# National Cybersecurity Center of Excellence

## Energy Sector Projects

National Cybersecurity Awareness Month Webinar
10/23/2018

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

# National Cybersecurity Awareness Month 2018

- Collaborative effort between government and industry

- Goal: Raise cybersecurity awareness and strengthen public and private engagement through events

- Week 4 Theme: Safeguarding the Nation's Critical Infrastructure

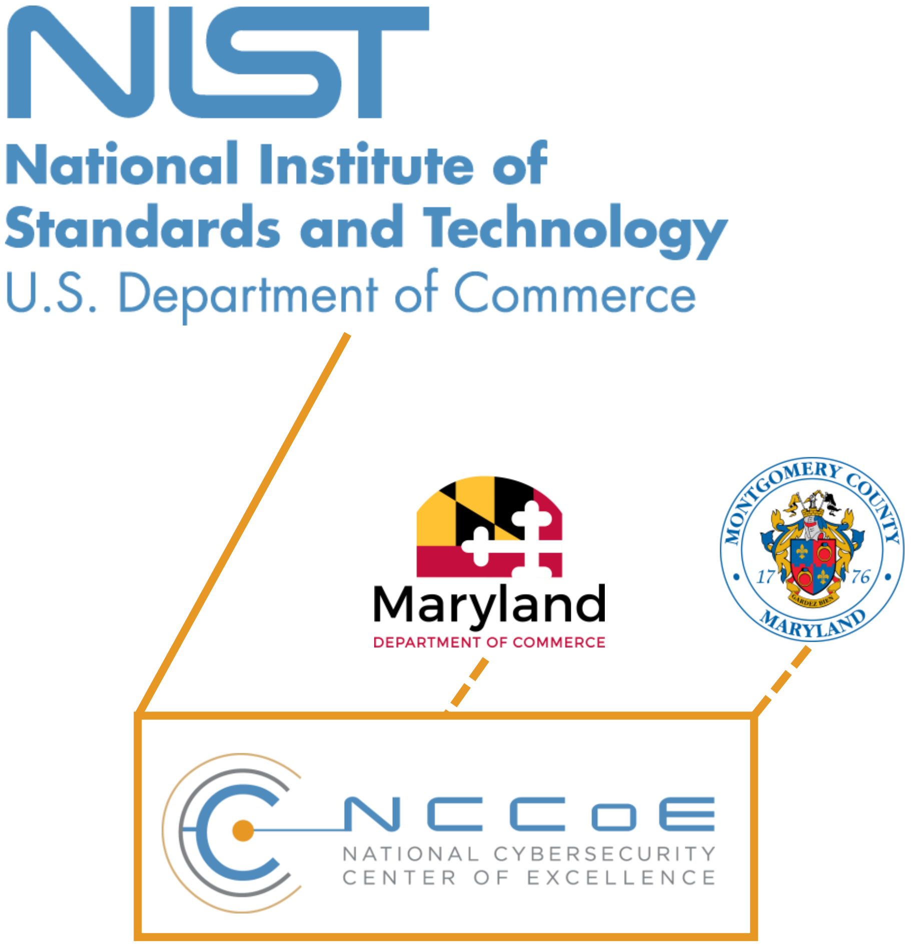
- Additional Cybersecurity Awareness Month Resources:
    - https://www.nist.gov/topics/cybersecurity/national-cyber-security-awareness-month

# 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.


NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Maryland
DEPARTMENT OF COMMERCE
MONTGOMERY COUNTY MARYLAND 17 76
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# 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

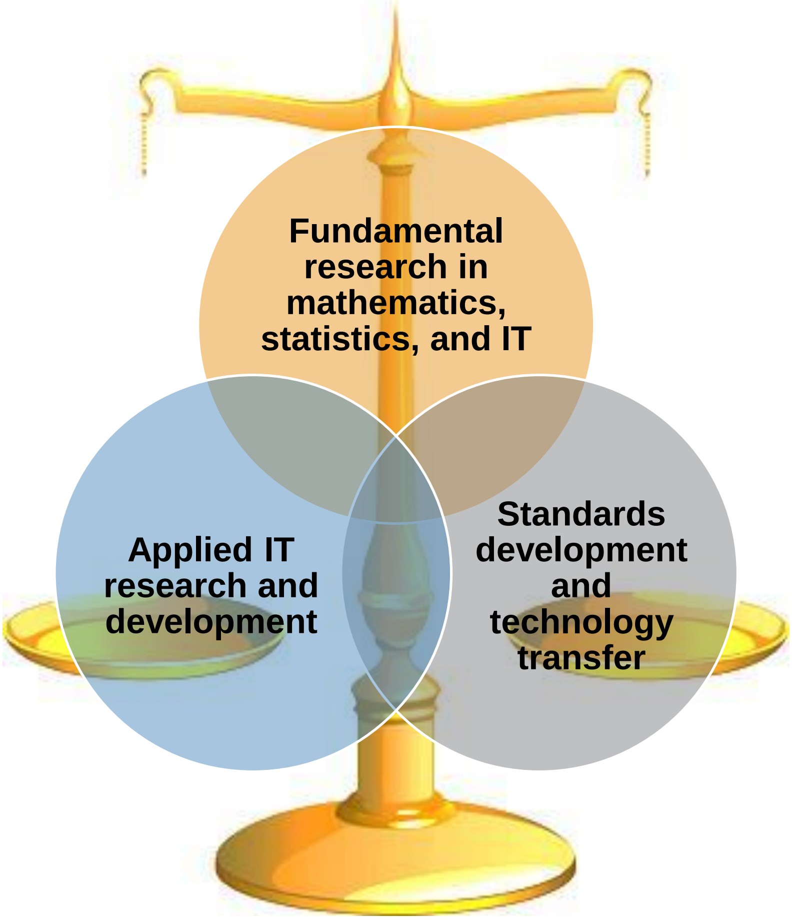
## Cultivating Trust in IT and Metrology through measurements, standards and tests

### ITL Programs

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

### Collaborations with

- Industry
- Federal/State/Local Governments
- Academia


Fundamental research in mathematics, statistics, and IT
Applied IT research and development
Standards development and technology transfer

# 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

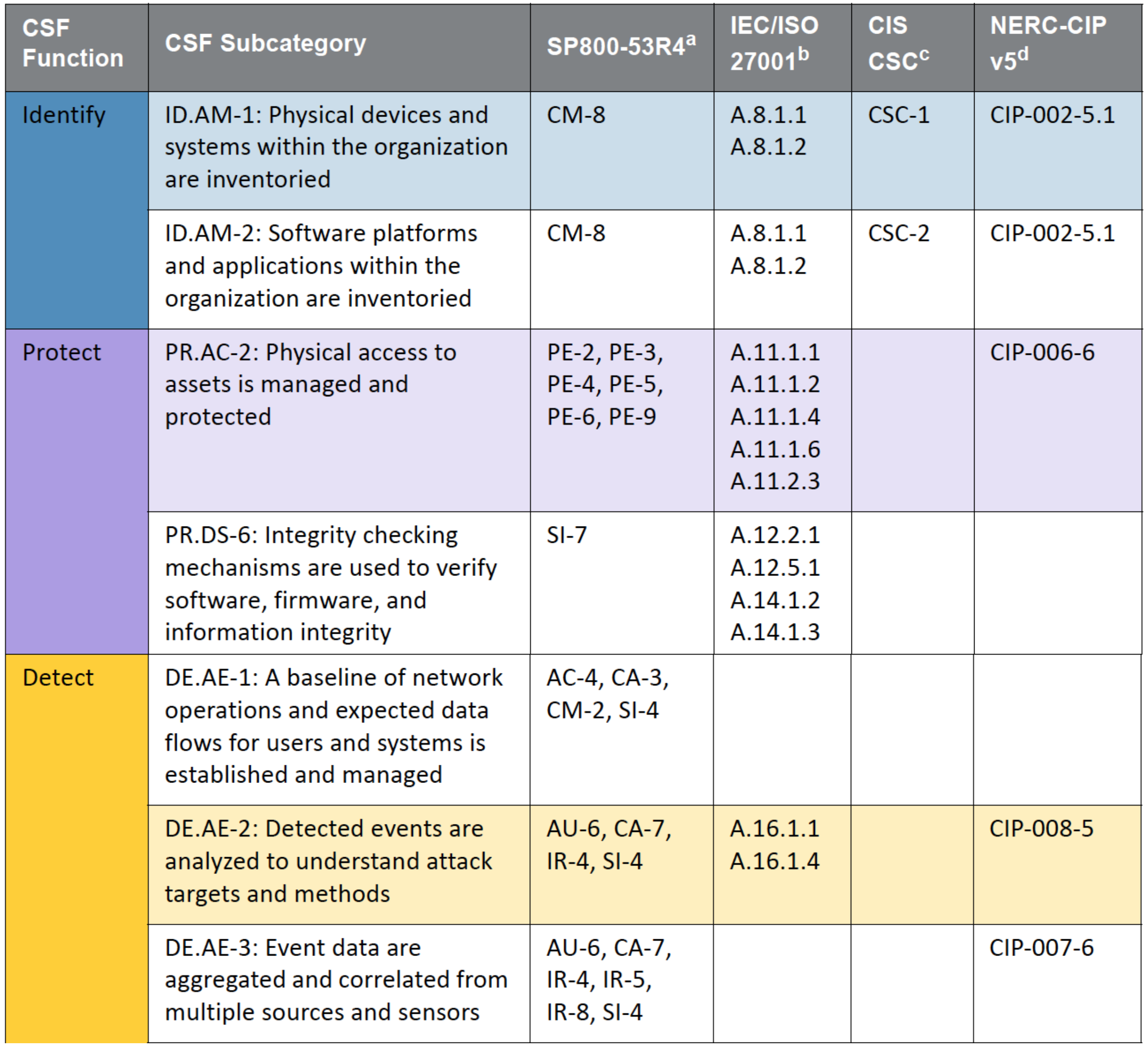
- High-level overview of the project, including summaries of the challenge, solution, and benefits

## 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

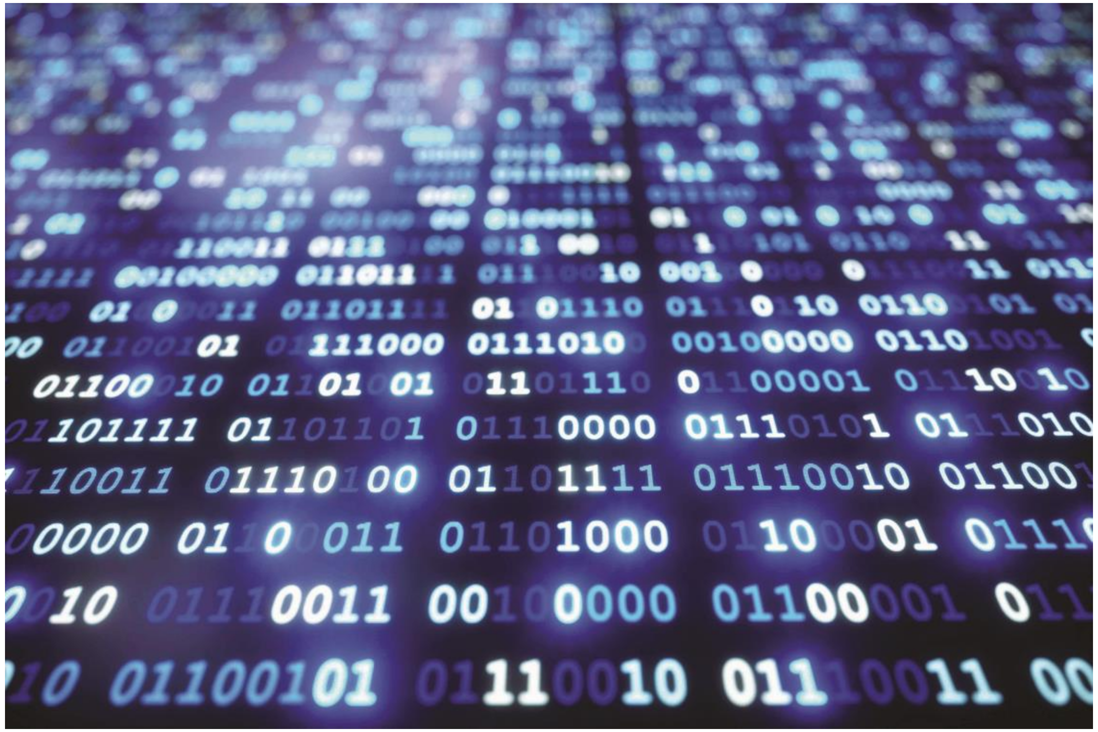
## Volume C: How-To Guide

- 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<br>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<br>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<br>A.11.1.2<br>A.11.1.4<br>A.11.1.6<br>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<br>A.12.5.1<br>A.14.1.2<br>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<br>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

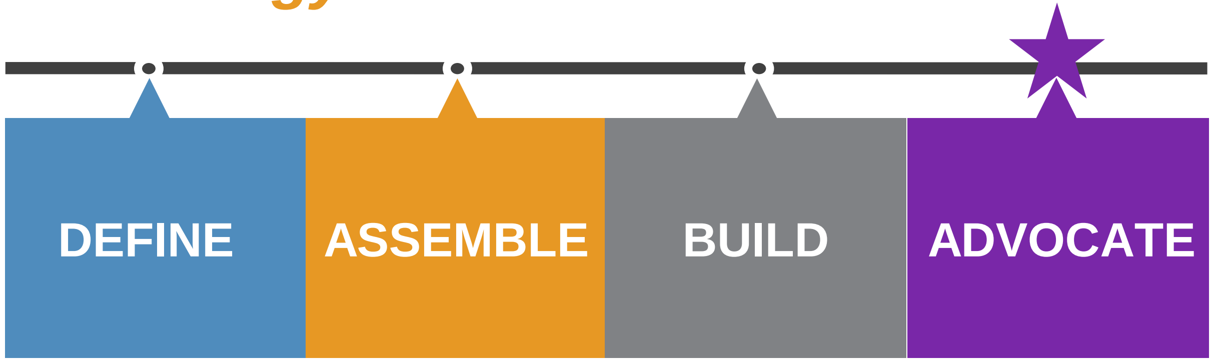
Email us at energy_nccoe@nist.gov

# 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

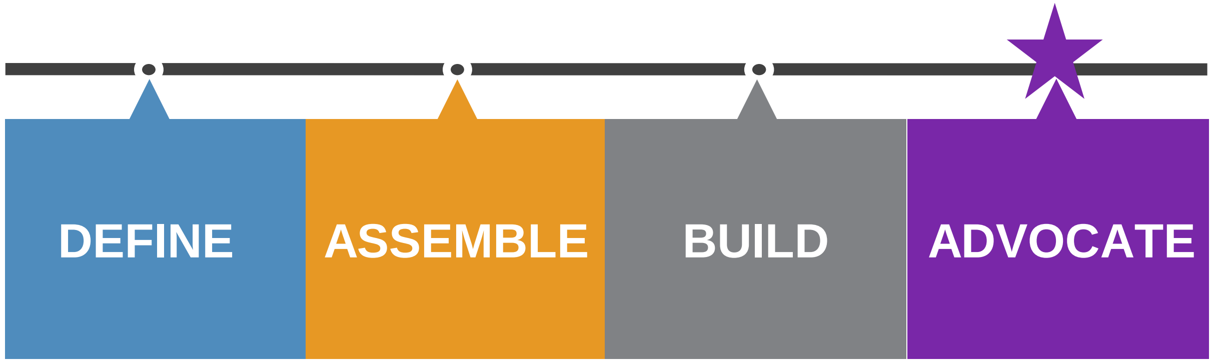
- Download NIST SP 1800-2, Identity and Access Management for Electric Utilities
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

# 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

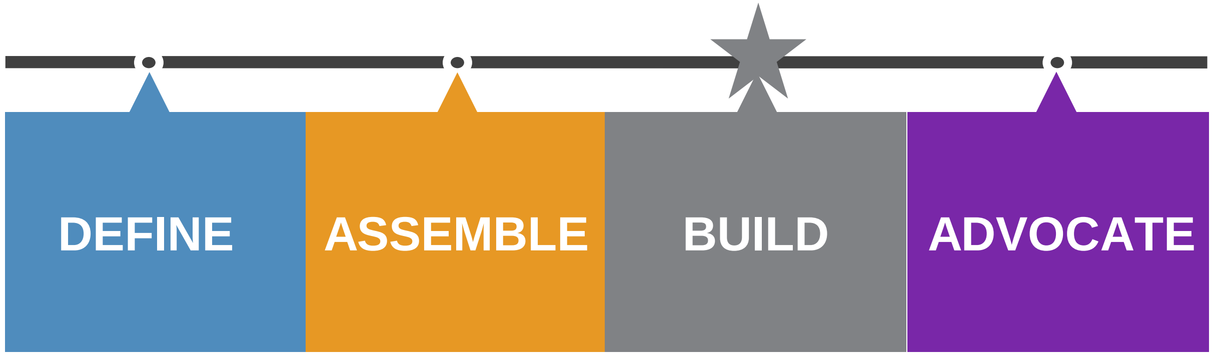
- Read SP 1800-7 Situational Awareness for Electric Utilities Practice Guide Draft
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

# 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.



DEFINE ASSEMBLE BUILD ADVOCATE

## 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 |

# 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

DRAGOS

ForeScout

FOXGUARD SOLUTIONS

KORE®

splunk>

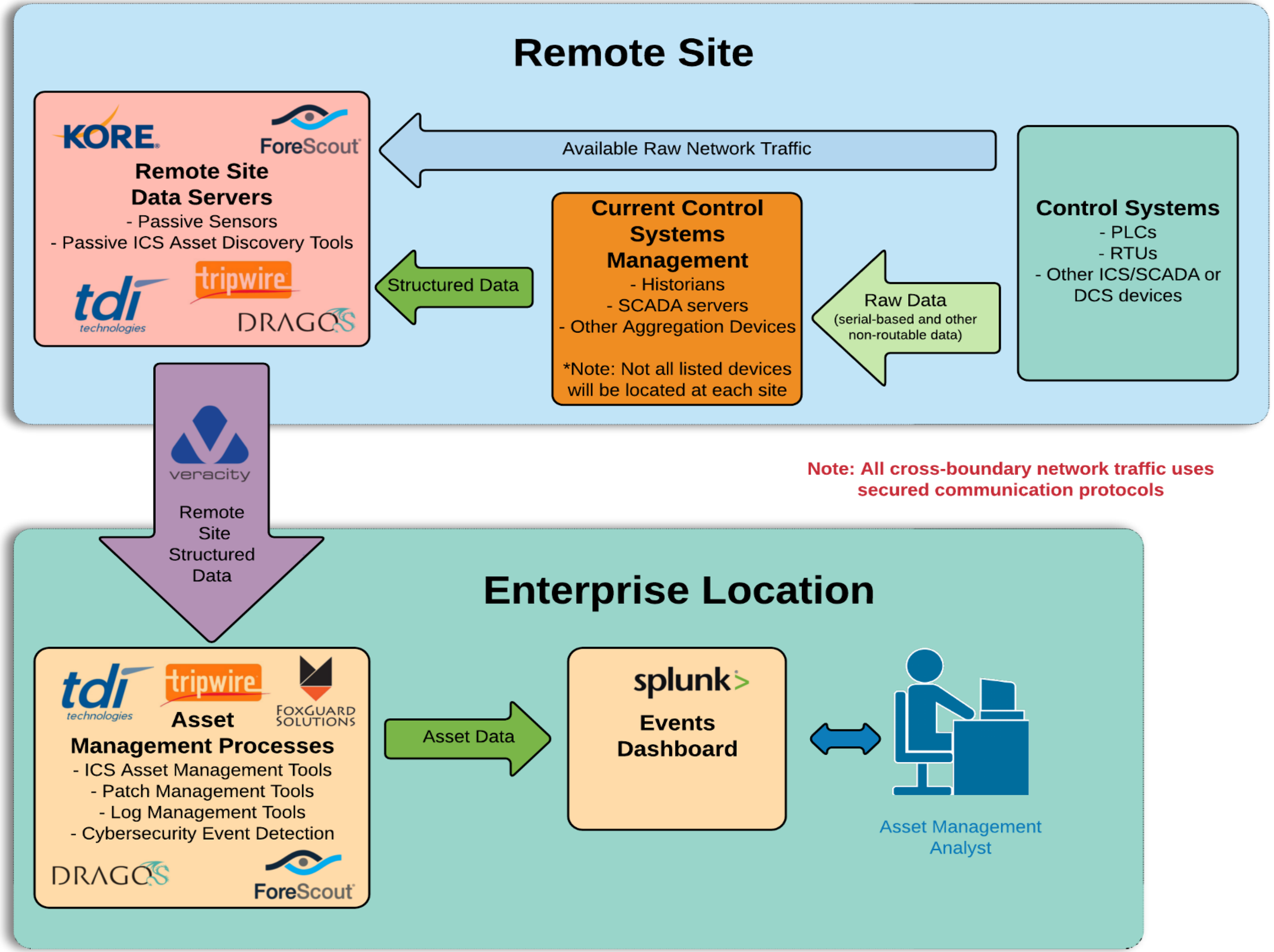
tdi technologies

tripwire

UNIVERSITY OF MARYLAND

VERACITY INDUSTRIAL NETWORKS

# ESAM Flow Diagram

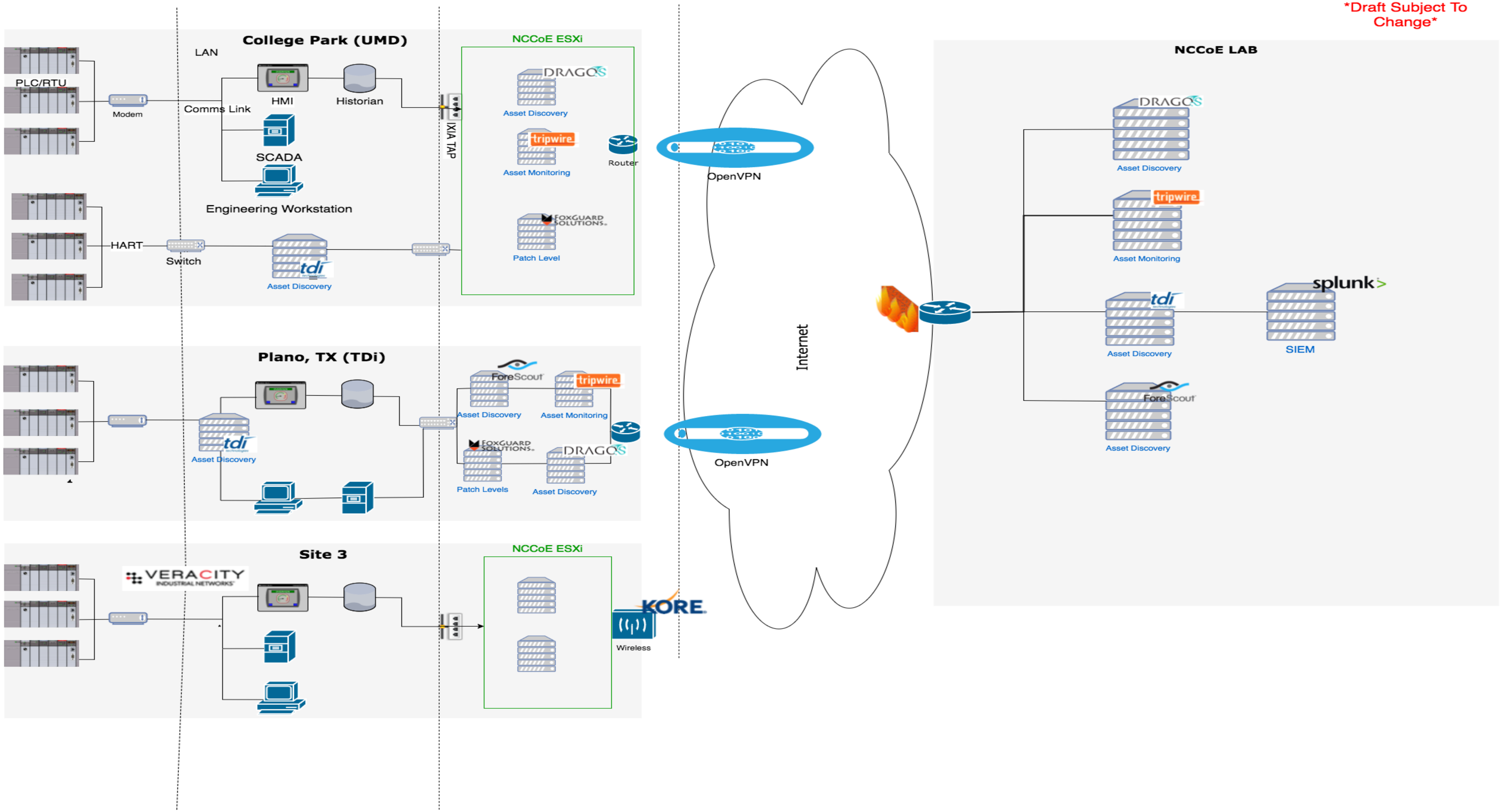


Remote Site
KORE
ForeScout
Remote Site Data Servers
- Passive Sensors
- Passive ICS Asset Discovery Tools
tdi technologies
tripwire
DRAGOS
Available Raw Network Traffic
Structured Data
Current Control Systems Management
- Historians
- SCADA servers
- Other Aggregation Devices
*Note: Not all listed devices will be located at each site
Raw Data (serial-based and other non-routable data)
Control Systems
- PLCs
- RTUs
- Other ICS/SCADA or DCS devices
veracity
Remote Site Structured Data
Enterprise Location
tdi technologies
tripwire
FOXGUARD SOLUTIONS
Asset Management Processes
- ICS Asset Management Tools
- Patch Management Tools
- Log Management Tools
- Cybersecurity Event Detection
DRAGOS
ForeScout
Asset Data
splunk>
Events Dashboard
Asset Management Analyst

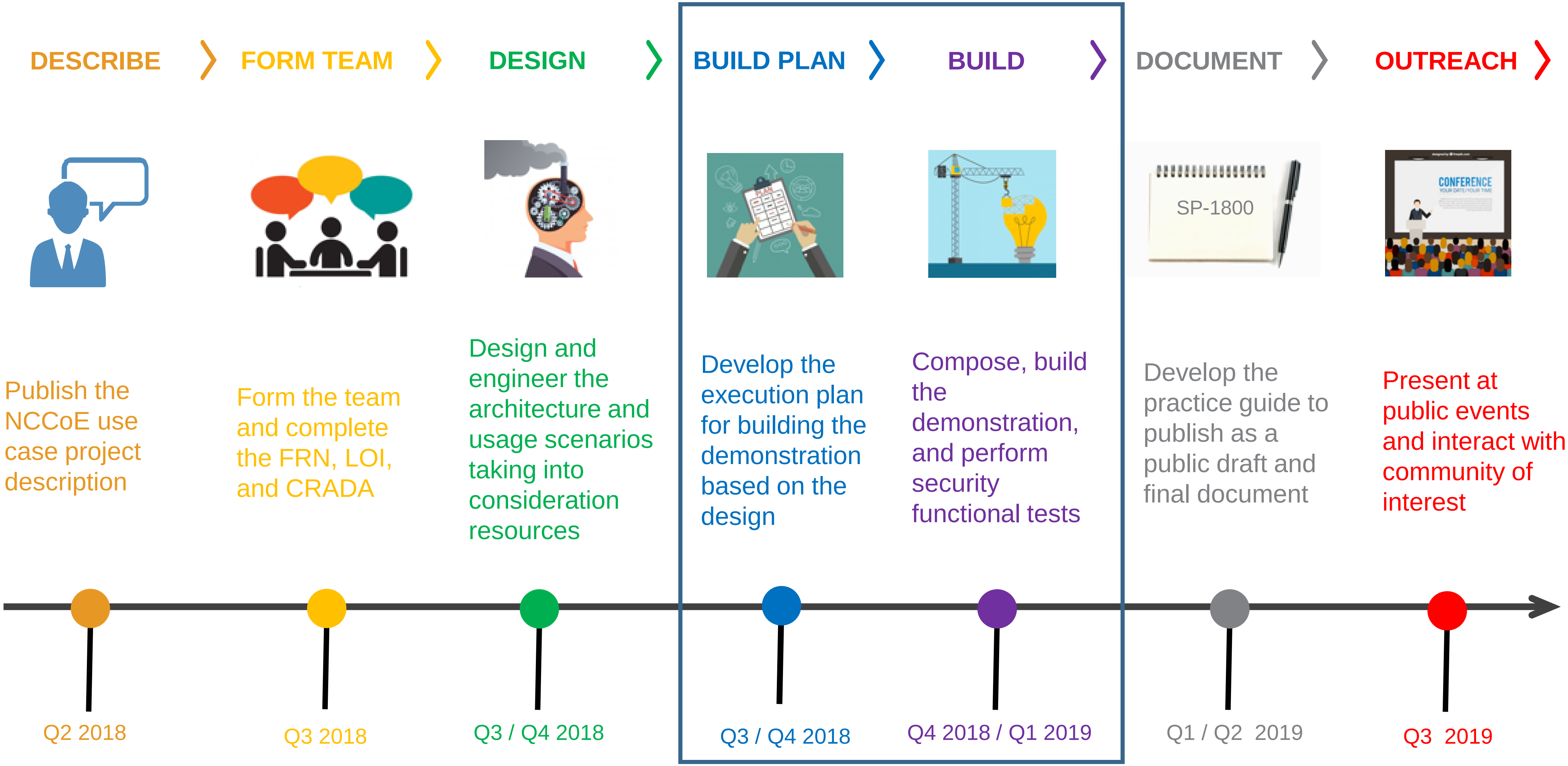
Note: All cross-boundary network traffic uses secured communication protocols

# ESAM Build Architecture to Date

*Draft Subject To Change*



# ESAM Project Execution Timeline



**DESCRIBE**

Publish the NCCoE use case project description

Q2 2018

**FORM TEAM**

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

Q3 2018

**DESIGN**

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

Q3 / Q4 2018

**BUILD PLAN**

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

Q3 / Q4 2018

**BUILD**

Compose, build the demonstration, and perform security functional tests

Q4 2018 / Q1 2019

**DOCUMENT**

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

Q1 / Q2 2019

**OUTREACH**

Present at public events and interact with community of interest

Q3 2019

# Industrial Internet of Things (IIoT)

## Previous Involvement

- CXO Roundtable: Industrial Control Systems (ICS) Cybersecurity Challenges
- GridSecCon: Asset Management for Energy Providers Training – IIoT Panel Discussion

## Collaborate with us!

Email energy_nccoe@nist.gov

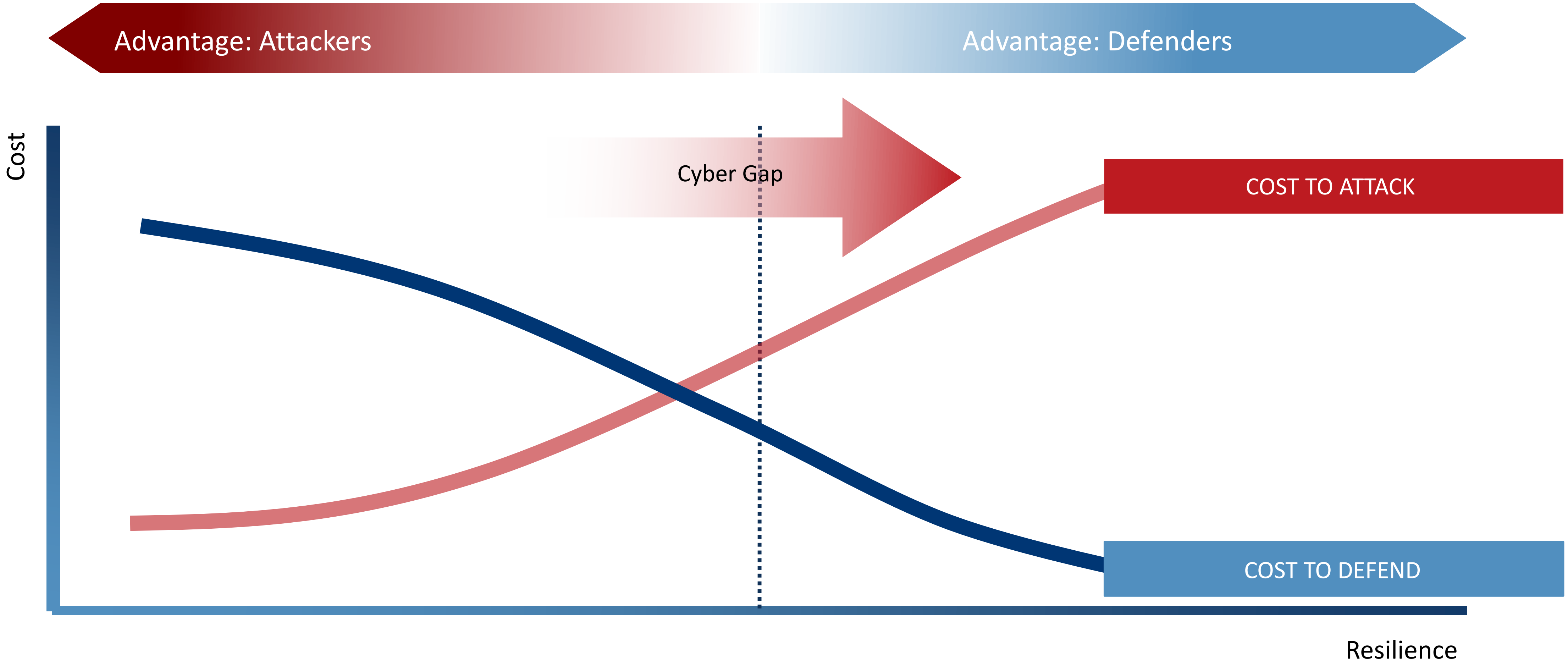
# Considerations for End-to-End Trust In the "IIoT"

BlackRidge
TECHNOLOGY

*NCCoE  Webinar – October 23, 2018*
*John Walsh - Chief Strategy and Technology Officer*
*Michael Murray - SVP & GM Cyber Physical Systems*

www.blackridge.us

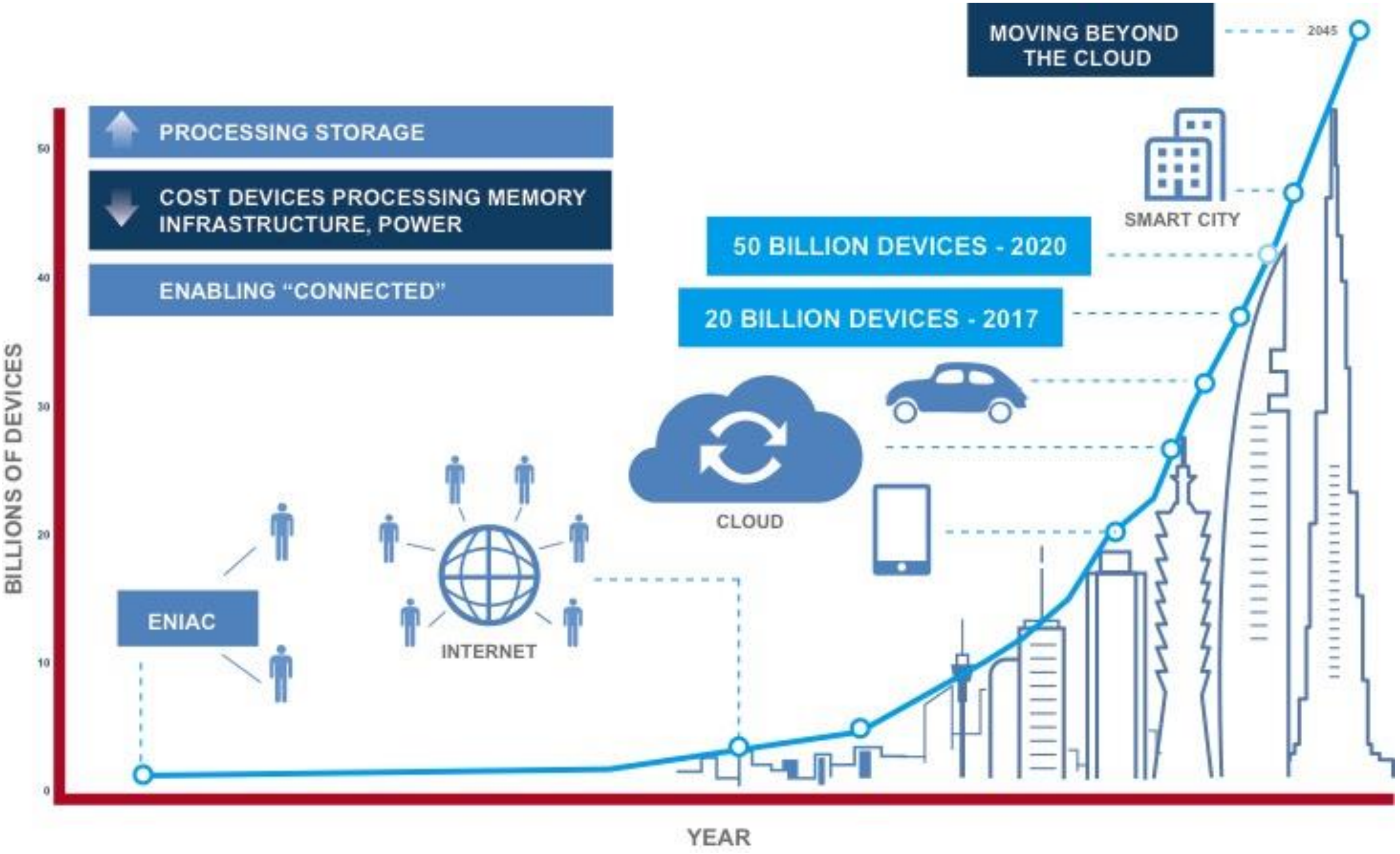
# End Game: Resilient Architectures Require Economic Asymmetry



BlackRidge TECHNOLOGY

# Expansion of Smart Devices And Systems Across Diverse Sectors

Was…"Sensor to Cloud."  Now… "Data/Analytics Density, Velocity, and Cost."

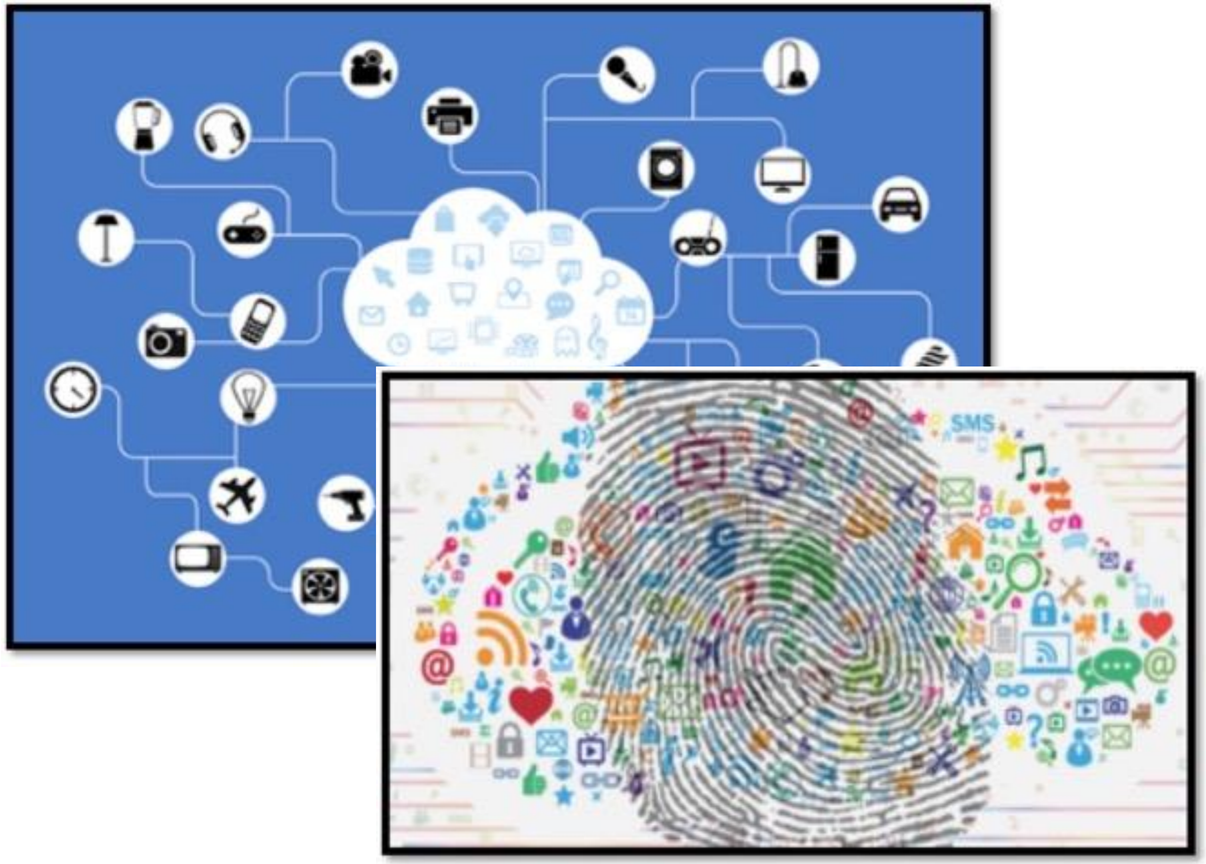


***IPV6 325 Trillion Trillion Trillion Identities……  Enabling Anonymity and Challenging Security in Cyber Space …. And What About 5G and Low Power Wireless.***

BlackRidge TECHNOLOGY

# Trust From Point to Point - “ Transport Identity”

- Creating New Outcomes On The Basis of The “Relationships of Things”
- Value Propositions - Economic Sustainability, Equipment Up-Time, Ease of Use, …….
- New Value Chains and Emerging Micro Services Require Trust – “Systems of Systems”
- Integrating IT/OT – “Security Stack”; Analytics; Incident Response….
- Complexity and Lack of Feature Scale-ability of Existing Security Approaches.
- Growing Recognition of the Threats and Liabilities
- Many Considerations on Data: Rights Management, Monetization, Protection / Privacy, Uses…..



- **Driving IT / OT Convergence and Brownfield Compatibility**
- **Was Security “Edge to Cloud” now Trust “Point to Point” (Zero Trust Architectures)**
- **NIST 800-160 Security Guide for Systems of Systems**

Homeland Security

US-CERT United States Computer Emergency Readiness Team

THE WHITE HOUSE WASHINGTON

PRESIDENTIAL EXECUTIVE ORDER ON STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

## Security Tip (ST18-001) Securing Network Infrastructure Devices

NCCIC encourages users and network administrators to implement the following recommendations to better secure their network infrastructure:

- ***Segment and segregate networks and functions.***
- ***Limit unnecessary lateral communications.***
- Harden network devices.
- ***Secure access to infrastructure devices.***
- ***Perform Out-of-Band network management.***
- Validate integrity of hardware and software.

## Segment and Segregate Networks and Functions

Security architects must consider the overall infrastructure layout, including segmentation and segregation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network.

## Technical Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

# Industrials and Utilities Leading The Way

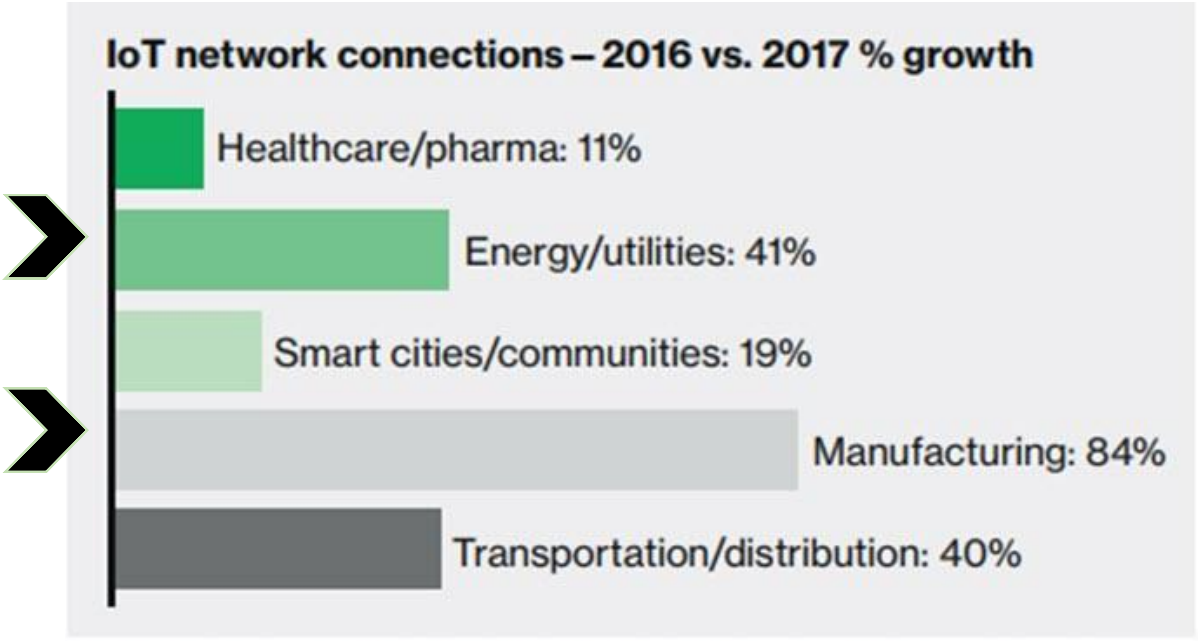
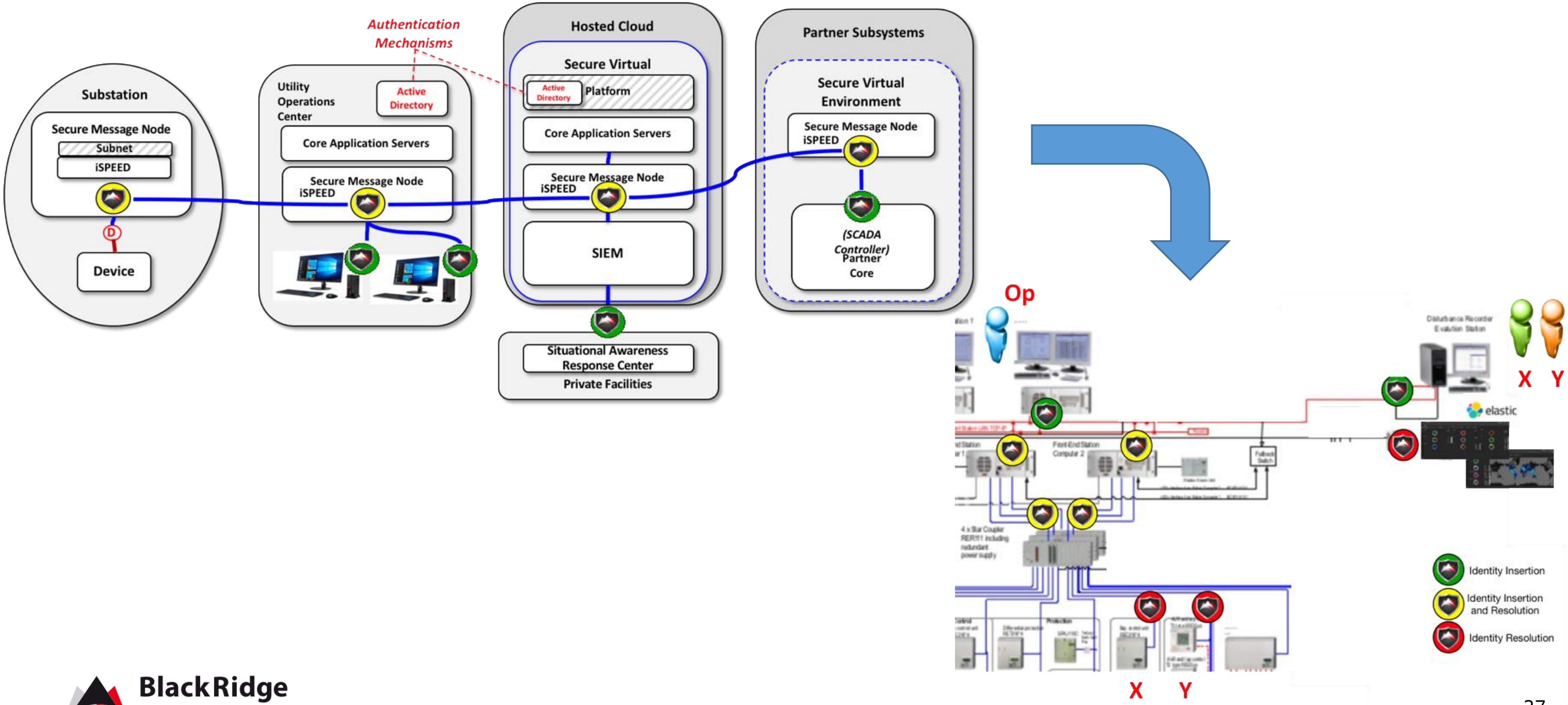


Figure 1: Year-on-year growth in Verizon IoT network connections

- Utilities connections growth 41% 2017
- Industrial segment of the Internet of Things (IIoT) growth is projected to grow 24% CAGR
- Security spending in the OT - 40% CAGR
- Brownfield to be greatest target
- Largest deficit for IT / cyber talent

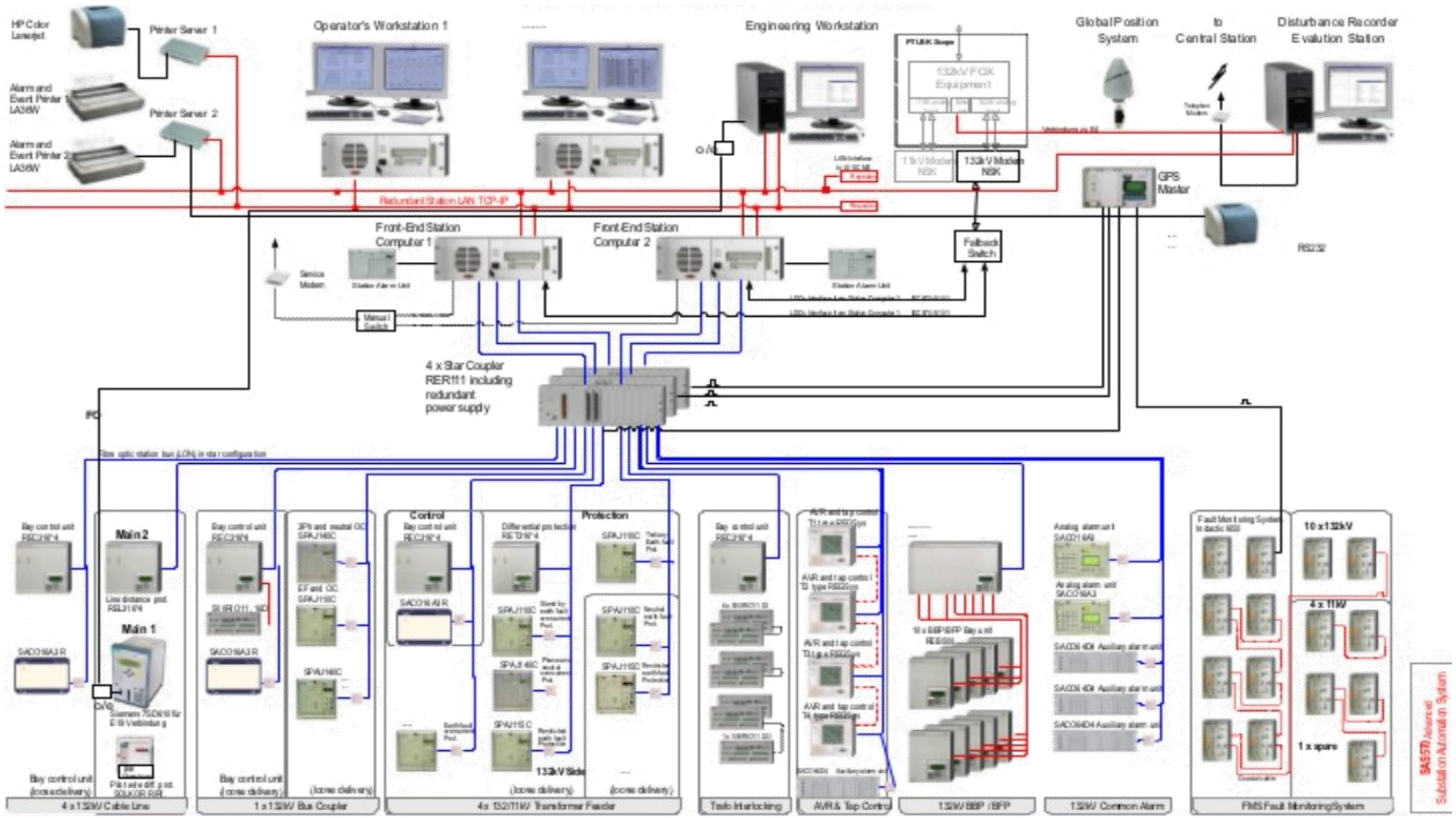
# We Can Accomplish A Lot With Proper Micro-Segmentation and Isolation



BlackRidge TECHNOLOGY

# Segmentation/Segregation of Legacy 0,1,2 layers

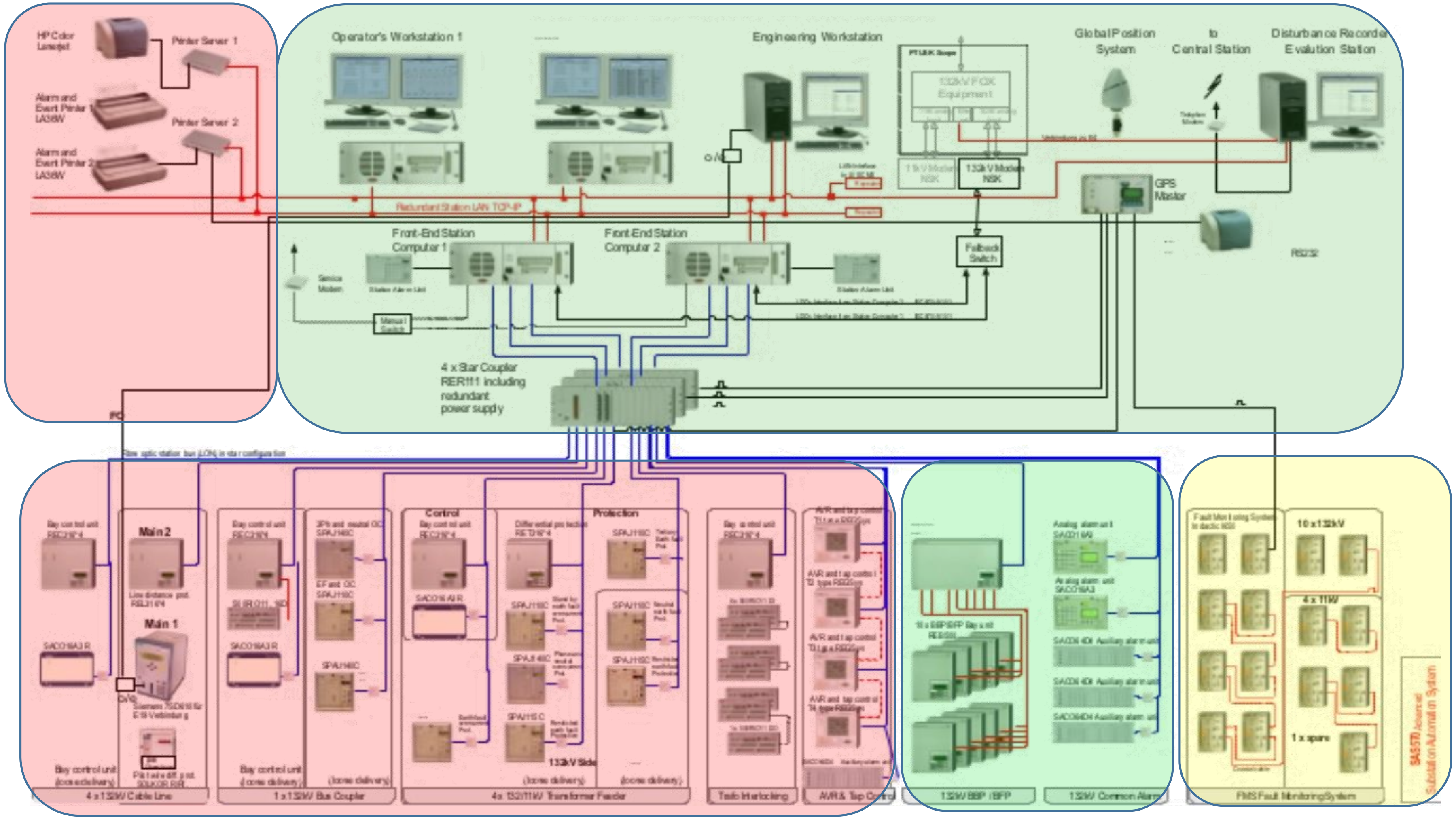
Legacy Systems are a tapestry of older sensors, controllers and trust policies.



HP Color Laserjet
Printer Server 1
Alarm and Event Printer 1 LA36W
Printer Server 2
Alarm and Event Printer 2 LA36W
Operator's Workstation 1
Redundant Station LAN TCP-IP
Engineering Workstation
132kV FOX Equipment
11kV Modem NSK
132kV Modem NSK
Global Position System
to Central Station
Disturbance Recorder Evalution Station
GPS Master
RS232
Front-End Station Computer 1
Front-End Station Computer 2
Service Modem
Station Alarm Unit
Manual Switch
Fallback Switch
4 x Star Coupler RER111 including redundant power supply
Fibre optic station bus (LON) in star configuration
Bay control unit REC316*4
Main 2
Line distance prot. REL316*4
Main 1
SACO16A3 R
Siemens 7SD610 for E18 Verbindung
Pilot wire diff. prot. SOLKOR R/R
Bay control unit (loose delivery)
4 x 132kV Cable Line
3Ph and neutral OC SPAJ140C
EF and OC SPAJ110C
SPAJ140C
(loose delivery)
1 x 132kV Bus Coupler
Control
Protection
Differential protection RET316*4
SPAJ110C
SPAJ115C
SACO16A1 R
132kV Side
4x 132/11kV Transformer Feeder
Trafo Interlocking
AVR and tap control
AVR & Tap Control
10 x BBP/BFP Bay unit REB500
132kV BBP / BFP
Analog alarm unit SACO16A3
SACO64D4 Auxiliary alarm unit
132kV Common Alarm
Fault Monitoring System
10 x 132kV
4 x 11kV
1 x spare
FMS Fault Monitoring System
SAS570 Advanced Substation Automation System

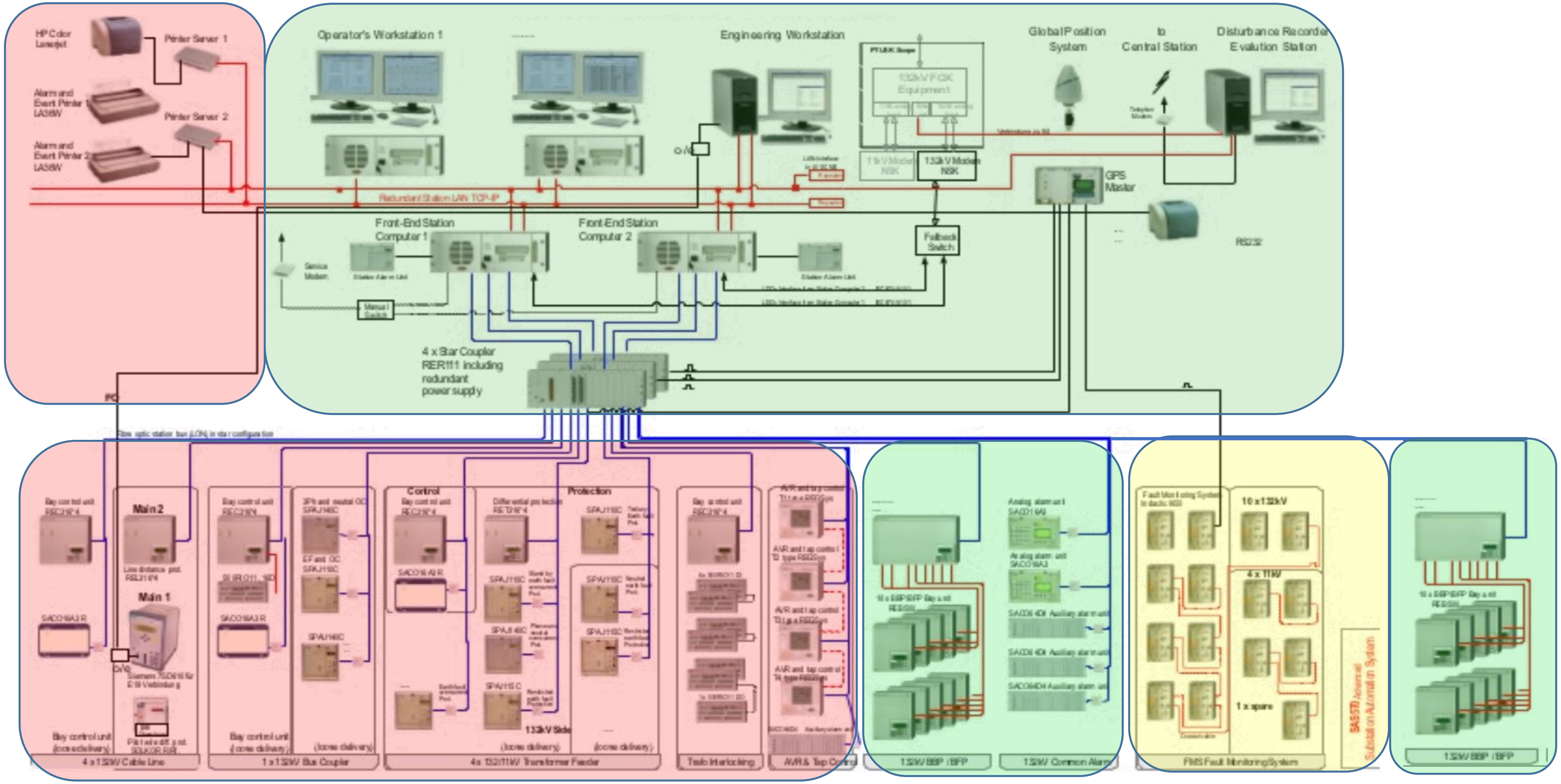
# Segmentation/Segregation of all Layers

New Systems can exist with legacy systems through Segmentation and Segregation.



# Segmentation/Segregation of New Systems

Policy and rule engines can be dynamically adapted based on pedigree and providence of authenticated data as new systems and architectures are added or adapted.



HP Color Laserjet
Printer Server 1
Alarm and Event Printer 1 LA36W
Printer Server 2
Alarm and Event Printer 2 LA36W
Operator's Workstation 1
Engineering Workstation
132kV FOX Equipment
Global Position System
to Central Station
Disturbance Recorder Evaluation Station
Redundant Station LAN TCP-IP
11kV Modem NSK
132kV Modem NSK
GPS Master
Front-End Station Computer 1
Front-End Station Computer 2
Service Modem
Station Alarm Unit
Manual Switch
Fallback Switch
RS232
4 x Star Coupler RER111 including redundant power supply
FO
Bay control unit REC316*4
Main 2
Line distance prot. REL316*4
Main 1
SACO16A3 R
Siemens 7SD610 für E/S Verbindung
Bay control unit (core delivery)
Pilot wire diff. prot. SOLKOR R/Rf
4 x 132kV Cable Line
SPAJ140C
EF and OC SPAJ110C
1 x 132kV Bus Coupler
Control
Protection
Differential protection RET316*4
SPAJ110C
SPAJ115C
132kV Side
(core delivery)
4x 132/11kV Transformer Feeder
AVR and tap control
Trafo Interlocking
AVR & Tap Control
10 x BBP/BFP Bay unit REB500
132kV BBP / BFP
Analog alarm unit SACO16A3
SACO64D4 Auxiliary alarm unit
132kV Common Alarm
Fault Monitoring System
10 x 132kV
4 x 11kV
1 x spare
FMS Fault Monitoring System
SAS570 Advanced Substation Automation System

BlackRidge TECHNOLOGY

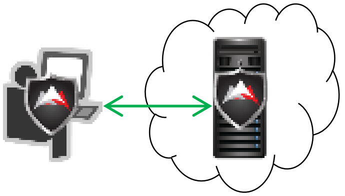
# What Can the Community of Interest do to Respond?

## Protect Critical Servers and Management Systems

- Protect high value servers and data (PII, algos, research, IP, ….)
- Protect Management Plane of IT networks and systems
- Data centers, IaaS cloud services, and IoT

## Isolate and Protect Cloud Services

- Control access to IaaS cloud servers by all parties
- All access attempts logged for audit history with attribution
- No unauthorized awareness of public cloud services



## Micro-Segmentation / Software-Based Segmentation / Compliance

- Infrastructure independent and supports heterogenous environments
- Separates security policy from network topology
- Addresses compliance, risk and regulatory requirements

## Identity-Based Networking

- Identity Based Policy and Network Access
- Topology Independent Networking

BlackRidge
TECHNOLOGY

# Questions?

**Jim McCarthy,** Senior Security Engineer

James.McCarthy@nist.gov

301-975-0228

**Titilayo Ogunyale,** Project Lead

Togunyale@mitre.org

301-975-0219

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

**John Walsh,** Chief Strategy and Technology Officer

Jwalsh@blackridge.us

**Michael Murray,** SVP & GM Cyber Physical Systems

Mmurray@blackridge.us

BlackRidge
TECHNOLOGY