National Cybersecurity Center of Excellence

Energy Sector Projects

GridSecCon 2018

10/16/2018

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

Agenda		
8:00-8:10	Welcome & Overview of NCCoE	Harry Perper
8:10-10:30	**Part I: Panel Presentations** 10 min Q&A after each presentation	
8:10-8:40	NCCoE/NIST	Jim McCarthy & Michael Powell
8:50-9:20	University of Maryland & TDi Technologies	Don Hill & Bill Johnson
9:30-9:50	Pacific Northwest National Laboratory (PNNL)	Mark Rice
10:00-10:30	Break	
10:30-12:00	**Part II: Open Dialogue and Discussion** IIoT Challenges in the Energy Space	
10:30-10:45	Introduction of Panelists	Harry Perper (Panel Moderator)
10:45-11:45	Questions and Discussion with Panelists	Jim McCarthy Mark Rice Jon Stanford Bill Johnson Patrick Miller
11:45-12:00	Summary of Morning, Way Ahead & Closing	

Foundations

Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

NIST Information Technology Laboratory

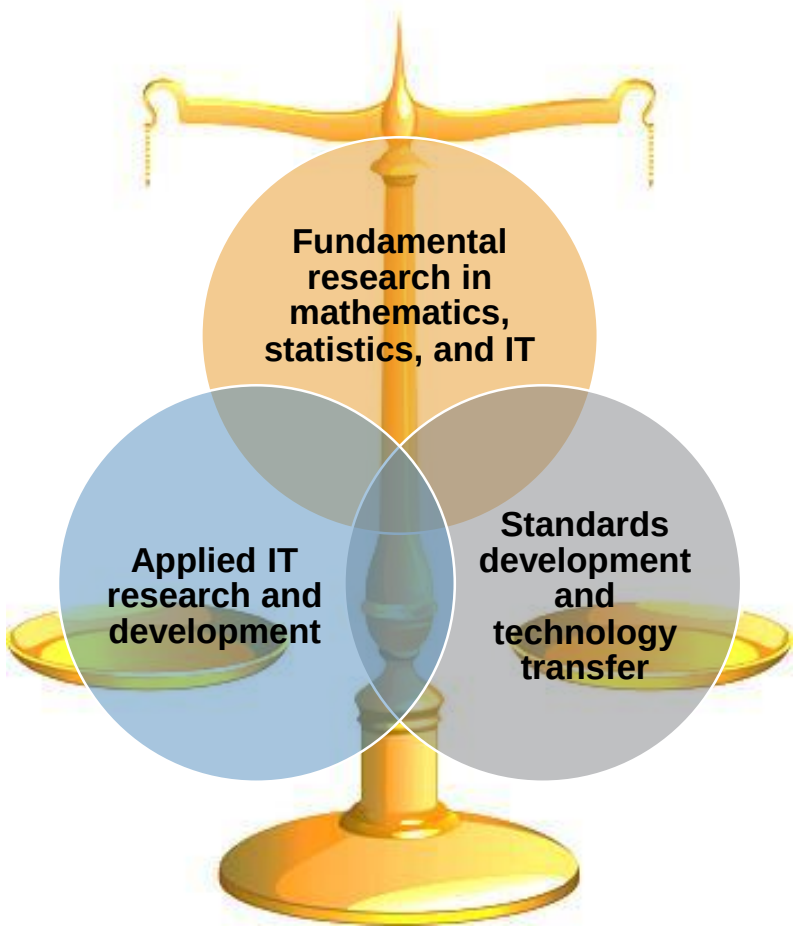
Cultivating Trust in IT and Metrology through measurements, standards and tests

ITL Programs

- Advanced Networking
- Applied and Computational Mathematics
- Cybersecurity
- Information Access
- Software and Systems
- Statistics

Collaborations with

- Industry
- Federal/State/Local Governments
- Academia



Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

NCCoE Tenets

Standards-based
Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable
Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available
Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent
Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

Sector-Based Projects

- Commerce/Retail
- Energy
- Financial Services
- Health Care
- Hospitality
- Manufacturing
- Public Safety/First Responder
- Transportation

Energy Sector

Projects

Asset Management **(Current Project)**

Identity and Access Management **(SP 1800-2)**

Situational Awareness **(SP 1800-7)**

Join our Community of Interest

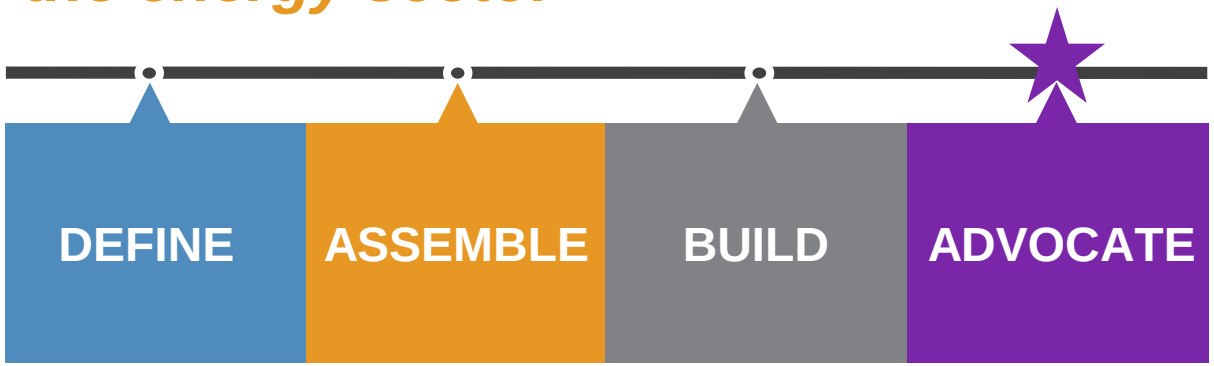
Email us at energy_nccoe@nist.gov

Identity and Access Management: SP 1800-2

Securing networked infrastructure for the energy sector

Overview

- Electric companies need to be able to control access to their networked resources
- Identity and Access Management (IdAM) implementations are often decentralized and controlled by numerous departments within a company
- The IdAM Practice Guide shows how an electric utility can implement a converged IdAM platform to provide a comprehensive view of all users within the enterprise across all silos, and the access rights they have been granted



Project Status

Final SP 1800-2 released July 2018

Collaborate with Us

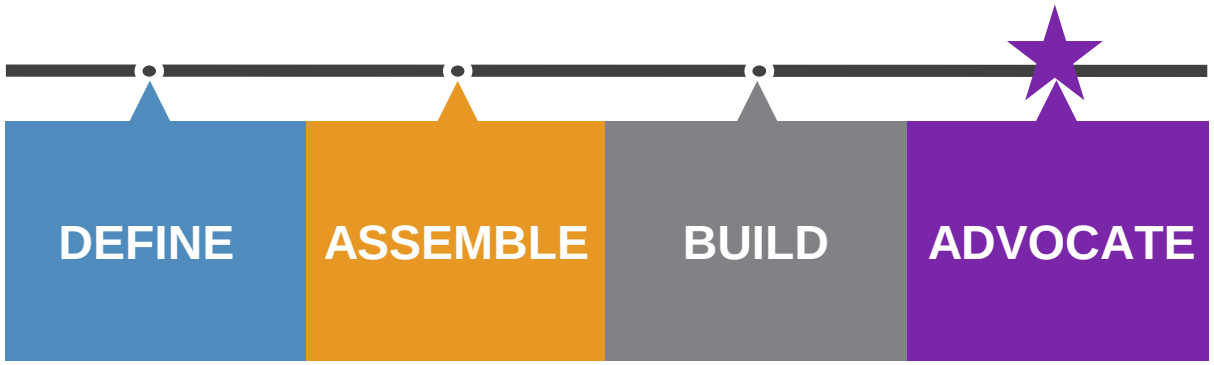
- Download NIST SP 1800-2, Identity and Access Management for Electric Utilities
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

Situational Awareness: SP 1800-7

Improving security for electric utilities

Overview

- Energy companies rely on operational technology to control the generation, transmission, and distribution of power
- A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots
- This project explores methods energy providers can use to detect and remediate anomalous conditions, investigate the chain of events that led to the anomalies, and share findings with other energy companies



Project Status

Released draft Practice Guide SP 1800-7 in Feb 2017, comment period closed April 2017

Collaborate with Us

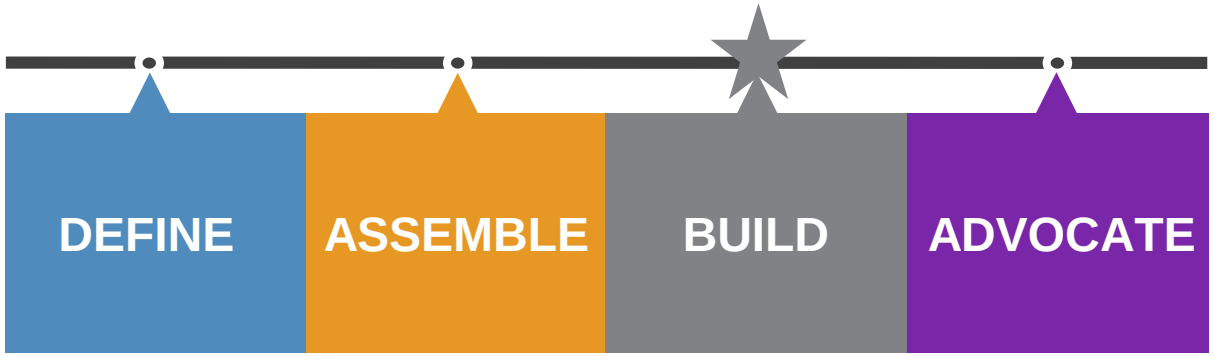
- Read SP 1800-7 Situational Awareness for Electric Utilities Practice Guide Draft
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

Asset Management

Assessing cyber risk on OT networks

Overview

- Industrial control system assets provide command and control information as well as key functions on OT networks, therefore any vulnerabilities in these assets can present opportunities for malicious actors.
- To properly assess cybersecurity risk within the OT network, energy companies must be able to identify all of their assets, especially those that are most critical.
- This project will provide a reference architecture and an example solution for managing, monitoring, and baselining assets, and will also include information to help identify threats to these OT assets.



Project Status

Released final Project Description March 2018

Collaborate with Us

- Read Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry Project Description
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

ESAM Project Milestones

June 2018	Build Team Kickoff
July/August 2018	Build Architecture
October/November 2018	Implementation
January/February 2019	Draft ESAM Practice Guide (PG)
March 2019	Draft ESAM Public Release

NCCoE ESAM Team: Contacts / Roles

Jim McCarthy	NIST/NCCoE – Principle Investigator	James.McCarthy@NIST.gov
Michael Powell	NIST/NCCoE – Project Engineer	Michael.Powell@NIST.gov
Titilayo Ogunyale	MITRE/NCCoE – Project Lead	TOgunyale@MITRE.org
John Wiltberger	MITRE/NCCoE – Lead Project Engineer	JWiltberger@MITRE.org
Devin Wynne	MITRE/NCCoE – Project Engineer	DWynne@MITRE.org
Lauren Acierto	MITRE/NCCoE – Outreach & Engagement	LAcierto@MITRE.org
Nikolas Urlab	MITRE/NCCoE – Project Engineer	NUrlab@MITRE.org

OT Asset Management Attributes

Asset Discovery:

- establishment of a full baseline of physical and logical locations of assets

Asset Identification:

- capture of asset attributes, such as manufacturer, model, operating system (OS), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions

Asset Visibility:

- continuous identification of newly connected or disconnected devices, and IP (routable and non-routable) and serial connections to other devices

Asset Disposition:

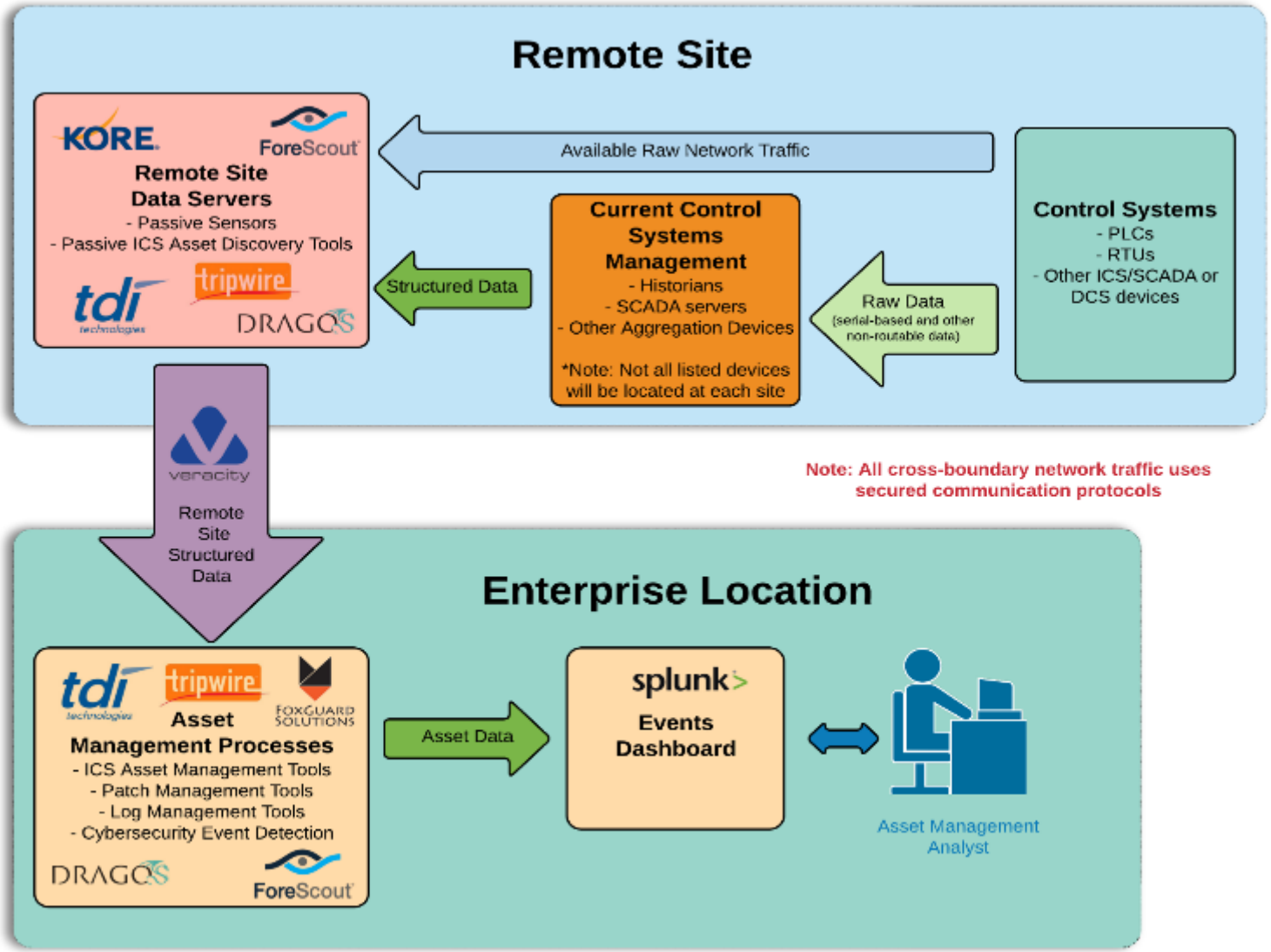
- the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (to include serial) with other devices

Alerting Capabilities:

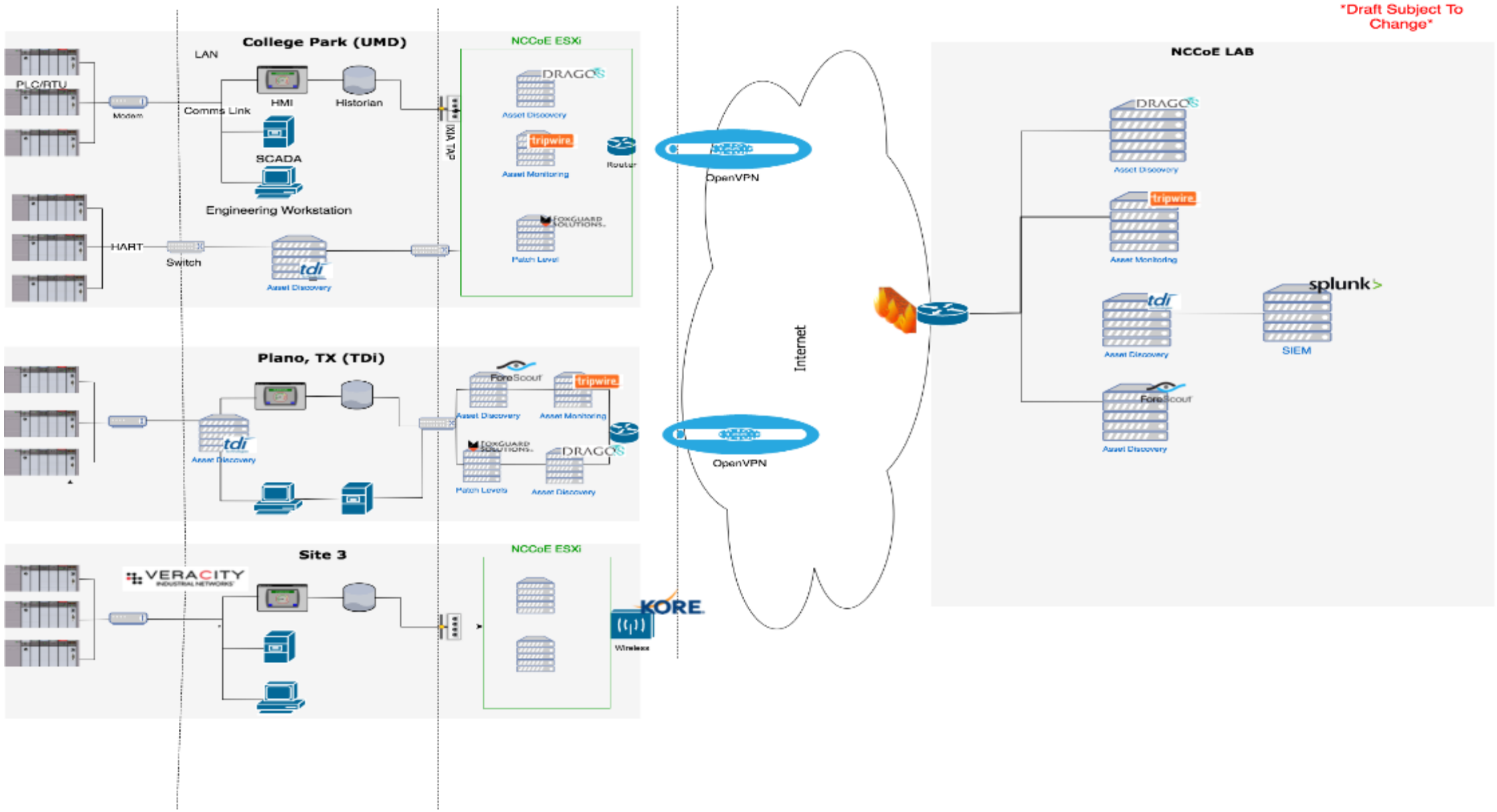
- detection of a deviation from the expected operation of assets

ESAM Build Team

ESAM Flow Diagram



ESAM Build Architecture to Date



ESAM Project Execution Timeline

DESCRIBE › **FORM TEAM** › **DESIGN** › **BUILD PLAN** › **BUILD** › **DOCUMENT** › **OUTREACH**

Publish the NCCoE use case project description

Form the team and complete the FRN, LOI, and CRADA

Design and engineer the architecture and usage scenarios taking into consideration resources

Develop the execution plan for building the demonstration based on the design

Compose, build the demonstration, and perform security functional tests

Develop the practice guide to publish as a public draft and final document

Present at public events and interact with community of interest

Q2 2018 | Q3 2018 | Q3 / Q4 2018 | Q3 / Q4 2018 | Q4 2018 / Q1 2019 | Q1 / Q2 2019 | Q3 2019

Manufacturing Behavioral Anomaly Detection Use Case

NISTIR 8219: Securing Manufacturing Industrial Control Systems – Behavioral Anomaly Detection

- **Single capability scope in two manufacturing demo environments**
  - Collaborative robotics system
  - Simulated chemical process system
- **Security characteristics were mapped to the Cybersecurity Framework**

Manufacturing Build Team

Behavioral Anomalies

- **Abnormal equipment operations**
  - High trouble call frequency
- **Sensor disruptions**
  - Door sensor failure
- **Communication disruptions**
  - Robot coordination failure
- **Environmental changes**
  - High work cell temperature
- **Data corruption**
  - Invalid process variable values

NISTIR 8219

Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

- **Project goal:**
  - demonstrate behavioral anomaly detection techniques that businesses can implement and use to strengthen the cybersecurity of their manufacturing processes.
- **Three detection methods:**
  - network-based
  - agent-based
  - operational historian/sensor-based

Questions?

Jim McCarthy, Senior Security Engineer

James.McCarthy@nist.gov

301-975-0228

Michael Powell, Security Engineer

Michael.Powell@nist.gov

301-975-0310

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov

University of Maryland

Don Hill

University of Maryland, College Park (UMCP)

Don Hill

University of Maryland
Electric, Steam & Chilled Water
Cogeneration Plant

University of Maryland
NIST NCCOE
Situational Awareness Project

Asset Management How Will UMD Benefit From ESAM?

By sustainableumd

Questions?

TDi Technologies

Bill Johnson

ConsoleWorks
Cybersecurity Operations Platform


One
Platform.
One Path.
ConsoleWorks
Cybersecurity Operations Platform

ConsoleWorks

Cybersecurity Operations Platform

YEARS IN BUSINESS 27

> "ConsoleWorks provides visibility with a level of fidelity not available in other solutions."
>
> Chris Inglis, Former Deputy Director , NSA

2 YEARS NATIONAL CYBERSECURITY EXCELLENCE PARTNERSHIP (NCEP)

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

6 LABS WHERE CONSOLEWORKS IS INSTALLED

AFIT | EPRI | NCCOE | ORNL | PNNL | TDI

5 CASES NCCoE USE CASES PARTICIPATED

- » Energy Sector Asset Management
- » Privileged Account Management for the Financial Sector
- » Energy Sector Identity and Access Management
- » Wireless Infusion Pump
- » Securing Picture Archiving and Communication system

5 RESEARCH PROGRAM PARTICIPATION

CREDC | DOE | ORNL | PNNL | SEEDS

CRITICAL INFRASTRUCTURE INDUSTRIES

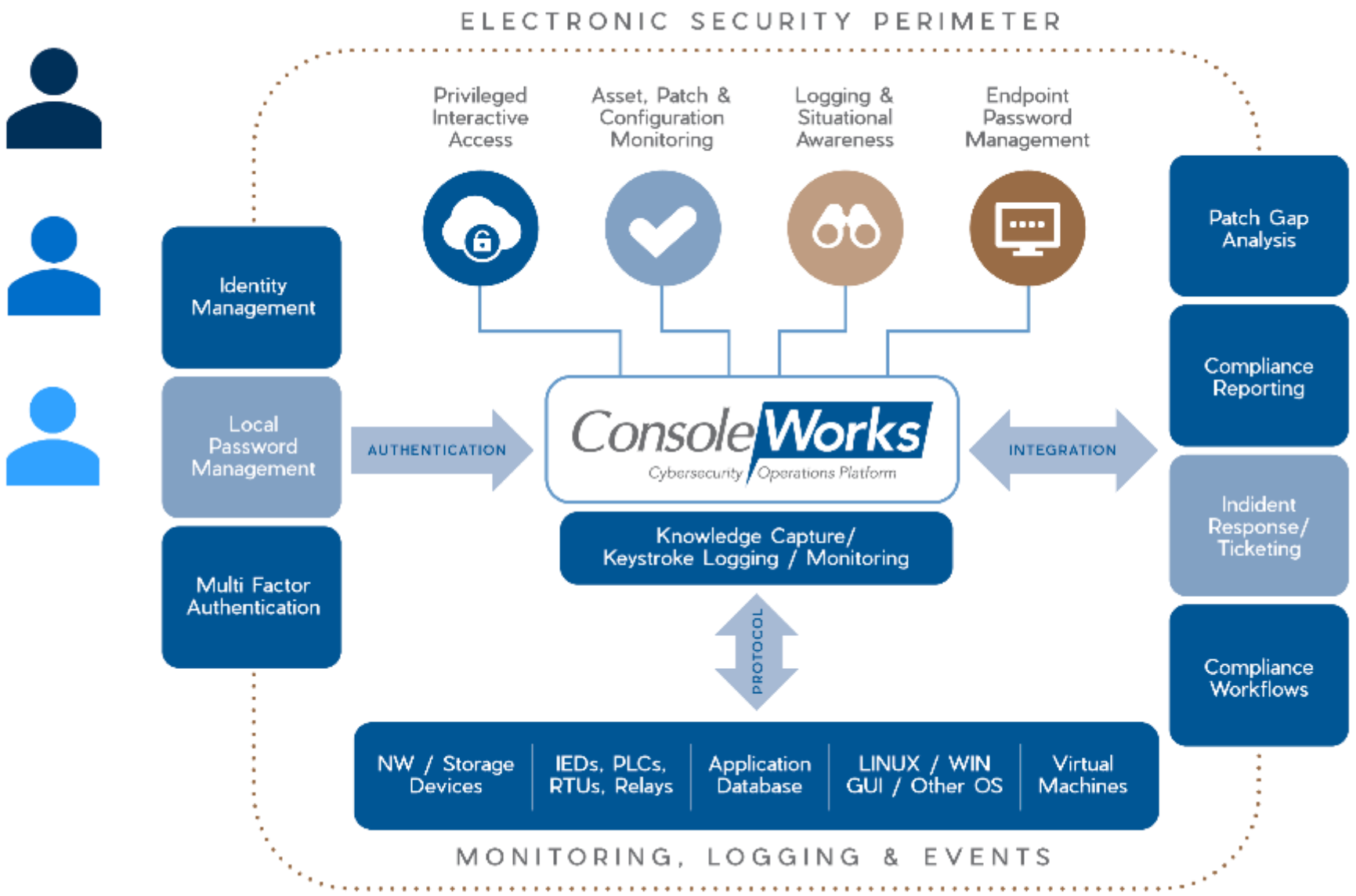
- ENERGY
- GOVERNMENT/ INTELLIGENCE
- TELECOM
- HEALTHCARE
- FINANCE

100K+ MANAGED ASSETS

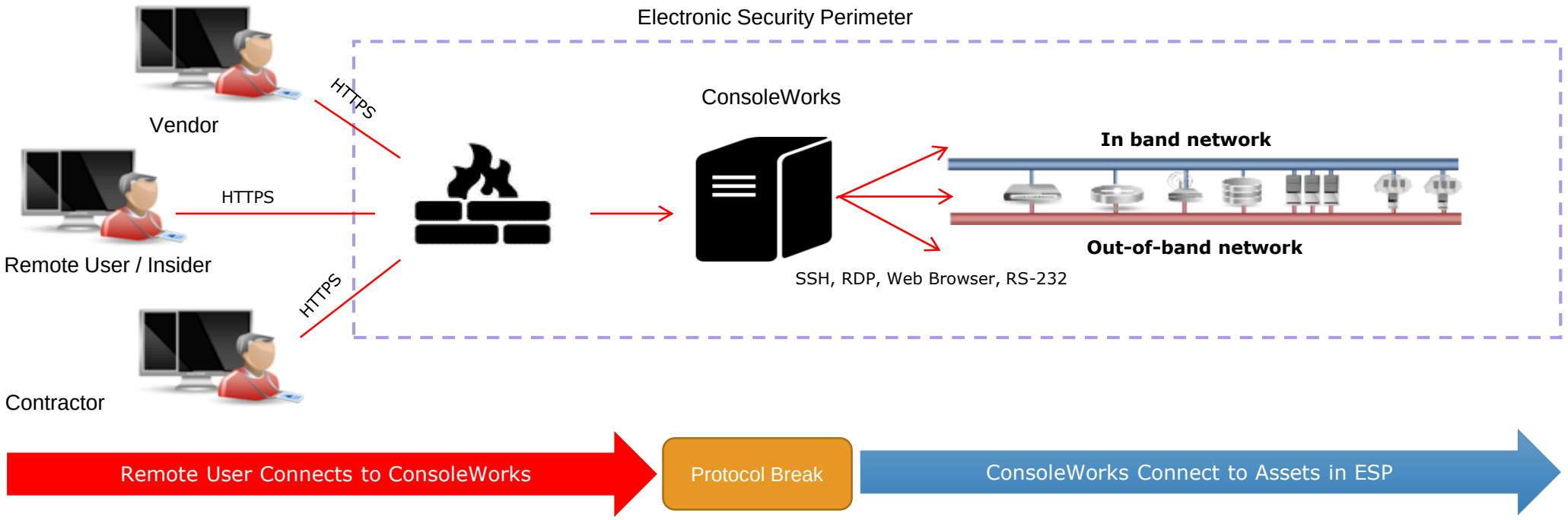
EXPERTISE

6 PATENTS

Single platform for IT and OT security, operations, and compliance of diverse, privileged resources – people and critical assets



ConsoleWorks – Our Approach is Key



Vendor / Protocol Agnostic – HTTPS, Serial, Telnet, MODBUS, etc.

RBAC – Vendor, Insider, Contractor, etc.

No Agents (software) installed on endpoints – No impact to performance, No warranties violated, No software to patch, etc.

History of Industry Investment

ConsoleWorks
Cybersecurity Operations Platform

Industrial Control Systems (ICS) Lab

GE Multilin ML3000
SEL 2404 - Clock
CISCO ASA 5510
HP ProCurve
CISCO ASA 5510
HP ProCurve
Cyclades Console Server

Monitor / Keyboard

GE Multilin 350
GE Multilin 850
(2) Modems
SEL 3355 – SEL Software
GE Multilin 850
NovaTech OrionLX

D20MX / EnerVista Software
HP DL360
HP DL380
HP DL360 - ConsoleWorks
UPS

SEL 2730M - Switch
SEL 2740 - SDN
SEL 2740 - SDN
SEL 2020
SEL 279H
SEL 3620 - Gateway
SEL 2032
SEL 251
SEL 251
SEL 2BFR – Breaker Failure Relay
SEL 501 – Dual Over current Relay
(2) SEL 587 – Current Differential Relay
SEL 321 – Phase and Ground Distance Relay
SEL 2411
SEL 700G
SEL 3530 - RTAC
SEL 421 – Protection Automation Control

Questions ?

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

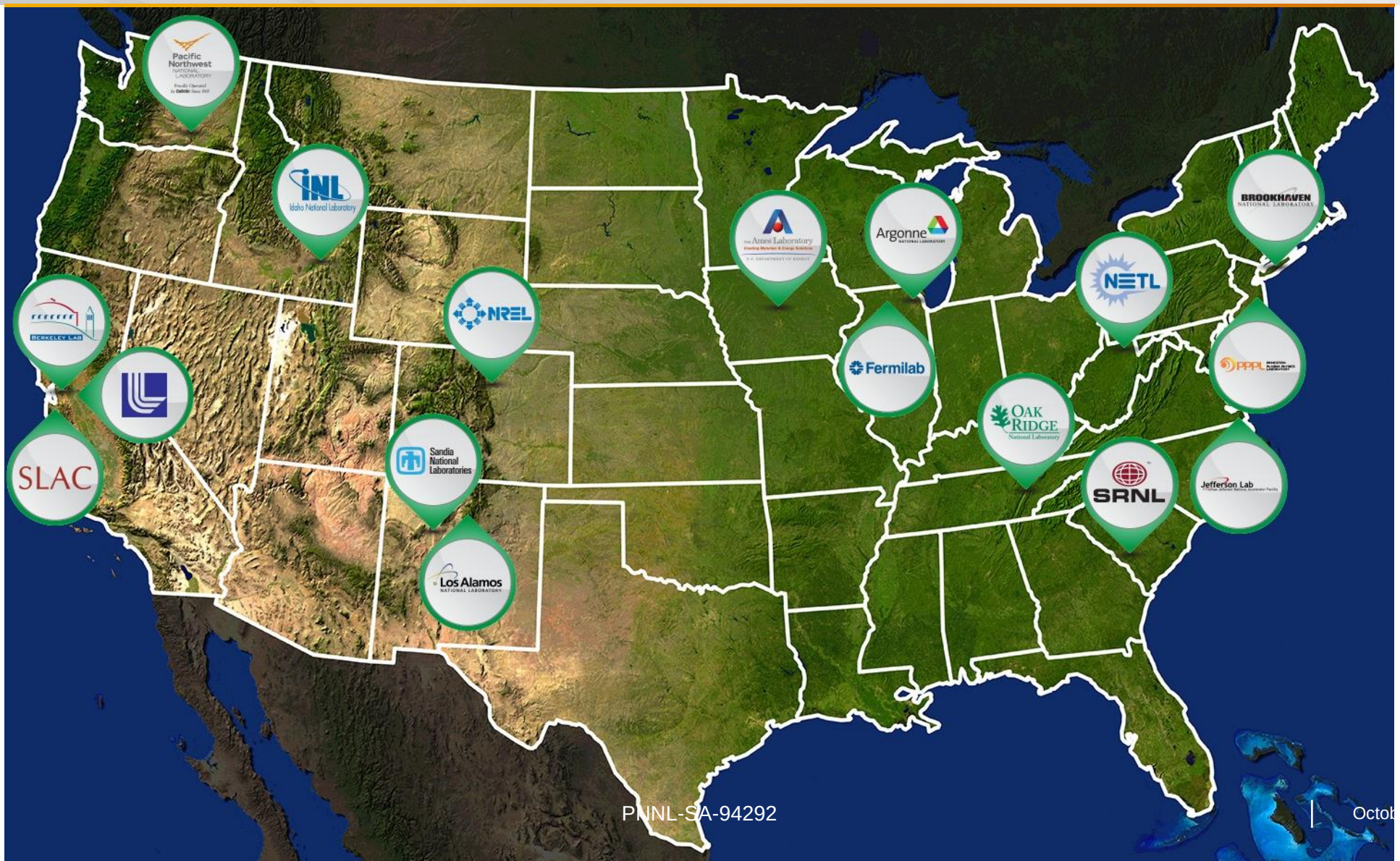
Pacific Northwest National Laboratory

IMPROVING CYBERSECURITY IN OT ENVIRONMENTS

DR. MARK RICE

Electricity Infrastructure
Energy & Environment Directorate
http://eioc.pnnl.gov
Richland, WA

The National Laboratory System



A PNNL Core Competency

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Cybersecurity for Energy Systems leverages the cyber expertise of PNNL's IT staff with the domain expertise in electrical, buildings, and related industrial control systems of building and power system engineers.

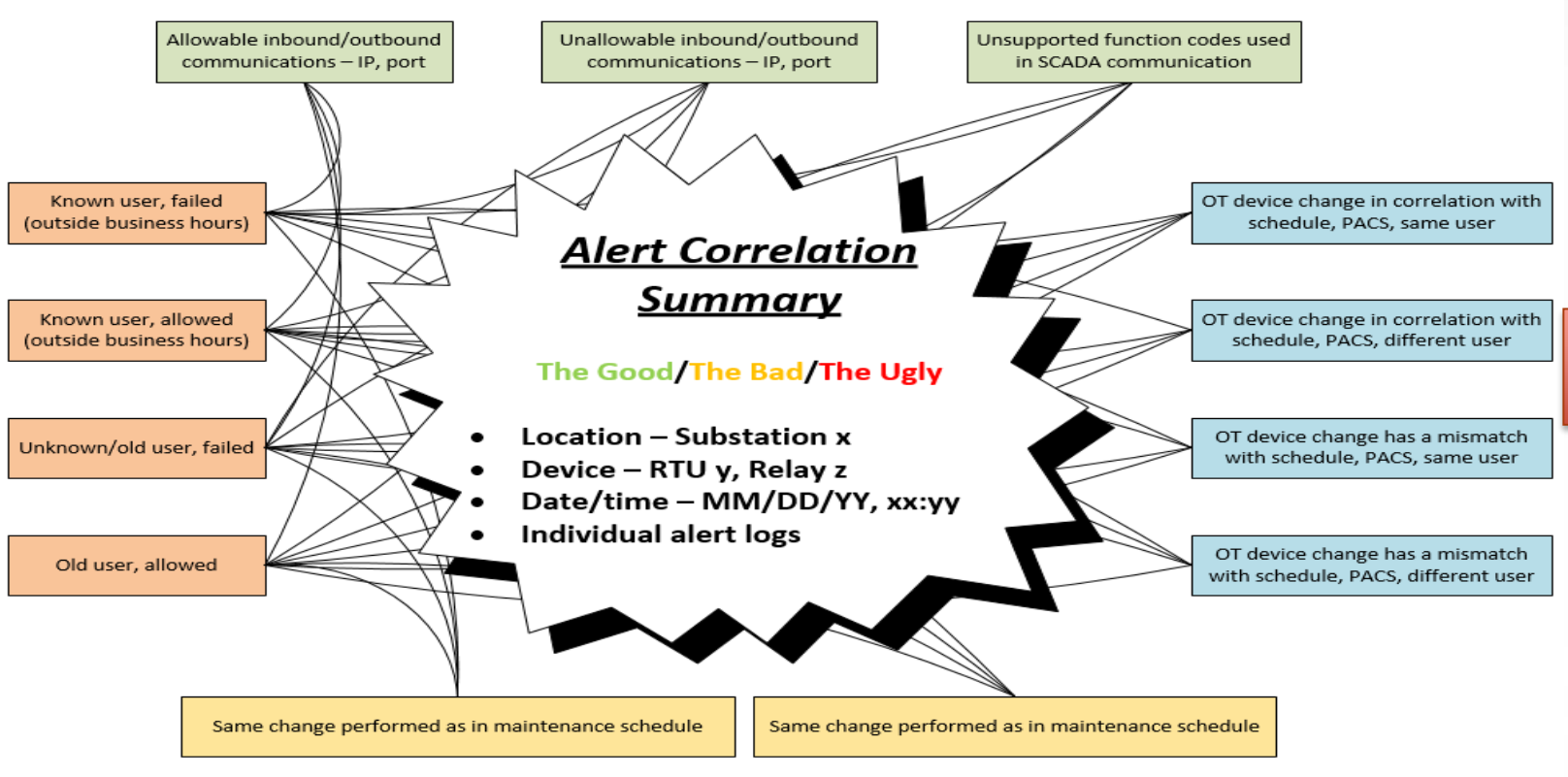
- 4,400 scientists, engineers and non-technical staff
- Mission-driven collaborations with government, academia and industry

Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Purpose: Define information that should be displayed to utility operators to increase their awareness of cybersecurity.

Correlating IT & OT logs to produce actionable alerts



Dashboard for Operators & Engineers

SSASS-E: Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Goal:

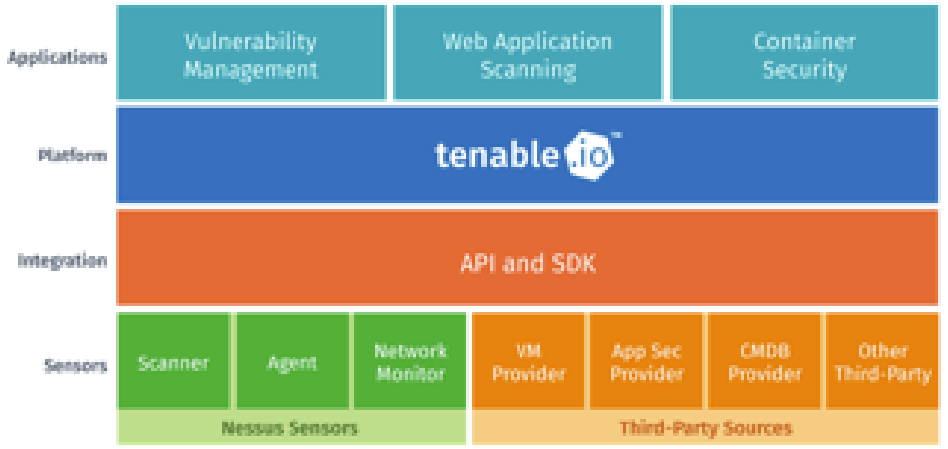
PNNL proposes to develop **a Safe and Secure Autonomous Scanning Solution for Energy Delivery Systems (**SSASS-E). This novel solution will develop, validate, and verify innovative safe scanning methodology, models, architectures and produce a prototype to transform that most widely deployed vulnerability scanner in the IT space to secure Energy Delivery System (EDS) technology.

NRECA
A Touchstone Energy Cooperative

P.U.D. CHELAN COUNTY

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

tenable™



SSASS-E: Advancing the State of the Art

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

State of Art

- Do not provide continuous monitoring
- Can cause disruption and degradation of service
- Do not provide combined vulnerability analysis and scanning across IT/OT

Requirements

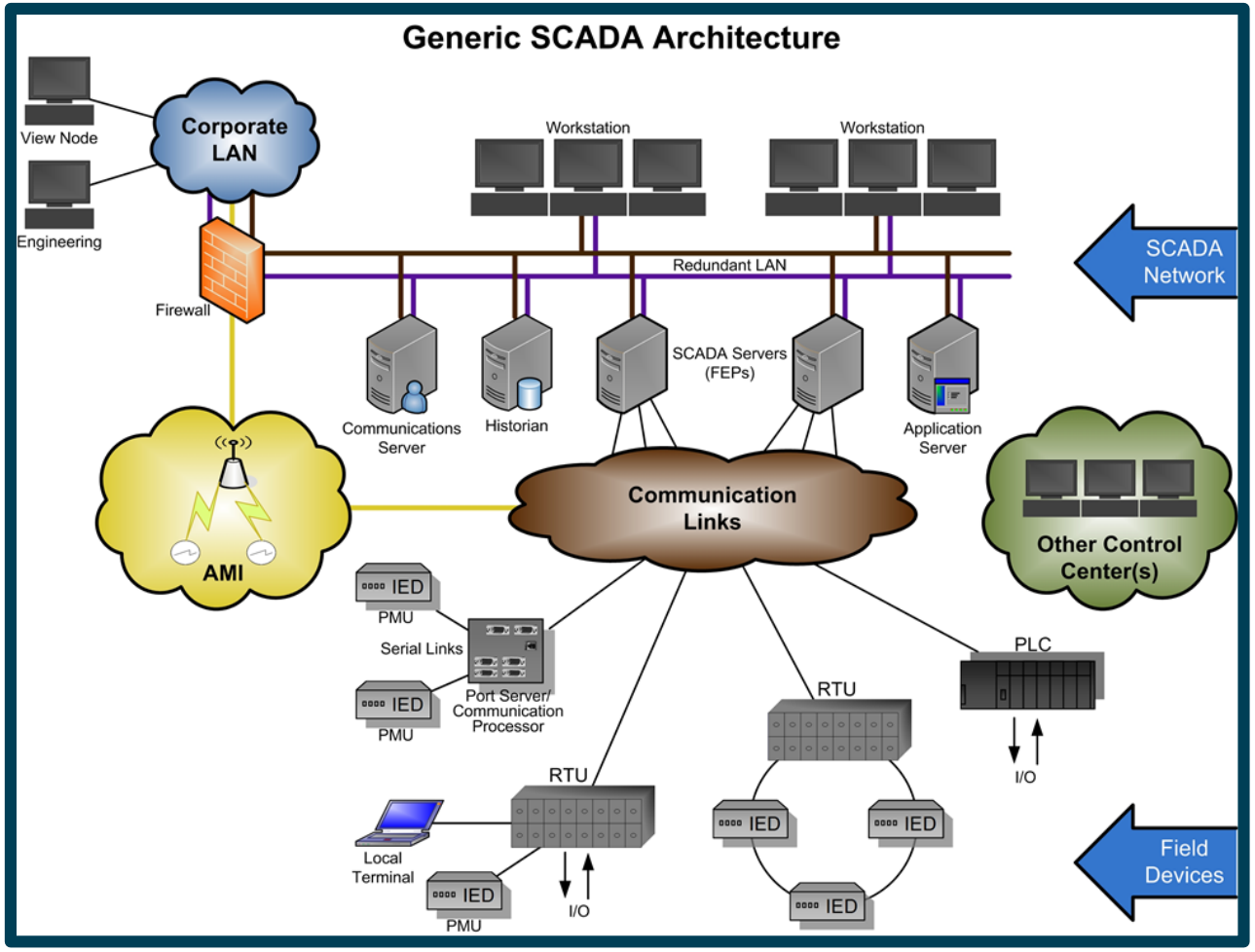
- Solutions for real-time vulnerability analysis & monitoring of EDS
- Owners/operators need tech to safely and continuously scan EDS (IT and OT) for evolving or emerging threats
- Utilities need a way to discover all critical cyber assets & manage vulnerabilities holistically

SSASS-E

- Provides improved methodology & technology for continuous monitoring of legacy and advanced critical IT/OT assets
- Provides a continuous monitoring solution that is safe, secure, and effectively eliminates blind spots in OT assets
- Applies to EDS and Oil & Natural Gas

SSASS-E: Preliminary technical plan

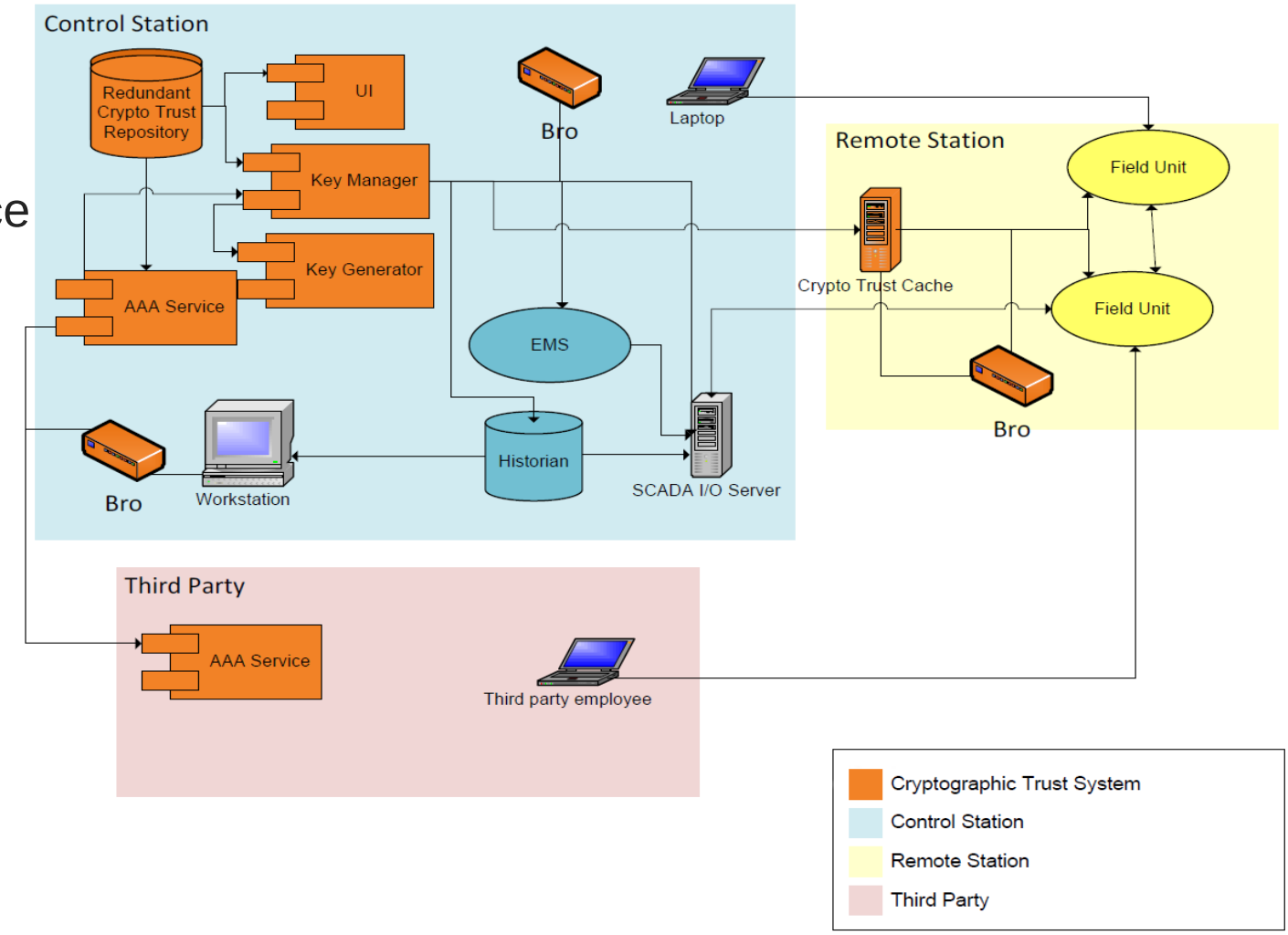
- **Active scanning:** Interrogate and query a device; OS identification; might be limited (active against telemetry systems)
- **Passive scanning deep packet**: Given knowledge of protocol and system, infer information
- **Passive scanning header/ broadcast**: Listen for broadcast and multicast traffic
- **Out of band**: Authenticated query of engineering access to device & existing or queried configuration files (active against engineering systems)



Automated Disruption-Tolerant Key Management

- Objective: Design a key management system to meet the unique requirements of EDS
  - Disruption-tolerant
  - Centrally-managed
  - Automated key management service for devices
  - Self-monitoring system
  - Integrated enterprise security
  - Increase assurance of 3rd-party connections

- Challenges in current approach
  - PKI
    - Revocation (CRL/OCSP)
    - Cost of management
  - Web of Trust
    - Completely distributed
    - No central control



Validation and Verification

- Key management often fails in edge case situations
  - Create list of normal and edge case scenarios
  - Instantiate models of scenarios in test environment
  - Empirically study performance
  - Comparative analysis of other key management systems
    - IEC-62351, NISTIR 7628, etc

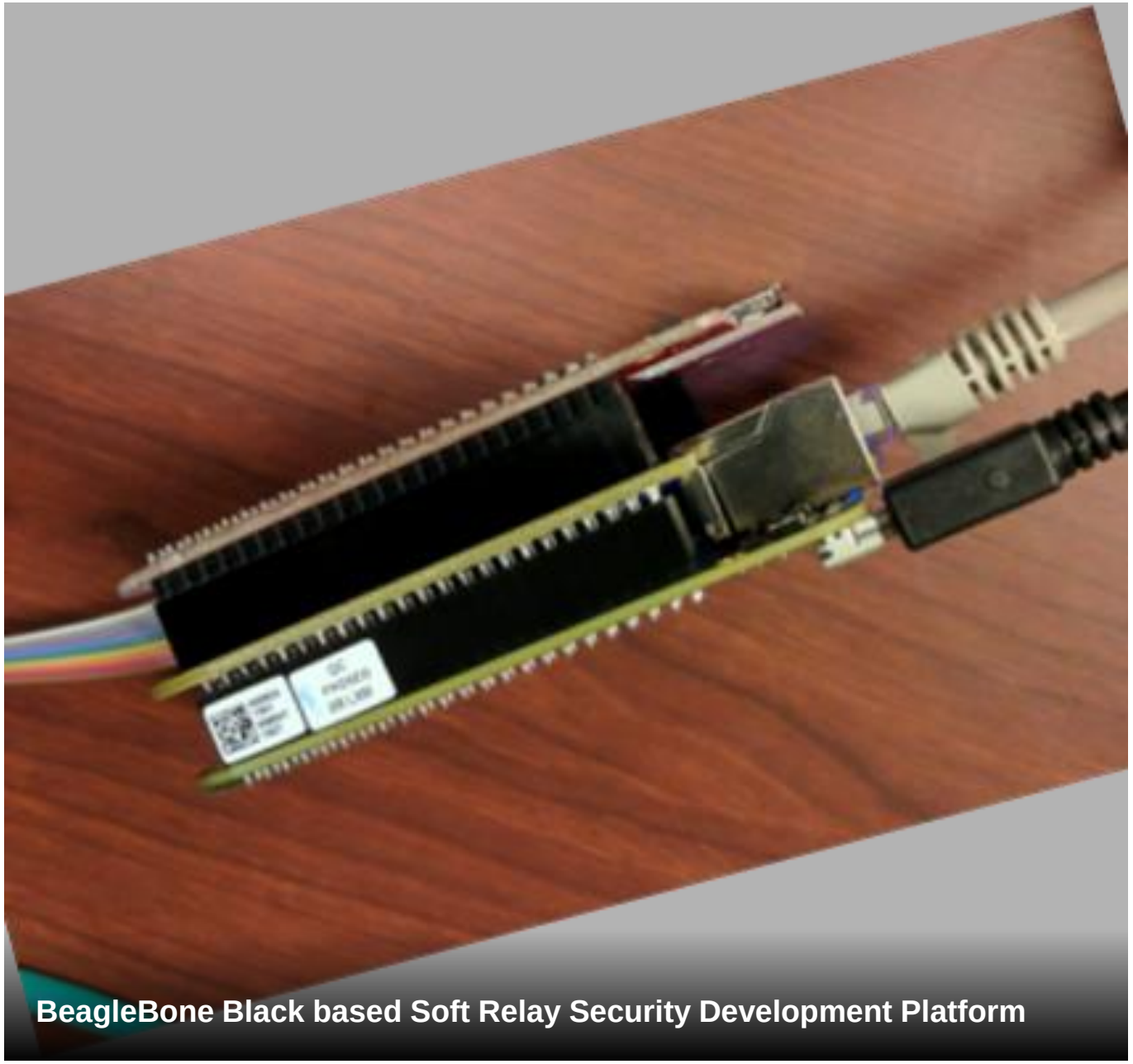
Testing Overview

- Goals
  - Exercise prototype under various conditions
  - Empirically understand performance
  - Provide comparative performance analysis to support utilization decisions
- Three phases of testing
  - Baseline (no security applied with real equipment)
  - ADTKM prototype (test functions of various ADTKM prototype features)
  - IEC 62351 implementation (test behavior/performance of PKI based solution for comparison)
- Categories of testing
  - Functionality testing
  - Performance testing
  - Security testing

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Project Outcomes

- Open Source code
  - https://github.com/pnnl/ADTKM (Coming soon)
- Open Source Development Platform
- Technical report of testing results and lessons learned
- Multiple publications in process

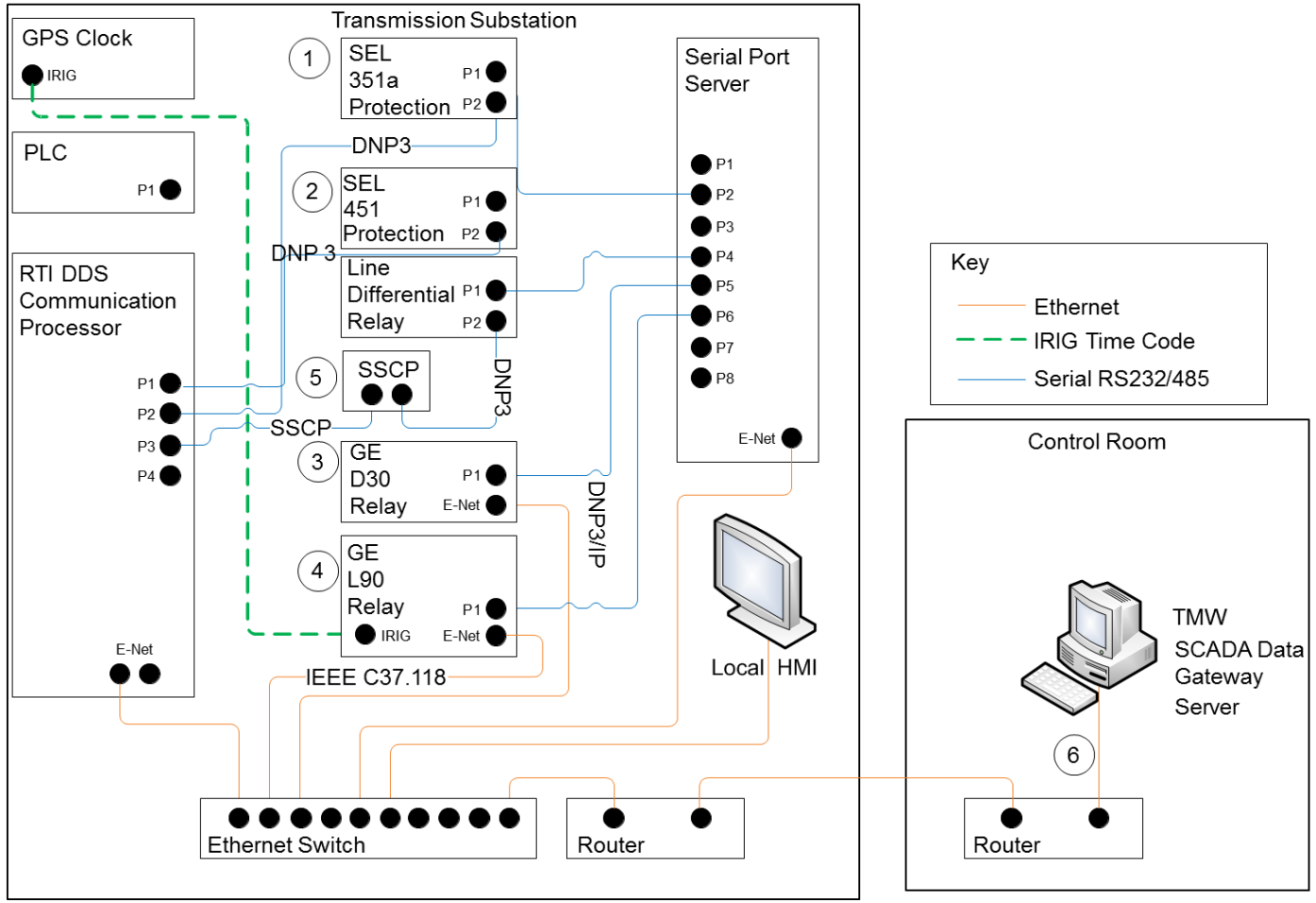


BeagleBone Black based Soft Relay Security Development Platform

Testbed Uses

- Technology assessment and prototyping
- Simulation and modeling, verification, and validation
- Experimentation
- Demonstration
- Training and education

Use Case RTI



General Questions

- How do you test new procurements today?
- How do you test for security today?
- Do you have HIL/real-time simulators?
- Any reference models that you use?
- What do you want out of a test environment?

Relevant Tests or Questions

- What sort of tests or questions would you pose to such an environment?
  - Upgrades
  - Security testing
  - Interoperability
  - Reliability
  - Interaction with Grid

Engagement Continuum

- Onsite co-experimentation
- Remote access testing
- Batch submission of questions/concerns to explore
- Review/read results

Energy Delivery Systems Cyber Security Research Showcase at PNNL

- 2 Control Centers
- Power Electronics Lab
- Interoperability Room
- Outdoor Test Pad
- Campus Control Center
- A ‘Living Laboratory’ Building

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Thank you

Mark Rice
Research Engineer
509-375-2435
Mark.Rice@pnnl.gov