CampusEnergy2021

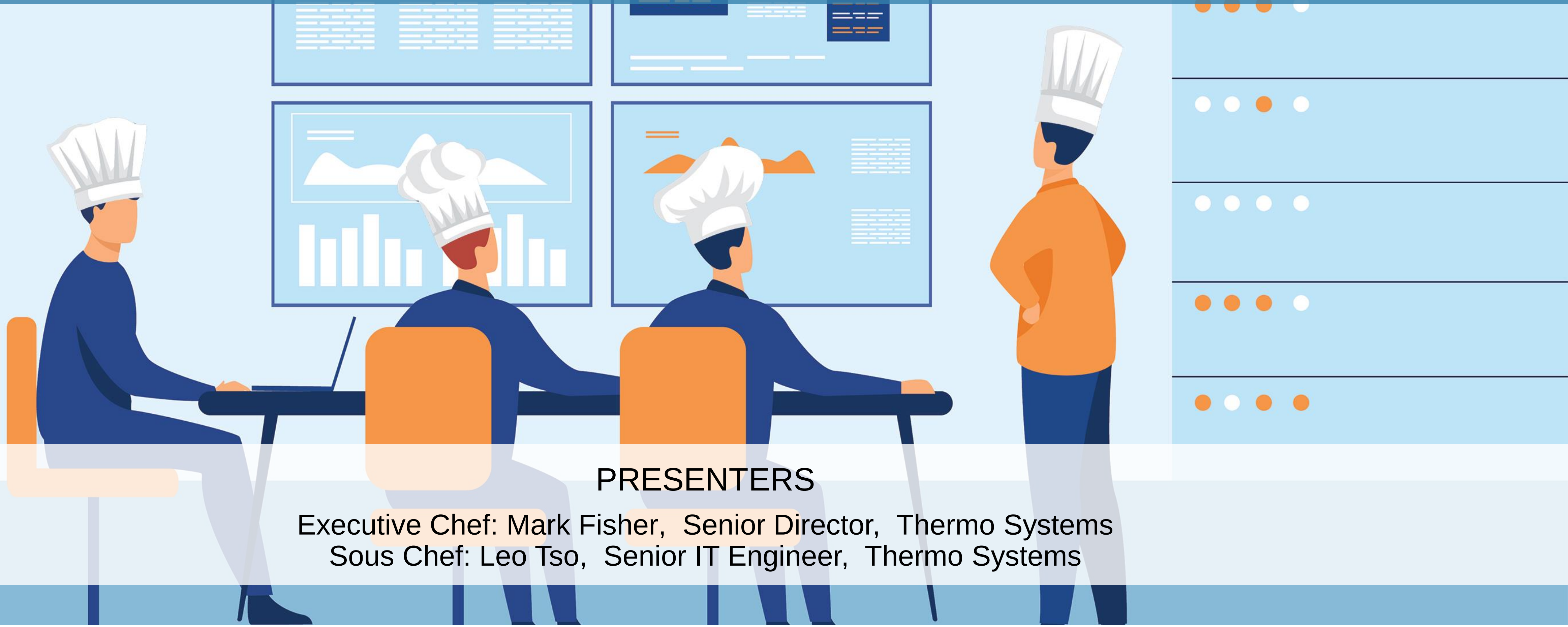
BRIDGE TO THE FUTURE

Feb. 16-18 | CONNECTING VIRTUALLY

WORKSHOPS | Thermal Distribution: March 2 | Microgrid: March 16

Baked In Cyber-Security

Princeton University



PRESENTERS

Executive Chef: Mark Fisher, Senior Director, Thermo Systems
Sous Chef: Leo Tso, Senior IT Engineer, Thermo Systems

CampusEnergy2021
BRIDGE TO THE FUTURE
Feb. 16-18 | CONNECTING VIRTUALLY
WORKSHOPS | Thermal Distribution: March 2 | Microgrid: March 16

THERMO SYSTEMS
INDUSTRIAL AUTOMATION & INFORMATION

INTERNATIONAL DISTRICT ENERGY ASSOCIATION

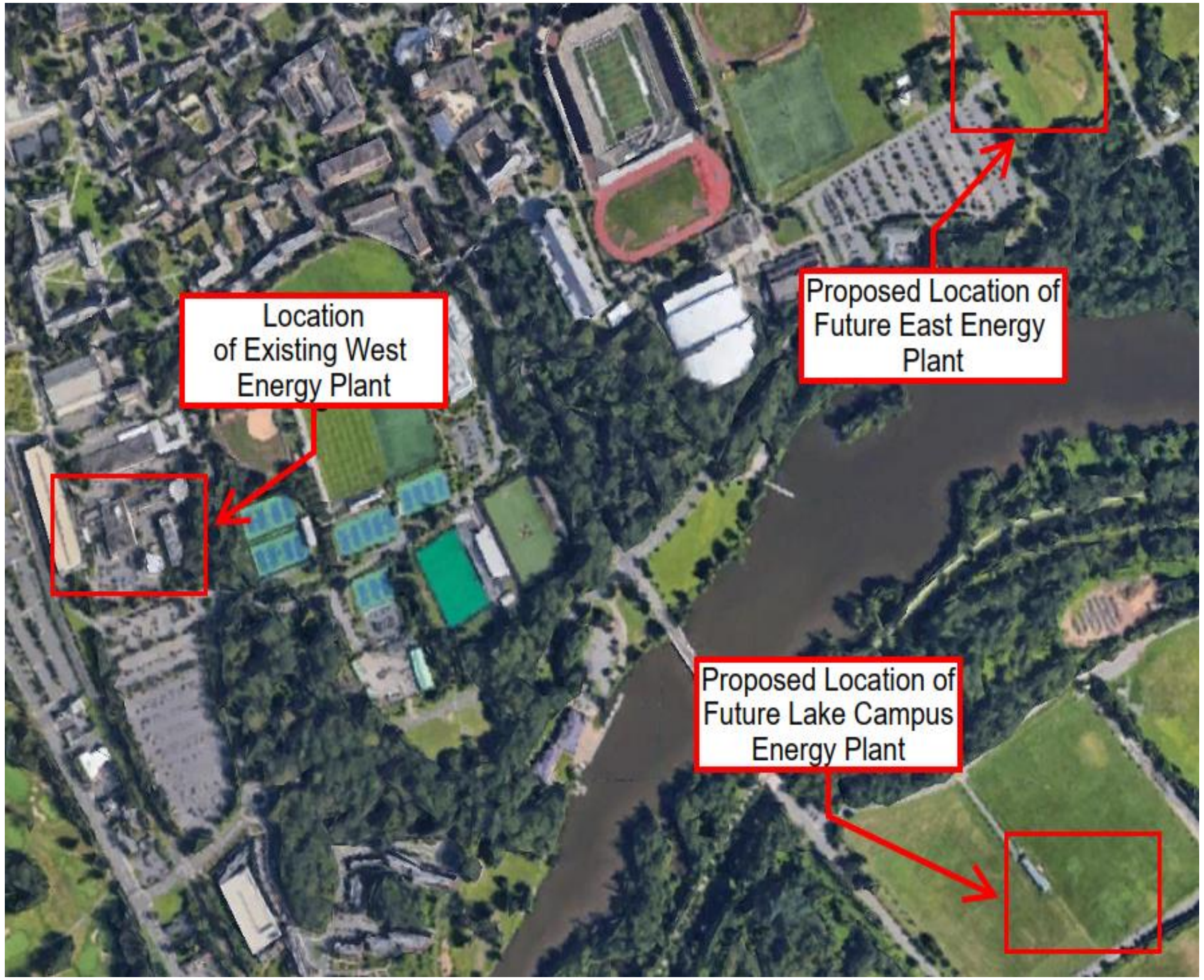
Q&A Will Not Be Answered Live

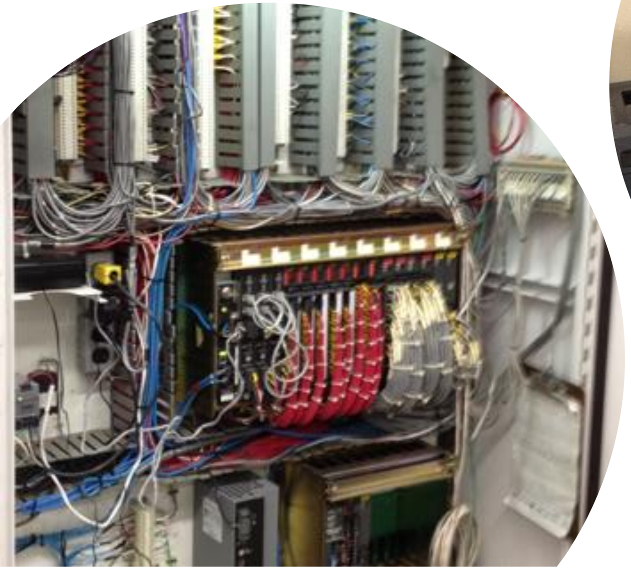
Please submit questions in the Q&A box.
The presenters will respond to questions off-line.

Origins

University Infrastructure Master Plan Initiatives Include:

- Replace equipment in the existing energy plant and campus buildings with more efficient, apropos, and environmentally friendly alternatives
- Begin to convert campus from steam to hot water heating
- Construct two new energy plants to support increasing demand, future GHG emission goals, and campus-wide heating scheme conversion
- MODERNIZATION OF THE EXISTING ENERGY PLANT CONTROL SYSTEM (EPCS) IN ORDER TO SUPPORT THE MASTER PLAN'S INITIATIVES





EPCS Modernization Drivers

- Control assets approaching EOL
- Server/workstation operating systems and application software no longer supported
- Running on proprietary, closed networks
  - Limits future expandability
  - Restricts desired future functionality
- Physical security to assets lacking
- Connection to “Outside World” not secure
- Anti-Virus protection non-existent
- Patching methodology extremely cumbersome

Problem Statement

Cyber-security must be baked in!

- The EPCS modernization effort must take cyber-security into account at every phase of the system's design, deployment, and operation
- It cannot be an afterthought that is "bolted on" at the last minute
- The technical, physical, and procedural aspects of cyber-security must all be considered during the design effort
- Several external vendors must be able to access the system for economic dispatch, regulatory monitoring, reporting, and remote support purposes.
    - All external connections must be as secure as possible and will be through the Campus Data Network. No direct connections to the internet.

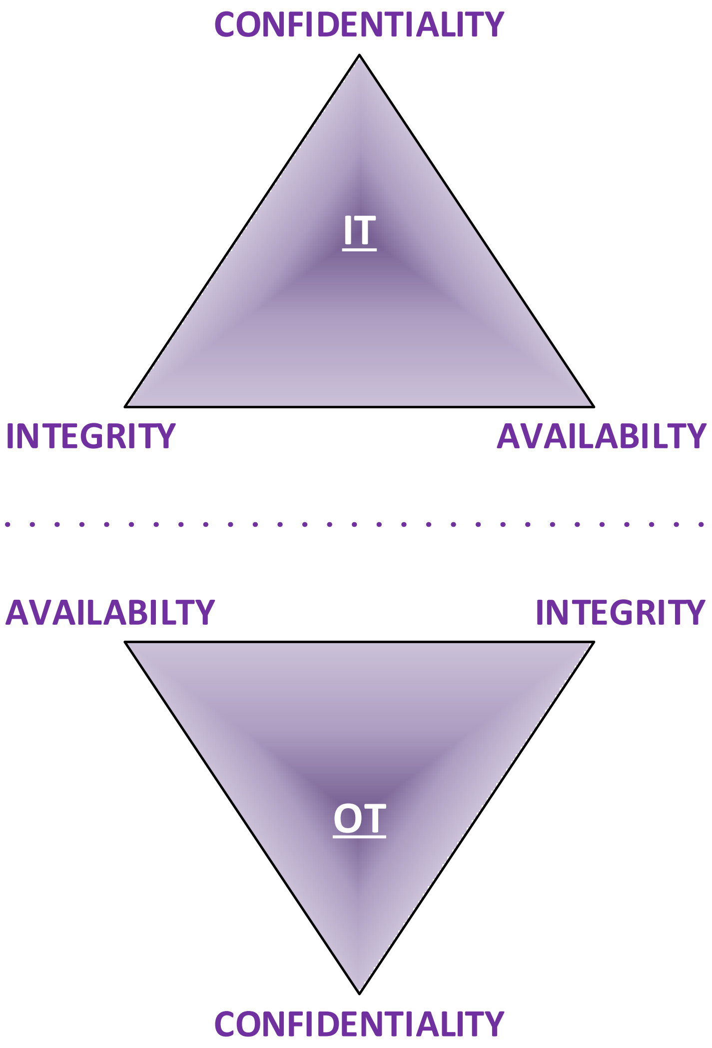
Baked in,
not sprinkled on

Where We Began

- Kicked off the cyber-security design effort as a project unto itself
- Included key stakeholders in the kickoff and all subsequent design activities – representatives from the following departments:
  - Engineering
  - University IT Personnel
  - Mission Critical OT Personnel
  - Energy Plant Operations
  - Energy Plant Maintenance

Notes On IT/OT Convergence

- University/Corporate IT and Mission Critical OT organizations have similar objectives from a cyber-security point of view
- However, the importance of those objectives to each organization are often 180° out of phase with each other
- It is important that each organization is aware of the other's drivers or an effective convergence is not possible



IT vs OT Design/Operation/Maintenance Considerations

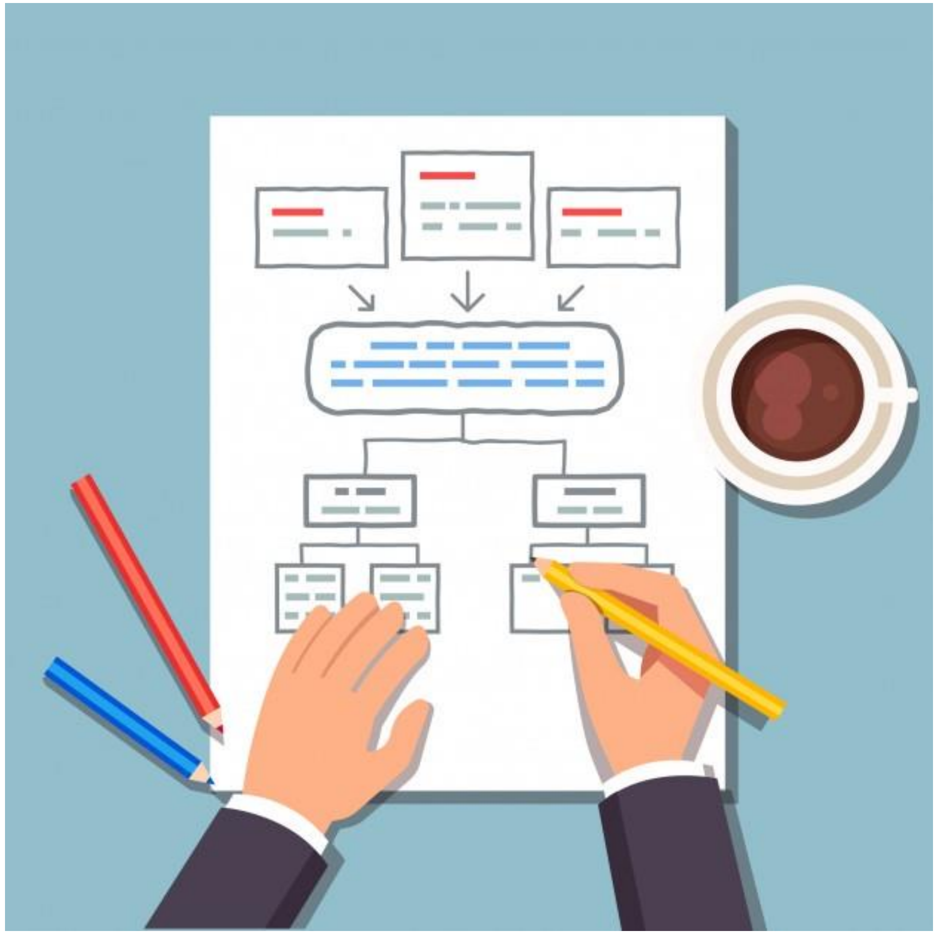
Consideration	IT Systems	OT Systems
Componentry	Often installed in secure, environmentally controlled areas like data centers.	Often installed directly on plant floors, even outdoors.
Routine Maintenance	Often powered down or rebooted during routine maintenance and troubleshooting.	Powering down or rebooting could result in loss of visibility to plant operations possibly resulting in loss of control, equipment damage, regulatory compliance issues, degradation of public confidence, injury or even death.
Patching	Often done automatically during off hours.	Should never be done automatically and should always occur during shifts when there are enough operational staff onsite to monitor the system for adverse affects of the patch. Patches should be validated by software vendors before deployment and should only occur to protect against know vulnerabilities or to take advantage of new/desired features.
AV Software	Definition files are often deployed automatically during off hours.	See Patching. A means to deploy AV definitions files and patches from a central location should be designed into the systems architecture.

The Recipe For Success

Automation System Security Plan (ASSP)

Develop a detailed ASSP that at a minimum includes:

- Defense in Depth (DiD) Strategy
- Network architecture concept design
- ISA99/IEC62443 model of network architecture concept
- Detailed network architecture depicting all network equipment and technical countermeasure appliances
- Technical countermeasure specifications
- User security levels and authentication, authorization, and accounting (AAA) framework
- List of physical countermeasures to deploy
- List of administrative policies and procedures
- IP address and VLAN schemes and listings
- Firewall Access Control Lists (ACLs)
- Distribution should be limited and controlled
- Document should be password protected



Preheat The Oven and Start To Prep

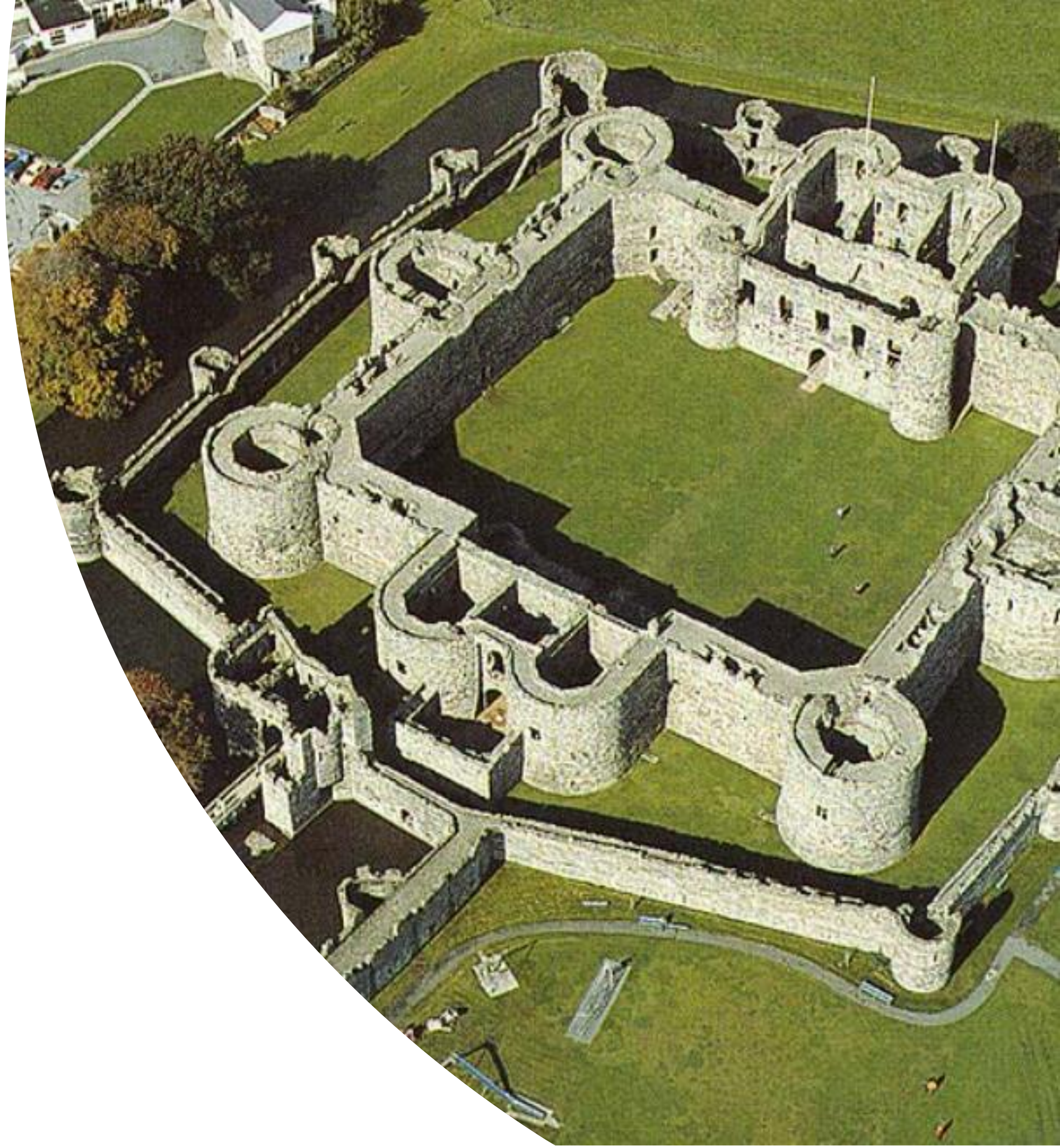
Defense in Depth Strategy

- A Defense in Depth (DiD) Strategy should be employed.

- There is no “Silver Bullet”.

- DiD countermeasures should be considered at three levels (The Ingredients):

  - Technical
  - Physical
  - Administrative

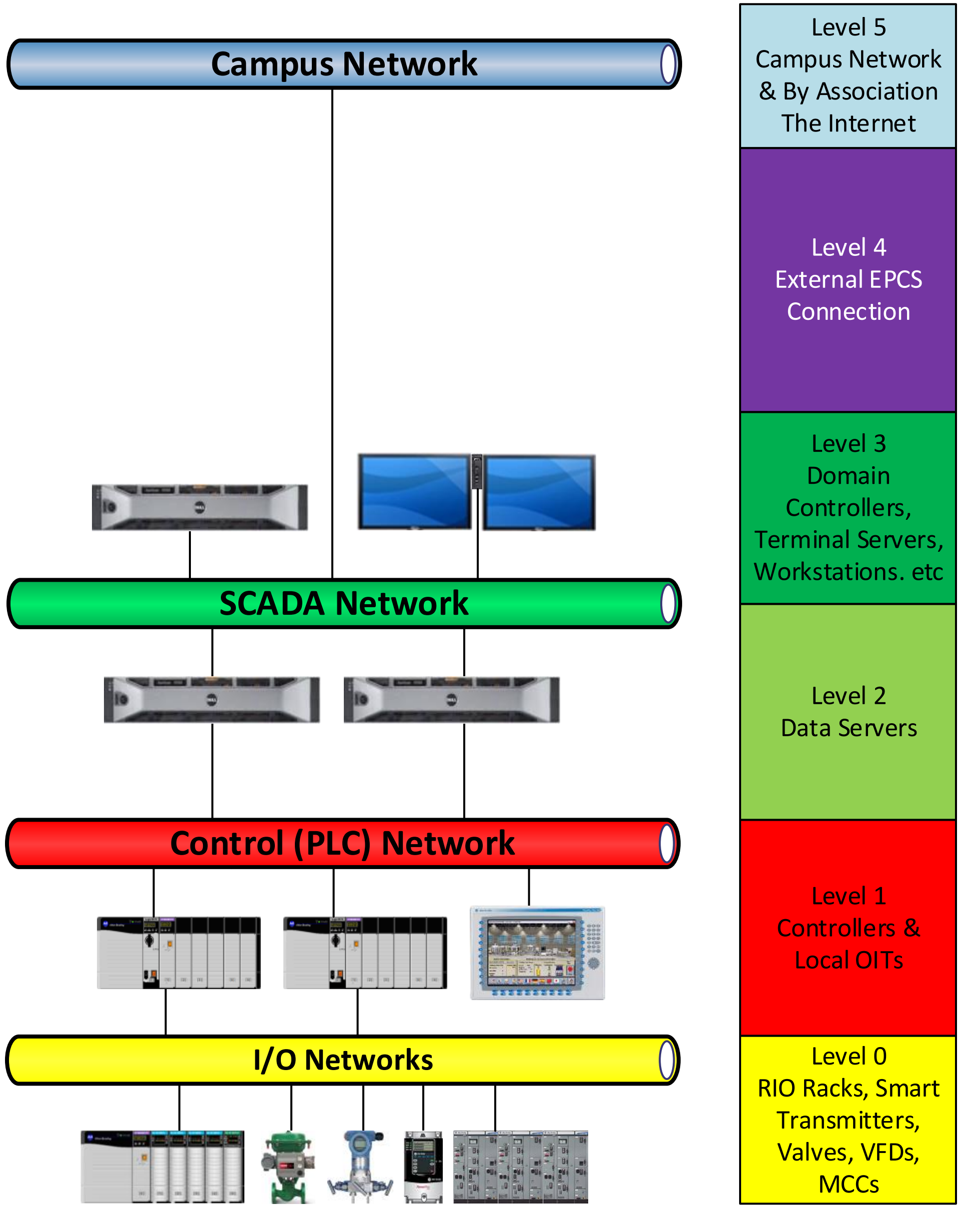


Add Ingredients and Mix Thoroughly

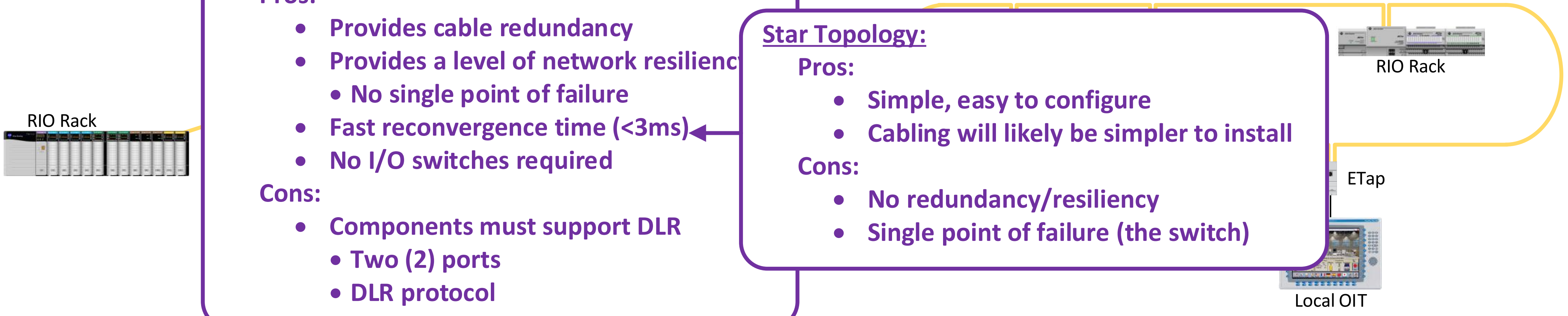
Network Architecture Concept Framework

Concept Framework should take into account:

- Redundancy/resiliency topologies
- Network segregation
  - Control (Level 1 PLC) & supervisory (Level 2/3 SCADA) networks
- Network separation
  - Campus (Level 5) & supervisory (Level 2/3 SCADA) networks
- Limit number of external threat vectors
  - Single point of connection to "Outside World"
  - Use of wireless technology was not a requirement
- Centralized:
  - Backup and restoration
  - User security control
  - Network monitoring
  - Patching and AV definition file deployment



I/O Network Topology Options Considered (Level 0)



Device Level Ring (DLR):

Pros:

- Provides cable redundancy
- Provides a level of network resiliency
  - No single point of failure
- Fast reconvergence time (<3ms)
- No I/O switches required

Cons:

- Components must support DLR
  - Two (2) ports
  - DLR protocol

Star Topology:

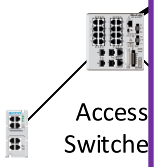
Pros:

- Simple, easy to configure
- Cabling will likely be simpler to install

Cons:

- No redundancy/resiliency
- Single point of failure (the switch)

Control & Supervisory Network Topology Options Considered (Levels 1, 2, 3)



Mesh Topology:

Pros:

- Provides cable redundancy

Cons:

- Does not provide any component r
- Cabling is very complicated
- Troubleshooting is very complicate
- Slow reconvergence times:
  - Spanning Tree (SPT): 20-50 sec
  - Rapid Spanning Tree (RSPT): 2-6 sec

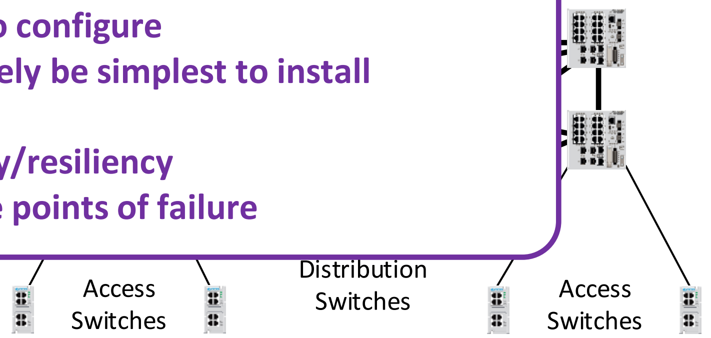
Star Topology:

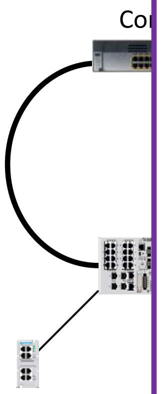
Pros:

- Simple, easy to configure
- Cabling will likely be simplest to install

Cons:

- No redundancy/resiliency
- Multiple single points of failure





Redundant Ring Topology:

Pros:

- Provides cable redundancy
- Provides component redundancy at t distribution levels
- Fast reconvergence times:
  - Resilient EtherNet Protocol (REP): 5
- Cabling is simpler then mesh topolog
- Troubleshooting is simpler than mesh

Cons:

- Requires twice the componentry at the core and distribution levels

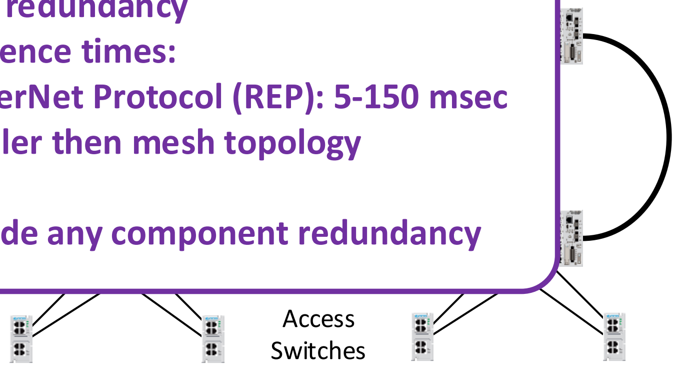
Ring Topology:

Pros:

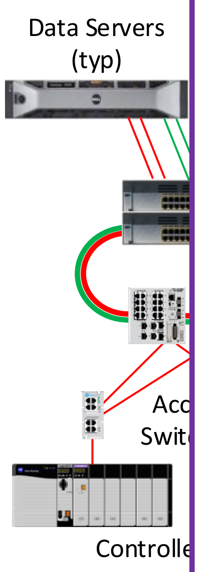
- Provides cable redundancy
- Fast reconvergence times:
  - Resilient EtherNet Protocol (REP): 5-150 msec
- Cabling is simpler then mesh topology

Cons:

- Does not provide any component redundancy



Control & Supervisory Network Segregation Options Considered (Levels 1, 2, 3)



Physical Segregation:

Utilizes:

- Two physically separate sets of compo cabling at the core and distribution le
- Proper subnetting (layer 2) and Virtual Networks - VLAN (layer 3) techniques still be used on each network

Pros:

- More secure than virtual segregation
- Control (PLC) and Supervisory (SCADA) are physically isolated to their respect

Cons:

- Uses twice the componentry and cablin and distribution levels when compare segregation

Virtual Segregation:

Utilizes:

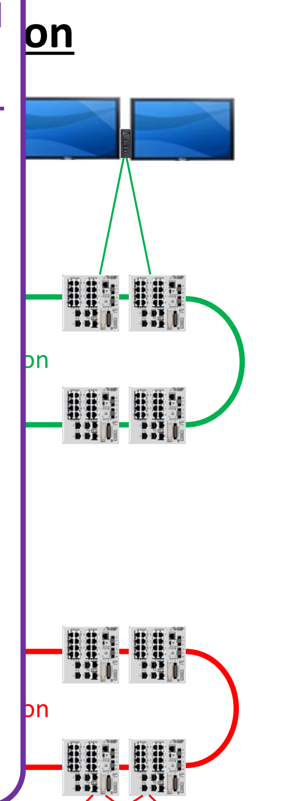
- Single set of componentry and cabling at the core and distribution levels
- Subnetting (layer 2) and Virtual Local Area Networks - VLAN (layer 3) techniques to virtually segregate the Supervisory (SCADA) and Control (PLC) networks from each other

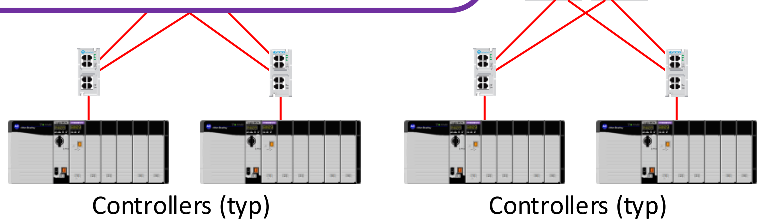
Pros:

- Uses half the componentry and cabling at the core and distribution levels when compared to physical segregation

Cons:

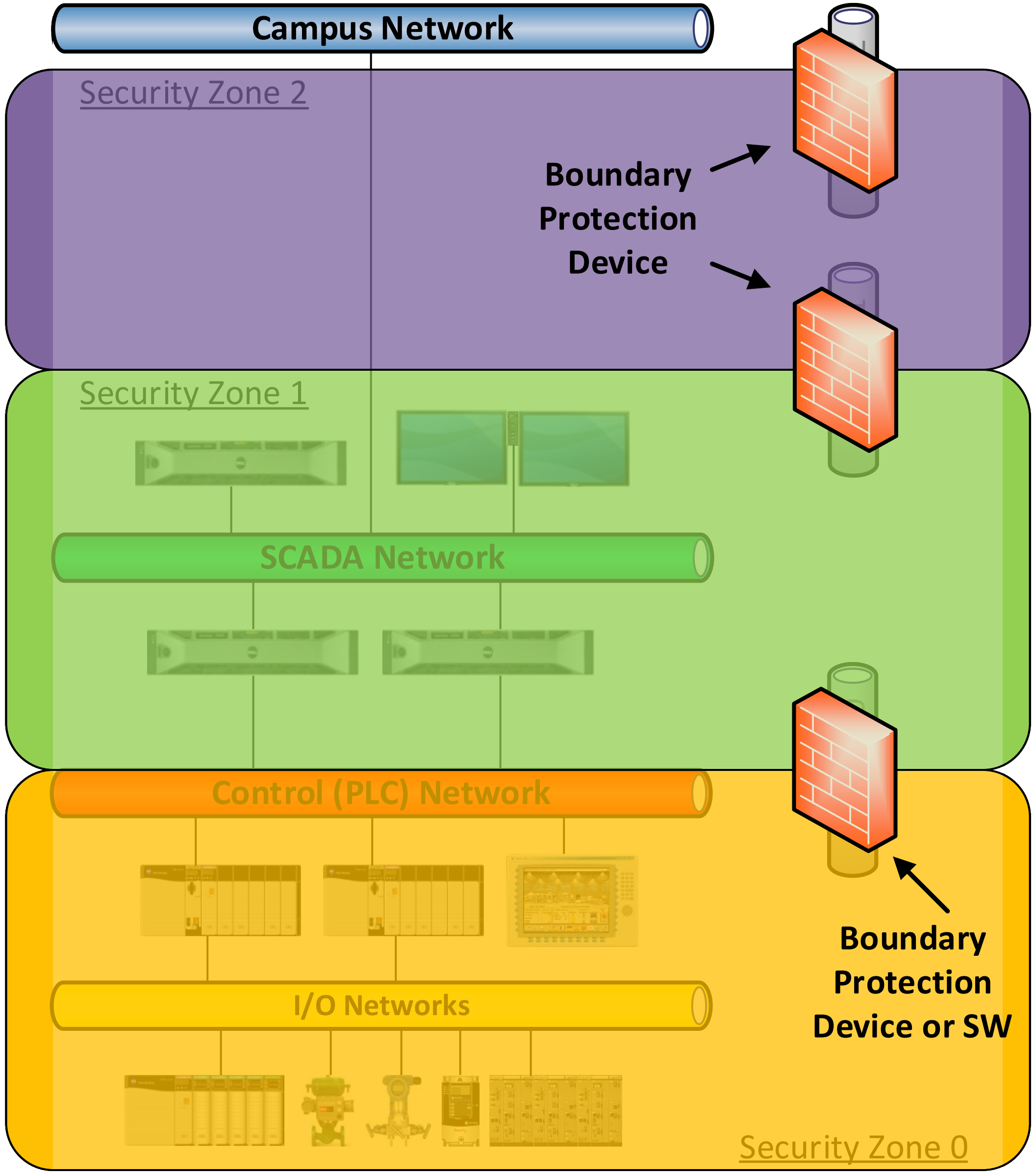
- Less secure then physical segregation
- All Control (PLC) and Supervisory (SCADA) network traffic traverses the ring which could affect throughput
- Detailed networking and routing experience required to implement and troubleshoot the network.





Modeling the Concept

- Begin with the previously designed conceptual network architecture.
- Use ISA99/IEC62443 security modeling techniques to define:
  - Security Zones
    - A grouping of logical or physical assets that share common security requirements
  - Communication Conduits
    - Logical grouping of communication paths "connecting" one security zone to another
  - Map the appropriate boundary protection device(s) onto each conduit.
    - Types of boundary protection devices include:
      - Air gap
      - Single firewall (hardware)
      - Unidirectional data diode (hardware/software)
      - De-Militarized Zone (DMZ) formed by two or more hardware firewalls
      - Firewall (software)



Supervisory & Campus Network Separation Options Consi

Unidirectional Data Diode:

Pros:

- Extremely secure method of network separation
- Allows "Outside World" connections, however, data can flow in only one direction – out from the plant

Cons:

- Data can flow in only one direction – out from the plant
- Data diode appliances tend to be expensive
- A thorough understanding of the type of data transferred is required

cure approach

s no connectivity to the "Outside World"

east expensive approach to implement

s no connectivity to the "Outside World"

t allow for 3rd party vendor connections for

es such as economic dispatch, regulatory

ring, and reporting

iode

ally historized

d alarm data

ere the data

nat is known

d predefined

ndalone Firewall:

s:

- Data can flow in in both directions – in and out from the plant
- 3rd party economic dispatching can be supported
- Remote support can be accomplished
- Next to air gap – least expensive method of separation

s:

- Least secure method of separation
- Detailed access control lists and firewall rules must be designed and routinely monitored in order to be effective

MZ)

De-Militarized Zone (DMZ) – Types Of DMZ Servers:

- Tier 2 Historian/Alarm/Event (HAE) Server
  - Data is mirrored from a tier 1 server located on the plant's supervisory (SCADA) network
  - Provides historical, alarm, and event data to "Outside World" while at the same time protecting the Tier HAE 1 server
- Reporting server
- 3rd party vendor interface servers:
  - Economic dispatch
  - Regulatory agencies
- Remote support jump servers
- Patching server
- Network monitoring server

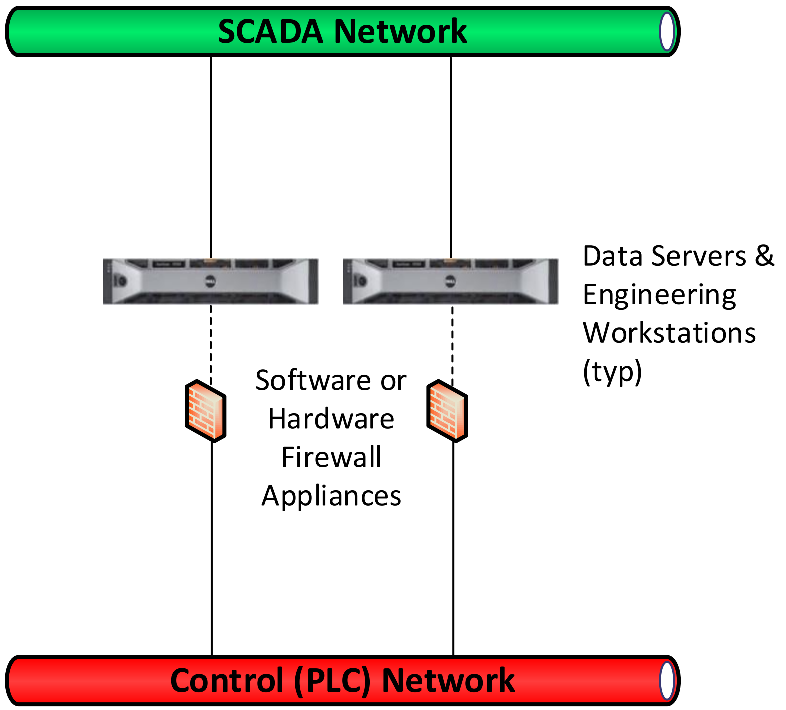
effective

Supervisory (SCADA-Levels 2/3) & Control (PLC-Level 1) Network Separation

- There is no direct link between these two networks

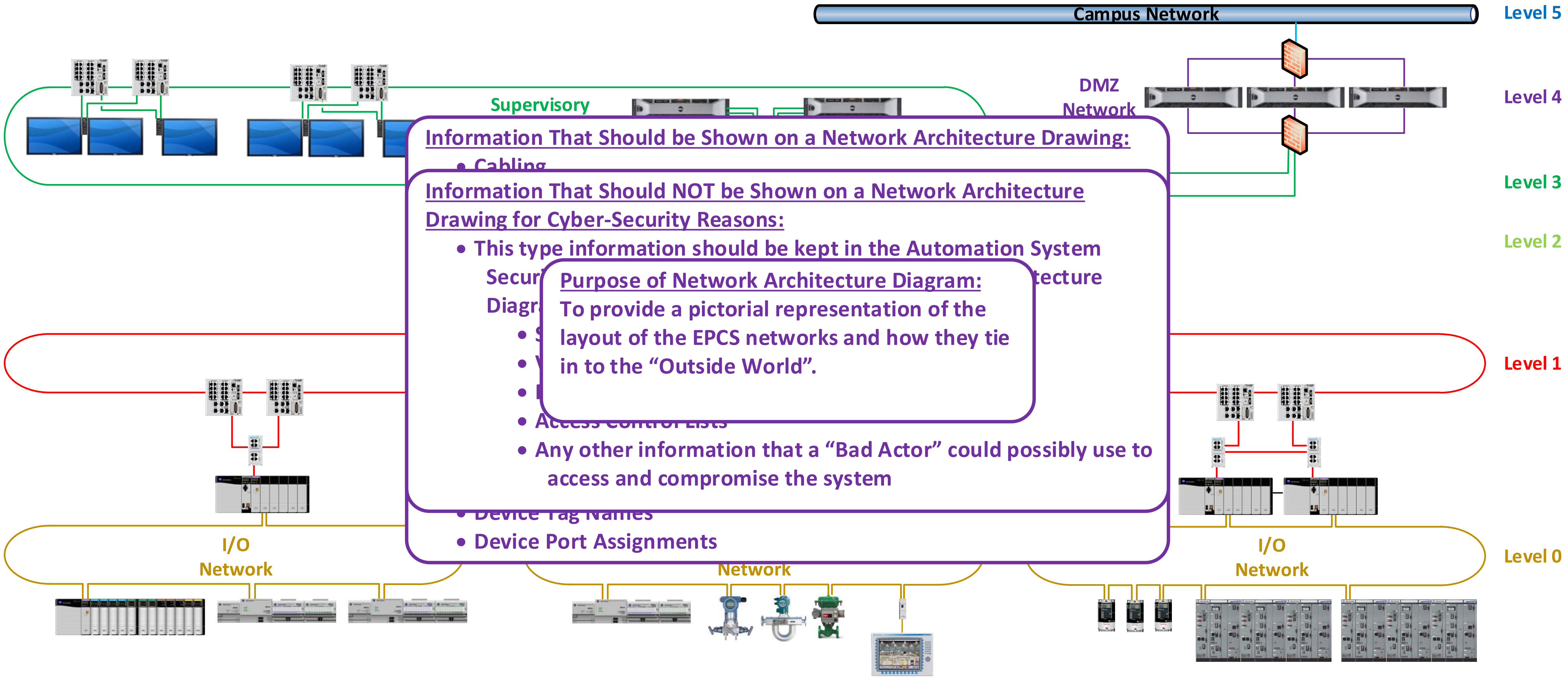
- Only two types of assets span these two networks
  - Data Servers
  - Engineering Workstations

- Two types of boundary devices were considered
  - Hardware
  - Software



Place in Oven and Bake Until Secure

Detailed Network Architecture



Information That Should be Shown on a Network Architecture Drawing:

- Cabling
- Device Tag Names
- Device Port Assignments

Information That Should NOT be Shown on a Network Architecture Drawing for Cyber-Security Reasons:

- This type information should be kept in the Automation System Secur… …tecture Diagr…
  - S…
  - V…
  - I…
  - Access Control Lists
  - Any other information that a "Bad Actor" could possibly use to access and compromise the system

Purpose of Network Architecture Diagram:

To provide a pictorial representation of the layout of the EPCS networks and how they tie in to the "Outside World".

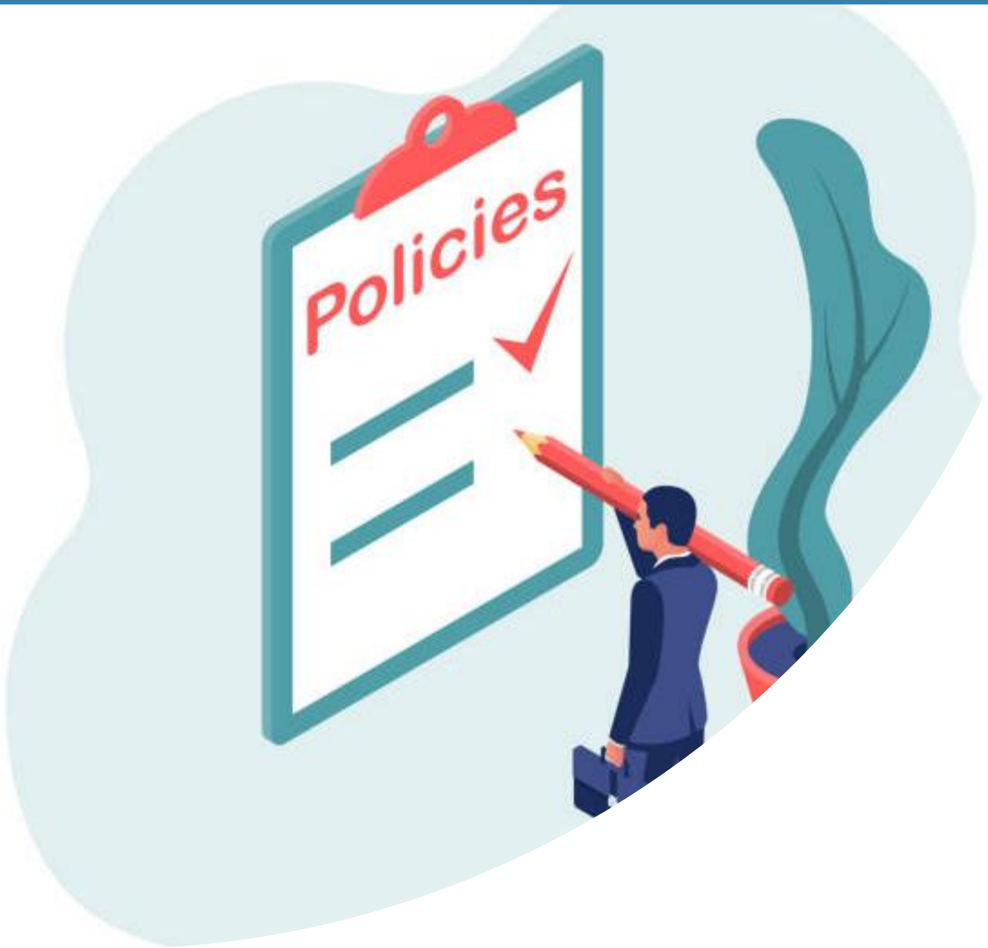
Physical Security Countermeasures Considered

- Avoid use of office grade equipment/cabling in industrial environments

- “Harden/Remove” Off-The-Shelf (OTS) software that comes pre-loaded on servers/workstations from manufacturers
  - Games
  - Internet browsers
  - Audio players
  - Camera utilities

- Use centralized:
  - Patching server
  - Mass storage device for backup, archival, and restoration
  - Network monitoring server

Administrative Policies & Procedures Considered



- Create EPCS specific security procedures
- Define the “hows”
- Include the following (at a minimum)
  - Physical access procedure
  - Cyber access procedure
  - Removable media usage procedure
  - Procedure to apply for a user account
  - User account maintenance procedures
  - Engineering workstation access procedure
  - Procedure to allow connection of vendor owned assets to EPCS network(s) for maintenance/troubleshooting
  - Procedure to apply for remote access privileges
  - Change control/configuration management procedures
  - Patch management/deployment procedure
  - AV definition file management/deployment procedure

Lessons Learned

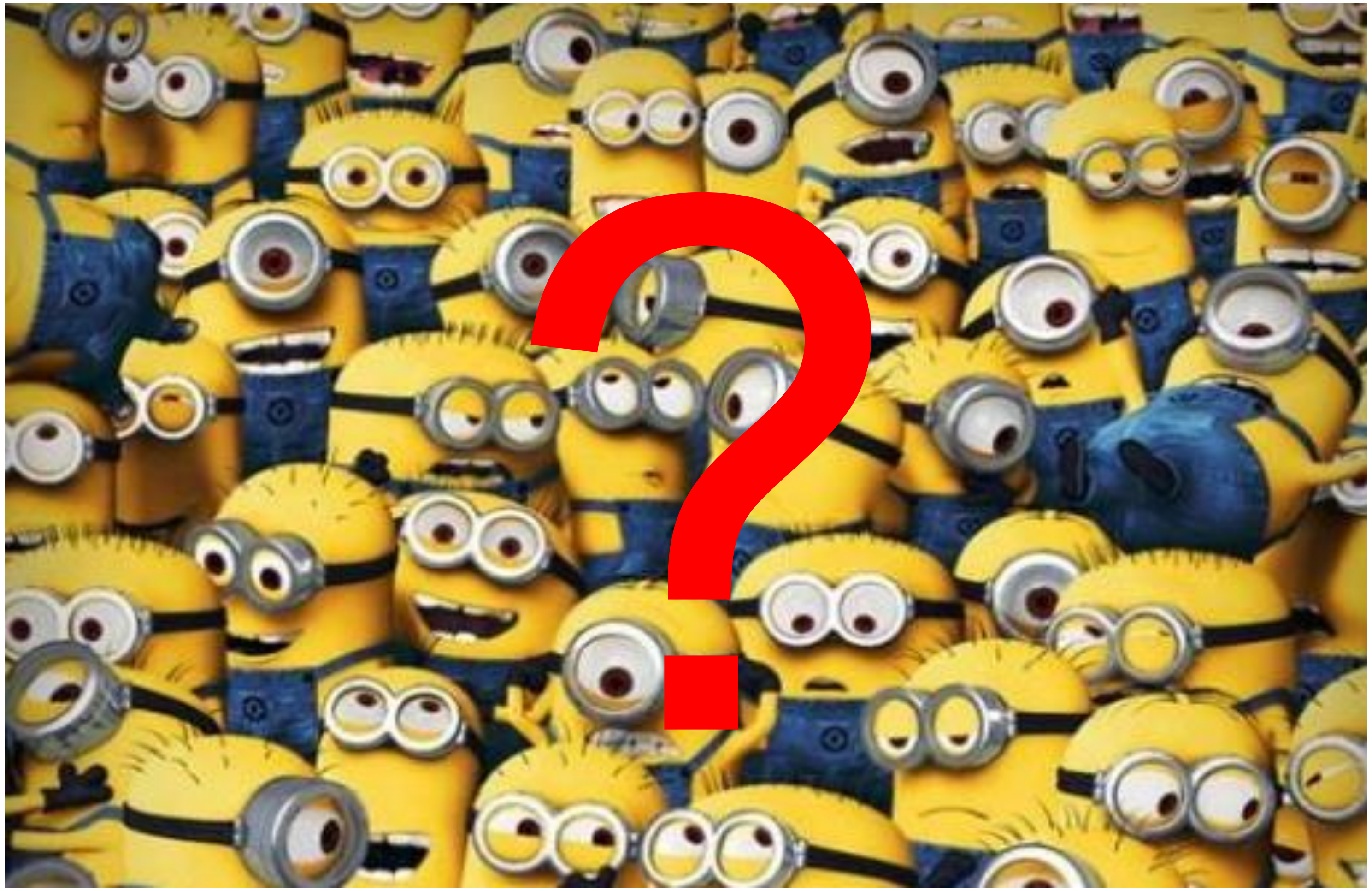
- Begin with a good recipe – the Automation System Security Plan (ASSP).

- Preheat and prep – Employ good Defense in Depth (DiD) strategies at every level of the design.

- Ingredients - Technology, Physical, and Administrative Countermeasures are the key ingredients of every good cyber-security design.

- Add ingredients – Start with a solid Conceptual Network Architecture Framework. Add in the Technology Countermeasures.

Questions?



Thank You!

Mark Fisher

Sr. Director
Thermo Systems, LLC
mark.fisher@thermosystems.com

- 32+ Years of Systems Integration Experience
- ISA Certified Automation Professional (CAP)
- ISA-99/IEC-62443 Certified Cyber Security Fundamentals Specialist (CSFS)
- Author: Instrumentation & Controls Chapter - IDEA District Cooling Best Practice Guide
- BSEE

Leo Tso

Sr. IT Engineer
Thermo Systems
leo.tso@thermosystems.com

- 17+ Years of IT/OT Experience
- Cisco Certified Network Professional (CCNP): Routing & Switching
- Cisco Certified Network Associate (CCNA): Security, Routing & Switching
- Cisco Certified Design Associate (CCDA)
- ISA99/IEC62443 Certified Cyber Security Fundamentals Specialist (CSFS)
- EC-Council Certified Ethical Hacker (CEH)
- CompuTIA Certified A+ Technician
- Microsoft Certified Professional (MCP)
- VMWare Certified Associate (VCA)
- BACS