Schaedler yesco

100 Years
Real Life Experience

Plant Floor Cybersecurity, Network Technologies, and Platforms

28 MARCH 2024

Products and Solutions for the Electrical Industry

So… Who are we?

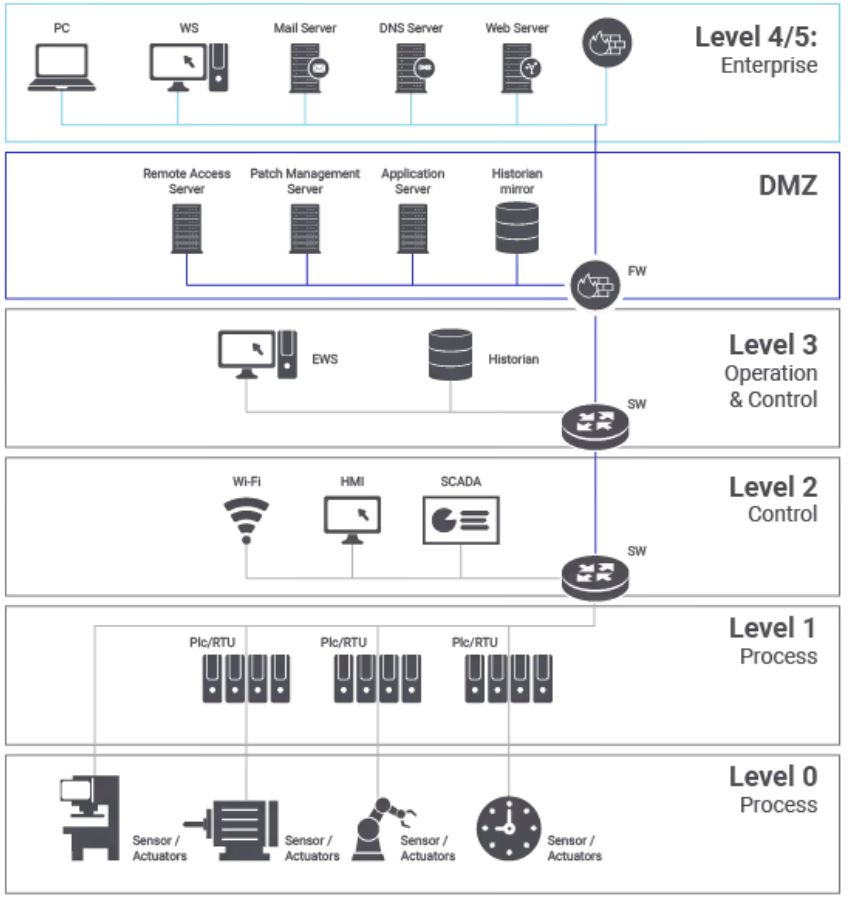
- Matt Pike
  - Sales Executive, Cybersecurity Services
  - Rockwell Automation
- Ankur Mohan
  - Solution Consultant
  - Rockwell Automation
- Frank Aponte Alsina
  - Smart Manufacturing Business Development Lead
  - Schaedler Yesco Distribution

Agenda

- OT Networking
- DX to Security
- OT Cybersecurity (NIST CSF, Minutes Matter)
- Rockwell Automation's OT Cybersecurity Partners
- How we can help (ASP and NSS Services)

OT Networking

- What is OT?
- Why would I want to network my automation devices (PLCs / HMIs / Drives / IO)?
- Can't I just plug everything into one switch?
- IT manages my OT Network. They probably have this Cybersecurity thing handled, right?
- My little manufacturing company can't possibly be a Cybersecurity target, can it?
- Cybersecurity is just server data, right?



ICS-Focused campaigns, attacks

Solarwinds – software supply chain attack

Israeli National Water Supply – targeted command & control systems

Taiwan State Energy Company – ransomware attack

56% of gas, wind, water, solar utilities breached in prior year*

Majority of IT security pros most concerned about critical infrastructure

2021 – Oldsmar, Florida Water Treatment Facility, JBS Foods, Colonial Pipeline, Accenture

2010

STUXNET

Worm targeting SCDA and modifying PLCS

OPERATION AURORA

APT cyberattack on 20+ high tech, security & defense companies

2011

NIGHT DRAGON

Worm targeting SCDA and modifying PLCS

DUQU

APT cyber attack on 20+ high tech, security & defense companies

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 government & research organizations

2014

HAVEX

Industrial control system Remote access trojan & information stealer

HEARTBLEED

Security bug and vulnerability exploited by attackers

2015

BLACK-ENERGY

Malware injected into Ukrainian power company network, cut power to the affected region

2016

BLACK-ENERGY

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

Ransom malware based on stolen NSA exploits the impacted ICS systems

INDUST-ROYER

Malware targeting electric utility – used in 2016 Ukraine grid attack

WANNACRY

General ransomware which impacted ICS systems

2018

SHAMOON3

Wiper oil & gas, telecom & gov Southeast Europe & Middle East

OPERATION AURORA

APT 20+ high tech, security & defense companies

2019

LOCKER-GOGA

Ransomware with wiper capabilities

BITPAYMER

Ransomware big game hunting

MAZE

Ransomware and stole/ exposed information

2020

EKANS RANSOMWARE

Design specially to target critical ICS process

RYUK RANSOMWARE

Encrypts network drives and other user resources while also deleting backups

2021

RANSOMWARE

Major brewing company

RANSOMWARE ATTACK

Canadian company's refusal to pay ransom resulted in detailed plans of military spy plane leaked on the dark web by hackers

UNAUTHORIZED ACCESS

Water system compromised - probably due to poor password security, and an outdated operating system

*https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1600101948/siemens-cybersecurity.pdf
**https://info.claroty.com/the_state_of_industrial_cybersecurity_form

Connect critical business functions with unified information

ERP

CRM

PLM

MES/MOM

Process simulation

IIoT

Analytics

CAD

Automation emulation

Augmented Reality

Historian

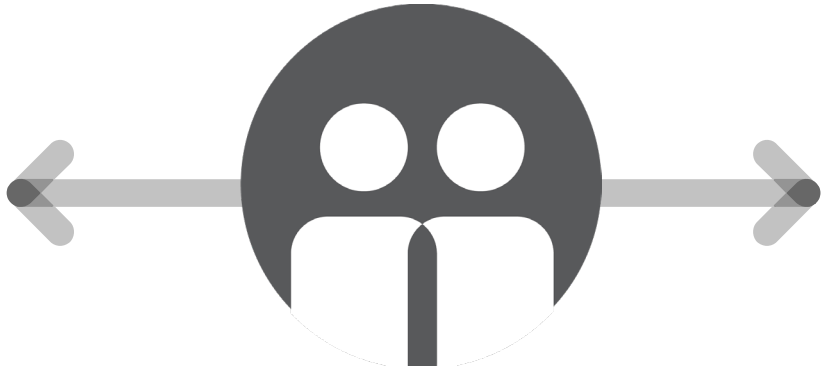
Rockwell Automation | InnovationSuite powered by PTC

Together, Cisco and Rockwell Automation can help

Leading digital transformation for The Connected Enterprise with industrial ready, world-class control, power and information systems and IT networking and security technologies

CISCO

Worldwide leader in IT networking and security



Rockwell Automation

Global leader in industrial control, power and information solutions

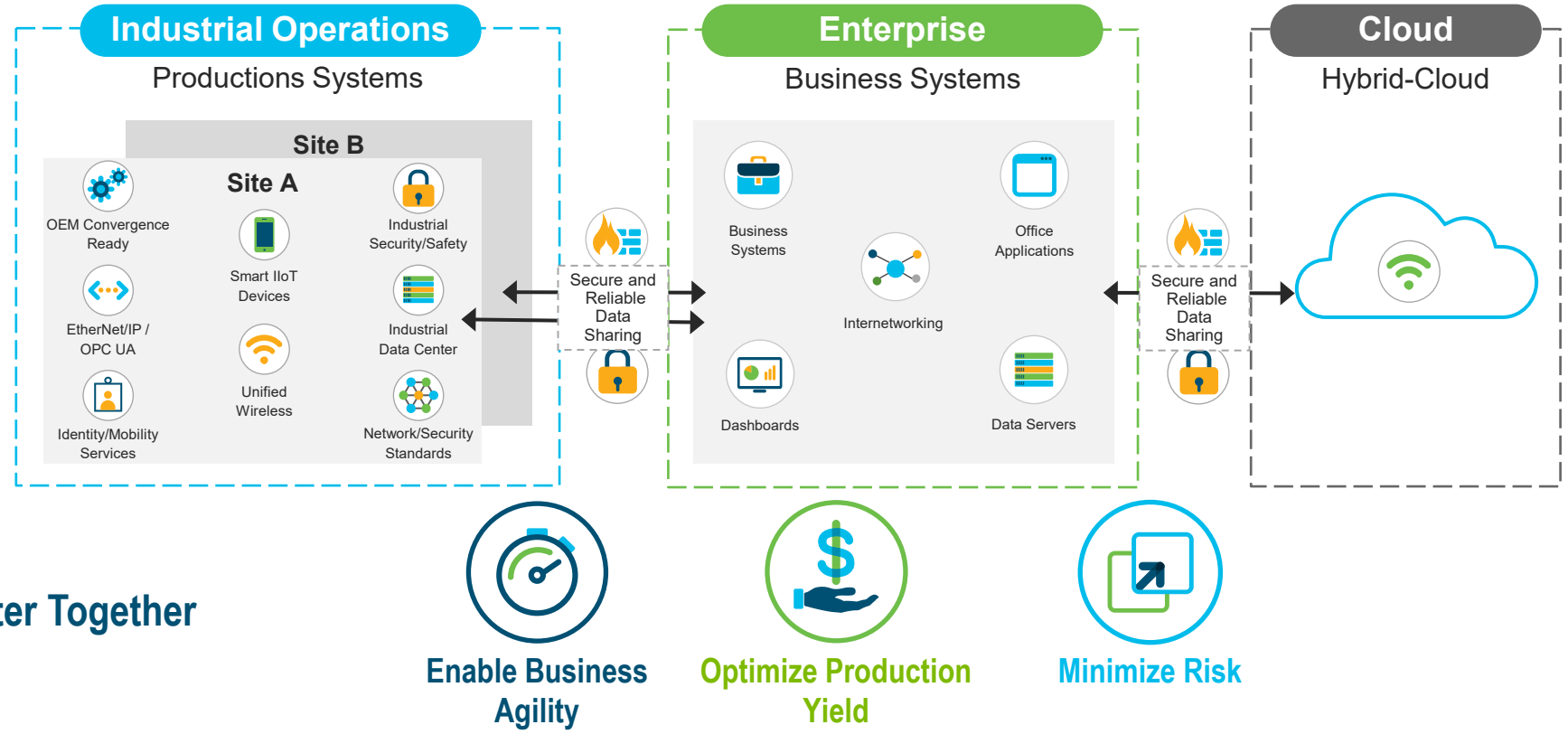
Trusted domain experts with a strategic alliance

Committed to future industry success

Dedicated to developing ground-breaking solutions

Introducing Converged Plantwide Ethernet (CPwE), a holistic blueprint for digital transformation

The CPwE Converged Network Architectures



Better Together

- **Enable Business Agility**
- **Optimize Production Yield**
- **Minimize Risk**

Collection of architected, tested and validated network and security designs

Simplify network and security design by connecting industrial operations and business systems

An open solution that adheres to regulatory standards creates flexibility and scalability

A converged infrastructure built on a common architecture framework makes the network data-ready

Network & Security challenges in industrial environments

Antiquated systems
Unpatched, legacy systems

Insecure design
Lack of segmentation

OT security skills
IT sec ⇔ Ops knowledge

Lack of visibility
Of what's out there

Access control
Access needs evolving

Change control
24/7/365 operations

Business needs
Real-time information

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Converged Architectures that CPwE Helps to Address

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

Enabling OT-IT Collaboration / Convergence / Integration

Challenges Associated with Converged Architectures that CPwE Helps to Address

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
Internet
Cloud
Cloud
Cloud
External DMZ/ Firewall
Identity Services

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) Level 3.5

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

Level 3 - Site Operations
(Control Room)

Identity Services
Active
Standby
NetFlow
Wireless LAN Controller (WLC)
Remote Access Server
Core Switches
NetFlow
NetFlow
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)

Industrial IT

IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O

Cell/Area Zone - Levels 0-2
Redundant LANs - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)

NetFlow
SSID 2.4 GHz
EtherNet/IP
LWAP
Thin Client
I/O
Controller
I/O
Soft Starter
Drive
Controller
I/O
I/O
I/O
Instrumentation

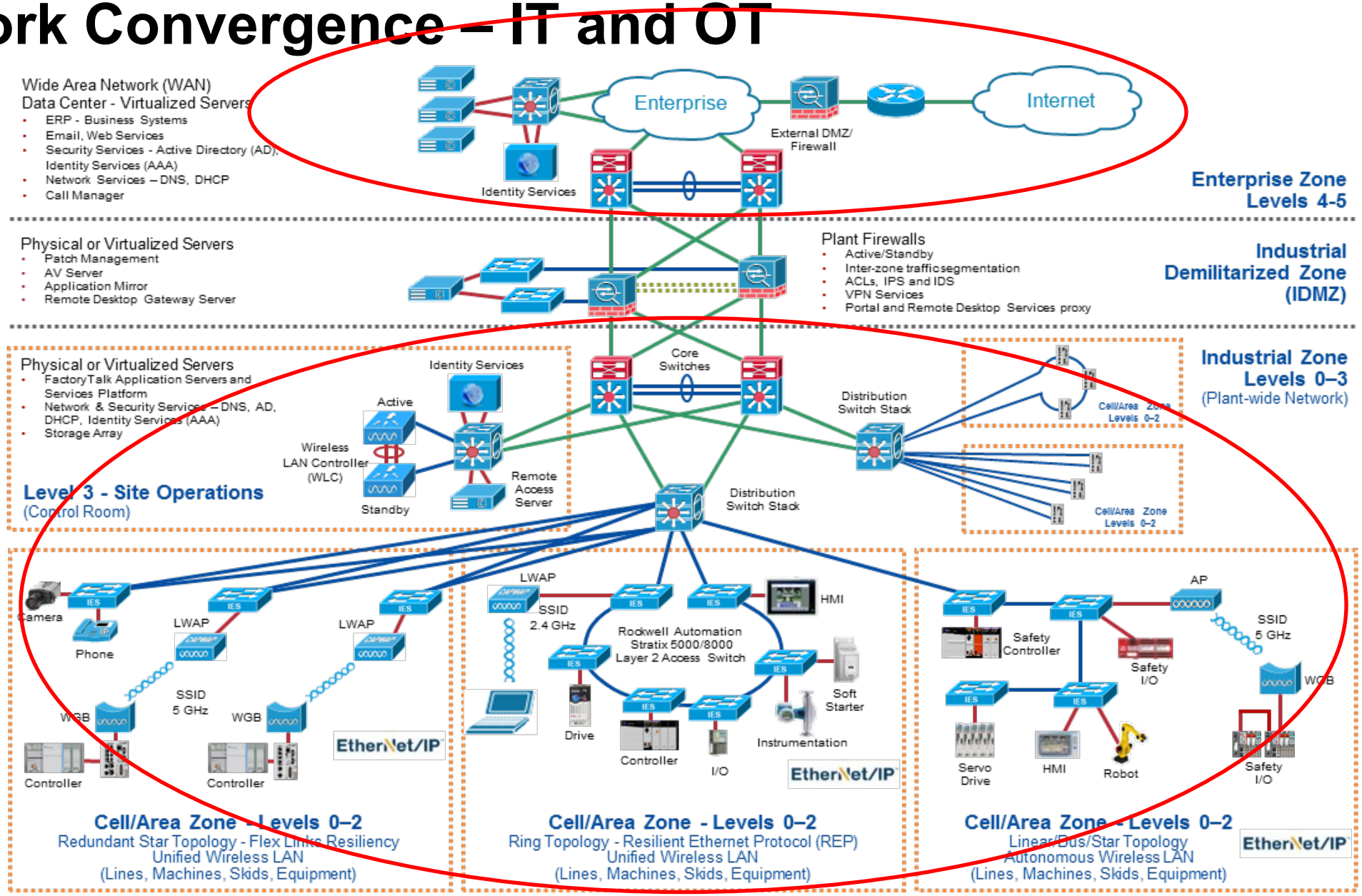
Cell/Area Zone - Levels 0-2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

NetFlow
EtherNet/IP
LWAP
SSID 5 GHz
Safety Controller
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller

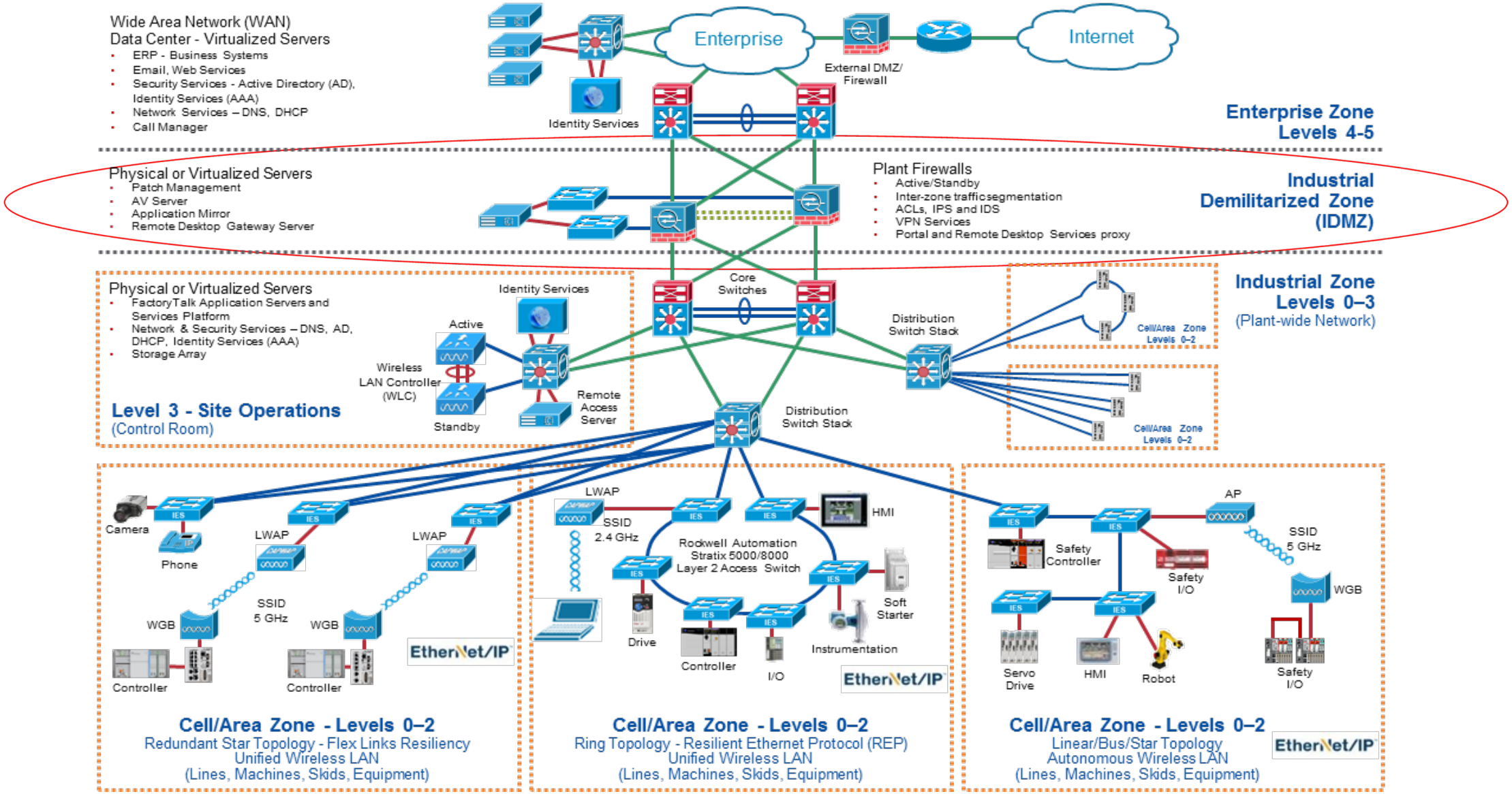
Cell/Area Zone - Levels 0-2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

Industrial IoT Operational Technology

Network Convergence – IT and OT



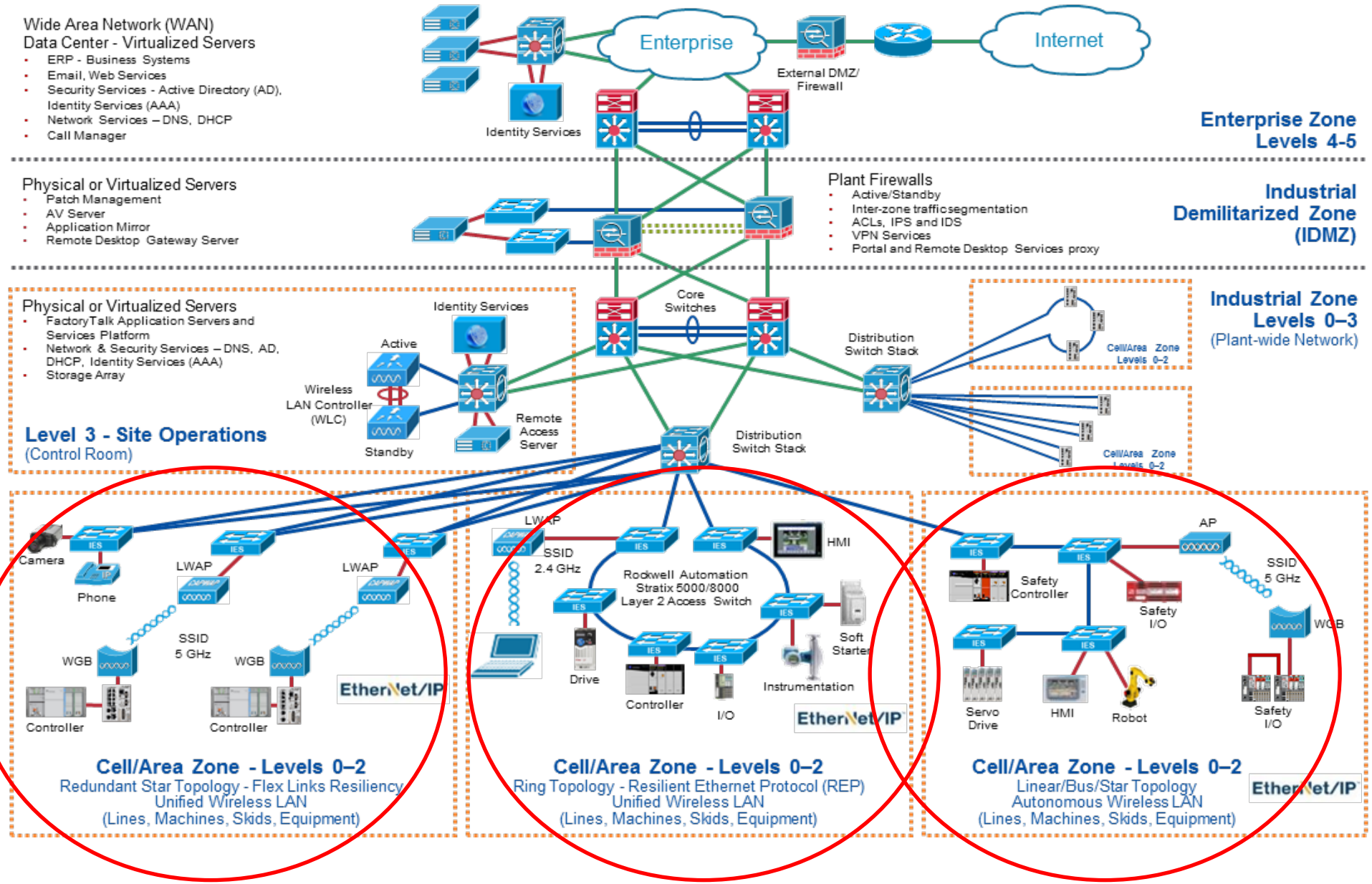
The IDMZ – Industrial Demilitarized Zone



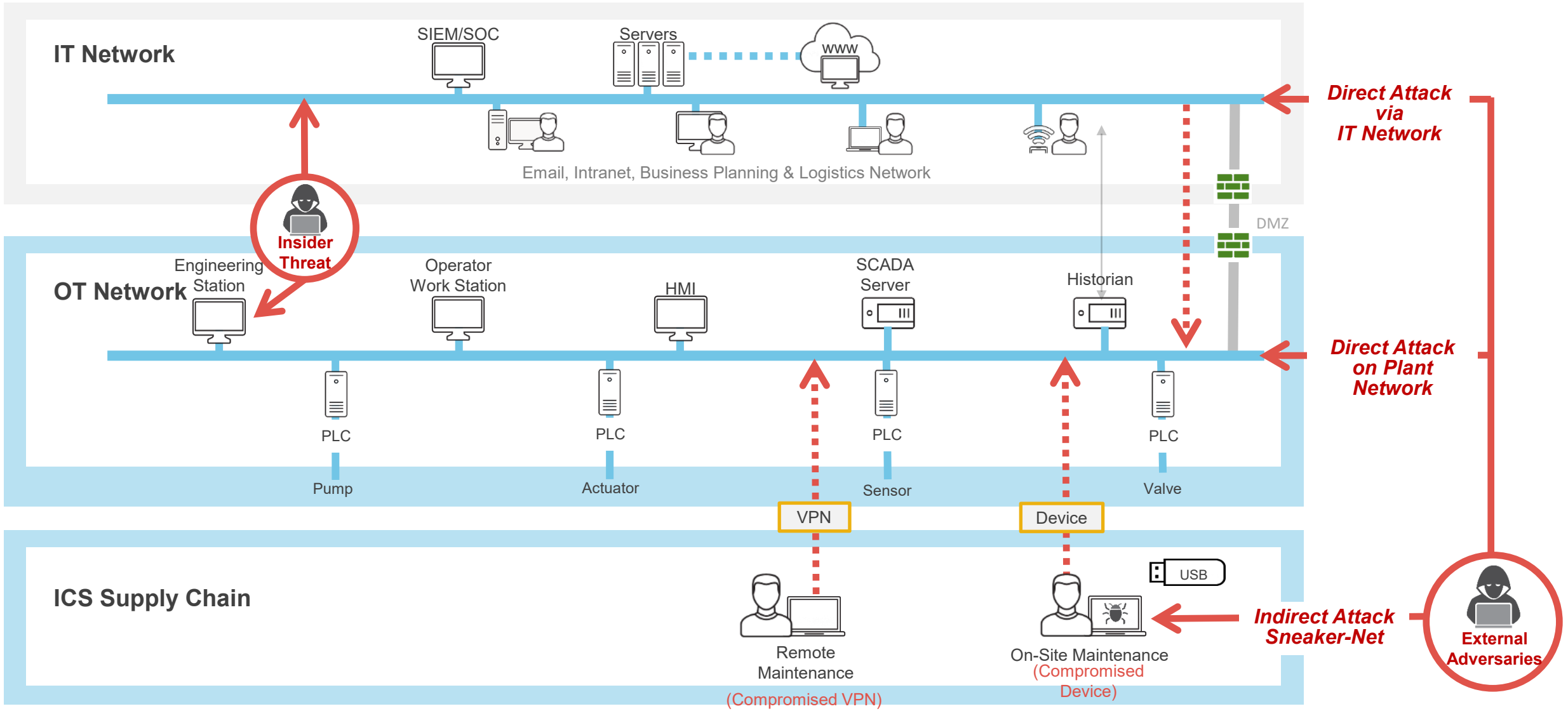
What is an Industrial DMZ?

- An IDMZ, or Industrial Demilitarized Zone, is a sub-network placed between a trusted network (industrial) and an untrusted network (enterprise). The IDMZ contains business facing assets that act as brokers between the trusted and untrusted networks.
- IACS traffic does not enter the IDMZ; it remains within the Industrial Zone
- All IACS network traffic from either side of the IDMZ terminates in the IDMZ
- Traffic never travels directly across the IDMZ.
- Primary services are not permanently stored in the IDMZ
- All data is transient; the IDMZ does not permanently store data
- A properly designed IDMZ can be unplugged if compromised and still allow the industrial network to operate without disruption.
- Why?
- To protect the production environment from the outside world

Cell/Area Zones



ICS Threat Vectors



Rockwell Automation

Cybersecurity Essentials

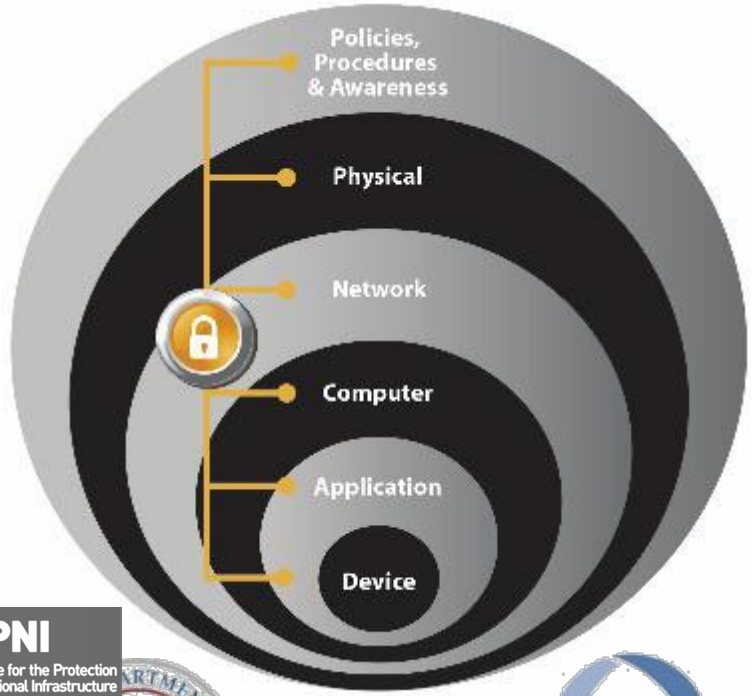
Rockwell Automation

Applying Products and Solutions to Assist in Defense in Depth

Defense-in-Depth

Deploying Network Security Within A Converged Plantwide Ethernet Architecture

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



- **Defense in Depth**
  - Shield targets behind multiple levels of diverse 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

OT Cybersecurity

- National Institute of Standards and Technology Cybersecurity Framework v2.0 (NIST CSF)
- Why does Rockwell Automation use this framework as opposed to something else?

NIST Cybersecurity Framework

Provides your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

- Organizational context
- Risk management strategy
- Roles and responsibilities
- Policies and procedures

- Asset management
- Business environment
- Risk assessment
- Risk management strategy
- Vulnerability management

- Awareness control
- Awareness and training
- Data security
- Countermeasure deployment
- Maintenance
- Protective technology

- Anomalies and events
- Security continuous monitoring
- Detection process

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

- Recovery planning
- Onsite Restoration
- Improvements
- Communications
- Training

Rockwell Automation's OT Cybersecurity Partners

Rockwell Automation

CLAROTY

CISCO

DRAGOS

FORTINET

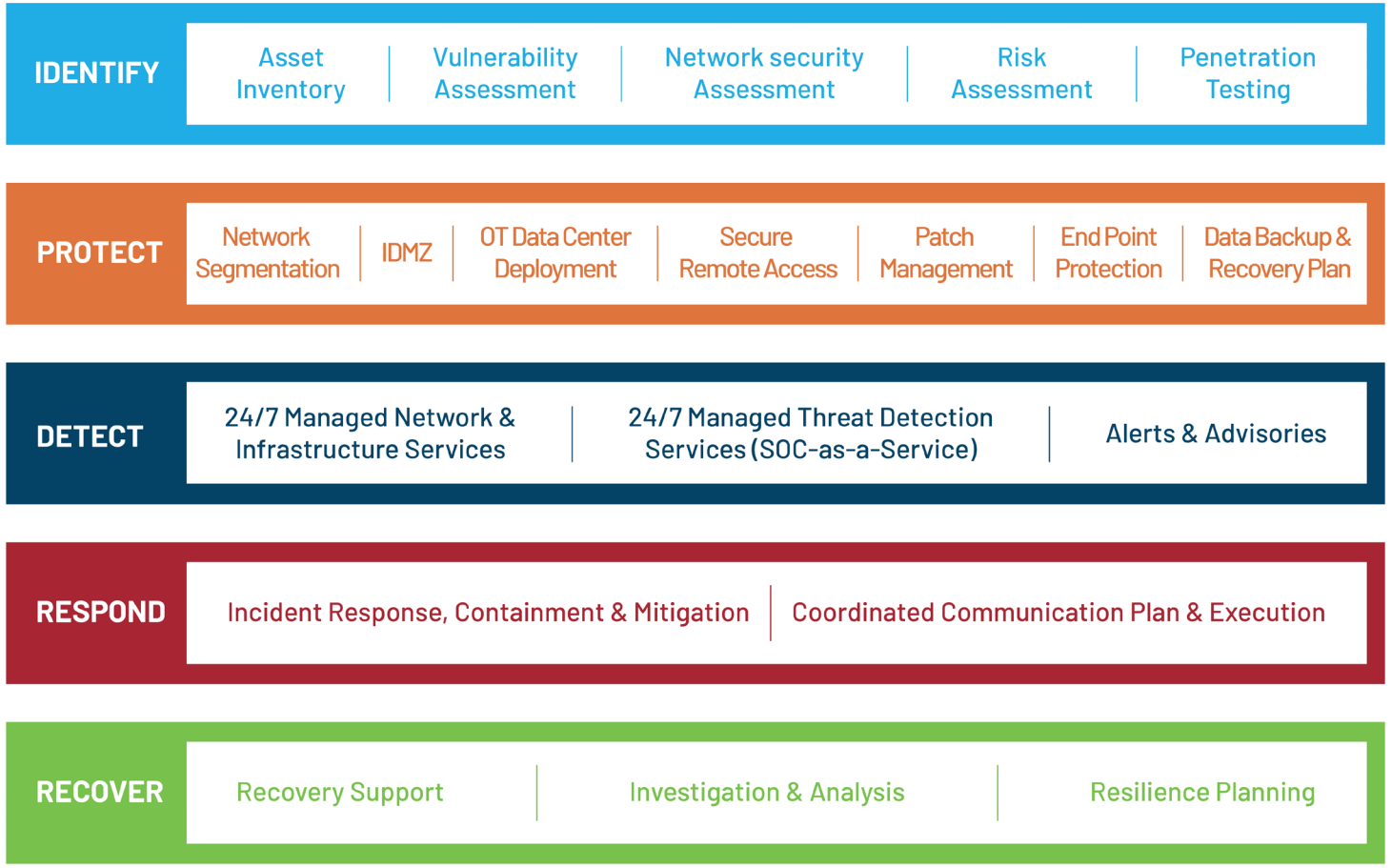
CROWDSTRIKE

VERVE
A ROCKWELL AUTOMATION COMPANY

THINMANAGER
A ROCKWELL AUTOMATION TECHNOLOGY

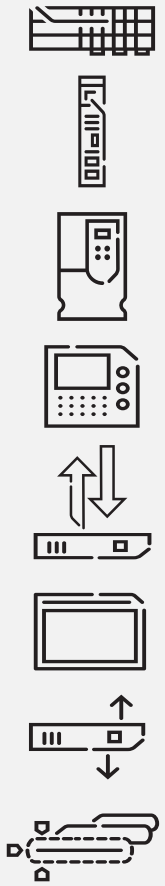
Schaedler yesco

How do Those Partners Apply to the NIST CSF



Cybersecurity Services Technology Partnership Overview

Assets



Technology & service partners

World class leading technology partners required to **protect** OT assets

Security appliances
CISCO · DELL · FORTINET

Threat detection
CLAROTY · DRAGOS · CISCO

Endpoint protection
CROWDSTRIKE

Vulnerability & risk management
VERVE

Secure remote access
CLAROTY · ASEM (A ROCKWELL AUTOMATION COMPANY)

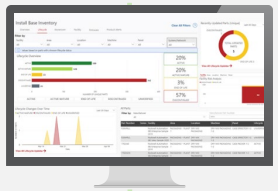
Incident response & threat intel
DRAGOS

Rockwell Automation

domain expertise to assess, implement and manage

managed services

Israel Secure Operations Center (SOC)



at a global scale

with local address- bringing 1000's of local engineers to support customers when and where they need us most

16 global remote support monitoring centers

Our domain expertise, digital insights at global scale and our partners, are what make us

the most comprehensive ICS Cybersecurity solution in the market

Managed Security Services and Support

24x7x365

Follow the Sun NOC and SOC – Tier 1, 2, 3 and Analyst Support

Alarm/Alert Monitoring

Administration

Patching, Firewall, Backups

Version Revisions and Updates

Data Enrichment, Tuning, Reporting

Phone, E-Mail, Chat, Tickets

Cyber Incident Response

Complex Issue Resolution (CIRT)

High-Level Product Support

123K Alarms Annually

99.3% SLA on Critical Alarms

20.3K Monitored Devices

30.3K Tickets Annually

13.2K Windows Devices Patched

11.2K Infrastructure Devices Patched

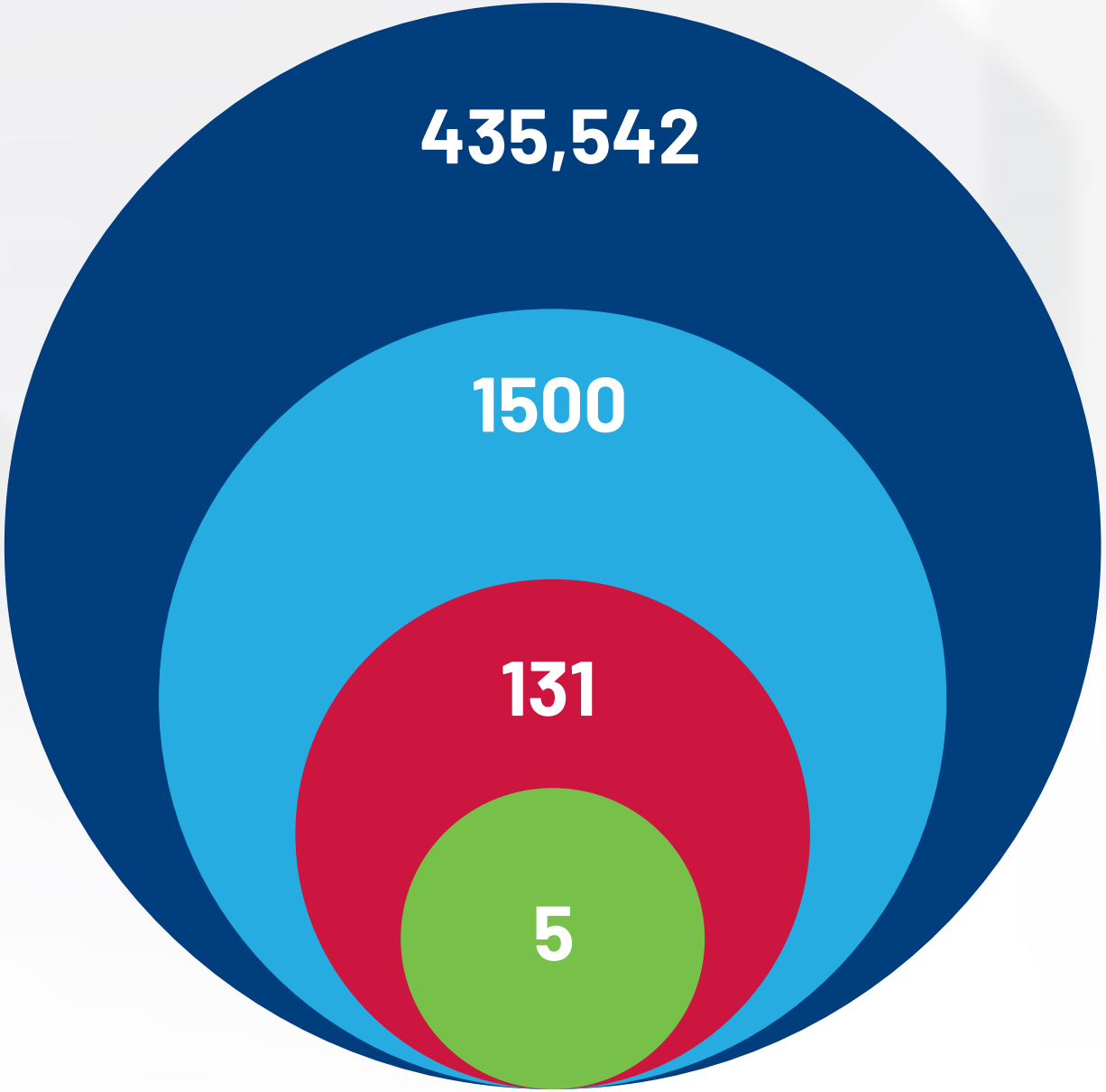
78 RA-CIRT Cases

4 Incident Responses

100% CSAT

Rockwell Automation

*Updated September 2023



Raw Security Alerts

Threat Detection platform triggers alerts when anomalies are detected within the environment

Alert Optimization

The Rockwell Automation analytics platform ingests alerts and tunes out false positives and duplicates to ensure that only actionable alerts are presented

Insights

Alerts are correlated and analyzed using the Rockwell Automation risk-based approach to determine when alerts rise to the importance of becoming an insight

Escalation to the Customer

Upon validation from a Rockwell Automation analyst that an insight requires escalation, Rockwell Automation will first attempt to resolve the Insight. If additional information is required from the customer, Rockwell Automation will escalate insight to customer with guidance on the next steps to further investigate and/or resolve the Insight

Risk Informed Cyber Strategy

This recommended approach improves risk posture with limited capital expenditure and shortened implementation timelines

✓ **Establish asset visibility**
- Conduct asset inventory analysis

✓ **Determine current risk posture**
- Conduct risk assessment
- Review and establish framework and standards

✓ **Develop base cyber hygiene program**
- Develop anti-malware strategy
- Execute physical to virtual server migrations
- Deploy anti-virus management measures
- Execute (OS) infrastructure patching services
- Create backup and recovery plan

✓ **OT network readiness**
- Conduct comprehensive assessment
- Create segmentation by design of logical network and IDMZ

This approach is a more foundational way to improve overall cybersecurity risk posture across the attack continuum with moderate capital investments and defined operational expenditures

✓ **Review comprehensive installed base**
- Hardware, software, and network
- Migrate legacy assets and networks

✓ **Deploy segmentation between IT and OT environment**
- Complete comprehensive IDMZ design and implementation
- Implement secure remote access strategy

✓ **Secure endpoints**
- Deploy endpoint security measures
- Implement modern machine and device level network

✓ **Deploy continuous threat detection**
- Deploy scalable threat detection services
- Develop and execute continuous risk management program

✓ **Monitor and management OT environment**
- Data centers, firewalls, networks, and applications 24x7x365

✓ **Create disaster recovery plan**
- Deploy and adjust disaster recovery plan

This approach outlines a comprehensive OT cyber strategy across the attack continuum providing a multi-year approach and a blueprint to all elements of a risk mitigation program. This would include detailed financial capital planning, cultural change management requirements, and workforce skills gap mitigation by providing real-time managed services

✓ **Modernize installed base**
- Migrate legacy automation hardware, software, process systems or platforms
- Migrate remaining critical physical infrastructures to full virtual environments

✓ **Modernize OT network**
- Implement detailed logical and physical network and IDMZ designs
- Deploy micro-segmentation strategy

✓ **Expand to integrated security management and administration**
- Network, firewall, data centers, applications, threat detection platforms, anti-virus and patch management

✓ **Augment workforce with security operations center**
- Integrate OT telemetry with security operations

✓ **Develop incident response handling**
- Create and deploy incident response workflows, procedures, and teams to increase speed of recovery

A NORTH AMERICAN

FOOD COMPANY

37 SITES
ENTERPRISE CONTRACT

In what areas did Rockwell Automation help?

CHALLENGES

- **Gain visibility into OT cybersecurity risks at manufacturing facilities, globally**
- **Tried a different approach with an independent consultant,** recommendation did not meet their needs
- Needed to select a proven and trusted **cybersecurity partner**

SOLUTION

- **Deployed Threat Detection Services at 37 sites**
- **Performed live monitoring** with an outsourced Security Operating Center (SOC)
- **Generated asset inventory reports** within weeks, across North America followed by global sites
- Created a **single enterprise dashboard** to view and manage risks, anomalies, and security events

BENEFITS

- **Gathered valuable data** and **aligned practices around an enterprise dashboard** as a single source of truth across the company.
- **Aligned with their corporate objectives** to have trained cybersecurity analysts monitoring their global enterprise.

GAINED VISIBILITY INTO CYBERSECURITY RISKS

CUSTOMER SUCCESS

Rockwell Automation

Questions?

100 Years
Real Life Experience

Products and Solutions for the Electrical Industry

1-800-998-1621 • www.sydist.com

Schaedler yesco