ANIE AUTOMAZIONE

ANIE FEDERAZIONE

CONFINDUSTRIA

# Guida per il Networking industriale

Maggio 2017

ANIE Automazione

# Guida per il Networking industriale

Maggio 2017

I lavori per realizzazione della Guida si sono chiusi a maggio 2017.

# Prefazione

I principali settori dell'economia industriale stanno subendo una profonda trasformazione determinata dalla possibilità per i robot, veicoli e sistemi di controllo industriale di connettersi a Internet. Questa tendenza sta portando al raggiungimento di livelli di automazione senza precedenti in tutti i processi aziendali. Siamo difatti entrati nell'era della quarta rivoluzione industriale, più comunemente nota come Industria 4.0, in cui la tecnologia del Web pervade la macchina e viceversa al fine di rendere le fabbriche sempre più intelligenti.

In quest'ultimo decennio è diventata sempre più marcata la tendenza a decentrare l'automazione industriale per gestire strutture di impianto con minori oneri di installazione, manutenzione, controllo e diagnostica. Ciò grazie alla disponibilità locale di apparecchiature intelligenti e alla loro connessione in rete.
Lo sviluppo della tecnologia di gestione remota dei sistemi di automazione allarga progressivamente i confini del controllo tradizionalmente conosciuto modificando la fisionomia dei modelli dell'automazione industriale. La classica struttura piramidale si sta appiattendo per via della veloce emancipazione dei dispositivi di campo, della progressiva ascesa della tecnologia di rete Ethernet anche verso tali apparati, delle dinamiche del mercato delle reti industriali basate sull'evoluzione dell'intelligenza a bordo, e del consolidamento e diffusione del Web anche tra le macchine che snellisce il controllo e favorisce l'utilizzo, anche da remoto, delle stazioni di monitoraggio e supervisione integrando i processi di automazione con l'IT.

In questo scenario in cui le macchine sono sempre online con persone e processi, e dove l'utilizzo sempre più diffuso di smart device favorisce la rapida diffusione delle informazioni e la loro condivisione tra i vari dispositivi, la macchina diventa l'attore principale che si occupa di avvisare gli operatori sul campo sul proprio stato diminuendo i tempi morti ed i fermi macchina. Diventa quindi essenziale utilizzare soluzioni d'automazione con elevato valore aggiunto. La trasversalità dei moduli Web Server oggi disponibili, grazie alle loro funzioni (SMS, Email, FTP, http client/server, Open VPN, pagine HTML/AJAX) e all'integrabilità nelle reti cablate o wireless (GSM/GPRS/HSPA) mediante protocolli standard di comunicazione (Modbus RTU, Modbus TCP, SNMP, IEC60870-5-104) rappresentano poi lo strumento ideale per soddisfare queste esigenze.

Le applicazioni di automazione industriale richiedono pertanto una soluzione di Networking omogenea, che possa integrare i dati di processo e diagnostica con la rete IT di stabilimento; la sicurezza dati e la sicurezza funzionale; PLC, I/O distribuiti e azionamenti con dispositivi standard Ethernet (PC, telecamere, router per accesso remoto via web).

Il Networking  industriale assume una rilevanza forse superiore ad altre tecnologie abilitanti a seguito della crescente attenzione verso queste nuove impostazioni organizzative di fabbrica volte a integrare i componenti della macchina o dell'impianto in un sistema in rete.

In Italia, grazie anche al piano del Governo volto ad incentivare gli investimenti privati in tecnologie e beni I4.0, si stanno ponendo le basi di un nuovo modello di gestione della manifattura "intelligente". Ciò alimenta importanti aspettative nel settore manifatturiero ed effettivamente questo strumento potrebbe attivare notevoli investimenti nel settore della meccanica strumentale con ricadute anche sui

fornitori di tecnologie.
Dall'insieme di queste considerazioni nasce il progetto del WG Networking di ANIE Automazione di realizzare una Guida al fine di offrire al lettore una panoramica sullo stato dell'arte delle tecnologie che concorrono all'infrastruttura di rete per la comunicazione industriale.
Il volume è organizzato in due sezioni: una prettamente tecnologica ed una dedicata alla presentazione di casi applicativi. Nella prima parte vengono descritti i principali aspetti tecnologici alla base del Networking industriale: dopo un'introduzione generale sul tema, si passa all'approfondimento di specifici aspetti quali l'Industrial Ethernet, l'infrastruttura di rete e la security; segue poi un capitolo dedicato alla normativa di riferimento, e un glossario nel quale si esplicita il significato di termini e parole chiave.
Nella seconda parte della Guida, vengono riportate le testimonianze dei principali fornitori di tecnologie di comunicazione in ambito industriale con case history relativi a varie applicazioni che consentono di comprendere meglio i benefici che derivano dalla scelta di determinate soluzioni.

Il lettore che approccia per la prima volta il tema può quindi trovare in questa Guida indicazioni utili ad apprendere rapidamente i principi fondamentali della tecnologia e delle sue possibili applicazioni per la gestione della produzione e dei processi aziendali in un'ottica 4.0.

*WG Networking industriale*
*di ANIE Automazione*

# ANIE Automazione e il WG Networking industriale

Ad ANIE Automazione aderiscono le imprese, piccole medie e grandi, produttrici di beni e di servizi operanti nel campo dell'automazione manifatturiera, di processo e delle reti di pubblica utilità. ANIE Automazione è una delle 13 Associazioni di settore di ANIE - Federazione Nazionale delle Imprese Elettrotecniche ed Elettroniche, aderente a Confindustria.

L'Associazione attraverso i suoi Gruppi rappresenta, sostiene e tutela le aziende che svolgono attività nei seguenti comparti merceologici:

- Automazione di processo
- Azionamenti Elettrici
- Componenti e Tecnologie per la Misura e il Controllo
- HMI-IPC-SCADA
- Meccatronica
- PLC-I/O
- Software Industriale
- Telecontrollo, Supervisione e Automazione delle Reti
- Telematica applicata a Traffico e Trasporti
- UPS - Gruppi Statici di Continuità

Nel Gruppo Componenti e Tecnologie per la Misura e il Controllo rientra il WG Networking industriale cui partecipano i principali fornitori di tecnologia ed esperti del settore, con l'obiettivo di:

- diffondere informazioni chiarificatrici su caratteristiche e applicabilità delle tecnologie che concorrono all'infrastruttura di rete per la comunicazione industriale;
- interfacciarsi con enti deputati alla regolamentazione dell'uso delle varie apparecchiature;
- condividere e supportare gli sviluppi normativi;
- quantificare e studiare il mercato.

Ciò attraverso la pubblicazione di articoli tecnologici sulla stampa specializzata; la realizzazione di guide esplicative; la partecipazione a fiere ed eventi di settore con iniziative dedicate; la promozione di giornate di studio e di approfondimento tecnologico; le attività di *lobby* e di monitoraggio dei lavori normativi nelle sedi competenti; indagini statistiche e analisi di mercato.

# Indice


1. Il Networking nelle applicazioni di Automazione Industriale pag. 6

2. Da Ethernet a Industrial Ethernet pag. 8
- 2.1 Cenni a caratteristiche di base del protocollo Ethernet pag. 8
- 2.2 Industrial Ethernet pag. 9
  - 2.2.1 Real Time Ethernet: Determinismo e Isocronia pag. 10
  - 2.2.2 Caratteristiche tecniche dei dispositivi pag. 11

3. Infrastruttura di rete Industrial Ethernet pag. 12
- 3.1 Caratteristiche di base pag. 12
  - 3.1.1 Tipologia di prodotti pag. 12
  - 3.1.2 Topologia di rete pag. 14
  - 3.1.3 Cablaggio pag. 17
  - 3.1.4 Comunicazione Wireless pag. 20
- 3.2 Caratteristiche specifiche pag. 21
  - 3.2.1 VLAN pag. 21
  - 3.2.2 Ridondanza pag. 22
  - 3.2.3 Routing pag. 25
  - 3.2.4 NAT pag. 26

4. Safety su reti Industrial Ethernet pag. 27
- 4.1 L'approccio "black channel" dei protocolli di scurezza pag. 27
- 4.2 Accenni e Profili Safety pag. 27

5. Security su reti Industrial Ethernet pag. 31
- 5.1 I rischi pag. 31
- 5.2 I concetti generali di protezione pag. 31
- 5.3 I sistemi di protezione pag. 31
  - 5.3.1 Port Security pag. 32
  - 5.3.2 VLAN pag. 32
  - 5.3.3 SNMP pag. 33
  - 5.3.4 HTTPS pag. 33
  - 5.3.5 VPN pag. 33
  - 5.3.6 Firewall pag. 33

6. Le norme di riferimento pag. 35

7. Glossario tecnico pag. 39

8. Case History pag. 42
- 8.1 Collegamento in rete dei parcheggi presso un aeroporto europeo pag. 42
- 8.2 Integrazione IT/OT per una rete di produzione ad alta disponibilità pag. 44
- 8.3 Ethernet nell'industria del bianco pag. 45

9. Le aziende del WG Networking industriale pag. 46

# 1. Il Networking nelle applicazioni di Automazione Industriale

Il mercato dell'automazione industriale vive una costante evoluzione, favorita anche dal sempre maggior impiego dell'intelligenza distribuita, con la necessità di far dialogare piattaforme differenti e specifiche, ognuna caratterizzata da un proprio linguaggio; senza dimenticare che, complice lo sviluppo dell'elettronica, un unico dispositivo è oggi spesso chiamato a supportare un numero crescente di funzioni.

La crescente presenza di soluzioni di Networking nel mondo industriale deriva quindi dal fatto che il processo d'interconnessione e condivisione delle informazioni, già consolidato nella vita quotidiana, influenza in maniera sempre più rilevante anche le applicazioni di automazione per il manufacturing. Tali applicazioni richiedono soluzioni di Networking omogenee, che possano integrare i dati di processo e diagnostica con la rete IT di stabilimento; la sicurezza dati e la sicurezza funzionale; PLC, I/O distribuiti e azionamenti con dispositivi standard Ethernet (PC, telecamere, router per accesso remoto via web).

Il mercato italiano paga ancora lo scotto di un'infrastruttura non pienamente sviluppata, che limita l'utilizzo di Internet, ma forte è la spinta verso la digitalizzazione e se la si ignora si rischia di essere oscurati in un mercato sempre più competitivo. Del resto progetti innovativi in ottica Industria 4.0 iniziano ad essere implementati in un numero crescente di realtà manifatturiere e la comunicazione dei dati acquisisce sempre più importanza nel contesto della fabbrica digitale. Generalmente la prima fase del progetto comprende l'analisi dei Big Data, la manutenzione preventiva e remota, mentre la seconda fase si concentra sull'integrazione dei processi aziendali attraverso le tecnologie Cloud per ottenere una sinergia tra tutte le varie realtà coinvolte nell'intero processo produttivo.

Non bisogna però dimenticare che se da un lato sempre più nuove tecnologie e protocolli di comunicazione dei dati continuano ad essere installati, dall'altro la base installata di attrezzature M2M e infrastrutture esistenti è spesso troppo preziosa e utile per potersene disfare. Così le reti industriali moderne devono essere in grado di abilitare diversi tipi di apparecchiature e verificare che vengano utilizzate a pieno potenziale anche quando i singoli componenti appartengono a diverse generazioni tecnologiche.

In ogni caso, un'infrastruttura di comunicazione affidabile, stabile, sicura e potente è un requisito importante per implementare con successo questo tipo di progetti. A sua volta però richiede un'attenta considerazione di aspetti come la gestione, l'operatività, la manutenzione della rete e la sicurezza dei dati che la attraversano al fine di un'adeguata progettazione e l'integrazione di queste architetture di rete. Un altro aspetto spesso sottovalutato è un'operatività scalabile per la rete.

La digitalizzazione della produzione è una rivoluzione diversa dalle precedenti perché il valore aggiunto viene creato oltre i confini della cella/macchina di produzione, e si ottiene scambiando i dati tramite un'infrastruttura IT. Il Networking per le applicazioni di automazione industriale assume una rilevanza forse superiore ad altre tecnologie abilitanti a seguito della crescente attenzione verso queste nuove impostazioni organizzative di fabbrica volte a integrare i componenti della macchina o dell'impianto in un sistema in rete.
Si pensi, ad esempio, ad una soluzione di supporto e assistenza remota che richiede di fornire l'accesso ai sistemi di produzione, a prescindere dalla loro posizione, in modo che gli esperti possano risolvere i problemi in modo competente e rapido. Nello scenario ideale, l'esperto può anche accedere ai dati inviati in modo continuo da una macchina così come al sistema di dati storici centrale. Attraverso l'analisi di queste informazioni potrà determinare possibili pattern e situazioni causa del malfunzionamento e quindi trovare le possibili soluzioni. Il valore aggiunto dei dati accessibili della macchina è direttamente proporzionale al numero di sistemi che si possono analizzare, quindi sono sempre maggiori gli sforzi compiuti per analizzare i dati prodotti della macchina. Ciò è vero soprattutto per gli OEM, che possono sfruttare le esperienze e i dati raccolti per offrire un servizio sempre più esteso ed articolato ai clienti.

La disponibilità di una rete di comunicazione avanzata diventa quindi essenziale nel processo produttivo, perché ogni connessione comunicativa contribuisce a ottimizzare i costi di produzione. Continuando con l'esempio, l'assistenza remota può supportare sedi diverse, aumentando la disponibilità generale dell'esperto e la produttività. Per la manutenzione di macchine sempre più complesse è necessario avere operatori molto specializzati e diviene molto difficile e costoso garantirne la disponibilità 24 ore al giorno, 7 giorni su 7. L'infrastruttura di comunicazione ha quindi anche un impatto diretto sull'efficienza della produzione stessa.

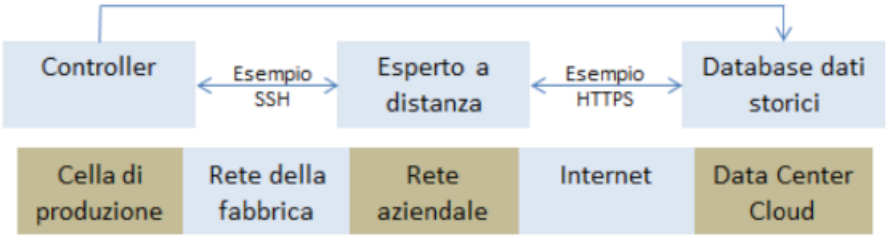



*Figura 1 – Esempio di infrastruttura di comunicazione dalla cella di produzione al data center Cloud*

L'esempio riportato in Figura 1 mostra diversi reparti di un'azienda che necessitano di un'infrastruttura di comunicazione che si estenda dagli uffici della sede centrale fino alle singole celle di produzione delle varie fabbriche. La cella di produzione, la fabbrica, l'azienda e la rete del data center generalmente rientrano sotto responsabilità di gestione diverse. Questa compartimentalizzazione, che per alcuni aspetti ha un suo valore, spesso crea problemi di comunicazione e conseguente complicazione e allungamento dei tempi di risoluzione dei problemi. Per questo motivo è necessario sviluppare un approccio che faciliti l'operatività, l'espansione e la risoluzione dei problemi dell'infrastruttura di comunicazione oltre i confini del singolo reparto. Nella realizzazione della struttura comunicativa che faciliti un progetto congiunto tra reparto di produzione e reparto IT, occorre considerare anche gli aspetti tecnici. Per una risoluzione dei problemi end-to-end è infatti necessario disporre di professionisti sulla catena di comunicazione delle rispettive componenti che conoscano le normali procedure di gestione di rete, dei dati e della security conformi ai criteri di audit.
L'interfacciamento delle celle di produzione con la rete della fabbrica e quindi con la rete IT dell'azienda deve considerare alcuni aspetti fondamentali, quali: la sicurezza dei dati tra la cella di produzione e la rete della fabbrica; l'integrazione dei sistemi nell'infrastruttura della rete della fabbrica (in molti casi, per l'integrazione nel concetto globale sono necessarie informazioni sulla VLAN o il supporto dei protocolli di IP routing in modo da garantire la disponibilità complessiva utilizzando diversi domini di rete); la terminazione dei tunnel VPN o delle sessioni IP (spesso è necessaria la terminazione dei tunnel VPN/IP per offrire agli esperti esterni l'accesso alle macchine); gli Edge Computing per la standardizzazione/normalizzazione dei dati e informazioni generate delle macchine.
La comunicazione dei dati e la security sono componenti importanti della digitalizzazione nell'ambito della produzione: lo sviluppo di concetti che favoriscano una transizione sicura e scalabile fra i reparti dovrebbe essere prioritario al fine di poter beneficiare dei vantaggi degli sviluppi di Industria 4.0 in tempi brevi.

# 2. Da Ethernet a Industrial Ethernet

## 2.1 Cenni a caratteristiche di base del protocollo Ethernet

Ethernet è un insieme di tecnologie standardizzate nate per la connessione di dispositivi diversi tra loro come personal computer e stampanti in reti locali.
Poco noto è che le radici di Ethernet risalgono al 1967. A Norman Abramson dell'Hawai University fu chiesto di sviluppare via radio una rete di connessione PC. Il progetto chiamato ALHOA andò a buon fine e portò alla nascita del protocollo CSM/IM anti collisione dati che venne poi usato anche per i futuri sviluppi di Ethernet.
Di seguito Robert Metcalfe e David Boggs, suo assistente allo Xerox PARC, formarono un gruppo di lavoro con la collaborazione delle aziende Xerox Corporation, Intel Corporation e Digital Equipment Corporation. Tra il 1978 e il 1980 furono prodotte le specifiche del protocollo di comunicazione 802.3 che definiscono sia le tecniche che a livello fisico (connettori, cavi, tipo di trasmissione, ecc.) oltre che a livello di indirizzo fisico delle schede di rete MAC, che del modello architetturale di rete ISO/OSI. Nasceva lo standard Ethernet v1.0 (il nome Ethernet è ispirato dal "luminiferous ether" che è il mezzo trasmissivo della luce e onde radio nello spazio).
Ethernet è un insieme di protocolli e strumenti di rete componenti fisici, che permette la comunicazione dati tra dispositivi sia attraverso diversi media di collegamento: cavi di rame in fibra ottica e onde radio.
Alla base di Ethernet c'è il modello ISO/OSI. Ogni parte o livello denominata Layer contribuisce in modo sequenziale al funzionamento delle comunicazioni dati tra PC o altri dispositivi.
Di seguito, una descrizione dei Layer e delle rispettive funzioni:

- Layer 7 - Application layer: gestisce le comunicazioni tra le applicazioni a indirizza i dati all'applicazione corretta. Esempio di protocolli gestiti: HTTP, FTP, TFTP, DHCP, DNS, SMTP, POP3, Telnet, SSH.
- Layer 6 - Presentation layer: converte i dati nei differenti formati in modo da renderli leggibili come dati, caratteri, immagini, audio. Esempio di formati gestiti: GIF, JPEG, MPEG, Quicktime, ASCII, EBCIDIC.
- Layer 5 - Session Layer: apre, mantiene e chiude le comunicazioni tra i dispositivi e le applicazioni. Questo layer identifica il tipo di dato e a quale sessione appartiene assicurando che tutte le richieste di dati siano aperte, inviate e chiuse nel modo corretto. Esempio di controlli eseguiti: Password Authentication Protocol (PAP); Remote Procedure Call (RPC).
- Layer 4 - Transport layer: trasferisce i dati da un dispositivo all'altro senza errori, controlla il flusso dati e la corretta sequenza di invio per il protocollo UDP invio e ricezione nel caso del protocollo TCP. Protocolli gestiti: UDP, TCP.
- Layer 3 - Network Layer: è responsabile degli indirizzi logici e instradamento dati in una rete. I router possono operare a questo livello. Protocolli gestiti: IP, Routing Information Protocol (RIP), Open Shortest (OSPF), EIGRP, IS-IS, IPSEC, GRE.
- Layer 2 - Data Link layer: definisce come i dispositivi comunicano nella rete, ed è responsabile della gestione degli indirizzi fisici schede di rete e della loro comunicazione. Il Media Access Control (MAC address) è gestito dal Data Link Layer, gli switches gestiti e non gestiti operano a questo livello. Protocolli gestiti: Ethernet, Frame Relay, Token Ring, Point-to-Point (PPP), Cisco Discovery Protocol (CDP), L2TP, PPTP.
- Layer 1 - Physical Layer: definisce come la comunicazione dati passi nel media, il mezzo di trasmissione scelto. I bit di dati possono essere trasmessi elettricamente, otticamente, o attraverso segnale radio. Viene inoltre fissato lo standard meccanico dei connettori. Standard e dispositivi gestiti: Media (coaxial cable, twisted-pair copper cable, fiber-optic cable), Connectori (RJ45), NICs, HUBs, Repeater.

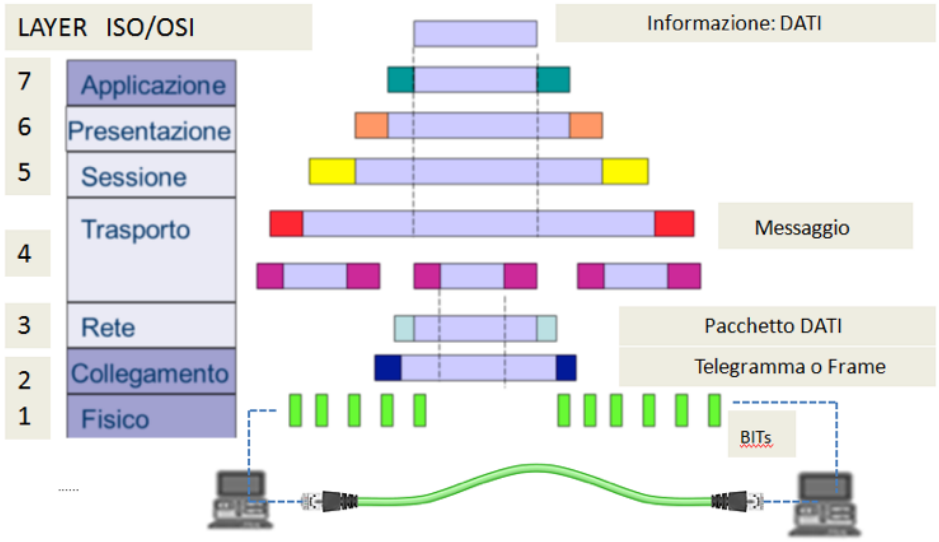



*Figura 2 – Modello ISO/OSI semplificato*

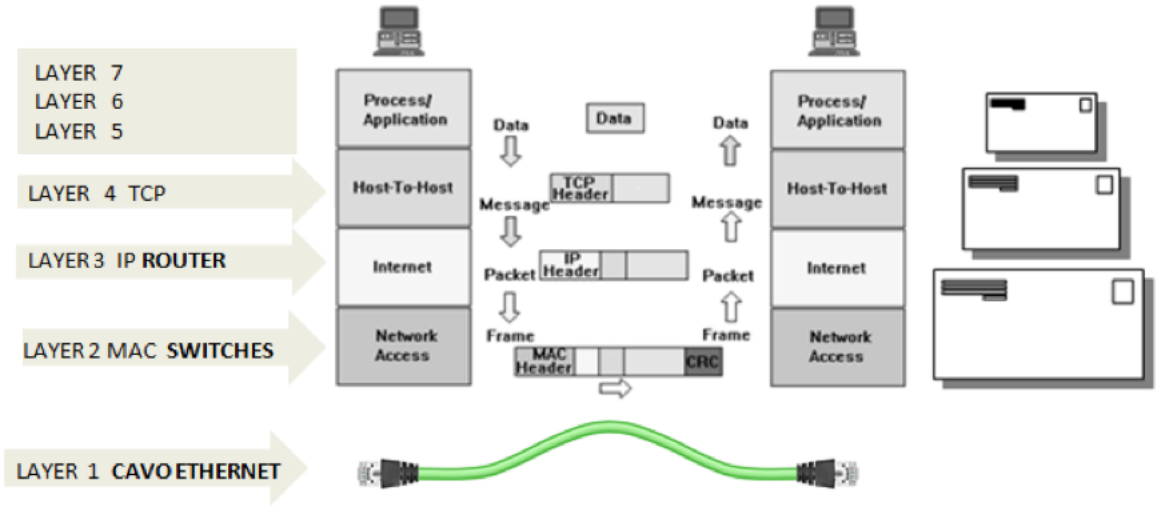



*Figura 3 – Esempio di passaggio tra i diversi layer e protocolli nella sequenza di invio/ricezione di una mail*

## 2.2 Industrial Ethernet

Sfruttando la base e i vantaggi a livello di interconnessione dispositivi offerti da Ethernet standard, in campo industriale ha preso piede sin dagli anni 80' uno standard chiamato Industrial Ethernet, che come dice la radice della definizione è la rete Ethernet applicata in campo industriale.
Cosa cambia rispetto a Ethernet usata comunemente nell'Information Techcnology a livello Office o domestico?
L'ambiente di utilizzo è più gravoso: condizioni ambientali, temperature di esercizio, disturbi radio e EMC generati dai dispositivi di potenza Drive Motori Brusheless, Motori Asincroni comandati da inverter, valvole e solenoidi, creano un ambiente avverso alle comunicazioni dati.

### 2.2.1 Real Time Ethernet: Determinismo e Isocronia

Altra grossa differenza è che Ethernet non nasce come protocollo di comunicazione deterministico. I dati trasmessi se non corretti vengono ritrasmessi, la comunicazione dati avviene con tempi variabili, e questo non costituisce nelle reti Office o Home una criticità. Se scarico un grosso file da Internet, il tempo di trasferimento dati sarà variabile e non lo posso sapere con sicurezza all'inizio della trasmissione/ricezione dati. I dati nella rete Ethernet standard se degradati o in ritardo risposta time-out vengono semplicemente ritrasmessi.
In ambiente industriale il determinismo della trasmissione dati è fondamentale, vitale per il funzionamento delle automazioni. I dati, che di solito non hanno grossi volumi, devono partire ed arrivare in tempi noti pre-determinati. Si pensi a un comando ad un attuatore dal quale ci si aspetta un feedback di operazione eseguita a volte in pochi millesimi di secondo, che deve essere acquisita e processata dal PLC o dal PC di controllo. Per il motivo descritto, l'industria usa le basi Ethernet ma con profili e protocolli appositamente studiati per garantire il determinismo nella trasmissione dati.
Tra i più diffusi protocolli industriali deterministici:

| Protocolli | Organizzazioni di sviluppo | Link ai siti delle organizzazioni con i dettagli |
|---|---|---|
| PROFINET RT/IRT | PNO | www.profibus.com |
| EtherNet/ IP | ODVA | www.odva.org |
| POWERLINK | EPSG | www.ethernet-powerlink.org |
| EtherCAT | ETG | www.ethercat.org |
| SERCOS III | Sercos International | www.sercos.org |

Esistono diversi approcci per implementare una rete industriale Ethernet deterministica:

- Basato su TCP / IP: i protocolli si basano sui livelli del protocollo standard TCP/IP con meccanismi in tempo reale integrati nel layer superiore del protocollo TCP/IP. Queste soluzioni di solito hanno prestazioni non ad alta velocità.
- Standard Ethernet: i protocolli vengono usati ai livelli alti del protocollo Ethernet. Queste soluzioni sfruttano l'evoluzione di Ethernet standard senza ulteriori investimenti.
- Standard Ethernet modificato: i livelli del protocollo Ethernet standard vengono personalizzati e modificati, così come i meccanismi e le infrastrutture. Queste soluzioni mettono al primo posto le prestazioni in velocità di comunicazione allo standard unificato di Ethernet.

Una differenza fondamentale dei vari sistemi Industrial Ethernet è nel modo in cui si organizzano i dati per il trasferimento dalle periferiche in campo ai master e come riescono a fornire prestazioni in tempo reale.
EtherCAT e SERCOS III comunicano utilizzando il Summation Frame Method: ad ogni ciclo, i dati per tutti i nodi di rete vengono inviati in un telegramma che viaggia da un nodo all'altro lungo l'anello o topologia della rete, raccogliendo le risposte dei nodi partecipanti. In questo meccanismo i nodi partecipanti leggono e scrivono al volo i dati. D'altro canto, il sistema di invio telegramma utilizzato da altri protocolli e sistemi funziona inviando singoli telegrammi ai nodi, che possono rispondere individualmente a telegrammi separati.
I sistemi utilizzano diversi meccanismi di accesso dati dalla rete e sincronizzazione delle trasmissione degli stessi. Alcuni esempi:

- Un master controlla la temporizzazione sulla rete della trasmissione dati. In ambiente POWERLINK, il master autorizza e coordina i singoli nodi per l'invio dei dati.
- Nelle reti EtherCAT e SERCOS III, il trasferimento dei telegrammi Summation Frame segue la temporizzazione del clock scandito dal master.
- PROFINET IRT usa switch e porte di comunicazione a bordo sincronizzati.
- EtherNet/IP impiega il CIP Sync per distribuire e sincronizzare la trasmissione dati usando lo standard IEEE 1588 per le informazioni temporali della rete.

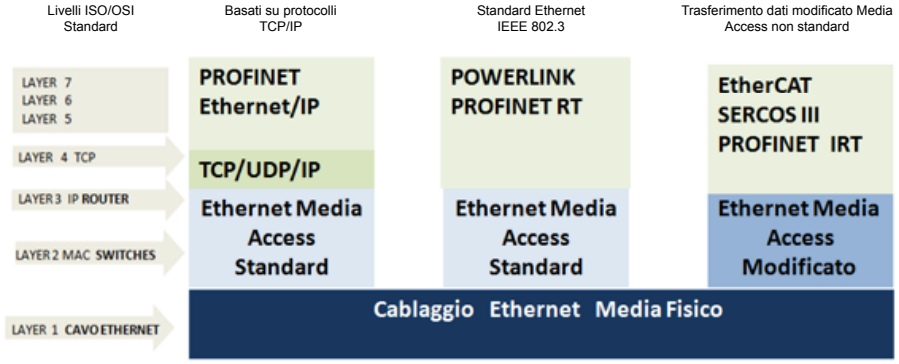



*Figura 4 – Approcci per implementare una rete industriale Ethernet deterministica*

### 2.2.2 Caratteristiche tecniche dei dispositivi

I dispositivi usati nelle reti industrial Ethernet devono avere caratteristiche di funzionamento in ambiente gravoso con un'escursione ampia delle temperature di funzionamento (arrivare da -20°C a +75°C può essere un esigenza), ed essere privi di ventole a bordo. Le tensioni di alimentazione standardizzate per l'automazione industriale sono a 24 V DC. Le norme EMC da rispettare sono diverse per l'ambiente più gravoso. Il montaggio a guida DIN nei quadri è uno standard meccanico. La resistenza a vibrazioni competano le principali caratteristiche tecniche elencate. In alcune applicazioni può essere richiesto il funzionamento in ambiente esplosivo.
Di seguito si riporta un esempio di approvazioni e norme applicate ad un dispositivo Industrial Ethernet:

- **Approvazioni:**

- **Norme:**

| | |
|---|---|
| Caduta libera | IEC 60068-2-32 |
| Norme EMC | FCC Part 15 Subpart B Class A, EN 55022 Class A, EN 61000-4-2 (ESE), livello 3, EN 61000-4-3 (RS), livello 3, EN 61000-4-4 (EFT), livello 3, EN 61000-4-5 (surge), livello 3, EN 61000-4-6 (CS), livello 3, EN 61000-4-8 |
| Settori a rischio di esplosione | UL/cUL, Class I Division 2, Groups A, B, C e D |
| Sicurezza | UL508, UL60950-1, CSA C22.2 No. 60950-1, EN60950-1 |
| Urti | IEC 60068-2-27 |
| Vibrazione | IEC 60068-2-6 |

I protocolli industriali usano la base Ethernet standard 802.3 ma i profili dei protocolli hanno funzionalità specifiche. Ecco perché tutti i dispositivi attivi usati con i diversi protocolli Industrial Ethernet PLC, PC, SWITCHES, PORT REPEATER, I/O di campo devono essere compliant e certificati dal consorzio di appartenenza del protocollo usato.

# 3. Infrastruttura di rete Industrial Ethernet

## 3.1 Caratteristiche di base

### 3.1.1 Tipologia di prodotti

I prodotti utilizzati in ambito Industrial Ethernet derivano essenzialmente dai corrispondenti componenti che ormai da anni vengono utilizzati per la gestione delle networks in ambito IT/Office. Con l'adozione dello standard Ethernet in ambito industriale si è reso necessario l'adattamento di questi componenti in ambienti particolari per natura o servizi di rete. Per questa ragione è possibile oggi trovare sul mercato componenti che rispondono a necessità di resistenza a temperature estese o  elettromagnetismo, come per ambienti con inquinamento da polveri chimiche o saline. Contestualmente è stato necessario ampliare il set di servizi per il supporto di particolari protocolli di comunicazione industriale che non snaturano lo standard Ethernet ma lo sviluppano, evolvendolo alla crescente necessità di interazione tra gli ambiti IT/OT e rendendolo uno degli elementi abilitatori dell'IIoT.
Sono disponibili molteplici apparati attivi nella gestione della network che, semplificando, possono essere raggruppati per funzionalità nelle seguenti categorie di prodotti:

*Switch/Router Industriali*

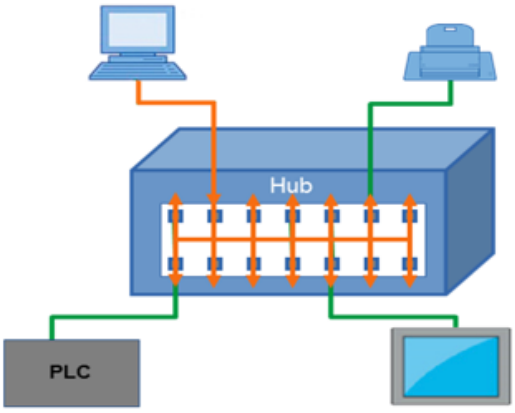



*Figura 5 - Esempio di funzionamento di un Hub Ethernet*

Switch e router industriali rappresentano indubbiamente il gruppo più corposo ed importante di prodotti relativi ad Industrial Ethernet. In particolare gli switch sono il componente base che permette la creazione di reti locali, ovvero Local Area Network (LAN), basate su comunicazione Ethernet. Per tale motivo è utile approfondirne il comportamento.
Per capire il funzionamento degli switch Ethernet si può partire da quello dei più semplici Hub, da cui essi derivano. Questi ultimi garantiscono il collegamento reciproco fra i diversi dispositivi Ethernet connessi alle porte, di cui sono muniti, mediante la semplice ripetizione elettrica del segnale. In sostanza il segnale ricevuto su una singola porta viene replicato in uscita su tutte le altre porte disponibili, in modo che il dispositivo destinatario possa, in ogni caso, essere raggiunto dal segnale. Questo comportamento, tuttavia, non risulta ottimale in termini di utilizzo della banda, in quanto durante la trasmissione di un dispositivo gli altri sono costretti a restare in "ascolto" anche quando non interessati da quella particolare comunicazione. Inoltre la possibilità che più dispositivi inizino la trasmissione nello stesso istante, comporta la possibile perdita di dati in un meccanismo definito come collisione. Pertanto questi dispositivi, ormai in disuso, agiscono solo sul livello fisico del protocollo Ethernet (Layer 1 della pila ISO/OSI).
Gli switch Ethernet ovviano a questo problema andando ad agire sul livello dati (Layer 2 ISO/OSI) del protocollo, sfruttando gli indirizzi fisici detti MAC contenuti nell'intestazione dei frame Ethernet inviati sulle proprie porte. Quando uno switch riceve un pacchetto su una specifica interfaccia, esso ne legge l'indirizzo a cui è destinato ed in base a una tabella degli indirizzi chiamata MAC Table, salvata in memoria, è in grado di inoltrare il frame sulla porta a cui è connesso il dispositivo destinatario. Qualora quest'ultima sia già impegnata nella trasmissione di un altro pacchetto, lo switch salva il pacchetto in memoria fino a che l'interfaccia non sia tornata disponibile per la trasmissione. Tale funzionamento, denominato Store & Forward, permette la trasmissione contemporanea di numerosissimi pacchetti, evitando il fastidioso problema delle collisioni. Se invece lo switch, inoltra direttamente il pacchetto sulla porta di destinazione senza salvarlo ed elaborarlo si ha l'utilizzo della modalità Cut-Through. Altra modalità simile è quella Fragment-free che differisce dalla Cut-Through solo per la definizione dell'instradamento controllando 64byte iniziali (rispetto ai 6byte del Cut-Through). Ciò chiaramente comporta un dispendio maggiore in termini di tempi rendendo questo meccanismo poco sfruttato.
La tabella degli indirizzi, usata dallo switch, viene creata in corsa dal dispositivo stesso mediante un meccanismo chiamato MAC Learning. Quando infatti un pacchetto giunge su una porta dello switch, questo verifica anche

l'indirizzo MAC sorgente del frame e, se non presente nella tabella, lo salva con la relativa porta d'ingresso, per potervi inviare successivamente i pacchetti a lui destinati. Qualora l'indirizzo del destinatario risulti sconosciuto, ovvero non presente nella tabella, lo switch invierà il pacchetto in broadcast su tutte le porte, aspettando la risposta del destinatario. Questo meccanismo permette di ricreare la tabella dei MAC, aggiornandola con l'associazione tra la porta utilizzata per l'invio del frame e la porta su cui è stata ricevuta la risposta del destinatario creando così un instradamento porta-indirizzo univoco. Grazie a questo meccanismo è possibile connettere qualsiasi dispositivo Ethernet sulle porte dello switch senza dover effettuare alcuna configurazione specifica, garantendo un'enorme flessibilità nello sviluppo della rete e rendendone l'uso possibile anche ad utenti poco esperti.

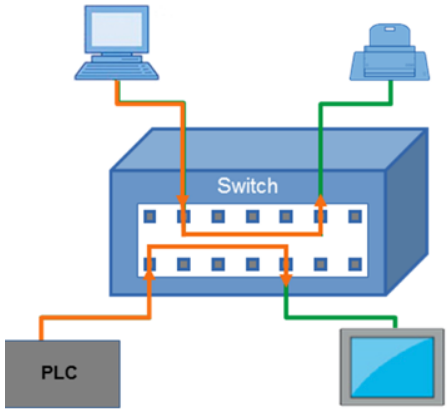



*Figura 6 - Esempio di funzionamento di uno switch Ethernet*

Ovviamente il modo in cui gli switch eseguono questi meccanismi è determinato dalle proprie caratteristiche hardware e software. Infatti, la memoria e la capacità di elaborazione degli switch possono essere limitate, comportando che, in caso di sovraccarico della rete, essi possano perdere pacchetti limitando la banda e la prestazioni generali della rete. Inoltre nel tempo gli switch hanno acquisito ulteriori feature software che ne distinguono il comportamento. Alcune di queste saranno analizzate nel seguito del capitolo.
Possiamo quindi distinguere le seguenti categorie:

- **Switch L2 non gestiti:** sono concepiti per il funzionamento più semplice di switching in modalità plug&play. Ovvero l'utente connette semplicemente i dispositivi allo switch per un funzionamento immediato, senza effettuare nessun'altra operazione. Essi infatti non sono configurabili e non supportano feature aggiuntive. A livello industriale alcuni dispongono del supporto automatico a specifici protocolli industriali e di una semplice diagnostica elettrica ed ottica. Ovviamente sono anche i dispositivi le cui prestazioni sono più limitate.
- **Switch L2 gestiti:** sono la famiglia più avanzata dei dispositivi basati su Layer 2. Al loro interno infatti risiede una CPU che dispone di un suo indirizzo ed è tipicamente raggiungibile dall'utente mediante connessioni basate su linea di comando o semplice interfaccia grafica. Oltre a poter funzionare esattamente come un modello non gestito, seppur con prestazioni in genere superiori, essi supportano infatti numerose altre caratteristiche software che possono essere configurate connettendosi al dispositivo. Inoltre permettono una diagnostica molto più raffinata, che può essere gestita anche da dispositivi terzi.
- **Switch L3 / Router:** i dispositivi di questo tipo possiedono in genere tutte le caratteristiche degli switch gestiti ma sono in grado di agire come bridge anche sul livello di rete (Layer 3 ISO/OSI). Essi sono quindi in grado di fare routing permettendo la comunicazione fra diversi domini di rete Ethernet. Per ulteriori dettagli si rimanda al paragrafo relativo al routing.

### *Sicurezza Industriale*

Questi dispositivi sono a loro volta switch e router industriali che però presentano caratteristiche specifiche per il mondo della sicurezza. Essi sono in grado di garantire la protezione delle reti industriali e dei dati sensibili da accessi esterni non autorizzati. A tale scopo questi dispositivi utilizzano diversi meccanismi come ad esempio firewall o VPN. Per maggiori dettagli si rimanda al capitolo relativo alla sicurezza industriale.

### *Wireless Industriale*

Questa categoria di dispositivi non è strettamente parte dell'Industrial Ethernet come switch e router ma permette alle reti industriali di comunicare attraverso l'etere grazie a tecnologie basate sul trasporto delle informazioni tramite microonde. Possiamo quindi distinguere fra due tipi di tecnologie:

- **Tecnologia per l'accesso remoto:** ovvero che permette di dare accesso ai dispositivi Industrial Ethernet ad internet, vengono in genere definiti Modem.

- **Tecnologia per la creazione di reti industriali Wireless locali (o IWLAN):** in questo caso possiamo distinguere fra dispositivi in grado di generare e gestire una rete Wireless detti Access Point e dispositivi, detti Client/Bridge, in grado di garantire solo il semplice accesso alle reti Wireless gestiti da Access Point o al più una comunicazione Peer-to-Peer.

Tutti questi dispositivi dispongono di una parte d'interfaccia radio e una parte d'interfaccia Ethernet, che a sua volta può integrare funzionalità tipiche di switch o router.
Per ulteriori dettagli si rimanda al paragrafo dedicato.

*Componenti Passivi*

Ai prodotti principali illustrati precedentemente dobbiamo infine aggiungere la componentistica passiva, quali cavi, connettori, adattatori ed accessori necessari per il buon dimensionamento delle reti quali le antenne per il Wireless.

### 3.1.2 Topologia di rete

L'Industrial Ethernet è estremamente flessibile e permette l'uso di numerose topologie di rete. Vediamo di seguito le casistiche principali:

*Topologia Lineare o a Bus*

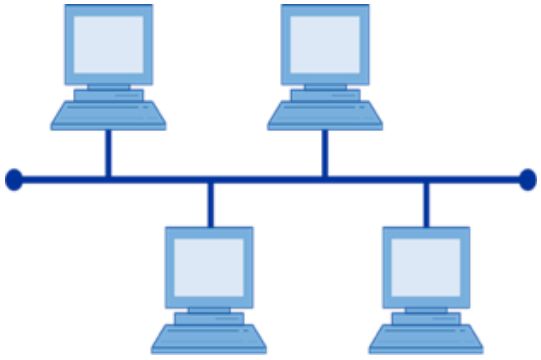


*Figura 7 - Esempio di topologia a bus*

Questa topologia è la più semplice che può essere implementata e riprende, ovviamente, la classica topologia prevista nei protocolli a bus di campo. Va tenuto conto però che per effettuare questi collegamenti si utilizzano dispositivi Ethernet che dispongono di più porte, tipicamente due. In questo modo è possibile implementare il collegamento Industrial Ethernet senza utilizzare prodotti dedicati come switch.

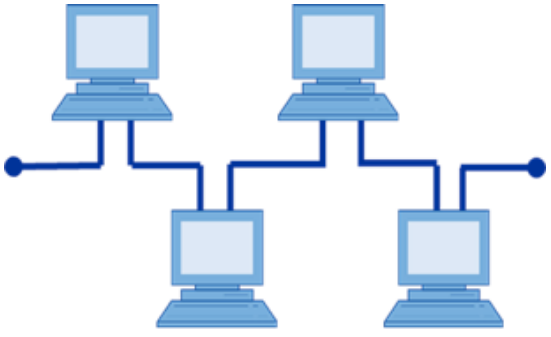


*Figura 8 - Topologia a Bus in Industrial Ethernet*

Questa topologia è la più semplice che può essere implementata e riprende, ovviamente, la classica topologia prevista nei protocolli a bus di campo. Va tenuto conto però che per effettuare questi collegamenti si utilizzano dispositivi Ethernet che dispongono di più porte, tipicamente due. In questo modo è possibile implementare il collegamento Industrial Ethernet senza utilizzare prodotti dedicati come switch.

Nella realtà tali dispositivi prevedono la presenza al loro interno di piccoli switch integrati. Ne consegue quindi che, a dispetto della semplicità ed economicità di questa soluzione topologica, il malfunzionamento o semplice spegnimento di un dispositivo od un problema ad un singolo cavo lungo la catena può comportare la perdita di tutti i dispositivi a valle.
Inoltre gli switch integrati presenti nei dispositivi all'inizio della catena devono gestire tutto il traffico diretto verso tutti i nodi successivi della catena. Se questo traffico dovesse risultare eccessivo si potrebbe verificare la perdita di pacchetti. Infine in questo modo la diagnostica risulta estremamente complessa dato che diventa difficile capire in certe situazioni a che punto della catena si è verificato un certo tipo di problema.
Come conseguenza si sconsiglia l'uso estensivo di questa topologia in particolare in reti il cui numero di dispositivi comincia a essere importante.

### *Topologia a Stella*

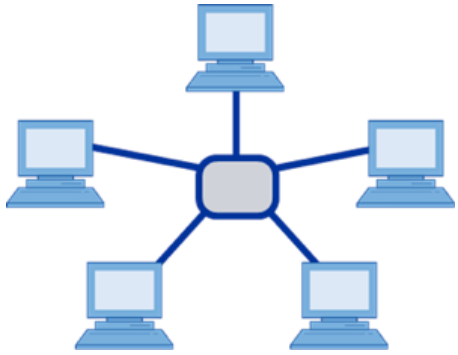


*Figura 9 - Esempio di topologia a stella*

Questa topologia è più classica nell'utilizzo di Industrial Ethernet. Essa prevede come elemento centrale la presenza di uno switch. Tutti gli altri dispositivi sono connessi alle porte di quest'ultimo. Come risultato si ha una topologia più efficiente in quanto le prestazioni di rete e la connettività dipendono unicamente dallo switch al centro. Inoltre un problema a un cavo o ad un singolo dispositivo non comporta la perdita di altri dispositivi.
Il problema di questa topologia rimane nel fatto che un eventuale problema allo switch compromette la rete intera. In questa configurazione permane la presenza di un single point of failure, ovvero un unico punto sensibile la cui rottura provoca la perdita di tutta la rete.

### *Topologia ad Albero*

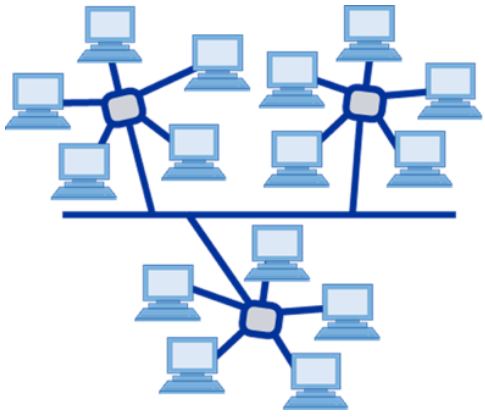


*Figura 10 - Esempio di topologia ad albero*

Questa topologia rappresenta l'unione fra la topologia lineare e quella a stella. In questo senso gli switch sono collegati linearmente fra di loro mentre i dispositivi comuni sono connessi a stella sui singoli switch. Lo scopo della topologia in oggetto è tipicamente quello di espandere la rete quando il numero di porte del singolo switch dovesse risultare non sufficiente per il numero dei dispositivi da connettere. Benché la topologia lineare basata su veri e propri switch sia intrinsecamente più robusta rimane il fatto che ciascuno di essi rappresenti ancora un single point of failure. Per questo motivo anche questa topologia risulta non protetta da malfunzionamenti.

### *Topologia ad Anello*

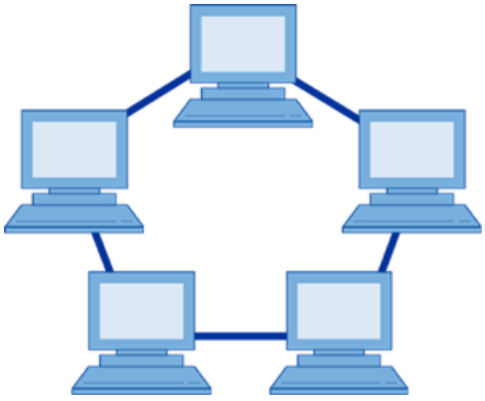


*Figura 11 - Esempio di topologia ad anello*

L'anello rappresenta la più semplice forma di ridondanza possibile in una rete. Ciascuno dei dispositivi o switch è collegato a due altri dispositivi. Questo permette quindi di evitare completamente la presenza di un single point of failure. La rete continuerà quindi a funzionare anche in seguito alla perdita di un unico dispositivo o collegamento.
Tuttavia l'uso di questa topologia è possibile solo sotto certe condizioni. Infatti collegando dei semplici dispositivi, come ad esempio degli switch non gestiti, in questa configurazione, il traffico Broadcast presente nella rete circolerebbe indefinitamente creando un fenomeno che viene definito come Broadcast Storm. In ultima istanza questo traffico impazzito tenderebbe a regime a congestionare la rete portandone al blocco. Per prevenirlo occorre utilizzare dei dispositivi che abbiano a disposizione feature in grado di gestire protocolli di ridondanza bloccando l'insorgere di traffico indesiderato sul nascere.
Ne consegue che l'implementazione di questa topologia risulta più oneroso per l'utente finale, sia in termini economici sia in termini di impegno e tempo dovuto alla sua configurazione.
Inoltre questa topologia garantisce la protezione solo per un singolo malfunzionamento. Ne consegue che questo tipo di reti vanno monitorate per intervenire tempestivamente ad operare il ripristino della funzionalità completa in caso di rottura dell'anello. Infatti un secondo malfunzionamento diventerebbe immediatamente critico.

### *Topologia Magliata o Mesh*

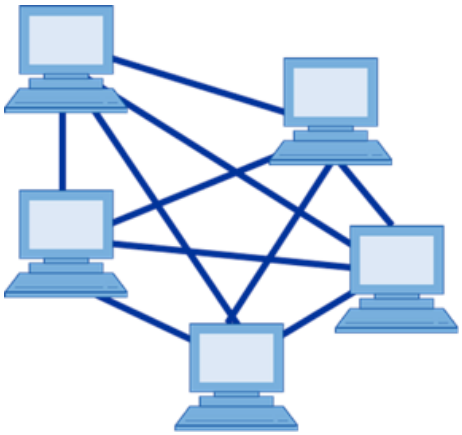


*Figura 12 - Esempio di topologia magliata*

Questa topologia prevede il collegamento contemporaneo di più dispositivi verso gli altri, in questo modo i malfunzionamenti che possono essere tollerati diventano molteplici. Si realizza quindi una ridondanza definitiva. Tuttavia i protocolli e i dispositivi necessari all'implementazione di questa topologia sono tanto più complessi quanto più lo è la topologia. Inoltre i tempi necessari per il ripristino della rete in seguito ad una rottura sono talvolta non abbastanza veloci per le esigenze dell'Industrial Ethernet.
Ne consegue che questa topologia è usata molto raramente in ambito industriale in quanto troppo costosa, complessa e lenta.

### 3.1.3 Cablaggio

Nella componentistica passiva dell'Industrial Ethernet un ruolo chiave è giocato dai cavi con i loro relativi connettori. Questi si dividono principalmente in cavi che fanno uso di segnale elettrico e quindi trasporto su rame e cavi che utilizzano invece un segnale ottico, detti fibre.

I primi rappresentano l'alternativa più semplice ed economica, tuttavia il loro raggio d'azione è limitato ad una lunghezza massima di cento metri e sono a loro volta suscettibili ai disturbi elettromagnetici.
Le fibre ottiche dal canto loro possono raggiungere distanze significativamente più lunghe, fino a decine di km. Inoltre essendo il segnale di tipo ottico non risentono minimamente dei campi elettromagnetici esterni.

Di contro le fibre ottiche sono estremamente più costose, più difficili da assemblare e presentano diverse categorie di cavi e connettori incompatibili fra di loro. Inoltre sono anche molto meno adattabili , in quanto tipicamente non supportano meccanismi di auto-negoziazione che permettano la retro compatibilità con collegamenti più lenti delle precedenti generazioni.

#### 3.1.3.1 Cavi in rame e relativi connettori

I cavi in rame sono costituiti da coppie di fili attorcigliati tra loro. Questo sistema è utilizzato per ottenere una migliore robustezza elettromagnetica, in quanto con la coppia si propaga il segnale in maniera differenziale e l'attorcigliamento diminuisce i nefasti effetti del cross-talking fra la coppia di fili presenti nel cavo. Possono essere Half Duplex ma al giorno d'oggi sono praticamente tutti Full Duplex grazie all'uso di più coppie di fili.
Si dividono in diverse categorie, attualmente in commercio troviamo:

- **Categoria 5/5e (Cat5/cat5e):** Ha sostituito il precedente Cat5; utilizza un segnale fino a 100 MHz, supportando velocità fino a 100 Mbit/s con due coppie di conduttori e 1000 Mbit/s con quattro coppie.
- **Categoria 6 (Cat6):** Ha requisiti più stringenti rispetto al cross-talk raggiungendo la frequenza di 250 MHz. Questo le permette di supportare velocità fino a 10 Gbit/s sebbene per un massimo di 55m invece che 100m.
- **Categoria 7 (Cat7):** Utilizza una frequenza fino a 600MHz con obbligo di schermatura. In questo modo è in grado di garantire la velocità di 10 Gbit/s sulla distanza di 100m.

Inoltre si ha anche una divisione in base al tipo di schermatura:

- **UTP (Unshielded Twisted Pair):** cavo non schermato, i conduttori sono protetti solo da una guaina plastica esterna.
- **FTP (Foil Twisted Pair):** cavo avvolto, i conduttori sono protetti da un foglio di alluminio che rappresenta una schermatura parziale in grado di fornire un primo grado di protezione da interferenze esterne.
- **STP (Shielded twisted Pair):** cavo schermato, presenta una seconda schermatura che protegge singolarmente le coppie di conduttori. Rappresenta il massimo grado possibile di protezione.

Ovviamente ad una maggiore schermatura corrisponde una minore flessibilità del cavo.

Per Industrial Ethernet si raccomanda sempre l'utilizzo di categoria industriale, sia per la maggiore schermatura che per robustezza fisica. Infatti, ad esempio, i classici cavi UTP non schermati sono concepiti per l'utilizzo in

ambito domestico e non sono adatti al rumore presente in ambito industriale. Allo stesso modo non sono in grado di sopportare certe sollecitazioni a cui sono sottoposti i queste applicazioni.

I connettori presenti per i cavi in rame sono tipicamente due:

- **Connettori RJ45:** nome comune del classico connettore 8P8C, ovvero a 8 posizioni e 8 contatti. E' utilizzato nella stragrande maggioranza delle applicazioni.
- **Connettori M12:** di forma circolare utilizzato in alcune applicazioni specifiche in ambito industriale.

*Figura 13 - Classici cavi in rame con connettori RJ45*

### 3.1.3.2 Fibre Ottiche e relativi connettori

Le fibre ottiche sono costituite da un nucleo ed un mantello che lo avvolge, tipicamente in vetro.
Grazie al meccanismo della riflessione totale, permettono la propagazione del segnale con bassa dispersione e quindi su distanze molto più elevate rispetto al rame al prezzo di una complessità, e quindi un costo, maggiore.

Possiamo suddividere le fibre nelle seguenti tipologie:

#### *Fibra in Plastica (POF/PCF)*

Con questo cavo il segnale ottico si propaga in un particolare tipo di polimero. In tal caso il segnale riceve un degrado molto maggiore rispetto al vetro e le distanze che possono essere raggiunte ne risultano molto limitate di poco superiore o simili a quelle raggiunte coi cavi in rame. Si ha però il vantaggio di avere un cavo semplificato ed economico ma anche fisicamente molto robusto. Questo tipo di soluzione è quindi molto adatta all'uso in ambienti dove problemi quali disturbi elettromagnetici, particolari sollecitazioni meccaniche o distanze in gioco leggermente eccessive rendano l'uso dei cavi in rame impraticabile.

#### *Fibra Multimodale in vetro*

Questo tipo di cavo possiede un nucleo abbastanza largo (50-100 µm) in cui il segnale ottico viaggia seguendo diversi modi di propagazione. In questo caso è possibile utilizzare un'elettronica meno raffinata a parità di banda, il che rende questa tipologia di cavo più conveniente. Tuttavia la dispersione dei modi nella fibra risulta piuttosto alta limitando la massima distanza raggiungibile a pochi km.

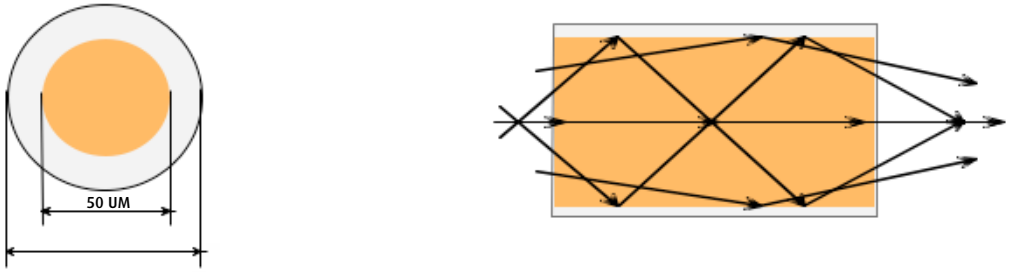



*Figura 14 - Esempio di propagazione multimodale*

### *Fibra Monomodale in vetro*

Con una sezione del nucleo decisamente più ridotta (diametro di 8-10 µm) questa tipologia di cavo necessita di una tecnologia trasmissiva molto più raffinata, tuttavia la dispersione ed il rapporto segnale-rumore si mantengono ottimi e permettono a questa tipologia di cavo di raggiungere distanze ragguardevoli di diverse decine di km.

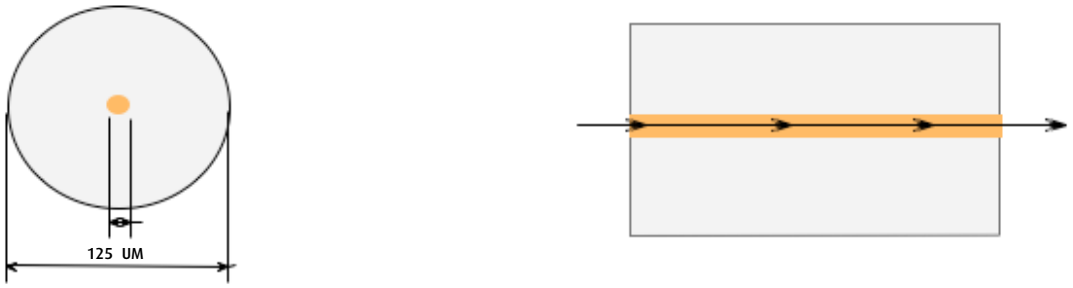



*Figura 15: Esempio di propagazione monomodale*

I connettori utilizzabili per fibre ottiche sono innumerevoli, quelli che più classicamente troviamo in ambito industriale sono:

*Figura 16 - Esempio di connettori per fibra ottica*

### *Connettori SC (Subscriber Connector)*

Di forma quadrata con ghiera ceramica, utilizzano un meccanismo push&pull per il loro aggancio che si chiude con una linguetta.

### *Connettori ST /BFOC (Straight Tip / Bayonet Fiber Optic Connector)*

Di dimensioni e caratteristiche simili al connettore SC ma utilizza un aggancio con avvitamento e baionetta che lo rende particolarmente adatto all'installazione in ambienti ricchi di vibrazioni.

### *Connettori LC (Lucent o Little Connector)*

Sono fra i connettori più piccoli a disposizione, simili agli SC, si chiudono con un più pratico aggancio a chiave, ragione per cui nel tempo hanno avuto un successo sempre più importante a scapito del connettore SC. Inoltre molto spesso le porte ottiche non sono totalmente integrate ma fanno uso di ulteriori dispositivi detti SFP (Small Form factor Pluggable) che tipicamente fanno uso di connettori LC.

### 3.1.4 Comunicazione Wireless

L'alternativa all'uso del cavo è la trasmissione radio. Questa comunicazione avviene attraverso dispositivi dedicati che utilizzano protocolli specifici, derivati dal mondo IT. In sostanza questi dispositivi si comportano da "traduttori" trasportando i pacchetti sul loro livello fisico e mettendoli a disposizione del mondo Industrial Ethernet a cui sono connessi.

#### *Wireless per accesso remoto*

I modem utilizzati per l'accesso remoto, permettono di accedere ad internet utilizzando le ormai pervasive reti cellulari con protocolli che permettono la trasmissione dati quali GPRS, EDGE,UMTS e LTE. Queste reti sono gestite da provider telefonici, motivo per cui questi dispositivi dovranno essere dotati, come i comuni cellulari, di opportune schede SIM per poter utilizzare il servizio. La trasmissione di dati attraverso internet è ovviamente un argomento molto delicato che necessita di opportuni accorgimenti di sicurezza per proteggere il passaggio di dati sensibili, in un ambente che potrebbe rivelarsi ostile. A tale proposito si rimanda al capitolo sulla sicurezza industriale.
La connettività ottenuta in questo senso permette di scambiare dati anche a grandissima distanza. L'affidabilità e la banda messa a disposizione da questi collegamenti ha avuto, ed ha ancora, una crescita esponenziale. Tuttavia il passaggio del vero e proprio Industrial Ethernet attraverso Internet è reso molto complesso dall'impossibilità di rispettare i tempi stringenti e le basse tolleranze di perdite di pacchetti spesso previste dai protocolli industriali. Per tale motivo, a livello industriale, questo tipo di comunicazione rimane utilizzata principalmente per funzionalità di supervisione, telecontrollo, teleassistenza o per la comunicazione fra reti industriali autonome appartenenti ad unico sistema produttivo.

#### *Wireless per creazione di Industrial Wireless LAN (IWLAN)*

Le tecnologie Wireless per la creazione di IWLAN sono, invece, pensate per l'emulazione dei cavi all'interno di aree limitate, su distanze fino ad un massimo di qualche centinaio di metri. Quindi tipicamente compatibili con le aree produttive industriali.
In questo campo il più celebre protocollo è IEEE 802.11 meglio conosciuto come WiFi. Tale protocollo è stato proprio concepito per garantire lo stesso Layer 2 del protocollo Ethernet, seppur con il proprio livello fisico basato sulla trasmissione radio. Altri protocolli ampiamente usati per queste connessioni sono quelli descritti in IEEE 802.15 quali Bluetooth, ZigBee e Wireless Hart usate in ambito IT per la creazione di aree personali Wireless (WPAN) su distanze più ridotte.
Nella realizzazione di IWLAN bisogna comunque prestare alcuni accorgimenti particolari, in quanto la natura fisica di questi collegamenti li porta a non essere una perfetta replica di un sistema di cablaggio.
Infatti, nell'accesso remoto Wireless, la coordinazione dello spettro di frequenza utilizzato è realizzato scrupolosamente in base a una serie di rigidi parametri. I provider pagano ingenti quantità di denaro per potersi riservare l'utilizzo esclusivo dei canali disponibili nelle diverse zone di appartenenza. Le WLAN, invece, fanno uso delle bande di frequenza lasciate al libero utilizzo dagli enti regolatori che, però, pongono, in genere, rigide limitazioni alla potenza che può essere emessa in queste gamme di frequenza per garantire la coesistenza di più sistemi. Questo accorgimento impatta, ovviamente, sulle massime distanze dei collegamenti, tuttavia non garantisce completamente dalle mutue interferenze che possono affliggere reti wireless estranee che si trovano a lavorare in prossimità sulla stessa porzione di spettro radio.
A tale scopo tutti i protocolli sopra descritti fanno genericamente utilizzo della banda libera a 2.4GHz, mentre il solo WiFi utilizza anche una serie di bande alla frequenza di 5 GHz.
La presenza di interferenze può portare, oltre che alla perdita totale di comunicazione nei casi più gravi, all'instabilità delle reti Wireless utilizzate, con frequenti perdite di pacchetti. Questo comportamento è del tutto inaccettabile per il trasporto di industrial Ethernet data la già citata sensibilità dei suoi protocolli. Per tale motivo risulta fondamentale nell'implementazione delle reti Wireless industriali una buona coordinazione di tutti i sistemi wireless presenti nell'area industriale, anche quelli non strettamente inerenti all'attività produttiva, ma che sono di pertinenza dell'impianto stesso.

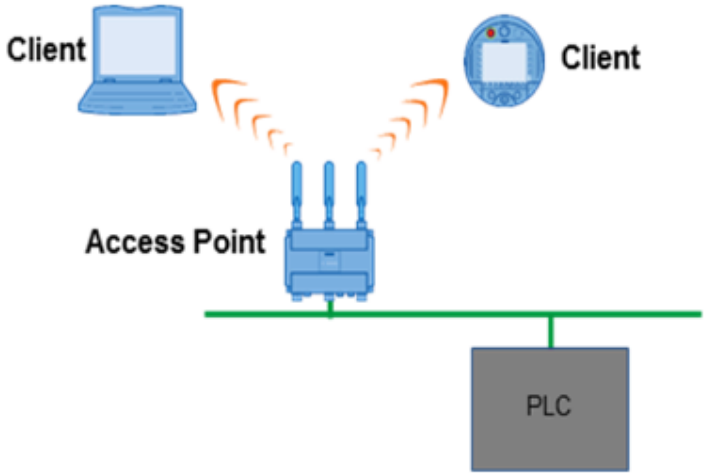



*Figure 17 - Esempio di rete integrata con connessioni IWLAN*

Inoltre i protocolli Wireless sono stati inizialmente concepiti per il trasporto dati nel mondo IT. L'accesso alla rete, soprattutto nei casi di collegamenti multipli è quindi effettuato in maniera non deterministica. La trasmissione dei dati avviene in maniera più complessa e la latenza, ovvero il tempo necessario all'attraversamento del dispositivo può essere significativamente più alto rispetto al cavo. Se si utilizza apparecchiature concepite per uso domestico in applicazioni industriali, la comunicazione diventa instabile e ancora una volta l'attività produttiva è messa a repentaglio. I dispositivi per IWLAN devono quindi possedere feature software che possano rendere compatibile il trasporto real time dei protocolli industriali sul loro livello fisico in modo da garantire adeguatamente la continuità produttiva. Allo stesso tempo i requisiti del protocollo industriale devono poter essere adeguatamente configurati in modo da venire incontro alle tempistiche del Wireless. Questo significa che le attività produttive più esigenti, ad esempio quelle che richiedono controlli sotto il millisecondo, risultano del tutto incompatibili con il trasporto Wireless.

## 3.2 Caratteristiche specifiche

In questo paragrafo andiamo ad analizzare alcune caratteristiche aggiuntive che caratterizzano i componenti come switch e router industriali.

### 3.2.1 VLAN

La gestione delle VLAN, descritta in IEEE 802.1q, è una caratteristica disponibile in alcuni switch gestiti e, solitamente in tutti i router. Questo meccanismo prevede la segmentazione logica del dominio di broadcast all'interno di unica rete Ethernet fisica.

Infatti quando si utilizza una rete tra dispositivi collegati fra di loro mediante esclusivamente protocollo Ethernet, si realizza una LAN (Local Area Network). Trattandosi di Ethernet tutti questi componenti sono quindi raggiungibili dal traffico di broadcast previsto dal protocollo. Ad esempio, quando uno switch tenta di imparare un nuovo indirizzo MAC sconosciuto inoltrando un pacchetto su tutte le sue porte, genera traffico broadcast. In tal caso si può dire che questa LAN rappresenta un unico dominio di broadcast.

Questo meccanismo fa si che quando si utilizza uno switch in senso classico esso possa rigorosamente far parte di un'unica LAN e quindi un unico dominio di broadcast. Se l'utente ha la necessità di escludere la comunicazione fra due gruppi di dispositivi è obbligato a creare due diverse LAN e quindi ad utilizzare due switch diversi anche qualora uno solo di essi possieda un numero di porte sufficienti a soddisfare tutte le connessioni richieste.

Per ovviare a questo problema è nato lo standard IEEE 802.1q che permette di aggiungere nell'intestazione dei frame Ethernet un ulteriore campo denominato VLAN identifier o VLAN tag, composto da 16 bit, diviso in:

- **12 bit di VLAN ID:** numero identificativo della VLAN;
- **3 bit di priorità VLAN** numero che identifica priorità della VLAN, descritto da IEEE 802.1p;
- **1 bit per il campo DEI:** originariamente indicava il formato dell'indirizzo MAC ed era chiamato CFI, ora viene usato a sua volta per la priorità.

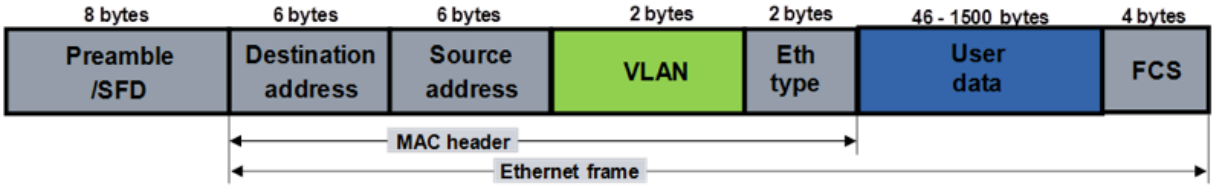



*Figura 18: Struttura del Frame Ethernet con VLAN Tag*

Grazie a questo meccanismo gli switch che supportano IEEE 802.1q sono in grado di identificare l'appartenenza di un frame Ethernet ad una specifica VLAN. In questo modo essi non inoltreranno più i frame in broadcast su tutte le porte ma solo su quelle che sono assegnate alla specifica VLAN potendo di fatto comporre delle LAN virtuali, da cui il termine VLAN. Come conseguenza due dispositivi appartenenti a due differenti VLAN non potranno mai comunicare fra di loro. Ciascuna di queste VLAN rappresenta quindi un diverso dominio di broadcast, seppur appartenenti al medesimo switch.
L'utente, quando intende creare delle VLAN, deve allora configurare le interfacce dello switch, con 2 possibili alternative:

- **Access Port:** interfaccia che supporta una unica VLAN
- **Trunk Port:** interfaccia che supporta più VLAN

In questo senso le Access Port permettono agli switch di assegnare un frame ad una specifica VLAN qualora questo non sia membro di alcune VLAN. Invece le porte Trunk permettono agli switch di condividere le diverse VLAN fra differenti switch.

Col tempo le VLAN sono state utilizzate in maniera sempre più estensiva in ambito IT per separare i differenti tipi di servizi, pur mantenendo un'unica infrastruttura di rete. Inoltre grazie ai bit di priorità è anche possibile gestire i diversi pacchetti con un diverso trattamento, ad esempio preservando il traffico ad alta priorità in caso di congestione della rete oppure permettendo al traffico Real Time di avere la precedenza rispetto a traffico meno importante. Tale meccanismo è definito come Quality of Service (QoS).
L'utilizzo delle VLAN in associazione al servizio QoS, permette la convivenza del traffico di automazione col traffico di tipo Office/IT presente sulla comune infrastruttura Ethernet, senza che quest'ultimo possa provocare delle interferenze e mantenendo le giuste priorità informative. Alcuni protocolli di Industrial Ethernet prevedono proprio l'utilizzo di questi meccanismo in maniera nativa per la propria gestione.
A tal proposito esistono anche switch non gestiti che sono preconfigurati per poter gestire questo tipo di protocolli in priorità permettendo ai pacchetti che vi appartengono di avere un comportamento di tipo deterministico.
Va infine considerato che non è possibile la trasmissione di pacchetti fra due diverse VLAN utilizzando comunicazione su Layer 2 e quindi con soli switch. Tale operazione è resa possibile solo facendo ricorso a dispositivi capaci di eseguire il routing dei pacchetti.

### 3.2.2 Ridondanza

Abbiamo visto nel precedente paragrafo 3.1.2 le possibili topologie di rete permesse nell'Industrial Ethernet. Alcune di esse prevedono la possibilità di creare collegamenti ridondanti in modo che in caso di failure il secondo collegamento possa supplire al primo, garantendo continuità di funzionamento al resto della rete. Questa

caratteristica risulta fondamentale in un ambito produttivo dove le conseguenze di una perdita di comunicazione possono essere nefaste.
Come già visto, la presenza del traffico di broadcast nel protocollo Ethernet non permette di utilizzare collegamenti ridondanti in maniera immediata. Con la chiusura di un percorso ad anello in una LAN Ethernet si rende questo traffico incontrollato. Infatti i pacchetti in broadcast continueranno ad essere inoltrati dagli switch lungo il percorso ad anello all'interno della rete rischiando di arrivare alla congestione della rete e, quindi, ad un suo malfunzionamento.
Per utilizzare Industrial Ethernet è quindi necessario l'utilizzo di protocolli che possano gestire i collegamenti ridondati, tali protocolli devono poter essere gestiti da tutti i dispositivi (i.e. switch) che fanno parte della rete e diventano partecipanti attivi nel ripristino della comunicazione, solitamente chiamata convergenza della rete, in tempi rapidi.

#### 3.2.2.1 Tipologie di ridondanza

La ridondanza può essere considerata su diversi livelli:

*Protezione di collegamento*

In questo caso si cerca di proteggere un singolo collegamento particolarmente critico fra due dispositivi, per proteggersi da problematiche semplici quali disconnessione o danneggiamento del cavo, oppure anche problemi propagativi in caso di trasmissione radio. Questo tipo di protezione è concettualmente semplice e sostanzialmente indipendente dal resto dalla rete. Per questo motivo è solitamente possibile utilizzarla in diversi punti della rete senza incorrere in particolari problemi.

*Protezione di anello*

Questo tipo di soluzione prevede la protezione di una rete lungo un unico percorso chiuso. Il vantaggio che si ottiene è quello di proteggersi oltre che dal semplice problema di un collegamento anche da un guasto di un dispositivo facente parte dell'anello. La protezione che si ottiene è comunque limitata in quanto solo una rottura può essere tollerata. Di contro la logica di intervento di queste protezioni è piuttosto semplice e pertanto permette tempi di intervento incredibilmente rapidi.

*Protezione a più livelli*

Parliamo genericamente di questo tipo di protezione quando l'intento della rete è conservare la comunicazione anche quando si registra più di un singolo guasto nello stesso momento. Questa tipologia è la più vasta e completa, tuttavia è anche la più complessa, motivo per cui le tempistiche necessarie al ripristino della comunicazione sono tipicamente abbastanza lunghe e fuori dall'ordine di grandezza richiesto dall'automazione industriale.

#### 3.2.2.2 Accenni a protocolli di ridondanza

Vediamo alcuni brevi accenni di alcuni fra i più noti protocolli per gestire la ridondanza a livello Ethernet:

*Link Aggregation Control Protocol LACP*

Questa feature prevede la possibilità di effettuare più collegamenti Ethernet fra due switch trattandoli logicamente come se fossero un unico collegamento. Questa tecnica ha due vantaggi, innanzitutto permette di aumentare la banda del collegamento fino, nel caso ideale, alla somma delle bande dei diversi collegamenti. In seconda istanza, il collegamento complessivo, continuerà a funzionare, a banda ridotta, anche quando uno dei collegamenti fisici dovesse incorrere in qualche problema. Esistono numerose versioni e tecniche per l'implementazione di questa funzionalità.

*Figura 19 - Esempio di aggregazione di link*

### *Parallel Redundancy Protocol PRP*

PRP è un protocollo, definito in IEC 62439-3, che prevede la duplicazione fisica dei frame da parte dello switch che supporta tale protocollo. Questi frame sono numerati dal protocollo stesso in modo che lato ricezione gli altri switch possano scartare uno dei due frame e mantenere una comunicazione univoca. Con questo meccanismo è possibile non solo creare una protezione sul singolo collegamento ma anche una vera e propria rete completamente ridondata. Il grande vantaggio di questa tecnica consiste nel fatto che il tempo di recupero da guasti sia essenzialmente nullo, motivo per cui ha riscosso un notevole successo nel mondo industriale. Tuttavia bisogna prestare attenzione a mantenere i percorsi ridondati simili perché qualora i frame subiscano un'eccessiva differenza sulla latenza del loro trasporto i dispositivi riceventi potrebbero essere messi in difficoltà nel riconoscere gli effettivi pacchetti.

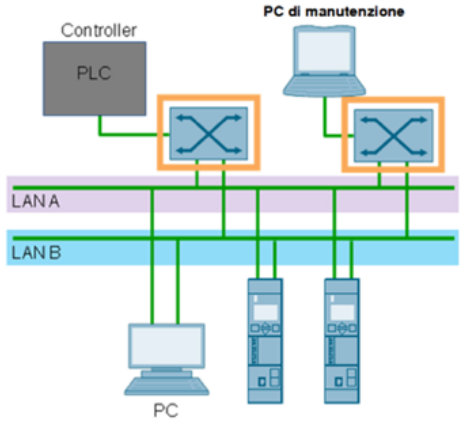



*Figura 20 - Esempio di comunicazione ridondata con PRP*

### *Hiper-Ring Protocol HRP/ Media Redundancy Protocol MRP*

Questi protocolli sono i più usati in ambito industriale, infatti permettono di implementare la protezione di anello in tempi rapidissimi, con MRP che deriva dal precedente HRP. Nella pratica si basano su un gestore, detto Ring Manager, che blocca il traffico su una delle due interfacce che possiede sull'anello. In questo modo, in condizioni di normale funzionamento, il percorso ad anello non si chiude. Il manager monitora costantemente lo status dell'anello e qualora rilevi una rottura va ad aprire l'interfaccia chiusa e avvisa gli altri membri dell'anello, detti Client, del cambio topologico, in modo che essi si adeguino alla nuova struttura. Questo sistema fa si che il tempo di convergenza del protocollo sia limitato a poche centinaia di ms, a seconda della grandezza dell'anello. In alcuni switch industriali questi protocolli sono già preconfigurati su alcune specifiche interfacce, inoltre questi switch sono anche in grado di negoziare in autonomia chi fra loro debba essere il manager dell'anello. Questi accorgimenti rendono la configurazione di questo protocollo molto semplice in quanto l'utente può semplicemente limitarsi ad effettuare le connessioni sulle interfacce corrette.

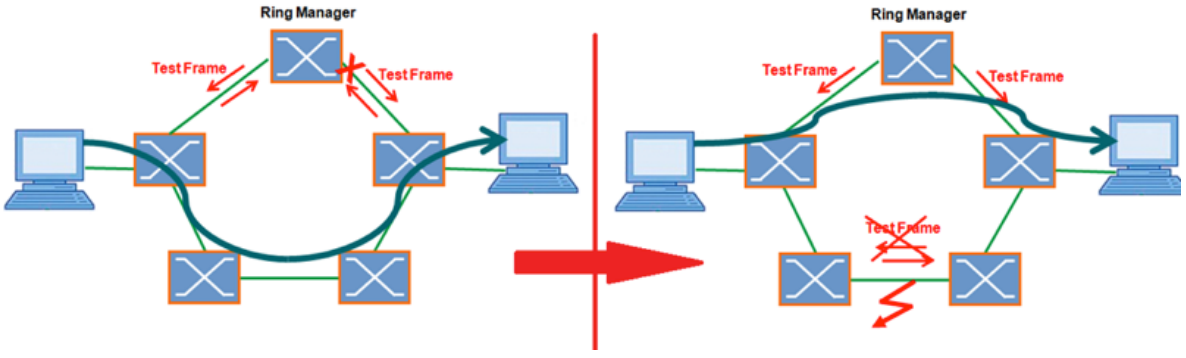



*Figura 21 - Esempio di MRP/HRP ad anello chiuso (sinistra) ed aperto (destra)*

*Rapid Spanning Tree Protocol RSTP*

RSTP, evoluzione del precedente STP, definito in IEEE 802.1w, è invece il protocollo di ridondanza Ethernet storicamente più diffuso nel mondo IT/Office. Questo protocollo similmente a HRP/MRP prevede la presenza di uno switch principale della rete detto root, e della chiusura fisica delle interfacce per impedire la chiusura dei percorsi ad anello. Il root della rete viene stabilito direttamente dai partecipanti alla rete in un processo definito come root election in base a dei parametri definiti dall'utente. Successivamente gli switch in base ad un algoritmo vanno a stabilire quali sono le interfacce che vanno chiuse per evitare percorsi ridondati aperti, mantenendo esclusivamente una topologia funzionante ad albero, da cui deriva il nome del protocollo. In caso di perdita di un nodo gli switch sono in grado di accorgersene in base a dei frame di controllo e intervengono per aprire un nuovo percorso. Con l'ulteriore evoluzione del protocollo Multiple Spanning Tree, Protocol (MSTP) è inoltre possibile strutturare diverse VLAN in modo da ottimizzare l'utilizzo delle interfacce all'interno della rete.
L'algoritmo di funzionamento del MSTP permette quindi di gestire topologie ad anello ma anche strutture decisamente più complesse. Con l'RSTP, e l'evoluzione MSTP i tempi di convergenza risultano però significativamente maggiori rispetto ai protocolli ottimizzati per la gestione degli anelli. Inoltre la sua configurazione è leggermente più complessa per una parametrizzazione ottimale, sebbene la connettività della rete in sé sia sempre garantita.

### 3.2.3 Routing

Industrial Ethernet può essere utilizzato per la creazione di sistemi chiusi e quindi di reti LAN autonome come nei tradizionali sistemi produttivi. Tuttavia il grande vantaggio che risiede nel suo utilizzo è dato dalla possibilità di interfacciare queste aree a monte in unica infrastruttura di rete e metterle in comunicazione a loro volta con altre parti di rete non strettamente aziendale. L'area in cui si effettua questo incontro viene definita come Backbone Aggregation.
Questo concetto di connettività è estremamente importante, infatti lo sviluppo dell'interconnettività è la chiave per giungere alla completa digitalizzazione dell'automazione industriale e quindi sfruttare tutti i vantaggi derivati dalla quarta rivoluzione industriale.

Per poter comunicare fra i diversi segmenti della rete occorrono dispositivi capaci di fare routing, ovvero di elaborare sul livello di rete (Layer 3 ISO/OSI) o meglio sul protocollo IP.

Infatti alle diverse LAN o VLAN sono assegnate delle sottoreti IP, ovvero un set rigido di indirizzi IP, definito per l'appunto dalla loro maschera di sottorete. I dispositivi all'interno di queste LAN possono comunicare esclusivamente fra di loro, con la notevole eccezione dei router. Essi hanno infatti interfacce su diverse sottoreti e possiedono una tabella, definita routing table, in cui sono memorizzate le interfacce su cui possono raggiungere le sottoreti a loro note. Quando un pacchetto giunge su un'interfaccia questi dispositivi eseguono l'operazione di routing che consiste nel verificare a quale sottorete sia destinato il pacchetto ed inoltrarlo sull'interfaccia corretta.

I router ovviamente riconoscono autonomamente le sottoreti su cui insistono le loro interfacce, tuttavia non hanno modo di conoscere eventuali sottoreti che si trovino interconnesse alle prime mediante altri router interposti fra di loro. Viene però lasciata all'utente la possibilità di inserire manualmente nella routing table queste sottoreti indicando al router l'interfaccia e l'indirizzo del successivo router da cui poter accedere a quella parte della rete. In questo modo il router sarà in grado di inviare correttamente il pacchetto al router successivo. Tale procedimento può essere ripetuto numerose volte permettendo al router di attraversare un grande numero di diverse sottoreti fino al raggiungimento del router che possiede la destinazione finale su un'interfaccia locale dove verrà riaffidato al Layer 2 sottostante. Tale procedimento è definito come routing statico.

Un dispositivo che dunque conosce l'indirizzo IP del suo destinatario non ha altro bisogno che di sapere quale sia il router nella sua sottorete, tale router viene definito come Default Gateway del dispositivo. Saranno poi i router a garantire il trasporto al destinatario finale anche qualora si trovasse dall'altra parte del mondo.

Il routing statico, può essere utilizzato senza problemi in caso di reti molto semplici, tuttavia inserire manualmente tutte le righe della tabella di reti complesse diventa incredibilmente oneroso. Inoltre in caso di modifiche alla rete si ha la necessità di andare a modificare una ad una tutte le tabelle di ciascun router presente nella rete. Per

ovviare a questo problema sono stati quindi concepiti dei protocolli basati su Layer 3, definiti come protocolli di routing. Essi prevedono che i router contigui si scambino autonomamente informazioni sulle proprie routing table andando a propagare in tutta la rete la posizione delle diverse sottoreti. In caso di cambiamenti dovuti a guasti o nuove configurazioni essi sono in grado di avvisare gli altri router della modifica topologica senza richiedere alcun intervento esterno, col notevole vantaggio di essere quindi in grado di gestire strutture ridondate anche particolarmente complesse. Tale procedimento si definisce come routing dinamico.

I protocolli di routing si dividono in esterni ed interni. I primi sono utilizzati per scambiare dati fra tutte le reti all'interno di Internet, fra cui il più celebre è BGP. I secondi servono invece per creare il routing dinamico all'interno di reti autonome, ovvero gestiti da un'unica entità, come per l'appunto un'impresa o un provider di servizi. Tipicamente in questi casi si usano RIP, IS-IS e OSPF.

Un altro protocollo importante relativo al routing è VRRP. Tale meccanismo permette a due router interconnessi di accordarsi fra di loro per creare una specifica ridondanza del router. I due dispositivi utilizzano lo stesso indirizzo IP ma uno dei due rimane silente, pronto ad intervenire solo in caso di guasto all'altro, senza che nessuno dei dispositivi nella rete locale se ne possa rendere conto. Questa tecnica risulta estremamente utile quando l'accesso da e verso una LAN risulti fondamentale e non possa tollerare problemi relativi ad un fault sul proprio gateway.

### 3.2.4 NAT

Il NAT ovvero "Network Address Translation" è una feature basata su Layer 3, oggi disponibile su diversi router. Questo meccanismo gli permette di realizzare una vera e propria traduzione degli indirizzi IP dei dispositivi a loro connessi permettendo ad una parte dei dispositivi, se non a tutto il mondo, di vedere un'altra parte con indirizzi diversi rispetto a quelli che realmente utilizzano.

Infatti agli albori della nascita di Internet e del protocollo IP si decise di utilizzare per gli indirizzi dei numeri a 32 bit che permettevano di avere a livello globale oltre 4 miliardi di indirizzi all'epoca ritenuti sovrabbondanti. Con l'esplosione della rete però, nel corso dell'ultima decade dello scorso secolo ci si rese presto conto che tale numero non sarebbe stato sufficiente a contenere tutti i dispositivi che presto si sarebbero interfacciati sulla rete. Le soluzioni trovate per affrontare questo problema furono due: da una parte una nuova versione del protocollo detta IPV6 che utilizzava indirizzi più estesi a 48 bit e dall'altra l'utilizzo del NAT.

Con questo meccanismo dei dispositivi possono essere configurati per utilizzare un certo set di indirizzi, ma in caso uno di questi voglia inviare un pacchetto verso l'esterno inoltrandolo verso il proprio gateway, quest'ultimo, abilitato all'uso del NAT, sostituisce nell'intestazione del pacchetto l'indirizzo sorgente reale con un altro. E' anche possibile che tutti i dispositivi nella rete utilizzino come indirizzo di NAT un unico indirizzo a loro assegnato. Tuttavia per poter distinguere il dispositivo origine del pacchetto, in modo da potergli inviare una risposta, il router può anche cambiare la porta di origine all'interno dell'intestazione TCP o UDP del pacchetto. Tale meccanismo si definisce Network Address & Port Translation (NAPT) o più semplicemente Port Forwarding e permette oggi di risparmiare numerosissimi indirizzi permettendo ai router di usare un unico indirizzo IP, detto indirizzo pubblico, per tradurre diversi indirizzi IP locali, detti indirizzi privati.

A livello industriale questo meccanismo torna invece utile per diversi motivi:

- Innanzitutto permette a sua volta di risparmiare indirizzi in una rete quando l'indirizzamento IP è gestito da un'entità estranea ai progettisti dell'impianto che hanno assegnato a tale unità produttiva meno indirizzi di quelli necessari a tutti i dispositivi connessi in rete.
- Inoltre questo meccanismo permette ai progettisti di creare progetti con indirizzi unici che non andranno riconfigurati in un secondo momento. Basterà infatti riconfigurare il gateway della rete con un NAT appropriato, rendendo gli OEM indipendenti dal cliente finale nella gestione dei loro progetti.
- Infine l'utilizzo del NAT può rendere possibile ai dispositivi a valle del router di vedere i pacchetti in arrivo dell'esterno come in arrivo dalla sottorete a cui appartengono, evitando quindi di dover impostare il default gateway per tutti i dispositivi nella rete che devono comunicare verso l'esterno.

# 4. Safety su reti Industrial Ethernet

## 4.1 L'approccio "black channel" dei protocolli di sicurezza

La teoria di come rendere i protocolli di sicurezza indipendenti dal bus specifico su cui verranno utilizzati viene comunemente definita come approccio di tipo "blach channel".

Questo approccio prevede che la nuova funzionalità di sicurezza sia costruita sulla base del protocollo esistente senza che il protocollo di sicurezza ne sia a conoscenza, pertanto il protocollo di sicurezza viene tenuto "al buio" o "black" dell'ambiente in cui opera.

E' previsto comunque lo sviluppo di blocchi di protocollo per la rilevazione di errori di comunicazione nelle varie interfacce interconnesse al bus di comunicazione.

Si tratta della direzione in cui gran parte dei protocolli dei bus di sicurezza si sono orientati negli sforzi per lo sviluppo, riducendo per quanto possibile le modifiche all'infrastruttura di rete.

L'esigenza di non interferire nelle pratiche di gestione del network è alla base di questo tipo di progettazione perché, qualora l'aggiunta del protocollo di sicurezza avesse richiesto modifiche nella normale gestione della rete sarebbero sorte due problematiche principali:

- Si sarebbero inevitabilmente sommati dei rischi legati alla coesistenza di vari layer introducendo elementi che avrebbero automaticamente posto limitazioni ad una rete che standard non sarebbe più stata;
- Si sarebbe usciti dall'idea base di un canale "black channel".

Tale sviluppo ha portato all'aggiunta, come sopra accennato, di una parte di blocchi funzione di comunicazione nei singoli elementi di sicurezza che si connettono con specifiche rispondenti alle normative 61508.
Infatti, questi elementi, oltre ad avere i blocchi funzione legati allo svolgimento della funzione specifica sono delegati anche alla gestione dei controlli squisitamente legati alla sicurezza della comunicazione stessa.
Questa filosofia aiuta a rendere l'installazione di componenti di sicurezza all'interno di una macchina o di un impianto meno complessa.
I sensori e gli attuatori si collegano alla rete, che supporta anche le funzioni di sicurezza.
Utilizzando il principio "black channel", i dati legati alla sicurezza vengono scambiati attraverso la rete esistente, consentendo l'integrazione delle varie tipologie di componentistica.
Come detto, il principio black channel permette lo scambio dei dati tipici della parte safety insieme a quelli tipici delle normali funzioni di automazione.
Quindi indipendentemente dal meccanismo di trasporto scelto per il trasporto dei dati "standard" sulla linea, le componenti di sicurezza sono in grado di trasmettere le loro informazioni utilizzando un protocollo isolato e sicuro creando un "tunnel" all'interno dello stesso canale.
Poiché i protocolli di sicurezza sono applicazioni puramente a livello di protocollo, senza caratteristiche fisiche proprie, la banda disponibile ed il tempo di ciclo dipendono dal protocollo di trasporto in cui sono incapsulati.
I possibili errori che potrebbero intervenire durante la trasmissione sono stati analizzati e resi di domino pubblico attraverso le normative IEC 61784-3 ed IEC 61508.
La loro prevenzione (e l'eventuale riconoscimento) deve essere implementata come una parte fondamentale del protocollo di sicurezza. La qualità di rilevamento e gestione degli errori dipende dal livello di sicurezza che deve essere raggiunto.

## 4.2 Accenni e Profili Safety

Vedremo ora i meccanismi legati ai profili di sicurezza e delle informazioni nelle comunicazioni industriali legate al controllo di processi o di macchine. Questi livelli sono regolamentati dalle normative IEC 61784-3.

Il numero di produttori che forniscono tecnologie di comunicazione legate alla sicurezza è in continuo aumento e la normativa di riferimento per questi prodotti è la IEC 61508.
Tale aumento si traduce in un aumento dei prodotti disponibili sul mercato che risolvono problematiche specifiche quali ad esempio PLC di sicurezza, Bus di campo che comprendono una parte di protocollo dedicata alla sicurezza, laser scanners per rilevare la presenza di operatori umani, barriere a infrarossi, ecc.
Molti produttori si stanno dedicando allo sviluppo di oggetti dedicati alla sicurezza.
Una parte fondamentale di questi prodotti è legata ai profili utilizzati nella comunicazione, i quali devono garantire i livelli di SIL (Safety Integrity Level) o di PLr (Performance Level required).

Negli anni passati abbiamo assistito ad un continuo aumento delle informazioni disponibili in un sistema di controllo, questo fattore è stato guidato da un miglioramento esponenziale delle prestazioni delle reti di comunicazione. Conseguenza prima la disponibilità di informazioni di diagnostica di dettaglio del singolo prodotto e della rete di comunicazione nel suo insieme.
In tutte le situazioni la comunicazione è una parte essenziale di un sistema che controlla funzioni critiche. Lo scambio di dati corrotti e la mancata rilevazione di questa condizione può portare a conseguenze molto serie sia dal punto di vista economico che da quello di danni a persone. Queste sono le motivazioni primarie per cui un sistema di sicurezza deve essere progettato in modo da garantire il livello SIL o PLr.

Le tecnologie di comunicazione di tipo Fieldbus sono ormai entrate nello stadio di maturità e sono comunemente accettate, anche perché riferite a normative internazionali codificate. Sono state sviluppate anche per supportare le comunicazioni di sicurezza in modo da garantire, anche in caso di perdita di informazioni, che il sistema intervenga portando l'impianto o la macchina in condizione sicura. Lo specifico utilizzo delle funzioni comuni da parte di gruppi di partecipanti viene definito "profilo".
Per le comunicazioni industriali, secondo le sette famiglie di protocolli (CPF) sono definite dieci tipologie di protocolli di comunicazione.

| CPF | Types of communications protocol | | |
|---|---|---|---|
| CPF1 | Foundation Fieldbus (Type 1) | FF High Speed Ethernet (Type 2) | FF FMS (Type 3) |
| CPF2 | Control Net (Type 4) | | |
| CPF3 | Profibus/Profinet (Type 5/Type6) | | |
| CPF4 | P-Net (Type 7) | | |
| CPF5 | World FIP (Type 8) | | |
| CPF6 | INTERBUS (Type 9) | | |
| CPF7 | SwiftNet (Type 10) | | |

*Figura 22 - Protocolli di comunicazione industriale*

Tra i primi costruttori che hanno iniziato ad utilizzare i principii della sicurezza nello sviluppo dei prodotti troviamo la tecnologia CAN e prodotti sviluppati dall'organizzazione ODVA (Open DeviceNet Vendor Association). Lo standard CIP Safety, pubblicato da ODVA rende possibile l'utilizzo in contemporanea di oggetti "standard" e di oggetti di "sicurezza" sullo stesso link di comunicazione. Le reti con tecnologia Profibus e Profinet sono legate ad un altro gruppo di leader di mercato nell'ambito dei bus di campo.
Anch'essi hanno sviluppato il concetto basato sulla coesistenza di informazioni "standard" e di "sicurezza". Questa soluzione si firma ProfiSafe ed insieme al profilo ProfiDrive sono state validate e preparate per l'utilizzo sia sulla rete ProfiBus che su ProfiNet.
Anche la tecnologia wireless si sta rapidamente evolvendo verso la sicurezza. Molti protocolli disponibili sono già validati per l'uso in ambito wireless.

Al livello informativo della gerarchia di comunicazione la parte di sicurezza viene realizzata nelle reti Ethernet sulla base dei protocolli di comunicazione sicura, ad esempio SNP (Simple Network Management Protocol), SSL (Secure Socket Layer), TLS (Transport Layer Security) e VPN (Virtual Private Networks).
Ad esempio, la tecnologia Profibus/Profinet ha sviluppato una soluzione sicura (Scalance S) per ProfiNet sulla base di VPN, per mezzo della modalità "tunnel" utilizzando il protocollo IPsec.

I principii di base della sicurezza dei bus di campo e la definizione di servizi aggiuntivi e dei protocolli di comunicazione sono definiti dalla normativa IEC 61784-3.
I requisiti richiesti ai bus di campo che supportano la sicurezza possono essere riassunti nei punti seguenti:

- Coesistenza di comunicazioni "standard" e di comunicazioni "sicure";
- Meccanismi di sicurezza per garantire il livello SIL richiesto sono collocati in un layer di comunicazione sicura aggiuntivo;
- La rete contiene elementi ridondanti, i dati vengono ritrasmessi due volte (valore attuale ed inverso), il sistema utilizza tecniche a due canali o strutture a tre canali;
- In caso di evento pericoloso il sistema deve interrompere le comunicazioni e mettersi in uno stato di sicurezza definito.

Sia nei sistemi aperti che in quelli chiusi il messaggio è uno dei principali soggetti dell'analisi di sicurezza.
Secondo la norma EN 50159-1 il messaggio è definito come una informazione di utilità, che viene generata da una sorgente e che deve essere trasmesso nel tempo $\Delta t$ dall'inizio della trasmissione alla stazione di destinazione. Attacchi al messaggio che siano trasmessi attraverso il link di comunicazione possono portare a cadute della comunicazione tra le stazioni. Il canale di comunicazione interferisce nella comunicazione dei messaggi attraverso rumori di fondo, interferenze o può causare indebolimento del segnale utile. Questi effetti sono generalmente definiti come Interferenze Elettromagnetiche (EMI) e hanno un forte effetto sull'integrità del messaggio quando non rilevati. Gli effetti del rumore possono mostrarsi in forme diverse che dipendono principalmente dalle caratteristiche fisiche del canale di comunicazione.

Nei bus di campo possiamo prevedere i seguenti tipi di attacco al messaggio:

- Corruzione del contenuto
- Ripetizione del messaggio non prevista
- Ordine di invio modificato
- Perdita di un messaggio
- Ritardo di comunicazione inaccettabile
- Aggiunta di messaggio non previsto

L'eliminazione del rischio comporta l'utilizzo di misure di sicurezza. Il tipo e la forza delle misure sono legati dipendono dall'applicazione e dal livello di SIL desiderato.

I seguenti requisiti devono essere soddisfatti nel protocollo di comunicazione:

- Mantenimento dell'Integrità di Comunicazione
- Gestione del timeout nell'invio dei messaggi
- Mantenimento della corretta sequenza di invio dei messaggi

Le seguenti misure di sicurezza sono state definite nei bus di campo per garantire i seguenti requisiti:

- Numero in sequenza
- Time stamp
- Timeout
- Autenticazione della connessione
- Messaggio di conferma di ritorno
- Codice di sicurezza

I requisiti relativi alle misure di sicurezza devono essere inclusi nelle specifiche del sistema e della sua sicurezza.
Possiamo vedere un esempio di Profilo di Sicurezza nella tecnologia Profibus e Profinet, denominato Profisafe nella figura sottostante.

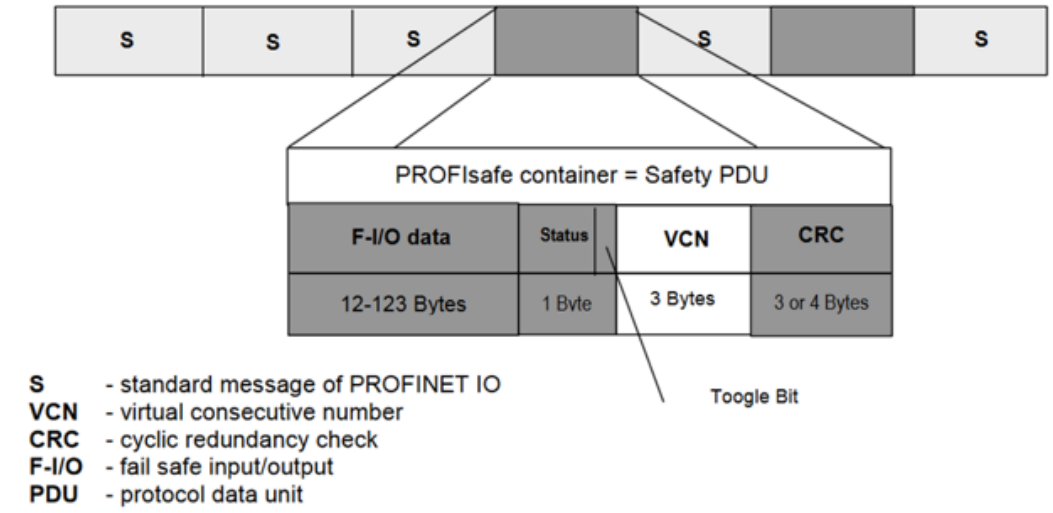



*Figura 23 - Esempio di profilo di sicurezza Profisafe*

Nel profilo Profisafe sono utilizzate le seguenti misure di sicurezza:

- Numerazione consecutiva
- Timer di watchdog con ricevuta
- Nome in codice per l'autenticità e la verifica della consistenza del dato

Il messaggio Profisafe con livello SIL 3 o Categoria 4 secondo le normative EN 954-1 (13849-1) soddisfa i livelli di sicurezza richiesti nell'industria di processo e manifatturiera. Le misure di sicurezza sono processate e monitorate in una unità fail-safe e sono in grado di eliminare gli errori di comunicazione che possono intervenire durante la trasmissione dei messaggi.

# 5. Security su reti Industrial Ethernet

## 5.1 I rischi

Proteggere i propri sistemi è divenuto un elemento critico di ogni attività industriale e delle infrastrutture.
I danni di un possibile attacco possono, infatti, provocare incidenti anche gravi. Pensiamo, ad esempio, a una centrale nucleare, a un aeroporto o a un veicolo con sistema di controllo via rete; un possibile attacco potrebbe provocare danni enormi sia alle persone sia alle cose.
Con la convergenza sulla rete IP di IT (Information Technology) e OT (Operation Technology) ed il collegamento di un numero sempre maggiore di dispositivi di automazione che in precedenza erano connessi su reti differenti, il tema della sicurezza e protezione nella comunicazione sta diventando sempre più rilevante.
Le tecnologie di comunicazione su rete Ethernet garantiscono vantaggi di maggior interoperabilità tra sistemi, ma potrebbero, se non attivate opportune protezioni, esporre potenzialmente gli apparati ai ben noti problemi di security che caratterizzano da decenni le tecnologie IT adottate nel mondo office.
Concentrandoci sui rischi attinenti il mondo industriale, tra questi possiamo senz'altro evidenziarne alcuni diretti (perdita di dati, perdita di know-how, fermi di produzione, modifica dei livelli di sicurezza degli impianti di produzione, ecc.) e alcuni indotti, quali ad esempio il costo di ricostituzione dei dati di produzione (storico, modifiche di impianti, traccia degli incidenti, ecc.), costo del ripristino di impianti "sabotati" o il costo, a volte incalcolabile, della perdita di reputazione sul mercato dell'azienda attaccata.
Senza contare le ripercussioni legali che possono derivare da incidenti mortali causati da propri impianti non più sotto controllo.

## 5.2 I concetti generali di protezione

L'approccio ad una corretta progettazione della rete dovrebbe implicare una gestione globale della Security aziendale, tenendo conto delle esigenze IT e OT in maniera olistica.
La Security può essere definita come l'insieme delle regole e norme rivolte alla sicurezza informatica che consentono alle aziende di mettere in atto quelle procedure tecniche atte a ridurre al minimo il numero di attacchi alla propria sicurezza informatica, in altre parole di diminuire la propria vulnerabilità.
In modo schematico, un'adeguata protezione contro intrusioni non volute in una rete Ethernet è basata su pochi concetti fondamentali.
Il primo è relativo a una corretta protezione delle porte di accesso alla rete, siano esse accessibili localmente (porte fisiche di switch, PC, PLC o altri dispositivi) o che possano prevedere accesso da remoto per operazioni di teleassistenza.
Un secondo concetto fondamentale è quello basato sulla segmentazione della rete in più zone, separate tra loro, che comunicano tra loro solo attraverso percorsi ben definiti e ben protetti (firewall, VPN, ...) secondo i principi inclusi all'interno della serie di norme internazionali IEC 62443 "Industrial communication networks - Network and system security".
Da ultima, ma non ultima per importanza, la presenza di soluzioni di controllo continuo della rete permette di poter accorgersi in tempo reale di anomalie indicative di accessi e modifiche già intervenute.

## 5.3 I sistemi di protezione

Le metodologie di protezione tipiche del mondo ufficio si stanno estendendo anche al mondo degli impianti industriali, almeno nei concetti generali. I due mondi, infatti, hanno comunque priorità differenti: il mondo ufficio focalizza la propria attenzione sulla protezione del dato mentre l'ambiente industriale, oltre a questo, è anche fortemente interessato alla disponibilità di servizio.
In un sistema di Security olistico della rete, vanno considerati in primo luogo diversi livelli di accesso per differenti classi di utilizzatori. Oggi esiste un'ampia disponibilità sul mercato di sistemi software per l'identificazione degli accessi che sono operativi in modo trasparente agli utenti e naturalmente senza utilizzare se non una minima

parte delle risorse di rete disponibili per non ridurre in nessun modo le prestazioni dei processi in corso. Ogni richiesta di accesso alla rete avvia un processo di identificazione che dovrebbe valutare anche aspetti quali il mezzo di connessione usato (rame, fibra, wireless), la posizione e la velocità (10, 100 Mbps, 1, 10 G) della porta di accesso sullo switch o router usata dal dispositivo che sta accedendo, oltre ad identificare il tipo dello stesso (netebook, tablet, smartphone, oppure altro) e successivamente applicare la policy definita per quello specifico utente su quella rete.
I moderni sistemi di identificazione sono in grado di validare l'accesso da uno specifico sistema operativo, oppure ad un determinato applicativo. Solo dopo aver verificato la congruità di ognuna delle precedenti discriminanti poste come condizioni, l'accesso dovrebbe essere consentito alla subnet di una specifica zona.
Esistono dunque diverse strategie che consentono la protezione nella comunicazione dati, cominciando dai livelli più bassi di protezione fisica dei cavi e apparati, fino ad arrivare a meccanismi di protezione a livello di protocollo di comunicazione.
Di seguito vengono illustrate per sommi capi alcune delle possibili soluzioni tecnologiche atte alla creazione di un adeguato sistema di difesa contro accessi non voluti a reti (Industrial) Ethernet.

### 5.3.1 Port Security

Uno degli approcci più comuni per mettere al sicuro la propria rete dati si basa sulla sicurezza fisica degli apparati. L'obiettivo alla base di quest'approccio è quello di impedire l'accesso fisico non autorizzato alle porte di rete degli apparati.
Se un malintenzionato ha accesso fisico a una porta di rete dell'impianto, potrebbe collegare un proprio dispositivo per cercare di rubare informazioni o dare disservizio.
Per operare tale protezione è necessario utilizzare dei dispositivi che supportano questa funzionalità, come i "Managed Switch", detti anche "Switch Gestiti", cioè switch che possiedono un'interfaccia amministrativa che consente di variarne la configurazione.
Una protezione di facile implementazione consiste nel disabilitare tutte le porte di rete che non sono utilizzate.
Tuttavia la protezione non risulta efficace nel caso in cui il malintenzionato abbia la possibilità di scollegare uno dei cavi delle porte funzionanti e collegarsi alla rete attraverso questa porta attiva.
Pertanto occorre configurare le singole porte in modo che solo i dispositivi autorizzati possano accedervi.
Questo si può realizzare impostando sull'apparato l'indirizzo fisico (MAC address) delle macchine autorizzate oppure utilizzando un sistema di autenticazione che viene descritto nello standard IEEE 802.1x.

### 5.3.2 VLAN

Una delle metodologie più utilizzate per proteggere una rete industriale, è quella di suddividerla in zone isolate tra loro, tipicamente classificate per area funzionale e/o criticità.
Operando in questo modo s'impedisce che l'accesso non autorizzato a una di queste zone possa essere utilizzato per accedere ad altre zone più critiche o vulnerabili.
Ad esempio, l'accesso a una zona di controllo qualità può essere mantenuta separata dalla produzione vera e propria.
Nella zona qualità, caratterizzata da un maggior passaggio di persone, un disservizio può essere tollerato, mentre in produzione no.
Le Virtual Local Area Network sono dunque delle reti logicamente separate ma situate sugli stessi supporti fisici. Possono essere considerate in senso lato una componente della Security perché la segmentazione realizza reti più strutturate e robuste.
Una catena di apparati di rete può propagare selettivamente più di una VLAN, rendendole disponibili anche a distanze molto elevate.
La trasmissione nelle reti che implementano le VLAN avviene secondo lo standard IEEE 802.1q, cioè aggiungendo un TAG al pacchetto dati che contiene il numero di VLAN sulla quale si vuole trasmettere.
Ciascun apparato di rete può definire, porta per porta, a quali VLAN appartengono, dunque quali TAG sono accettati o meno.

### 5.3.3 SNMP

Simple Network Management Protocol è un protocollo di comunicazione definito dall'IETF (Internet Engineering Task Force) che consente la configurazione, la gestione e la supervisione degli apparati collegati a una rete.
Attraverso opportuni cruscotti di supervisione è possibile monitorare lo stato della rete; il verificarsi di alcuni eventi, come l'inserimento di un nuovo dispositivo nella rete, l'aumento improvviso del traffico e del carico di lavoro degli apparati, può offrire utili indicazioni per prevenire le intrusioni.
Il protocollo SNMP consente anche la configurazione a distanza degli apparati che può essere sfruttata per contrastare il verificarsi di un attacco. Ad esempio, è possibile disabilitare la porta di rete alla quale il malintenzionato si è collegato.

### 5.3.4 HTTPS

HTTPS è l'acronimo di HyperText Transfer Protocol over Secure socket layer.
In altre parole si tratta di un protocollo di comunicazione che rende sicura la trasmissione HTTP, comunemente utilizzata dai dispositivi, attraverso l'utilizzo di algoritmi di cifratura e autenticazione dei dati trasmessi. L'utilizzo di questo protocollo assicura la protezione da un attacco di tipo "Man In The Middle", cioè da parte di un terzo soggetto che s'interpone tra i due dispositivi per intercettare o modificare i valori scambiati.
HTTPS garantisce:

- L'autenticità di chi trasmette. Impedisce a una terza parte di falsificare i dati e spacciarsi per il mittente.
- Protezione del dato. Impedisce a un malintenzionato di poter leggere i dati che i due dispositivi si stanno scambiando.
- Integrità del dato. Impedisce a un malintenzionato di modificare i dati trasmessi tra i due dispositivi.

### 5.3.5 VPN

Una grossa percentuale della comunicazione dati in un impianto industriale avviene "in chiaro", cioè senza alcun meccanismo di protezione del dato.
Questo scenario ha sia origini storiche, dove chi ha implementato i sistemi di comunicazione non si è posto il problema della sicurezza, ma anche una logica di comunicazione in una zona intrinsecamente considerata sicura. Basti pensare a una zona di produzione dove l'accesso all'edificio (e dunque alla rete) è consentito al solo personale autorizzato.
Con l'avvento di Industry 4.0 e dell'IOT (Internet Of Things) i sistemi vengono spesso collegati alla rete globale di Internet per trarre vantaggi dalle più recenti tecnologie, come i servizi di Amministrazione Remota e Cloud.
Questo impone l'adozione di meccanismi di protezione del dato che viene veicolato su una rete considerata "non sicura".
Le Virtual Private Network vengono incontro a questa esigenza: implementano un meccanismo di protezione, basato su sistemi di cifratura e firma digitale, che impediscono l'intercettazione e contraffazione dei dati da parte di malintenzionati.
Le reti VPN offrono alle aziende, a un costo relativamente contenuto, la possibilità di effettuare teleassistenza sicura dei propri apparati e la possibilità di estendere la rete locale, nel caso l'azienda operi su un ampio territorio.

### 5.3.6 Firewall

Il Firewall è un elemento di rete perimetrale necessario per la protezione in ambito industriale qualora essa venga esposta a una rete non sicura, tipicamente Internet.
Il firewall regola gli accessi dalla zona non sicura verso la zona sicura, impedendo accessi indesiderati e che potrebbero danneggiare l'impianto.
La zona non sicura viene tipicamente indicata come WAN (Wide Area Network) mentre la rete sicura è indicata con l'acronimo LAN (Local Area Network); in questa concezione il firewall regola gli accessi tra WAN e LAN.
A volte è presente una terza zona di rete chiamata DMZ (DeMilitarized Zone) atta a ospitare i sistemi che per loro

natura devono rimanere isolati dalla LAN ma che necessitano comunque una protezione da attacchi provenienti dalla WAN.
Un firewall, per poter essere efficace, deve essere configurato da personale specializzato che inserisce le regole di accesso.
Tali regole operano dei filtri sul traffico in ingresso/uscita in base ai dispositivi che generano i dati, ai protocolli e alla direzione del traffico.
I sistemi firewall più evoluti implementano anche dei filtri selettivi di protocollo industriale come OPC o MODBUS che possono consentire solo certe operazioni, ad esempio la sola lettura delle variabili MODBUS e non la loro scrittura.

# 6. Le norme di riferimento

La progettazione delle reti di comunicazione industriale richiede una conoscenza aggiornata, oltre che delle realizzazioni tecnologiche, architetture di rete e modalità operative, anche dei vincoli relativi alle normative vigenti. Le reti di comunicazione sono infatti quei componenti che danno vita ad un sistema di automazione in quanto consentono di interconnettere i sensori e gli attuatori, con i dispositivi di elaborazione delle modalità di controllo e i sistemi da controllore, che divengono sempre più complessi e richiedono sempre maggiore integrazione anche in ottica di Industria 4.0.

### *Reti industriali*

La normativa sulle reti di comunicazione per l'automazione industriale è definita in ambito internazionale dal sottocomitato 65C "Industrial networks" dell'International Electrotechnical Commission (IEC; www.iec.ch) nel quale vengono stabiliti sia i requisiti generali per le reti di comunicazione via cavo/fibra ottica e wireless, sia le specifiche norme delle reti per l'automazione di fabbrica e quelle per il controllo di processo.
A livello europeo l'attività è svolta dal comitato tecnico 65X del CENELEC (CLC; www.cenelec.eu) che collabora con il comitato tecnico IEC 65 in modo che la normativa internazionale sia in linea con le regole e gli interessi europei. Se alla fine dei lavori, nonostante i contributi dei membri europei in IEC, ciò non risulta possibile per alcuni specifici aspetti non accettabili per il nostro mercato, è previsto che il CLC 65X produca un documento "Common modifications" nel quale vengono elencate le modifiche della norma che si devono applicare in Europa per tali aspetti.
A livello nazionale l'attività è svolta dal sottocomitato tecnico 65C del Comitato Elettrotecnico Italiano (CEI; www.ceinorme.it), che da un lato coordina le iniziative per le normative nazionali sul tema e dall'altro lato partecipa direttamente ai lavori di CENELEC e IEC a sostegno degli interessi nazionali.
Di seguito si riportano i riferimenti delle principali serie di norme in vigore che regolano reti di comunicazione industriale internazionali, molte delle quali recepite a livello europeo e nazionale:

- CEI EN 62601 Reti industriali - Rete di comunicazione wireless e profili di comunicazione - WIA-PA
- CEI EN 62657 Reti di comunicazione industriale - Reti di comunicazione wireless
- CEI EN 61158 Reti di comunicazione industriale - Specificazioni del bus di campo
- CEI EN 62734 Reti industriali - Rete di comunicazione wireless e profili di comunicazione - ISA 100.11a
- CEI EN 61918 Reti di comunicazione industriale - Installazione di reti di comunicazione in ambienti industriali
- CEI EN 61784 Reti di comunicazione industriale - Profili
- CEI EN 62439 Reti di comunicazione industriale - Reti di comunicazione ad alta disponibilità
- CEI EN 62591 Reti di comunicazione industriale - Reti di comunicazione senza fili e profili di comunicazione - WirelessHart
- CEI EN 50325 Sottosistema di comunicazione industriale basato su ISO 11898 (CAN) per interfacce controllore-dispositivo
- IEC 62948 Industrial networks - Wireless communication network and communication profiles - WIA-FA
- IEC 62953 Industrial communication networks - Fieldbus specifications - ADS-net
- IEC TR 62685 Industrial communication networks - Profiles - Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)
- IEC 62541 OPC Unified Architecture - Part 100: Device Interface

Per ciò che riguarda più nello specifico i bus di campo più utilizzati in questo ambito, la tabella che segue ne riassume caratteristiche e riferimenti normativi:

| | | |
|---|---|---|
| Industrial Ethernet | Lo standard industriale basato sullo standard internazionale Ethernet | IEEE 802.3 |
| PROFINET | Il principale standard Industrial Ethernet per l'automazione | IEC 61158<br>IEC 61784 |
| ETHERCAT | Protocollo di comunicazione ad elevate prestazioni per connessioni Ethernet deterministiche | IEC 61158 |
| ETHERNET/IP | Standard di comunicazione industriale per Ethernet IEEE 802.3 basato su TCP/UDP/IP | IEC 61784-1 |
| POWERLINK | Protocollo di comunicazione realtime deterministico e open source per lo standard Ethernet | IEC 61508 |
| SERCOS | Standard internazionale per le comunicazioni realtime, basato sullo standard IEEE 802.3 | IEC 61491<br>IEC 61158<br>IEC 61784<br>IEC 61508 |
| Industrial Wireless LAN | Lo standard industriale per la comunicazione wireless basato sullo standard internazionale | IEEE 802.11 |

Altri bus di campo, come CanOpen e ModBus, sono diffusi ma non ancora normati.

### *Livello fisico della rete*

| | |
|---|---|
| Connessione elettrica/meccanica tra host e linea di trasmissione | IEEE RS232 (seriale, tra i più consolidati)<br>IEEE RS422<br>IEEE RS485 |
| Controllo sistemi - connessioni elettriche | UL310<br>UL486-486B<br>UL 508A |
| Cablaggio strutturato per il mercato dell'automazione | ISO/IEC 61918 |
| Cablaggi generici | ISO IEC 24702<br>EN 50173-3 |
| Test di cablaggio | CEI EN 50346 |
| Cavi | ISO/IEC 1180<br>CEI EN 50173-x<br>CEI EN 50174-x<br>CEI EN 50288-x<br>EIA/TIA 568 |

### *Sottostazioni elettriche*

Le sottostazioni elettriche che compongono l'infrastruttura di rete possono essere ottimizzate in conformità agli standard internazionali IEC 60870-5-104 Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles, IEC 61850 Communication networks and systems for power utility automation, DNP3 (Distributed Network Protocol), Fieldbus, ecc.; la loro progettazione deve tener conto delle più avverse condizioni elettromagnetiche, elettrostatiche, ambientali e climatiche secondo gli standard IEC 61850-3 Communication networks and systems for power utility automation - Part 3: General requirements e IEEE 1613 Communications networking devices in electric power substations; devono inoltre poter supportare in tempo reale i protocolli secondo la IEC 61850 Communication networks and systems in substations.

### *Safety e Security*

La soluzione per preservare la sicurezza dei dati consiste innanzitutto in una corretta valutazione dei rischi e delle possibili contromisure che rendono il danno tollerabile attivando le giuste tecniche e linee guida indicate dallo standard IEC 62443 Industrial Network and system security (ISA-99), ma anche cercando di ridurre i rischi di vulnerabilità alla fonte grazie a prodotti certificati secondo i vari standard da questi supportati. La Secure's Communications Robustness Testing (CRT) è, ad esempio, una certificazione che risponde ai criteri ISA.
Altri standard internazionali legati alla sicurezza dei dati:

- ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security
- ISO/IEC 27001 Information security management
- ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security controls
- ISO/IEC 21827 Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®)

Tra i principali standard internazionali ed europei di riferimento per le applicazioni safety:

- IEC 61784-3 Functional safety communication
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)
- IEC 62061 Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems
- EN ISO 13849-1,-2 Safety of machinery - Safety-related parts of control systems
- La figura 24 mette in evidenza le relazioni tra i diversi standard internazionali sulla sicurezza dei dati e delle macchine e i protocolli di comunicazione impiegati nei sistemi di controllo industriale.

### *Motion Control*

Il sistema di comunicazione è l'elemento fondamentale per coordinare le attività tra i controller e i drive e fornire quindi una connessione tra questi processi distribuiti.
I profili per applicazioni di Motion Control sono stati standardizzati nelle tre parti dello standard IEC 61800-7 Generic interface and use of profiles for power drive systems. Il concetto che è alla base di tale standard è essenzialmente quello di integrare le funzionalità di Motion Control all'interno delle sequenze logiche di un PLC. I processi applicativi vengono ottimizzati tramite la distribuzione dei compiti tra i drive ed il controllore. La combinazione tra le attività svolte dal controllore e dai singoli drive consente di realizzare delle applicazioni di Motion Control vero e proprio.

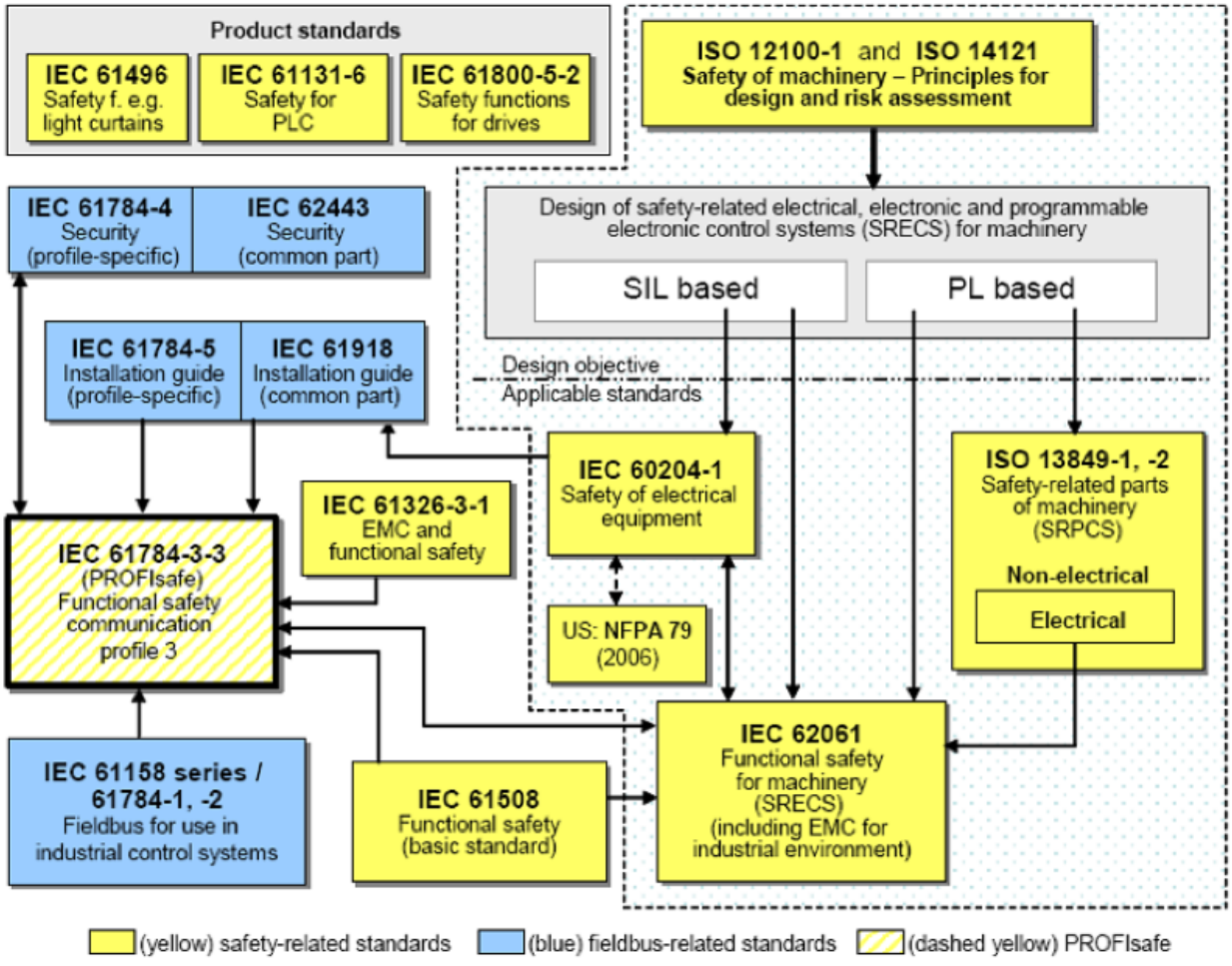



*Figura 24 - International fieldbus and safety standards for factory automation*

# 7. Glossario tecnico

Si riporta di seguito il significato dei principali termini e tecnologie cui si è fatto riferimento nei precedenti capitoli della guida, e che si configurano come elementi caratterizzanti o strettamente connessi all'infrastruttura di rete per la comunicazione industriale.

**Access Point**
Dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata o ad un router, permette all'utente mobile di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di scheda wireless. Se esso viene collegato fisicamente ad una rete cablata (oppure via radio ad un altro access point), può ricevere ed inviare un segnale radio all'utente grazie ad antenne e apparati di ricetrasmissione, permettendo così la connessione sotto forma di accesso radio. La funzionalità di Access Point è anche normalmente integrata nei più moderni router.

**Broadcast**
Nelle reti di calcolatori, il termine broadcast indica una modalità di instradamento per la quale un pacchetto dati inviato ad un indirizzo particolare (detto appunto di broadcast) verrà consegnato a tutti i computer collegati alla rete (ad esempio, tutti quelli su un segmento di rete ethernet, o tutti quelli di una sottorete IP).
Bus di campo
Reti di comunicazione basate su vari protocolli ottimizzati per il collegamento di dispositivi di automazione di processo quali Programmable Logic Controller (PLC), microcontrollori, sensori, attuatori ed altre apparecchiature coinvolte nel processo produttivo.

**DMZ**
Una DMZ (demilitarized zone) è un segmento isolato di LAN raggiungibile sia da reti interne sia esterne, ma caratterizzata dal fatto che gli host attestati sulla DMZ hanno possibilità limitate di connessione verso host specifici della rete interna.
Ethernet
Famiglia di tecnologie standardizzate per reti locali, sviluppato a livello sperimentale da Robert Metcalfe e David Boggs allo Xerox PARC, che ne definisce le specifiche tecniche a livello fisico (connettori, cavi, tipo di trasmissione, etc.) e a livello MAC del modello architetturale di rete ISO-OSI.
Con il termine Industrial Ethernet ci si riferisce in genere a quelle applicazioni che utilizzano Ethernet per le comunicazioni a livello di campo, ossia di PLC e periferia.

**Firewall**
I firewall utilizzano specifici protocolli per monitorare e limitare la richiesta di servizi, i dati in essi contenuti e la direzione del flusso di informazioni. I diritti di accesso possono essere definiti sulla base di autenticazione e identificazione. I firewall possono essere impiegati per criptare i pacchetti di dati.

**Gateway**
Dispositivo che consente la comunicazione tra reti diverse cablate (ad esempio tra Ethernet e bus di campo) o tra reti cablate e reti wireless (ad esempio tra Ethernet e Bluetooth).

**HTTPS**
L'HyperText Transfer Protocol over Secure Socket Layer è un protocollo per la comunicazione sicura attraverso una rete di computer, largamente utilizzato su Internet. HTTPS consiste nella comunicazione tramite il protocollo HTTP all'interno di una connessione criptata dal Transport Layer Security (TLS) o dal Secure Sockets Layer (SSL). Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti.

**LAN**
LAN (Local Area Network) è una rete di computer che permette di condividere applicazioni, dati, stampanti e altri servizi. Fisicamente è limitata ad un'area locale come un edifico o un gruppo di edifici.

**MAC**
Il Media Access Control è uno strato del modello architetturale standardizzato ISO-OSI, definito nello standard IEEE 802, che contiene funzionalità di controllo dell'accesso al mezzo fisico per canali broadcast, funzionalità di framing e controllo di errore. Fa parte del livello datalink, di cui rappresenta il sottolivello inferiore sovrastato dal sottolivello LLC e limitato inferiormente dal livello fisico.

**Modem**
Dispositivo di ricetrasmissione che ha funzionalità logiche di modulazione/demodulazione (analogica o numerica) in trasmissioni analogiche e digitali. Nell'accezione più comune il modem è un dispositivo elettronico che rende possibile la comunicazione remota tra sistemi di automazione (ad esempio PC o PLC). Questo dispositivo permette la MOdulazione e la DEModulazione dei segnali contenenti informazione; dal nome di queste due funzioni principali il dispositivo prende appunto il nome di MODEM. In altre parole, sequenze di bit vengono ricodificate come segnali elettrici. I modem GSM/GPRS/EDGE/UMTS/HSDPA sono i modem presenti nei telefoni cellulari di terza generazione. Consentono di accedere ad internet a velocità variabili tramite i servizi di connessione offerti dagli operatori telefonici di telefonia cellulare.

**NAT**
Nel campo delle reti telematiche, il network address translation o NAT è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router all'interno di una comunicazione tra due o più host. Sono molto note anche alcune tipologie specifiche di NAT, come l'IP masquerading e il port forwarding.

**Rete di comunicazione**
Una rete di comunicazione è un sistema hardware e software che consente a più dispositivi di comunicare fra di loro entro un tempo accettabile condividendo risorse comuni.

**Ridondanza**
Nell'ingegneria dell'affidabilità, la ridondanza è definita come l'esistenza di più mezzi per svolgere una determinata funzione, disposti in modo tale che un guasto del sistema possa verificarsi solo in conseguenza del guasto contemporaneo di tutti questi mezzi.

**Router**
Dispositivo di rete che, in una rete informatica a commutazione di pacchetto, si occupa di instradare i dati, suddivisi in pacchetti, fra sottoreti diverse. È quindi, a livello logico, un nodo interno di rete deputato alla commutazione di livello 3 del modello OSI o del livello Internet nel modello TCP/IP.

**SNMP**
Il Simple Network Management Protocol è un protocollo di rete che appartiene alla suite di protocolli Internet definito dalla IETF (Internet Engineering Task Force). Opera al livello 7 del modello OSI e consente la configurazione, la gestione e la supervisione (monitoring) di apparati collegati in una rete (siano essi nodi interni di commutazione come i dispositivi di rete e nodi terminali di utenza), riguardo a tutti quegli aspetti che richiedono azioni di tipo amministrativo.

**Switch**
Dispositivo di rete che agisce sull'indirizzamento e sull'instradamento all'interno delle reti LAN mediante indirizzo fisico (MAC), selezionando i frame ricevuti e dirigendoli verso il dispositivo corretto (leggendo il MAC di destinazione). L'instradamento avviene per mezzo di una corrispondenza univoca porta-indirizzo.

**TCP/IP**
Una suite di protocolli Internet indica un insieme di protocolli di rete su cui si basa il funzionamento logico della rete Internet. A volte si parla anche di suite di protocolli TCP/IP, in funzione dei due più importanti protocolli in essa definiti: il Transmission Control Protocol (TCP) e l'Internet Protocol (IP). Il rispettivo modello di architettura di rete a strati rappresenta lo standard de facto nell'ambito delle reti dati in contrapposizione allo standard de iure rappresentato invece dal modello ISO-OSI.

**Topologia di rete**
Modello geometrico (grafico) finalizzato a rappresentare le relazioni di connettività, fisica o logica, tra gli elementi costituenti la rete stessa (detti anche nodi). Il concetto di topologia si applica a qualsiasi tipo di rete di

telecomunicazioni: telefonica, rete di computer, Internet, ecc.

**WAN**
WAN (Wide Area Network) è una rete utilizzata per scambiare dati su ampie aree come ad esempio città o distretti industriali.

**WLAN**
WLAN (Wireless Local Area Network) è una rete che opera senza cavi in accordo con le norme IEEE.

**VLAN**
Il termine VLAN (Virtual LAN) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale (tipicamente IEEE 802.3) basata su switch, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.

**VPN**
Una Virtual Private Network è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano come tecnologia di trasporto un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

**VRRP**
Il Virtual Router Redundancy Protocol è un protocollo per le reti di calcolatori che fornisce (agli host presenti sulla rete) l'assegnamento automatico dei router IP disponibili, incrementando la disponibilità e l'affidabilità delle rotte tramite una selezione automatica del default gateway per le sottoreti destinazione. Può essere usato su reti Ethernet, MPLS e token ring sia IPv4 che IPv6.

# 8. Case History

## 8.1 Collegamento in rete dei parcheggi presso un aeroporto europeo

### *Comunicazione universale via Ethernet*

Per collegare le colonnine di erogazione ticket e le casse automatiche dei numerosi parcheggi coperti e scoperti di un aeroporto sono stati utilizzati degli switch managed.
L'aeroporto dispone di sette parcheggi coperti e tre scoperti, garantendo in tal modo ai passeggeri un luogo sicuro in cui lasciare l'auto mentre sono in viaggio.
L'intera area di parcheggio comprende 14.000 posti auto gestiti da 57 distributori automatici di biglietti con funzione di cassa e 35 barriere di controllo.

Per un regolare svolgimento dell'operazione di parcheggio è previsto un sistema di informazione/guida e un sistema di gestione dei parcheggi.
Il sistema di guida ai parcheggi informa il passeggero in arrivo sui posti ancora disponibili, al coperto o all'esterno.
Il sistema di gestione parcheggi controlla gli ingressi e le uscite ed effettua tutte le procedure di pagamento.
Un'unica società operativa, la cui sede si trova presso l'aeroporto, gestisce entrambi i sistemi.

### *Perdite finanziarie a causa della mancanza di affidabilità*

La società di gestione dei parcheggi garantisce anche alla società di gestione dell'aeroporto e ai loro provider di servizi l'assistenza necessaria per tutte le esigenze IT e di telecomunicazione.
Nel suo ruolo di gestore, tale società è consapevole dell'importanza di avere un sistema di informazione/guida e gestione dei parcheggi che funzioni con la massima affidabilità, poiché ogni guasto del sistema può portare a una perdita finanziaria.

### *Il collegamento in rete basato su IP consente futuri ampliamenti*

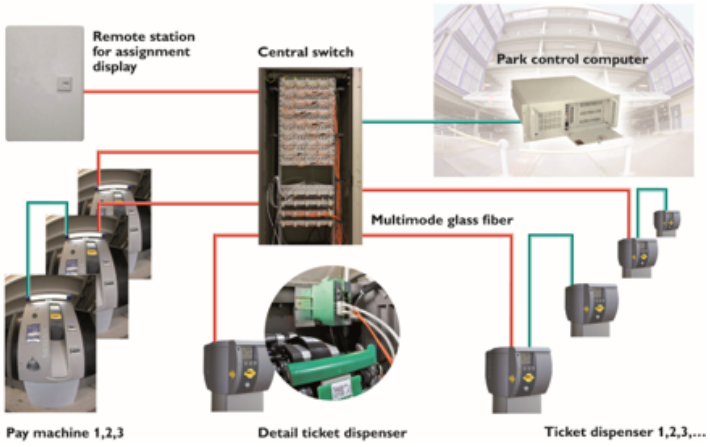
Partendo da questo presupposto, l'elevata affidabilità della soluzione di comunicazione costituiva un criterio fondamentale per il collegamento in rete del sistema di gestione dei parcheggi.
La dorsale di comunicazione di questo nuovo progetto è una rete Ethernet.
Con la costruzione di una nuova struttura, tutti i parcheggi esistenti e i parcometri venivano collegati in una nuova rete. Fino ad allora lo scambio dei dati avveniva su cavi telefonici e il sistema locale in uso era limitato alle funzioni di base.
Ora i parcheggi, incluse tutte le macchine automatiche installate, gli ingressi e le uscite, potevano essere collegati nella rete Ethernet dell'aeroporto.
Grazie alla trasmissione basata su IP è possibile realizzare una comunicazione che si presta, in modo semplice e flessibile, a future estensioni della funzionalità del sistema, grazie all'impiego di standard aperti.
Tali estensioni possono includere, ad esempio, il controllo e la manutenzione a distanza mediante accesso VPN (Virtual Private Network) o la trasmissione remota di eventi, ad esempio la trasmissione di informazioni a dispositivi mobili.

### *Switch industriali compatti e robusti*

Per la realizzazione del progetto, tutte le colonnine di erogazione ticket, le barriere di controllo e le casse automatiche dovevano essere collegate alla rete.
Poiché alcuni dei parcheggi sono molto distanti tra di loro, sono stati usati cavi in fibra di vetro Multimodale.
Tuttavia, le unità di controllo, integrate nelle colonnine di erogazione ticket e nelle casse automatiche, disponevano solo di un'interfaccia in rame.
Sul posto erano quindi necessari componenti infrastrutturali decentrati per il collegamento delle fibre di vetro, in grado di sopportare le variazioni di temperatura in estate e in inverno, poiché le colonnine sono in parte ubicate all'aperto.
La società di gestione iniziò quindi a cercare uno switch industriale compatto e robusto con collegamento in fibra ottica.
"A quel punto era chiaro che avremmo dovuto prendere in considerazione i componenti di rete di automazione per l'industria, ovvero componenti per ambienti industriali critici. Ed è precisamente questo tipo di condizioni che i nostri sistemi di gestione dei parcheggi devono affrontare".

### *La gestione integrata permette una configurazione uniforme e funzioni di diagnostica*

Gli switch industriali usati per collegare le singole unità del sistema di gestione dei parcheggi alla rete Ethernet operano in un ampio range di temperatura, da -40°C a +70°C e costituiscono quindi la soluzione ideale per le condizioni climatiche dei parcheggi.
La loro esecuzione compatta, e il montaggio su guide di supporto, hanno semplificato l'installazione degli switch nei componenti dei parcheggi garantendo inoltre la flessibilità necessaria per integrare le unità di controllo basate su IP, presenti agli ingressi, alle uscite e nelle casse per il pagamento, nella rete dell'aeroporto.




Complessivamente sono stati connessi 30 switch managed a una dorsale in fibra di vetro multimodale con un collegamento a stella.

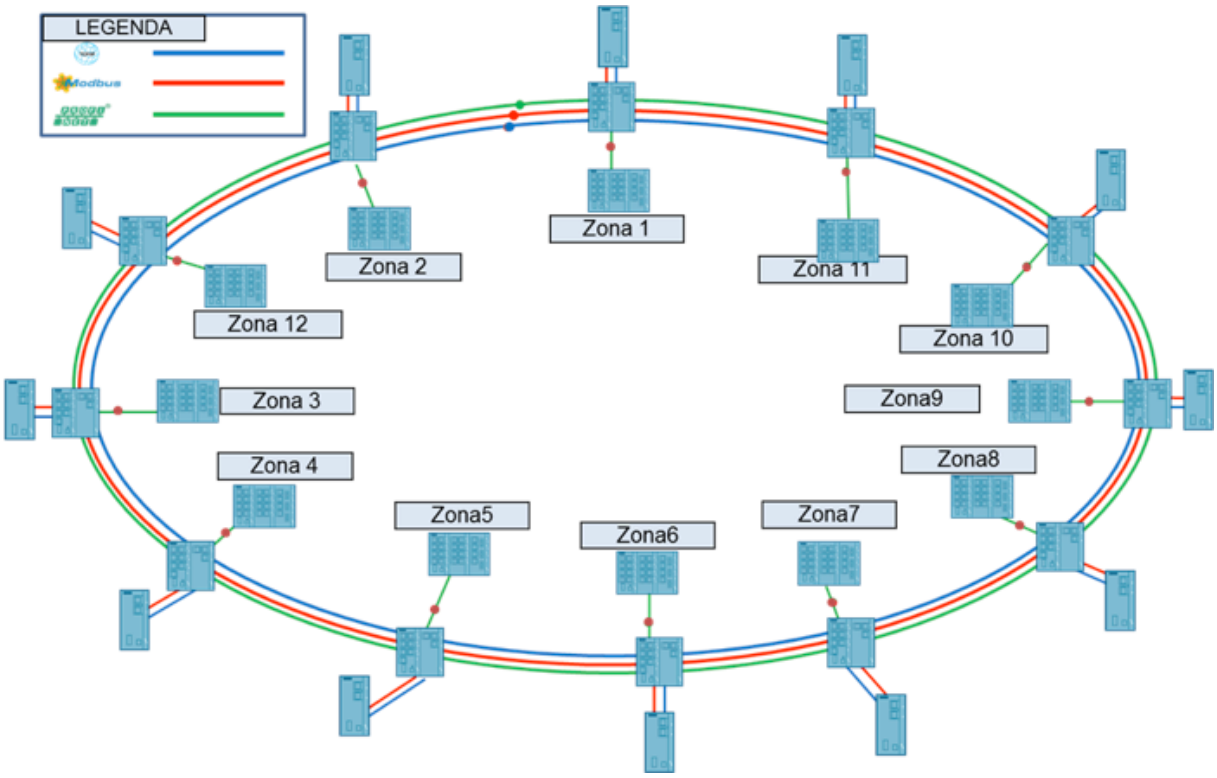
Dal momento che gli ingressi e le uscite dei parcheggi hanno due corsie, è stato possibile collegare anche le colonnine di erogazione ticket con cavi in rame, in modo facile ed economico.
Anche i "calcolatori di livello", che determinano la disponibilità di spazio su ogni piano del parcheggio, sono collegati alla rete mediante switch managed e fibra in vetro.
Tutti i componenti infrastrutturali dispongono di un sistema di gestione, al quale l'operatore può accedere via web o attraverso lo standard di gestione di rete SNMP (Simple Network Management Protocol).
Gli switch decentrati consentono non solo di ampliare la rete centrale nelle aree esterne in termini di connessione fisica, ma forniscono anche possibilità di configurazione e diagnostica uniformi e universali.

### *Funzionamento più stabile e affidabile*

"Gli switch sono facili da installare e la rete si è dimostrata stabile e affidabile", ha dichiarato il responsabile della società di gestione. "Grazie a questi switch, compatti e potenti, tutti i componenti della gestione dei parcheggi sono ora collegabili in rete".

### 8.2 Integrazione IT/OT per una rete di produzione ad alta disponibilità

Il cliente di questo scenario dispone di un grande numero di celle di automazione, trattandosi di una catena di produzione realizzata con macchine di diversi integratori. In tale scenario la disponibilità della rete è di massima importanza in quanto un fermo della produzione ricadrebbe su tutta la catena e non sarebbe tollerabile. Per questo motivo una topologia ridondata ad anello è stata scelta per garantire l'accesso a tutte le celle di produzione anche in caso di guasto di un componente di rete.




Il traffico di automazione è gestito tramite l'utilizzo del protocollo Profinet che permette la gestione deterministica e in tempo reale di tutte le periferiche di rete ed i loro controllori. Al contempo è necessario garantire anche comunicazioni di tipo TCP/IP e Modbus per gestire il controllo di ulteriori elementi di rete presenti all'interno della struttura verso i sistemi di supervisione che afferiscono alla rete Office IT. Questo significa che gli switch dell'anello non solo garantiscono la ridondanza della struttura di rete stessa ma anche la segmentazione attraverso tre diversi livelli di comunicazione. Gli switch dell'anello sono quindi tutti di tipo gestito e ne garantiscono la ridondanza in tempi ridottissimi tramite protocollo Media Redundancy Protocol (MRP) mentre la segmentazione della rete è gestita mediante l'uso del protocollo IEEE 802.1q VLAN che separa i diversi flussi in modo che non possano interferirisi fra di loro e massimizzando quindi le risorse dell'infrastruttura.

Il traffico Profinet viene poi trasportato mediante un ulteriore switch managed, con numerose porte, verso le celle di automazione ("zone" nella figura"), mentre invece gli altri livelli di comunicazione afferiscono mediante un interfaccia Gigabit attraverso dispositivi Firewall ad hoc. Tutti gli accessi alla rete IT del cliente sono quindi ridondati lungo l'anello e l'accesso alla rete di produzione è altamente protetto in maniera integrale grazie al controllo del traffico e degli accessi esercitato dal firewall.
In questo modo è stato possibile costruire una sicura potente ed affidabile interfaccia fra la rete di produzione OT e la rete office IT realizzando quindi il concetto di "Backbone Aggregation".

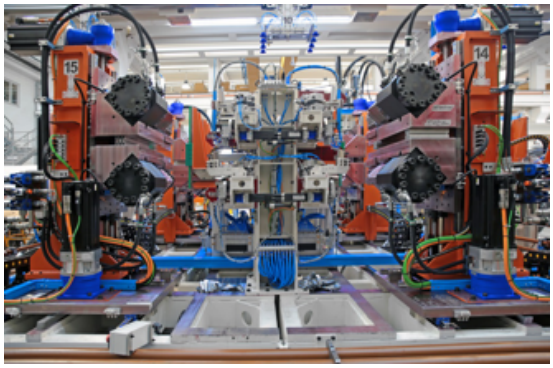
## 8.3 Ethernet nell'industria del bianco

EtherNet/IP connette completamente l'impianto per la produzione di chassis per lavatrici realizzato da un costruttore italiano di macchine per la lavorazione a freddo della lamiera destinate al settore degli elettrodomestici.

### *Background*

L'industria del bianco in Europa ha avuto tra i suoi protagonisti molti marchi italiani. Oggi, tuttavia, diversi tra quei nomi storici sono stati acquisiti da grandi aziende internazionali del settore e nelle case degli italiani sono pochi gli elettrodomestici di produzione nazionale.
Eppure, nella realizzazione degli apparecchi oggi proposti dalle multinazionali, il rinomato Made in Italy è ancora presente, come dimostra la storia di questo OEM specializzato nella realizzazione di macchine automatiche per la lavorazione a freddo della lamiera, destinate proprio alla produzione di elettrodomestici per uso casalingo e commerciale: frigoriferi, congelatori, lavatrici, lavastoviglie ecc.

### *La sfida*



I requisiti particolari di questo progetto erano quelli di una linea per la produzione di chassis esterni di lavatrici destinata al mercato centro-americano. Le specifiche della linea con un tempo ciclo di 15 secondi hanno portato ad adottare un'architettura di automazione avanzata e performante, in grado di gestire fino a 64 assi.
Nella linea - un impianto di circa 70 m di lunghezza - è caricato automaticamente un foglio di lamiera, già tranciato e pre-verniciato (in bianco, rosso, grigio o nero), sul quale la macchina esegue i tagli e le piegature necessarie, sul lato lungo e su quello corto. Dopo avere eseguito, in ultimo, la piegatura a U, il pezzo passa, tramite un manipolatore a ventose, alle stazioni successive, dove è eseguito, tramite un sistema di clinciatura e bottonatura, il montaggio automatico del pannello posteriore. Dalla linea esce quindi lo chassis finito. L'impianto è stato concepito per realizzare 240 lavatrici all'ora e produrre così, su un turno giornaliero, circa 1.800 pezzi.

### *La soluzione*

Il sistema di automazione implementato sulla linea include servo-motori, servo-azionamenti, azionamenti CA, I/O, controllori, ethernet switch, interfacce operatore e un PC industriale.
Denominatore comune per la comunicazione tra i dispositivi è il protocollo EtherNet/IP per facilitare lo scambio delle informazioni con il sistema IT del cliente.

### *I risultati*

La modularità e versatilità della soluzione è un elemento fondamentale per il cliente, che vede così protetto il suo investimento e può intervenire sull'impianto adattandolo a eventuali esigenze future, senza dover stravolgere o riprogettare l'intero sistema.
Tutte le macchine sono collegate con il sistema IT e la comunicazione diretta tra uffici direzionali e produzione agevola qualsiasi modifica si renda necessaria alla lavorazione. Ad esempio, dal sistema gestionale è possibile implementare in linea l'etichettatura richiesta per il modello in produzione.
Il collegamento della macchina in rete è funzionale anche al servizio di teleassistenza, che consente di intervenire da remoto 24h su 24, 7 gg su 7.

# 9. Le aziende del WG Networking industriale

ADVANTECH

HARTING
Pushing Performance

OMRON

PHOENIX CONTACT

Rockwell Automation

Schneider Electric

sbc
SAIA BURGESS CONTROLS

SIEMENS

telestar

Weidmüller


Federazione ANIE
**ANIE Automazione**
Viale Lancetti, 43 - 20158 Milano - Tel. 02 3264.252 - Fax 02 3264.327
anieautomazione@anie.it - www.anieautomazione.it - www.anie.it
www.forumtelecontrollo.it - www.forumeccatronica.it - @ANIEAutomazione