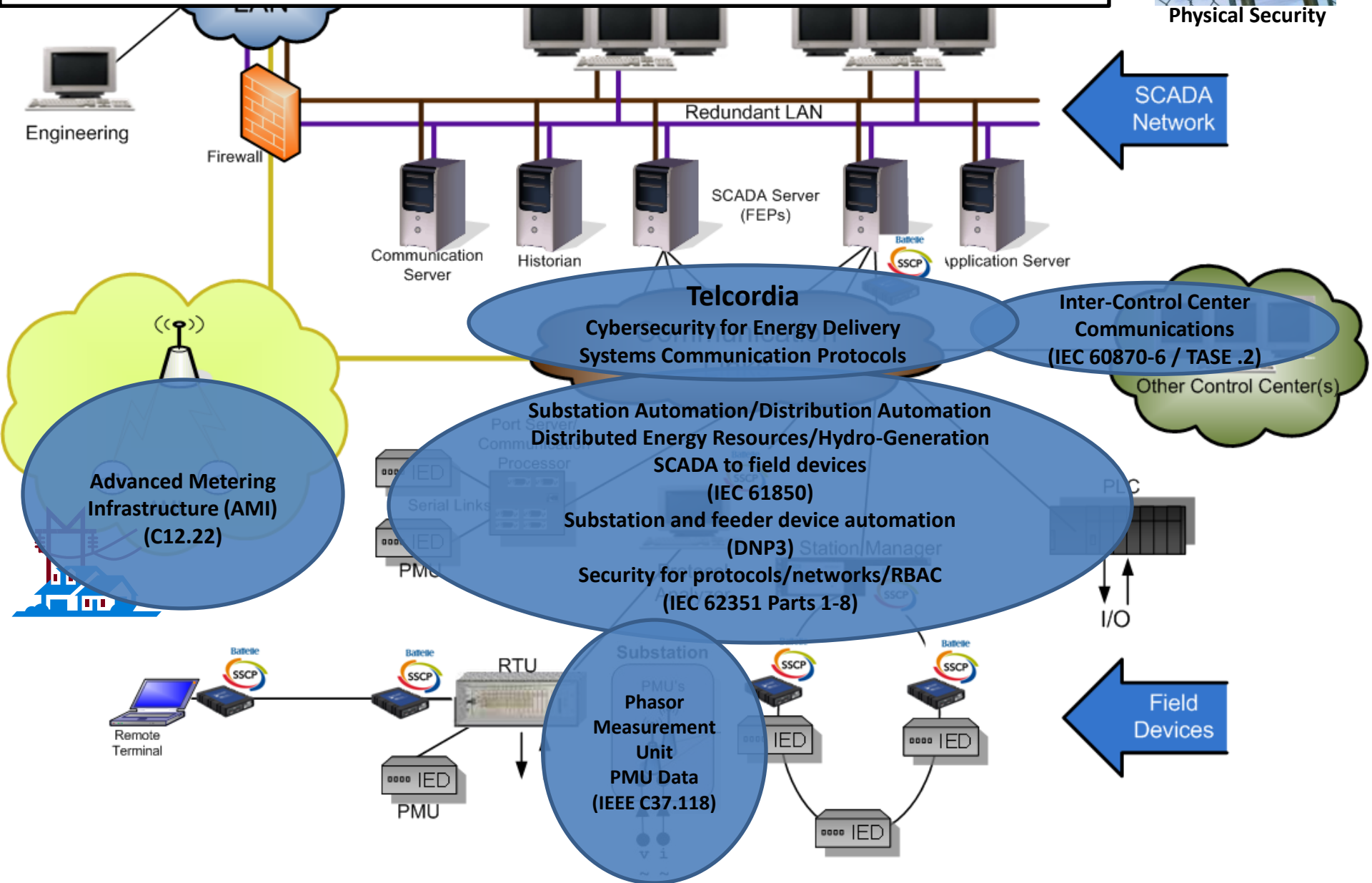
Physical Security



Research energy-sector communication protocol vulnerabilities, and develop mitigations that harden these protocols against cyber-attack and that enforce proper communications within energy delivery systems

Project Lead: Telcordia Technologies
Partners: University of Illinois, Electric Power Research Institute (EPRI), DTE Energy

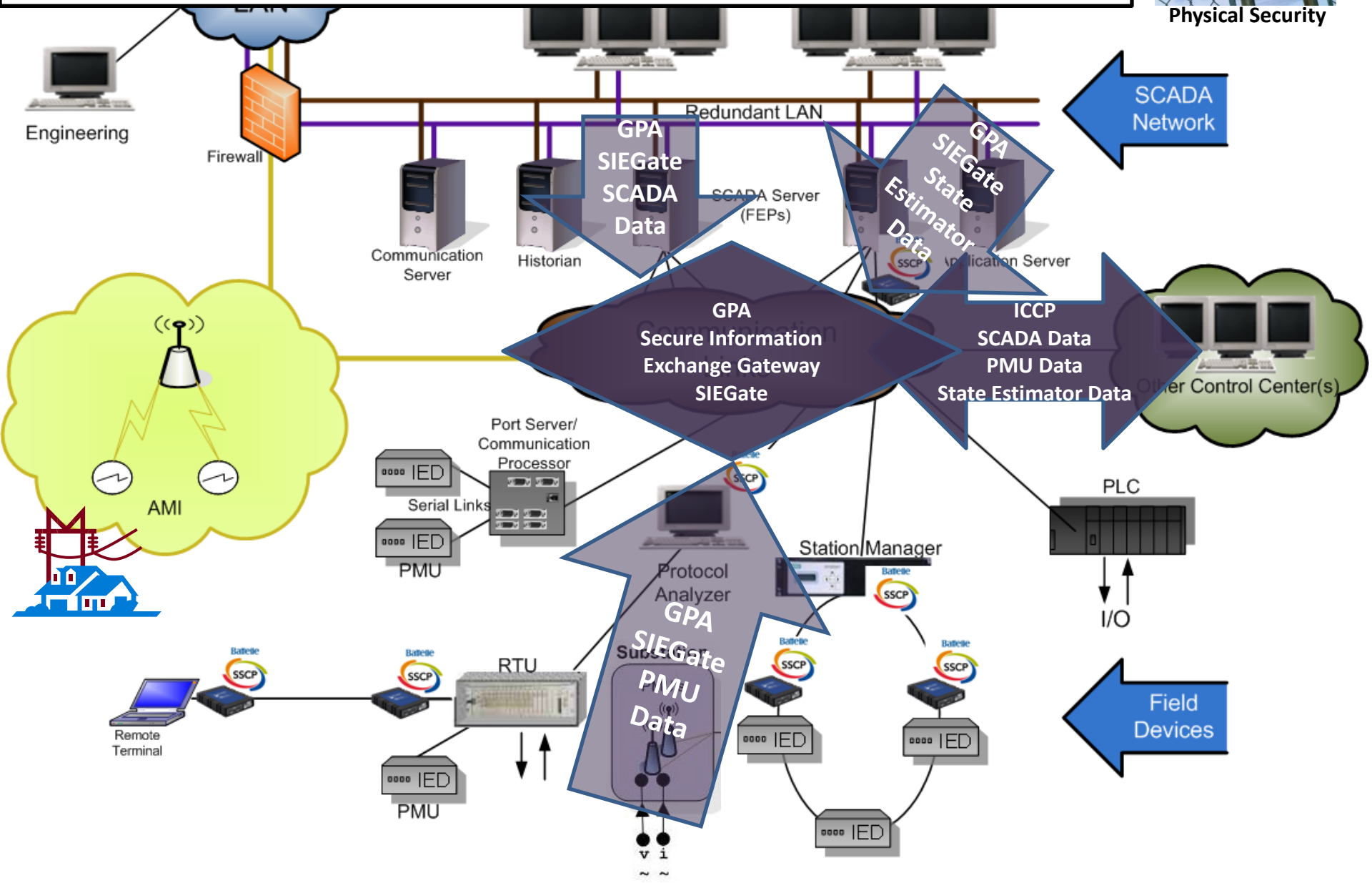
Physical Security



Research, develop and commercialize a Secure Information Exchange Gateway that provides secure communication of data between control centers

Project Lead: Grid Protection Alliance
Partners: University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D

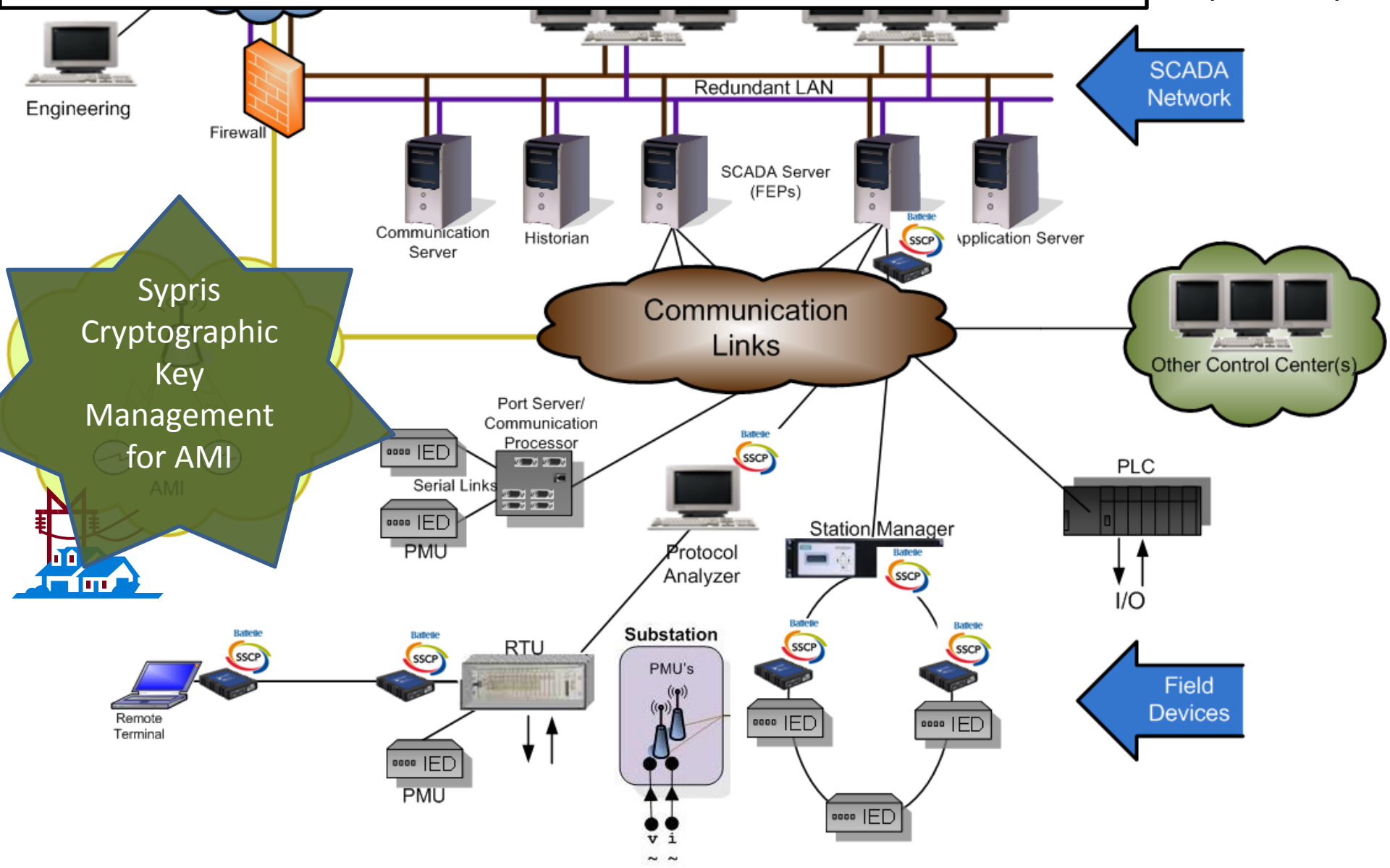
Physical Security



Research, develop and commercialize a cryptographic key management capability scaled to secure communications for the millions of smart meters within the Smart Grid Advanced Metering Infrastructure

Project Lead: Sypris Electronics
Partners: Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), Oak Ridge National Laboratory (ORNL), Electric Power Research Institute (EPRI)

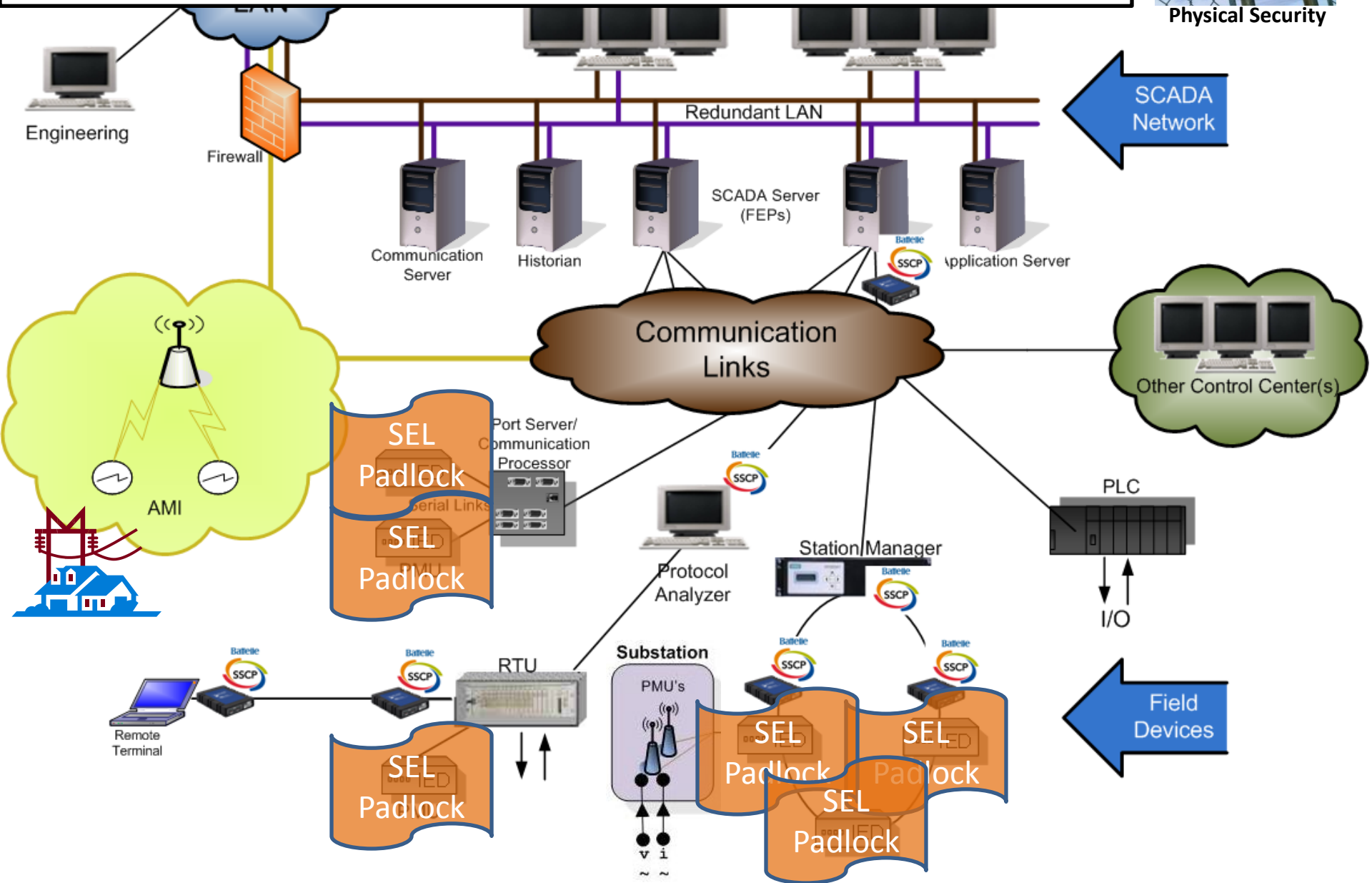
Physical Security



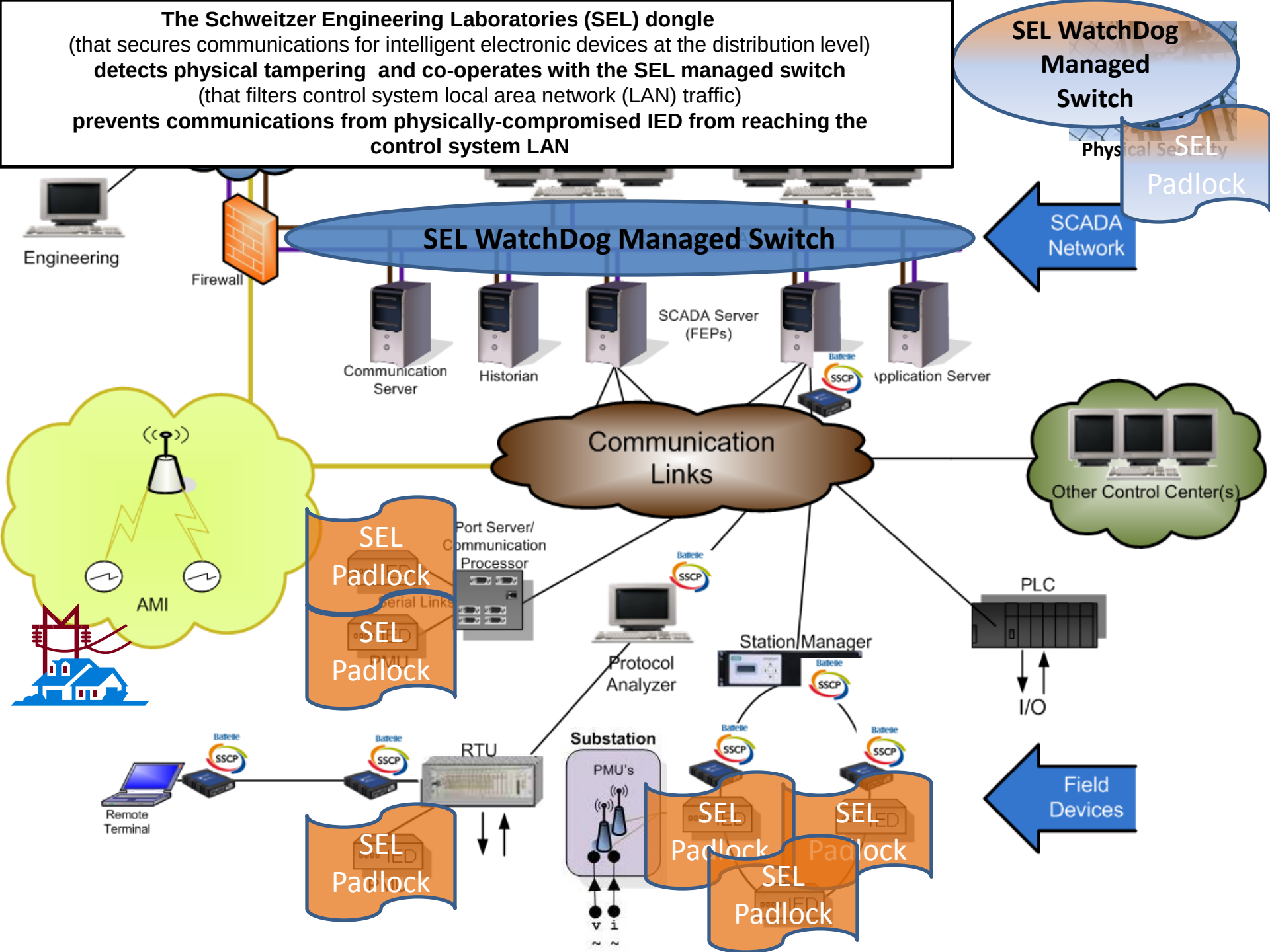
Research, develop and commercialize a low-power, small-size dongle that provides strong authentication, logging, alarming and secure communications for intelligent field devices operating at the distribution level

Project Lead: Schweitzer Engineering Laboratories (SEL)
Partners: Tennessee Valley Authority (TVA), Sandia National Laboratories (SNL)

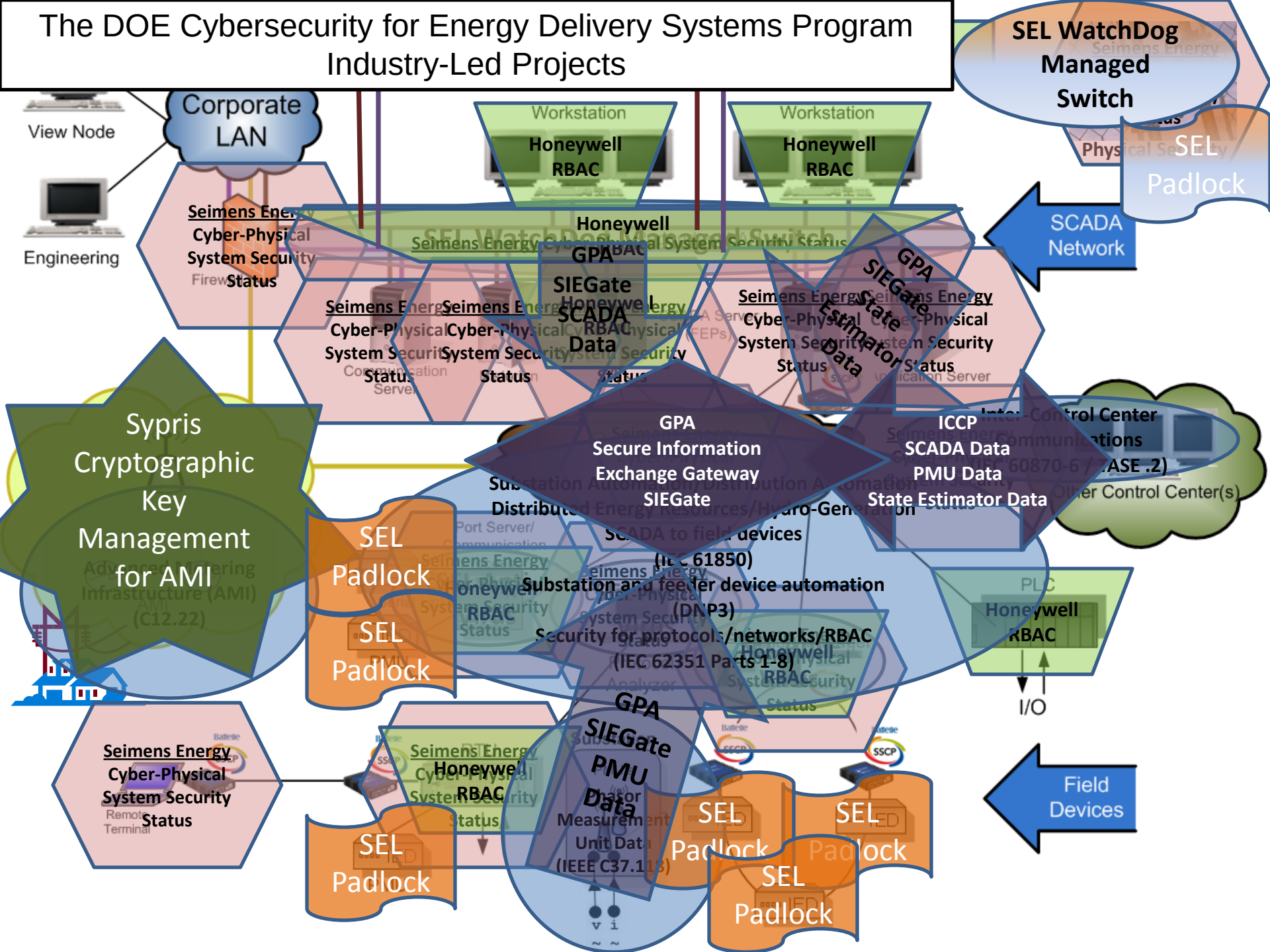
Physical Security



The Schweitzer Engineering Laboratories (SEL) dongle
(that secures communications for intelligent electronic devices at the distribution level)
detects physical tampering and co-operates with the SEL managed switch
(that filters control system local area network (LAN) traffic)
prevents communications from physically-compromised IED from reaching the control system LAN



The DOE Cybersecurity for Energy Delivery Systems Program Industry-Led Projects



Trustworthy Cyber Infrastructure for the Power Grid

(TCIPG, University-Led Collaboration)

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

Recent Papers

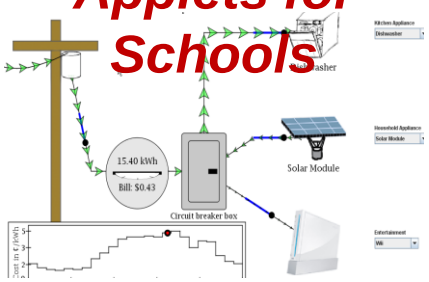
Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

Katherine M. Rogers, *Student Member, IEEE*, Ray Klump, *Member, IEEE*, Himanshu Khurana, *Senior Member, IEEE*, Thomas J. Overbye, *Fellow, IEEE*

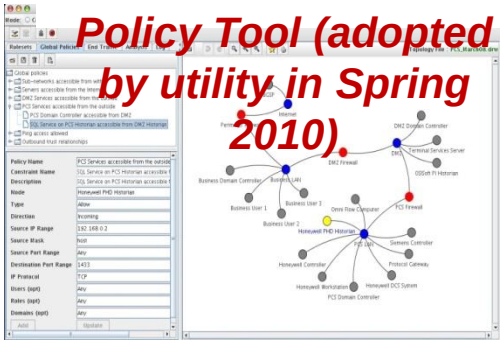
Building Security In

Smart-Grid Security Issues

Applets for Schools



TCIPG NetAPT Network Access Policy Tool (adopted by utility in Spring 2010).



Funding

$18.8 million over 5 years (2009-2014)

from DOE and DHS

Facilities

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

Game-changing R&D Needed to Make *Survivable* Systems a Reality

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

CMU-SEI 2011 Research

System Simplex-based intrusion detection and mitigation

- Augments SCADA systems with a safety controller that takes over if the primary controller moves out of a safety envelope or exhibits changes in its timing profile due to changes in executed code.

Designing SCADA systems for the self-verifiability of their security and survivability (seed project)

- Investigating decentralized, network-based distributed information fusion to identify and isolate subverted SCADA system components.

Predictable encryption in tightly constrained real-time systems (seed project)

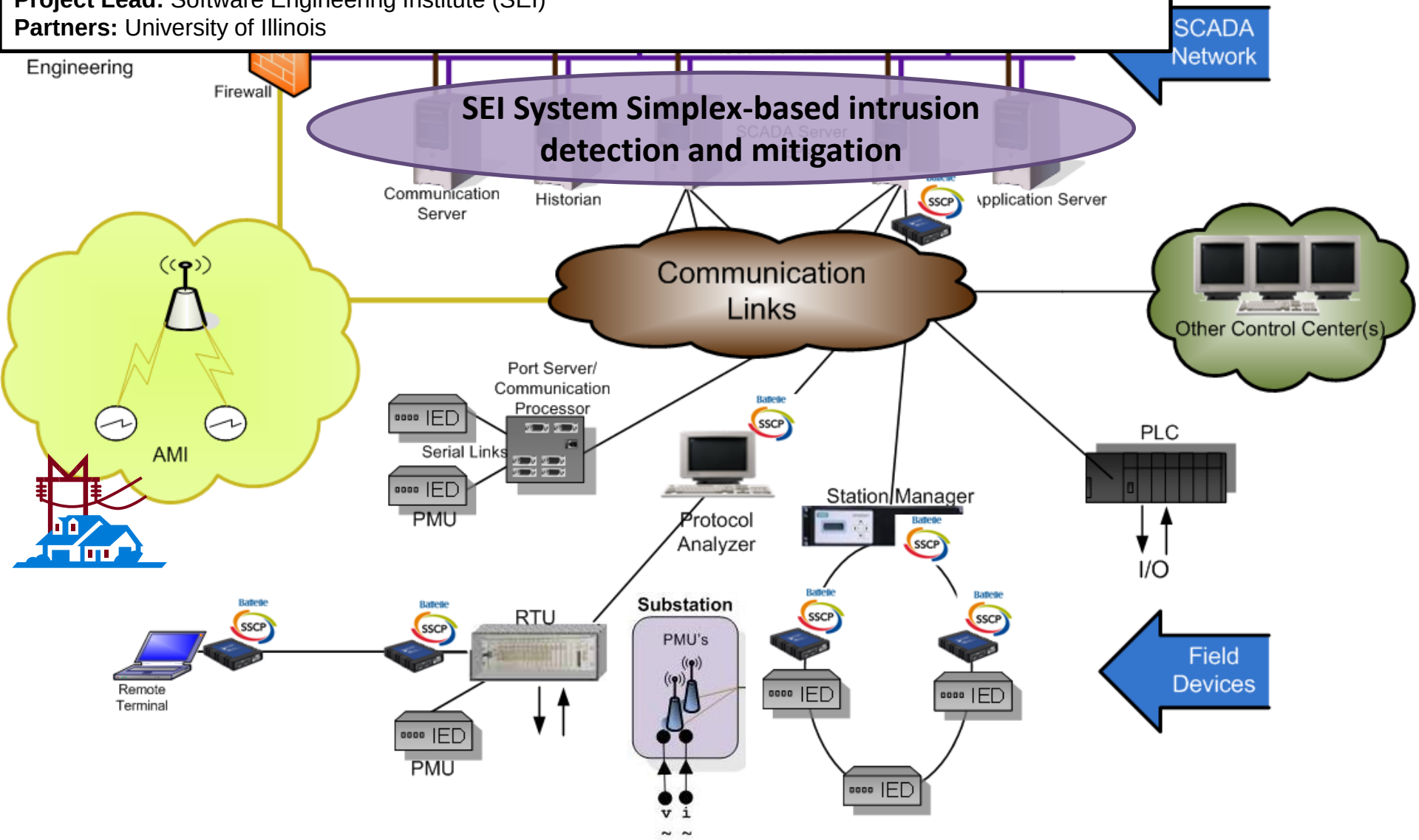
- Investigating techniques that diminish the impact of using encrypted communication in tightly time-constrained reactive system components by exploiting hidden slack and using efficient encryption techniques.

Develop and demonstrate real-time intrusion detection and mitigation based on analytic redundancy and timing analysis. Uses the System Simplex architecture, adding a control subsystem to SCADA systems that

- automatically takes over when the primary control subsystems move out of a safety envelope or their timing profile changes due changes in executed code
- is less efficient, but simpler, and consequently easily verifiable
- is implemented in dedicated hardware (FPGA)

Project Lead: Software Engineering Institute (SEI)
Partners: University of Illinois

Physical Security

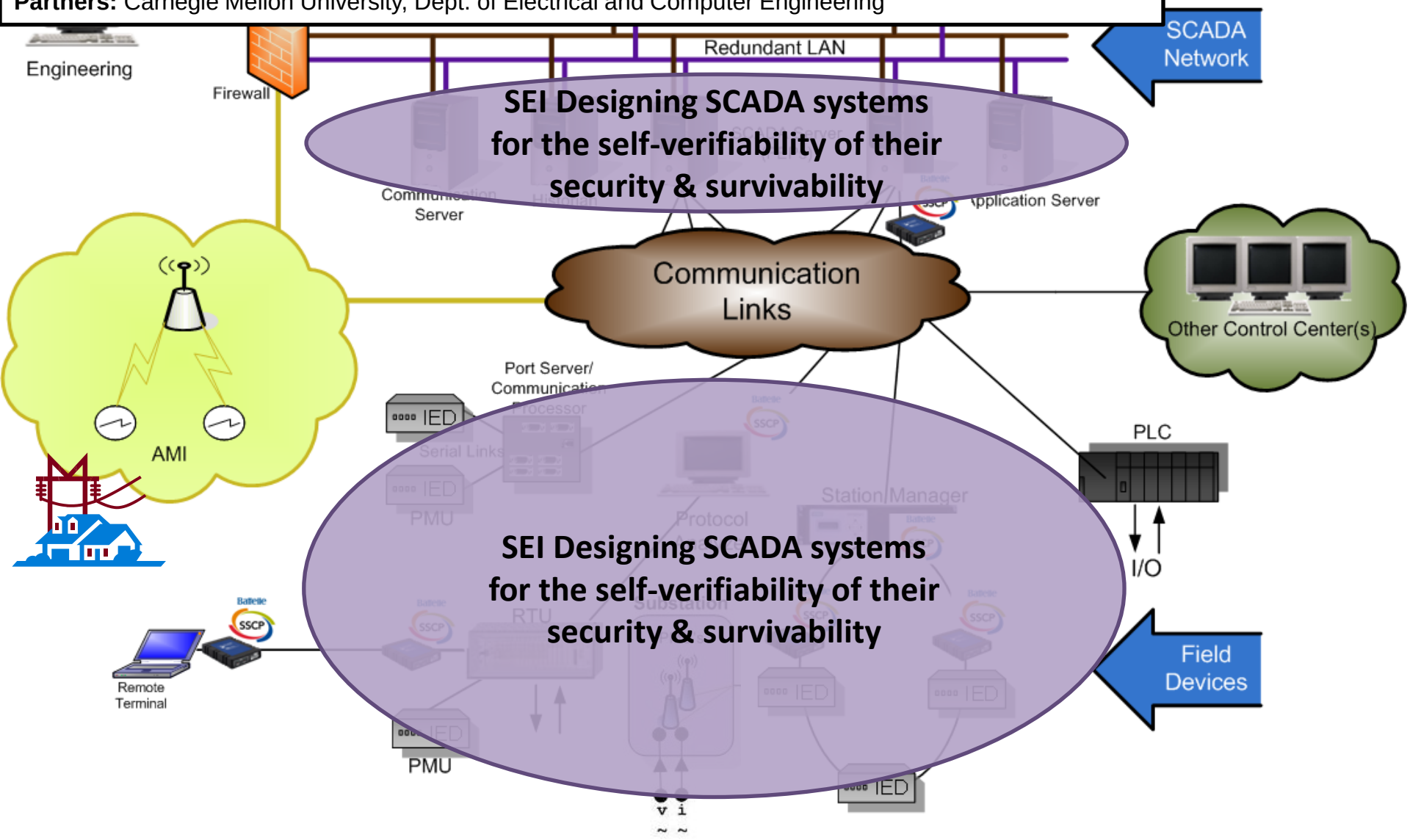


Perform decentralized, network-based distributed information fusion to identify and isolate subverted SCADA system components, using

- autonomous agent-based distributed information fusion techniques,
- knowledge of electrical properties of power grid, and
- knowledge of SCADA functions and topology.

Project Lead: Software Engineering Institute (SEI)
Partners: Carnegie Mellon University, Dept. of Electrical and Computer Engineering

Physical Security



SEI Designing SCADA systems for the self-verifiability of their security & survivability

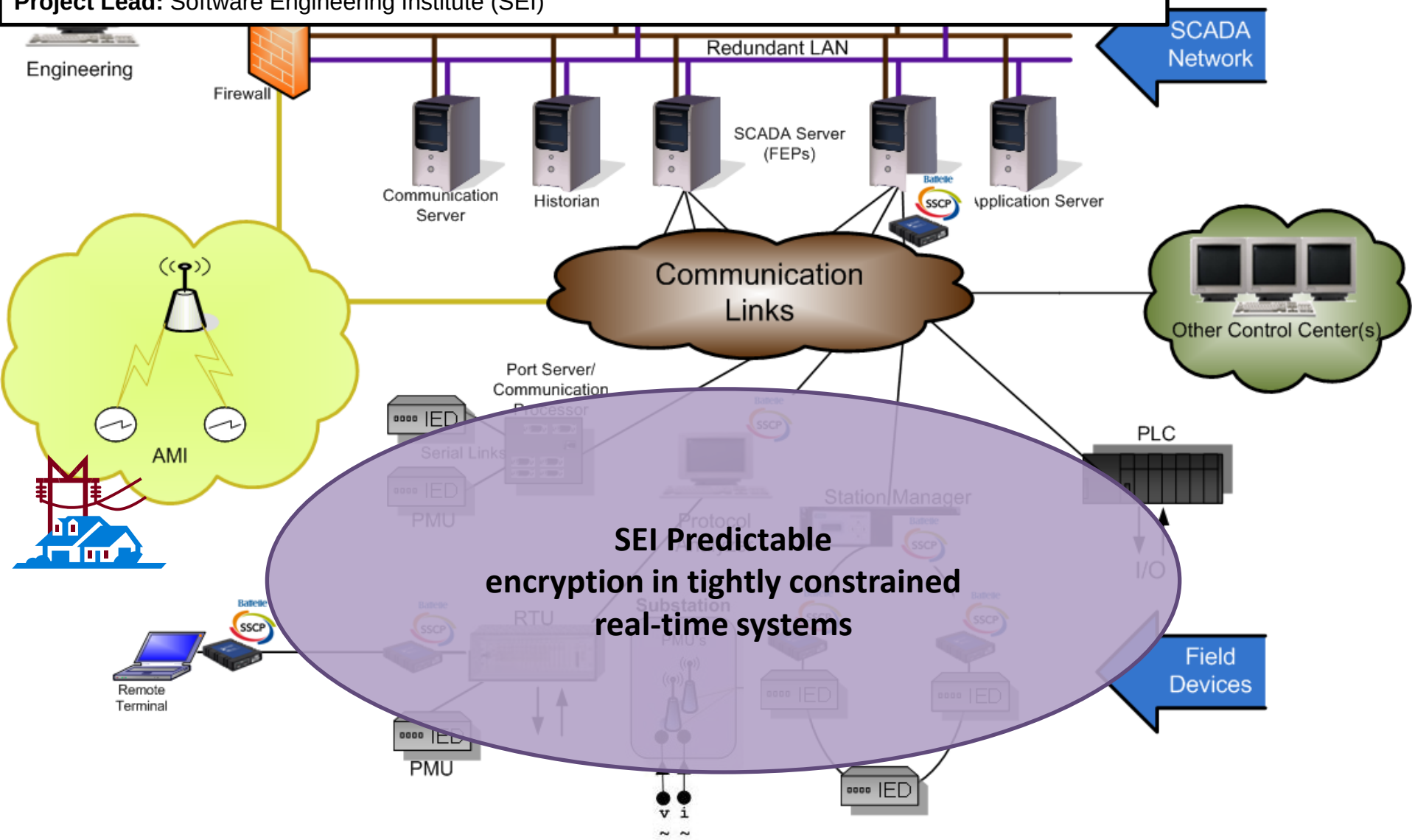
SEI Designing SCADA systems for the self-verifiability of their security & survivability

Develop techniques to diminish the impact of the using encrypted communication in tightly time-constrained reactive system components by

- separating critical and non-critical computation, removing non-critical computation from the critical path, and exploiting previously hidden slack
- using efficient encryption techniques such as the use of one-time pad encryption and pre-computation (during slack) of elements of encryption computations

Project Lead: Software Engineering Institute (SEI)

Physical Security



SEI Predictable encryption in tightly constrained real-time systems

CEDS 2010 Research Call National Laboratory-Led Projects

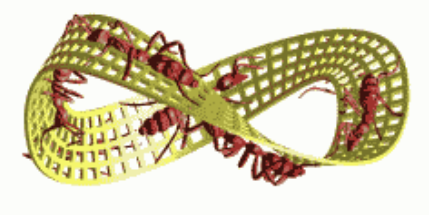
- High-Level (4th Gen) Language Microcontroller Implementation
  - Limits direct access to device memory
  - Hardens microcontrollers against low-level cyber-attacks (such as buffer overflow)
  - Develop standardized security library to implement secure authentication and data encryption down to the hardware level
    - **National Laboratory Lead:** Idaho National Laboratory (INL)
    - **Partners:** Siemens Corporate Research
- Control System Situational Awareness Technology Interoperable Tool Suite
  - Shows all control system network communications taking place (Sophia);
  - Collects all wireless mesh network data message routes;
  - Reports unexpected behavior (Mesh Mapper);
  - Monitors system health;
  - Distinguishes between component failure and cybersecurity incidents (Intelligent Cyber Sensor);
  - Performs data fusion for situational awareness (Data Fusion System);
  - Determines global effects of local firewall rules (NetAPT)
    - **National Laboratory Lead:** Idaho National Laboratory (INL)
    - **Partners:** Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho

CEDS 2010 Research Call National Laboratory-Led Projects

- Automated Vulnerability Detection For Compiled Smart Grid Software
  - Performs static analysis of compiled software and device firmware
    - **National Laboratory Lead:** Oak Ridge National Laboratory (ORNL)
    - **Partners:** Software Engineering Institute (SEI), The University of Southern Florida (USF), EnerNex Corporation
- Next Generation Secure, Scalable Communication Network for the Smart Grid
  - Uses adaptive hybrid spread-spectrum modulation format
  - Provides superior resistance to multipath, noise, interference and jamming
  - Appropriate for high quality-of-service (QoS) applications.
    - **National Laboratory Lead:** Oak Ridge National Laboratory (ORNL)
    - **Partners:** Pacific Northwest National Laboratory (PNNL), Virginia Tech, OPUS Consulting, Kenexis Consulting
- Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector
  - Across multiple organizational boundaries found in Smart Grid architectures
  - Uses *Digital Ants* - many lightweight and mobile agents whose activities

    Correlates to produce emergent behavior

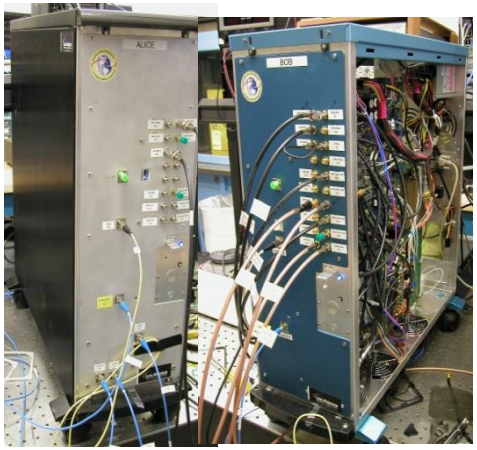
    Draws attention to anomalous conditions--potentially indicative of a cyber-incident



    - **National Laboratory Lead:** Pacific Northwest National Laboratory (PNNL)
    - **Partners:** Wake Forest University, University of California-Davis, Argonne National Laboratory (ANL), SRI International

LANL Quantum Communications Testing for Smart Grid Applications

- Apply new and existing hardware to testing with SmartGrid hardware and data



LANL third generation QC hardware (F3) will provide electronic control for the transmitter and the receiver

Miniaturized electro-optics will be used in the QC transmitter—small enough to deploy with SCADA hardware

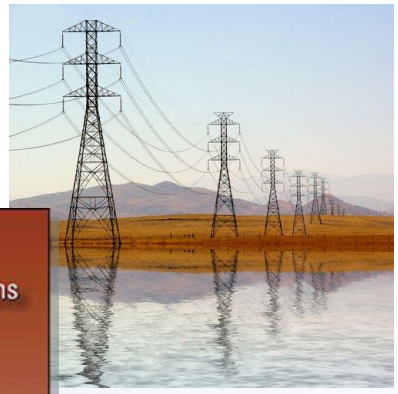
- Goals:
  - Provide hardware for data protection tests
  - Test the ability of a QC system to protect realistic data volume/bandwidth without increasing latency or error rate
  - Increase data integrity and authentication
  - Analyze denial-of-service resistance and protection switching capability

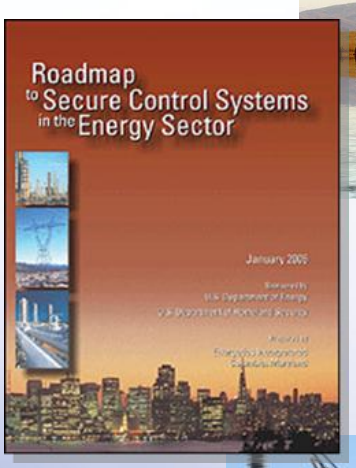
Jane E. Nordholt
Los Alamos National Laboratory
P-21, M/S D434
JNordholt@LANL.gov
505-667-3807

ORNL Grid Security with Quantum Architectures and Resources (Grid SQuARe)

Cyberspace Sciences & Information Intelligence (CSIIR) Group

Computational Sciences & Engineering Division





Problem Statement:

- **The electric power industry is embarking upon an infrastructure transformation that will result in a national power grid that is more responsible, reliable, and resilient. While the final form of the grid will not be known for quite some time, it is clear that a smarter grid will make better use of information. With increased information flow comes increased vulnerability to cyber attacks.**

Technical Approach:

- **We are studying the feasibility of quantum information approaches to securing the electric grid, taking into account the unique topology of the grid, as well as the capabilities of various quantum technologies. Using this study as a starting point, we will develop quantum devices that can be integrated into smart-grid instruments.**

Benefit:

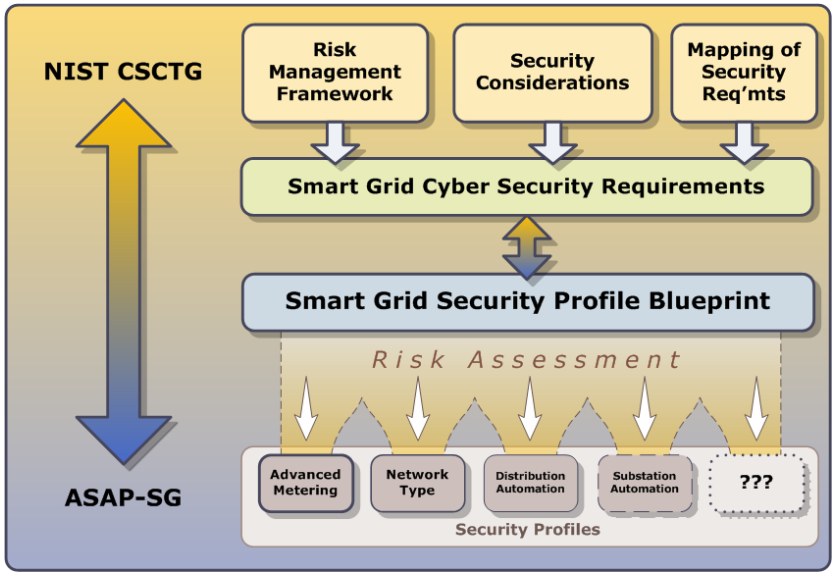
- **Comprehensive implementation plan for quantum approaches to electric grid security.**
- **Quantum technologies developed explicitly for electric grid implementation.**

Point of Contact: **Warren P. Grice, Ph.D.**
(865) 241-2061
gricew@ornl.gov

OAK RIDGE National Laboratory

ASAP-SG
Advanced Security Acceleration Project - Smart Grid

- Industry-government collaboration (50/50 cost share) to accelerate security standards development for Smart Grid (May 2009 – till finished)
- Completed *"Security Profile for Advanced Metering Infrastructure, v 1.0"* - major contribution to NISTIR 7628
- Security Profile drafts for 3rd Party Data Access and Distribution Automation completed, HAN getting started
- DOE funding Software Engineering Institute and Oak Ridge National Laboratory working with Enernex
- Industry sponsors
  - American Electric Power
  - Con Edison
  - Consumers Energy
  - Florida Power & Light
  - Southern California Edison
  - Oncor
  - BC Hydro

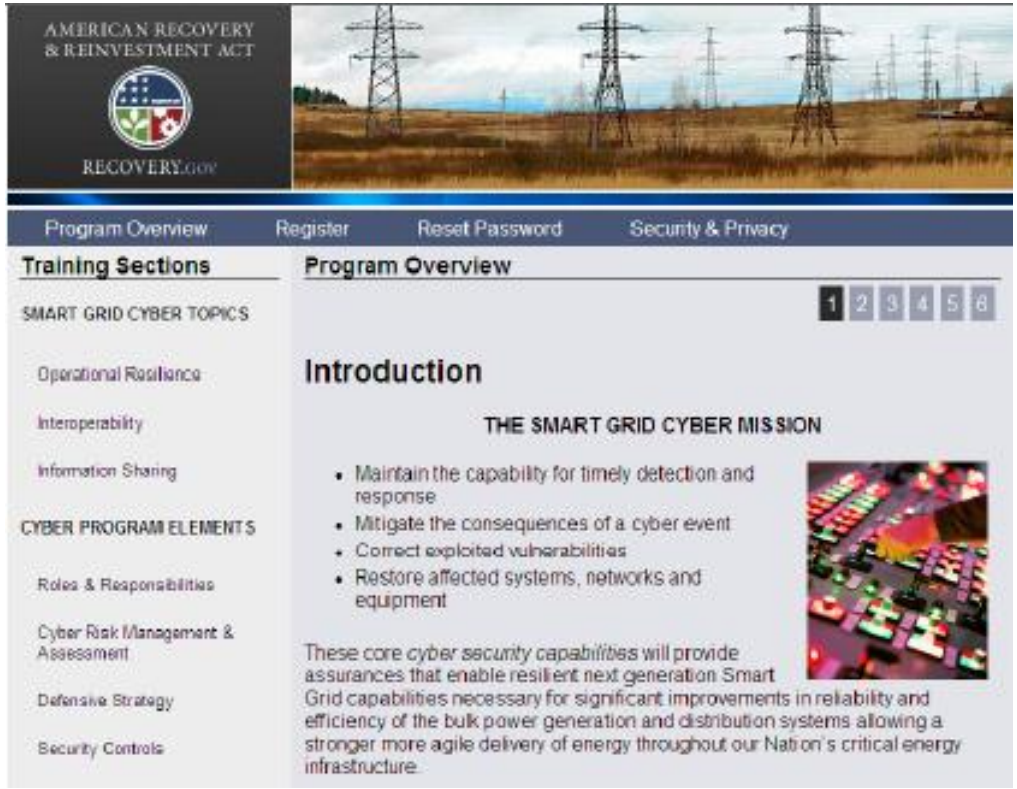


Cybersecurity - *Critical to Smart Grid Success*

- Organized interagency group (DOE, NIST, FERC, DHS, CIA) to develop cyber security requirements for RFP
- Cyber security plans - major factor in Merit Review
- Utilized technical merit review team and cybersecurity SME team to provide independent reviews
- Risk assessment required
- DOE will work with recipients to ensure cyber security is adequate

ARRA Cyber Security Website

www.ARRAsmartgridcyber.net

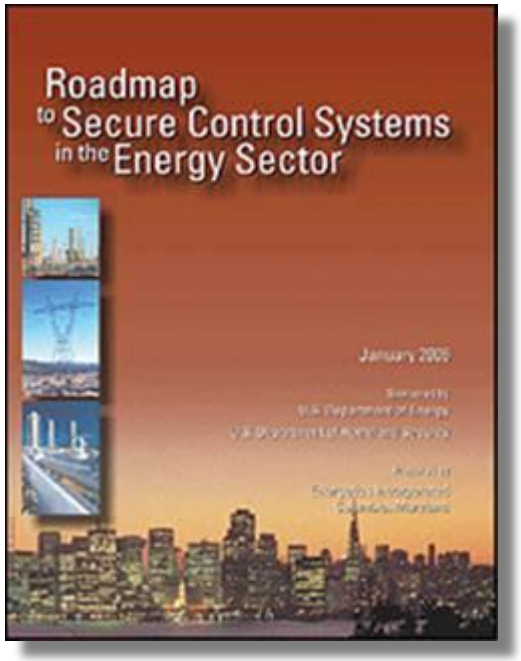


For more information …

ie Roadmap

interactive energy Roadmap to secure control systems

Visit:

www.oe.energy.gov/controlsecurity.htm

www.controlsystemsroadmap.net