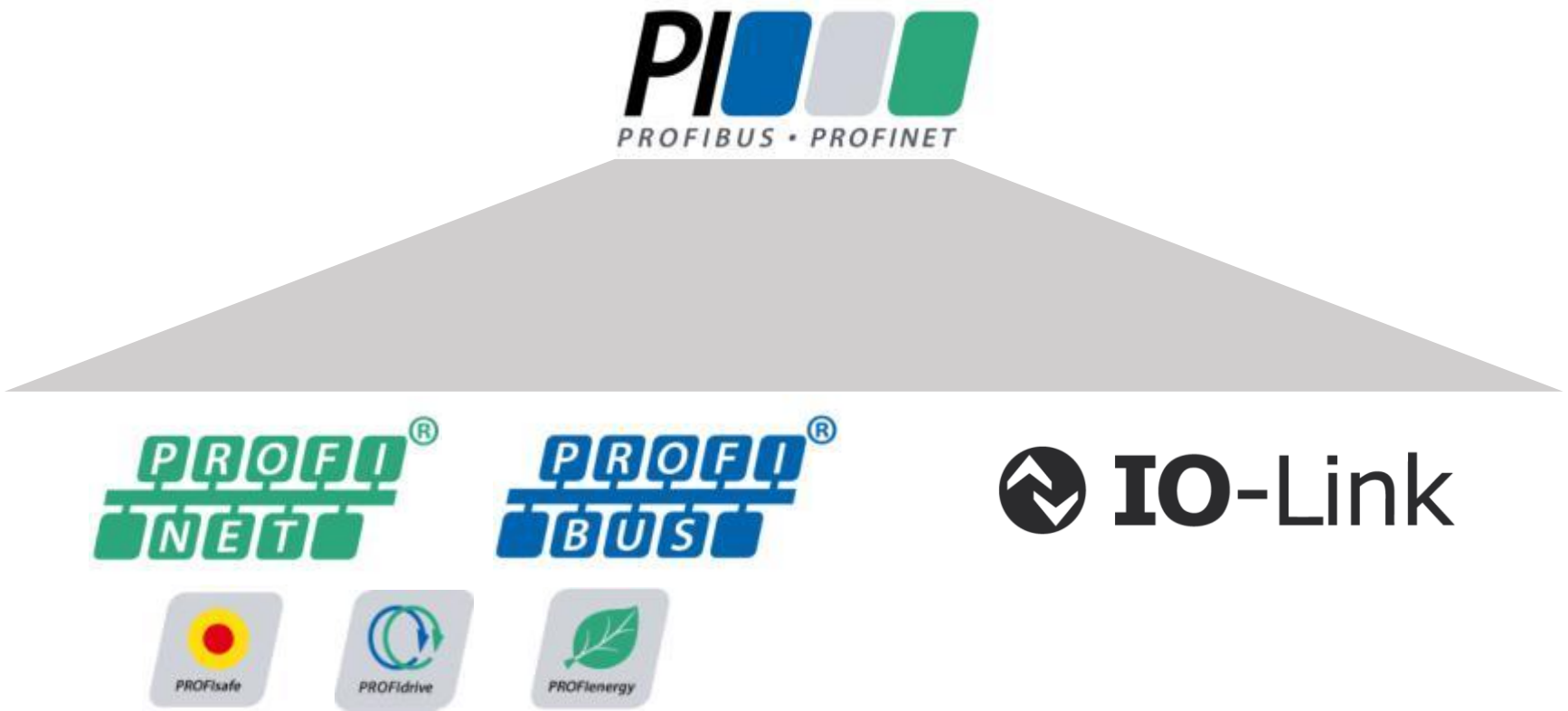
Conciliare performance e security nelle reti industriali PROFINET

Paolo Ferrari
Università di Brescia - Tel: +39-030-3715445
CSMT Gestione Scarl
Centro di Competenza PROFIBUS e PROFINET – Brescia
e-mail: profilab@csmt.it

Chi siamo



PI International: una presenza mondiale

Canada
PICC, PITC

USA
RPA, PICC, PITC, PITL

Brasile
RPA, PICC, PITC

Bolivia
PICC, PITC

Cile
RPA, PICC, PITC

Argentina
PICC, PITC

Paesi Bassi
RPA, PICC, PITC, PITL

Belgio
PICC, PITC

Francia
RPA, PICC, PITC

Germania
RPA, PICC, PITC, PITL

Svizzera
PICC, PITC

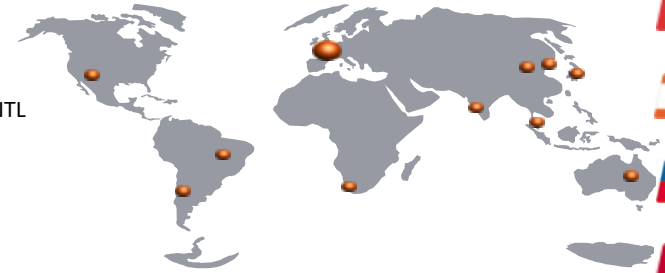
Italia
RPA, PICC, PITC

Spagna
RPA, PICC, PITC

UK
RPA, PICC, PITC

Irlanda
RPA, PICC, PITC

Polonia
RPA, PICC, PITC



Norvegia
RPA, PICC, PITC

Svezia
RPA, PICC

Rep. Ceca
RPA, PICC, PITC, PITL

Finlandia
RPA

Danimarca
RPA

Turchia
PICC

Libano
PICC

Taiwan
RPA

Medio Oriente / EAU
RPA, PICC

Arabia Saudita
PICC, PITC

Sudafrica
RPA, PICC, PITC

India
RPA, PICC

Cina
RPA, PICC, PITL

Asia sudorientale
RPA

Corea
RPA, PICC

Giappone
RPA, PICC, PITL

Australia/ Nuova Zelanda
RPA, PICC, PITC

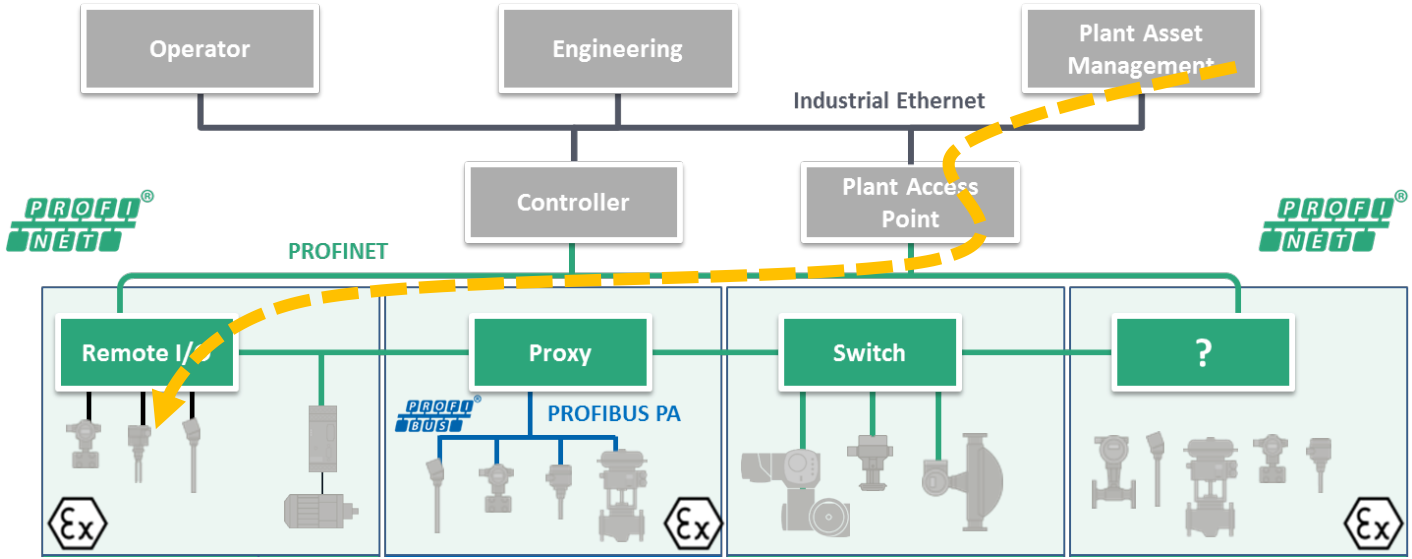
PI nel mondo:	Supporto tecnico PI:
25 Associazioni PI regionali (RPA)	56 Centri di Competenza PI (PICC) 32 Centri di Formazione PI (PITL) 9 Test Lab PI (PITL)

Consorzio PI in Italia

73 aziende consorziate e 3 Centri di Competenza

Reti PROFINET nell'era Industry 4.0

- PROFINET permette un approccio completo
  - Performance adatte ad ogni applicazione, dal processo fino al motion control
  - Pronto per gli accessi Industrial Internet of Things propri di Industry 4.0.



Safety vs. Security

Security: protezione delle macchine dagli uomini

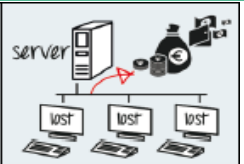
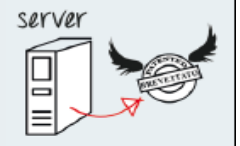
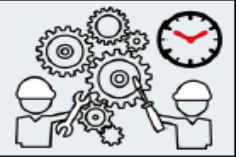
Security

Definizione inclusa nella specifica tecnica IEC/TS 62443-1-1:2009 ”Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, concepts and models”:

”Prevenzione di accessi illegali o non voluti o di interferenze nello specifico e previsto funzionamento di un sistema di comando e controllo per l’automazione industriale”

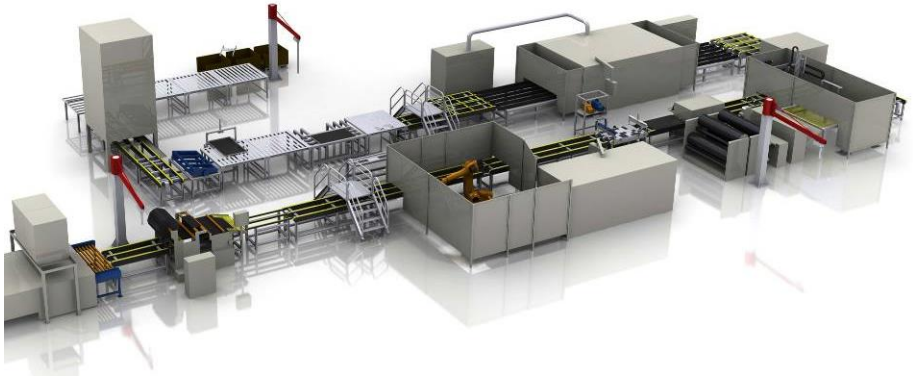
Non è possibile ignorare la Security

Quando si opera in ambiente industriale, le possibili conseguenze di una non adeguata protezione di una rete possono essere molto costose… o peggio…

Perdita dei dati: Improvvisamente tutti i tuoi dati vengono persi. Quale potrebbe essere il costo della ricostruzione di questi dati?	
Perdita di know-how: Un competitor riesce ad accedere ai tuoi dati sensibili (progettazione, ingegnerizzazione, …). Quanto può valere economicamente il danno?	
Fermi di produzione: A causa di problemi legati alla security, la produzione deve arrestarsi per alcune ore. Quale può essere il costo del fermo impianto?	
Ore lavoro dei lavoratori: Quante ore lavoro sarebbe necessario impiegare per risolvere i danni generati da una falla nelle tue misure di security?	
Reputazione: Quanto potrebbe essere importante un danno alla tua reputazione se i clienti non riponessero in te la giusta fiducia circa la protezione da Cyber attacchi?	

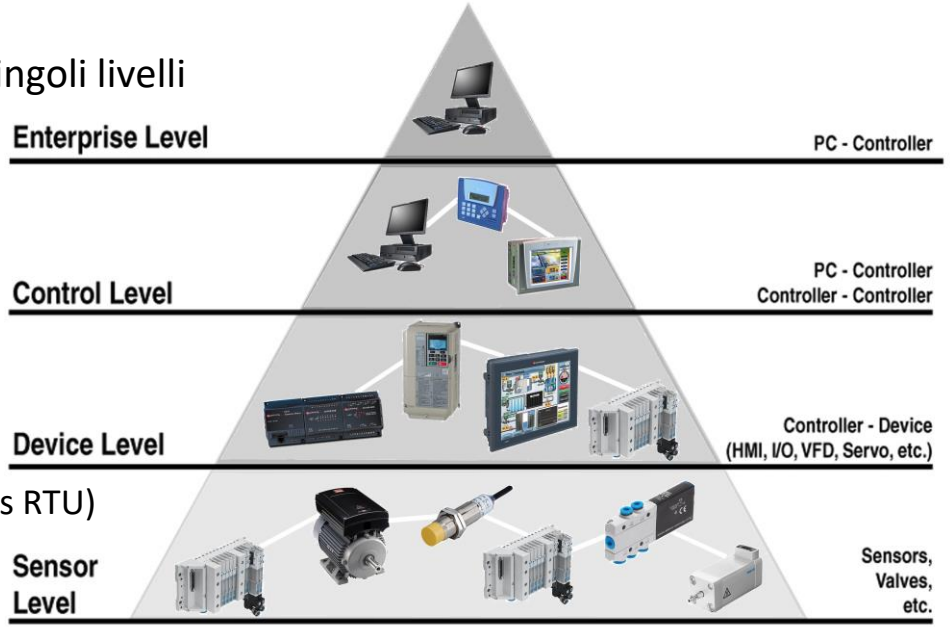
Perchè invece la ignoravamo?

- Perché fino a ieri la security non era prioritaria?
  - Con fieldbus su base seriale (Modbus RTU, PROFIBUS, Devicenet, CAN) le macchine non sono interconnesse direttamente tra loro
  - I progettisti di automazione come security intendevano evitare accessi al progetto installato sul sistema di controllo



Le reti industriali tradizionali

- Concepite con modello a piramide (ISA95)
  - Organizzate secondo livelli gerarchici
  - Dialogo verticale solo tra controllori dei singoli livelli
    - Ethernet
    - Ethernet
    - Bus di campo seriali(PROFIBUS, CAN, Modbus RTU)
    - Bus di campo seriali (CAN, ASI, RS232)



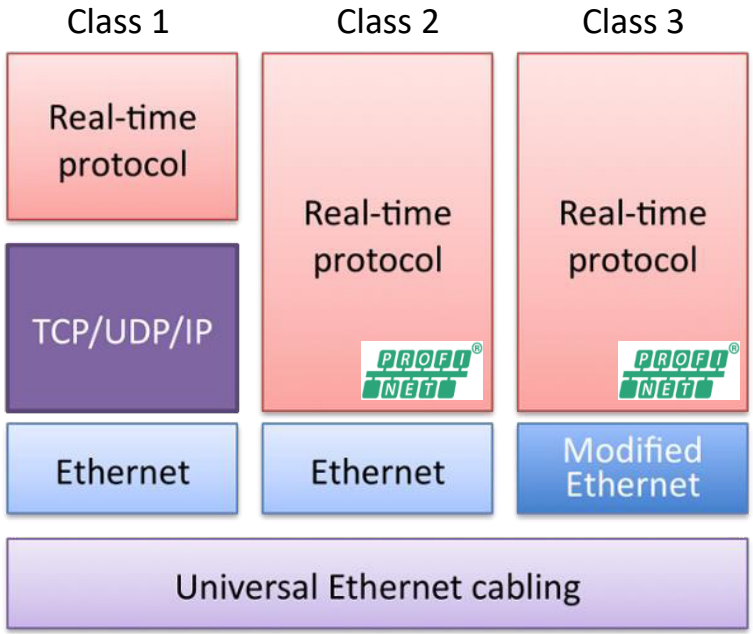
Real-Time Ethernet

- Dal 2000 nascono le Real-time Ethernet
  - a basso livello si può usare Ethernet
  - piccole aggiunte a Ethernet standard per garantire determinismo (jitter < 1us)
  - 3 classi di implementazione

1. Real-time sopra lo stack IP
2. Real time sopra Ethernet
3. Real time sopra Ethernet+modifiche HW

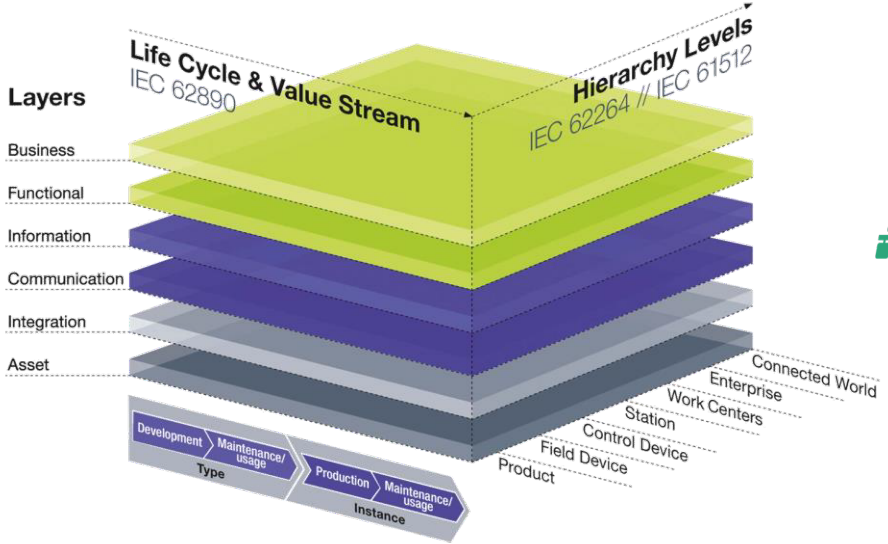
  - Prestazioni: Class 3 > Class 1

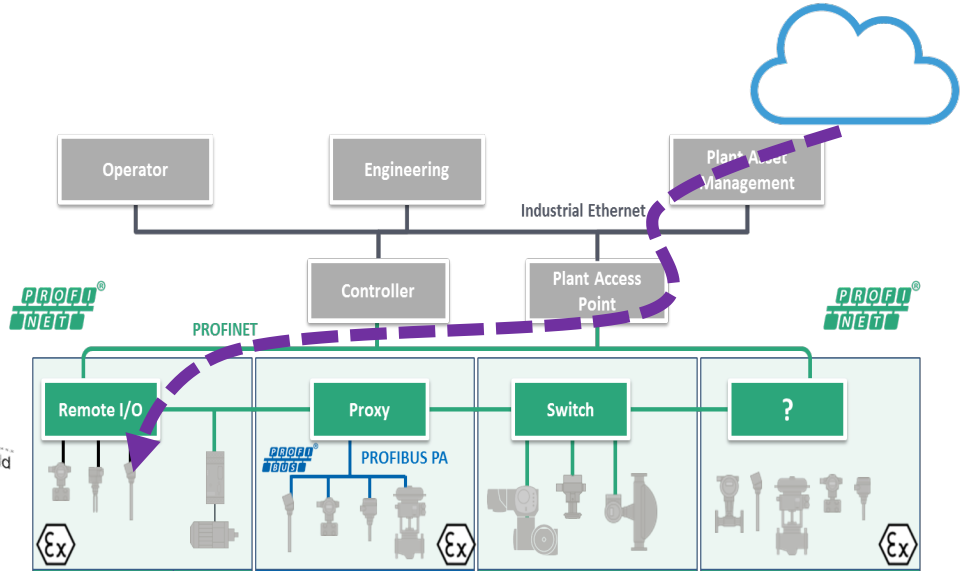
  - Class 2 e Class 3 spediscono i dati di processo direttamente nei pacchetti ethernet



Nuovi accessi per Industry 4.0

- Il modello di Industry 4.0 è a «cubo» (RAMI 4.0) (3ª dimensione = ciclo di vita)
  - La gerarchia è meno evidente
  - Accesi verticali verso ogni dispositivo





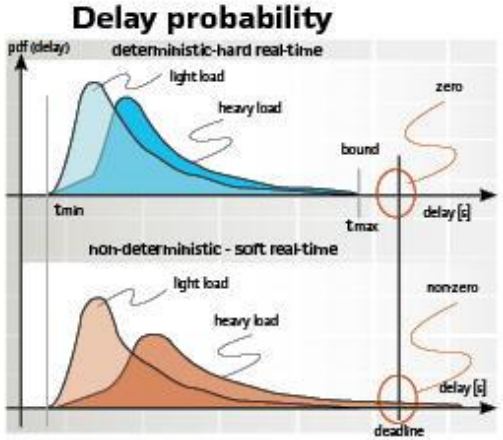
Security per le reti industriali

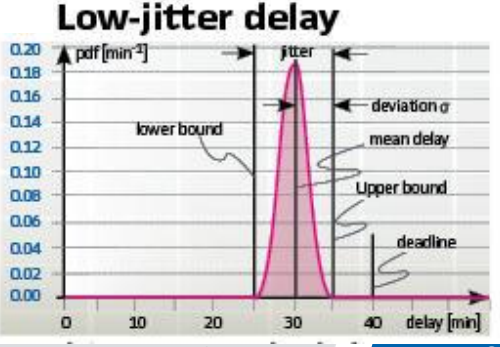
- I concetti di sicurezza per gli ambienti office non possono essere **«semplicemente»** trasferiti alle reti di automazione.
  - Le misure di sicurezza implementate per i sistemi di automazione **non devono essere in conflitto** con i requisiti operativi relativi ai protocolli real-time.
  - L'obiettivo delle misure di sicurezza nell'area di automazione è una rete di automazione **affidabile** che soddisfa i requisiti.
  - sistemi di automazione: prestazioni massime **e non** per massima sicurezza.
- Un sistema sicuro garantisce la riservatezza, l'integrità e la disponibilità di sistemi e dati, anche in presenza di attacchi dannosi.
- Per ottenere il massimo livello di sicurezza **ragionevole** per i sistemi e le reti di automazione, è essenziale un processo di gestione della sicurezza.
  - **Analisi dei rischi** (misure per la riduzione del rischio a un livello ragionevole)
  - Misure organizzative / tecniche (ingegneria dei sistemi) **coordinate**
  - **Ripetizione** periodica / su evento

Security per IT e per reti industriali

- Nei sistemi IT i ritardi e il jitter nella trasmissione dei dati sono tollerabili.

- Nei sistema di automazione, ritardi e jitter definiscono le prestazioni real-time.
  - Contesto generale: i sistemi di automazione si basano su una grande varietà di dispositivi anche **con risorse limitate**
  - Interazione uomo-macchina: controllo affidabile e funzionamento dei processi tecnici devono essere possibili in **tutte** le situazioni (anche in critiche): le misure di sicurezza **non devono interferire** con l'operatività dei sistemi di automazione.





Security per IT e vulnerabilità delle reti industriali

- Obiettivi di sicurezza: Un obiettivo centrale nell'area IT aziendale è la protezione dei dati da perdite o modifiche (ad esempio "proteggere i server").
- Al contrario, le linee di produzione hanno strutture e applicazioni granulari che sono suddivise in molte sotto-componenti.

➢Sistemi Business IT

(1) Confidentiality

(2) Integrity

(3) Availability

➢ Sistemi automazione

(1) Availability

(2) Integrity

(3) Confidentiality

- Le reti industriali **non** hanno, ad oggi, sistemi di autenticazione adeguati.

Principali vincoli della Security per le reti industriali

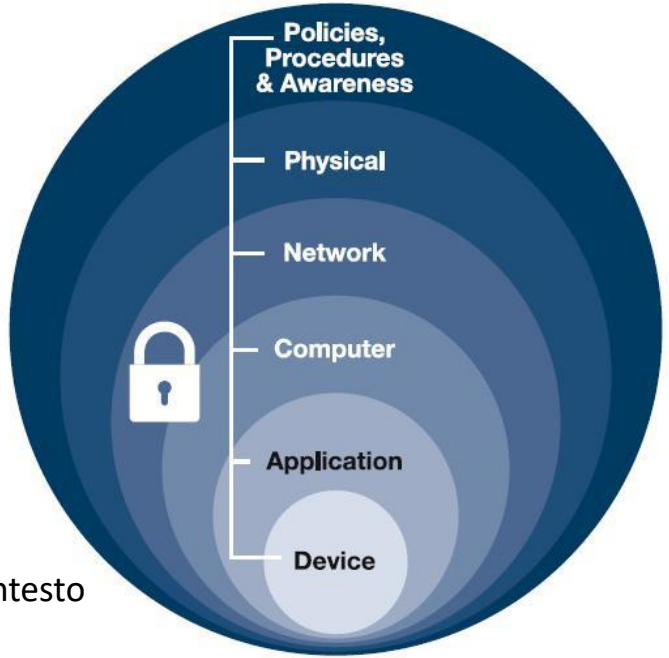
- **Sicurezza per sistemi senza funzioni di sicurezza**.
  - fornire una sicurezza adeguata anche per i sistemi di automazione che non dispongono delle risorse tecniche necessarie (ad esempio per ragioni economiche).
- **Funzionamento in tempo reale**.
  - non deve interferire con i requisiti in tempo reale, riducendo il tempo critico di reazione associato all'interazione tra l'uomo e la macchina. (Ad esempio interruttore di arresto di emergenza usando una password!)
- **Integrazione trasparente ed economicamente vantaggiosa.**
  - supportare l'integrazione trasparente ed economica della sicurezza in un ambiente industriale per diverse tipologie di applicazioni.
- **Robustezza.**
  - Mantiene il normale funzionamento, anche in condizioni sfavorevoli e / o in caso di input imprevisto. (attacchi Denial of Service - DoS)

Requisiti speciali della Security per le reti industriali

- Disponibilità e affidabilità: molti processi di produzione devono essere eseguiti in modo continuo.
  - Le misure IT come i riavvii del sistema potrebbero non essere applicabili.
  - Le prove Beta durante il funzionamento sono praticamente inutilizzabili
  - Gli aggiornamenti non possono sempre essere implementati tempestivamente: cambiamenti software richiedono in anticipo test dettagliati **su sistemi reali** ($$$).
- Architettura di sicurezza: sistema di automazione nel suo complesso:
  - funzionamento affidabile/continuo come unità (ininterrotto, no errori in tutti i device).
  - per ragioni di costo, la ridondanza viene utilizzata principalmente quando un guasto di un dispositivo causerebbe gravi danni all'impianto o al prodotto
- Rischi e requisiti di sicurezza: la **sicurezza funzionale** e il **rischio** di impianti produttivi differiscono dai rischi normalmente considerati nel mondo IT.
- Aggiornamento del firmware / gestione delle patch: gli aggiornamenti del firmware nel mondo dell'automazione richiedono una pianificazione speciale

Approccio efficace: "defence in depth"

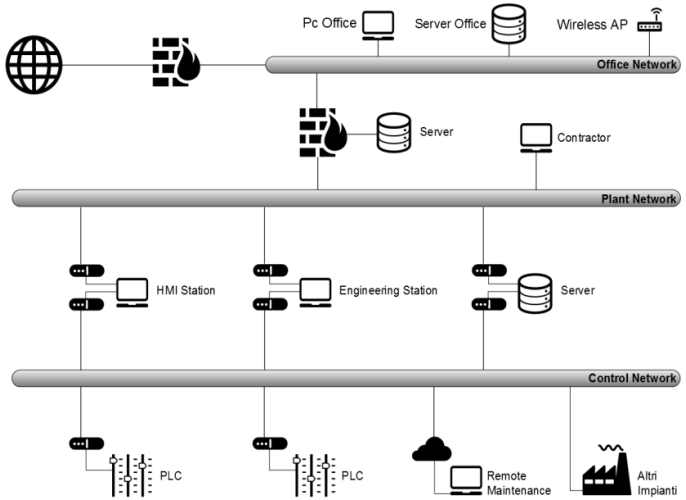
- Questo modo di salvaguardia impedisce una serie di attacchi a vari livelli e pone quindi una sfida maggiore per un potenziale aggressore.
  - Ogni livello individuale in sé rappresenta un ostacolo di sicurezza relativamente facile da superare.
  - Tuttavia, quando combinato con gli altri livelli, il risultato è molto difficile da superare.
- Con l'approccio di difesa in profondità:
  - Sono presenti diversi livelli di difesa
  - Ogni livello implementa un meccanismo di sicurezza diverso
  - Ogni livello viene implementato in modo dipendente dal contesto



Applicazione della teoria alla pratica

Misure e soluzioni tecnologiche per garantire un adeguato livello di Security di una rete andranno quindi scelte in funzione delle esigenze specifiche

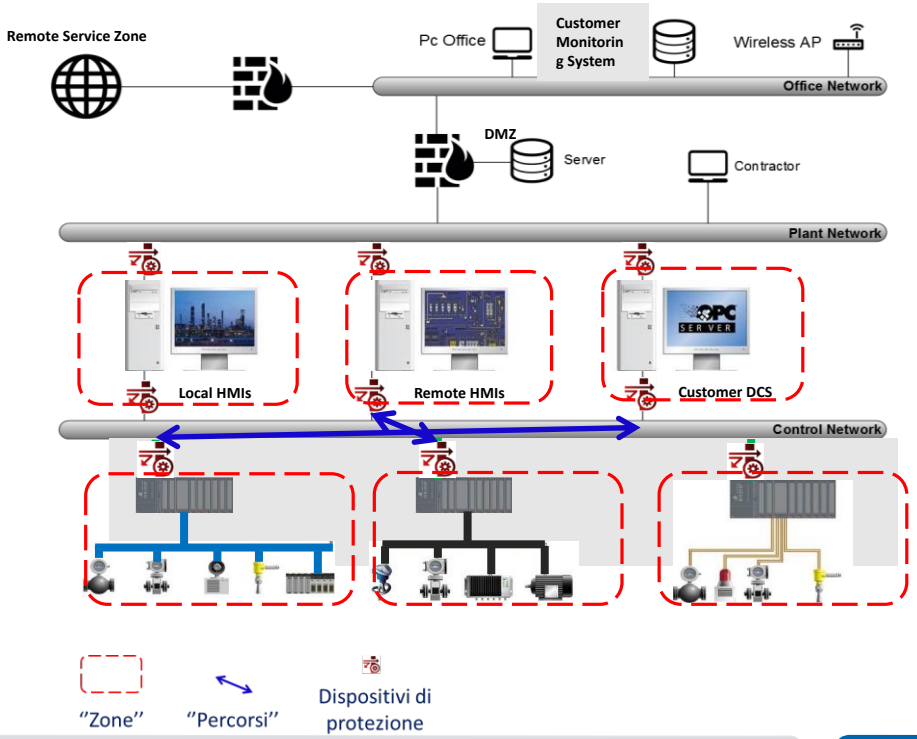
- Tra tali misure possiamo elencare
  - un'opportuna segmentazione di rete con adeguata protezione (routing/firewall) dei punti di segmentazione,
  - una corretta gestione delle prerogative di accesso locale alla rete
  - un'efficace protezione degli accessi da remoto (VPN, firewall, security cloud)



Nota: l'utilizzo di strumenti di monitoraggio continuo di rete permetterà anche la rilevazione immediata di tentativi di intrusioni non autorizzate

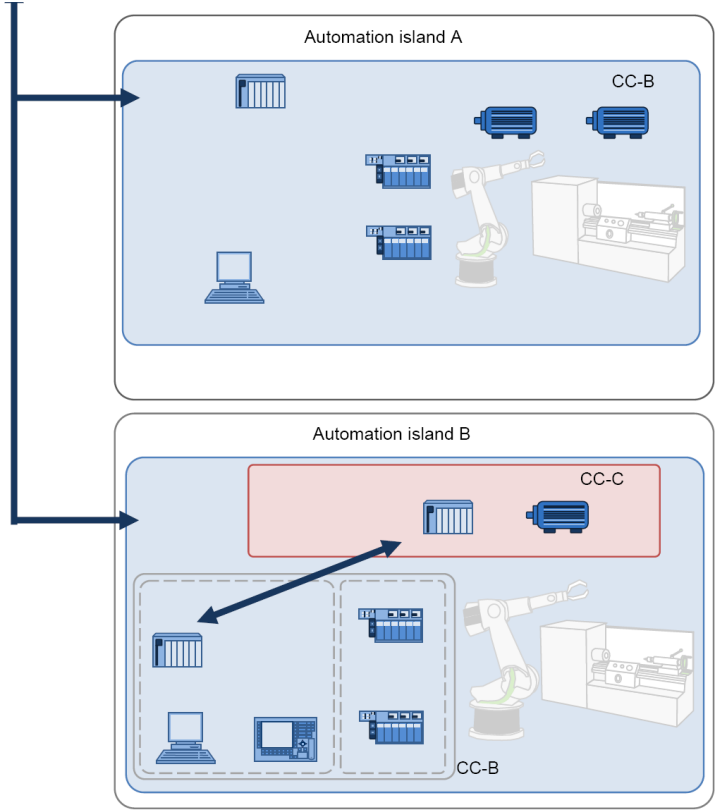
Applicazione alla pratica: le zone

- Dividere in "zone"!
  - Per il concetto di segmentazione della rete può essere utile fare riferimento alla serie di norme IEC 62433, all'interno della quale vengono esplicitati i concetti di ''zone'' (anche dette ''celle'' o ''isole'') e ''percorsi''
  - Una ''zona'' è definita come un insieme di dispositivi appartenenti a una rete che condividono medesime necessità di security
  - Ogni scambio dati tra diverse ''zone'' deve seguire un ben determinato ''percorso''
  - Ogni ''percorso'' deve essere adeguatamente protetto (Routing/Firewall/VPN)



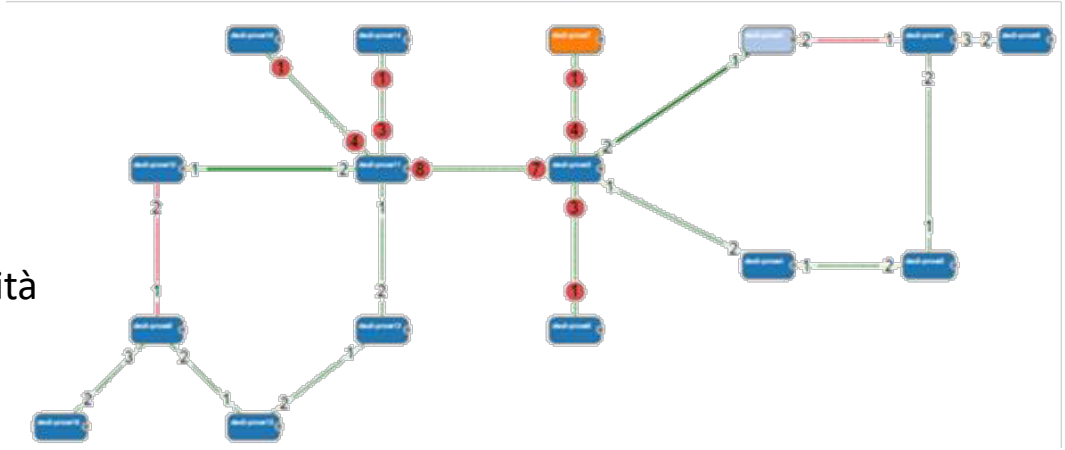
PROFINET: Creazione di sottoaree indipendenti

- Si individuano delle isole di automazione che contengono componenti funzionalmente correlati
  - Vincoli meccanici
  - Vincoli normativi
  - Interfacce uomo macchina
  - Postazioni di lavoro
  - Ergonomia
  - Flusso dati interno: (non attraversa i confini)
  - Flusso dati esterno: (attraversa i confini)
  - Dispositivi sincronizzati



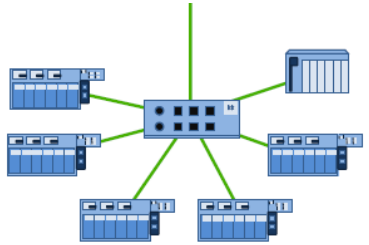
PROFINET: Topologia di rete

- PROFINET garantisce flessibilità di progettazione del layout di rete
  - Tutte le topologie standard sono possibili con PROFINET
  - Un numero di combinazioni quasi illimitato
- La topologia di rete risulta principalmente da criteri quali :
  - Posizione dei componenti
  - Le distanze da coprire
  - Requisiti EMC
  - Requisiti di isolamento elettrico
  - Requisiti per una maggiore disponibilità
  - Considerazione dei carichi di rete .

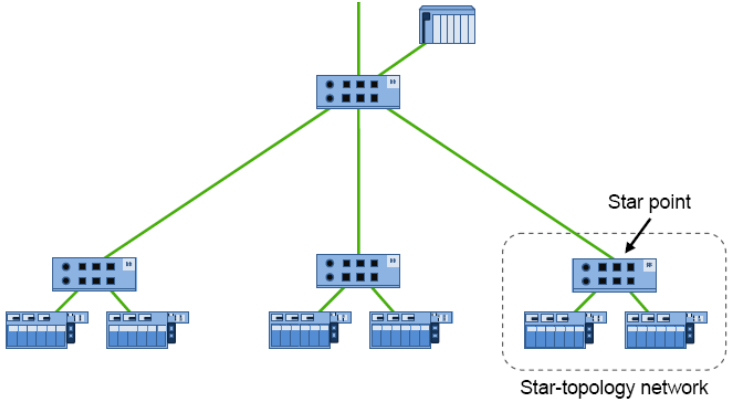


PROFINET: Topologia di rete

- Topologia a stella
  - Serve uno switch
  - Ogni dispositivo ha il suo cavo



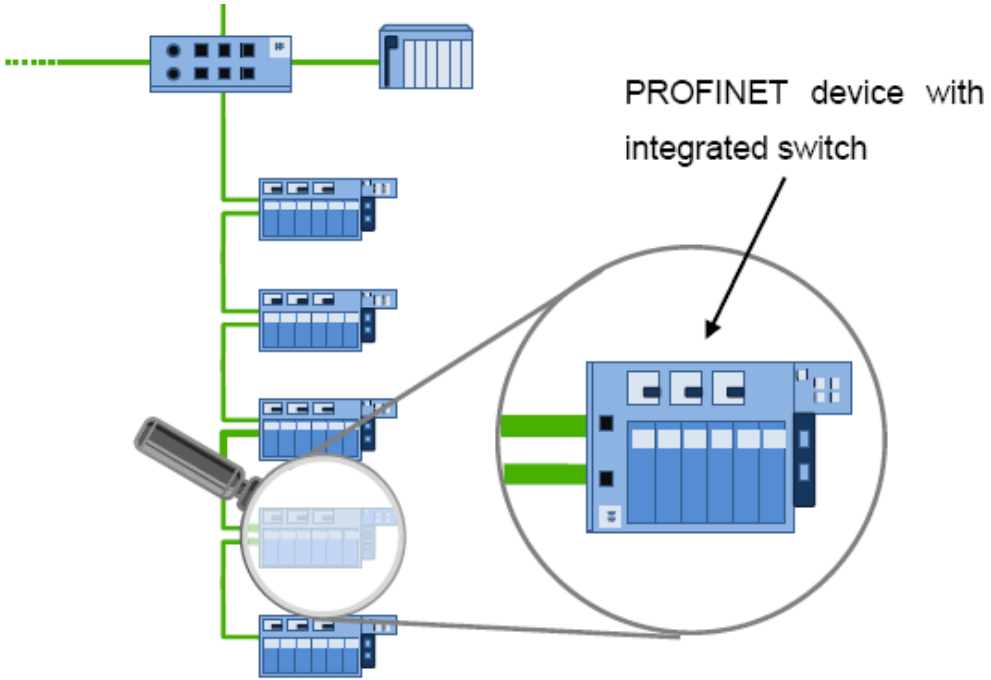
- Topologia ad albero
  - Esistono dei livelli gerarchici
  - Efficiente quanto si connettono tra loro gruppi di dispostivi che parlano principalmente a livello locale



PROFINET: Topologia di rete

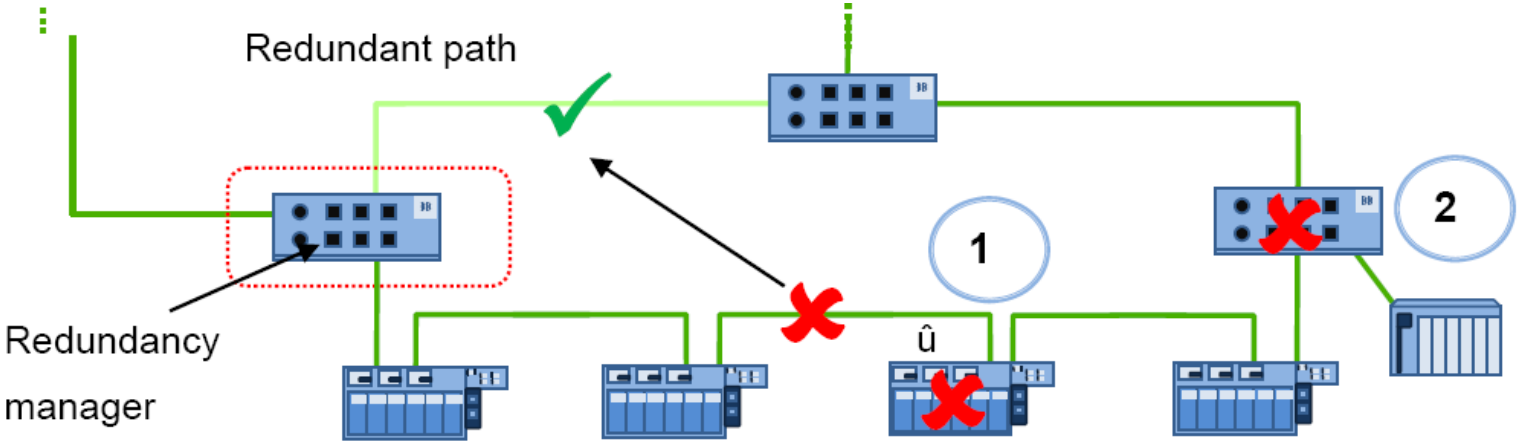
- Topologia lineare
  - Richiama visivamente PROFIBUS
  - Si usano gli switch integrati
  - Non servono switch aggiuntivi

- IMPORTANTE
  - Se un dispositivo della catena si spegne, seguenti sono scollegati dalla rete!



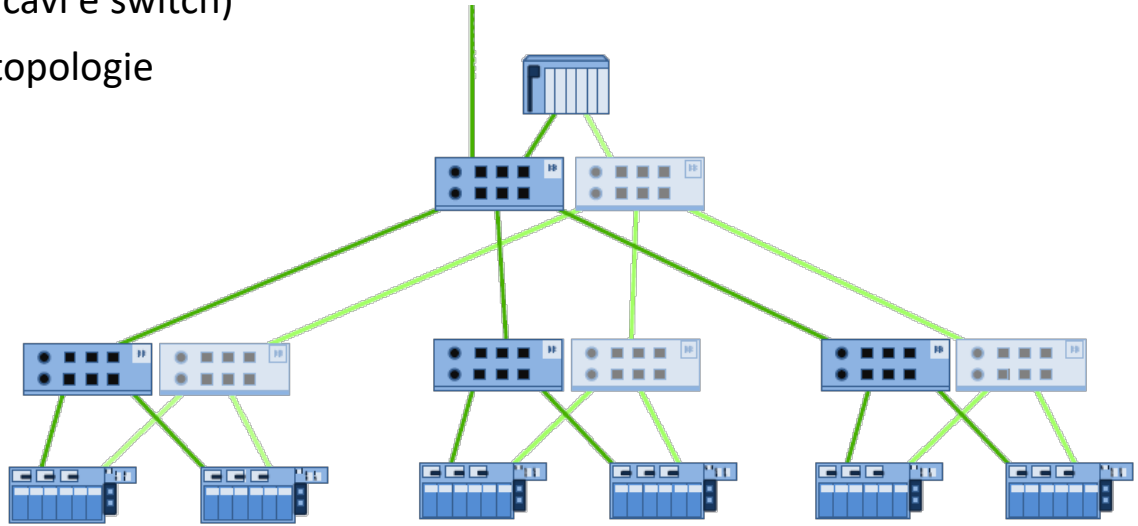
PROFINET: Topologia di rete - ridondanza

- Topologia ad anello
  - Aumenta la disponibilità
  - Un dispositivo dell'anello gestisce la ridondanza (Redundancy manager)
  - Se si verifica 1 guasto la connessione è ancora possibile
  - Se si verificano 2 guasti un segmento di rete resta isolato



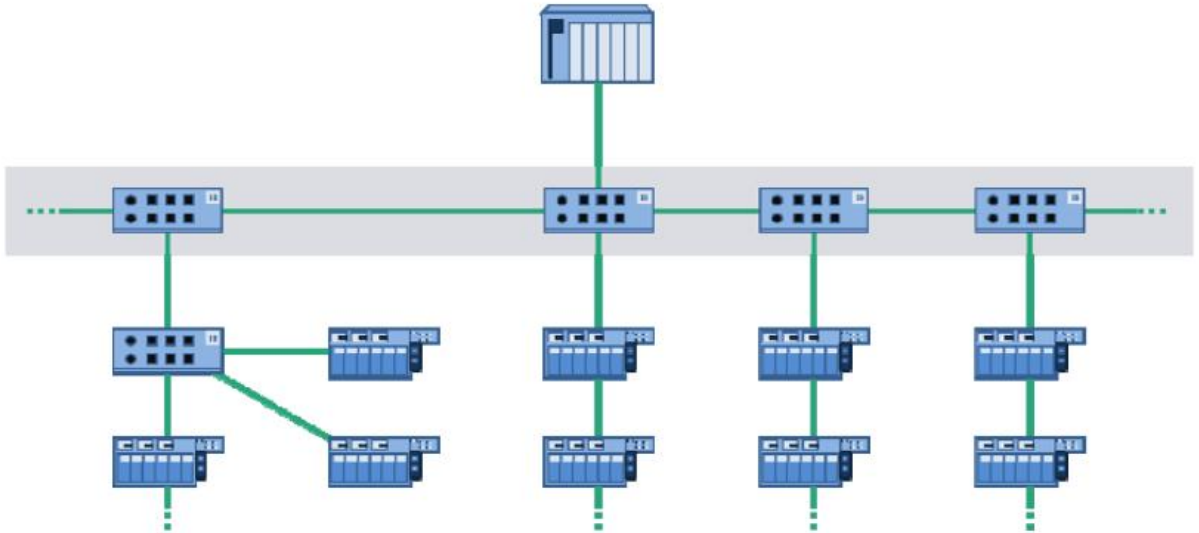
PROFINET: Topologia di rete - ridondanza

- Topologia a doppia rete
  - Aumenta la disponibilità
  - Sono richieste due interfacce di comunicazione indipendenti per ogni dispositivo
  - Raddoppia tutta l'infrastruttura (cavi e switch)
  - (E' possibile raddoppiare anche topologie lineari o ad anello)



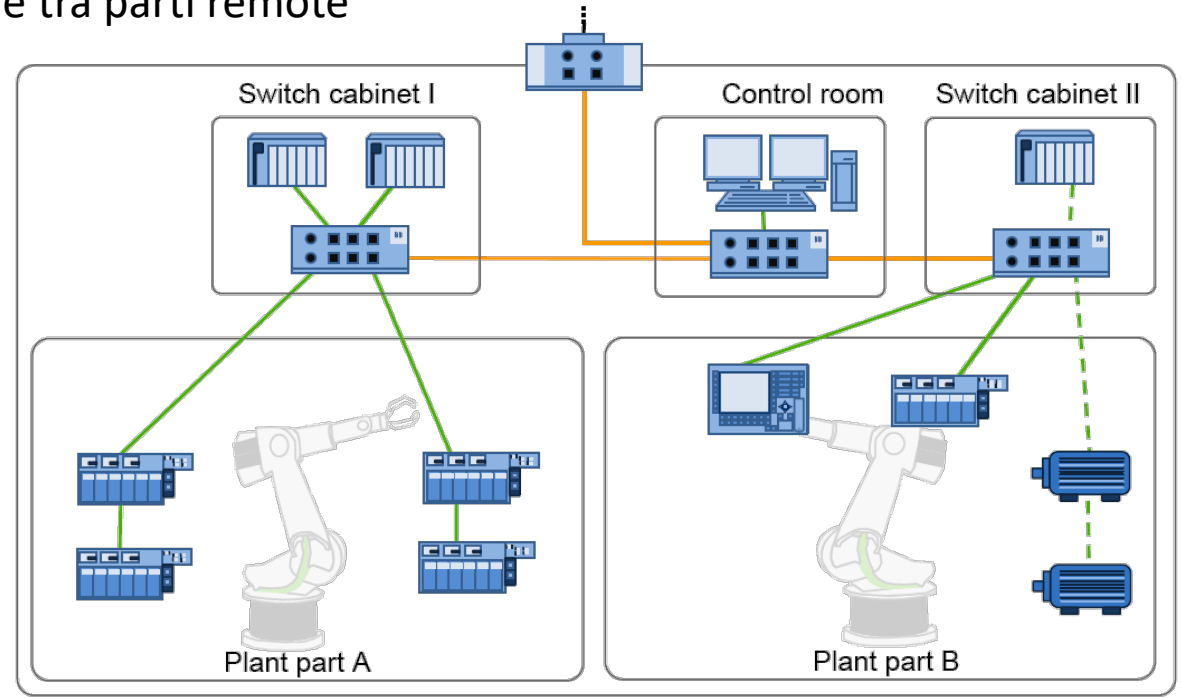
PROFINET: Struttura di riferimento

- Tra tutte le possibili combinazioni si raccomanda di partire da una struttura simile a quella mostrata per poi declinarla secondo le esigenze
  - Si suggerisce di usare switch managed CC-B per la backbone



Esempio: automazione di fabbrica

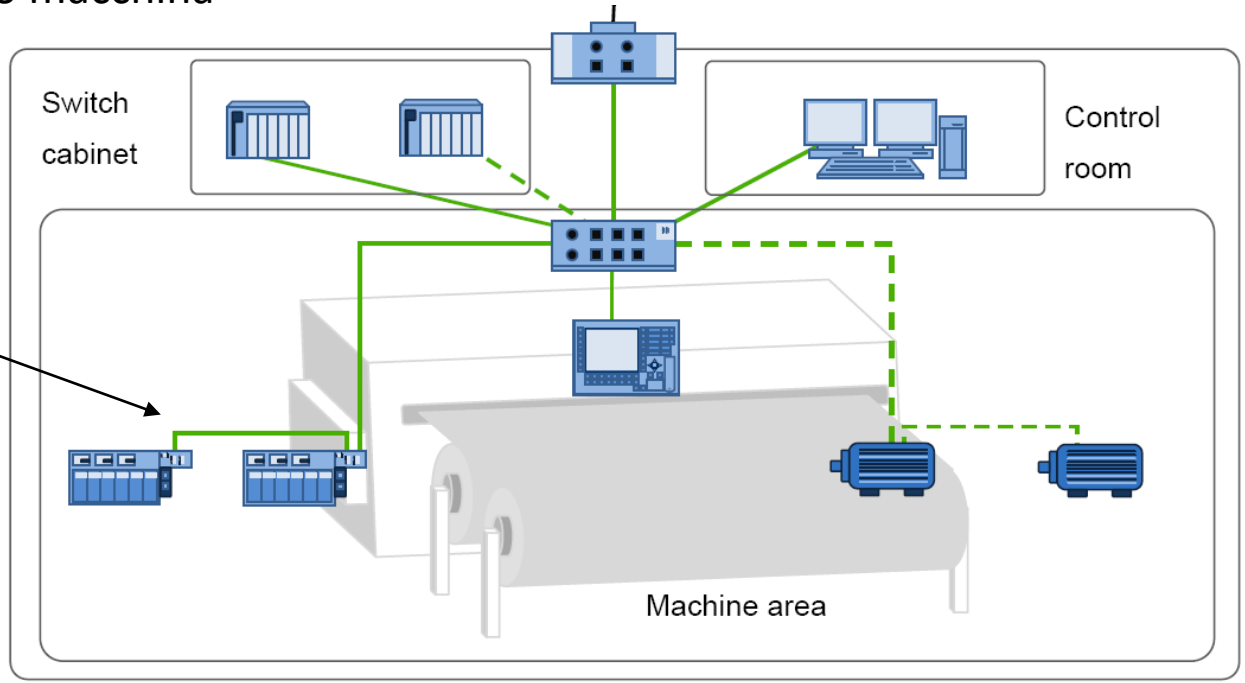
- Controllori e switch vicino al campo
- Fibre ottiche tra parti remote



Esempio: bordo macchina

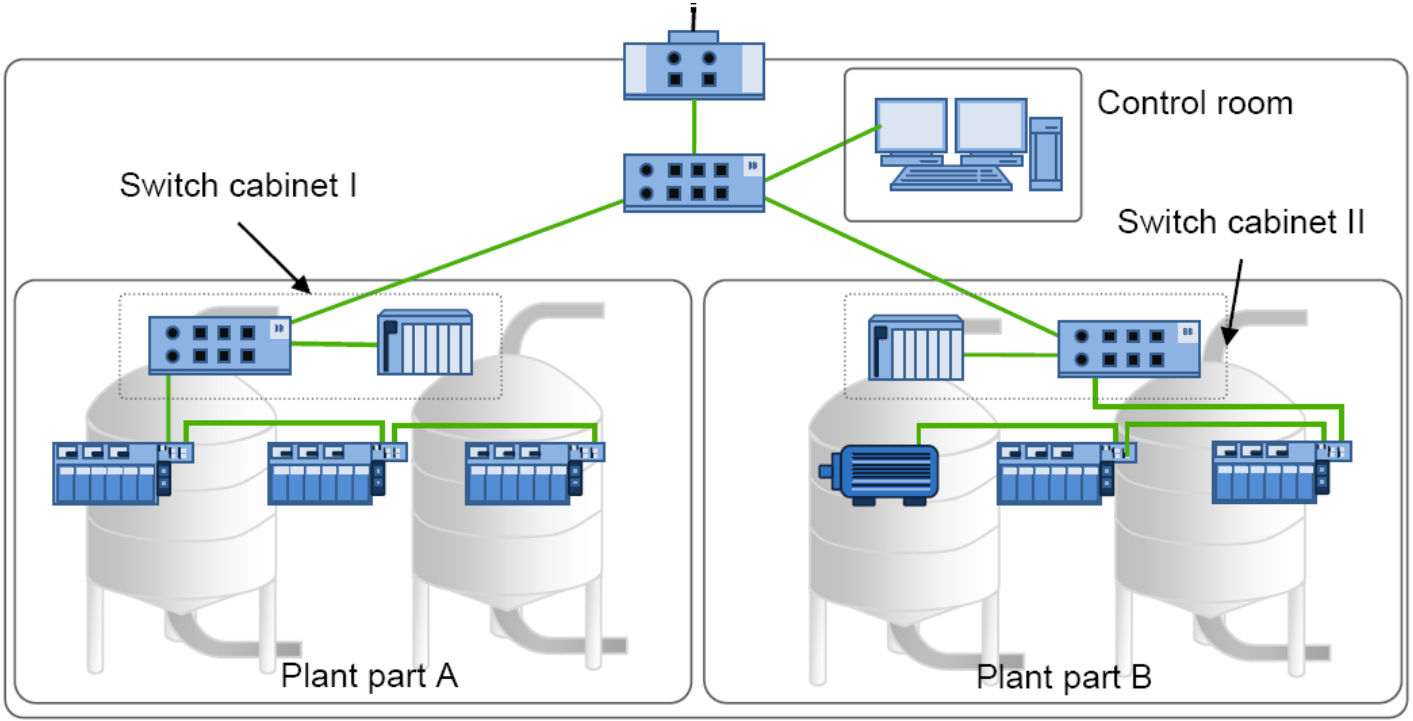
- Catene di dispositivi permettono un cablaggio ridotto.
- Switch a bordo macchina

Usare catene corte di dispositivi!



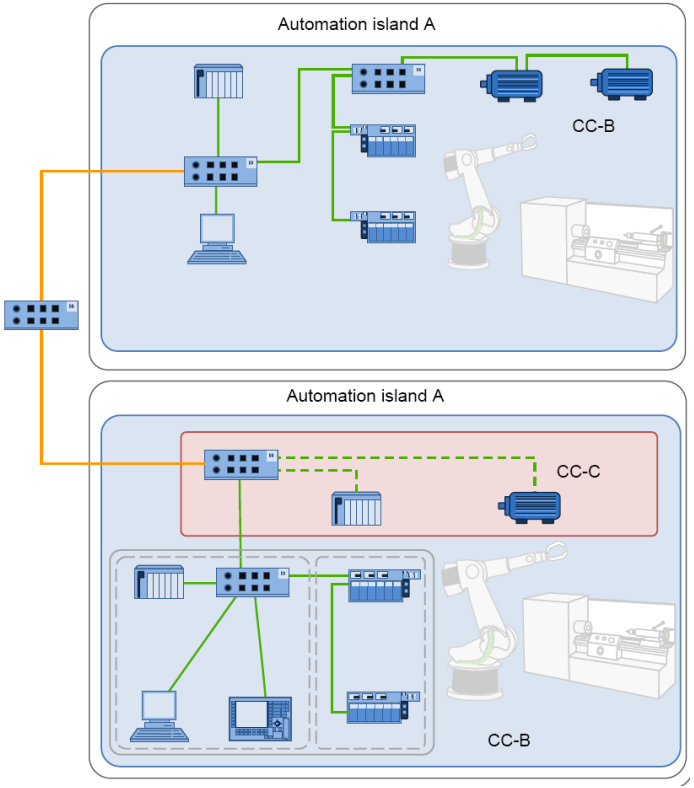
Esempio: impianto di processo

- Struttura modulare e gerarchica



Topologia finale della rete PROFINET

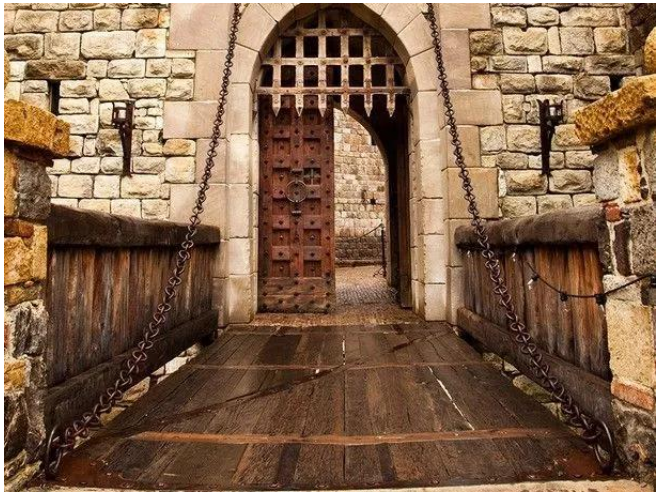
- Applicazione delle regole precedenti
  - I componenti sono collegati all'interno dell'isola di automazione
  - Backbone di switch
  - Struttura gerarchica tra le isole



Definire i punti di accesso

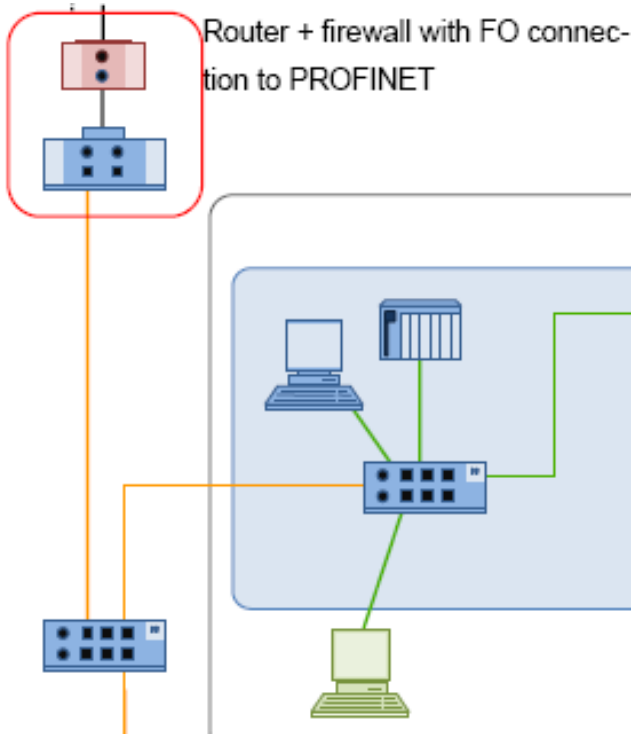
- Occorre definire attraverso quali punti avvengono gli accessi e le relative opzioni.
  - Tutti i percorsi di comunicazione devono essere realizzati in modo sicuro
  - I punti seguenti sono necessari per la creazione di un «punto di accesso controllato»:
    - Quali percorsi sono necessari?
    - Quali servizi sono richiesti per il percorso richiesto?
    - Che porte di comunicazione devono essere attivate?
    - Quale è il motivo per cui serve il percorso?
    - Quale persona/dispositivo deve essere

  autorizzato per usare il percorso di comunicazione?
- Il risultato è una struttura degli accessi basata su dei casi d'uso



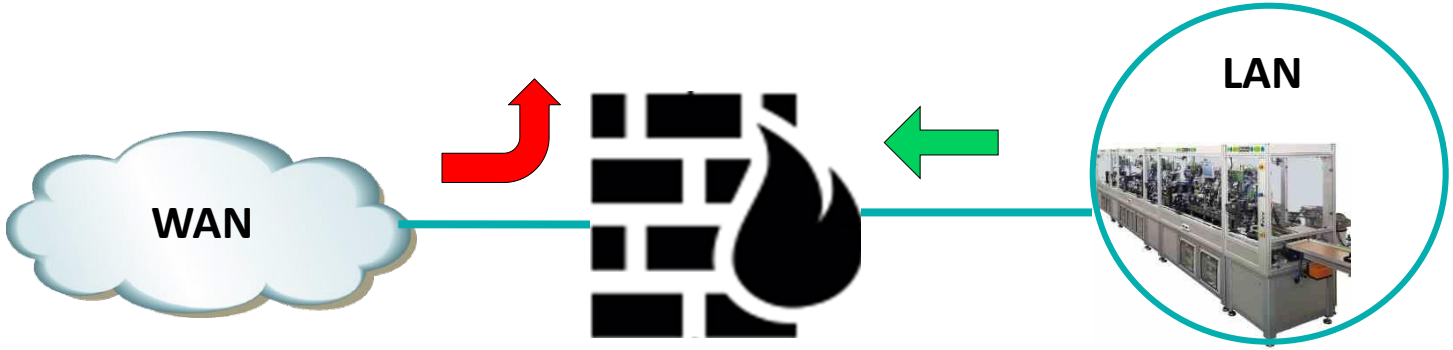
Security:unico accesso alla rete di fabbrica

- Il canale di accesso dati per la comunicazione verticale è fondamentale
- Bisogna garantire
  - Banda adeguata alle funzionalità Industry 4.0 che si vogliono implementare
  - Sicurezza (security)
- Accessi Layer 3 (IP) e non Layer 2 (MAC)
  - Si usano router con funzionalità firewall



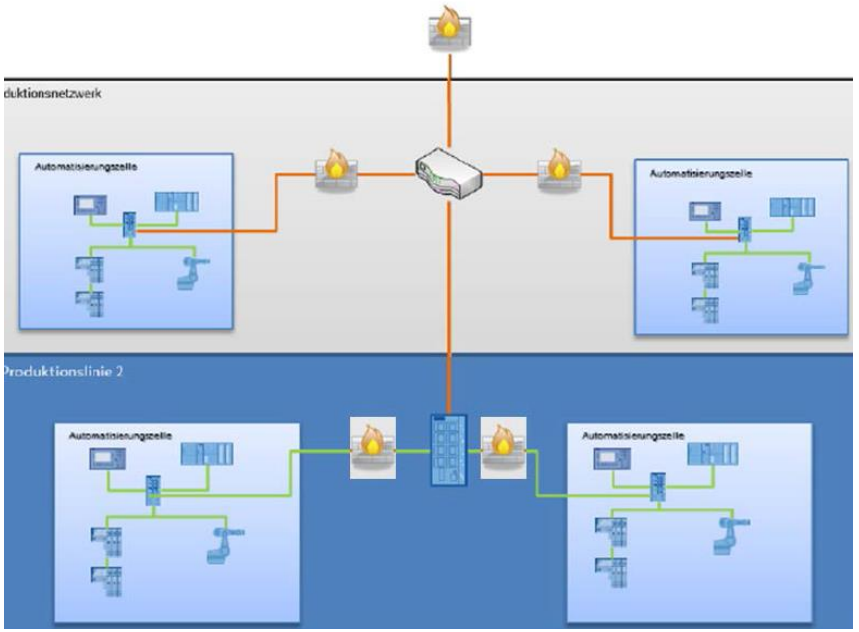
Firewall

- Un Firewall è dispositivo hardware e/o firmware che si parametrizza per controllare gli accessi.
- Per esempio può permettere la comunicazione solo da una rete protetta (rete LAN) verso l'esterno (rete WAN, normalmente non sicura), impedendo accessi in senso opposto



Soluzione con la massima Security

- Se le celle si scambiano dati in IP, si può ulteriormente incrementare la security
- Ogni celle ha le sue politiche di accesso controllate da un firewall specifico
- In ogni caso l'accesso dall'esterno all'interno è controllato da un firewall
- I tempi di reazione dello scambio dati tra cella e cella sono leggermente aumentati rispetto a prima



Le minacce più trascurate – Accesso fisico

- Spesso gli sforzi per incrementare la security sono facilmente vanificati
  - Usare solo cabinet che si possono chiudere a chiave (chiavi codificate)
  - Evitare porte di rete facilmente accessibili in posti non sorvegliati

Le minacce più trascurate – Accesso fisico

- Access Point wireless «di servizio»
  - Non gestiti (spesso neppure industry grade)
  - Spesso dimenticati dopo il commissioning
  - La comodità di solito non è indice di sicurezza….

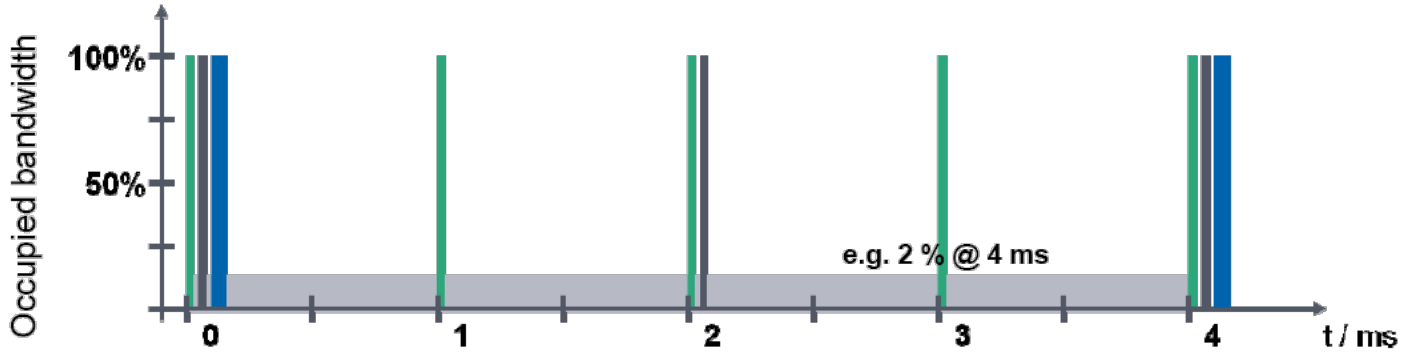
Le minacce più trascurate – Switch Managed non configurati

- Switch managed installati in rete ma non configurati
  - Collocati nei cabinet senza prima essere configurati
  - Hanno tutti valori di default, esattamente come sul manuale del costruttore…..

- Rischio potenzialmente altissimo (attacchi Man-In-The-Middle)

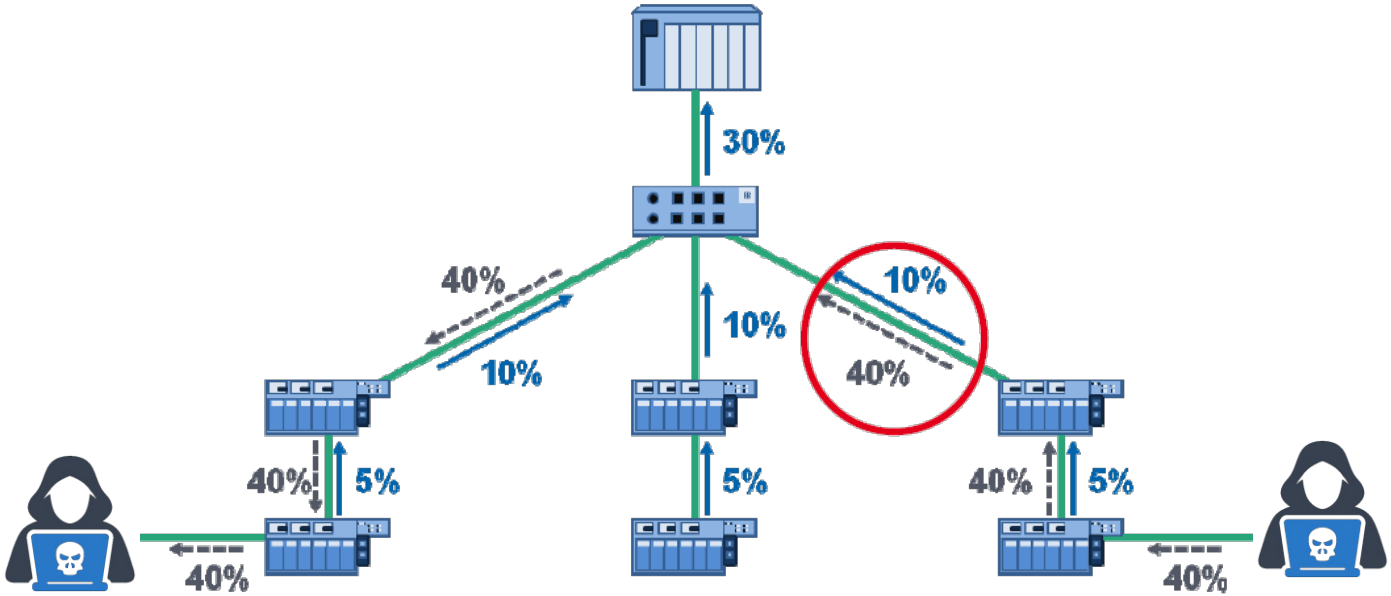
Le minacce più trascurate – attacchi DoS

- **Carico di rete**: Il rapporto tra la quantità di traffico sul link e la massima capacità del link
- Il carico di rete dipende da quale è l'intervallo in cui viene misurato
- La rete Ethernet è bidirezionale
  - esistono due carichi di rete , uno per ciascuna direzione nel link
  - In una rete ogni link può avere un carico diverso.
  - Ragionando "worst case" serve trovare il link con il massimo carico



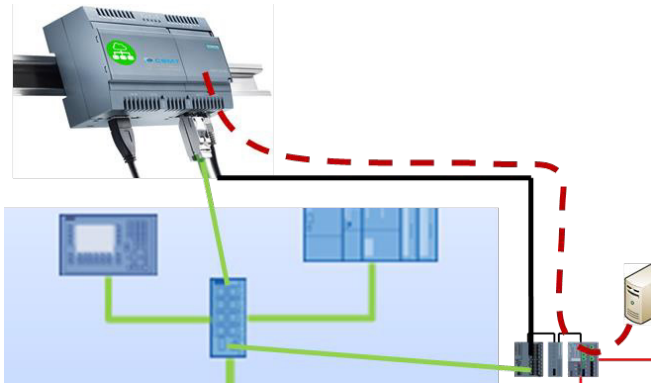
Esempio attacco DoS

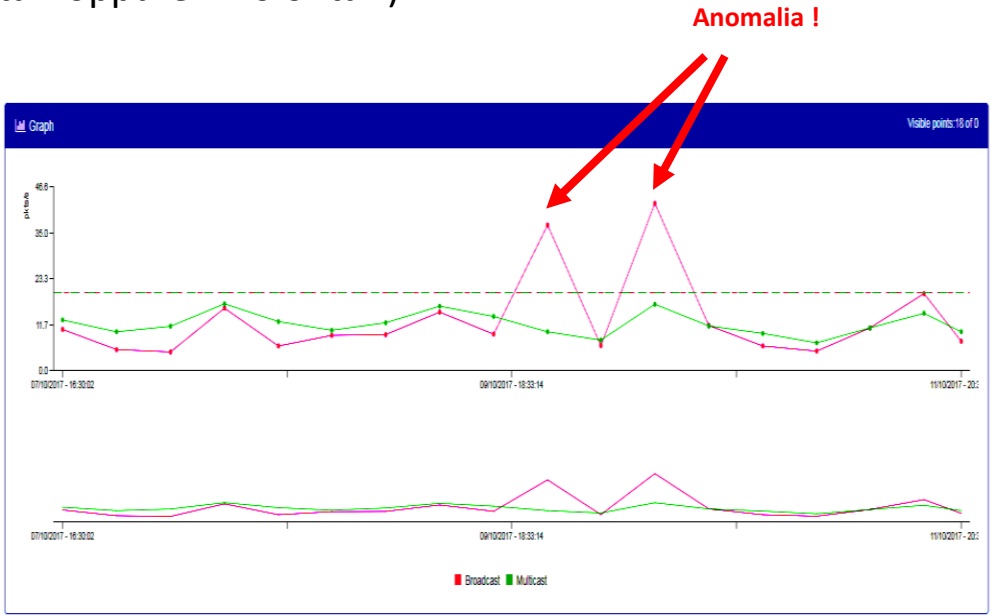
- Dispositivi non PROFINET presenti sulla rete, accessi «Industry 4.0» non controllati oppure malevoli possono generare un consistente carico di rete “non controllato” !
- Sistema mal progettato: il traffico anomalo non real time sovraccarica molti dispositivi



Le minacce più trascurate – attacchi DoS

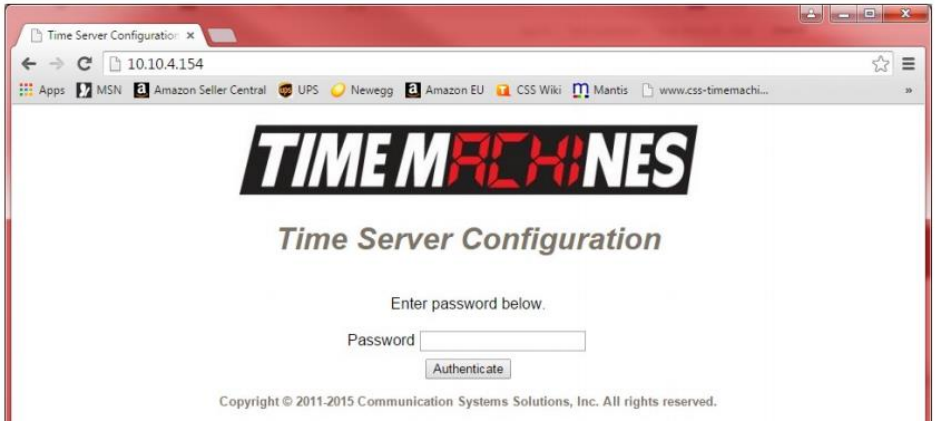
- La rete è inondata di messaggi non utili
  - Broadcast o Multicast flooding (volontari oppure involontari)
  - Richiesta di connessioni TCP anomale
- Bisogna sorvegliare il comportamento del sistema





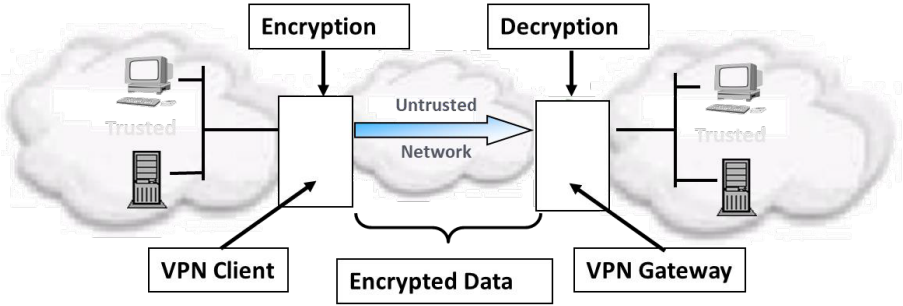
Le minacce più trascurate - interfacce di configurazione

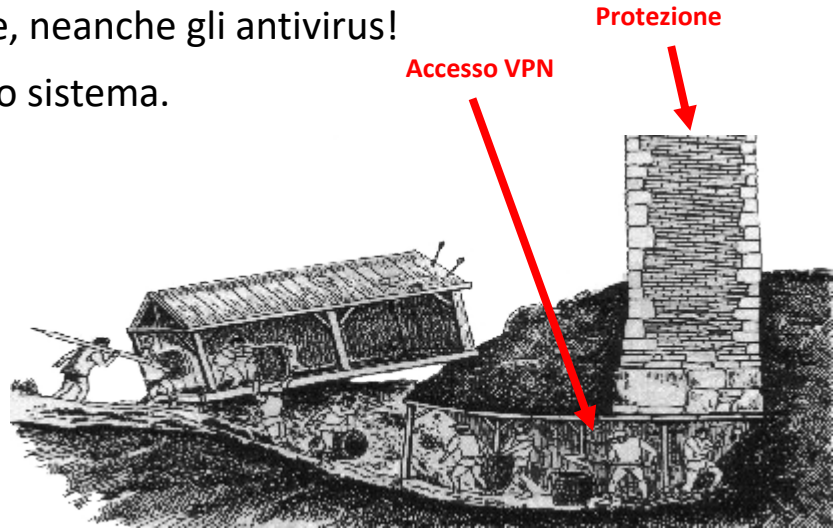
- Tool e protocolli di configurazione dei dispositivi di campo basati su TCP oppure su pagine WEB
  - Spesso con protezioni non attivate o importanti falle di sicurezza
  - Cambiare sempre le password di default
  - Sorvegliare il comportamento del sistema



Le minacce più trascurate – accessi VPN

- Le Virtual Private Network permettono una comunicazione crittografata e quindi sicura attraverso una rete ”insicura” (ad esempio Intenet)…
- Spesso usate per teleassistenza via Internet
  - Il collegamento è cifrato: nessuno lo può analizzare, neanche gli antivirus!
  - Un utente remoto compromesso pregiudica l’intero sistema.





Le prossime mosse di PROFINET

- PROFINET introdurrà importanti novità in tema di sicurezza

Security objective	Description	Relevance for PROFINET
Integrity	Property of a system for the protection against unauthorized data manipulation.	High: Message packets must not be falsified as this could, for example, lead to the unintentional activation of actuators or the recording of incorrect measured values.
Confidentiality	Information is only accessible to certain users and remains hidden from third parties.	Low: The security objective "confidentiality of IO data" is estimated as low as long as no conclusions can be drawn with regard to company secrets (e.g., recipes).
Availability	Property of system, to always perform the required function.	High: Depending on the production process, there are generally high to very high availability requirements. This is especially true for critical infrastructures.
Authenticity	Unique identification of a system component and its data.	High: The authenticity ensures that the data can be uniquely assigned to its source. The components must "identify" themselves for this purpose and have a counterfeit-proof digital identify.

Le prossime mosse di PROFINET (continua)

Security objective	Description	Relevance for PROFINET
Authorization	Enforce the permissions assigned to an authenticated user (human user, software process or device) that allow him to perform the required actions in the automation system and monitor the use of those permissions.	High: The usage control ensures that only authorized users can intervene in the automation system.
Non-repudiation	Ability to prove the occurrence of an alleged event or activity and the person or entity causing it.	Medium: Refers to installations where traceability of user intervention is required. For example, pharmaceutical plants operated in accordance with FDA 21 CFR Part 11 [FDA2018] [TEB2015].

PI Italia
PROFIBUS • PROFINET

GRAZIE

per l‘attenzione

PROFINET® PROFIBUS® PROFIsafe PROFIenergy PROFIdrive IO-Link FDI