

#WEBINAR 10/11/2020

Cyber Risk: analisi, soluzioni e strategie

MEMBER OFFICINA LIBERTY



Dopo Industry 4.0 La Cyber- Security

La Resilienza del mondo Industriale



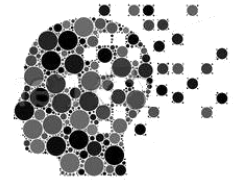
Centro di competenza
Profibus / Profinet

 **CSMT**
POLO TECNOLOGICO

Non è possibile ignorare la CYberSecurity

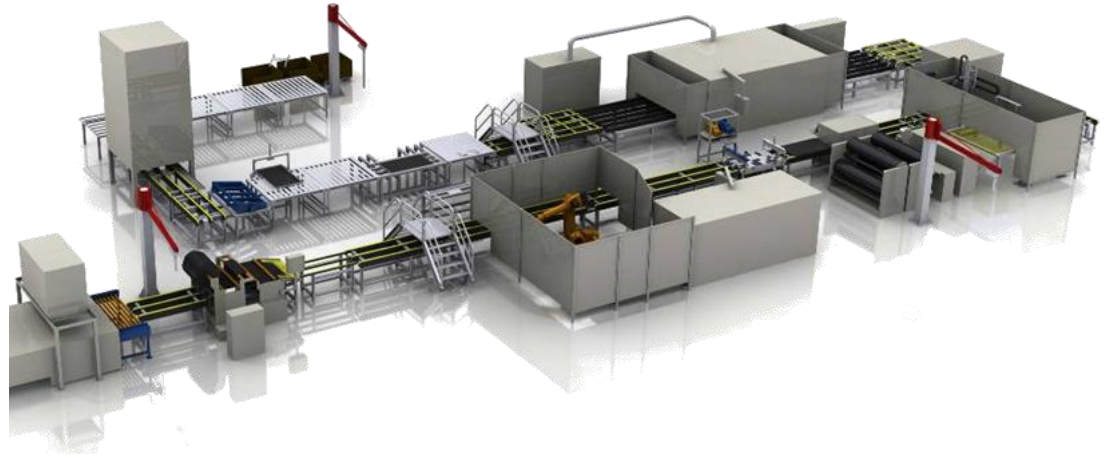
Quando si opera in ambiente industriale, le possibili conseguenze di una non adeguata protezione di una rete possono essere molto costose... o peggio...

- PERDITA DI DATI: Costo ricostruzione dei dati stessi
- PERDITA DI KNOW-HOW: Dati venduti ai competitor
- FERMO PRODUZIONE: Costo dovuto agli arresti produttivi
- ORE LAVORO DEI LAVORATORI: Costo ore necessarie per il ripristino
- REPUTAZIONE: Quanto costa la perdita di reputazione sul mercato?



Perchè invece la ignoravamo?

- 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

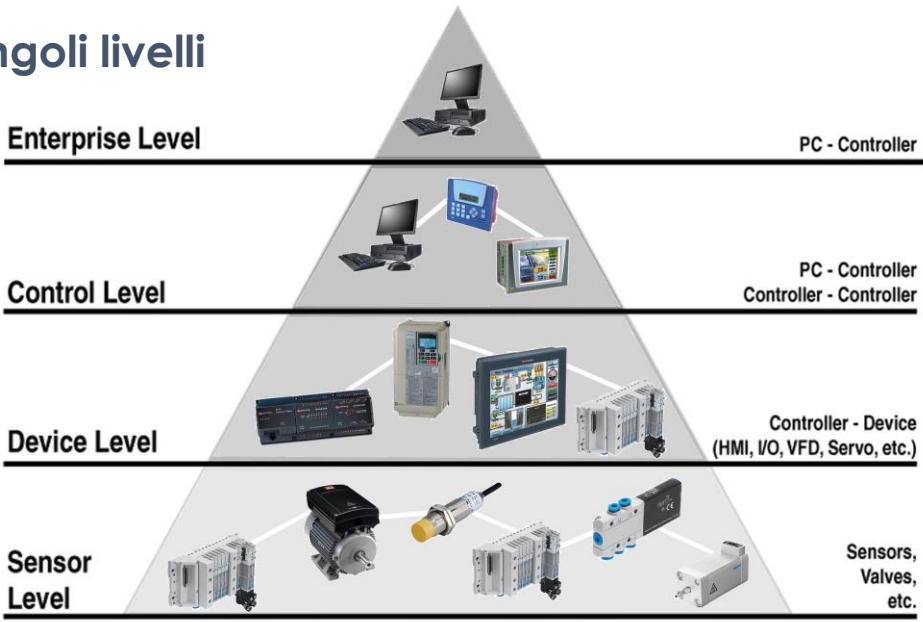
Concepiti con modello a piramide (ISA95)
Organizzate secondo livelli gerarchici
Dialogo verticale solo tra controllori dei singoli livelli

Ethernet

Ethernet

Bus di campo seriali
(PROFIBUS, CAN, Modbus RTU)

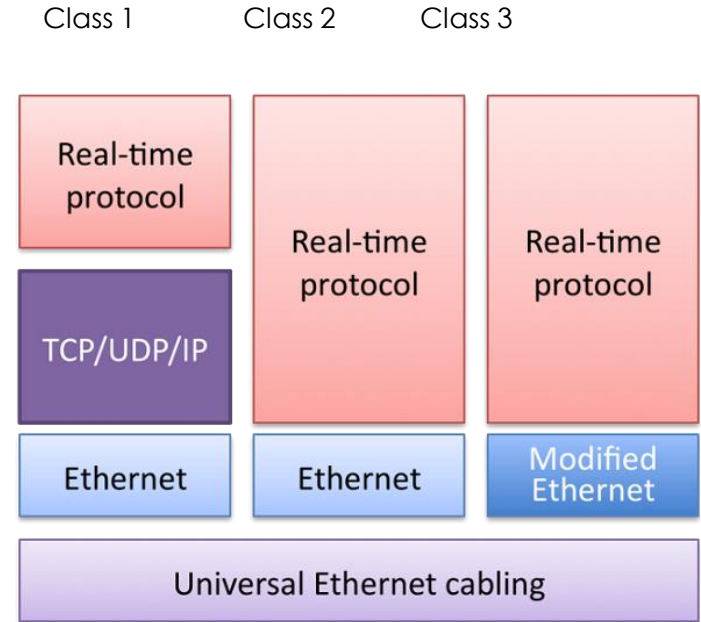
Bus di campo seriali
(CAN, ASI, RS232)



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

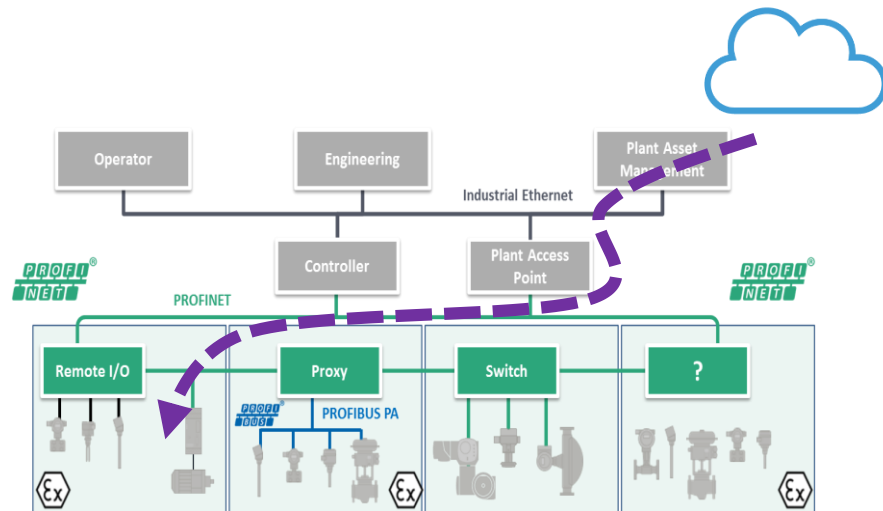
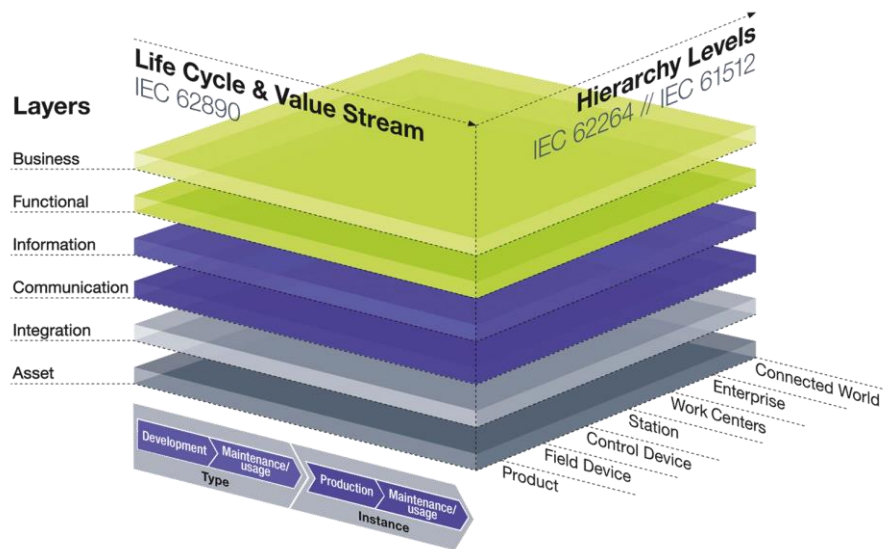


Nuovi accessi per Industry 4.0

Il modello di Industry 4.0 è a «cubo» (RAMI 4.0)

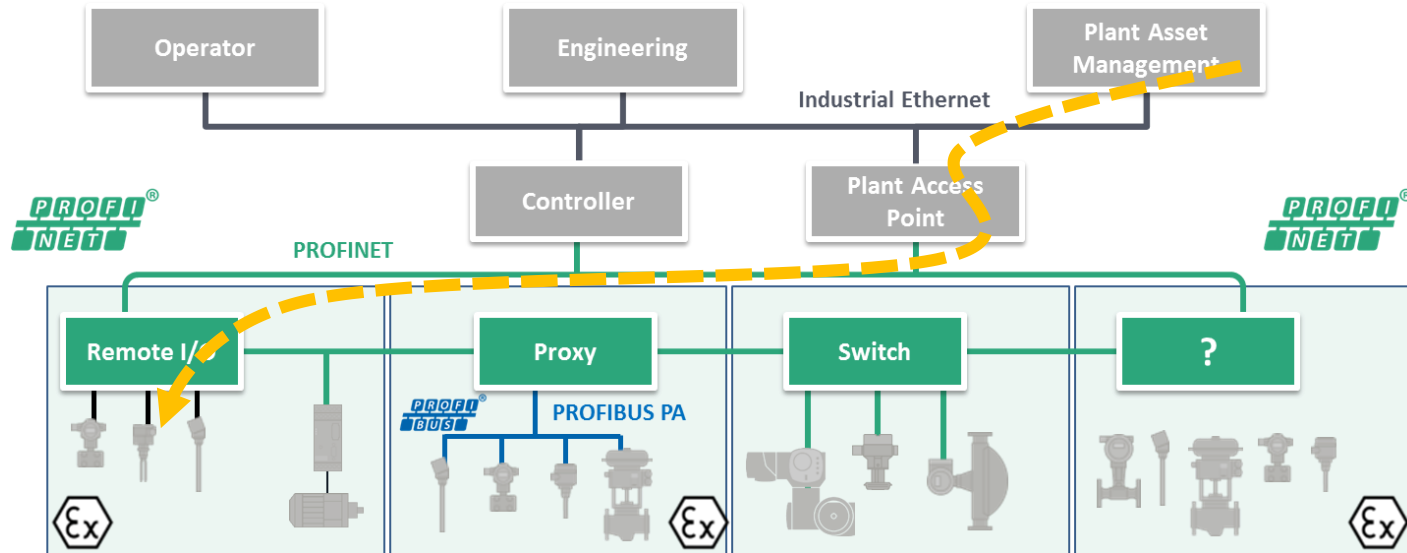
La gerarchia è meno evidente

Accessi verticali verso ogni dispositivo



Esempio: 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.



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**

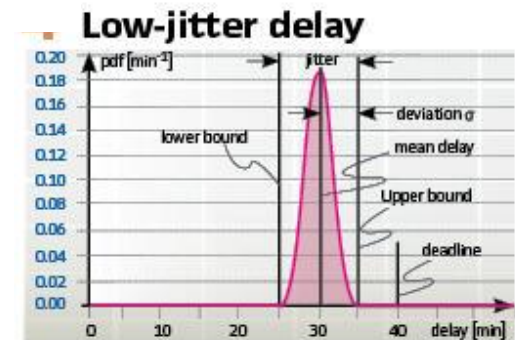
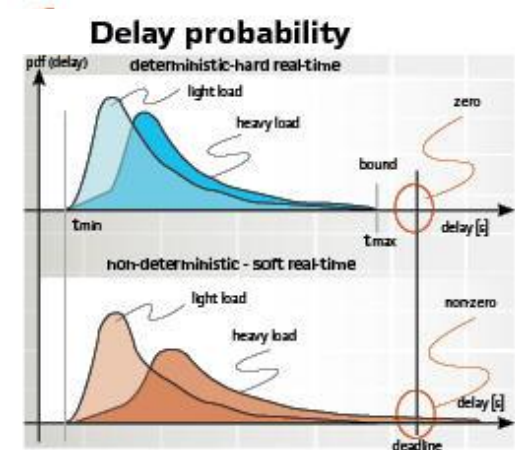
Security per IT e per reti industriali

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.



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

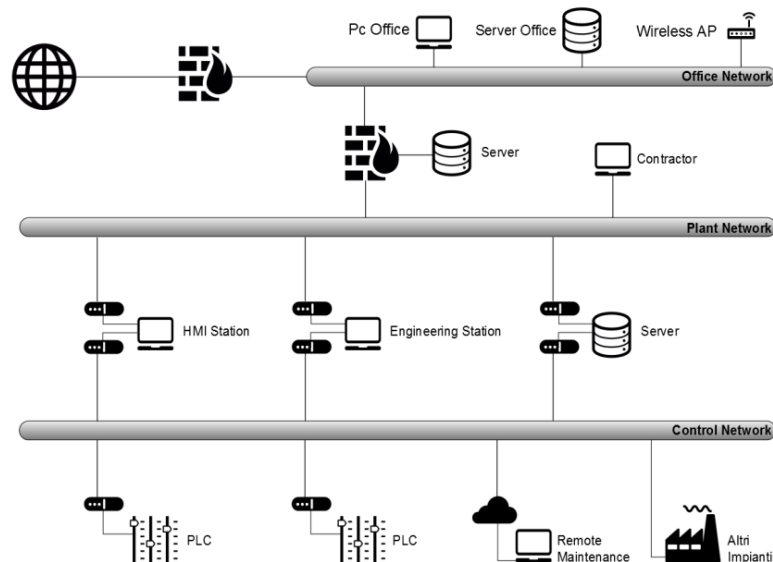


Applicazione della teoria alla pratica

Misure e soluzioni tecnologiche scelte in funzione di esigenze specifiche

- ❑ opportuna segmentazione di rete con adeguata protezione (routing/firewall) dei punti di segmentazione,
- ❑ corretta gestione delle prerogative di accesso locale alla rete
- ❑ 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

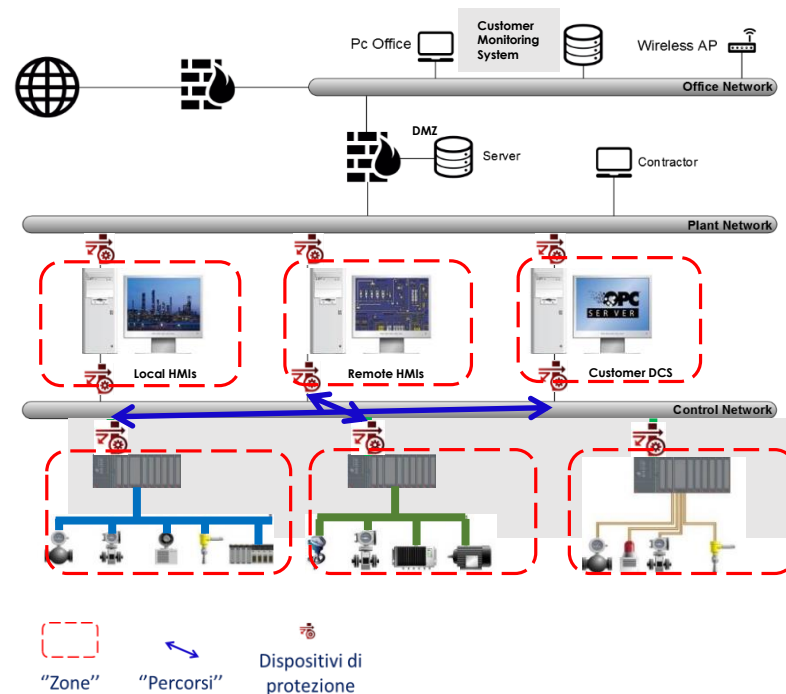
Dividere in "zone"

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

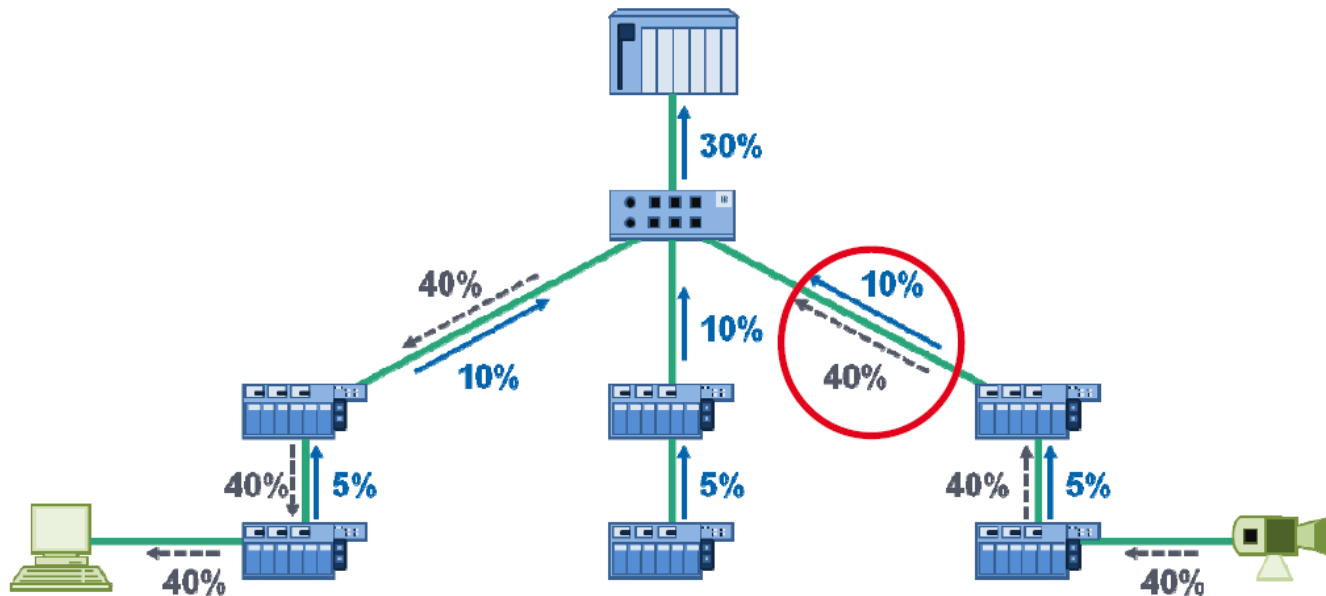
Ogni scambio dati tra diverse "zone" deve seguire un ben determinato "percorso"

Ogni "percorso" deve essere adeguatamente protetto (Routing/Firewall/VPN)



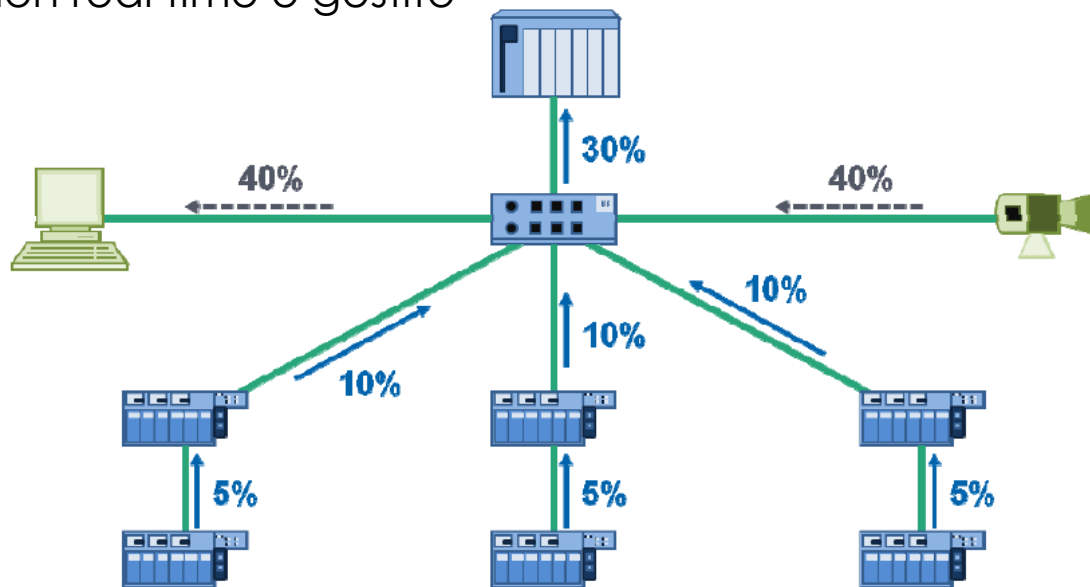
La Topologia: traffico non real time

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



La Topologia: traffico non real time

- Sistema progettato in modo migliore:
 - Il traffico non real time ha un percorso nella rete il più possibile diverso da quello di PROFINET
 - Il traffico non real time è gestito



Sistemi di difesa

- ❑ La conoscenza della rete e tecnologie in campo
- ❑ La Formazione
- ❑ Scelta degli Strumenti



Minacce Reali

- Access Point wireless «di servizio»
- Accessi Fisici
- Switch managed installati in rete ma non configurati
- Attacchi DoS
- Interfacce di Configurazione



Le minacce più trascurate – Accessi Wireless

- 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 – 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: Switch Managed non configurati

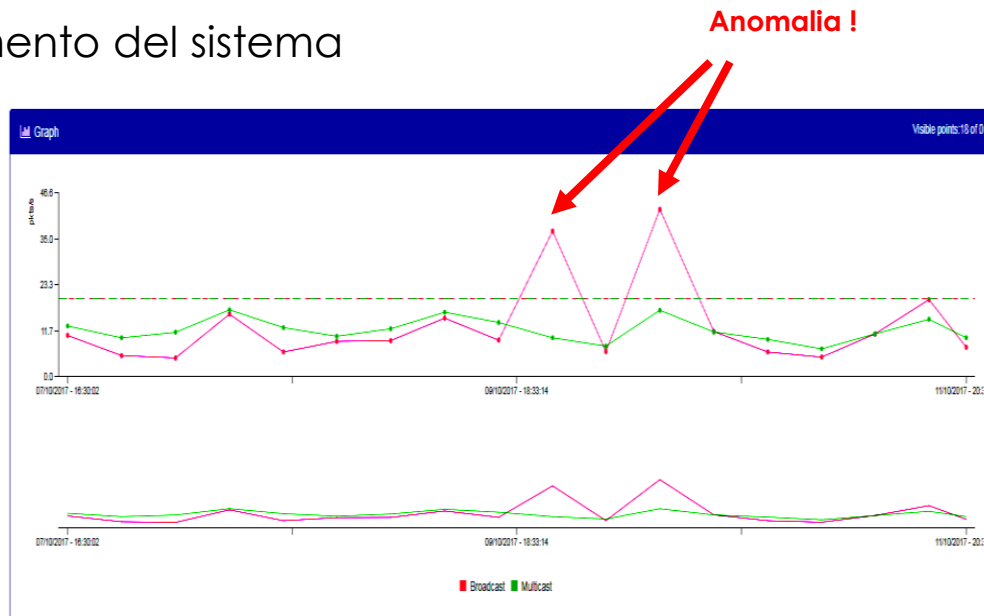
- Switch managed installati in rete ma non configurati
 - Collocati nei cabinet senza prima essere configurati
 - Hanno tutti valori di default, esattamente come sul manuale del costruttore.....

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



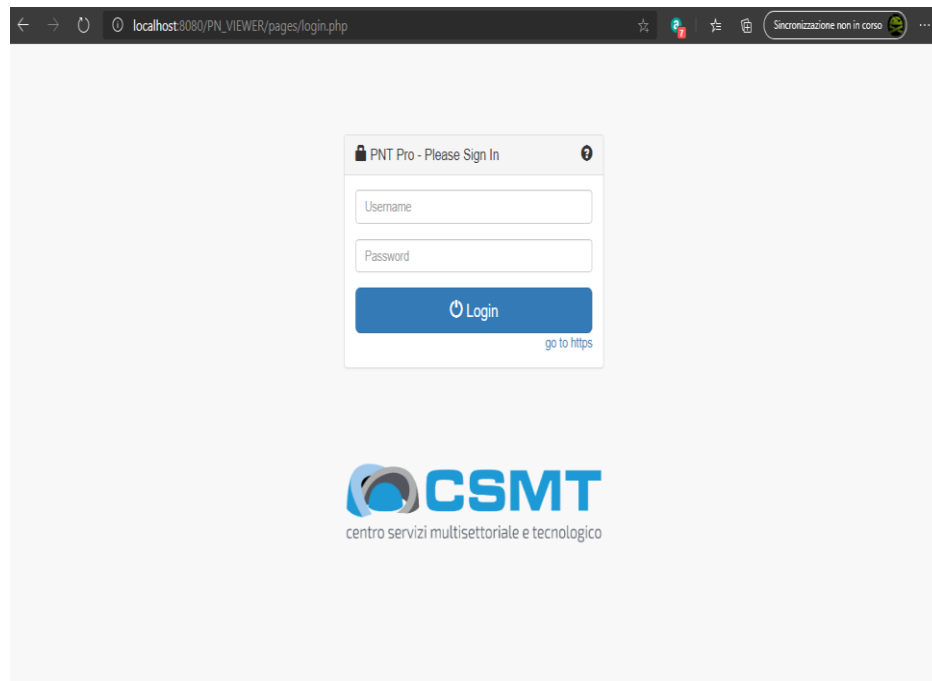
Le minacce più trascurate – attacchi DoS

- 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



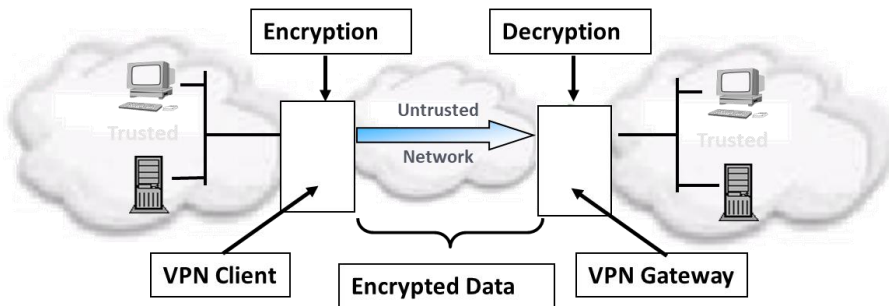
Le minacce più trascurate: interfacce di configurazione

- 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
 - Aggiornare Firmware dei dispositivi in campo



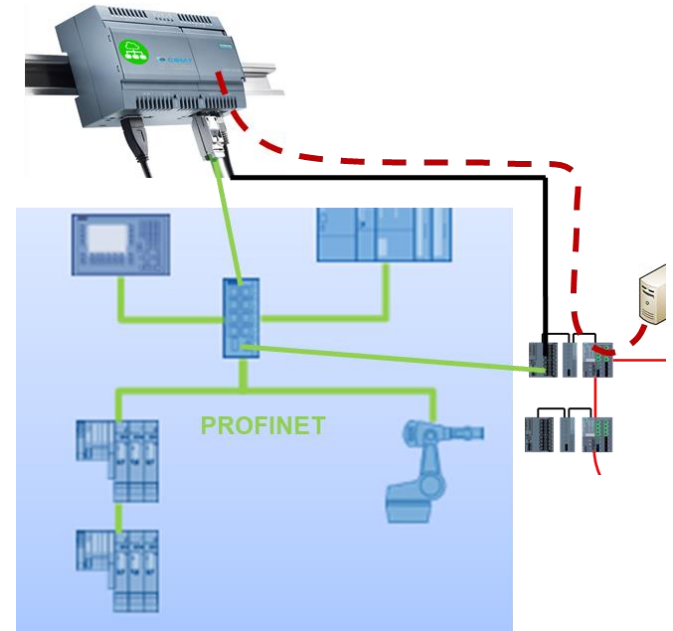
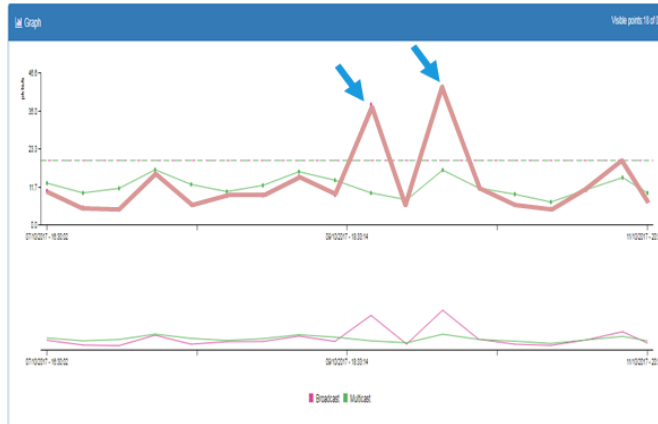
Le minacce più trascurate – accessi VPN

- Le Virtual Private Network permettono una comunicazione crittografata e quindi sicura attraverso una rete "insicura" (ad esempio Internet)...
- 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.



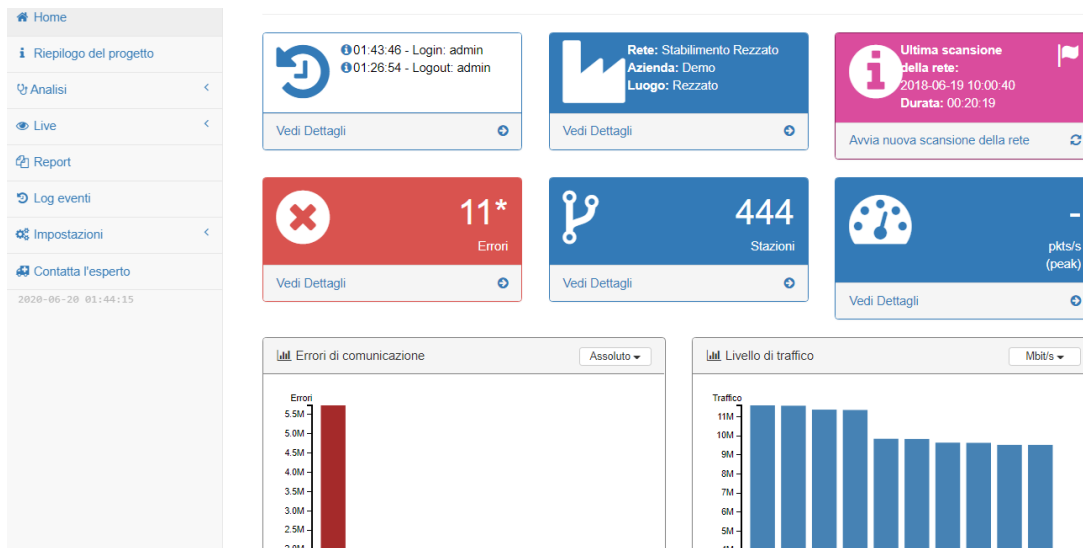
Esempi reali monitoraggio permanente PROFINET

- CASO: installazione dispositivo di monitoraggio permanente
- Risultati
 - Individuati dispositivi PN non configurati
 - Individuati altri cavi/connettori difetto
 - Individuati comportamenti anomali di PC



Esempio di sistema di monitoraggio: PNT-PRO

- sistema di troubleshooting e monitoraggio per reti profinet.
- Rilevamento errori di trasmissione
- Manutenzione predittiva



Grazie per l'attenzione!


Daniele Rovetta

CSMT Gestione

Sales & Project Manager

Centro di competenza Profibus/Profinet

 d.rovetta@csmt.it

 +39 (030) 6595111