# Using Architecture to build a defensible ICS

SANS ICS SUMMIT 2021

# Agenda

1. What is Security Architecture
2. Planning Security Architecture Activities
3. Establishing Security Architecture Activities
4. Upkeep of Security Architecture
5. Next Steps

# /whois
## @beLarge

Operational Technology Security Lead at CyberCX

Cyber Security Specialist who has worked across IT and OT in Cyber Security & Network Engineering roles for just under 15 years

An infrastructure tourist & cyber security architecture enthusiast

Experience in Rail, Electricity Generation, Aviation, Emergency Services and Consulting

Vice Chair of the Queensland Branch of the Information, Telecommunications and Electronics Engineering (ITEE) College of Engineers Australia

Bach Eng (Telecomms) and Master Business (Applied Finance)

GRID, SCF, CCNP/CCDP(Lapsed), Cyber Security Foundation+Practitioner (ALC)

# What is Architecture?

# From the Sliding Scale of Cyber Security

Rob M Lee states “Architecture refers to the **planning**, **establishing**, and **upkeep** of systems with security in mind. Ensuring that security is designed into the system provides a foundation upon which all other aspects of cyber security can build.” (p5)

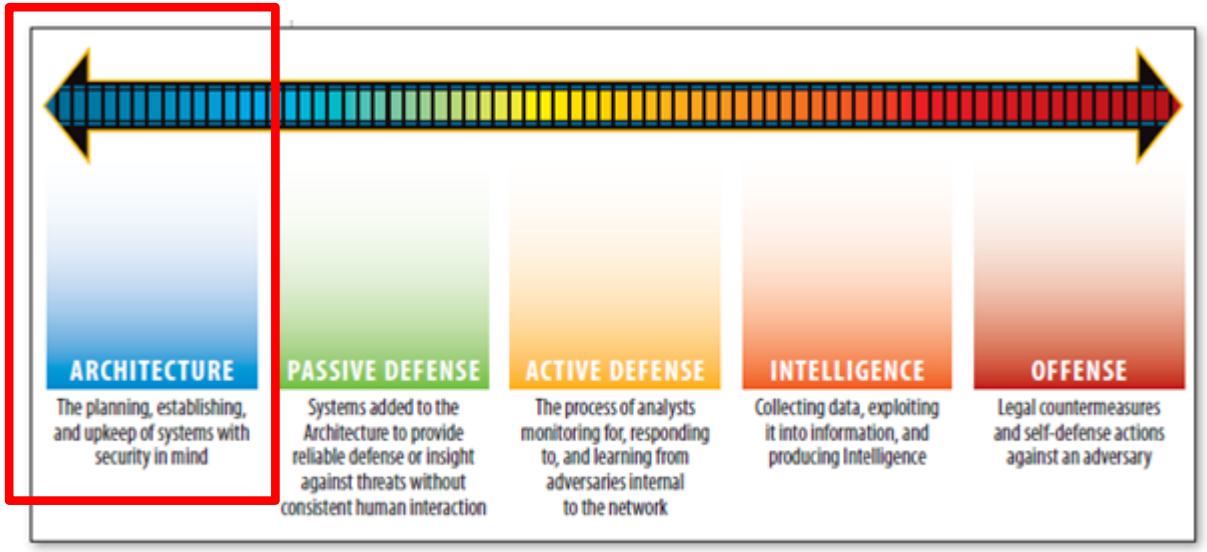



*Figure 1. The Sliding Scale of Cyber Security*

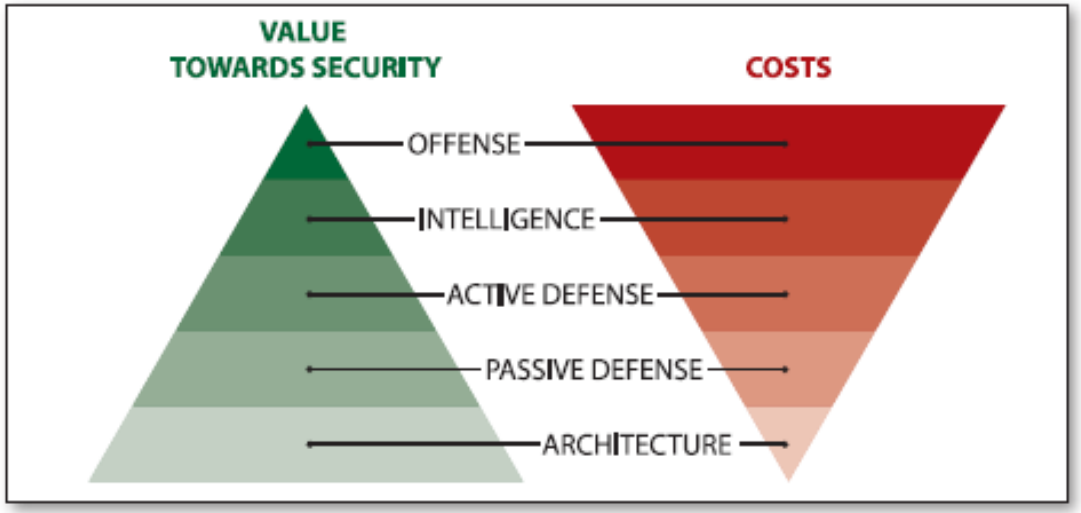



*Figure 2. Value Towards Security (Left) vs. Cost (Right)*

Source - https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

# From the Draft C2M2 v2

| Term | Definition |
| --- | --- |
| cybersecurity architecture | How cybersecurity practices and controls are structured and implemented to maintain the confidentiality, integrity, and availability of the organization's assets and services. |
| enterprise architecture | The design and description of an enterprise's entire set of IT and OT: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. |
| network architecture | A framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection. |

Source - https://apps.dtic.mil/sti/citations/AD1078768

# From the Draft C2M2 v2 (cont.)

The ARCHITECTURE Domain Objectives and Practices:

1. Establis
2. Implem
3. Implem
4. Implem
5. Manage

**1. Establish and Maintain Cybersecurity Architecture Strategy and Program**

**2. Implement Segmentation as an Element of the Cybersecurity Architecture**

**3. Implement App**

**4. Implement Data Security as an Element of the Cybersecurity Architecture**

| | | |
|---|---|---|
| MIL1 | a. | Sensitive data (e.g., PII, PCI, PHI, CEII, IP, operations data) is protected at rest (e.g., encrypted, masked, password-protected, subject to access control lists) at least in an ad hoc manner |
| | b. | Sensitive data (e.g., PII, PCI, PHI, CEII, IP, operations data) is protected in transit (e.g., encrypted, masked, transmitted using protected mechanisms) at least in an ad hoc manner (ASSET-2c) |
| MIL2 | c. | Key management infrastructure (i.e., key generation, key storage, key destruction, key update, and key revocation) are established and maintained to support the protection of data-at-rest and data-in-transit |
| | d. | Cryptographic controls are established and maintained to support the protection of data-at-rest and data-in-transit as required in the cybersecurity architecture |
| | e. | The cybersecurity architecture includes controls (e.g., data loss prevention tools, physical data exfiltration controls) to manage the transmission of data within and between systems based on security requirements (ARCHITECTURE-1e) |
| MIL3 | f. | The cybersecurity architecture includes protections for all data-at-rest (i.e., on-premise and cloud-based file storage and databases) for selected data categories (ASSET-2c) |
| | g. | The cybersecurity architecture includes protections for all data-in-transit (e.g., within internal networks, across network boundaries, and external traffic, including cloud solutions) for selected data categories (ASSET-2c) |
| | h. | Data protections are tested (e.g., controls validation) according to organization-defined triggers (e.g., time elapsed, changes to system architecture, changes to threat environment) |
| | i. | The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and information (due to errors or malicious activity) |

Source - https://apps.dtic.mil/sti/citations/AD1078768

# ESA vs Security Solution Architecture

## Enterprise Security Architecture (ESA)

Should work with the business to define security strategy and justification

Defines the enterprise wide security artefacts such as:

- Architectural Principles
- Attributes Modelling (SABSA)
- Domain Model
- Trust Models
- Pattern Repositories

Run the Architectural Review Board (ARB).

## Security Solution Architecture

A key pivot role between the whole of enterprise and delivering projects

Focuses on producing solution designs that address cyber security requirements as per the enterprise methodology

More than likely part of the projects team.

Some good material in NIST NICE (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center)
Worker Roles Enterprise Architect (SP-ARC-001) and  Security Architect (SP-ARC-002)

# Planning activities

UNDERSTAND THE BUSINESS, UNDERSTAND YOUR SYSTEMS, UNDERSTAND YOUR REQUIREMENTS

# SABSA

The Sherwood Applied Business Security Architecture (SABSA) is a Security Architectural framework that can provide business justification for cyber security efforts.

| | ASSETS (What) | MOTIVATION (Why) | PROCESS (How) | PEOPLE (Who) | LOCATION (Where) | TIME (When) |
|---|---|---|---|---|---|---|
| CONTEXTUAL ARCHITECTURE | Business Decisions | Business Risk | Business Process | Business Governance | Business Geography | Business Time Dependence |
| CONCEPTUAL ARCHITECTURE | Business Knowledge & Risk Strategy | Risk Management Objectives | Strategies for Project Assurance | Roles & Responsibilities | Domain Framework | Time Management Framework |
| LOGICAL ARCHITECURE | Information Assets | Risk Management Policies | Process Maps & Services | Entity & Trust Framework | Domain Maps | Calendar & Timetable |
| PHYSICAL ARCHITECTURE | Data Assets | Risk Management Practices | Process Mechanisms | Human Interface | ICT Infrastructure | Process Schedule |
| COMPONENT ARCHITECTURE | ICT Components | Risk Management Tools & Standards | Process Tools & Standards | Personnel Mgmt. Tools & Standards | Locator Tools & Standards | Step Timing & Sequencing Tools |
| SERVICE MGMT ARCHITECTURE | Service Delivery Management | Operational Risk Management | Process Delivery Management | Personnel Management | Management of Environment | Time & Performance Management |

The Business View

The Architect's View

The Designer's View

The Builder's View

The Tradesman's View

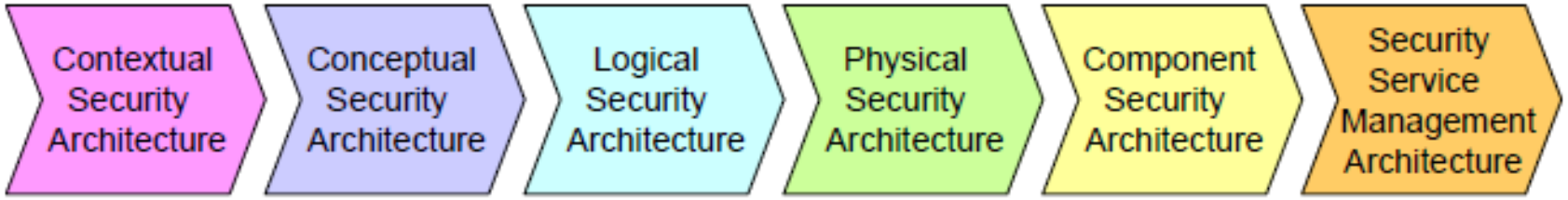
The Service Manager's View

From W100 *SABSA White Paper (2009)* - https://sabsa.org/white-paper-requests/

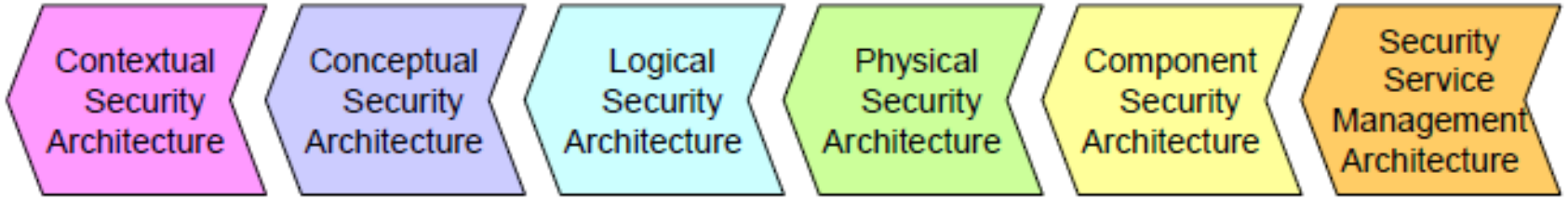
# SABSA (cont.) – Two Way Traceability

The SABSA Matrix also provides two-way traceability:

- Completeness: has every business requirement been met? The layers and matrix allow you to trace every requirement through to the components that provide a solution.




- Business Justification: is every component of the architecture needed? When someone questions 'Why are we doing it this way?' the rationale is plain by tracing back to the business requirements that drive the specific solution.



# SABSA (cont.) – Domain Modelling

A domain is "*A set of elements subject to a common security policy defined and owned by a single security policy authority*"

A Logical Domain:

- A Line of Business
- A logical classification (such as Information Sensitivity)
- A community of users (e.g. a department)

A Physical Domain:

- A set of physical elements (e.g. Same Physical Location or Tech Layer) subject to a common security policy

# Cyber Security Capabilities

Thinking in security capabilities is a key concept as it is the bridge between the Conceptual ESA Approach and the Security Solution Architecture – example capabilities:

| C2M2 (ESA) | ISA/IEC 62443 (Logical and Component) | NIST 800-82 (Component) |
|---|---|---|
| Cyber Security Program Management<br>• Network Security Architecture<br>• Network Security Segmentation | FR1 – Identity and Authentication Control (IAC) | System and Communications Protection (SC)<br>• SC-2 Application Partitioning<br>• SC-7 Boundary Protection |
| Situational Awareness<br>• Perform Logging<br>• Perform Monitoring | FR3 – System Integrity (SI) | Access Control (AC)<br>• AC-2 Account Management |
| Event and Incident Response, Continuity of Operations (IR)<br>• Detect Cyber Security Events<br>• Escalate Cybersecurity Events and Declare Incidents | FR5 – Restrict Data Flows (RDF) | Configuration Management (CM)<br>• CM-2 Baseline Configuration |
| Threat and Vulnerability Management<br>• Identify and Respond to Threats<br>• Reduce Cybersecurity Vulnerabilities | FR6 – Timely Response to Events (TRE) | Media Protection (MP)<br>• MP-1 Media Access<br>• MP-7 Media Use |

# Establishing activities

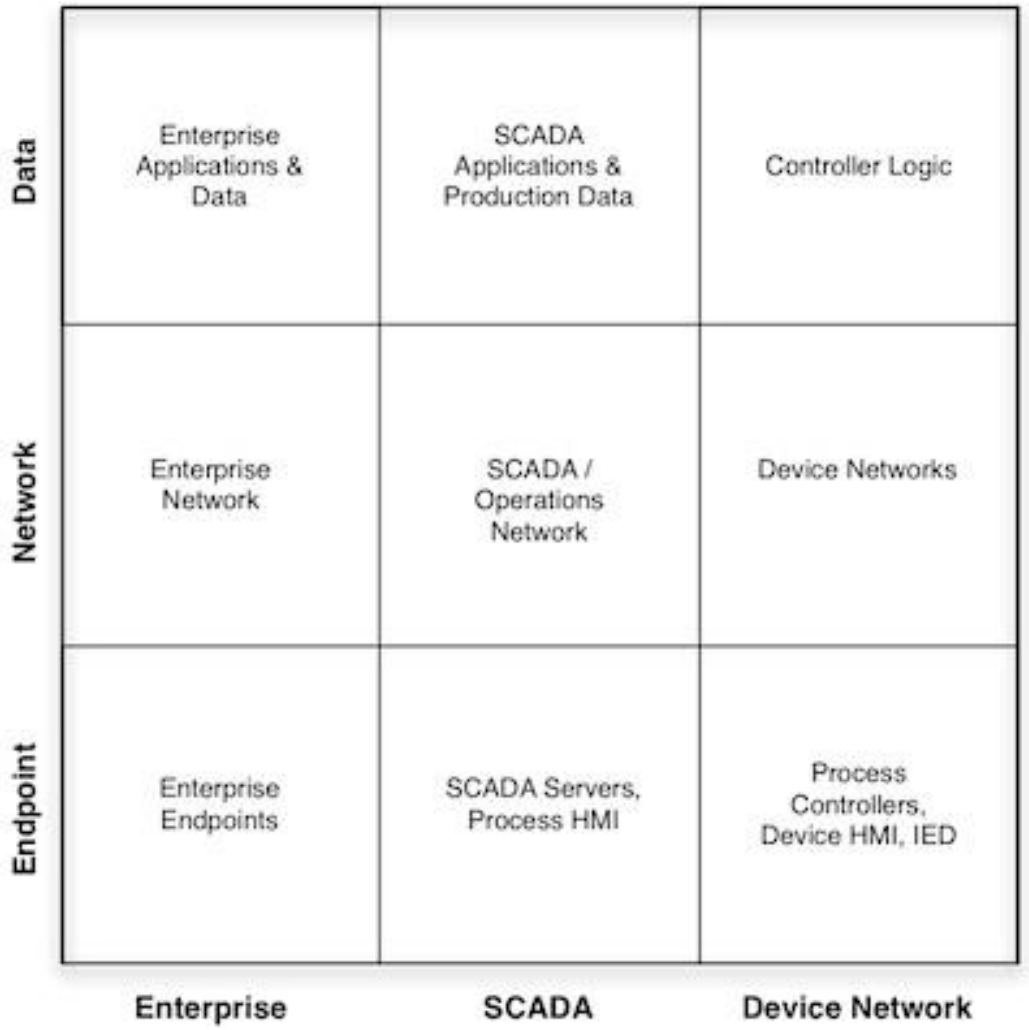
HOW TO BUILD IN CYBER SECURITY THROUGHOUT THE LIFE CYCLE OF THE SYSTEM

# Knapp's 3x3 Model

From Knapp & Samani's *Applied Cyber Security and the Smart Grid*

Considers the location and the component layer.

This is a simple visual model to communicate control placement and to help identify any blind spots




Source - https://www.securityweek.com/new-cyber-security-model-scada

# Zones & Conduits

From ISA/IEC 62443 –

A **Zone** is defined as "*a grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access, or responsible organization.*"

A **Conduit** is defined as *"a logical grouping of communication channels that share common security requirements  connecting two or more zones."*

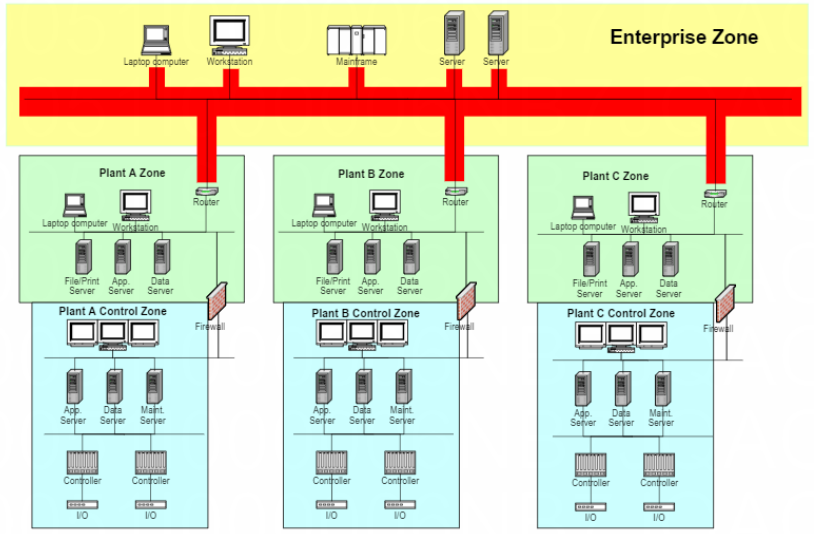



Figure 21 – Enterprise Conduit

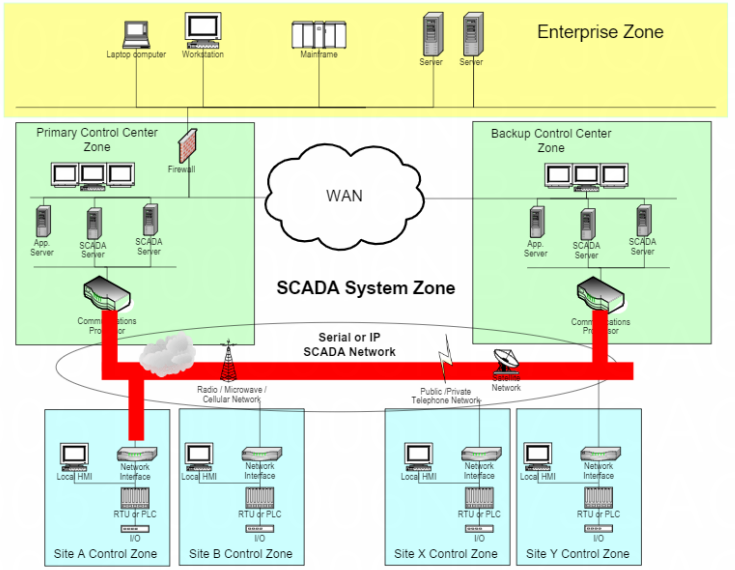


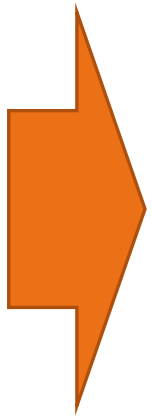

Figure 22 – SCADA Conduit Example

Source - https://gca.isa.org/isagca-quick-start-guide-62443-standards & ANSI/ISA 62443-1-1

# Controls – NIST 800-82

A key reference document that outlines:

- Overview of Industrial Control Systems
- ICS Risk Management and Assessment
- ICS Security Program and Deployment
- ICS Network Architecture
- **Application of Security Controls to ICS**
- Excellent Appendix Material
  - Sources of Threat Sources, Vulnerabilities and Incidents
  - Current Activities in ICS
  - ICS Security Capabilities and Tools
  - ICS Overlay (800-53 Applied to ICS)



The document provides an excellent pick list for:

- Security Controls with ICS Specific Recommendations and Guidance
- Library of Threats and Vulnerabilities

Source - https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

# Controls – ISA/IEC 62443

62443-3-3 Provides Control Recommendations –

Foundational Requirements

FR 1 – Identification and Authentication Control (IAC)

FR 2 – Use Control (UC)

FR 3 – System Integrity (SI)

FR 4 – Data Confidentiality (DC)

FR 5 – Restricted Data Flow (RDF)

FR 6 – Timely Response to Events (TRE)

FR 7 – Resource Availability (RA)

Also has the concept of System Requirements (SR) and Requirement Enhancements (RE)

# Controls – ISA/IEC 62443 (cont.)

For example, for FR 5 – Restricted Data Flow

| SRs and REs |
| --- |
| FR 5 – Restricted data flow (RDF) |
| SR 5.1 – Network segmentation |
| RE (1) Physical network segme |
| RE (2) Independence from non-networks |
| RE (3) Logical and physical iso networks |
| SR 5.2 – Zone boundary protection |
| RE (1) Deny by default, allow b |
| RE (2) Island mode |
| RE (3) Fail close |

**9.3 SR 5.1 – Network segmentation**

**9.3.1 Requirement**

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

**9.3.2 Rationale and supplemental guidance**

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirem

Network segmentation and the leve overall network architecture used b within their control systems. Logica some measure of protection, but n compromised. Physically segmenti that single-point-of-failure case, b These trade-offs will need to ISA-62443-2-1 (99.02.01)).

In response to an incident, it ma network segments. In that event, t

**9.3.3 Requirement enhancements**

(1) Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

(2) Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

(3) Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

Referenced from ISA 62243-3-3

# Visibility – Dragos CMF

A lot of effort is invested in **Identification** and **Protection** activities, but often **Detection** is overlooked.

"Prevention is Ideal, but Detection is a Must."

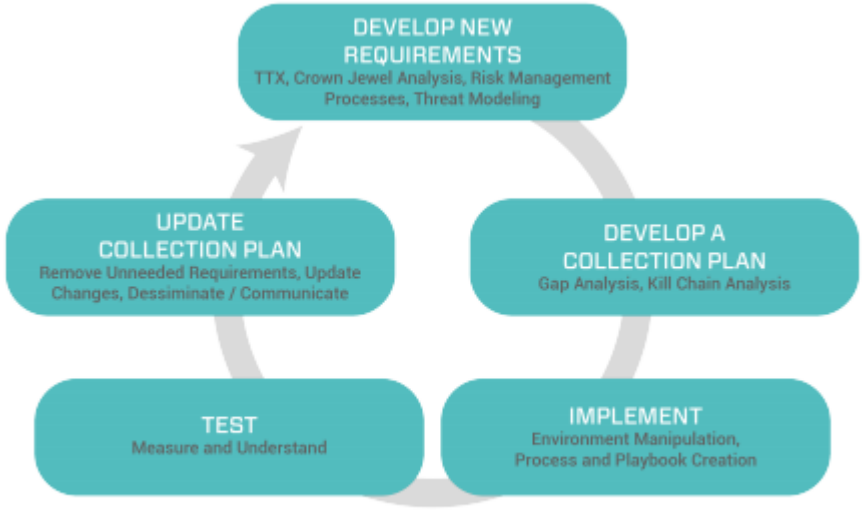



*Figure 1: CMF Development and Improvement Model*

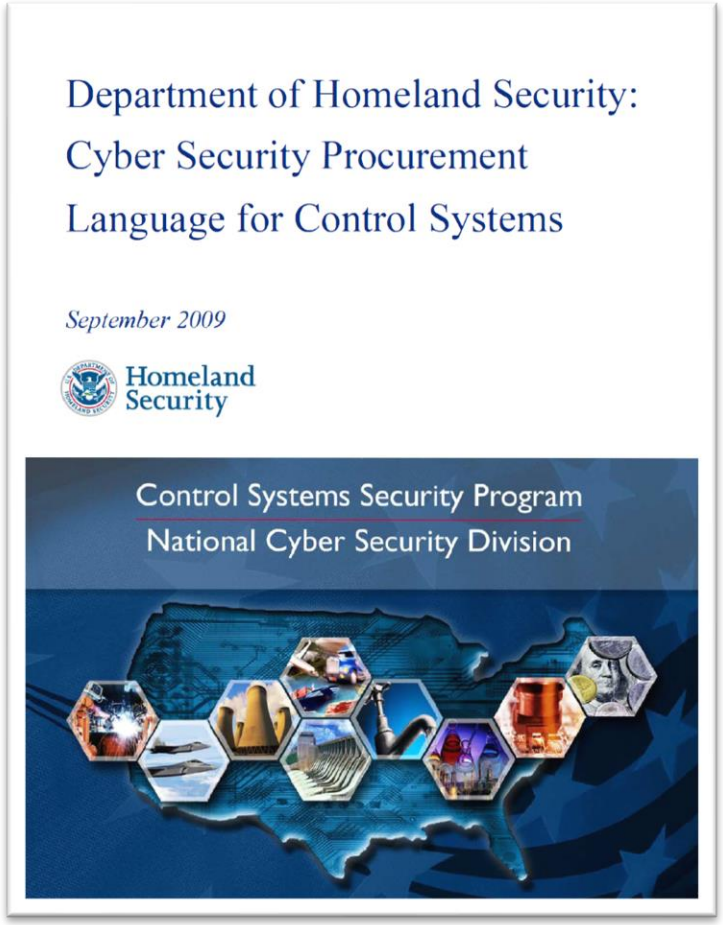
| | CONTROL CENTER | CONTROL CENTER | CONTROL CENTER | TRANSMISSION SUBSTATION | TRANSMISSION SUBSTATION |
|---|---|---|---|---|---|
| ASSET TYPE | Windows Human Machine Interface | Data Historian | Network Monitoring Appliance | Windows Human Machine Interface | Remote Terminal Units |
| DATA TYPE | Windows Event Logs | Alarms | Alerts | Windows Event Logs | Syslog |
| QUESTION TYPE (KILL CHAIN PHASES) | Exploration, Installation, Actions on Objectives | Actions on Objectives | Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives | Exploitation, Installation, Actions on Objectives | Installation, Actions on Objectives |
| FOLLOW-ON COLLECTION | Registry Keys | Set Points and Tags | Packet Capture | Registry Keys | Controller Logic |
| DATA STORAGE LOCATION | Enterprise SIEM | Local | Enterprise SIEM | Local | Local |
| DATA STORAGE TIME | 60 Days | 120 Days | 30 Days | 30 Days | 7 Days |

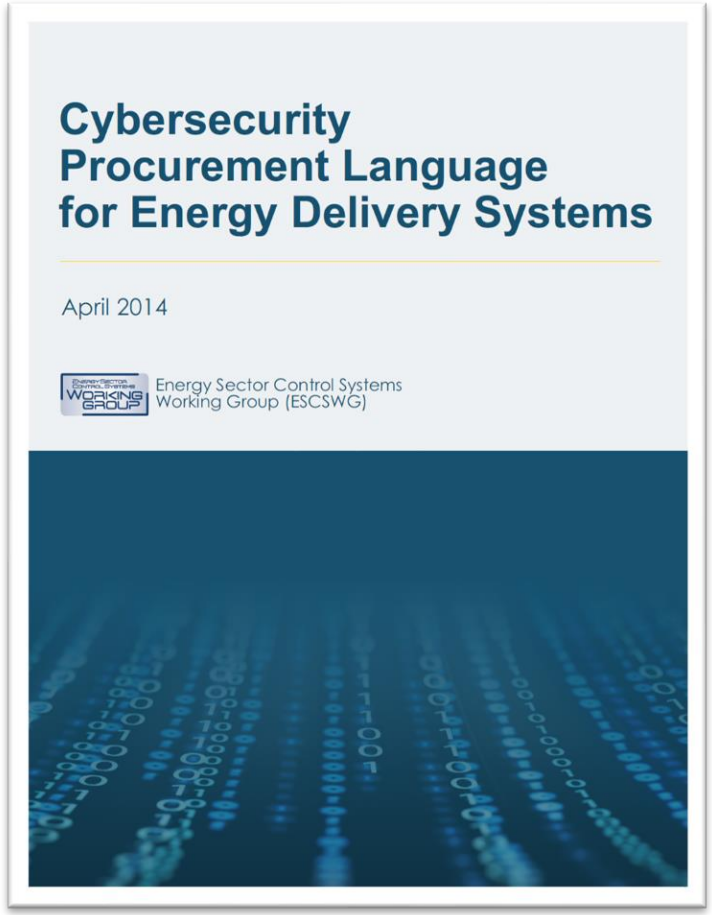
*Figure 2: Sample CMF of a Hypothetical Electric Company*

Source - https://www.dragos.com/blog/industry-news/building-a-collection-management-framework-for-industrial-control-systems/

# Supply Chain and Procurement Advice

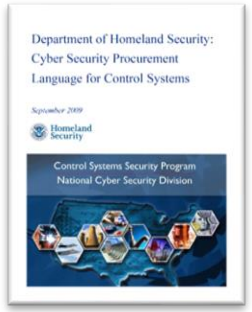
One of the most difficult challenges, but consider the below documents for support & advice




Source - https://us-cert.cisa.gov/ics/Recommended-Practices

# Supply Chain and Procurement Advice (cont.)


Department of Homeland Security:
Cyber Security Procurement
Language for Control Systems

September 2009

Homeland Security

Control Systems Security Program
National Cyber Security Division

## 2. SYSTEM HARDENING

System hardening refers to making changes to the default configurati
operating system (OS), software applications, and required third-party so
vulnerabilities.

### 2.1 Removal of Unnecessary Services

Unnecessary services and programs are often installed on network de

#### 2.1.1 Basis

Unused services in a host operating system that are left enabled are p
on the network and are generally not monitored because these services ar
used for control systems operation and maintenance shall be enabled to li

#### 2.1.2 Language Guidance

Often, networked devices ship with a variety of services enabled and
programs/utilities pre-installed. These range from system diagnostics to c
have well-known vulnerabilities. Various attacks have been crafted to exp
information leading to compromise the system.

Any program that offers a network service that "listens" on specific a
requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP
combination of IP address and TCP or User Datagram Protocol (UDP) po
activity is simply disabling or removing any services or programs, which
system operation, thus removing potential vulnerabilities.

Port scans are the normal method of ensuring existence of required se
services. A port scan shall be run before the FAT with a representative, fi
configuration. All input/output (I/O) ports need to be scanned for UDP an
before the FAT and again prior to the SAT. Port scans can rarely be used
cases, scanners will disrupt operations.

#### 2.1.3 Procurement Language

Post-contract award, the Vendor shall provide documentation detailin
system services, scripts, configuration files, databases, and all other softw
configurations, including revisions and/or patch levels for each of the con
the control system.

The Vendor shall provide a listing of services required for any compu
system applications or required to interface the control system applicatior
ports and services required for normal operation as well as any other port
emergency operation. The listing shall also include an explanation or cros
service is necessary for operation.

The Vendor shall verify and provide documentation that all services

The Vendor shall provide, within a pre-negotiated period, appropriate
and/or workarounds to mitigate all vulnerabilities associated with the pro
established level of system security.

operation and maintenance of the control system prior to the FAT. The Vendor shall provide
documentation on what is removed and/or disabled. The software to be removed and/or disabled shall
include, but not be limited to:

1. Games
2. Device drivers for network devices not delivered
3. Messaging services (e.g., MSN,[h] AOL IM)
4. Servers or clients for unused Internet services
5. Software compilers in all user workstations and servers except for development workstations and servers
6. Software compilers for languages that are not used in the control system
7. Unused networking and communications protocols
8. Unused administrative utilities, diagnostics, network management, and system manage
9. Backups of files, databases, and programs used only during system development
10. All unused data and configuration files
11. Sample programs and scripts
12. Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acr
OpenOffice, etc.).

#### 2.1.4 FAT Measures

The Vendor shall verify that the Purchaser requires the results of cyber security scans (
a vulnerability and active port scan, with the most current signature files) run on the contro
primary activity of the FAT. This assessment is then compared with an inventory of the req
patching status, and documentation, to validate this requirement. Other measures provided

1. The Vendor shall provide for each networked device or class of device (e.g., server, wo
switch) the following configuration documentation lists:
   a. Network services required for the operation of that device. Indicate the service n
   (e.g., TCP and UDP) and port range
   b. Dependencies on underlying operating system services
   c. Dependencies on networked services residing on other network devices
   d. All the software configuration parameters required for proper system operation
   e. Certified OS, driver, and other software versions installed on the device
   f. Results found by the vulnerability scans with mitigations affected.
2. The Vendor shall install firmware updates available for the computer or network devic
the system manufacturer at the time of installation and provide documentation.
3. The Vendor shall provide a summary table indicating each communication path require
system. Include the following information in this table:

h. Product Disclaimer
References herein to any specific commercial product, process, or service by trade name, trademark, manu
otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U
any agency thereof.

4

   a. Source device name and media access control (MAC) and/or IP address
   b. Destination device name and MAC and/or IP address
   c. Protocol (e.g., TCP and UDP) and port or range of ports.
4. The Vendor shall perform network-based validation and documentation steps on each device:
   a. Full TCP and UDP port scan on Ports 1–65535. This scanning needs to be completed during a simulated "normal system operation."

#### 2.1.5 SAT Measures

The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

#### 2.1.6 Maintenance Guidance

Document the system operating system and software patches as the system software evolves to allow traceability and to verify no extra services are reinstalled. Anytime the system is upgraded, it is recommended that system Vendors rerun appropriate subsets of the FAT on the baseline system before delivery to the purchaser.

#### 2.1.7 References


North American Electric Reliability Corporation (NERC) CIP-007-1 R2, "Ports and Services," Cyber Security—Critical Infrastructure Protection, June 1, 2006.

ANSI/ISA-99.00.01, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 5.[i]

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3, B.14, C.3.

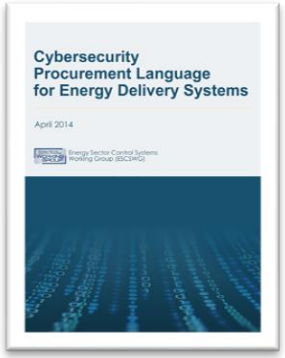
National Institute of Standards and Technology (NIST)[j]—Special Publication 800-42, "Guideline on Network Security Testing."


#### 2.1.8 Dependencies

None. This topic is stand-alone.

Source - https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

# Supply Chain and Procurement Advice (cont.)




## 3. THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM

The Supplier's life cycle security program is an important consideration in the procurement process. Vulnerabilities frequently result from architecture, design, weaknesses, and vulnerabilities in hardware, software, and firmware coding, as well as in bundled third-party products. Many energy delivery system security vulnerabilities are the direct result of writing software with inadequate attention to secure coding practices that reduce the risk of successful deliberate and persistent malicious attacks. Life cycle security programs provide a structured way for developing robust products with fewer weaknesses and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer's environment. Supplier post-production support is critical for maintaining secure software and systems, including remediating newly discovered vulnerabilities and ensuring that spare parts can be replaced with genuine parts. Validating that hardware, software, or firmware has been delivered as it was ordered and shipped—without being tampered with or otherwise modified—is also important. After a product has been removed from service, the disposal of that product provides opportunities for the compromise of information and configurations that the Acquirer or Supplier may deem sensitive.

### 3.1 Secure Development Practices

Secure product development practices are a set of processes integrated into the system development life cycle (SDLC) that reduce the security risks of the overall product. These practices help to develop more robust hardware, software, and firmware with fewer weaknesses and vulnerabilities, as well as identify and remediate weaknesses and vulnerabilities before implementation. Secure development practices ensure that security is integrated into all phases of the SDLC and is considered a key component of system development.

Baseline procurement language:

3.1.1. The Supplier shall provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided energy delivery system hardware, software, and firmware. If applicable, the Supplier shall document how the most critical application security weaknesses (including *OWASP Top 10* or *SANS Top 25 Most Dangerous Software Errors*) are addressed in the Supplier's SDLC.

3.1.2. As specified by the Acquirer, the Supplier shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and service for the product are provided. The Supplier shall notify the Acquirer of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur within [a negotiated time period] prior to initiating a change in the list of countries.



3.1.3. The Supplier shall provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. The Supplier shall use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. This testing may be done by the Supplier or an independent entity. The Supplier shall provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

3.1.4. The Supplier shall provide summary documentation of its coding reviews, including defect lists and plans to correct identified vulnerabilities.

3.1.5. The Supplier shall communicate security-related technical issues with a single technical point of contact (e.g., a company support email address or a company support phone number), as specified by the Acquirer. The Supplier shall communicate with the Acquirer within [a negotiated time period] (see Section 3.3.3). This is not intended for non-technical contract-related issues.

3.1.6. The Supplier shall provide documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language (SQL) injection, directory traversal, Remote File Include, Cross-Site Scripting (XSS), and buffer overflow.

3.1.7. The Supplier shall provide a contingency plan for sustaining the security of the procured product in the event the Supplier leaves the business (e.g., security-related procedures and products placed in escrow).

3.1.8. The Acquirer shall have the right to request documentation of the Supplier's implemented cybersecurity program, including recent assessment results or conduct periodic [at a negotiated frequency and scope] on-site security assessments at the Supplier's facilities. These on-site security assessments may be conducted by an independent third party, at the discretion of the Acquirer.

### 3.2 Documentation and Tracking of Vulnerabilities

When security vulnerabilities are discovered in hardware, software, and firmware, the timely application of corrective actions and/or mitigation steps can reduce the likelihood that adversaries will be able to exploit these vulnerabilities in energy delivery systems. Some of these vulnerabilities may be publicly disclosed before the Supplier can develop remedies; others may be kept from disclosure until remedies are available.

Security breaches may also affect the cybersecurity of the procured product. Such breeches may involve a compromise of security involving the Supplier's organization, or any organization involved in the product's supply chain. Security breaches may result in the loss of sensitive product design



Source - https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

# Case Studies

SCADA REFERENCE AND DCS REFERENCE

# SCADA Reference – Railway System

Railways operate many Industrial Control Systems (ICS) and Asset Protection Systems, examples such as –

1. Safety Critical Railway Signalling Systems
2. Safety Critical Power Supervisory Systems
3. Wayside Asset Protection Systems
4. Voice and Radio Telecommunication Systems

Some requirements

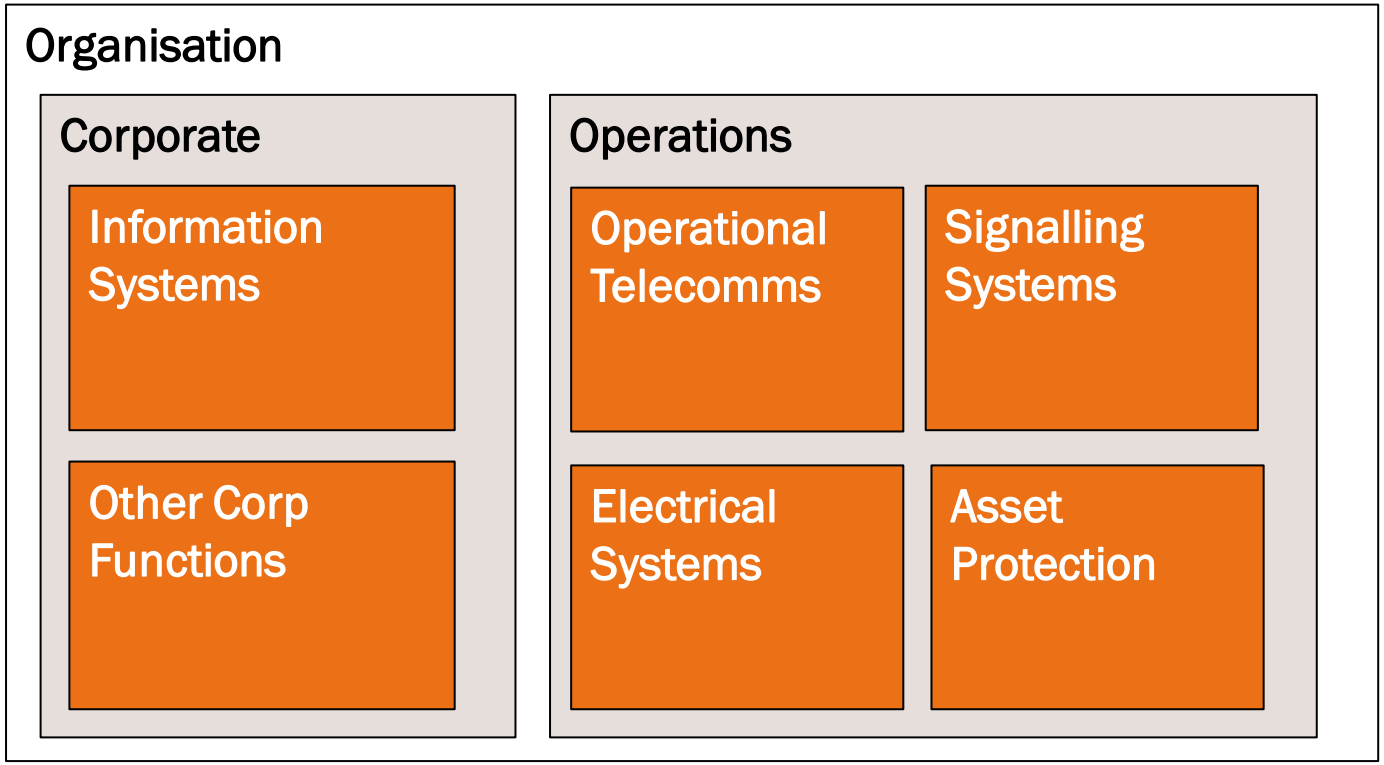
1. A common network to transport both Information and Operational Technology Systems that can segregate and segment services
2. Build a system that is flexible to be carried across Private Optical Fibre, Microwave Transmission Systems, Carrier Data Services and even Satellite Systems
3. High Availability
4. Cost Effective

# SCADA Reference – Railway System (cont.)

Domain Model – The Conceptual View – ESA View

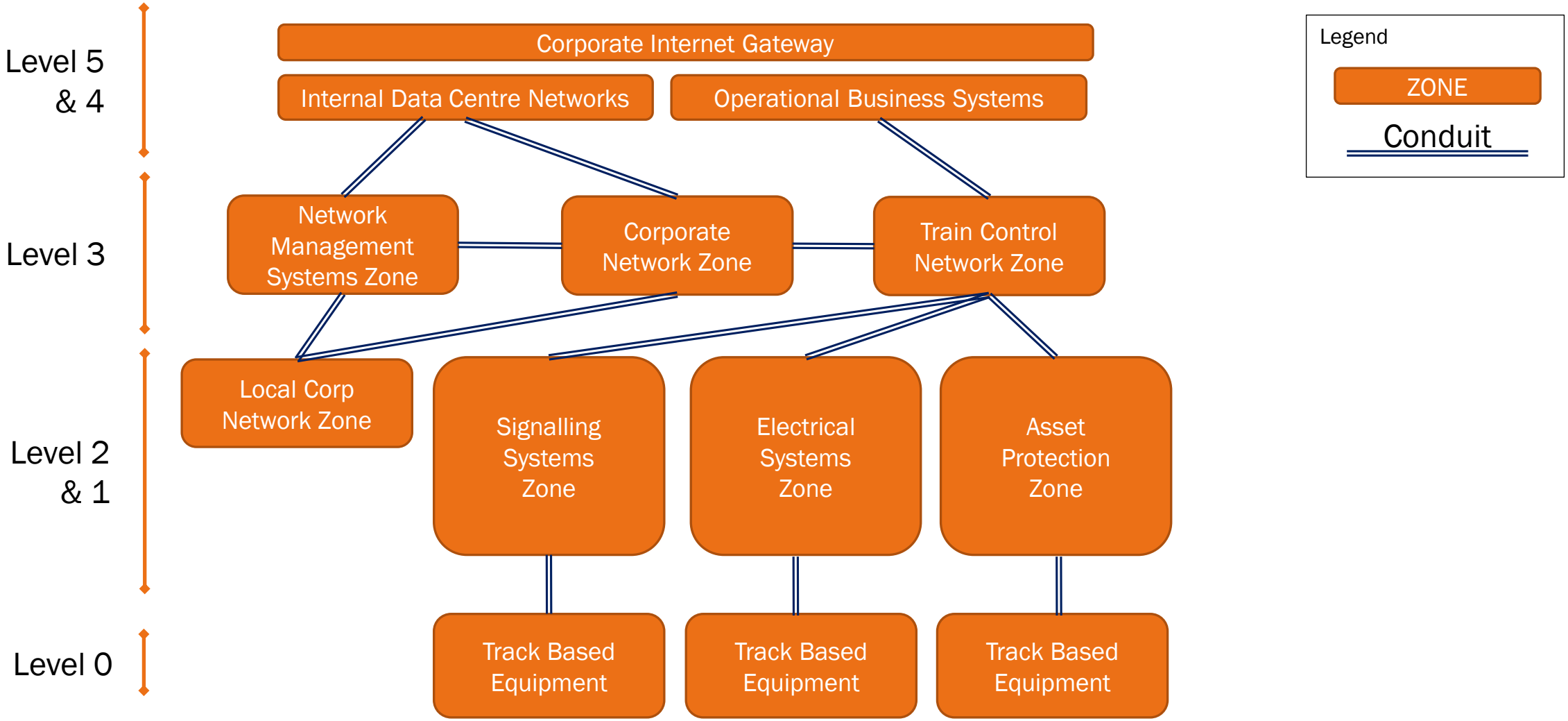
This helps the Enterprise Security Architect:

- Define Policy Domains and Policy Authorities
- Understand the interaction between domains, which will drive Security Capability Selection



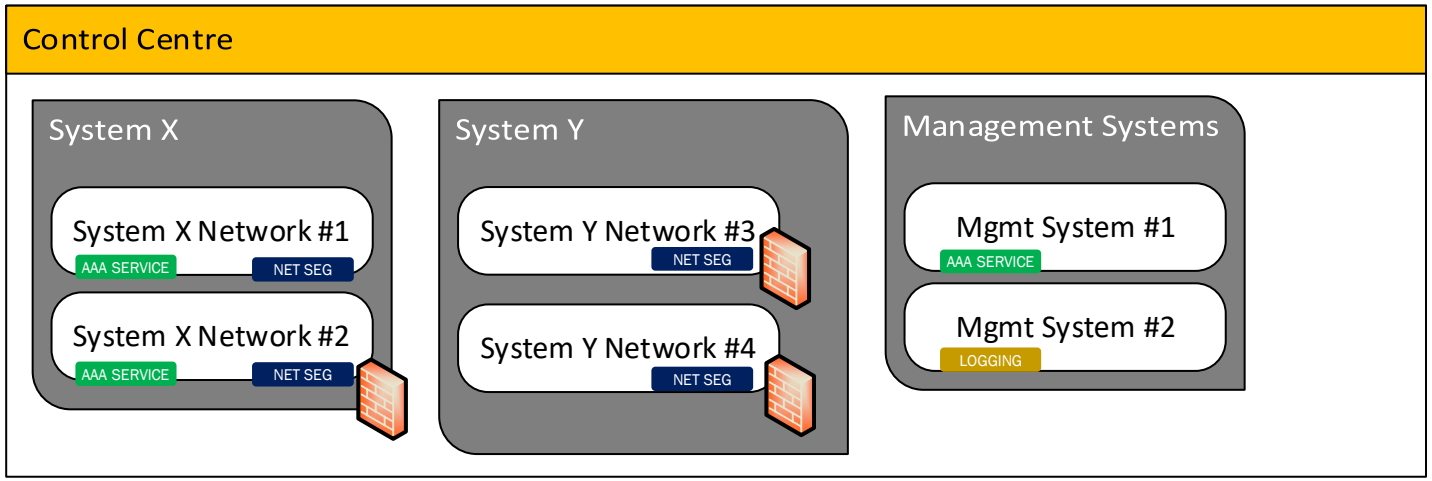
# SCADA Reference – Railway System (cont.)

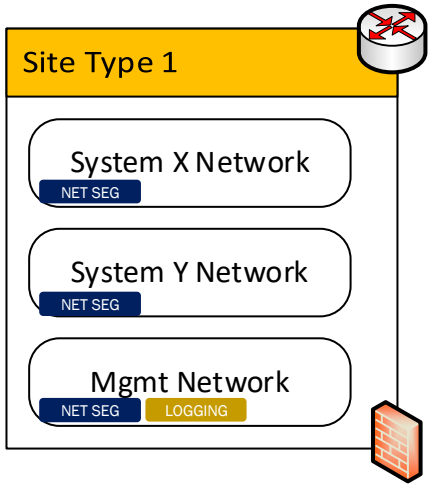
Zones and Conduits - Logical – The Designers View

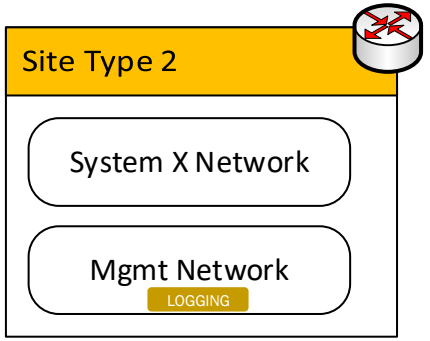


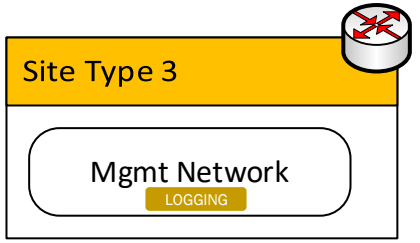
# SCADA Reference – Railway System (cont.)

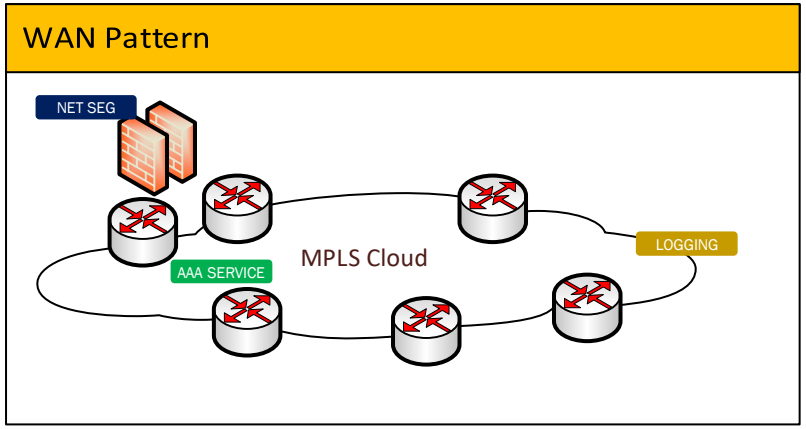
## Example Physical Architectures – The Builders View

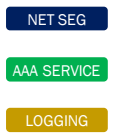


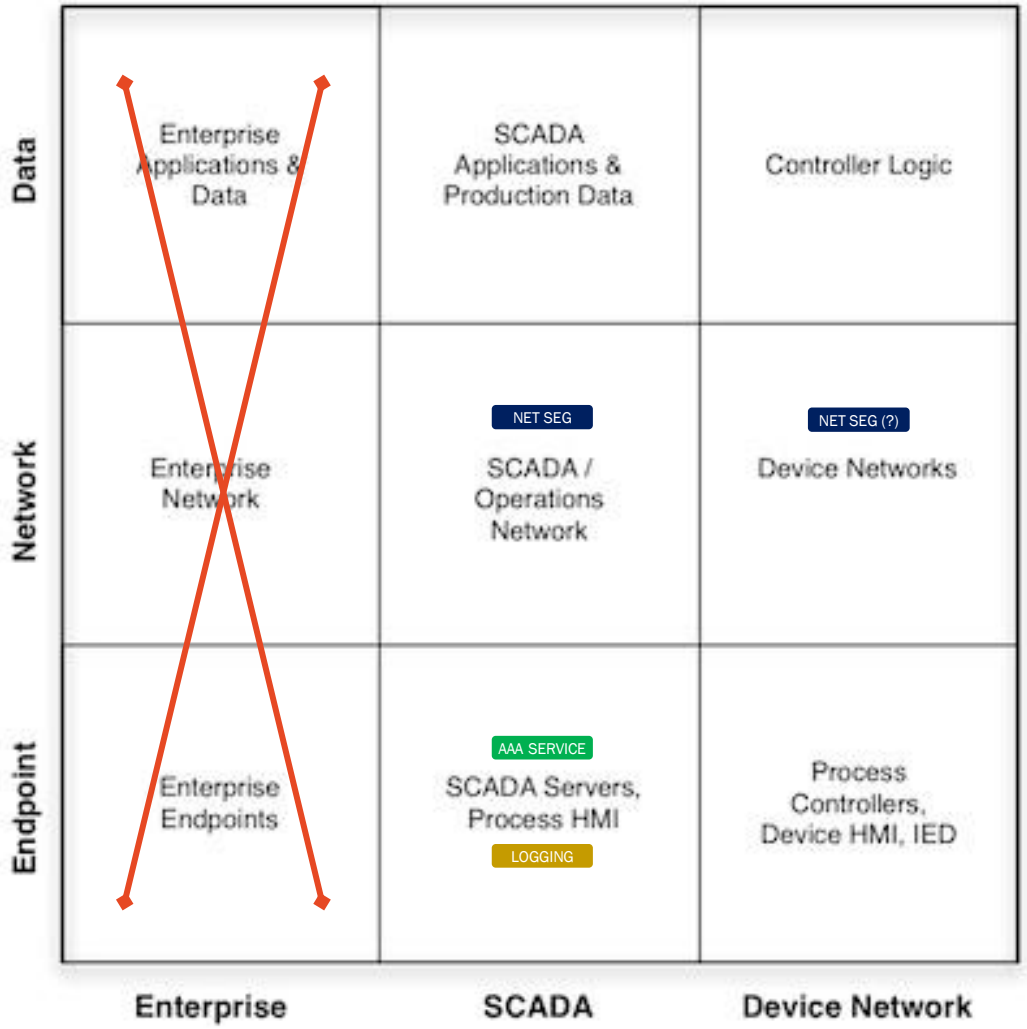



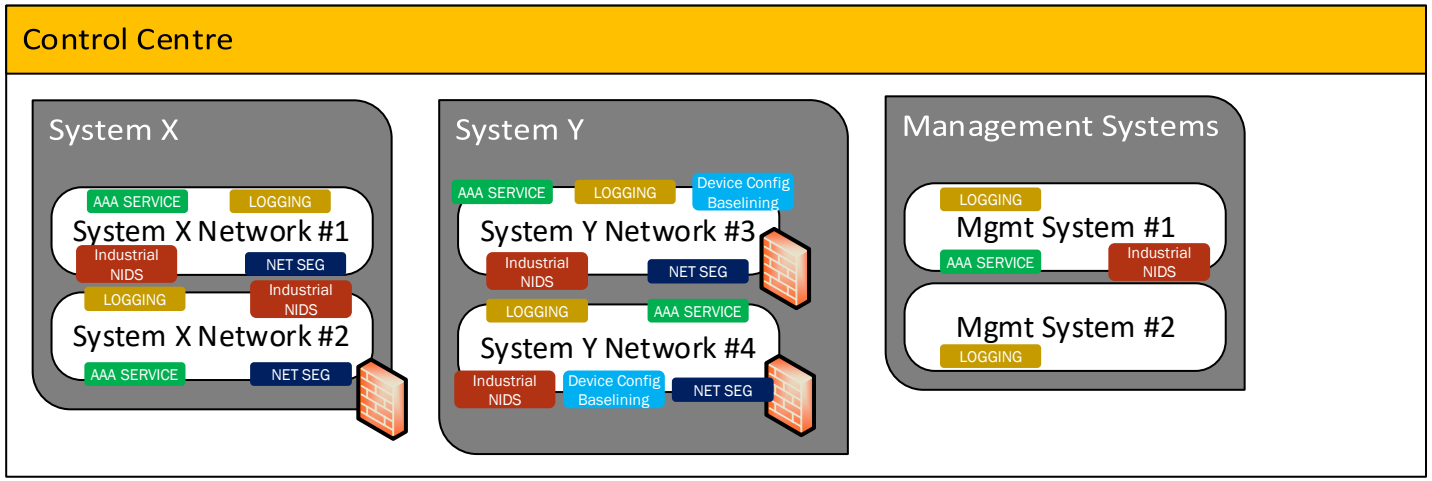
# SCADA Reference – Railway System (cont.)

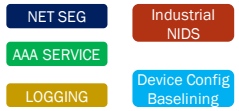
Review - Consider Knapp's 3x3

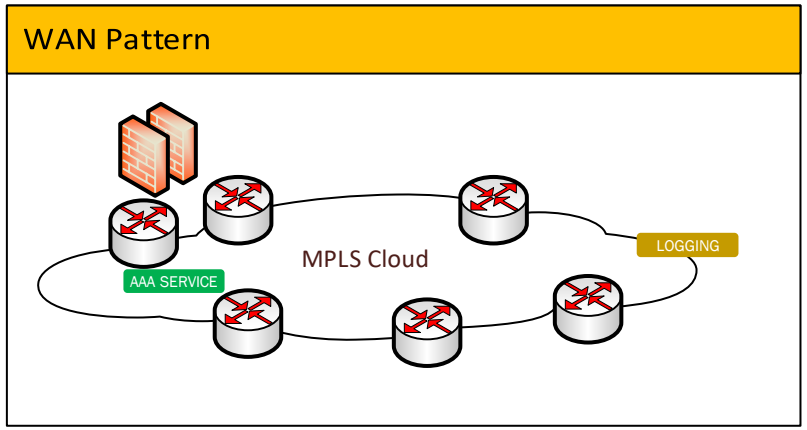


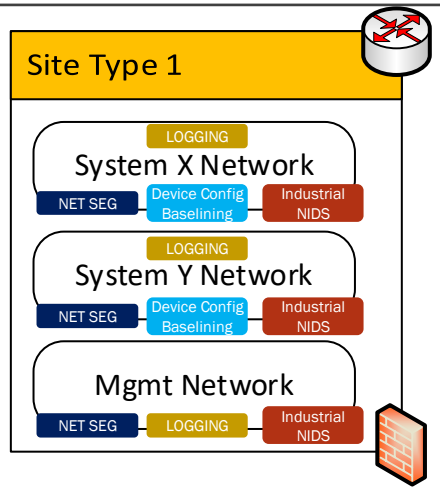
# SCADA Reference – Railway System (cont.)

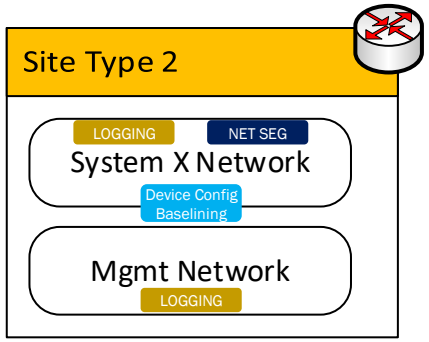
## Example Physical Architectures – The Builders View

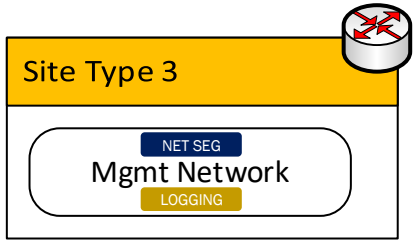


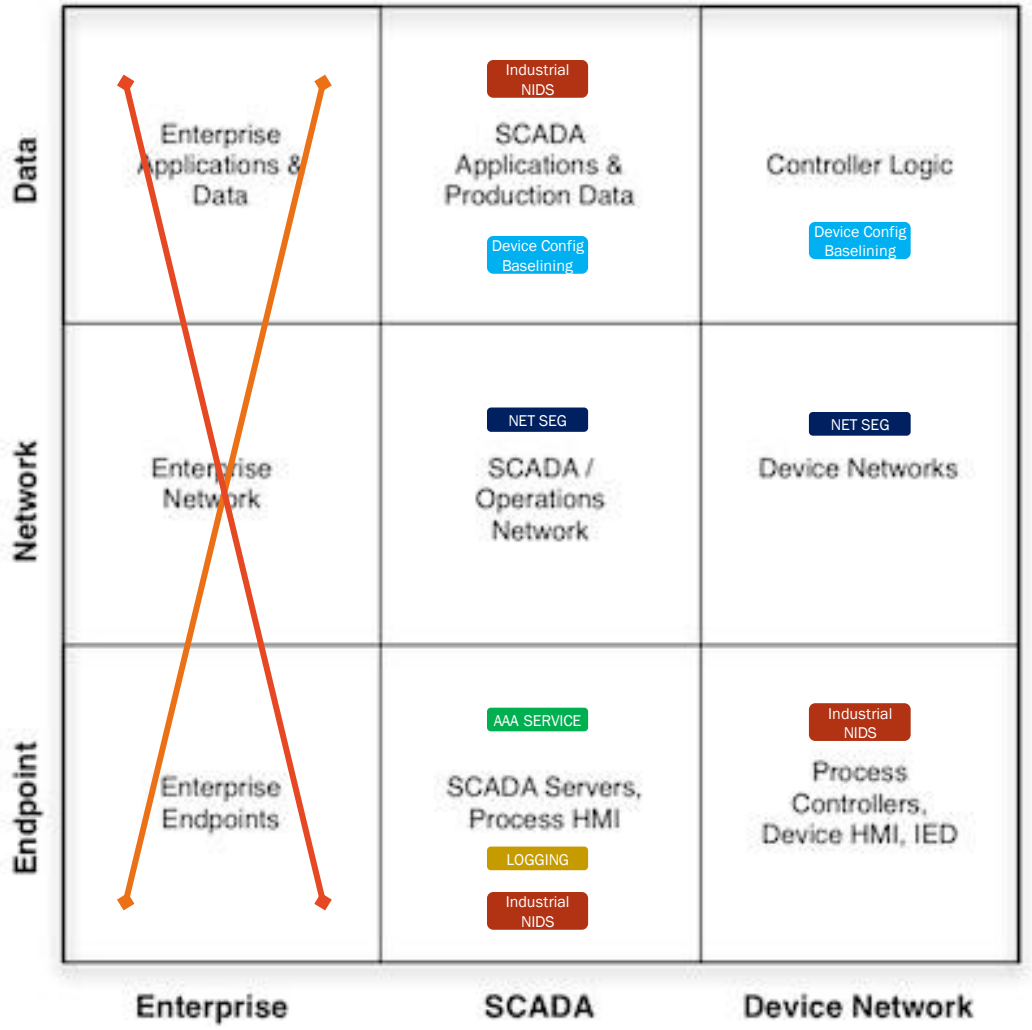



# SCADA Reference – Railway System (cont.)

Review - Consider Knapp's 3x3



# DCS Reference – Electricity Generation

A Coal Fired Power Station is a large, complicated and interconnected Process. A Power Station has many sub systems:

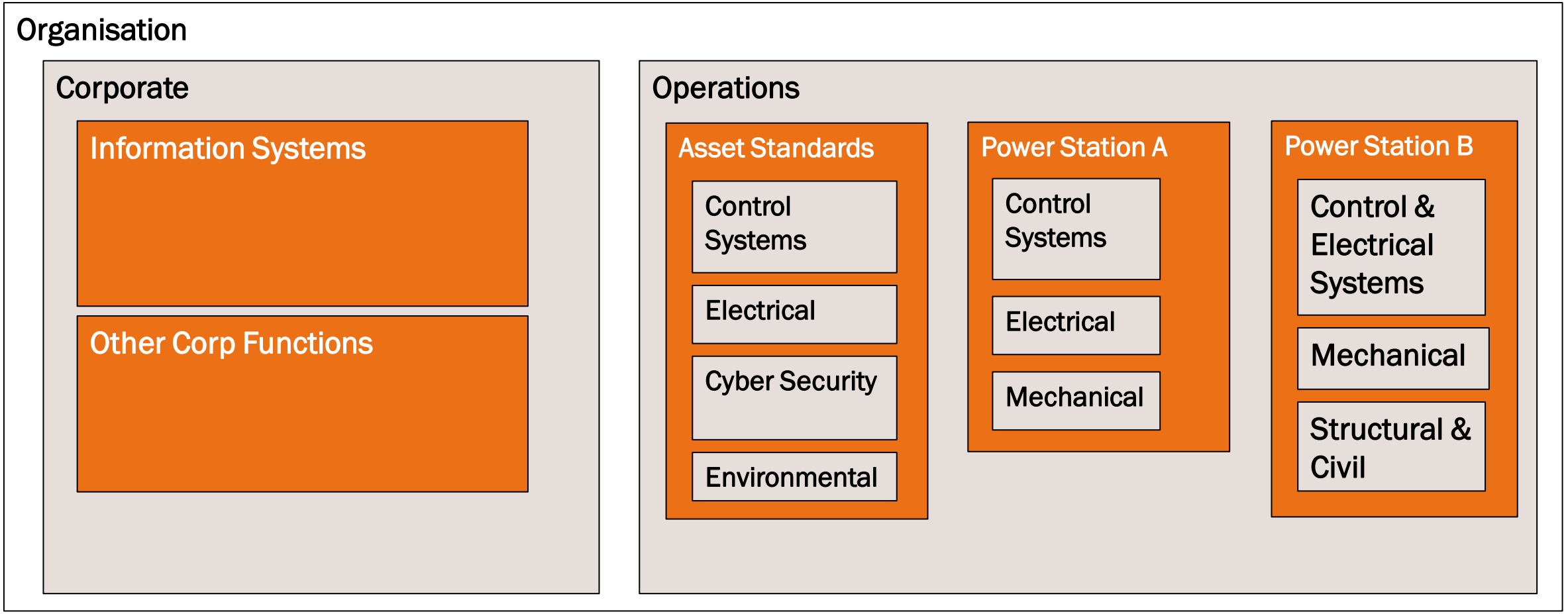
1. Air & Fuel
2. Steam Cycle
3. Electrical Generation Equipment
4. Water Chemistry Systems
5. Balance of Plant (BoP) - Station Equipment

Requirements

1. You have to work within the Vendor's Distributed Control System (DCS) approved standards or risk support issues
2. Build an integrated Control and Monitoring System
3. Is probably within a small contained geographic region, so LAN Networking & Security services are a critical sub system
4. Availability is especially critical for Energy
5. You need to consider a secure method of allowing the DCS vendor to have access to the system for telemetry and remote support
6. You need to expose process data to enable real time business decisions

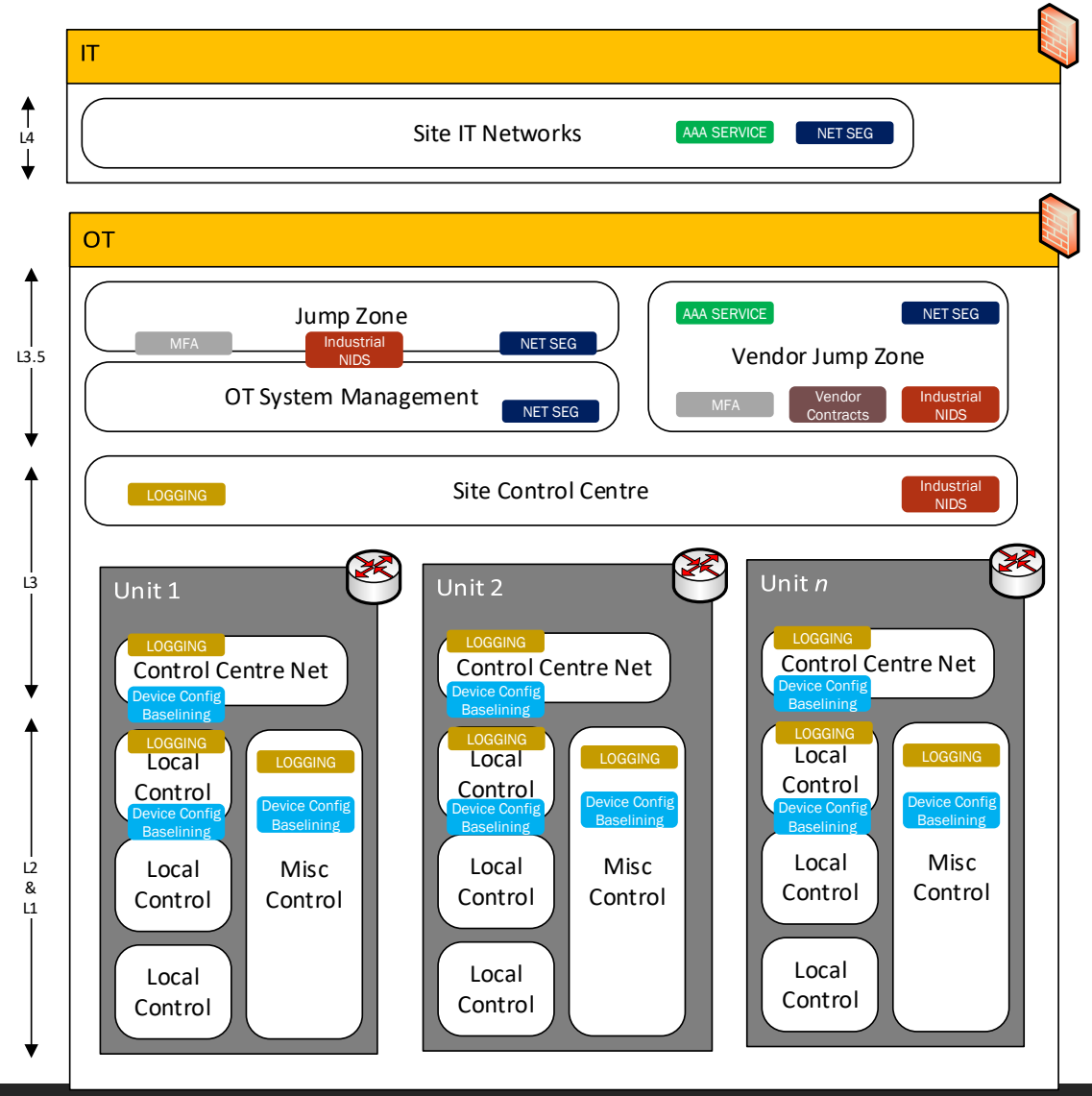
# DCS Reference – Electricity Generation (cont.)

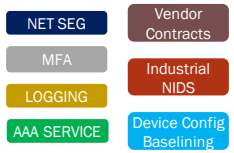
Domain Model – The Conceptual View – ESA View



# DCS Reference – Electricity Generation (cont.)

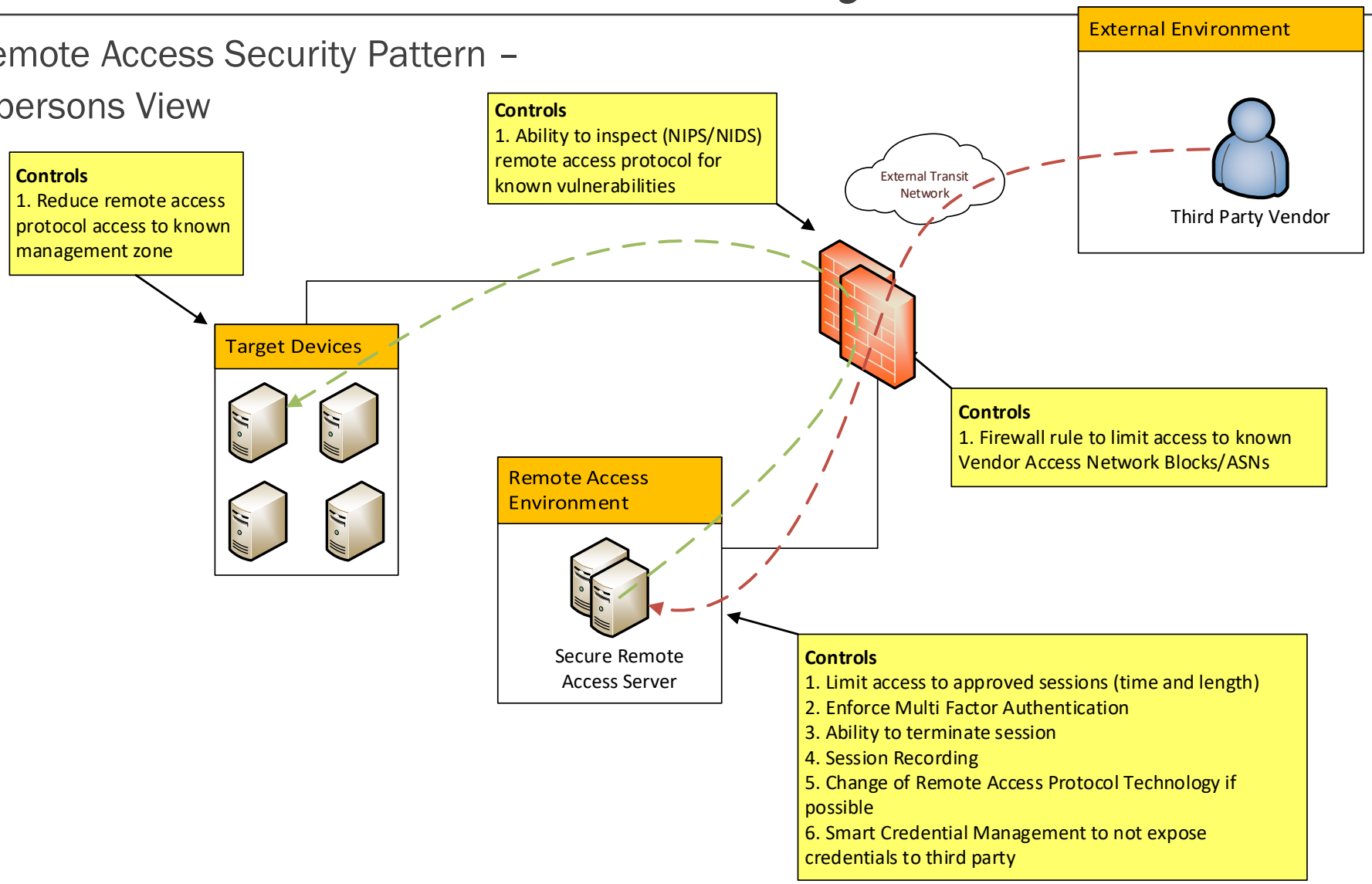
## Example Physical Architectures – The Builders View



# DCS Reference – Electricity Generation (cont.)

Example Remote Access Security Pattern –
The Tradespersons View



# Upkeep of Architecture

HOW TO SUSTAIN CYBER SECURITY MANAGEMENT OF SYSTEMS

# Make Architecture a Living Process

- Architecture can not be a fire and forget project
- Seek management support and buy in – articulate that architecture is a whole of life cycle capability
- It has to be embedded within the Business, Technology and Projects Processes

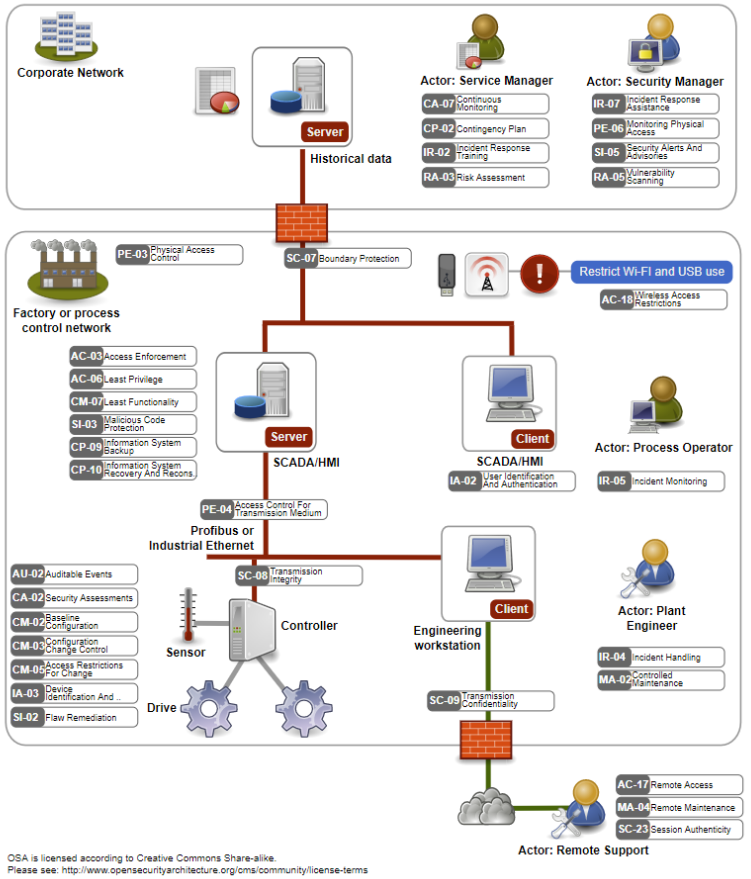
# OpenSecurityArchitecture.org – Patterns

Security Patterns are an excellent tool to help:

- share knowledge;
- sustain standards;
- simplify operational cyber security risk; and
- to make the Architecture Review Board (ARB) process as efficient as possible.

OpenSecurityArchitecture.org SP-023 is an excellent example

This can be a reference design that can be reused in the organisation and makes the Design and Review Process Simpler - it is easier to do version control with a pattern.




Source - https://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/293-draft-sp-023-industrial-control-systems

# Next Steps

SOME HOMEWORK FOR YOU WHEN YOU GET BACK TO WORK

# Next steps

## Next Week

1. Review the content of this presentation and rate your organisations capability against
   - Architecture Planning Capability
   - Architecture Establishing Capability
   - Architecture Upkeep Capability
2. Reach out to your tech teams to seek their views & support

## Next Month

1. Build a central point to keep your architectural material
2. Consider whether the C2M2 v2 materials are a good starting point for your organisation
3. Identify your capability gaps and what the plan is to fill them
4. Seek Management Support

## Next 6 Months

1. Embed managing Cyber Security across the life cycle of new projects
2. Build an uplift program to audit your *as-is* state for security capabilities and build a plan to get them to the *to-be* state

# Questions?

 @beLarge

 https://github.com/belarge