



Holistic Cybersecurity for Industrial IoT Applications

Arun Siddeswaran, Cisco Systems, Inc.
Gregory Wilcox, Rockwell Automation, Inc.

October 10, 2018

Industrial IoT (IIoT) offers the promise of business benefits through the use of innovative technology. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices.

No single product, technology or methodology can fully secure IIoT applications. Protecting IIoT assets requires a holistic security approach to help address different types of threats. This approach uses multiple layers of diverse technologies for protection and detection, applied at different levels of IIoT applications, while being implemented by different personas.

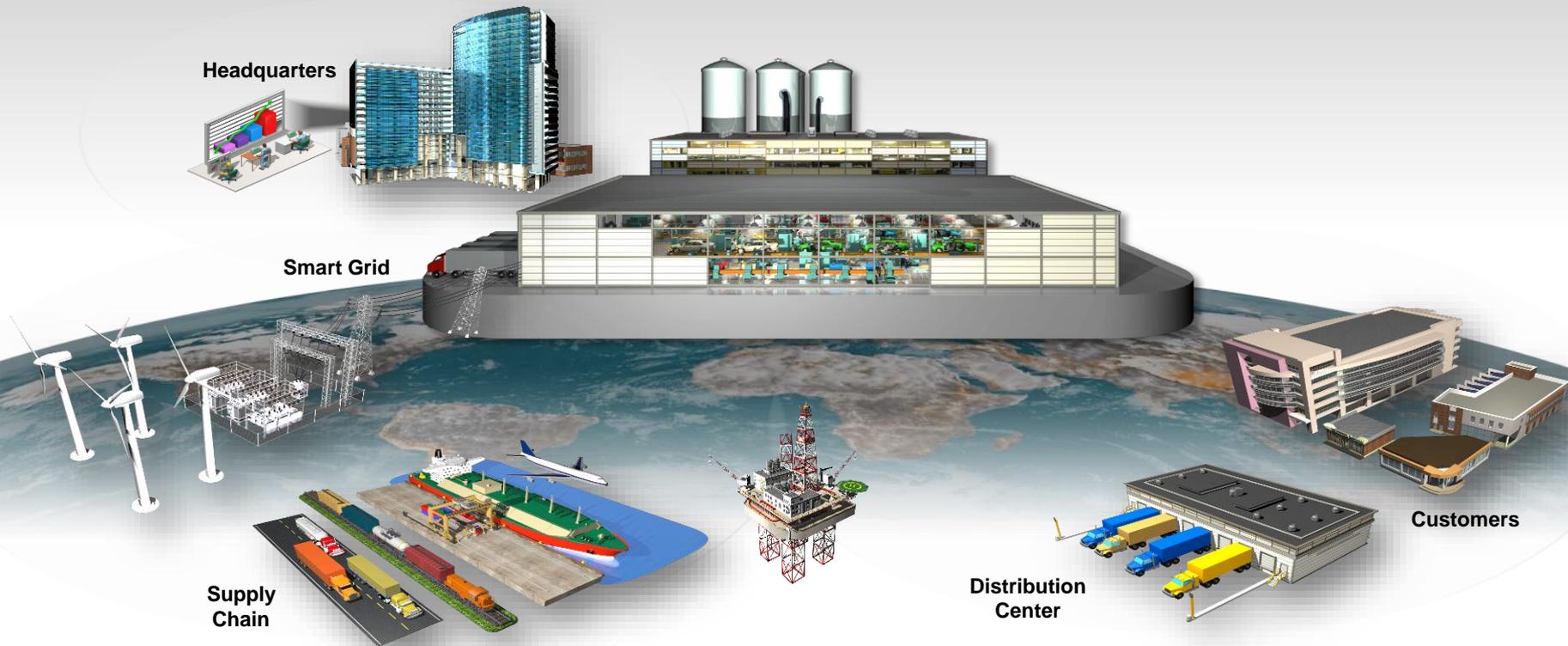
This paper, authored and presented by Cisco Systems and Rockwell Automation, will provide an overview of a holistic IIoT security framework. This framework incorporates aspects of IEC-62443 and NIST 800-82, leverages CIP Security™ for security zoning, addresses OT and IT personas, and enables secure connectivity from smart devices to smart machines to cloud applications.

- Industrial IoT (IIoT) Opportunities / Challenges
- Industrial Security Trends
- Holistic and Diverse Plant-wide Security
- Key Takeaways
- Recommended Resources



Industrial IoT (IIoT) Opportunities / Challenges

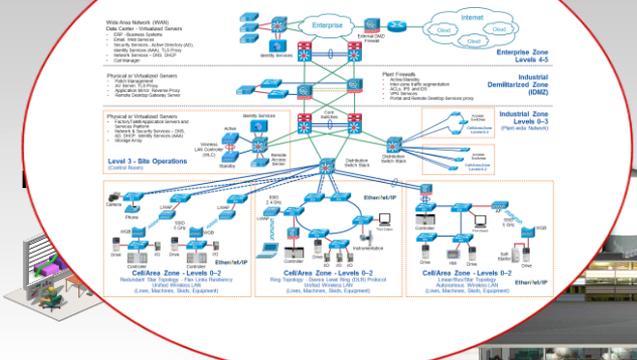
Industrial IoT Architectures



Source: Rockwell Automation

Industrial IoT Architectures

Connected Architectures



Industrial Standards



SMART



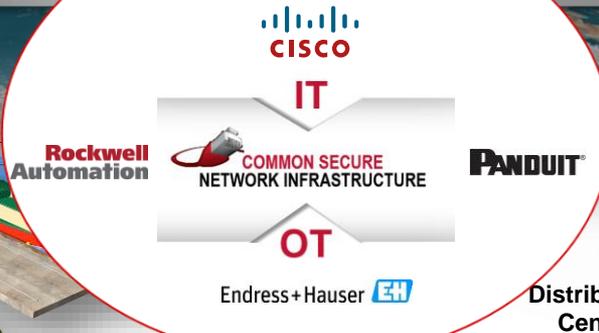
PLANTS / OPERATIONS

EQUIPMENT / SKIDS / MACHINES



DEVICES

Convergence



Cybersecurity Threats

Threat Types

- Malware
- Removable Media
- Spyware
- DDoS
- Ransomware
- Spear Phishing

Threat Actors

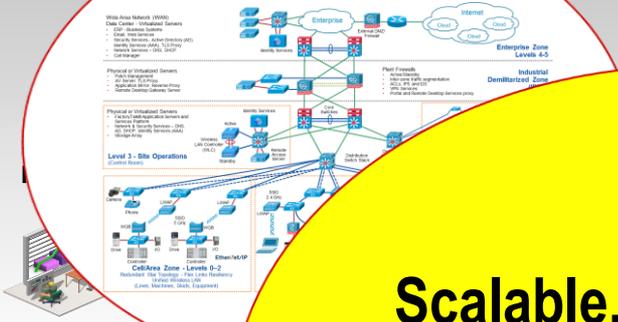
- Internal/Insiders
- Hackers
- Hacktivist
- Cyber Criminals
- Nation States

Increasing Risk

Powerful, yet simple to use tools are readily available

Industrial IoT Architectures

Connected Architectures



Industrial Standards



Scalable, Reliable, Safe, Secure and Future-ready Industrial IoT Architectures requires an ecosystem.

SMART



PLANTS / OPERATIONS

EQUIPMENT / SKIDS / MACHINES



DEVICES



Endress + Hauser

Distribution Center

Cybersecurity Threats

Threat Types

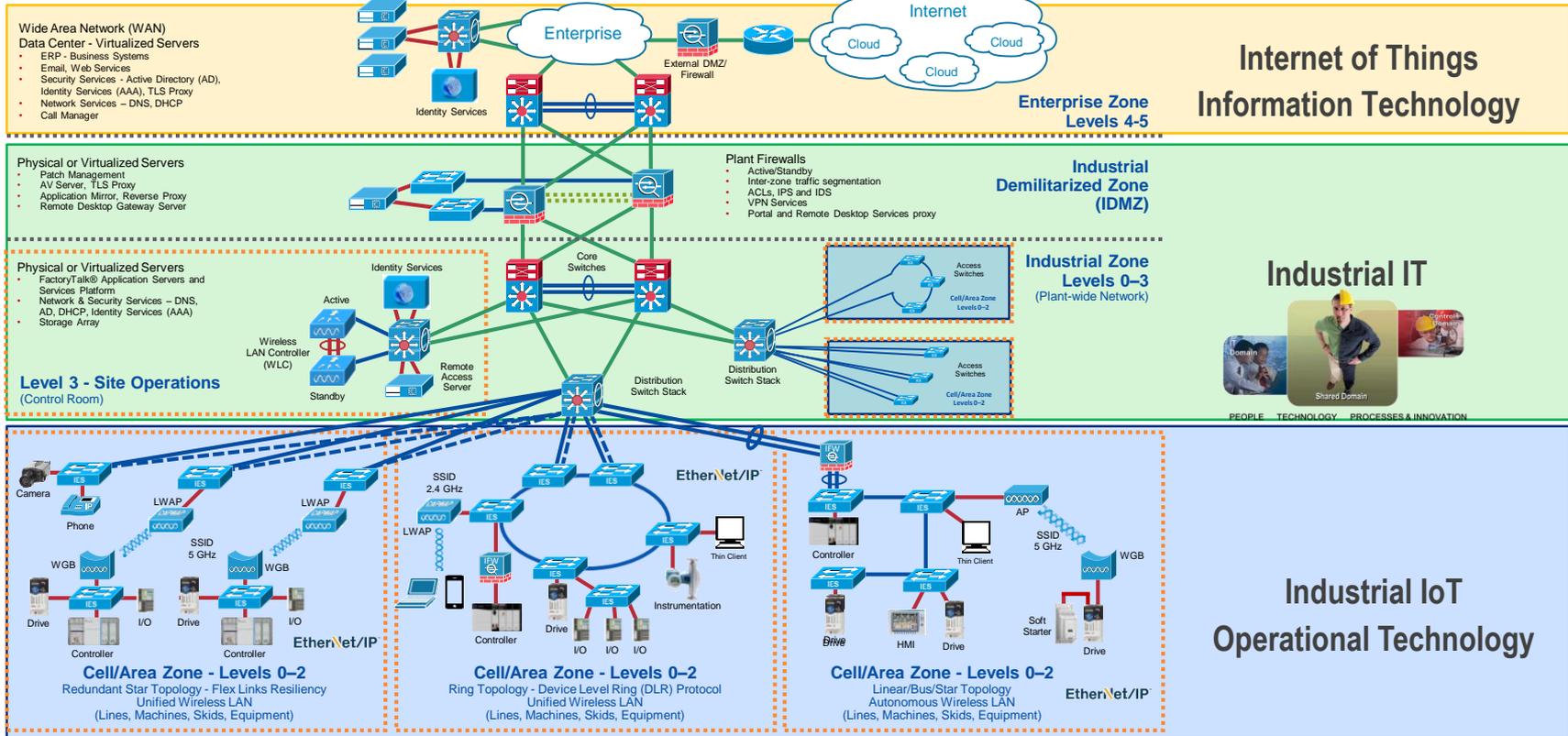
- Removable Media
- DDoS
- Spear Phishing
- Ransomware

Threat Actors

- Internal/Insiders
- Hackers
- Hactivist
- Cyber Criminals
- Nation States

Increasing Risk

Powerful, yet simple to use tools are readily available



Cybersecurity – OT vs. IT

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
 ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	Can be difficult to deploy
 SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	Up to 40+ years
 OUTSOURCING	Common/widely used	Rarely used (vendor only)
 APPLICATION OF PATCHES	Regular/scheduled	Slow (vendor specific, compliance testing required)
 CHANGE MANAGEMENT	Regular/scheduled	Legacy based – unsuitable for modern security

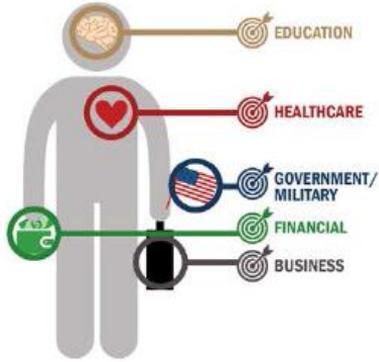
SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
 TIME CRITICAL CONTENT	Delays are usually accepted	Critical due to safety
 AVAILABILITY	Delays are usually accepted	24 x 7 x 365 x forever (Integrity also critical)
 SECURITY AWARENESS	Good in both private and public sector	Generally poor inside the control zone
 SECURITY TESTING/AUDIT	Scheduled and mandated	Occasional testing for outages / audit for event recreation
 PHYSICAL SECURITY	Secure	Traditionally good

Source: U.S. Department of Homeland Security



Industrial Security Trends

World Wide Threat Assessment Information



Cyber threats increasing in frequency, scale, sophistication and severity of impact



Several nations have undertaken offensive cyber operations against private sector targets



Cyber threat cannot be eliminated, rather, cyber risk must be managed



The likelihood of a catastrophic attack is remote at this time; rather, we envision an ongoing series of low-moderate level cyber attacks which will impose cumulative costs on U.S. economic competitiveness and national security

Director of National Intelligence James Clapper to the House Permanent Select Committee on Intelligence - September 10, 2015



Cybersecurity Spending Trends

Cybersecurity market estimated to be worth \$75.4B in 2015

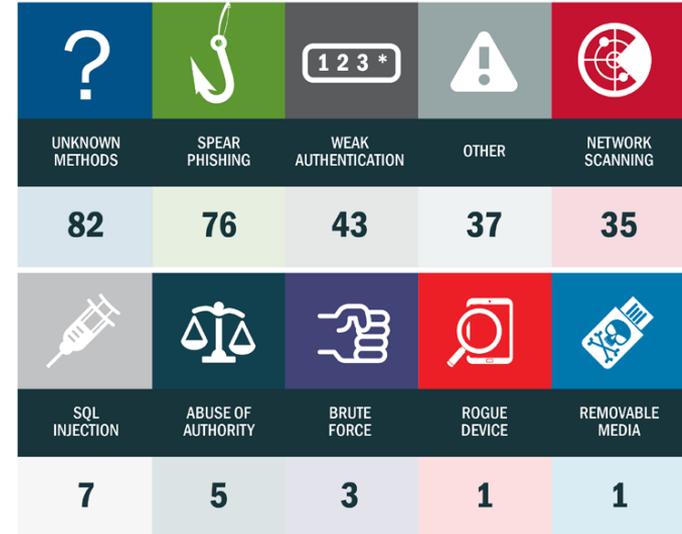
- Expected to reach \$101B in 2018 and \$170B by 2020

Source: U.S. Department of Homeland Security

State of the World: Risk Evolution



FY16 Incidents by Sector: 290 Total



FY16 Infection Vector: 290 Total

Source: U.S. Department of Homeland Security

Balancing Cost vs. Risk vs. Productivity

Stance on Availability, Safety and Security

- Drivers for determining overall tolerance to risk and for developing risk management policies:
 - Business practices
 - Corporate / local standards
 - Application requirements
 - Applicable industry security standards
 - Government regulations and compliance
- Security/safety policies and procedures, for access control and network and security ownership:
 - Alignment with industrial functional safety standards such as [IEC 61508](#), [IEC 62061](#) (SIL), [ISO 13849](#) (PL)
 - Alignment with industrial security standards such as [IEC-62443](#) (formerly ISA99), [NIST 800-82](#) and [ICS-CERT](#)

Established Industrial Security Standards

- International Electrotechnical Commission (IEC)
 - IEC 62443 (Formerly ISA99), Industrial Automation and Control Systems (IACS) Security
 - Zones and Conduits
 - Defense-in-Depth
 - Security Zones
- National Institute of Standards and Technology (NIST)
 - NIST 800-82, Industrial Control System (ICS) Security
 - Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
 - Defense-in-Depth
 - Security Zones



NIST

- Department of Homeland Security
 - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
 - National Cybersecurity & Communications Integration Center (NCCIC)
 - Recommended Practices, Secure Network Architecture
 - Defense-in-Depth
 - Security Zones
- Department of Homeland Security
 - Idaho National Lab
 - DHS INL/EXT-06-11478
 - Control Systems Cyber Security: Defense-in-Depth Strategies
 - Defense-in-Depth
 - Security Zones



Established Industrial Security Standards

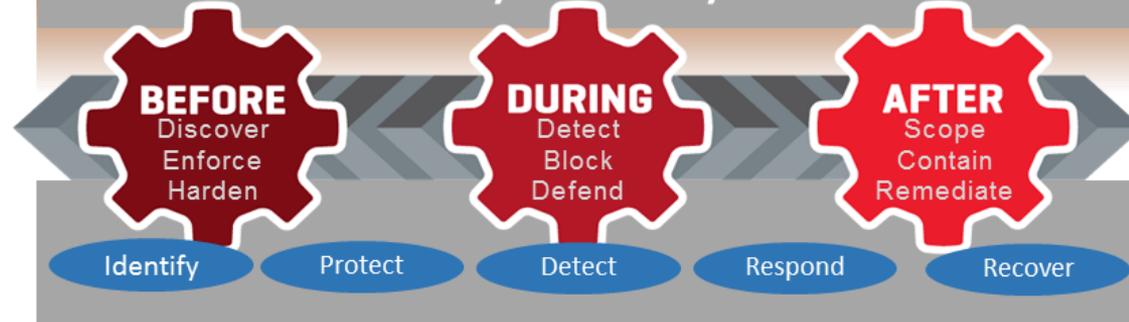
IEC 62443 Industrial Automation and Control System Security

General	Policies & Procedures	System	Component / Product
1-1 Models and concepts	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

IEC 62443

- Series of Standards
- Availability, Integrity, Confidentiality
- Security Zones & Secure Conduits
- Multiple Levels of Foundational Requirements
- Multiple System Security Levels (SL 1 – SL 4)

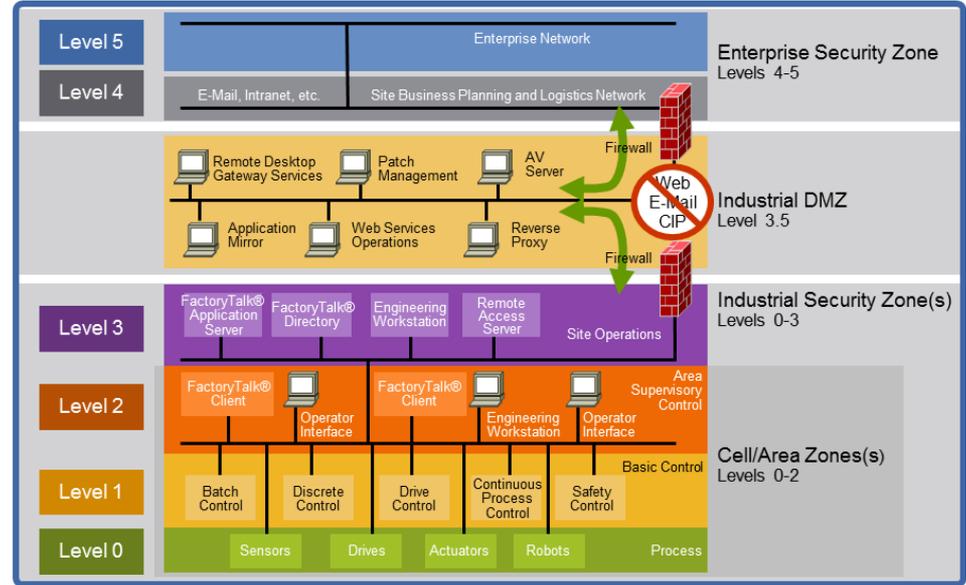
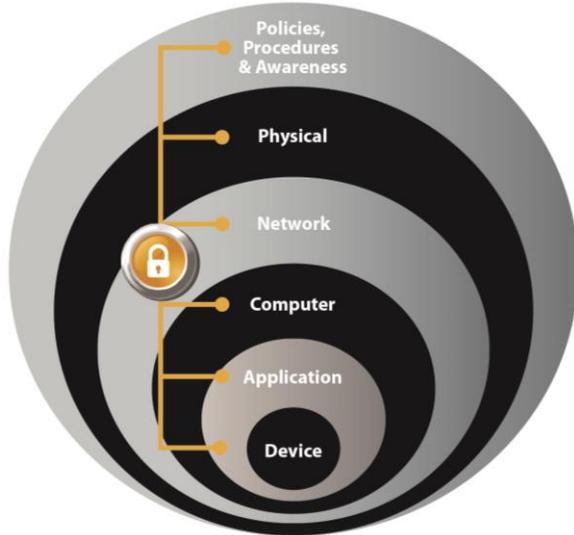
NIST 800-82 Cybersecurity Framework





Holistic and Diverse Plant-wide Security

Holistic and Diverse Plant-wide Security

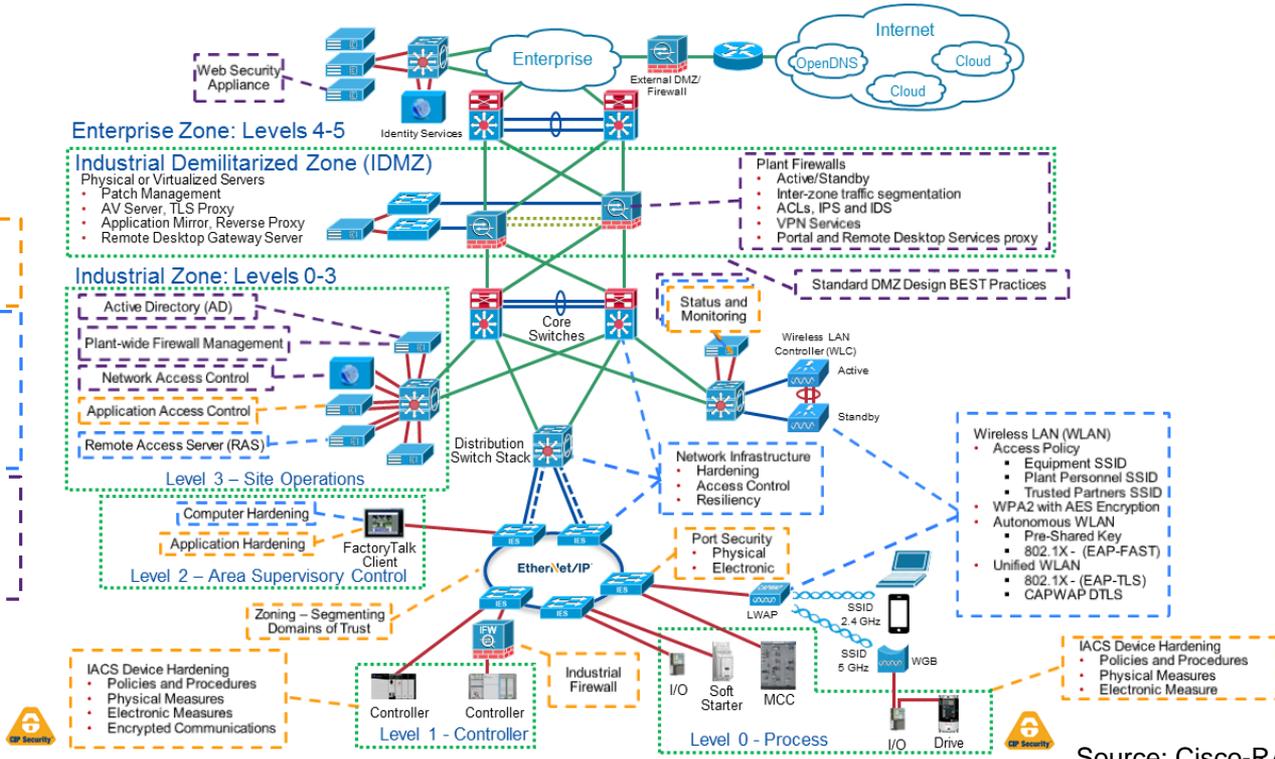


- Levels – ISA 95, Purdue Reference Model
- Zones – IEC 62443, NIST 800-82, DHS/INL/ICS-CERT Recommended Practices

Source: Cisco-RA CPwE

Holistic and Diverse Plant-wide Security

- Personas**
- Control System Engineers (OT)
 - Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
 - IT Security Architects in Collaboration with Control Systems Engineers



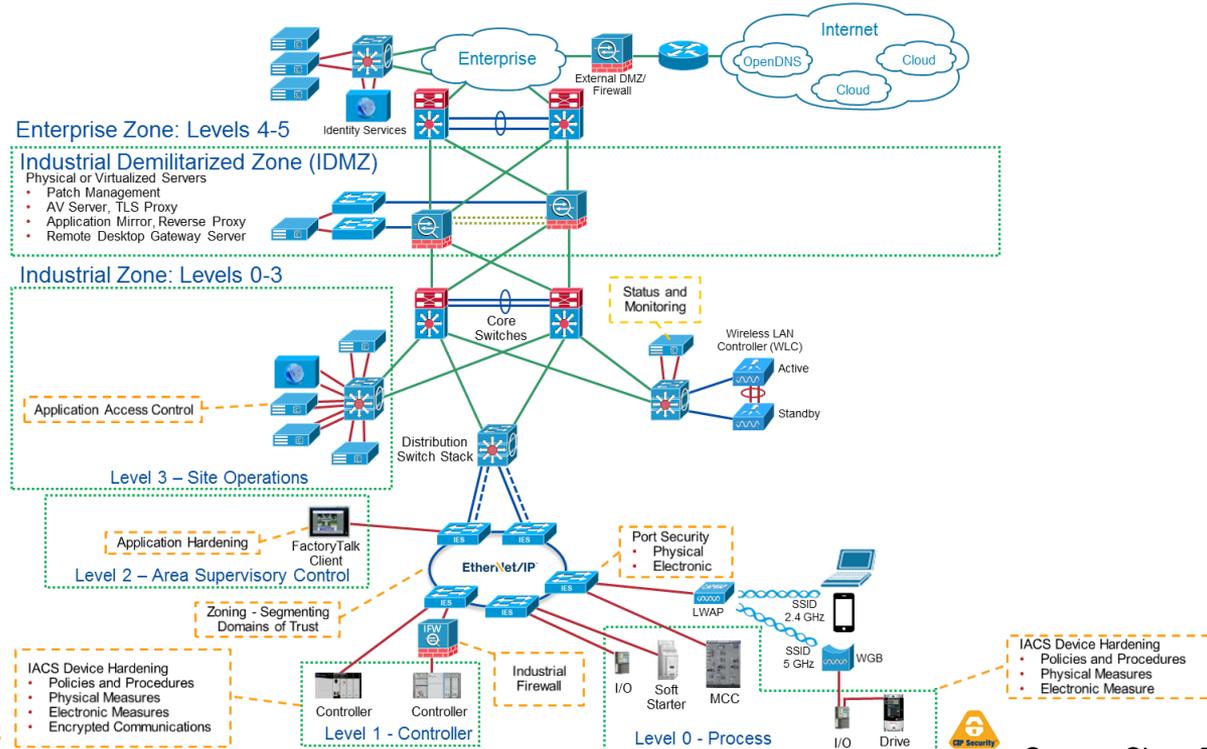
- Defense-in-Depth**
- Architectural Best Practices for Holistic and Diverse Threat Detection and Protection
 - IEC 62443
 - Zones & Conduits
 - Availability, Integrity, Confidentiality
 - NIST 800-82
 - Cybersecurity Framework
 - Identify, Protect, Detect, Respond, Recover
 - DHS/INL/ICS-CERT
 - Recommended Practices

Source: Cisco-RA CPwE

OT Persona - Holistic and Diverse Plant-wide Security

Personas

Control System
Engineers (OT)



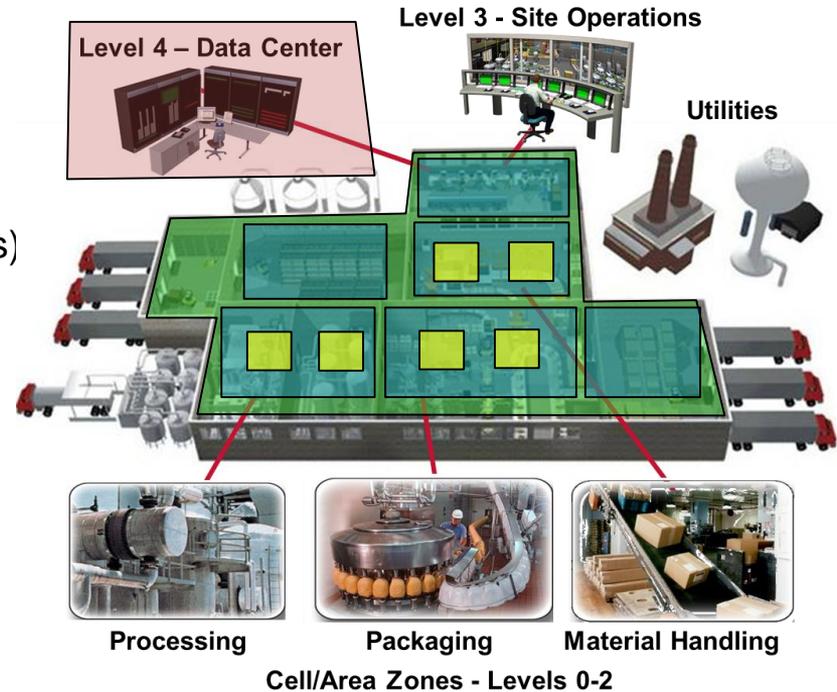
- Defense-in-Depth
- Architectural Best Practices for Holistic and Diverse Threat Detection and Protection
 - IEC 62443
 - Zones & Conduits
 - Availability, Integrity, Confidentiality
 - NIST 800-82
 - Cybersecurity Framework
 - Identify, Protect, Detect, Respond, Recover
 - DHS/INL/ICS-CERT
 - Recommended Practices

Source: Cisco-RA CPwE

OT Persona - Holistic and Diverse Plant-wide Security

Plant-wide Zoning

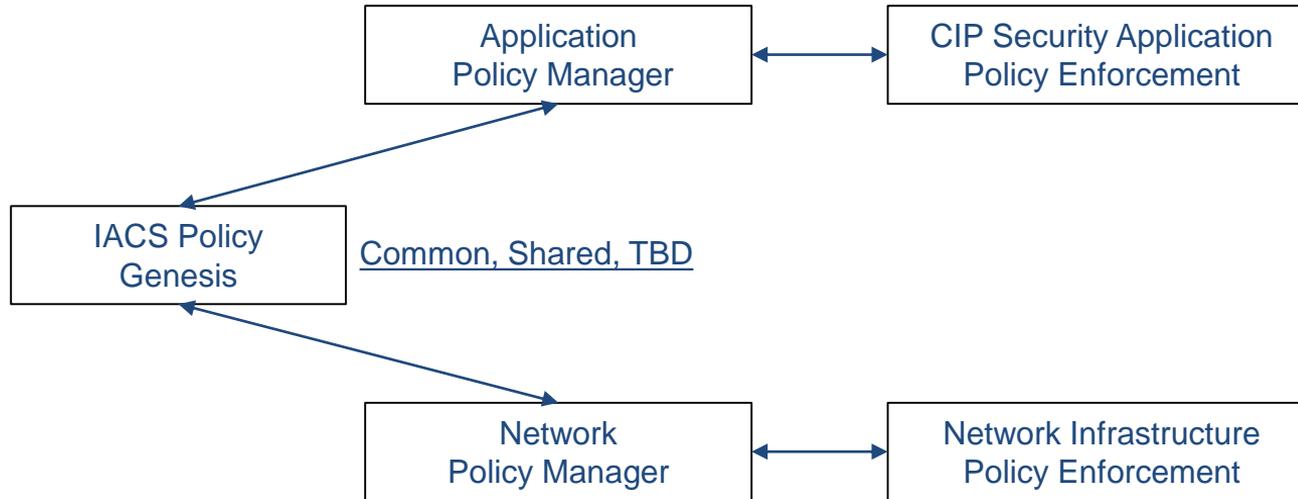
- Functional Areas / Security Groups
- Smaller Connected LANs
 - Smaller Broadcast and Fault Domains
 - Smaller Domains of Trust (Security Groups)
- IACS application micro-segmentation
- Alignment with Security Standards
 - IEC 62443-3-2, Security Zones and Secure Conduits Model
 - DHS/INL/ICS-CERT Recommendations
- Industrial IoT Technology Mix
- Building Block Approach for Future-Ready Scalability



Source: Rockwell Automation

OT Persona - Holistic and Diverse Plant-wide Security

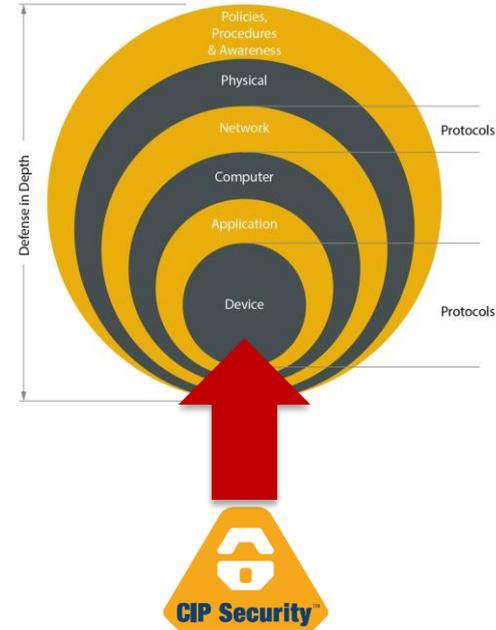
IACS Device Policy Genesis



Source: Rockwell Automation

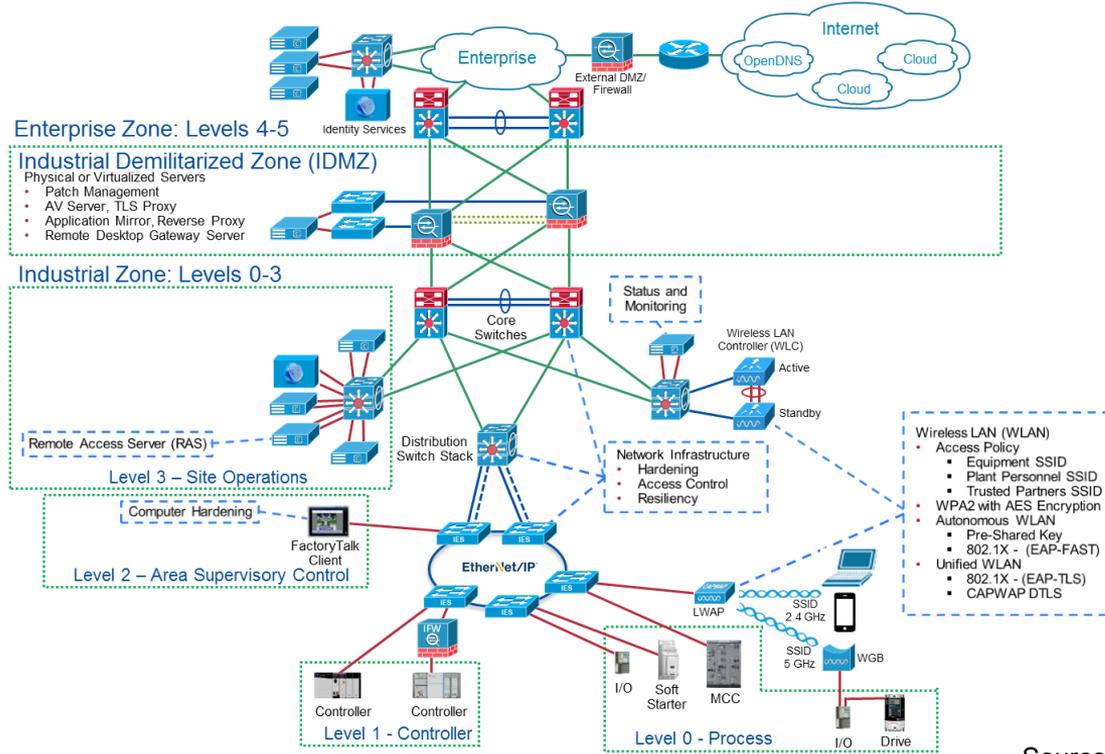
Application / Device Security

- CIP Security™, part of a holistic and diverse defense-in-depth security approach
- Connections between Trusted Endpoints
 - Reject data that has been altered (integrity)
 - Reject messages sent by untrusted people or untrusted devices (authenticity)
 - Reject messages that request actions that are not allowed (authorization)
- Capabilities
 - System management
 - Micro-segmentation
 - Device-based firewall
 - Legacy Device Support – e.g. Whitelisting
- This does not replace the need for network security – e.g. firewalls, segmentation.



OT/IT Persona - Holistic and Diverse Plant-wide Security

Personas
Control System Engineers
in Collaboration with IT
Network Engineers
(Industrial IT)

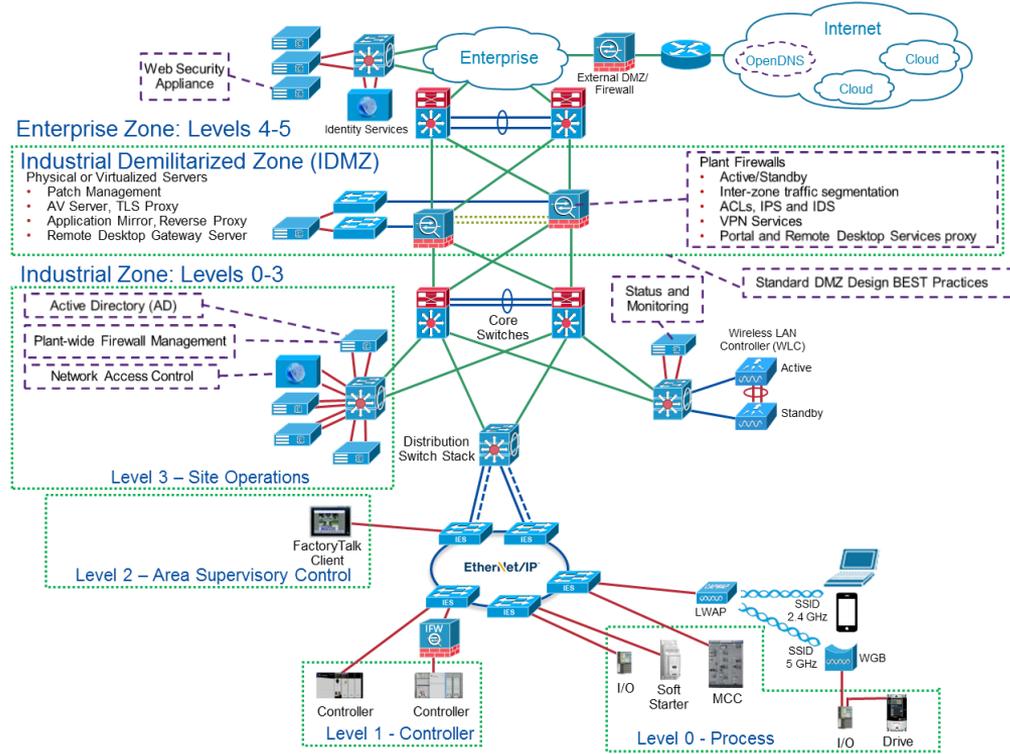


- Defense-in-Depth
- Architectural Best Practices for Holistic and Diverse Threat Detection and Protection
 - IEC 62443
 - Zones & Conduits
 - Availability, Integrity, Confidentiality
 - NIST 800-82
 - Cybersecurity Framework
 - Identify, Protect, Detect, Respond, Recover
 - DHS/INL/ICS-CERT
 - Recommended Practices

Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security

Personas
IT Security Architects in
Collaboration with Control
Systems Engineers



- Defense-in-Depth
- Architectural Best Practices for Holistic and Diverse Threat Detection and Protection
 - IEC 62443
 - Zones & Conduits
 - Availability, Integrity, Confidentiality
 - NIST 800-82
 - Cybersecurity Framework
 - Identify, Protect, Detect, Respond, Recover
 - DHS/INL/ICS-CERT
 - Recommended Practices

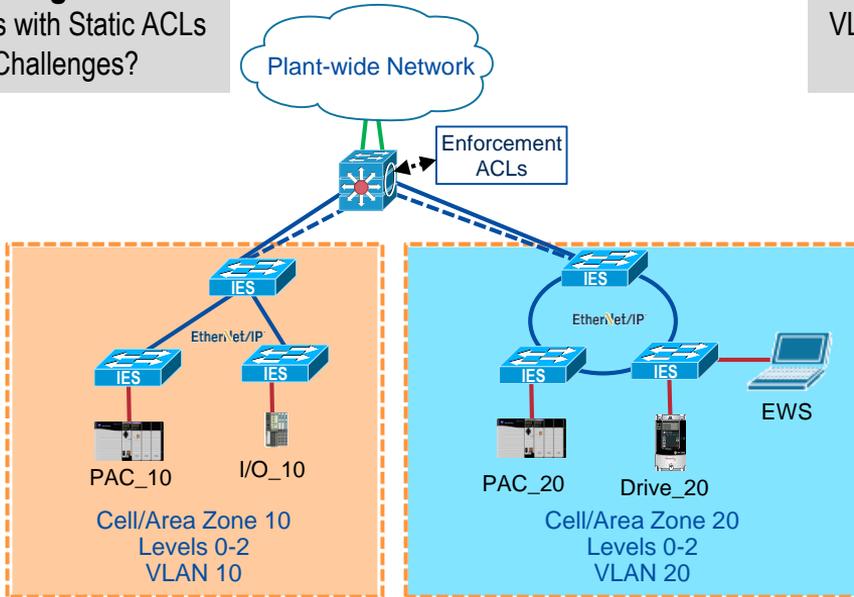
Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Segmentation (Zoning) - Functional Areas / Security Groups

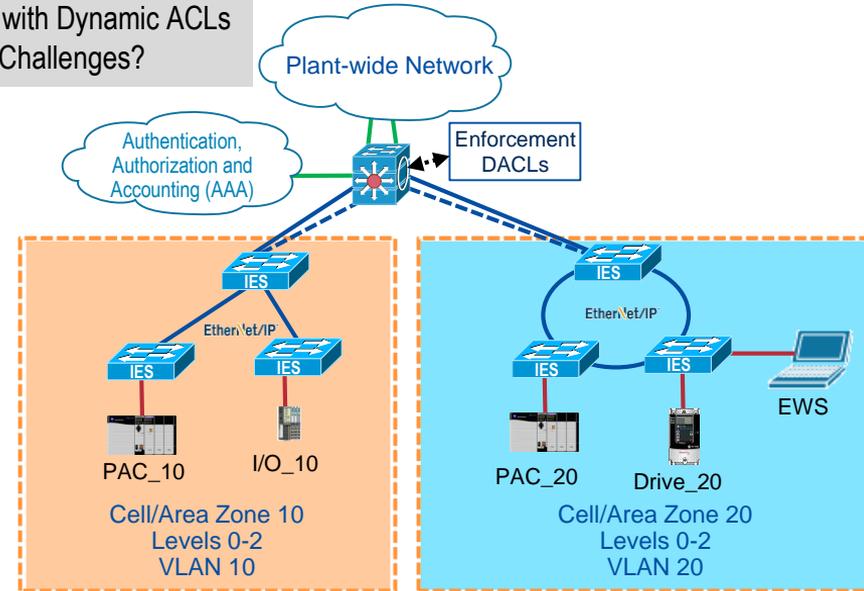
Logical

VLANs with Static ACLs
 Challenges?



Logical

VLANs with Dynamic ACLs
 Challenges?



Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Segmentation (Zoning) - Functional Areas / Security Groups

Assign role-based groups

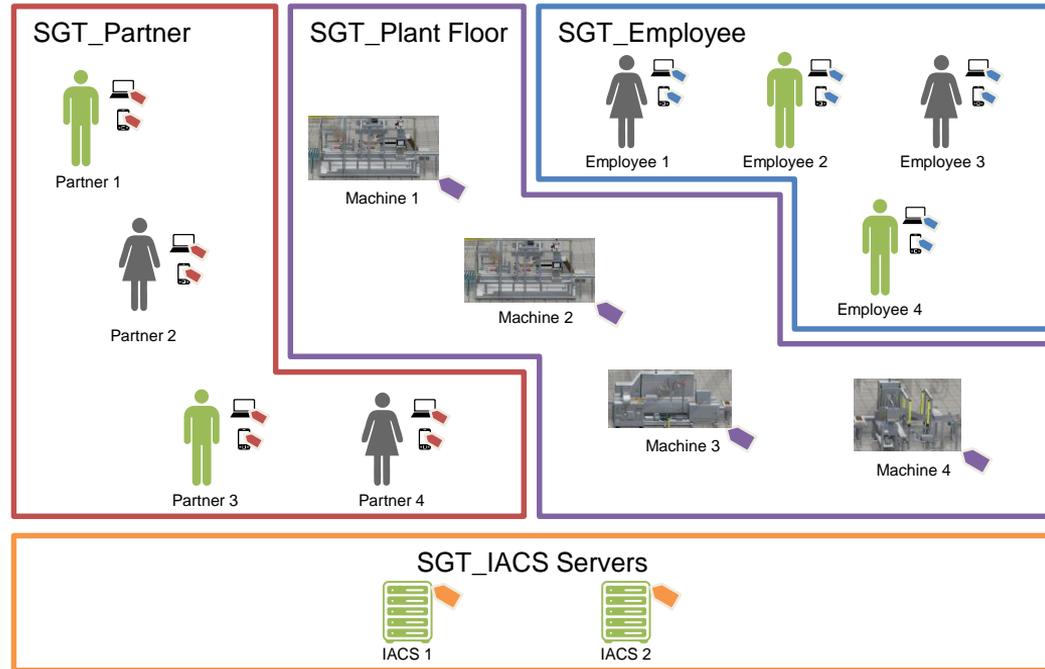
Assign business-based groupings to provide consistent policy and access independent of network topology

Get up and running quickly

Utilize Identity Services and Security Group Tagging (SGT) to support group design

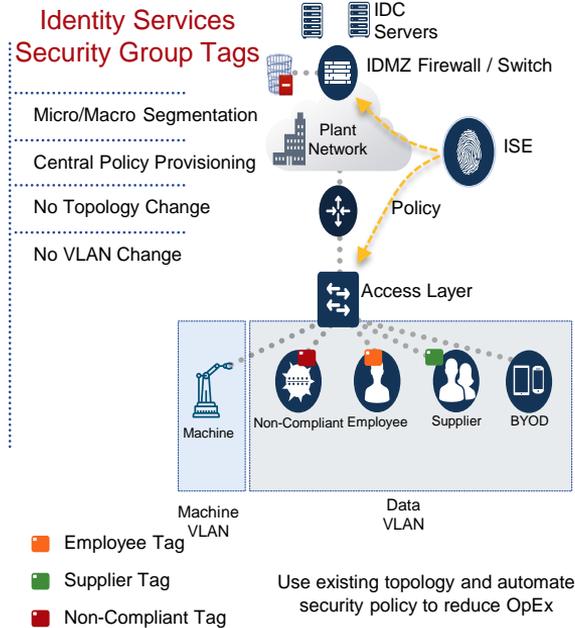
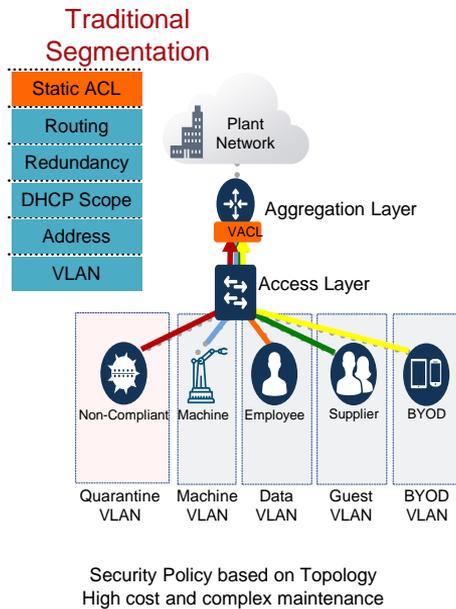
Establish context-aware groups

Leverage attributes such as location and device type to define group assignments



IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Segmentation (Zoning) - Functional Areas / Security Groups



Source: Cisco Systems

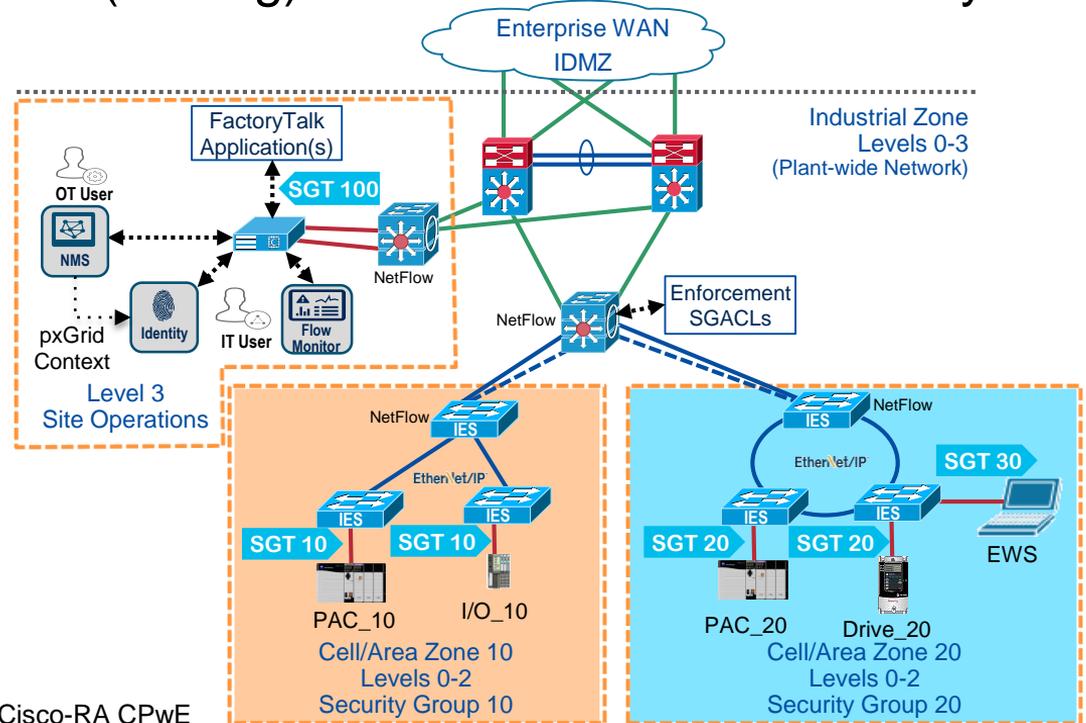
IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Segmentation (Zoning) - Functional Areas / Security Groups

Virtual
Software-Defined
Security Group Segmentation
Challenges?

Sample SGACL Policy Table
Role-based Enforcement

	SGT 100	SGT 30	SGT 10	SGT 20
SGT 100	-	N	Y	Y
SGT 30	N	-	Y	Y
SGT 10	Y	Y	Y	N
SGT 20	Y	Y	N	Y

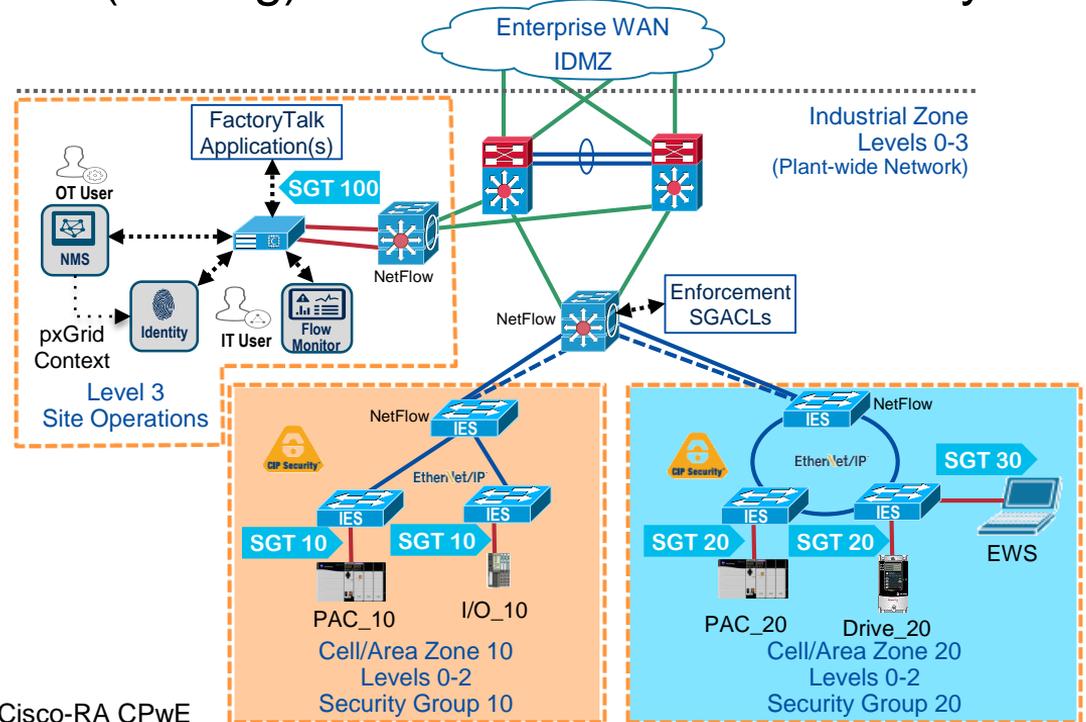
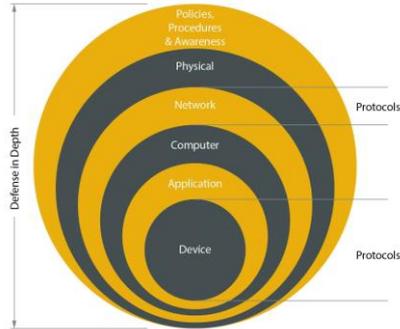


Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Segmentation (Zoning) - Functional Areas / Security Groups

Virtual
Software-Defined
Security Group Segmentation
Challenges?



Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Traffic Flow Analysis

Monitor



- Understand your network normal
- Gain real-time situational awareness of all traffic

Detect



- Leverage Network Behavior Anomaly detection & analytics
- Detect behaviors linked to APTs, insider threats, DDoS, and malware

Analyze



- Collect & Analyze holistic network audit trails
- Achieve faster root cause analysis to conduct thorough forensic investigations

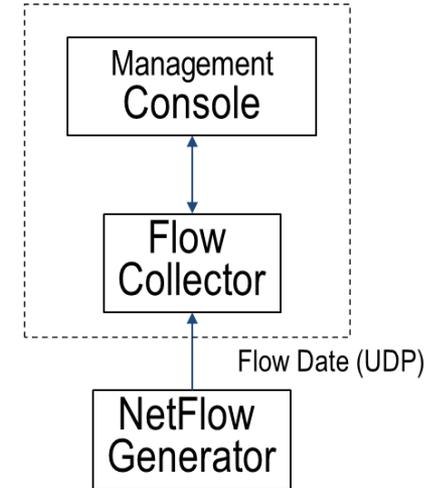
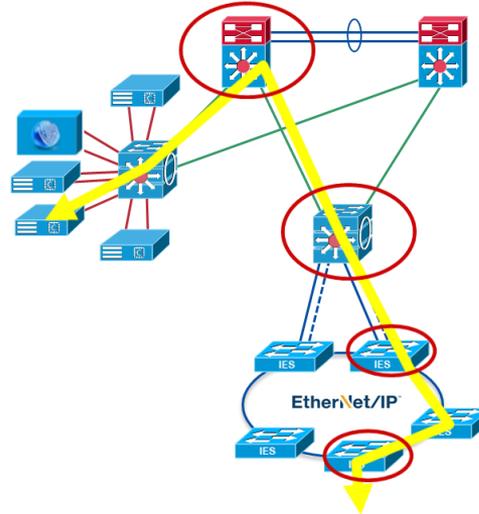
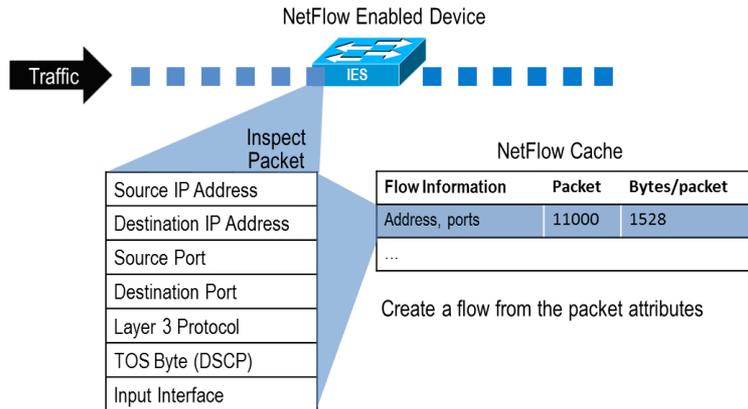
Respond



- Accelerate network troubleshooting & threat mitigation
- Respond quickly to threats by taking action to quarantine through Identity Services

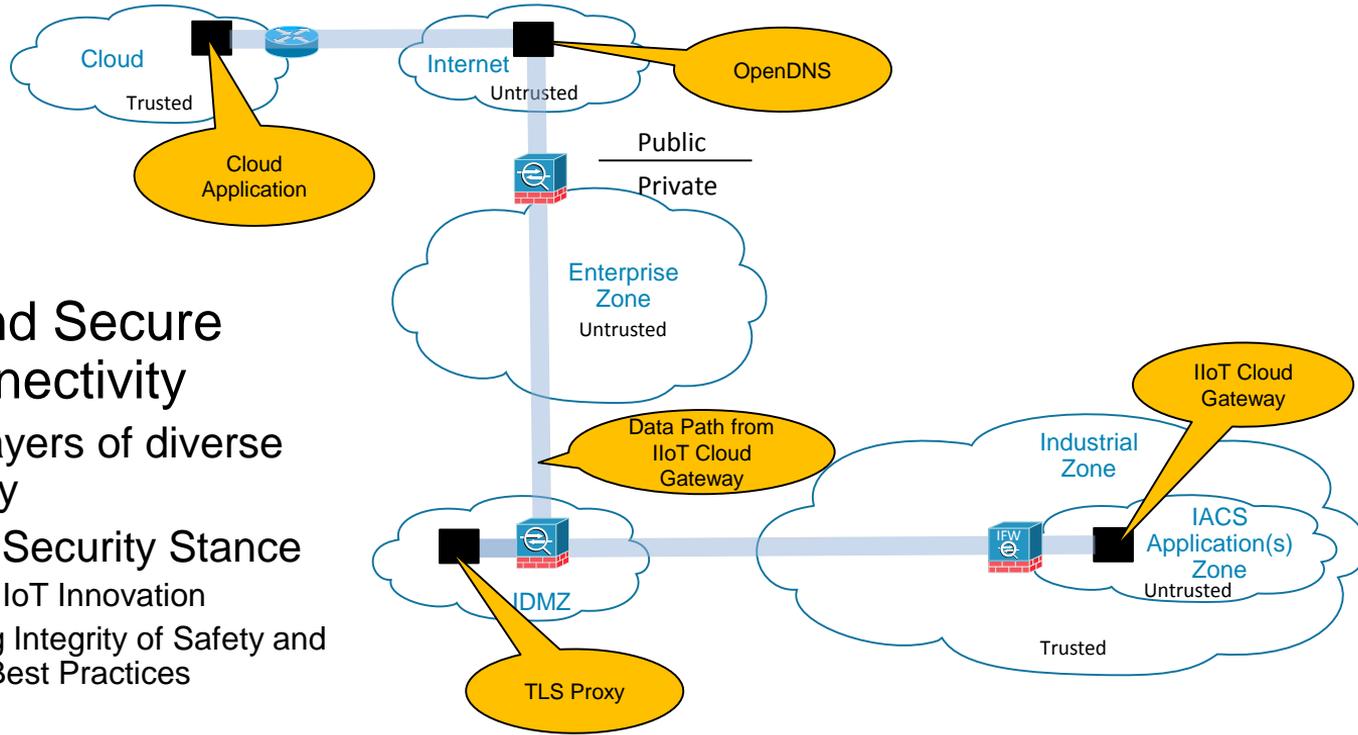
IT Persona - Holistic and Diverse Plant-wide Security

Network Security - Traffic Flow Analysis



Source: Cisco-RA CPwE

IT Persona - Holistic and Diverse Plant-wide Security



Reliable and Secure Cloud Connectivity

- Multiple layers of diverse technology
- Balanced Security Stance
 - Enabling IIoT Innovation
 - Protecting Integrity of Safety and Security Best Practices

Source: Cisco-RA CPWE

IT Persona - Holistic and Diverse Plant-wide Security

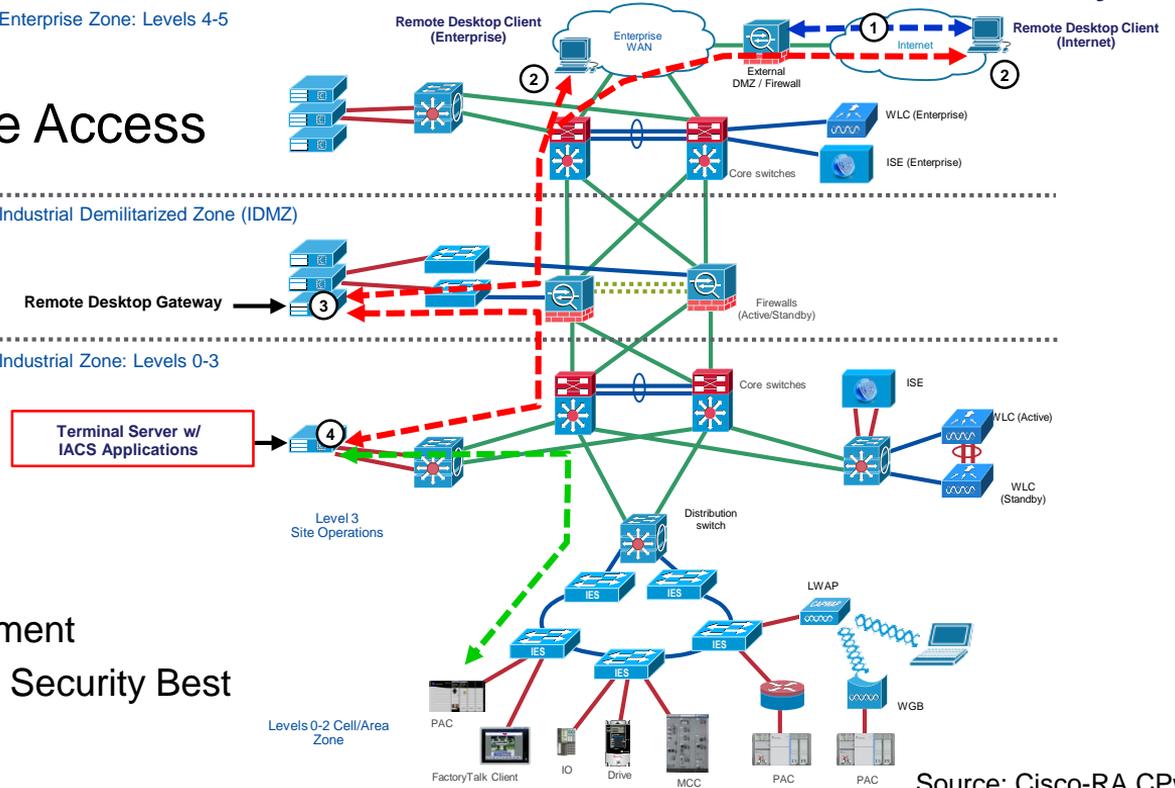
Reliable and Secure Remote Access

- **Balanced Security Stance**
 - Multiple layers of diverse technology
 - Edge firewall with access policies
 - IDMZ best practices
 - Identity services for AAA
 - Remote access server
 - Security zoning
 - Enabling Remote Asset Management
 - Protecting Integrity of Safety and Security Best Practices

Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone: Levels 0-3

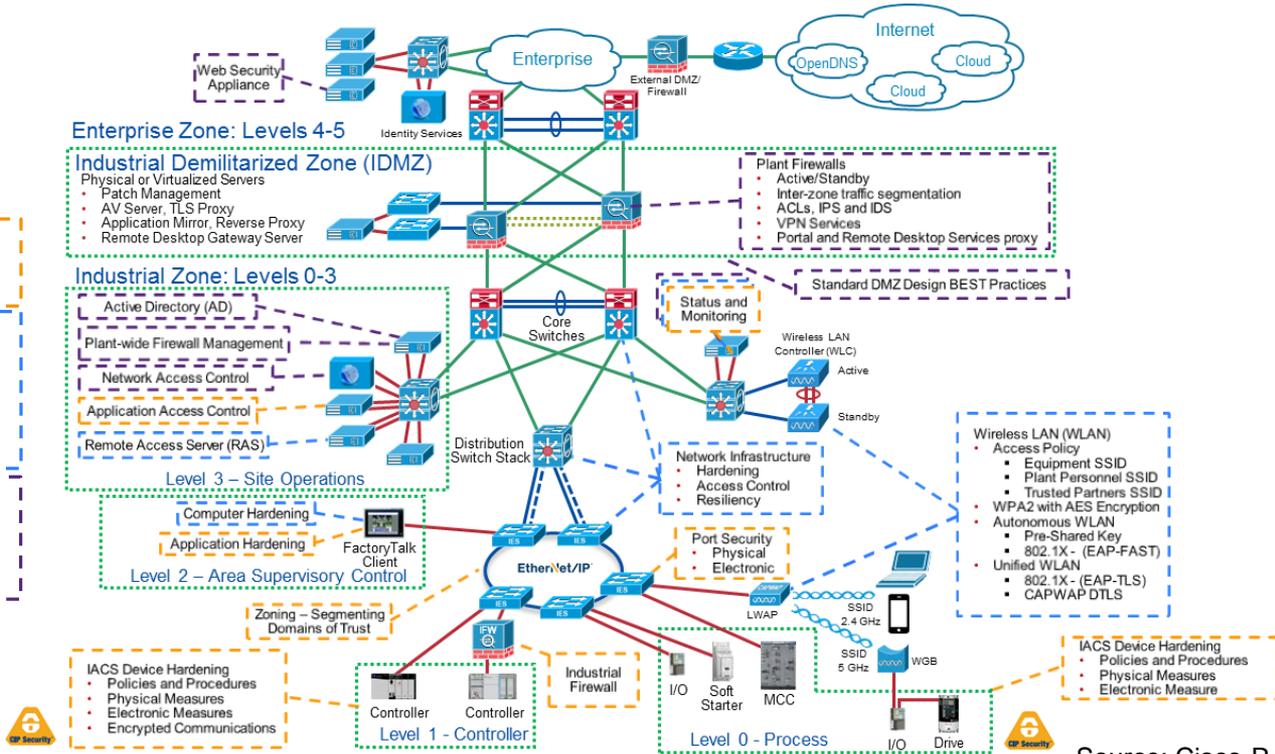


Source: Cisco-RA CPWE

Holistic and Diverse Plant-wide Security

Personas

- Control System Engineers (OT)
- Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
- IT Security Architects in Collaboration with Control Systems Engineers



- Defense-in-Depth**
- Architectural Best Practices for Holistic and Diverse Threat Detection and Protection
 - IEC 62443
 - Zones & Conduits
 - Availability, Integrity, Confidentiality
 - NIST 800-82
 - Cybersecurity Framework
 - Identify, Protect, Detect, Respond, Recover
 - DHS/INL/ICS-CERT
 - Recommended Practices

Source: Cisco-RA CPwE



Key Takeaways

Key Takeaways - ODVA Members

- Develop products that align with Industrial Automation and Control System (IACS) Security Standards and Technologies:
 - IEC 62443
 - Education and awareness for your teams and customers
 - Strategy to address 4-1 and 4-2, where it makes sense for your business
 - CIP Security
 - Harden EtherNet/IP products
 - Adopt CIP Security where it makes sense for your business
 - Conformance testing
 - Participate in PlugFest

Key Takeaways: End Users, System Integrators, OEMs

- Utilize standards, reference models, tested and validated reference architectures (simplified design, quicker deployment, reduced risk in deploying new technology).
- No single product, technology or methodology can fully secure IIoT applications. Protecting IIoT assets requires a holistic security approach to help address different types of internal and external threats. This approach uses multiple layers (administrative, physical, electronic) of diverse technologies for threat protection and detection, applied at different levels of IIoT applications, while being implemented by different personas.
- Although industrial security should be holistic for greenfield IIoT projects, there are many solutions available to help industrial operations incrementally improve the security stance for their legacy IIoT architectures.

Key Takeaways: End Users, System Integrators, OEMs

- Implement risk management policies for availability, safety and security: determination of risk tolerance, performing a risk assessment and implementing risk mitigation solutions.
- Align with Industrial Automation and Control System (IACS) Security Standards.



Recommended Resources

- ODVA
 - [The Common Industrial Protocol \(CIP\) and the Family of CIP Networks](#)
 - [Network Infrastructure for EtherNet/IP: Introduction and Considerations](#)
 - [Media Planning and Installation Manual](#)
 - [Guidelines for Using Device Level Ring \(DLR\) with EtherNet/IP](#)
 - [Securing EtherNet/IP Networks](#)

Recommended Resources

- Converged Plantwide Ethernet (CPwE) Architectures
 - [Cisco](#)
 - [Rockwell Automation](#)
- Education / Awareness
 - Industrial IP Advantage (IIPA) eLearning industrial-ip.org
- Training / Certification
 - Industrial Networking Specialist
 - [IMINS Training, 200-401 Exam](#)
 - CCNA Industrial
 - [IMINS2 Training, 200-601 Exam](#)



THANK YOU