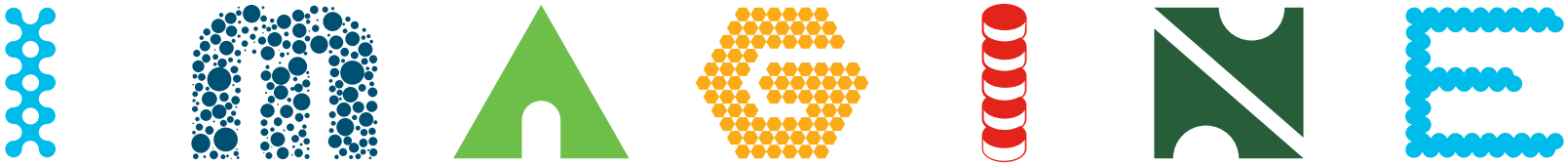


INTUITIVE

Cisco live!

June 10-14, 2018 • Orlando, FL

#CLUS

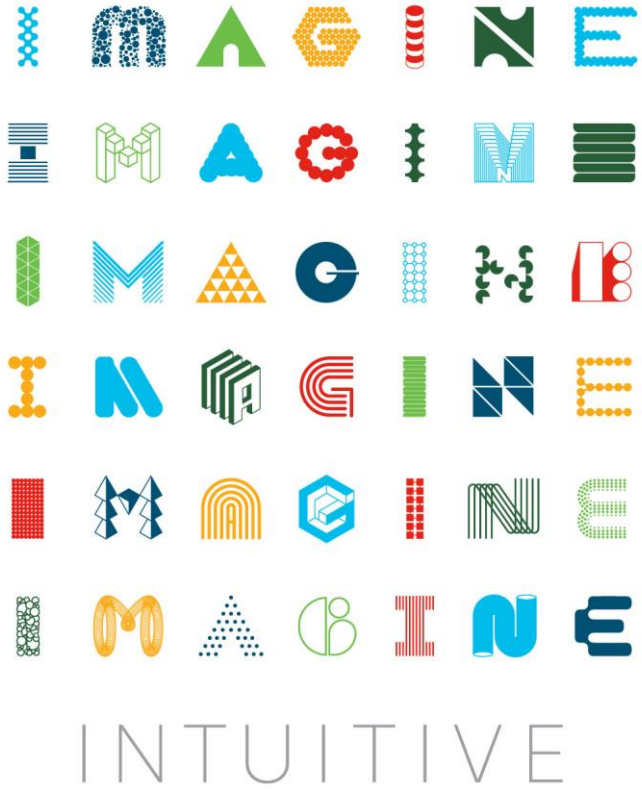
Industrial Security: IT vs OT Deployment Practices

Robert Albach ralbach@cisco.com

Product Line Manager

Industrial Security

BRKIOT-2115



Cisco Webex Teams

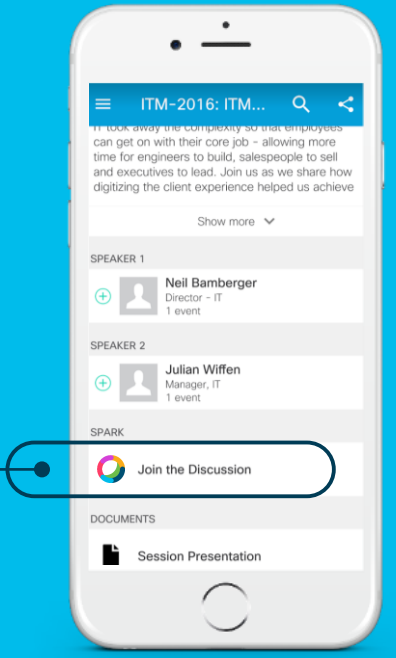
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.



cs.co/ciscolivebot#BRKIOT-2115

$1.5+ Billion

Source:

Government mandated financial statements across industrial companies

2017's Top Security News

2018's Top Security News

Boeing & Aerospace | Business | Technology

Boeing hit by WannaCry virus, but says attack caused little damage

Originally published March 28, 2018 at 3:16 pm | *Updated March 28, 2018 at 9:16 pm*

ANDY GREENBERG SECURITY 12.14.17 10:00 AM

UNPRECEDENTED MALWARE TARGETS INDUSTRIAL SAFETY SYSTEMS IN THE MIDDLE EAST

AutoSploit

As the name might suggest AutoSploit attempts to automate the exploitation of remote hosts. Targets are collected automatically as well by employing the Shodan.io API. The program allows the user to enter their platform specific search query such as; `Apache`, `IIS`, etc, upon which a list of candidates will be retrieved.

s7-metasploit-modules

Siemens Simatic S7 Metasploit Modules

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

April 2018 Lesson: Bad Headlines; System Boundaries

INSECURE SCADA SYSTEMS BLAMED IN RASH OF PIPELINE DATA NETWORK ATTACKS

by Lindsey O'Donnell

April 4, 2018 , 10:12 am

After a cyberattack shut down numerous pipeline communication networks this week, experts are stressing the importance of securing third-party systems in supervisory control and data acquisition (SCADA) environments.

Technology

Cyberattack Pings Data Systems of At Least Four Gas Networks

By Naureen S Malik, Ryan Collins, and Meenal Vamburkar
April 3, 2018, 1:29 PM CDT *Updated on April 4, 2018, 8:39 AM CDT*

mrt★ News Sports Business & Energy Lifestyle Entertainment Reader Services

Cyber attack shuts Energy Transfer's pipeline data system

Energy Transfer system connects gas suppliers in Permian to customers out west

Ryan Collins and Meenal Vamburkar, Bloomberg Updated 2:30 pm, Monday, April 2, 2018

Goal of this Presentation:
Educate and Prepare you to provide security for industrial environments.

Our Assumptions About You:

You are primarily an IT professional with current or pending operational responsibilities.

This *MAY* be your first introduction to industrial security.

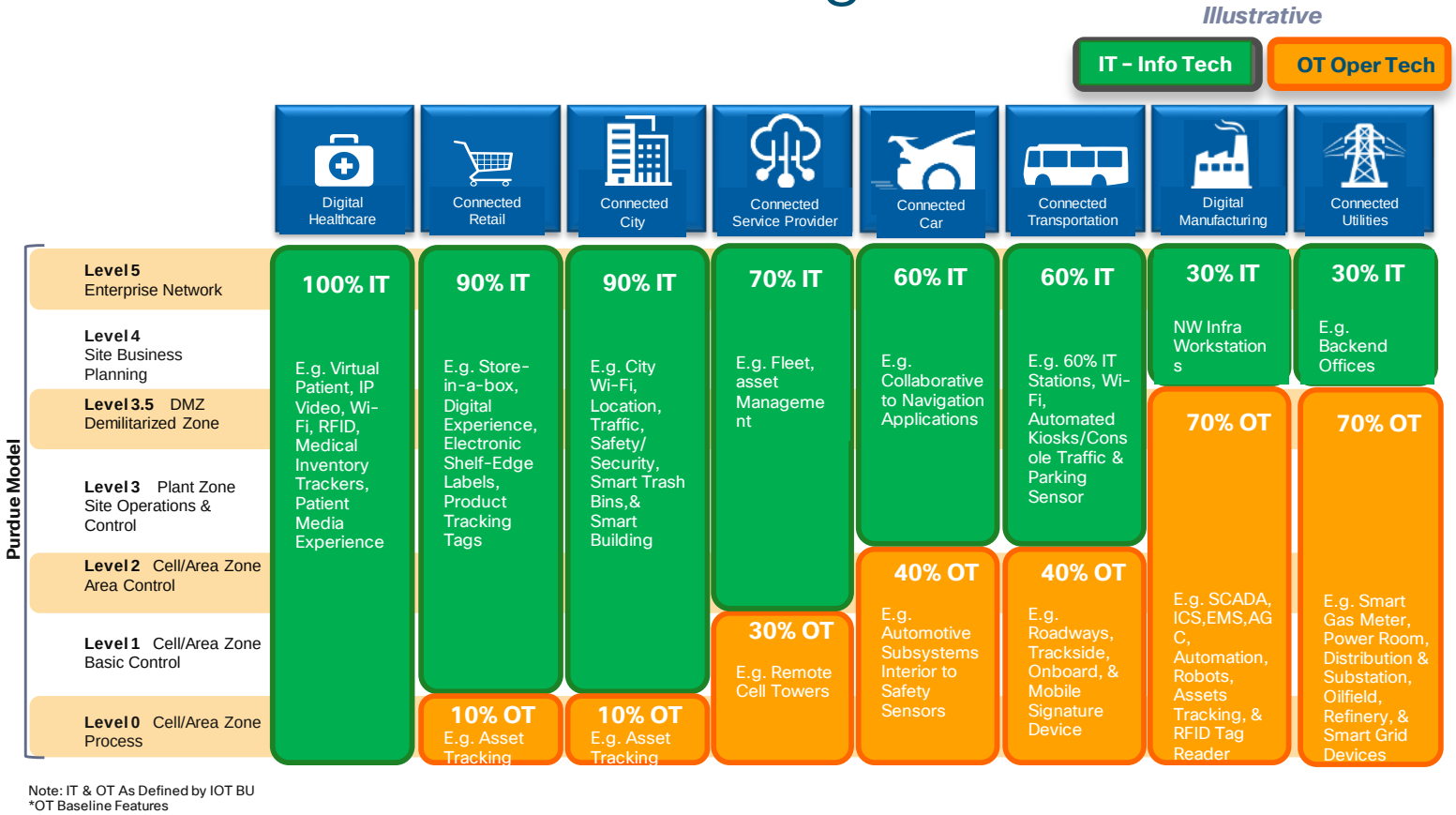
Agenda

- Information and Industrial Network Differences
- Industrial Protocols – their security challenges
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 4 Attack Discussions
- Closing / Question & Answer

What is the OT Thing?

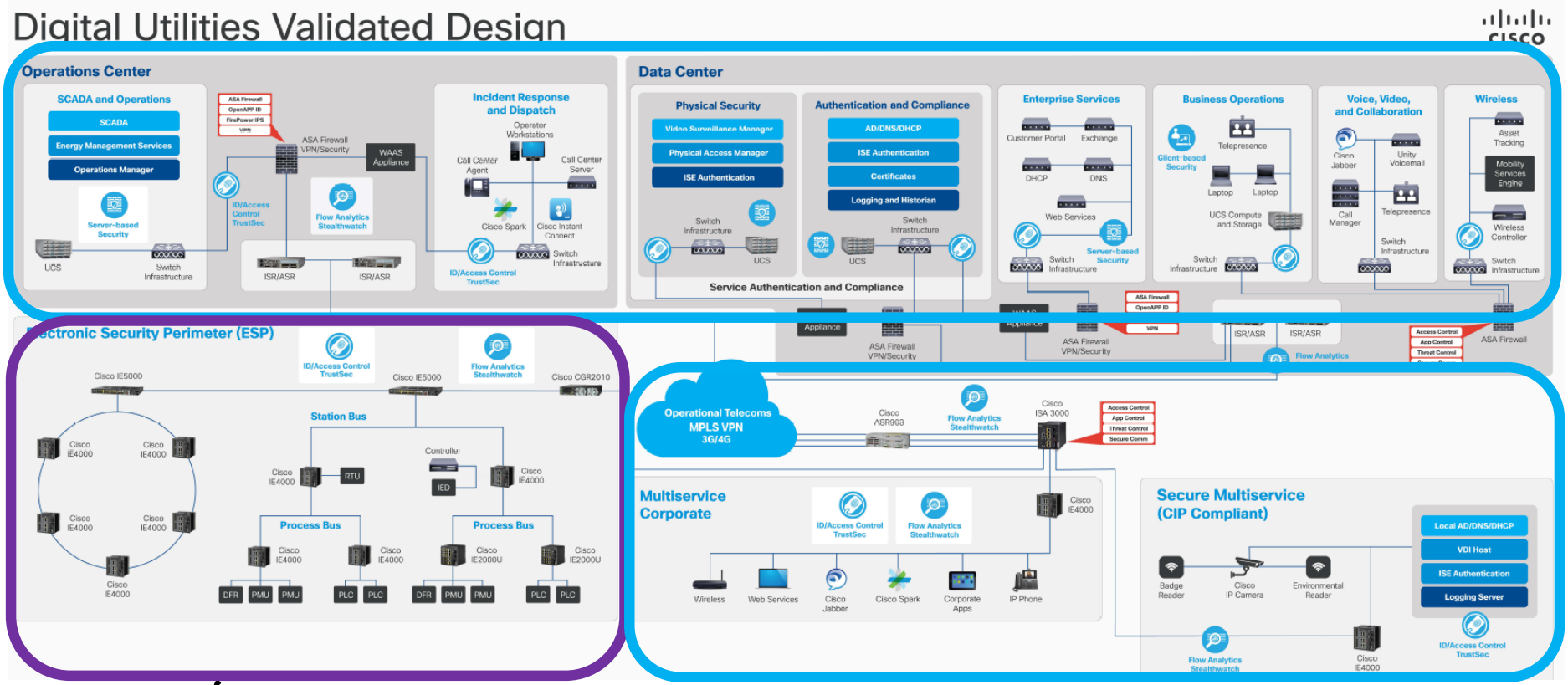
- Operations Technology
  - “Industrial” NW and Compute
    - Intelligent Electronic Devices (IEDs)
    - Autonomous but highly limited
  - More than SCADA
    - ...and what is that SCADA(Supervisory Control and Data Acquisition) thing?
    - Or is that ICS (Industrial Control Systems)?
    - Same / Different
    - Depends on your POV

Holistic View of Vertical Segments



Note: IT & OT As Defined by IOT BU
*OT Baseline Features

OT / IT Technology Splits – Electric Transmission



How OT Networks were Built

- Manufacturing
  - Ad Hoc – Built by our paint system provider.
  - Multiple sources – Paint sprayer and drier.
  - Assembled – Conveyer belt through paint sprayer into drier.

- Utilities
  - Top Down – “We built this sub-station.”
  - Integrated – “We interface with LCRA here (grid interconnects).”
  - Telecomm groups – <if the utility is large enough>

How OT Networks were Built- 2

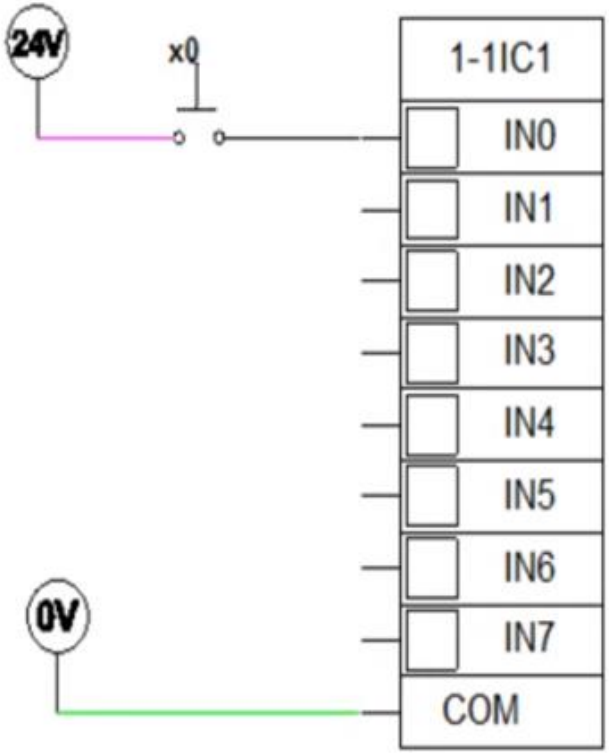
- Transport
  - Bus / Train / Plane
  - Ticketing systems / boarding systems / physical security / signaling / control / etc.
  - Each from a different source / different “network”

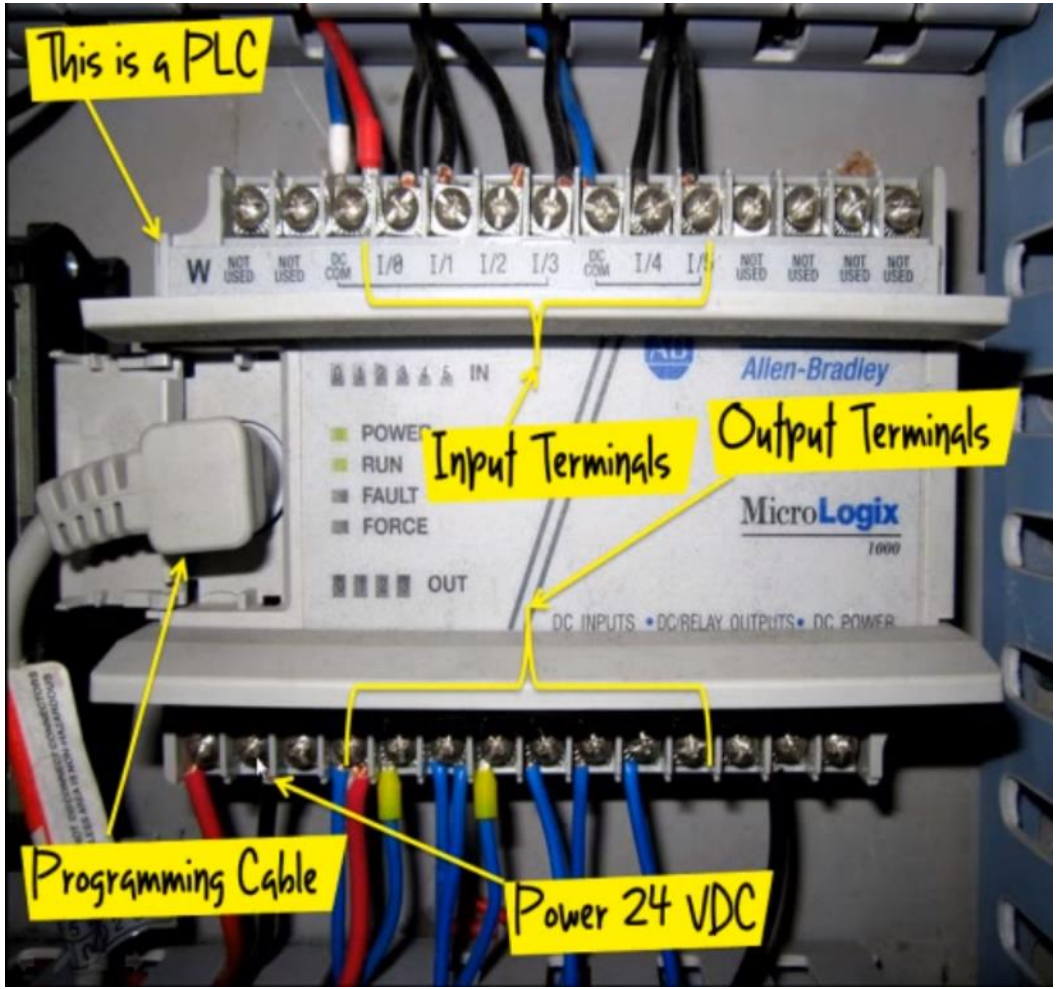
- Oil and Gas / Mining
  - Upstream – exploration / drilling / production /
  - Midstream – transport: barge / rail / pipeline
  - Downstream – refinery / pipeline / retail

Assets to Protect

	Asset	Description	Examples and Notes
	IED	Intelligent Electronic Device – Commonly used within a control system, and is equipped with a small microprocessor to communicate digitally.	Sensor, actuator, motor, transformer, circuit breaker, pump
	RTU	Remote Terminal Unit – Typically used in a substation or remote location. It monitors field parameters and transmit data back to central station.	Overlap with PLC in terms of capability and functionality
	PLC	Programmable Logic Controller – A specialized computer used to automate control functions within industrial network.	Most PLCs do not use commercial OS, and use “ladder logic” for control functions
	HMI	Human Machine Interfaces – Operator’s dashboard or control panel to monitor and control PLCs, RTUs, and IEDs.	HMIs are typically modern control software running on modern operating systems (e.g. Windows).
	Supervisory Workstation	Collect information from industrial assets and present the information for supervisory purposes.	Unlike HMI, a supervisory workstation is primarily read-only.
	Data Historian	Software system that collects point values and other information from industrial devices and store them in specialized database.	Typically with built-in high availability and replicated across the industrial network.
	Other Asset	Many other devices may be connected to an industrial network.	For example, printers can be connected directly to a control loop.

How to Wire a PLC

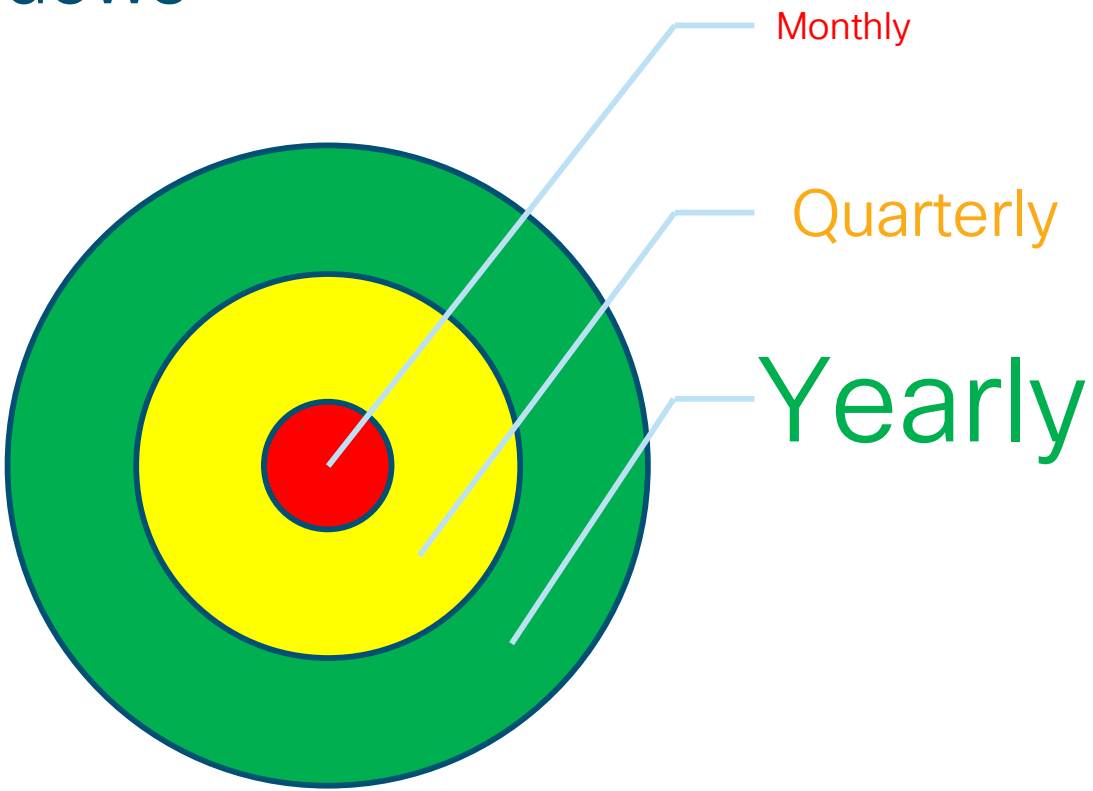




IT/OT Differences in Priorities

	IT Network	Operational Network
Focus	Protecting Intellectual Property and Company Assets	24/7 Operations, High OEE, **Safety**, and Ease of Use
Priorities	1. Confidentiality 2. Integrity 3. Availability	***1. Availability*** ***2. Integrity*** ***3. Confidentiality***
Types of Data Traffic	Converged Network of Data, Voice and Video (Hierarchical)	Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical)
Access Control	Strict Network Authentication and Access Policies	Strict Physical Access Simple Network Device Access
Implications of a Device Failure	Continues to Operate	Could Stop Processes, Impact Markets, Physical Harm
Threat Protection	Shut Down Access to Detected Threat and Remediate	Potentially Keep Operating with a Detected Threat
Upgrades and Patch Mgmt	ASAP During Uptime	Scheduled During Downtime

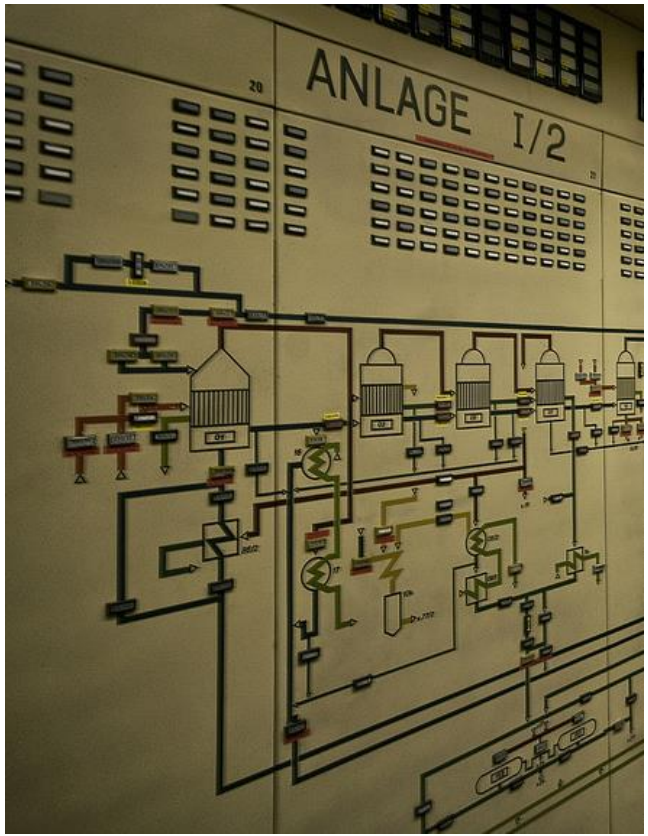
Maintenance Windows



Every Network has its Challenges

IT Networks
- Many Applications
- Dynamic
- Interoperability unconstrained
- Knowledgeable workers in market

OT Networks
- Fixed / Limited Applications
- Stagnant / Stable
- Limited interoperability



IT Networks – Data Flows

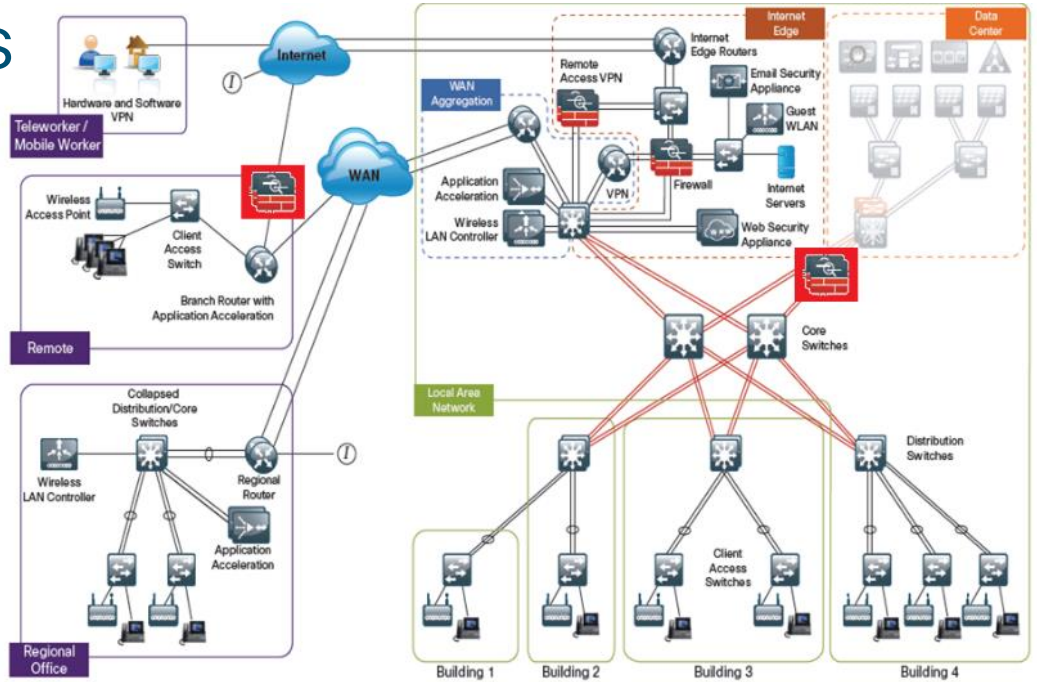
End points are smart – human driven.

If data leaves – it goes far...

- Web – data center / internet
- Email
- File / Print shares
- Nearby devices largely unrelated

When the end points talk:

- Short conversations
- Many connections
- Short TCP sessions – SYN SYN/ACK ACK
  - a few secs max
- Largely egalitarian – anybody talk to anybody

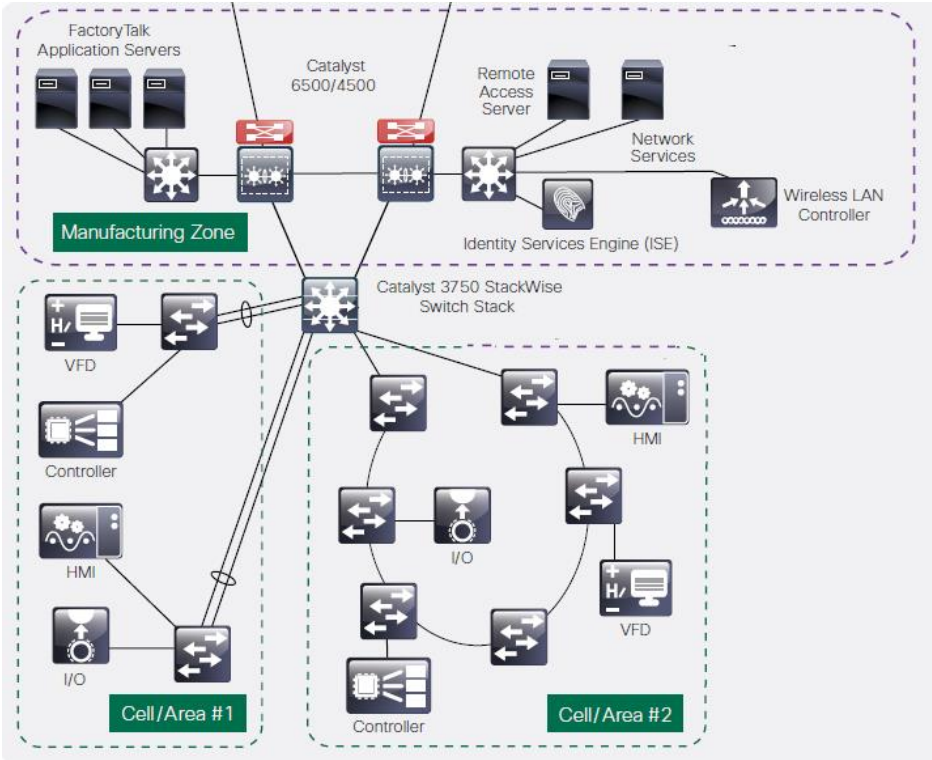


OT Networks – Data Flows

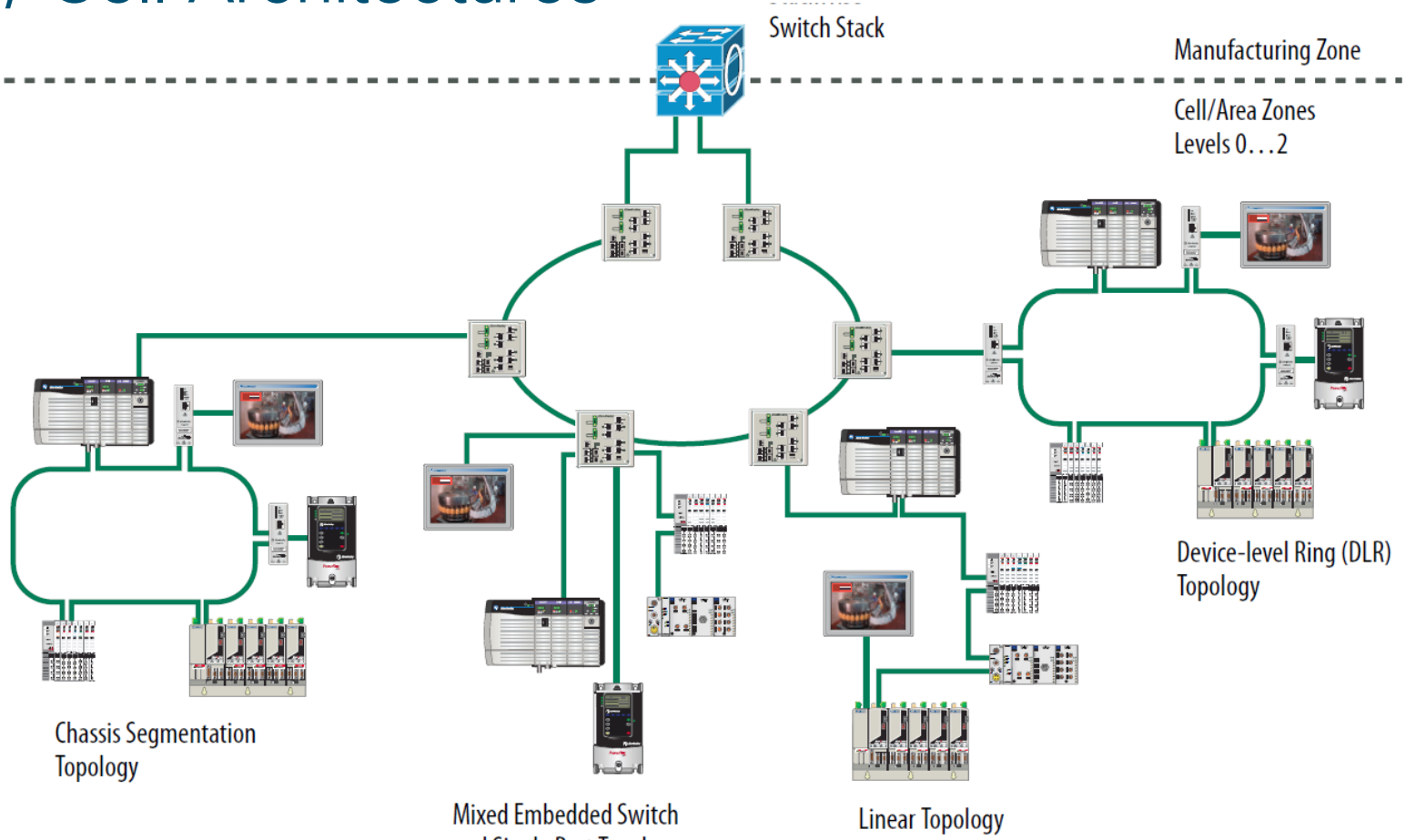
End points are not smart – repetitive.

If data leaves – it stays close
Interaction is largely local
Movement not very visible
if it does leave – streams out
Not a conversation usually

When the end points talk:
Long conversations
Few connections
Long TCP sessions – lots of keep alives– hours / days!

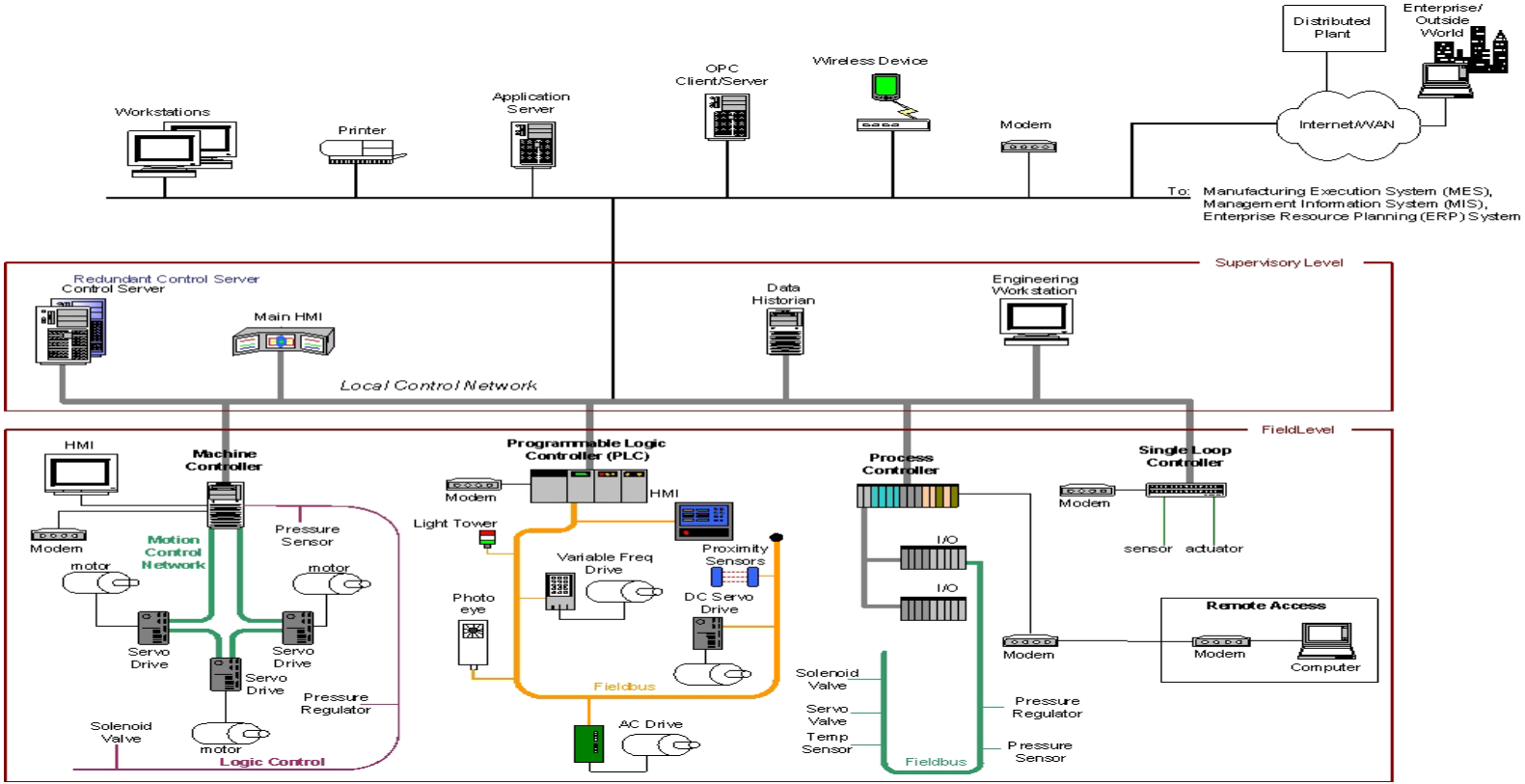


Machine / Cell Architectures

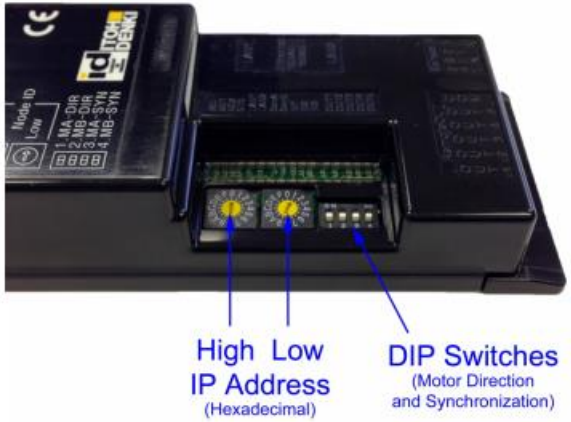


Rockwell Embedded Switch Technology Architectures

By Count most of the “things” in IoT: Won’t have an IP Address



How To:
Set an IP Address



Switch	Position	Description
IP Address High Byte	0 ~ F	Hexadecimal setting of IP address' last octet. 192.168.1.xxx Example 1: High Byte: "0" Low Byte: "1" Hexadecimal value "01" = 1 (decimal) IP Address: 192.168.1.1 Example 2: High Byte: "A" Low Byte: "7" Hexadecimal value "A7" = 167 (decimal) IP Address: 192.168.1.167
IP Address Low Byte	0 ~ F	

...and TIME is different too.

- NTP – Network Time Protocol
  - Precision levels – coarse
  - CPU or mother board oscillator
- PTP – Precision Timing Protocol
  - Precision levels 100 ns
  - Specialized HW <Phy level>

Industrial Solutions

Time-Sensitive Networking:
A Technical Introduction

Smart Grid

Environmental Needs

- Obvious – More strenuous
  - Cold / Heat
  - Vibration / Shock
- Next Obvious – Enclosures not enough
- Not so Obvious
  - Operating Environment
  - Storage Environment

Operating Environment – -40C to 60C in a fully enclosed cabinet (no airflow)

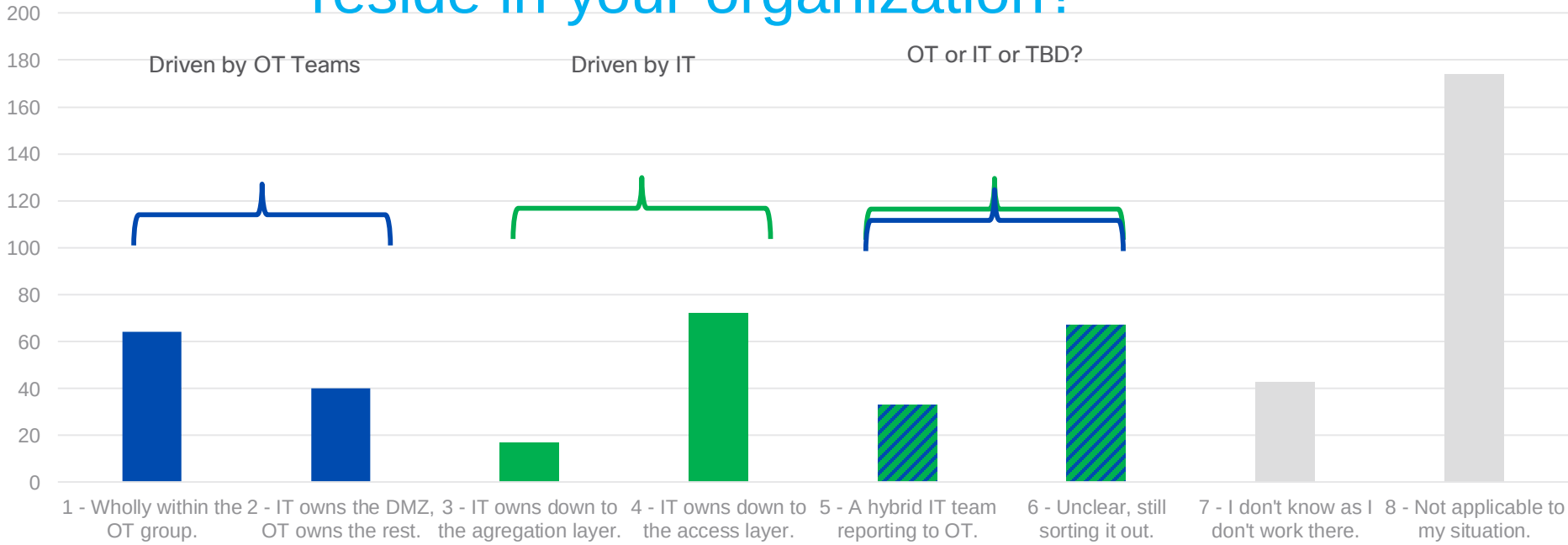
Storage Environment – Temperature: -40 to +85 degrees C

Industrial Needs are More than Environmental

- Driven by the IT vs. OT differences discussed
  - Latency over Throughput
  - Application control over Threat control
  - Simplicity over Sophistication
  - This equipment *might* get swapped out in a decade.
  - …Availability over Security
- Power, alarm connectors, IO connector are often different

Organizational Questions: The Hardest Part

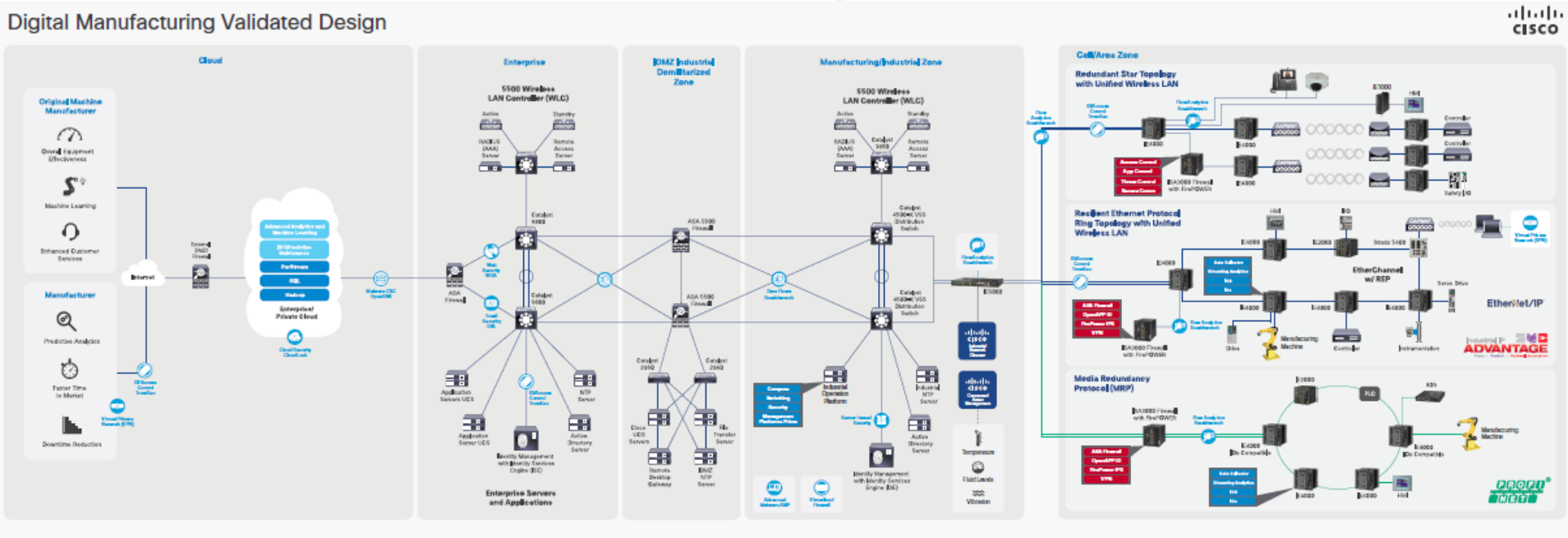
Where does the security role for OT reside in your organization?



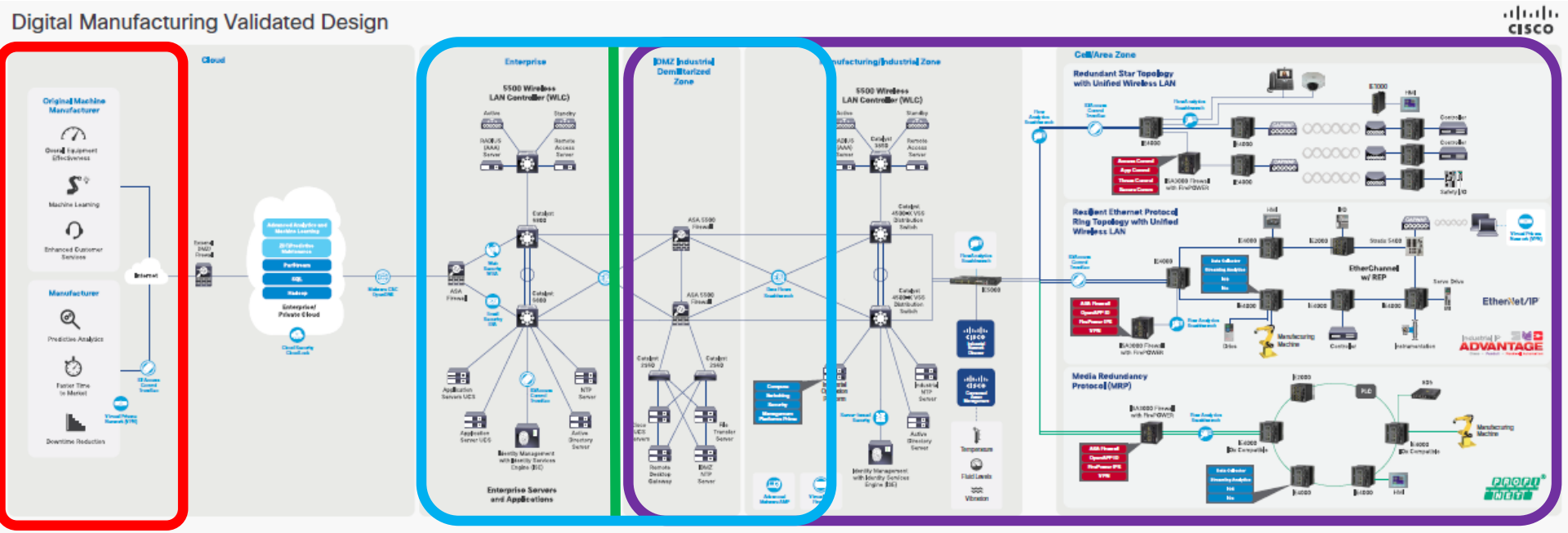
IoT Sec Talks 2016 May – 620 respondents

The Vision of the Future – Connected Systems

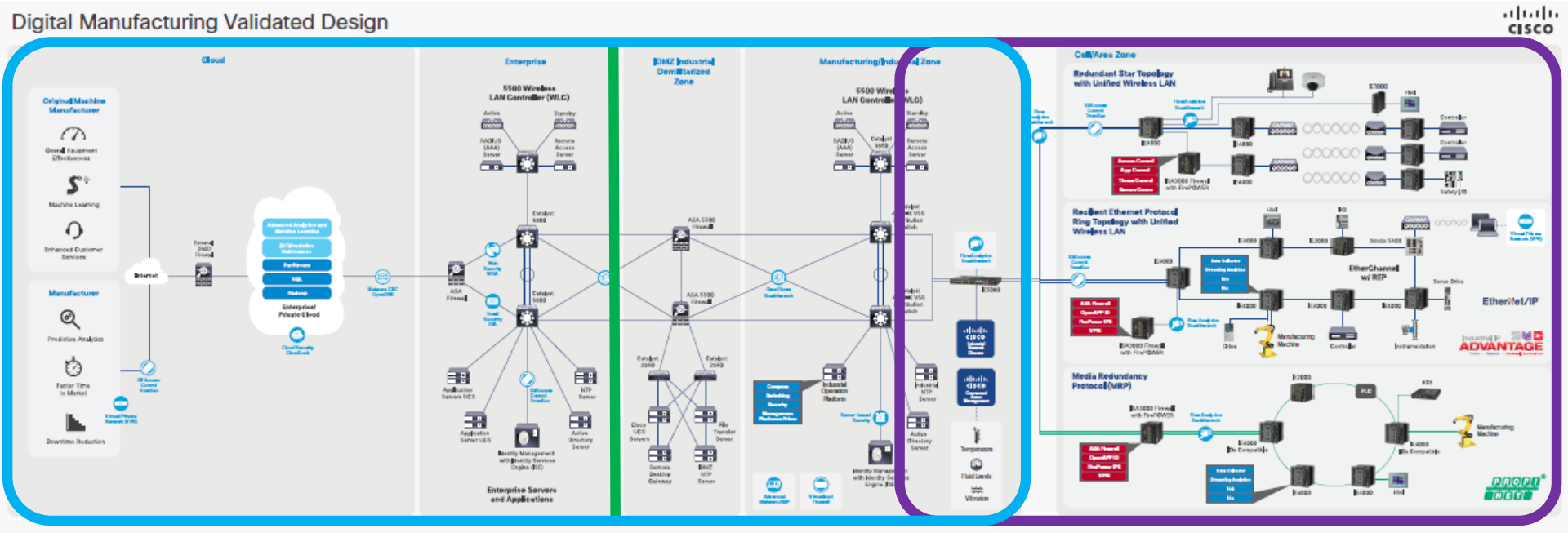
From Cloud to Enterprise to Cell



Organizational Boundaries

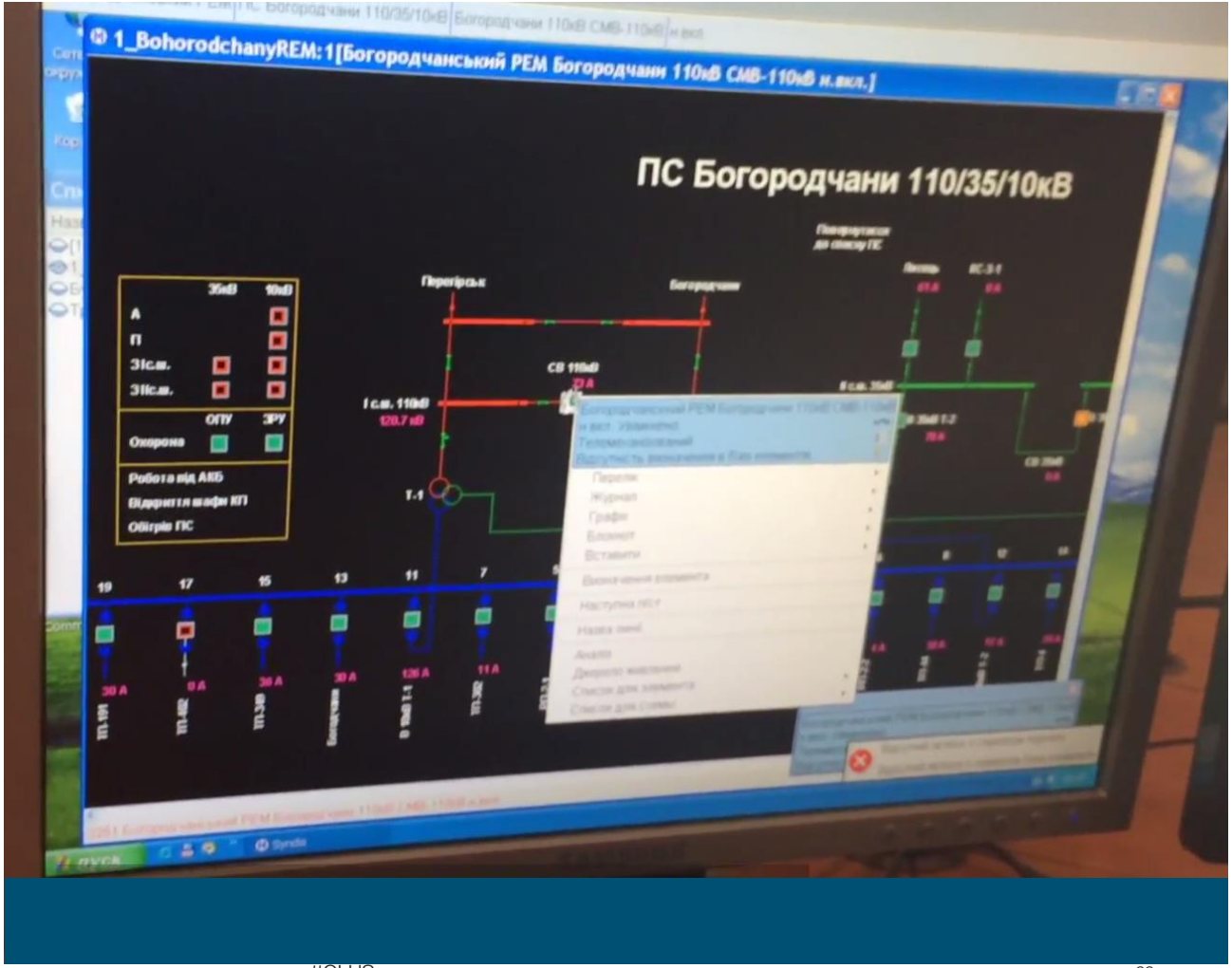


Technology Stacks in Connected Manufacturing



2015 Ukraine Utility Attack

Video Capture (with captions)



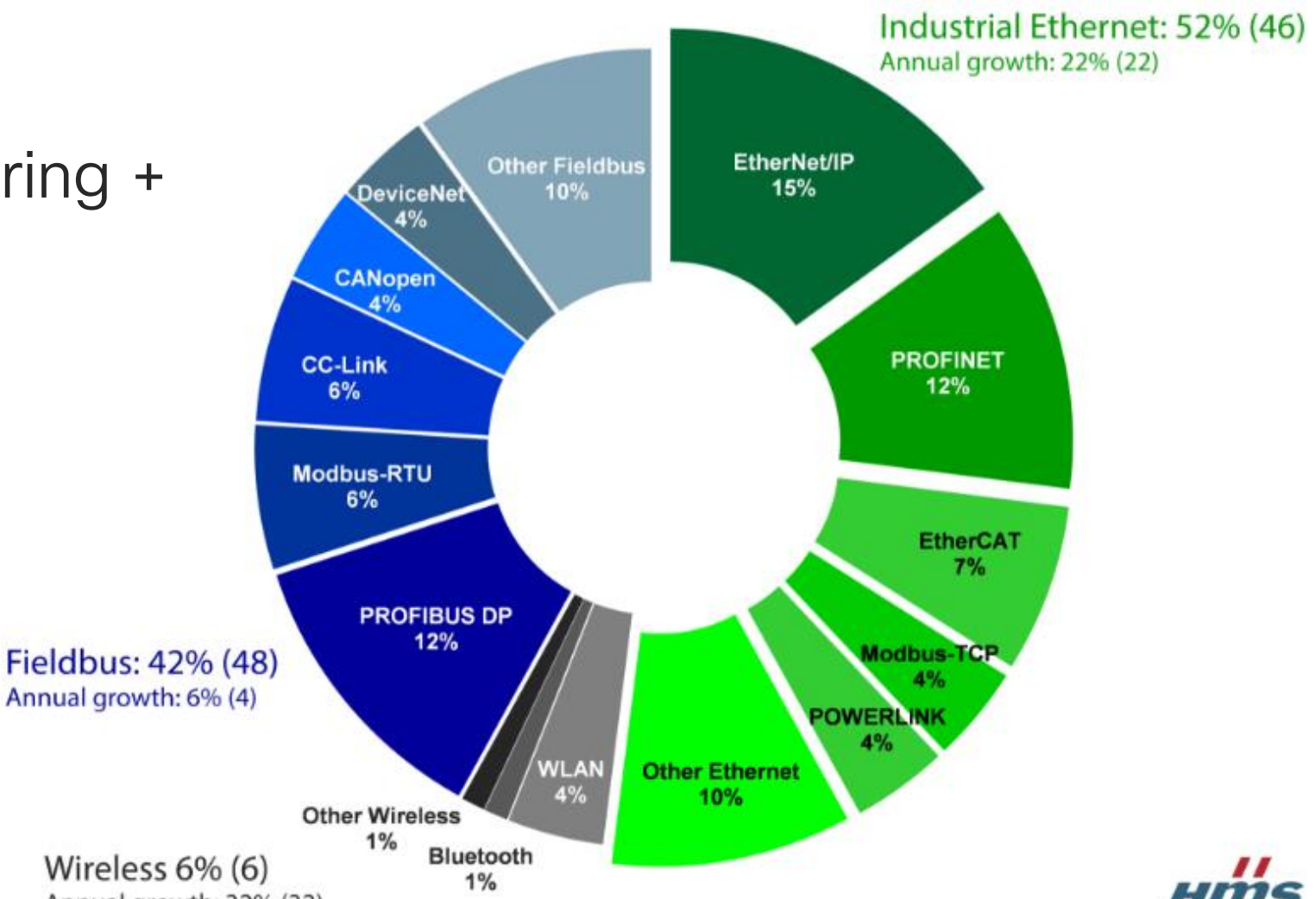
Summary: Industrial Network Differences

- Emphasis on Availability and Safety First!
- Continually operating / Infrequently interrupted
- Very different network patterns
- Physical environment drives unique equipment
- Understand that there are different boundaries that impact security

Agenda

- Information and Industrial Network Differences
- **Industrial Protocols – their security challenges**
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 4 Attack Discussions
- Closing / Question & Answer

Industrial Networks: Manufacturing +



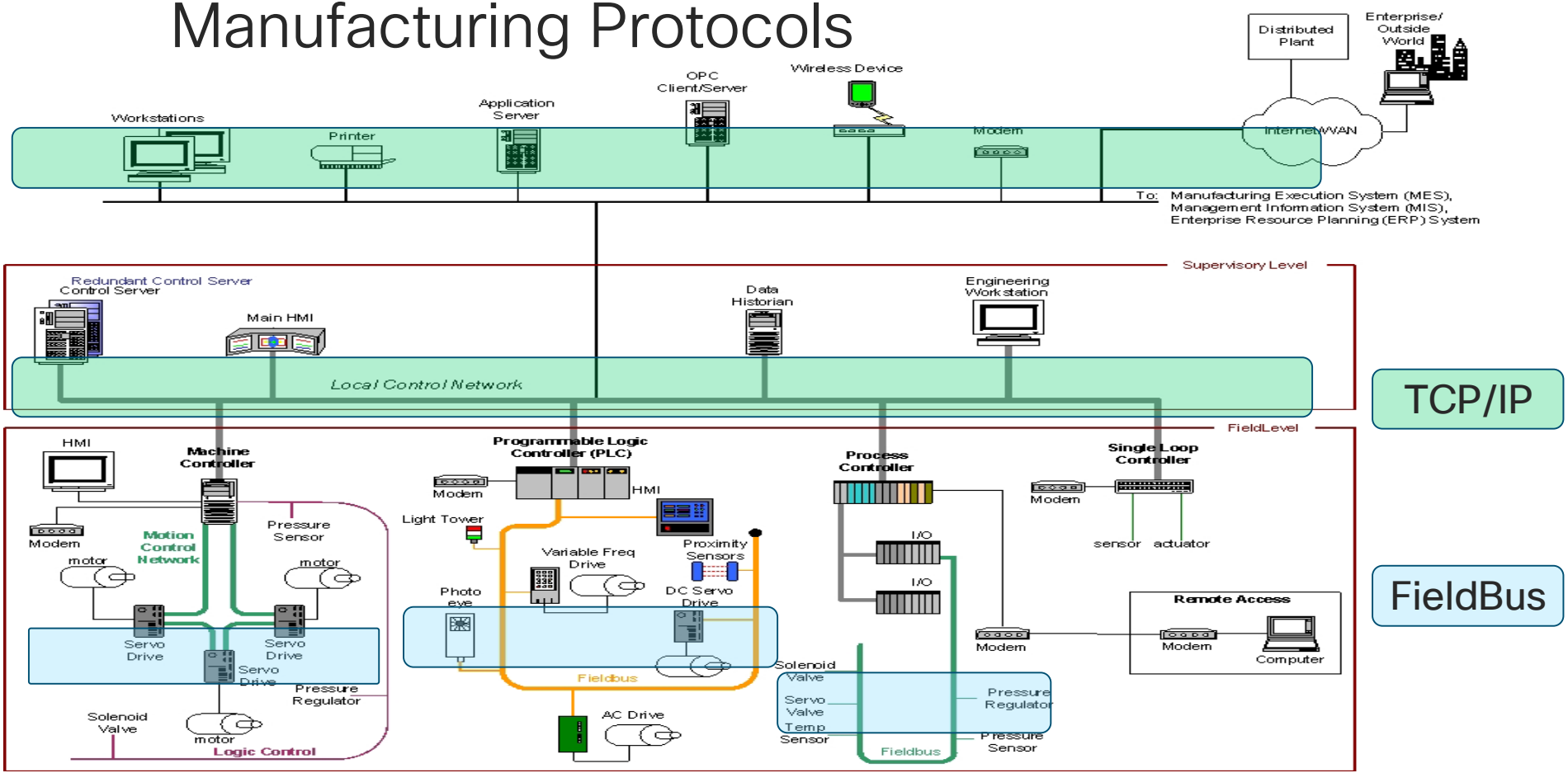
Industrial Protocols – General Security Concerns

- Early developments of many protocols made few provisions for security
  - Focus was on interoperability and continuity
  - Master / Slave relationships within serial communications
  - No encryption (but there are reasons not to in some cases)

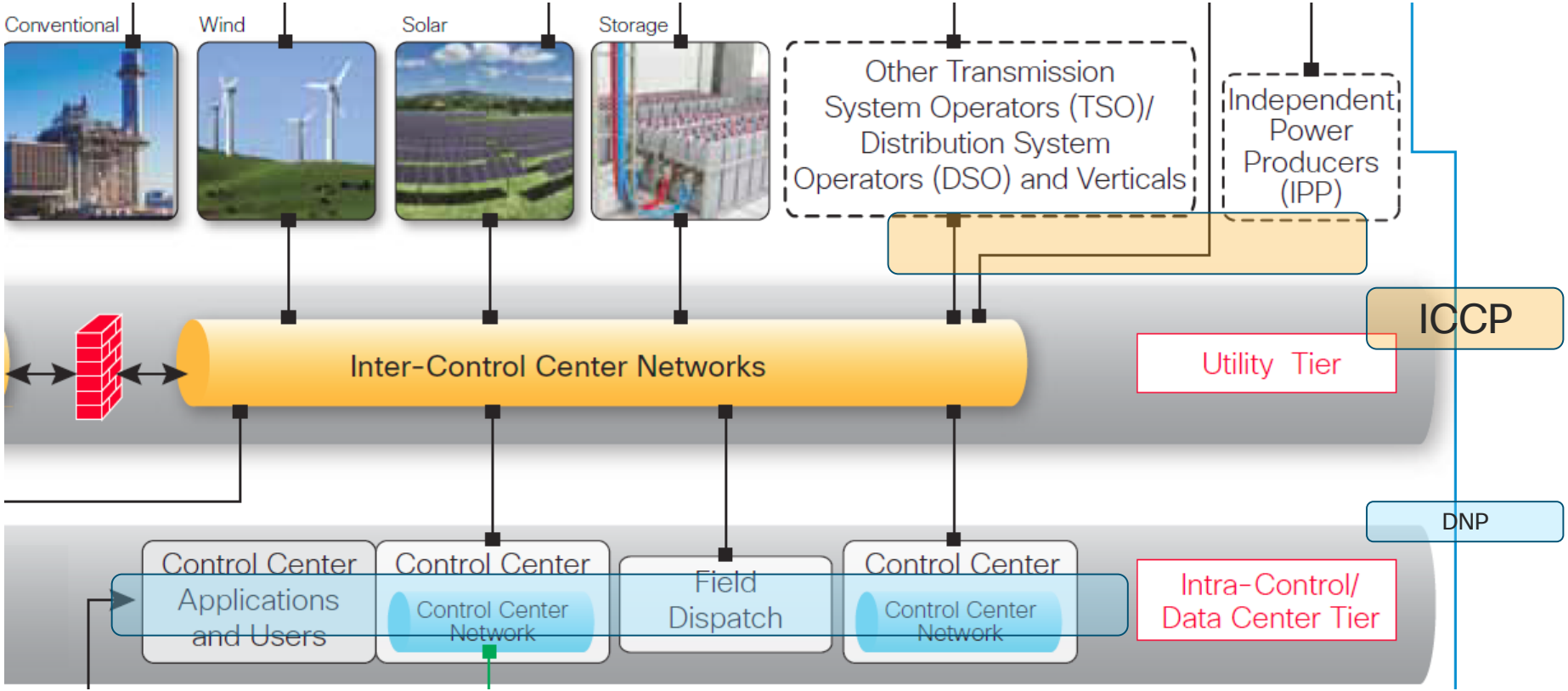
- Authentication is commonly lacking
  - The most common Ethernet/IP base OT protocol lacked authentication till 2015
- Broadcasting for communications

- Assumption of limited communication complexity

Where are these Protocols Found?
Manufacturing Protocols

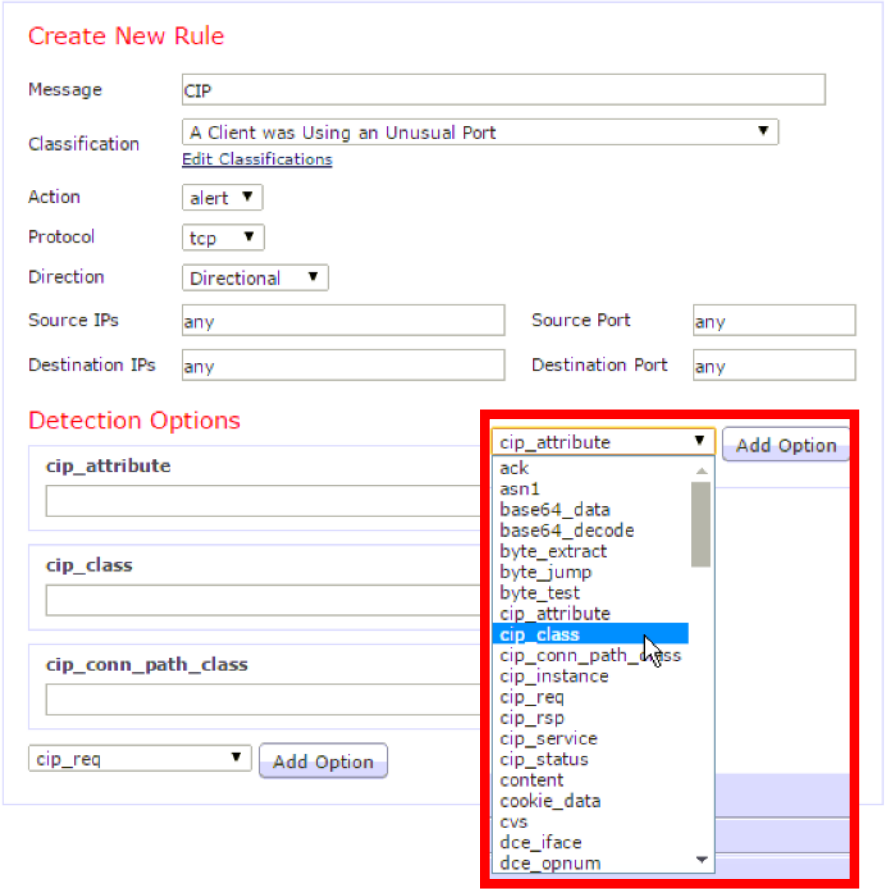


Where are these Protocols Found?
Utility Protocols



Protocol Awareness:

- Moving beyond simple specification study
- Build stateful analysis of the protocol
- Industrial protocols may have connections that last > 24 hrs.
- Normal reg-ex based rules are more limited



Summary of Industrial Protocol Security

- Industrial Protocols Born from Proprietary Systems
  - Minimal if any interoperability
- Little to no built in security in older systems
  - Growth of security coming for NEW systems
- Visibility challenges
  - Proximity for true view and control
  - Protocol awareness critical

Agenda

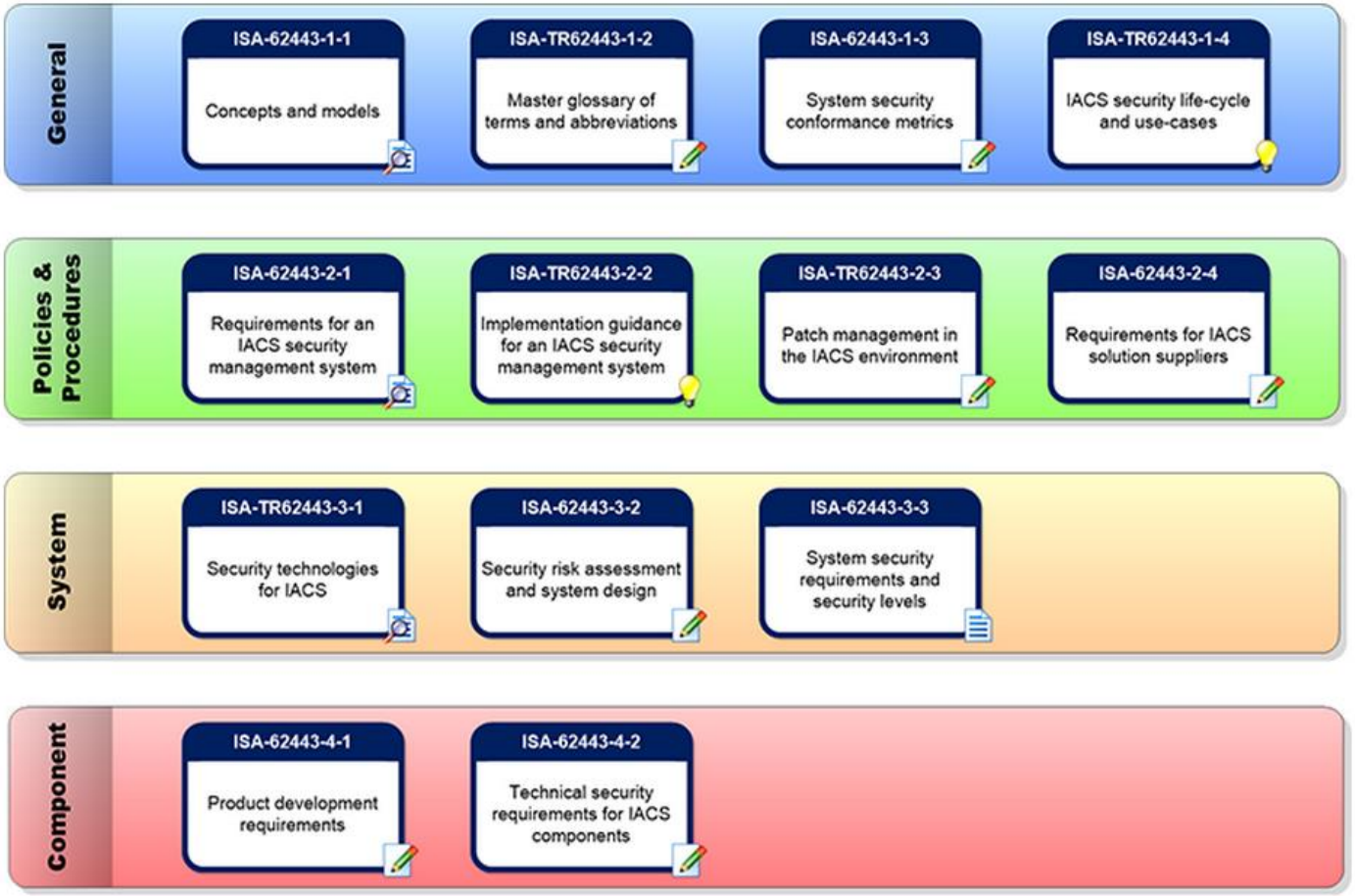
- Information and Industrial Network Differences
- Industrial Protocols – their security challenges
- **Standards in Industrial spaces**
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 4 Attack Discussions
- Closing / Question & Answer

ISA-99 – Security Attitude (Terms)

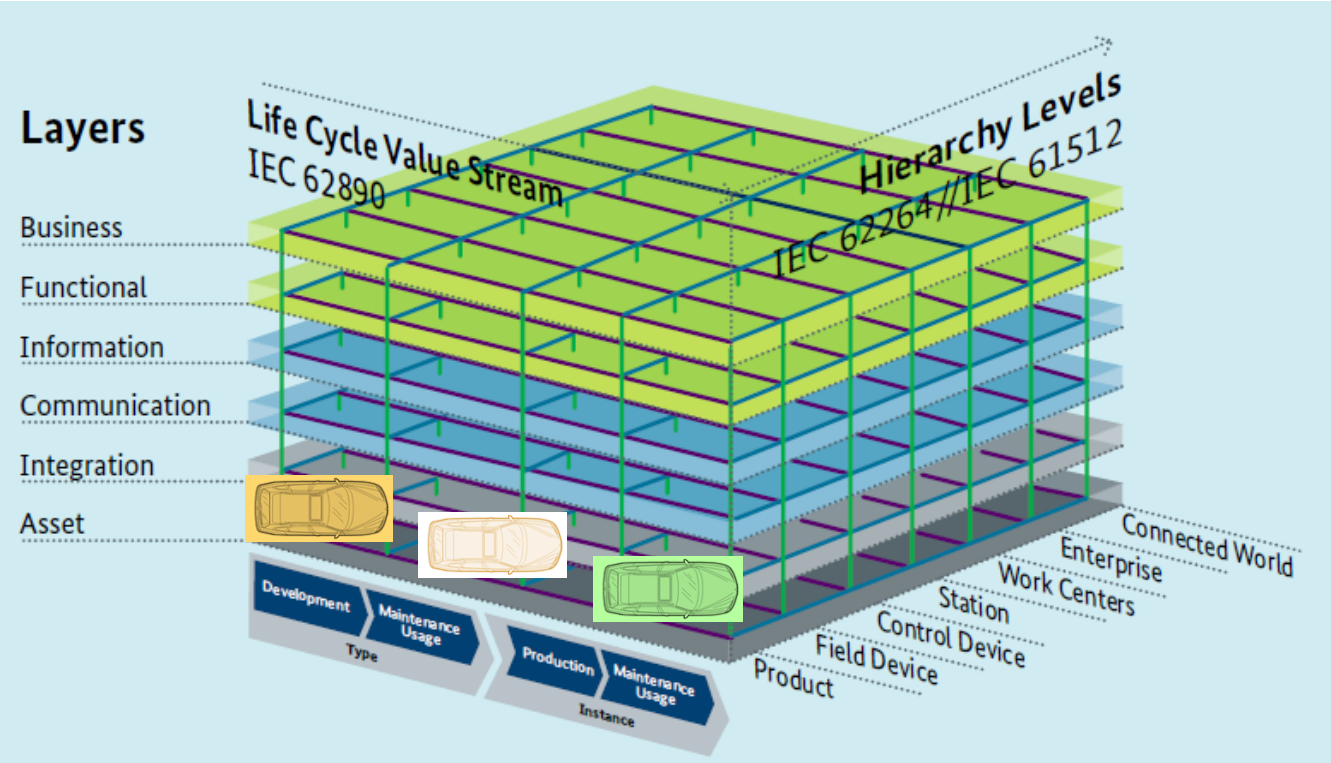
2.3 Security Objectives

A critical requirement of IACS security measures is that they must not have the potential to cause impacts to essential services and functions, including emergency procedures. In contrast, IT security measures as often deployed do have this potential. IACS security goals focus on control system availability, plant safety, plant protection, plant operations (even in a degraded mode) and time-critical system response. General IT security goals often do not place the same emphasis on these factors, typically being more concerned with protecting information than physical assets. This difference in emphasis is often referred to as CIA (confidentiality, integrity, and availability) vs. IAC (integrity, availability, confidentiality).

ISA-99 ≈ IEC 62443



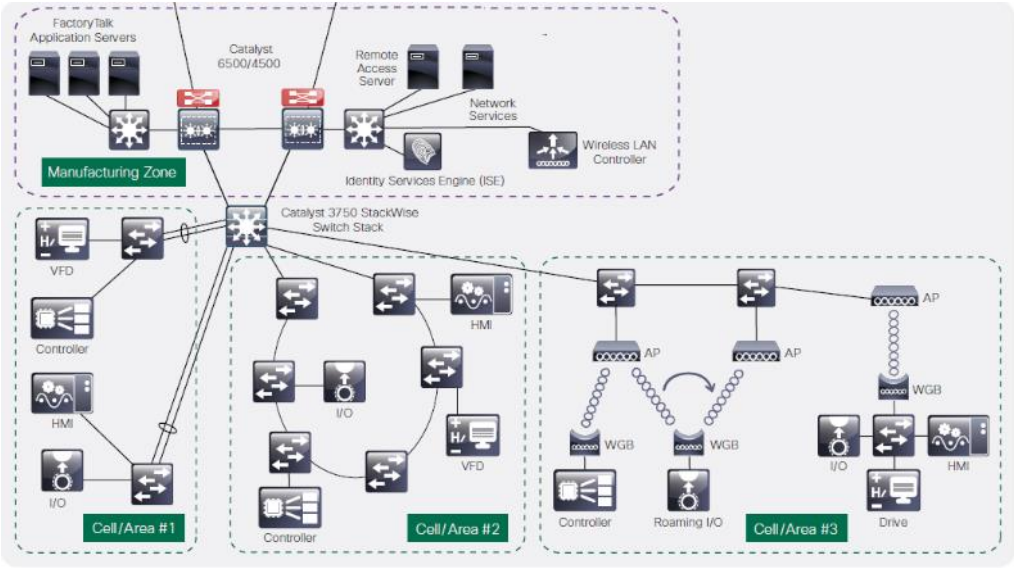
Reference Model: RAMI 4.0



Jochem, Klasen, Linke, Jaenicke, Gamer, Stolz, Mehrfield, Teuscher, Fritsche. 2016
Security in RAMI4.0
Federal Ministry for Economic Affairs and Energy (BMWi)

Zones

- Design your networks
  - Physical / Logical Organization
  - Mostly Physical



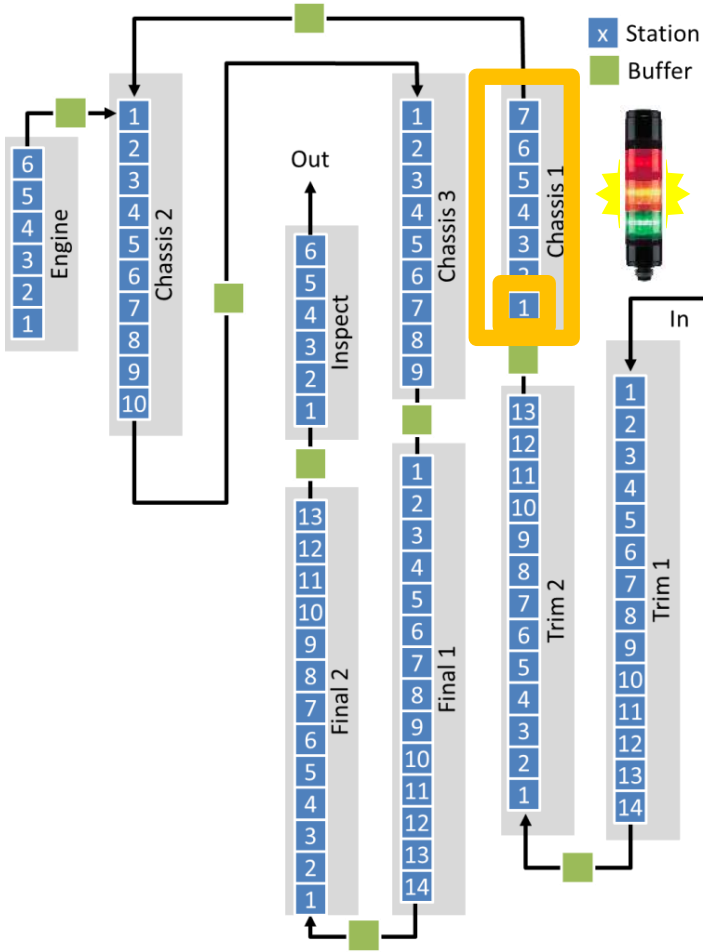
- Remember the OT NW Traffic Profile?
  - Intra-"cell" traffic is dominant
  - Little cell to cell communication

Connectivity / Network Segmentation Zone Definition

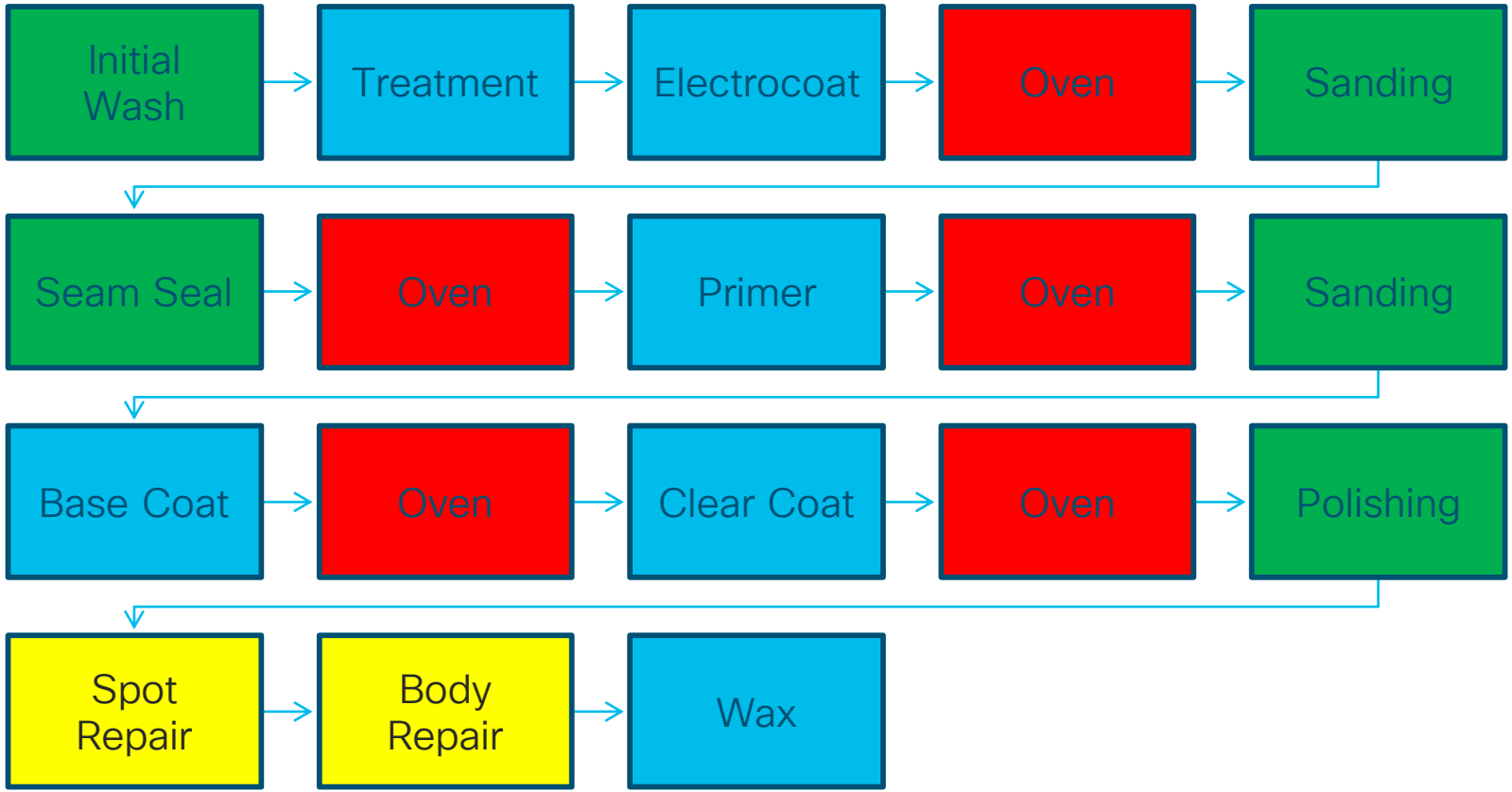
Design of the Assembly Line will drive network and security design:

First – What is the right level of control for:
- Each Station;
- Each “Line”;
- The whole system

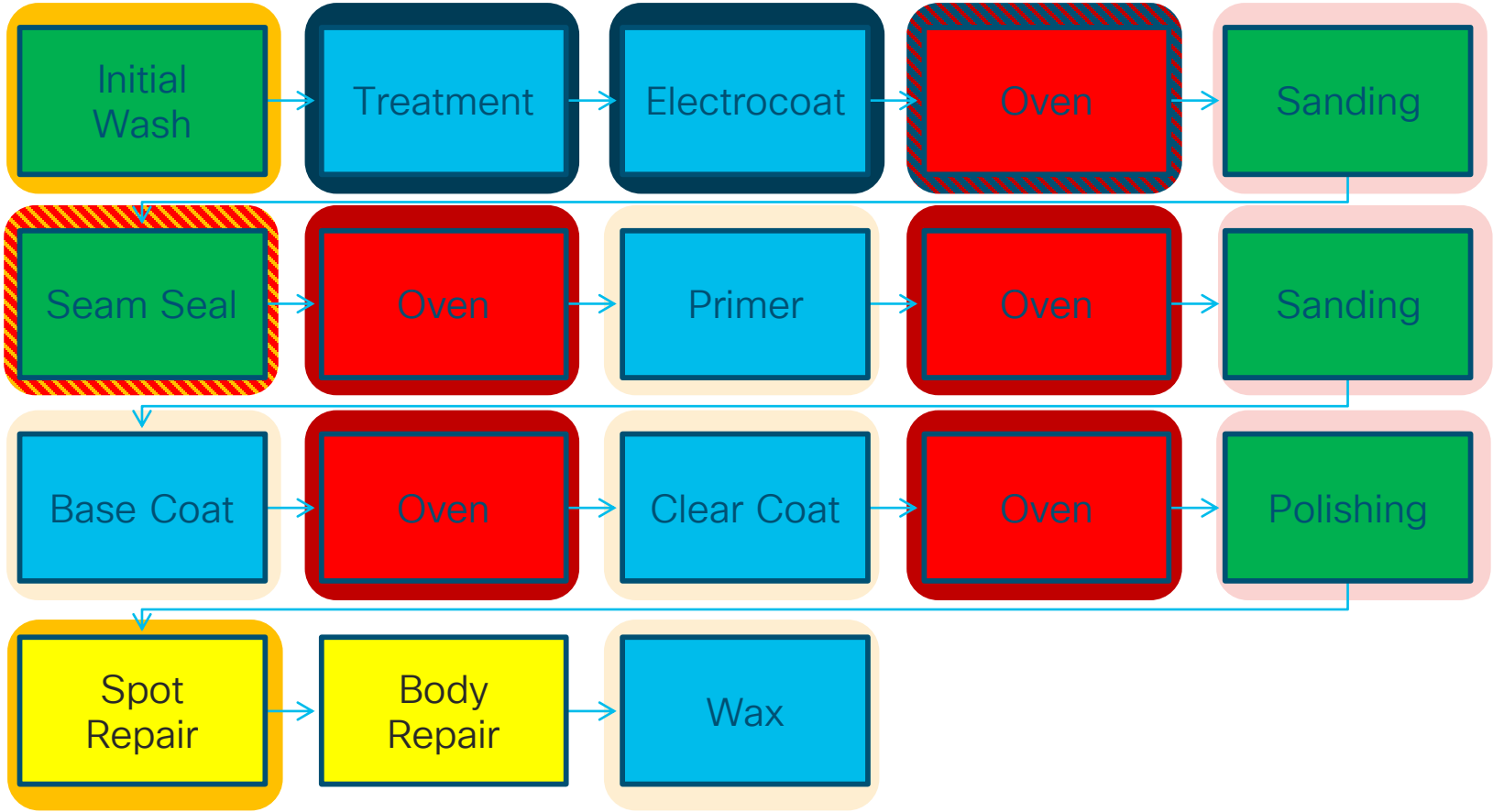
Second – What are the applications responsible for each level?
- Applications that control normal operation;
- Applications that control safety;
- Applications that feed operational / business analytics;
- Applications that provide for maintenance.



How To Paint a Car – w 90 robots over 4 km



How Many Zones? / How Many Vendors?



Conduits

- Controlled Communications Paths
  - ACLs
  - DACLs?
  - Or perhaps Security Group Tags (SGTs)?
  - VLANs
- Secured Communications
  - VPNs

Firewall Rules Recommendations


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

Special Publication 800-82
INITIAL PUBLIC DRAFT

Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security

- In summary, the following should be considered as recommended practice for general firewall rule sets:
- The base rule set should be deny all, permit none.
- Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
- All rules should restrict traffic to a specific IP address or range of addresses.
- Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the DMZ.
- Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).
- All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.
- Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.
- Control network devices should not be allowed to access the Internet.
- Control networks should not be directly connected to the Internet, even if protected via a firewall.
- All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.

Industry Rules: North American Pipeline Regs

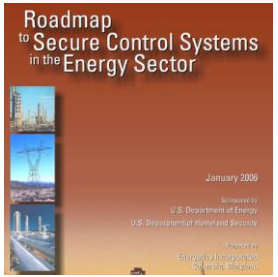
Pipeline Security Guidelines
April 2011
Transportation Security Administration

INGAA
Control Systems Cyber Security Working Group

Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry

DOE Office of Electricity Delivery and Energy Reliability

A Summary of Control System Security Standards Activities in the Energy Sector



PART 192 – TRANSPORTATION OF NATURAL AND OTHER GAS BY PIPELINE: MINIMUM FEDERAL SAFETY STANDARDS
PART 193 – LIQUEFIED NATURAL GAS FACILITIES: FEDERAL SAFETY STANDARDS

Strategy for Securing Control Systems
Coordinating and Guiding Federal, State and Private Sector Initiatives
October 2009
Homeland Security

Pipeline SCADA Security

Department of Homeland Security
6 CFR Part 27
Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

API STANDARD 1164
SECOND EDITION, JUNE 2009

REAFFIRMED, OCTOBER 2016

Summary of Industrial First Principals

- Highly focused on standards

- Network Segmentation is key
  - Zones
  - Conduits

- Many other standards depending on your industry.

Agenda

- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- Standards in Industrial spaces
- **A Phased Approach to Industrial Security**
- Four Common Industrial Security Use Cases
- Some Industrial Protocols and their Security Issues
- Closing / Question & Answer

Phasing in Security

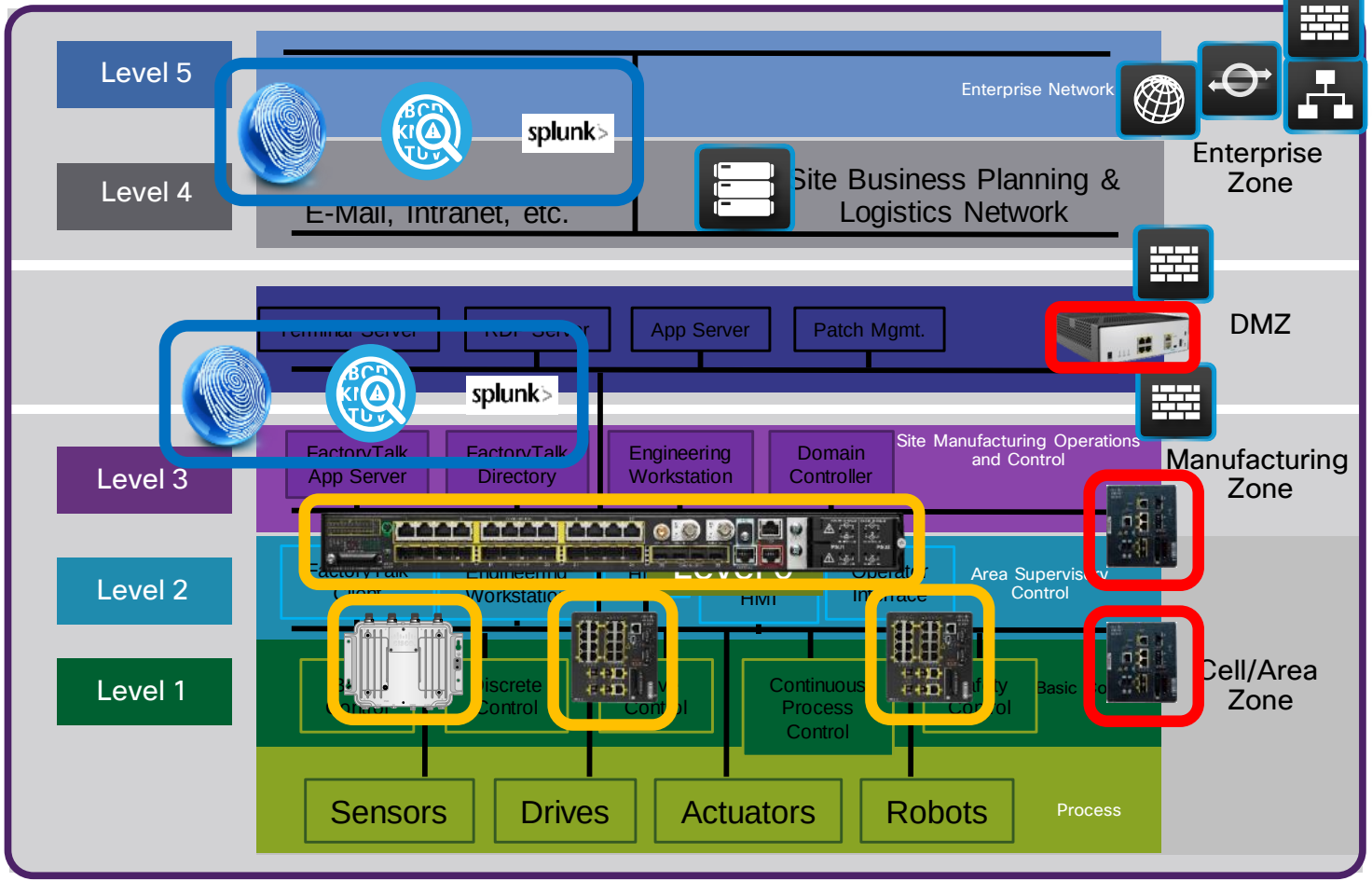
- Avoid Interruptions
- Building trust over time

- Assume Multi-year Effort

Security Phasing Approaches – Standards

US Department of Homeland Defense: Continuous Diagnostics and Mitigation		
CDM – Phase 1	CDM – Phase 2	CDM – Phase 3
Asset Control – What is the state of the endpoints I must secure?	Manage People and Services – Who can do what?	Process Planning – What to do and how do we improve?

Evolve to Security: Phased Security Architecture



First Phase – Secured Connectivity

Zone Segmentation
Controlled Conduits

Second Phase – Secured Visibility & Control

Application Control
Threat Control

Third Phase – Converged Security & Depth

Policy Driven Response
Deeper Vision / Control

Summary of Phased Security Architecture

- Long – running pre-existing operations
- Introduction of new elements must be done carefully over years
- Phases of introduction
  - Modern networking and networking design
  - Dedicated threat and application visibility
  - Converging with advanced security practices

Agenda

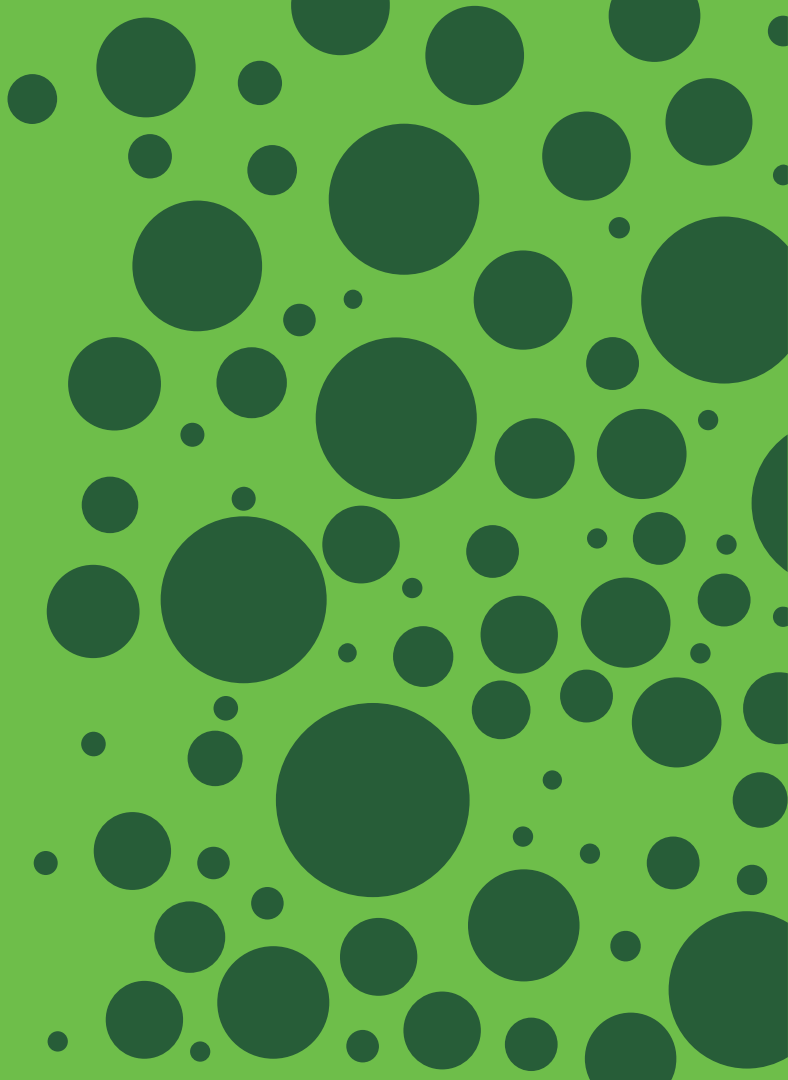
- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- A Phased Approach to Industrial Security
- Standards in Industrial spaces
- **Four Common Industrial Security Use Cases**
- 4 Attack Discussions
- Closing / Question & Answer

Security Use Case Themes

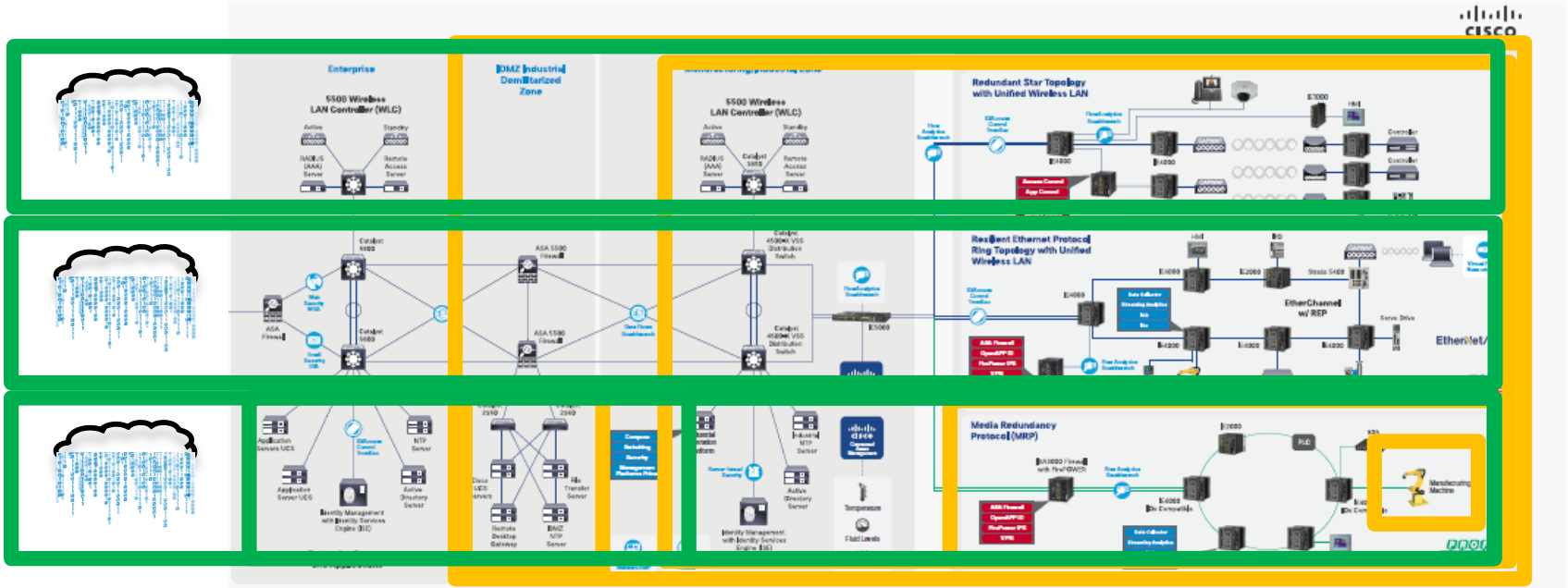
- Secure Connectivity
- Threat Control
- Safe Environment
- Secure Remote Access

- What can connect
- What can talk to what
- What is vulnerable
- Protect the vulnerable
- Network protection
- Device protections
- What are the controls for access
- How to secure access

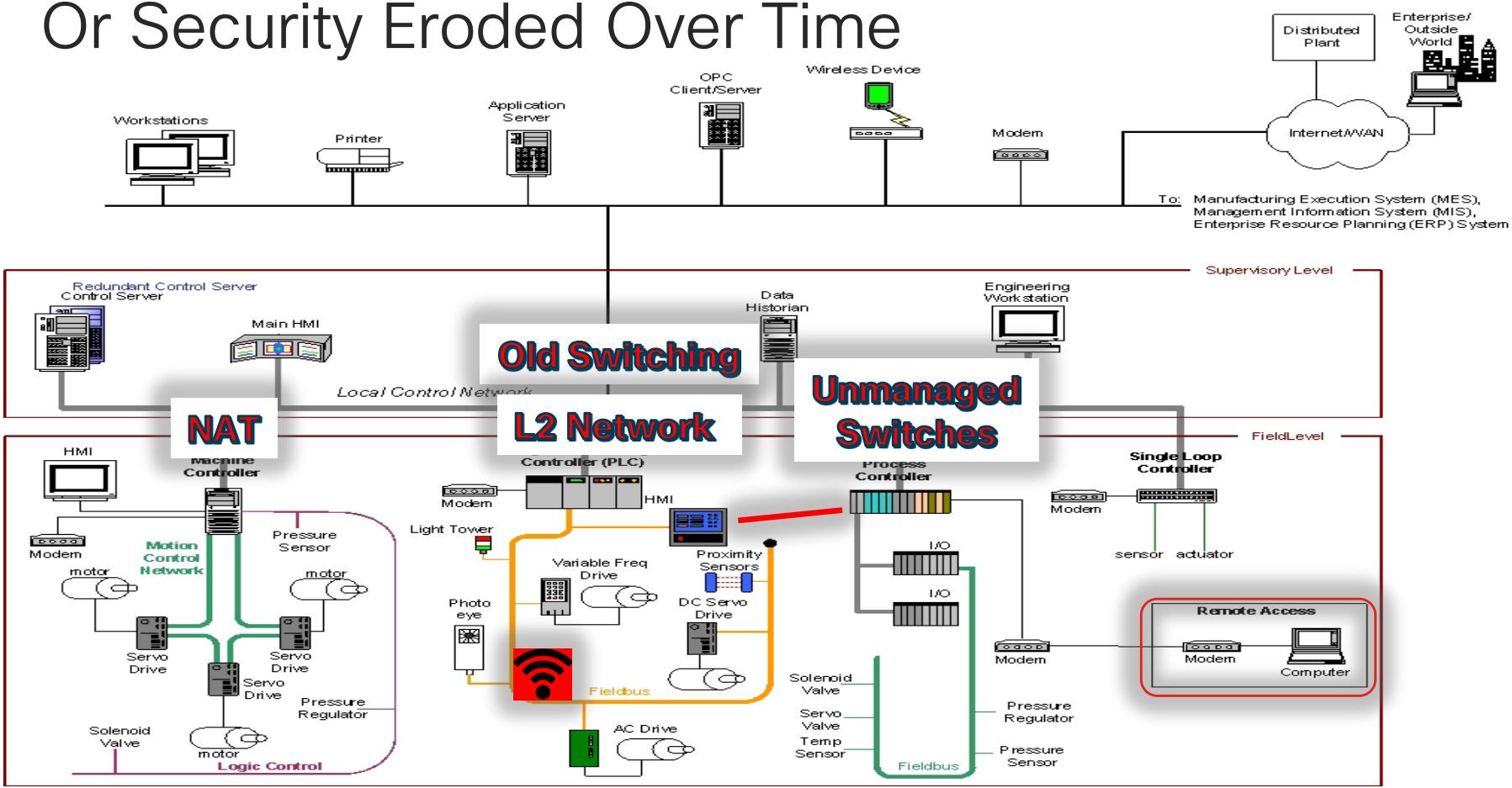
Use Case: Transitioning to Secured Connectivity



Security Use Case: Network Segmentation …and Application Segmentation and Control



Original Designs Lack Security / Or Security Eroded Over Time



Building out Secured Connectivity

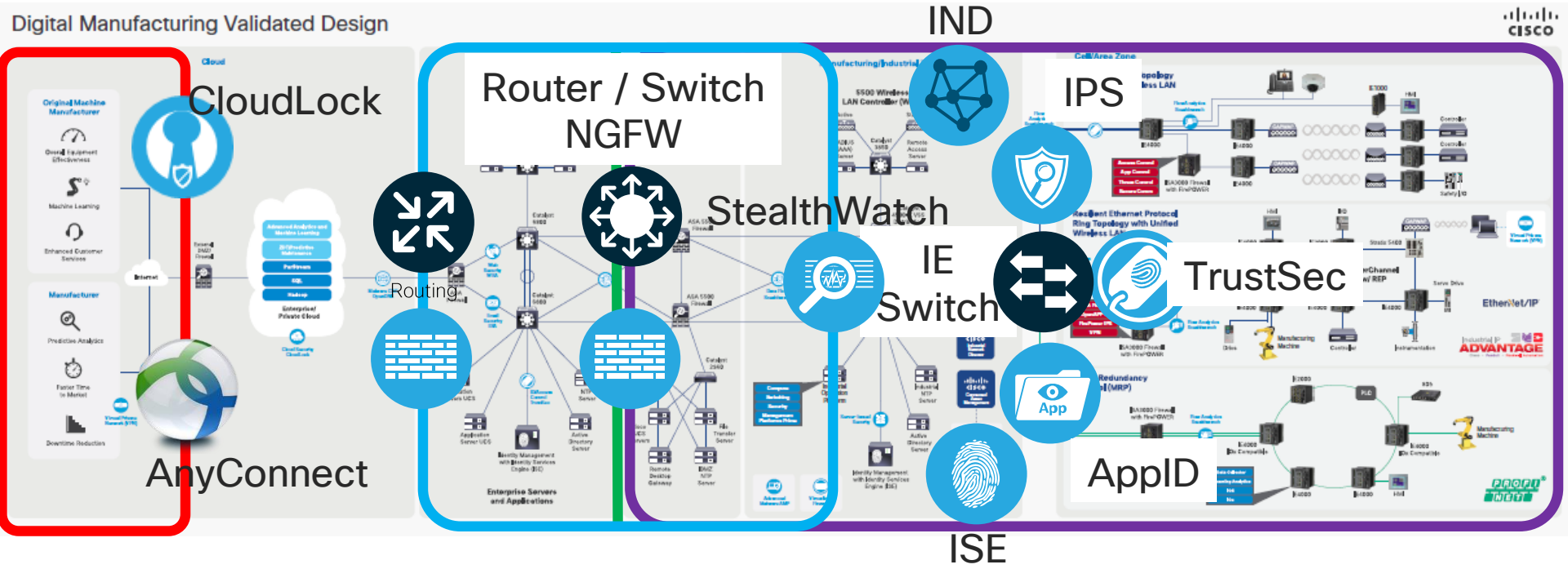
- Design the network with Zones / Conduits in mind.
- Build the network with the future in mind – dedicated security appliances / features

- What to deploy:
  - Industrial Switches / Routers / Wireless (combinations)
  - NW Expertise

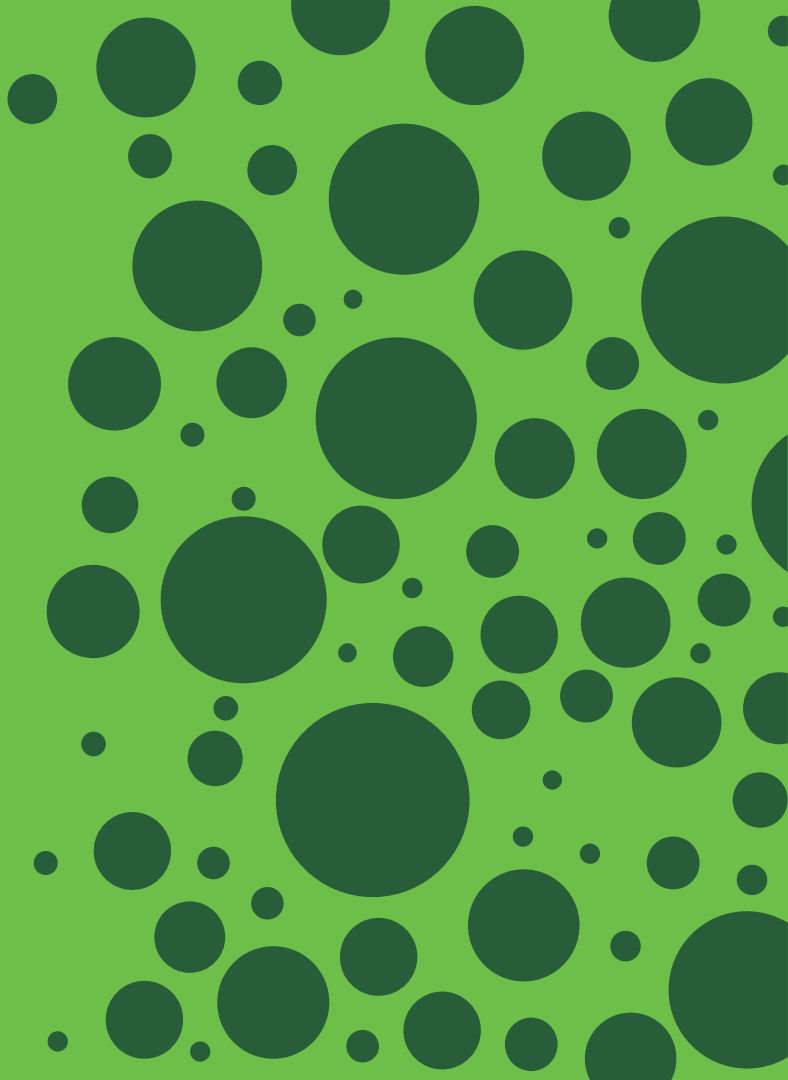
The Case for Purposeful Network Design

You can only see and control what the network allows.

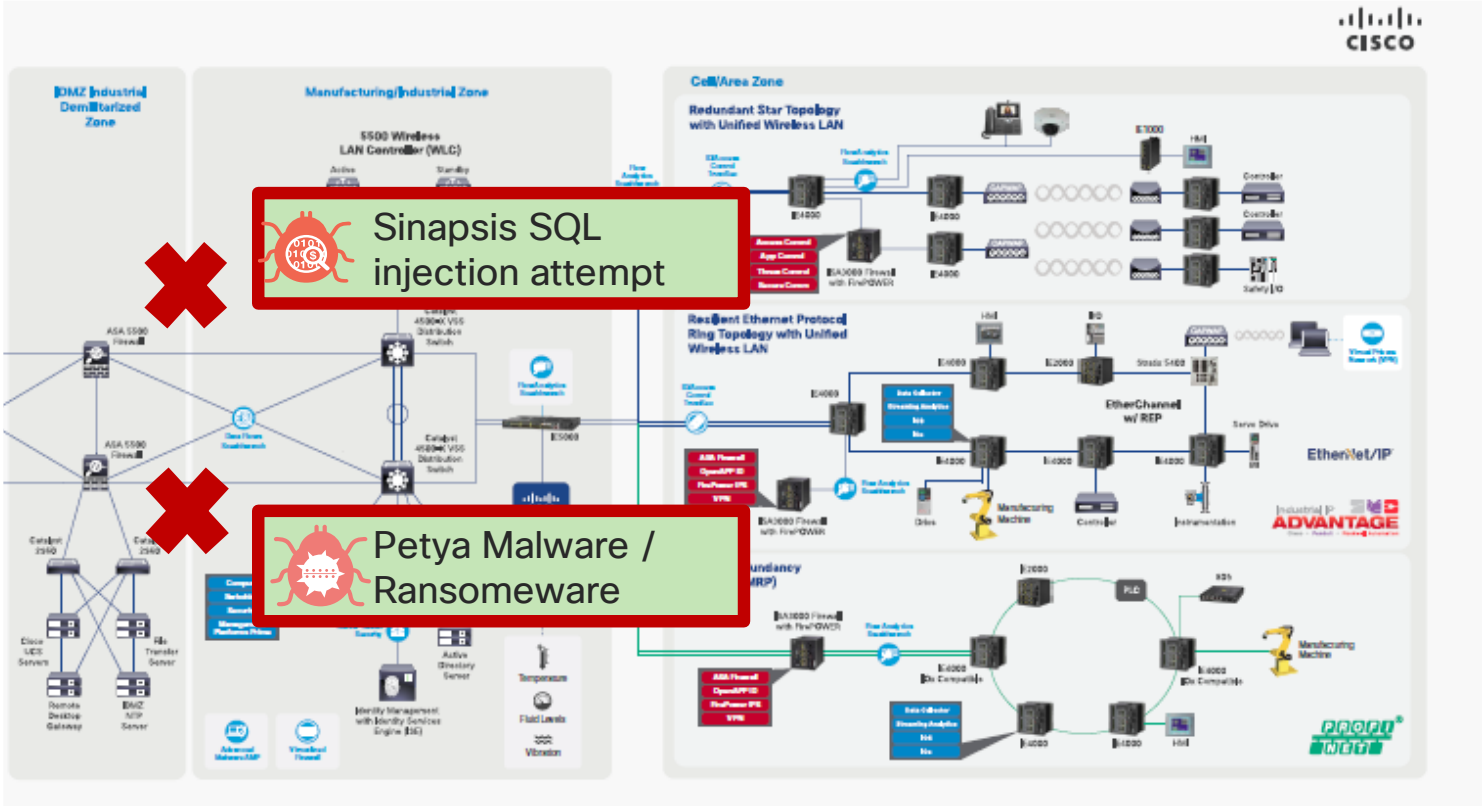
Segmentation: How To



Use Case: Threat Control – Identification and Actions



Security Use Case:
Vulnerability Exploitation / Malware Protection



/c schtasks /Create/SC once /TN “” /TR “C:\Windows\system32\shutdown.exe /r /f” /ST <HH:MM>

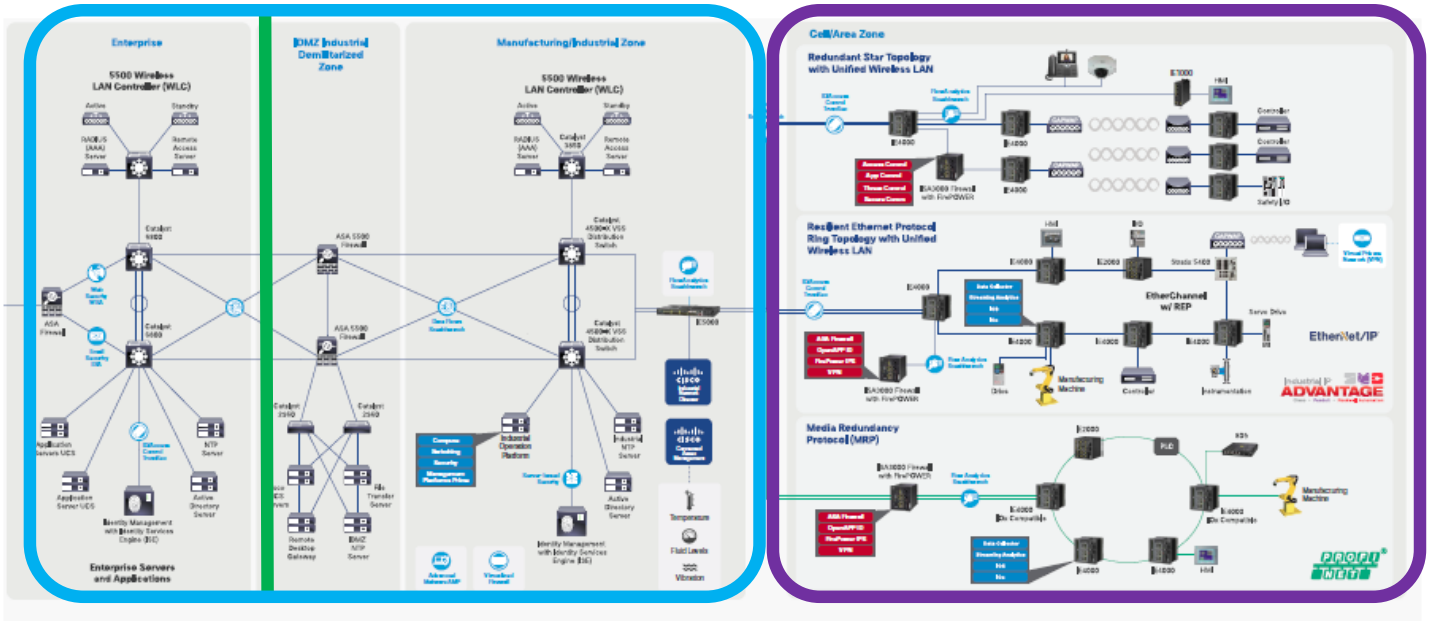
Quantifying Threats by Technology Stack

Vulnerabilities by Top 50 Vendors:

IT – 99.53%

OT – 0.47%

IT Stack Vulns – 44%
[Web – 35%]



https://www.cvedetails.com/vendor 2018 April

OT Assets and Threat To System

2016 ICS Vuln	IT Like Component	Asset	Threat Description
13%		NW	Human Error, Failure, Attacks
2%		Data Historian	Minimal immediate Impact on System
52%		Supervisory Workstation	Human Error, Failure, Attacks
4%		HMI	Human Error, Failure, Attacks
20%		PLC / IO	Command / Program Errors, Failure, Attacks
7%		RTU / Converters	Valid Inputs and Source, Failure, Attacks
		IED	Failure, Valid Inputs and Source, Physical Security

Optimal Targets

Cisco Talos – ICS Research

180+ ICS Vulnerability Protection Rules in 2017

```
<-> PROTOCOL-SCADA IEC 61850 virtual manufacturing device domain variable enumeration attempt (protocol-scada.rules)
<-> PROTOCOL-SCADA IEC 61850 device connection enumeration attempt (protocol-scada.rules)
<-> SERVER-WEBAPP Advantech WebAccess openWidget directory traversal attempt directory traversal attempt(server-webapp.rules)
<-> SERVER-WEBAPP Advantech WebAccess openWidget directory traversal attempt directory traversal attempt(server-webapp.rules)
<-> SERVER-WEBAPP Advantech WebAccess openWidget directory traversal attempt directory traversal attempt(server-webapp.rules)
<-> SERVER-WEBAPP Advantech WebAccess cross site scripting attempt (server-webapp.rules)
<-> SERVER-WEBAPP Advantech WebAccess cross site scripting attempt (server-webapp.rules)
<-> PROTOCOL-SCADA IEC 104 force on denial of service attempt (protocol-scada.rules)
<-> PROTOCOL-SCADA IEC 104 force off denial of service attempt (protocol-scada.rules)
<-> BROWSER-PLUGINS Advantech WebAccess ActiveX clsid access attempt (browser-plugins.rules)
<-> BROWSER-PLUGINS Advantech WebAccess ActiveX clsid access attempt (browser-plugins.rules)
<-> PROTOCOL-SCADA Siemens SIPROTEC V4.24 crafted packet denial of service attempt (protocol-scada.rules)
```

FROM BOX TO BACKDOOR: USING OLD SCHOOL TOOLS AND TECHNIQUES TO DISCOVER BACKDOORS IN MODERN DEVICES

Thursday at 11:00 in 101 Track

45 minutes

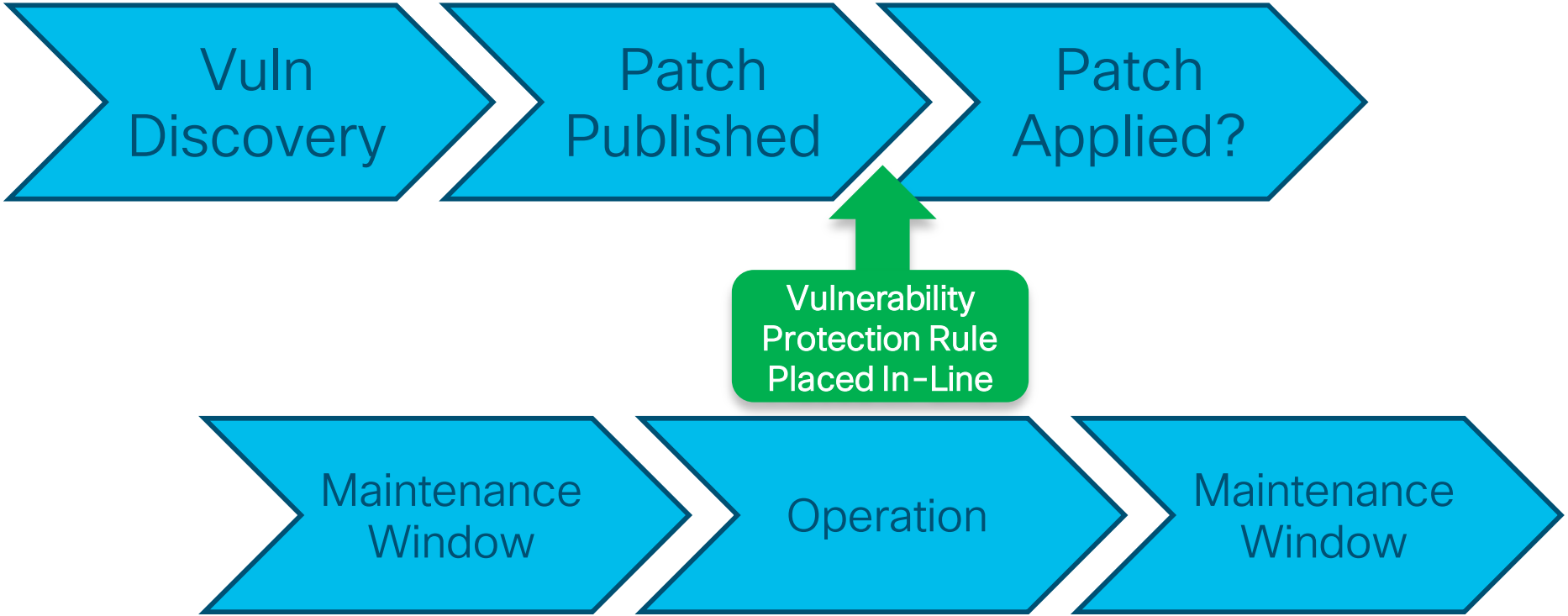
Patrick DeSantis
Senior Security Research Engineer, Cisco Talos

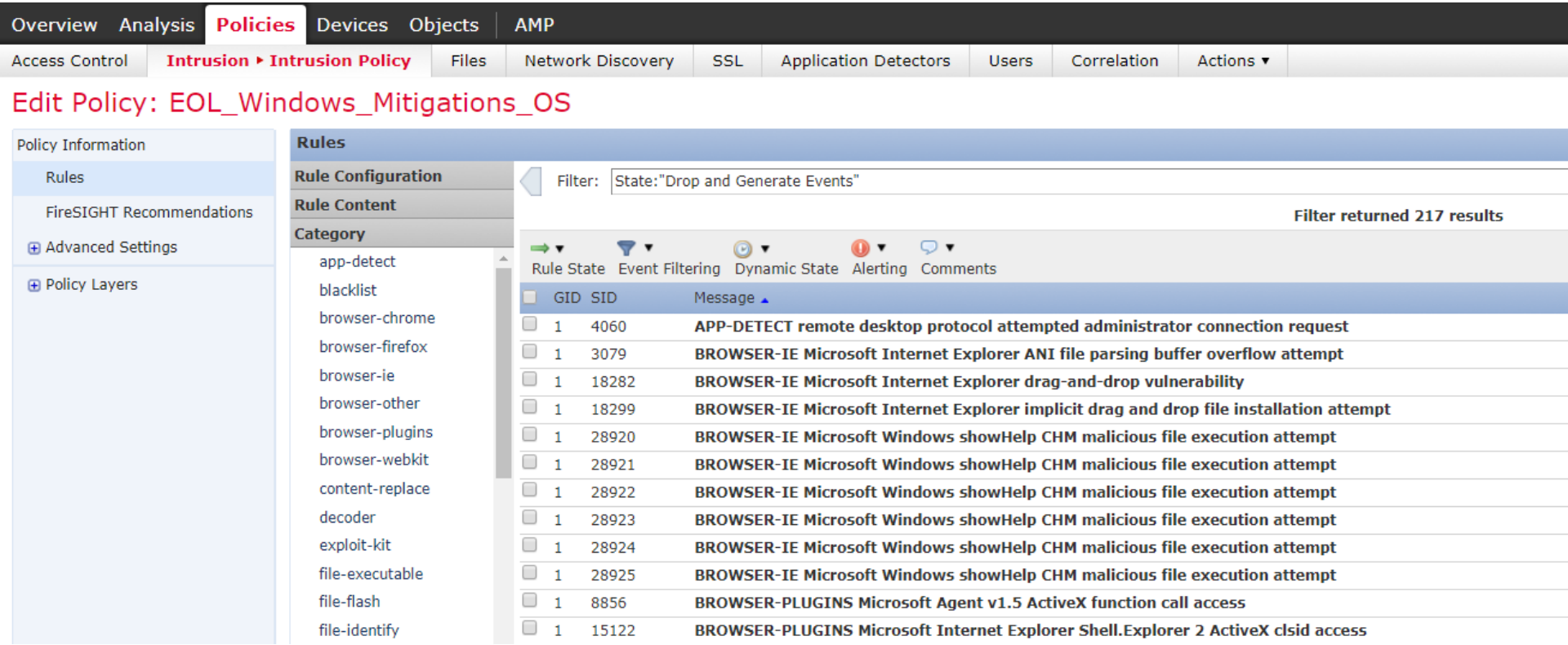
Stringing together the exploitation of several seemingly uninteresting vulnerabilities can be a fun challenge for security researchers, penetration testers, and malicious attackers. This talk follows some of the paths and thought processes that one researcher followed while evaluating the security of several new "out of the box" Industrial Control System (ICS) and Internet of Things (IoT) devices, using a variety of well known exploitation and analysis techniques, and eventually finding undocumented, root-level, and sometimes un-removable, backdoor accounts.

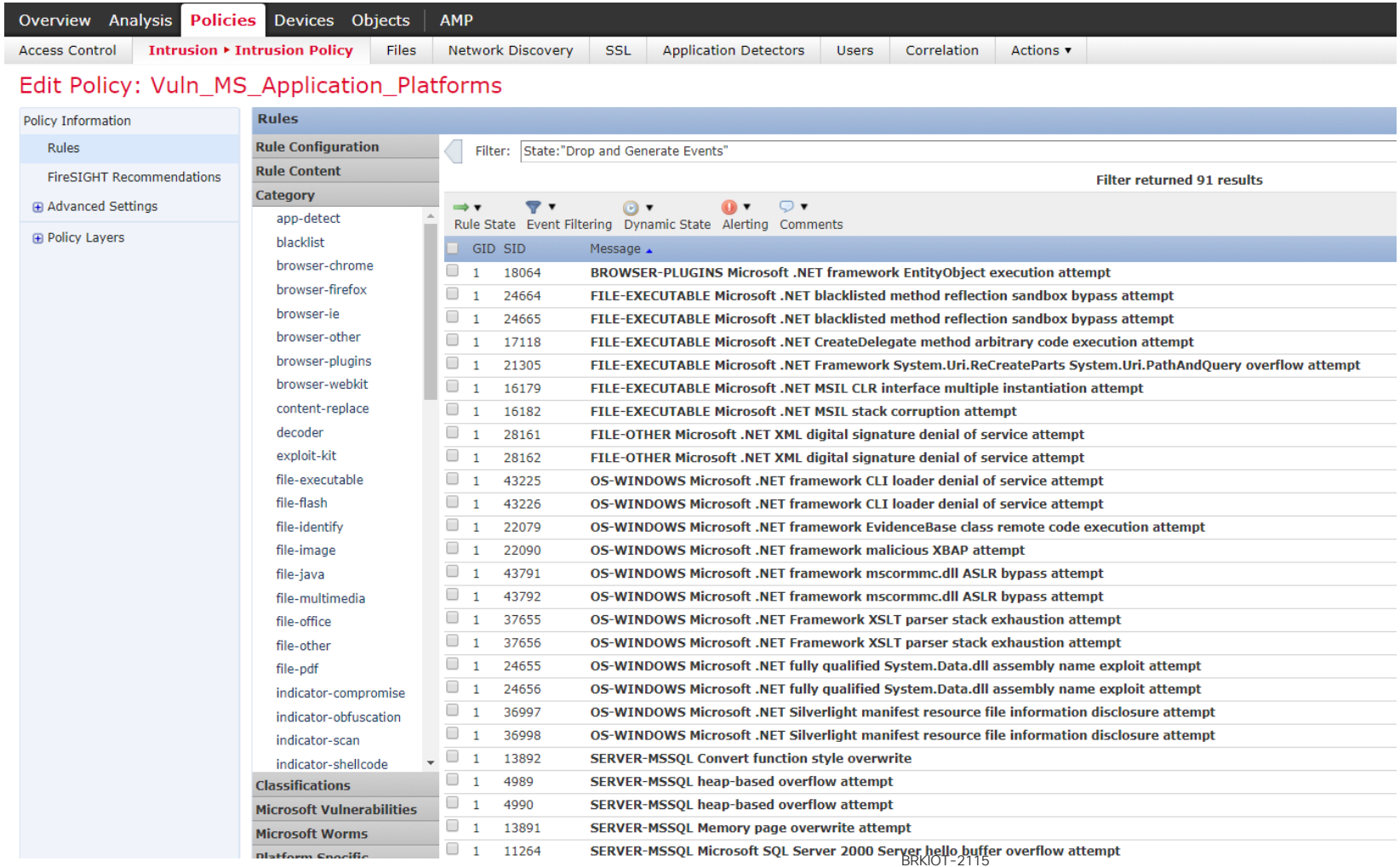
Patrick DeSantis

Patrick DeSantis is a security researcher with Cisco Talos and focuses his efforts on discovery and exploitation of vulnerabilities in technologies that have an impact on the physical world, such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT), and anything else that looks like it's asking to be hacked. Patrick's background includes work in both the public and private sectors, as well as a pile of information security certifications and a few college degrees.

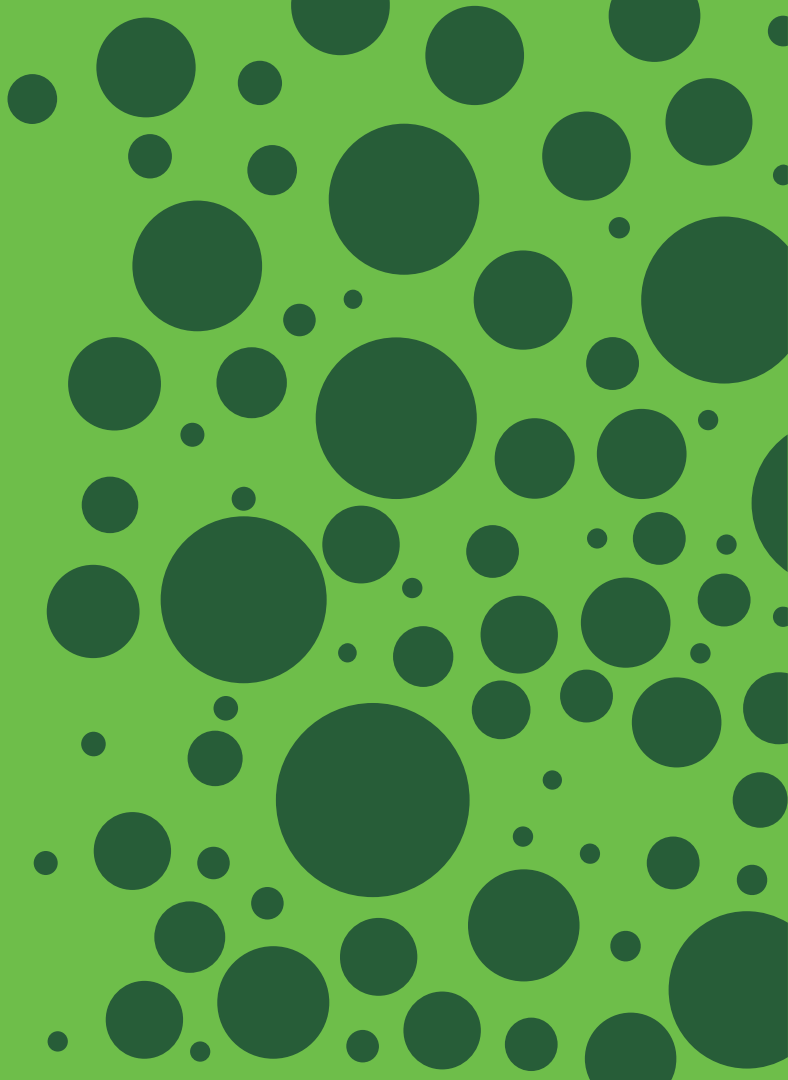
Mitigations – When "Fix it" Has to Wait






Overview Analysis Policies Devices Objects AMP
Access Control Intrusion ▸ Intrusion Policy Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Edit Policy: Vuln_MS_Application_Platforms
Policy Information
Rules
FireSIGHT Recommendations
Advanced Settings
Policy Layers
Rules
Rule Configuration
Rule Content
Category
app-detect
blacklist
browser-chrome
browser-firefox
browser-ie
browser-other
browser-plugins
browser-webkit
content-replace
decoder
exploit-kit
file-executable
file-flash
file-identify
file-image
file-java
file-multimedia
file-office
file-other
file-pdf
indicator-compromise
indicator-obfuscation
indicator-scan
indicator-shellcode
Classifications
Microsoft Vulnerabilities
Microsoft Worms
Filter: State:"Drop and Generate Events"
Filter returned 91 results
Rule State Event Filtering Dynamic State Alerting Comments
GID SID Message
1 18064 BROWSER-PLUGINS Microsoft .NET framework EntityObject execution attempt
1 24664 FILE-EXECUTABLE Microsoft .NET blacklisted method reflection sandbox bypass attempt
1 24665 FILE-EXECUTABLE Microsoft .NET blacklisted method reflection sandbox bypass attempt
1 17118 FILE-EXECUTABLE Microsoft .NET CreateDelegate method arbitrary code execution attempt
1 21305 FILE-EXECUTABLE Microsoft .NET Framework System.Uri.ReCreateParts System.Uri.PathAndQuery overflow attempt
1 16179 FILE-EXECUTABLE Microsoft .NET MSIL CLR interface multiple instantiation attempt
1 16182 FILE-EXECUTABLE Microsoft .NET MSIL stack corruption attempt
1 28161 FILE-OTHER Microsoft .NET XML digital signature denial of service attempt
1 28162 FILE-OTHER Microsoft .NET XML digital signature denial of service attempt
1 43225 OS-WINDOWS Microsoft .NET framework CLI loader denial of service attempt
1 43226 OS-WINDOWS Microsoft .NET framework CLI loader denial of service attempt
1 22079 OS-WINDOWS Microsoft .NET framework EvidenceBase class remote code execution attempt
1 22090 OS-WINDOWS Microsoft .NET framework malicious XBAP attempt
1 43791 OS-WINDOWS Microsoft .NET framework mscormmc.dll ASLR bypass attempt
1 43792 OS-WINDOWS Microsoft .NET framework mscormmc.dll ASLR bypass attempt
1 37655 OS-WINDOWS Microsoft .NET Framework XSLT parser stack exhaustion attempt
1 37656 OS-WINDOWS Microsoft .NET Framework XSLT parser stack exhaustion attempt
1 24655 OS-WINDOWS Microsoft .NET fully qualified System.Data.dll assembly name exploit attempt
1 24656 OS-WINDOWS Microsoft .NET fully qualified System.Data.dll assembly name exploit attempt
1 36997 OS-WINDOWS Microsoft .NET Silverlight manifest resource file information disclosure attempt
1 36998 OS-WINDOWS Microsoft .NET Silverlight manifest resource file information disclosure attempt
1 13892 SERVER-MSSQL Convert function style overwrite
1 4989 SERVER-MSSQL heap-based overflow attempt
1 4990 SERVER-MSSQL heap-based overflow attempt
1 13891 SERVER-MSSQL Memory page overwrite attempt
1 11264 SERVER-MSSQL Microsoft SQL Server 2000 Server hello buffer overflow attempt

Use Case: Application Visibility and Control:

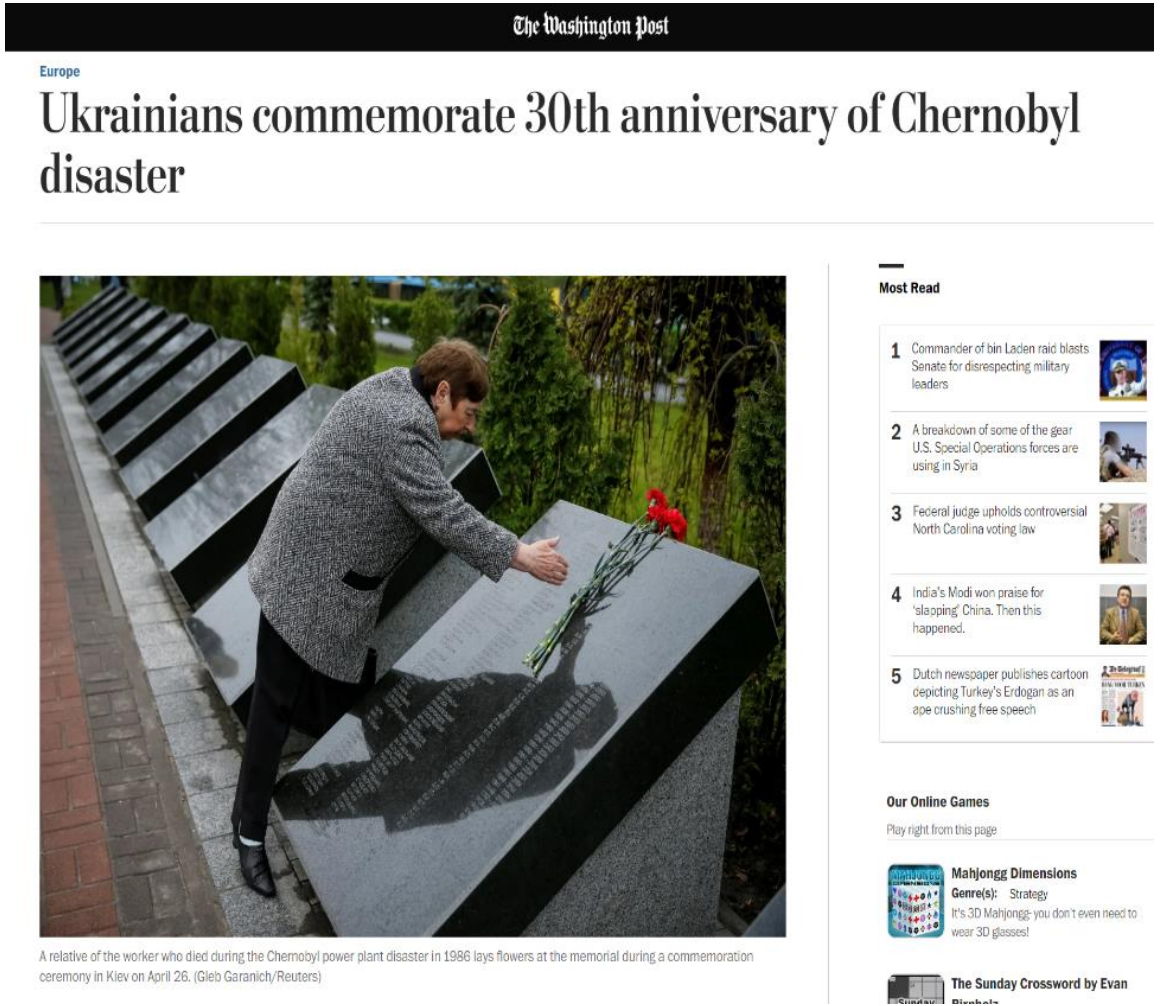


Safety Is EVERYTHING

Impact in Ukraine:

Error

20,000 years of radiation



The Washington Post

Europe

Ukrainians commemorate 30th anniversary of Chernobyl disaster

A relative of the worker who died during the Chernobyl power plant disaster in 1986 lays flowers at the memorial during a commemoration ceremony in Kiev on April 26. (Gleb Garanich/Reuters)

Most Read

1 Commander of bin Laden raid blasts Senate for disrespecting military leaders

2 A breakdown of some of the gear U.S. Special Operations forces are using in Syria

3 Federal judge upholds controversial North Carolina voting law

4 India's Modi won praise for 'slapping' China. Then this happened.

5 Dutch newspaper publishes cartoon depicting Turkey's Erdogan as an ape crushing free speech

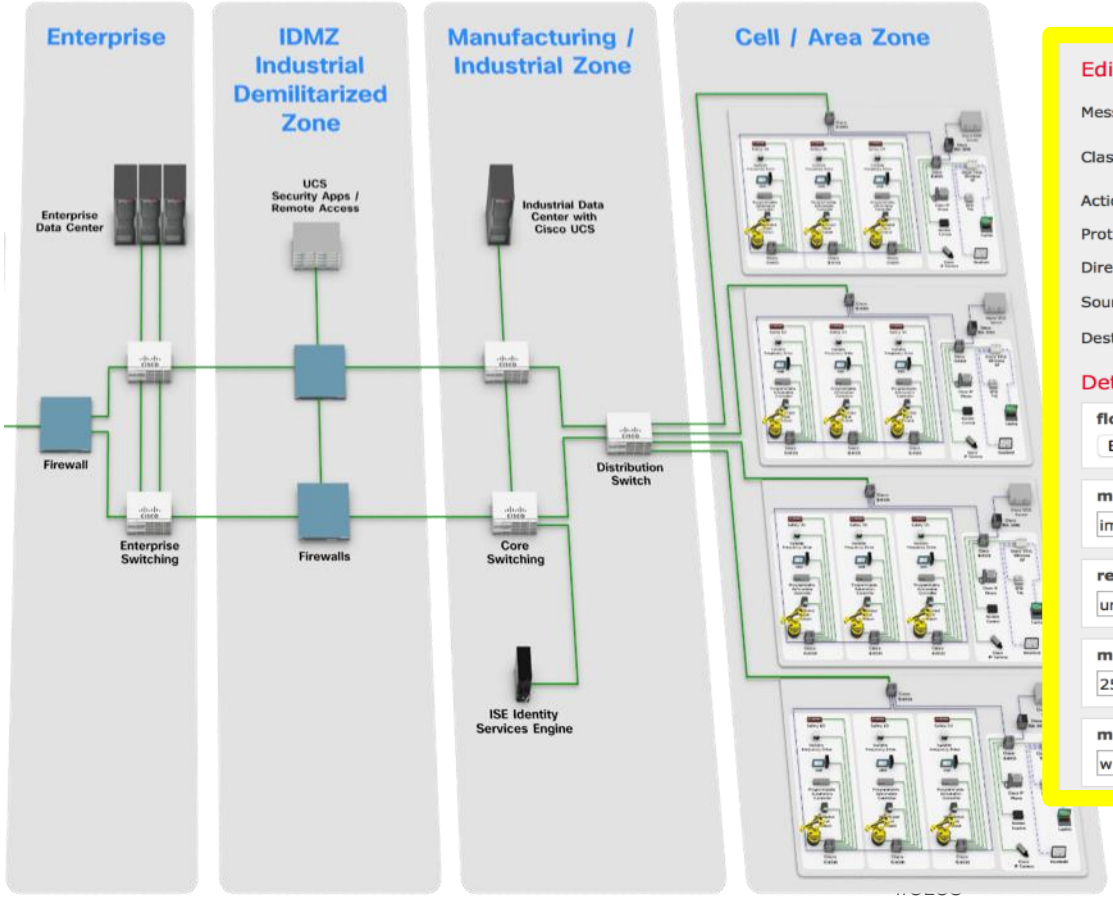
Our Online Games

Play right from this page

Mahjongg Dimensions
Genre(s): Strategy
It's 3D Mahjongg- you don't even need to wear 3D glasses!

The Sunday Crossword by Evan

Protect Critical Infrastructure – Safety Enforcement



Edit Rule 1:1000025:1 (View Documentation, Rule Comment)

Message	PROTOCOL-SCADA Modbus RTU-2000 cooler power OFF from external s		
Classification			
	Edit Classifications		
Action	alert		
Protocol	tcp		
Direction	Directional		
Source IPs	$EXTERNAL_NET	Source Port	any
Destination IPs	$HOME_NET	Destination Port	502

Detection Options

flow
Established | To Server

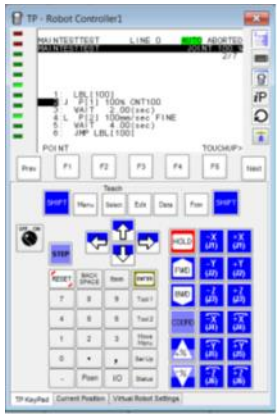
metadata
impact_flag red

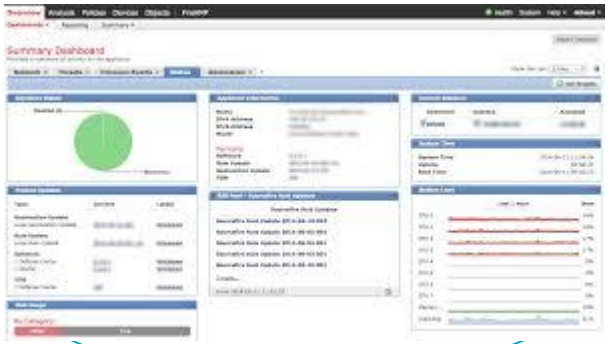
reference
url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

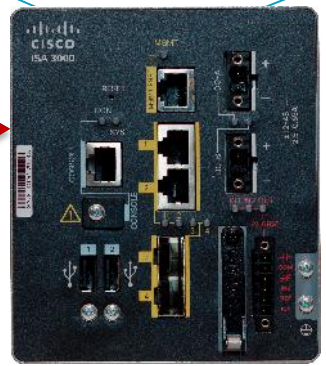
modbus_unit
255

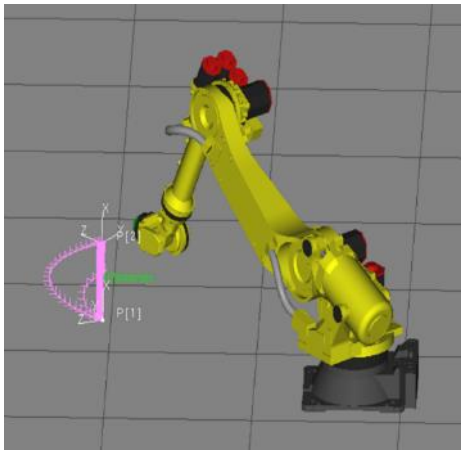
modbus_func
write_single_coil

Stopping Misconfiguration of a Robot Arm

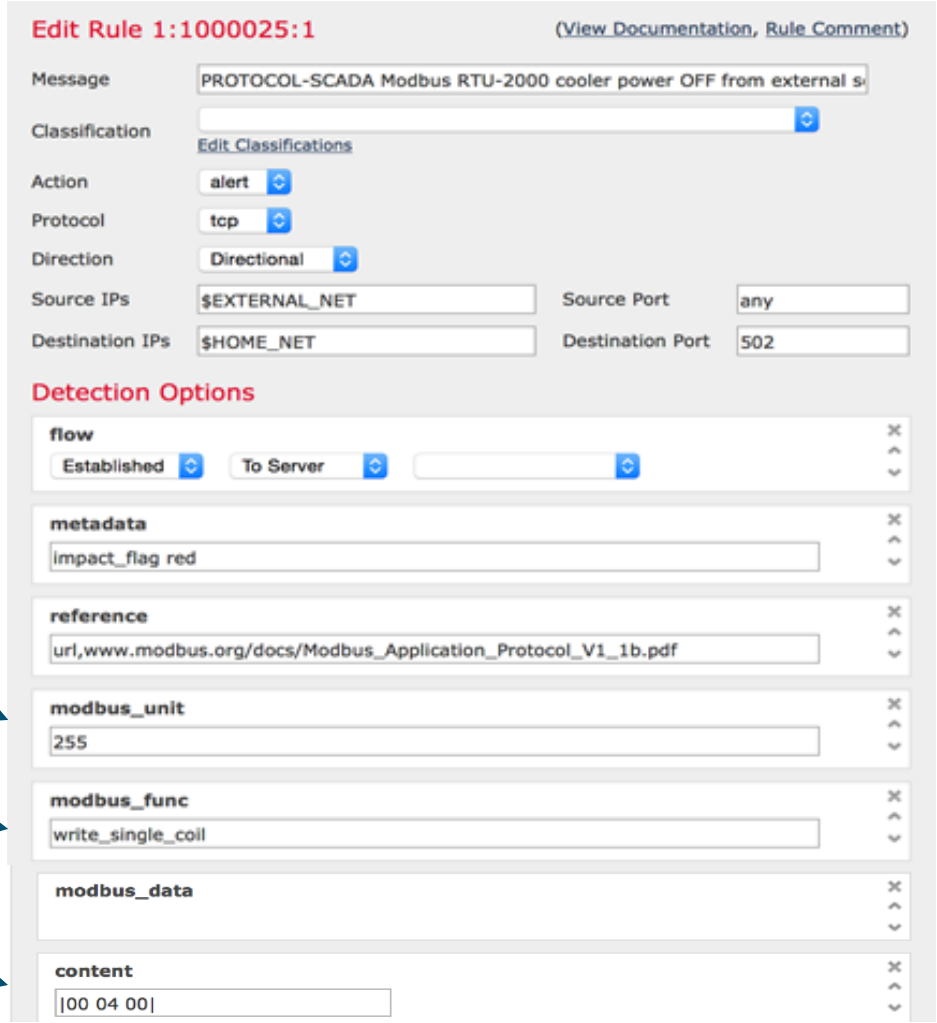








Protocol Parser – Modbus

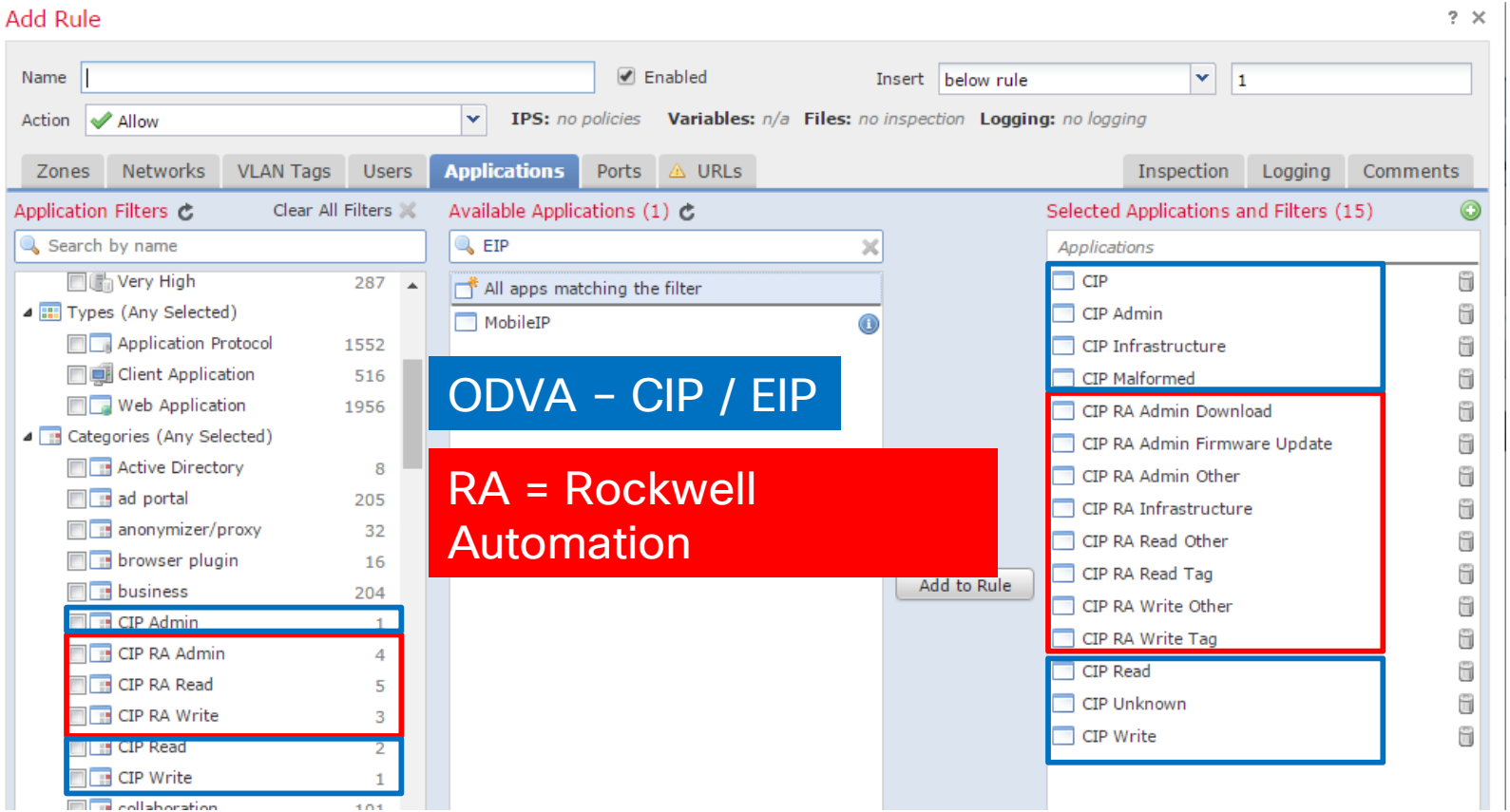


Unit

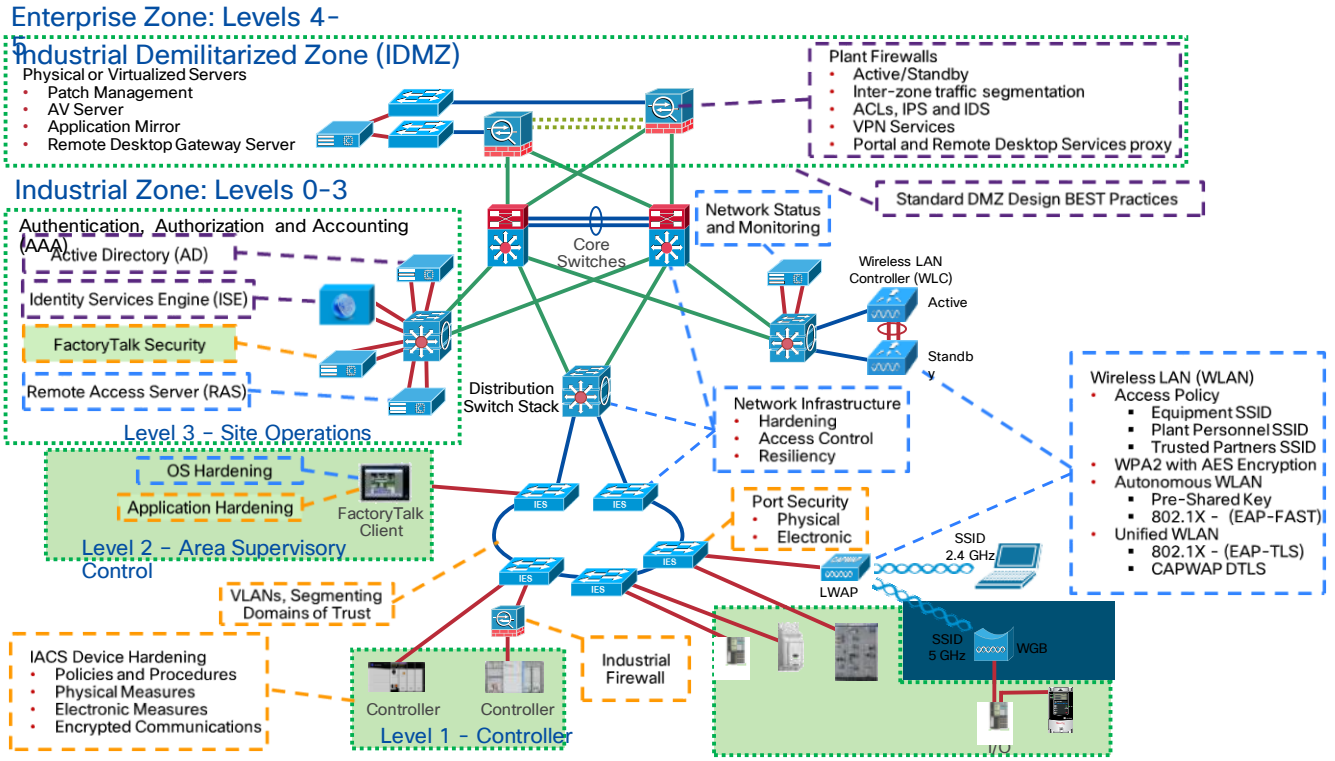
Function

Parameter Value (Data)

Industrial Protocol Identification



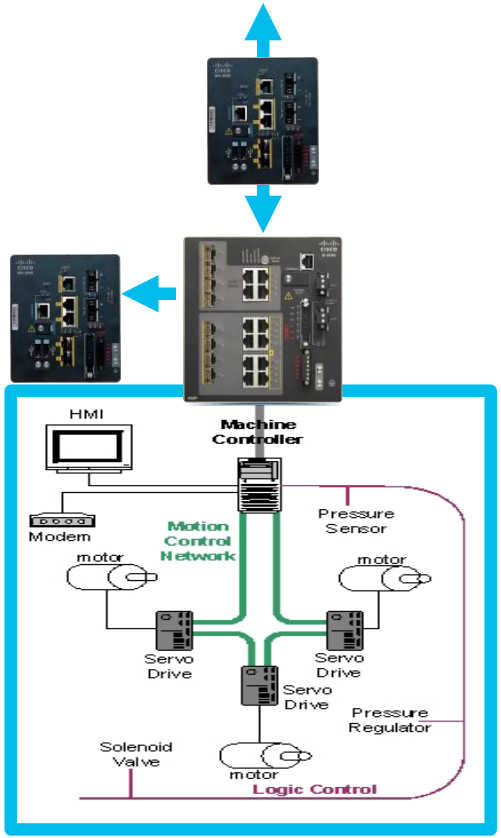
The OT Control System Application Stack



Deploying In-Line Security Slowly / Safely

First:
Learn Out of Band – via span / Tap – cycle through rules Provide Flow to Stealthwatch

Second:
Tune rules / see what would hit and potential impacts. Use flow learning for possible ACLs.

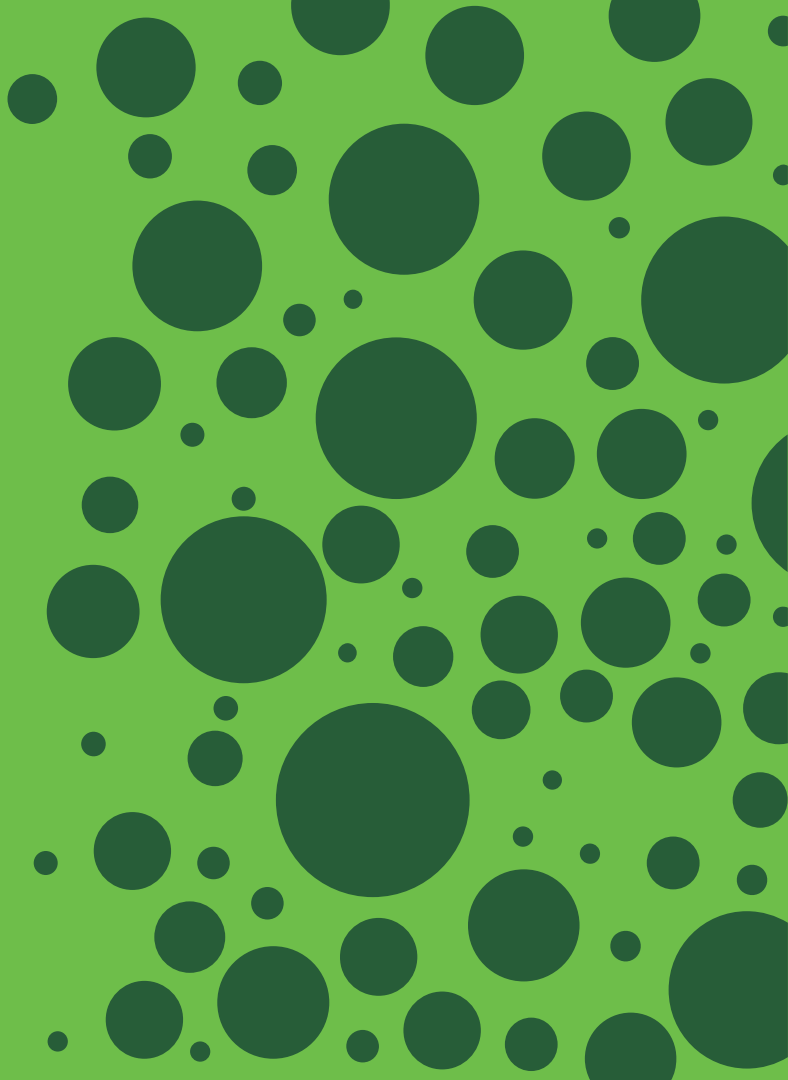


Third:
Move in-line but with “alert” only. Check latency and other network impacts.

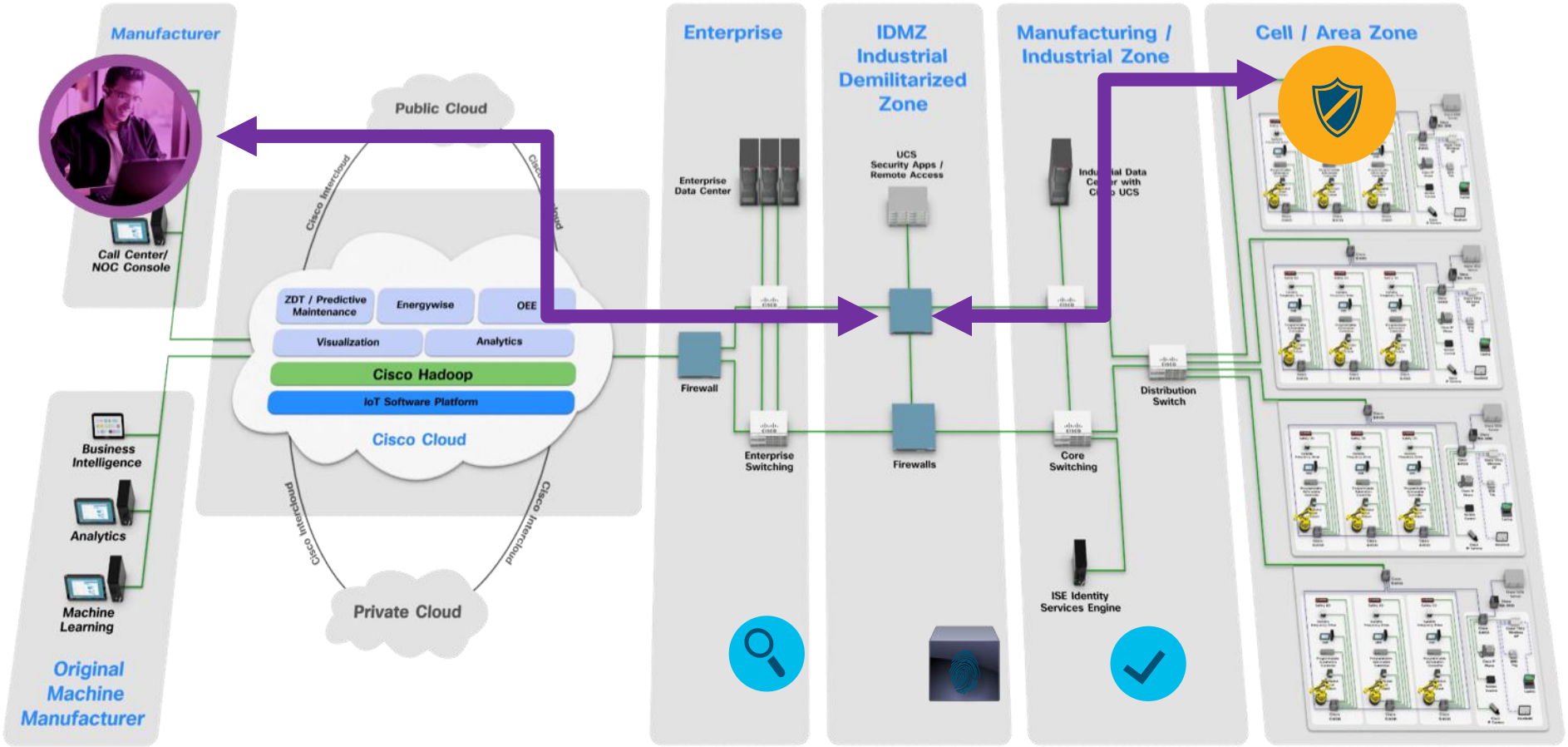
Fourth:
Go live and active.

Sleep well.

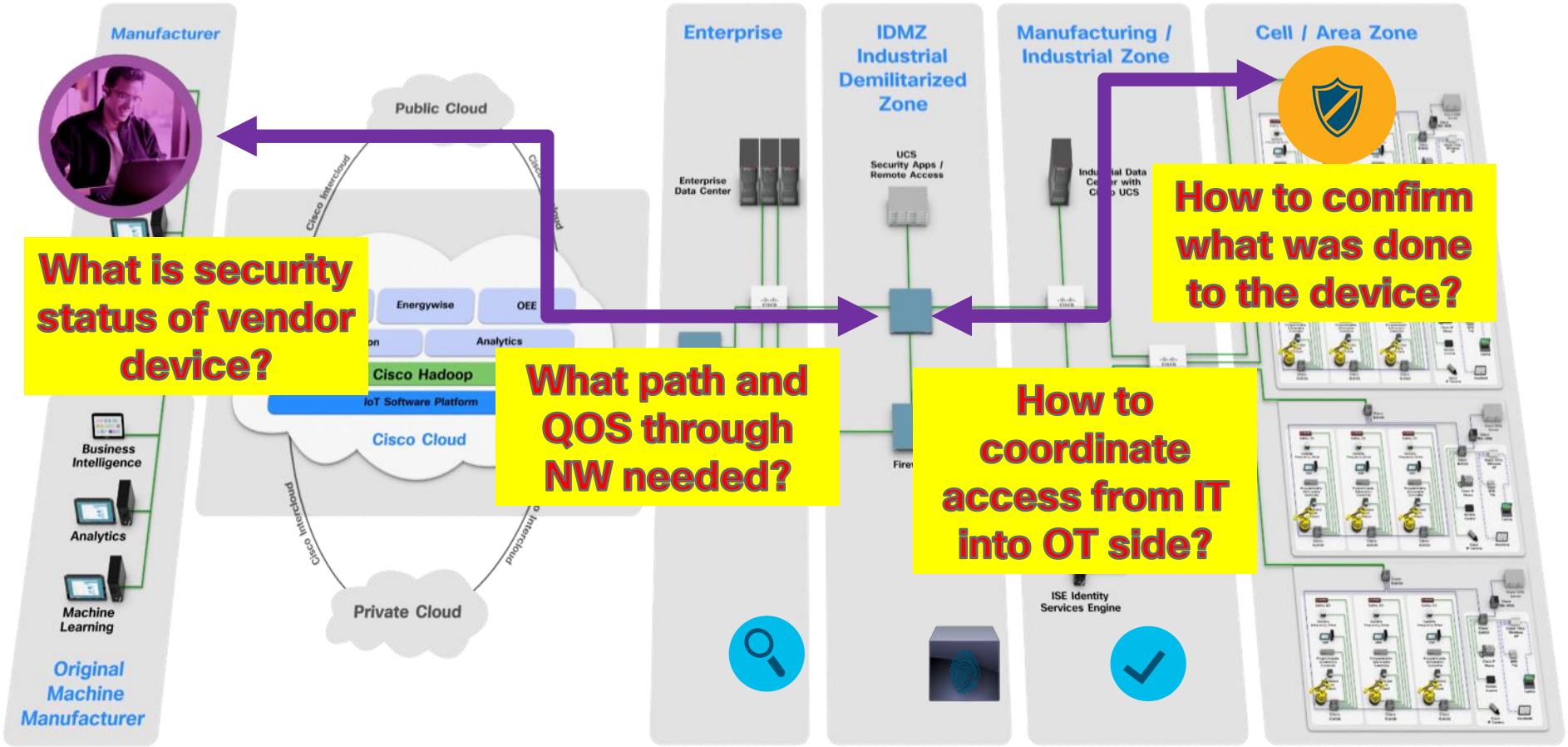
Use Case: Remote Access – A Challenging Necessity



Protect Critical Infrastructure: Allow Secured Remote Access



Protect Critical Infrastructure: Allow Secured Remote Access



For Your Reference

Remote Access Guidance DHS

Configuring and Managing Remote Access for Industrial Control Systems

November 2010

Homeland Security

CPNI
Centre for the Protection of National Infrastructure

Remote Access in Contracts:

- **Ver.10 XXXX Maintenance Support Agreement**
- SERVICE AGREEMENT TERMS AND CONDITIONS
- XXXXX, a division of YYYYY North America Corporation (“ZZZZZ”) will perform the services (“Services”) listed below and on the above pages of this service agreement and any exhibits ("Exhibits") attached to it (together, the “Agreement”) under the following terms and conditions:
- 4. Customer’s Responsibility
- Throughout the term of this Service Agreement, Customer agrees to:
- c. provide suitable remote access to the System to enable ZZZZZ to perform its services hereunder, including but not limited to VPN access to the System;
- d) REMOTE SERVICE. For on-site options, if remote Service is available, the Customer will allow NNN to keep diagnostic and maintenance programs resident on Customer's system or site for the exclusive purpose of performing diagnostics and repair. The Customer has no ownership interest in this software provided by NNN. NNN may remove these programs and any NNN -loaned equipment upon termination of coverage. Customer's system must be configured to permit access. For NNN to provide remote Service, the Customer must allow NNN remote access to eligible NNN systems using the appropriate protocol and method supported by that system. The Customer must provide the necessary equipment designated for that protocol and method of communication to provide remote access to the eligible NNNNt system. **NNN will advise the Customer what is required at the time of installation.**

If this was a North American Utility: This Approach Would be the Law

CIP-005-7 Table R5 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.

Trusted Security Contractor – Failure to Protect

"A third-party URE contractor exceeded its authorized access by improperly copying certain URE data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. "

Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	**Standard**	**Req.**	**VRF/VSL**	**Discovery Method***	**Risk**	**Penalty Amount**
WECC2016016233	CIP-003-3	R4	Medium/ Severe	SR	Serious	$2.7M
WECC2016016234	CIP-003-3	R5	Lower/ Severe			

Security Flowdown

DFARS 252.204-7012 (b) Adequate Security.
The Contractor shall provide adequate security on all covered contractor information systems.

- **Flowdown is a requirement of the terms of the contract with the Government, which must be enforced by the prime contractor as a result of compliance with these terms**

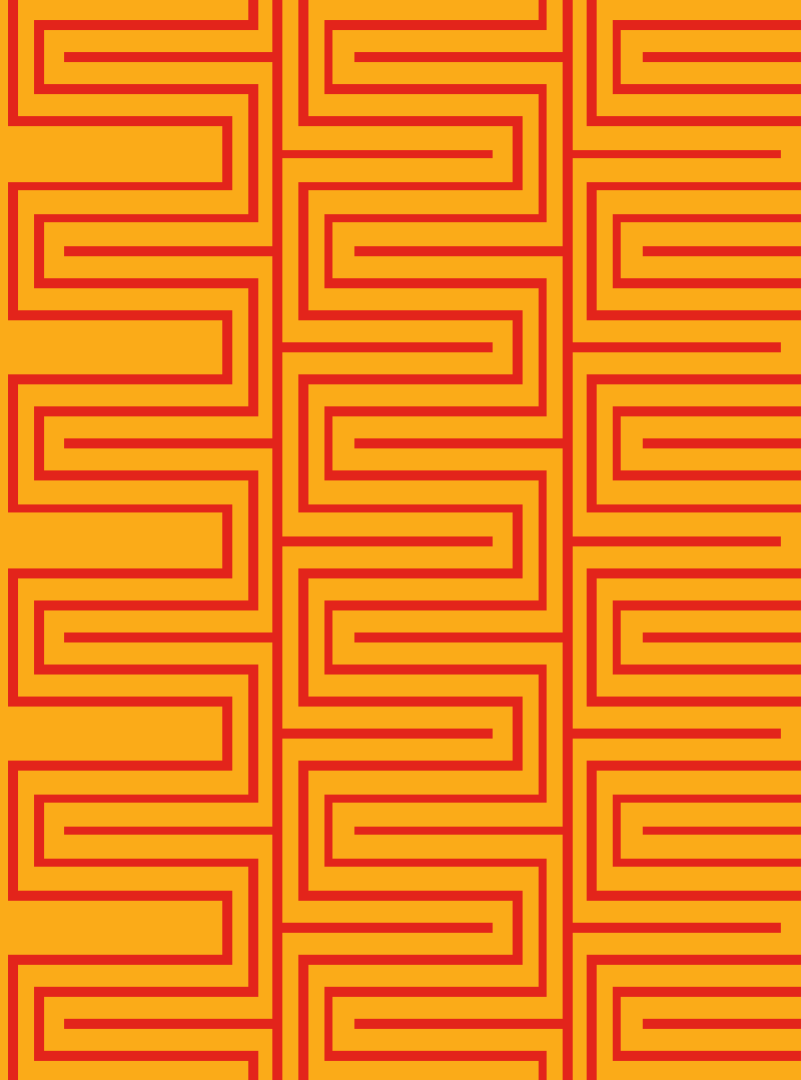
Summary of Common Use Cases

- Secured Communications
  - Segmentation and Hierarchical Network Design
- Threat Control
  - Vulnerability identification and mitigation
- Enhanced Safety and Control
  - Securing equipment from unwanted activity
- Remote Access to Industrial Equipment
  - End to End Who, What, When, Where

Agenda

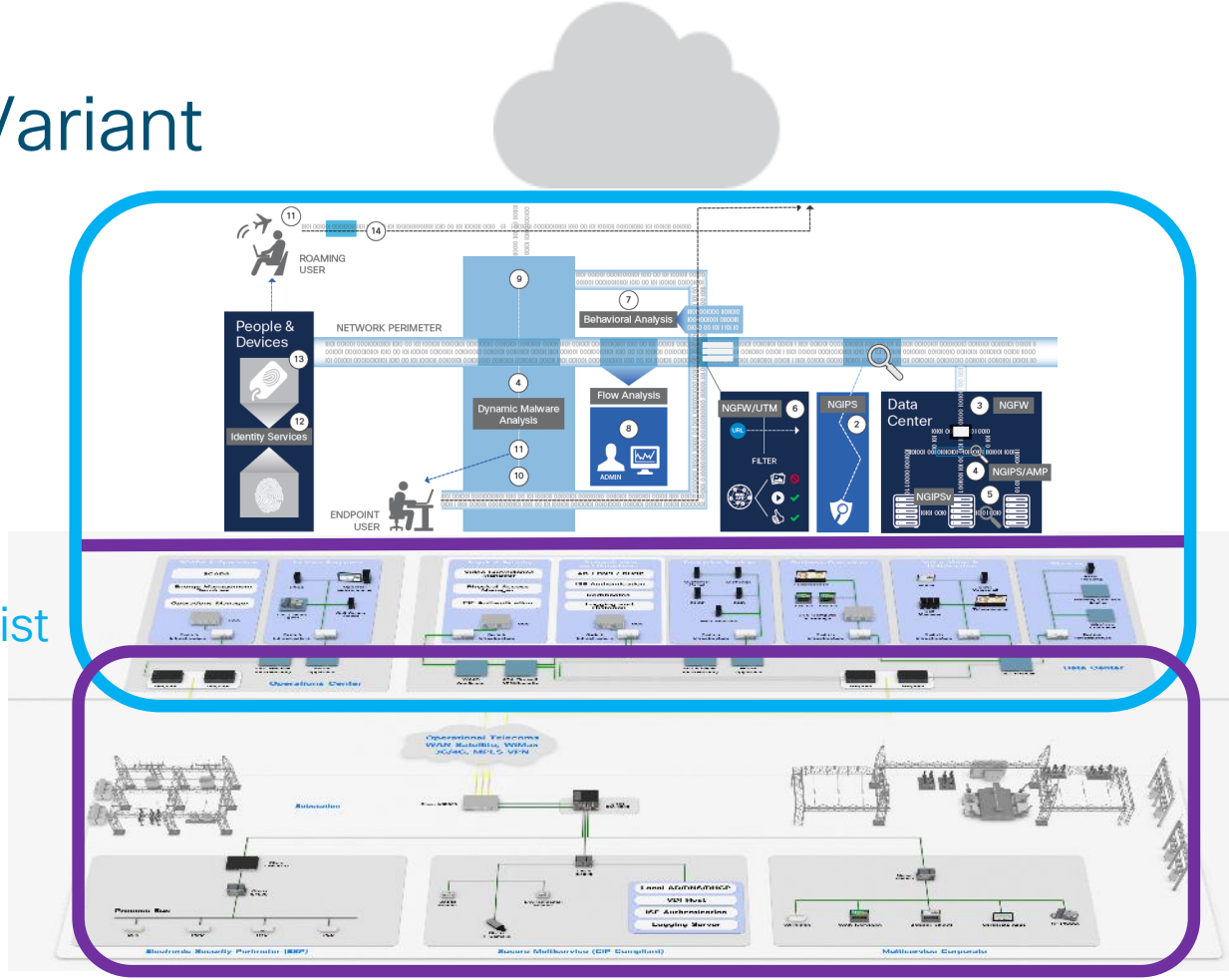
- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 4 Attack Discussions
- Closing / Question & Answer

“Attacks”: Manufacturing; Utilities; Transport; and Your boundaries



Kill Chain – ICS Variant

- Intrusion Phase
  - Reconnaissance
  - Targeting
  - Weaponization
    - Develop / Test
  - Delivery / Exploit / Persist
  - Install
  - Modify Systems
  - Command and Control
  - Attack
  - Anti-Forensics



ICS Attack Data Analysis – Malware

- Incidental Infections
  - Untargeted Virus, Worms
  - WannaCry/Petya/Not-Petya
    - $1.5B in losses
  - Thousands

- ICS Themed Attacks
  - Targeted Malware, nothing ICS specific – just named to get OT interest
  - Tens

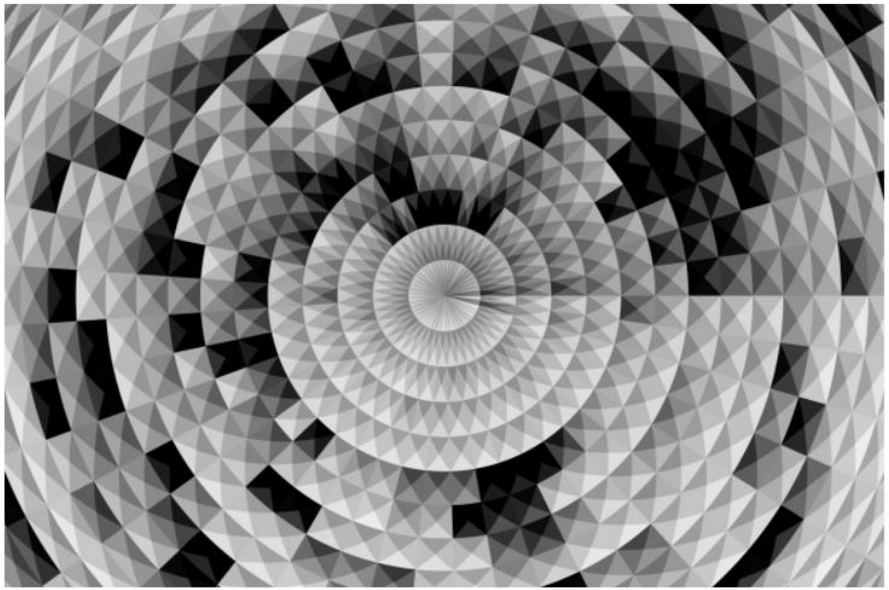
- ICS Specifically Tailored
  - Written for ICS systems OR modified for ICS systems
  - 3+3
    - Stuxnet
    - Havex
    - Black Energy 2
    - CrashOverride (Industroyer)
    - Trisis (Hatman)
    - *VPNFilter*

Credit – Dragos Security – Project Mimics

Attacks Can Break Things...

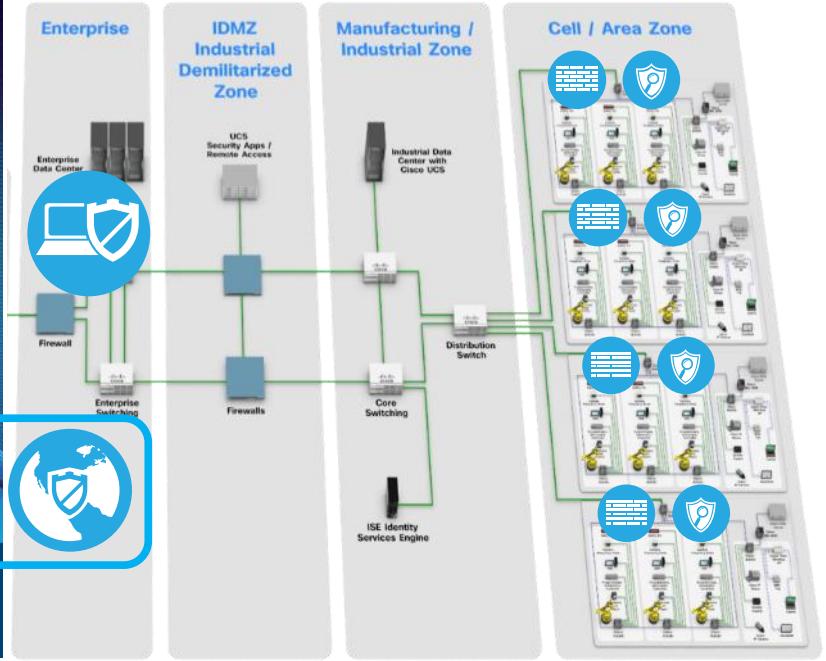
KIM ZETTER SECURITY 01.08.15 5:30 AM

A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER



German Smelter Attack: Reconnaissance / Targeting

- What is known:
  - Phishing Attack
  - Malware
  - Access to ICS System
  - Shutdown commands
  - Damaged smelter



* OT Baseline features

2017 / 2018's Top Security News

Not a targeted attack

Impact in Ukraine:

Attack

3+ hours of lost power

@ month of degradation

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

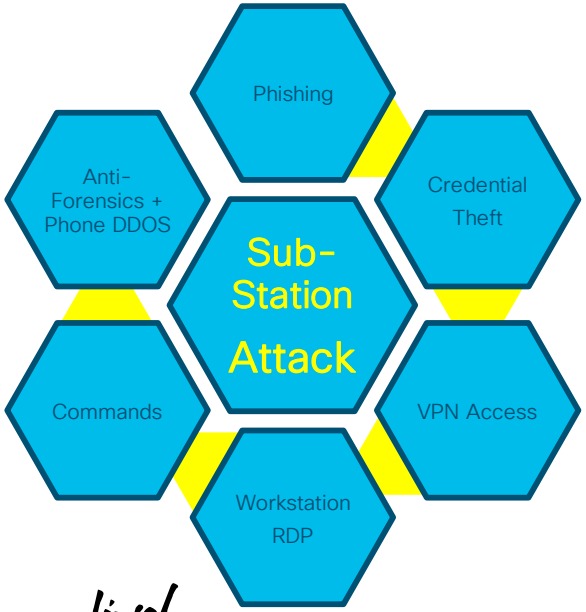
2015 Ukraine Utility Attack – Simplified View

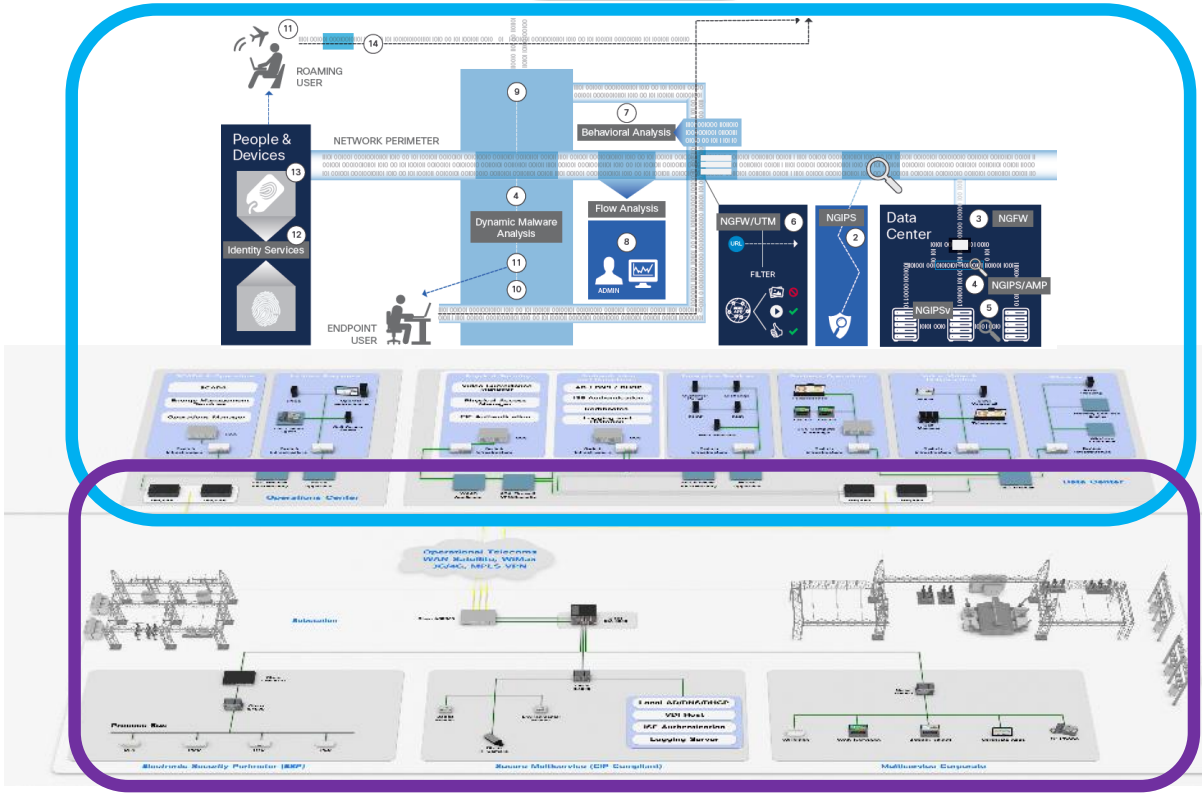
2016 Variations

- Spear Fishing into IT
- BlackEnergy Malware Placed
- Credential Theft for Access
- VPN access from outside
- Remote management tools
- DOS of ICS components
- Control protocol commands
- Firmware update / corruption
- UPS system disabled
- KillDisk anti-forensics wipe
- Telephone DDOS

Kill Chain – ICS Variant

- Attacks start on IT side
- Work their way to OT

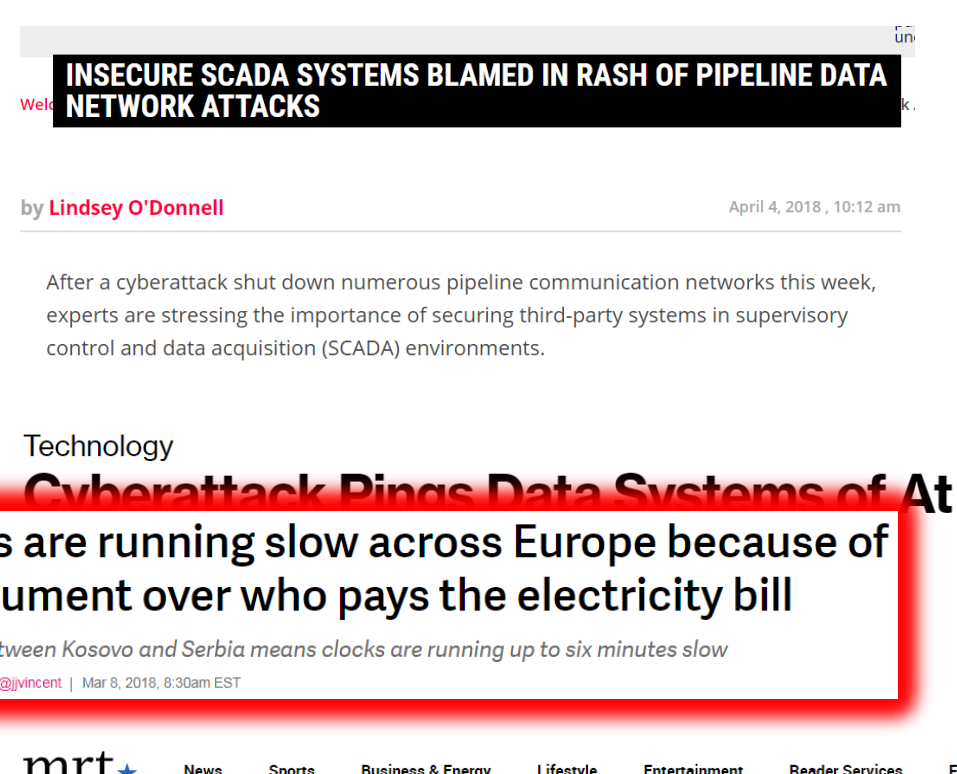




System Boundaries

"Your perimeter is not the boundary of your network it's the boundary of your telemetry."

the grugq



Impact in LA:

Attack

intersections snarled for 4 days

Key signals targeted, officials say

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

January 09, 2007 | Sharon Bernstein and Andrew Blankstein | Times Staff Writers

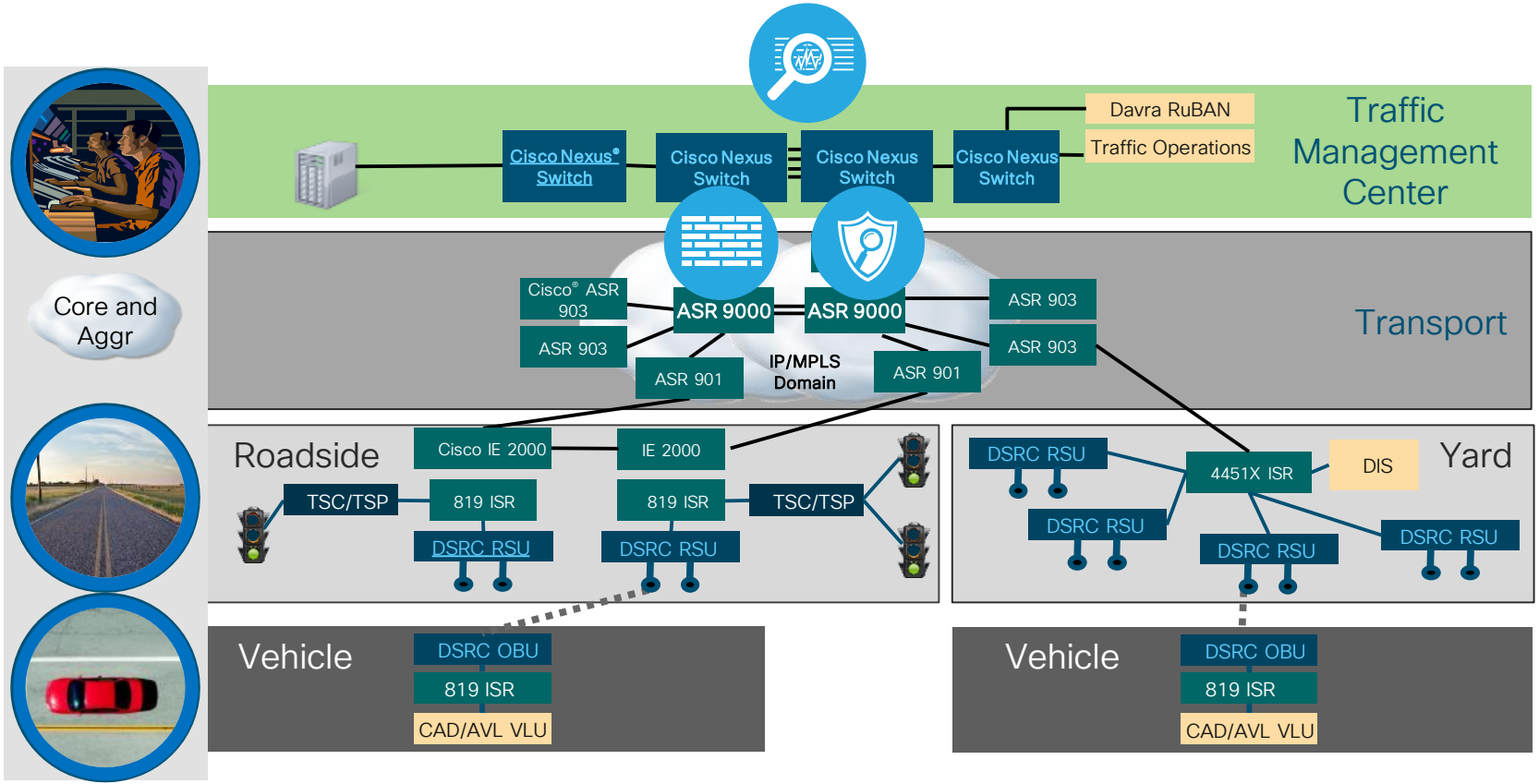
Email Share G+1 0

Back in August, the union representing the city's traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

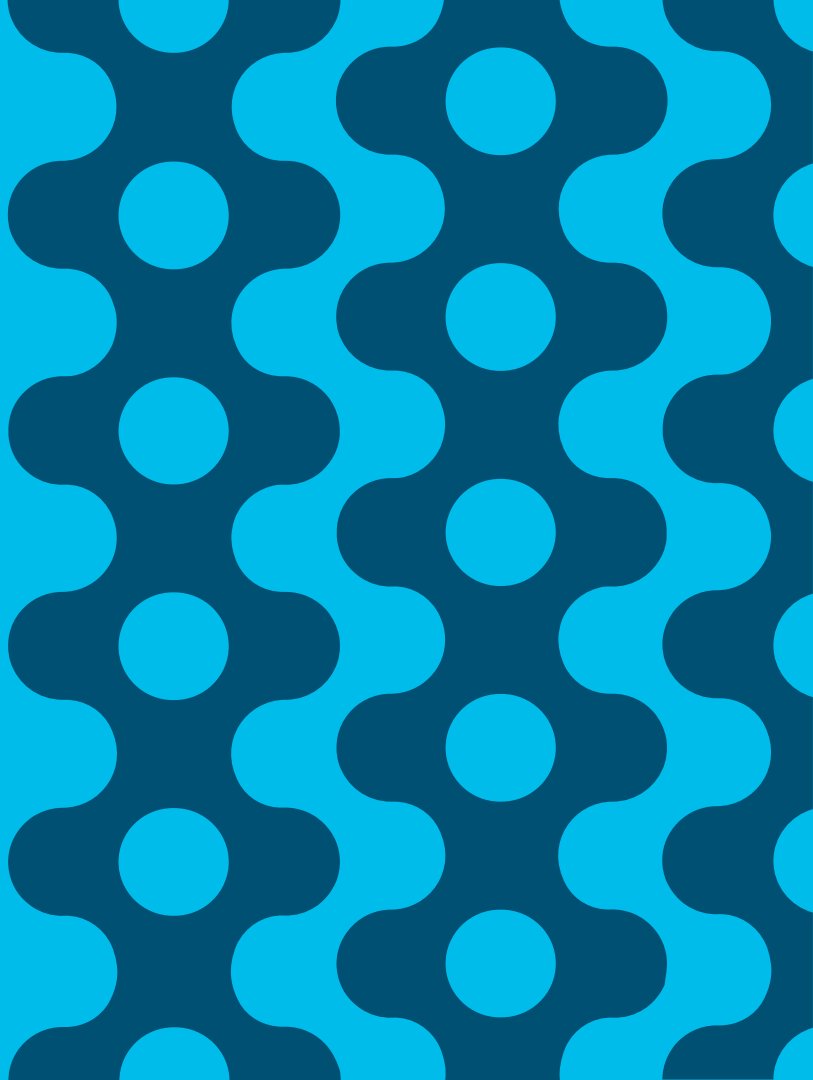
City officials took the threat seriously.

Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.

Stolen Credentials / Problematic Commands



Cisco Validated Designs: Your Guides to Security



Cisco live!

Partner Driven Validated Designs

Rockwell Automation and Cisco Four Key Initiatives:

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Validated Design for Industrial DMZ

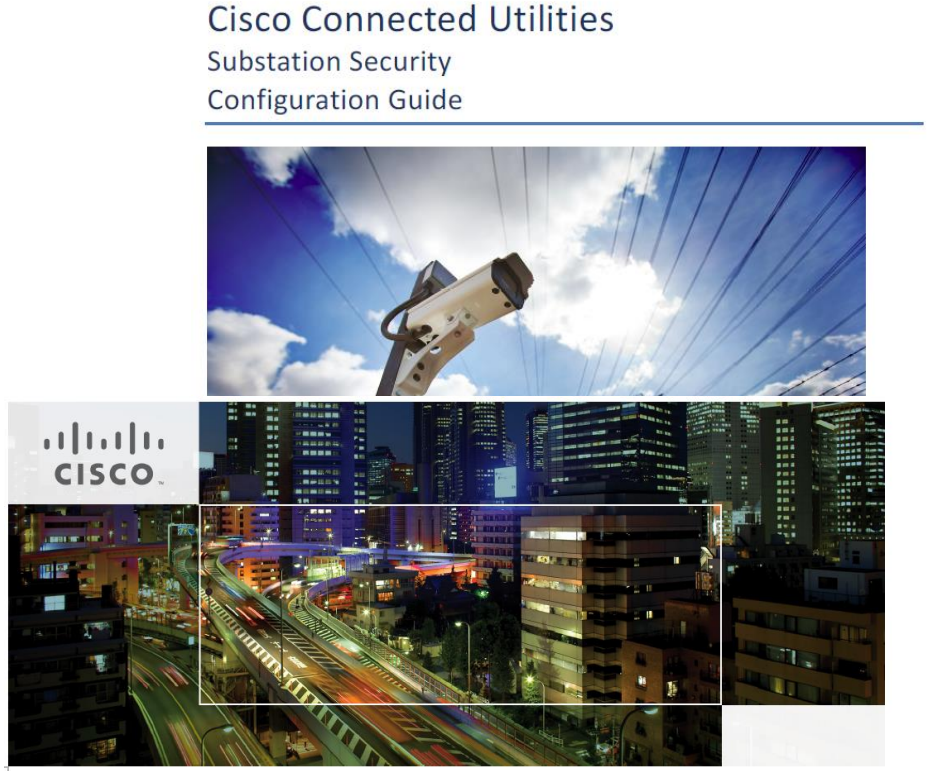
CPwE Industrial Demilitarized Zone (IDMZ)

Design and Implementation Guide (May 2017)

White Paper

At-a-Glance (PDF - 207 KB) 

Connected Utilities Validated Designs



Cisco Connected Pipelines

- Cisco combines its own expertise in oil and gas systems with entities such as Schneider Electric for deployment services.
- An end-to-end smart connected solution based on industry best practices for pipeline infrastructures and network architectures.
- Flexible, modular, approach from assessment, design, and test to deploy install and support.
- Collaborative expertise and service from the leaders in SCADA, network connectivity, and security resulting in cost savings and optimized operations.

Schneider Electric

Cisco Connected Pipelines

Prevent Pipeline Accidents, Sabotage, and Theft

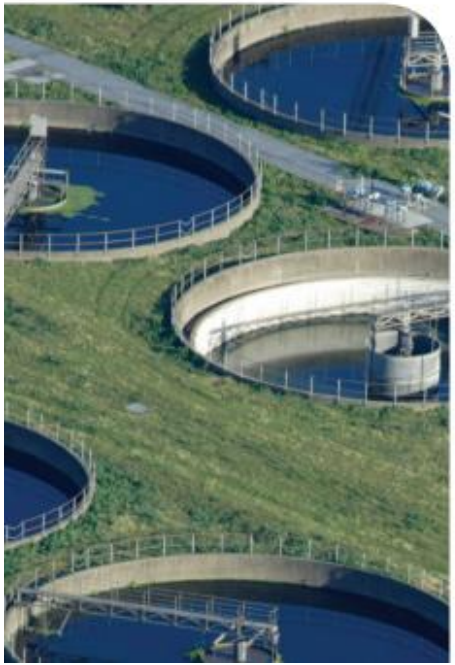
A disturbance is occurring along a large, remote section of your pipeline. "Optical microphones," the recording capabilities of your fiber network, detect movement. Is it an animal nearby, someone walking – or are laborers planning to dig, unaware of the pipeline? Or is it sabotage?

Video analytics software begins relaying images of earth-digging machines heading for the pipeline. Alerts are sent to the pipeline operator, who determines the activity is unauthorized and dispatches security. They arrive soon after and stop the digging before intruders damage the pipeline.

This is Cisco® Connected Pipelines for Oil and Gas in action. With it, pipeline operators are protecting their assets from accidents and cyber and physical attacks. They are reducing leaks and spills and the inevitable public outrage over environmental damage. And they are gaining greater control over longer stretches of their pipelines with existing expert resources.

Strong Growth, Dangerous Locations

Cisco Partnerships for Water Management



Cisco and Rockwell Automation Solutions for Water Management At-A-Glance

Challenges Facing the Water Industry

Today's water industries are approaching a crisis in many countries between the economy and more extreme weather patterns, drought, and flooding that are challenging our water systems. Utility operations teams need to become more agile and efficient to deal with rapidly changing conditions. Primary challenges include:

- Rising costs of maintenance, equipment, and supplies
- Retiring workers being replaced with less experienced technicians
- Dealing with leakage issues, especially in drought-impacted countries
- Managing facilities within geographic areas with fewer personnel
- Remaining compliant with changing regulations; for example, the European Union now dictates that companies retain six months of water treatment data

Agenda

- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 4 Attack Discussions
- Closing / Question & Answer

Tasks for your OT Security Journey

1 First

- Update your network
  - Gain a view of the network and applications
  - Establish access control that reflects the networks

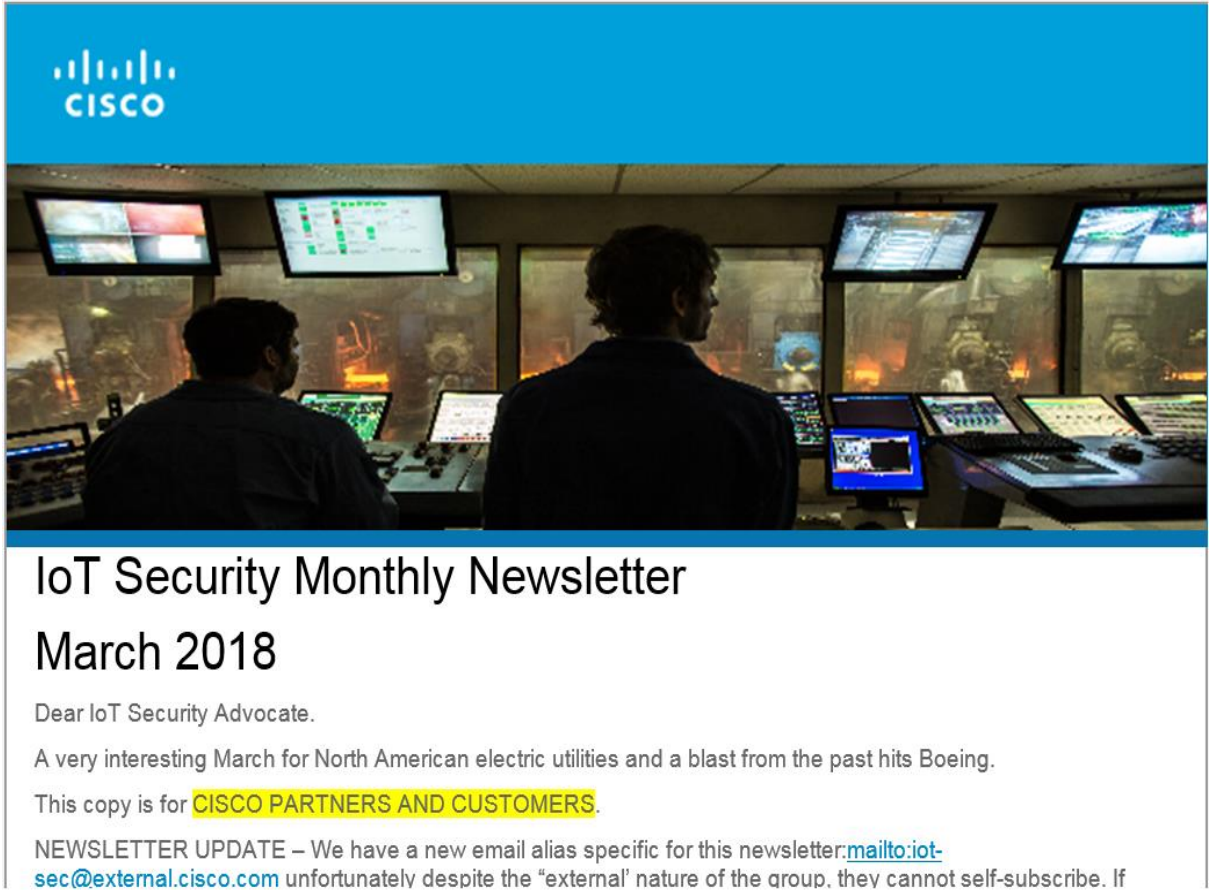
2 Second

- Understand your applications
  - Who is talking to who
  - What are they saying
  - Establish base lines
- Determine what is truly necessary

3 Third

- Get Help
  - IT has done security for years
  - Look at design guides
  - Consider external services
- Act
  - Commit to making change

Industrial Security Newsletter



IoT Security Monthly Newsletter

March 2018

Dear IoT Security Advocate.

A very interesting March for North American electric utilities and a blast from the past hits Boeing.

This copy is for CISCO PARTNERS AND CUSTOMERS.

NEWSLETTER UPDATE – We have a new email alias specific for this newsletter:mailto:iot-sec@external.cisco.com unfortunately despite the "external' nature of the group, they cannot self-subscribe. If

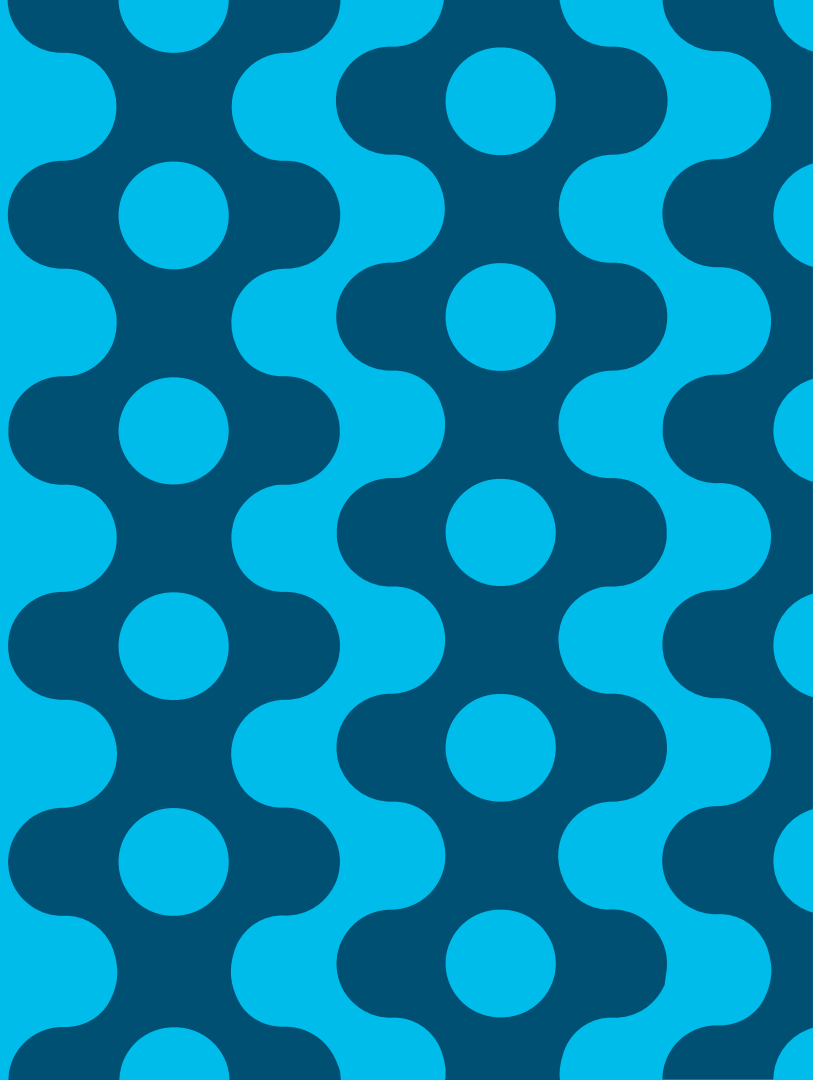
OT Insights

Solution Overview and Demo

Hazim Dahir

Session ID

Improving Operational Reliability and Enabling New Business Outcomes

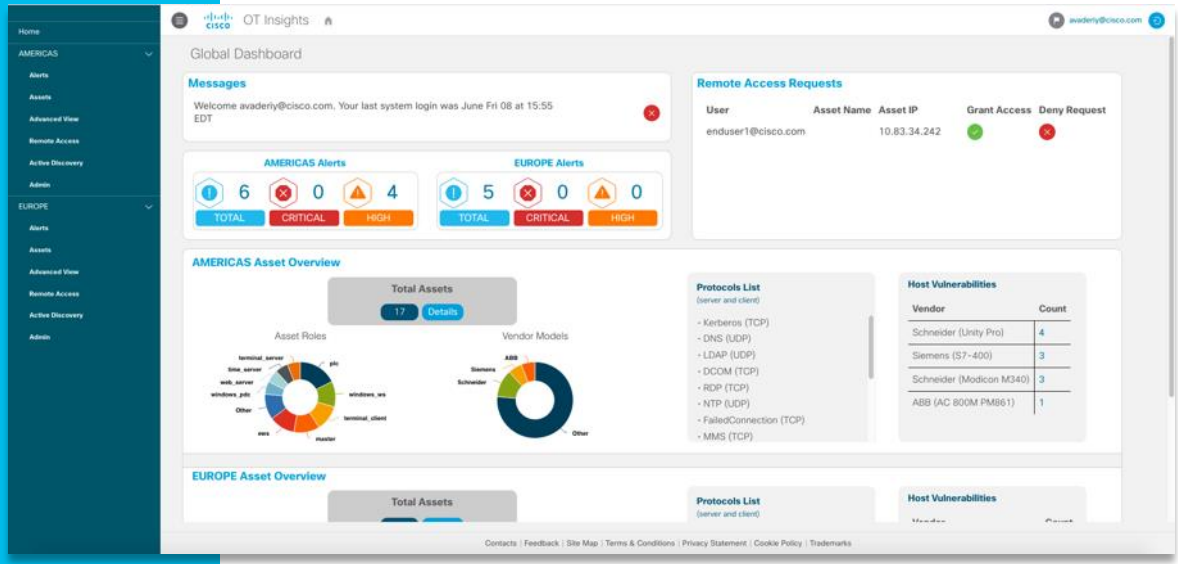


Cisco live!

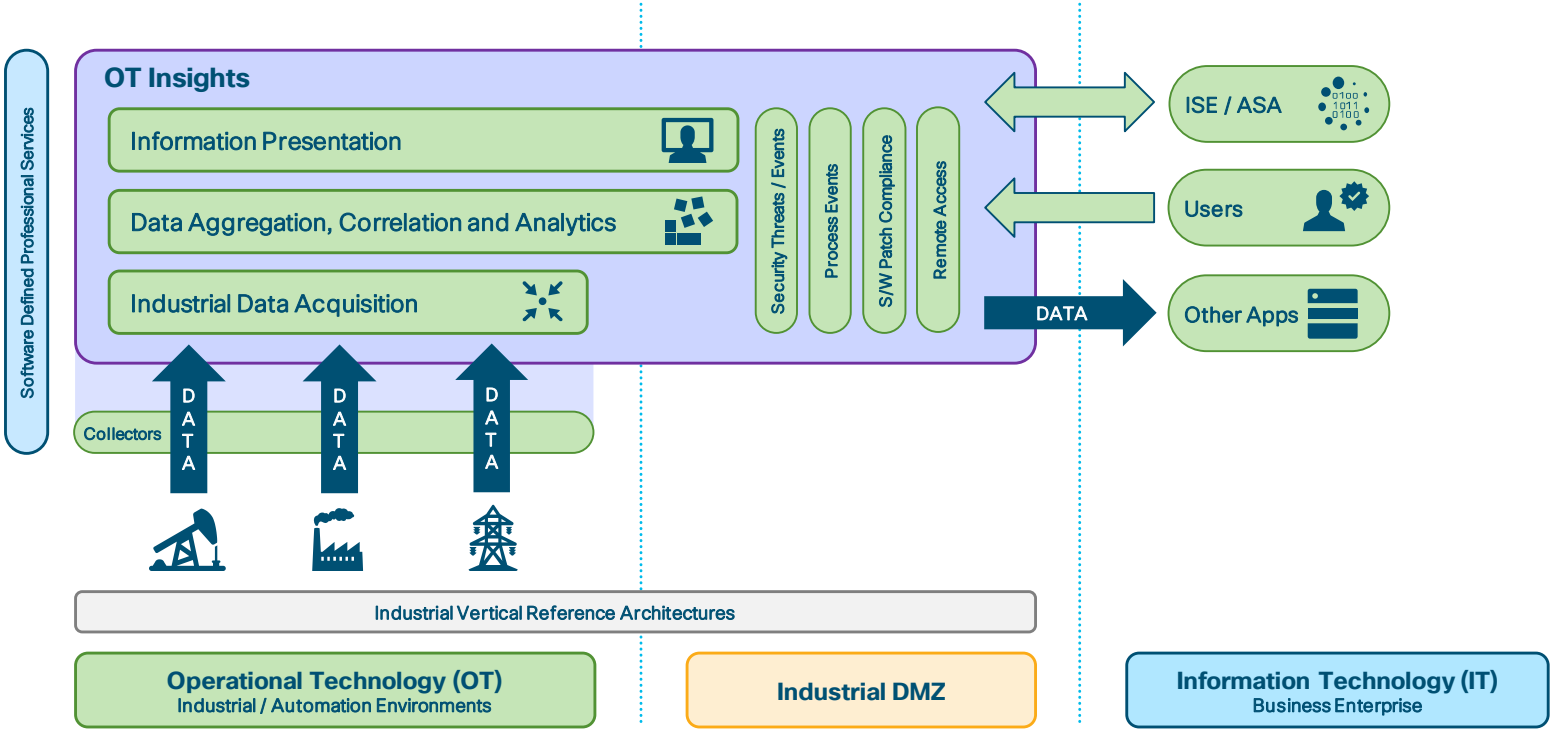
Services Solution

Flexible, scalable platform to proactively improve operations and security:

- Visualization of industrial process and security events by region, site and asset
- Designed for quick issue analysis and resolution and post-event response
- Tailored to industrial operations roles and responsibilities
- Remote access user provisioning, session control, and recording
- On demand report generation and data export to external platforms
- Extensible and modular visualization of operational and asset metrics



Solution Architecture



Q & A

ralbach@cisco.com

Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

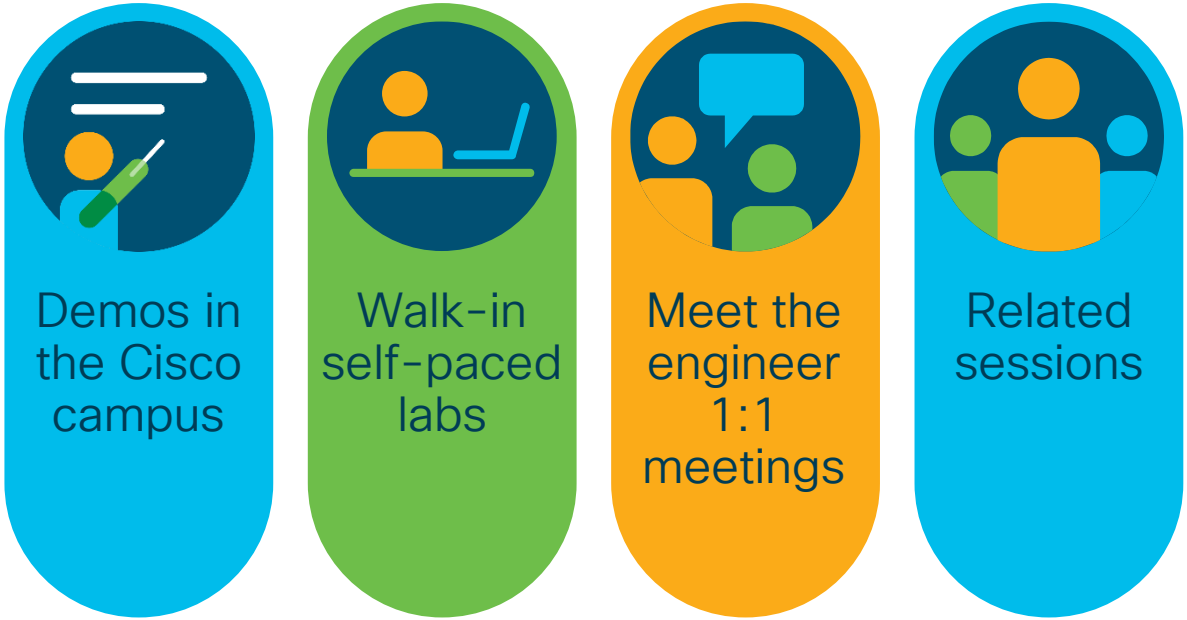
Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Internet of Things (IoT) Cisco Education Offerings

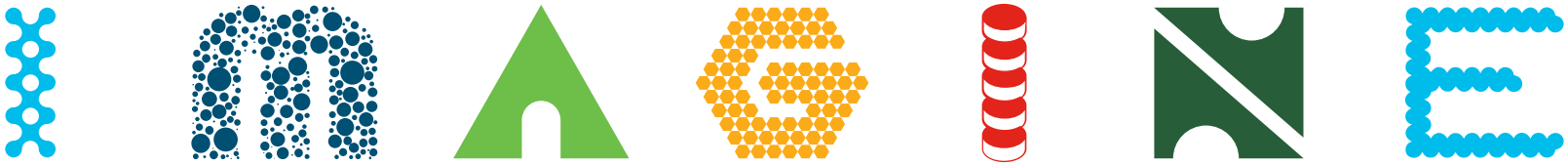
Course	Description	Cisco Certification
NEW! Managing Industrial Networks for Manufacturing (IMINS2 v1.3)	An associate level instructor led lab based training focuses on common industrial application protocols, security, wireless and troubleshooting designed to prepare you for the CCNA Industrial certification	CCNA® Industrial
Managing Industrial Networks with Cisco Networking Technologies (IMINS)	This instructor led lab based training addresses foundational skills needed to manage and administer networked industrial control systems for today's connected plants and enterprises. It helps prepare plant administrators, control system engineers and traditional network engineers for the Cisco Industrial Networking Specialist certification.	Cisco Industrial Networking Specialist
Control Systems Fundamentals for Industrial Networking (ICINS)	For IT and Network Engineers, provides an introduction to industry IoT verticals, automation environment and an overview of industrial control networks (E-Learning)	Pre-learning for IMINS, IMINS2 training & certifications
Networking Fundamentals for Industrial Control Systems (INICS)	For Industrial Engineers and Control System Technicians, covers basic IP and networking concepts, and introductory overview of Automation industry Protocols.	Pre-learning for IMINS, IMINS2 training & certifications

For more details, please visit: http://learningnetwork.cisco.com
IMINS2 http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-industrial.html
IMINS http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/internet-of-things/iot-networking.html
Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com

Continue your education



Thank you



INTUITIVE

Cisco live!

June 10-14, 2018 • Orlando, FL

#CLUS