DataTour 2019

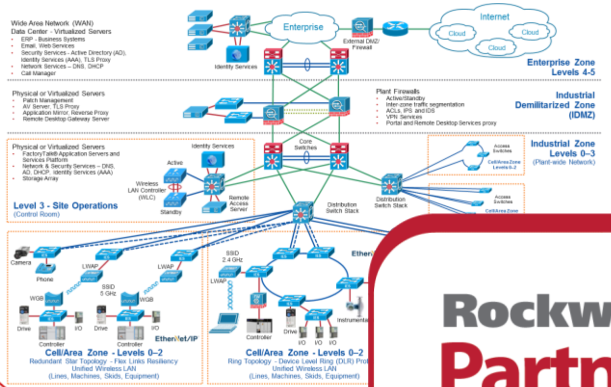
Petr **DRAHOTA**

Konzultant pro návrh strojů

The Connected Enterprise

Optimized fo

Connected Architectures



Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
Storage Array
Identity Services
Core Switches
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Level 3 - Site Operations
(Control Room)
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0-2
Access Switches
Cell/Area Zone
Industrial Zone Levels 0–3
(Plant-wide Network)
Camera
Phone
LWAP
LWAP
SSID 5 GHz
WGB
WGB
Drive
I/O
Drive
I/O
Controller
Controller
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
SSID 2.4 GHz
LWAP
Controller
Drive
I/O
I/O
I/O
Instrumenta
Ethern
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Prot
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Industrial Standards

ISA

IEEE

ODVA

TIA online.org

Rockwell Automation
PartnerNetwork™

SIMPLIFY · COLLABORATE · INNOVATE

ENTERPRISE	Strategic Alliance Partners
SALES AND SOLUTIONS	Distributors • System Integrators • OEMs
PRODUCTS AND TECHNOLOGIES	Encompass™ Referenced Products • Licensed Developers

T

Rockwell Automation

COMMON SECURE NETWORK INFRASTRUCTURE

PANDUIT®

OT

Endress+Hauser EH

rity Threats

Malware DDoS

Spyware

Phishing

Ransomware

Threat Actors

Internal

Hackers

Hacktivist

State

Criminal

Supply Chain

Distribution Center

ckwell Automation

Industrial Application Convergence

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

Information

I/O, Motor Control

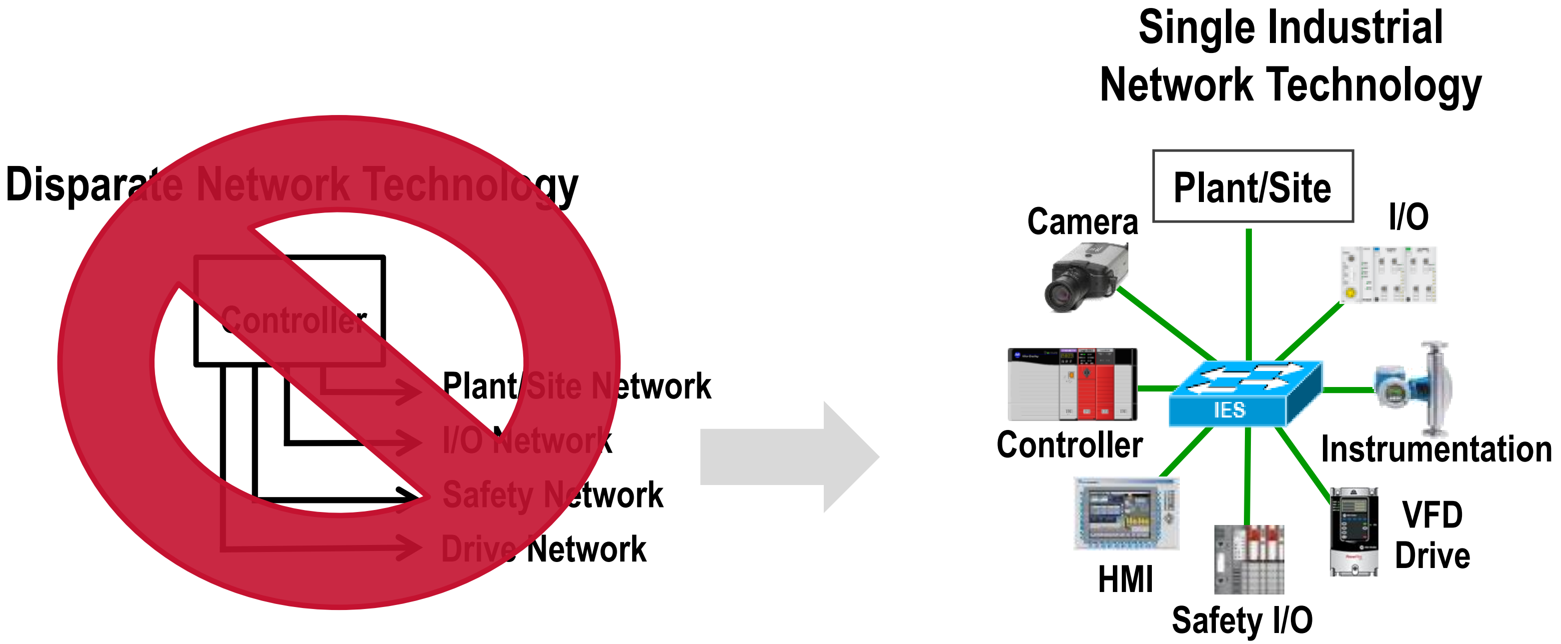
Safety Applications

Process Power Control

High Availability

Energy Management

Multi-discipline Industrial Network Convergence – Industrial Internet of Things



EtherNet/IP™

EtherNet/IP Advantage

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

- Single industrial network technology for:
  - Multi-discipline Network Convergence - Discrete, Continuous Process, Batch, Motor, Safety, Motion, Power, Time Synchronization, Supervisory Information, Asset Configuration/Diagnostics
- Established
  - Risk reduction – broad availability of products, applications and vendor support
  - ODVA: Cisco Systems®, Endress+Hauser, Rockwell Automation® are principal members
  - Supported – Conformance testing, defined QoS priority values for EtherNet/IP devices
- Standard – IEEE 802.3 Ethernet and IETF TCP/IP Protocol Suite
  - Enables convergence of OT and IT – common toolsets (assets for design, deployment and troubleshooting) and skills/training (human assets)
  - Topology and media independence – flexibility and choice
  - Device-level and switch-level topologies; copper - fiber - wireless
- Portability and routability – seamless plant-wide / site-wide information sharing
  - No data mapping – simplifies design, speeds deployment and reduces risk

Single Industrial Network Technology

EtherNet/IP™

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

ISO

Open Systems Interconnection

Industrial Internet of Things (IIoT)

Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	Logical Addressing, Packet Delivery, Routing	IETF IP
Layer 2	Switches IES	Data Link	Framing of Data, Error Checking	IEEE 802.3/802.1/802.11
Layer 1	Cabling/RF	Physical	Signal type to transmit bits, pin-outs, cable type	IEEE : TIA-1005

5-Layer TCP/IP Model

EtherNet/IP Device Selection

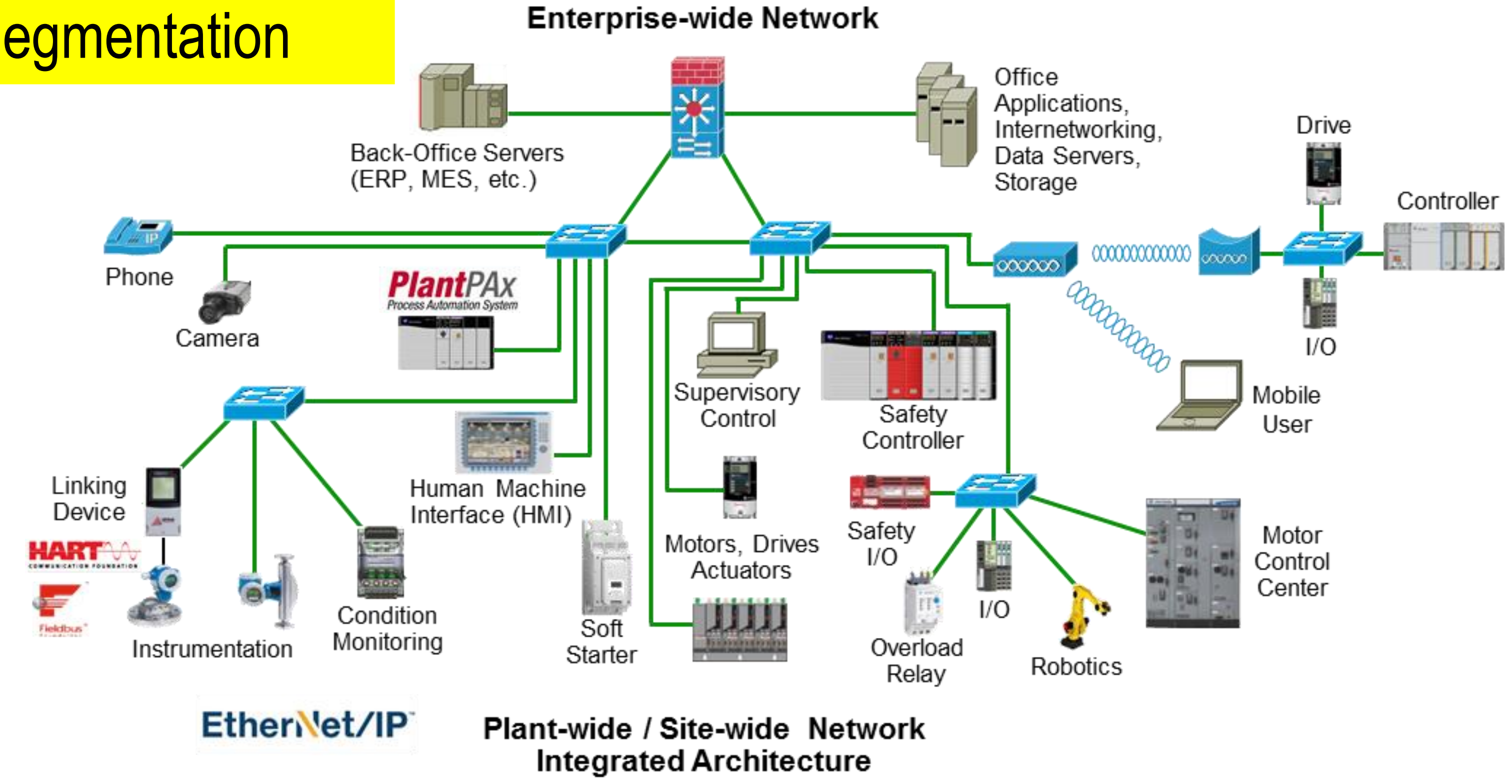
Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

- ODVA
  - Conformance tested,
    with declaration of conformity
  - PlugFest - interoperability testing in a full multi-vendor system configuration
- Selection of Controllers
  - # EtherNet/IP ports, types, topology
  - Environment: on-machine / in-panel
  - Communication speed
  - Maximum # of nodes
  - Minimum requested packet interval (RPI)
  - Maximum I/O data size per RPI
- Selection of Sensor / Actuators
  - Application Requirements
  - Environment: on-machine / in-panel
  - # EtherNet/IP ports, types, topology
  - Communication speed
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Selection Tools
  - Integrated Architecture Builder (IAB)
  - EtherNet/IP Capacity Tool
  - System Configuration Drawings (PCDs)

Industrial IoT (IIoT) – IACS Convergence

Challenges Associated with Technology Convergence

Large LAN, Lacking Natural Boundaries and Segmentation



Flat, Open and Non-Resilient
Industrial Automation and Control System (IACS)
Network Infrastructure

IACS Application Requirements

Challenges Associated with Technology Convergence

What is secure? What is real-time? What is resilient?

	Process Automation	Discrete Automation	Loss Critical
Function	Information Integration, Slower Process Automation	Time-critical Discrete Automation	Multi-axis Motion Control
Communication Technology	.Net, DCOM, TCP/IP	Industrial Protocols - CIP	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	10 ms to 1 second or longer	1 ms to 100 ms	100 µs to 10 ms
Industries	Oil & Gas, chemicals, energy, water	Auto, food and beverage, semiconductor, metals, pharmaceutical	Subset of Discrete automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing

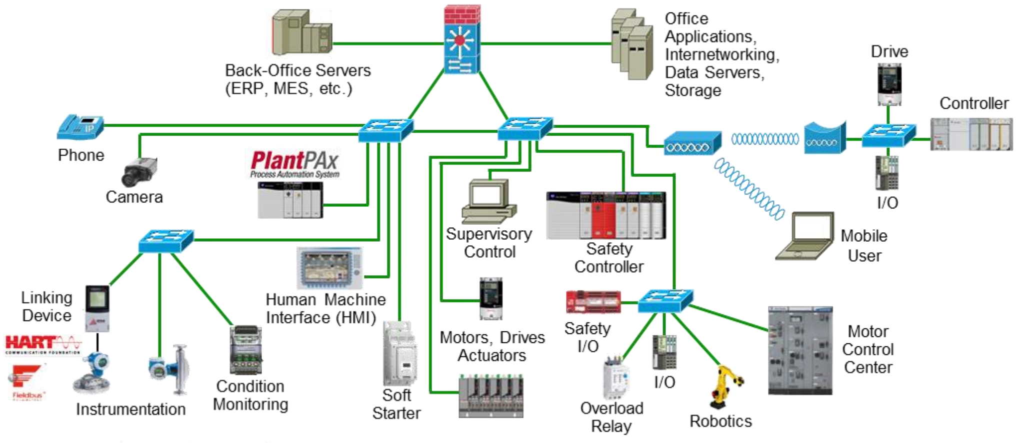
- Only you can define what this means for your application.
- Application dependent.
- One size does not fit all!

Source: ARC Advisory Group

Industrial IoT (IIoT) – IACS Convergence

Challenges Associated with Technology Convergence

Large LAN, Lacking Natural Boundaries and Segmentation

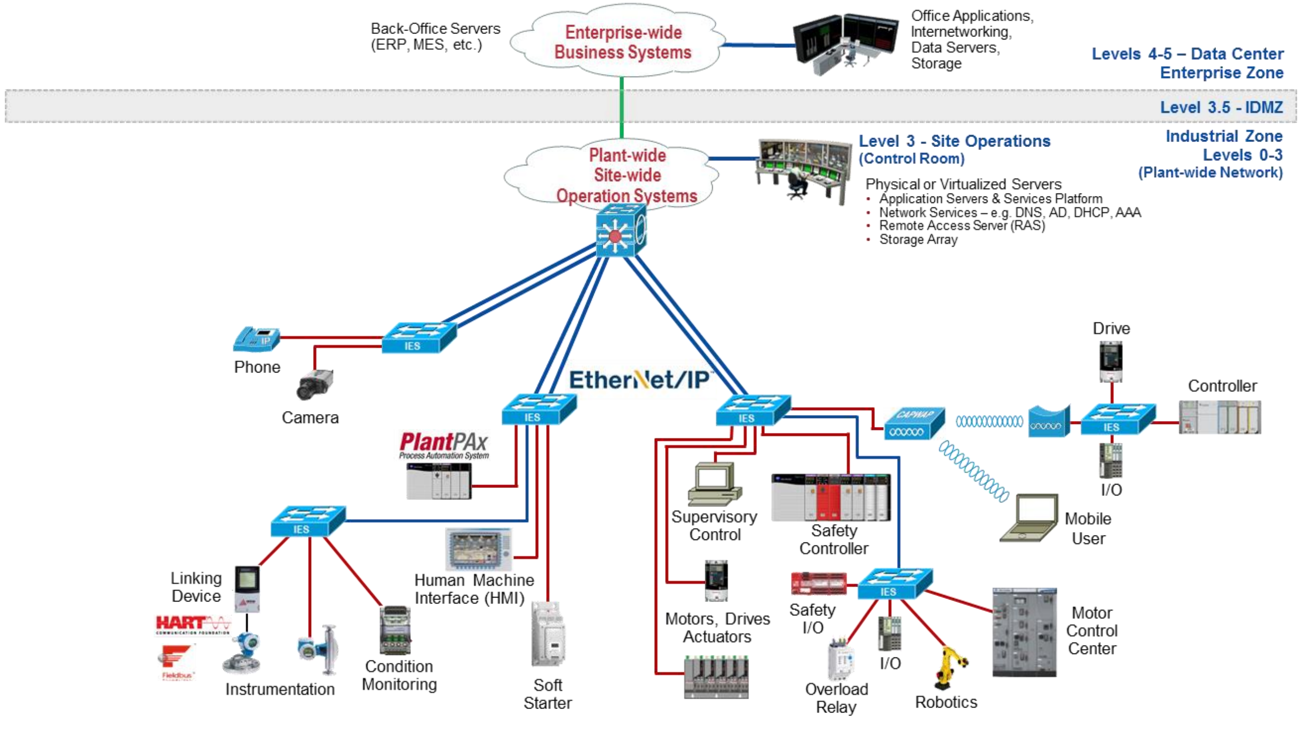


EtherNet/IP

Plant-wide / Site-wide Network
Integrated Architecture

Flat, Open and Non-Resilient IACS Network Infrastructure

Smaller Connected LANs to Create Boundaries and Segmentation



Plant-wide / Site-wide Network
Integrated Architecture – Intelligent Motor Control

Structured and Hardened IACS Network Infrastructure

Cisco and Rockwell Automation®

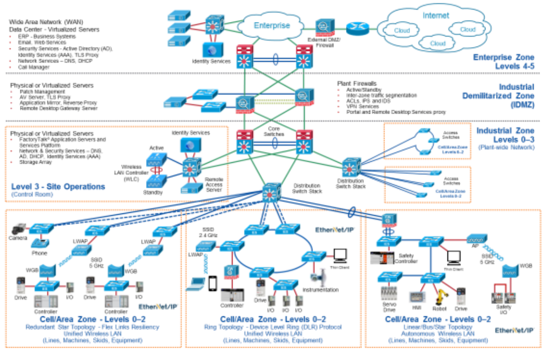
Structured and Hardened Network Infrastructure

Rockwell Automation Strategic Alliance

Plant of the Future - Common Technology View:

A single scalable architecture, using open and standard Ethernet, IP and Wi-Fi networking technologies, enabling the Industrial Internet of Things (IIoT) to help achieve the flexibility, visibility and efficiency required in a competitive manufacturing environment.

EtherNet/IP™ ODVA


Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
Storage Array
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0-2
Access Switches
Cell/Area Zone Levels 0-2
Industrial Zone Levels 0–3 (Plant-wide Network)
Level 3 - Site Operations (Control Room)
Camera
Phone
LWAP
LWAP
SSID 5 GHz
WGB
WGB
Drive
Controller
I/O
Drive
Controller
I/O
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
SSID 2.4 GHz
LWAP
EtherNet/IP
Thin Client
Instrumentation
Controller
Drive
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Safety Controller
Thin Client
AP
SSID 5 GHz
WGB
Servo Drive
HMI
Robot
Drive
Safety I/O
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP

Converged Plantwide Ethernet (CPwE) Architectures:

Collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation. The content of CPwE is relevant to both operational technology (OT) and information technology (IT) disciplines. CPwE consists of documented architectures, best practices, design guidance and configuration settings to help manufacturers with development and deployment of a scalable, reliable, safe, secure and future-ready plant-wide industrial network infrastructure.

Joint Product Collaboration:

Combining the best of Rockwell Automation and Cisco - Stratix® 2500/Stratix 5000/Stratix 8000 families of managed industrial Ethernet switches, Stratix 5950 Security Appliance, and Stratix 5900 Services Router.

Workforce Development - People and Process Optimization:

Education, training, certifications and services to help facilitate OT and IT technology, network and cultural convergence.

CISCO CERTIFIED SPECIALIST

CISCO CERTIFIED CCNA INDUSTRIAL

Industrial IP ADVANTAGE

Cisco live!

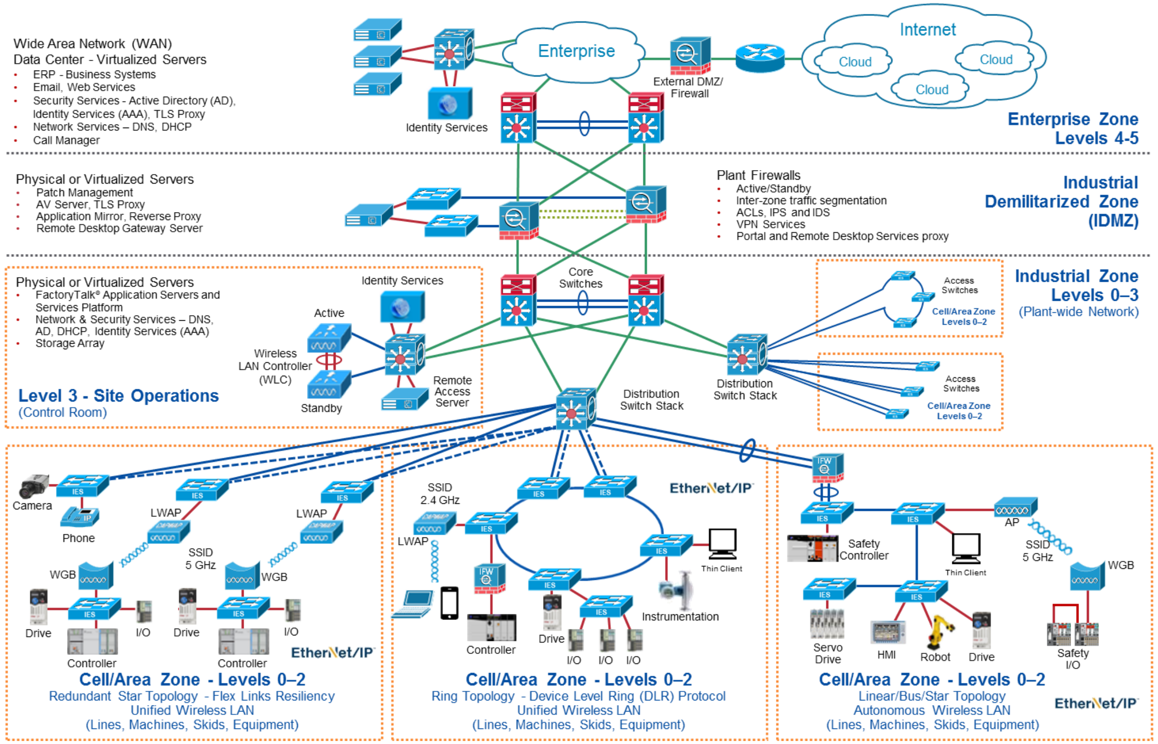
Rockwell Automation TechED Inspire. Educate. Innovate.

Rockwell Automation Automation Fair

Reference Architectures

Structured and Hardened Network Infrastructure

- What are reference architectures?
  - Baseline architectures, considerations and best practices for design and implementation.



Wide Area Network (WAN)
Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager

Enterprise Zone Levels 4-5

Physical or Virtualized Servers
- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Demilitarized Zone (IDMZ)

Physical or Virtualized Servers
- FactoryTalk® Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Level 3 - Site Operations
(Control Room)

Industrial Zone Levels 0–3
(Plant-wide Network)

Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

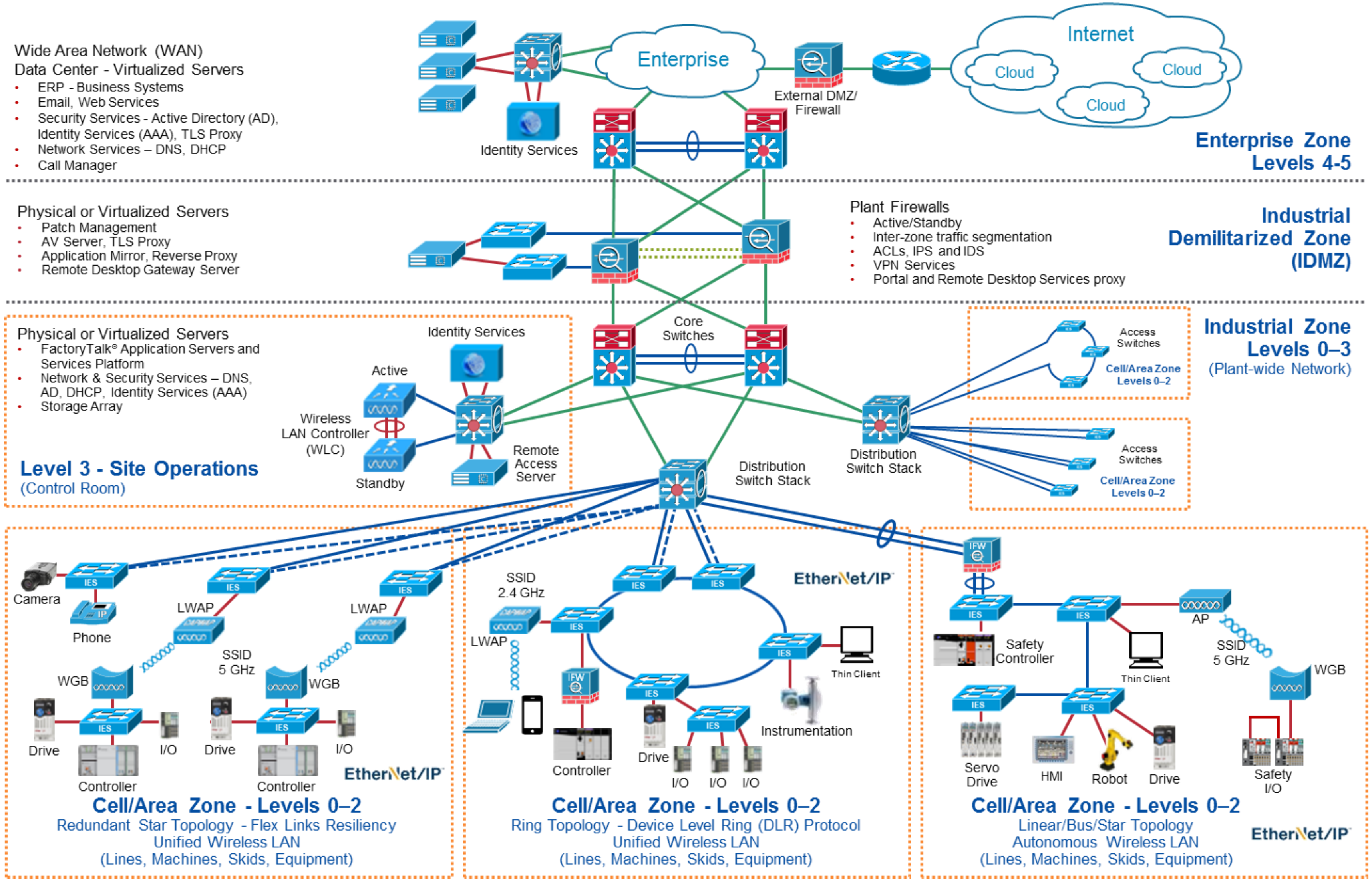
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)

- Reference Architectures:
  - Marketectures – high-level marketing illustrations
  - White papers and knowledgebase articles based on proof of concept (PoC) testing
  - Accelerator Toolkits:
    - Examples - Drives and Motion, Water Wastewater, Safety, Energy Management
  - System Configuration Drawings
    - Examples – Stratix®, MCC, Wi-Fi, ControlLogix®
  - Converged Plantwide Ethernet (CPwE) Architectures:
    - Cisco / Rockwell Automation Strategic Alliance
    - Tested and Validated Architectures
      - Test labs – Cisco, Rockwell Automation and Panduit
    - White papers, design guides, application guides

Reference Architectures

Structured and Hardened Network Infrastructure



Wide Area Network (WAN)
Data Center - Virtualized Servers

- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager

Physical or Virtualized Servers

- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls

- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Physical or Virtualized Servers

- FactoryTalk® Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Single Industrial Network Technology

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

	ISO		Open Systems Interconnection	Industrial Internet of Things (IIoT)
Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	Logical Addressing, Packet Delivery, Routing	IETF IP
Layer 2	Switches IES	Data Link	Framing of Data, Error Checking	IEEE 802.3/802.1/802.11
Layer 1	Cabling/RF	Physical	Signal type to transmit bits, pin-outs, cable type	IEEE : TIA-1005

5-Layer TCP/IP Model

PUBLIC

CPwE Logical Model - Built on Technology and Industry Standards

Logical Zoning (Segmentation)

OT Standards

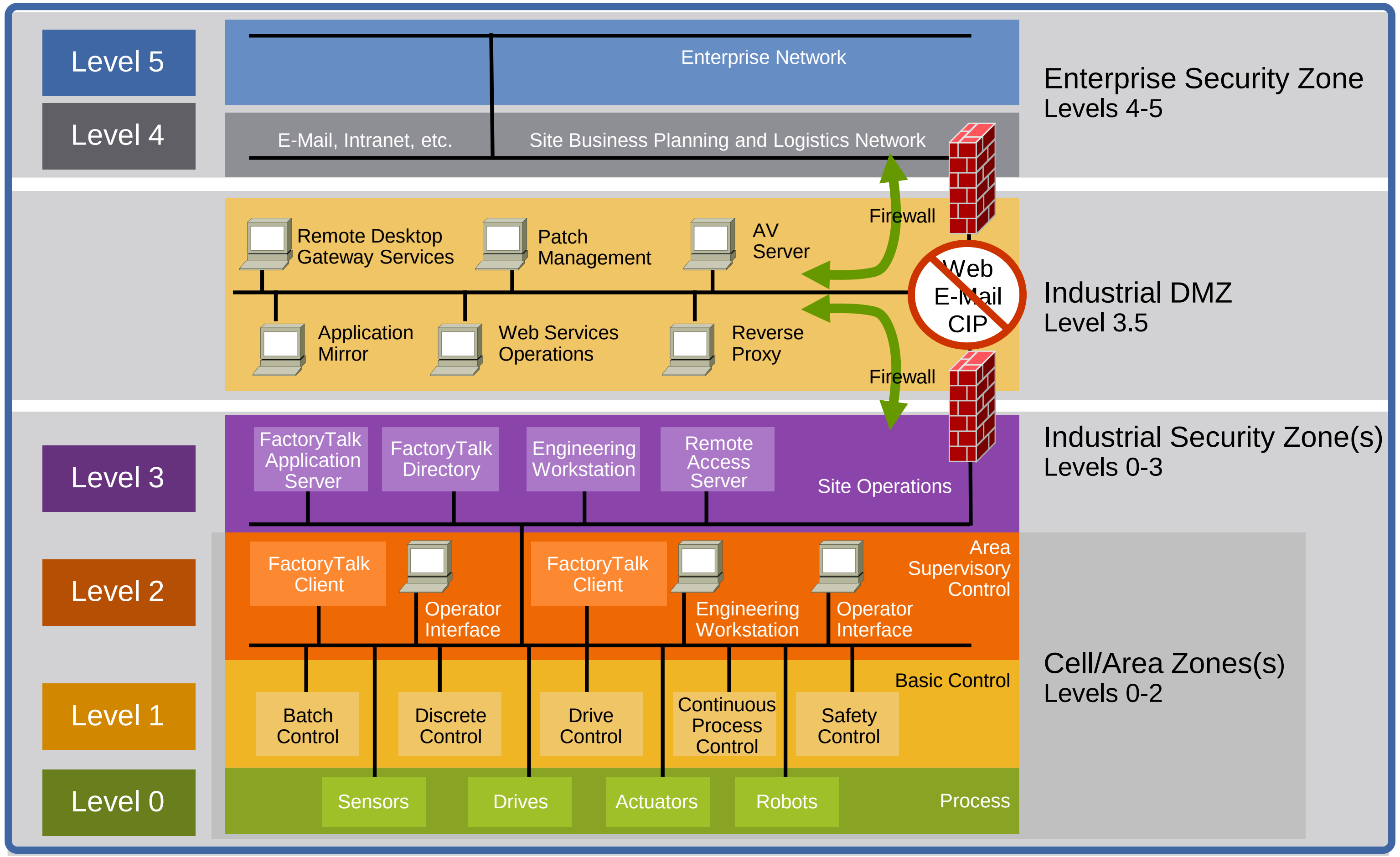
- Operational Levels
  - ISA 95, Purdue – Levels 0-5
    - Level 0 Sensor/Actuators
    - Level 1 Controller
    - Level 2 Local Supervisor
    - Level 3 Site Operations
    - Levels 4-5 Enterprise
- Functional / Security Zones
  - IEC-62443, NIST 800-82, DHS/INL/ICS-CERT
    - Enterprise, Industrial, IDMZ
    - Industrial Subzones – Cell/Area, Site Operations

IT Standards

- Network Technology
  - OSI Reference Model – 7 Layers
  - IEEE 802.1, 802.3, 802.11
  - IETF TCP, UDP, IP
- Network Switch Hierarchy
  - Campus Network Model
    - Layer 2 Access
    - Layer 3 Distribution/Aggregation
    - Layer 3 Core

CPwE Logical Model - Operational Levels - Functional / Security Zones

Logical Zoning (Segmentation)



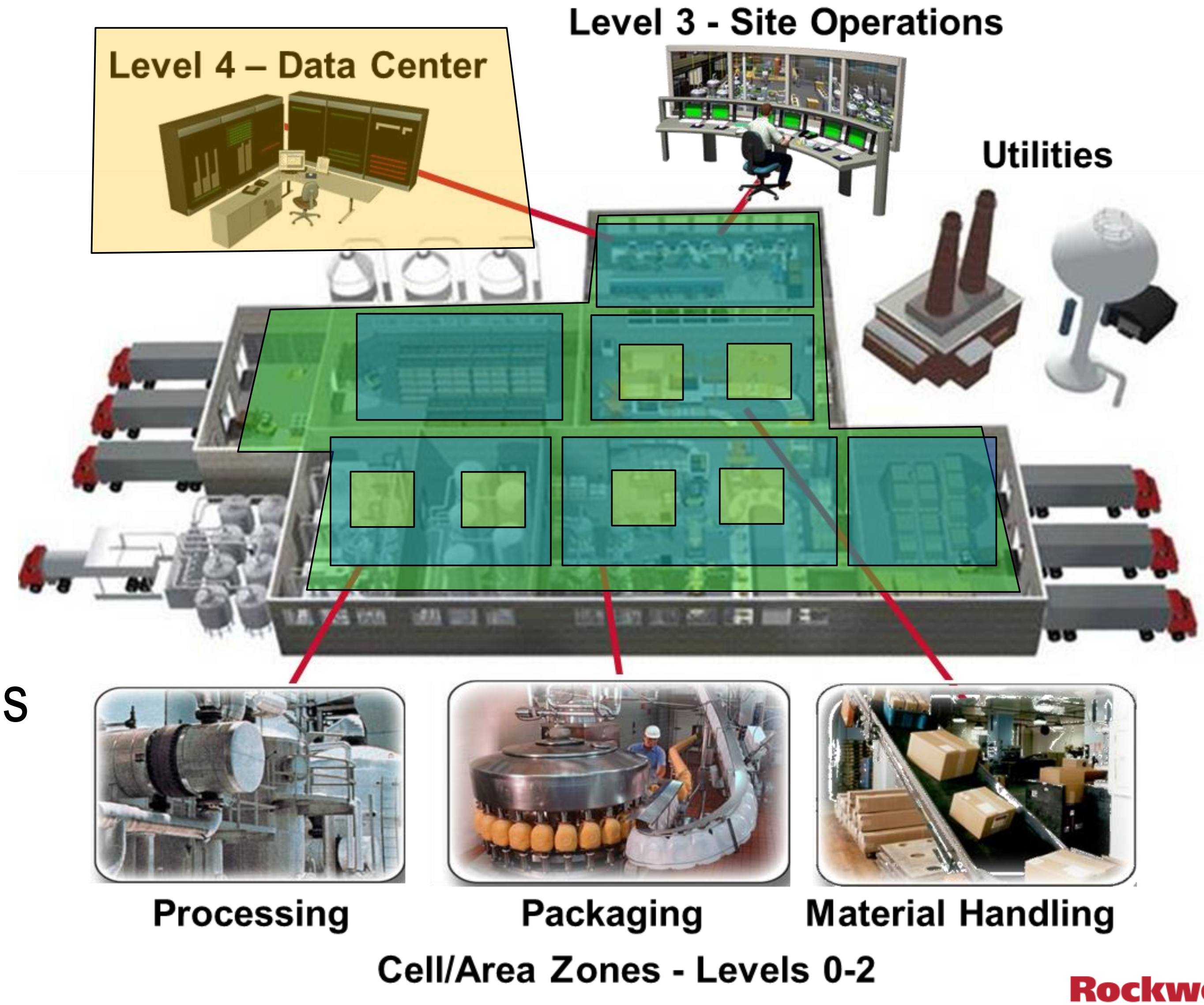
- Levels – ISA 95, Purdue Reference Model
- Zones – IEC 62443, NIST 800-82, DHS/INL/ICS-CERT Recommended Practices

Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)

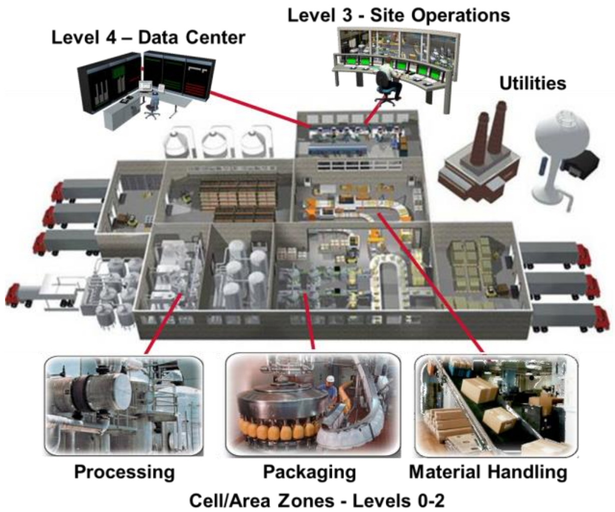
Plant-wide Zoning

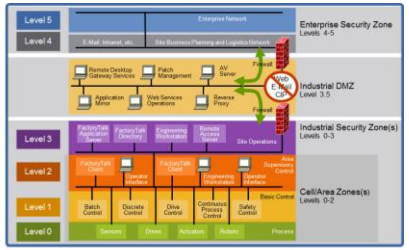
- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- IEC 62443-3-2 Security Zones and Secure Conduits Model
- DHS/INL/ICS-CERT Best Practices
- Industrial IoT Technology
- Building Block Approach for Scalability

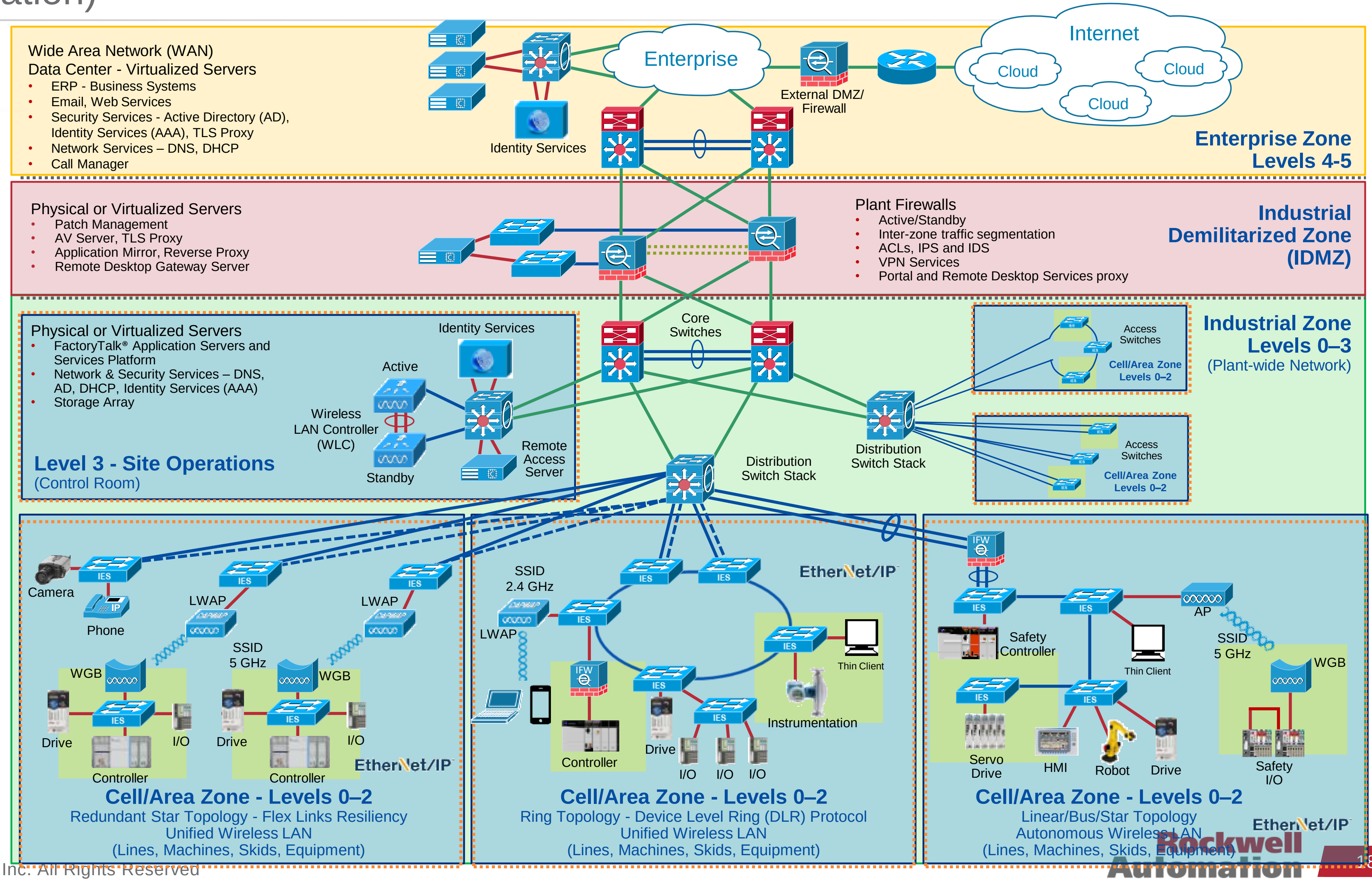


Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)







Wide Area Network (WAN)
Data Center - Virtualized Servers

- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager

Enterprise Zone Levels 4-5

Physical or Virtualized Servers

- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls

- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0–3
(Plant-wide Network)

Physical or Virtualized Servers

- FactoryTalk® Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Level 3 - Site Operations
(Control Room)

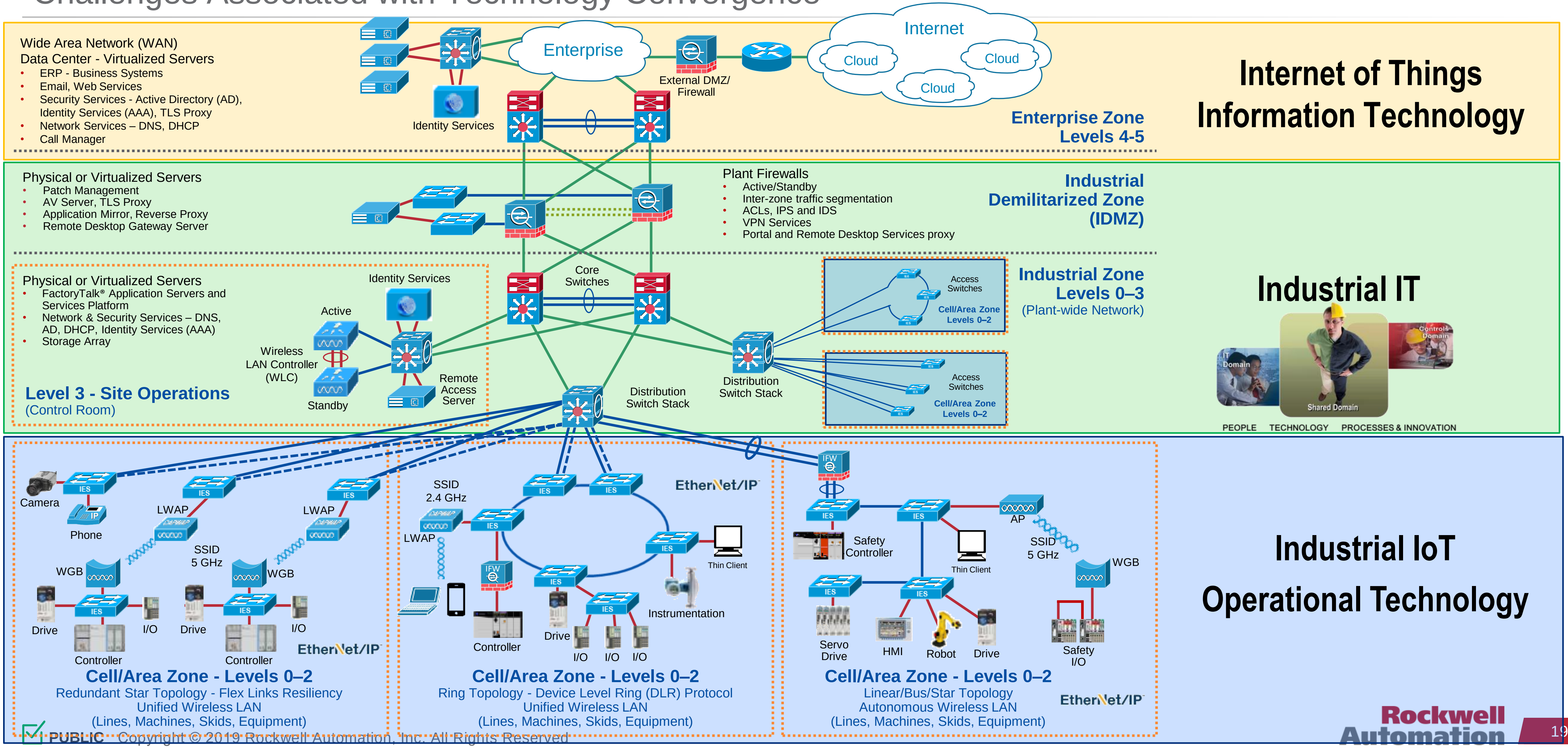
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)

OT-IT Collaboration / Convergence

Challenges Associated with Technology Convergence



Wide Area Network (WAN)
Data Center - Virtualized Servers

- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager

**Enterprise Zone
Levels 4-5**

**Internet of Things
Information Technology**

Physical or Virtualized Servers

- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls

- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Demilitarized Zone (IDMZ)

Physical or Virtualized Servers

- FactoryTalk® Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Level 3 - Site Operations
(Control Room)

**Industrial Zone
Levels 0–3**
(Plant-wide Network)

Industrial IT

**Industrial IoT
Operational Technology**

Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)

Rockwell Automation

Structured and Hardened Network Infrastructure

Zoning (Segmentation)

- Smaller Connected LANs to help:
  - Minimize network sprawl
  - Modular building block approach for scalable, reliable, safe, secure and future-ready network infrastructure
  - Segment Industrial IoT Technologies
  - Smaller Layer 2 broadcast domains
    - Restrict Layer 2 broadcast traffic
    - Smaller fault domains (e.g. Layer 2 loops)
    - Smaller domains of trust (security)

- Multiple techniques to create smaller network building blocks (Layer 2 domains)
  - Logical zoning – geographical and functional organization of IACS devices
  - Multiple network interface cards (NICs) – e.g. CIP bridge
  - Campus network model - multi-tier switch hierarchy – Layer 2 and Layer 3
  - Virtual Local Area Networks (VLANs) with Access Control Lists (ACLs), Firewalls
  - Network Address Translation (NAT)
  - Software-Defined Segmentation via Security Group Tagging (SGT)

OT-IT Collaboration / Convergence

Challenges Associated with Technology Convergence

- Technology Differences
  - Software and hardware toolsets
  - Varying implementations of Layer 2/3 network services may create incompatibilities
    - Availability, Performance, Traffic Types, Security
- Cultural Differences
  - Availability SLA (service level agreement)
    - Minutes/Hours vs. Hours/Days
  - Policies
    - Security – CIA vs. AIC
    - QoS – prioritization of voice and video
    - NAT, Multicast
- Skill-gaps – Workforce Development
  - OT personnel with knowledge of IT skills and requirements
  - IT personnel with knowledge of OT skills and requirements
  - Lack of Industrial IT personnel
- Functional Differences and Incompatibilities between IT:
  - Technologies – e.g. resiliency
  - Products – e.g. QoS policies
  - Applications – e.g. WebEx and Skype
  - Solutions – e.g. network access control

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Environment	• Plant-floor • Control Room • Control Panel, Industrial Distribution Frame (IDF)	• Carpeted Space, Data Center • Data Communication or Wiring Closet, Intermediate Distribution Frame (IDF)
Switches	• Managed and unmanaged • Layer 2 is predominant • DIN rail or panel mount is predominant	• Managed • Layer 2 and Layer 3 • Rack mount
Wireless	• Autonomous (locally managed) – point solutions • Mobile equipment (emerging) and personnel (prevalent)	• Unified (centrally managed) solutions • Mobile personnel – corporate provided or BYOD • Guest access
Computing	• Industrial Hardened Panel Mount Computers and Monitors • Desktop, Notebook • 19" Rack Server • Virtualization - becoming prevalent • Hardening – sporadic patching and white listing	• Desktop, Notebook • Tablets • 19" Rack Server and Blade Server • Unified Computing Systems (UCS) • Virtualization – widespread • Hardening - patching and white listing

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Network Technology	• Standard IEEE 802.3 Ethernet and proprietary (non-standard) versions • Standard IETF Internet Protocol (IPv4) and proprietary (non-standard) alternatives • Sporadic use of standard Layer 2 and Layer 3 network and security services	• Standard IEEE 802.3 Ethernet • Standard IETF Internet Protocol (IPv4 and IPv6) • Pervasive use of standard Layer 2 and Layer 3 network and security services
Network Availability	• Switch-Level and Device-Level topologies • Ring topology is predominant for both, Redundant Star for switch topologies is emerging • Standard IEEE, IEC and vendor specific Layer 2 resiliency protocols	• Switch-Level topologies • Redundant Star topology is predominant • Standard IEEE, IETF, and vendor specific Layer 2 and Layer 3 resiliency protocols
Service Level Agreement (SLA)	• Mean time to recovery (MTTR) - Minutes, Hours	• Mean time to recovery (MTTR) - Hours, Days
IP Addressing	• Mostly Static	• Mostly Dynamic

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Traffic Type	• Primarily local – traffic between local assets • Information, control, safety, motion, time synchronization, energy management • Smaller Ethernet frames for control traffic • Industrial application layer protocols: CIP, Profinet, IEC 61850, Modbus TCP, etc.	• Primarily non-local – traffic to remote assets • Voice, Video, Data • Larger IP packets and Ethernet frames • Standard application layer protocols: HTTP, SNMP, DNS, RTP, SSH, etc.
Performance	• Low Latency, Low Jitter (1 ms, 100s ns) • Data Prioritization – QoS – Layer 2 and 3	• Low Latency, Low Jitter (100s ms, 10s ms) • Data Prioritization – QoS – Layer 3
Security	• Open by default, must secure by design, architecture and configuration • Industrial security standards – e.g. IEC, NIST • Inconsistent deployment of security policies • No line-of-sight to the Enterprise or to the Internet	• Pervasive • Enterprise security best practices • Strong security policies • Line-of-sight across the Enterprise and to the Internet

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Focus	24/7 operations, high OEE	Protecting intellectual property and company assets
Precedence of Priorities	Availability Integrity Confidentiality	Confidentiality Integrity Availability
Types of Data Traffic	Converged network of data, control, information, safety and motion	Converged network of data, voice and video
Access Control	Strict physical access Simple network device access	Strict network authentication and access policies
Implications of a Device Failure	Production is down ($$'s/hour … or worse)	Work-around or wait
Threat Protection	Isolate threat but keep operating	Shut down access to detected threat
Upgrades	Scheduled during downtime	Automatically pushed during uptime

Single Industrial Network Technology

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

EtherNet/IP™

Open Systems Interconnection

What makes EtherNet/IP industrial?

Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	Logical Addressing, Packet Delivery, Routing	IETF IP
Layer 2	Switches	Data Link	Framing of Data, Error Checking	IEEE 802.3/802.1/802.11
Layer 1	Cabling/RF	Physical	Signal type to transmit bits, pin-outs, cable type	IEEE : TIA-1005

Physical Layer Hardening

Infrastructure Device Hardening

Common Application Layer Protocol

PUBLIC

Rockwell Automation

Security-enabling The Connected Enterprise

Faster Time to Market

Lower Total Cost of Ownership

Improved Asset Utilization

Enterprise Risk Management

1. **Faster time to market –** Security and safety for On-Machine™, centralized, and distributed applications. All applications are developed using a common integrated design environment.

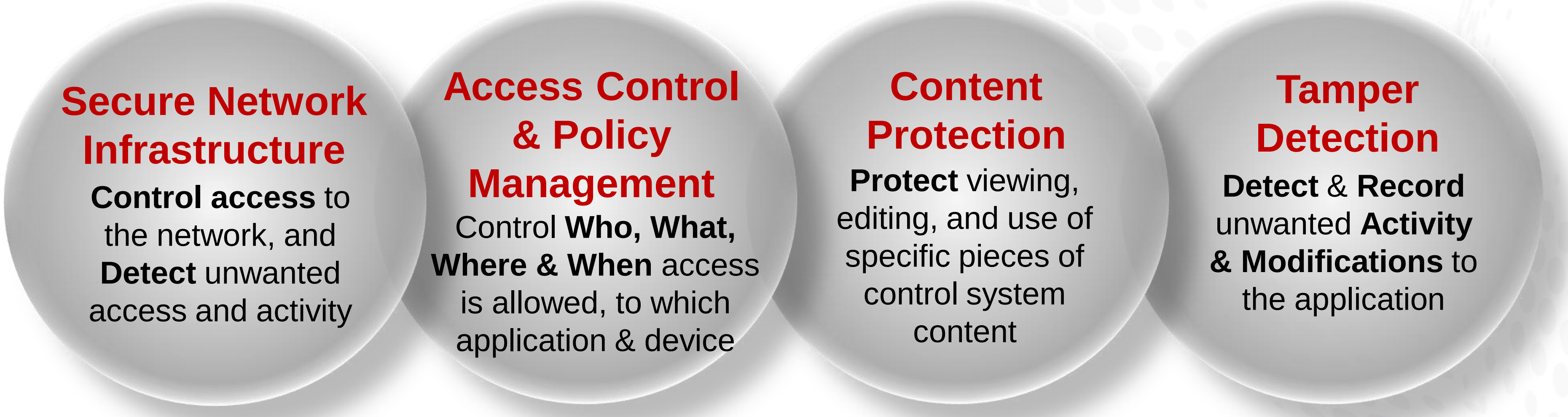
2. **Lower total cost of ownership –** “Security built-in” & enterprise integration. Integrating security capabilities into the products provides customer value through architecture consolidation and simplification.

3. **Improved asset utilization –** Security incidents can impact the availability of machines and systems for weeks, even months. Security systems should enable strong prevention, accurate detection, and quick mitigation of events.

4. **Enterprise risk management –** Intellectual property, compliance, brand/product integrity, and the protection of people, processes, and machines are all at risk without a holistic, defense-in-depth approach to security.

Secure automation & information

Defending the digital architecture



Secure Network Infrastructure

Control access to the network, and **Detect** unwanted access and activity

Access Control & Policy Management

Control **Who, What, Where & When** access is allowed, to which application & device

Content Protection

Protect viewing, editing, and use of specific pieces of control system content

Tamper Detection

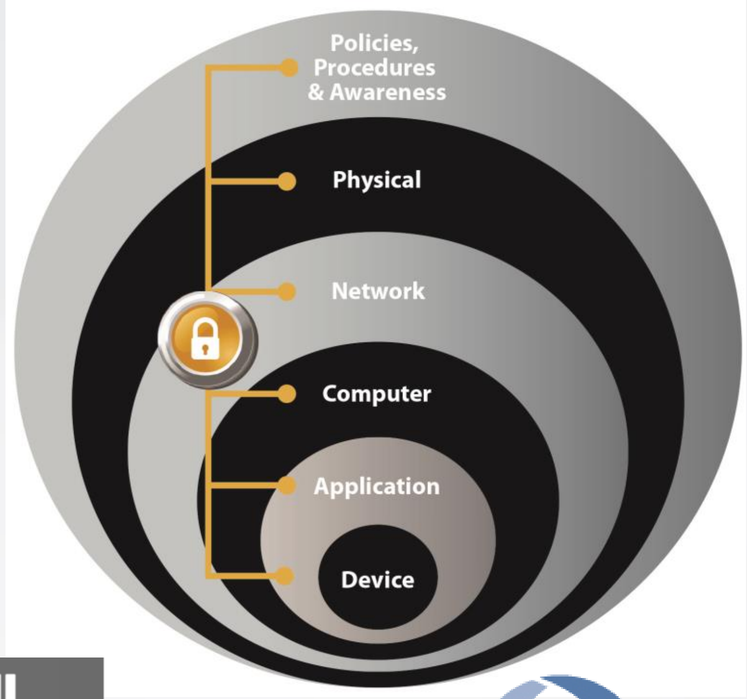
Detect & **Record** unwanted **Activity & Modifications** to the application

INDUSTRIAL SECURITY

MUST BE IMPLEMENTED **AS A SYSTEM**

Holistic approach

A secure application depends on multiple layers of protection and industrial security must be implemented as a system.



CPNI Centre for the Protection of National Infrastructure

U.S. Department of Homeland Security

ISA

NIST

IEC

Defense in depth

Shield targets behind multiple levels of security countermeasures to reduce risk

Openness

Consideration for participation of a variety of vendors in our security solutions

Flexibility

Able to accommodate a customer’s needs, including policies & procedures

Consistency

Solutions that align with Government directives and Standards Bodies

ICS-Focused Campaigns

2010

STUXNET
Worm Targeting SCADA and Modifying PLCs

OPERATION AURORA
APT Cyber Attack on 20+ High Tech, Security & Defense Companies

2011

NIGHT DRAGON
Advanced Persistent Threat Targeting Global Energy

DUQU
Worm Targeting ICS Information Gathering and Stealing

2012

SHAMOON
Virus Targeting Energy Sector Largest Wipe Attack

FLAME
Virus use for Targeted Cyber Espionage in the Middle East

GAUSS
Information Stealer Malware

2013

RED OCTOBER
Cyber-Espionage Malware Targeting Gov't & Research Organizations

2014

HAVEX
Industrial Control System Remote Access Trojan & Information Stealer

HEARTBLEED
Security anomaly and Vulnerability Exploited by Attackers

2015

BLACKENERGY
Malware Injected into Ukrainian Power Company Network, Cut Power to the Affected Region.

2016

BLACKENERGY
Malware Injected into Power Company Network, Attackers Cut Power to the Affected Region.

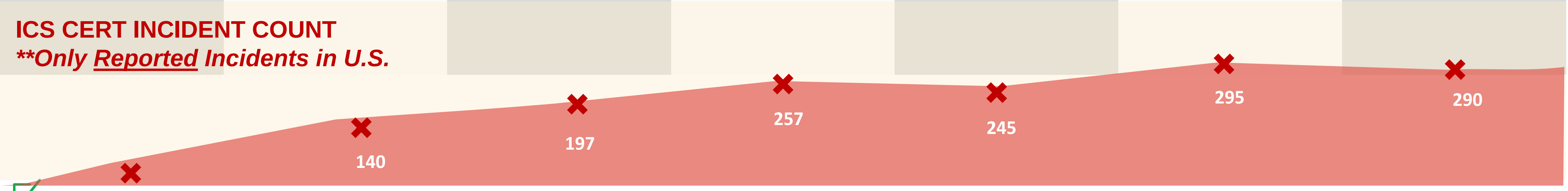
OP GHOUL
Spear-phishing Campaign Targeting Middle East Industrial Organizations

2017

NOTPETYA
Ransomware Malware Based On Stolen NSA Exploits that Impacted ICS Systems

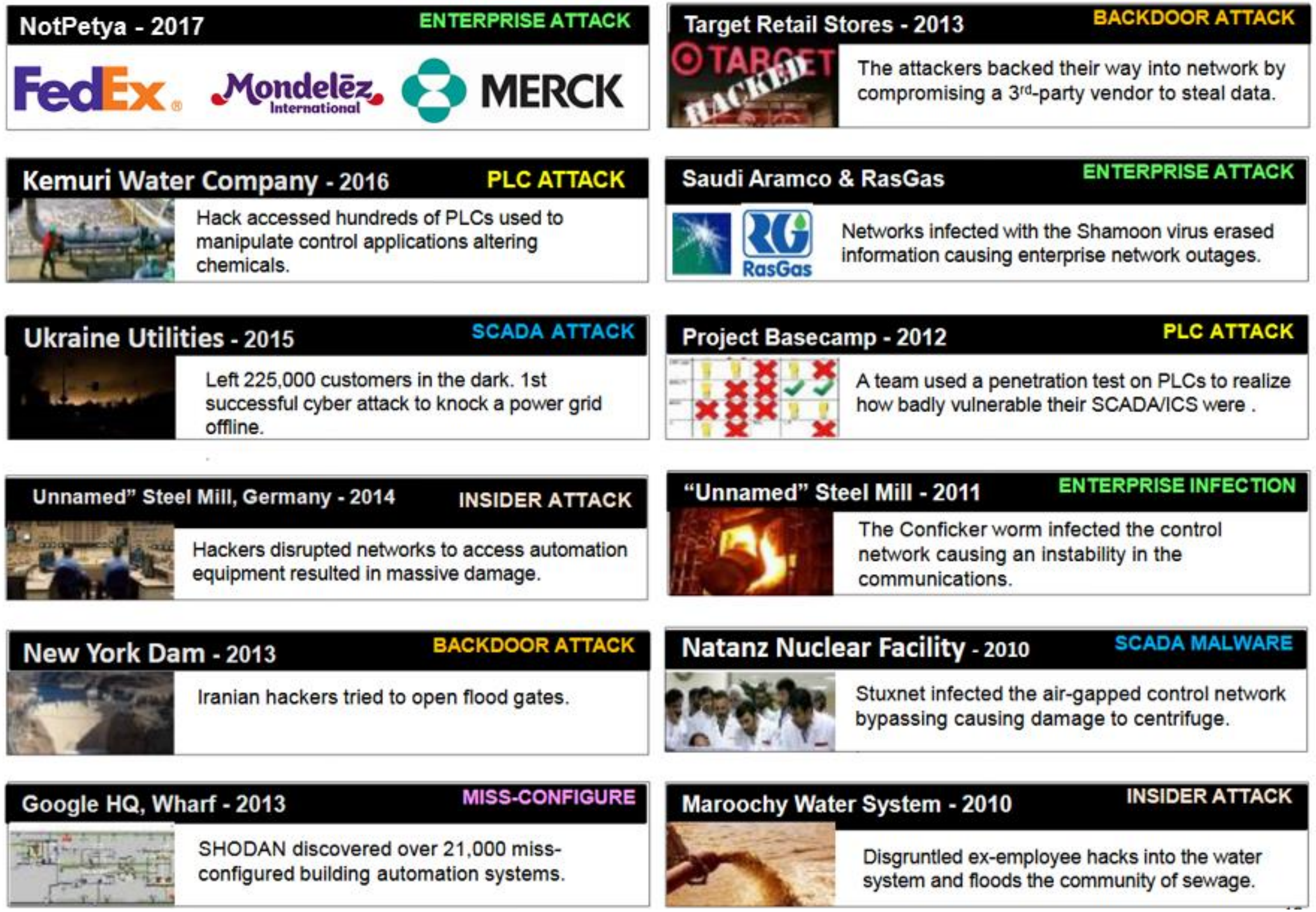
INDUSTROYER
Malware Targeting Electric Utility – Used in 2016 Ukraine Grid Attack

WANNACRY
General ransomware which impacted ICS Systems


ICS CERT INCIDENT COUNT
Only Reported Incidents in U.S.

>1000

Threat examples



NotPetya - 2017 ENTERPRISE ATTACK

FedEx
Mondelēz International
MERCK

Target Retail Stores - 2013 BACKDOOR ATTACK

TARGET
HACKED

The attackers backed their way into network by compromising a 3rd-party vendor to steal data.

Kemuri Water Company - 2016 PLC ATTACK

Hack accessed hundreds of PLCs used to manipulate control applications altering chemicals.

Saudi Aramco & RasGas ENTERPRISE ATTACK

RasGas

Networks infected with the Shamoon virus erased information causing enterprise network outages.

Ukraine Utilities - 2015 SCADA ATTACK

Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.

Project Basecamp - 2012 PLC ATTACK

A team used a penetration test on PLCs to realize how badly vulnerable their SCADA/ICS were .

Unnamed" Steel Mill, Germany - 2014 INSIDER ATTACK

Hackers disrupted networks to access automation equipment resulted in massive damage.

"Unnamed" Steel Mill - 2011 ENTERPRISE INFECTION

The Conficker worm infected the control network causing an instability in the communications.

New York Dam - 2013 BACKDOOR ATTACK

Iranian hackers tried to open flood gates.

Natanz Nuclear Facility - 2010 SCADA MALWARE

Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.

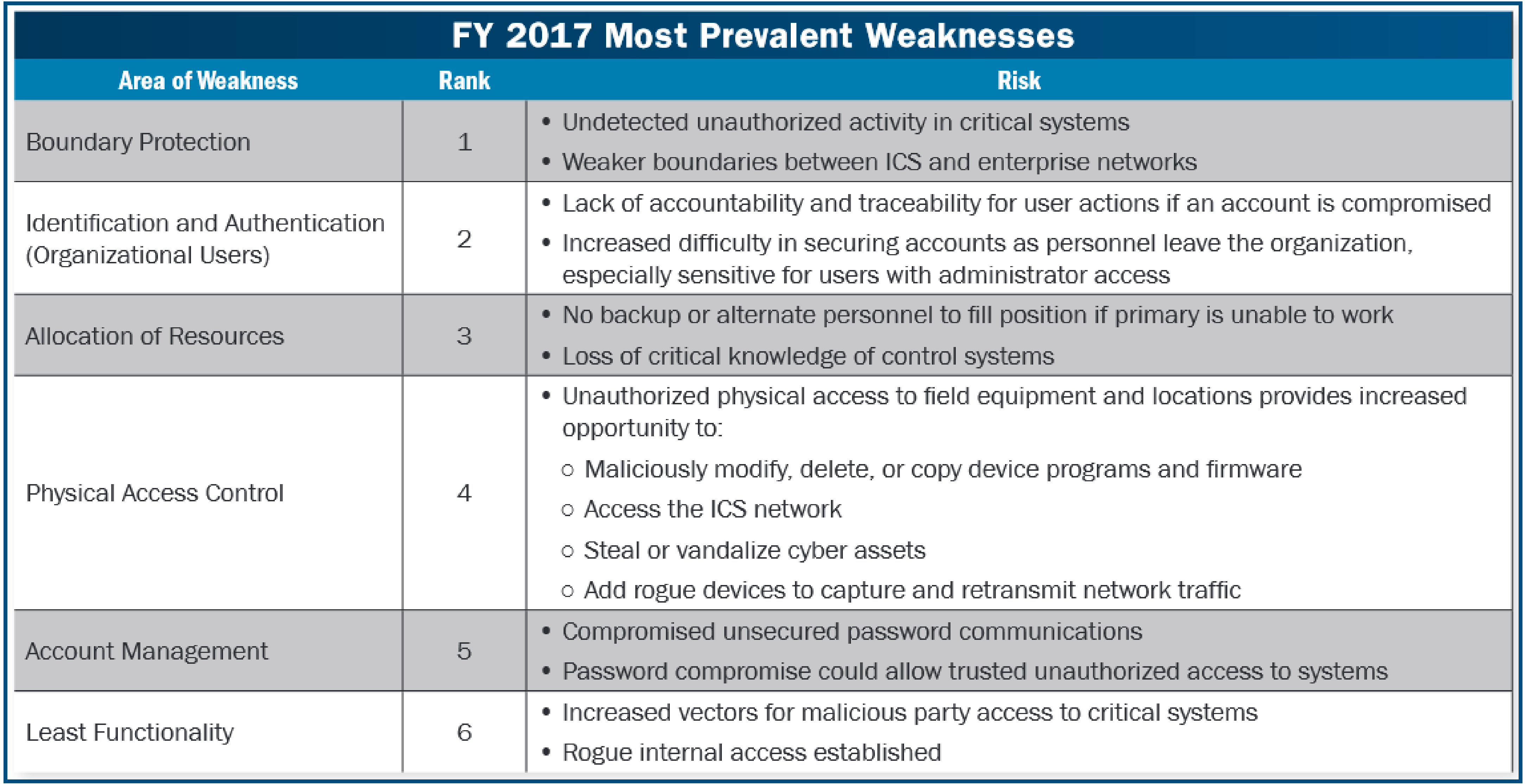
Google HQ, Wharf - 2013 MISS-CONFIGURE

SHODAN discovered over 21,000 miss-configured building automation systems.

Maroochy Water System - 2010 INSIDER ATTACK

Disgruntled ex-employee hacks into the water system and floods the community of sewage.

2017 ICS-CERT Top 6 Weaknesses



FY 2017 Most Prevalent Weaknesses

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

ISA/IEC 62443

Certified products, systems and system delivery

Series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

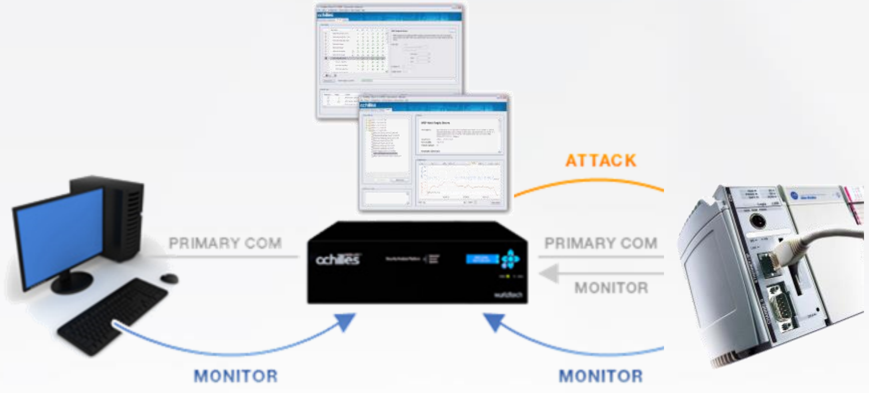
Applies to those responsible for ***designing, manufacturing, implementing, or managing*** industrial control systems:

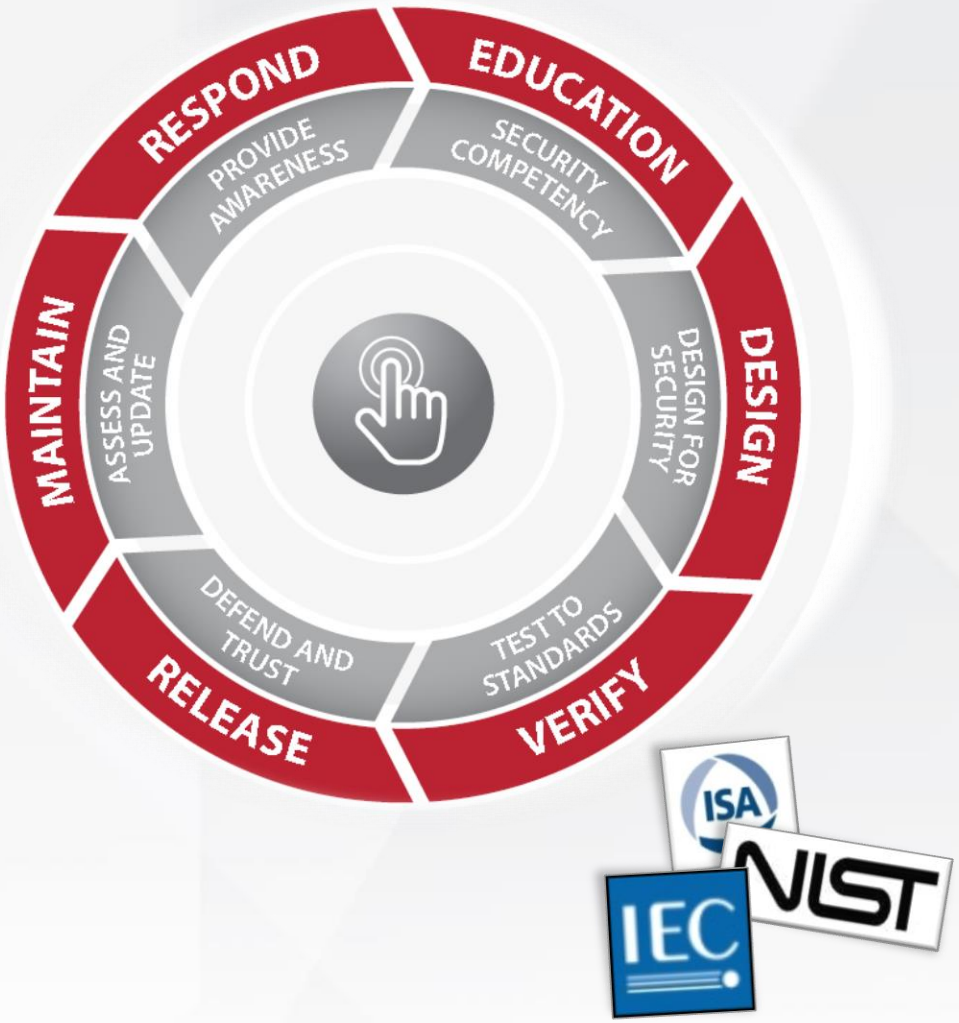
- End-users (i.e. asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors

Security built-in

Vendors must build security into products with a focus on security throughout the products lifecycle…

- *Product Security Office*
- *Secure Development Lifecycle*





PUBLIC Copyright © 2019 Rockwell Automation, Inc. All Rights Reserved

Secure network infrastructure

New validated architectures

Achieve infrastructure security through a common, validated system architecture leveraging the Stratix® portfolio and Cisco security solutions.

Design and Implementation Guides:

- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide
- Segmentation Methods within the Cell/Area Zone
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone
- Deploying Identity Services within a Converged Plantwide Ethernet Architecture
- Site-to-site VPN to a Converged Plantwide Ethernet Architecture
- Deploying industrial firewalls within a Converged Plantwide Ethernet Architecture

- Download these and more at:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page

IDENTITY SERVICES ENGINE

Adaptive Security Appliances

Rockwell Automation

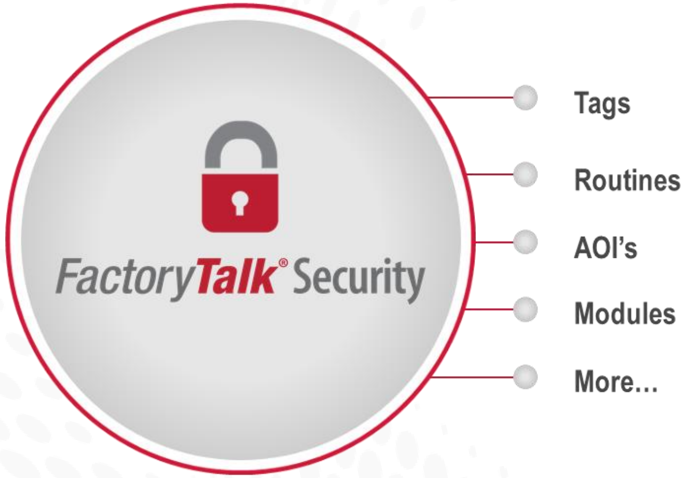
Rockwell Automation Strategic Alliance

CISCO

User access control and authorization

FactoryTalk® Security software

- Provides a **centralized authority** to **verify identity** of each user
  - Active Directory integration
  - Disconnected environment support
- **Grants or deny user's requests** to perform a particular set of actions on resources within the system



- Authenticate the user
- Authorize use of applications
- Authorize configuration access to controllers

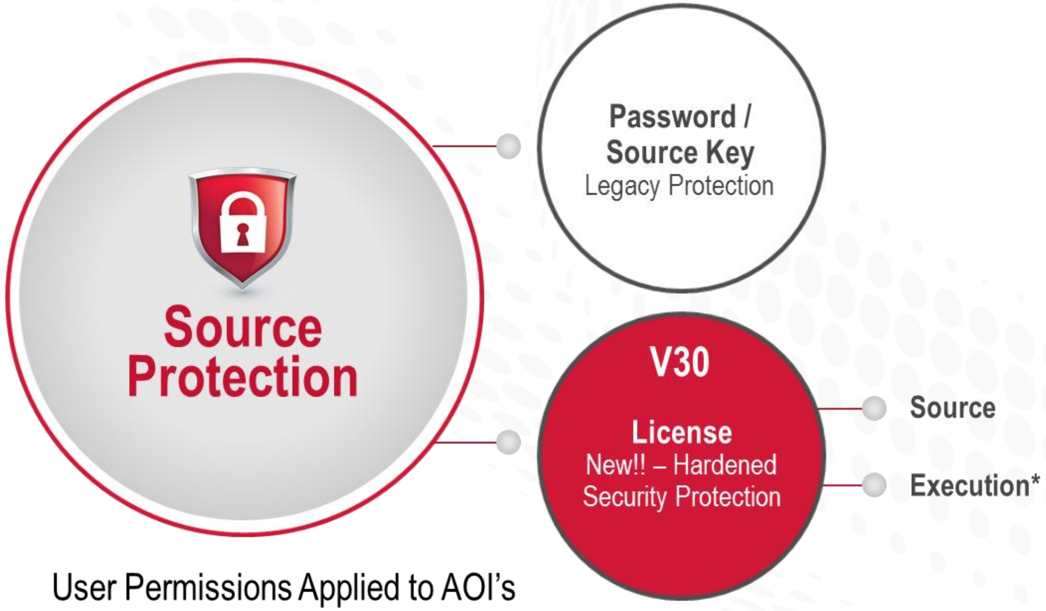
From v28:
- Temporary privilege escalation
- Guest user access
- Reusable permission sets (routines, AOIs, and tags)
- Secondary security authority

License-based source protection

Content protection features

A solution for customers to help protect the design & execution of Logix content

- **Source Protection**: Control of who can view and edit the source code of objects.
- **Execution Protection**: Control of which controllers these objects can be executed in. Prevent the duplication of code in an unauthorized machine.

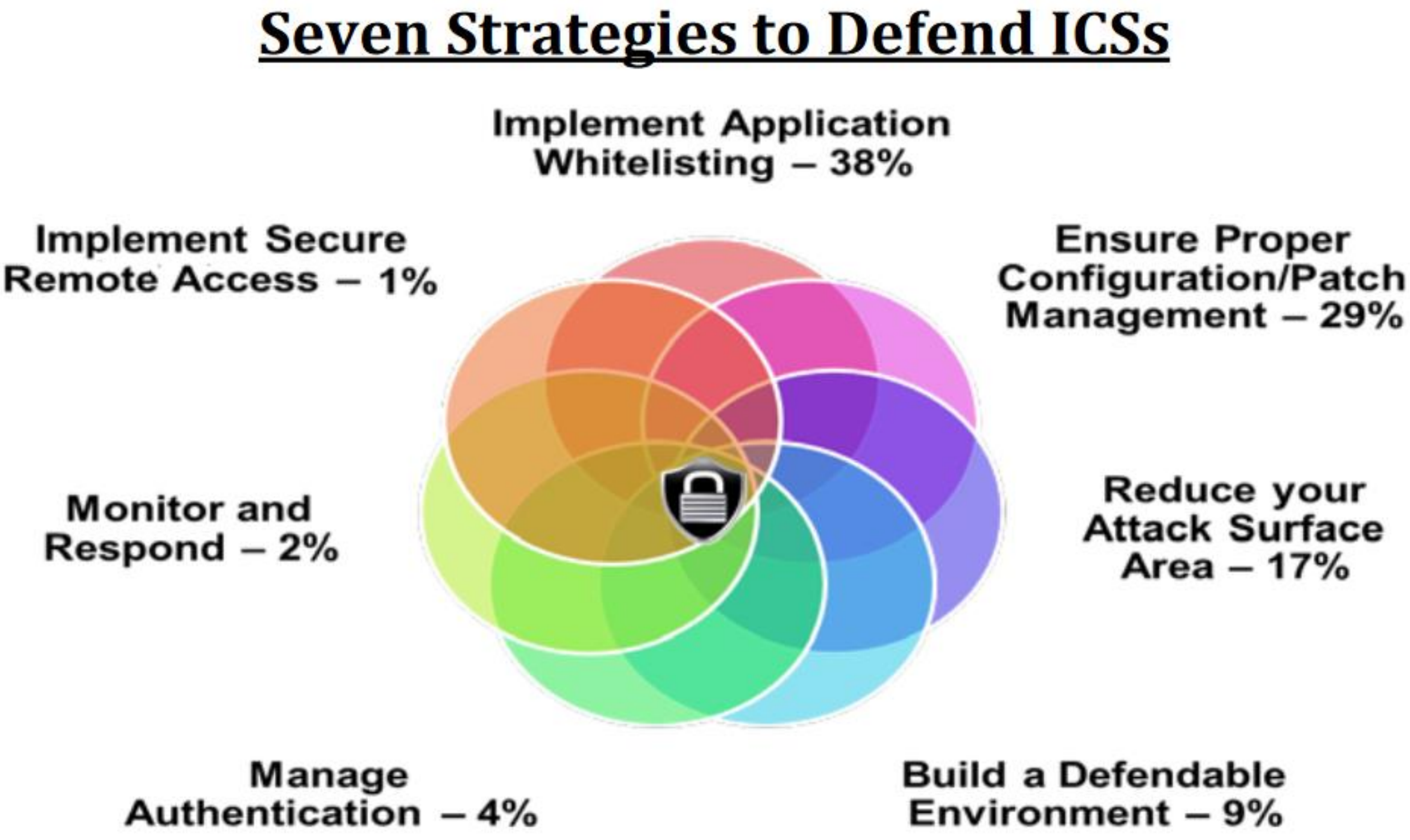


User Permissions Applied to AOI's and Routines: Protect, Edit, Copy, Export, View

*Supported by ControlLogix® 5580, CompactLogix™ 5480, CompactLogix™ 5380 controllers

Seven Strategies to Defend ICS

Percentage of ICS-CERT Incidents Potentially Mitigated by Each Strategy



Seven Strategies to Defend ICSs

Implement Application Whitelisting – 38%

Ensure Proper Configuration/Patch Management – 29%

Reduce your Attack Surface Area – 17%

Build a Defendable Environment – 9%

Manage Authentication – 4%

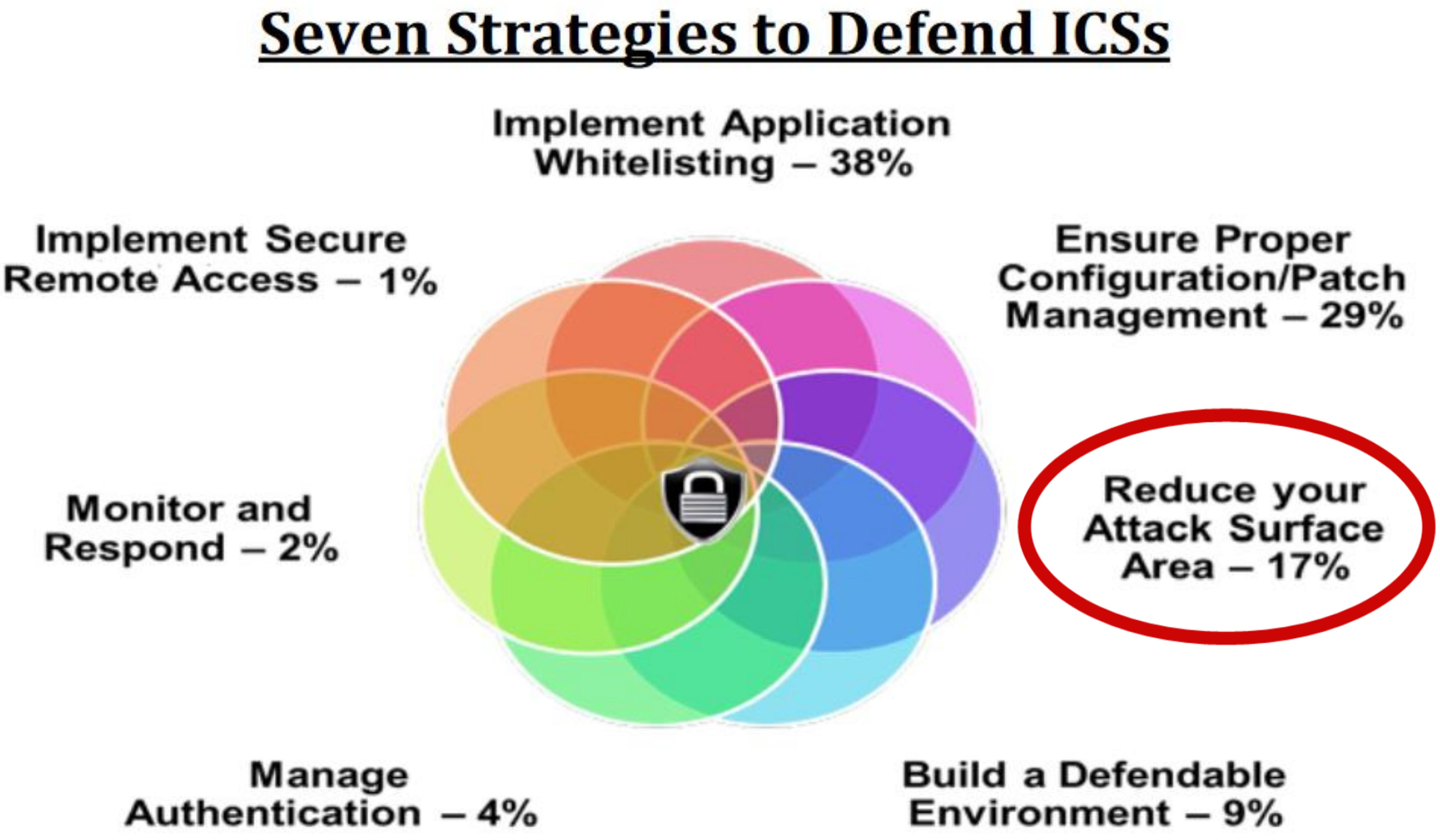
Monitor and Respond – 2%

Implement Secure Remote Access – 1%

Seven Strategies to Defend ICS

Reduce your attack surface area

Isolate ICS networks from any untrusted networks, especially the Internet.
Lock down all unused ports…



Seven Strategies to Defend ICSs

Implement Application Whitelisting – 38%

Implement Secure Remote Access – 1%

Ensure Proper Configuration/Patch Management – 29%

Monitor and Respond – 2%

Reduce your Attack Surface Area – 17%

Manage Authentication – 4%

Build a Defendable Environment – 9%

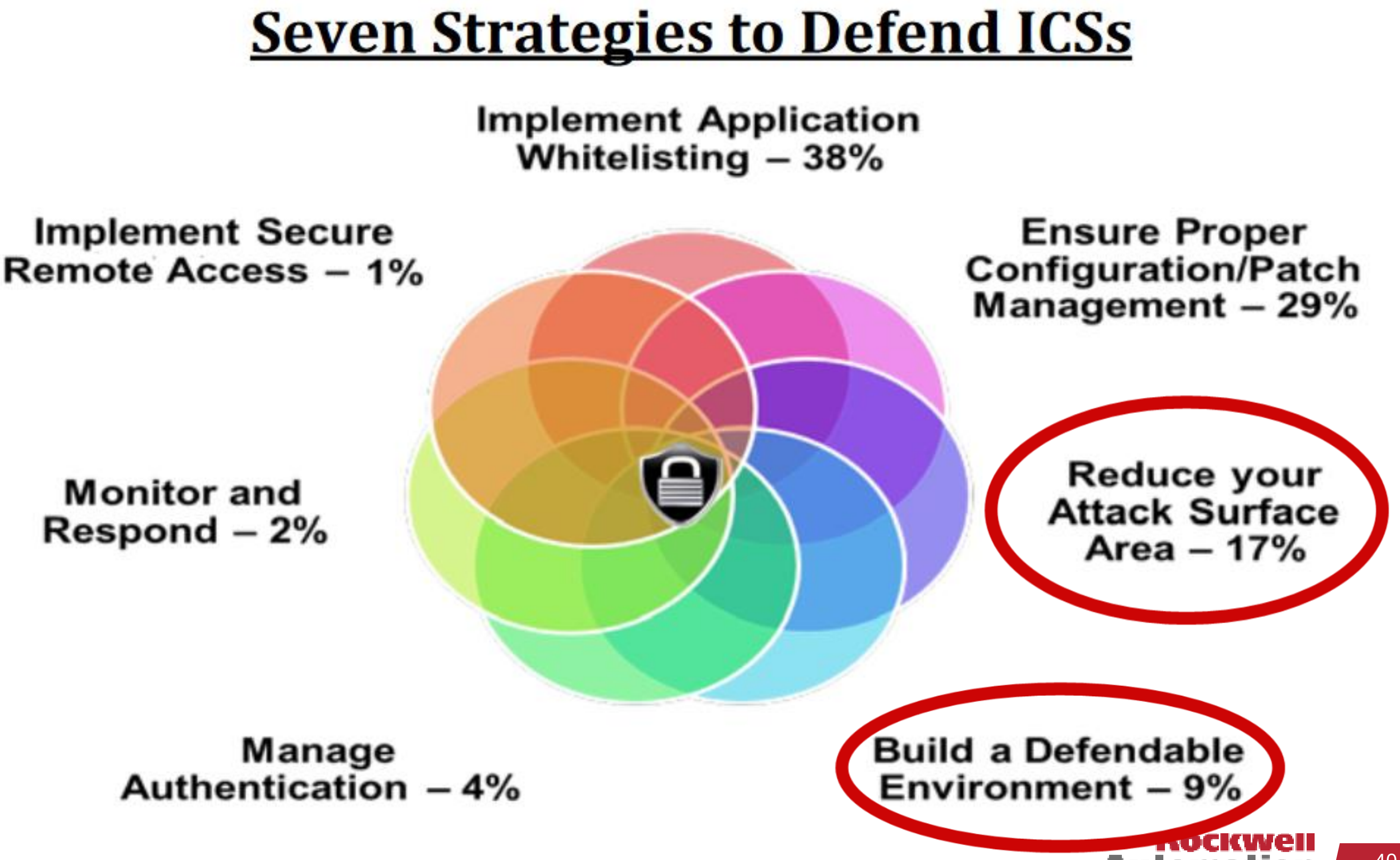
Seven Strategies to Defend ICS

Reduce your attack surface area

Isolate ICS networks from any untrusted networks, especially the Internet.
Lock down all unused ports…

Build a defendable Environment

Limit damage from network perimeter breaches. **Segment networks** into logical enclaves and **restrict host-to-host communications** paths…


Seven Strategies to Defend ICSs
Implement Application Whitelisting – 38%
Implement Secure Remote Access – 1%
Ensure Proper Configuration/Patch Management – 29%
Monitor and Respond – 2%
Reduce your Attack Surface Area – 17%
Manage Authentication – 4%
Build a Defendable Environment – 9%

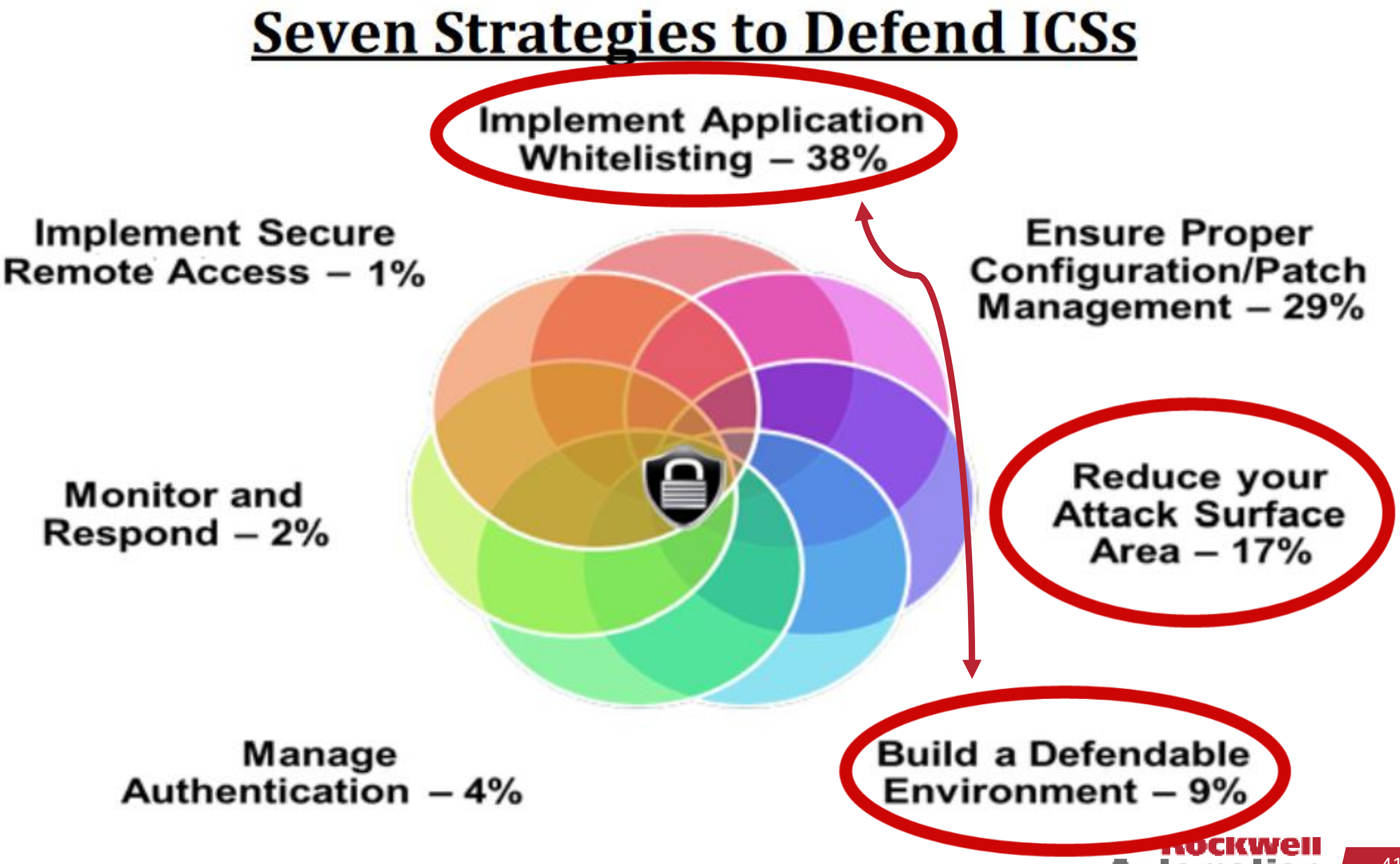
Seven Strategies to Defend ICS

Reduce your attack surface area

Isolate ICS networks from any untrusted networks, especially the Internet.
Lock down all unused ports…

Build a defendable Environment

Limit damage from network perimeter breaches. **Segment networks** into logical enclaves and **restrict host-to-host communications** paths…



Seven Strategies to Defend ICSs

Implement Application Whitelisting – 38%

Implement Secure Remote Access – 1%

Ensure Proper Configuration/Patch Management – 29%

Monitor and Respond – 2%

Reduce your Attack Surface Area – 17%

Manage Authentication – 4%

Build a Defendable Environment – 9%

Industrial Ethernet Switch Type Selection

Managed Infrastructure

	Advantages	Disadvantages
Managed Switches	▪ Loop prevention and resiliency ▪ Security services ▪ Management services (Multicast, DHCP per port and DLR) ▪ Diagnostic information ▪ Segmentation services (VLANs) ▪ Prioritization services (QoS)	▪ More expensive ▪ Requires some level of support and configuration to start up
Unmanaged Switches	▪ Inexpensive ▪ Simple to set up	▪ No loop prevention or resiliency ▪ No security services ▪ No diagnostic information ▪ No segmentation or prioritization services ▪ Difficult to troubleshoot, no management services
ODVA Embedded Switch Technology	▪ Cable simplification with reduced cost ▪ Ring loop prevention and resiliency ▪ Prioritization services (QoS) ▪ Time Sync Services (IEEE 1588 PTP Transparent Clock) ▪ Diagnostic information	▪ Limited management capabilities ▪ May require minimal configuration

Managed Infrastructure Selection

Managed Infrastructure

Managed Switches

- Access switching or distribution routing
- Diagnostic information
- Network Address Translation (NAT)
- Segmentation / VLAN capabilities
- Prioritization services (QoS)
- Network resiliency

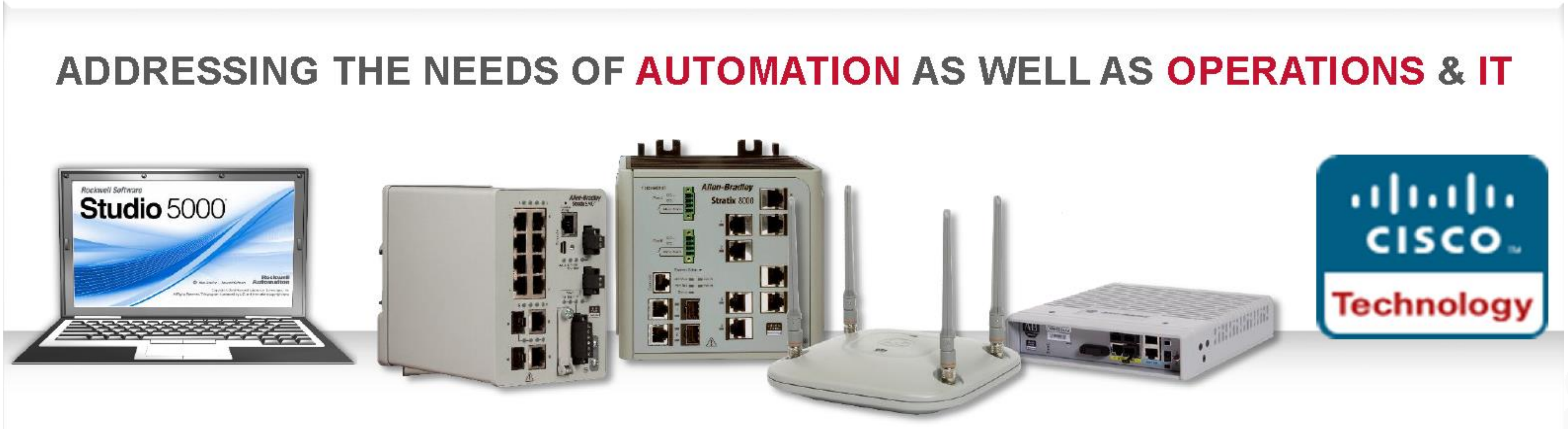
Security Appliances

- Secure real-time control communication
- Routing and firewall capabilities
- Intrusion protection
- Access control lists

- Manageability by OT and IT tools
  - Topologies - Switch-level and device-level
  - Switching – network services
  - Routing – connected, static, dynamic
  - Wireless Access Points - Autonomous and Unified Architectures
  - Security Appliances - Industrial firewalls with inspection profiles for EtherNet/IP – deep packet inspection (DPI)

The Stratix® portfolio

Integrating industrial and enterprise environments



ADDRESSING THE NEEDS OF AUTOMATION AS WELL AS OPERATIONS & IT

Products that offer …

- Layer 2 and Layer 2 switching for simple to complex network applications
- Advanced security services
- Plant-floor and Enterprise integration

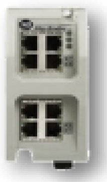
Technology that offers …

- Advanced switching, routing & security features
- Common tools for Controls & IT
- Improved Maintainability

Network Switch Product Overview

Stratix® 2000

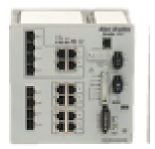
Stratix® 2500



Stratix® 6000

Stratix® 5700/
ArmorStratix™ 5700

Stratix® 8000/8300



Stratix® 5400

Stratix® 5410

UNMANAGED

LIGHTLY MANAGED

FULLY MANAGED

HIGH PERFORMANCE MANAGED

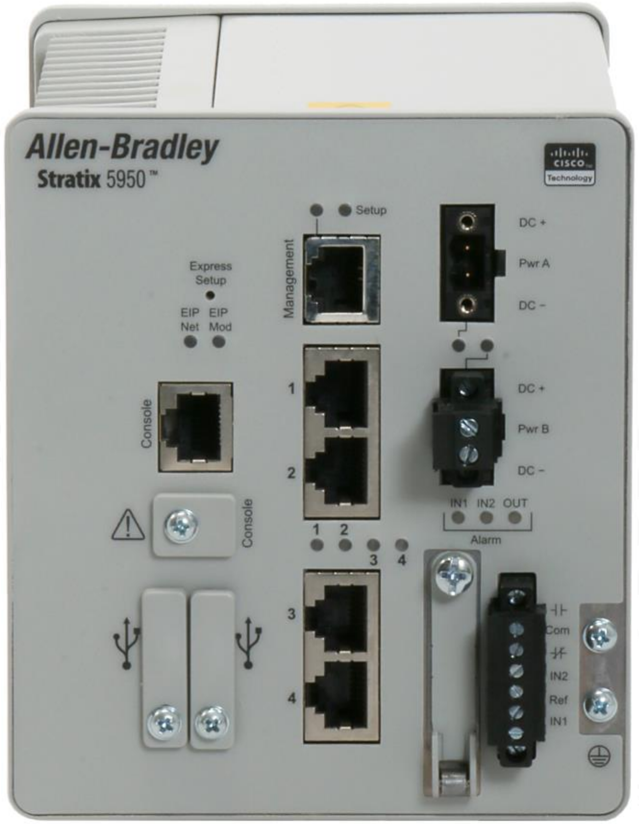
100M/1G ◂- - - - - - - - - - - - - - - - - - -▸ 100M ◂- -▸ 100M/1G ◂- -▸ 1G/10G

Network security appliance

Stratix® 5950 security appliance

Strategic collaboration between Cisco and Rockwell Automation

- Based on recognized and proven technologies
  - Adaptive Security Appliance for Firewall and VPN
  - SourceFire FirePOWER technology for inspection and detection
  - Enhanced with OT context of protocols, behaviors, and features

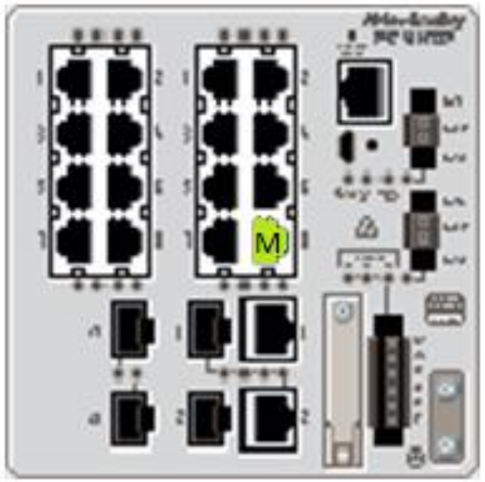


- Key Features:
  - Deep packet inspection for ICS protocols
  - Threat & Application Update Service

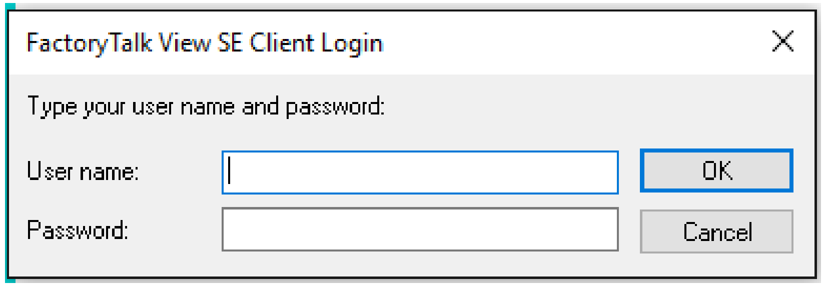
- DIN rail mount
- Connectivity Options:
  - (4) 1Gig Copper
  - (2) 1Gig Copper and (2) SFP
- Industrially-hardened

Unused ports

- Why do we need to enable a maintenance port? Cant we connect?
  - It’s a common security practice to shut down all unused ports
    - However, with the proper credentials we can use our CIP™ integration to activate or deactivate the port easily from the HMI



Maintenance Port Enabled


FactoryTalk View SE Client Login

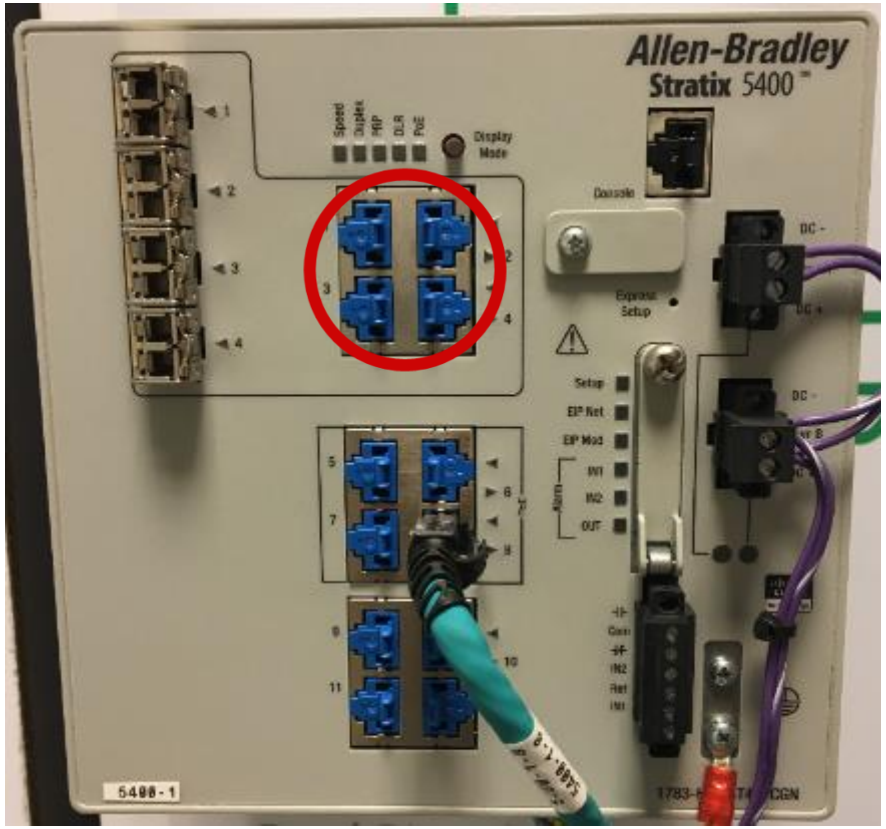
Type your user name and password:

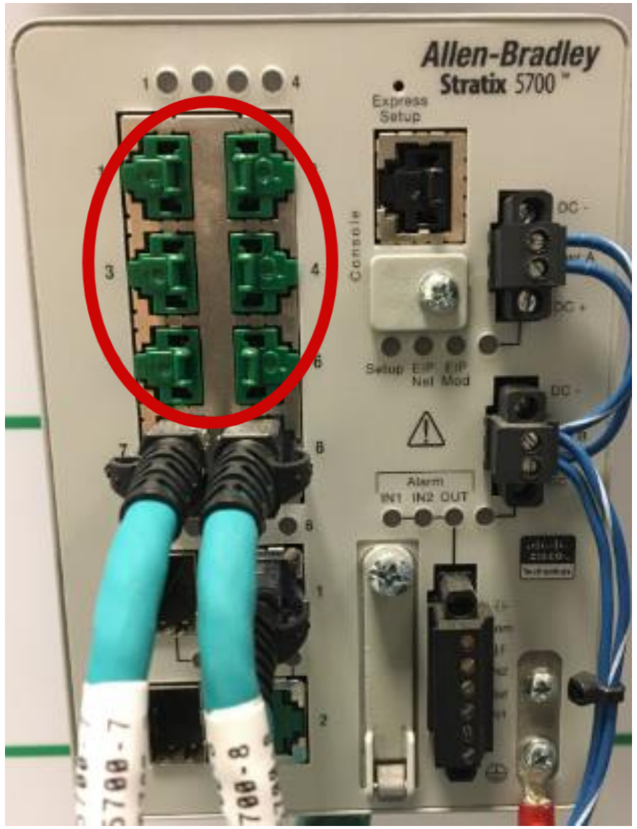
User name:

Password:

Unused ports

- Additionally, ports typically have a port lock in place
    - Can only be removed using special tools





Unused ports and cables

- You can even lock cables and prevent them from being removed!