
National Nuclear Security Administration


U.S. DEPARTMENT OF HOMELAND SECURITY


NATIONAL SCIENCE FOUNDATION


The Office of the National Coordinator for
Health Information Technology


NATIONAL INSTITUTES OF HEALTH


NIST
National Institute of
Standards and Technology


DARPA

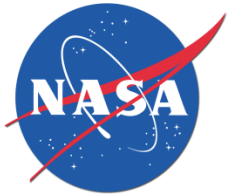

NITRD


NOAA
NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE


UNITED STATES
ENVIRONMENTAL PROTECTION AGENCY


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


NASA


Office of Science
U.S. DEPARTMENT OF ENERGY

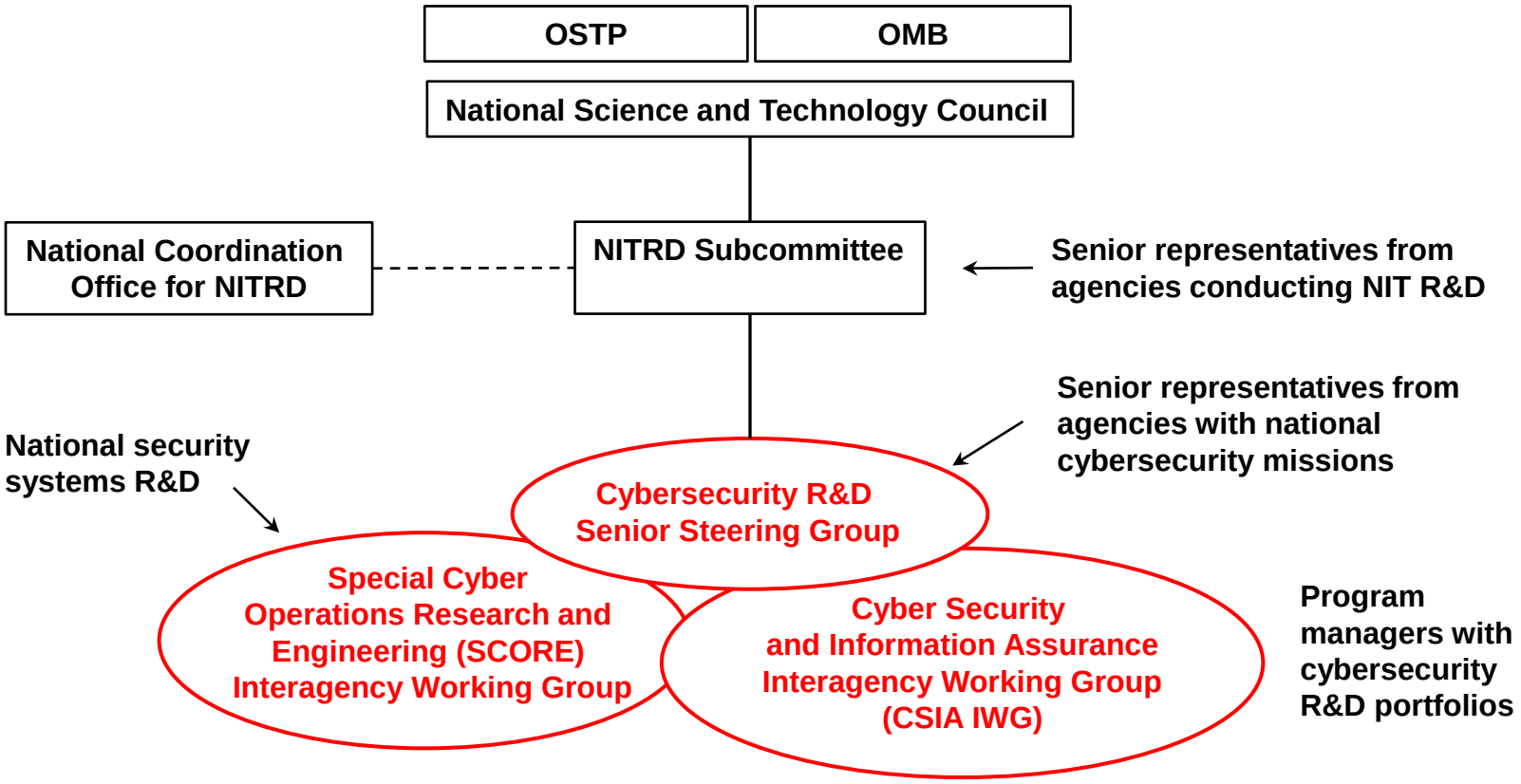

AHRQ


NATIONAL
ARCHIVES

Networking and IT R&D (NITRD) Program

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Support NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Scope
  - Approximately $4B/year across 14 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

NITRD Structure for Cybersecurity R&D Coordination



Coordinated Effort on Game-Changers

- It's about trustworthiness of digital infrastructure
  - Security, reliability, resiliency, privacy, usability
  - How can we:
    - Enable risk-aware safe operations in compromised environments
    - Minimize system risk while increasing adversaries' costs and exposure
    - Support informed trust decisions, allowing for effective risk/benefit analyses and implementations
- Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda
  - Comprehensive National Cybersecurity Initiative, Cyberspace Policy Review: http://www.whitehouse.gov/cybersecurity
  - Aneesh Chopra, President's Chief Technology Officer
  - Howard Schmidt, White House Cybersecurity Coordinator
  - NITRD Senior Steering Group, Interagency WGs CSIA, …

For More Information

Tomas Vagoun, PhD
CSIA IWG Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

http://www.nitrd.gov
http://cybersecurity.nitrd.gov

Federal Cybersecurity Research and Development Program: Strategic Plan

Federal Cybersecurity Research and Development Program: Strategic Plan

Donna Dodson

Division Chief Cybersecurity Advisor, Information Technology Lab, National Institute of Standards and Technology (NIST)

Presented by Federal NITRD Program

July 18, 2011

Tailored Trustworthy Spaces: Solutions for the Smart Grid Workshop

Federal Cybersecurity R&D Strategic Thrusts

- Research Themes
- Science of Cyber Security
- Transition to Practice
- Support for National Priorities

R&D Coordination Through Themes

- Theme ≠ Hard Problem
- To compel a new way of operating / doing business
- To attack underlying causes to bring about changes
- To provide shared vision of desired end state
- Established through robust community discussion of what matters
- Recognizes that independent thinking is vital to good research

Research Themes

Initial Themes (2010)

- Tailored Trustworthy Spaces
  - Supporting context specific trust decisions
- Moving Target
  - Providing resilience through agility
- Cyber Economic Incentives
  - Providing incentives to good security

New Theme (2011)

- Designed-in Security
  - Developing and evolving secure software systems

Annually re-examine themes, enrich with new concept, provide further definition or decomposition

Tailored Trustworthy Spaces

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Yet we tend to treat the cyber world as a homogenous, undifferentiated space

⇨ TTS: a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

TTS Paradigm

- Users can select/create different environments for different activities satisfying variety of operating capabilities
  - Confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to create new environments with mutually agreed characteristics and lifetimes
- Must be able to base trust decisions on verifiable assertions

Moving Target

- Controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

Moving Target Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- Shift burden of processing onto attackers

Cyber Economics & Incentives

- A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - New theories and models of investments, markets, and the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models and support for “personal data ownership”

CEI Paradigm

- Promotion of science-based understanding of markets, decision-making and investment motivation
  - Security deployment decisions based on knowledge, metrics, and proper motivations
  - Promote the role of economics as part of that understanding
- Creation of environments where deployment of security technology is balanced
  - Incentives to engage in socially responsible behavior
  - Deterrence for those who participate in criminal and malicious behavior

Designed-in Security

- Designing and developing SW systems that are resistant to attacks
- Generating assurance artifacts to attest to the system's capabilities to withstand attacks

Designed-in Security Paradigm

- Require verifiable assurance about system's attack-resistance to be natively part of the SW design, development, and evolution lifecycle
- Enable reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and the required assurance evidence
- Stimulate further developments in methods and tools for detecting flaws in SW

Example NIST programs

- Moving Target
  - Select NIST programs reduce and dynamically modify the attack surface through automation (by reducing/eliminating exploits of vulnerabilities and by configuration automation). E.g.,
    - NVD, SCAP, Continues Monitoring & Reporting, Attack Graphs with SCAP, Remediation are components in achieving MT objectives
    - As frequency hopping is key to preventing the jamming of communications, automation (defining and changing system config. state) maybe key to frustrating cyber attacks
- Trusted Tailored Spaces
  - Policy Machine can tailor policy through configuration alone to the specific access control policy needs of enterprises and their missions
    - Science of Security: Based on a unification theory of access control and data services

Example NIST programs

- Cyber Economics
  - NIST cryptographic algorithms are designed to preclude cost-effective attacks for decades considering Moore's Law
    - Attacks on protocols and applications must focus elsewhere!
- Designed-in Security
  - Hardware Roots of Trust establish a solid foundation for software security mechanisms
    - A secure BIOS is a fundamental building block for trustworthy desktop and laptop systems
    - Industry acceptance of NIST BIOS Protection Guidelines will have immediate impact, and support emerging trust measurements

Federal Cybersecurity R&D Strategic Thrusts

- Research Themes
- ⇨Science of Cyber Security
- Transition to Practice
- Support for National Priorities

Science of Cyber Security

- A strategic research priority on the *science of security* to
  - Organize the knowledge in the field of security
  - Investigate universal concepts that are predictive and transcend specific systems, attacks, and defenses
  - Resulting in a cohesive understanding of underlying principles to enable investigations that impact large-scale systems
  - Enable development of hypotheses subject to experimental validation
  - Support high-risk explorations needed to establish such a scientific basis
  - Form public-private partnerships of government agencies, universities, and industry

Security Science

Today

- Mature **Crypto** Science
  - Adversary Models
  - Work Factor Metrics
  - Tempest, Physical Eng'g, etc.
- Formal Analysis Technology
  - Correctness Techniques/Tools
  - Protocol Verification
  - Efficient State Space Analysis
- Ad Hoc Cyber Engineering
  - Informal principles
  - Rudimentary Adversary Models
  - Process oriented Metrics
- Fragmented SoS Community

Future

- Mature **Cyber Security** Science
  - Formal Cyber Adversary Models
  - Cyber Security Metrics
  - Design & Implementation Support
- Objective Evaluation Techniques
  - Rigorous Toolset
  - Repeatable
- Trust Engineering Methodology
  - Construction/Composition Tools
  - Principled Design
  - Formal Discipline
- Coordinated SoS Community
  - Persistent, Self sustaining
  - Collaborative Structures (VO, Interest Grps)

Science of Cyber Security Questions

- What can we take from other sciences?
  - Are there any “laws of nature” in cyberspace that can form the basis of scientific inquiry in the field of cyber security?
  - Are there specific mathematical abstractions or theoretical constructs that should be considered?
  - Are there philosophical/methodological foundations of science that the cyber security research community should adopt?
- What sciences can we leverage?
  - Which scientific domains and methods, such as complexity theory, physics, theory of dynamical systems, network topology, formal methods, discrete mathematics, economics, social sciences, etc. can contribute to a science of cyber security?

Science of Cyber Security Questions (2)

- What is measurable in cyber security?
  - Currently security measures are very weak
  - How can we improve our ability to quantify cyber security?
- What is the role of experiments?
  - How do we structure efforts to do meaningful experiments?
- What theories can we expect?
  - How can we develop functional theories concerning complex computational processes?
  - How can we develop sound theories of the users and their interactions with the systems?
  - How can we develop sound theories of the adversary?

Science of Cyber Security Questions (3)

- How do we account for the human element in security?
  - Nature just exists, but adversaries cheat and use strategies to creatively violate models and assumptions
  - For any model of computer security, an adversary only needs to attack successfully one assumption of the model to subvert the security
- We need better models for analyzing how to achieve desired functions in systems with damaged and degraded or partial capabilities
  - Models of security tend to be binary (secure/unsecure) and localized within boundaries or abstraction layers
  - We need ways to reason about uncertainty and results within tolerances

Science of Cyber Security Questions (4)

- What are the impediments to advancing a scientific basis for cyber security?
- What measures and metrics can help us assess progress?
- Is there a special role for Government?

Some Potential Science of Security Research Topics

- Methods to model adversaries
- Techniques for component, policy, and system composition
- A control theory for maintaining security in the presence of partially successful attacks
- Sound methods for integrating the human in the system: usability and security
- Quantifiable, forward-looking, security metrics (using formal and stochastic modeling methods)
- Measurement methodologies and testbeds for security properties
- Development of comprehensive, open, and anonymized data repositories

Transition to Practice

- Concerted effort to get results of federally funded research into broad use
  - Integrated demos
  - Conferences and workshops
  - "Matchmaking" efforts
    - Among Agencies
    - Between research and product
  - Potential funding for last mile

Support for National Priorities

- Goals
  - Maximize cybersecurity R&D impact to support and enable advancements in national priorities

- Examples of Supported National Priorities
  - Smart Grid
  - Health IT
  - Financial Services
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)

Summary

- Coordinated effort among government agencies
- Focus on game-changing themes
  - Encourages research collaborations based on tangible topics and desired future capabilities
- Strategic Plan for Federal Cybersecurity R&D Program
  - To be released soon, followed by a public comment period

Think Big, Think Novel

It's about making our nation more cybersecure, not about the quest for the next 12-month, 12-page chunk of work.*

*J.M.Wing, CACM Blog Entry "Breaking the Cycle", August 2009.
http://cacm.acm.org/blogs/blog-cacm/38402-breaking-the-cycle/fulltext

For More Information

Tomas Vagoun, PhD
CSIA IWG Technical Coordinator
vagoun@nitrd.gov
http://www.nitrd.gov
http://cybersecurity.nitrd.gov

Donna F Dodson
donna.dodson@nist.gov
http://csrc.nist.gov

U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

NITRD Tailored Trustworthy Spaces Workshop

July 18-20, 2011

Hank Kenchington
Deputy Assistant Secretary R&D
Office of Electricity Delivery and Energy Reliability
Department of Energy

Edinburgh Castle – built around 1140 AD

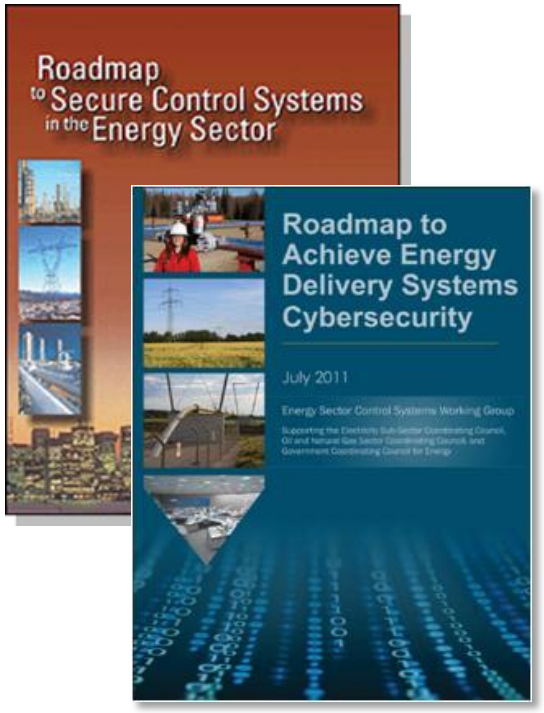
Grid Modernization – national priority

- Grid Modernization – A national priority
- Effective cyber security solutions are essential element to modernizing the nation's electric grid
- Requires effective public-private participation

A smarter, modernized, and expanded grid will be pivotal to the United States' world leadership in a clean energy future.

- A Policy Framework for the 21st Century Grid
June 2011

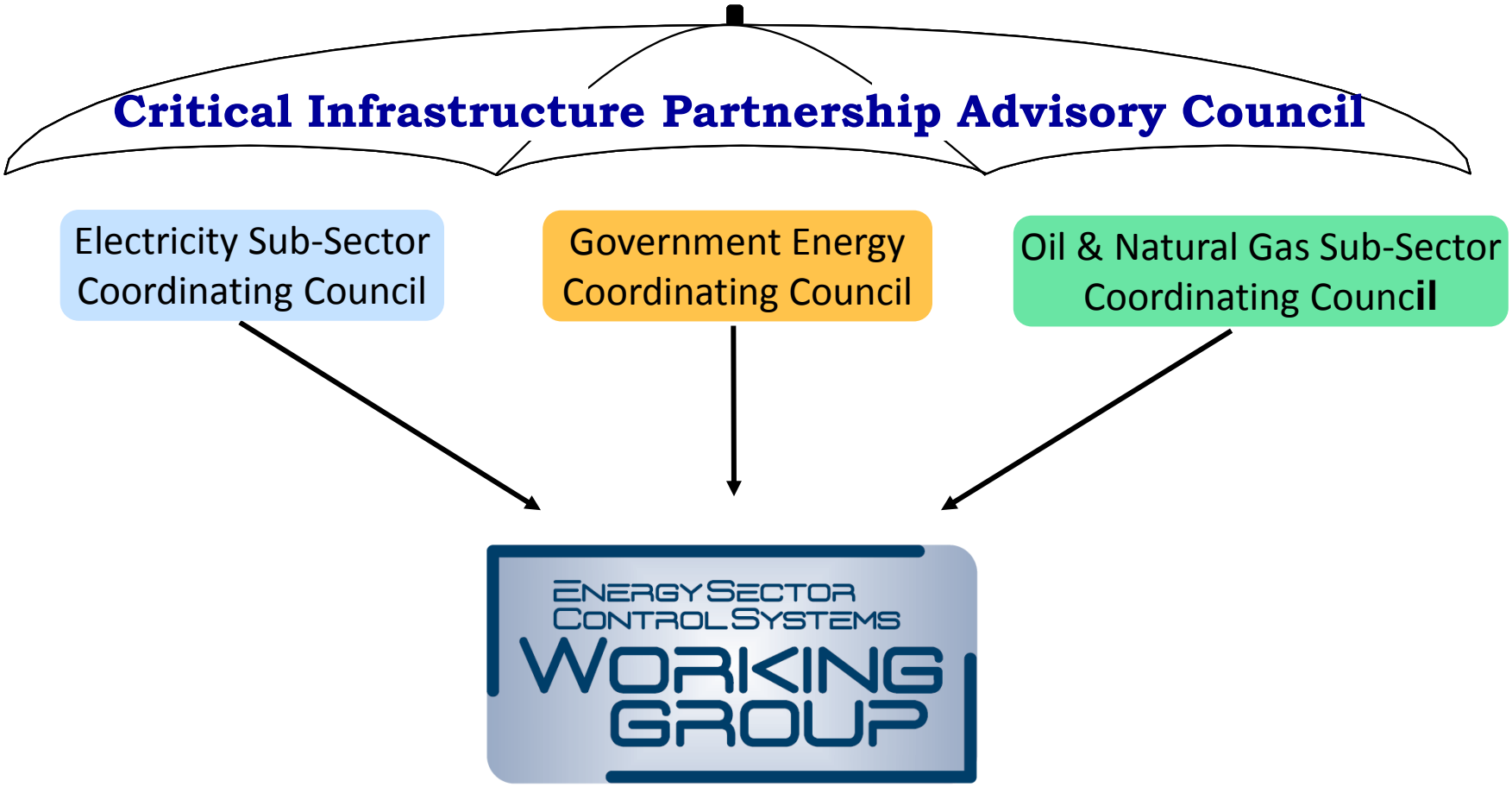
Roadmap – Energy Sector Framework for Public-Private Collaboration



- Published in January 2006
- ***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

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Public-Private Working Group Oversees Roadmap Implementation



Tangible progress has been made to mitigate cyber risks in energy sector since 2006

Measure and Assess Security Posture

- 37 Vulnerability assessments of control systems and components by Idaho National Laboratory
- Bandolier Security Audit Files by Digital Bond enable asset owners to audit/ optimize the security configurations of control systems
- NERC Top Ten Vulnerabilities of Control Systems and Associated Mitigations

Develop and Integrate Protective Measures

- "Hardened" technologies now available and being deployed – secure SCADA communications protocol, SCADA/EMS (ABB, AREVA, Siemens, Telvent, et al)
- Lemnos Interoperable Security project -interoperable configuration profile for creating secure communications channels between various vendor products
- ASAP-SG security profiles for AMI and third-party data access

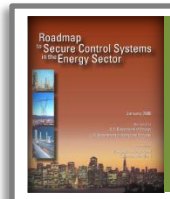
Detect Intrusion and Implement Response Strategies

- ICS-CERT established by DHS to address threats and vulnerabilities
- Over 2300 representatives from energy sector have participated in control systems security training events supported by DoE

Sustain Security Improvements

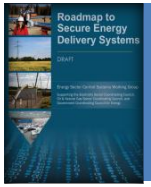
- FBI, DOE, DHS, and ES-ISAC collaborated to quickly provide *actionable guidance* on VPN vulnerability to the electricity industry
- The EnergySec online forum allows stakeholders to share threat and incident information, and communicate and coordinate confidentiality

2011 Roadmap – updated to reflect changing threat and technological landscape



2006 Roadmap

Measure and Assess Security Posture	Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation.
Develop and Integrate Protective Measures	Next-generation control system components and architectures that off built-in, end-to-end security will replace older legacy systems
Detect Intrusion and Implement Response Strategies	Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions
Sustain Security Improvements	Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances



2011 Roadmap

Build a Culture of Security	Cybersecurity practices are reflective and expected among all energy sector stakeholders
Assess and Monitor Risk	Continuous security state monitoring of all energy deliver system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators
Develop and Implement New Protective Measures to Reduce Risk	Next-generation energy delivery system architectures provide “defense in depth.” and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident
Manage Incidents	Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment
Sustain Security Improvements	Collaboration between industry, academia, and government maintains cybersecurity advances

DOE Strategic Approach to Energy Sector Cybersecurity

Work closely with Federal and State government, and the private sector to:

- Implement ***Roadmap to Achieve Energy Delivery Systems Cybersecurity***
- Identify and fund gaps in infrastructure R&D and testing to accelerate the development and deployment of resilient networks and systems
- Conduct vulnerability research to better understand weaknesses and develop mitigations
- Conduct analysis to assess risks, security posture, and increase ability to mitigate risks
- Encourage “culture of security”
- Provide secure sharing of threat information and facilitate incident response

DOE R&D and Outreach – a portfolio approach to developing and deploying solutions

Research, Development, and Demonstration Activities

Higher Risk, Longer Term Projects
→ Core NSTB Program
→ Academia Projects
→ No Cost Share

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

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

Partnering

Path to Commercialization

Training, Education, Standards Development, and Other Outreach Activities

Core NSTB Program

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

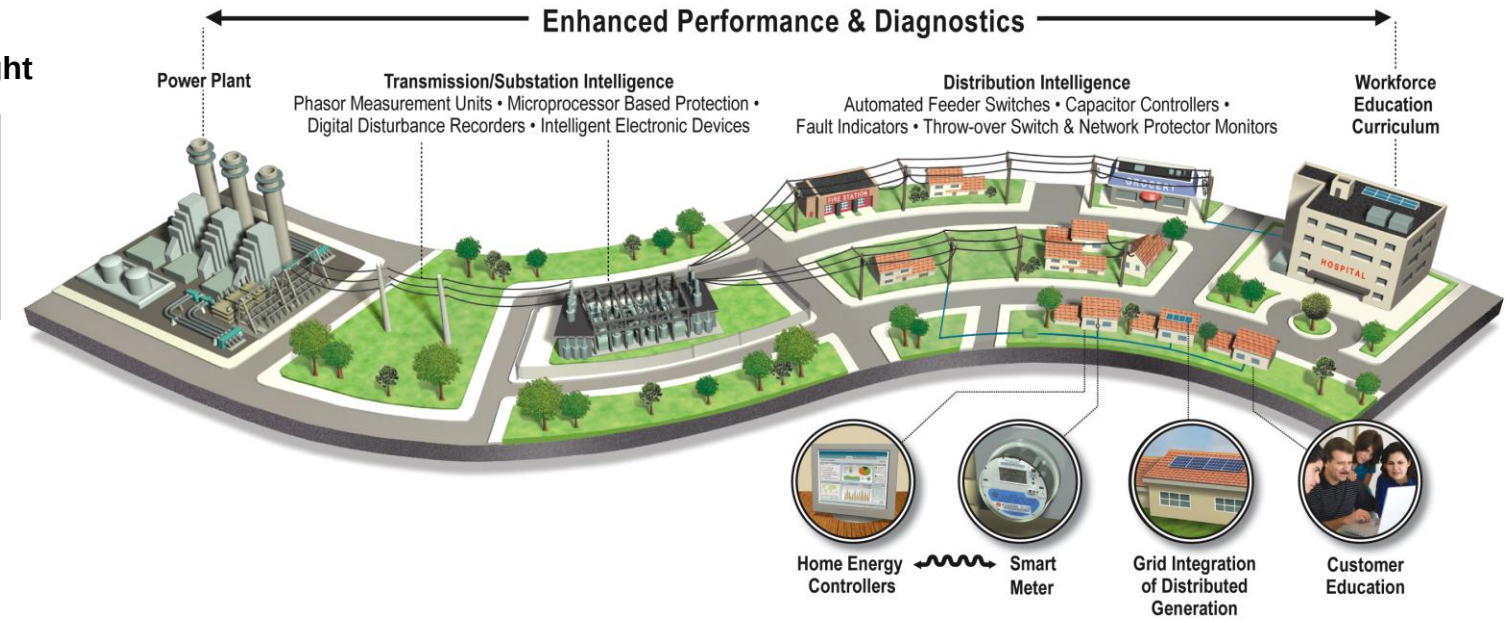
Academia Projects (TCIPG)

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

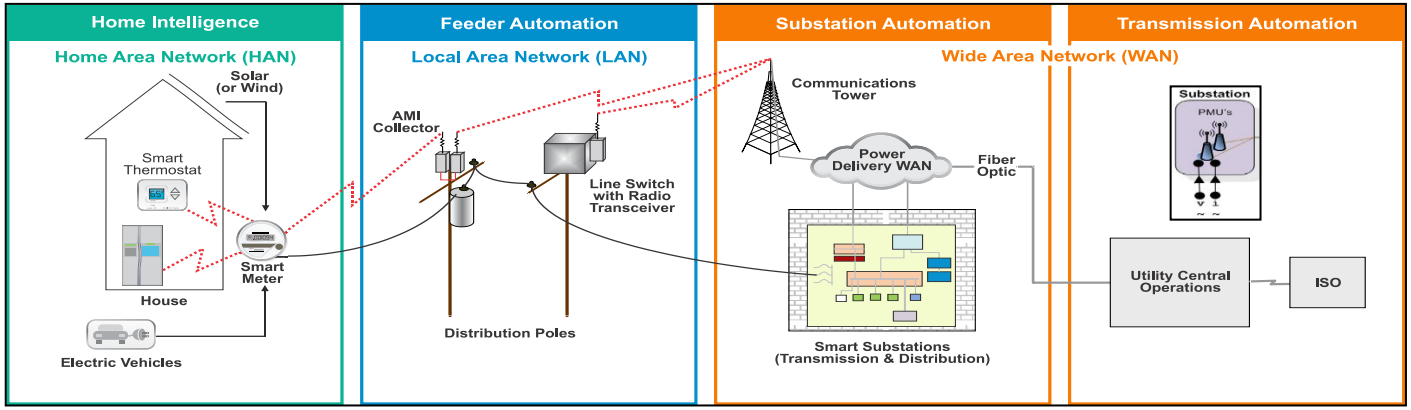
+$9 billion in public/private investments in Smart Grid technologies now being deployed

Grid modernization requires seamless, secure communications across multiple interconnected domains and platforms

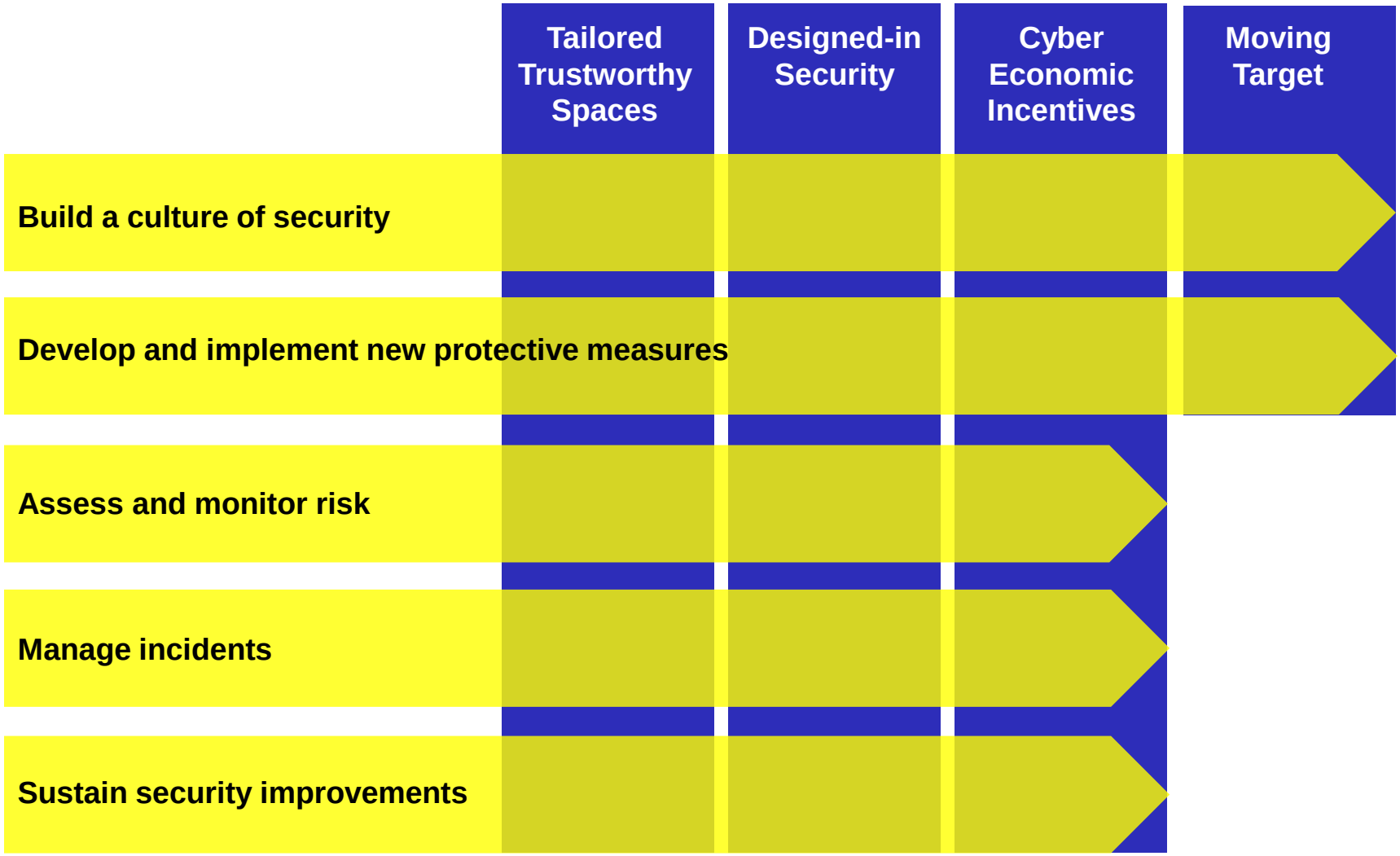
Florida Power and Light



Generic Smart Grid Communications Architectures



NITRD cybersecurity strategies support Energy Roadmap goals



Many Energy Roadmap needs support NITRD “game changing” strategies

Tailored Trustworthy Spaces supports context specific trust decisions

- Develop techniques to provide explicit, managed communications trust
- Develop trusted platform modules and trusted network connections for real-time communications that are nonproprietary

Moving Target provides resilience through agility

- Develop security validation test beds
- Develop tools for secure change management across widely distributed systems

Cyber Economic Incentives provide incentives to good security

- Increase executive understanding of energy delivery cybersecurity issues and risks
- Integrate cybersecurity awareness, education, and outreach programs into energy sector and vendor operations

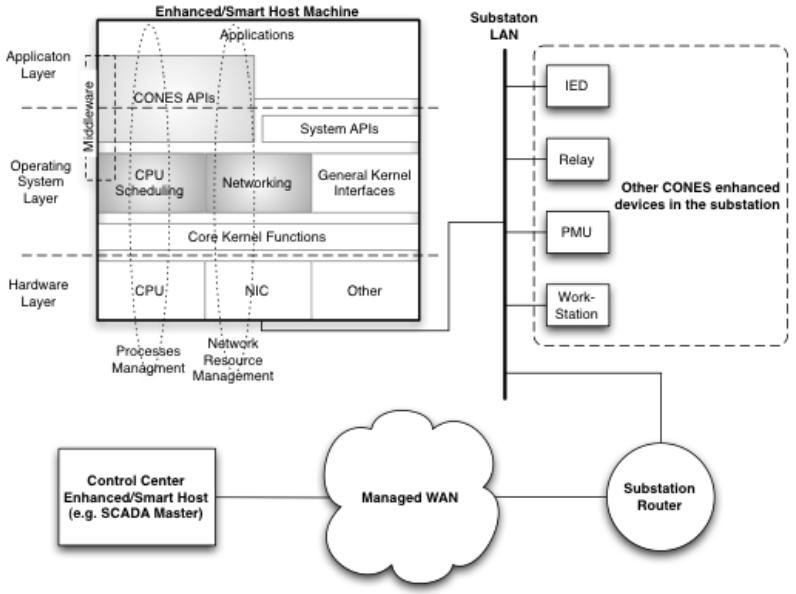
Designed-in Security develop and evolve secure software systems

- Develop scalable built-in security for embedded operating systems
- Adopt agreed upon, available intrinsic data and source integrity in SCADA/EMS protocols to develop control systems that will inherently respond to and defend themselves against internal and external threats

Several DOE efforts utilize Tailored Trustworthy Spaces concepts

- **SIEGate** – a secure information exchange gateway that provides secure communication of data between control centers (Grid Protection Alliance, University of Illinois, PNNL, PJM, AREVA T&D)

- **Secure and real-time communication substrate** - trustworthy cyber infrastructure and technologies for wide-area monitoring and control, and active demand management (TCIPG)
  - Converged Networks for SCADA (CONES) an architecture and platform for maintaining real-time and secure communications for control in a converged network



- **Trust Anchors** – Monitoring and control devices to independently verify systems function, reveal deceptive malicious function, attest to system state, and verify correctness of system tests (SNL)

Conclusions

- Effective cybersecurity solutions are critical to grid modernization
- Cyber threat capabilities are outpacing defenses
- When you can’t win the game – change the game!
- Application of tailored trustworthy spaces concepts in smart grid technologies/applications can help “change the game”
- Game changers are needed TODAY!

Thank you!

Tailored Trustworthy Spaces: The Right Security for the Job

What is a Tailored Trustworthy Space?

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Today's cyberspace recreates those environments, but security mechanisms and policies lack the flexibility to accommodate different behaviors

The vision is of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

New Paradigm

- Users can select different environments for different activities (e.g., online banking, commerce, healthcare, personal communications) providing operating capabilities across many dimensions, including confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to create new environments with mutually agreed upon characteristics and lifetimes

Enabling Informed Trust Decisions

- Provide users with:
  - Context-specific trust services
  - Coherent policy implementation: an integrated set of security choices (or defaults) appropriate to the tasks at hand
  - User/provider/system visible rules and attributes
  - Means to negotiate boundaries and rules of the space

Key Concept

- TTS is about knowing how trustworthy your system is and understanding whether is it good enough for what you are trying to do.
- TTS is not about guaranteeing high trust

Challenge: Identifying dimensions of a tailored trustworthy space

- What is needed to safely support the activity we want to conduct?
  - Degree of identification / authentication
  - Information flow rules
  - Strength of separation mechanisms
  - Degree of monitoring / violation detection

Challenge: Policy Specification and Management

- How to we propose, decide upon, and instantiate our rules in the system?
  - Convenient specification of a tailored space
  - Convenient mechanisms to know it
  - Convenient mechanisms to change it

Challenge: Assuring Correct Operation

- How do we know our tailored solution is doing the job?
  - Validation of platform integrity
  - Challenge: Violation detection
  - Challenge: Verifiable separation of spaces
  - . . . and many more

What's New?

Nothing. Few of these individual problems or component technologies are novel

Everything. A structure that puts the pieces together to provide integrated, usable support for diverse trust environments would change the game.

Which technology areas matter?

- Identity management
- Component assurance
- Composition methods and logics
- Trust negotiation and management
- ...

What is the state of the art?

- Wide variance in the maturity of required technology
- Human dimension – how do we understand and establish trust levels – is least explored and most critical to success

NIST and the Cyber Security Working Group

Marianne Swanson, Chair
Smart Grid Interoperability Panel - Cyber Security Working Group
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology (NIST)

Energy Independence and Security Act

- In the Energy Independence and Security Act (EISA) of 2007, Congress established the development of a Smart Grid as a national policy goal.

- Under EISA, NIST is directed to *"coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems"* as well as maintain the reliability and security of the electricity infrastructure.

Cyber Security Working Group (CSWG)

- To address the cross-cutting issue of cybersecurity, NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009.

- Moved under the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the Cyber Security Working Group (SGIP–CSWG).

- The CSWG now has more than 650 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.

CWSG Active Sub-groups and Leads

- **AMI Security Group**
  - Doug McGinnis & Sandy Bacik
- **Architecture Group**
  - Sandy Bacik
- **Design Principles Group**
  - Daniel Thanos & Annabelle Lee
- **High-Level Requirements Group**
  - Dave Dalva & Victoria Yan
- **Privacy Group**
  - Rebecca Herold
- **Security Testing and Certification Group**
  - Nelson Hastings & Sandy Bacik
- **Standards Group**
  - Frances Cleveland

“Guidelines for Smart Grid Cyber Security”

NIST Interagency Report 7628 - August 2010

- Development of the document lead by NIST
- Represents significant coordination among
  - Federal agencies
  - Private sector
  - Regulators
  - Academics

Recent Accomplishments

- Recent Activities
  - SGIP Priority Action Plan (PAP) Collaboration
  - Ongoing outreach and education efforts
    - 8 States (4 PUCs)
    - Over 1000 participants
  - CSWG Three Year Plan
  - Privacy subgroup developing a "Best Practices" document on best ways to protect privacy when sharing data with third parties
  - Coordination with DOE's NESCO and NESCOR groups
  - Coordination with the ASAP-SG
  - Task force developed to harmonize proposed work item IEC 62443-2-4 with NISTIR 7628

- Cybersecurity Review of Standards
  - Completed:
    - Over 20 reviews of standards and PAP deliverable requirements
      - 5 IEC Common Information Model Standards
      - SEP 1.0, 1.1 and Draft 2.0
  - Future:
    - Renewable Standards
    - IEC 1815 (DNP3) and IEC 1815.1 (Mapping between DNP3 and IEC 61850)

Continuing Work

- Collaborating with DOE and NERC to develop a harmonized energy sector enterprise-wide risk management process.
- Analyzing AMI use cases to determine detailed AMI security requirements.
- Coordinating with the SGIP Smart Grid Test and Certification Committee (SGTCC) to develop guidance and recommendations on Smart Grid conformance, interoperability, and cybersecurity testing.
- Developing a virtual test environment for the NEMA upgradeability standard.
- Developing a NISTIR 7628 High Level Requirements Assessment Guide.

Cyber-Physical Attacks – Collaboration

- Assessing the impact of cyber-physical attacks will require expertise in:
  - Cybersecurity
  - Physical security
  - The electric infrastructure
- The CSWG will provide cybersecurity expertise to help address cyber-physical threats in coordination with other federal agencies and industry groups.
  - Draft white paper on research and path forward
- It is anticipated that this collaborative effort may result in the NISTIR 7628 high-level security requirements being augmented to address cyber-physical security threats.

How to get involved

- To join the CSWG mailing list, contact:
  - Marianne Swanson (marianne.swanson@nist.gov)
  - Tanya Brewer (tanya.brewer@nist.gov)

- All are welcome to dial into the CSWG conference calls
  - Teleconference Day & Time: Biweekly on Mondays, 11am Eastern Time
  - Call-in number: 866-793-6322
  - Participant passcode: 3836162

- CSWG TWiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Questions?

U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Working to Achieve Cybersecurity in the Energy Sector

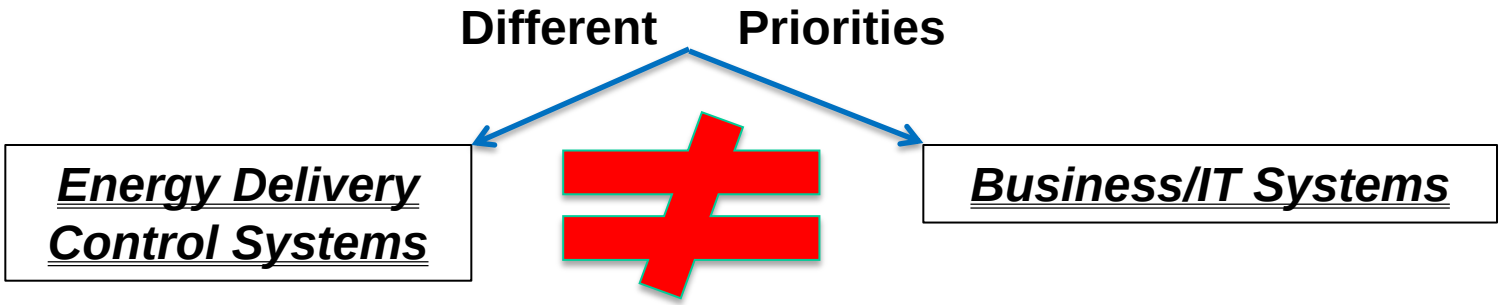
"Cybersecurity for Energy Delivery Systems (CEDS)"

Carol Hawk, Ph.D.
Department of Energy

Energy Sector Cybersecurity Challenges

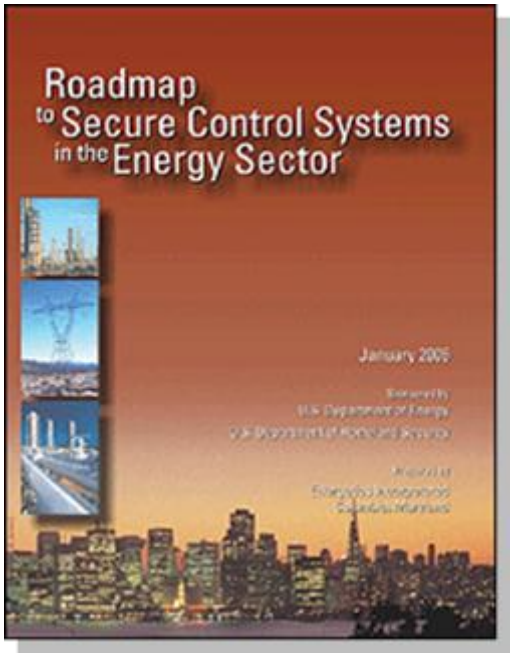
- **Open Protocols**
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- **Common Operating Systems**
  - Standardized computational platforms increasingly used to support control system applications
- **Interconnected to Other Systems**
  - Connections with enterprise networks to obtain productivity improvements and information sharing
- **Reliance on External Communications**
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- **Increased Capability of Field Equipment**
  - “Smart” sensors and controls with enhanced capability and functionality, demand response communication networks

Business/IT Cybersecurity Solutions Can **Break** Energy Delivery Control Systems



- **Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades**
- **Energy delivery control system components may 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**
- **Energy delivery control system 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 Public-Private Collaboration

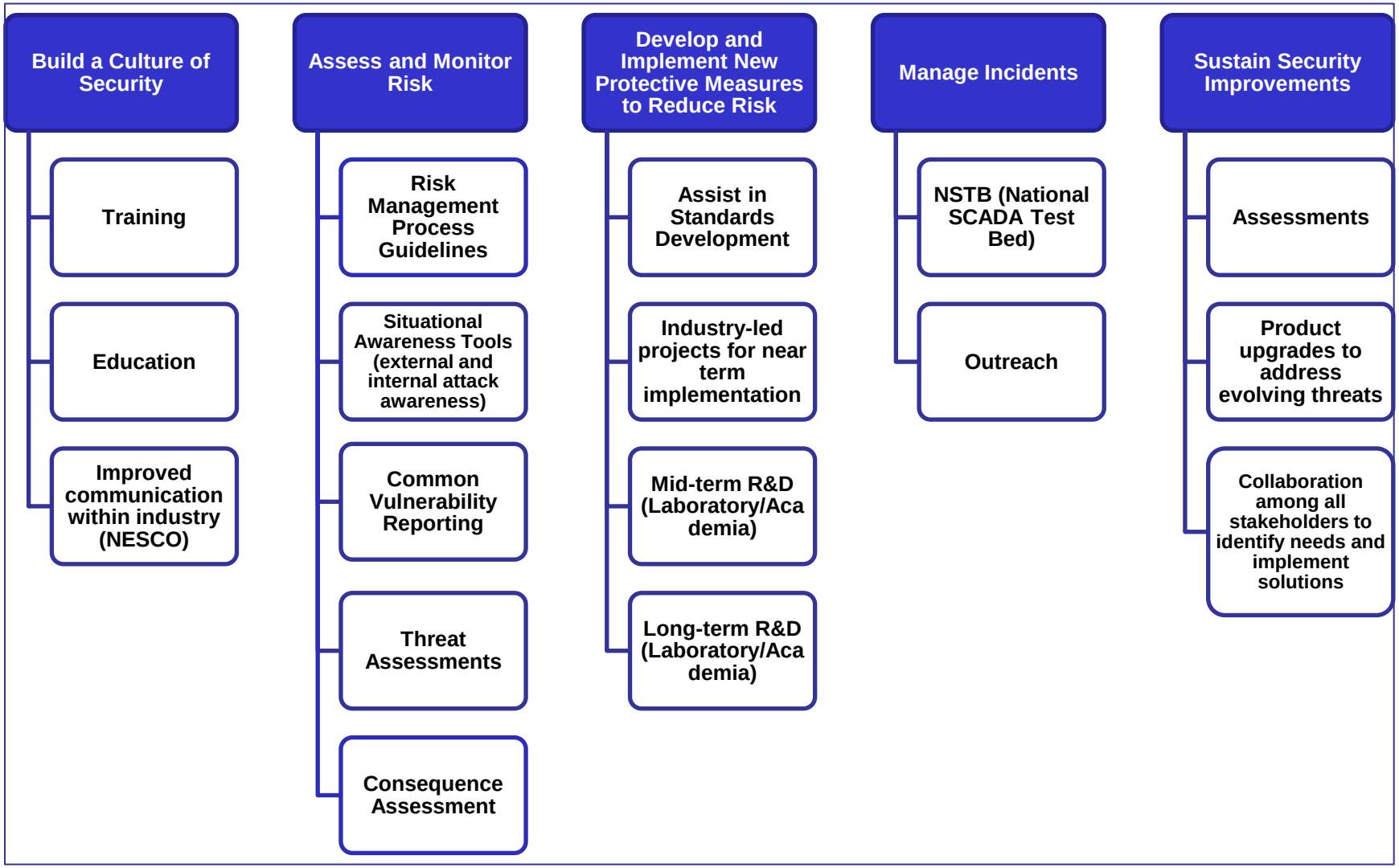


- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in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

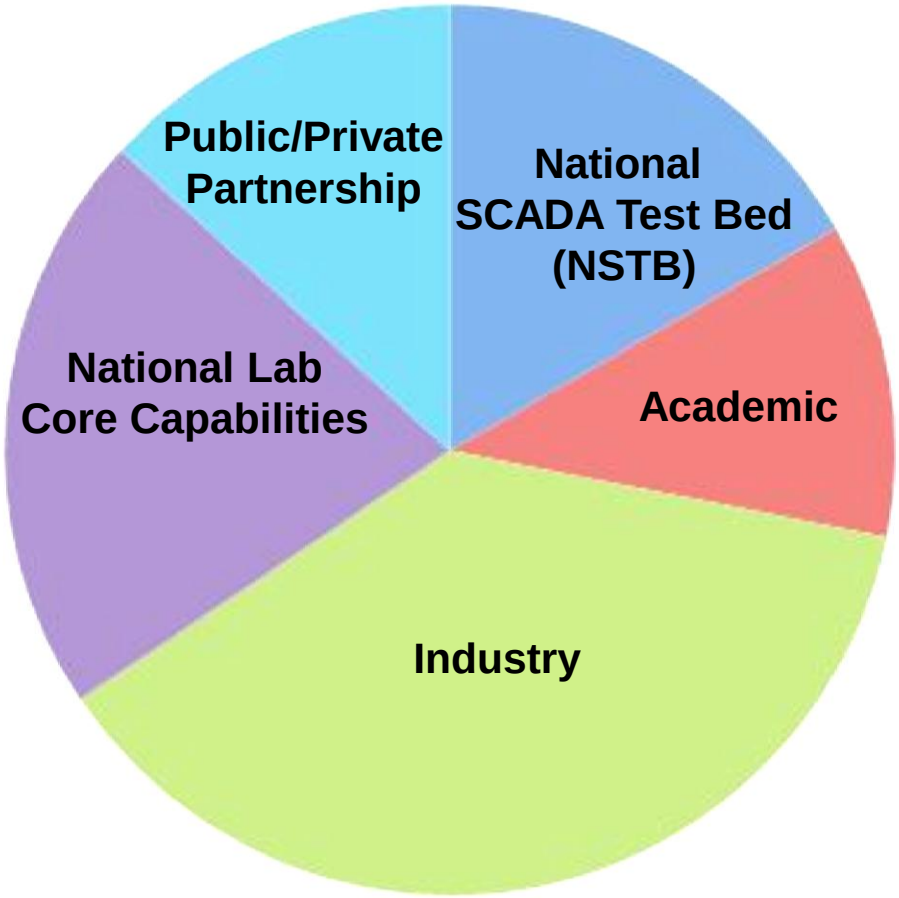
Roadmap Vision

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.

DOE activities align with 2011 Roadmap



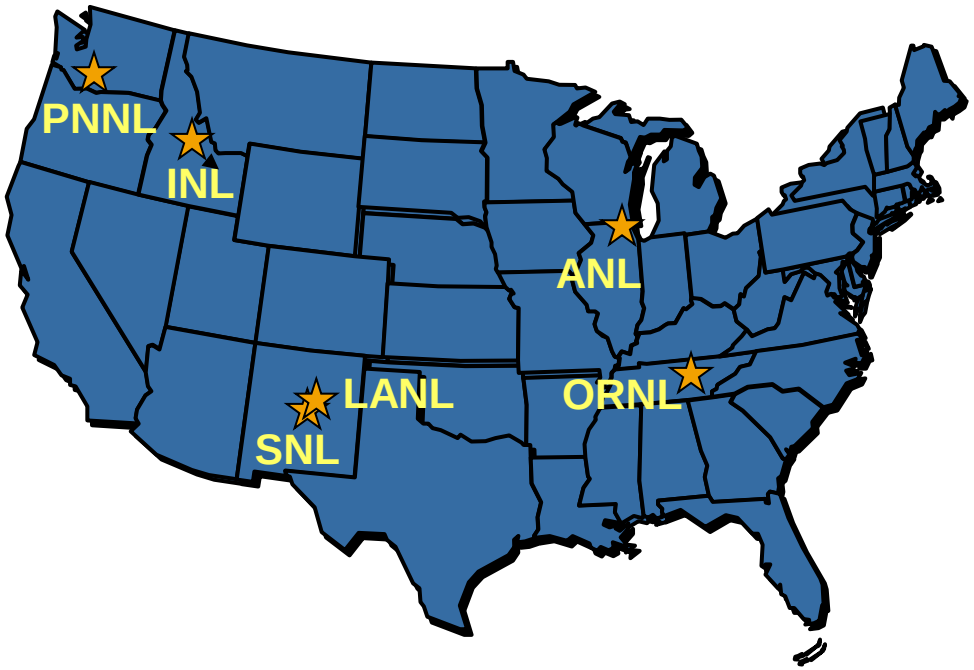
Cybersecurity for Energy Delivery Systems (CEDS) Program—5 Key Areas



DOE National SCADA Test Bed (NSTB)

DOE multi-laboratory program . . . established 2003

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

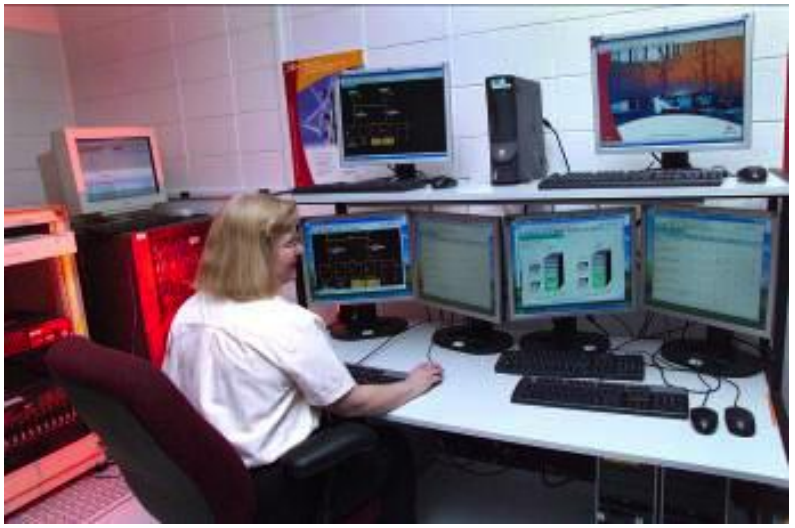


"..the only reliable way to measure security is to examine how it fails"

Bruce Schneier, Beyond Fear

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

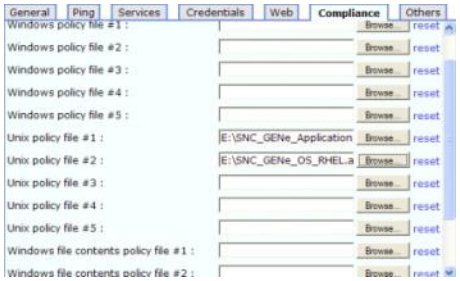
OSIsoft.

OSI
opening your world

CEDS—Industry Accomplishments

- Hallmark Cryptographic Serial Communication
  - → Commercialized technologies that provide secure communications between remote devices and control centers

- Bandolier Security Audit Files
  - → Enables asset owners using the Nessus vulnerability scanner to optimize security configurations of their control systems



- Lemnos Interoperable Security
  - → Developed and demonstrated an interoperability configuration profile for creating a secure communications channel between two control system networks operated by different vendors

CEDS—Academia Accomplishments

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

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

Recent Papers

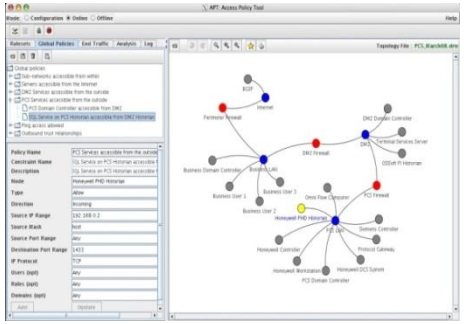
Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

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

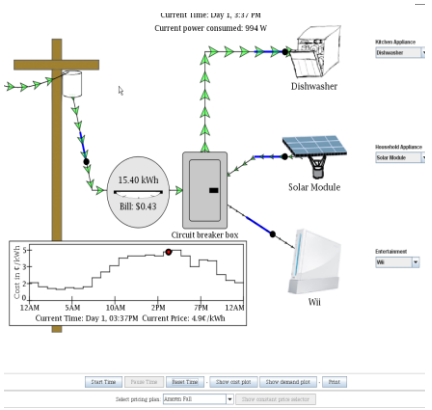
Building Security In

Smart-Grid Security Issues

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



Applets for Schools



Facilities

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

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

NEW CEDS Activities

13 CEDS projects started in 2010 to help harden the U.S. energy infrastructure against cyber intrusion

8 Industry-led projects

5 National Laboratory-led projects

Generic SCADA Architecture

Physical Security

Industry-Led Projects

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

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

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

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

Industry-Led Projects

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

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

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

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

National Laboratory-Led Projects

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

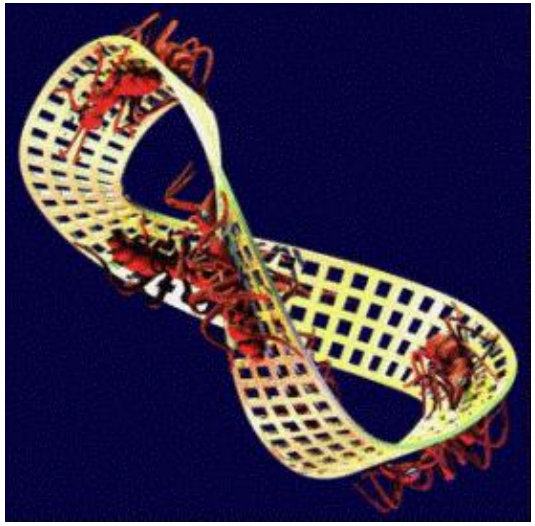
2. **Control Systems Situational Awareness Technology Interoperable Tool Suite**—a situational awareness tool suite for control systems that will show network communications, collect wireless mesh network data message routes, report unexpected behavior, monitor system health, distinguish between component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

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

National Laboratory-Led Projects

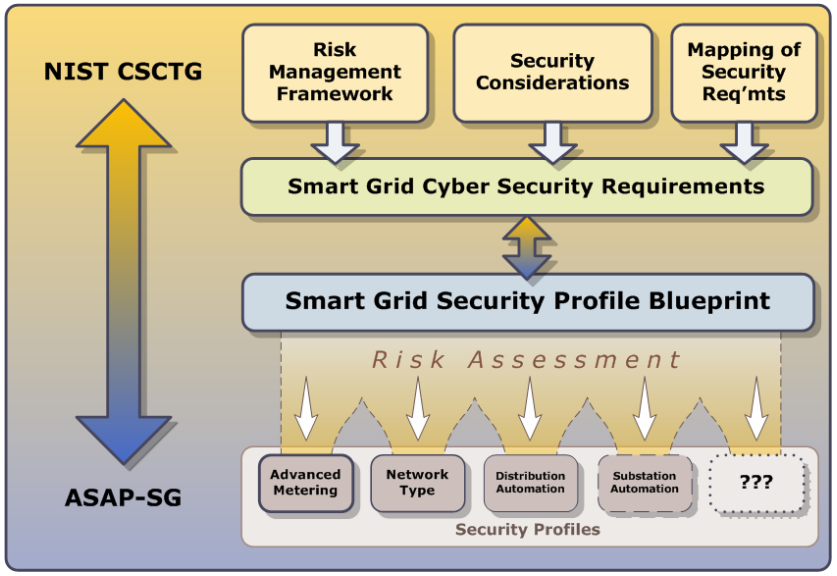
4. **Next Generation Secure, Scaleable Communication Nework for the Smart Grid**—a secure, scalable communication network for the smart grid using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming→ **Oak Ridge National Laboratory**,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

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



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

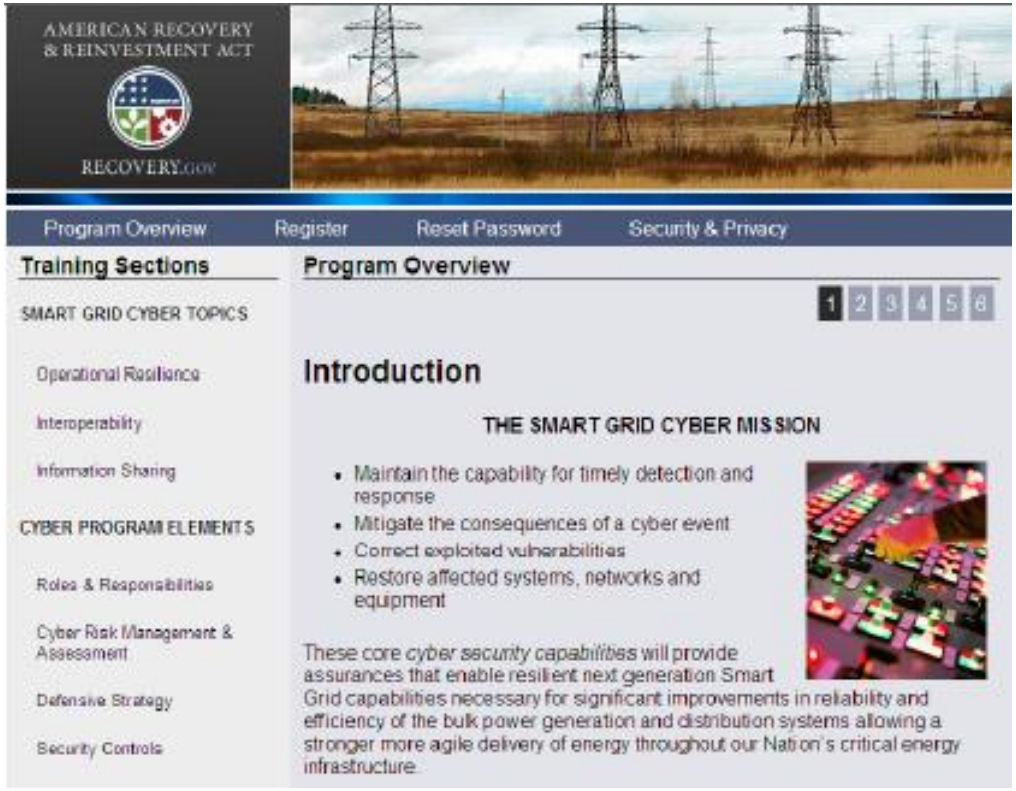


Cybersecurity - *Critical to Smart Grid Success*

- 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 …

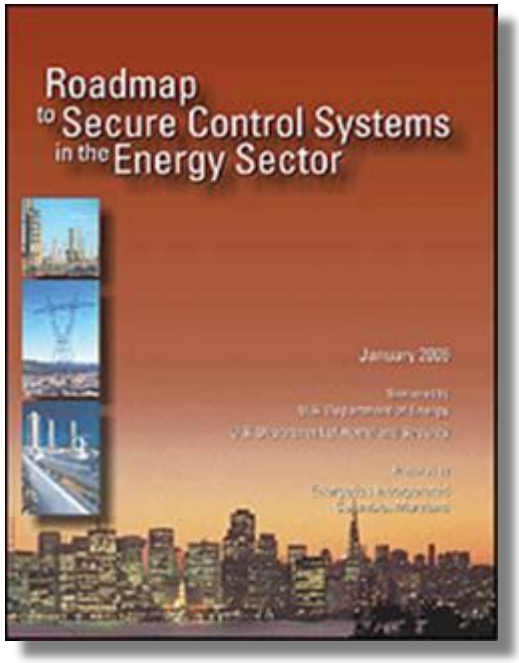
Contact:

US Department of Energy

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

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

ie Roadmap
interactive energy Roadmap to secure control systems



Visit:

www.oe.energy.gov/controlsecurity.htm

www.controlsystemsroadmap.net

CONCEPTUAL SECURITY ARCHITECTURE

Sandy Bacik

July 18, 2011

Architecture as usually practiced

(Apologies to Mr Adams and my fellow architects)

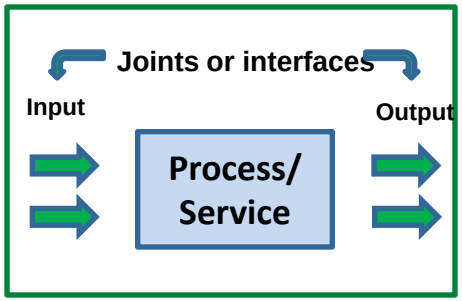
There is never enough time (or money) to do it right the first time

There is always enough time and money to fix it over and over again

-Anonymous

Simple Building Architecture Example

Magic in this case is the ability to infer the options



Vision
- Comfort
- Green
- Budget

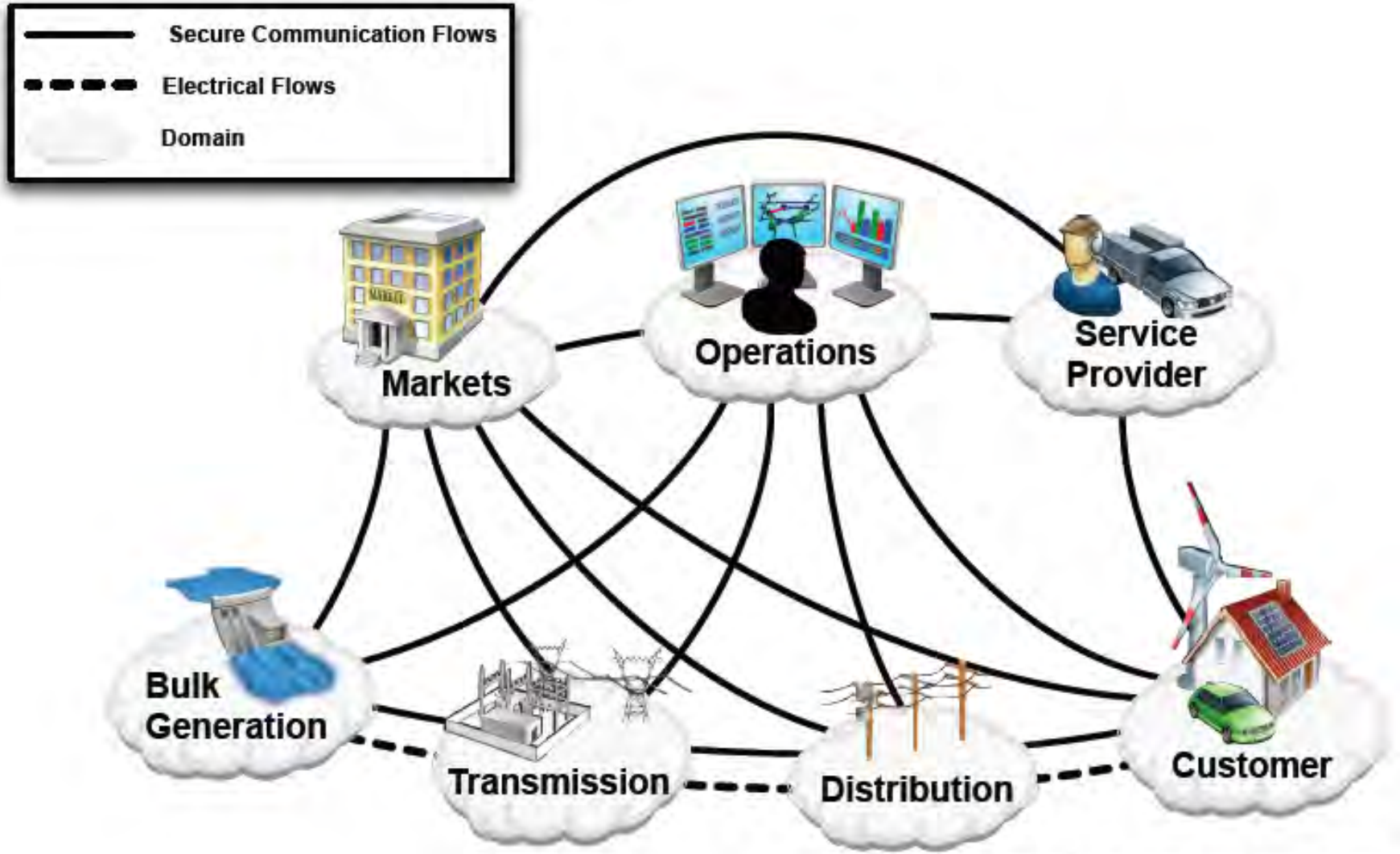
Require-ments
- Water
- Heat/Air
- Light
- Outside environ
- Sanitary
- Energy Eff
- Material Reuse
- Op Costs
- Initial Cost
- Timeframe

Business Services
- Hot Water
- Source
- Treatment
- Rebates
- Rate
- Incentive

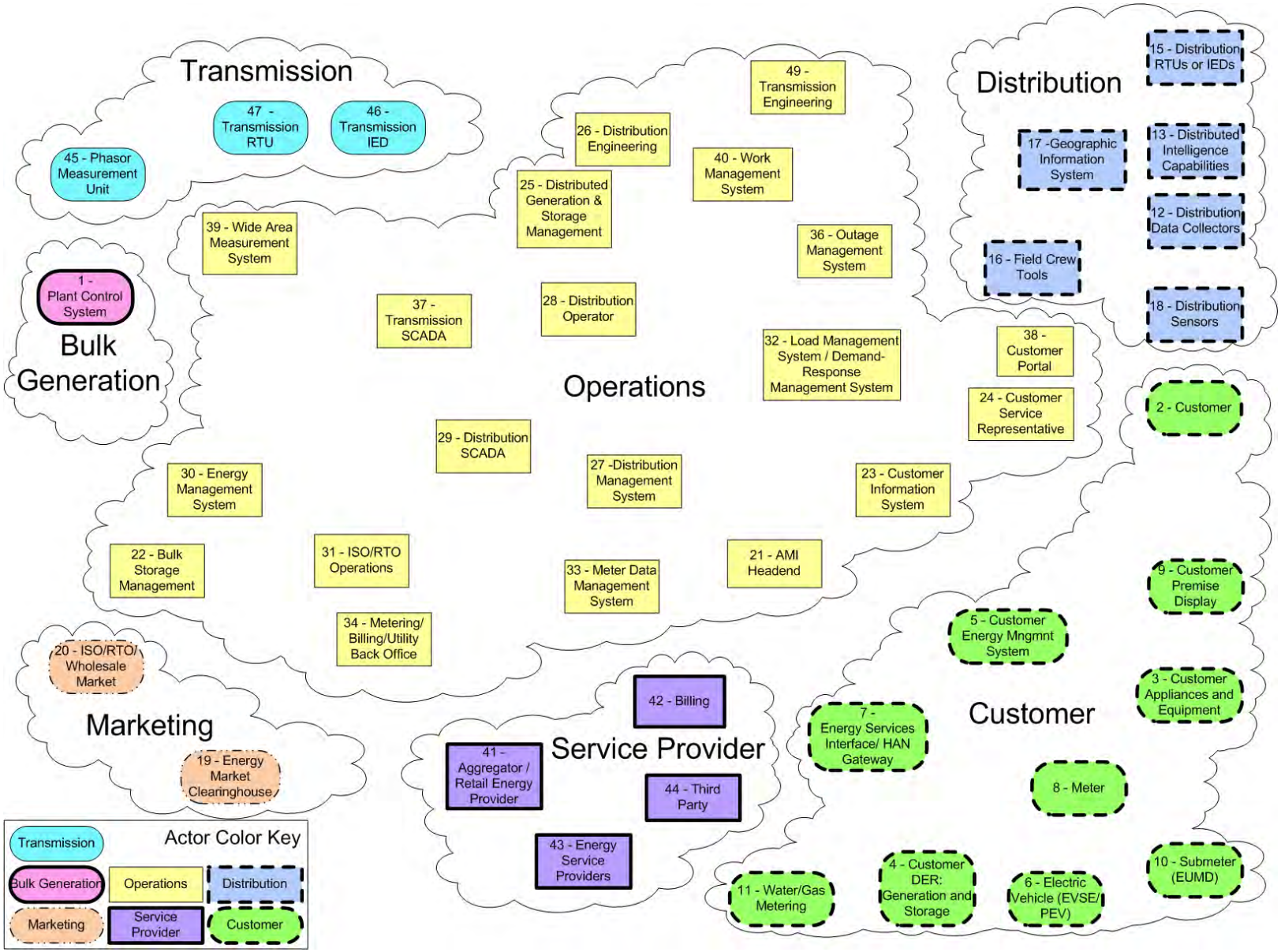
Application Services
- Solar
- Gas
- Electric

Technical Services
- Panels
- Batteries
- Inverter
- &c

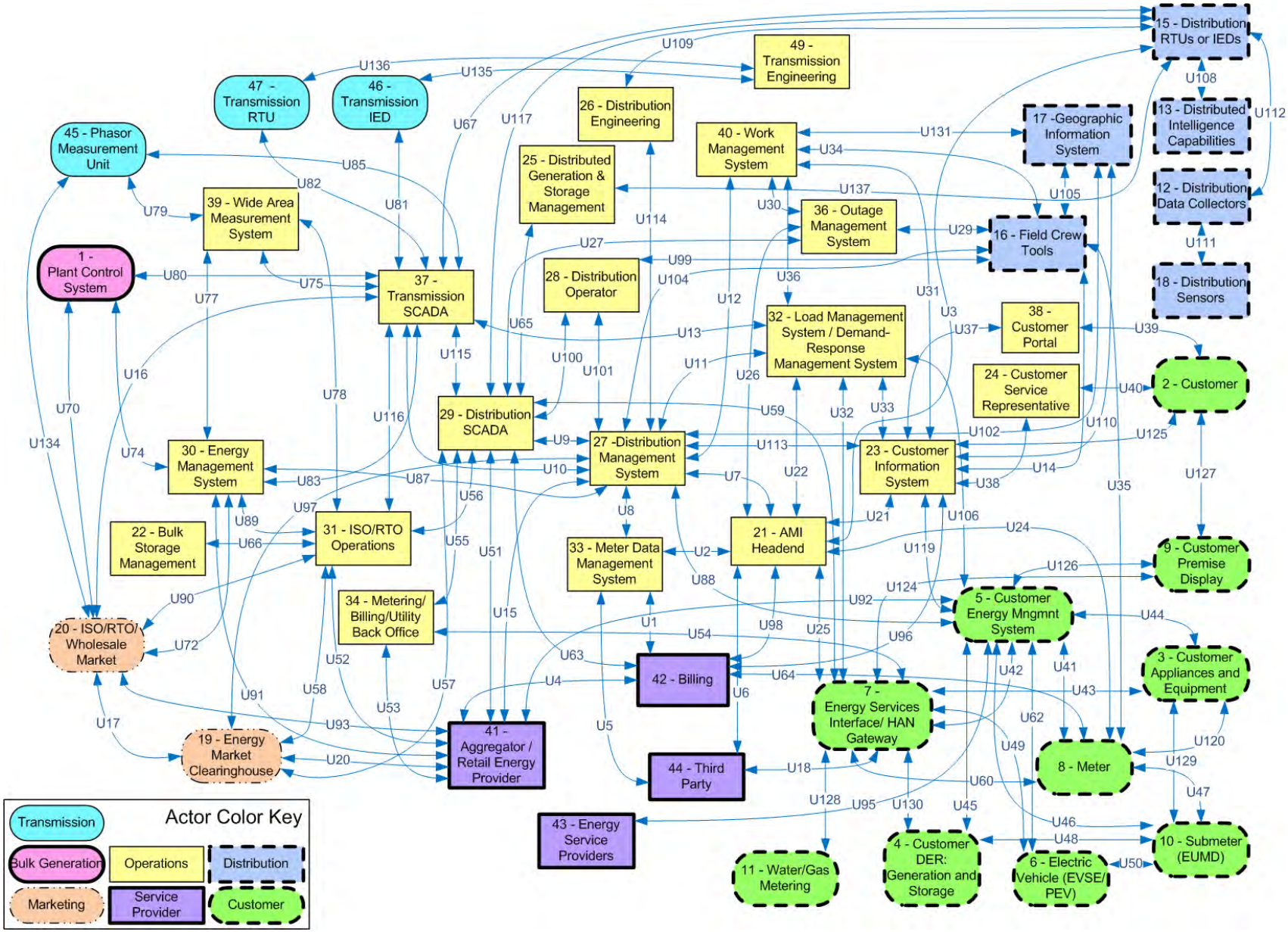
SMART GRID DOMAINS



NIST Smart Grid Framework 1.0 January 2010


Transmission
47 - Transmission RTU
46 - Transmission IED
45 - Phasor Measurement Unit
Bulk Generation
1 - Plant Control System
39 - Wide Area Measurement System
37 - Transmission SCADA
Operations
49 - Transmission Engineering
26 - Distribution Engineering
40 - Work Management System
25 - Distributed Generation & Storage Management
36 - Outage Management System
28 - Distribution Operator
32 - Load Management System / Demand-Response Management System
29 - Distribution SCADA
27 -Distribution Management System
30 - Energy Management System
23 - Customer Information System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
34 - Metering/ Billing/Utility Back Office
Distribution
15 - Distribution RTUs or IEDs
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
12 - Distribution Data Collectors
16 - Field Crew Tools
18 - Distribution Sensors
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
9 - Customer Premise Display
5 - Customer Energy Mngmnt System
3 - Customer Appliances and Equipment
Customer
7 - Energy Services Interface/ HAN Gateway
8 - Meter
10 - Submeter (EUMD)
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
11 - Water/Gas Metering
Marketing
20 - ISO/RTO/ Wholesale Market
19 - Energy Market Clearinghouse
Service Provider
42 - Billing
41 - Aggregator / Retail Energy Provider
44 - Third Party
43 - Energy Service Providers
Actor Color Key
Transmission
Bulk Generation
Marketing
Operations
Service Provider
Distribution
Customer

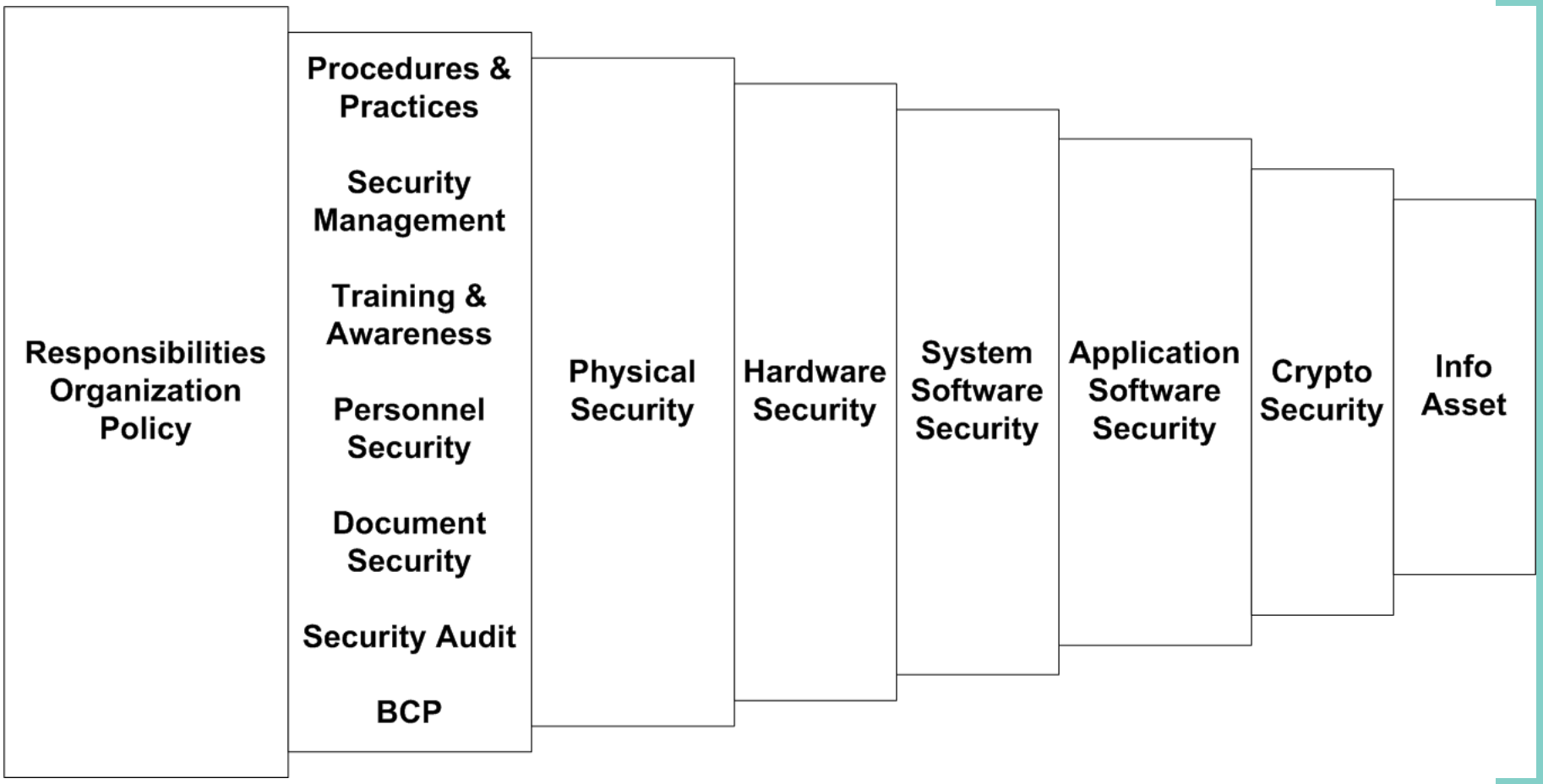
"SPAGHETTI" DRAWING



To Ensure Traceability

- Architecture needs to map to
  - Goals / Objectives
  - Requirements
  - Services

Multi-Layering of Security



Security Tools – More Than Just a Firewall

Management, Audit, Measurement, Monitoring, and Detection Tools
- Log Auditing Utilities
- Virus and Malicious Code Detection Systems
- Intrusion Detection Systems
- Vulnerability Scanners
- Forensics and Analysis Tools (FAT)
- Host Configuration Management Tools
- Automated Software Management Tools

Authentication and Authorization Technologies
- Role-Based Authorization Tools
- Password Authentication
- Challenge/Response Authentication
- Physical/Token Authentication
- Smart Card Authentication
- Biometric Authentication
- Location-Based Authentication
- Password Distribution and Management Technologies
- Device-to-Device Authentication

Filtering/Blocking/Access Control Technologies
- Network Firewalls
- Host-based Firewalls
- Virtual Networks

Physical Security Controls
- Physical Protection
- Personnel Security

Encryption Technologies and Data Validation
- Symmetric (Secret) Key Encryption
- Public Key Encryption and Key Distribution
- Virtual Private Networks (VPNs)

Industrial Automation and Control Systems Computer Software
- Server and Workstation Operating Systems
- Real-time and Embedded Operating Systems
- Web Technologies

Cyber Security Requirements – High Level

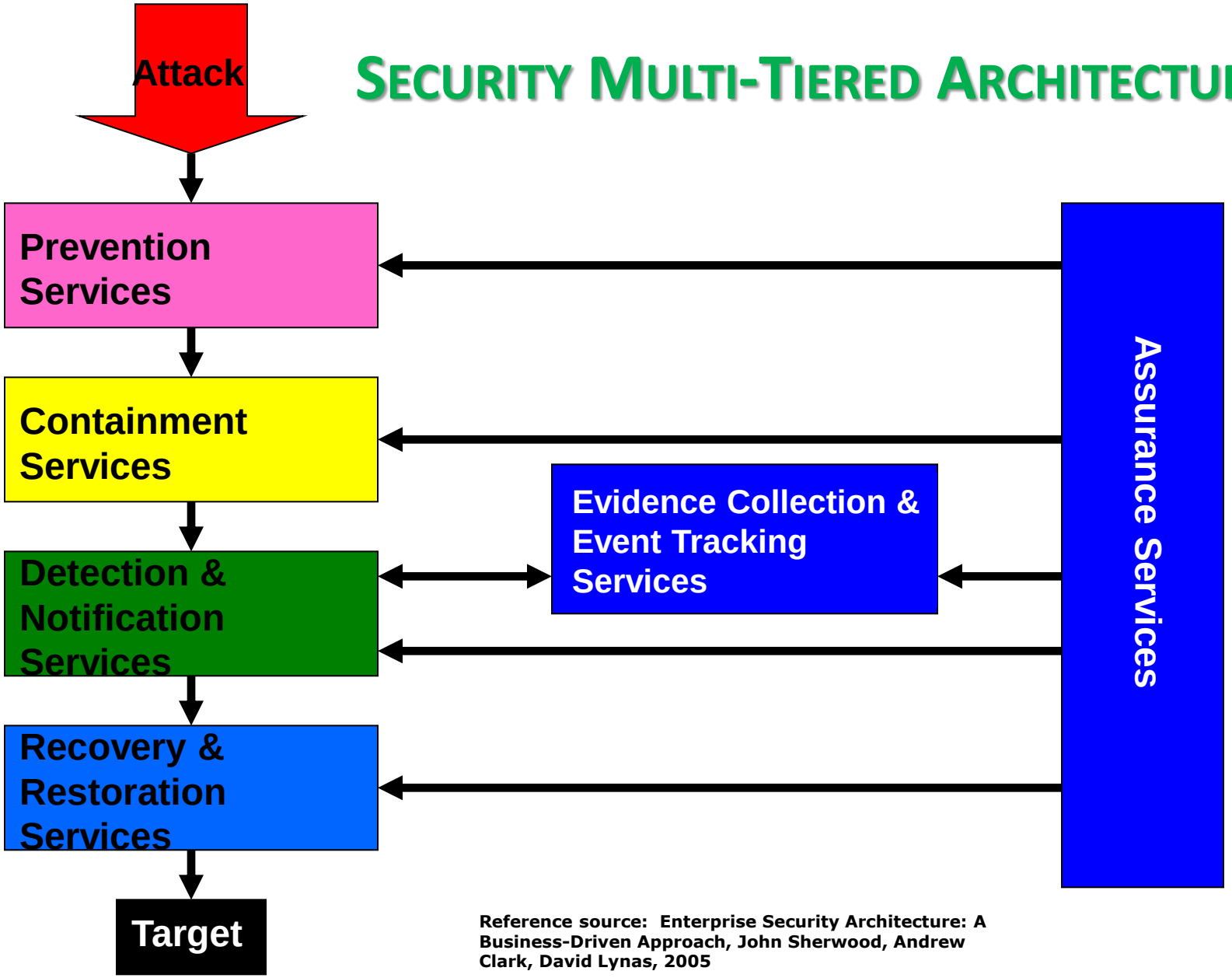
Functional Requirements

- Auditing
- Cryptographic Support
- User Data Protection
- Event Monitoring
- Identification & Authentication
- Functional Management
- Security Event Monitoring
- Physical Protection
- System Configuration
- Resource Utilization
- Trusted Path/Channels

Assurance Requirements

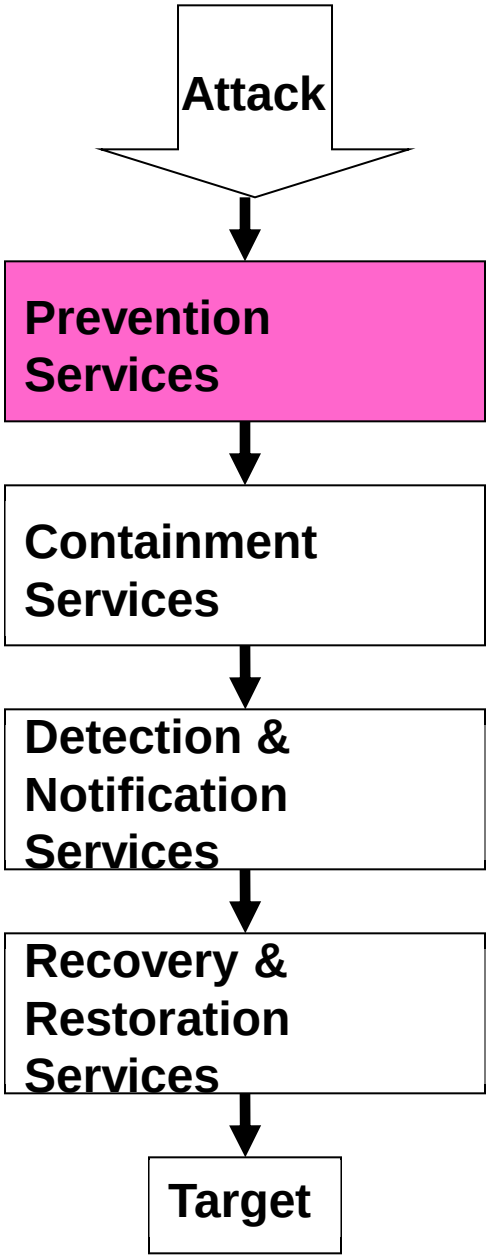
- Configuration Management
- Delivery & Operation
- Guidance Documents
- Life Cycle Support
- Security Awareness
- Operation & Maintenance
- System Architecture
- Testing
- Vulnerability Assessment
- Assurance Maintenance

Security Multi-Tiered Architecture



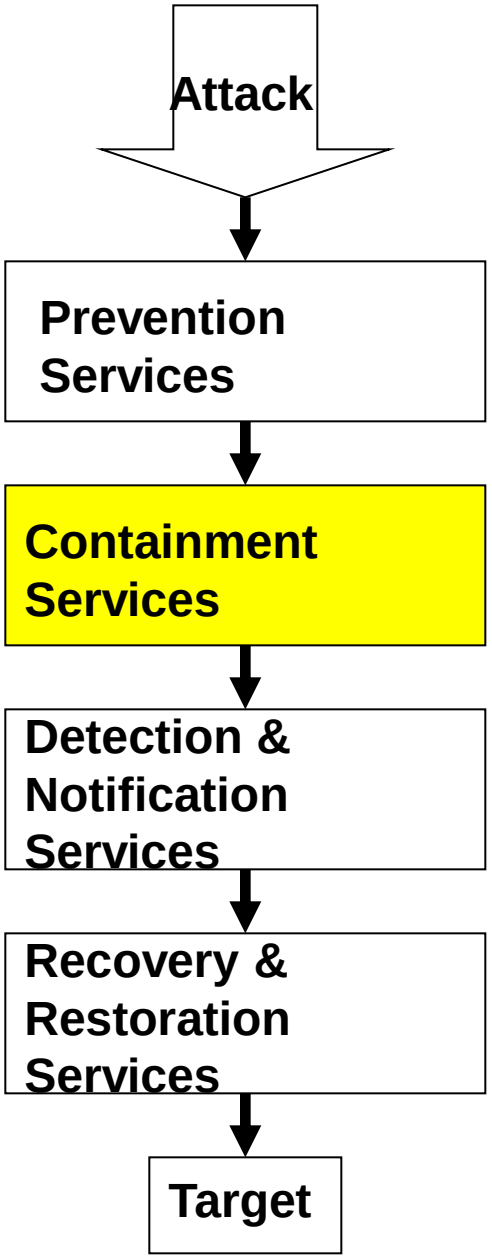
Reference source: Enterprise Security Architecture: A Business-Driven Approach, John Sherwood, Andrew Clark, David Lynas, 2005

Prevention Services



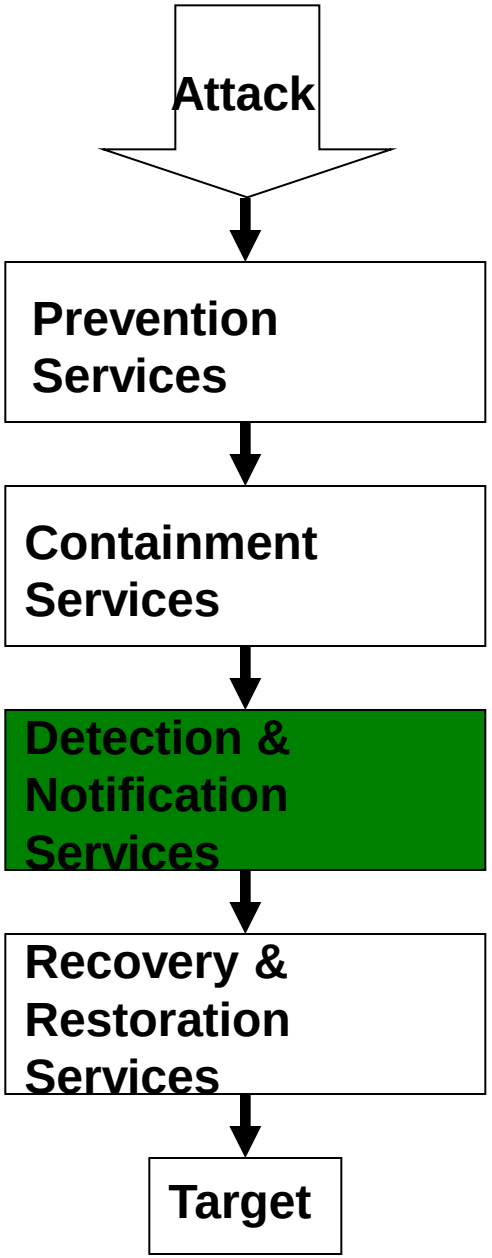
Security Architecture Tier	Security Services	Detail
Prevention	Entity Security Services	Unique Naming
		Registration
		Public Key Certification
		Credentials Certification
		Directory Service
		Authorization
		Authentication
	Communications Security	Session Authentication
		Message Origin Authentication
		Message Integrity Protection
		Message Content Confidentiality
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security
		Environment Security
		Non-repudiation
		Message Replay Protection
		Traffic Flow Confidentiality
	Application & System Security	Authorization
		Logical Access Controls
		Audit Trails
		Stored Data Integrity Protection
		Store Data Confidentiality
		Software Integrity Protection
		Software Licensing Management
		System Configuration Protection
		Data Replication & Backup
		Software Replication & Backup
		Trusted Time
		User Interface for Security
	Security Management	Policy Management
		Training & Awareness
		Operations Management
		Provisioning
		Monitoring
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security Devices
		Environmental Security

Containment Services



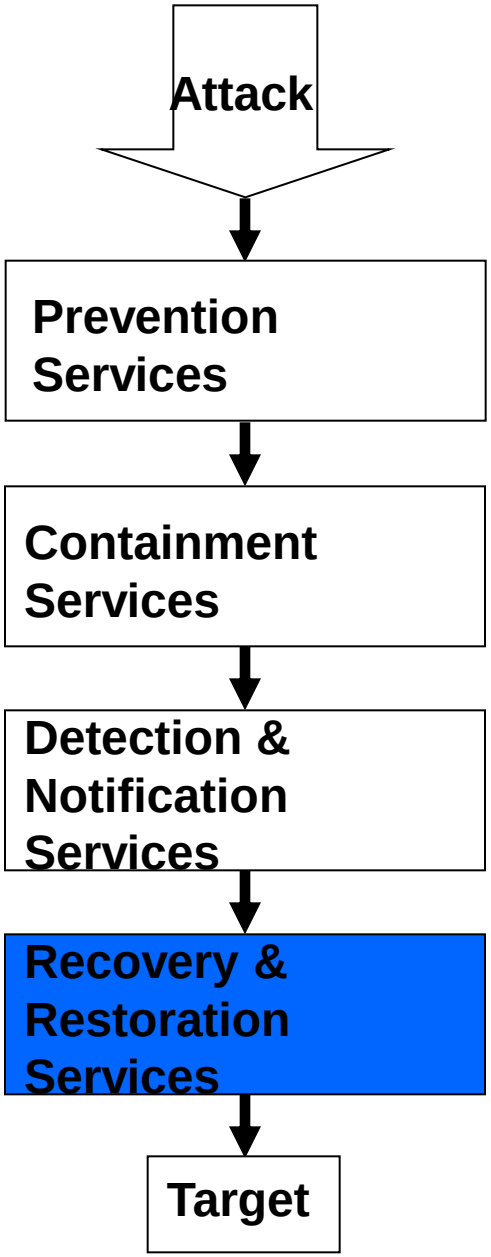
Security Architecture Tier	Security Services
Containment	Entity Authorization
	Store Data Confidentiality
	Software Integrity Protection
	Physical Security
	Environmental Security
	Training & Awareness

Detection & Notification Services



Security Architecture Tier	Security Services
Detection & Notification	Message Integrity Protection
	Store Data Confidentiality
	Security Monitoring
	Intrusion Detection
	Security Alarm Management
	Training & Awareness
	Measurement & Metrics

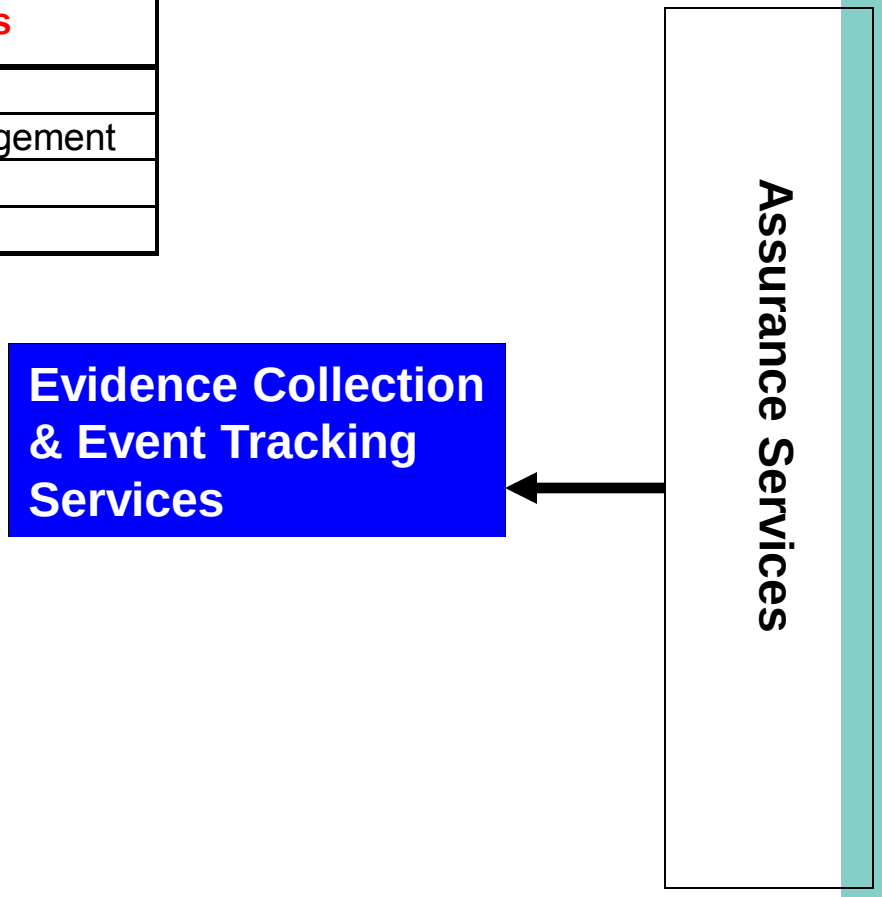
Recovery & Restoration Services



Security Architecture Tier	Security Services
Recovery & Restoration	Incident Response
	Data Replication & Backup
	Software Replication & Backup
	Disaster Recovery
	Crisis Management

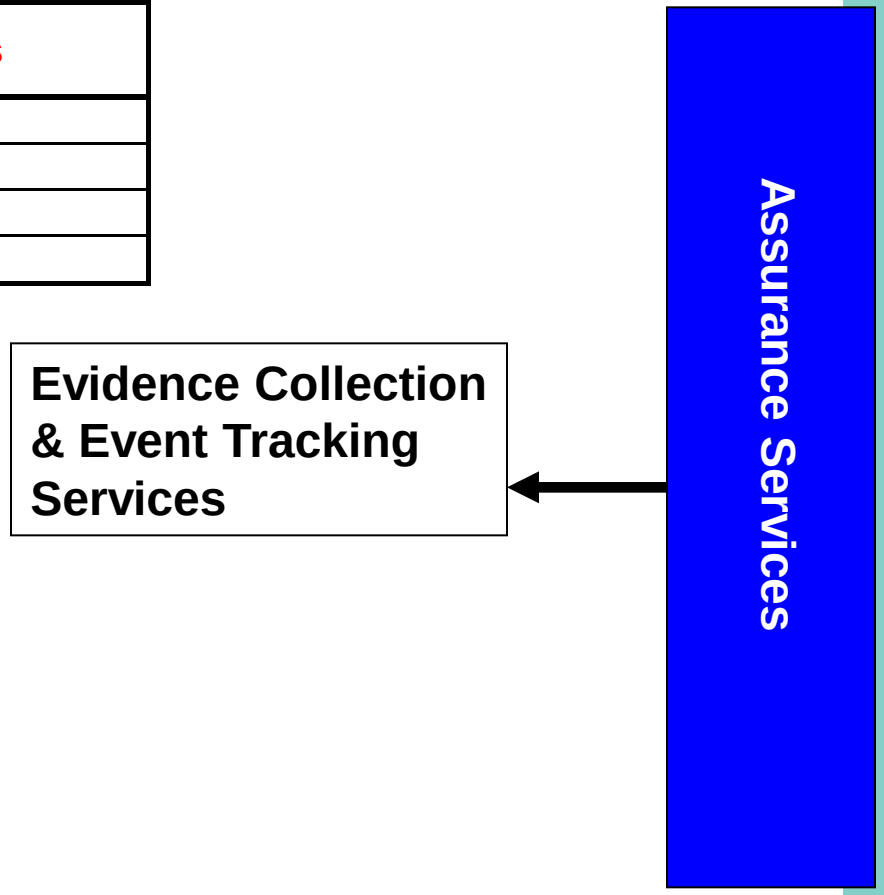
Event Collection & Tracking Services

Security Architecture Tier	Security Services
Event Collection & Event Tracking	Audit Trails
	Security Operations Management
	Security Monitoring
	Measurement & Metrics



ASSURANCE SERVICES

Security Architecture Tier	Security Services
Assurance	Audit Trails
	Security Audit
	Security Monitoring
	Measurement & Metrics



SABSA Overview

- SABSA provides a **holistic** approach to cyber/information security and is baselined against the '*ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*' standard
- Five layer framework that answers the why, how, who, where and when for security architecture
- Five layers are Contextual Architecture, Conceptual Architecture, Logical Architecture, Physical Architecture and Component Architecture
- A sixth layer is added for Service Management Architecture and is synonymous with Operational Security Architecture
- Compatible and complementary to other architecture frameworks, including Zachman, TOGAF, DODAF, etc.

SABSA Framework – Fully Qualified

Business Architecture
Security Architecture
Information Architecture
Application Architecture
Technology Architecture
Risk Management & Information Security

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Action and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

BASIC BACKGROUND INFORMATION

Basic Cybersecurity Objectives

- Availability is the most important security objective for power system reliability. The time latency associated with availability can vary—
  - ≤ 4 ms for protective relaying
  - Subseconds for transmission wide-area situational awareness monitoring
  - Seconds for substation and feeder SCADA data
  - Minutes for monitoring noncritical equipment and some market pricing information
  - Hours for meter reading and longer-term market pricing information; and
  - Days/weeks/months for collecting long-term data such as power quality information.
- Integrity for power system operations includes assurance that—
  - Data has not been modified without authorization
  - Source of data is authenticated
  - Time stamp associated with the data is known and authenticated; and
  - Quality of data is known and authenticated.
- Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online—
  - Privacy of customer information
  - Electric market information; and
  - General corporate information, such as payroll, internal strategic planning, etc

Created an initial business attribute list

- **Attribute classes:**
  - **User attributes**
  - **Management attributes**
  - **Operational attributes**
  - **Risk management attributes**
  - **Legal and regulatory attributes**
  - **Technical strategy attributes**
  - **Business strategy attributes**

Defense Strategy of Security Services

- Using a standard attack multi-tier security services and review common security service services
- Review generic message list and apply security services
- http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p1.xls

Cannot go all the way to specific implementations

- We cannot go all the way to specific technology and implementations because
  - Do not know organizational objectives
  - Do not know specific organizational requirements
  - Do not know organizational size or scope
- Order – Eat – Pay or Order – Pay – Eat example

Transmission

Tim Yardley – University of Illinois
Information Trust Institute

NITRD TTS Workshop

July 18-20, 2011

Setting The Stage

- Fairly static security settings
  - Tailored to their mission
  - Predominately perimeter security
- Generally single operating domain
- Varied technology and communication mediums in use
- Some stringent requirements (“low” msec)
- Some very loose requirements (hourly, daily)
- Humans and Machines involved

Use Case 1

Use case 1

- Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data
  - NISTIR-7628, pg. 129
- “Normal” Operations
  - Things are generally operating per-norm

Use case 1 - Description

- Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Use case 1 - Scenario

- Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include
  - Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)
  - Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions
  - Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies
  - Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components

Use case 1 – SG Characteristics

- Characteristics
  - Provides power quality
  - Optimizes asset utilization
  - Anticipates and responds to system disturbances
- Potential Stakeholder issues
  - Customer safety
  - Customer device standards
  - Demand response acceptance by customers

Use case 1 – Cyber Security

- Integrity is vital to the safety and reliability of the transmission system
- Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)
- Confidentiality is not important

Use case 1 – Potential Actors

- Operators
- Field Technicians
- Control Centers
- Substations
- Devices, Power Assets
- Vendors, Third party contractors
- Attackers
- External Actors
  - Any of the above, but not in your control

Use case 1 – Potential Transactions

- Monitoring
  - Loss of, Inaccurate, Verifiable
- Maintenance operations
  - Pre, On-going, Post
- Automation
  - External, Internal, Cooperative
- System experiences a disturbance
  - Physical, Cyber, or Cyber-Physical

Use case 1 – Potential Information

- Topology
- Planning data
  - Models, Forecasts, etc.
- Operational data
  - Measurements, Alarms, etc.
- Out-of-band communication
  - Field interactions, External interactions, etc.
- Ancillary information
  - Weather, News reports, etc.

Use case 1 – Example

- Poll substation for data
- Input data into EMS/state estimation
- Output current state into
  - Contingency analysis
  - Control actions
  - Etc.
- Analyze/Apply results

Use Case 2

Use case 2

- Real-Time Emergency Transmission Operations
  - NISTIR-7628, pg. 131
- “Emergency” Operations
  - Something bad has happened

Use case 2 - Description

- Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Use case 2 - Scenario

- During emergencies, the power system takes some automated actions and the operators can also take actions
  - Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery
  - Operators manage emergency alarms
  - SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and pre-arming of fast acting emergency automation
- SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts)
  - Operators performs system restorations based on system restoration plans prepared (authorized) by operation management

Use case 2 – SG Characteristics

- Characteristics
  - Provides power quality
  - Optimizes asset utilization
  - Anticipates and responds to system disturbances
- Potential Stakeholder issues
  - Customer safety
  - Customer device standards
  - Demand response acceptance by customers

Use case 2 – Cyber Security

- Integrity is vital to the safety and reliability of the transmission system
- Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)
- Confidentiality is not important

Use case 2 – Potential Actors

- Operator
- Field Technician
- Control Center
- Substation
- Device
- Emergency Agency or Person
- External Actor
  - Any of the above, but not in your control

Use case 2 – Potential Transactions

- Communication
  - None, Physical only, Full
- Islanding
  - Controlled, Forced,
- Alarming
  - Verifiable, False
- Analysis
  - Locatable, No Results
- Restoration
  - Internal, External, Cooperative

Use case 2 – Potential Information

- Topology
- Planning data
  - Models, Forecasts, etc.
- Operational data
  - Measurements, Alarms, etc.
- Out-of-band communication
  - Field interactions, External interactions, etc.
- Ancillary information
  - Weather, News reports, etc.

Use case 2 – Example

- Prioritize alerts and alarms
- Poll substations for data (priority based)
- Input data into EMS/state estimation
- Output current state into
  - Contingency analysis
  - Control actions
    - Enable disturbance monitoring
    - Enable emergency automation
  - Etc.
- Analyze/Apply results

Scenarios

Scenario 1

- Areas that are operating close to margins determined by contingency analysis or state estimation may be of more concern in the short time frame than others. This means that areas that are near capacity, under maintenance, experiencing issues, or more “fragile” than others may have dynamic constraints that change with conditions. Further, these locations will vary based on state estimation solutions, contingency analysis, etc.

Scenario 2

- Some areas are more critical than other areas due to how they are connected, how the BES is constructed, or the current state of the system. For example, lines that are inter-ties, or connected to major assets feeding high demand areas may be more important than others despite their relatively lower capacity. Another example may be that a location is geographically distant from generation and as a result has voltage stability issues due to this topology.

Tailoring

Properties

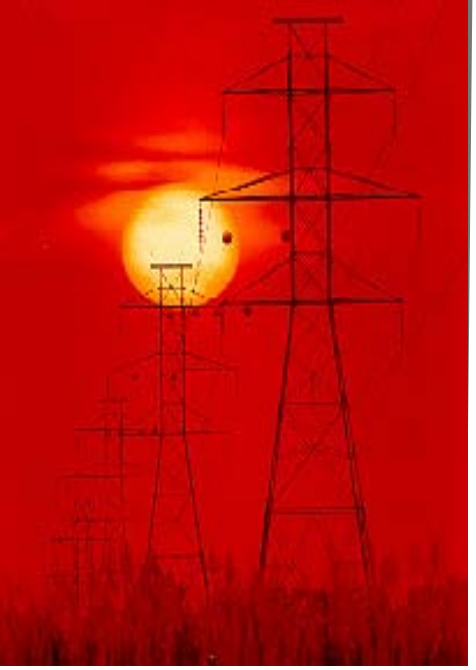
- Availability, Authentication, Integrity, Timeliness, Non-repudiation, logging, time accuracy, alarm reporting, provenance, guaranteed latency, Privacy, Confidentiality

Tailoring Cases

- State Estimation
  - Operational vs Pricing/Market
- Confidentiality
  - It actually is important… Emergency operations
  - Perhaps Authentication can handle this?

Property Working Document

- Automated machine to machine actions for distributed protection and control
  - Less impt: Privacy, Confidentiality
  - SCADA - slow
  - Line protection – fast
- Authentication
  - Emergency response (drop auth if necessary?)



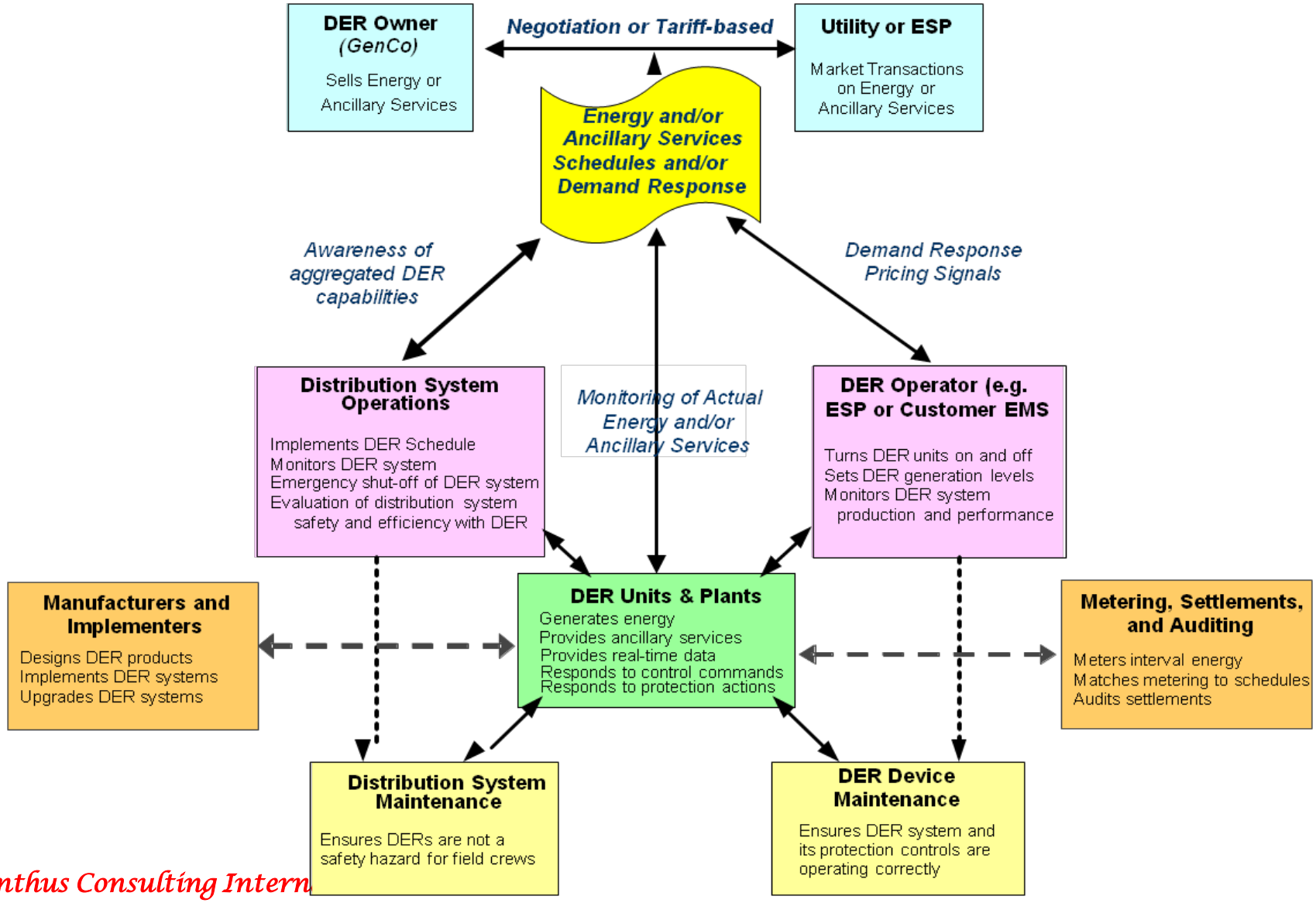
Virtual Power Plant of Distributed Energy Resources (DER) Systems Used for Distribution System Volt/Var Management

Frances Cleveland

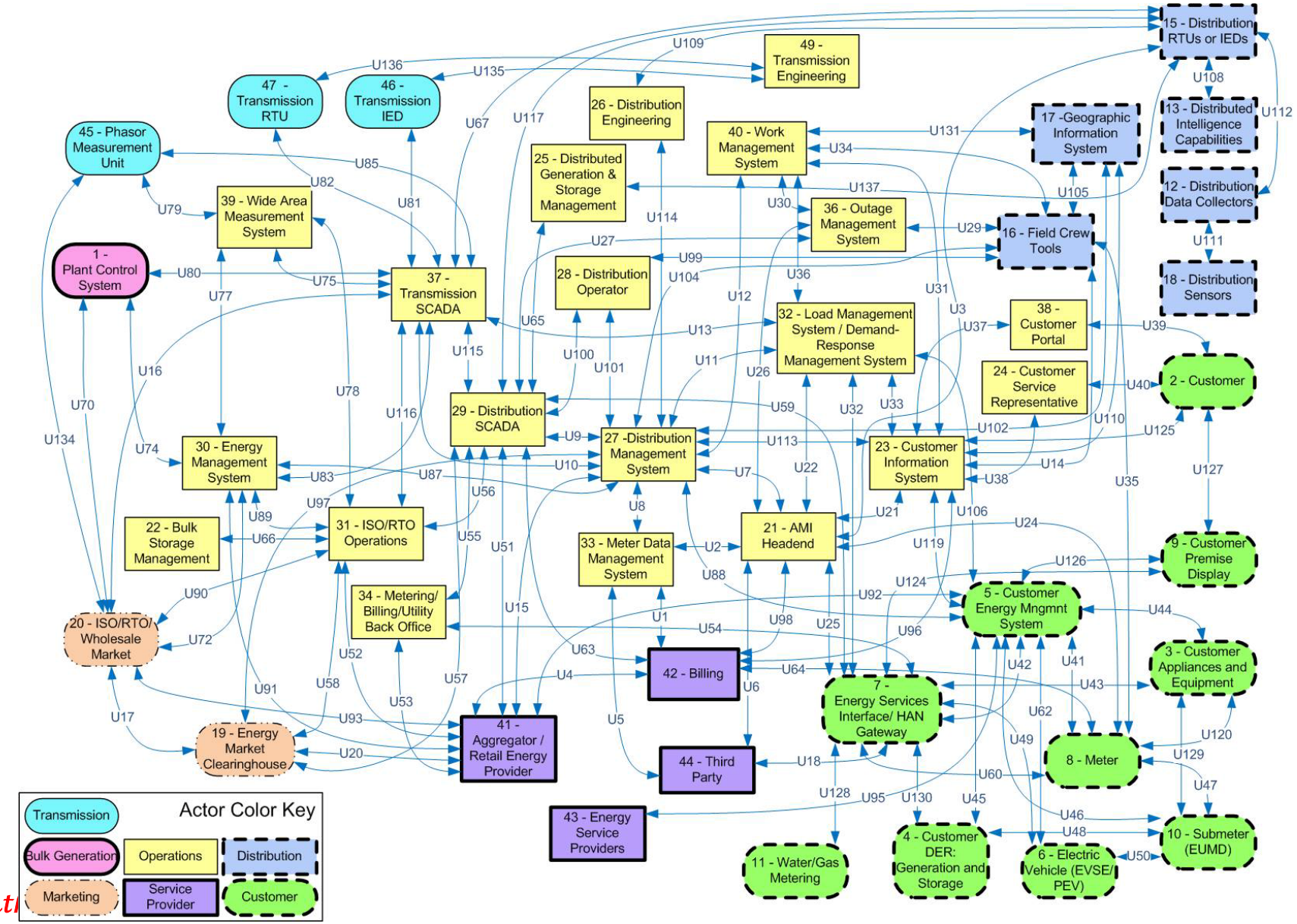
fcleve@xanthus-consulting.com

Xanthus
Consulting International

DER Stakeholders / Actors
(In California, 12,000 MW must be added by 2020)



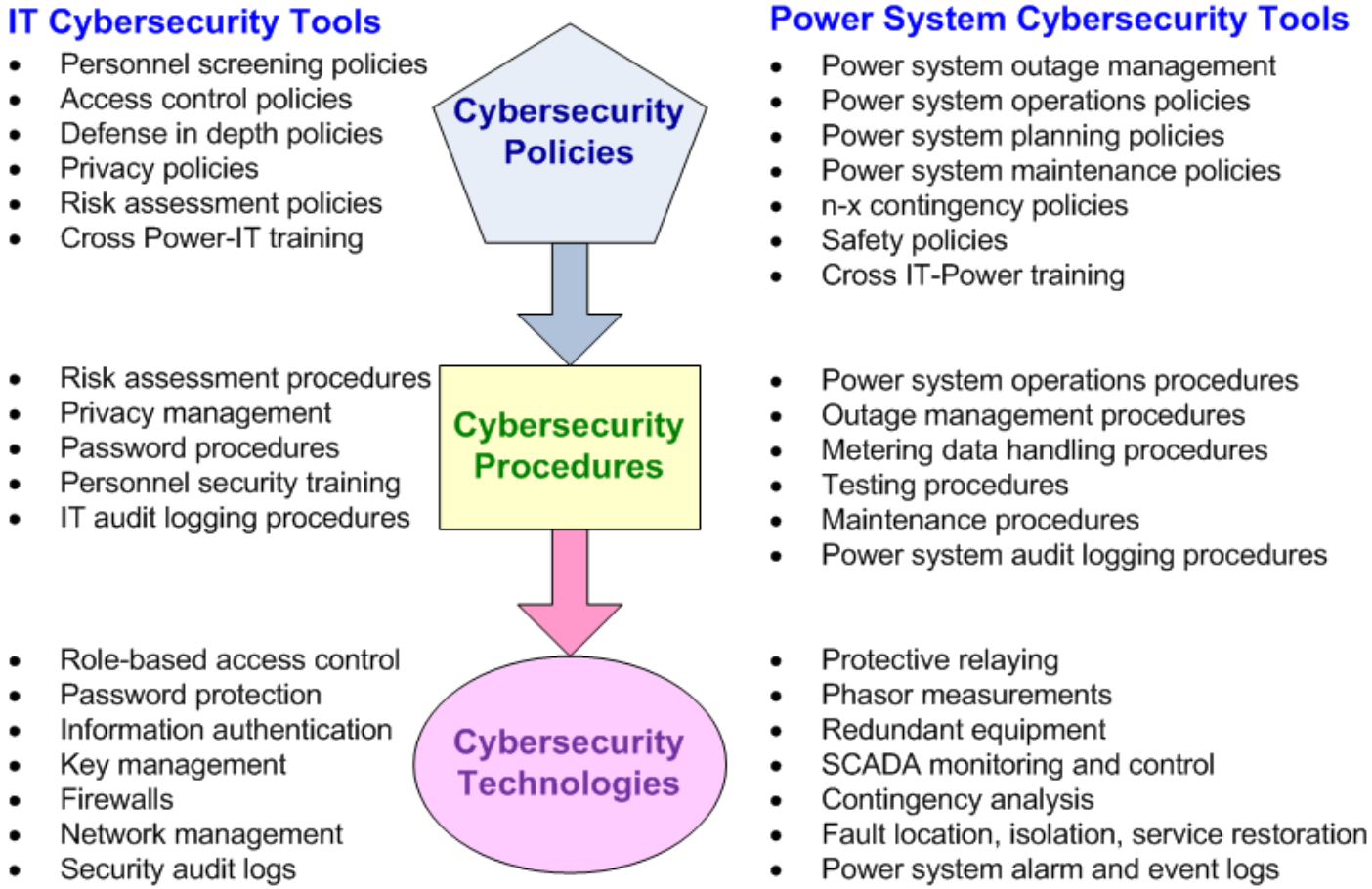
NISTIR 7628 “Spaghetti” Diagram



Policies, procedures, and technologies

Goals for Electric Sector Cybersecurity:

- ***Availability/Reliability*** of the Power System
- ***Integrity*** of Critical Information
- ***Confidentiality*** of Sensitive Data



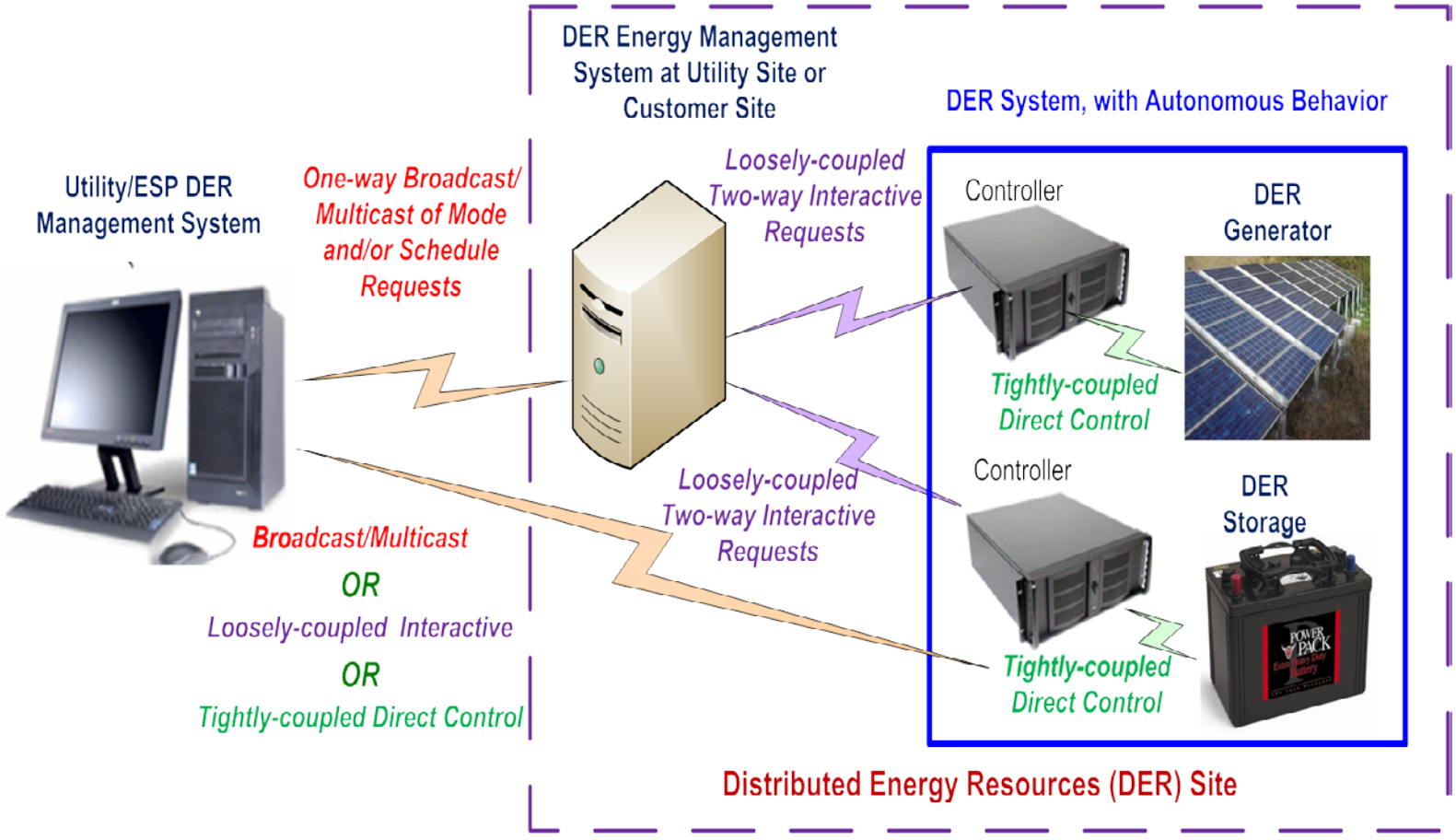
NISTIR 7628 Interface Categories to Identify Security Catalog Requirements (copied from NISTIR)

Logical Interface Categories		Logical Interfaces		Security			NIST Catalog of Security Requirements									
#	Interface Category Description	Interface	#	C	I	A	SG.PE	SG.SA	SG.CM	SG.SC	SG.MA	SG-IR	SG.SI	SG.AC	SG.AU	SG.RA
1	Interface between control systems and equipment with high availability requirements, and with compute and/or bandwidth constraints, for example: • Between distribution protective relays and protected equipment • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	Distribution protective relaying Trans. SCADA & substation IEDs	U108a U67	L	H	H	PE-2 PE-3 PE-4 PE-21 PE-22	SA-12 SA-13	CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 CM-11	SC-2 SC-3 SC-5 SC-6 SC-7 SC-8 SC-11 SC-12 SC-14 SC-15 SC-20 SC-22	MA-2 MA-4 MA-10	IR-8 IR-9 IR-15 IR-18	SI-4 SI-7 SI-8 SI-9 SI-10 SI-11	AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 AC-24 AC-25	AU-2 AU-3 AU-4 AU-8 AU-16	RA-5

Use Case Narrative – Background

- A university campus has many buildings with photovoltaic arrays on their roofs.
- Each PV array has an associated controller located within the building.
- Some of these buildings also have
  - large battery systems,
  - while a couple of diesel generators are available for backup for some critical laboratories, but may be used occasionally for additional generation.
  - Many professors and students have Electric Vehicles that are available for energy management
- The university has a customer energy management system (CEMS) that manages these DER systems, with a contract to respond to an energy service provider's (ESP) signals for providing energy and ancillary services to the utility grid.
- These ancillary services include volt/var management.

Virtual Power Plant 3-Lever Configuration



DER Management: Interactions between Components

Scenario

- On a hot afternoon:
  - the utility determines that the transmission system needs more vars,
  - broadcasts a signal (using IEC 61850 over the DNP3 protocol over a cellphone wireless data channel, similar to Amazon's Kindle) to the ESP (and many other entities) to "go into volt/var mode 3".
- The ESP in turn sends this request to the CEMS,
  - including some additional information based on their contractual relationship with the university,
  - (using IEC 61850 over web services through a virtual private network over the Internet).
- The CEMS commands some of the building PV systems and one battery storage system to provide the volt/var mode 3,
  - while also commanding one diesel generator to run for an hour to help charge up the other battery systems
  - (using IEC 61850 over SEP 2.0 over the campus LAN).
- Responses from the controllers to these commands allow the CEMS to determine if additional steps need to be taken.

Use Case Steps (1-3)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
1	Transmission system needs vars	Utility DMS	ESP	Request for volt/var mode 3	• Request for volt/var mode 3	IEC 61850 DNP3 Cellphone systems	**Authentication** **Integrity** **Provenance** **Non-repudiation**
2	ESP receives request	ESP	CEMS	Request for volt/var mode 3	• Request for volt/var mode 3 • Maintain same energy output • Ensure battery storage is full by 6 pm	IEC 61850 Web services Internet	**Authentication** **Integrity** **Confidentiality** **Non-repudiation** **Timeliness** **Guaranteed delivery** **Time accuracy** **Logging**
3	CEMS receives request	CEMS	Some PV systems	Command for volt/var mode 3	• Command to go into volt/var mode 3 within 5 minutes	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**

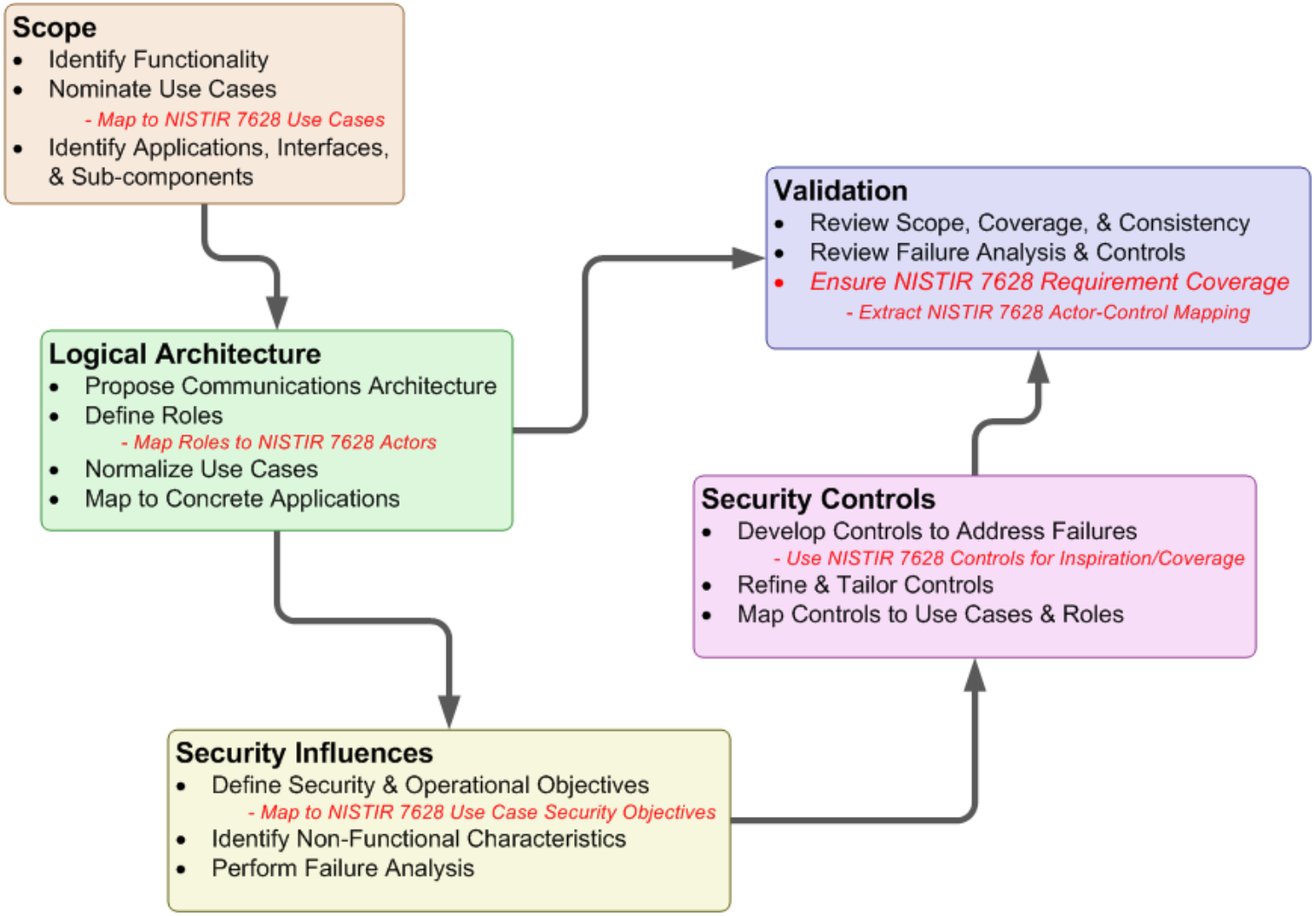
Use Case Steps (4-6)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
4	CEMS receives request	CEMS	One battery system and some EVs	Command for volt/var mode 3	• Command to go into volt/var mode 3 within 5 minutes	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**
5	CEMS receives request	CEMS	One diesel generator	Command to turn on and provide x kW of energy for 2 hours	• Command to turn on and generate x kW	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**
6	Upon mode change	PV systems	CEMS	Acknowledging going into volt/var mode 3	• Ack	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Alarm reporting** **Logging**

Use Case Steps (7-8)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
7	Upon mode change	Battery systems	CEMS	Error going into volt/var mode 3	• Error message	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Alarm reporting** **Logging**
8	Continuously	Monitoring devices at the connection between the campus and the grid	CEMS	Using report by exception, monitor the energy, vars, and other electrical parameters	• Measurements of watts, vars, voltage, frequency, etc.	IEC 61850 Web services LAN	**Authentication** **Availability** **Alarm reporting** **Logging**

Use Case to Control Process



Basic Steps

1. Scope
   a) Nominate functionality (i.e., use case titles)
   b) Delineate real-world application/component coverage

Black Box

2. Logical Architecture
   a) Nominate logical architecture
   b) Define roles by functionality
   c) Refine use cases & logical architecture

White Box

3. Security Constraints
   a) Define security & operational objectives
   b) Perform failure analysis

Justification

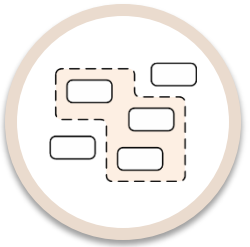
4. Security Controls
   a) Define controls (including recommended network segmentation)
   b) Map and tailor controls to roles

Reqmts

5. Validation

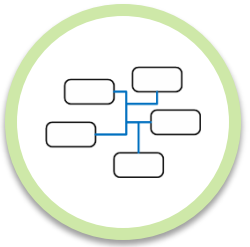
Process Notes: Scope

- Why is this important?
  - First point of entry for new audiences
  - Will likely dictate whether the document gets broad review and engagement
- What does it do?
  - End users must be able to figure out if this document applies to them or not
  - Need an easy and clear “yes” or “no” answer
  - Should not have to understand the rest of the document
- What is the approach?
  - Define functionality covered in real-world terms
  - Provide examples using real-world terminology



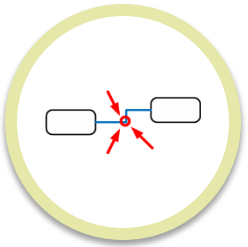
Process Notes: Logical Architecture

- Why is this important?
  - Lack of coverage for functionality is the root of security vulnerabilities
  - Lack of coverage is rarely intentional
    - Ambiguity in terminology
    - Changes in functionality over time
- What does it do?
  - Provides abstract (vendor-neutral) representation of the system to bind controls
  - Removes ambiguity about functionality covered
- What is the approach?
  - Define roles in terms of functionality
  - Describe relationships between the roles
  - Define the functionality in terms of use cases
    - Use a normalized format that facilitates verification of coverage



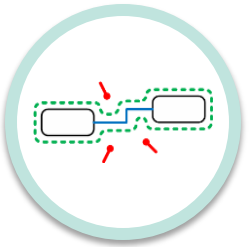
Process Notes: Security Constraints

- Why is this important?
  - Security ultimately has a cost
  - How do we know we are investing in the right place?
- What does it do?
  - Provides justification for selection of controls
  - Provides traceability for ***when*** (not if) system functionality changes
  - Provides a means to quantifiably claim coverage
- What is the approach?
  - Define objectives for system operation
    - What the system should do
    - What the system should **NOT** do
  - Define failures the system should prevent
    - Bind to functionality (avoidance is one means of mitigating risk)
    - Look at both common and functionality-specific failures

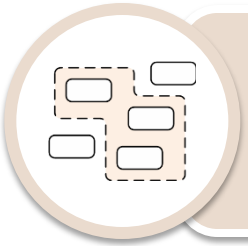


Process Notes: Security Controls

- Why is this important?
  - Actions and requirements must be precisely defined
- What does it do?
  - Provides actionable guidance for the end user
  - Establishes a context to link high-level objectives to low-level security mechanisms
- What is the approach?
  - Generate controls
    - Brainstorm controls from failures
    - Normalize controls into approachable and useful organization for the end user
  - Map to logical architecture
    - System (i.e., network segmentation)
    - Roles
  - Adapt controls to specific context for each role
    - (e.g., consider resource constraints, access requirements, maintenance…)

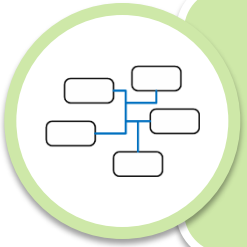


Document Essentials



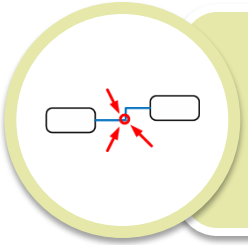
Scope

- Functionality Covered
- Applications, Interfaces, & Sub-Components
- Explicit Examples



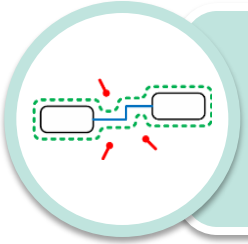
Logical Architecture

- Communications Architecture
- Roles
- Use Cases
- Mapping to Concrete Applications



Security Considerations

- Contextual & Operational Assumptions
- Security Principles
- Failure Analysis



Security Controls

- Network Segmentation
- Control Definitions
- Mapping of Controls to Roles & Segments

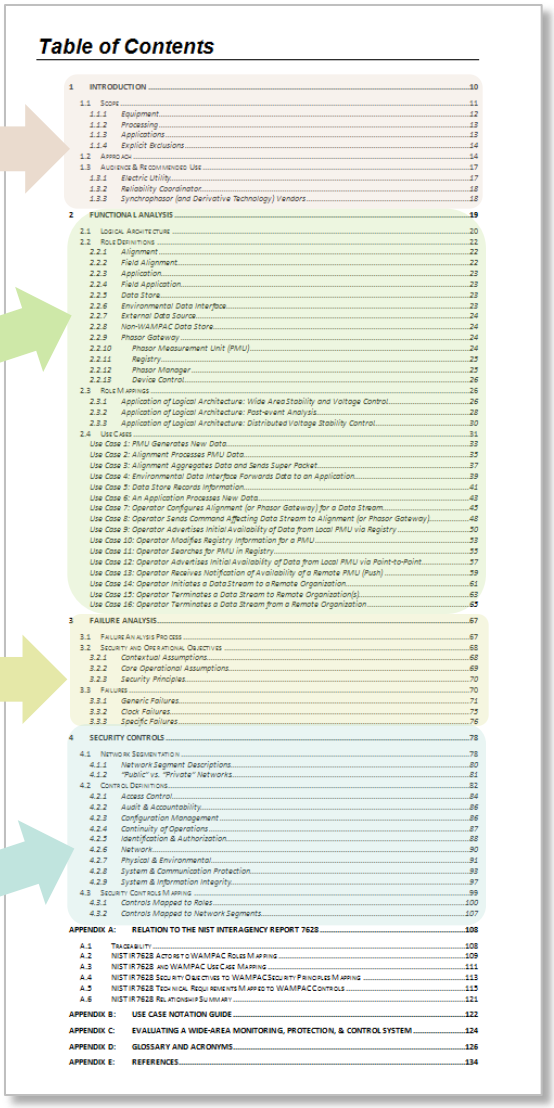


Table of Contents

1 INTRODUCTION 10
1.1 Scope 11
1.1.1 Equipment 12
1.1.2 Processing 13
1.1.3 Applications 13
1.1.4 Explicit Exclusions 14
1.2 Approach 14
1.3 Audience & Recommended Use 17
1.3.1 Electric Utility 17
1.3.2 Reliability Coordinator 18
1.3.3 Synchrophasor (and Derivative Technology) Vendors 18
2 FUNCTIONAL ANALYSIS 19
2.1 Logical Architecture 20
2.2 Role Definitions 21
2.2.1 Alignment 22
2.2.2 Field Alignment 22
2.2.3 Application 23
2.2.4 Field Application 23
2.2.5 Data Store 23
2.2.6 Environmental Data Interface 23
2.2.7 External Data Source 24
2.2.8 Non-WAMPAC Data Store 24
2.2.9 Phasor Gateway 24
2.2.10 Phasor Measurement Unit (PMU) 24
2.2.11 Registry 25
2.2.12 Phasor Manager 25
2.2.13 Device Control 26
2.3 Role Mappings 26
2.3.1 Application of Logical Architecture: Wide Area Stability and Voltage Control 26
2.3.2 Application of Logical Architecture: Post-event Analysis 28
2.3.3 Application of Logical Architecture: Distributed Voltage Stability Control 30
2.4 Use Cases 31
Use Case 1: PMU Generates New Data 33
Use Case 2: Alignment Processes PMU Data 35
Use Case 3: Alignment Aggregates Data and Sends Super Packet 37
Use Case 4: Environmental Data Interface Forwards Data to an Application 39
Use Case 5: Data Store Records Information 41
Use Case 6: An Application Processes New Data 43
Use Case 7: Operator Configures Alignment (or Phasor Gateway) for a Data Stream 45
Use Case 8: Operator Sends Command Affecting Data Stream to Alignment (or Phasor Gateway) 48
Use Case 9: Operator Advertises Initial Availability of Data from Local PMU via Registry 50
Use Case 10: Operator Modifies Registry Information for a PMU 53
Use Case 11: Operator Searches for PMU in Registry 55
Use Case 12: Operator Advertises Initial Availability of Data from Local PMU via Point-to-Point 57
Use Case 13: Operator Receives Notification of Availability of a Remote PMU (Push) 59
Use Case 14: Operator Initiates a Data Stream to a Remote Organization 61
Use Case 15: Operator Terminates a Data Stream to Remote Organization(s) 63
Use Case 16: Operator Terminates a Data Stream from a Remote Organization 65
3 FAILURE ANALYSIS 67
3.1 Failure Analysis Process 67
3.2 Security and Operational Objectives 68
3.2.1 Contextual Assumptions 68
3.2.2 Core Operational Assumptions 69
3.2.3 Security Principles 70
3.3 Failures 70
3.3.1 Generic Failures 71
3.3.2 Clock Failures 73
3.3.3 Specific Failures 76
4 SECURITY CONTROLS 78
4.1 Network Segmentation 78
4.1.1 Network Segment Descriptions 80
4.1.2 "Public" vs. "Private" Networks 81
4.2 Control Definitions 82
4.2.1 Access Control 84
4.2.2 Audit & Accountability 86
4.2.3 Configuration Management 86
4.2.4 Continuity of Operations 87
4.2.5 Identification & Authorization 88
4.2.6 Network 90
4.2.7 Physical & Environmental 91
4.2.8 System & Communication Protection 93
4.2.9 System & Information Integrity 97
4.3 Security Controls Mapping 99
4.3.1 Controls Mapped to Roles 100
4.3.2 Controls Mapped to Network Segments 107
APPENDIX A: RELATION TO THE NIST INTERAGENCY REPORT 7628 108
A.1 Traceability 108
A.2 NIST IR 7628 Actors to WAMPAC Roles Mapping 109
A.3 NIST IR 7628 and WAMPAC Use Case Mapping 111
A.4 NIST IR 7628 Security Objectives to WAMPAC Security Principles Mapping 113
A.5 NIST IR 7628 Technical Requirements Mapped to WAMPAC Controls 115
A.6 NIST IR 7628 Relationship Summary 121
APPENDIX B: USE CASE NOTATION GUIDE 122
APPENDIX C: EVALUATING A WIDE-AREA MONITORING, PROTECTION, & CONTROL SYSTEM 124
APPENDIX D: GLOSSARY AND ACRONYMS 126
APPENDIX E: REFERENCES 134

For Each Use Case You Need To Think About

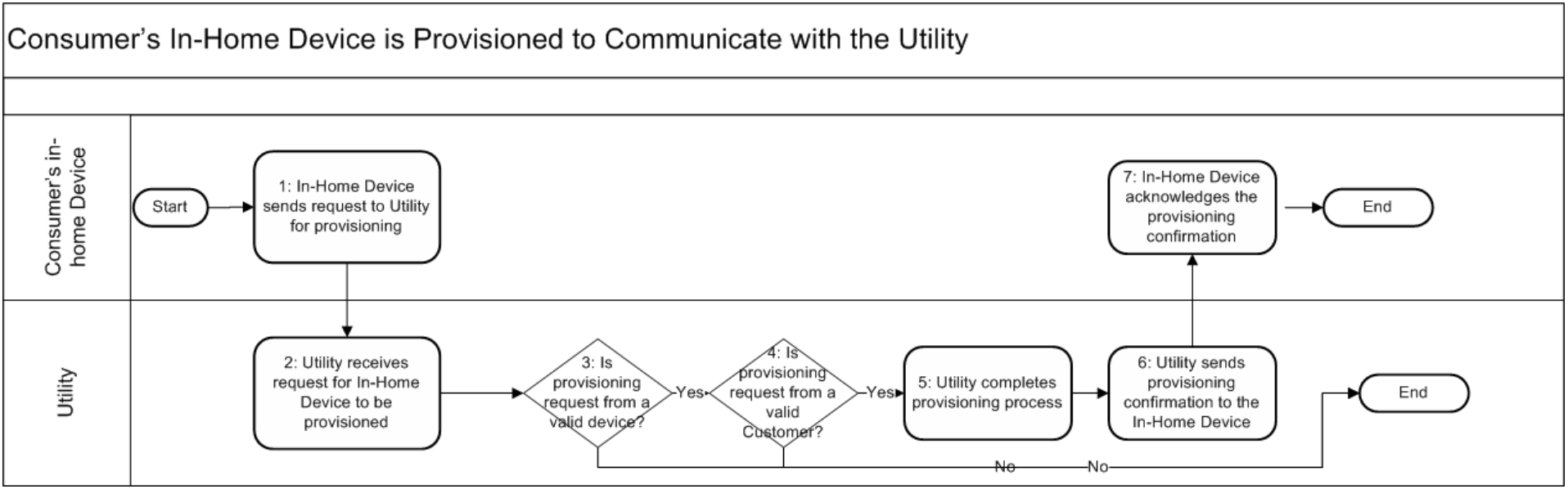
- Preconditions
- Minimal Guarantees
- Success Guarantees
- Trigger

Use case 1 - Customer's In Home Device is Provisioned to Communicate With the Utility

Use case 1 - Summary

- Scenario: Customer's In Home Device is Provisioned to Communicate With the Utility
- Description: This scenario describes the process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device, or smart appliance.

Use case 1 – Business Flow



Use Case 1 – SG Characteristics

- Characteristics
  - Enables active participation by consumers
  - Accommodates all generation and storage options
  - Enables new products, services and markets
- Potential Stakeholder issues
  - Customer device standards
  - Customer data privacy and security

Use Case 1 – SG CyberSecurity Objectives

- To protect passwords
- To protect key material
- To authenticate with other devices on the AMI system

Use case 1 – Potential Transactions

- Registration of the customer device
- Authentication of the customer device
- Receiving information from the utility
- Sending information to the utility
- Receiving a command from the utility
- Recording information on the device

Use case 1 – Potential Information

- Customer ID
- Customer authentication
- Device location information
- Device ID
- Device type
- Device configuration
- Device authentication information
- Logging information
- Time of day

Use case 1 – Potential Failures With (1)

- Send Data
  - Sends to wrong place
  - Sends wrong data
  - Sends corrupted data
  - Spurious send
  - Not authorized to send
  - Sends data late (not timely)
- Receive data
  - Not from authorized sender/from wrong sender
  - Receives wrong data
  - Receives corrupted data
  - Spurious receive
  - Does not receive timely data
  - Data is inappropriately rejected

Use case 1 – Potential Failures With (2)

- Store data
  - Allows unauthorized access and manipulation
  - Storage corrupted
  - Storage exhaustion
- Process data
  - Does not execute in a timely fashion (resource starvation)
  - Mis-configured
  - Subverted to execute wrong code

Use case 1 – Potential Failures With (3)

- Potential specific failures
  - Communication interruption – verbal, email and other non-energy use information
  - Does not act on a authenticated command
  - Acts on a authenticated command against local policy
  - Stolen credentials used to authorize command
  - Processes unrecognized command
  - Processes unauthenticated command
  - Fails to execute action based on changes to its operational parameters, its data, or its internal state
  - Processes an incorrectly formatted message
  - Does not respond to a message in a timely fashion
  - Fails to execute action in a timely fashion after receiving a legitimate message

Use case 1 – Potential Failures With (4)

- Potential specific failures
  - Need to have graceful failure (fail safely)
  - Default failure configuration (e.g. DR)
  - Fails to protect information or resources against authorized access
  - Fails to accept authorized and valid message
  - Fails to execute action based on changes to its operational parameters, its data, or its internal state
  - Executes wrong action based on changes to its operational parameters, its data, or its internal state
  - Accepts corrupted configuration file
  - Hardware, facilities or both fail and prevent proper operation
  - Failure to provide adequate protection against reasonable expectations for harm due to natural phenomenon, such as earthquakes, hurricanes, tornadoes, and electromagnetic interference
  - Failure to provide recovery mechanisms essential for the restoration of a failed or compromised system

Use case 1 – Potential Controls for Each Failure

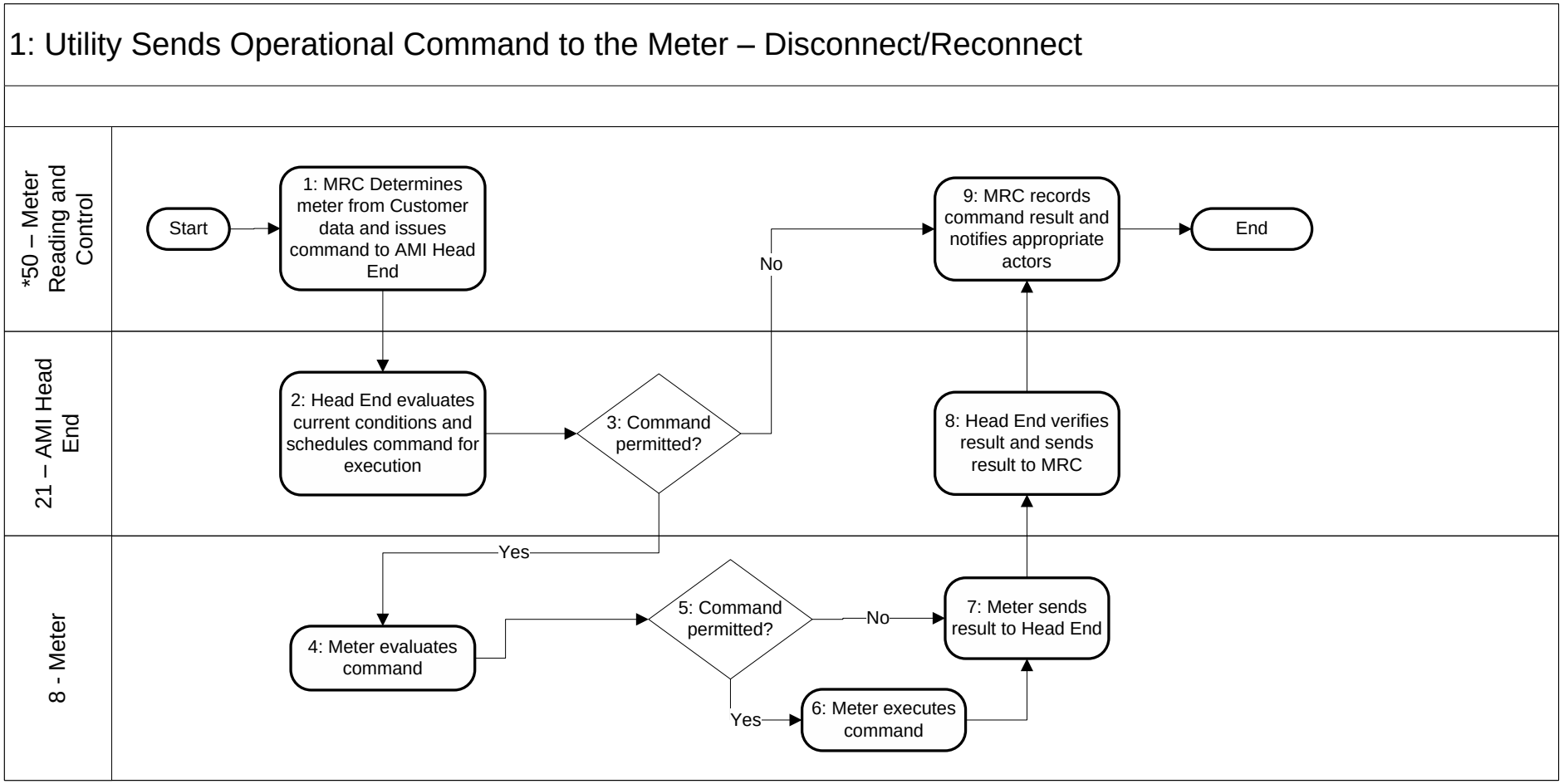
- Define at least one control for each failure
- Create a mapping back and forth to ensure every failure has a control and for every control we can indentify at least one failure

Use case 2 - Remote Connect/Disconnect of Meter

Use case 2 - Summary

- Scenario: Remote Connect/Disconnect of Meter
- Description: Traditionally, utilities send a metering service person to connect or disconnect the meter. With an AMI system, the connect/disconnect can be performed remotely by switching the remote connect/disconnect (RCD) switch for the following reasons:
  - Remote Connect for Move-In
  - Remote Connect for Reinstatement on Payment
  - Remote Disconnect for Move-Out
  - Remote Disconnect for Nonpayment
  - Remote Disconnect for Emergency Load Control
  - Unsolicited Connect / Disconnect Event

Use case 2 – Business Flow



Use Case 2 – SG Characteristics

- Characteristics
  - Optimizes asset utilization and operate efficiently
  - Operates resiliently against attack and natural disasters
- Potential Stakeholder issues
  - Customer data privacy and security
  - Retail Electric Supplier access
  - Customer data access
  - Customer Safety

Use Case 2 – SG CyberSecurity Objectives

- Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved
- Availability to turn meter back on when needed is important
- Confidentiality requirements of the RCD command is generally not very important, except related to non-payment

Use case 2 – Potential Transactions

- Valid registration of device/meter
- Authentication of the device/meter
- Receiving information from the utility
- Sending information/confirmation to the utility
- Receiving a command from the utility
- Recording information on the device

Use case 2 – Potential Information

- Customer ID
- Customer authentication
- Device location information
- Device/Meter ID
- Device/Meter type
- Device/Meter configuration
- Device/Meter authentication information
- Logging information
- Time of day
- Command information from device/meter and utility
- Response to the command from device/meter and utility

Use case 2 – Potential Failures With

- Sending information
  - Authorization
  - Authentication
  - Disclosure
  - Availability
  - Logging / Auditing
  - Communication links – down, delay, etc
- Receiving information
- Information storage
- Communication method
- The information itself

Use case 2 – Potential Controls for Each Failure

- Define at least one control for each failure
- Create a mapping back and forth to ensure every failure has a control and for every control we can indentify at least one failure

Policy Machine

Tailoring access control policies and data services to missions

David Ferraiolo, Serban Gavrila
National Institute of Standards and Technology

dferraiolo@nist.gov

The Policy Machine (PM)

A logical “machine” comprising:

- a fixed set of data and relations used to express (combinations of) access control policies and delivery of data services
- a fixed set of administrative operations for configuring the data and relations
- a fixed set of functions for making access control decisions and enforcing the policies

PM Data & Relations

- Basic elements
  - Users, processes, operation, and objects
- Containers
  - User attributes, object attributes, and policy classes
- Relations
  - Assignments (defining membership in containers)
  - Associations (defining privileges)
  - Prohibitions (denies for users and processes)
  - Obligations (Event/Response)

Unification through Privileges

- Through proper representation privileges (user, operation, object) appear and disappear at three levels
- Level 1: Privileges are specifications of users that can perform read and/or write operations on data objects.
- Level 2: Users are administrators that can perform administrative operations on the data elements and relations resulting in privileges of first and second levels. The users in the second level may include those of the first.
- Level 3: Capabilities in the third level are arbitrary, but data service specific. Although arbitrary, capabilities are composed of sequences of operations of the second level that act upon objects of the first and second levels. These sequences are executed by authorized users of the second level, as commands, or automatically, in response to events, by the PM as obligations.

Some Benefits
(demonstrated by prototype)

- Access Control as a Data Service operate as one
- Through a single authenticated session, users are offered capabilities of file management (to include support for office applications), email, workflow, and forms and records management. Others services could be accommodated as well.
- Select capabilities (of different services) are delivered to select users, under combinations of arbitrary, but **mission tailored** forms of **discretionary**, **mandatory**, and **history-based** (event driven) access controls.
- Data services naturally interplay.
- Data is naturally protected across services.

Prohibitions (Denies)

- User denies
  - u-deny(*u*, *opset*, *oset*}). Any process executing on behalf of user *u* cannot perform any operation in *opset* on any object in *oset*.
- Process denies
  - p-deny(*p*, *opset*, *oset*). Process *p* cannot perform any operation in *opset* on any object in *oset*.

Computing an Access Decision

A process access request $\langle op, o \rangle_p$ is granted if and only if there is a PM privilege (*u*, *op*, *o*) where *u* is process *p*'s user, and (*op*, *o*) is not denied to *u* or *p*.

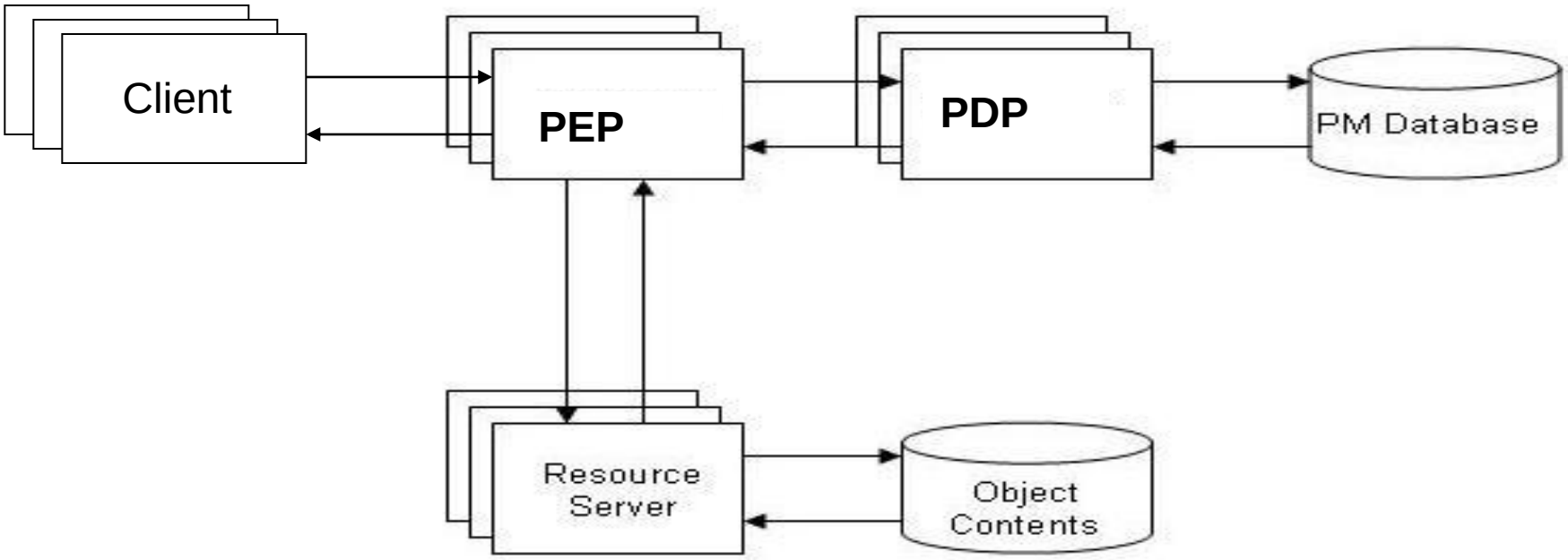
Obligations (Event-Response)

- Format: **when** *event-pattern* **do** *response*
- Event: successful execution of an operation (e.g., reading of an object's content, or creation of a user).
- Event pattern: the context in which an event occurs (operation, object, user, containers, etc.)
- Response: sequence of administrative operations that may dynamically change the configuration of PM relations.
- Example: **when** process reads object from "Top Secret" **do** create p-deny(process, {write}, not "Top Secret").

Policies

- Tailored policies through configuration of relations alone. E.g., Combinations of mission specific forms of:
  - DAC
  - RBAC
  - History and object-based Separation of Duty
  - Workflow
  - Forms of confinement (e.g., only doctors can read medical records, MLS, I know who has access to my data and I can revoke access, only users in *abc* group can read message *xyz*)
  - Chinese wall (conflict of interest)
- Library of configurations and commands exist for immediate instantiation

General Architecture



Conclusion
Native PM advantages

- The PM is a unification framework where data services and access controls operate as one.
- A user authenticates once but may exercise legitimate capabilities over a multitude of data services
- Data services (to include AC as a data service) naturally interplay
- Code normally included in apps for controlling access, sharing and distributing data is displaced by PM configuration– Eliminating some vulnerabilities and making Apps development easier
- Data can’t leak into local environment or to outside world
- Combinations of mandatory, discretionary, and history-based access controls are comprehensively enforced across applications
- Access control policies can be tailored to mission of subscriber
- Library of pre-existing configurations

Research Challenges in Tailored Trustworthy Spaces

Dr. Sam Weber

Trustworthy Computing Program, NSF

What is Trustworthy Computing?

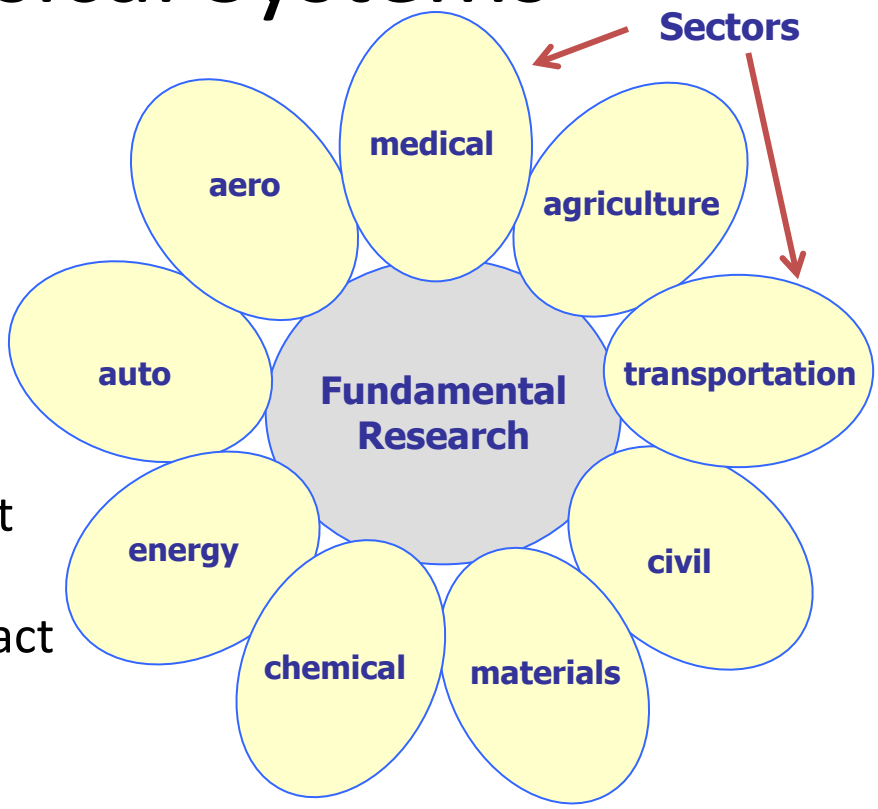
(from FY11 solicitation)

- "Envisions a future pervasive cyber infrastructure that supports a wide range of requirements for trustworthy operation, despite known and future threats and an increasingly complex operating environment. Trustworthy operation requires security, reliability, privacy, and usability. "
- Supports approaches from theoretical to experimental to human centric
- Theories, models, cryptography, algorithms, methods, architectures, languages, tools, systems, and evaluation frameworks
- Studies of tradeoffs among security, privacy, usability
- Methods to assess, reason about, and predict system trustworthiness
- Methods to increase attacker cost, **enable tailored security environments**, and incentivize security deployment, socially responsible behavior, and deter cyber crimes
- Multi-disciplinary work incorporating legal, social, and ethical implications strongly encouraged

- Small / Medium / Large (to $500K / $1.2M / $3M) awards totaling $55M

Cyber-Physical Systems

- Cyber-Physical Systems
  - deeply integrate **computation, communication, and control** into **physical** systems
  - exploit pervasive, networked computation, sensing, and control
- "CPS will transform how we interact with the physical world just like the Internet transformed how we interact with one another."
- **CPS Solicitation (NSF 11-516)**
  - Abstracting from sectors to more general principles
  - Apply these to problems in new sectors



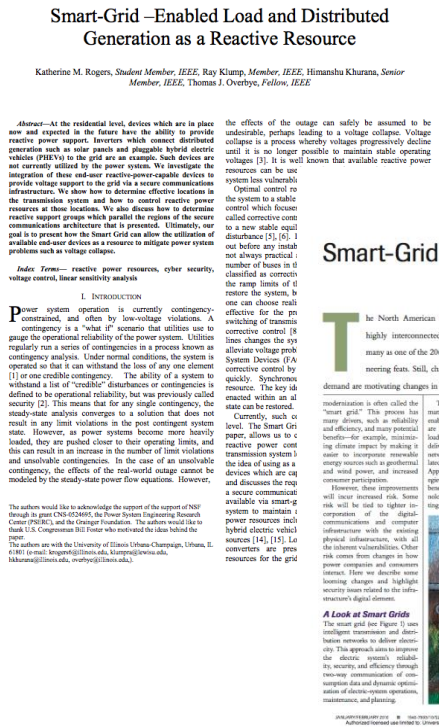
•CPS Summit Website: http://varma.ece.cmu.edu/summit/index.html

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

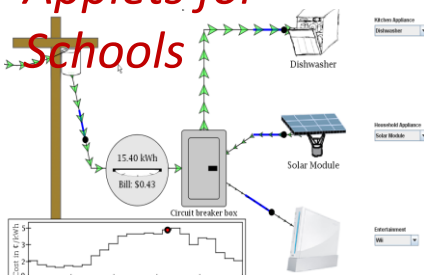
Katherine M. Rogers, *Student Member, IEEE*, Ray Klump, *Member, IEEE*, Himanshu Khurana, *Senior Member, IEEE*, Thomas J. Overbye, *Fellow, IEEE*

Building Security In

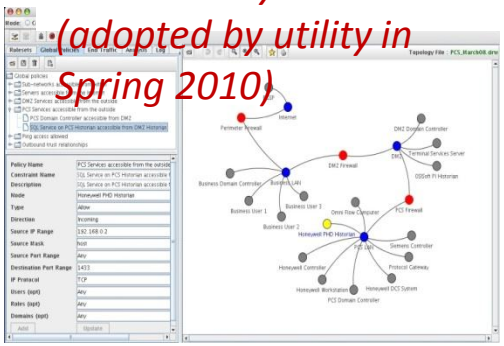
Editors: John Steven, jsteven@cigital.com
Gunnar Peterson, gunnar@arctecgroup.net
Deborah A. Frincke, deborah.frincke@pnl.gov

Smart-Grid Security Issues

Applets for Schools



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

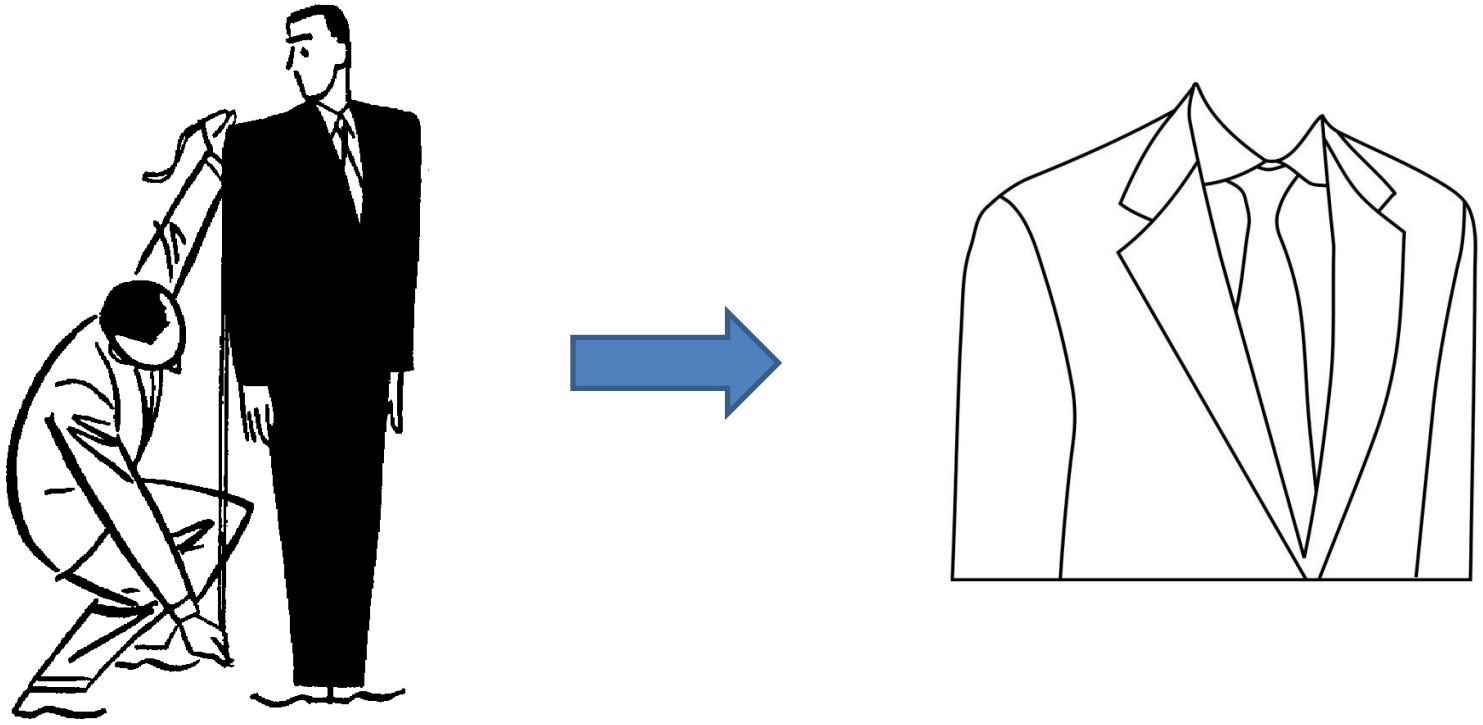


- Funding started with NSF, transferred to DOE and DHS
- Facilities
- Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

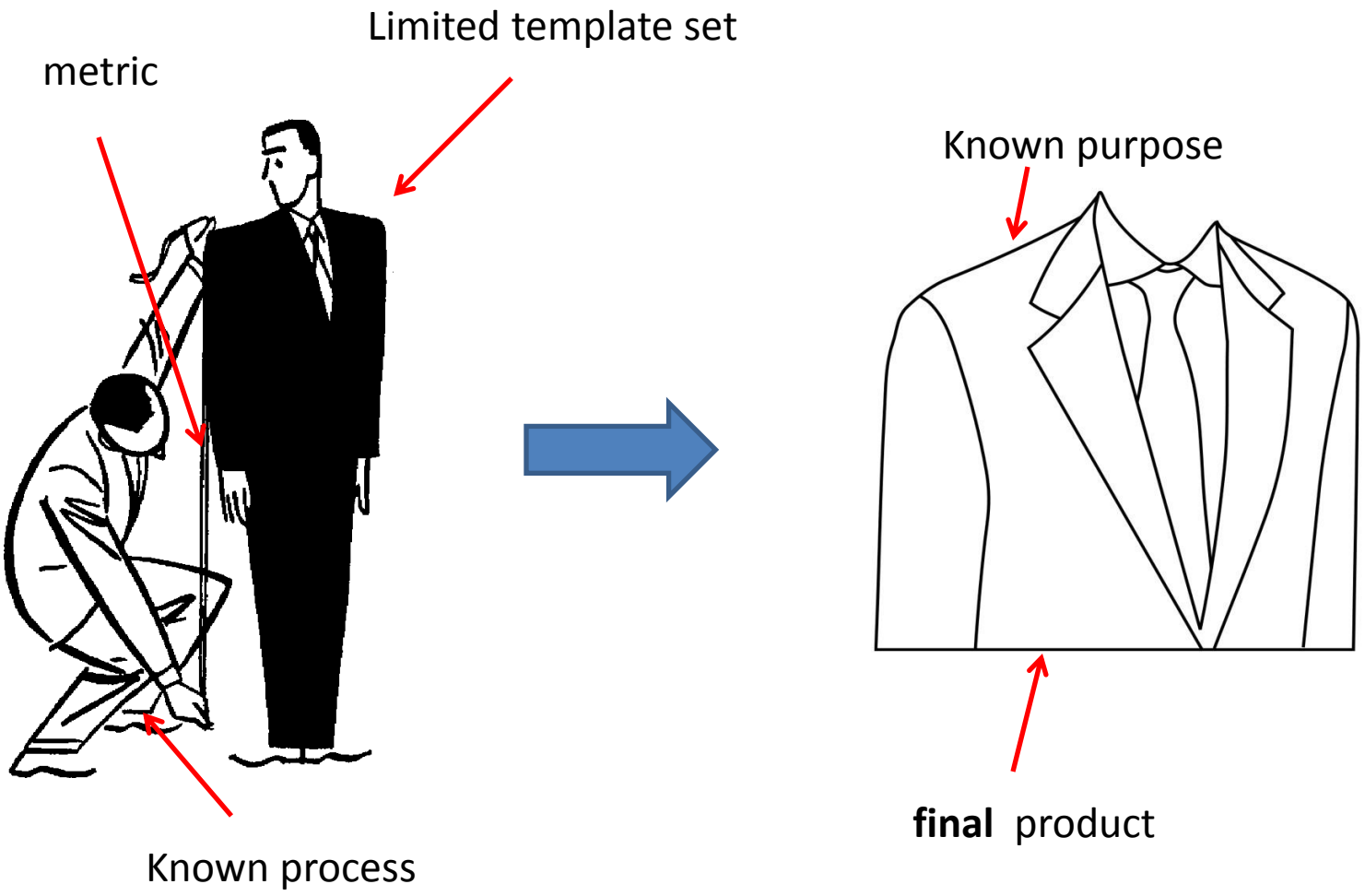
Game-changing R&D Needed to Make *Survivable* Systems a Reality

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

Tailored Trustworthy Spaces



Tailored Trustworthy Spaces

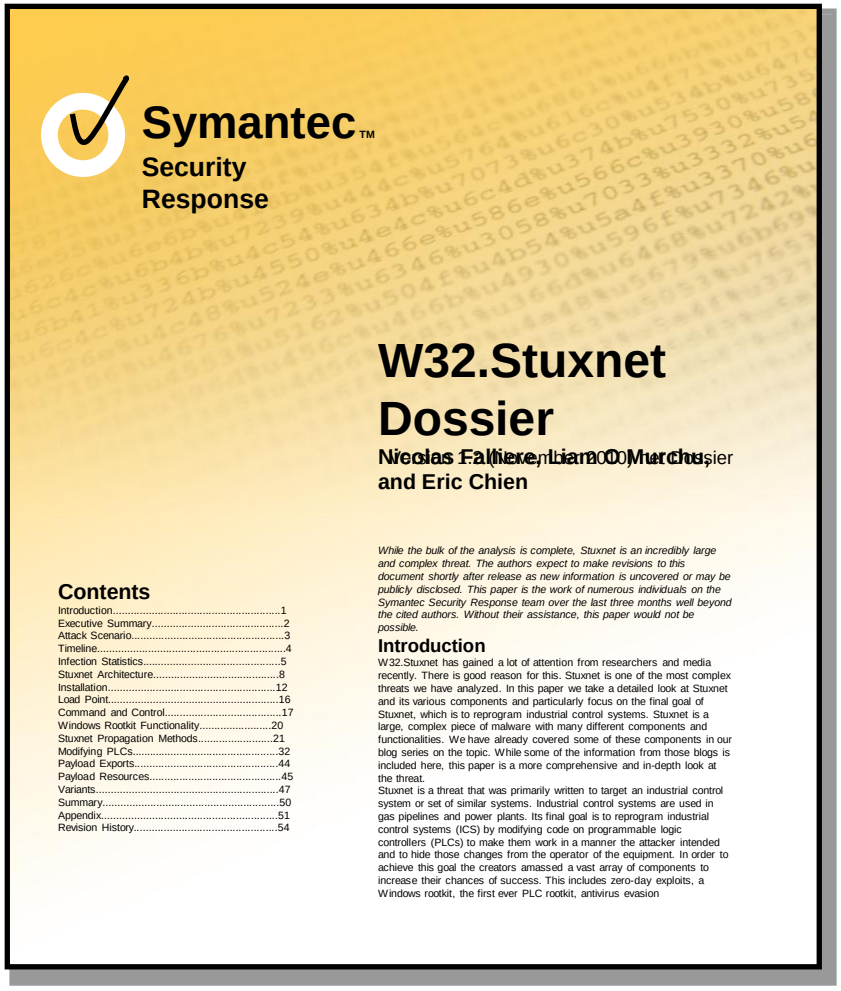


Metrics?

- What are principles, resources? Does "ownership" exist?
  - Eg. health care records
  - Eg. pacemakers
  - Eg. privacy implications of power usage
  - Eg. does anyone know actual policy?

Stuxnet

- Preliminary version seen June 2009
- Final version June 2010
- Reverse engineered, exposing sophisticated attack on Siemens S7 controllers (presumably of Iranian centrifuges), August – November 2010
- Exploits 4 zero-days, jumps airgap via USB
- Ralph Langner, Langner Communications:
  - “Even though Stuxnet … is not a generic attack, several parts of [it] are generic, and … these are easy to copy.”
  - “Once .. these generic attack techniques are implemented in exploit tools… all bets are off. Mitigation of any of these exploits is very difficult”



Symantec™
Security
Response

W32.Stuxnet Dossier

Nicolas Falliere, Liam O Murchu, and Eric Chien

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.

Contents

Introduction....1
Executive Summary....2
Attack Scenario....3
Timeline....4
Infection Statistics....5
Stuxnet Architecture....8
Installation....12
Load Point....16
Command and Control....17
Windows Rootkit Functionality....20
Stuxnet Propagation Methods....21
Modifying PLCs....32
Payload Exports....44
Payload Resources....45
Variants....47
Summary....50
Appendix....51
Revision History....54

Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our blog series on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion

http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html?page=full

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?ref=stuxnet

Meaning of “Trustworthy”?

- Realistic threat models?
  - Car tuners, thieves, blackmailers, terrorists
- Security vs safety
- How to respond to threat?
  - Nuclear power plant not like airplane or car

Tailored System?

- Systems continually in flux
  - How does new state compare to old? Have assumptions been violated?
- Systems involve humans
  - "Nudging users towards privacy" (Acquisti et al)
  - Implications of incentives?
- Supply chain variations

“Fabric”

- Secure control systems
  - See TRUST center
  - Resonance effects
- How to sandbox code with different environmental assumptions?

Summary

- Tailoring for amoebas
- See NSF active awards:

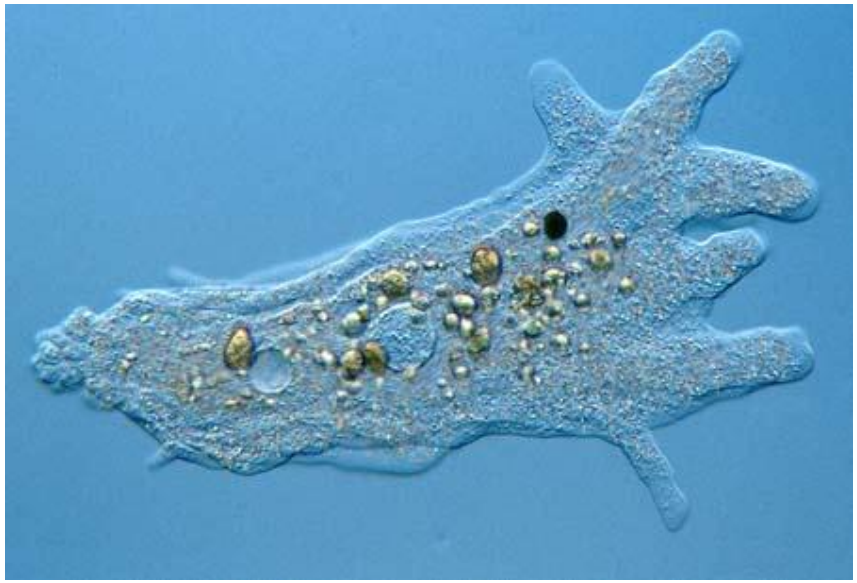
www.nsf.gov/awardsearch

Many search options available

Trustworthy Computing = Prog. Element 7795

Cyber-Physical Systems = Prog. Element 7918

Results include abstract of award and PI-email



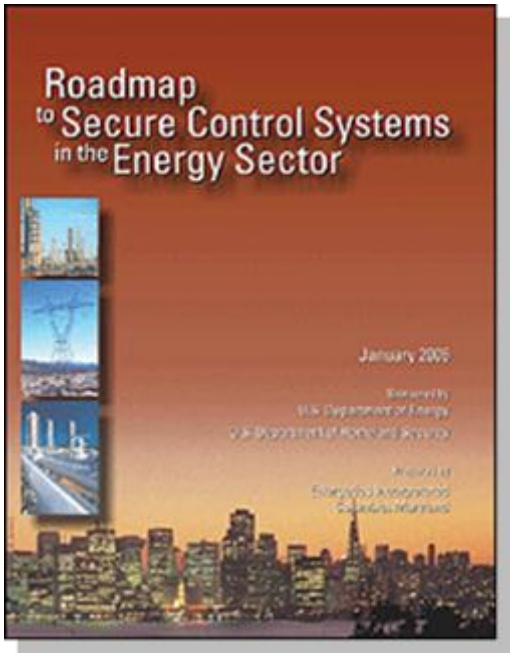
U.S. Department of Energy

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

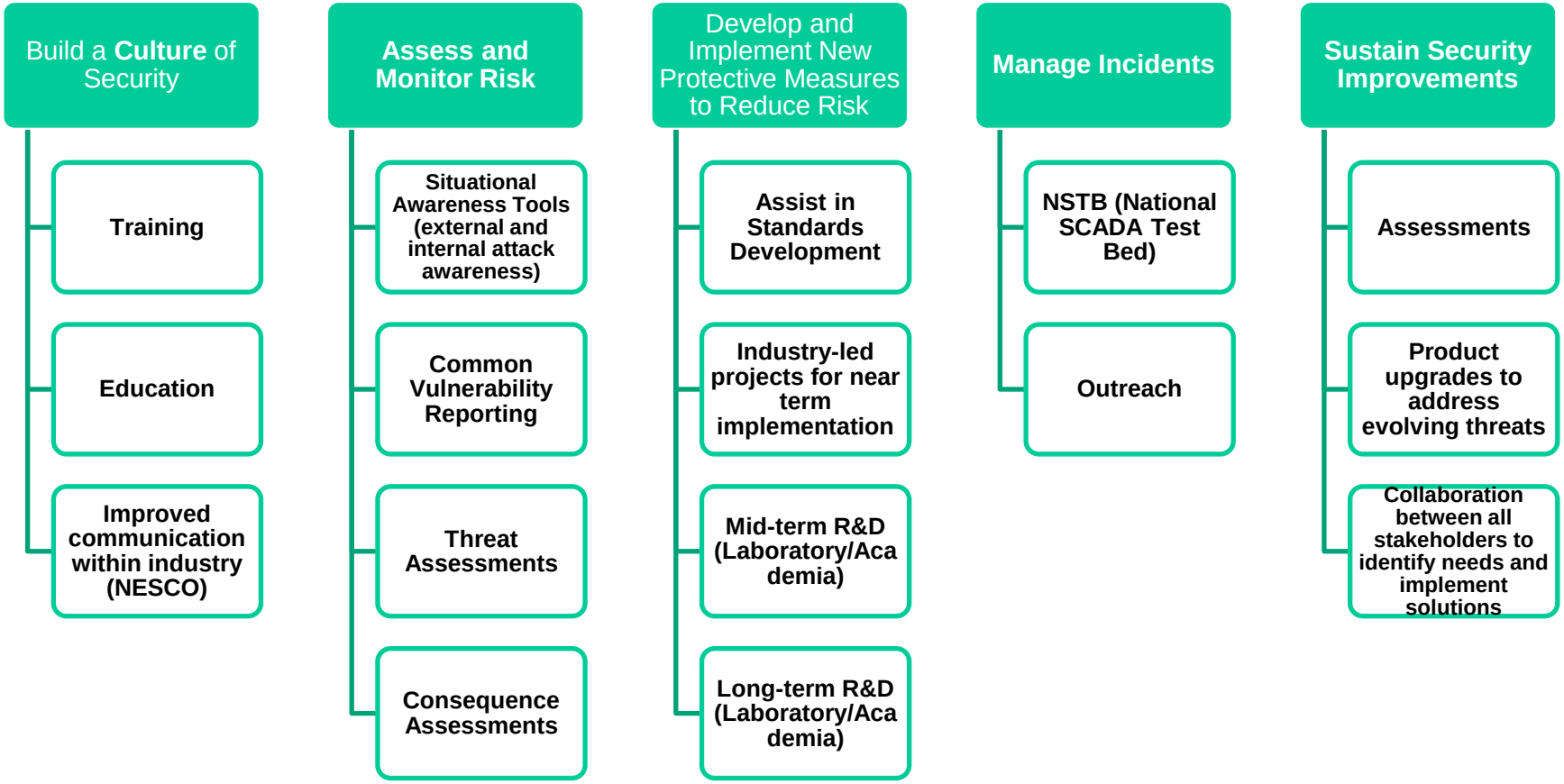


- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in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

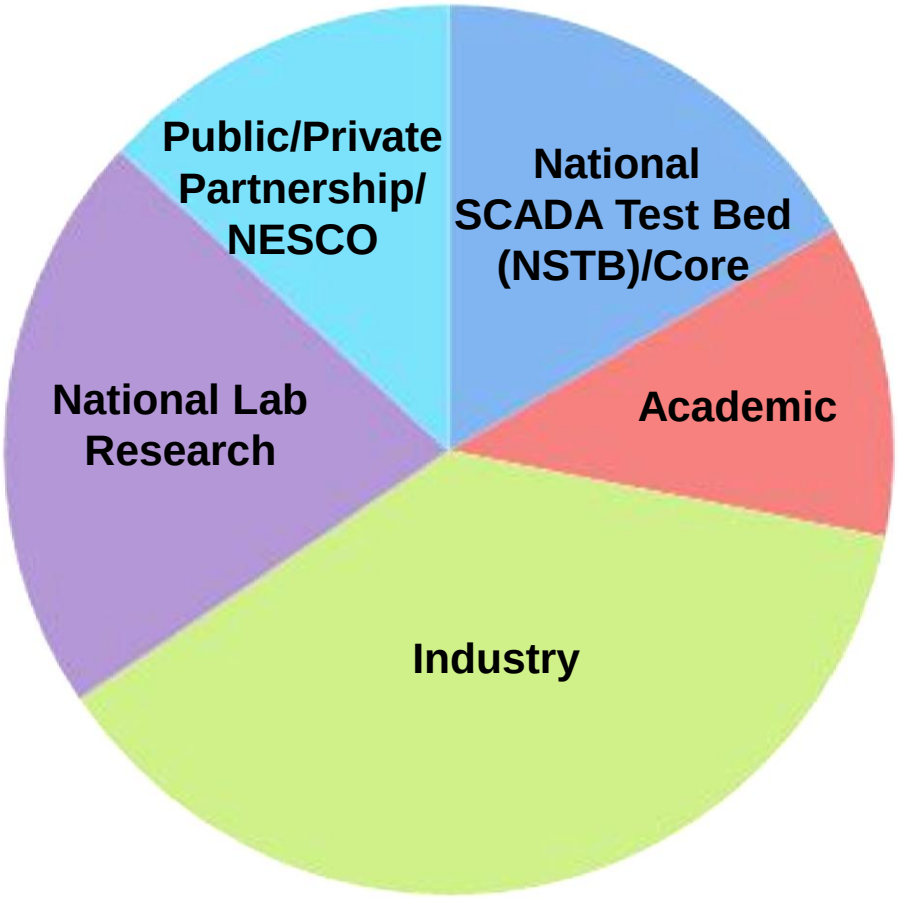
Roadmap Vision

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



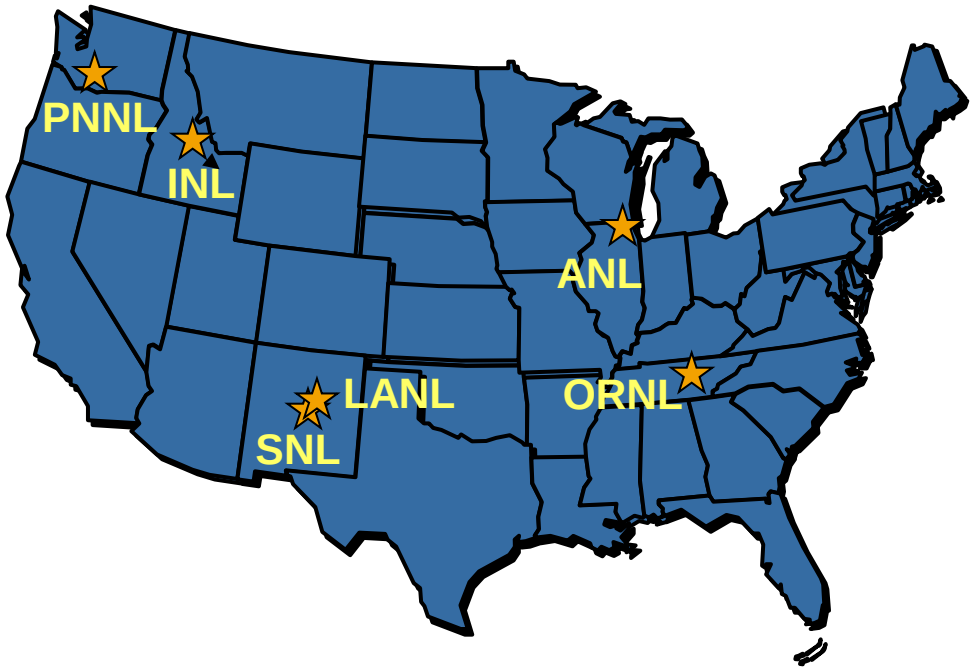
Cybersecurity for Energy Delivery Systems (CEDS) Program—5 Key Areas



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

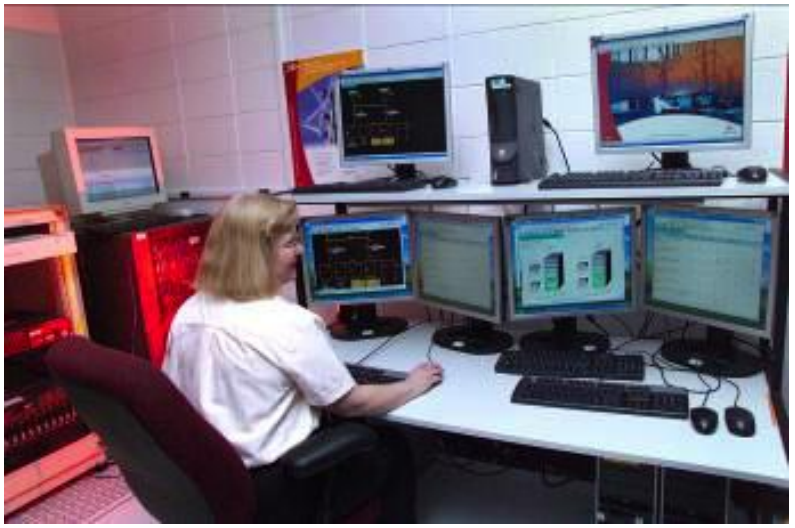
OAK RIDGE Cyber Security Program
- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

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:

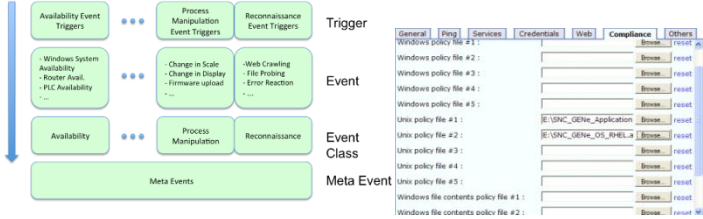
- CenterPoint Energy
- Pacific Northwest National Laboratories (PNNL)
- "Early Adopters"

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

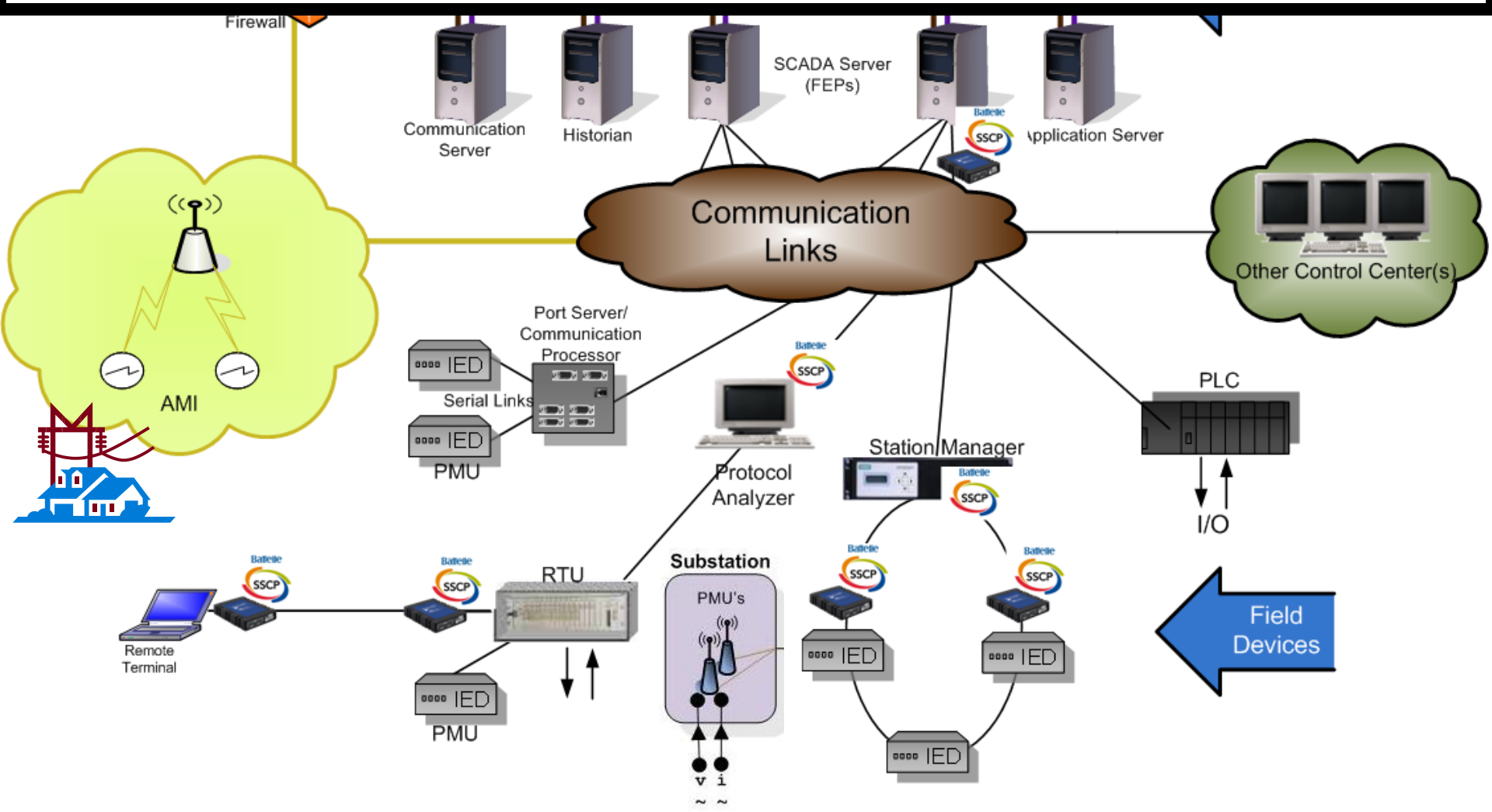
Participants:

- 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)

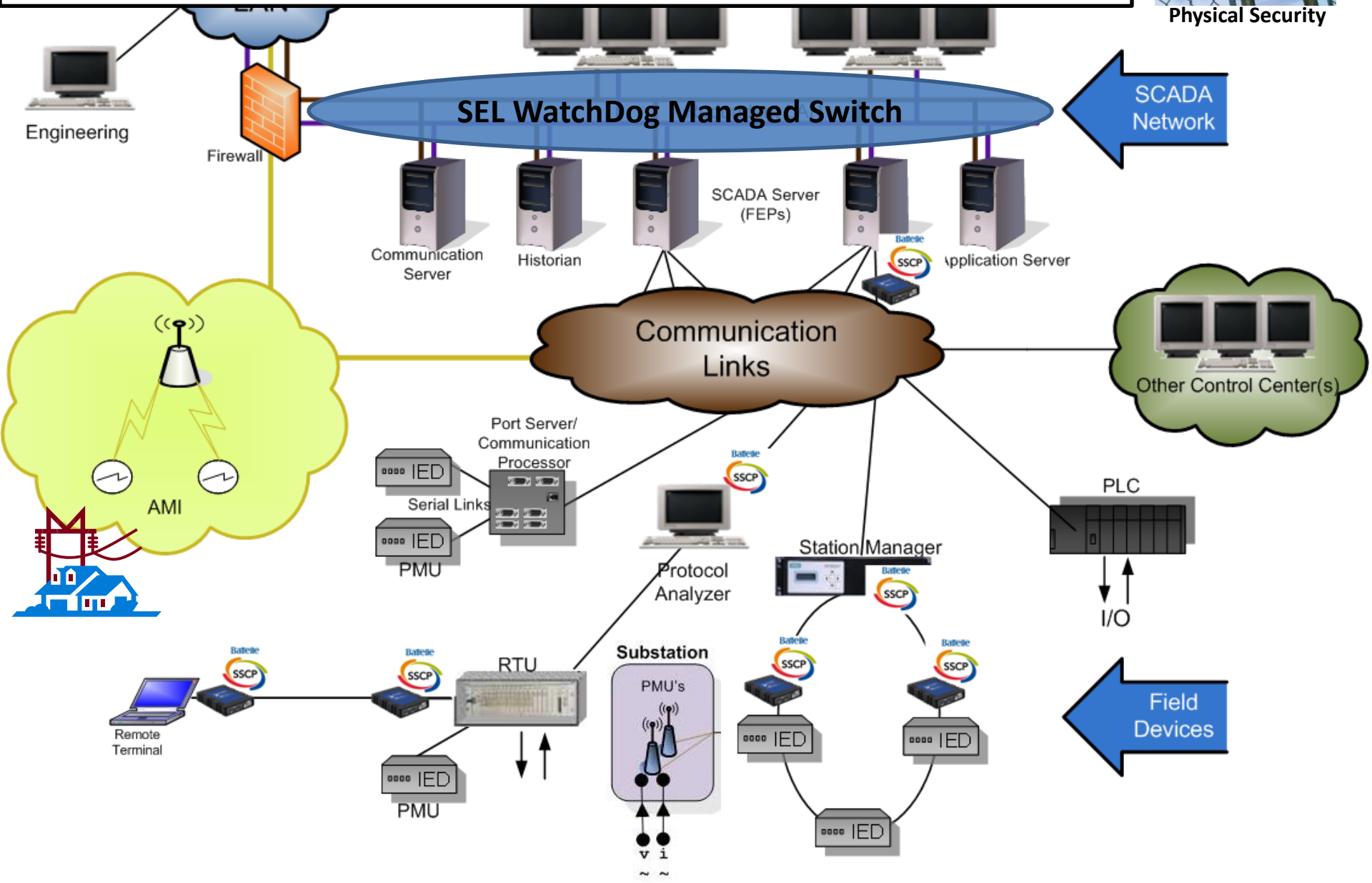
The 2010 DOE Cybersecurity for Energy Delivery Systems Program
Industry-Led
&
National Laboratory-led Projects



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)

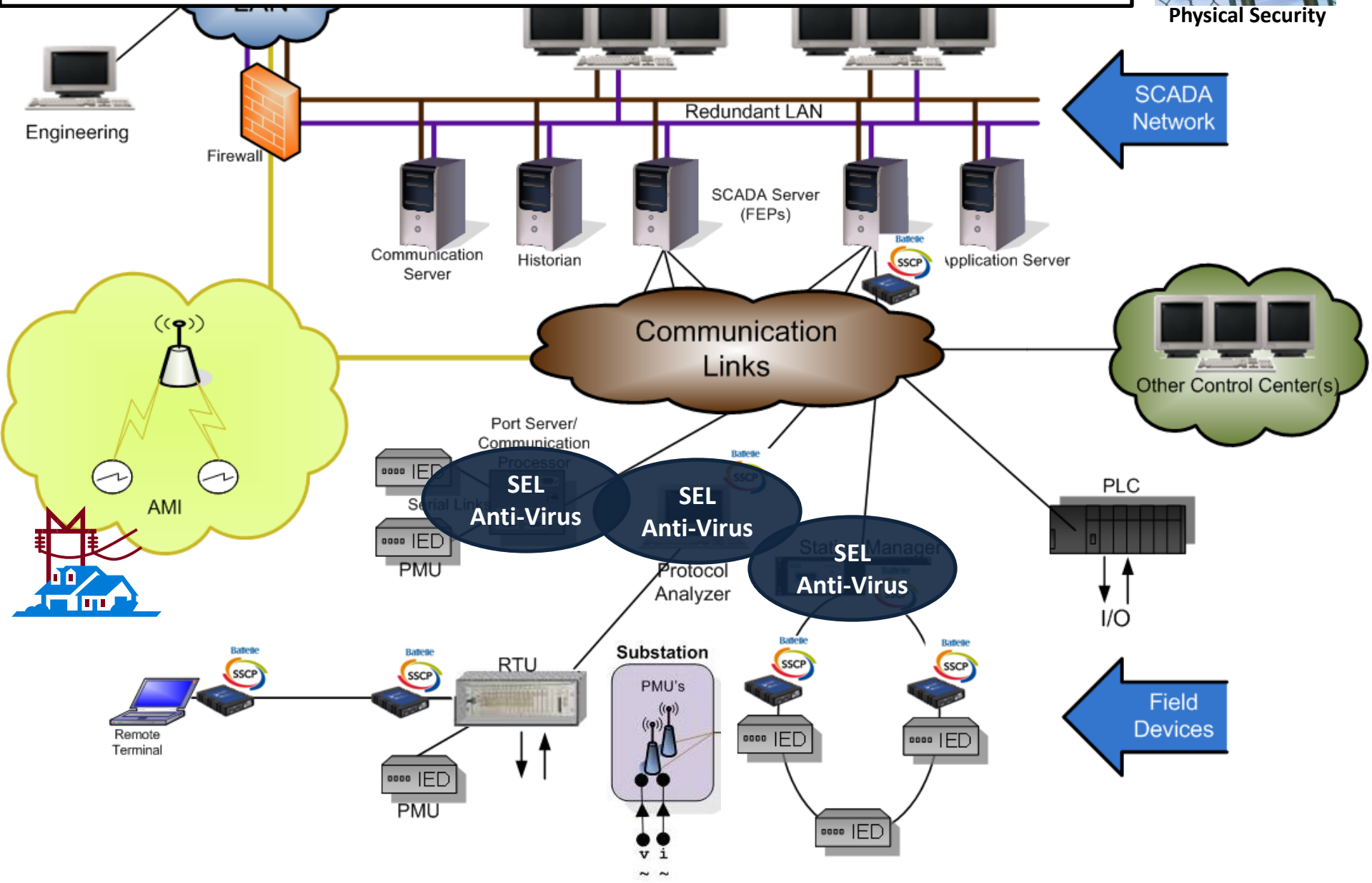
Physical Security



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

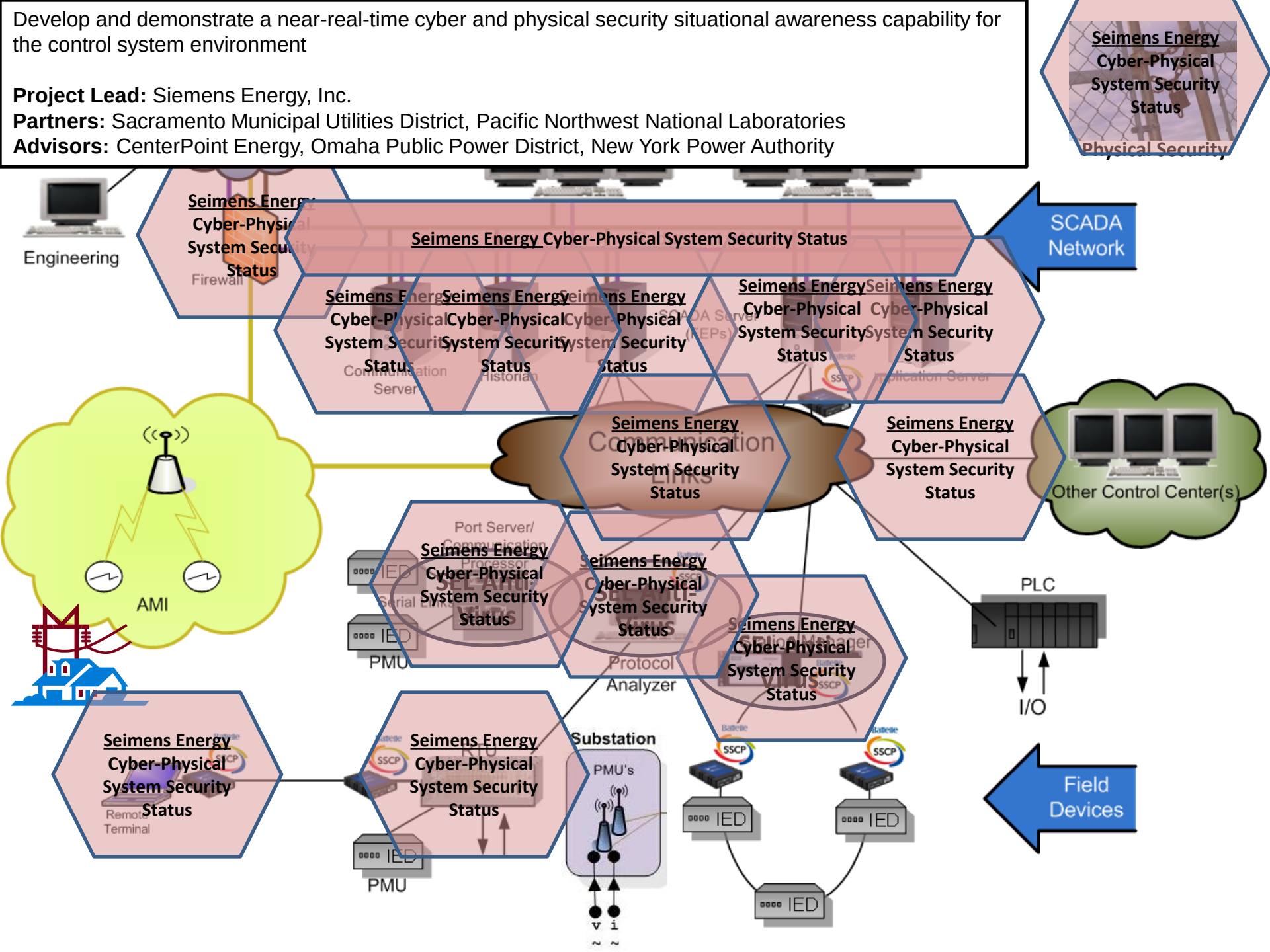
Project Lead: Schweitzer Engineering Laboratories (SEL)
Partners: Dominion Virginia Power (DVP), Sandia National Laboratories (SNL)

Physical Security



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

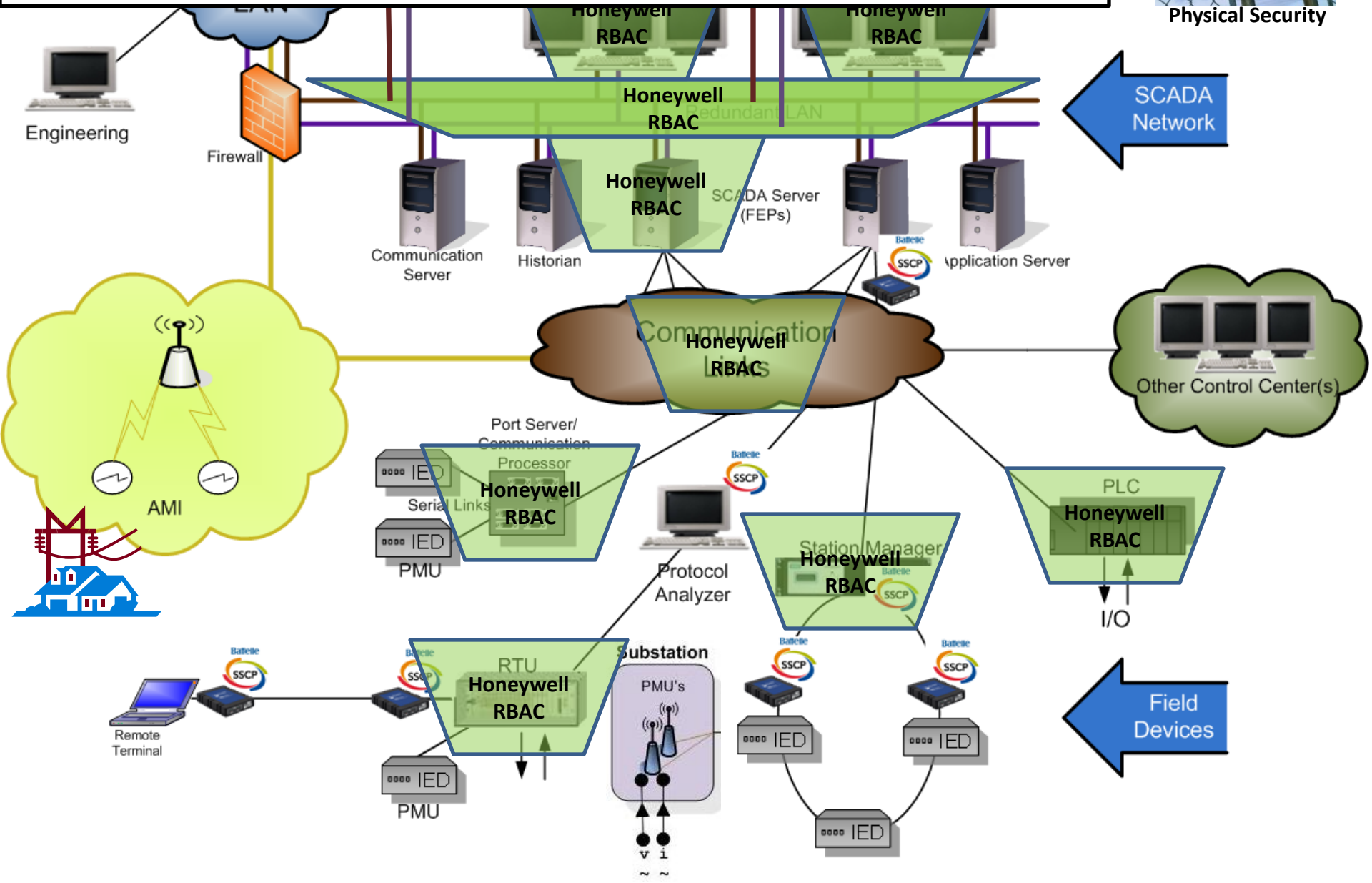
Project Lead: Siemens Energy, Inc.
Partners: Sacramento Municipal Utilities District, Pacific Northwest National Laboratories
Advisors: CenterPoint Energy, Omaha Public Power District, New York Power Authority



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

Engineering

Firewall

Redundant LAN

SCADA Network

Communication Server

Historian

SCADA Server (FEPs)

Application Server

Telcordia
Cybersecurity for Energy Delivery Systems Communication Protocols

Inter-Control Center Communications (IEC 60870-6 / TASE .2)

Other Control Center(s)

Advanced Metering Infrastructure (AMI) (C12.22)

Substation Automation/Distribution Automation
Distributed Energy Resources/Hydro-Generation
SCADA to field devices
(IEC 61850)
Substation and feeder device automation
(DNP3)
Security for protocols/networks/RBAC
(IEC 62351 Parts 1-8)

IED

PMU

PLC

I/O

Remote Terminal

RTU

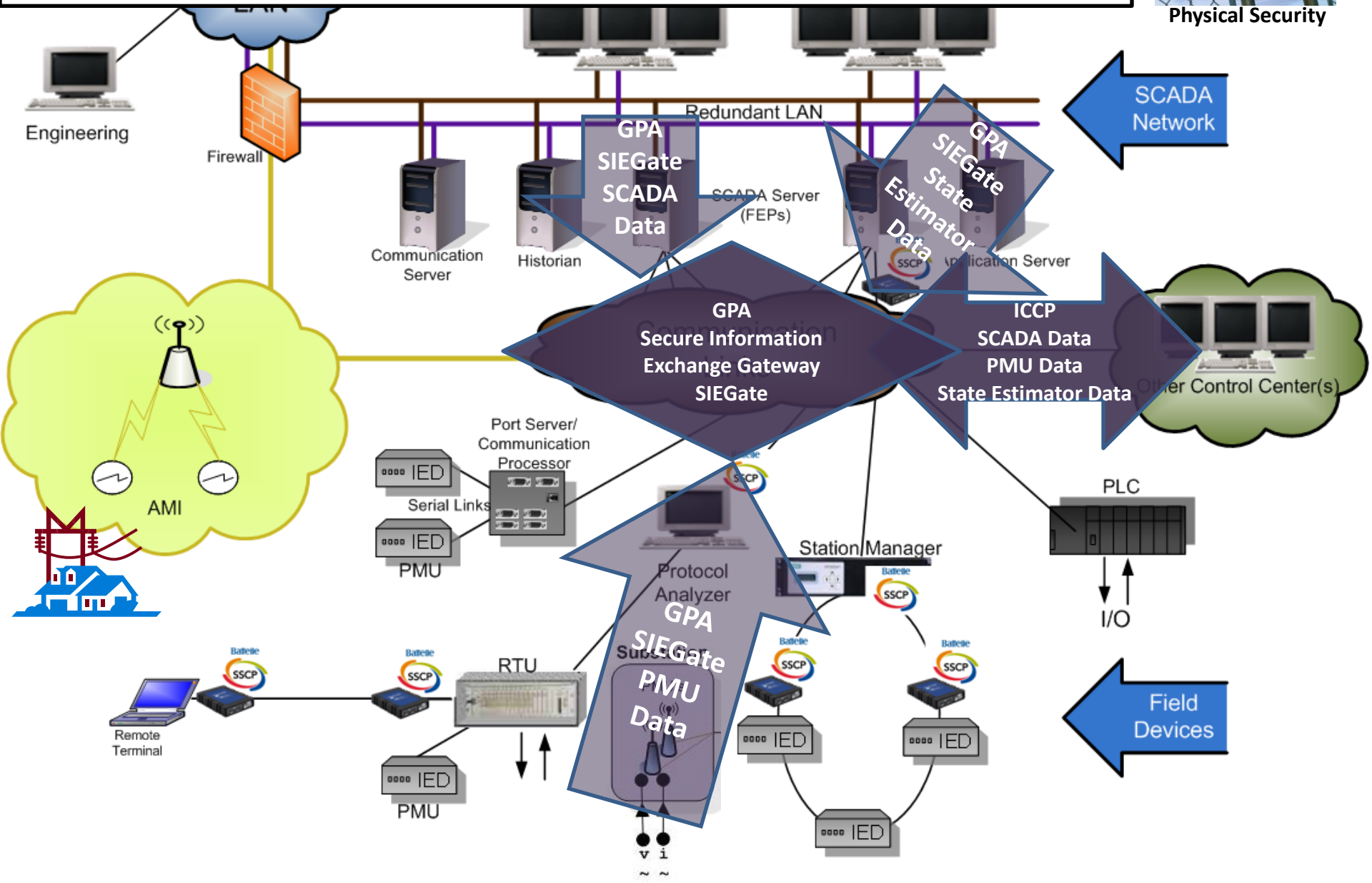
Phasor Measurement Unit
PMU Data
(IEEE C37.118)

Field Devices

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

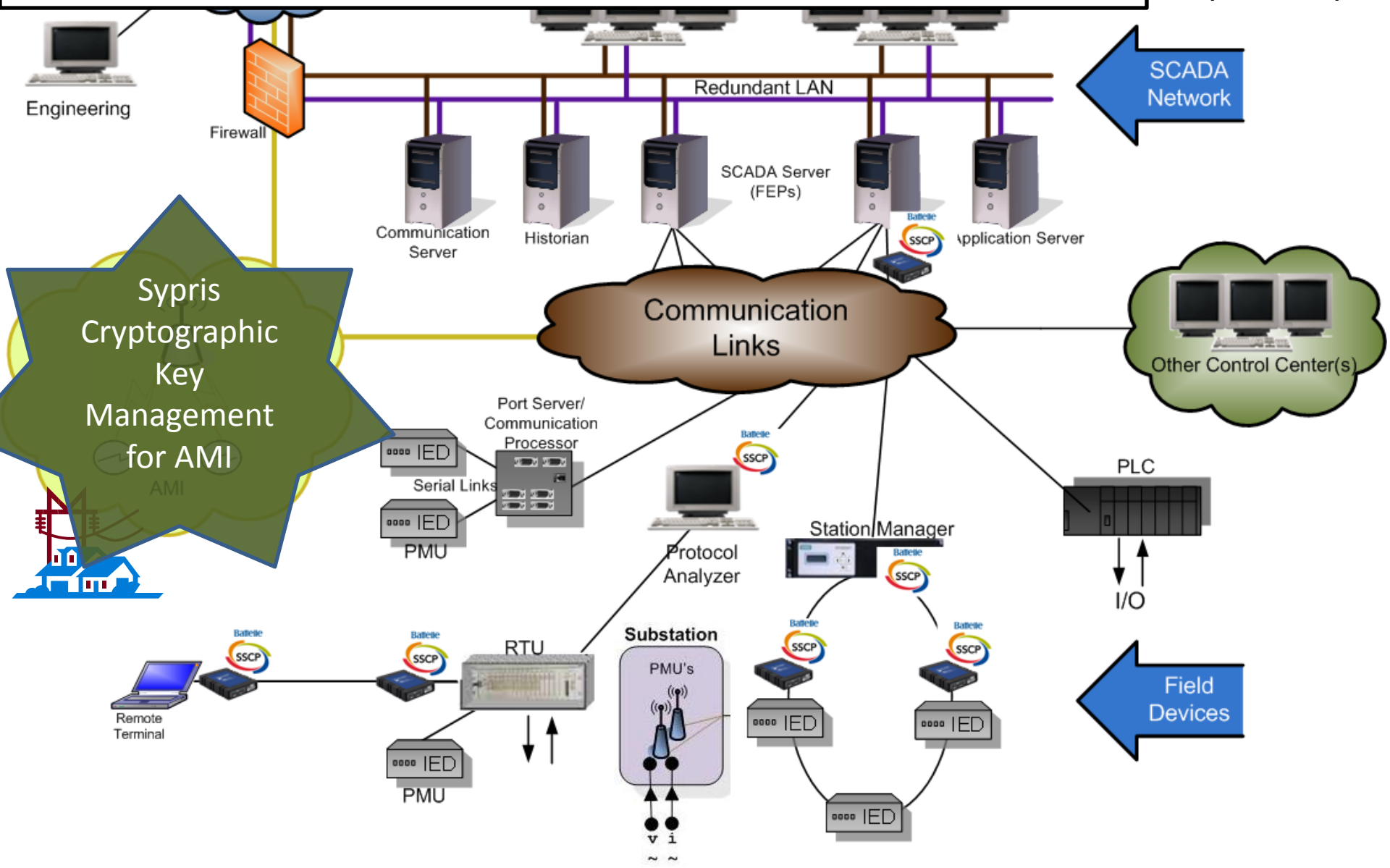

Physical Security



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



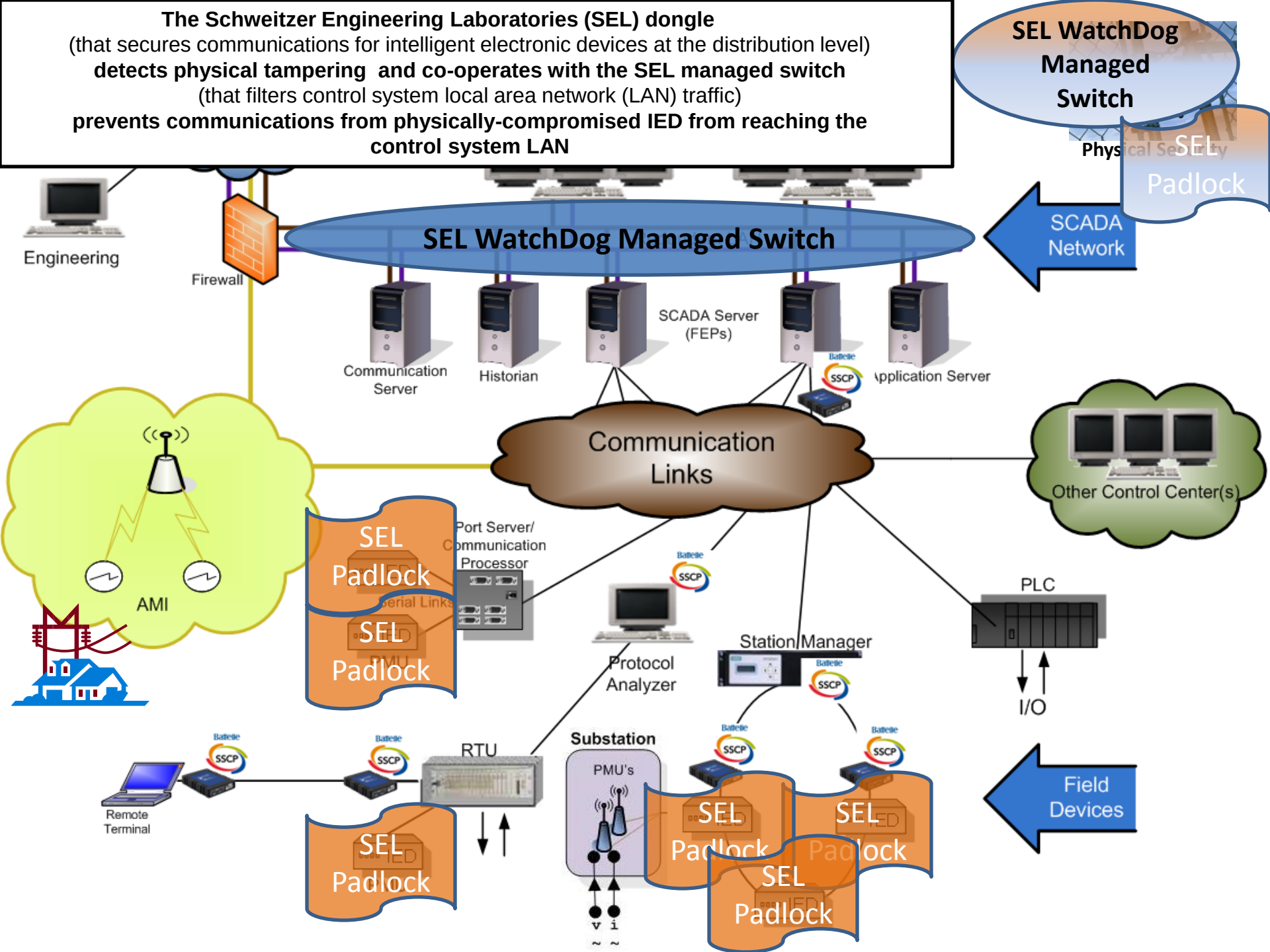
Research, develop and commercialize a low-power, small-size dongle that provides strong authentication, logging, alarming and secure communications for intelligent field devices operating at the distribution level

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

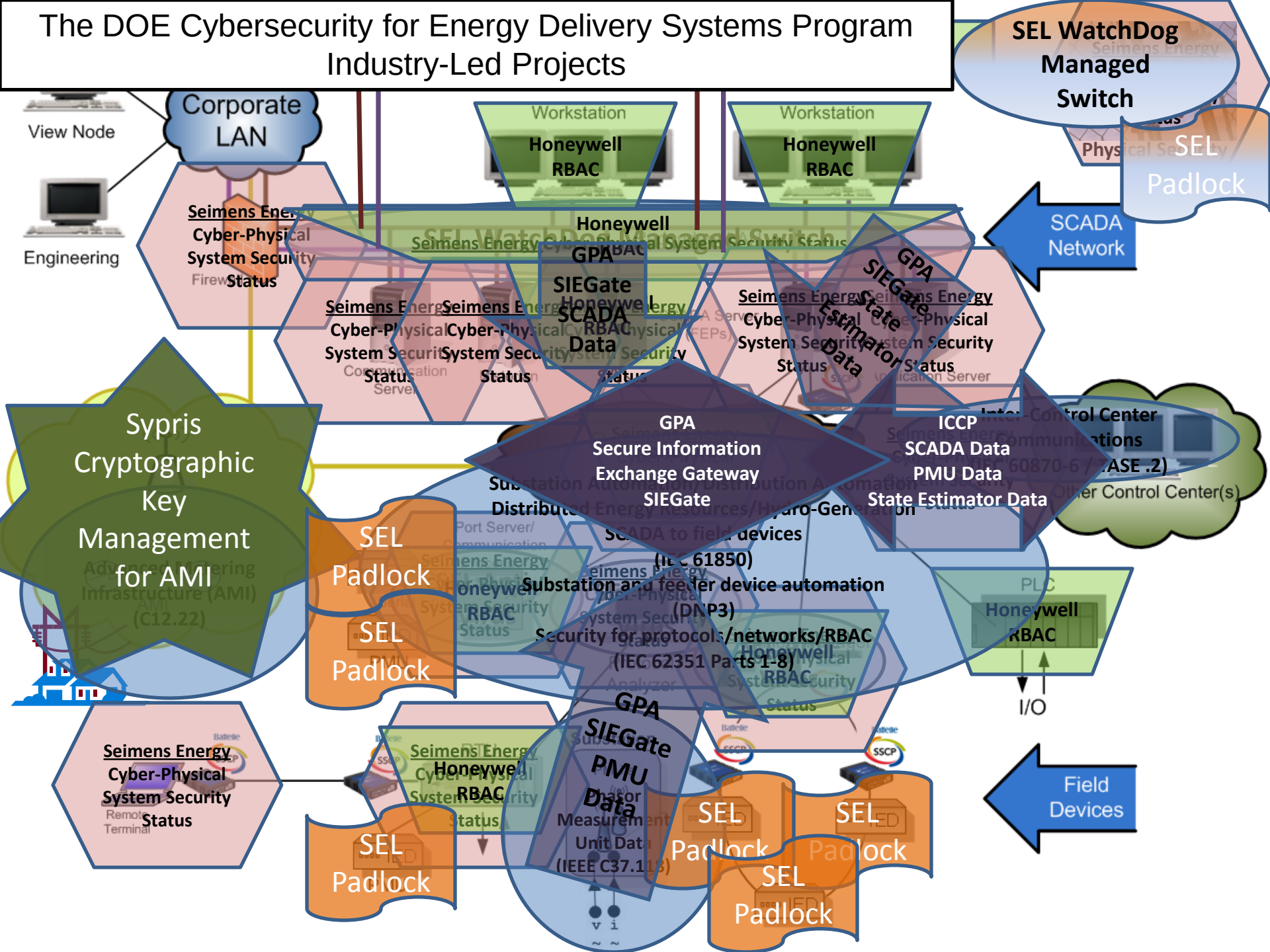
Physical Security

Engineering
Firewall
Redundant LAN
SCADA Network
Communication Server
Historian
SCADA Server (FEPs)
Application Server
Communication Links
Other Control Center(s)
AMI
SEL Padlock
SEL Padlock
Port Server/ Communication Processor
Protocol Analyzer
Station Manager
PLC
I/O
RTU
Substation
PMU's
SEL Padlock
SEL Padlock
SEL Padlock
Remote Terminal
Field Devices

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

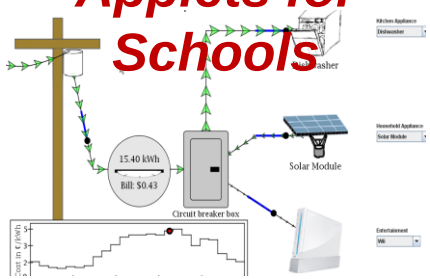
Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

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

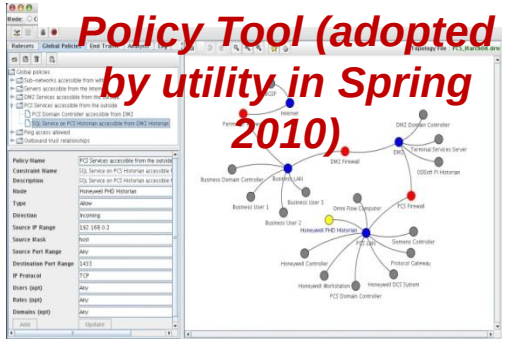
Building Security In

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)

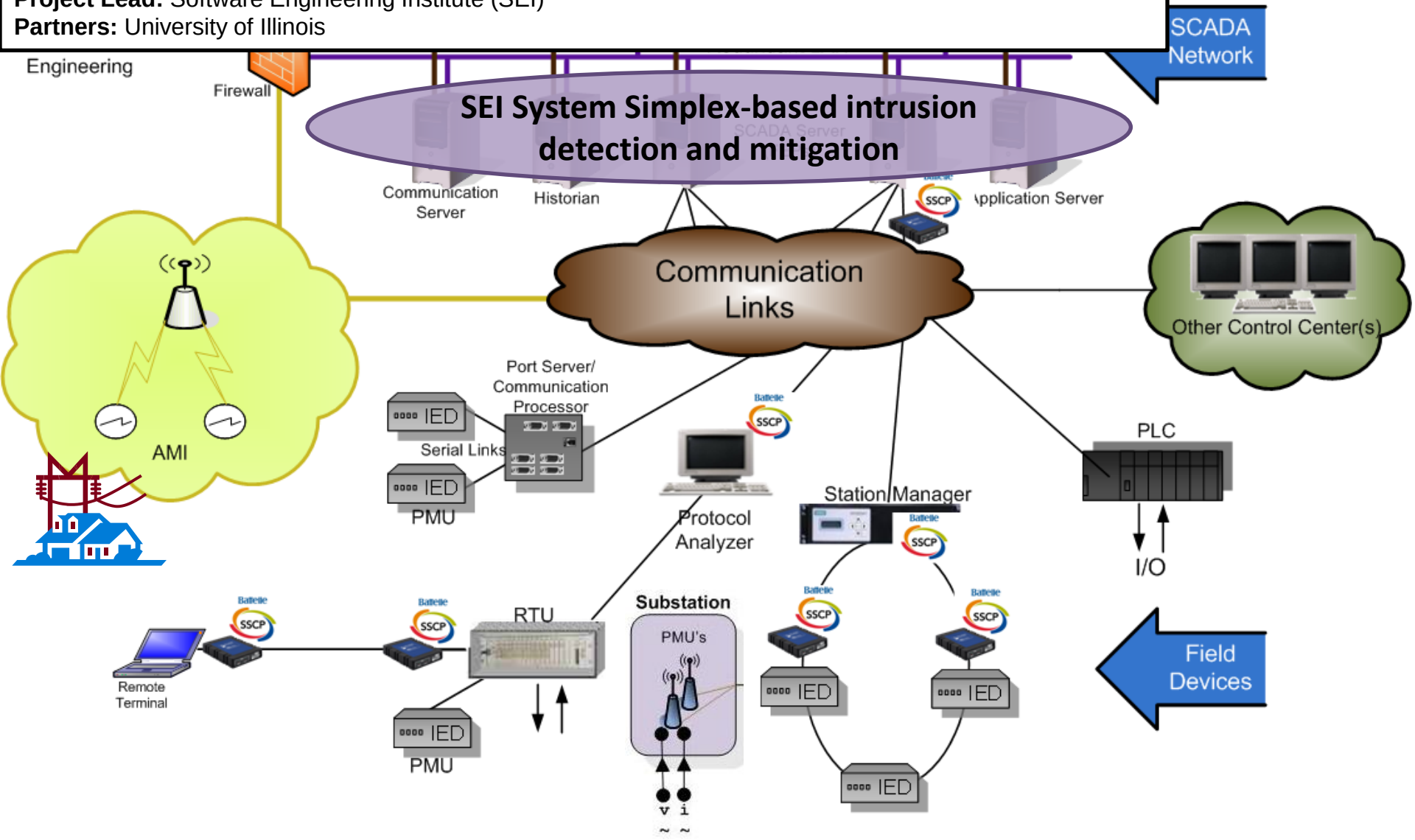
- Investigating techniques that diminish the impact of using encrypted communication in tightly time-constrained reactive system components by exploiting hidden slack and using efficient encryption techniques.

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

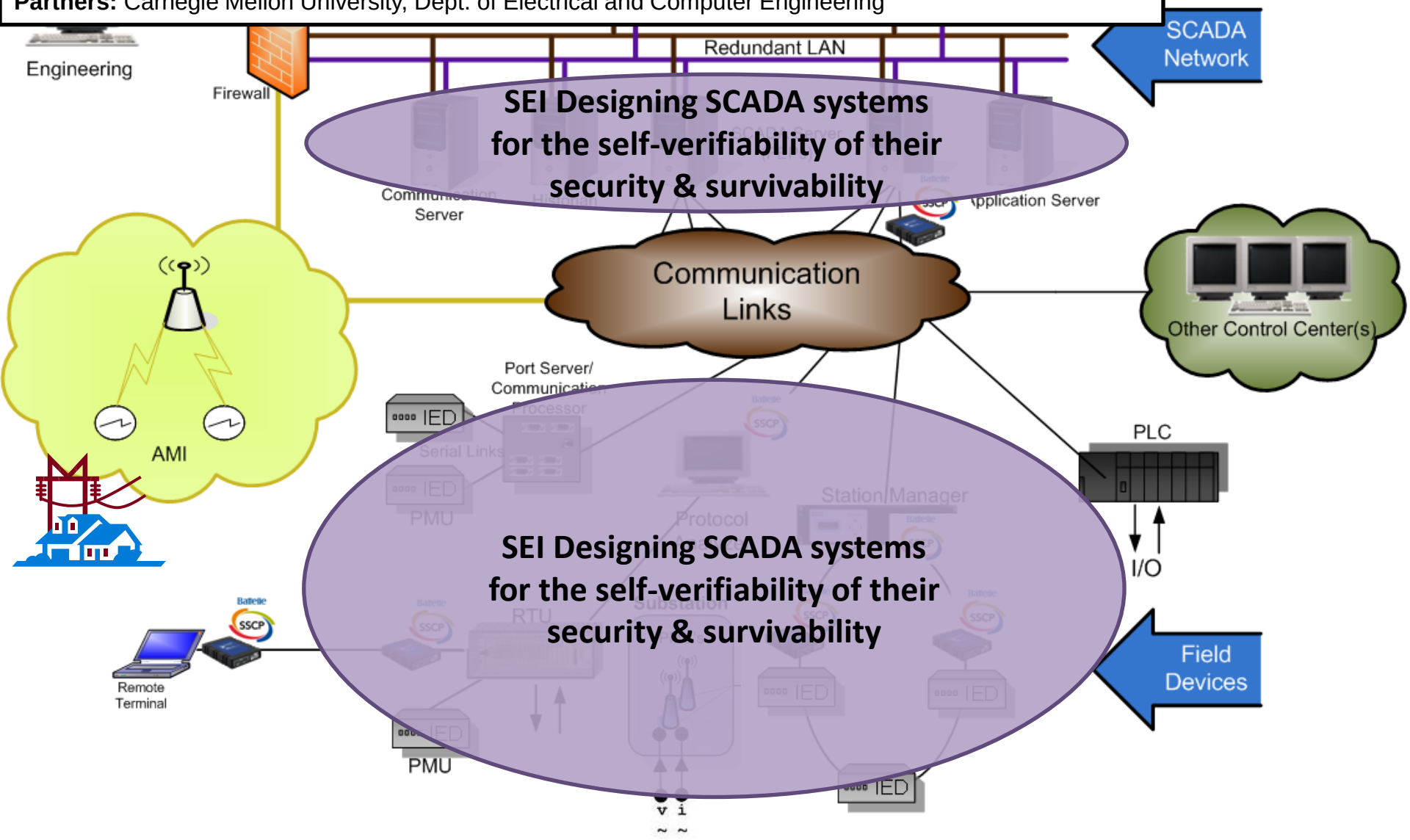


Perform decentralized, network-based distributed information fusion to identify and isolate subverted SCADA system components, using

- 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

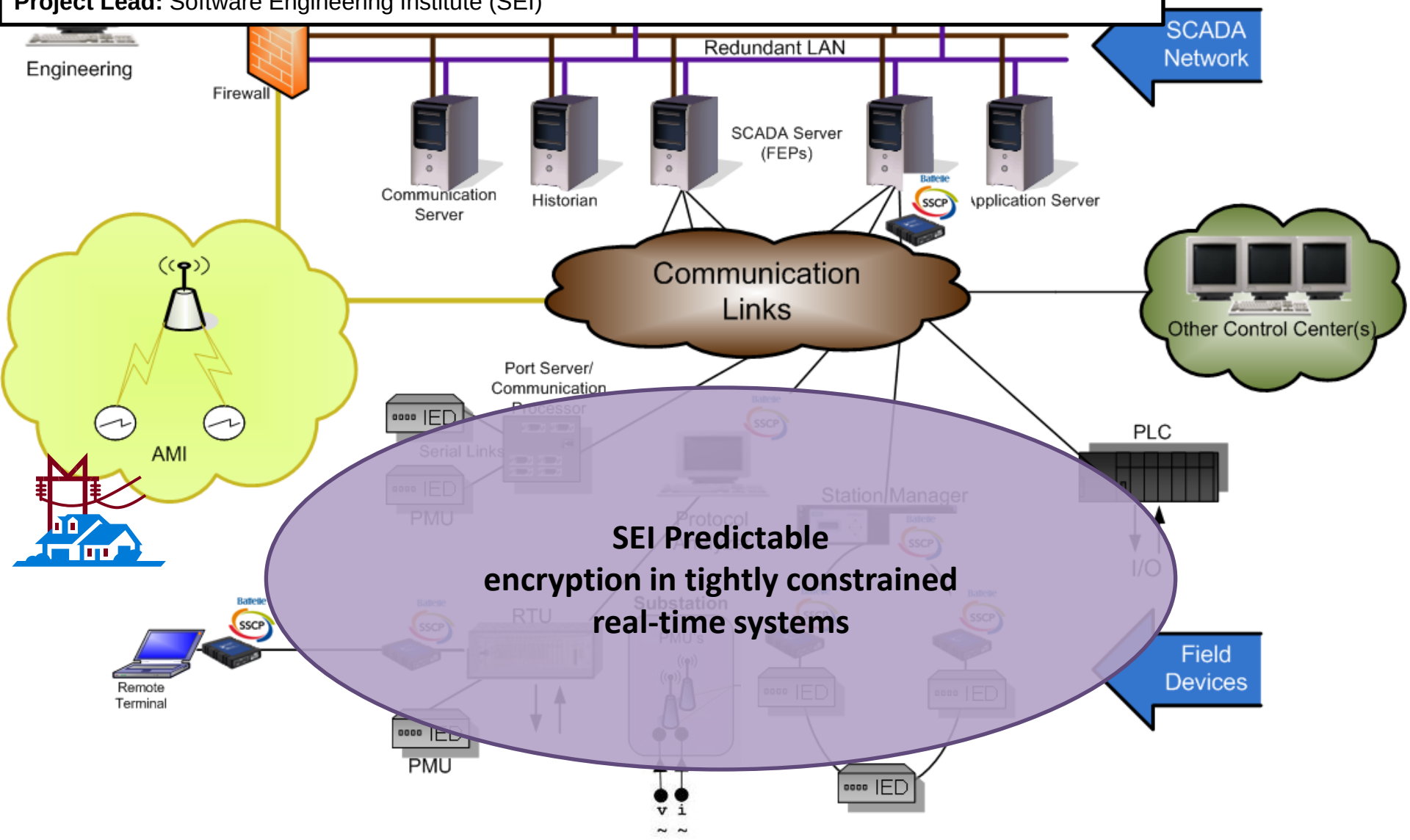


Develop techniques to diminish the impact of the using encrypted communication in tightly time-constrained reactive system components by

- 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



CEDS 2010 Research Call National Laboratory-Led Projects

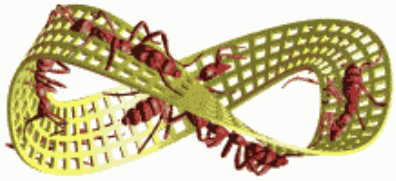
- High-Level (4th Gen) Language Microcontroller Implementation
  - Limits direct access to device memory
  - Hardens microcontrollers against low-level cyber-attacks (such as buffer overflow)
  - Develop standardized security library to implement secure authentication and data encryption down to the 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

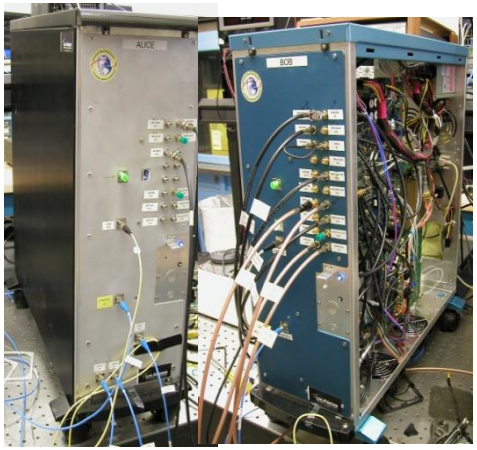
    Draws attention to anomalous conditions--potentially indicative of a cyber-incident



    - **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

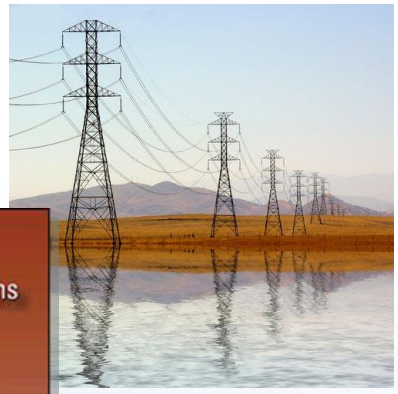
- Goals:
  - Provide hardware for data protection tests
  - Test the ability of a QC system to protect realistic data volume/bandwidth without increasing latency or error rate
  - Increase data integrity and authentication
  - Analyze denial-of-service resistance and protection switching capability

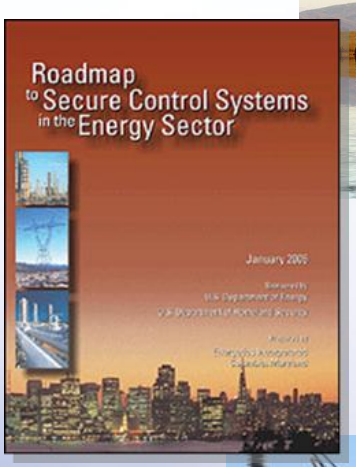
Jane E. Nordholt
Los Alamos National Laboratory
P-21, M/S D434
JNordholt@LANL.gov
505-667-3807

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:

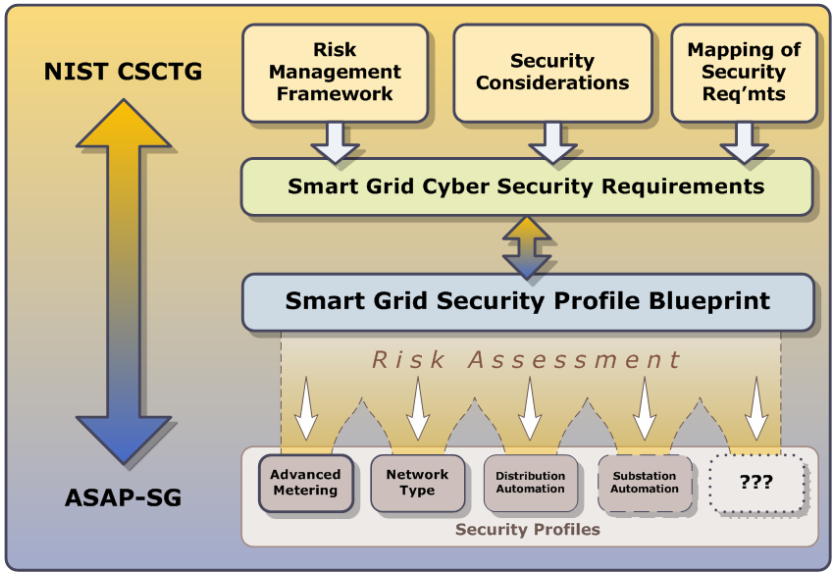
- **Comprehensive implementation plan for quantum approaches to electric grid security.**
- **Quantum technologies developed explicitly for electric grid implementation.**

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

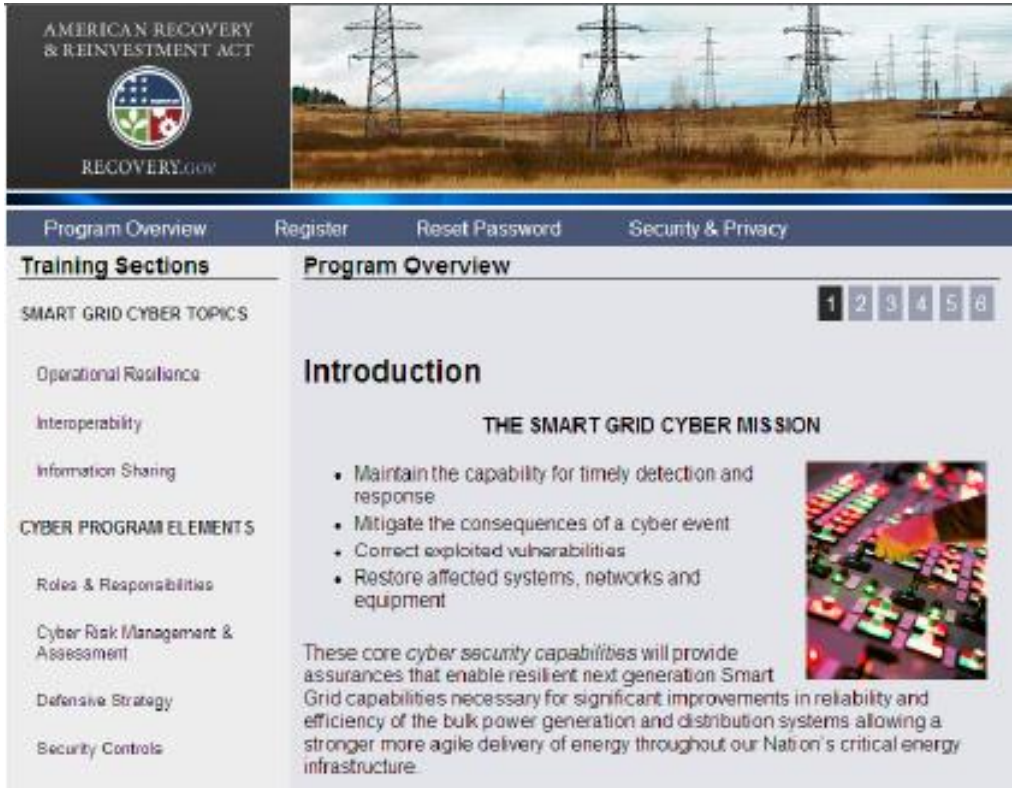


Cybersecurity - *Critical to Smart Grid Success*

- 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 …

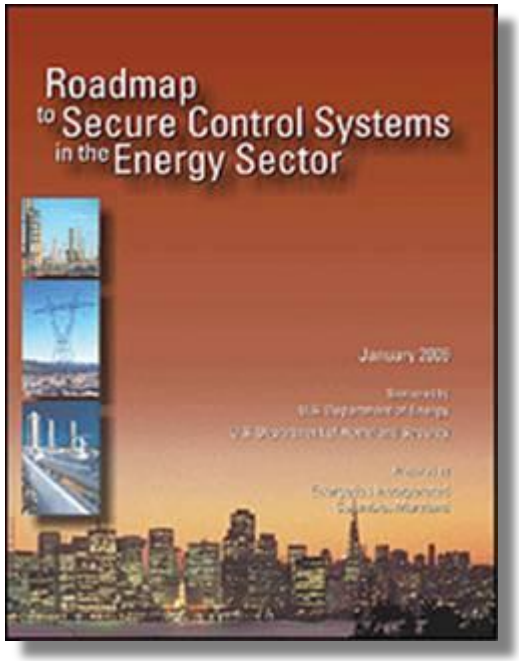
ie Roadmap

interactive energy Roadmap to secure control systems

Visit:

www.oe.energy.gov/controlsecurity.htm

www.controlsystemsroadmap.net



TCIPG Highlights

Bill Sanders
on behalf of the TCIPG Team

July 20, 2011

NITRD TTS: Solutions for Smart Grid Workshop

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

Smart Grid Security Efforts @ Illinois

TCIPG: Trustworthy Cyber Infrastructure for the Power Grid

- Drive the design of an resilient cyber infrastructure electric power which operates through attacks
- $18.8 M over five year, started Oct. 1, 2009
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

Ilinois's Singapore Adv. Digital Sciences Center Smart Grid Subprogram

~$15M effort / 5 years

Projects in Microgrids, DERs, and HANs

Korean National Smart Grid TestBed on Jeju Island.

Project concerning tesbed and cyber security research DDOS)

CACAIS

Testbed

Products tested & validated in CACAIS testbed: $1.2M FY10 funding from ONR

Illinois Center for a Smarter Electric Grid

Validation & Compliance Services

- $2.5M, YR1 DCEO funding
- Test bed & lab equipped with HW/SW to perform validation of Smart Grid systems
- Critical Infrastructure Protection (CIP): pre-audit check for compliance to NERC standards
- Prepare for NERC reliability compliance audits

4 DOE Office of Electricity Security Projects with:

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Entergy THE POWER OF PEOPLE

GRID PROTECTION ALLIANCE

DTE Energy

Telcordia

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest NATIONAL LABORATORY

pjm

GRID PROTECTION ALLIANCE

ALSTOM

Honeywell

INL

TCIPG Vision & Research Focus

Vision: Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, which operates through attacks

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications
- Quantifying security and resilience

TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University

TCIPG External Advisory Board

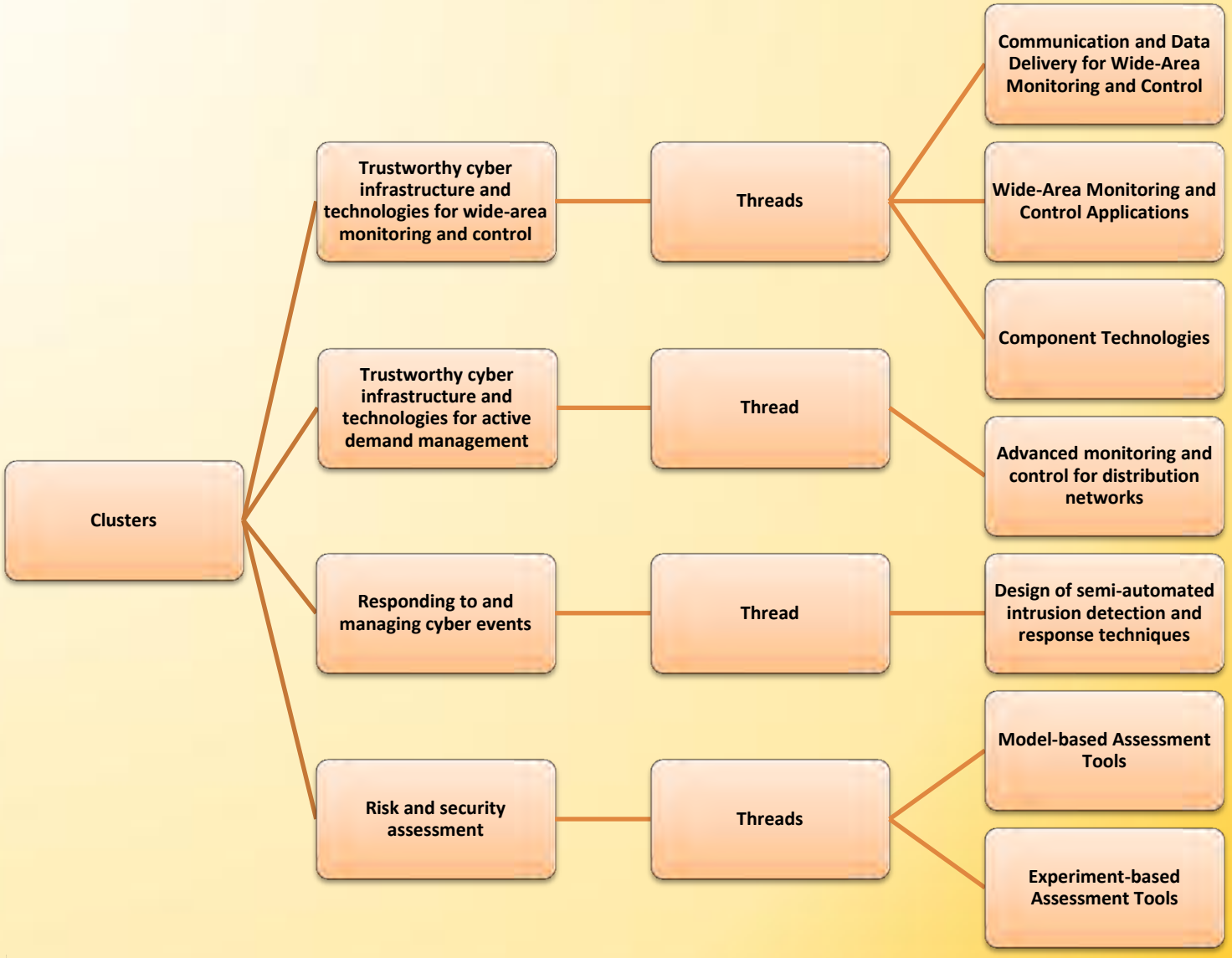
- Marija Ilic (CMU)
- Jeff Katz (IBM)
- Himanshu Khurana (Honeywell)
- Scott Mix (NERC)
- Paul Myrda (EPRI)
- David Norton (FERC)
- Mahendra Patel (PJM)
- Dave Whitehead (SEL)

TCIPG Industry Interaction Board

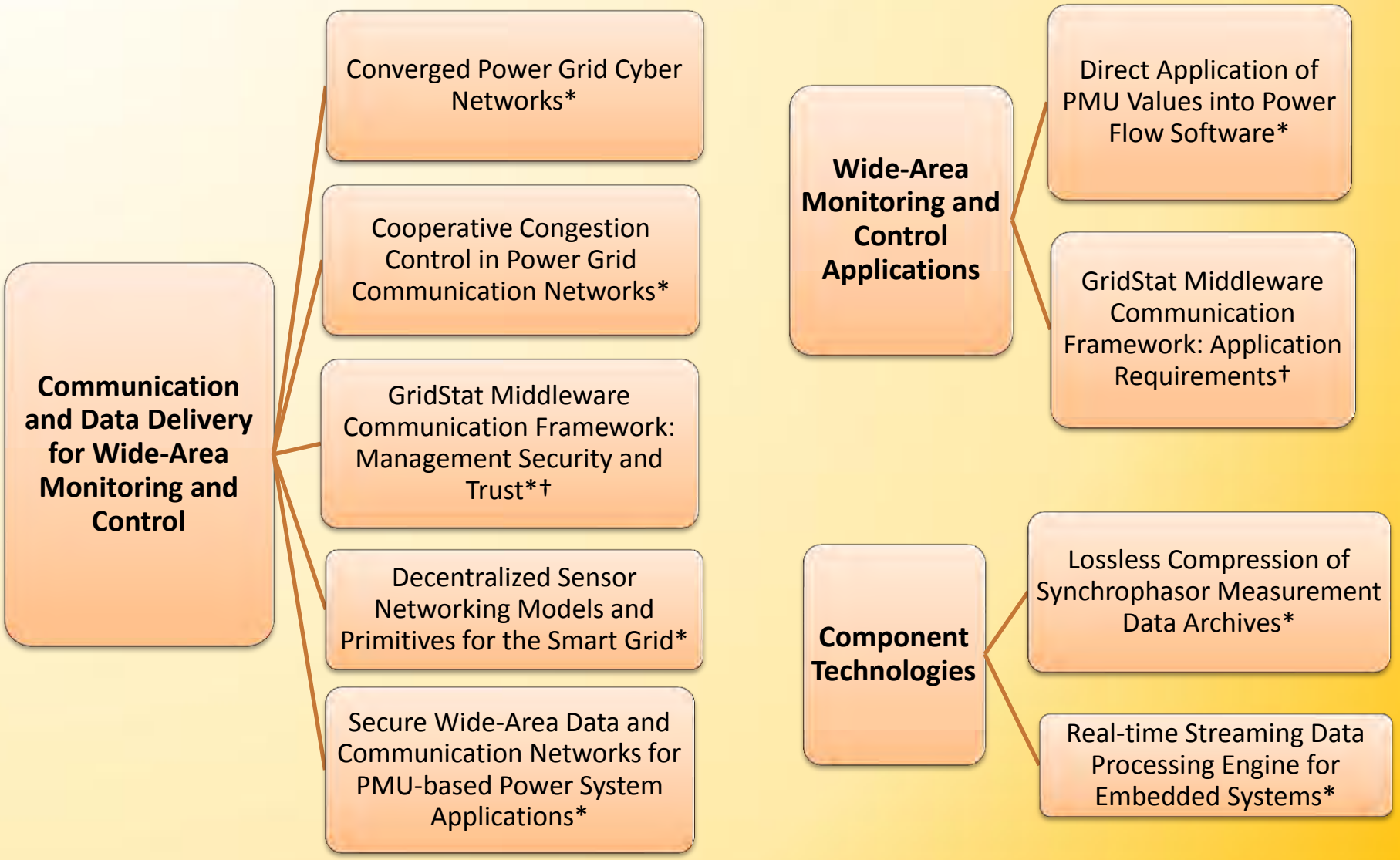
TCIPG Clusters and Cross-Cutting Efforts

- Clusters integrate work in specific technical areas over the life of the project:
  - Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
  - Trustworthy cyber infrastructure and technologies for active demand management
  - Responding to and managing cyber events
  - Risk and security assessment
- Cross-Cutting Efforts address issues that cross technical clusters:
  - Education and workforce development
  - Testbed and evaluation methodologies
  - Industry interactions and technology transition

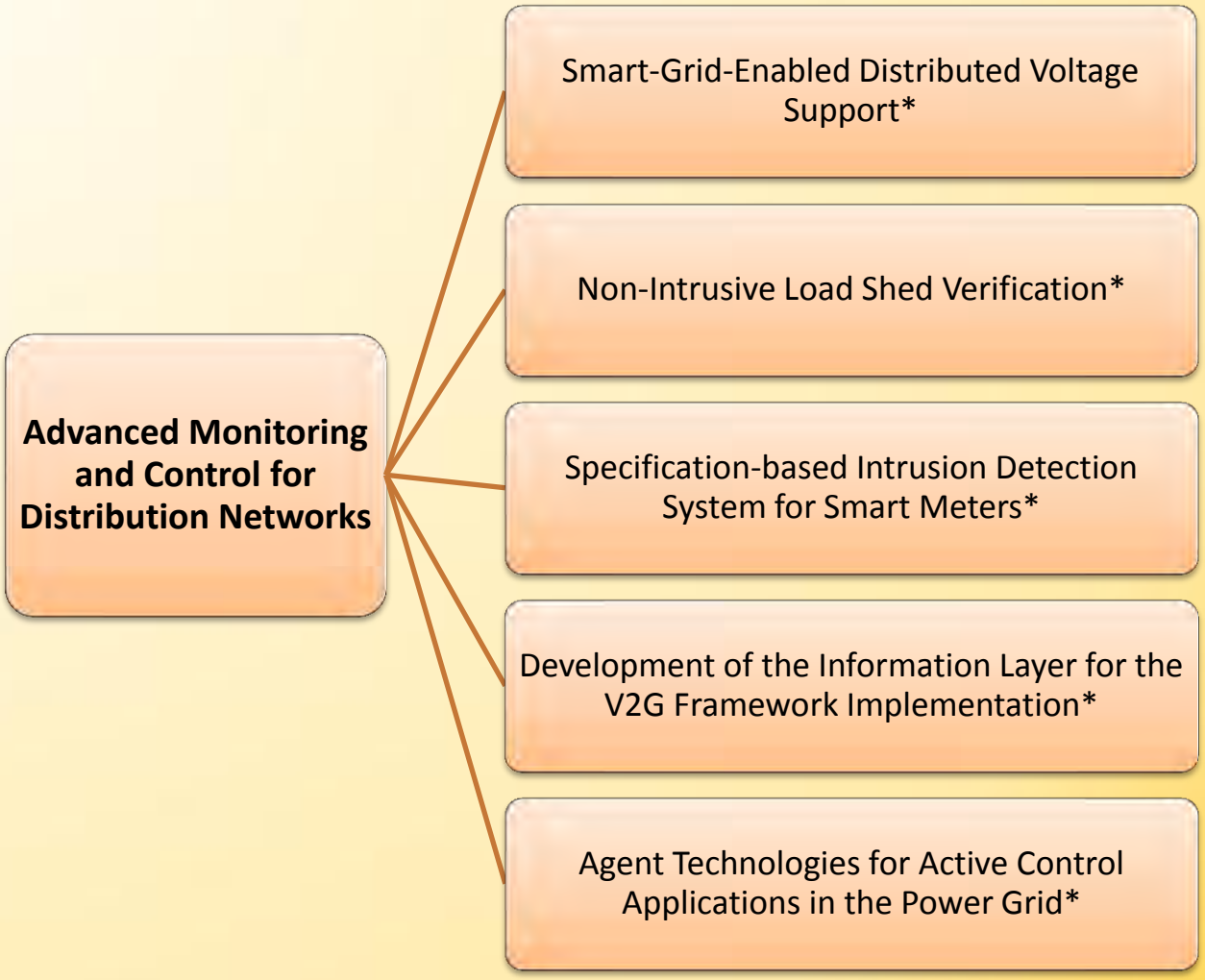
TCIPG Technical Clusters and Threads



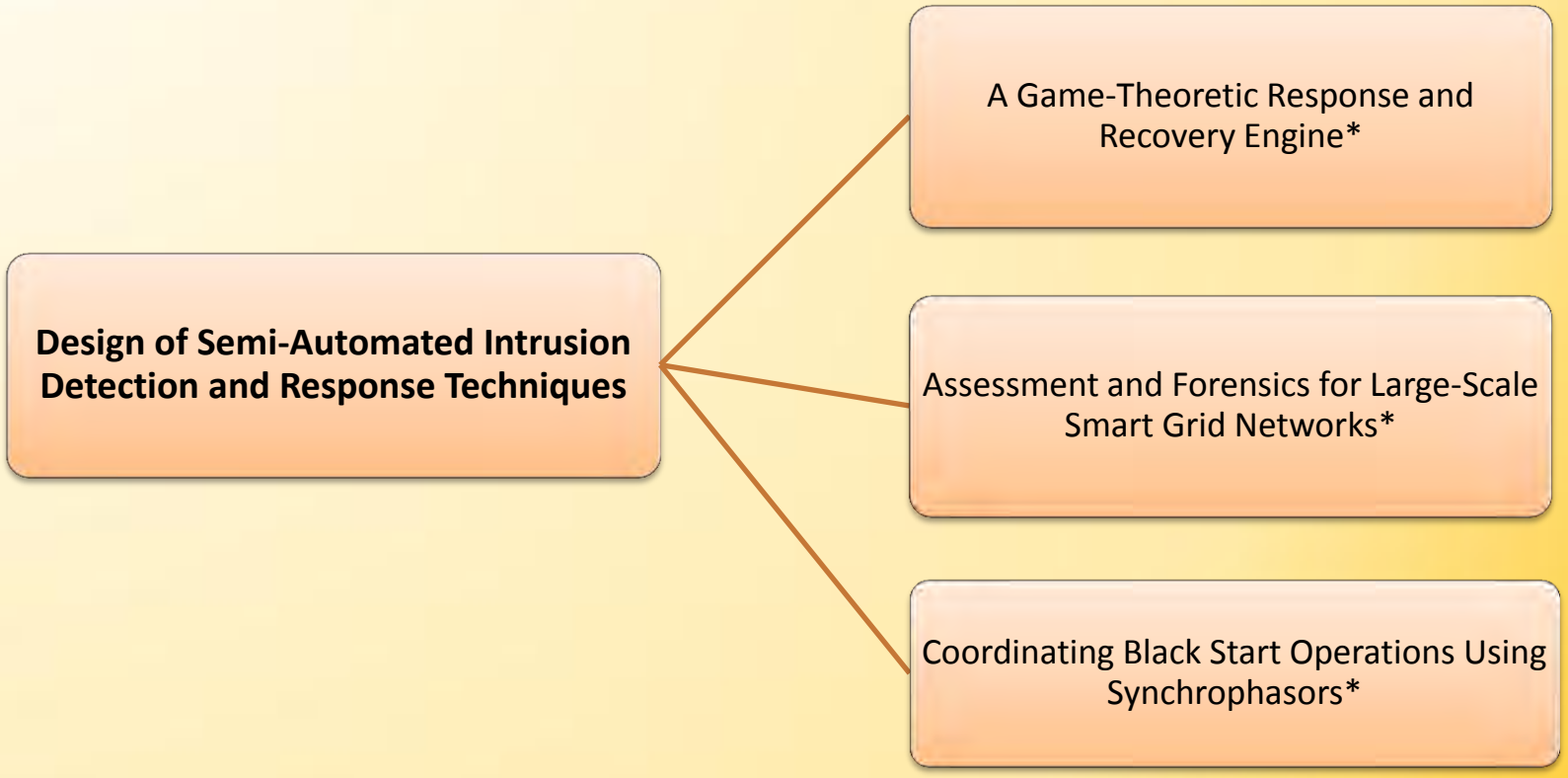
Cluster: Trustworthy Cyber Infrastructure and Technologies for Wide-Area Monitoring and Control



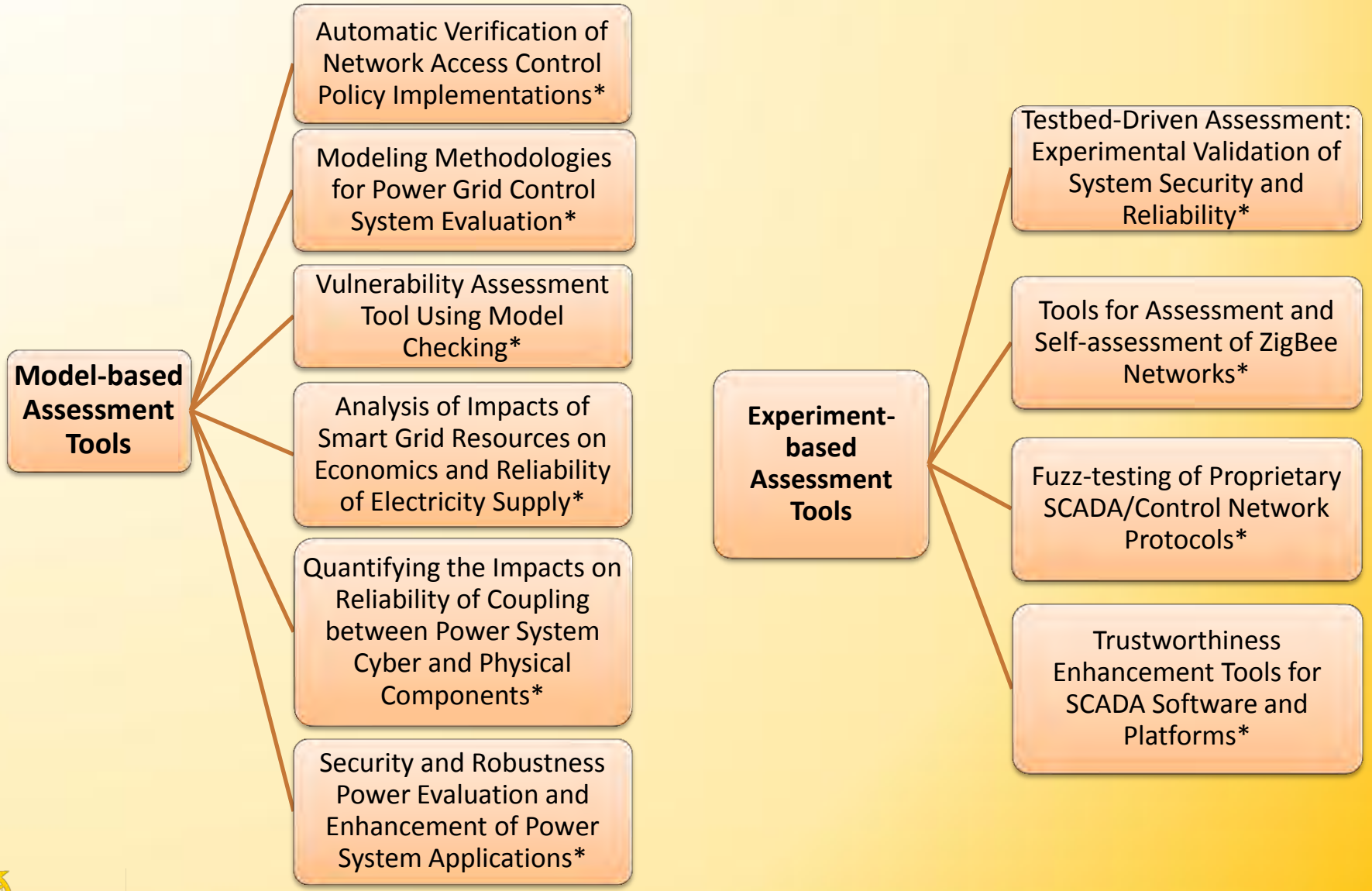
Cluster: Trustworthy Cyber Infrastructure and Technologies for Active Demand Management



Cluster: Responding to and Managing Cyber Events



Cluster: Risk and Security Assessment



Smart Grid Testbed Facilities Overview

- Multiple funding sources (NSF, DHS, DOE, State of Illinois, Office of Naval Research)
- Six years of enabling research for smart grid efforts (e.g., TCIP, TCIPG)
- Directed focus of supporting research in the power grid

Smart Grid Testbed Facilities
Current "State"

- Extensive end-to-end power hardware and software
  - 6 years of support and millions in equipment (purchased and donated)
  - Local expertise on a wide variety of real systems
- Encompassing Simulation and Emulation capabilities
  - Power, Network, and co-simulation
  - Protocols, Transport mediums
- Flexible framework being implemented and advancing towards tailored operating constraints

Smart Grid Testbed Facilities
Current Operating Model

- Advanced Academic Research
  - TCIPG (DOE, DHS)
  - CACAIS (ONR)
  - ICSEG (State of Illinois)
- Leveraged as a resource for various other smart grid projects at Illinois

Smart Grid Testbed Facilities
Near Term Direction

- Tailored environment to support external interaction
- Automated isolation and integration with a wide variety of resources
- Leveraging of the extensive work done under TCIPG and assist pipelining promising work into Industry

- Operating Model: Open for collaborative research

Smart Grid Testbed Facilities
Future Direction

- Fully automated isolation and customizable environment to time-share access to all resources in a repeatable and flexible manner
- Provide advanced cross-cutting expertise, talented resource pool, and uniquely available resources for wide use and to cooperatively engage in advanced research, support of industry agenda, and accelerated transition to practice
- Critical Infrastructure … beyond the smart grid

- Operating Model: Open for facility driven use, sponsored research, or technical testing

TCIPG Webcasts: Technologies for a Resilient Power Grid

- Present topics on research, development, and design of a secure and resilient power grid
- Webcasts are open to the public and attract a broad audience from industry, academia, and government
- Webcast first Friday of each month at 1:00 p.m. CT

CALL FOR SPEAKERS

TCIPG Seminar Series: Technologies for a Resilient Power Grid

beginning Fall 2010

The new TCIPG Seminar Series on Technologies for a Resilient Power Grid seeks speakers to present topics in the broad area of research, development, and design for secure and resilient systems related to the power grid. The scope includes all power grid systems, from traditional systems involved in generation, transmission, and distribution to emerging systems dealing with distributed generation, renewable integration, and demand-response. The seminars will be held on the campus of the University of Illinois at Urbana-Champaign, normally on the first Friday of every month at 1:00 p.m. Central Time, and streamed live on the Web. The seminars will be open to the public and are expected to attract a broad audience from industry, academia, and government. TCIPG will cover speakers' travel costs.

If you are interested in appearing as a speaker in the series, please contact TCIPG principal scientist Himanshu Khurana at hkhurana@iti.illinois.edu.

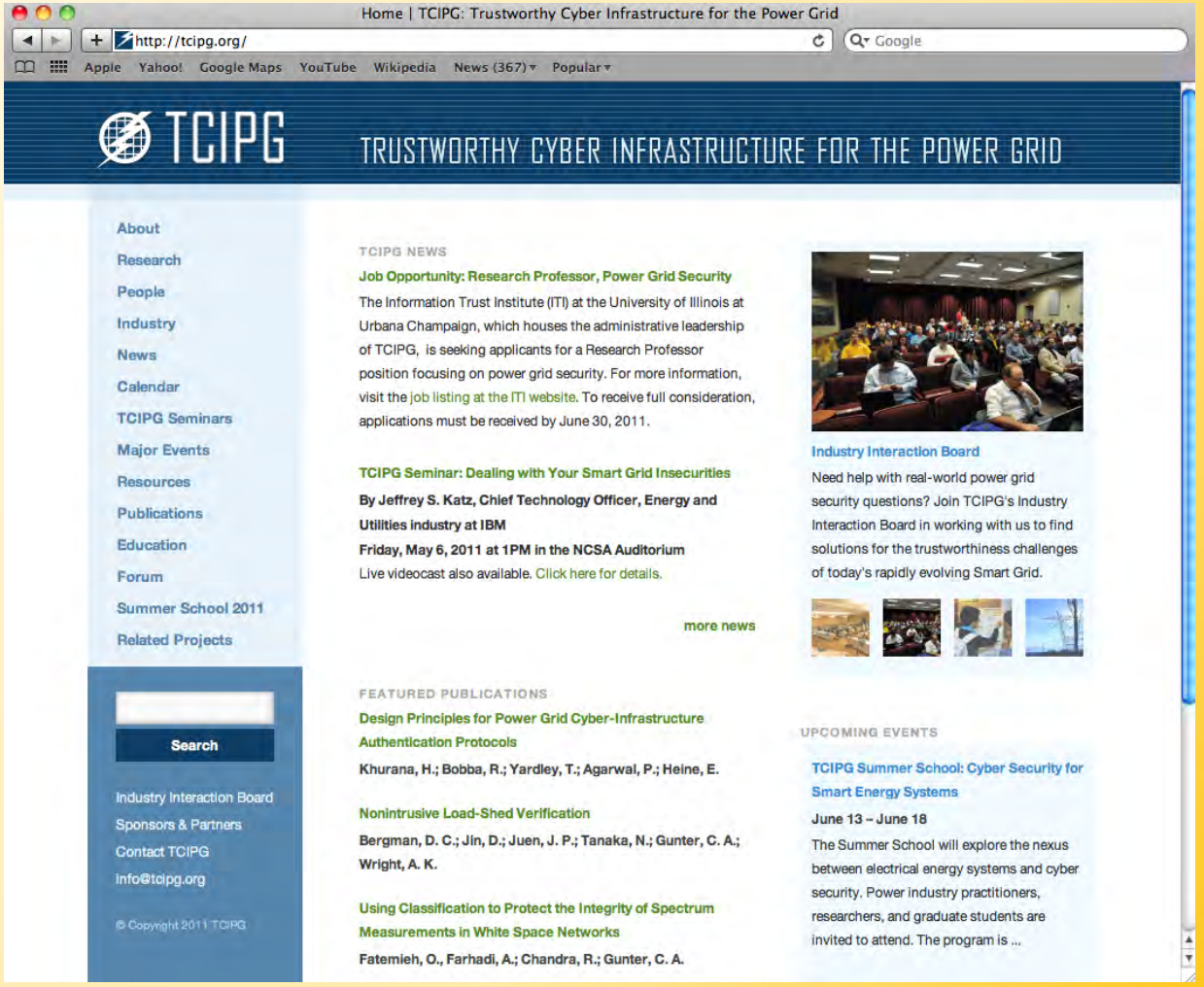
The new seminar series is presented by the TCIPG Center (Trustworthy Cyber Infrastructure for the Power Grid), whose partner institutions are the University of Illinois at Urbana-Champaign, Cornell University, Dartmouth College, the University of California at Davis, and Washington State University. The TCIPG Center, which is a successor to the earlier NSF-funded TCIP Center, was founded in 2009 by the U.S. Department of Energy with additional support from the U.S. Department of Homeland Security. It is housed in the University of Illinois Information Trust Institute.

The TCIPG Center's work involves the development and integration of information technologies with the key properties of real-time availability, integrity, authentication, and confidentiality needed to build a more resilient power grid. Its objectives are to develop and evaluate technologies needed for realizing select Smart Grid applications, such as wide-area monitoring and control, demand response with controllable load, and plug-in hybrid electric vehicles. Ultimately, TCIPG research is expected to result in a secure and real-time communication system, an automated attack response system, and risk assessment and security validation techniques.

www.tcipg.org

To Learn More

- www.tcipg.org
- info@tcipg.org
- Request to be on our mailing list



Source: www.logiic.org

LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity)

- The LOGIIC program is an ongoing collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate
- LOGIIC was formed to facilitate cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems
- The program undertakes collaborative research and development projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector
- The program objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality

Source: www.logiic.org

LOGIIC Governance

- The Automation Federation serves as the LOGIIC host organization and has entered into agreements with the LOGIIC member companies
- Member companies contribute financially and technically, provide personnel who meet regularly to define projects of common interest, and provide staff to serve on the LOGIIC Executive Committee
- The U.S. Department of Homeland Security, Science and Technology Directorate has contracted with scientific research organization SRI International to provide scientific and technical guidance as well as project management for LOGIIC

Source: www.logiic.org

LOGIIC Members

- Current members of LOGIIC include BP, Chevron, Shell, Total, and other large oil and gas companies that operate significant global energy infrastructure.

"LOGIIC is a model example of how leading industry organizations can team with government in a public-private partnership to ensure the security and safety of the automation systems that are crucial to our critical infrastructures"

Ted Angevaare, Shell

Source: www.logiic.org

LOGIIC Projects

1. 2005-2006 LOGIIC Correlation Project
   - See www.cyber.st.dhs.gov/logiic/
2. Safety Instrumented Systems (SIS)
   - LOGIIC seeks to evaluate and improve the level of security of Safety Instrumented Systems as these are increasingly integrated with process control systems
   - These goals are to be achieved by an evaluation process conducted by subject matter experts working closely with system vendors
   - The results of this project will ultimately benefit not only the members of LOGIIC but also the oil and gas industry as a whole.
3. …
4. …

Source: www.logiic.org

ELECTRIC POWER RESEARCH INSTITUTE

EPRI Cyber Security Projects

NITRD TTS: Solutions for the Smart Grid

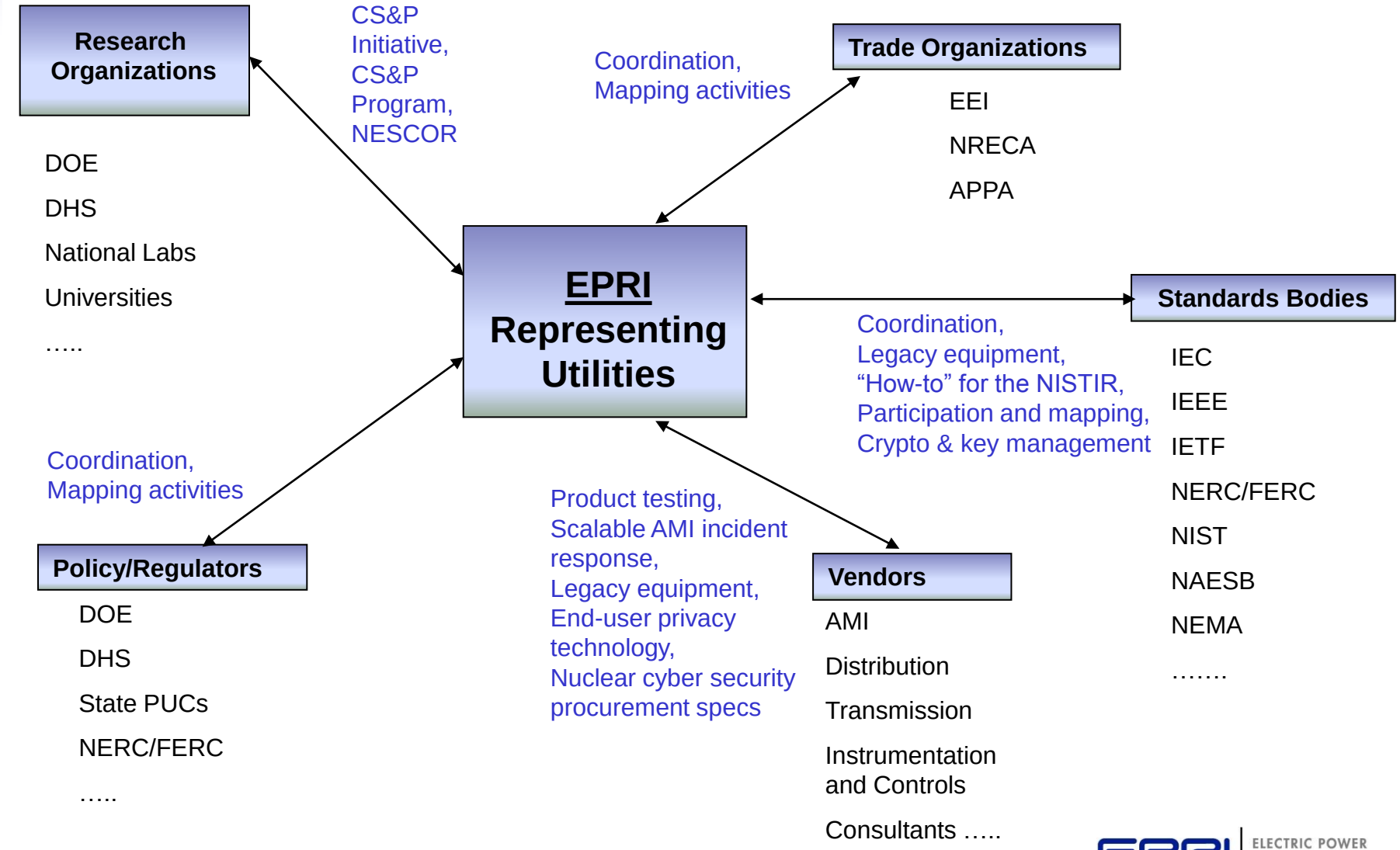
Galen Rasche

Technical Executive

grasche@epri.com

2011-July-20

EPRI Cyber Security Activities Landscape



DOE National Electric Sector Cyber Security Organization (NESCO)

EnergySec	EPRI
• Primary grant recipient	• Research and analysis
• Information and resource sharing • Collaboration • Situational/tactical awareness • Rapid notification • Forensics	• Mitigate risks from imminent threats and vulnerabilities • Harmonize cyber security requirements • Assess cyber security posture of standards and technologies
• Focus on near-term issues	• Focus on longer-term issues • Support near-term efforts of EnergySec

EPRI Power Delivery and Utilization (PDU) Cyber Security and Privacy Initiative

Objectives:

- Prevent cyber incidents by creating requirements, developing guidelines, and addressing legacy systems
- Create framework for responding to AMI incidents
- Inform the development of the research agenda for the **Cyber Security and Privacy Program** for the next three to five years

Activities:

Map Activities Landscape	**Protect Legacy Systems**
Guidelines for NISTIR 7628	**AMI Incident Response**
Contribute to Industry Efforts	**Assess Cyber-Physical Attacks**

Generation Sector Initiative Project

- Cyber Security Strategies for Instrumentation & Control Systems
- 2011 and 2012 Supplemental

- Tasks:
  - Integrating Data Diodes to Meet Compliance
  - Compliant Integration of Wireless Devices into GEN Environment
  - Change Management Tools and Techniques

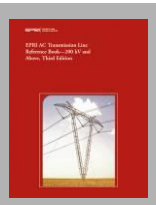
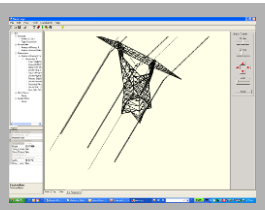
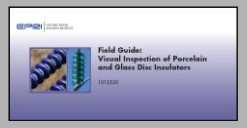
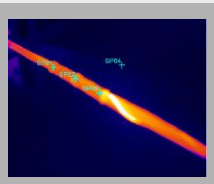
Nuclear Sector Initiative Project

- Cyber Security Procurement Requirements For Plant Digital Systems

- April 2011 – July 2012 (TBD)

- Scope:
  - Develop generic procurement language for cyber-security requirements
  - Create consensus with utilities and vendors
  - Develop guideline and draft procedures for using the procurement language

PDU P183: Cyber Security and Privacy Program Summary Overview

Prevention	 Risk Management For Cyber-Physical Attacks	 Security Testing Tools For End-User Devices	 Security Requirements For New Technology
Protection	 Secure Remote Access to Substations	 Secure DER Architectures	 Risk Mitigation For Legacy Systems
Response / Recovery	 Standardized AMI Security Objects	 Network and Security Management For Transmission	 Framework for Unified Event Monitoring	 Resiliency From Cyber Incidents

Short Term → Long Term

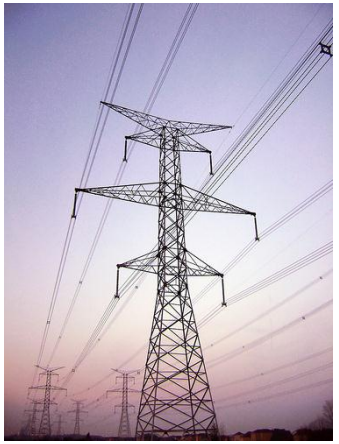
EPRI ELECTRIC POWER RESEARCH INSTITUTE

P183A: Cyber Security and Privacy Technology Transfer and Industry Collaboration

- **Mapping the Smart Grid Cyber Security and Privacy Landscape**
  - Provide members regular updates on document
- **Technology Transfer and Industry Collaboration**
  - Support active participation and contribution to:
    - UtiliSec
    - NIST SGIP (CSWG and DPG)
    - NAESB Privacy Task Group
  - Deliver detailed updates on:
    - NERC, DHS ICSJWG
- **White papers on government activities**

P183B: Security Technology for Transmission and Distribution Systems

- Mitigating risk of legacy equipment
  - Frameworks for incident response
    - Security Architectures for the Smart Grid



Projects:

- Security Strategies for Legacy Systems
- Network Security Management for Transmission Systems
- Risk Management for Cyber-Physical Incidents
- Assessment of Substation Remote Access Security
- Security Architectures for Distributed Energy Resources

P183C: Security and Privacy for End Use Technology

- Standardizing AMI security objects
- Supporting user data privacy
  - Scalable key management techniques

Projects:

- Standardized Security Objects for AMI
- Cryptography and Key Management
- Technology Solutions for Supporting Privacy of End-User Data
- Tools and Techniques for Security Testing of End-User Devices

Cryptography and Key Management

- Millions of meters containing crypto keys for:
  - Authentication, integrity of updates and commands, confidentiality
  - Current key management technology does not scale
- Build on work by the CSWG Cryptography Subgroup and the Design Principles Group
- Tasks:
  - Specify primary elements of the Crypto Key Management System (CKMS)
  - Define the performance criteria
  - Select and configure CKMS technology
  - Document the analysis

Technology for End-User Privacy

- Background
  - Smart Grid enabled bi-directional flow of information
  - Granularity and quantity of information collected
  - Introduction of third-party data access
- Project builds work by CSWG Privacy Subgroup, ABA Privacy Working Group, NAESB Data Privacy Task Force, and the EU Smart Grid Task Force
  - Identify and evaluate technology required to store, aggregate, analyze and protect energy usage
  - Analyze in the context of system bandwidth and processing constraints
  - Develop logical architecture and test a reference implementation

Discussion

Galen Rasche
grasche@epri.com

Together…Shaping the Future of Electricity