Sicurezza delle reti industriali: casi, esempi ed accorgimenti fondamentali

Paolo Ferrari
Dipartimento di Ingegneria dell'Informazione, Università di Brescia
Via Branze 38 - 25123 Brescia (Italy)
e-mail: paolo.ferrari@unibs.it
CSMT Gestione Scarl
Centro di Competenza PROFIBUS e PROFINET - Brescia

Safety vs. Security

Security: protezione delle macchine dagli uomini

Security

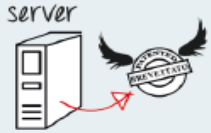
Definizione inclusa nella specifica tecnica IEC/TS 62443-1-1:2009 ”Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, concepts and models”:

”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”

© 2017 PROFIBUS e PROFINET Italia

Non è possibile ignorare la Security

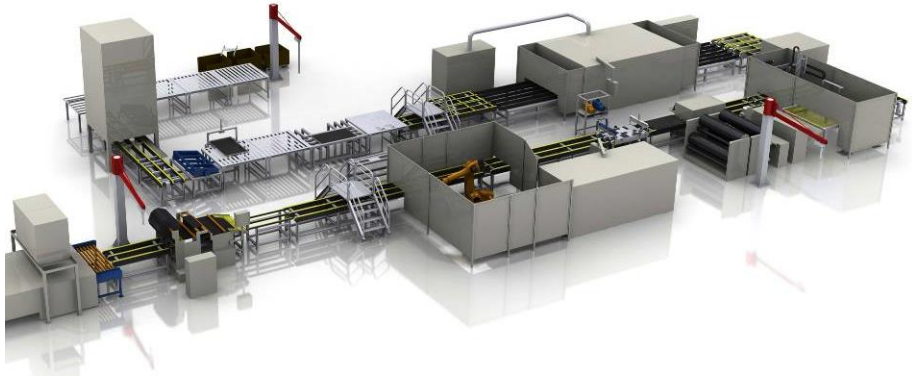
Quando si opera in ambiente industriale, le possibili conseguenze di una non adeguata protezione di una rete possono essere molto costose… o peggio…

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?	

© 2017 PROFIBUS e PROFINET Italia

Perchè invece la ignoravamo?

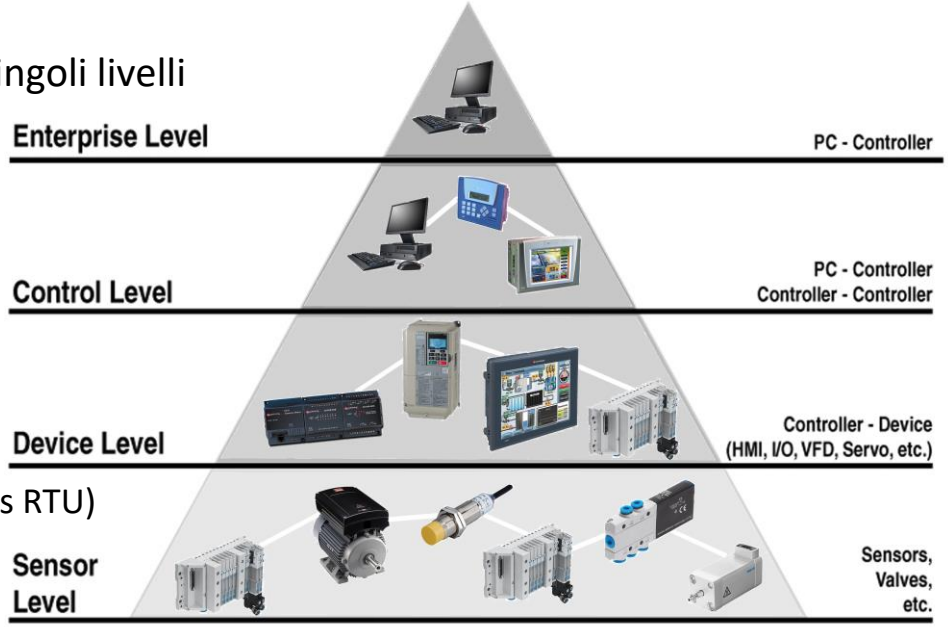
- Perché fino a ieri la security non era prioritaria?
  - Con fieldbus su base seriale (Modbus RTU, PROFIBUS, Devicenet, CAN) le macchine non sono interconnesse direttamente tra loro
  - I progettisti di automazione come security intendevano evitare accessi al progetto installato sul sistema di controllo



© 2017 PROFIBUS e PROFINET Italia

Le reti industriali tradizionali

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



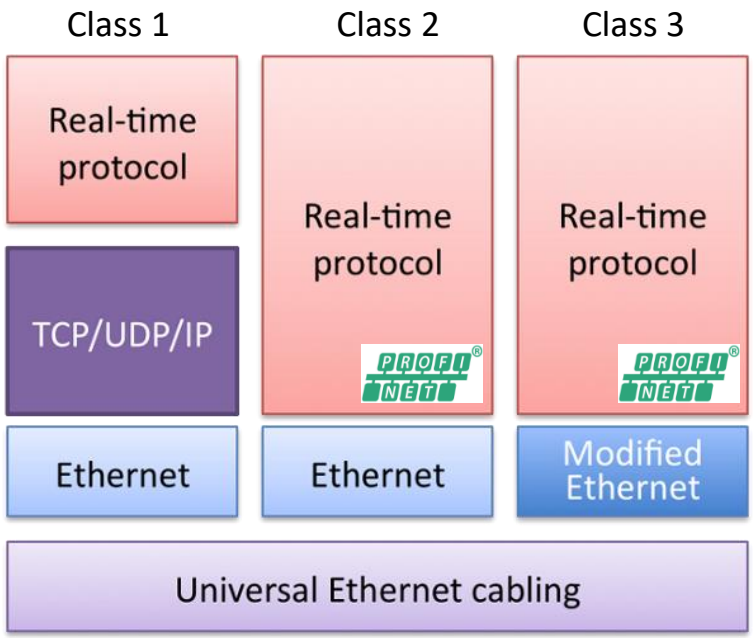
  - Ethernet
  - Ethernet
  - Bus di campo seriali(PROFIBUS, CAN, Modbus RTU)
  - Bus di campo seriali (CAN, ASI, RS232)

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

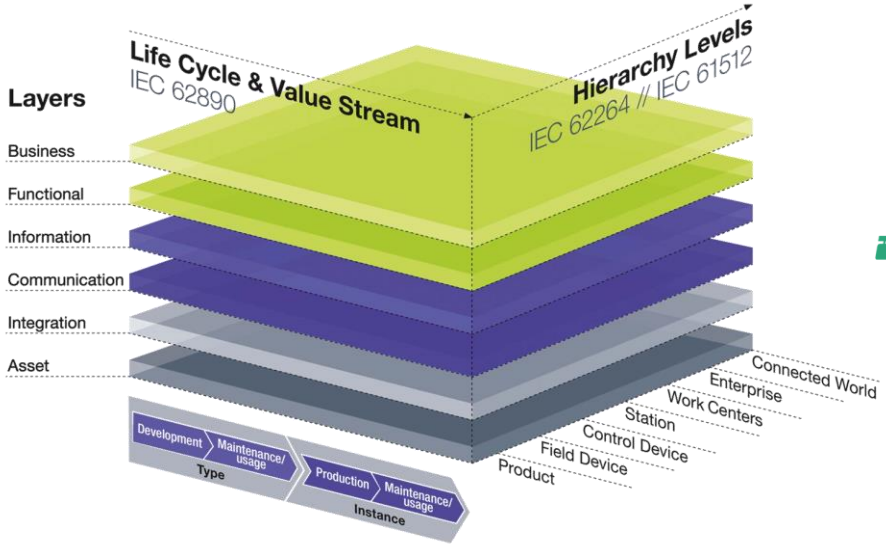
  - Prestazioni: Class 3 > Class 1

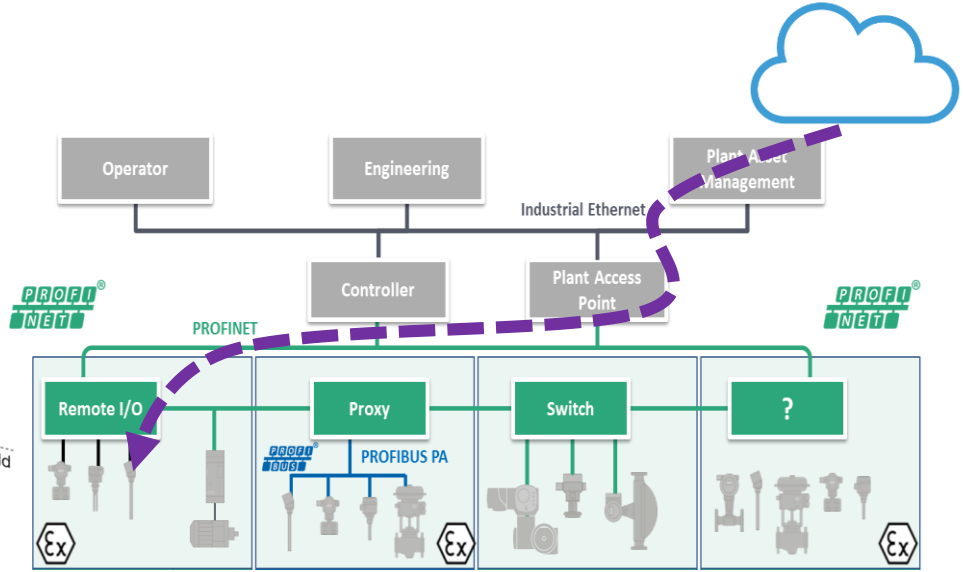


  - Class 2 e Class 3 spediscono i dati di processo direttamente nei pacchetti ethernet

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
  - Accessi verticali verso ogni dispositivo





Security per le reti industriali

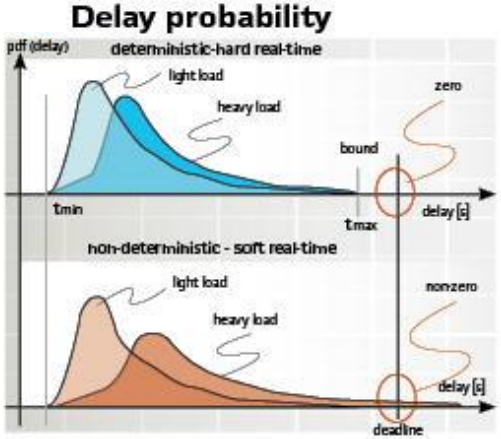
- I concetti di sicurezza per gli ambienti office non possono essere **«semplicemente»** trasferiti alle reti di automazione.
  - Le misure di sicurezza implementate per i sistemi di automazione **non devono essere in conflitto** con i requisiti operativi relativi ai protocolli real-time.
  - L'obiettivo 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

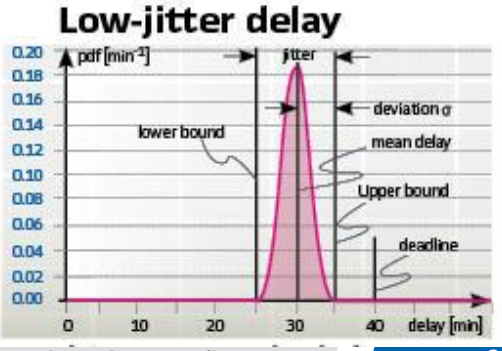
© CSMT Gestione vietata la riproduzione

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.





© CSMT Gestione vietata la riproduzione

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.

© CSMT Gestione vietata la riproduzione

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)

© CSMT Gestione vietata la riproduzione

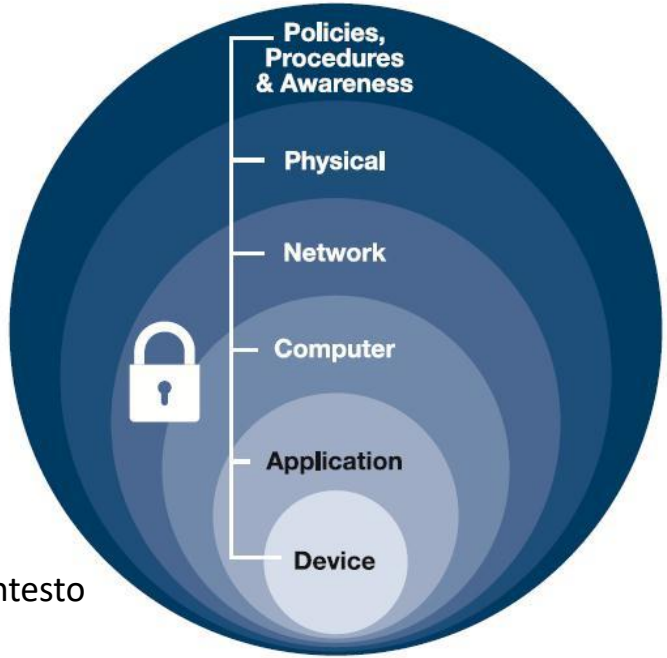
Requisiti speciali della Security per le reti industriali

- 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

© CSMT Gestione vietata la riproduzione

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

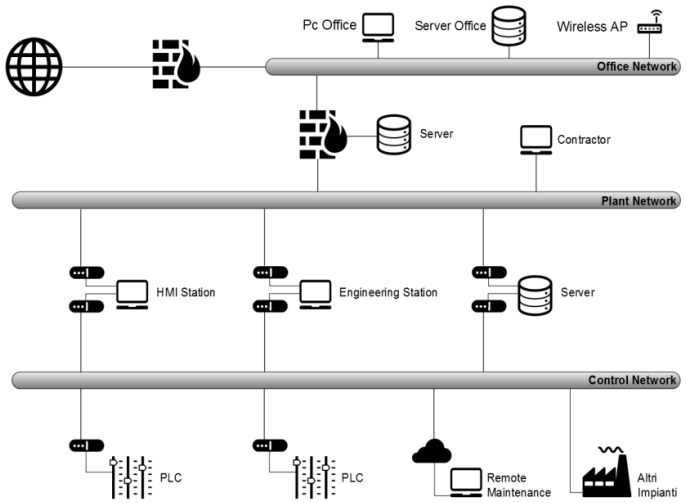


© CSMT Gestione vietata la riproduzione

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)

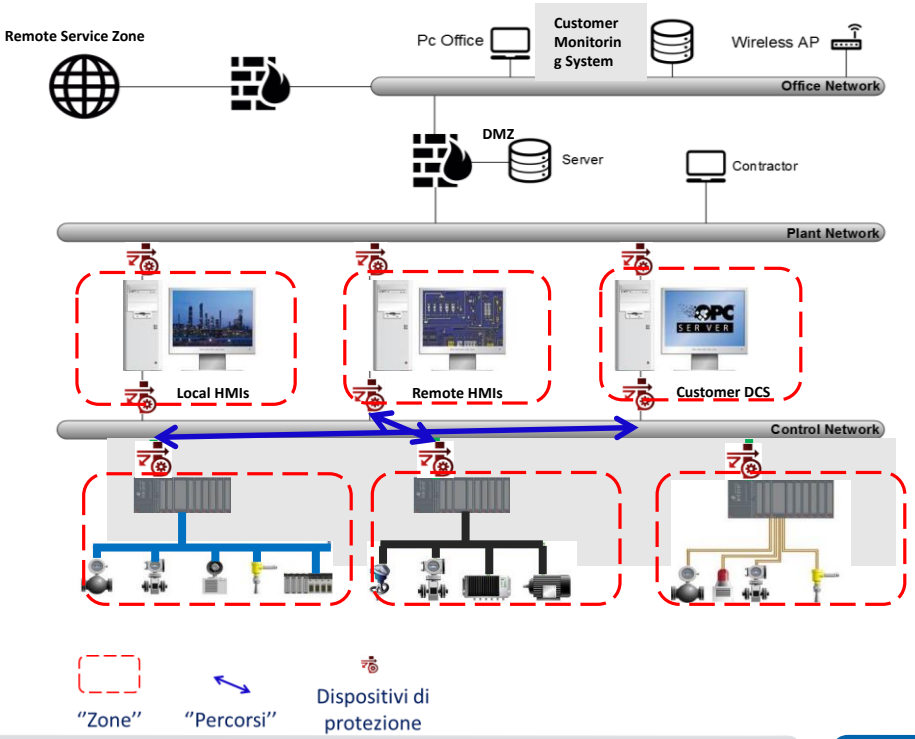


Nota: l'utilizzo di strumenti di monitoraggio continuo di rete permetterà anche la rilevazione immediata di tentativi di intrusioni non autorizzate

© CSMT Gestione vietata la riproduzione

Applicazione alla pratica: le zone

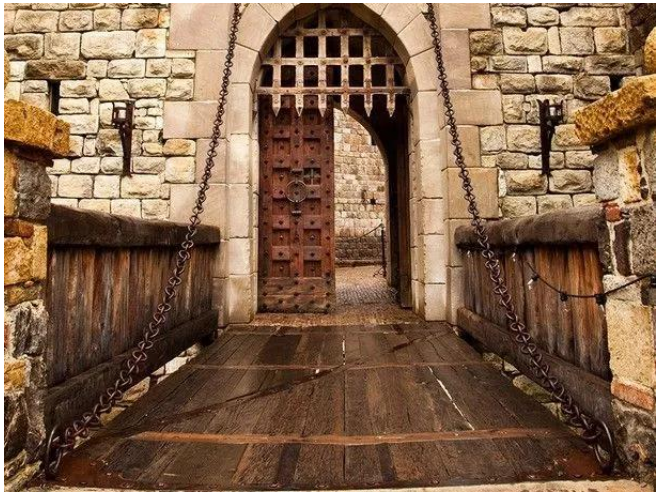
- Dividere in "zone"!
  - Per il concetto di segmentazione della rete può essere utile fare riferimento alla serie di norme IEC 62433, all’interno della quale vengono esplicitati i concetti di ‘’zone’’ (anche dette ‘’celle’’ o ‘’isole’’) e ‘’percorsi’’
  - Una ‘’zona’’ è definita come un insieme di dispositivi 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)



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

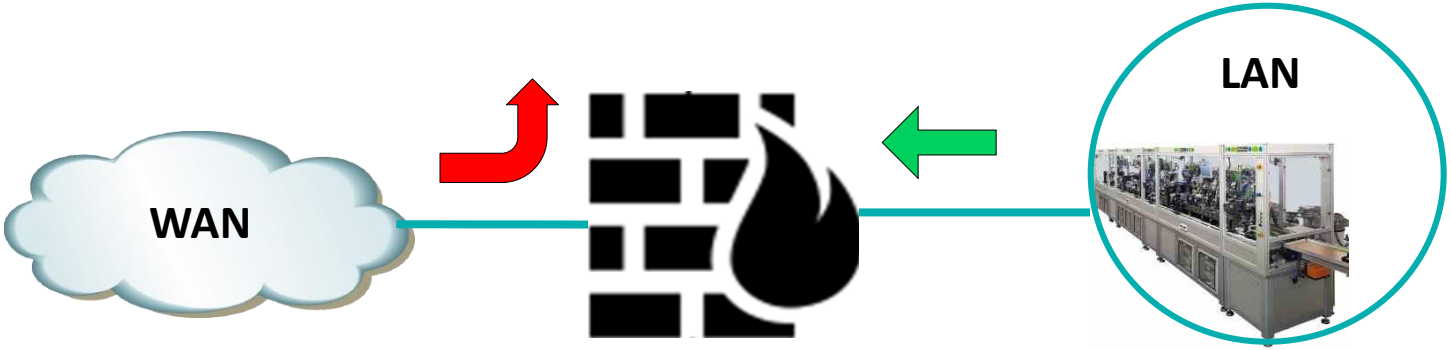
  autorizzato per usare il percorso di comunicazione?
- Il risultato è una struttura degli accessi basata su dei casi d'uso



© CSMT Gestione vietata la riproduzione

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

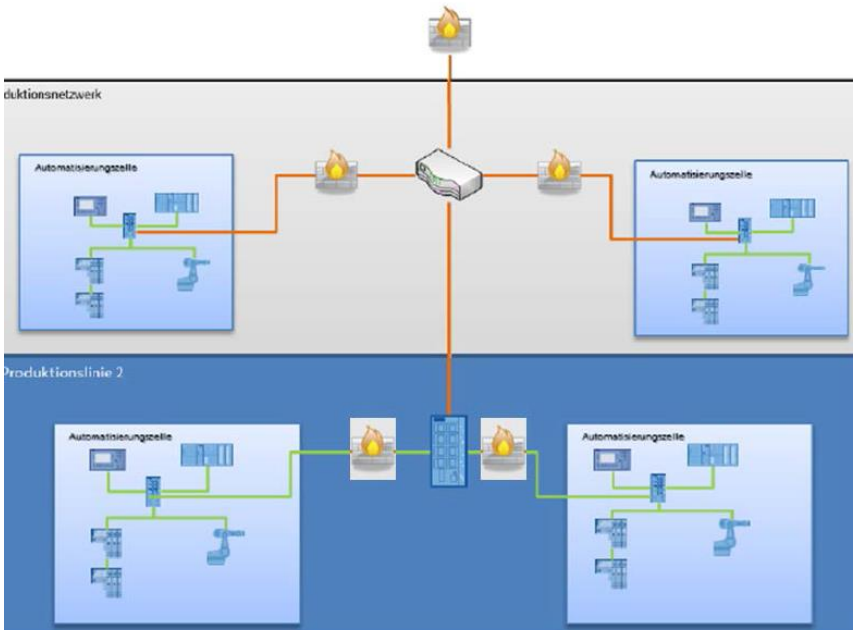


© 2017 PROFIBUS e PROFINET Italia

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



© CSMT Gestione vietata la riproduzione

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

© CSMT Gestione vietata la riproduzione

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….

© CSMT Gestione vietata la riproduzione

Le minacce più trascurate – Switch Managed non configurati

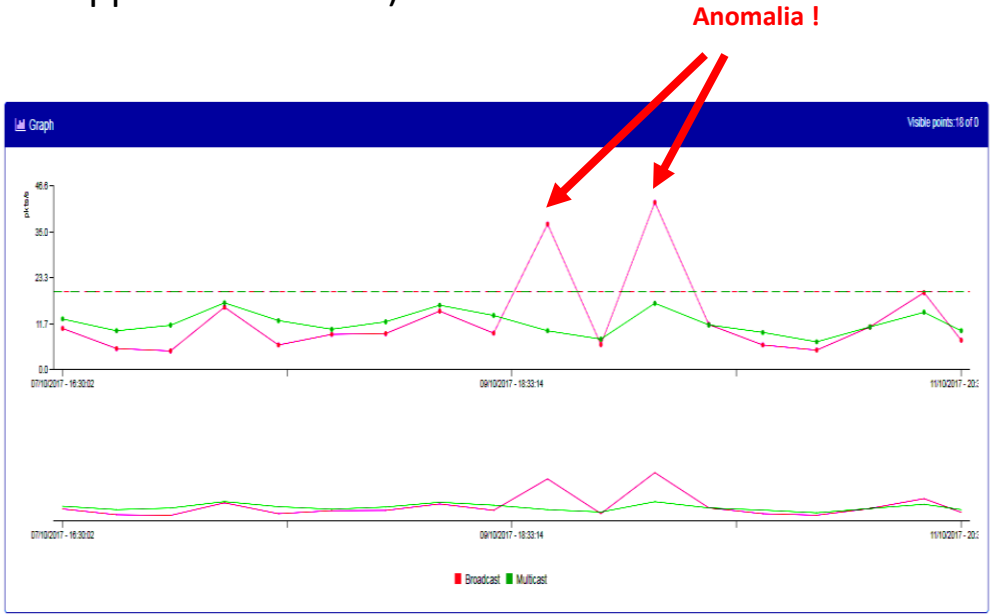
- Switch managed installati in rete ma non configurati
  - Collocati nei cabinet senza prima essere configurati
  - Hanno tutti valori di default, esattamente come sul manuale del costruttore…..

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

© CSMT Gestione vietata la riproduzione

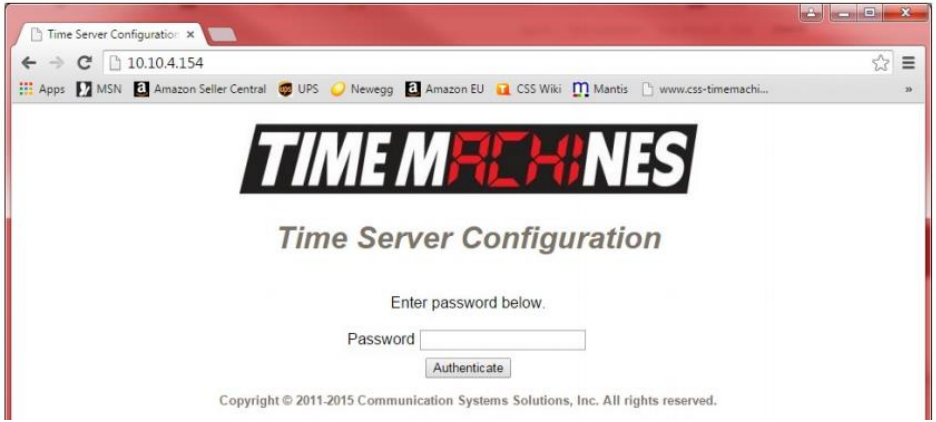
Le minacce più trascurate – attacchi DoS

- 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



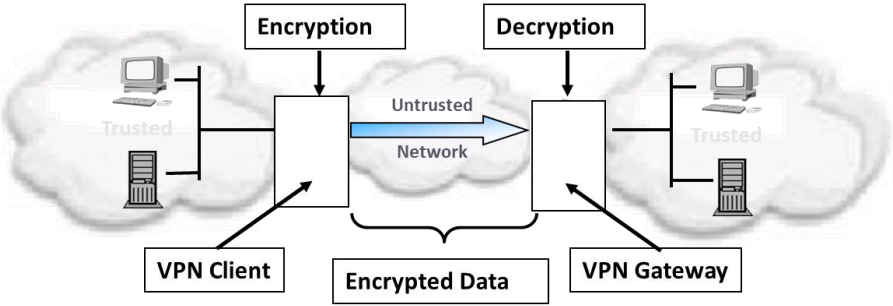
Le minacce più trascurate - interfacce di configurazione

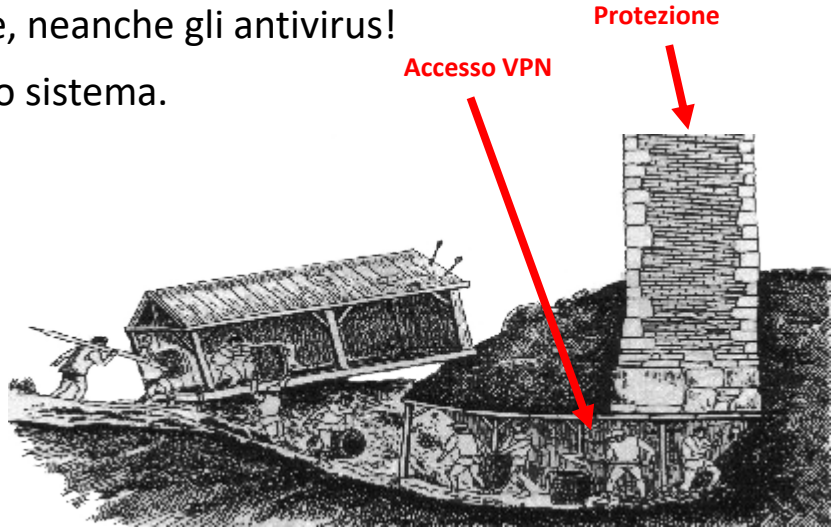
- Tool e protocolli di configurazione dei dispositivi di campo basati su TCP oppure su pagine WEB
  - Spesso con protezioni non attivate o importanti falle di sicurezza
  - Cambiare sempre le password di default
  - Sorvegliare il comportamento del sistema



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.





PI Italia
PROFIBUS • PROFINET

GRAZIE

per l‘attenzione

PROFINET® PROFIBUS® PROFIsafe PROFIenergy PROFIdrive IO-Link FDI