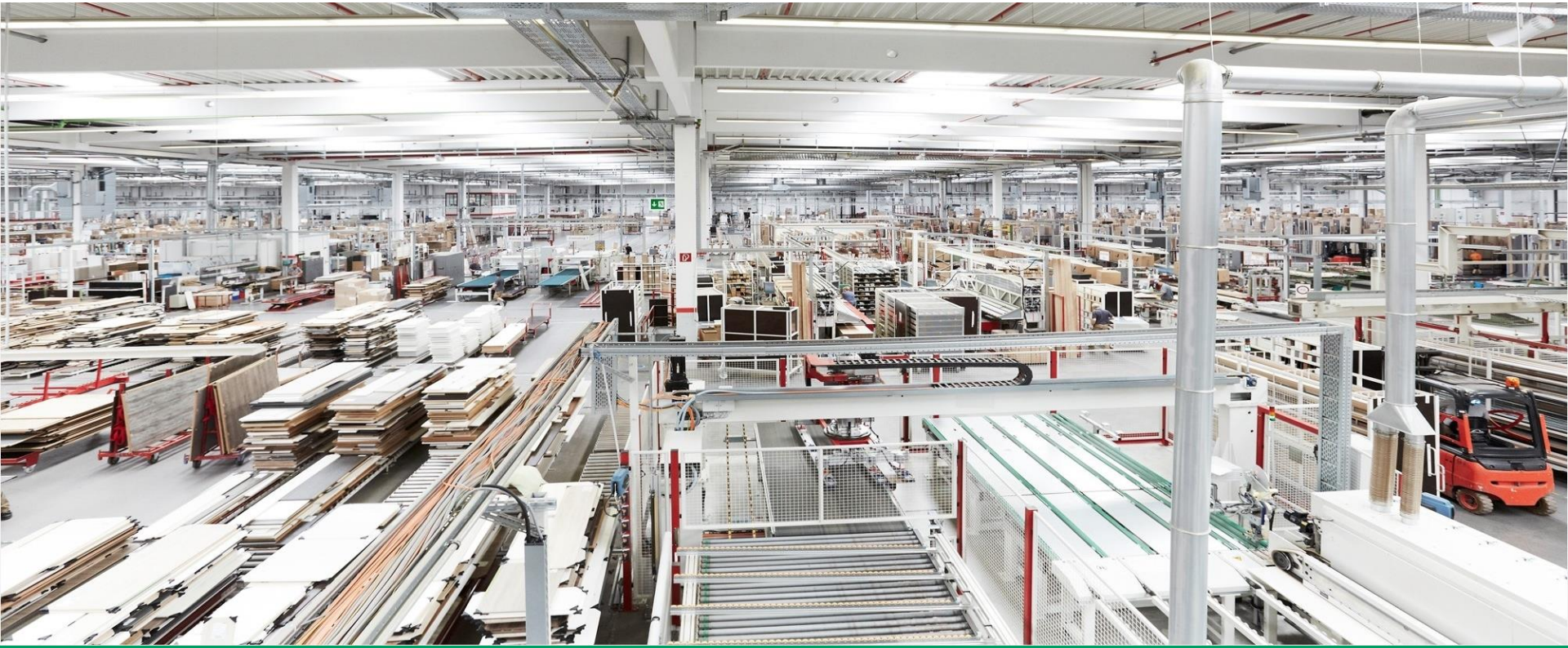
Protezione Cyber-Physical dei Sistemi SCADA ed ICS

Ing. Luigi Morabito
BU Transport & Infrastructure

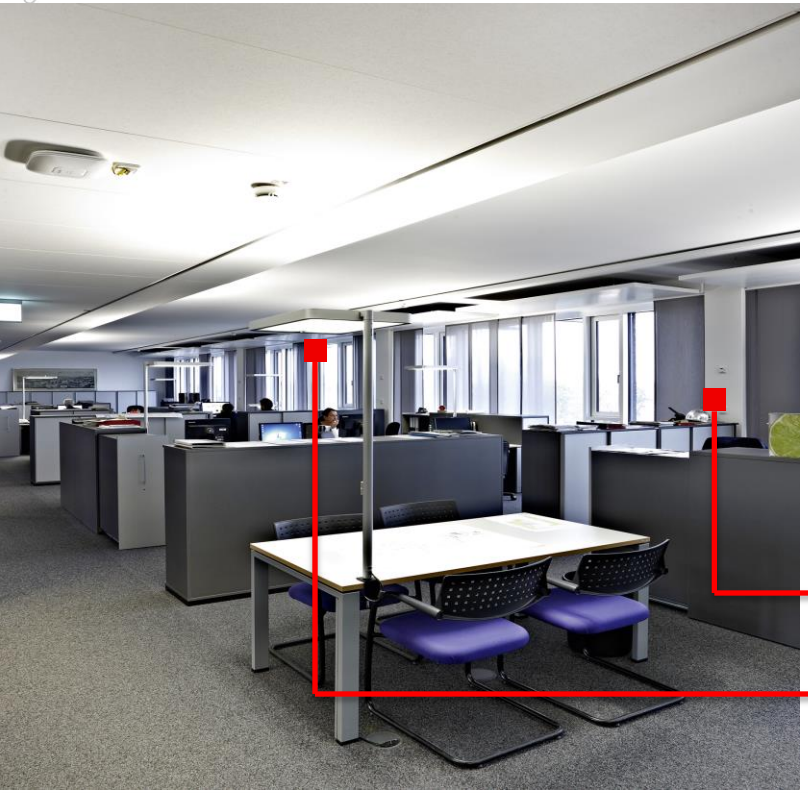
Ing. Mirko Vincenti
Infrastructure & Building Automation Manager

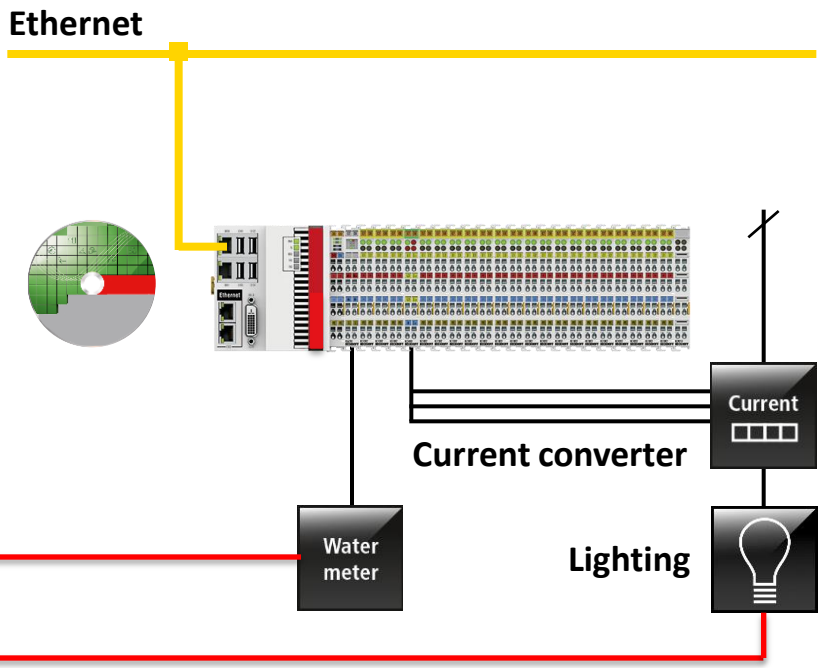
Protezione Cyber-Physical dei Sistemi SCADA e ICS

Problematica che si propaga in tutti gli scenari

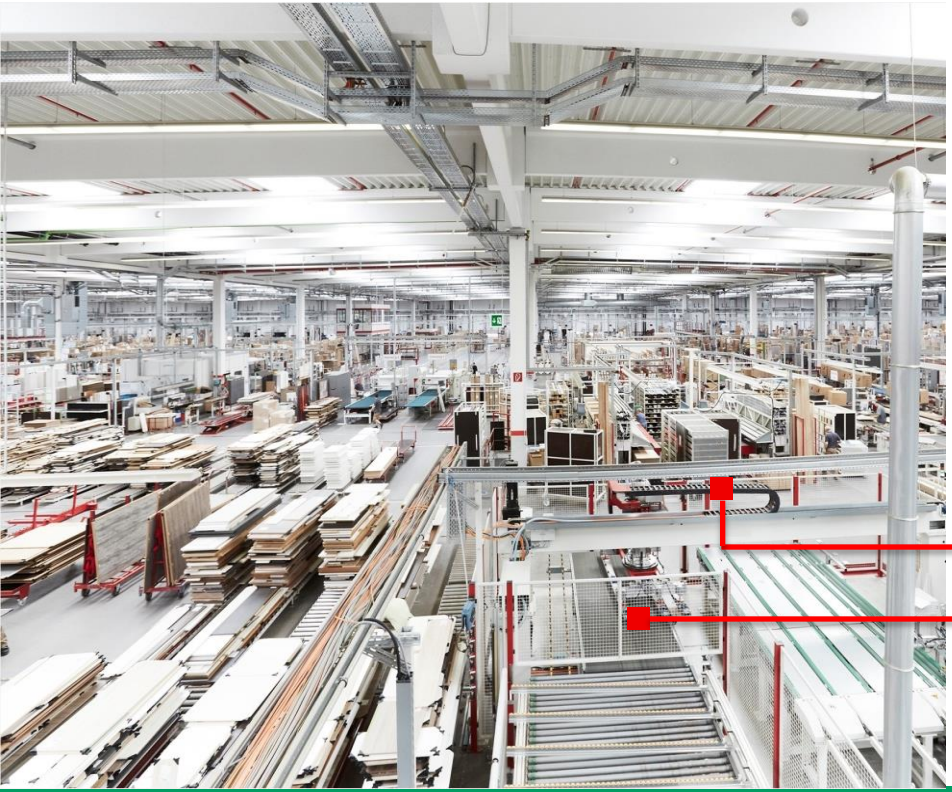


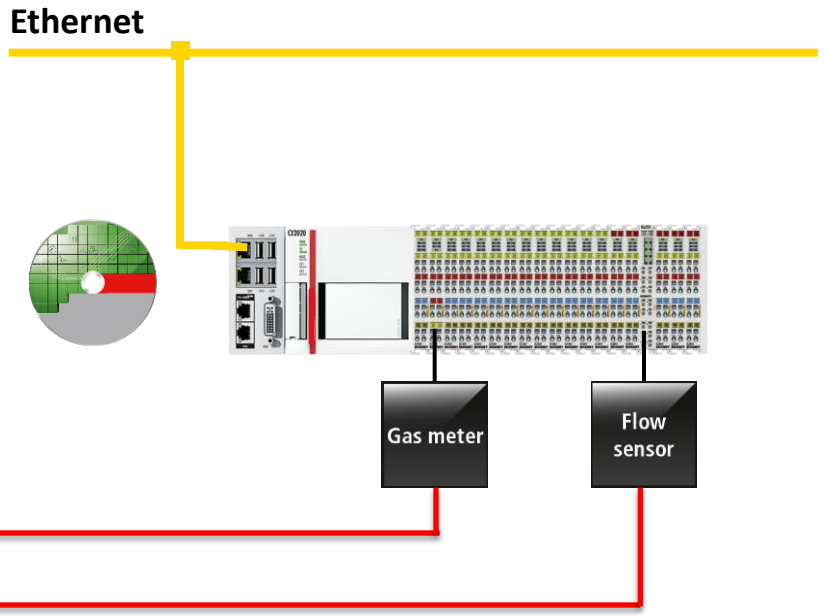
Caso applicativo: edificio amministrativo



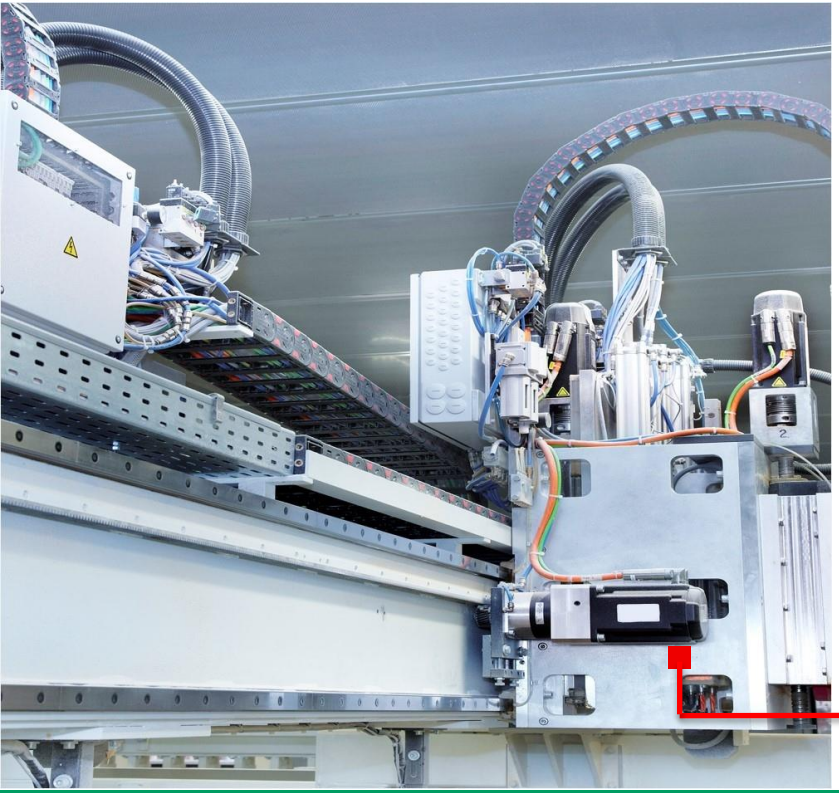


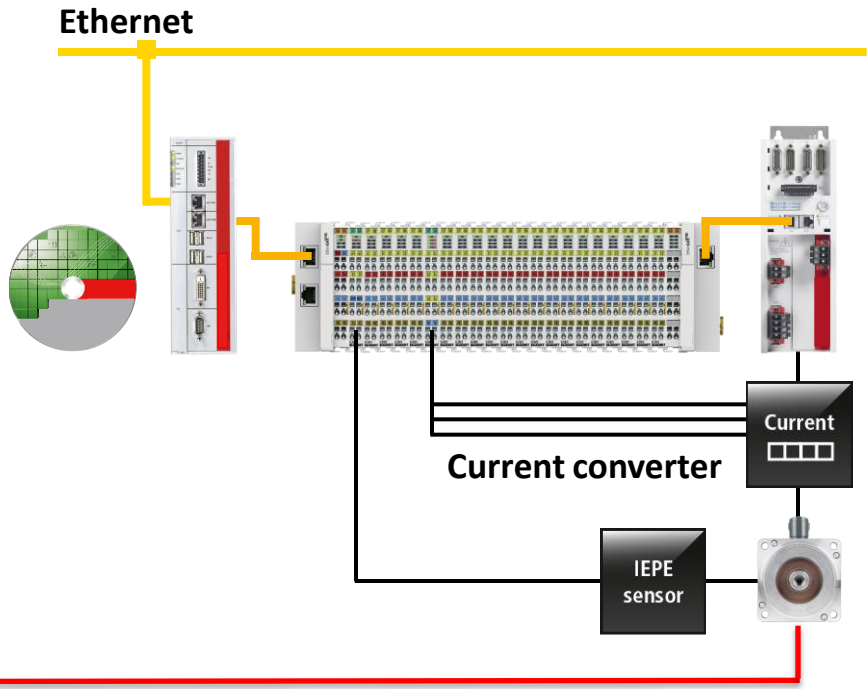
Caso applicativo: impianti di produzione





Caso applicativo: macchine e impianti





Infrastrutture di rete SCADA e OT

Che cos'è? E' un sistema informatico distribuito per il monitoraggio e controllo di sistemi fisici, costituito da:

- sensori che misurano le grandezze da controllare
- attuatori che eseguono i comandi
- una rete di PLC e microcontrollori che acquisiscono i dati dai sensori o direttamente dai dispositivi/impianti
- software che acquisisce, elabora e presenta i dati

Sono sistemi per cui le analisi di funzionamento risultano molto complesse:

- ✓ Elevato numero di protocolli utilizzati, proprietari e non;
- ✓ Verifiche molto complicate, difficoltà nell'ottenere la disponibilità dell'ambiente operativo per i test, con l'aggravante che spesso l'ambiente di test non lo rispecchia in toto.

Sicurezza dei sistemi SCADA

I sistemi SCADA eseguono attività critiche e forniscono servizi essenziali all'interno di infrastrutture che per forza di cose sono diventate “critiche”. Sono considerati oggi dagli analisti parte della spina dorsale di qualsiasi paese.

In origine questi sistemi sono stati progettati per un ambiente con l'unico intento di monitorare in locale i processi senza considerare i requisiti di sicurezza e le necessità di proteggerli da minacce esterne, avendo spesso un ciclo di vita di decenni. Ad oggi molti di questi sistemi operano in un contesto completamente diverso da quello per il quale sono stati progettati. Inoltre, l’infrastruttura di comunicazione può essere locale o distribuita geograficamente.

Le Infrastrutture Critiche, e in particolare i sistemi di controllo, richiedono la protezione da una varietà di minacce informatiche che potrebbero compromettere il loro funzionamento ordinario.

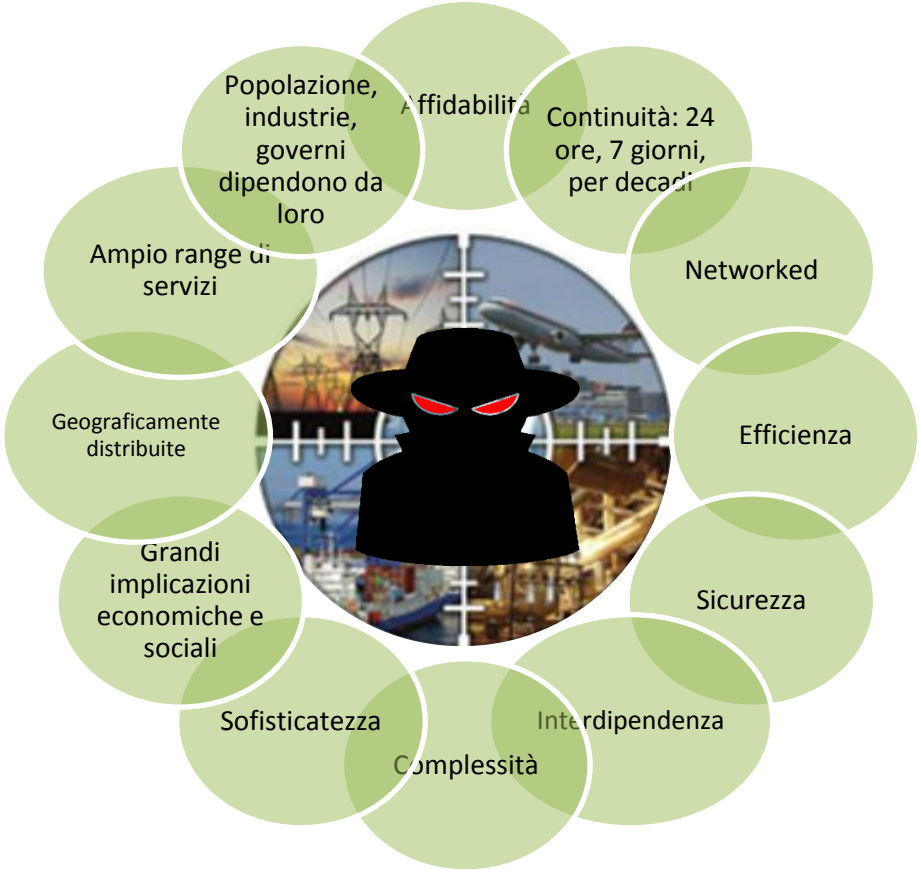
Rischi delle reti SCADA

Quasi tutti gli SCADA sono valutati oggi come affidabili e flessibili, ma mancano spesso di sicurezza. La compromissione delle reti SCADA può causare l'interruzione di servizi critici, processi di reindirizzamento, o la manipolazione dei dati operativi, azioni che potrebbero avere gravi conseguenze.

- ✓ Sistemi e prodotti a supporto dell'ambiente operativo non aggiornati
- ✓ Mancanza di segregazione della rete asservita al sistema SCADA
- ✓ Ambienti di test non adeguati
- ✓ Autenticazione e profilazione
- ✓ Protocolli di comunicazione non sicuri
- ✓ Policy di sicurezza delle macchine non sempre rispettate

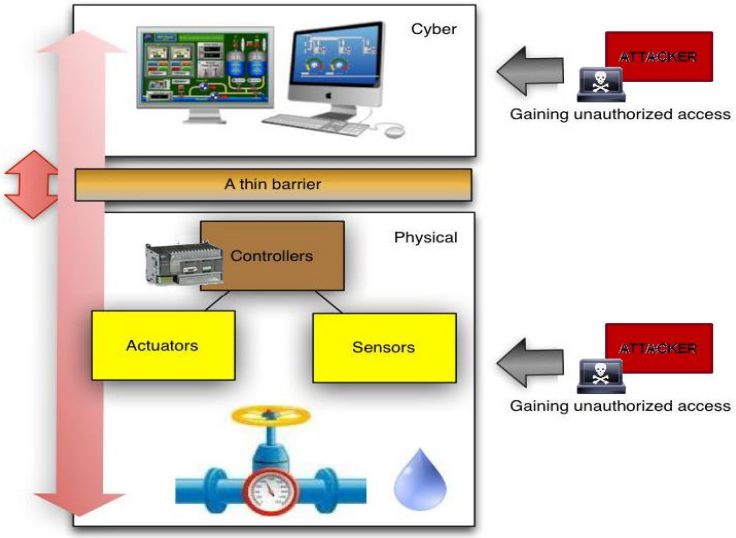
Rischi delle reti SCADA

Le peculiari caratteristiche e i requisiti che devono soddisfare hanno reso le Infrastrutture Critiche ed, in particolare, i sistemi SCADA un bersaglio molto appetibile per vari tipi di attaccanti, da singoli individui cercando di testare le proprie capacità, ad organizzazioni criminali o terroristiche ben strutturate, organizzate, motivate e sovvenzionate, fino a veri e propri Stati.



Vulnerabilità delle reti SCADA

- ✓ Spesso, se il sistema è stato realizzato con prodotti commerciali, il framework alla base del sistema non risulta aggiornato all'ultima versione disponibile.
- ✓ I PLC e le RTU che costituiscono le reti d'acquisizione degli SCADA solitamente utilizzano protocolli di comunicazione che non prevedono alcun meccanismo di sicurezza (autenticazione, crittografia, etc.) e sono quindi fortemente esposti agli attacchi (backdoor, buffer overflow, etc.).
- ✓ In genere, a livello IT, il perimetro è ben protetto, ma vengono molto spesso sottovalutate le minacce che possono nascere all'interno della rete.

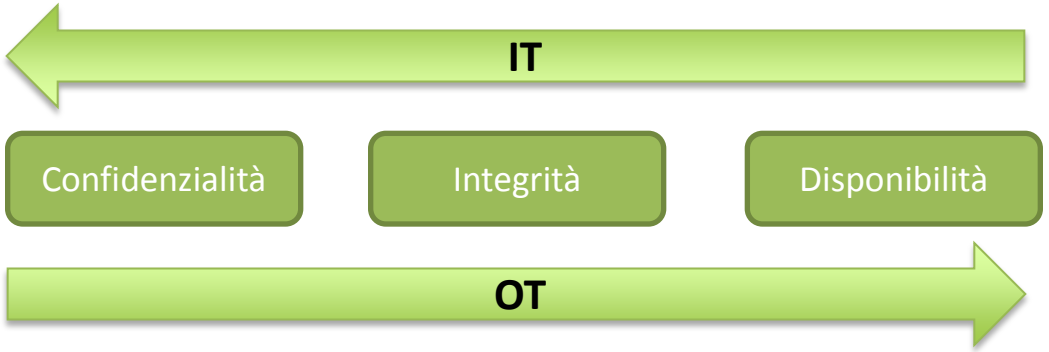


Data la loro stretta relazione, **il dominio fisico e quello cyber non devono essere considerati separatamente** perché la loro interazione crea potenziali vulnerabilità per gli attaccanti ma la loro sinergia potrebbe fornire soluzioni innovative ai Security Manager.

Sicurezza dei sistemi SCADA – OT vs. IT

La sicurezza degli SCADA è ancora oggi in evoluzione, ma e molto più indietro rispetto a quella dei normali sistemi informatici, soprattutto per un motivo specifico: i sistemi informatici classici solitamente gestiscono dati (in sostanza bit), mentre gli SCADA gestiscono impianti (macchine, valvole, interruttori, sistemi complessi) per centrali elettriche, del gas, idroelettriche, stazioni ferroviarie, etc. Quindi, **i processi governati dagli SCADA sono completamente diversi da quelli gestiti dai classici sistemi IT.**

Protezione di una sistema SCADA con un sistema di sicurezza IT → **IMPROPRIO & INSUFFICIENTE**

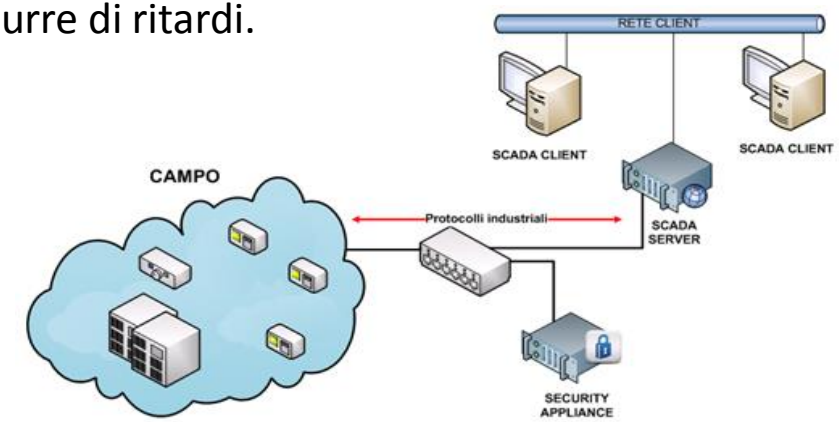


Approccio standard per la protezione SCADA

Molte delle soluzioni ad oggi proposte sul mercato lavorano raccogliendo il traffico di rete da una porta dello switch, su cui viene mirrorato tutto il traffico della rete SCADA.

Questo approccio garantisce:

- Separazione completa dalla rete industriale;
- Una installazione "plug and play" senza alcun blocco sull'operatività;
- Funzionamento in tempo reale senza introdurre di ritardi.



La soluzione per la protezione cyber-physical

Protezione intrinseca

- ✓ Utilizzo di protocolli di comunicazione Client/Server che consentono un elevatissimo livello di sicurezza grazie alla sincronizzazione tra le macchine e l'autenticazione forte con utente/password e firma digitale (e.s., OPC-UA).
- ✓ Generazione autonoma di certificati validi per l'autenticazione Client/Server.
- ✓ Comunicazioni criptate per garantire la protezione e confidenzialità dei dati in transito.
- ✓ Utilizzo di piattaforme software certificate in termini di sicurezza cyber, che rispettino degli standard riconosciuti ed attualizzati (e.s., Common Criteria).
- ✓ Integrazione del controllo di sistemi di sicurezza fisica dell'infrastruttura.

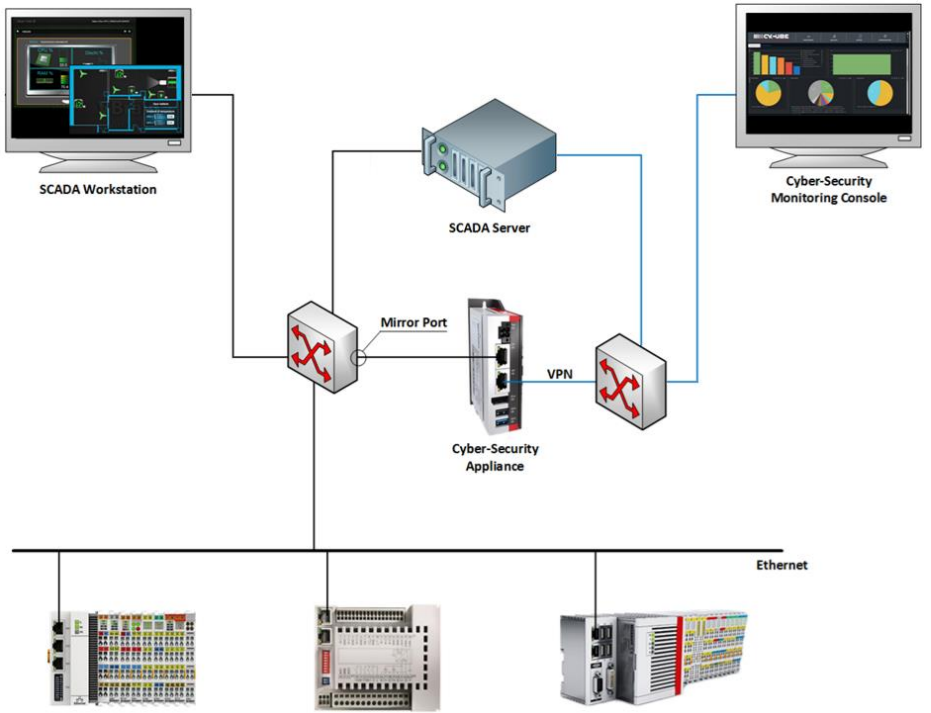
Protezione estrinseca

- ✓ Ecosistema distribuito di appliance per l'analisi del traffico nelle reti PLC, SCADA, business, etc.
- ✓ Fusione tra funzionalità ben note calate sullo scenario applicativo ma trasparenti rispetto alle tecnologie utilizzate, specifico per un'analisi profonda del traffico su vari protocolli.

La soluzione per la protezione cyber-physical

Mirroring: Approccio <u>passivo e non invasivo</u> che consente di non dover sconvolgere la configurazione di rete.

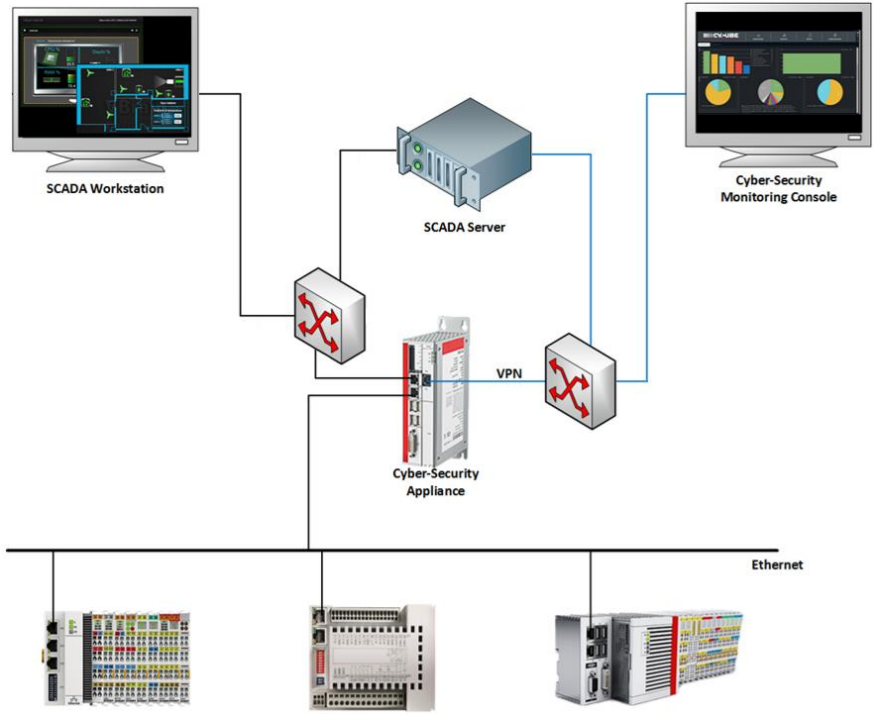
- **Packet sniffing**
- **IDS**
- **Deep packet analysis**
- **Port scan detection**



La soluzione per la protezione cyber-physical

Bridge: Approccio attivo che consente di agire filtrando il traffico ed eventualmente isolando la porzione di rete potenzialmente compromessa.

Firewall
IPS
Deep packet analysis
Port scan detection

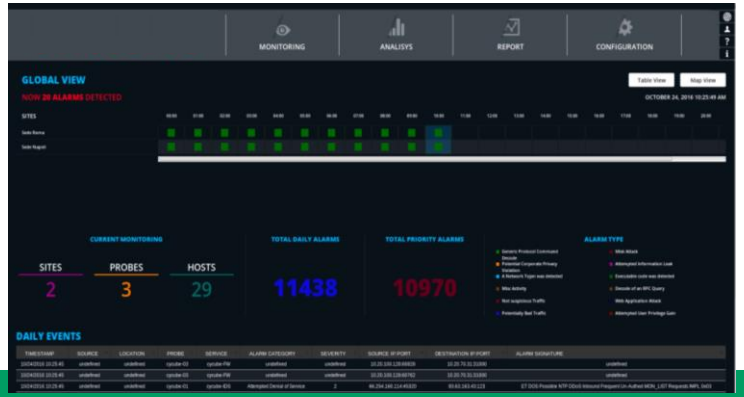


La soluzione per la protezione cyber-physical

La **Console di Monitoraggio** permette la gestione ed il monitoraggio delle varie appliance di cyber-security distribuite sull'impianto.

Rappresenta uno strumento che completa il sistema di Situational Awareness, fornendo in tempo reale tutte le informazioni relative al tipo, gravità e posizione degli attacchi, i dispositivi o impianti colpiti, etc.

Inoltre, dà la possibilità ai Security Operators di aggiornare e gestire in maniera semplice e da remoto le varie appliance di cyber-security.

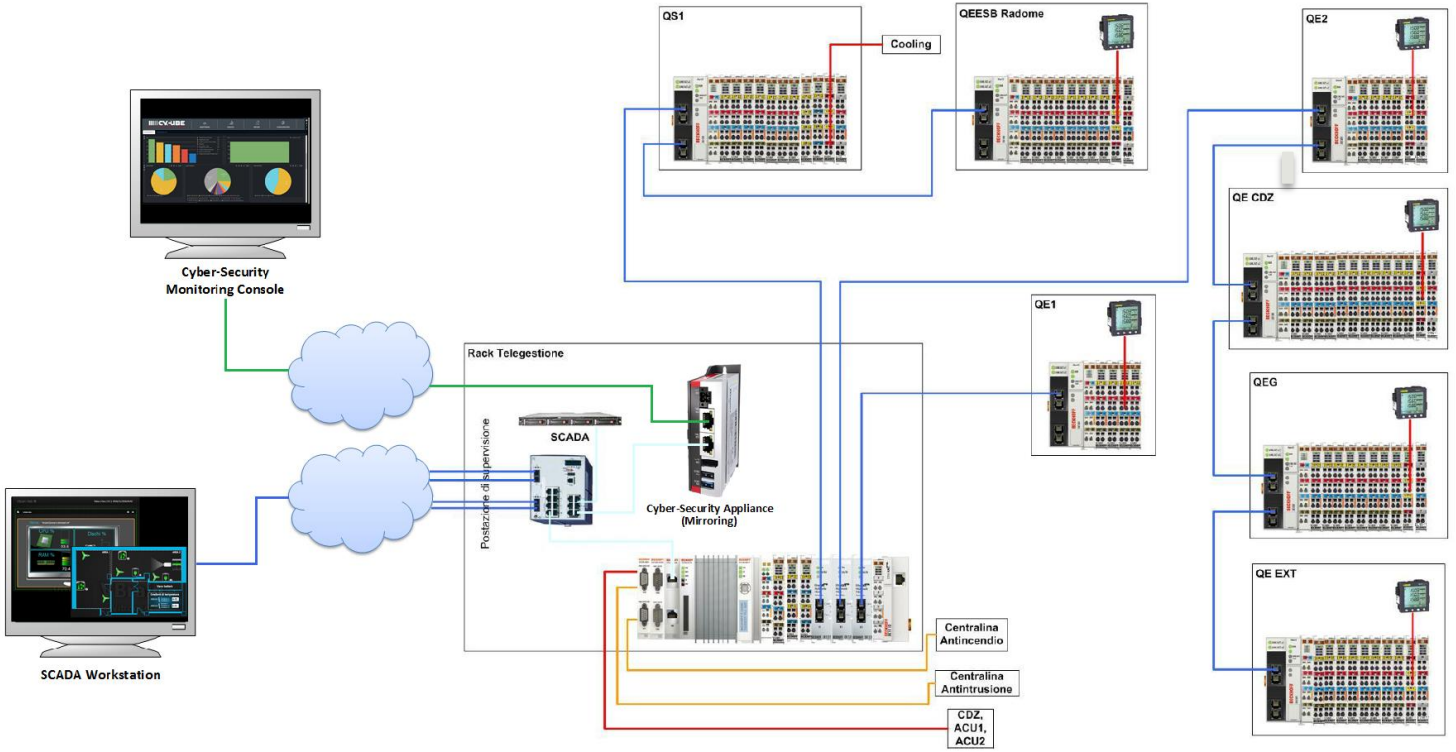


La soluzione per la protezione cyber-physical

- ✓ Fase di apprendimento che consente di creare un profilo di sicurezza perfettamente ritagliato sul sistema da controllare.
- ✓ Controllo a tutti i livelli della pila ISO/OSI, compreso il livello applicativo di molti protocolli.
- ✓ Rappresentazione delle informazioni che permette di mettere in evidenza tutte le comunicazioni presenti sulla rete e di identificare per ognuna un livello di rischio.
- ✓ Interazione tra SOC e sala di controllo che rende più efficiente la gestione del sistema durante l'attivazione delle contromisure.

Caso applicativo

Uso di un Industrial PC per la protezione cyber di un sistema BMS:



Grazie per l’attenzione