# NIST / NCCoE Cybersecurity Portfolio: OSIsoft PI in The Situational Awareness Use Case

Presented by **Jim McCarthy**

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Topics

- Brief Overview: NIST Cyber Security Portfolio
- Cybersecurity Framework (CSF)
- National Cybersecurity Center of Excellence (NCCoE)
- Situational Awareness for The Energy Sector (Use of OSIsoft PI)

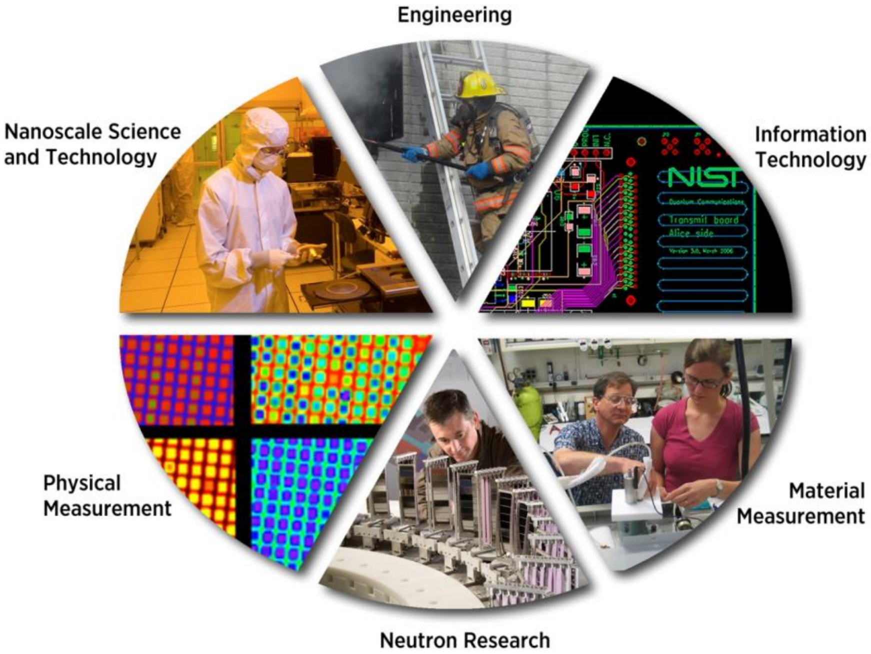
# National Institute of Standards and Technology

## NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

## NIST works with

- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations



NIST's Laboratories

# NIST Cybersecurity Portfolio

| Areas of Focus | Some Major Activities |
|---|---|
| Cryptographic Technologies | Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, E-Voting, Quantum Computing |
| Security Management and Assurance | Cybersecurity Framework for Critical Infrastructure, FISMA, Public Safety Network, Cyber-Physical System, Health IT, Smart Grid, Supply Chain, NICE, Outreach and Awareness |
| Secure Systems and Applications | Identity Management, Biometric Standards, Cloud Computing and Virtualization Technologies, Security Automation, Infrastructure Services and Protocols |
| Security Components and Mechanisms | Virtualization, Security Automation (SCAP), Trust Roots, Continuous Monitoring, USGv6 |
| Security Test and Metrics Group | Crypto Validation Programs, CAVP, CMVP (FIPS 140), SCAP Validation, NVD |
| National Cybersecurity Center of Excellence | Work with business sectors to identify real-world cybersecurity opportunities and collaborate with IT vendors to develop commercially available solutions to accelerate the adoption of technology |

# Improving Critical Infrastructure Cybersecurity

*“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”*

Executive Order 13636, 12 February 2013

# The NIST Cybersecurity Framework……

- Includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations.
- Is consistent with voluntary international standards.

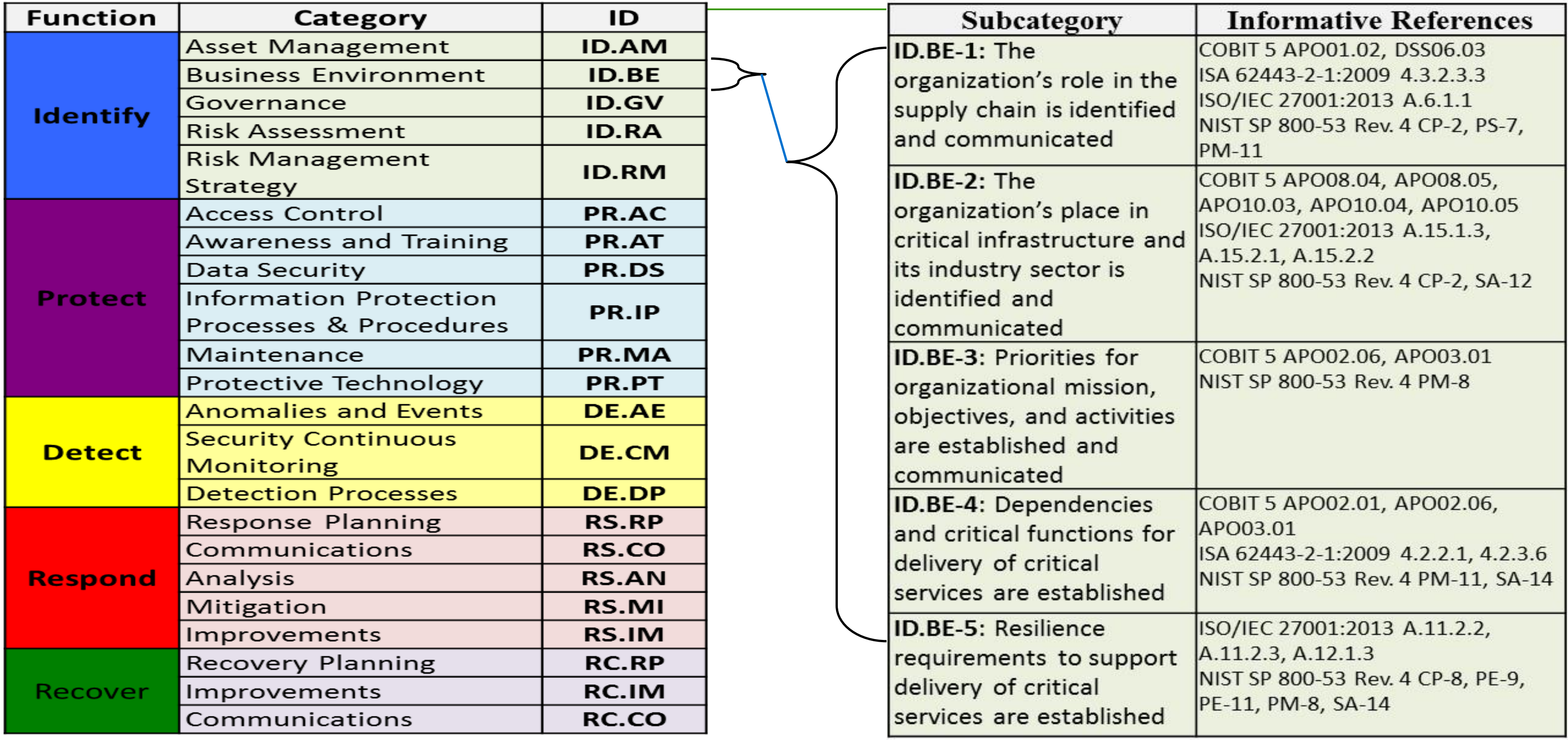
# Core

## *Cybersecurity Framework Component*

| | Function | Category | ID |
|---|---|---|---|
| What processes and assets need protection? | Identify | Asset Management | ID.AM |
| | | Business Environment | ID.BE |
| | | Governance | ID.GV |
| | | Risk Assessment | ID.RA |
| | | Risk Management Strategy | ID.RM |
| What safeguards are available? | Protect | Access Control | PR.AC |
| | | Awareness and Training | PR.AT |
| | | Data Security | PR.DS |
| | | Information Protection Processes & Procedures | PR.IP |
| | | Maintenance | PR.MA |
| | | Protective Technology | PR.PT |
| What techniques can identify incidents? | Detect | Anomalies and Events | DE.AE |
| | | Security Continuous Monitoring | DE.CM |
| | | Detection Processes | DE.DP |
| What techniques can contain impacts of incidents? | Respond | Response Planning | RS.RP |
| | | Communications | RS.CO |
| | | Analysis | RS.AN |
| | | Mitigation | RS.MI |
| | | Improvements | RS.IM |
| What techniques can restore capabilities? | Recover | Recovery Planning | RC.RP |
| | | Improvements | RC.IM |
| | | Communications | RC.CO |

# Core

*Cybersecurity Framework Component*



| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| Protect | Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | COBIT 5 APO01.02, DSS06.03<br>ISA 62443-2-1:2009 4.3.2.3.3<br>ISO/IEC 27001:2013 A.6.1.1<br>NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2<br>NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | COBIT 5 APO02.06, APO03.01<br>NIST SP 800-53 Rev. 4 PM-8 |
| **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | COBIT 5 APO02.01, APO02.06, APO03.01<br>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6<br>NIST SP 800-53 Rev. 4 PM-11, SA-14 |
| **ID.BE-5:** Resilience requirements to support delivery of critical services are established | ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3<br>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |

# ABOUT THE NCCOE

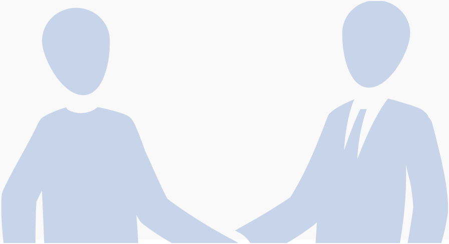
# NCCOE FOUNDATIONS

## NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

## PARTNERSHIPS

Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.



## NIST CYBERSECURITY THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Hardware roots of trust
- Vulnerability management
- Secure networking
- Usability and security

# WHO WE ARE AND WHAT WE DO

## VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

## MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

## GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

## GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

## GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

## The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

## Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

# NCCOE CURRENT PROJECTS

## Energy

- Identity and Access Management
- Situational Awareness

## Financial Services

- IT Asset Management
- Access Rights Management

## Healthcare

- Electronic Health Records on Mobile Devices
- Infusion Pumps

## Transportation: Maritime

- Cybersecurity Profile for Bulk Liquid Transfer

## Consumer/Retail

- Multifactor Authentication for e-Commerce

## Public Safety/First Responder

- Mobile Single Sign-On
- Authentication for Law Enforcement Vehicle Systems

## Manufacturing

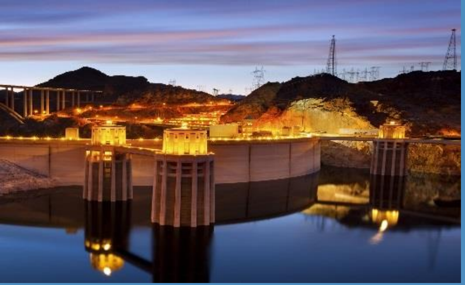
- Behavioral Anomaly Detection

## Mobile Device Security

- Mobile Device Security: Cloud & Hybrid Builds

## Attribute Based Access Control

## Derived Personal Identity Verification



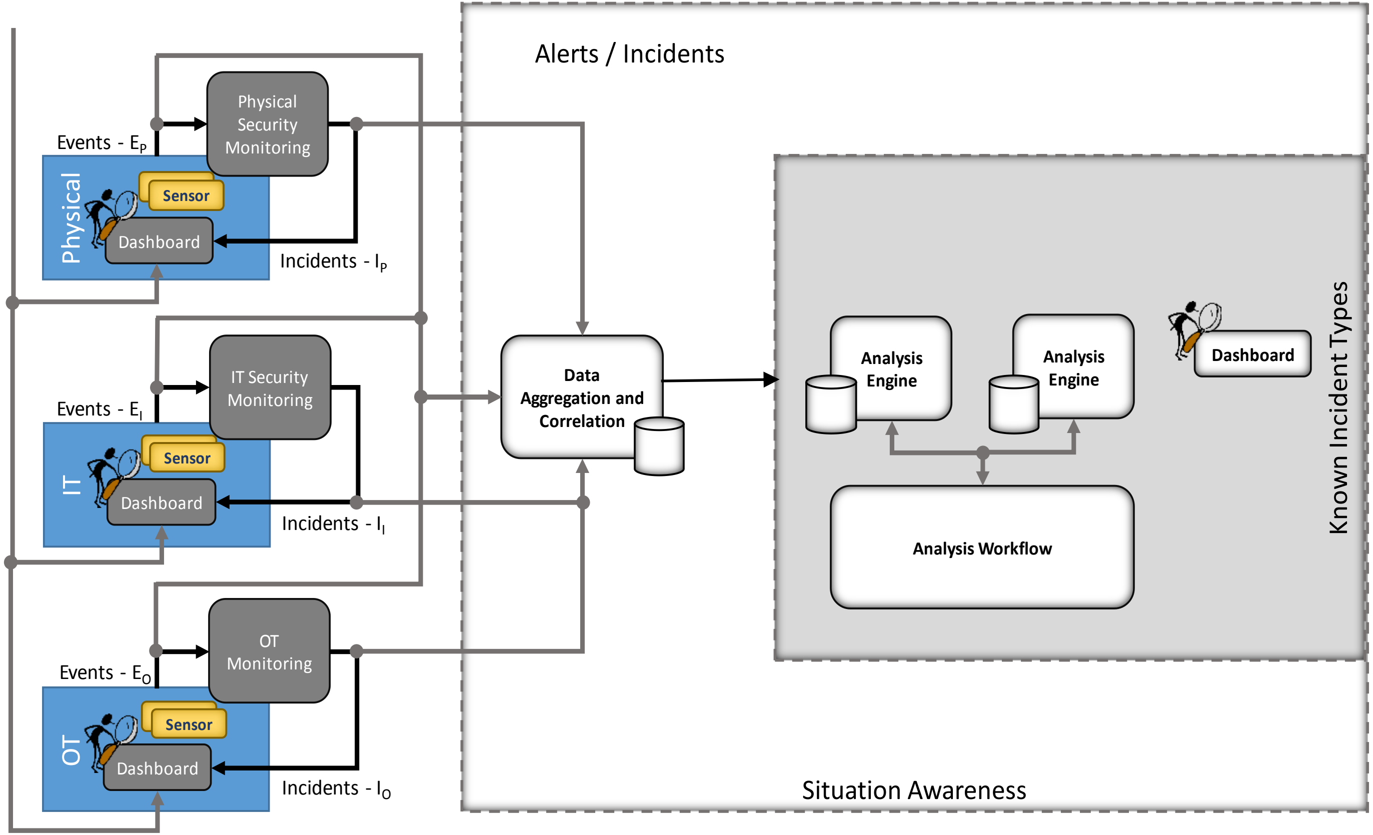
# Energy Sector Situational Awareness Practice Guide

## SP-1800-7 (Draft)

# NIST SP 1800-7 Practice Guide (draft) ;

- Situational Awareness for Electric Utilities
- Provide real-time / near real-time monitoring and detection capability for Energy Sector
- Correlation of alerts a necessity (OT, IT, PACS)
- Utilizes numerous Cybersecurity capabilities
- Call for collaboration  - 02/2015
- Requirements included need for ICS data historian
- OSIsoft PI selected by NCCoE to provide this capability for build
- Draft released 02/16/2017
- Comment period open until 04/17/2017
- https://nccoe.nist.gov/projects/use_cases/situational_awareness

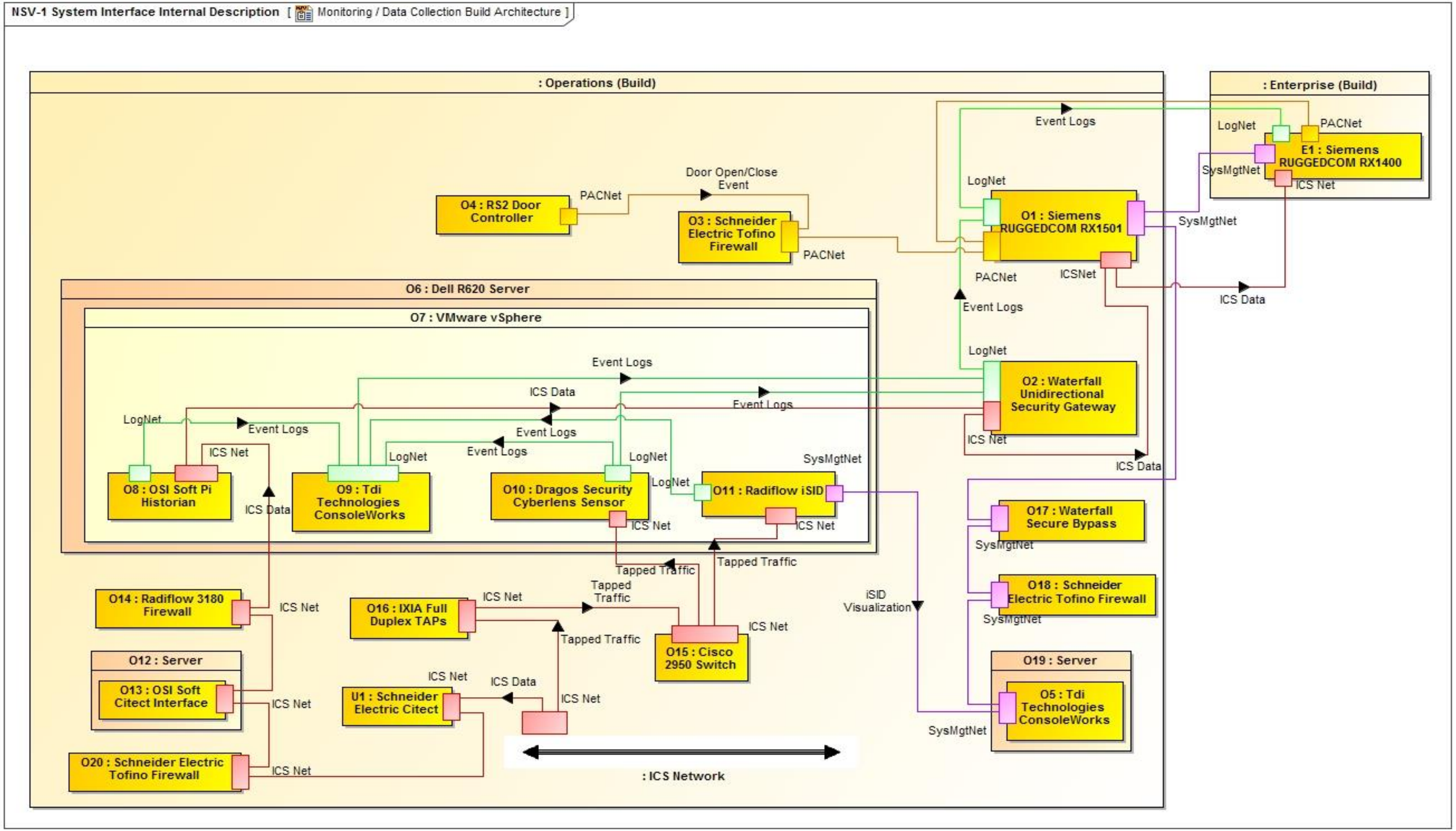
# SITUATIONAL AWARENESS CONCEPT



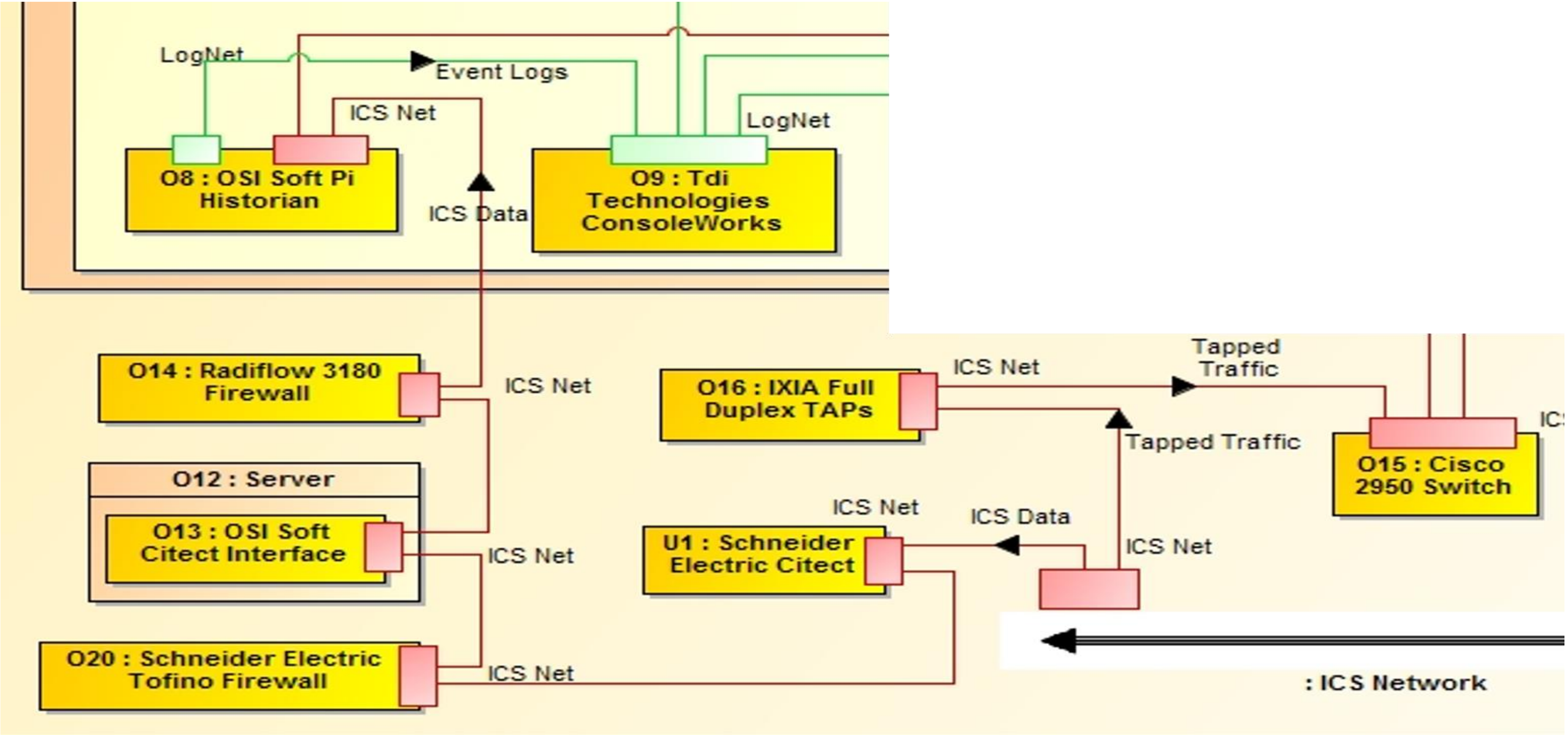
# PI System Highlights in SP 1800-7;

- Critical component for Situational Awareness (SA)
- Utilized Citect Connector and Historian features as no other historian data was available Co-gen plant (UMd)
- Required SCADA connector to feed data into PI System
- Provided only available interface between SCADA server and SA build
- Aggregation point for SCADA data to feed to anomaly detection tool (ICS network was baselined)
- Note: PI System capabilities extend far beyond what it was used for in build

# ARCHITECTURE



# ARCHITECTURE PI SYSTEM


LogNet
Event Logs
ICS Net
LogNet
O8 : OSI Soft Pi Historian
ICS Data
O9 : Tdi Technologies ConsoleWorks
O14 : Radiflow 3180 Firewall
ICS Net
O16 : IXIA Full Duplex TAPs
ICS Net
Tapped Traffic
Tapped Traffic
IC
O15 : Cisco 2950 Switch
O12 : Server
O13 : OSI Soft Citect Interface
ICS Net
ICS Net
ICS Data
U1 : Schneider Electric Citect
ICS Net
O20 : Schneider Electric Tofino Firewall
ICS Net
: ICS Network

# SUMMARY

- Brief description of NIST’s areas of focus
- NIST Cybersecurity Portfolio
- Cybersecurity Framework
- NIST National Cybersecurity Center of Excellence (NCCoE)
- Situational Awareness Practice Guide SP 1800-7 (draft)
- Key role and use of PI System in the guide

# CONTACT US

https://nccoe.nist.gov/projects/use_cases/energy_sector

301-975-0200

energy_nccoe@nist.gov

9700 Great Seneca
Hwy, Rockville, MD
20850

100 Bureau Drive, Mail Stop
2002, Gaithersburg, MD 20899

# Questions/comments

***Thank You***