

Hernán Lovera
Jefe de productos
Industrial IoT



**Rockwell
Automation**

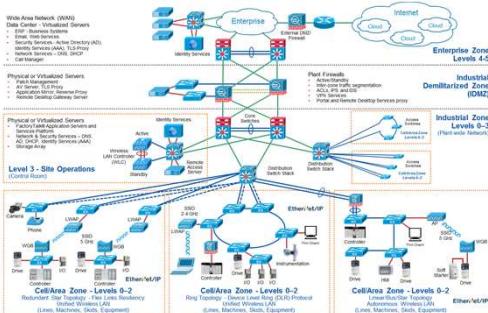


Desafíos de redes convergentes IT/OT & Ciberseguridad industrial



The Connected Enterprise

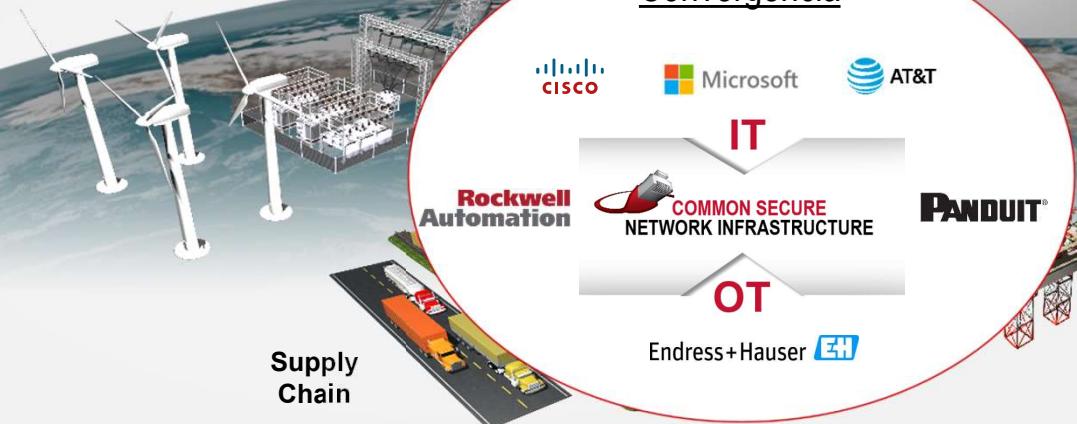
Arquitecturas conectadas



Estándares industriales



Smart Grid



Industria



Amenazas de seguridad cibernetica

Tipos de Amenazas

Malware DDoS

Spyware Phishing

Ransomware

Actores

Internal

Hackers State

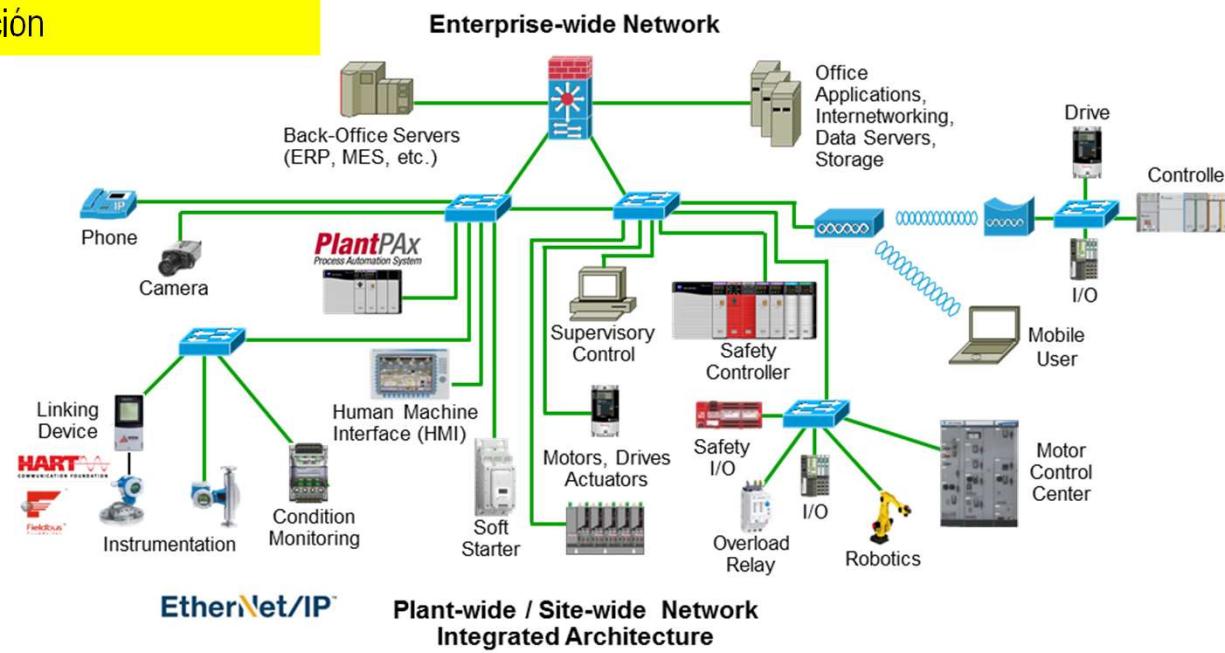
Criminal

Distribution Center

Rockwell Automation

Arquitecturas convergentes: ¿Cual es la situación que afrontamos?

LAN grande, carente de límites naturales y de segmentación



Plana, abierta y no poseen capacidad de recuperarse



Arquitecturas convergentes: ¿Cual es la situación que afrontamos?

Ethernet industrial en toda la planta:

- **Única tecnología de red para el sistema de control, automatización industrial (IACS) y las disciplinas de información, por ejemplo: scada, drives, safety y motion**

Diferentes requisitos:

- Rendimiento,
- Flexibilidad,
- Disponibilidad,

Otras cuestiones:

- **IACS Abierto por defecto** - debe ser protegido por diseño, arquitectura y configuración
- Soluciones de networking no preparadas para garantizar operatividad de planta. (**Equipos nos admisibles**)
- **Los clientes deben invertir en sus propios laboratorios de pruebas** para validar la tecnología y los productos para cumplir con los requisitos de sus aplicaciones

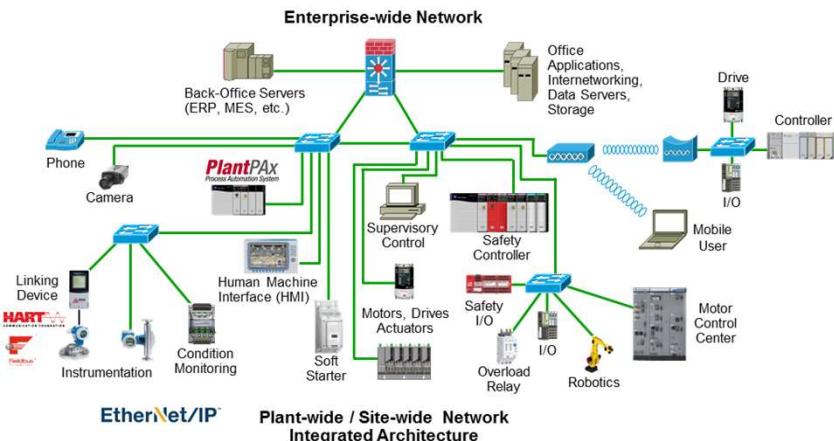
Migración de LAN aisladas, a grandes LAN planas y abiertas:

- Pérdida de fronteras y segmentación natural.
- Expansión de la red - **falta de disciplina en el diseño**



Arquitecturas convergentes: El camino a seguir...

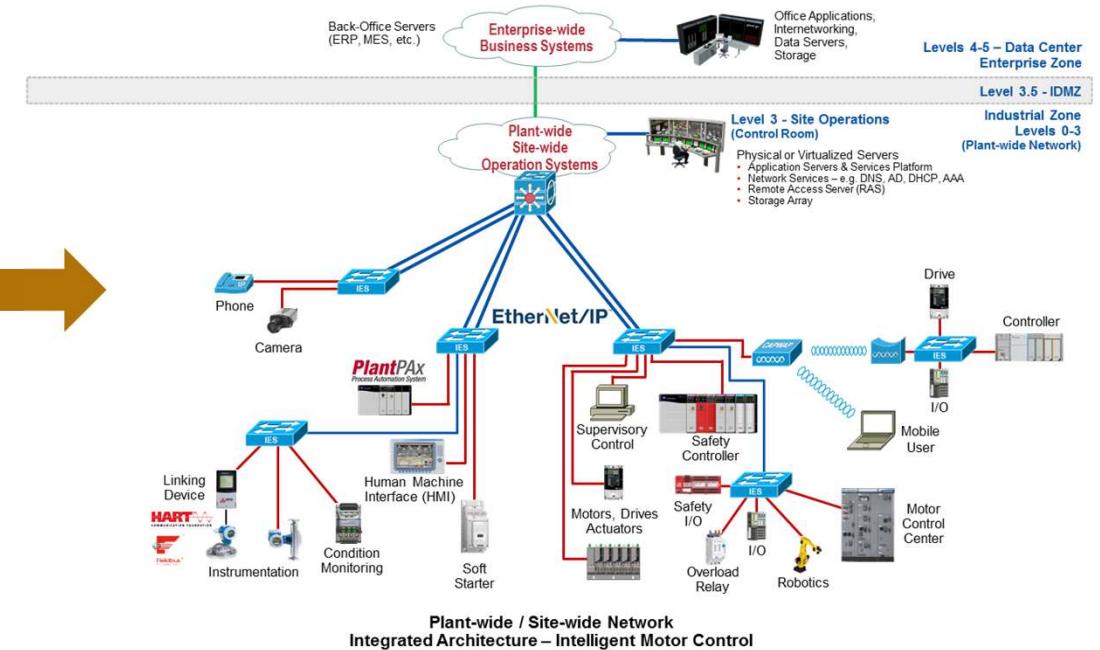
LAN grande, carente de límites naturales y de segmentación



Flat, Open and Non-Resilient
IACS Network Infrastructure

Plana, abierta y no poseen capacidad de recuperarse

Redes LAN pequeñas e interconectadas, con límites claros bien definidos



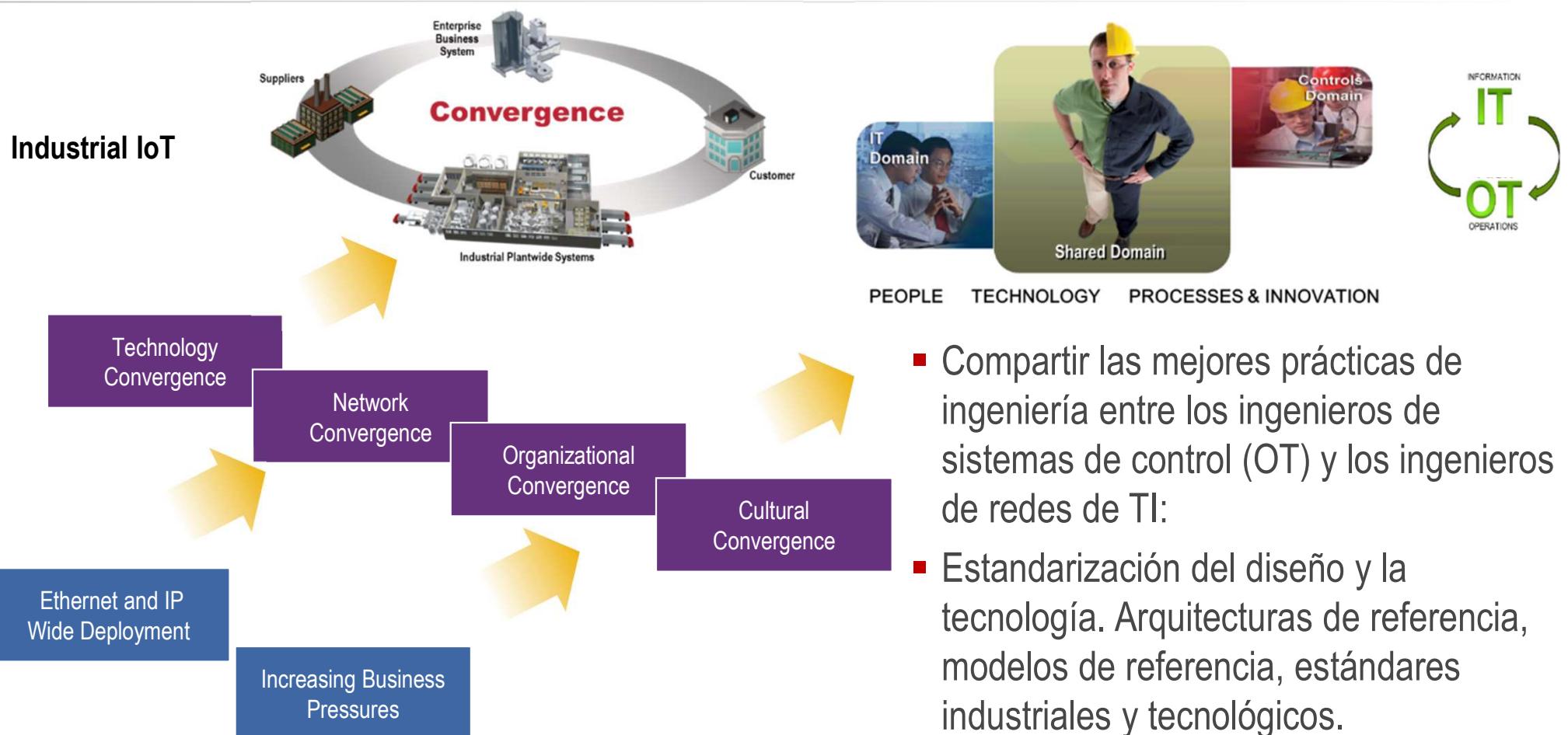
Estructurada y robusta



Convergencia,
Tecnológica y Cultural



Arquitecturas convergentes: OT – IT colaboración,



Arquitecturas convergentes: Tecnologías y culturas – Similares pero diferentes

Criterio	Industrial OT Network	Enterprise IT Network
Entorno	<ul style="list-style-type: none"> • Piso de planta • Sala de control • Tablero de Control, Industrial Distribution Frame (IDF) 	<ul style="list-style-type: none"> • Data Center • Data Communication, • Intermediate Distribution Frame (IDF)
Switches	<ul style="list-style-type: none"> • Administrable, No administrable • Capa 2 • Riel DIN 	<ul style="list-style-type: none"> • Administrable • Capa 2 y Capa 3 • Montaje 19"
Wireless	<ul style="list-style-type: none"> • Administración local • Equipamiento móvil. Sistemas inaccesible. Mantenimiento. 	<ul style="list-style-type: none"> • Administración centralizada • Acceso corporativo y a invitados – Internet.
Informática	<ul style="list-style-type: none"> • Computadoras y paneles de monitoreo robustos (HMIs) • Desktop, Notebook • 19" Rack Servers • Sistemas operativos obsoletos • Virtualización - cada vez más frecuente. • Hardening –actualizaciones solo paradas de planta 	<ul style="list-style-type: none"> • Desktop, Notebook, Tablets, Celulares. • 19" Rack Servers • Sistemas operativos actuales • Virtualización • Hardening – actualizaciones automáticas



Arquitecturas convergentes: Tecnologías y culturas – Similares pero diferentes

Criterio	Industrial OT Network	Enterprise IT Network
Tecnología de redes	<ul style="list-style-type: none"> IEEE 802.3 Ethernet estándar y versiones propietarias (no estándar) Protocolo estándar de Internet IETF (IPv4) y alternativas propietarias (no estándar) Uso esporádico de los servicios de red y seguridad estándar de Capa 2 y Capa 3 	<ul style="list-style-type: none"> Ethernet IEEE 802.3 estándar Protocolo de Internet IETF estándar (IPv4 e IPv6) Uso generalizado de los servicios de red y seguridad estándar de Capa 2 y Capa 3
Disponibilidad de la red	<ul style="list-style-type: none"> Topologías de nivel de switch y nivel de dispositivo. La topología en anillo es predominante para ambas, está surgiendo la topología estrella para switchs. IEEE estándar, IEC y protocolos de redundancia de capa 2 específicos del proveedor 	<ul style="list-style-type: none"> Topologías de nivel de switchs La topología estrella redundante es predominante IEEE estándar, IETF y protocolos de redundancia de capa 2 y capa 3 específicos del proveedor
Acuerdo de nivel de servicio (SLA)	<ul style="list-style-type: none"> Mean time to recovery (MTTR) - Minutos, horas 	<ul style="list-style-type: none"> Mean time to recovery (MTTR) – Horas, días.
Direccionamiento IP	<ul style="list-style-type: none"> Mayormente estático 	<ul style="list-style-type: none"> Mayormente dinámico



Arquitecturas convergentes: Tecnologías y culturas – Similares pero diferentes

Criterio	Industrial OT Network	Enterprise IT Network
Tipo de tráfico	<ul style="list-style-type: none"> Principalmente local - tráfico entre activos locales Información, control, seguridad, movimiento, sincronización horaria, gestión de energía. Protocolos de capa de aplicación industrial: CIP, Profinet, IEC 61850, Modbus TCP, etc. 	<ul style="list-style-type: none"> Principalmente no local - tráfico a activos remotos Voz, Video, Datos Paquetes Protocolos de capa de aplicación estándar: HTTP, SNMP, DNS, RTP, SSH, etc.
Rendimiento	<ul style="list-style-type: none"> Baja latencia, Baja fluctuación (1 ms, 100ns) Priorización de datos - QoS - Capas 2 y 3 	<ul style="list-style-type: none"> Baja latencia, Bajo fluctuación (100ms, 10ms) Priorización de datos – QoS – Capa 3
Seguridad	<ul style="list-style-type: none"> Abierto por defecto, debe ser protegido por diseño, arquitectura y configuración. Normas de seguridad industrial, por ejemplo, IEC, NIST Despliegue inconsistente de las políticas de seguridad No hay acceso a toda la empresa, tampoco a internet 	<ul style="list-style-type: none"> Dominante Políticas de seguridad fuertes Acceso a toda la empresa y a internet



Arquitecturas convergentes: Tecnologías y culturas – Similares pero diferentes

Criterio	Industrial OT Network	Enterprise IT Network
Foco	Operación 24/7	Proteger la propiedad intelectual y los activos de la empresa.
Precedencia de prioridades	Disponibilidad Integridad Confidencialidad	Confidencialidad Disponibilidad Integridad
Tipos de tráfico de datos	Red convergente de datos, control, información , seguridad y movimiento.	Red convergente de datos, voz y video .
Control de acceso	Acceso físico estricto Acceso simple a dispositivos de red	Políticas estrictas de autenticación y acceso a la red
Implicaciones de una falla del dispositivo	Perdidas de producción (\$\$'s/Hora ... o peor)	Trabajo alrededor o esperar
Protección contra amenazas	Aísla la amenaza pero sigue operando	Cerrar el acceso a la amenaza detectada
Actualizaciones	Programado durante el tiempo de inactividad	Lanzado automáticamente durante el tiempo de actividad



Arquitecturas convergentes: Lecciones aprendidas de los clientes

- El cambio de cultura corporativa toma tiempo
- Se requieren cambios de personas, procesos y tecnología para la transformación de industrial IoT.
- Los **cambios de comportamiento** serán necesarios para asegurar el éxito.
- **Crear un plan de convergencia OT-IT temprano**
 - Será importante definir KPI para medir el éxito
 - Comunicar y celebrar éxitos entre locaciones.
 - Involucrar de forma anticipada a todos los sectores:
 - Operaciones, ingeniería, seguridad, mantenimiento, IT, etc.
- La **infraestructura de red es fundamental**
- Los equipos de trabajo y el liderazgo en el frameworks deben ser definidos al comienzo.
- Definir el alcance de los procesos y aplicaciones
- Desarrollar **planes de mitigación**
- Se necesita un **marco de trabajo y una estrategia**.



Camino a la
convergencia



Redes industriales: Arquitecturas de red seguras y confiables para la empresa conectada

Pilares:

- Escalable
- Confiable
- Seguro
- Preparado para el futuro

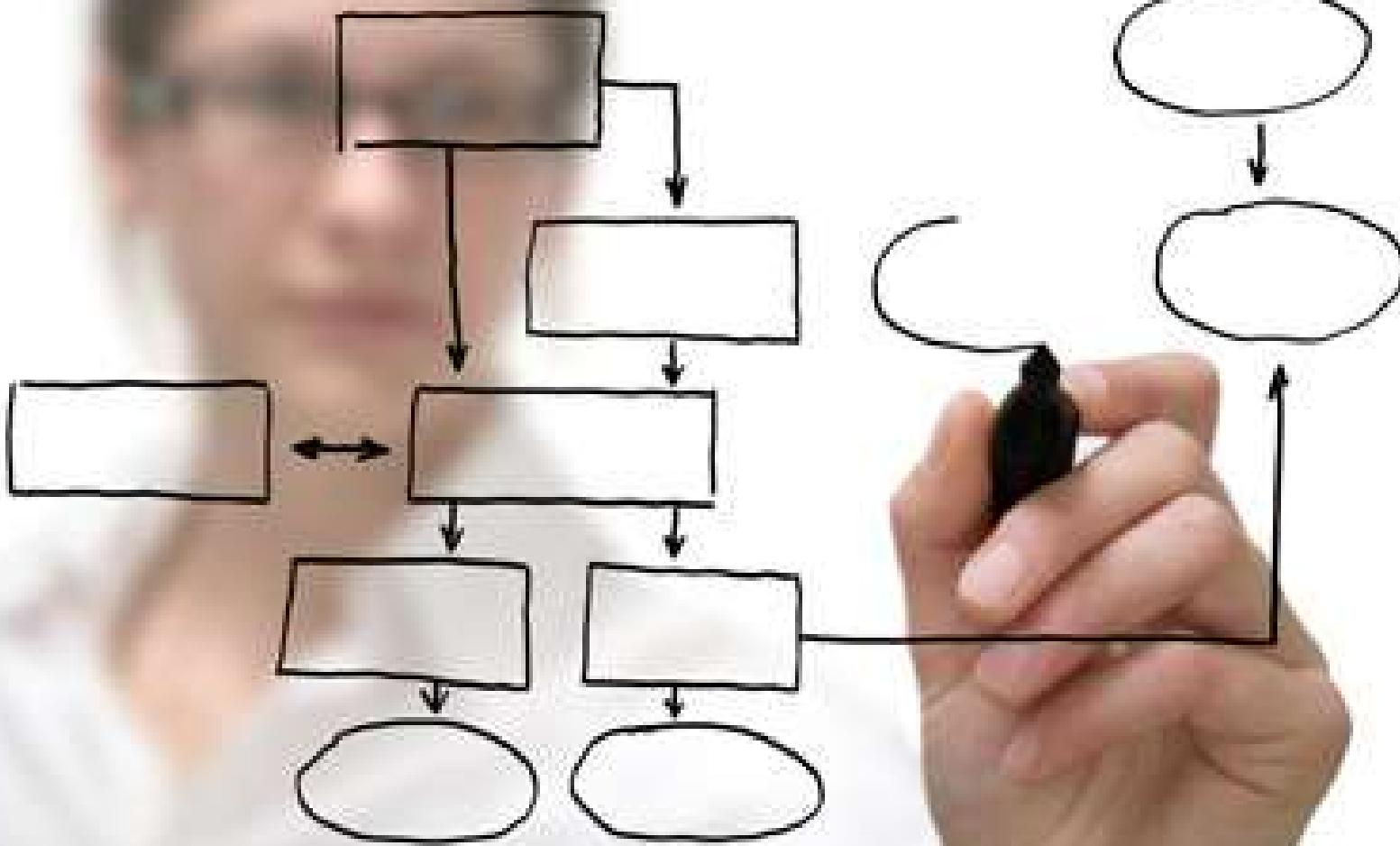
Claves del éxito:

- Zonificación (segmentación)
- Infraestructura gestionada
- Resistente a fallos
- Datos de tiempo crítico
- Soluciones Inalámbricas y movilidad
- Seguridad holística y defensa en profundidad





¿Cómo nos organizamos?



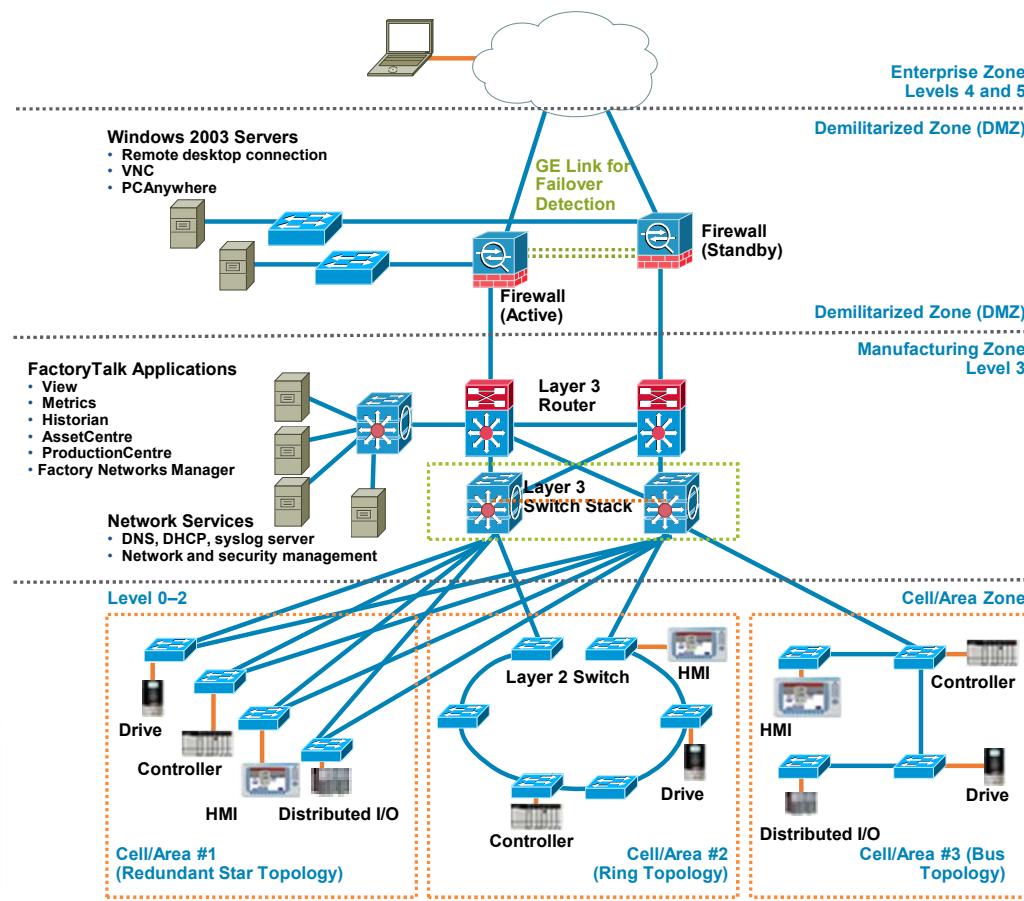
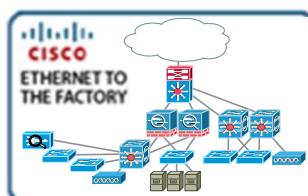
FRAMEWORK
CPwE



Redes industriales: Arquitectura de referencia..

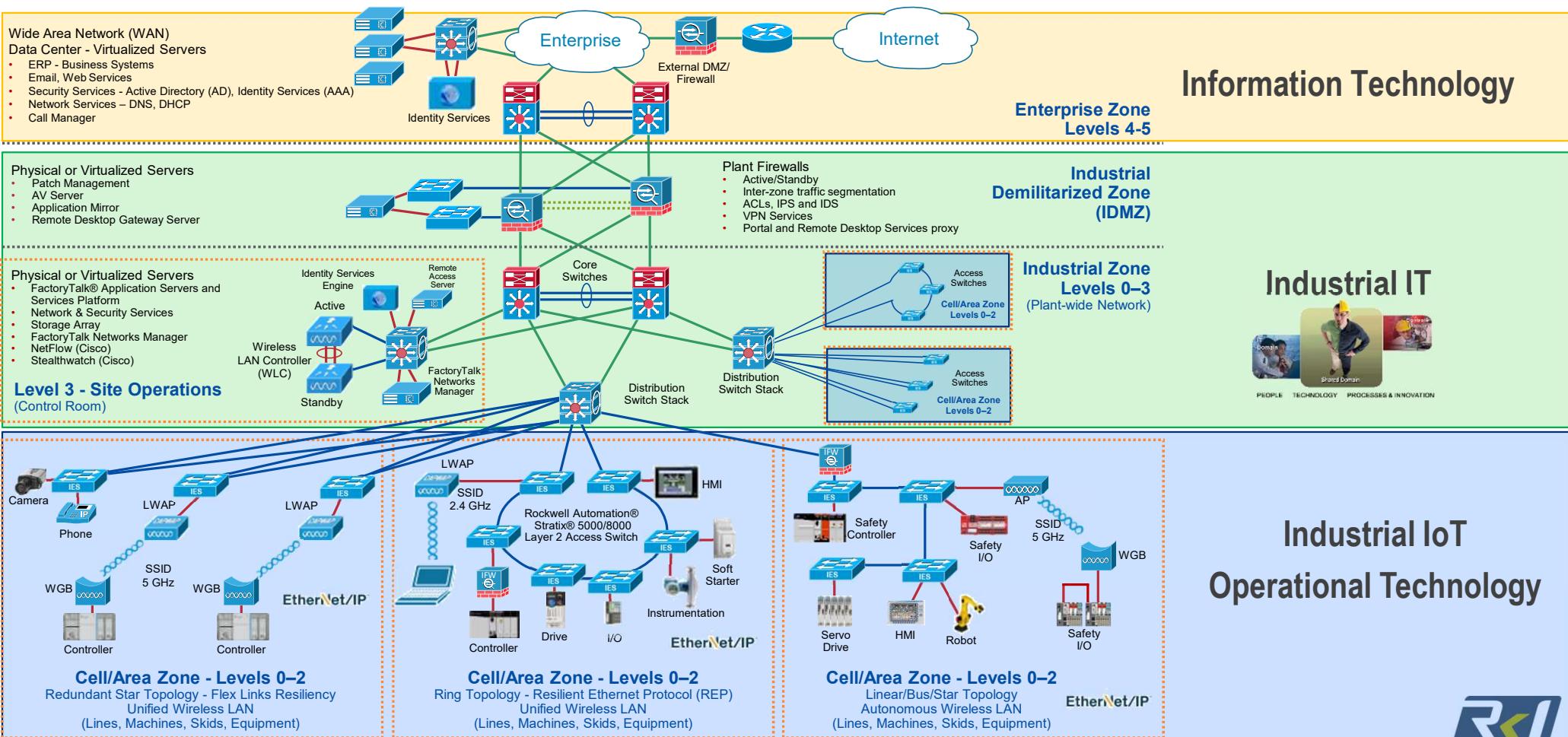
The Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

- Guía de diseño
 - Recomendaciones y mejores prácticas
 - Metodología
 - Documentación con parámetros de configuración.
 - Arquitecturas probadas y validadas
- Preparado para el futuro



Redes industriales: Arquitectura de referencia..

Industrial IoT & Industrial IT (Bridging OT-IT)

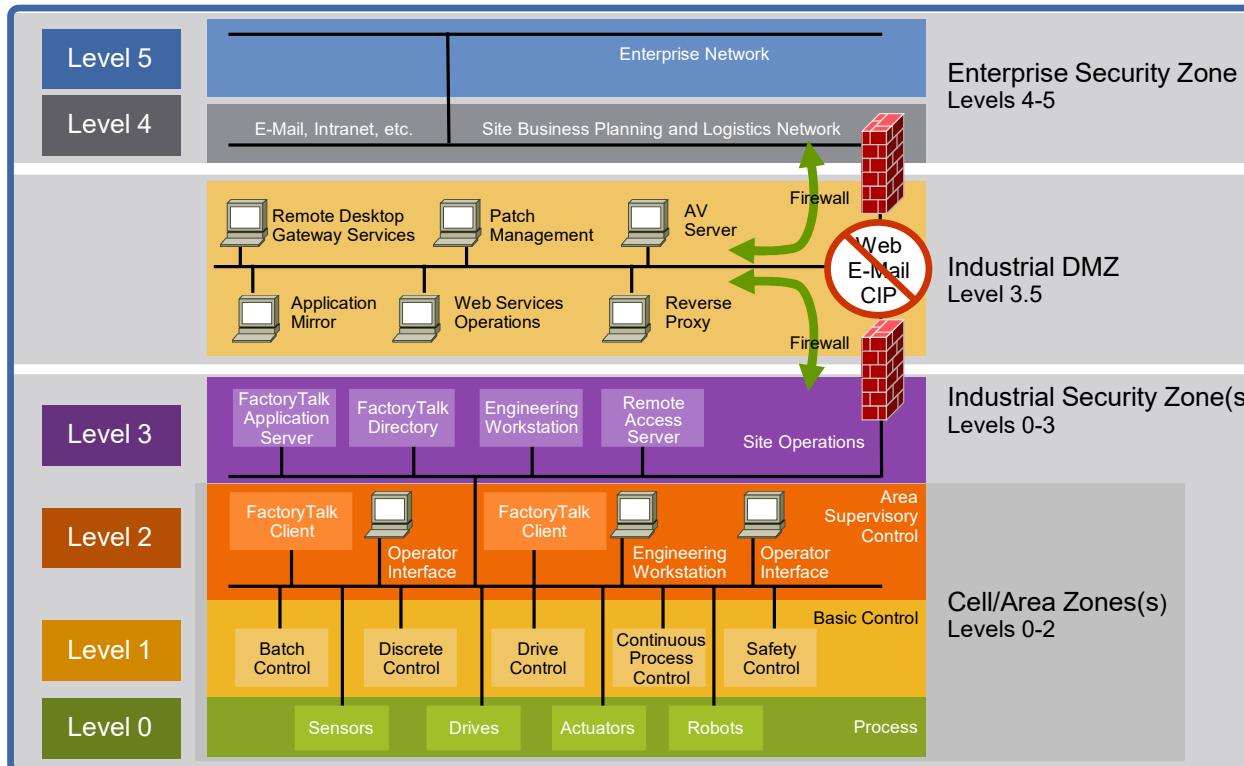


**Industrial IoT
Operational Technology**



Camino a la convergencia: Modelo lógico CPwE

OT Standards - Operational Levels - Functional / Security Zones



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



Camino a la convergencia: Construyendo los estándares industriales

Built on Technology and Industry Standards

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



Tendencias de seguridad industrial

Estándares de seguridad industrial establecidos

- International Society of Automation
 - IEC-62443 (Formerly ISA-99), Industrial Automation and Control Systems (IACS) Security
 - Zones and Conduits
 - Defense-in-Depth
 - IDMZ Segmentation



- National Institute of Standards and Technology
 - NIST 800-82, Industrial Control System (ICS) Security
 - Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
 - Defense-in-Depth
 - IDMZ Segmentation



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



WHERE
DO I
START



Administración y
Visibilidad



Redes industriales: ¿Switches administrables o no?

	Ventajas	Desventajas
Switches No Administrables	<ul style="list-style-type: none"> ▪ NO se requiere de experiencia previa. ▪ Plug & play 	<ul style="list-style-type: none"> ▪ NO Previene loops ▪ NO Brinda servicios seguros ▪ NO Provee Diagnóstico ▪ NO Servicios de segmentación(VLANs) ▪ NO Cálida de servicios(QoS) ▪ NO Redundancia de redes ▪ NO Administración de mensajería multicast
Switches Administrables	<ul style="list-style-type: none"> ▪ Previene loops ▪ Brinda servicios seguros ▪ Provee Diagnóstico ▪ Servicios de segmentación(VLANs) ▪ Cálida de servicios(QoS) ▪ Redundancia de redes ▪ Administración de mensajería multicast 	<ul style="list-style-type: none"> ▪ Más costoso ▪ En ciertos casos requieren de configuración al inicializarse
Switches Administrables + ODVA	<ul style="list-style-type: none"> ▪ Previene loops en Añillos ▪ Cálida de servicios(QoS) ▪ Time Sync Services (IEEE 1588 PTP) ▪ Provee Diagnóstico ▪ Administración de mensajería Multicast 	<ul style="list-style-type: none"> ▪ Capacidades de gestión limitadas ▪ Puede requerir una configuración mínima

Redes industriales: Administración y Visibilidad

- Administración / Configuración:
 - Interface Línea de comando Cisco
 - Cisco Network Assistant
 - Configurable vía AOP y administrado como parte de un proyecto de RSLogix™ 5000.
 - Disponible mediante la interface Web embebida (**Device Manager**)
 - Puertos inteligentes o “**Smartport**” – optimización del funcionamiento de los puerto.
 - Macros que permiten setear al switch para aplicaciones de automatización.
- Diagnóstico y Monitoreo:
 - Diagnóstico en tiempo real disponible mediante AOP y interface web embebida.
 - Visibilidad y acceso a la información de red mediante **TAGs de RSLogix 5000 predefinidos**. Permitiendo el acceso a información de HMI / SCADA de planta.
 - **FactoryTalk® Network Manager™**
 - Herramienta amigable y conocida por IT – **Cisco Network Assistant**, **CiscoWorks**, **Cisco Netflow**, **SNMP**.



Redes industriales: Visibilidad y Administración

FactoryTalk® Network Manager™

The screenshot displays four panels of the FactoryTalk Network Manager interface:

- Network Topology:** Shows a hierarchical tree of network segments (e.g., CEMKE, Distrib) with various nodes (routers, switches, hosts) represented by icons and IP addresses.
- Alarms:** A table listing 5 alarms, including topology changes and half-duplex port errors.
- Design > Plug and Play:** A table showing 1 unclaimed PRP device, with details like name, serial, and product ID.
- Physical Device View:** A grid showing the status of multiple Allen-Bradley Stratix 3100 modules, with indicators for power and link status.

Hirschmann HiVision

The screenshot shows the Hirschmann HiVision interface with the following components:

- Map:** A graphical representation of the network topology with various devices (switches, routers, hosts) and their connections.
- Configuration Tree:** A hierarchical tree view of network components, including Octopus STX, Point I/O, RAIL RS20 4-port, and M12-MSC Modbus-Support.
- Event Log:** A table listing recent events, such as status impairment errors and redundancy manager warnings.

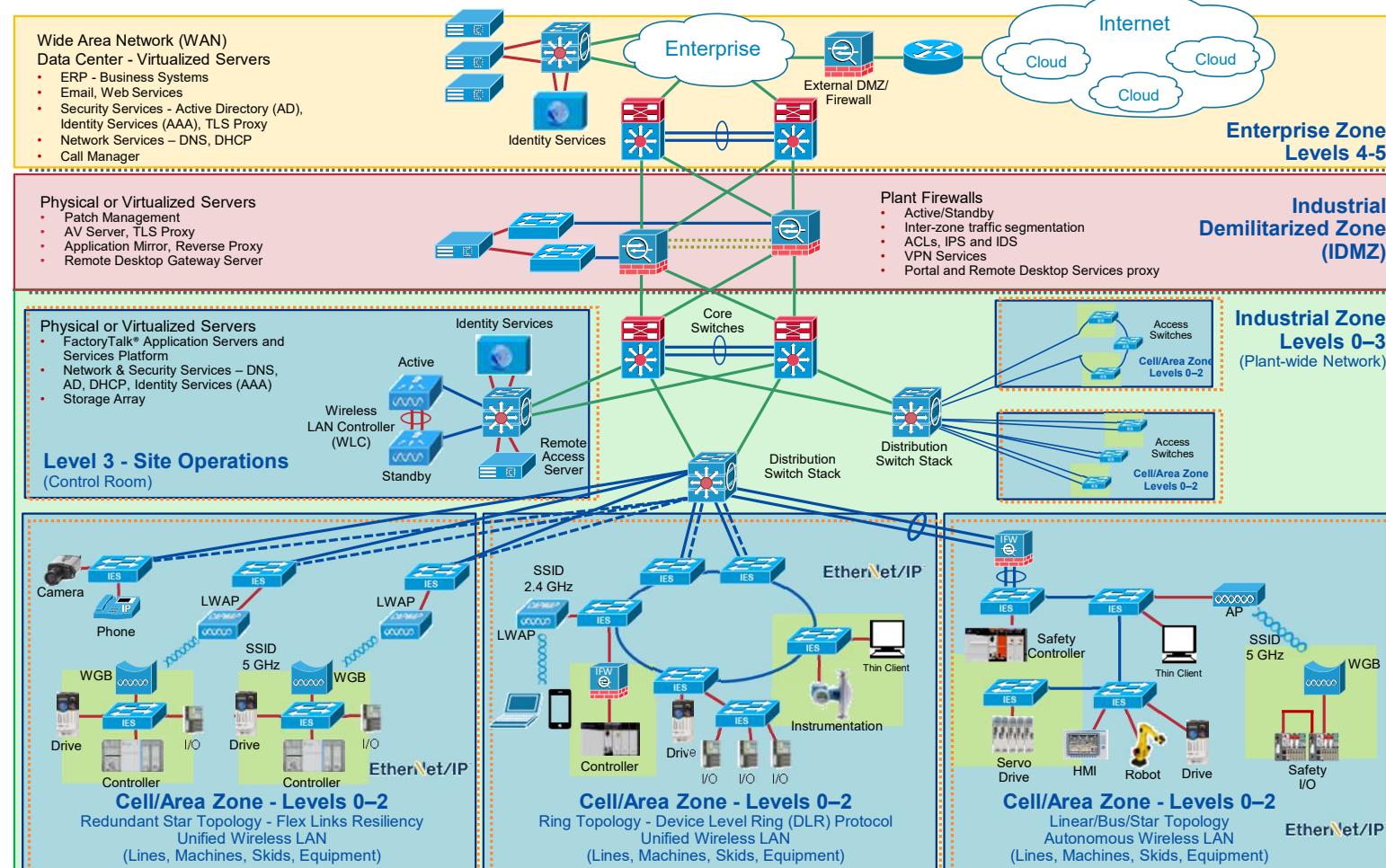


Zonificación
(Segmentación)



Zonificación Lógica - Segmentación

CPwE Logical Framework – Modular Building Blocks

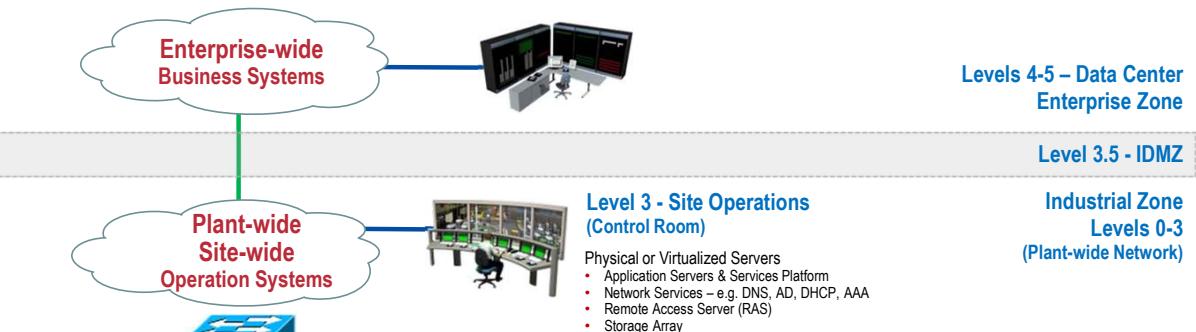
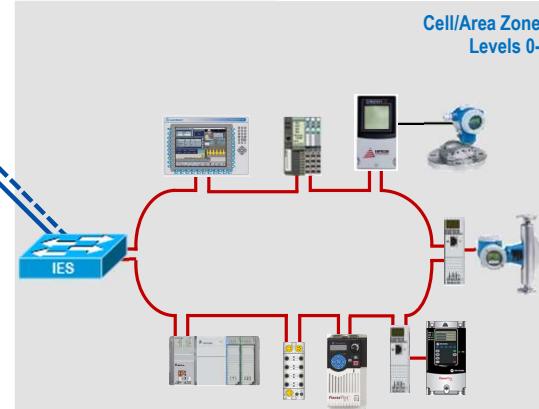
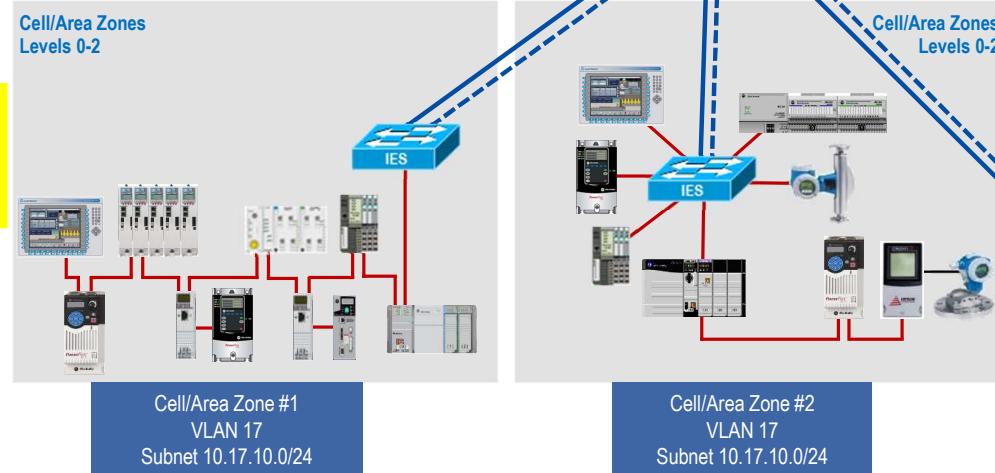
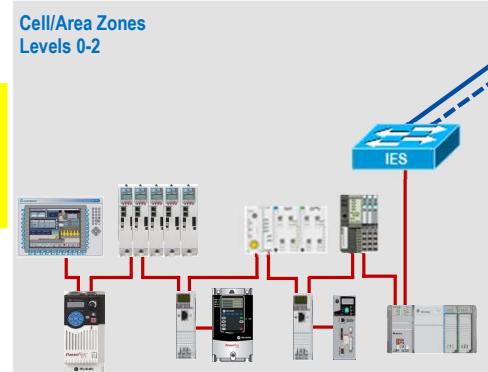


Sin segmentar (no recomendado)

Segmentation – Network Services

**LAN grande,
Falta de límites naturales y segmentación**

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address



EtherNet/IP™

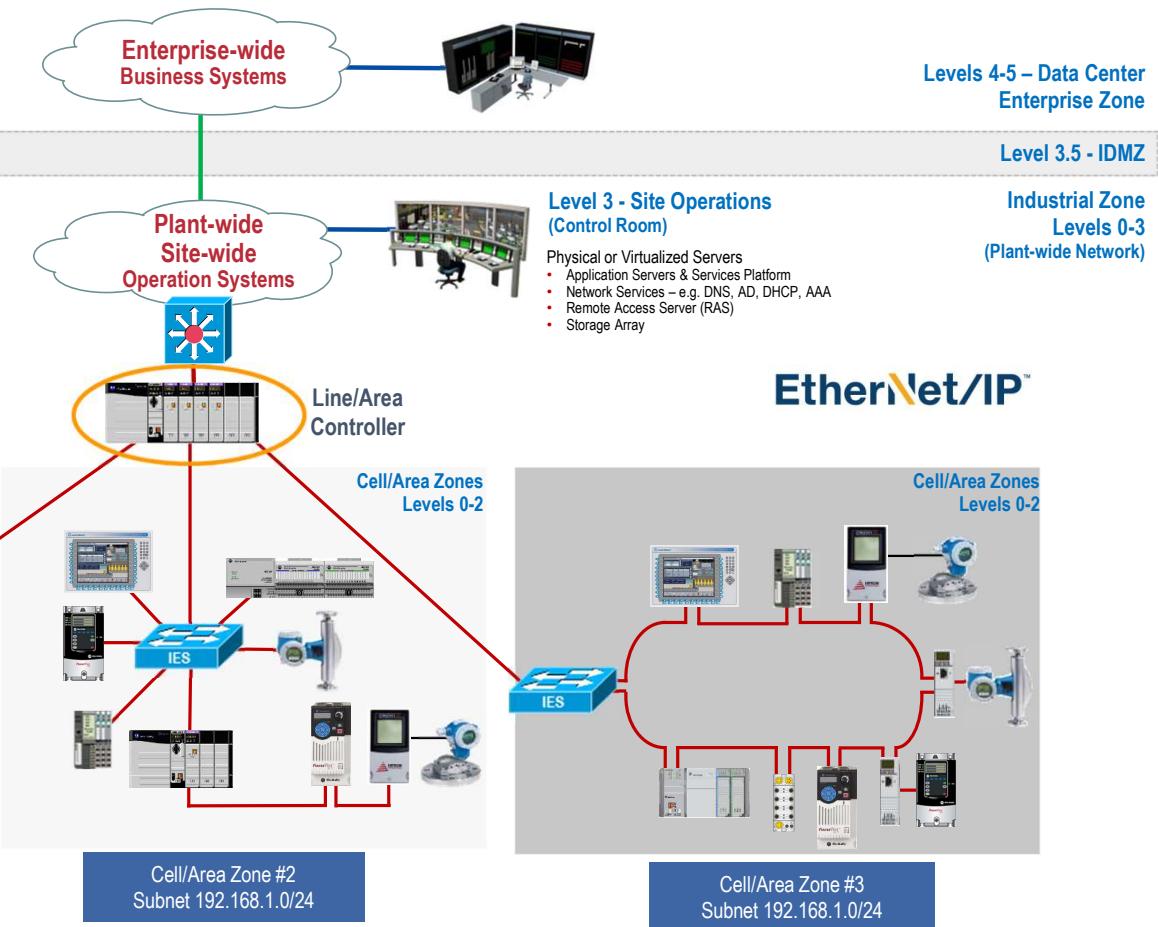
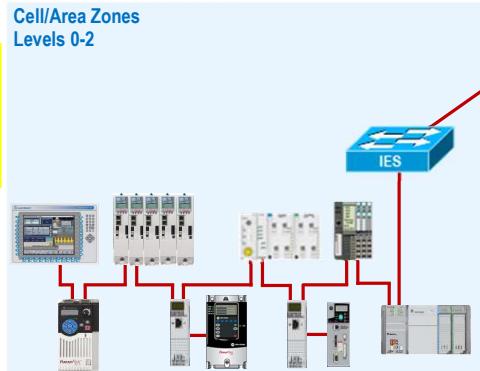
Múltiples interfaces de red (NICs) - CIP™ Bridge

Segmentation – Network Services

Redes conectadas más pequeñas para crear límites y segmentación

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

- Dominio de Broadcast acotado L2
- Espacio de red IP reutilizable



Segmentado mediante Layer 3 NAT

Segmentation – Network Services

Redes conectadas más pequeñas para crear límites y segmentación

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #1
Subnet 192.168.1.0/24



Enterprise-wide
Business Systems



Plant-wide
Site-wide
Operation Systems

Level 3 - Site Operations
(Control Room)

- Physical or Virtualized Servers
- Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Storage Array

Levels 4-5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

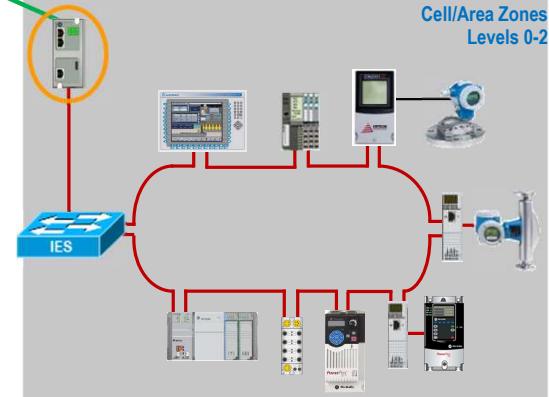
Industrial Zone
Levels 0-3
(Plant-wide Network)

EtherNet/IP™

Cell/Area Zones
Levels 0-2



Cell/Area Zone #2
Subnet 192.168.1.0/24



Cell/Area Zone #3
Subnet 192.168.1.0/24

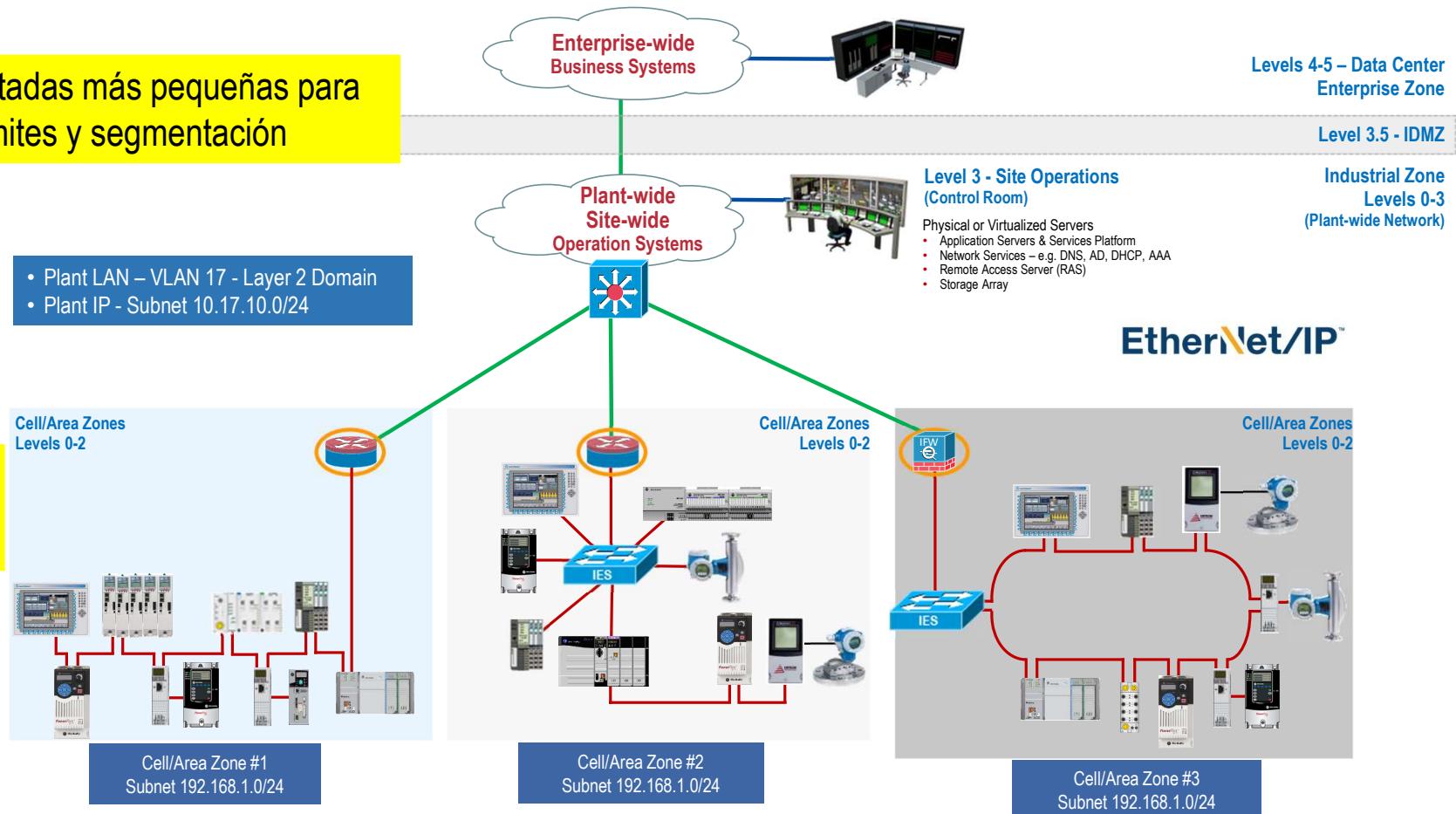
Segmentado mediante L3 - Integrated Services Router / firewalls

Segmentation – Network Services

Redes conectadas más pequeñas para crear límites y segmentación

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

- Dominio de Broadcast acotado L2
- Espacio de red IP reutilizable

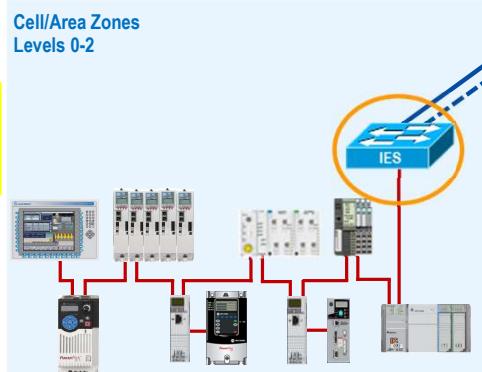


Segmentado mediante VLAN sin NAT

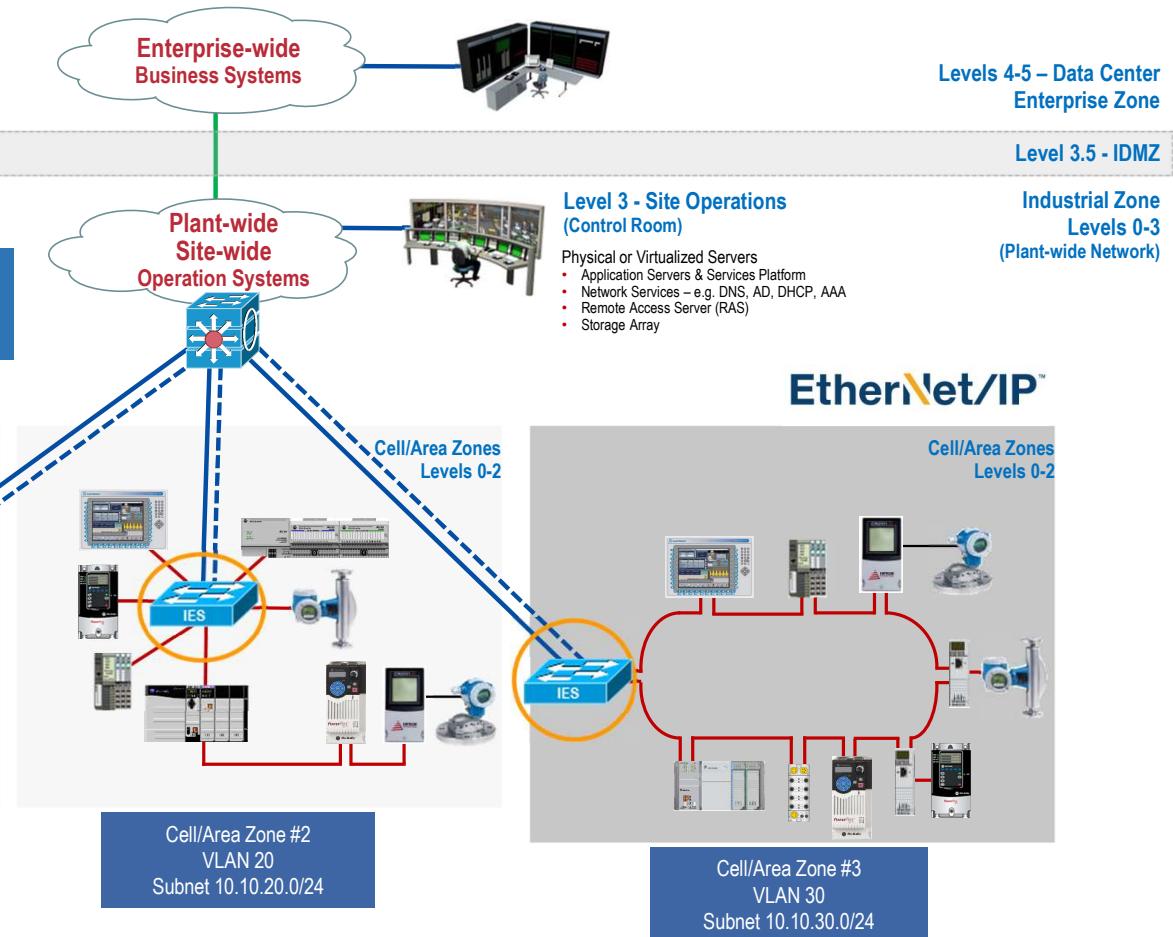
Segmentation – Network Services

Redes conectadas más pequeñas para crear límites y segmentación

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address



Cell/Area Zone #1
VLAN 10
Subnet 10.10.10.0/24

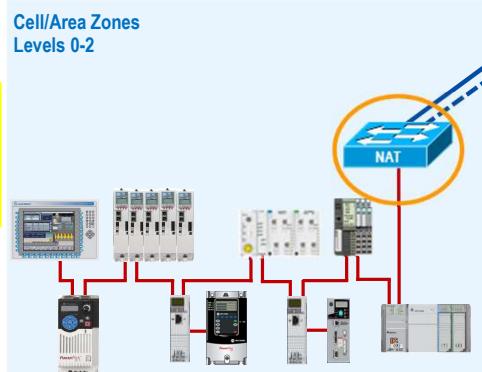


Segmentado mediante VLAN con NAT L2

Segmentation – Network Services

Redes conectadas más pequeñas para crear límites y segmentación

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24



Cell/Area Zone #1
VLAN 10
Subnet 192.168.1.0/24



Level 3 - Site Operations (Control Room)

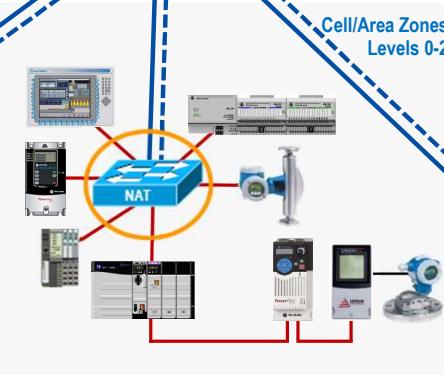
- Physical or Virtualized Servers
 - Application Servers & Services Platform
 - Network Services – e.g. DNS, AD, DHCP, AAA
 - Remote Access Server (RAS)
 - Storage Array

Levels 4-5 – Data Center Enterprise Zone

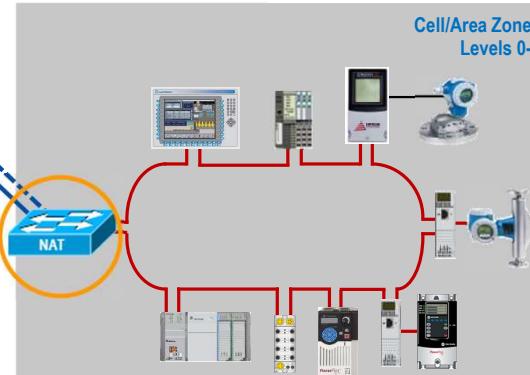
Level 3.5 - IDMZ

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

EtherNet/IP™



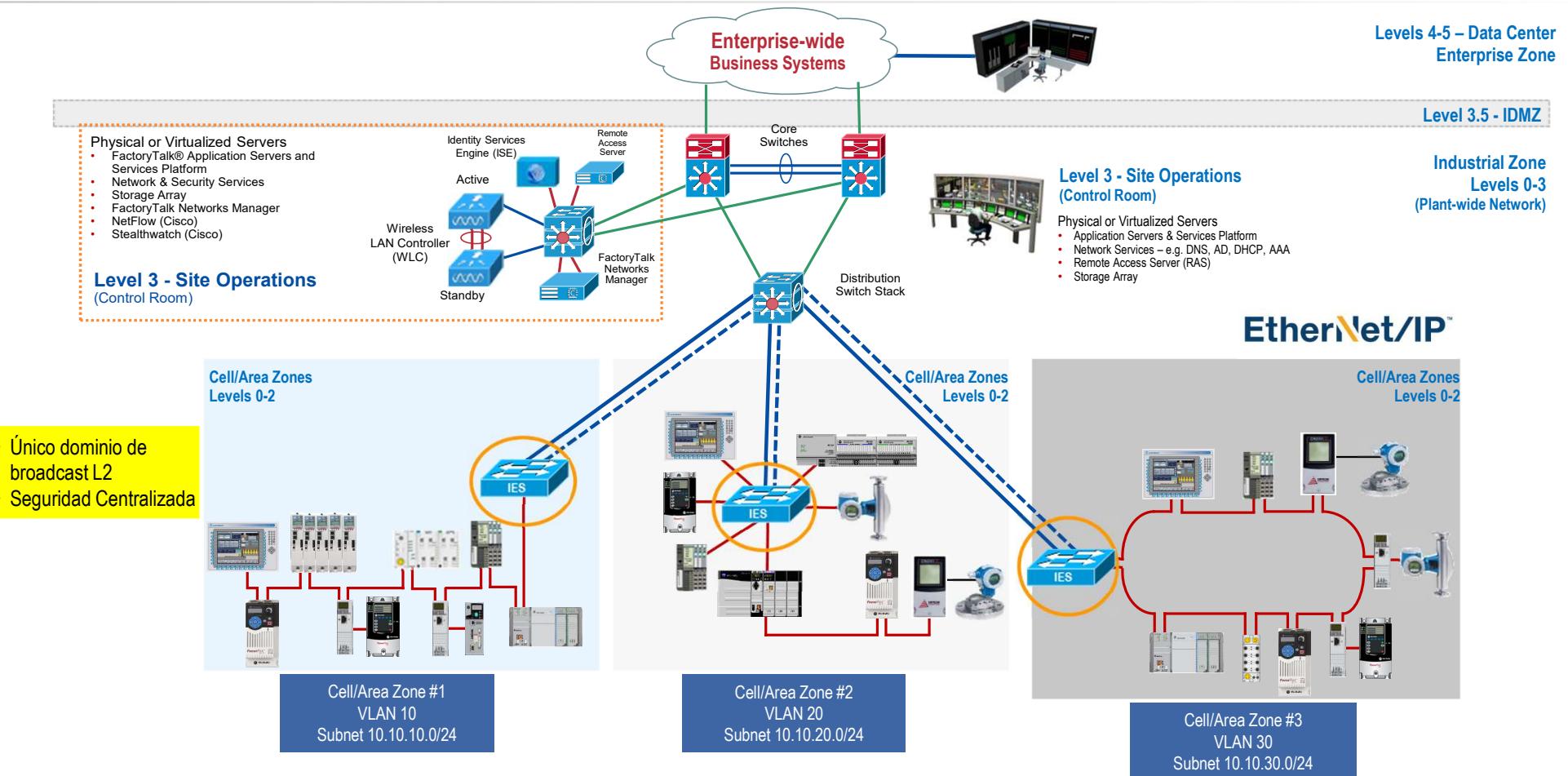
Cell/Area Zone #2
VLAN 20
Subnet 192.168.1.0/24



Cell/Area Zone #3
VLAN 30
Subnet 192.168.1.0/24

Segmentado mediante ACL, dACL o TrustSec

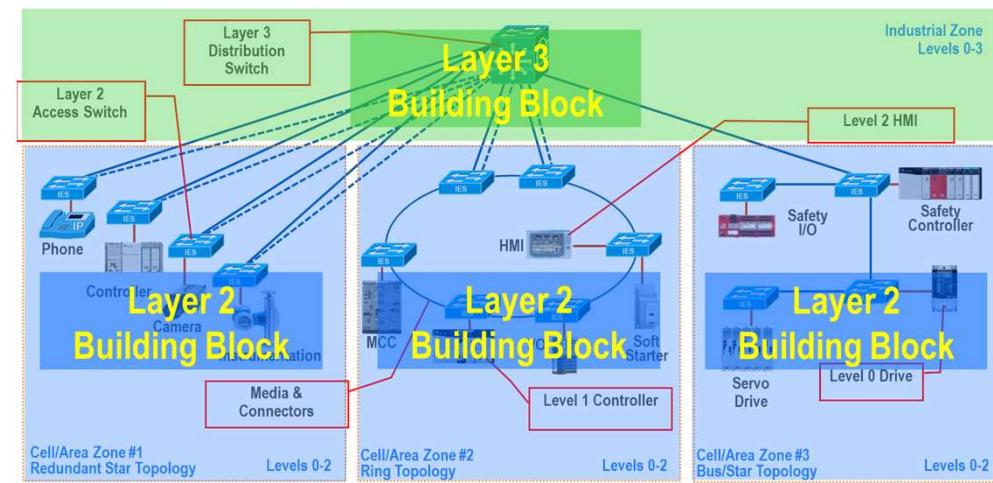
Segmentation – Network Services



Consideraciones en el diseño e implementación

Segmentation – Network Services

- Diseño en bloques de acuerdo a la funcionalidad o niveles de seguridad del sistema.
- Limitar la extensión de la red
- LAN conectadas más pequeñas:
 - Dominios de fallas pequeños (ej. Loops L2)
 - Dominios de broadcast pequeños
 - Dominios de confiabilidad pequeños (security)
- Segmentar de acuerdo a Tecnologías IoT
- Múltiples técnicas de segmentación
 - Multiples NICs, NAT, VLAN, VLAN+NAT, Firewalls,
 - L3 Switchs, Access Control List (ACL), dACL, TrustSec



Visibilidad OT &
Ciberseguridad



Solución integral de seguridad en OT

Network Security	Log Management	Vulnerability Assessment	Change Detection	Integrity Monitoring
Integrated <ul style="list-style-type: none">• Network discovery• Network access control• Denial of Service (DoS) protection• Zones (network segmentation) & conduits (traffic filtering)• Bandwidth limitation• Deep Packet Inspection for Industrial Protocols	Passive <ul style="list-style-type: none">• Syslog data collection• Log filtering & management• Investigation analytics & reporting	Periodic <ul style="list-style-type: none">• Security vulnerability & configuration assessment• Best practice & policy tests	Continuous <ul style="list-style-type: none">• Real-time change detection• Best practice assessment & remediation• Compliance analytics & reporting	



Software de visibilidad industrial - TIV

Mapeo preciso de la red OT

- » Descubrimiento pasivo de dispositivos e inventario (Marca, Modelo, Versión, Serial, Hash).
- » Soporta protocolos IT y más de 50 protocolos industriales. (EtherNet/IP, ModBus, DNP3, S7, PROFINET, IEC 101/104, GOOSE, and Bacnet)
- » Visualización del tráfico entre dispositivos.

Detección de amenazas automatizadas

- » Aprendizaje dinámico de comportamientos de referencia seguros.
- » Identificación de comportamientos anómalos (cambios, commandos, etc).

Identificación de vulnerabilidades en las redes OT

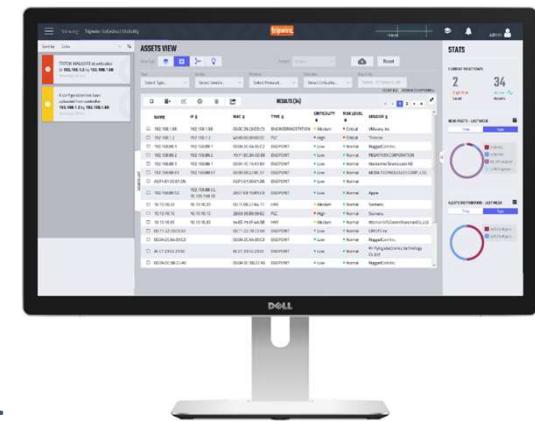
- » CVEs, información procesable.

Gestión de cambios en tiempo real

- » Lee cambios en configuraciones en el momento que se hacen y reporta las modificaciones.

Registro de eventos

- » Tripwire Log Center, centralización y correlación de eventos registrados.



Dispositivos

- Mapeo de los dispositivos en comunicación, el tráfico debe pasar por el switch monitoreado.

The screenshot shows the Tripwire Industrial Visibility software interface. At the top, there's a header bar with the Tripwire logo, user information ('admin'), and a graph showing network traffic. Below the header is a search bar and filter options for 'Type', 'Vendor', 'Protocol', 'Criticality', and 'Search By'. The main area is titled 'ASSETS VIEW' and displays a table of 'RESULTS (31)'. The columns include NAME, IP, MAC, TYPE, CRITICALITY, RISK LEVEL, VENDOR, and NETWORK. The data shows various industrial assets like PLCs, Engineering Stations, and Endpoints from vendors like Rockwell Automation, CISCO SYSTEMS, INC., and VMware, Inc.

NAME	IP	MAC	TYPE	CRITICALITY	RISK LEVEL	VENDOR	NETWORK
10.1.30.40	10.1.30.40	00:50:56:B9:E2:AD	Engineering Station	Medium	Critical	VMware, Inc.	Default
64:D1:54:37:D8:D6		64:D1:54:37:D8:D6	Endpoint	Low	Normal		Default
10.1.30.1:Card 2 \ Addr 255			PLC	High	Normal	Rockwell Automation	Default
F4:54:33:92:89:96		F4:54:33:92:89:96	Endpoint	Low	Normal	Rockwell Automation	Default
Chemical_plant	10.1.30.1	00:10:9C:C0:04:9D	PLC	High	Critical	Rockwell Automation	Default
00:12:01:09:ED:87		00:12:01:09:ED:87	Endpoint	Low	Normal	CISCO SYSTEMS, INC.	Default
192.168.1.2	192.168.1.2	00:01:9C:BD:A9:4F	Endpoint	Low	Normal	Rockwell Automation	Default
00:1D:9C:C3:88:9E		00:1D:9C:C3:88:9E	Endpoint	Low	Normal	Rockwell Automation	Default
10.1.30.41	10.1.30.41	00:50:56:B8:6D:68	Endpoint	Low	Normal	VMware, Inc.	Default
00:1D:9C:D0:08:D1		00:1D:9C:D0:08:D1	Endpoint	Low	Normal	Rockwell Automation	Default
10.1.30.6	10.1.30.6	00:1D:9C:A1:60:4E	Endpoint	Low	Normal	Rockwell Automation	Default



Descubrimiento de nodos e inventario en forma pasiva (Marca, Modelo, Versión, Serial, Hash):

- Port mirroring
- VLAN mirroring
- SPAN port
- Etc



Alertas

- Información detallada, procesable y para tomar acción en Tiempo Real.

Integridad

Avisa de cualquier cosa que pueda afectar la integridad de la planta y su funcionamiento.

Seguridad

Actividades no tan communes, malware, tráfico anormal a dispositivos.

The screenshot shows the Tripwire Industrial Visibility platform. On the left, there are three vertical cards: 'Asset Details' (with a blue exclamation mark icon), 'Configuration Changes' (with a blue gear icon), and 'Alert Timeline' (with a blue clock icon). The main area displays an alert titled 'Configuration Upload'. The alert details section shows a configuration file named 'MainProgram-Data' was added from IP 10.1.30.10, MAC 00:50:56:89:E2:AD, and Network Default. The asset details section shows the asset is a PLC at 10.1.30.10, part of the 'Engineering Station' group, with a medium risk level and high criticality. The configuration changes section shows the file was added. The alert timeline section shows the alert was created yesterday at 20:19.

FILENAME	STATUS
MainProgram-Data	ADDED

New Alert 55: A configuration has been uploaded from controller 10.1.30.1:Card 2 \ Addr 12 by 10.1.30.10, by user ENG_AB\Administrator
Yesterday, 20:19

Redes industriales: Resumen

- ✓ Diseño y soluciones fundamentadas por Frameworks tales como CPwE u Otros
 - Diseño en bloques (zonas/segmentar)
 - Proponer arquitecturas que sean escalables / robustas
 - Ciberseguridad desde el inicio
 - No existe una única solución
- ✓ Las redes no son las de antes, necesitamos gestionarlas, administrarlas y contar con visibilidad.
- ✓ Desarrollar nuevas habilidades / socios estratégicos





Tecnología en Automatización y Control



Hernán Lovera

Jefe de Producto
Industrial IoT



Cel: (0054) 911 6020-0569

Tel: 011-5263-7225

Exclusivo para clientes: 0810-122-0217

Correo: h.lovera@racklatina.com.ar