Considerazioni sulla progettazione di reti EtherNet/IP™ robuste

Marco Rizzi
Solution Architect - IA

Rockwell Automation

Perchè è importante?
Requisiti applicativi

- Cos'è il real time?
  - Dipende dall'Applicazione….. Solo voi potete definire cosa significa per la vostra applicazione



Funzione	Integrazione delle Informazioni, Automazione Processi Lenti	Automazione Processi Discreti Tempi-critici	Motion Control
Tecnologia della Comunicazione	.Net, DCOM, TCP/IP	Protocolli Industriali - CIP	Soluzioni Hardware e Software, ad esempio, Integrated Motion in reti EtherNet/IP, PTP
Periodo	10 ms to 1000 ms	1 ms to 100 ms	100 µs to 10 ms
Industrie	Oil & Gas, chimica, energia, Acque	Auto, Food & Beverage, Semiconduttori, Metals, Farmaceutica	Macchine con automazione a stati
Applicazioni	Pompe, compressori, mixers, strumentazione	Material handling, filling, labeling, palletizing, packaging	Presse per stampa, trafilatrici, web making, pick and place

Source: ARC Advisory Group

Perchè è importante?

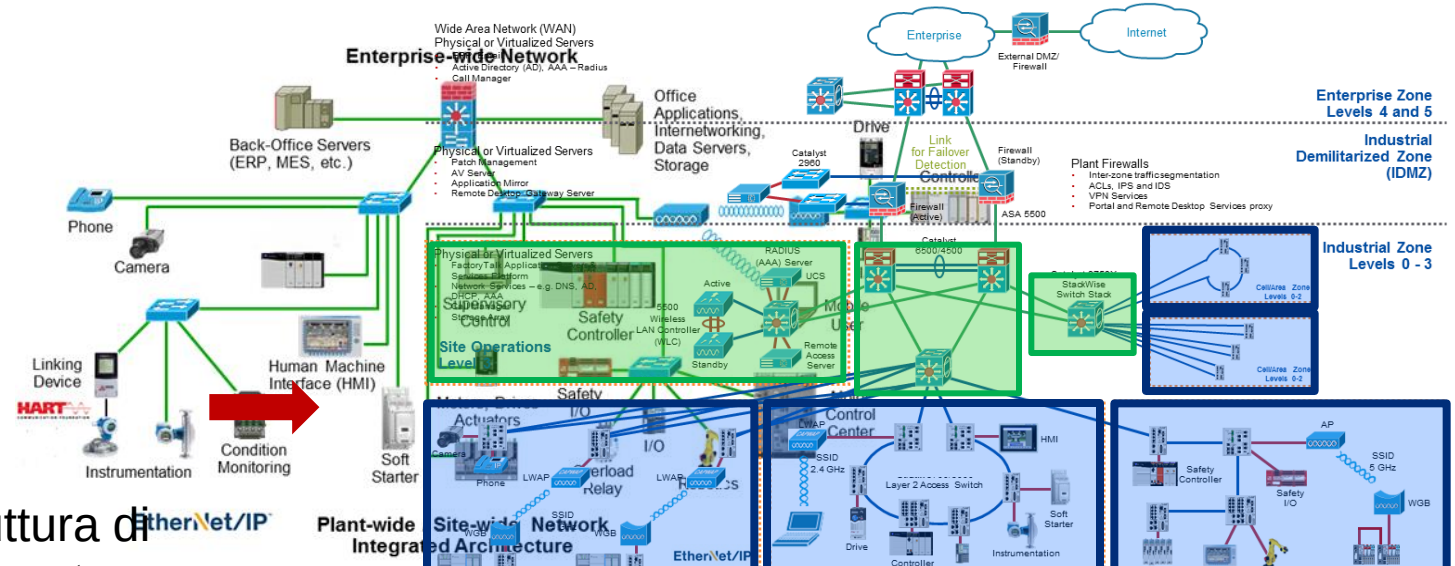
Requisiti applicativi

- Infrastruttura scalabile, robusta, sicura e pronta per il futuro:
  - Applicazioni
  - Software
  - Reti

Internet delle Cose, Internet di Tutto

Perchè è importante?

Integrazione tra Automazione Industriale e Sistemi di Controllo



IACS con Infrastruttura di Rete “Piatta” e Aperta

IACS con Infrastruttura di Rete “Piatta” e Aperta

IACS con Infrastruttura di Rete Strutturata e Rafforzata

Metodologia Progettazione Reti Industriali

EtherNet/IP™ Considerazioni sulla progettazione della rete

- Comprendere l'Applicazione e I Requisiti Funzionali
  - Elementi da collegare – industriali e non-industriali
  - Requisiti dei Dati per Disponibilità, integrità e confidenzialità
  - Requisiti dei Modelli di Comunicazione, topologia e resilienza
  - Tipologie di traffico – informazioni, controllo, sicurezza, sincronizzazione dei tempi, controllo azionamenti, voce, video
- Sviluppare un Quadro Logico (roadmap)
  - **Migrare da reti piatte a reti strutturate rafforzate**
  - Definire zone e segmentazioni, collocare applicazioni ed oggetti nel quadro logico in base ai requisiti
- Sviluppare una struttura fisica su cui allinearsi che supporti il quadro logico
- Schierare un Modello di Sicurezza Olistico di Difensa in Profondità
- Ridurre I rischi, semplificare il progetto velocizzare il dispiegamento:
  - Utilizzare gli standards dell'information technology (IT)
  - Seguire gli standards dell' industrial automation technology (IAT)
  - Utilizzare modelli di riferimento ed architetture di riferimento

Metodologia Progettazione Reti Industriali

EtherNet/IP™ Considerazioni sulla progettazione della rete

- Comprendere l'Applicazione e I Requisiti F
  - Elementi da collegare – industriali e non-industriali
  - Requisiti dei Dati per Disponibilità, integrità e confidenzialità
  - Requisiti dei Modelli di Comunicazione, topologia e resilienza
  - Tipologie di traffico – informazioni, controllo, sicurezza, sincronizzazione dei tempi, controllo azionamenti, voce, video
- Sviluppare un Quadro Logico (roadmap)
  - **Migrare da reti piatte a reti strutturate rafforzate**
  - Definire zone e segmentazioni, collocare applicazioni ed ogget
- Sviluppare una struttura fisica su cui alli logico
- Schierare un Modello di Sicurezza Olistico
- Ridurre I rischi, semplificare il progetto velo
  - Utilizzare gli standards dell'information technology (IT)
  - Seguire gli standards dell' industrial automation technology (IAT)
  - Utilizzare modelli di riferimento ed architetture di riferimento

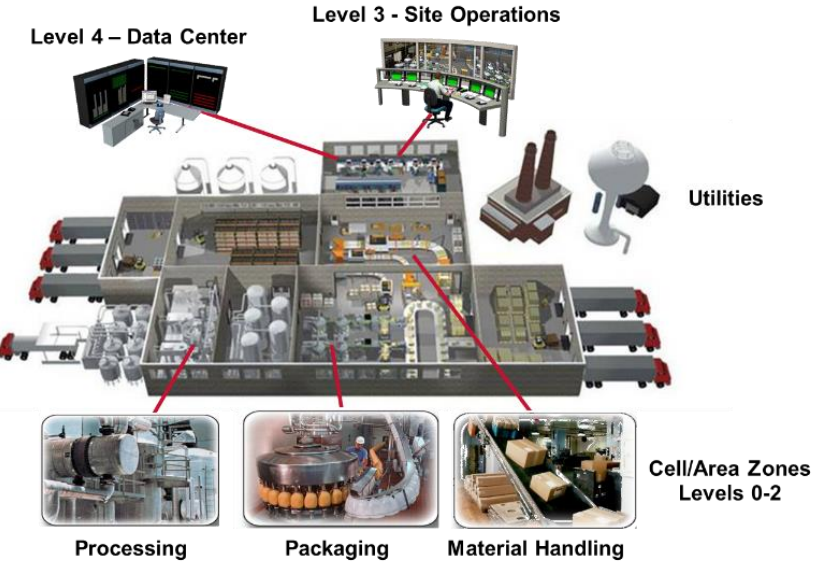
Evitare la Crescita Disordinata della Rete

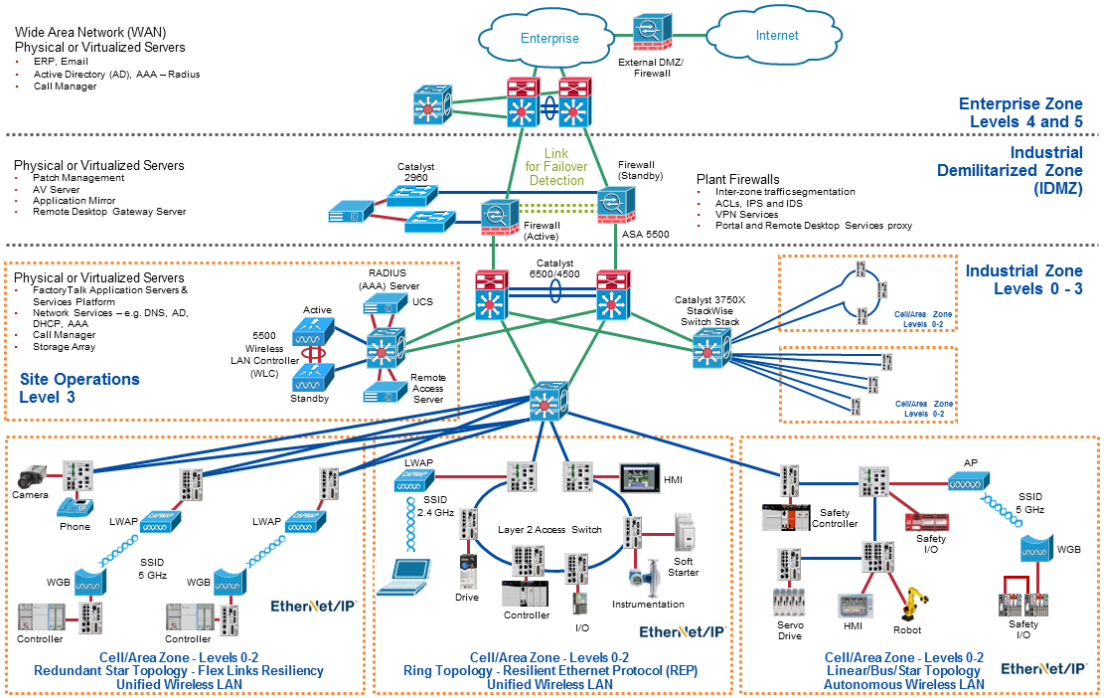
Utilizzare Soluzioni di Integrazione Disponibili

Perchè l'Infrastuttura di Rete è Importante

Cosa Fare ?

Architetture di Riferimento





Considerazioni sulla Progettazione delle Reti

Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

Considerazioni sulla Progettazione delle Reti

Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

OSI Modello di riferimento a 7 Strati

EtherNet/IP™

Interconnessione tra Sistemi Aperti

Cosa Rende EtherNet/IP™ industriale?

Layer Name	Layer No.	Funzione	Esempi
Applicazione	Layer 7	Servizi di Rete per le App	CIP IEC 61158
Presentazione	Layer 6	Crittografia/Altri Processi	
Sessione	Layer 5	Gestione Applicazioni multiple	
Trasporto	Layer 4	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Rete	Layer 3	Packet Delivery, Routing	IETF IP
Data Link	Layer 2	Framing of Data, Error Checking	IEEE 802.3/802.1
Fisico	Layer 1	Signal type to transmit bits, pinouts, cable type	TIA - 1005

Routers

Switches

Cabling

Physical Layer Hardening

Infrastructure Device Hardening

Common Application Layer Protocol

5-Layer TCP/IP Model

IEEE 802.3 Ethernet @ 100 Mbps, full-duplex, Switched Network

- 1 bit = 10 ns (1 byte = 80 ns)
- La Dimensione del frame Ethernet varia da
  - Short frame - 64 bytes = 512 bits
  - Long frame - 1518 bytes = 12144 bits
  - Alcuni frame di Ethernet sono conteggiati separatamente
    - Preambolo e Start Frame Delimiter (SFD) = 64 bits
    - Interframe Gap = 96 bits
- Banda passante teorica per Ethernet @ 100 Mbps, full-duplex, Switched Network
  - Short frame con 64 bytes ≈ 148,000 frames/second
  - Long frames con 1518 bytes ≈ 8,000 frames/second

- EtherNet/IP™ @ 100 Mbps (IEEE 802.3 Ethernet), full-duplex, Switched Network
  - Dimensione totale header per un frame di I/O in EtherNet/IP di 64 bytes
    - Il messaggio implicito di connessione EtherNet/IP aggiunge 18 bytes
    - Lo User Datagram Protocol aggiunge 8 bytes
    - Il Protocollo Internet aggiunge 20 bytes
    - Il Protocollo Ethernet aggiunge 18 bytes
  - Lunghezza frame (short frame) per un implicit message di EtherNet/IP è:
    - 64 byte + I/O data size (bytes)
    - Le dimensioni di un tipico “implicit message” sono < 36 bytes

Banda passante teorica per EtherNet/IP @ 100 Mbps, full-duplex, Switched Network

- Le dimensioi di un Tipico “I/O frame” (64 byte + 36 byte I/O data) sono ≈ 104,000 frames/second
- Le dimensioni Massime di un I/O (64 byte + 511 byte I/O data) sono ≈ 21,000 frames/second
  - Normal CIP Forward_Open

EtherNet/IP™ @ 100 Mbps (IEEE 802.3 Ethernet), full-duplex, Switched Network

- Dimensione totale di un header per un frame di I/O in EtherNet/IP è 64 bytes
  - EtherNet/IP messaggio implicito di connessione aggiunge 18 bytes
  - Lo User Datagram Protocol aggiunge 8 bytes
  - Il Protocollo Internet aggiunge 20 bytes
  - Il Protocollo Ethernet aggiunge 18 bytes
- Lunghezza frame (short frame) per un implicit message EtherNet/IP è:
  - 64 byte + I/O data size (bytes)
  - La dimensione Tipica di implicit message per I/O è < 36 bytes

Banda passante teorica per EtherNet/IP @ 100 Mbps, full-duplex, Switched Network

- Dimensione tipica per I/O frame (64 byte + 36 byte I/O data) ≈ 104,000 frames/second
- Dimensione massima per I/O frame (64 byte + 511 byte I/O data) ≈ 21,000 frames/second
  - Normal CIP Forward_Open

Esempio di banda passante EtherNet/IP™

- Il Controller scambia 36 bytes di dati I/O con 10 nodi I/O ad 1 ms Requested Packet interval (RPI)
  - RPI = 1 ms
    - 1,000 frames/second in ogni direzione
  - Ogni nodo I/O deve essere in grado di:
    - Consumare 1,000 frames/second
    - Produrre 1,000 frames/second
  - Il Controllore deve essere in grado di:
    - Consumare 10,000 frames/second
    - Produrre 10,000 frames/second

Considerazioni progettuali che andrebbero sempre fatte

- Prestazioni dei Controllori
  - Massimo # di nodi (Connessioni CIP)
  - RPI Minimo (quanto veloce)
  - Dimensioni massime dati I/O per RPI
- Prestazioni Nodi I/O
  - RPI Minimo (quanto veloce)
  - Dimensioni massime dati I/O per RPI
- Latenza e Instabilità infrastruttura di rete
- Velocità / Duplex (potenziale incongruenza)
- Ambiente – ad esempio, interferenze EMI

Rappresenta circa il 10% della banda totale della rete

RIEPILOGO DEI VANTAGGI

- Singola tecnologia di rete industriale per:
  - Convergenza su unica rete multidisciplinare - Discreti, Processi Continui, Batch, Azionamenti, Sicurezza, Controllo di Moto, Potenza, Sincronizzazione dei tempi, Supervisione, Configurazione/Diagnostica degli asset e Gestione dell'Energia
- Consolidata – oltre 375 fornitori, con oltre 7,500,000 nodi installati
  - Riduzione Rischi – ampia disponibilità di prodotti, applicazioni e supporto fornitori
  - Supportata – Valori di priorità QoS dei dispositivi EtherNet/IP™ predefiniti
- Standard – IEEE 802.3 Ethernet e IETF TCP/IP Protocol Suite
  - Abilita l'integrazione di IAT ed IT – voce, video e dati - tools comuni (risorse per progettazione, installazione e ricerca guasti) e competenze/addestramento (risorsa umana)
  - Tecnologia IT standard – Servizi di rete Layer 2 e Layer 3 standard, Segmentazione (VLANs), Prioritizzazione (QoS), Topologie a Percorsi Ridondanti con Protocolli di Resilienza
  - Indipendenza dai media e dalle Topologie – flessibilità e scelta
  - Topologie a livello di nodo ed a livello switch; rame - fibra - wireless
- Portabilità e instradamento – condivisione informazioni trasparente su impianto / sito
  - Nessuna mappatura dati – progettazione semplificata, installazione rapida, riduzione rischi

RIEPILOGO DEI VANTAGGI

- Singola tecnologia di rete industriale per:
  - Convergenza su unica rete multidisciplinare - Discreti, Processi Continui, Batch, Azionamenti, Sicurezza, Controllo di Moto, Potenza, Sincronizzazione dei tempi, Supervisione, Configurazione/Diagnostica [illegible] stione dell'Energia
- Consolidata – oltre 375 fornitori, con ol[illegible] nodi installati
  - Riduzion[illegible] a disponibilità di pr[illegible] oni e supporto fornitori
  - Support[illegible] orità QoS dei dispositivi EtherNet/IP™ predefiniti
- Standard – IEEE 802.3 Ethernet e IETF TCP/IP Protocol Suite
  - Abilita l'integrazione d[illegible] IAT ed IT – voce, video e dati - tools comuni (risorse per progettazione, installazione e ric[illegible] ompetenze/addestramento (risorsa umana)
  - Tecnologia IT standard – Servizi di rete Layer 2 e Layer 3 standard, Segmentazione (VLANs), Prioritizzazione (QoS), Topologie a Percorsi Ridondanti con Protocolli di Resilienza
  - Indipendenza dai media e dalle Topologie – flessibilità e scelta
  - Topologie a livello di nodo ed a livello switch; rame - fibra - wireless
- Portabilità e instradamento – condivisione informazioni trasparente su impianto / sito
  - Nessuna mappatura dati – progettazione semplificata, installazione rapida, riduzione rischi

Industrial Automation Technology

Internet Engineering Task Force

Information Technology

Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

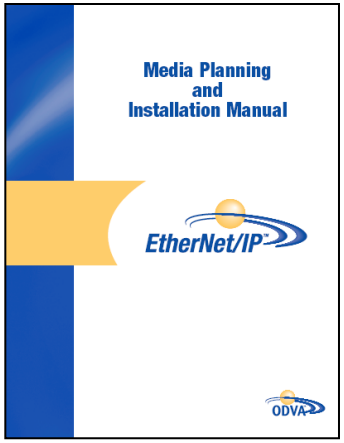
- Progettare ed implementare un layer fisico robusto
- Classificazione Ambientale MICE
- Più di un Cavo
  - Connettori
  - Pannelli per Patching
  - Gestione Cavi
  - Mitigazione disturbi
    - Messa a terra, Ancoraggio e Schermatura
- Media Fisici Standard
  - Cablati vs. Wireless
  - Rame vs. Fibra
  - UTP vs. STP
  - Singlemode vs. Multimode
  - SFP – LC vs. SC
- Scelta Topologie Standard
  - Switch-Level e Device-Level

M = Mechanical rating (mechanical load, shock, vibration, pressure, impact)

I = Ingress rating (penetration of foreign particles, dust, dampness, immersion)

C = Climatic rating (climatic load, radiation, liquids, gases, contamination)

E = Electromagnetic rating (electrostatic, electromagnetic and similar loads)



Guida ODVA

Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

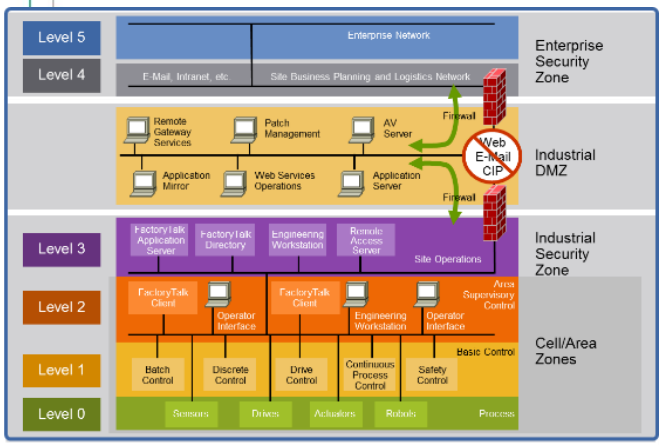
- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

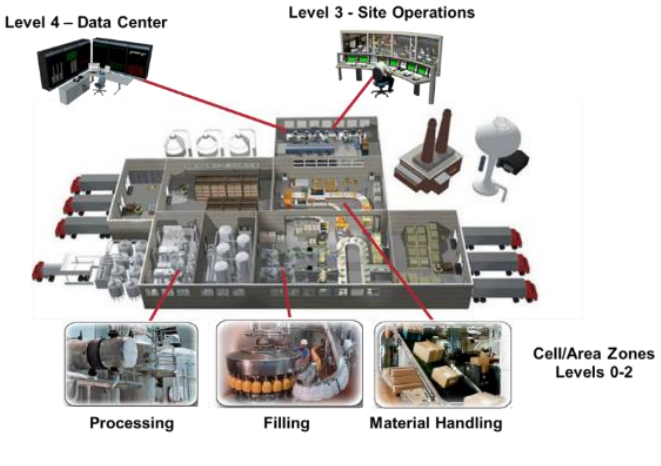
- Struttura di rete modulare a blocchi per permettere: 1) minimizzare la crescita disordinata della rete 2) Costruire un'infrastruttura scalabile, infrastruttura di rete robusta e pronta per applicazioni future
  - Fault domains contenuti (ad esempio, loops di Layer 2)
  - Dominii broadcast limitati
  - Dominii attendibili più contenuti (security)
- Tecniche multiple per creare blocchi di rete più piccoli (dominii Layer 2)
  - Struttura e gerarchia
    - Modelli logici – organizzazione geografica e funzionale per nodi di IACS
    - Modello di rete campus – modelli di switch multilivello – Layer 2 e Layer 3
    - Quadro logico
  - Segmentazione
    - Network interface cards multiple (NICs) – ad esempio, CIP bridge
    - Apparecchiature per Network Address Translation (NAT)
    - Virtual Local Area Networks (VLANs)
    - VLANs con funzioni NAT

- Struttura di rete modulare a blocchi per permettere: 1) minimizzare la crescita disordinata della rete 2) Costruire un'infrastruttura scalabile, infrastruttura di rete robusta e pronta per applicazioni future
  - Fault domains contenuti (ad esempio, loops di Layer 2)
  - Dominii broadcast limitati
  - Dominii attendibili più contenuti (security)
- Tecniche multiple per creare blocchi di rete più piccoli (dominii Lay
  - Struttura e gerarchia
    - Modelli logici – organizzazione geografica e funzionale per nodi d
    - Modello di rete campus – modelli di switch multilivello – Layer 2 e Layer 3
    - Quadro logico
  - Segmentazione
    - Network interface cards multiple (NICs) – ad esempio, CIP bridge
    - Apparecchiature per Network Address Translation (NAT)
    - Virtual Local Area Networks (VLANs)
    - VLANs con funzioni NAT

Industrial Automation Control System

IACS





Wide Area Network (WAN)
Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager

Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Physical or Virtualized Servers
- FactoryTalk® Application Servers and Services Platform
- Network Services – for example DNS, AD, DHCP, AAA
- Call Manager
- Storage Array

Site Operations Level 3

Enterprise
Internet
External DMZ/ Firewall

Enterprise Zone Levels 4 and 5

Link for Failover Detection
Catalyst 2960
Fire wall (Acti ve)
Firew all (Stan dby)
ASA 5500

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

Industrial Demilitarized Zone (IDMZ)

RADIUS (AAA) Server
UCS
Acti
5500 Wireless LAN Controller (WLC)
Stan dby
Remote Access Server
Catalyst 6500/4500
Catalyst 3750X StackWise Switch Stack

Industrial Zone Levels 0–3

Cell/Area Zone Levels 0–2
Cell/Area Zone Levels 0–2

Cam era
Pho ne
LWAP
WG
SSID 5 GHz
LWAP
WG
Cont roller
Cont roller
Ethernet/IP

Cell/Area Zone Levels 0–2 Redundant Star Topology - Flex Links Resiliency Unified Wireless LAN

LWAP
SSID 2.4 GHz
HMI
Soft Starter
Drive
Cont roller
I/O
Instrumentation
Ethernet/IP

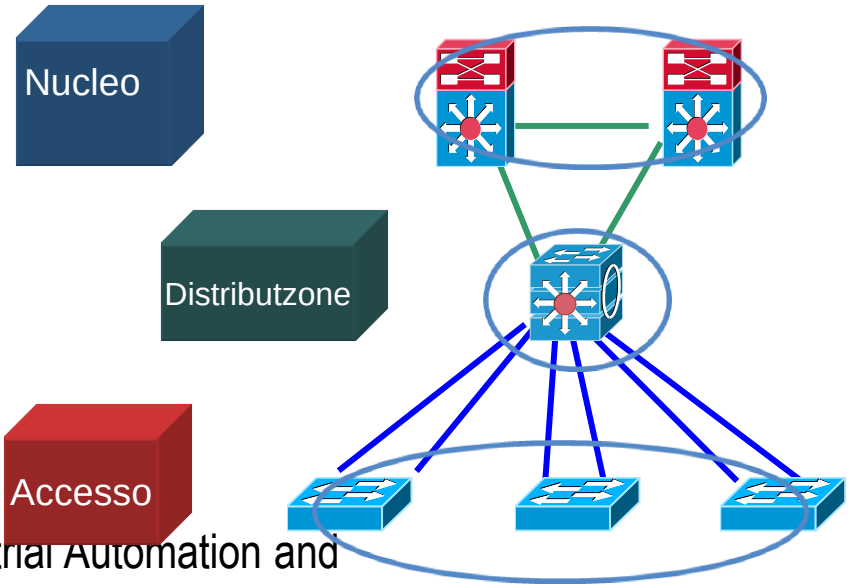
Cell/Area Zone - Levels 0–2 Ring Topology - Resilient Ethernet Protocol (REP) Unified Wireless LAN

Safety Cont roller
Safety I/O
Servo Drive
HMI
Robot
AP
SSID 5 GHz
WGB
Safety I/O
Ethernet/IP

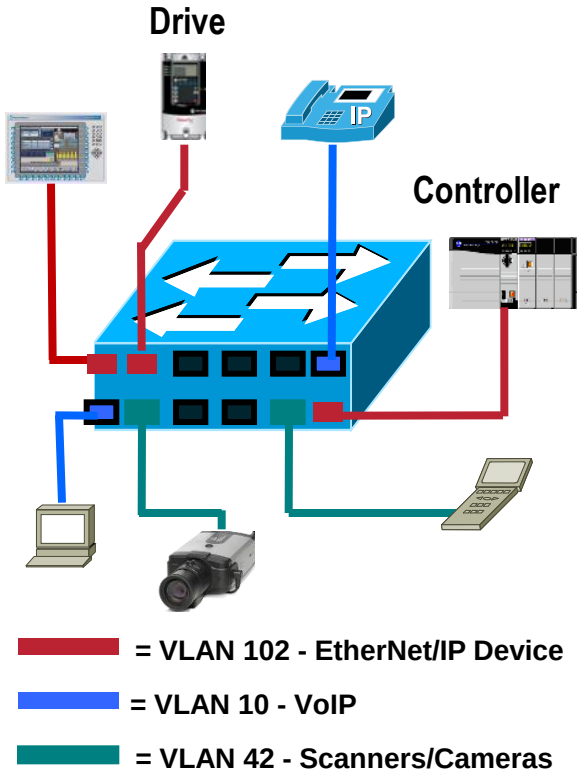
Cell/Area Zone - Levels 0–2 Linear/Bus/Star Topology Autonomous Wireless LAN

- Blocchi strutturali gerarchici, modulari e scalabili
- Creazione di dominii contenuti – demarcazione e segmentazione chiari
  - Dominii di errore (ad esempio, loops di Layer 2), dominii di broadcast, dominii di “fiducia” [naturalmente “trust”] (security)

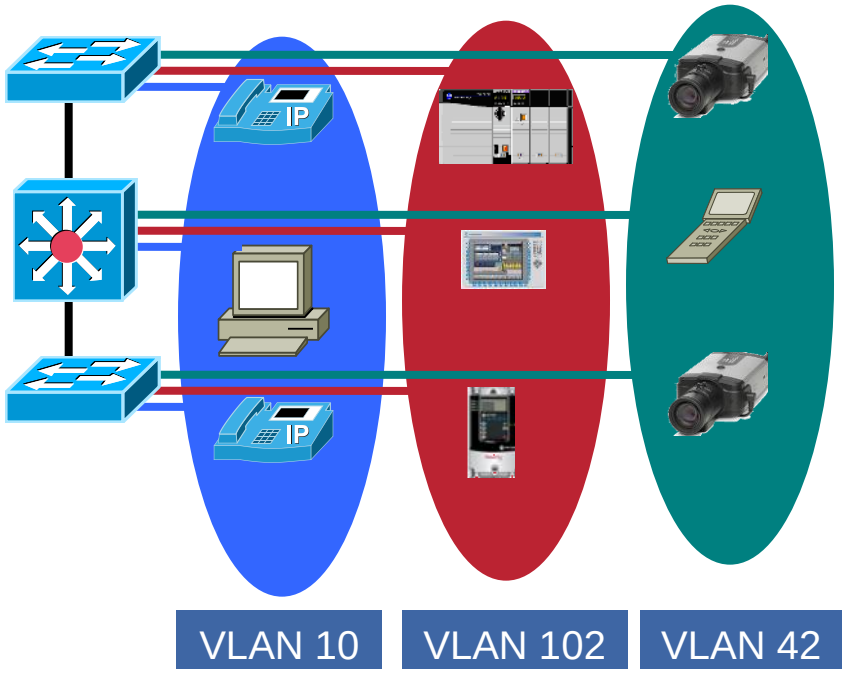
- Semplice da espandere, comprendere e per la ricerca guasti
- Modelli di switch multilivello
  - Nucleo
    - Switch di distribuzione aggregati
    - Dorsale di rete
    - Connettività di tipo Industrial DMZ
  - Distribuzione
    - Switch di accesso aggregati
    - Fornisce servizi di Layer 3
  - Accesso
    - Aggregazione di componenti dei vari Industrial Automation and Control System (IACS)
    - Fornsce servizi di Layer



- Servizi di rete di Layer 2, VLANs segmentare una rete in modo logico senza le restrizioni delle connessioni fisiche
  - VLAN stablita all'interno o attraverso switches
- I dati sono spediti solo alle porte all'interno della stessa VLAN
  - I nodi all'interno di ogni VLAN possono comunicare con altri nodi sulla stessa VLAN
- Segmentare il traffico per limitare comunicazioni broadcast e multicast non desiderate
- Software configurabile attraverso switches di tipo managed
- Benefici
  - Facilità di cambiamenti di rete – riduzione dei cablaggi di rete
  - Semplificazione gestione della sicurezza di rete - dominii fiduciari
  - Aumento dell'efficienza



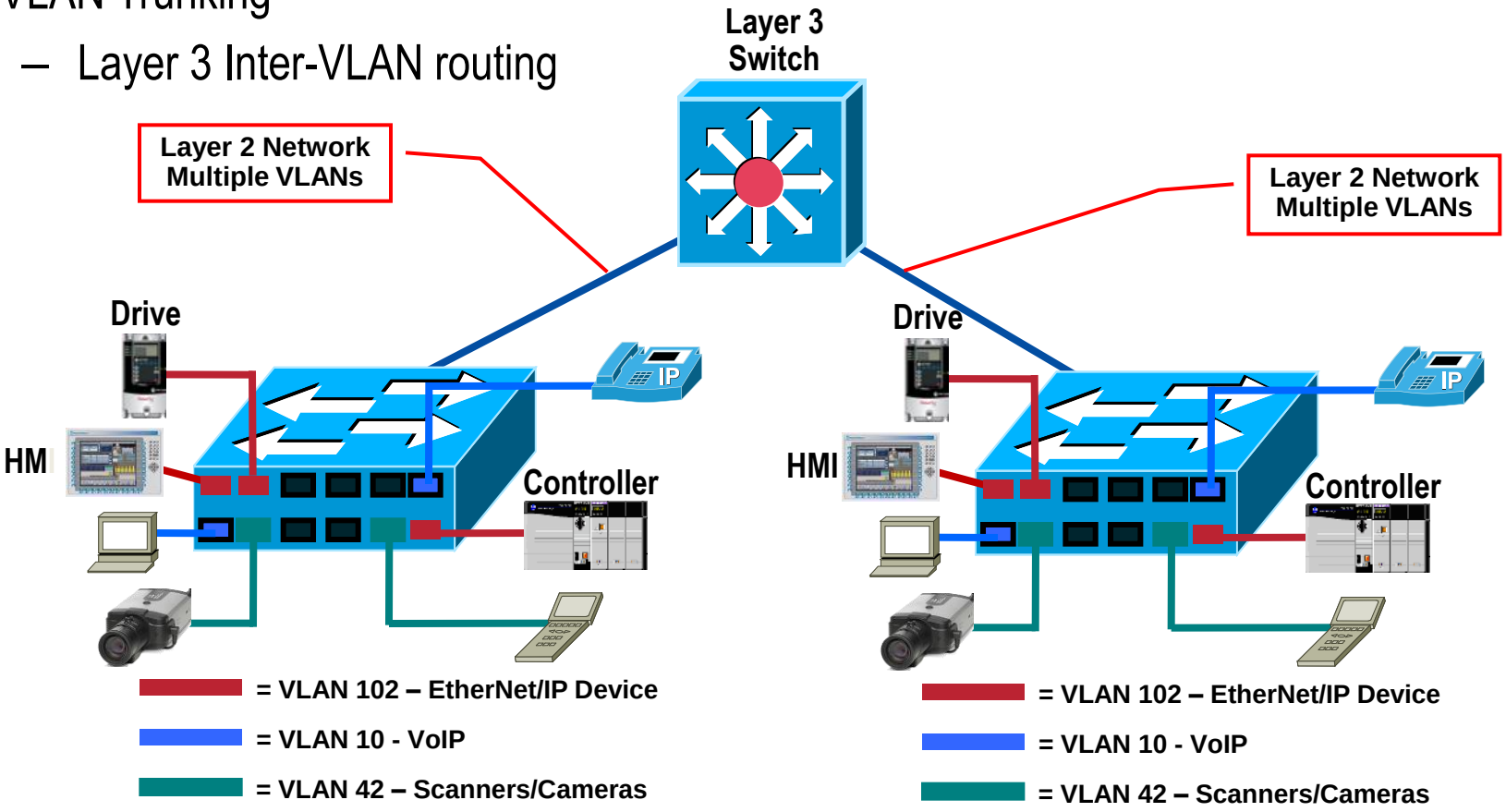
- Layer 2 VLAN Trunking
  - Independente dalla posizione fisica dello switch
  - Raggruppamento logico degli assets per tipo, ruolo, area logica, area fisica o un ibrido delle due
  - I nodi comunicano come se fossero sullo stesso segment fisico – nessuna modifica di cablaggio richiesta



- Software configurabile utilizzando switches managed
- Un device di Layer 3 (Router o switch Layer 3) per trasferire il traffic tra VLANs diverse
  - Inter-VLAN routing

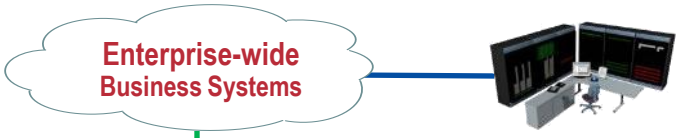
Segmentazione
Virtual Local Area Networks (VLANs)

- Switch Multi-Layer di Layer 2
  VLAN Trunking
  - Layer 3 Inter-VLAN routing



Nessuna Segmentazione (Sconsigliato)

Plant-wide / Site-wide Network



Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

Industrial Zone
Levels 0-3

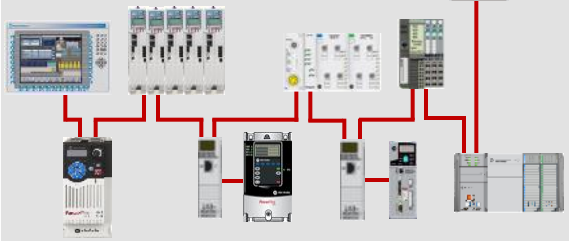
EtherNet/IP™

Level 3 - Site Operations

Physical or Virtualized Servers
- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

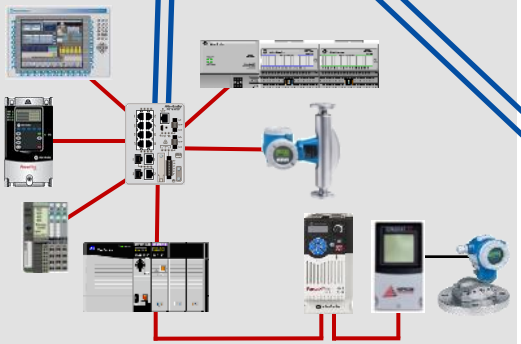
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address

Cell/Area Zones
Levels 0-2



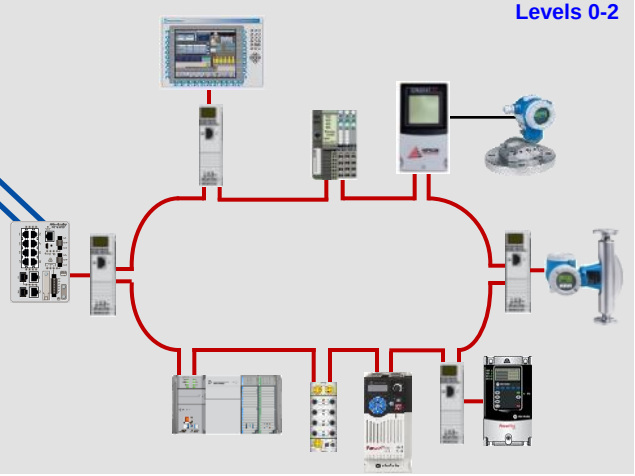
Cell/Area Zone #1
Subnet 10.17.10.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #2
Subnet 10.17.10.0/24

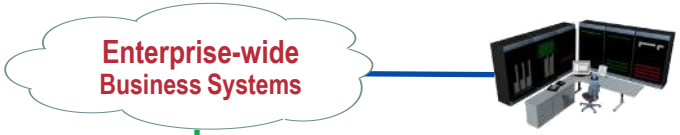
Cell/Area Zones
Levels 0-2



Cell/Area Zone #3
Subnet 10.17.10.0/24

Segmentazione NIC Multiple

Plant-wide/Site-wide Network



Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

Industrial Zone
Levels 0-3

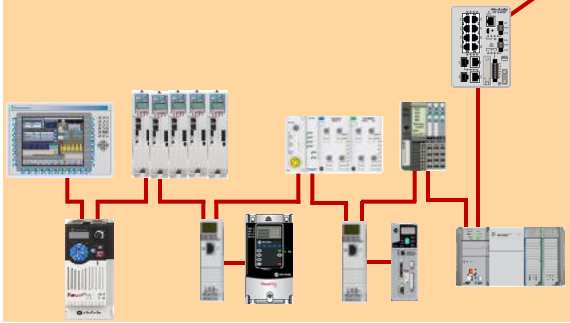
EtherNet/IP™

Level 3 - Site Operations

Physical or Virtualized Servers
- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

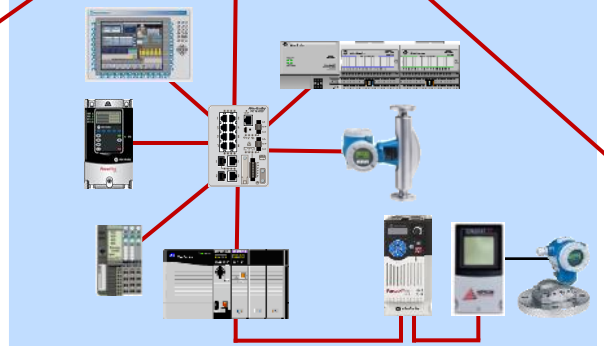
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

Cell/Area Zones
Levels 0-2



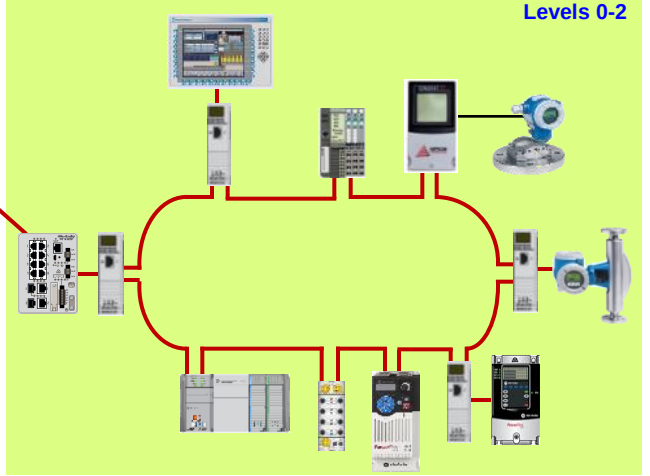
Cell/Area Zone #1
Subnet 192.168.1.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #2
Subnet 192.168.1.0/24

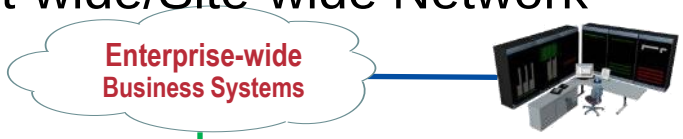
Cell/Area Zones
Levels 0-2



Cell/Area Zone #3
Subnet 192.168.1.0/24

Segmentazione Apparecchiature con NAT

Plant-wide/Site-wide Network



Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

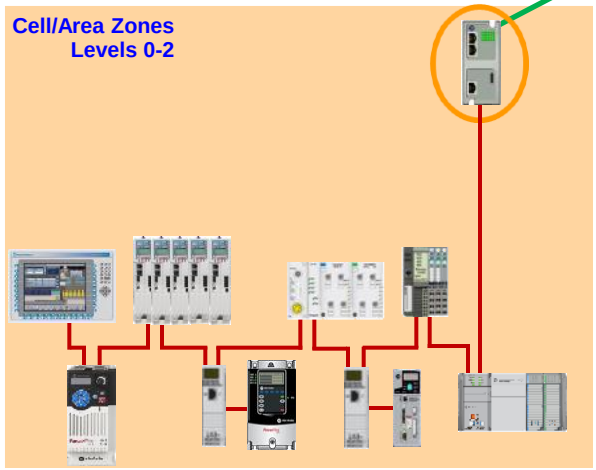
Industrial Zone
Levels 0-3

EtherNet/IP™

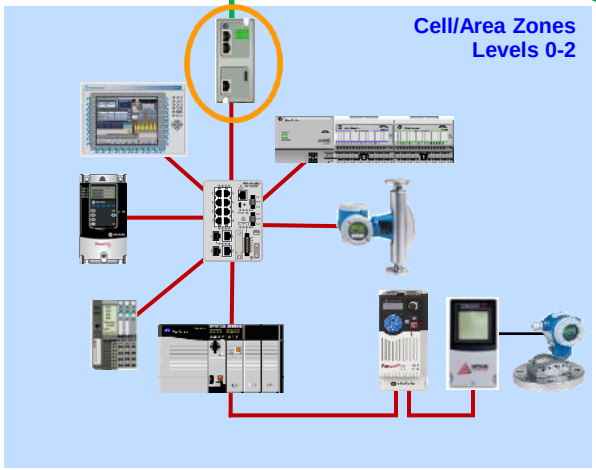
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

Level 3 - Site Operations

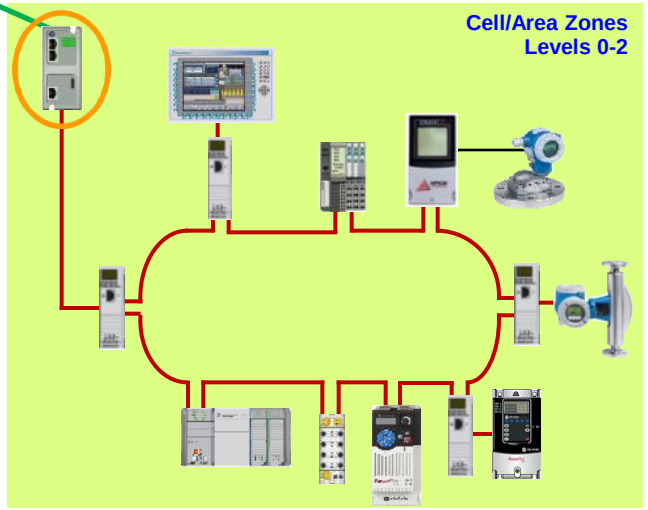
Physical or Virtualized Servers
- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array



Cell/Area Zone #1
Subnet 192.168.1.0/24

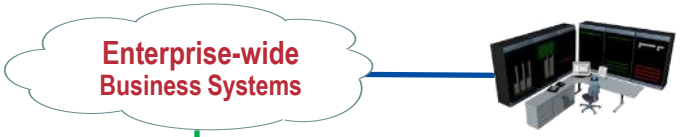


Cell/Area Zone #2
Subnet 192.168.1.0/24



Cell/Area Zone #3
Subnet 192.168.1.0/24

Servizi di Segmentazione Integrati nel Router
Plant-wide/Site-wide Network



Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

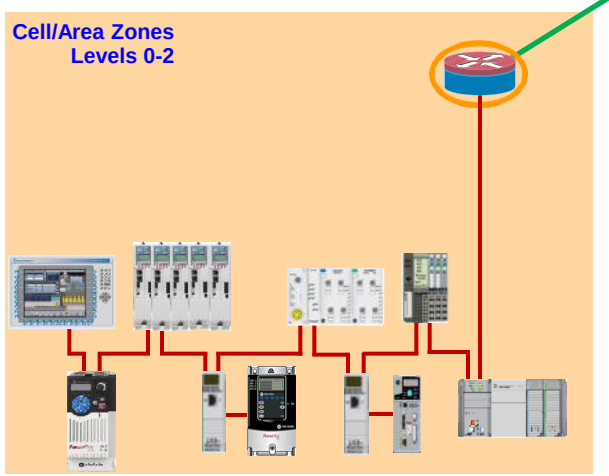
Industrial Zone
Levels 0-3

EtherNet/IP™

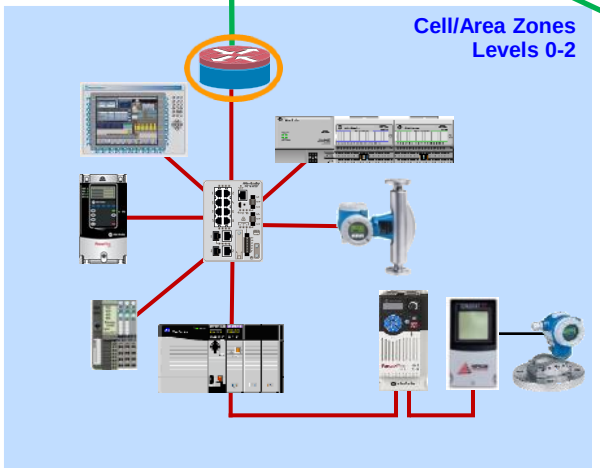
Level 3 - Site Operations

Physical or Virtualized Servers
- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

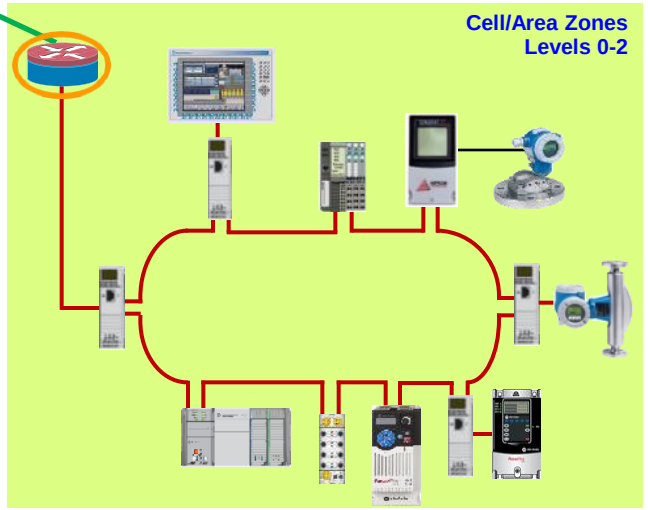
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24



Cell/Area Zone #1
Subnet 192.168.1.0/24



Cell/Area Zone #2
Subnet 192.168.1.0/24



Cell/Area Zone #3
Subnet 192.168.1.0/24

Segmentazioen VLAN senza NAT
Plant-wide/Site-wide Network

Enterprise-wide
Business Systems

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

EtherNet/IP™

Plant-wide
Site-wide
Operation Systems

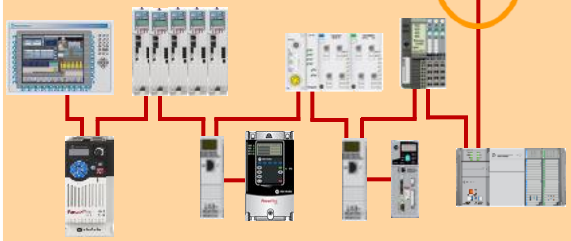
Level 3 - Site Operations

Industrial Zone
Levels 0-3

Physical or Virtualized Servers
- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

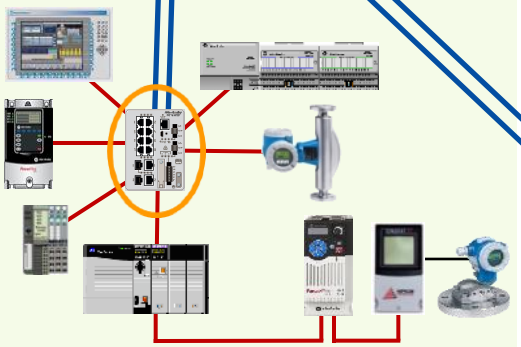
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address

Cell/Area Zones
Levels 0-2



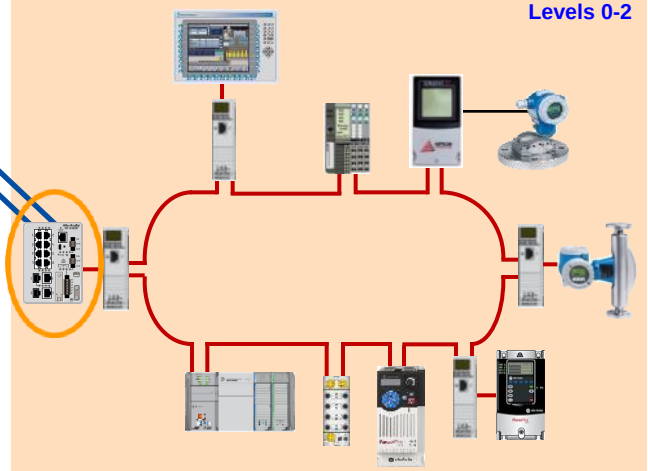
Cell/Area Zone #1
VLAN10
Subnet 10.10.10.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #2
VLAN20
Subnet 10.10.20.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #3
VLAN30
Subnet 10.10.30.0/24

Segmentazione VLAN con NAT

Plant-wide/Site-wide Network

ANIE AUTOMAZIONE

Enterprise-wide
Business Systems

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

Industrial Zone
Levels 0-3

EtherNet/IP™

Plant-wide
Site-wide
Operation Systems

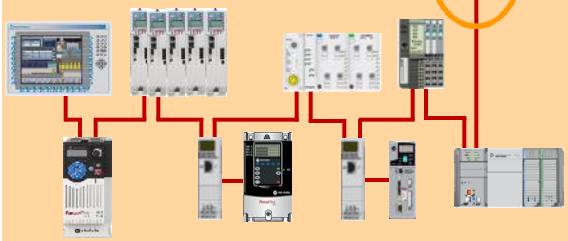
Level 3 - Site Operations

Physical or Virtualized Servers

- Application Servers and Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

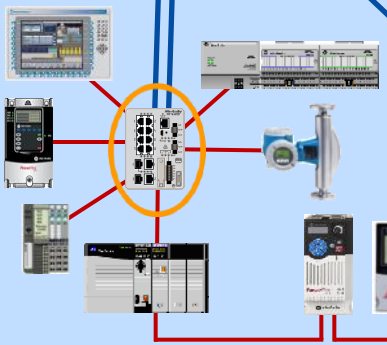
- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

Cell/Area Zones
Levels 0-2



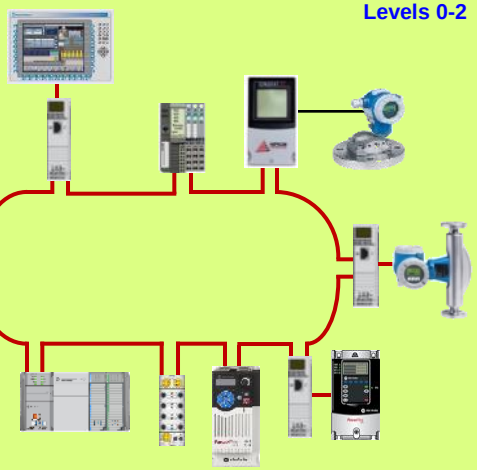
Cell/Area Zone #1
VLAN10
Subnet 192.168.1.0/24

Cell/Area Zones
Levels 0-2



Cell/Area Zone #2
VLAN20
Subnet 192.168.1.0/24

Cell/Area Zones
Levels 0-2

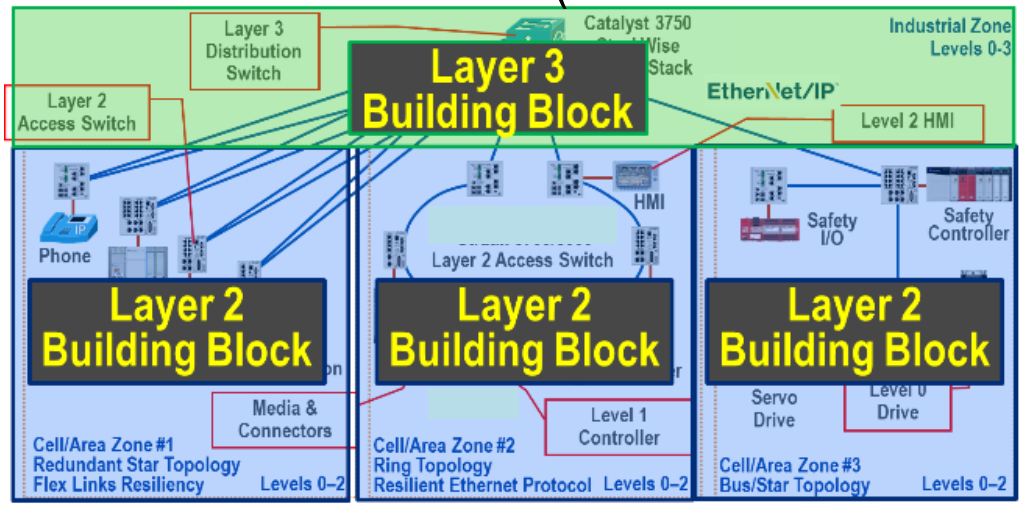


Cell/Area Zone #3
VLAN30
Subnet 192.168.1.0/24

Segmentazione di Rete

Considerazioni di Progetto e Implementazione

- Progettare blocchi strutturali contenuti per aiutare a 1) minimizzare la crescita disordinata della rete e 2) costruire un'infrastruttura di rete scalabile, robusta e pronta per applicazioni future
  - Dominii di guasto delimitati (ad esempio, loops di Layer 2)
  - Dominii di broadcast limitati
  - Dominii di "fiducia" (trust) delimitati (security)
- Tecniche multiple per costruire sezioni di rete limitate (dominii di Layer 2)
  - Struttura e gerarchia
  - Segmentazione



- VLANs
  - Segmentare tipi di traffic diversi su VLANs separate (CIP, VoIP, HTTP)
  - Creare sottoreti IP più limitate per ogni VLAN
  - All'interno di una stessa Cella/Area
    - Utilizzare segmenti VLAN di Layer 2 tra switches con tipologie di traffico simili
    - Quando si segmenta, utilizzare 802.1Q, VTP in modalità trasparente
  - Utilizzare le funzioni di routing/switching Inter-VLAN di Layer 3
    - Tra VLANs all'interno della stessa Cella/Area
    - Tra zone
  - Assegnare tipologie di traffico diverse ad un'unica VLAN, diversa dalla VLAN 1

- VLAN
  - Se … VLANs separate (CIP, VoIP, HTTP)
  - Cr … gni VLAN
  - All …
    - … 2 tra switches con tipologie di traffico simili
    - Quando si segmenta, utilizzare 802.1Q VTP in modalità trasparente
  - Utilizzare le funzioni di routi…
    - Tra VLANs all'interno della s…
    - Tra zone
  - Assegnare tipologie di traffi… dalla VLAN 1

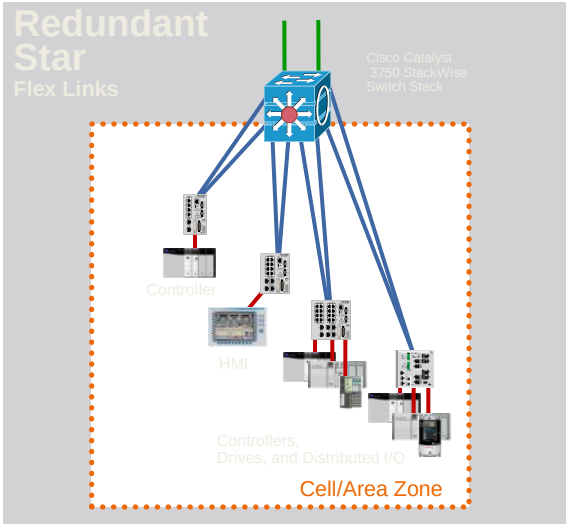
802.1q è il protocollo di segmentazione utilizzato per inviare diversi VLAN-ID (tagged or untagged) attraverso un altro link ad un router, uno switch o un server

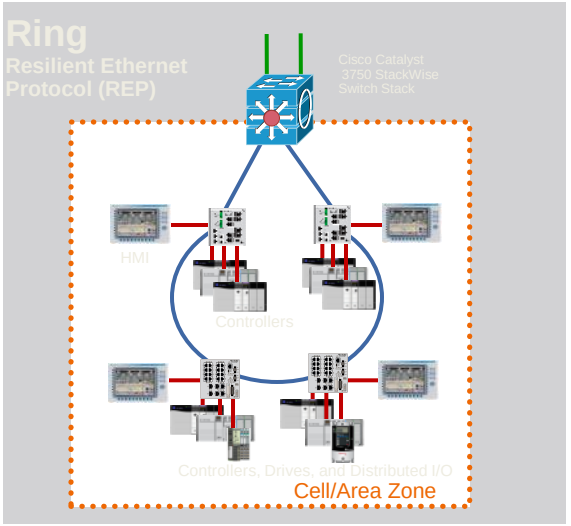
VTP è un protocollo di condivisione delle informazioni, utilizzato per inviare informazioni RELATIVE alla VLAN sulla rete gestita da switches Cisco. E' un protocollo proprietario utilizzato solo da Cisco. *VTP non può essere usato come protocollo di segmentazione.* VTP può essere utilizzato in modalità server, client o in modalità trasparente per condividere informazioni

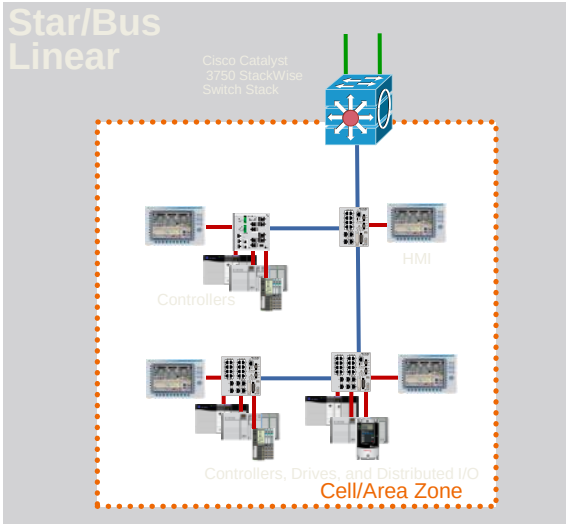
Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

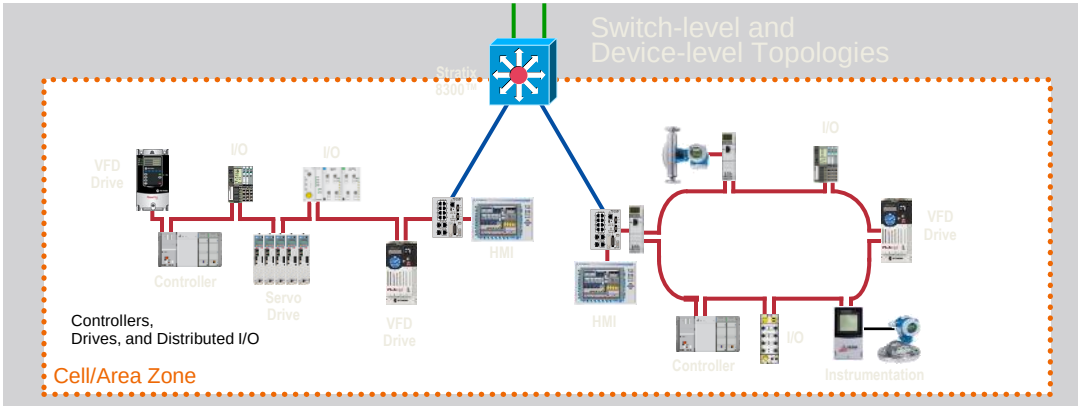
Topologie a livello Switch



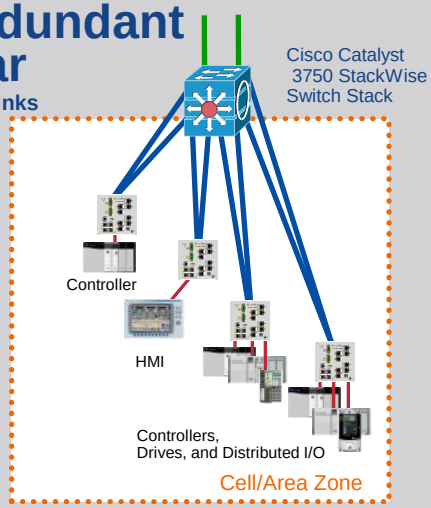




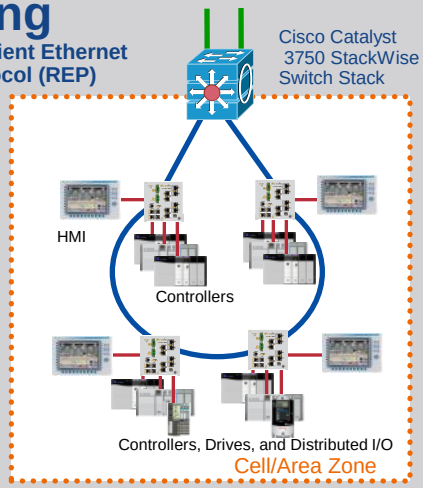
Topologie a livello Nodo



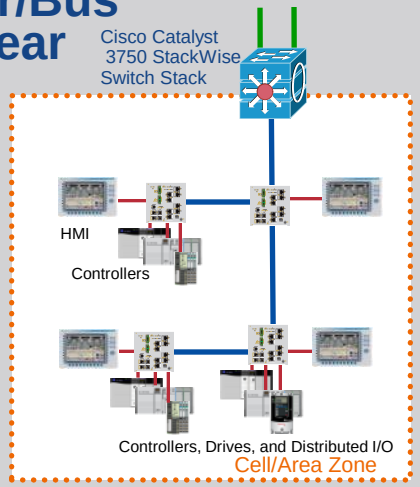
Redundant Star
Flex Links



Ring
Resilient Ethernet Protocol (REP)



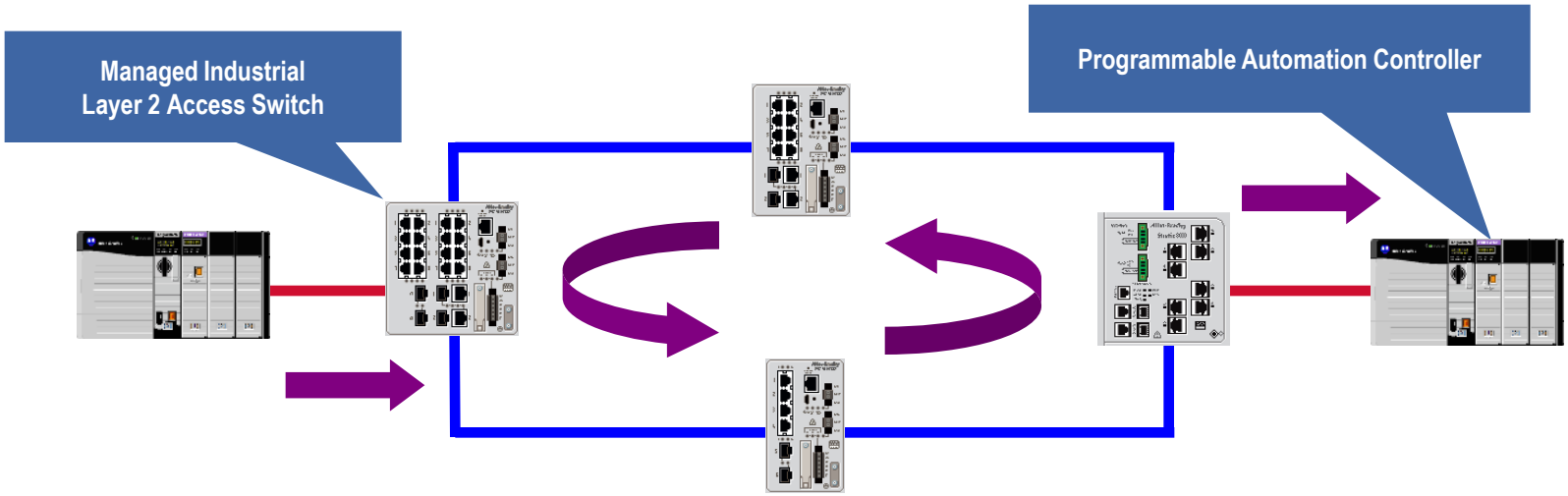
Star/Bus Linear



	Redundant Star	Ring	Linear
Requisiti di Cablaggio			
Facilità di Configurazione			
Implementazione Costi			
Larghezza di Banda			
Ridondanza e Integrità			
Turbative Durante Aggiornamenti di Rete			
Rapidità di Ristabilimento della Rete			
Prestazioni e TCO della Rete	**Migliore**	**Accettabile**	**Peggiore**

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

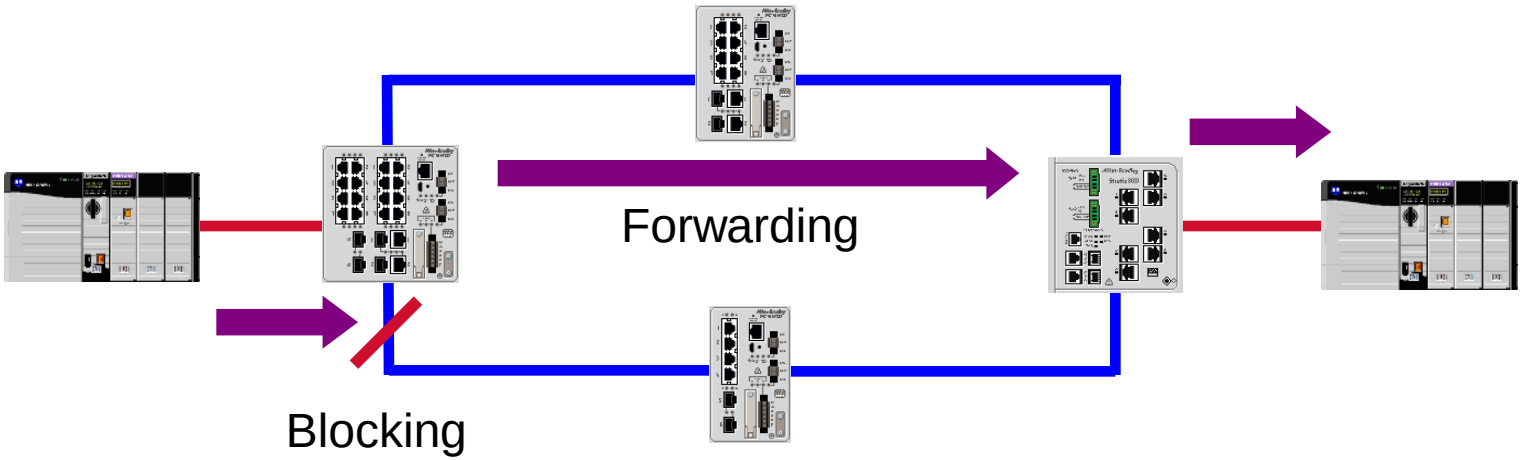
Evitare I loop



- Percorsi ridondanti creano un loop switching (bridging) loop
  - Senza una configurazione appropriata, un loop genererà una trasmissione incontrollata, saturando la rete, utilizzando così TUTTA la banda disponibile, rendendo inutilizzabile una rete gestita da switch di Layer 2 (bridged)
    - I frames Ethernet di Layer 2 non hanno il time-to-live (TTL)
    - Un frame di Layer 2 frame può richiudersi su se stesso per sempre…

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

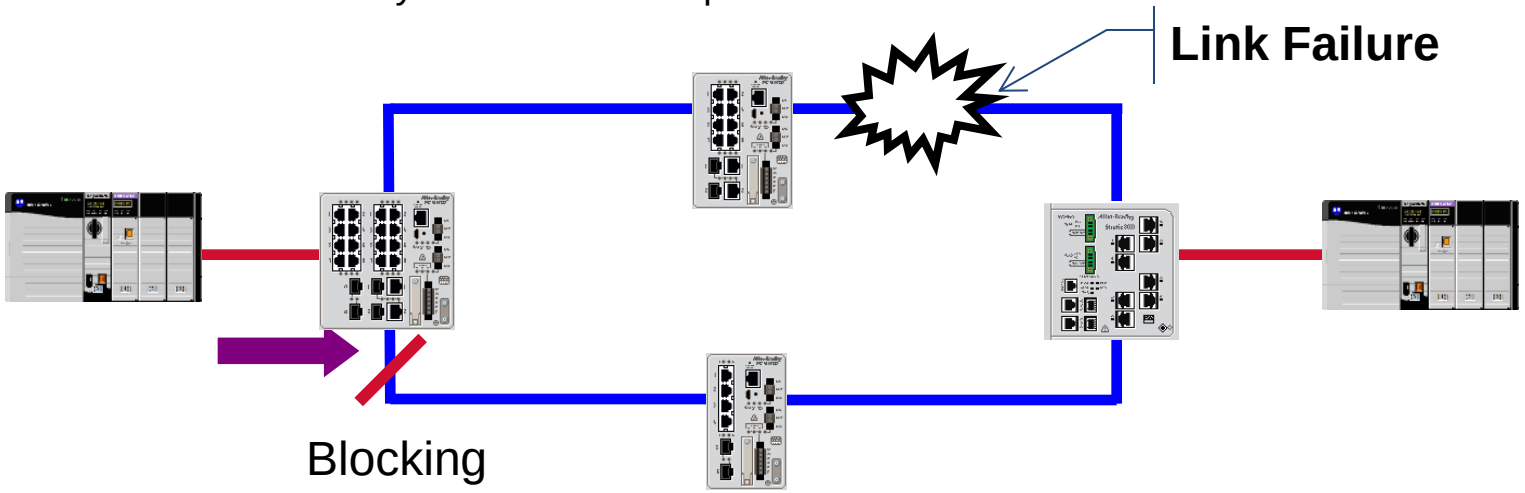
Layer 2 - evitare I loop



- Un protocollo di resilienza di Layer 2 gestisce percorsi ridondanti evitando la creazione di loop switching (bridging)

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

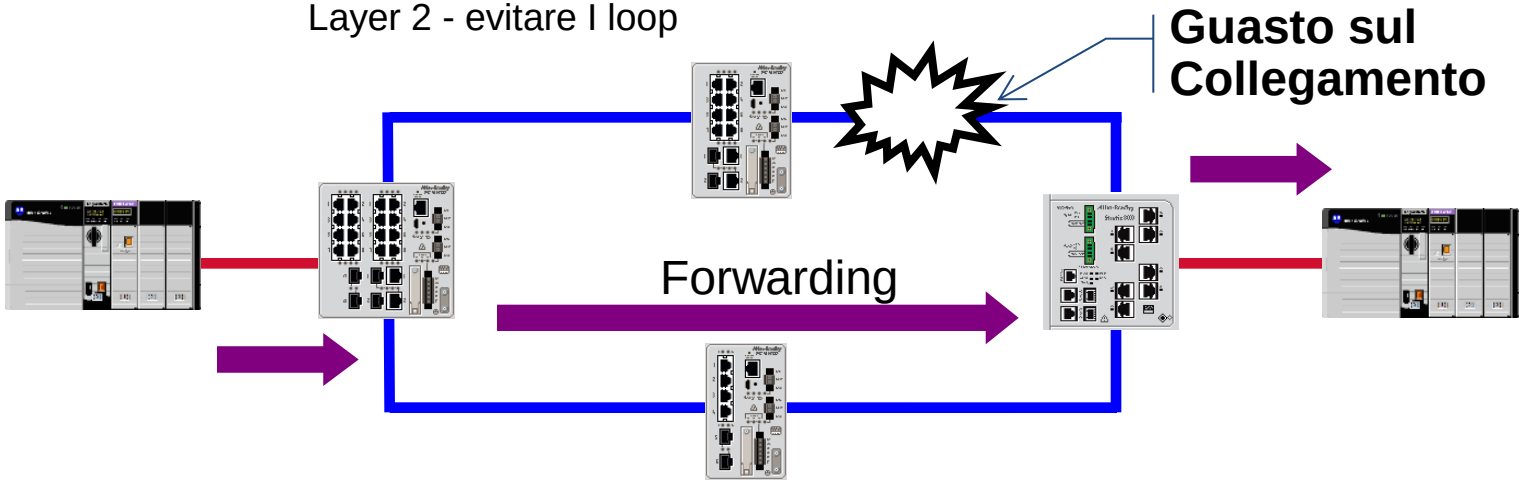
Layer 2 - evitare I loop



- Il ristabilimento della rete (ristabilimento funzionalità, recupero, e così via) deve avvenire prima che la funzionalità dell'Industrial Automation and Control System (IACS) venga impattata

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

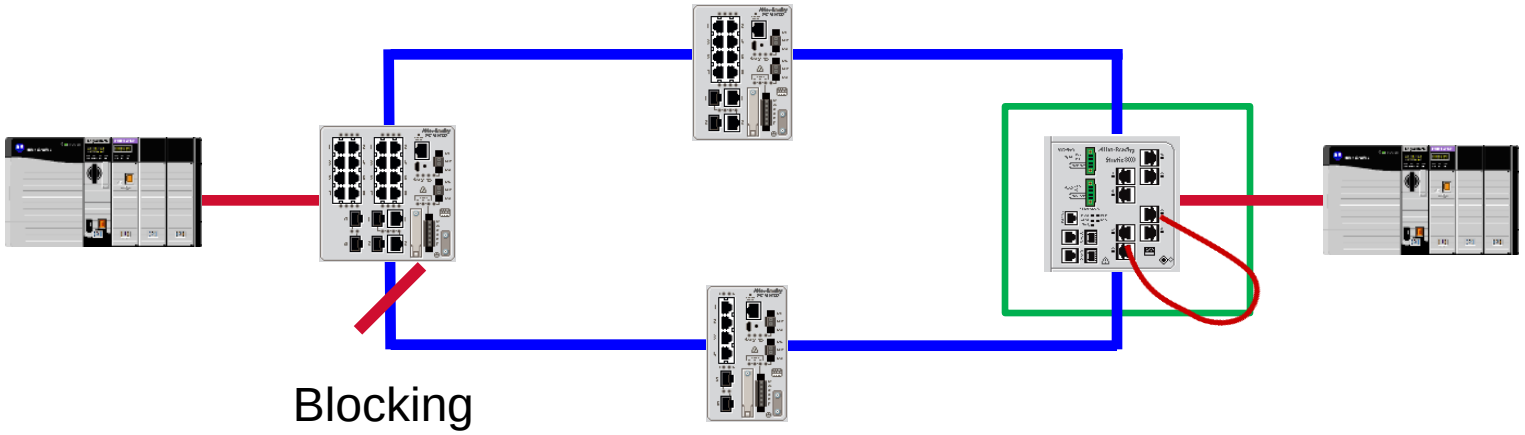
Layer 2 - evitare I loop



- Il ristabilimento della rete deve avvenire in tempi suffcientemente veloci da evitare il timeout della connessione dei controllori:
  - Tempo tipico di una istruzione di Message (MSG) - Esplicito, CIP Classe 3
    - Timeout istruzione – valore di default 30 secondi
  - TAG prodotti e consumati ed I/O - Implicito, CIP Classe 1
    - Timeout connessione - 4 x RPI, con un minimo di 100 ms
  - I/O di Sicurezza - Implicito, CIP Classe 1
    - Timeout connessione - 4 x RPI di default

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

Layer 2 - evitare I loop



- Da NON dimenticare il rischio potenziale di loops sullo stesso switch

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

- Industrial rispetto COTS
- Managed rispetto Unmanaged

	Vantaggi	Svantaggi
Switches Managed	▪ Prevenzione Loop ▪ Servizi di Security ▪ Informazioni di diagnostica ▪ Servizi di segmentazione (VLANs) ▪ Prioritizzazione servizi (QoS) ▪ Resilienza di rete ▪ Servizi di gestione Multicast	▪ Più costosi ▪ Richiedono della configurazione delle conoscenze tecniche specifiche allo start up
Switches Unmanaged	▪ Economici ▪ Semplici da impostare	▪ Nessuna prevenzione di loop ▪ Nessun servizio di security ▪ Nessuna informazione di diagnostica ▪ Nessuna servizio di segmentazione o prioritizzazione ▪ Ricerca problem difficoltosa ▪ Nessun support resilienza di rete
ODVA Embedded Switch Technology	▪ Semplificazione cablaggi e riduzione costi ▪ Prevenzione creazione loop e disponibilità resilienza di rete ▪ Servizi di prioritizzazione (QoS) ▪ Servizi di Time Sync (IEEE 1588 PTP Transparent Clock) ▪ Informazioni diagnostiche ▪ Gestione dei servizi multicast	▪ Possibilità di gestione limitate ▪ Potrebbe richeidere una configurazione minima

Topologie con Percorsi Ridondanti e Proto ienza

- Industrial rispetto COTS
- Managed rispetto Unmana

Commercial Off The Shelf

	Vantaggi	Svantaggi
Switches Managed	▪ Prevenzione Loop ▪ Servizi di Security ▪ Informazioni di diagnostica ▪ Servizi di segmentazione (VLANs) ▪ Prioritizzazione servizi (QoS) ▪ Resilienza di rete ▪ Servizi di gestione Multicast	▪ Più costosi ▪ Richiedono della configurazione delle conoscenze tecniche specifiche allo start up
Switches Unmanaged	▪ Economici ▪ Semplici da impostare	▪ Nessuna prevenzione di loop ▪ Nessun servizio di security ▪ Nessuna informazione di diagnostica ▪ Nessuna servizio di segmentazione o prioritizzazione ▪ Ricerca problem difficoltosa ▪ Nessun support resilienza di rete
ODVA Embedded Switch Technology	▪ Semplificazione cablaggi e riduzione costi ▪ Prevenzione creazione loop e disponibilità resilienza di rete ▪ Servizi di prioritizzazione (QoS) ▪ Servizi di Time Sync (IEEE 1588 PTP Transparent Clock) ▪ Informazioni diagnostiche ▪ Gestione dei servizi multicast	▪ Possibilità di gestione limitate ▪ Potrebbe richeidere una configurazione minima

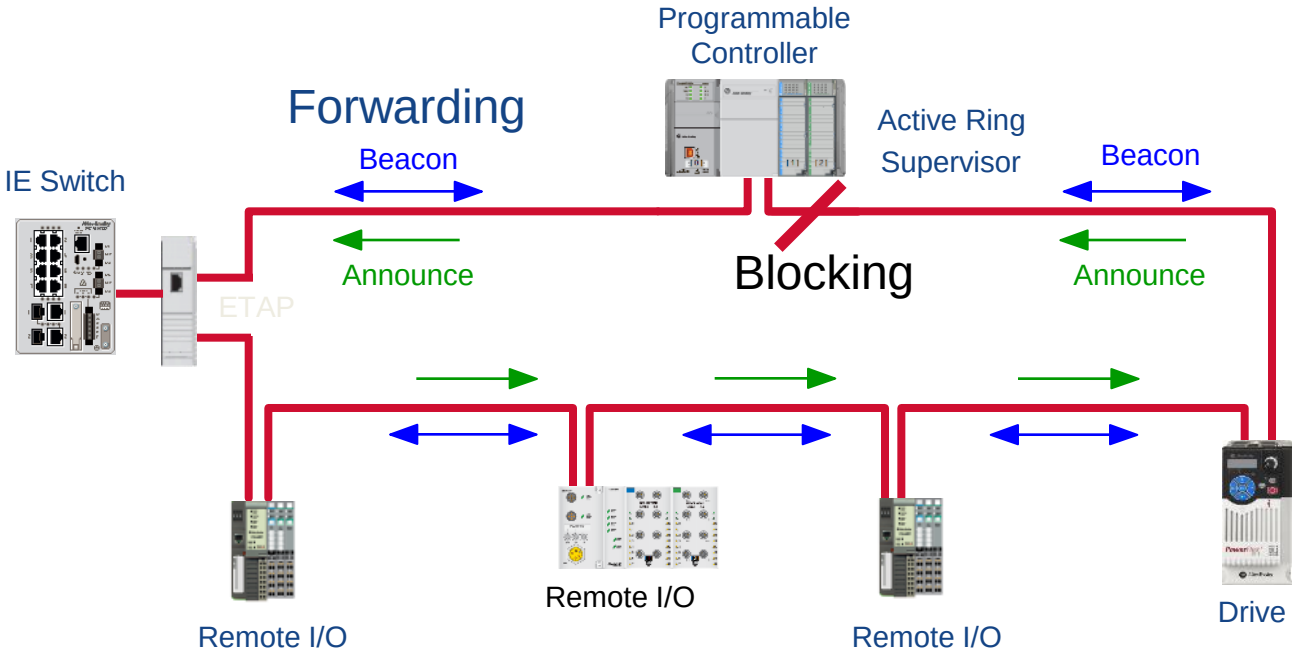
Protocolli con Resilienza di Rete

L'Applicazione Guida la Scelta

Protocollo di Resilienza	Vari Fornitori	Ring	Redundant Star	Network Convergence > 250 ms	Network Convergence 60–100 ms	Network Convergence 1–3 ms	Layer 3	Layer 2
STP (802.1D)	X	X	X					X
RSTP (802.1w)	X	X	X	X				X
MSTP (802.1 s)	X	X	X	X				X
rPVST+		X	X	X				X
REP		X			X			X
EtherChannel (LACP 802.3ad)	X		X		X			X
Flex Links			X		X			X
DLR (IEC and ODVA)	X	X				X		X
StackWise		X	X			X	X	X
HSRP		X	X	X			X	
GLBP		X	X	X			X	
VRRP (IETF RFC 3768)	X	X	X	X			X	

Ristabilimento della Rete

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

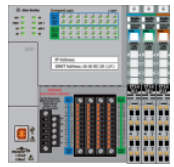


Topologia con Device Level Ring e Protocollo Device Level Ring

- Il Supervisore blocca il traffico su una porta
- Spedisce pacchetti di riferimento (beacon frame) su entrambe le porte per rilevare l'interruzione sull'anello
- Ristabilito l'anello, il supervisore riceve I pacchetti su entrembe le porte iniziando la transizione al modo normale, bloccando una porta

Topologie con Percorsi Ridondanti e Protocolli di Resilienza



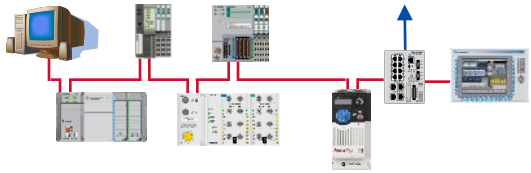
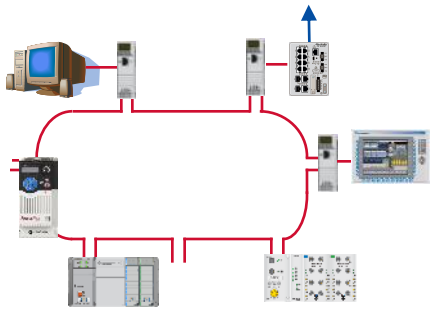







- ODVA – uno standard aperto che consente ai fornitori di sviluppare prodotti compatibili
- Supporta topologie lineari e ad anello, implementate sia su rame che su fibra
- Il traffic di rete viene gestito per assicurare la trasmissione dei dati critici nei tempi necessari (Quality of Service, IEEE-1588 Precision Time Protocol, Multicast Management)

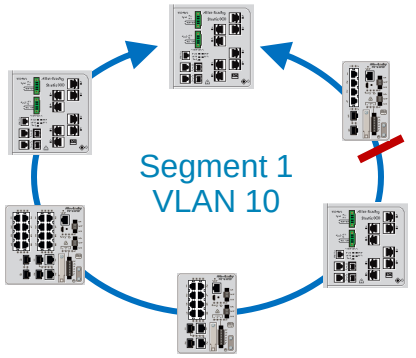
- L'anello è una rete fault tolerant al singolo guasto
- Progettata per un ristabilimento delle comunicazioni in 1-3 ms per reti EtherNet/IP™ semplici

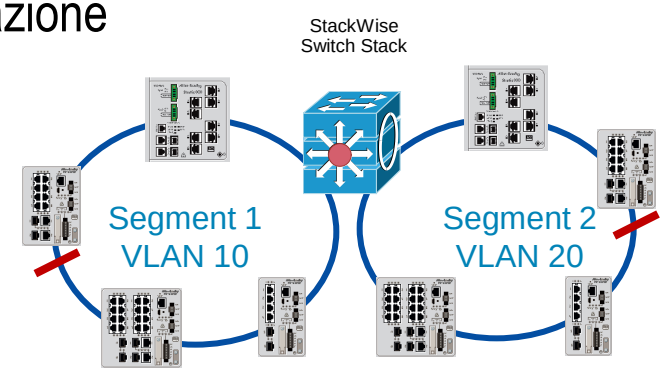



EtherNet/IP™ ODVA™

Topologie con Percorsi Ridondanti e Protocolli di Resilienza

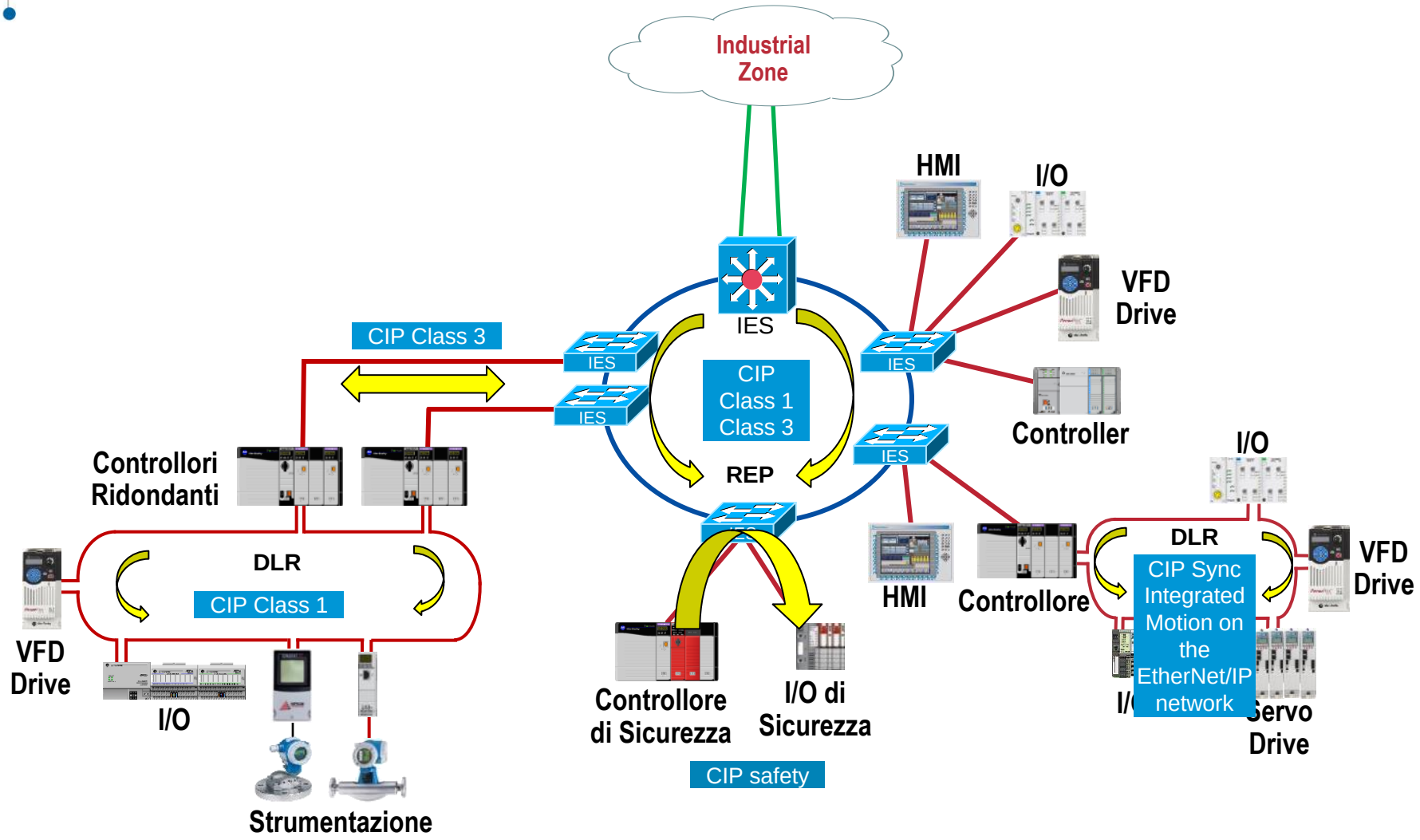
- Un segment REP è una catena di porte di switch connessi uno all'altro e configurati con lo stesso ID per segment REP
- Topolgie di percorsi ad anello ridondati a livello di switch possono essere costruite utilizzando segmenti REP, L'anello è una rete fault tolerant al singolo guasto
- Il protocollo REP è adatto ad applicazioni di IACS che possono sopportare tempi di ripristino della rete fino a 100 ms (su interface che utilizzano la fibra).
- E' il solo protocollo resiliente che può essere utilizzato a livello di switch ed utilizzabile sia con applicazioni di Automazione Industriale che con applicazioni in ambito IT





Resilient Ethernet Protocol

Esempio di architettura



Resilient Ethernet Protocol

Considerazioni di Progetto e di Implementazione

- Il protocollo REP consente un rapido recupero della rete (recupero da guasto) rispetto ai protocolli RPVST+ o MSTP per una topologia ad anello degli switch
- Il protocollo REP è adatto ad applicazioni IACS che possono sopportare interruzioni di rete fino a 100 ms (con interface in fibra)
  - Connessioni HMI
  - Connessioni Prodotte/Consumate, di I/O con un RPI lento
  - Non è bumpless per RPIs veloci
- Per applicazioni IACS che richiedono tempi di ripristino più veloci possono essere usate o una topologia di switch a stella ridondante con protocollo di resilienza Flex Links, oppure una topologia tipo Device Level Ring utilizzando il protocollo di resilienza ODVA DLR
- Utilizzare la fibra come media ed il transceiver SFPs per tutti I collegamenti tra switch – Sia per topologie ad anello che a stella

Resilient Ethernet Protocol

Considerazioni di Progetto e di Implementazione

- Il protocollo REP consente un rapido recupero della rete (recupero da guasto) rispetto ai protocolli RPVST+ o MSTP per una topologia ad anello degli switch
- Il protocollo REP è adatto ad applicazioni IACS che possono sopportare interruzioni di rete fino a 100 ms (con interface in fibra)
  - Connessioni HMI
  - Connessioni Prodotte/Consumate, di I/O con un RPI lento
  - Non è bumpless per RPIs veloci
- Per applicazioni IACS che richiedono tempi di ripristino più veloci possono essere usate o una topologia di switch a stella ridonda[illegible]collo di resilienza Flex Links, oppure una topologia tipo Devic[illegible] utilizzando il protocollo di resilienza ODVA DLR
- Utilizzare la fibra come media ed il transceiver SFPs per tutti i collegamenti tra switch – Sia per topologie ad anello che a stella

Small Form-Factor Pluggable transceiver

Resilient Ethernet Protocol

Considerazioni di Progetto e di Implementazione

- La scelta della Topologia Ridondante e del Protocollo di Resilienza dipende dall'applicazione
  - Topologie sia a livello di Switch che a livello di Nodo
  - Topologia ad anello rispetto alla Topologia a Stella Ridondante
  - Ambiente misto, più fornitori di switch – Migrazione di prodotti esistenti
  - Dispersione geografica dei nodi EtherNet/IP™ del Sistema IACS
  - Posizionamento gerarchico nell'architettura - Layer 2 rispetto a Layer 3
  - Prestazioni
    - Tolleranza a: tempo di ripristino della rete, Perdita di Pacchetti, Latenza e Instabilità

Resilient Ethernet Protocol

Considerazioni di Progetto e di Implementazione

- Utilizzare fibra e SFPs per I collegamenti tra switch – topologie ad anello e a stella ridondante
- Utilizzare MSTP per la distribuzione su switch di fornitori diversi, in topologie a stella ridondante o ad anello, con CIP™ explicit messaging ad es. Per HMI, o unicast CIP implicit per applicazioni di I/O con un RPI maggiore o uguale a 100 ms
- Utilizzare Flex Links per la distribuzione, di topologie a stella ridondante, con trasmissione unicast o multicast per applicazioni di I/O CIP implicit msg
- Utilizzare REP per la distribuzione su switch, topologia ad anello a livello di switch, unicast per applicazioni di I/O CIP implicit msg
- Utilizzare DLR per topologia ad anello a livello di nodi, e per applicazioni come CIP safety, Ridondanza dei Controllori, applicazioni in multicast di I/O CIP e Integrated Motion su rete EtherNet/IP™

Resilient Ethernet Protocol

Considerazioni di Progetto e di Implementazione

Multiple Spanning Tree Protocol

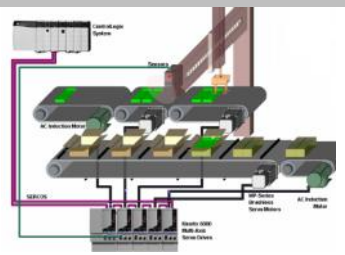
- Utilizzare fibra e [illegible] llegamenti tra switch – topologie ad anello e a stella ridondan
- Utilizzare MSTP per la distribuzione su switch di fornitori diversi, in topologie a stella ridondante o ad anello, con CIP™ explicit messaging ad es. Per HMI, o unicast CIP implicit per applicazioni di I/O con un RPI maggiore o uguale a 100 ms
- Utilizzare Flex Links per la distribuzione, di topologie a stella ridondante, con trasmissione unicast o multicast per applicazioni di I/O CIP implicit msg
- Utilizzare REP per la distribuzione su switch, topologia ad anello a livello di switch, unicast per applicazioni di I/O CIP implicit msg
- Utilizzare DLR per topologia ad anello a livello di nodi, e per applicazioni come CIP safety, Ridondanza dei Controllori, applicazioni in multicast di I/O CIP e Integrated Motion su rete EtherNet/IP™

Educare, utilizzare line guida e considerazioni progettuali per aiutare a ridurre **Latenze** e **Instabilità** (Latency e Jitter), aumentare Disponibiltà, Integrità e Confidenzialità dei dati. Tutto per ottenere una soluzione di rete EtherNet/IP ™ con infrastruttura **Scalabile**, **Robusta**, **Sicura** e pronta per il **Futuro**:

- Tecnologia per una rete industriale singola
- Livello fisico robusto
- Segmentazione / Struttura (blocchi modulari e scalabili)
- Prioritizzazione - Quality of Service (QoS)
- Topologie a percorsi ridondanti con protocolli di Resilienza
- Time Synchronization – PTP, CIP Sync e Motion Integrato sulla rete EtherNet/IP
- Gestione del Multicast
- Soluzioni per il ripristino della rete
- Sicurezza – Difesa-in-profondità secondo il modello olistico
- Accesso Remoto Scalabile e Sicuro
- Wireless – 802.11

Soluzioni per il Ripristino della Rete

Allestimento nuove linee, ad esempio, Macchine



Sistema di Controllo
Plant-wide Industrial Automation Systems

Allestimento nuove linee, ad esempio, Skid di Processo

Plant-wide / Site-wide Industrial Automation Systems

- Considerazioni di progetto e dispiegamento che un fornitore affidabile (ad esempio, OEM, SI, Appaltatore) deve prendere in considerazione per ottenere un'integrazione senza soluzione di continuità della sua fornitura (ad esempio, macchina, skid) all'interno dell'infrastruttura di rete dell'impianto o del reparto del cliente

Il dialogo bidirezionale e precoce è CRITICO !

Soluzioni per il Ripristino della Rete

Considerazioni di Progetto e Implementazione

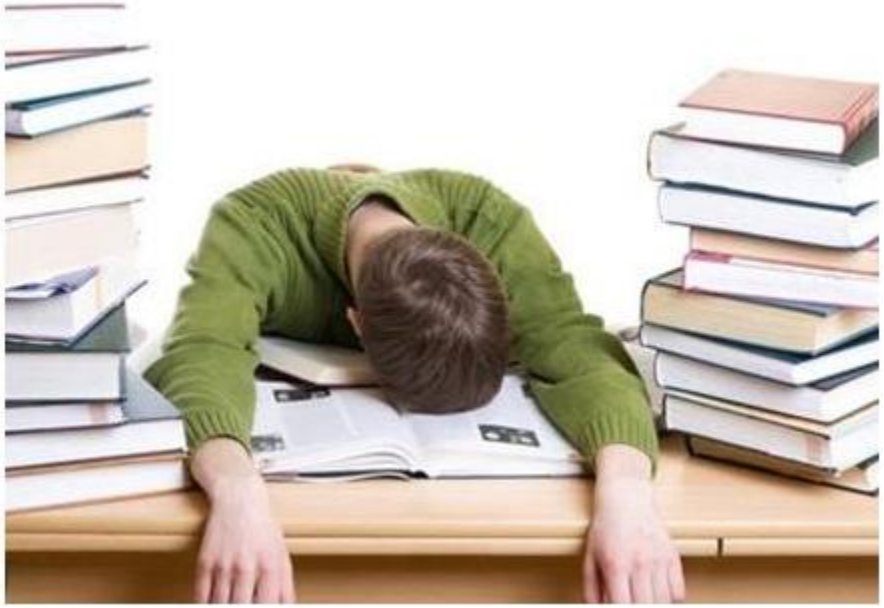
- Utilizzo di una sola tecnologia di rete industriale basata su standard Ethernet e tecnologia IP per l'infrastruttura in una rete multidisciplinare
  - Infrastruttura commune di rete – utilizzo degli asset
  - Pronta per sviluppi futuri - sostenibilità
- Schema di indirizzamento IP
  - Chi lo gestisce? L'utilizzatore finale (OT/IT) o l'OEM?
  - Gamma di indirizzi (class), subnet, default gateway (routability)
  - Convenzioni di Implementazione – statico/dinamico, configurabile via hardware/software, NAT/DNS
- Utilizzo dei Servizi di Rete
  - Managed switches, topologie a livello switch e a livello device
  - Segmentazione, prioritizzazione dei dati
  - Disponibilità – prevenzione di loop, topologie a percorso ridondante con protocolli di resilienza
  - Servizi di Time Synchronization
    - IEEE 1588 Precision Time Protocol (PTP w/E2E)
    - Applicazioni CIP Sync – primo guasto, SOE, Integrated Motion sulla rete EtherNet/IP™

Soluzioni per il Ripristino della Rete

Considerazioni di Progetto e Implementazione

- Posizionamento della Security – allineamento con l'utilizzatore finale: procedure di business e operative, standards corporate e locali, politiche di sicurezza (security) industriale, tolleranza al rischio, stato attuale dell'infrastruttura di rete
  - Accesso fisico, sicurezza delle porte, access control lists, applicazioni di security, accesso remoto
  - Allineamento agli standards di sicurezza indutriali per i Sistemi di Automazione e Controllo Industriali (IACS) come ISA/IEC-62443 (ex ISA99) e NIST 800-82

Grazie per l'attenzione



E ora mi spengo...prometto !