cisco Live!

#CiscoLive

The bridge to possible

Zero Trust Networking for: Industrial Environments

Realities and Opportunities

Robert Albach – Sr. Product Manager
ralbach@cisco.com

BRKIOT-2012

Cisco Webex App

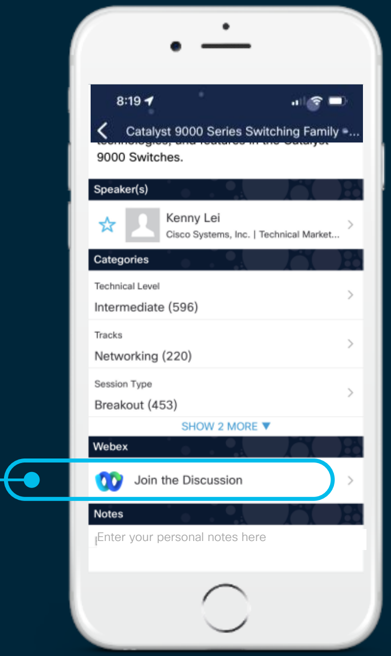
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

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

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

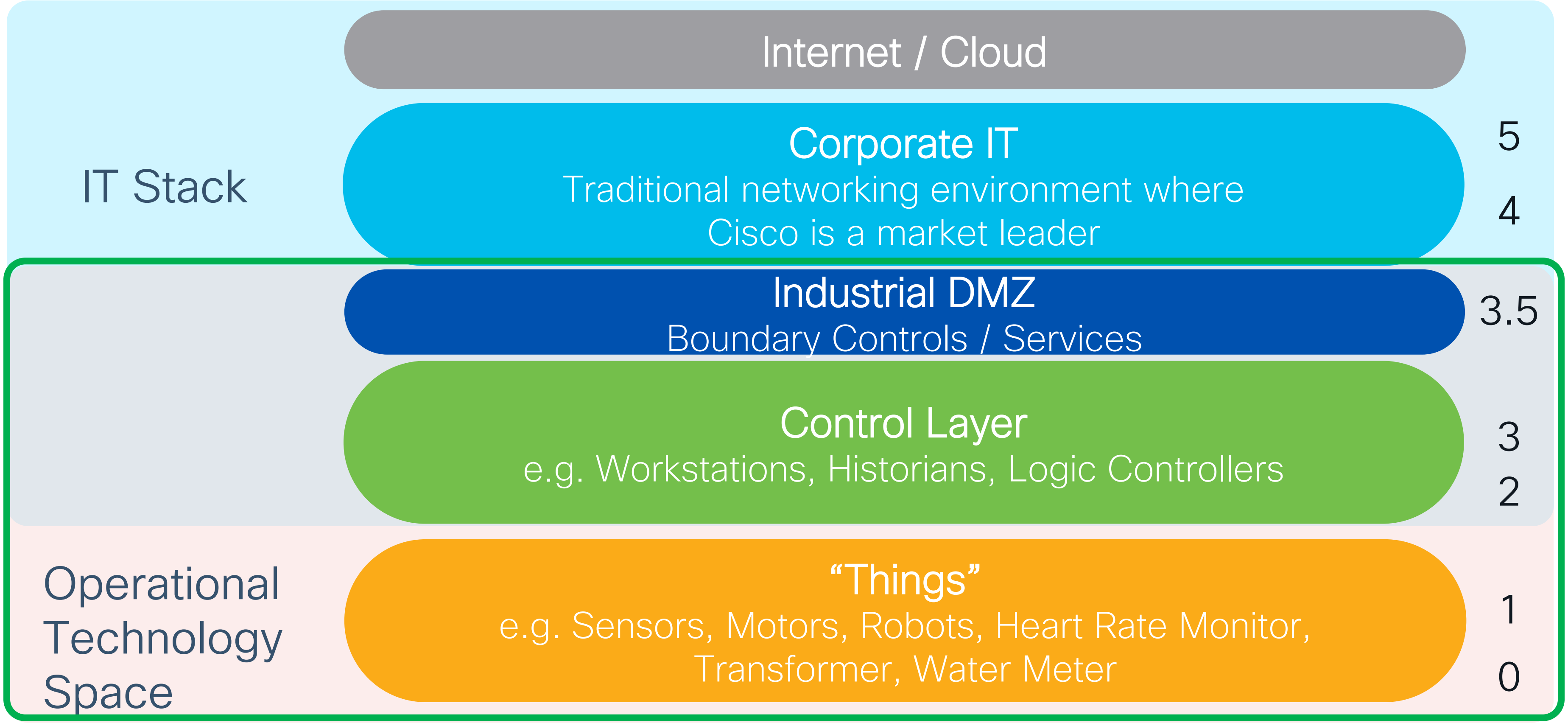
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2115

Agenda

- Industrial System Definitions
- Zero Trust – History and Definitions
- What Industrial Security Experts Say
- Progress – Slowly (But Surely?)
- What Does Work?

Industrial System Definitions

Network Layers With Purdue Model



IT Stack

Internet / Cloud

5

4

Corporate IT
Traditional networking environment where Cisco is a market leader

3.5

Industrial DMZ
Boundary Controls / Services

3

2

Control Layer
e.g. Workstations, Historians, Logic Controllers

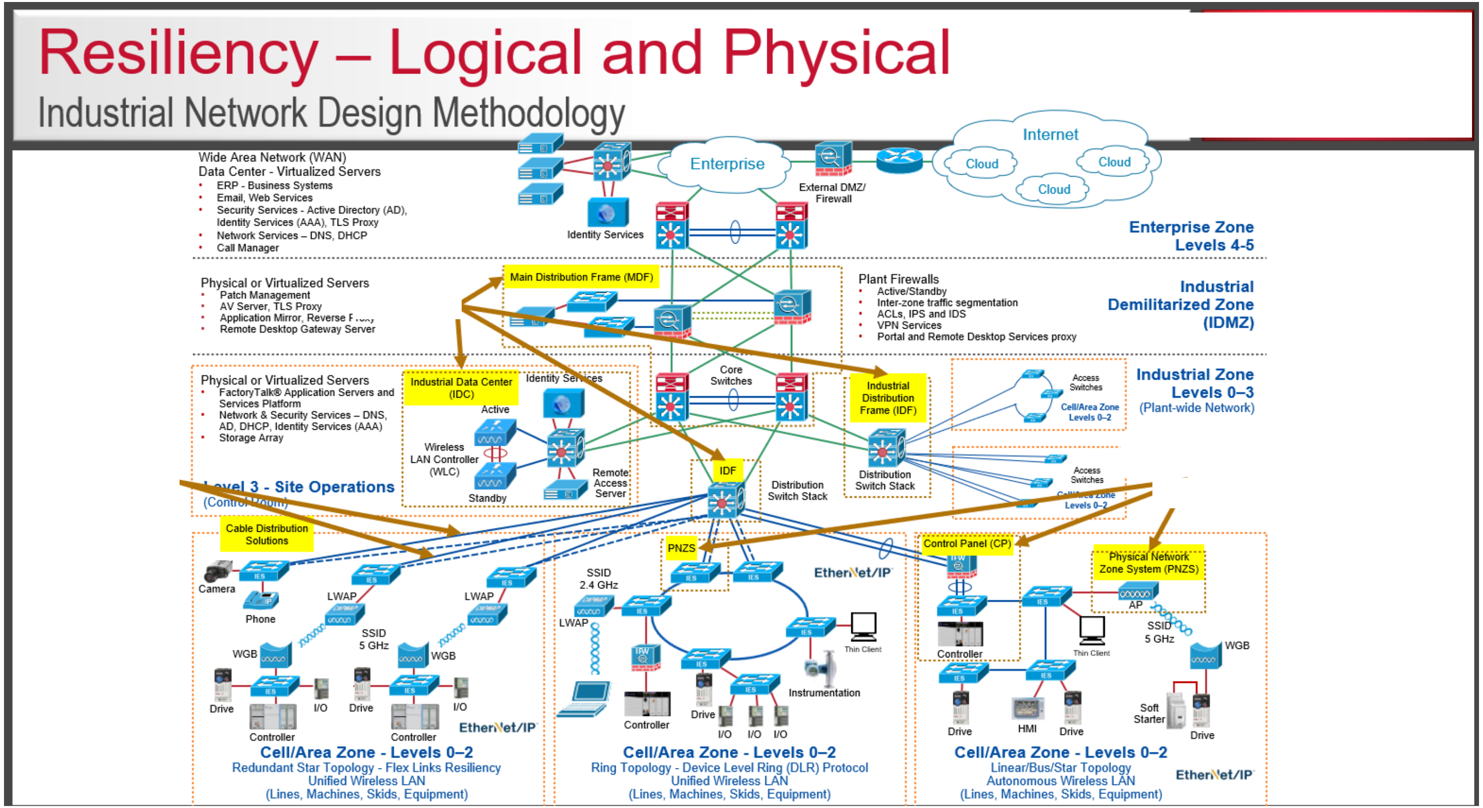
Operational Technology Space

1

0

“Things”
e.g. Sensors, Motors, Robots, Heart Rate Monitor, Transformer, Water Meter

How Many Zones And The Differentiation



Resiliency – Logical and Physical

Industrial Network Design Methodology

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

Level 3 - Site Operations
(Control Room)

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

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)

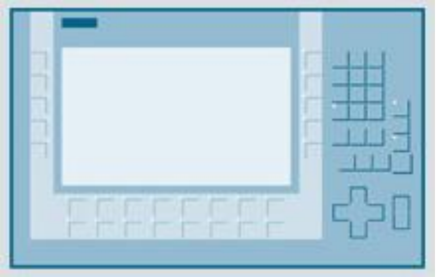
Control Loops

“Things”
e.g. Sensors, Motors, Robots, Heart Rate Monitor, Transformer, Water Meter

Controller

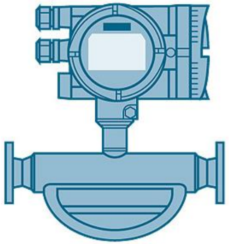
Target Pressure
6psi

Human Machine Interface (HMI)



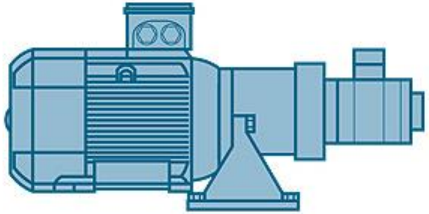
Tag
Value
5psi

Sensor

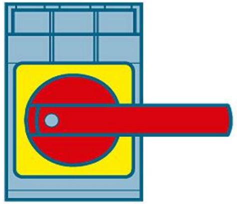


Motor
Speed
+20%

Actuator



Safety System



ISA 99 / IEC 62443 Zones and Conduits

Zones – A grouping of logical or physical assets

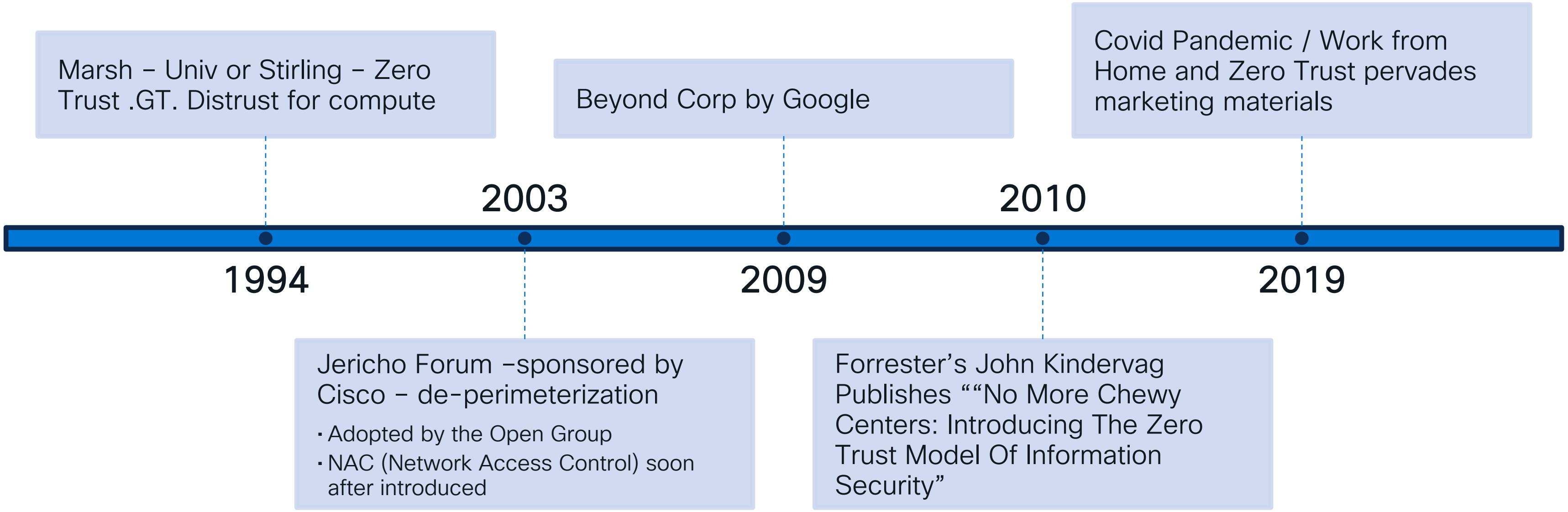
- based upon risk
- or other criteria such as:
  - criticality of assets
  - operational function
  - physical or logical location
  - required access
  - responsible organization.

Conduits – logical grouping of communication channels

- that share common security requirements
- connecting two or more zones.

Zero Trust – History and Definitions

Zero Trust – A Brief History



1994

Marsh – Univ or Stirling – Zero Trust .GT. Distrust for compute

2003

Jericho Forum –sponsored by Cisco – de-perimeterization

- Adopted by the Open Group
- NAC (Network Access Control) soon after introduced

2009

Beyond Corp by Google

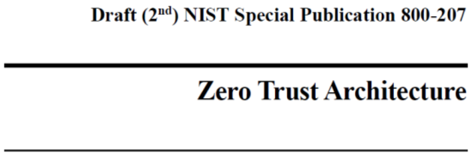
2010

Forrester's John Kindervag Publishes ""No More Chewy Centers: Introducing The Zero Trust Model Of Information Security"

2019

Covid Pandemic / Work from Home and Zero Trust pervades marketing materials

No More Perimeter Based Security

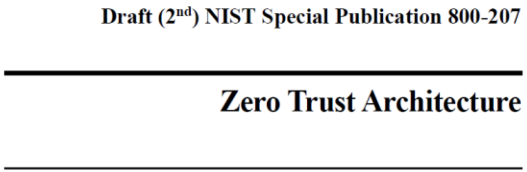


Draft (2nd) NIST Special Publication 800-207

Zero Trust Architecture

Tenets of Zero Trust

- All data sources and computing services are considered resources.
- All communication is secured *regardless of network location*.
- *Access* to individual enterprise resources is *granted on a per-session* basis.
- *Access* to resources is determined by *dynamic policy* – including the observable state of client identity, application, and the requesting asset – and may include other behavioral attributes.
- The enterprise ensures that all owned and associated *devices are in the most secure state possible* and monitors assets to ensure that they remain in the most secure state possible.
- All resource *authentication and authorization are dynamic and strictly enforced* before access is allowed.
- The *enterprise collects as much information as possible* about the current state of network infrastructure and communications and uses it to improve its security posture.



Draft (2nd) NIST Special Publication 800-207

Zero Trust Architecture

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet). Authentication and authorization (both user and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise- owned network boundary. Zero trust focus on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

What Industrial Security Experts Say

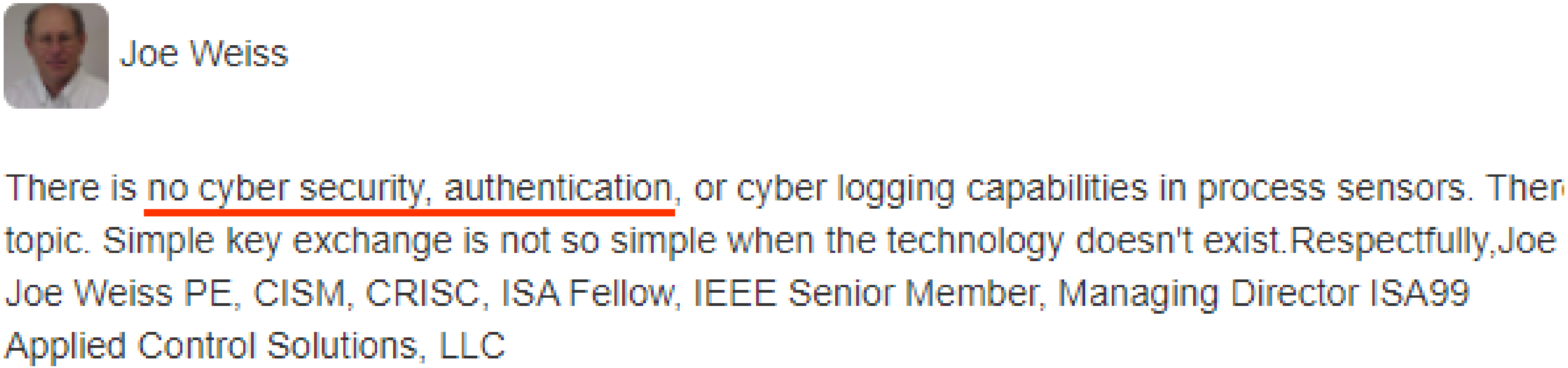
(You Should Have) Zero Trust In PLCs

Published on October 5, 2021

Dale Peterson

ICS Security Catalyst, Founder of S4 Events, Consultant, Speaker, Podcaster, Get my newsletter friday.dale-peterson.com/signup

Before we talk about zero trust, we have to realize that the most critical part of our ICS, the PLCs and controllers, almost all have a total trust or trust all security principle and adding basic authentication in these devices needs to be prioritized in your systems.



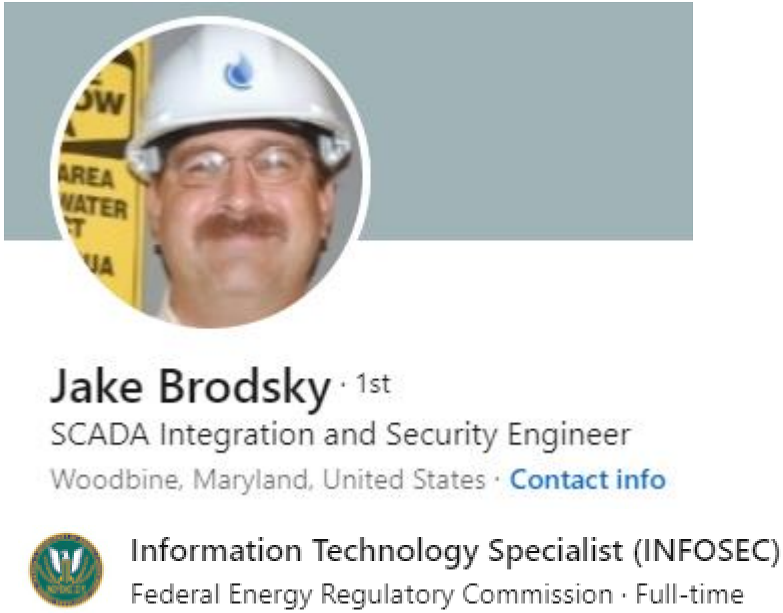
Joe Weiss

There is no cyber security, authentication, or cyber logging capabilities in process sensors. Ther

topic. Simple key exchange is not so simple when the technology doesn't exist.Respectfully,Joe

Joe Weiss PE, CISM, CRISC, ISA Fellow, IEEE Senior Member, Managing Director ISA99

Applied Control Solutions, LLC



Jake Brodsky · 1st

SCADA Integration and Security Engineer

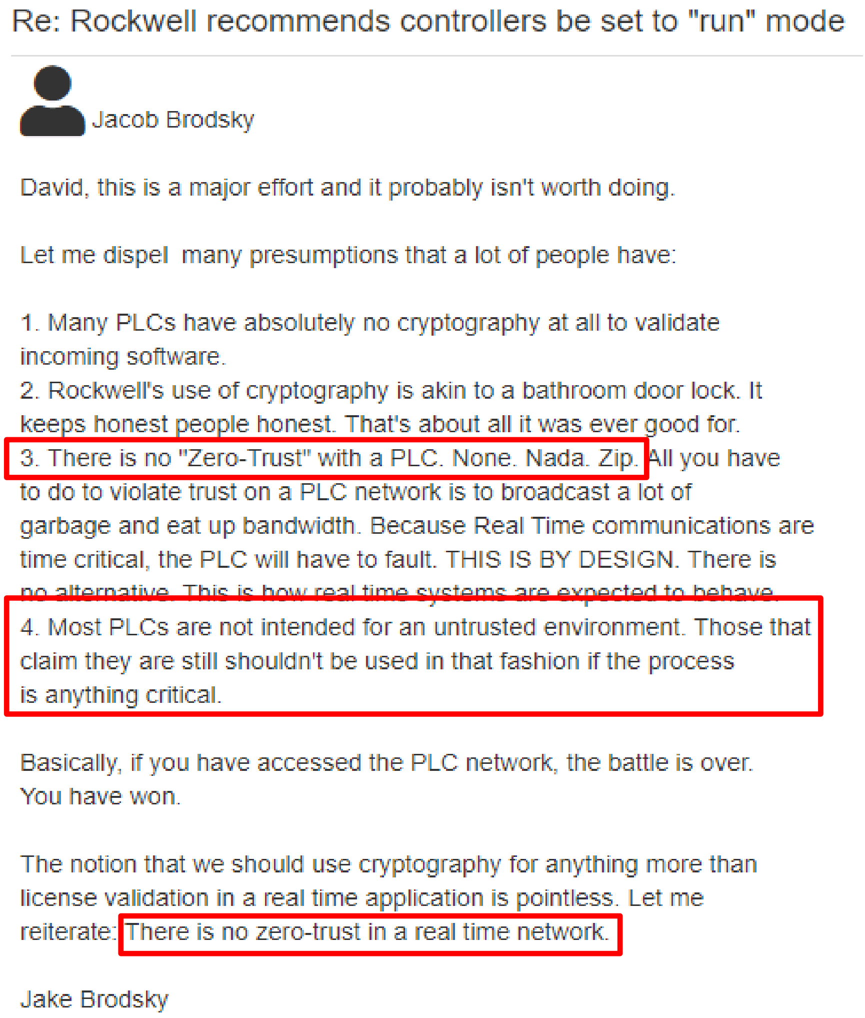
Woodbine, Maryland, United States · Contact info

Information Technology Specialist (INFOSEC)

Federal Energy Regulatory Commission · Full-time

Dale Peterson
@digitalbond

Jake Brodsky introduces the idea of PLC Secure Coding Practices at #S4x20 with some great examples. youtu.be/JtsyyTfSP1l



Re: Rockwell recommends controllers be set to "run" mode

Jacob Brodsky

David, this is a major effort and it probably isn't worth doing.

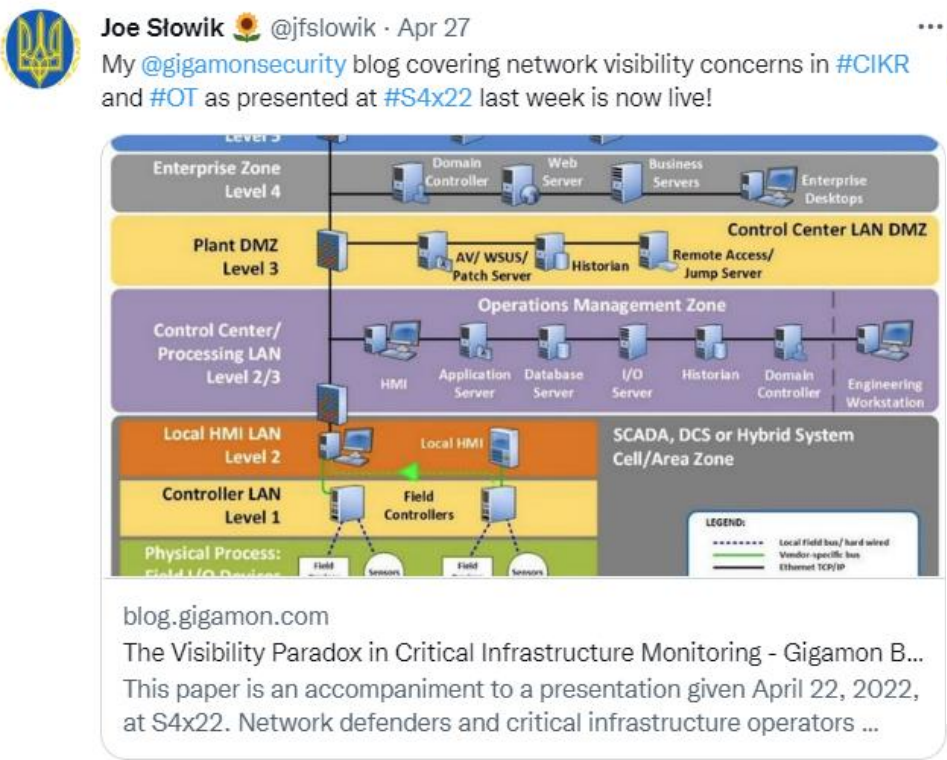
Let me dispel many presumptions that a lot of people have:

1. Many PLCs have absolutely no cryptography at all to validate incoming software.
2. Rockwell's use of cryptography is akin to a bathroom door lock. It keeps honest people honest. That's about all it was ever good for.
3. There is no "Zero-Trust" with a PLC. None. Nada. Zip. All you have to do to violate trust on a PLC network is to broadcast a lot of garbage and eat up bandwidth. Because Real Time communications are time critical, the PLC will have to fault. THIS IS BY DESIGN. There is no alternative. This is how real time systems are expected to behave.
4. Most PLCs are not intended for an untrusted environment. Those that claim they are still shouldn't be used in that fashion if the process is anything critical.

Basically, if you have accessed the PLC network, the battle is over. You have won.

The notion that we should use cryptography for anything more than license validation in a real time application is pointless. Let me reiterate: There is no zero-trust in a real time network.

Jake Brodsky



Joe Słowik 🌻 @jfslowik · Apr 27

My @gigamonsecurity blog covering network visibility concerns in #CIKR and #OT as presented at #S4x22 last week is now live!

blog.gigamon.com

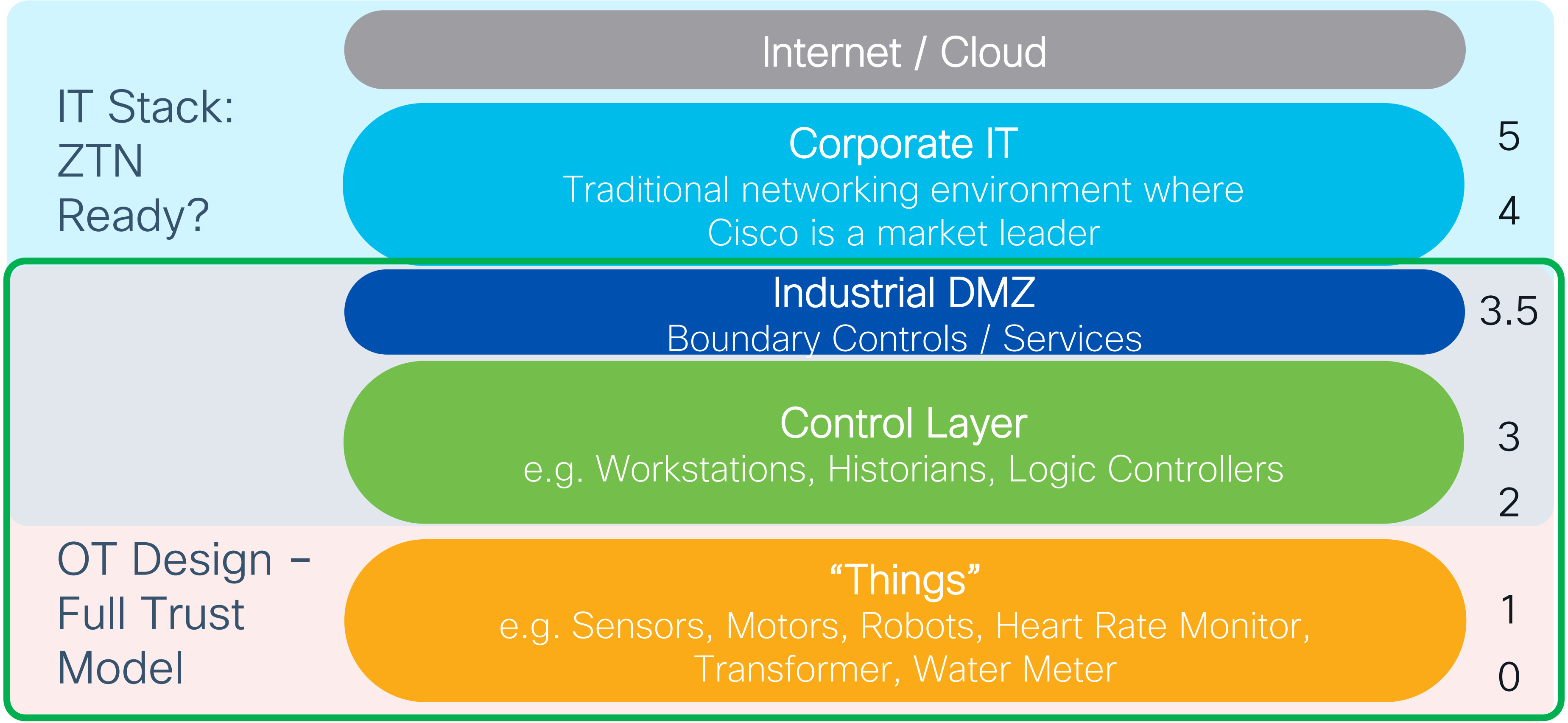
The Visibility Paradox in Critical Infrastructure Monitoring - Gigamon B...

This paper is an accompaniment to a presentation given April 22, 2022, at S4x22. Network defenders and critical infrastructure operators ...

Joe Słowik 🌻 @jfslowik · Apr 27

Progress – Slowly (But Surely?)

Zero Trust Readiness With Purdue Model



IT Stack: ZTN Ready?

Internet / Cloud

Corporate IT

Traditional networking environment where Cisco is a market leader

5

4

Industrial DMZ

Boundary Controls / Services

3.5

Control Layer

e.g. Workstations, Historians, Logic Controllers

3

2

OT Design – Full Trust Model

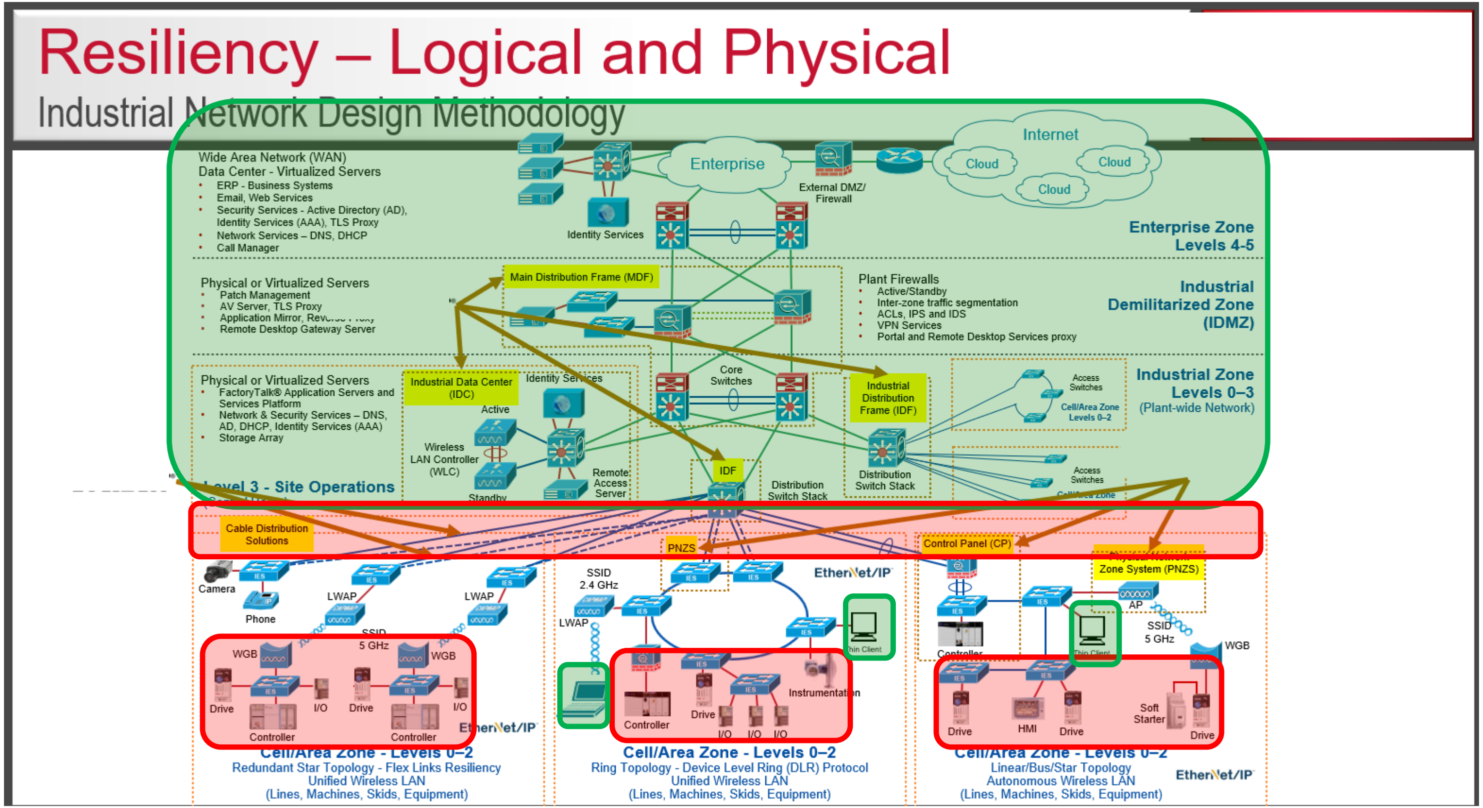
“Things”

e.g. Sensors, Motors, Robots, Heart Rate Monitor, Transformer, Water Meter

1

0

Assets and Their Zero Trust Readiness



Resiliency – Logical and Physical

Industrial Network Design Methodology

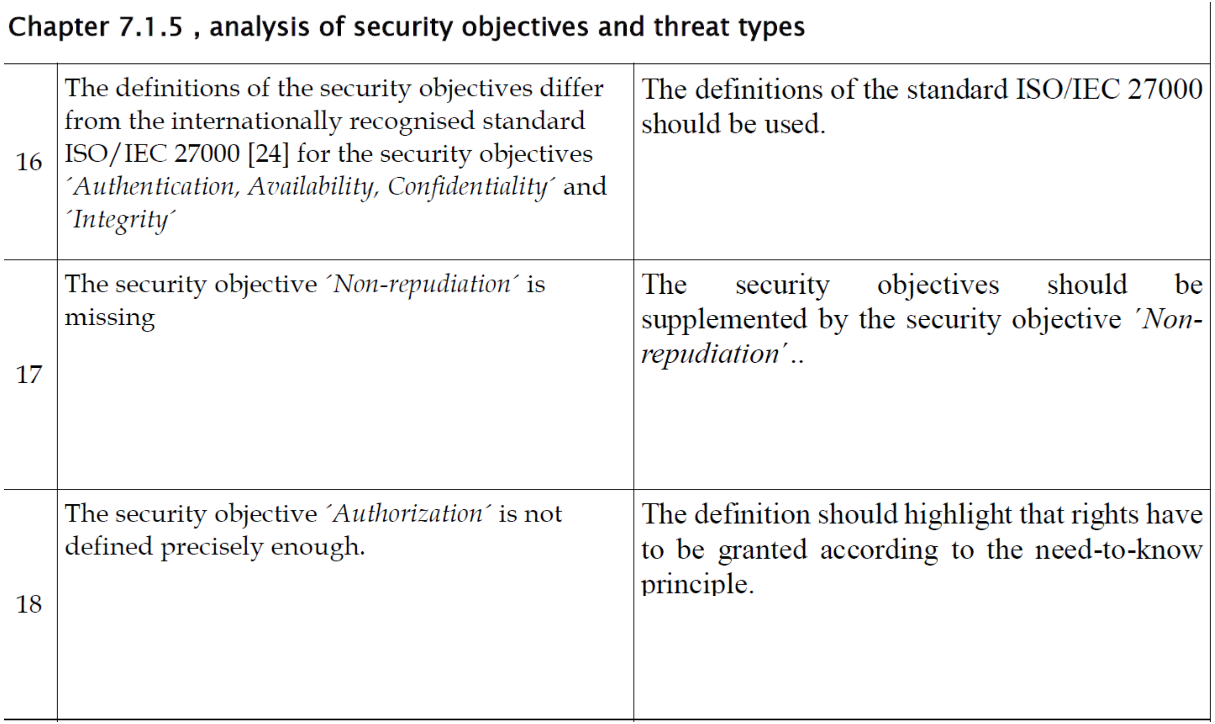
Wide Area Network (WAN)
Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server
Main Distribution Frame (MDF)
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
Industrial Data Center (IDC)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
Industrial Distribution Frame (IDF)
IDF
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)
Level 3 - Site Operations
Cable Distribution Solutions
PNZS
Control Panel (CP)
Physical Network Zone System (PNZS)
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
EtherNet/IP
Thin Client
Controller
Drive
Instrumentation
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)
Controller
AP
SSID 5 GHz
WGB
Thin Client
Drive
HMI
Drive
Soft Starter
Drive
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP

OPC Standard – Needs for Improvement

Bundesamt
für Sicherheit in der
Informationstechnik

OPC UA Security Analysis

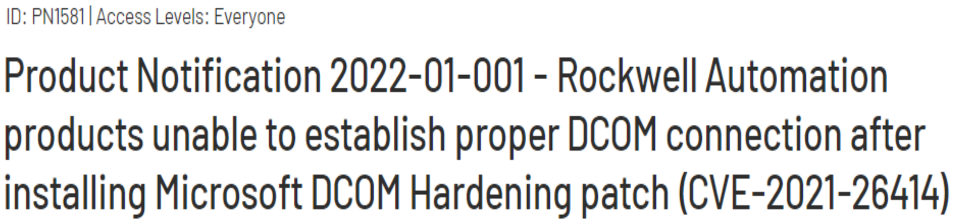
02/03/2017



Chapter 7.1.5 , analysis of security objectives and threat types

16	The definitions of the security objectives differ from the internationally recognised standard ISO/IEC 27000 [24] for the security objectives *´Authentication, Availability, Confidentiality´* and *´Integrity´*	The definitions of the standard ISO/IEC 27000 should be used.
17	The security objective *´Non-repudiation´* is missing	The security objectives should be supplemented by the security objective *´Non-repudiation´*..
18	The security objective *´Authorization´* is not defined precisely enough.	The definition should highlight that rights have to be granted according to the need-to-know principle.

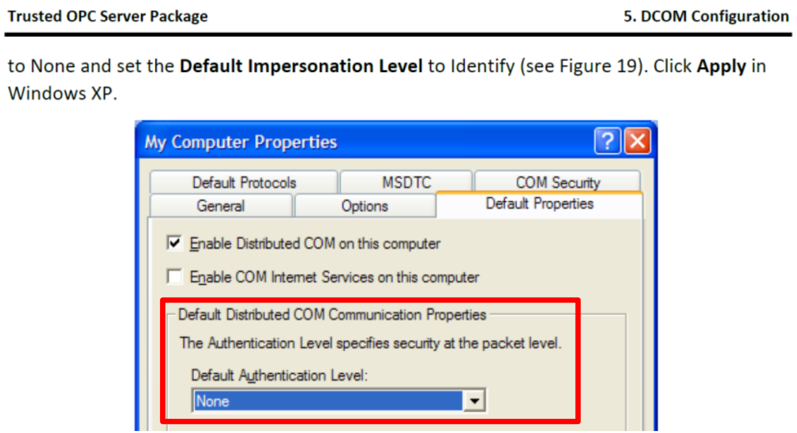
Factory Talk and DCOM Authentication



ID: PN1581 | Access Levels: Everyone

Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (CVE-2021-26414)

The Microsoft patch addresses a vulnerability in DCOM. The Microsoft patch increases the minimum authentication level used when establishing DCOM connections. The affected Rockwell Automation products use FactoryTalk® Services Platform, FactoryTalk® Live Data, OPC-DA, or are using Windows® APIs to establish DCOM connections between two computers.



Trusted OPC Server Package — 5. DCOM Configuration

to None and set the **Default Impersonation Level** to Identify (see Figure 19). Click **Apply** in Windows XP.

My Computer Properties

☑ Enable Distributed COM on this computer

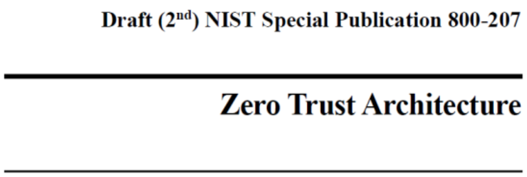
□ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

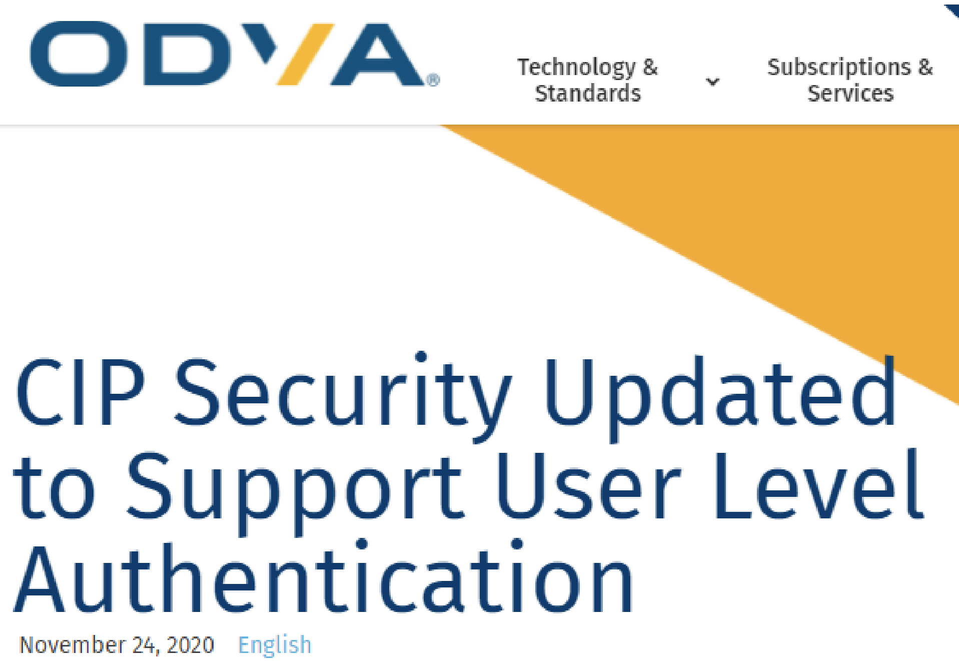
Default Authentication Level: None

Automation Industry Standards Readiness



Draft (2nd) NIST Special Publication 800-207

Zero Trust Architecture



ODVA

Technology & Standards

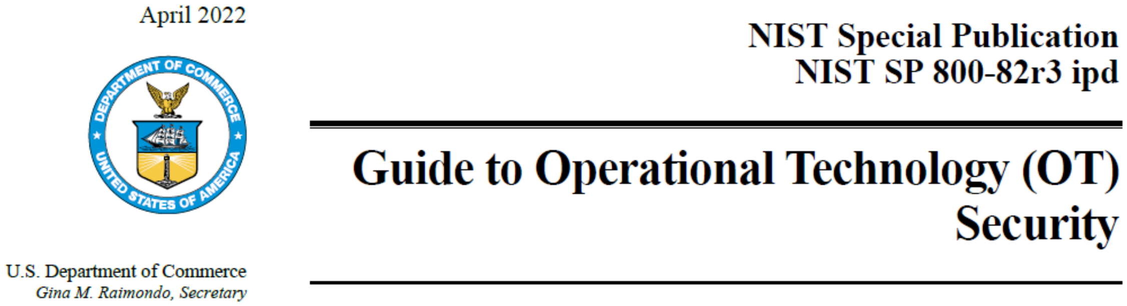
Subscriptions & Services

CIP Security Updated to Support User Level Authentication

November 24, 2020 English

- All resource *authentication and authorization are dynamic and strictly enforced* before access is allowed.

What Does Work?



April 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

NIST Special Publication
NIST SP 800-82r3 ipd

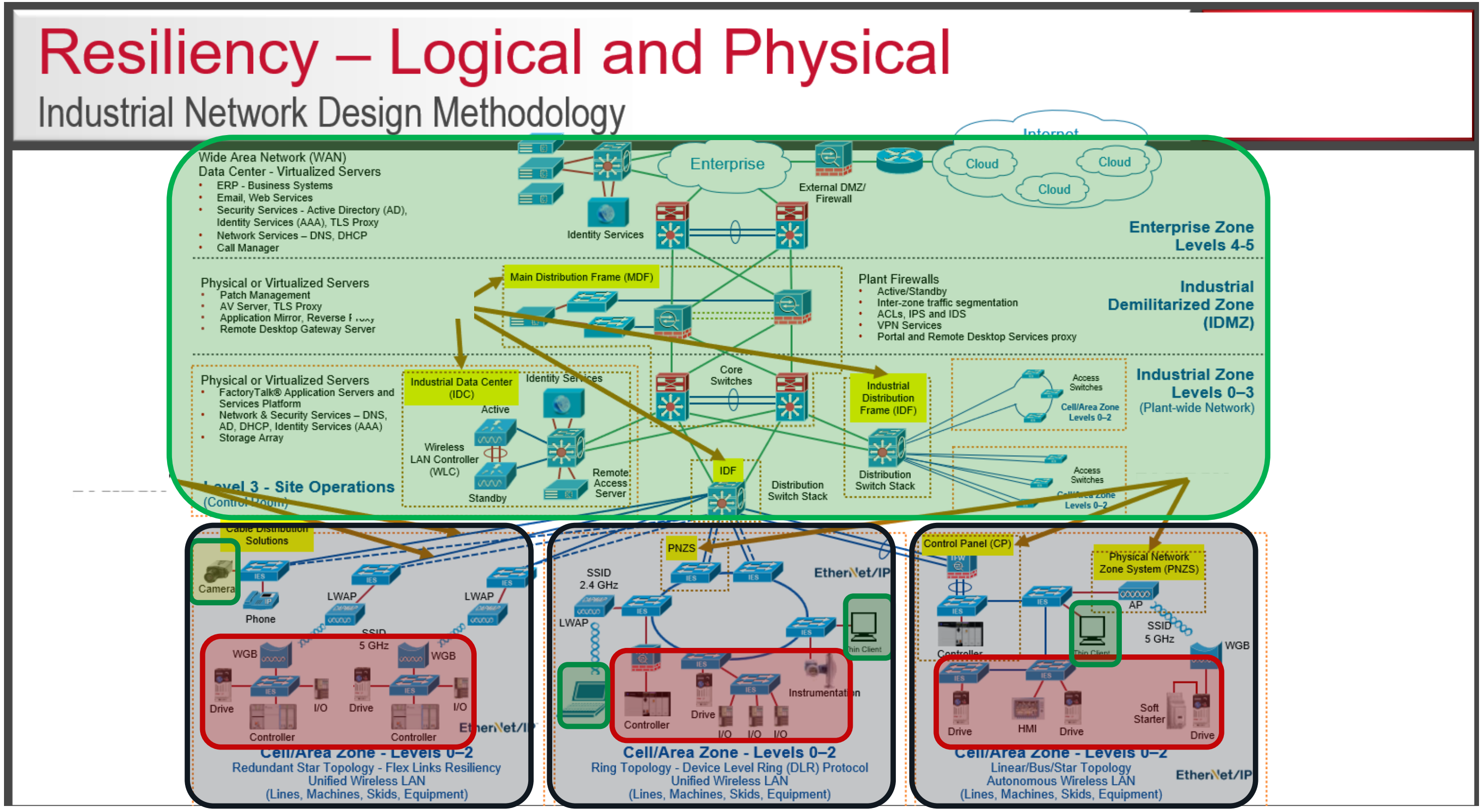
Guide to Operational Technology (OT) Security

OT-Specific Guidance and Recommendations

Some OT components (e.g., PLCs, Controllers, HMI) may not support the technologies or protocols required to fully integrate with a ZTA implementation. As a result, a ZTA implementation might not be practical for some OT devices. Instead, organizations should consider applying ZTA on compatible devices such as those typically found at the functionally higher levels of the OT architecture (e.g., Purdue Model Levels 3, 4, 5, and the OT DMZ).

Organizations may also want to consider the impact on operations and safety function. For example, would any adverse impacts occur if the ZTA solution increases the latency to respond to resource requests or if one or more ZTA components become unavailable? Based on this analysis, organizations should consider adjusting the ZTA implementations to minimize latency and ensure adequate redundancy to minimize risks to OT and safety operations….

How To Progress: Zones of Zero Trust Readiness



Resiliency – Logical and Physical

Industrial Network Design Methodology

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

Physical or Virtualized Servers

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

Plant Firewalls

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

Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Identity Services
Enterprise Zone Levels 4-5
Main Distribution Frame (MDF)
Industrial Demilitarized Zone (IDMZ)
Industrial Data Center (IDC)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
Industrial Distribution Frame (IDF)
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3 (Plant-wide Network)
IDF
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Level 3 - Site Operations (Control Room)
Cable Distribution Solutions
Camera
IES
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)
PNZS
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)
Control Panel (CP)
IFW
Physical Network Zone System (PNZS)
AP
SSID 5 GHz
WGB
Controller
Thin Client
Drive
HMI
Drive
Soft Starter
Drive
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP

How To: Move Down from Enterprise Zone

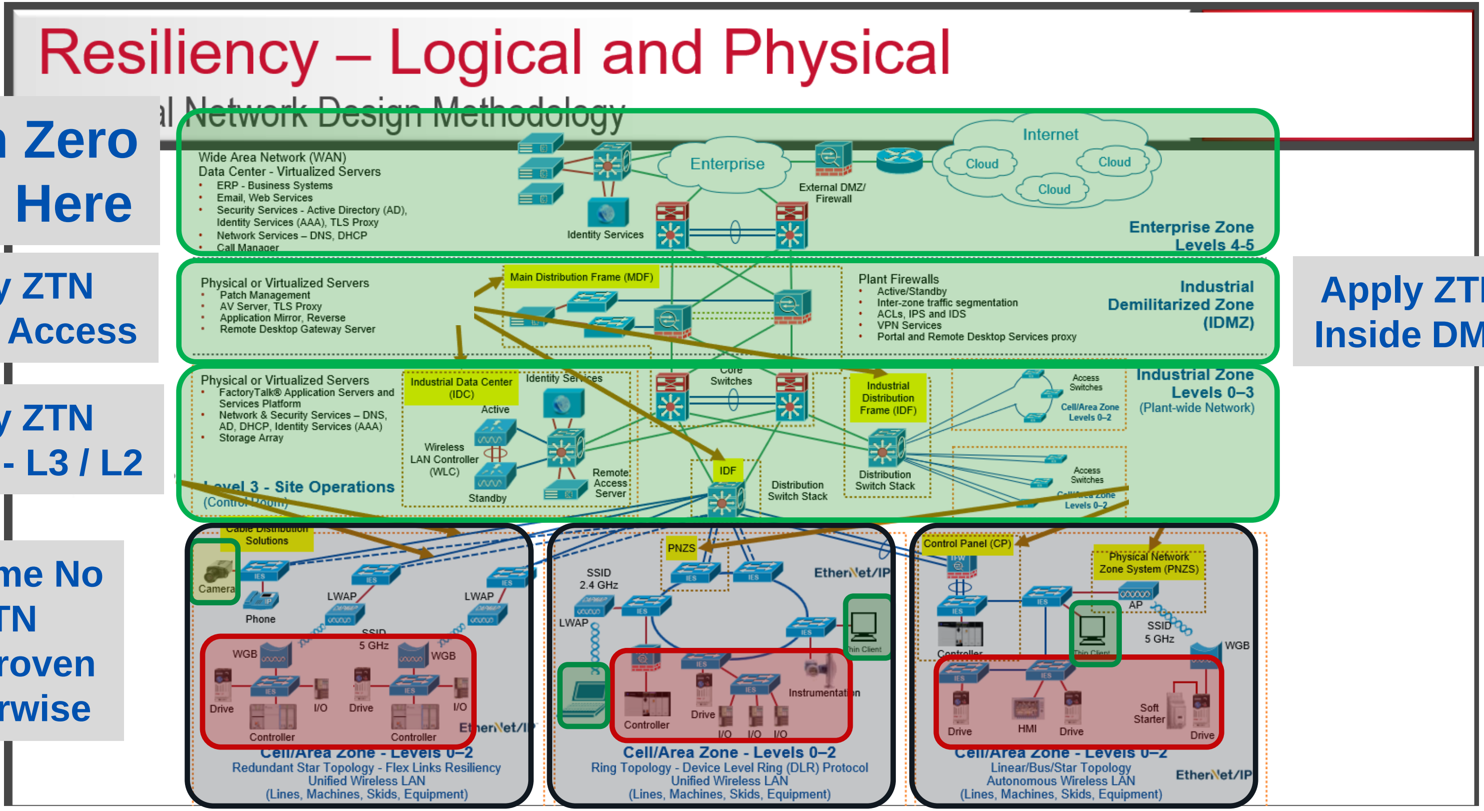
Learn Zero Trust Here

Apply ZTN To DMZ Access

Apply ZTN To Intra - L3 / L2

Assume No ZTN Till Proven Otherwise

Apply ZTN Inside DMZ



Resiliency – Logical and Physical

al Network Design Methodology

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
- 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

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)

Enterprise
Identity Services
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Main Distribution Frame (MDF)
Industrial Demilitarized Zone (IDMZ)
Industrial Data Center (IDC)
Identity Services
Active
Standby
Wireless LAN Controller (WLC)
Remote Access Server
Core Switches
Industrial Distribution Frame (IDF)
IDF
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)
Cable Distribution Solutions
Camera
Phone
IES
LWAP
LWAP
SSID 5 GHz
WGB
WGB
Drive
Drive
I/O
I/O
Controller
Controller
EtherNet/IP
PNZS
SSID 2.4 GHz
LWAP
EtherNet/IP
Thin Client
Controller
Drive
Instrumentation
I/O
I/O
I/O
Control Panel (CP)
IFW
Controller
Physical Network Zone System (PNZS)
AP
Thin Client
SSID 5 GHz
WGB
Drive
HMI
Drive
Soft Starter
Drive
EtherNet/IP

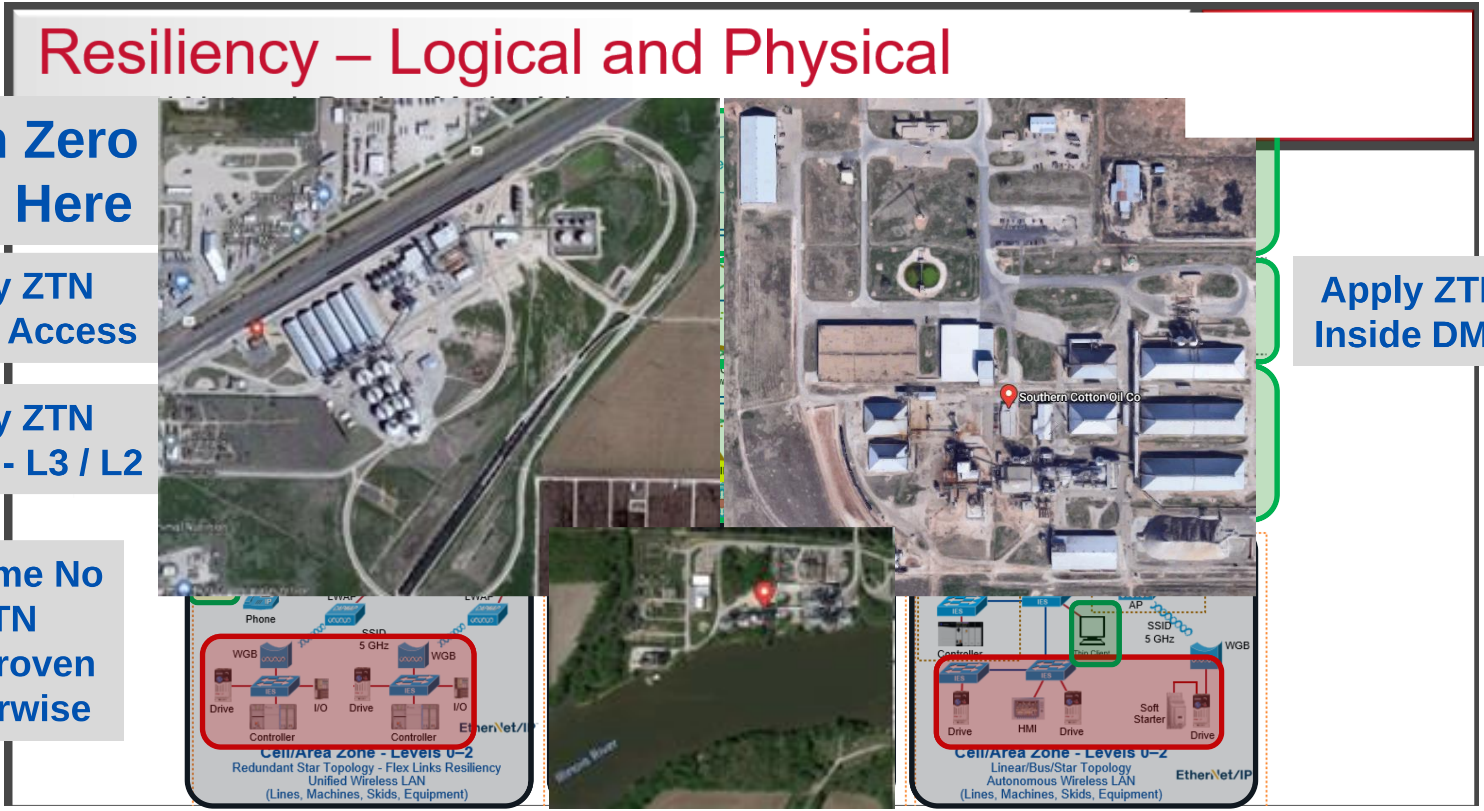
Mapping to Your Sites: Operations + Sales

Learn Zero Trust Here

Apply ZTN To DMZ Access

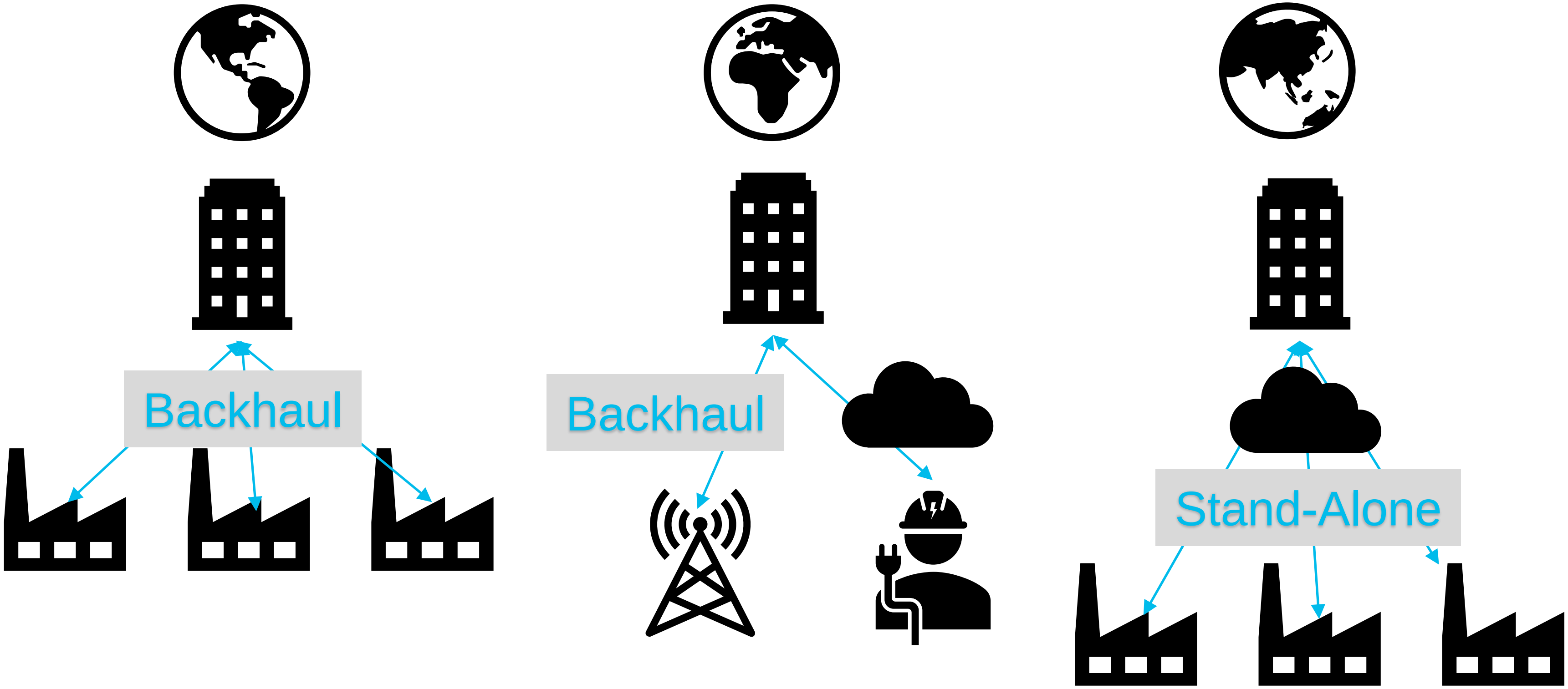
Apply ZTN To Intra - L3 / L2

Assume No ZTN Till Proven Otherwise

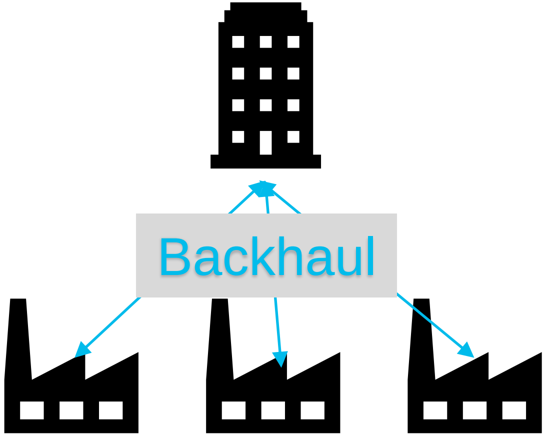


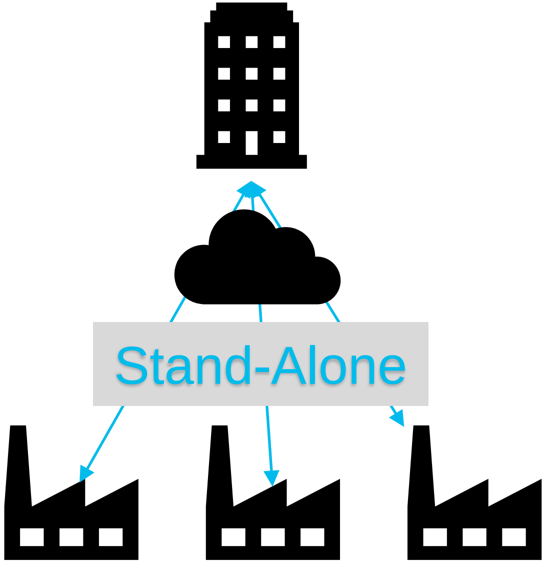
Apply ZTN Inside DMZ

Zero Trust Across Distributed Sites?



WAN Design Impacts on Zero Trust Decisions

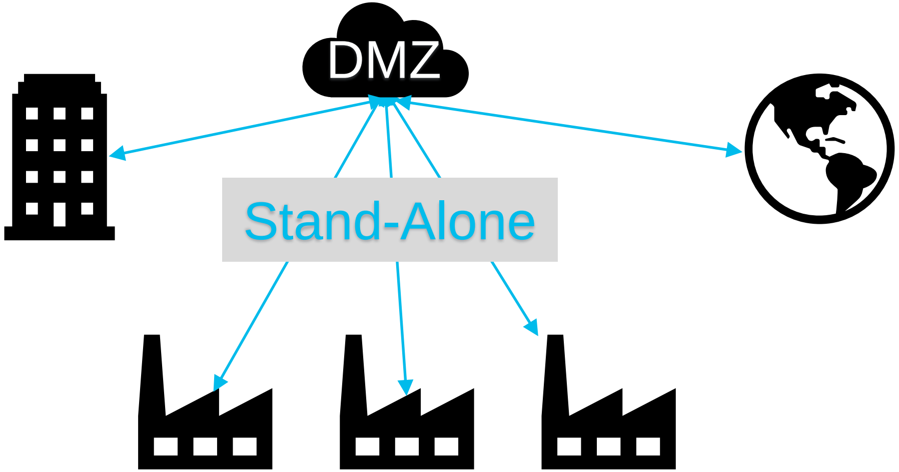




Centralized internet access
More expensive comms

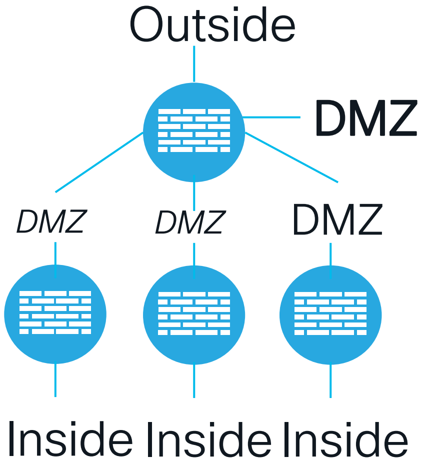
Multiple internet interfaces
Less expensive comms

Alternate Architectures –



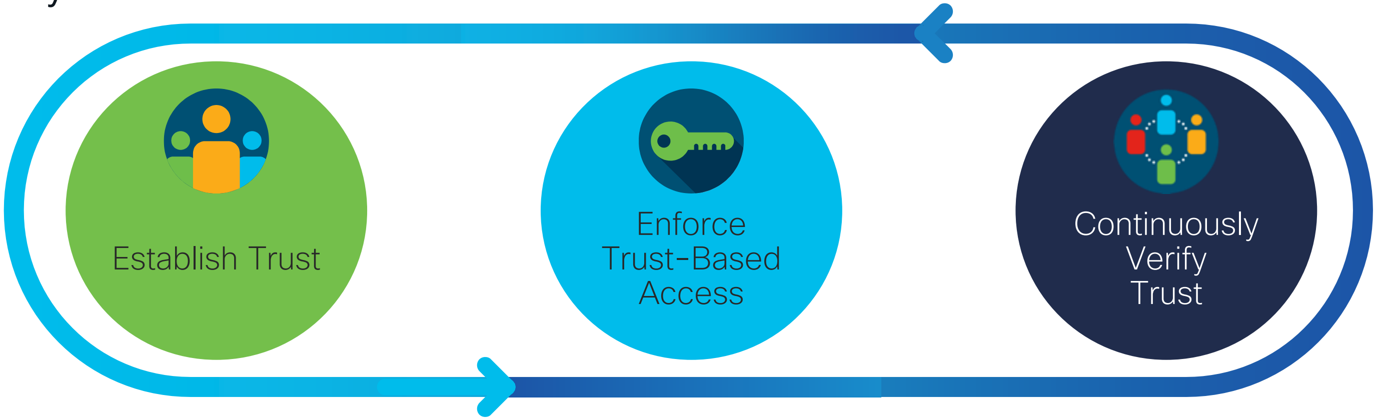
Multiple internet interfaces
Less expensive comms

Regional
Multi-Site



How Does Cisco Zero Trust Work?

3 Step Cyclical Process



Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

We establish trust by verifying:

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise

We enforce access to:

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins
- ✓ Users, Devices and Things

We continuously verify:

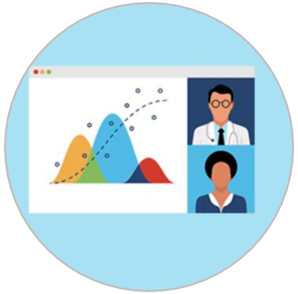
- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

Cisco Zero Trust

A comprehensive approach to securing all access across your networks, applications, and environment.

Workforce

Ensure only the **right users** and **secure devices** can access applications



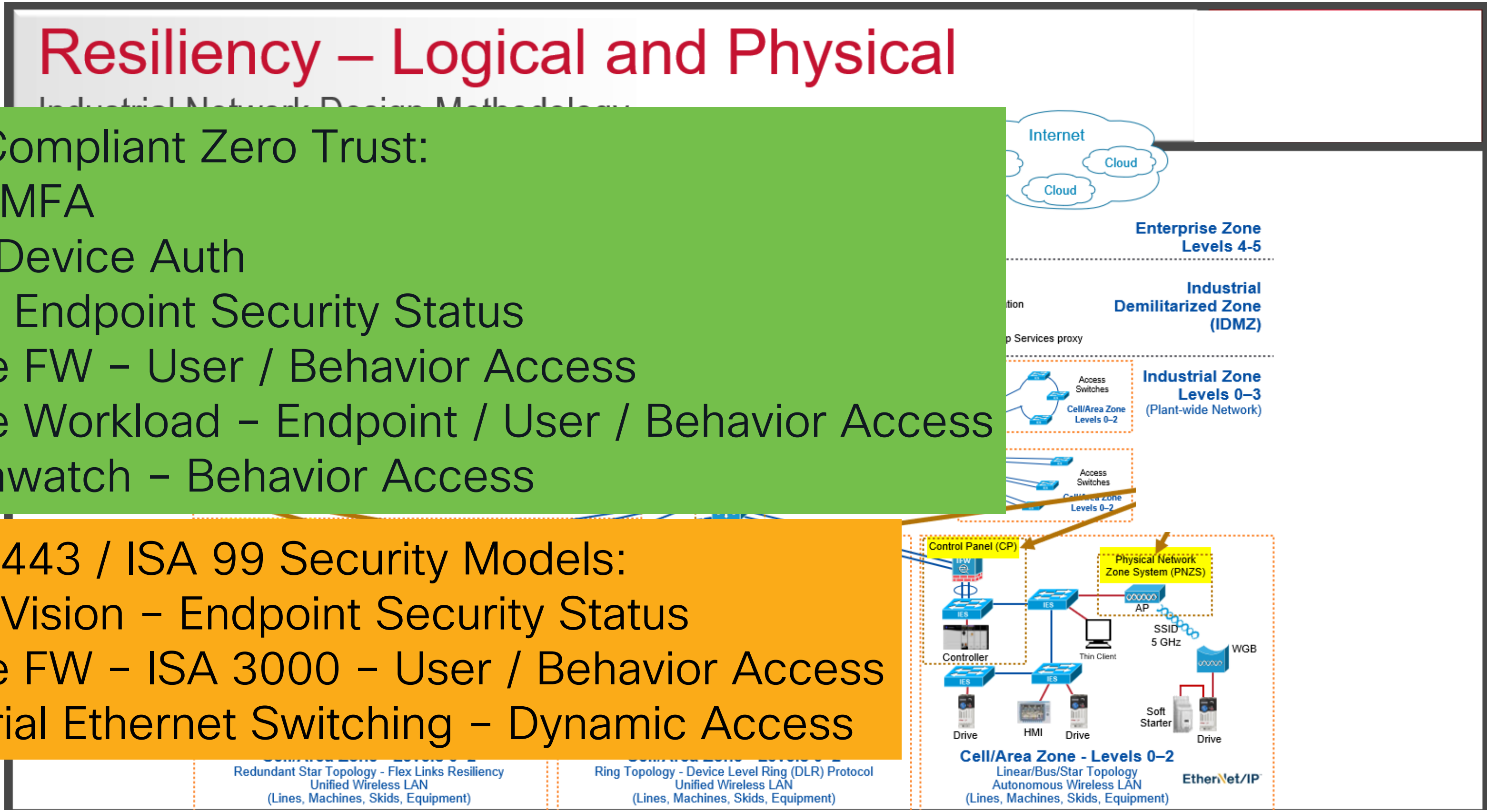
Workloads

Secure all connections within your **apps,** across multi-cloud

Workplace

Secure **user** and **device connections across your network**, with Some exceptions….

Application of Security Models that Fit



Resiliency – Logical and Physical

Industrial Network Design Methodology

NIST Compliant Zero Trust:
Duo – MFA
ISE - Device Auth
AMP – Endpoint Security Status
Secure FW – User / Behavior Access
Secure Workload – Endpoint / User / Behavior Access
Stealthwatch – Behavior Access

IEC 62443 / ISA 99 Security Models:
Cyber Vision – Endpoint Security Status
Secure FW – ISA 3000 – User / Behavior Access
Industrial Ethernet Switching – Dynamic Access

Cisco Zero Trust / 62443 Customer Security Profile

	Establish Trust	Enforce Trust-Based Access	Continuously Verify Trust
Workload – Data Center	• Tetration – Application Dependency Mapping • ACI – Group Based Policy	• ACI – Enforcement • Tetration – Enforcement	• Tetration – Visibility/Behavioral • ACI – Network Assurance Engine
Workplace – Industrial Zones	• ISE – User/Device Authentication • ISE/DNAC – Device Classification/Profiling	• SGT – User/Device Mapping Segmentation • Software Defined Access (SDA) • Secure FireWall (ISA 3000)	• Cyber Vision / StealthWatch – Anomaly Detection • ISE/DNAC – Device Classification/Profiling
Workforce – Users	• Duo – MFA • Duo – Device Insights	• Duo – Adaptive Policies	• Duo – Unified Device Visibility

Extended Protection

- Umbrella
- AnyConnect
- Next-Generation Firewall
- Cisco Secure X
- WSA
- SD-WAN

Summary:

- Zero Touch should be more than a marketing message –
  follow the standards – they exist for a reason.
- If the network and assets look like an IT stack then zero touch *might* work.
- Below layer 3 the required infrastructure is not ready – don’t confuse network placement as good enough.
- You can advance but do it with a plan.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

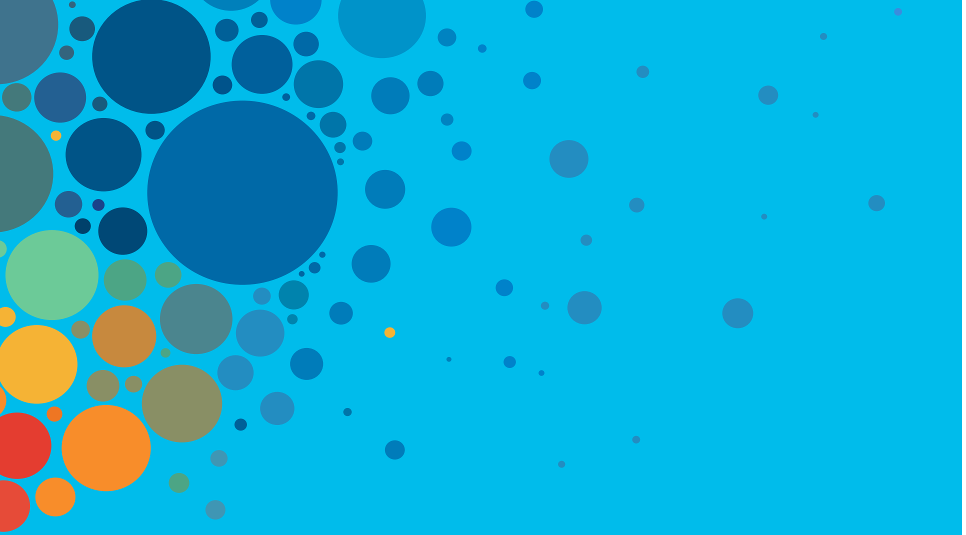
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

CISCO Live!

#CiscoLive