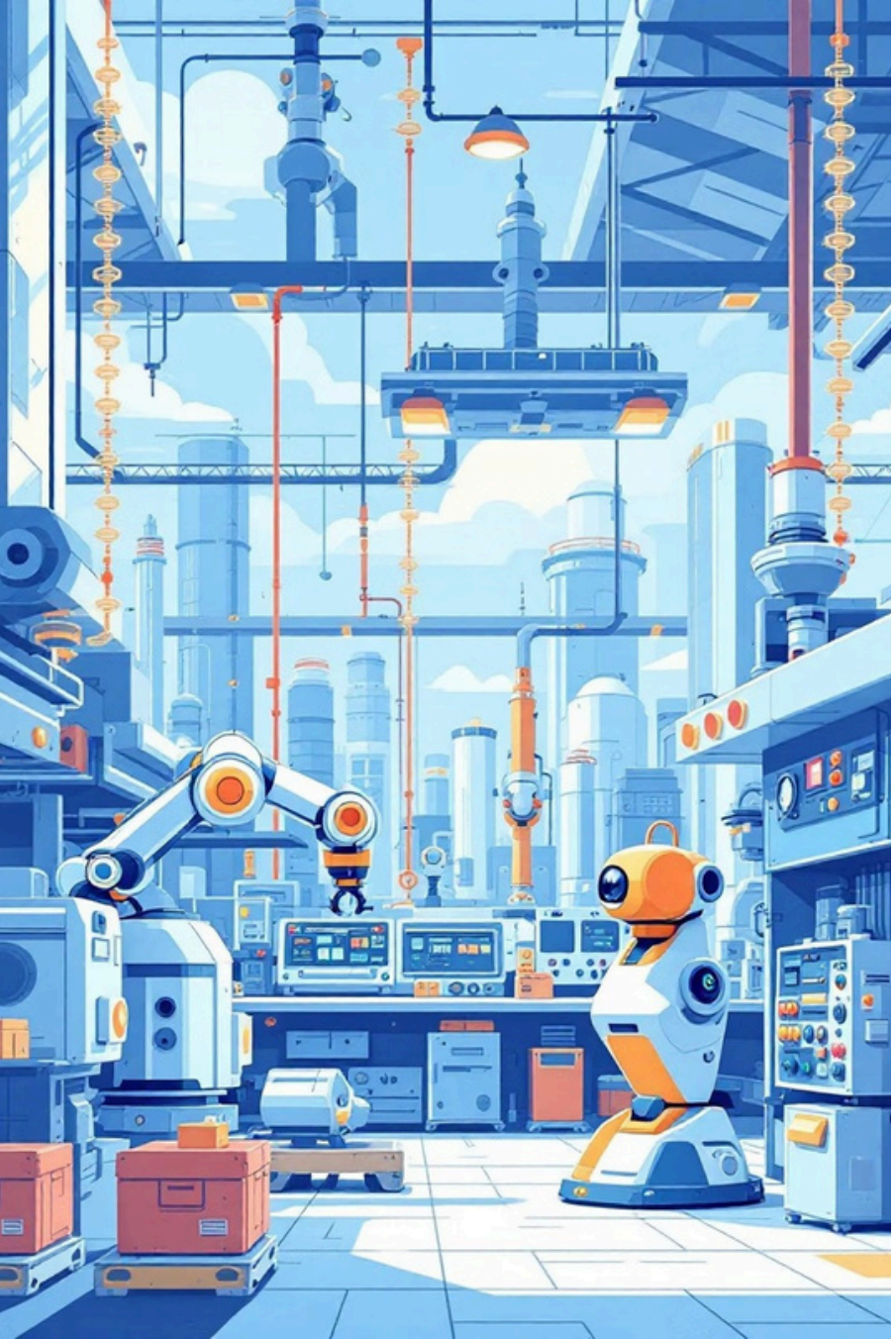
Co-funded by the European Union

Cyber-In

WP3- CASCADE TRAINING ITALY
PROGETTO CYBER - IN

Novembre 2025

ECOLE - AFGP PIAMARTA



Sessione 1

Cyber-In

Cos'è un PLC e perché è fondamentale nell'automazione industriale

Una panoramica completa sui controllori logici programmabili,la cybersecurity negli ambientiindustriali e l'importanza della segmentazione di rete per proteggere i sistemi critici.

Definizione e Funzionamento Sommario del PLC

Cos'è un PLC

PLC=Programmable Logic Controller, un dispositivo elettronico programmabile che controlla macchinari e processi industriali in tempo reale.

Come Funziona

Riceve input da sensori, elabora istruzioni secondo la logica programmata e comanda attuatori per automatizzare operazioni complesse.

Evoluzione Storica

Nato neglianni '60 per sostituire i sistemi a relè, oggi è il cuore dell'Industria 4.0 con capacità avanzate come IoT e integrazione AI.

Evoluzione e Vulnerabilità dei PLC Moderni

Trasformazione Digitale

Dagli anni '60 oggi: da sistemi semplici isolati a dispositivi intelligenti connessi in rete e integrati con sistemi IT aziendali.

Questa **connettività aumenta la superficie di attacco**: molti PLC sono ancora privi di protocolli di sicurezza nativi adeguati.

Sfide di Sicurezza

Gli aggiornamenti software sono difficili da implementare perché fermare la produzione anche per poche ore comporta costi elevati.

I sistemi legacy operano spesso con software obsoleti e vulnerabilità note non corrette.

Cyber-In

Cyber-In

Il cervello dell'automazione industriale

Schema concettuale: i sensori rilevano condizioni fisiche (temperatura, pressione, posizione), il PLC elabora le informazioni secondo la logica programmata e gli attuatori eseguono le azioni (motori, valvole, cilindri pneumatici).

Cyber-In

Cybersecurity in Ambienti IT e OT: Cosa Significa?

Information Technology (IT)

Gestione di dati, reti aziendali e sistemi informatici. Focus su confidenzialità, integrità e disponibilità delle informazioni digitali. **(PRIVACY)**

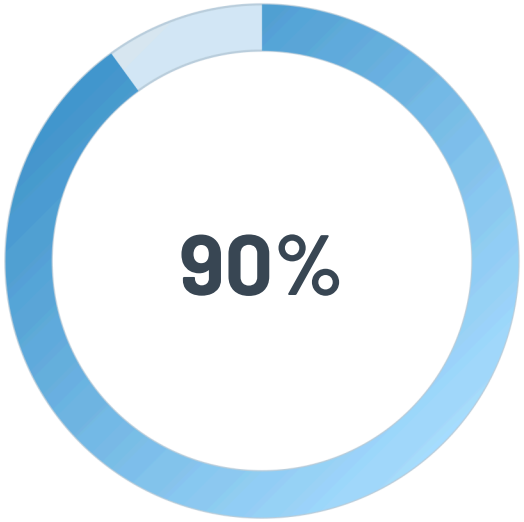
Operational Technology (OT)

Hardwaree software che controllano processi fisici industriali (es. PLC, SCADA, DCS). (Priorità alla continuità operativa e **sicurezza fisica**).

Cybersecurity

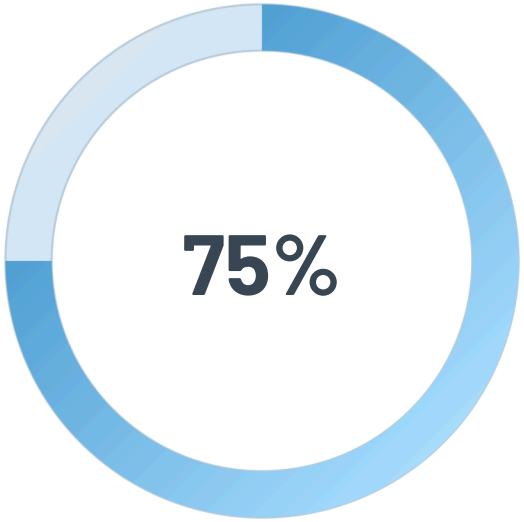
Protezione di dispositivi, reti e dati da attacchi informatici che possono causare danni economici, interruzioni operative e rischi per la sicurezza umana.

Perché la Cybersecurity OT è Critica



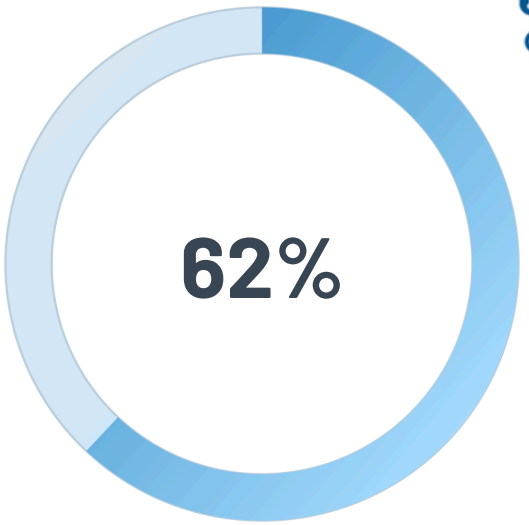
Aziende Colpite

Delle aziende consistemi OT hanno subito incidenti di sicurezza negli ultimi 2 anni



Costi Elevati

Dei fermiproduzione causati da attacchi cyber costano oltre ¬500K



Rischi Fisici

Degli incidenti OT comportano potenziali rischi per la sicurezza del personale

---

Gli attacchi a PLC o sistemi OT possono fermare impianti, danneggiare macchinari o mettere a rischio la sicurezza umana. La **convergenza IT-OT** espone i sistemi industriali a nuove minacce informatiche precedentemente limitate ai soli ambienti informatici.

Principali Minacce ai PLC e Sistemi OT

Malware e Ransomware

Software malevolo che blocca, manipola o cripta i processi industriali richiedendo riscatti. Esempi: Stuxnet, WannaCry.

Accessi Non Autorizzati

Infiltrazione tramite password deboli, credenziali predefinite non modificate o vulnerabilità software non patchate.

Attacchi DoS/DDoS

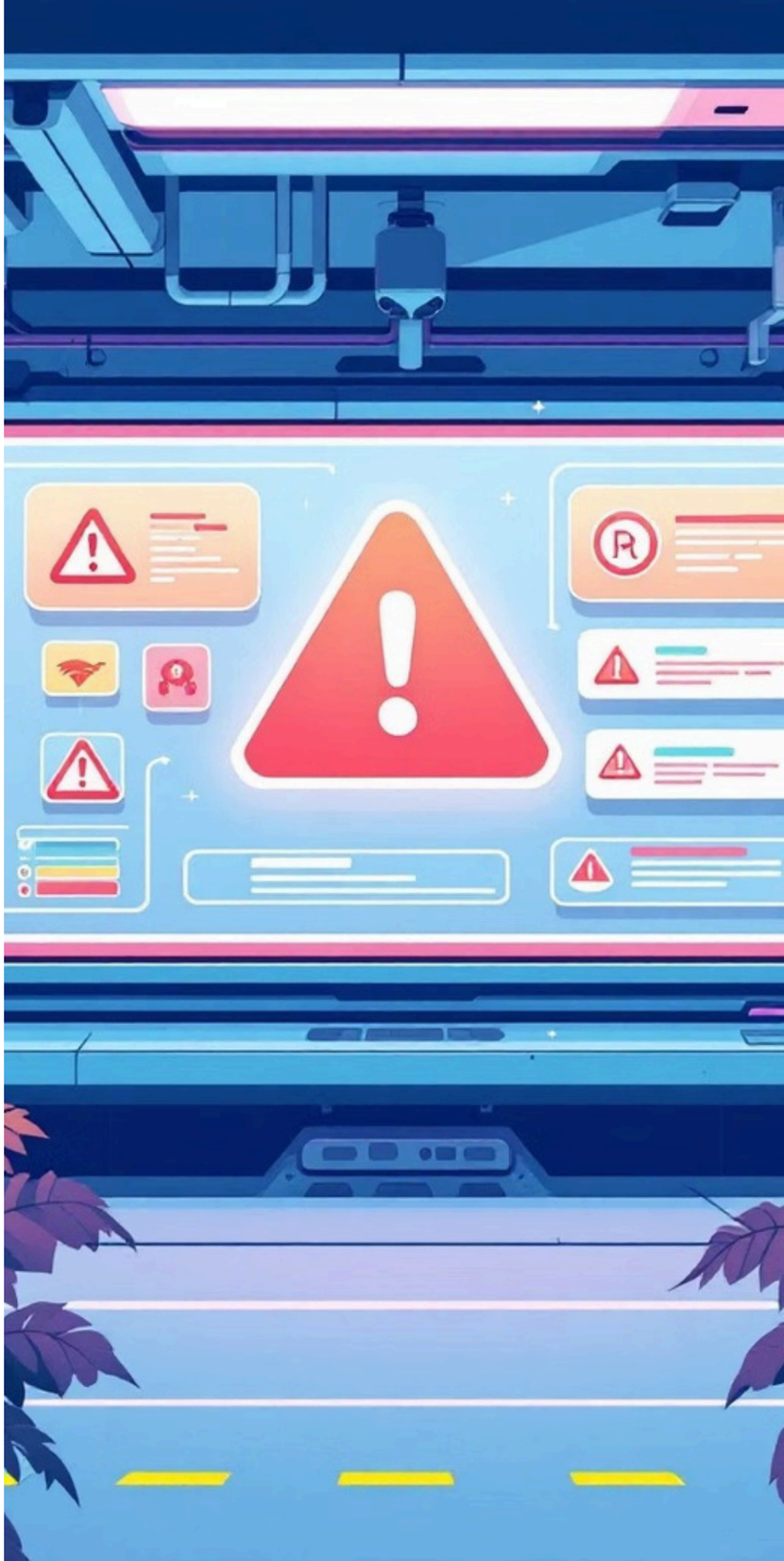
Sovraccarico dei sistemi che blocca la comunicazione tra PLC e dispositivi, causando interruzioni operative critiche.

DoS (Denial-of-Service) mira a bloccare un servizio web

DDoS (Distributed Denial-of-Service) utilizza molteplici fonti (spesso una rete di dispositivi compromessi, chiamata botnet) per sopraffare il bersaglio con un volume di traffico molto più elevato e piùdifficile dacontrastare.

Errore Umano e Phishing

Email fraudolente e ingegneria sociale che ingannano operatori, aprendo la porta agli hacker nei sistemi industriali.



Segmentazione di Rete: La Frontiera della Sicurezza OT

Principi Fondamentali

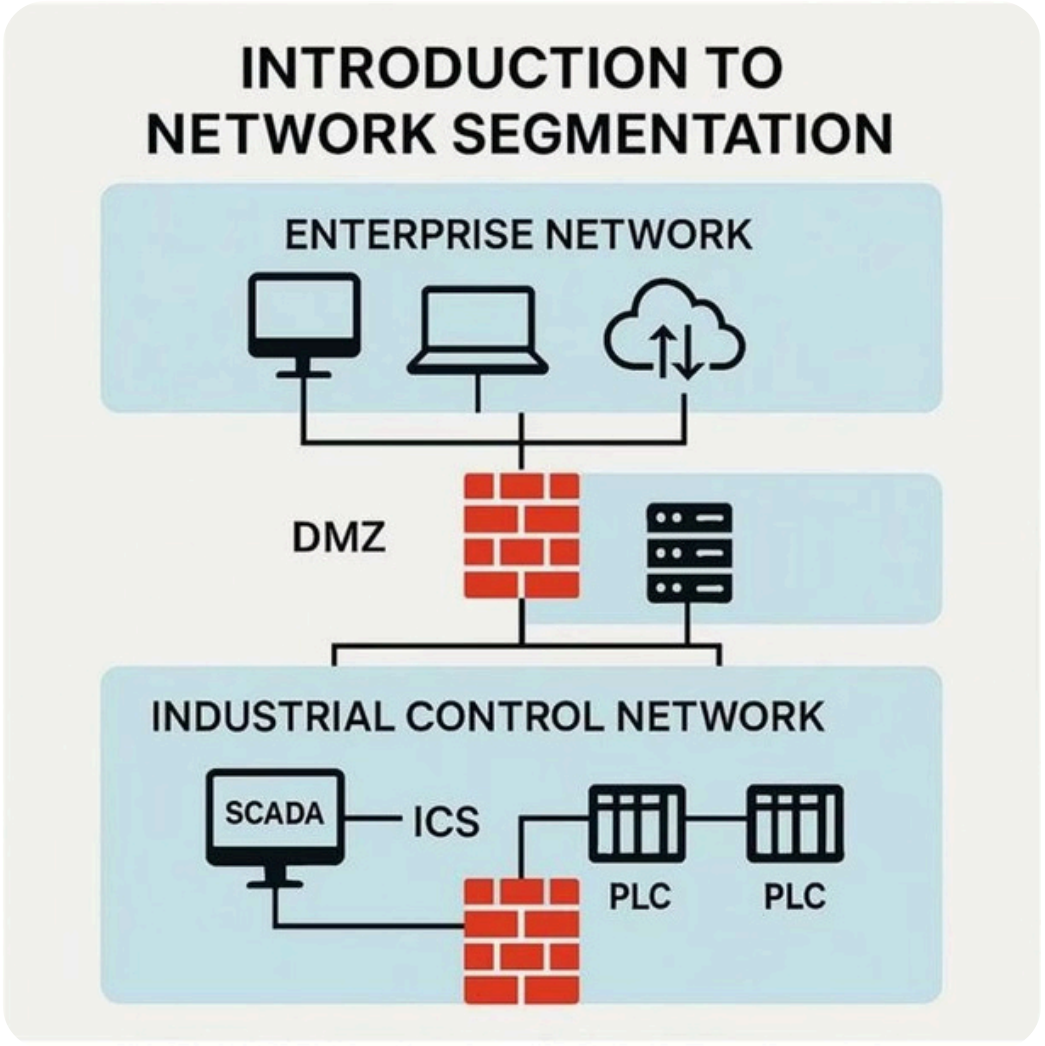
Separare fisicamente e logicamente le reti OT da quelle IT e da internet per **limitare la superficie di attacco**.

Implementazione di zone di sicurezza con livelli crescenti di protezione.

Strumenti e Tecnologie

- Firewall industriali con regole specifiche per protocolli OT
- Gateway unidirezionali (data diodes) per flussi controllati
- DMZ (Demilitarized Zone) tra IT e OT
- Controlli di accesso rigorosi basati su ruoli
- Monitoraggio continuo del traffico di rete

La segmentazione riduce drasticamente il rischio di propagazione laterale degli attacchi e isola i sistemi critici dalle minacce esterne.



Concetti chiave: " Isolamento logico e fisico: l'isolamento logico utilizza VLAN, mentre la segmentazione fisica utilizza hardware separato. La scelta dipende dalla criticità del sistema, dalla tolleranza al rischio e dai requisiti operativi. "

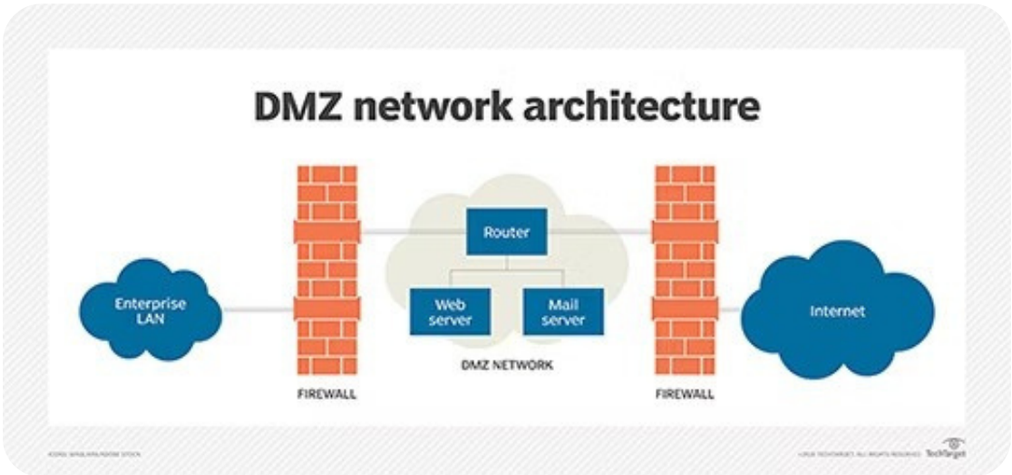
Controllo degli accessi tra segmenti: gateway, firewall ed elenchi di controllo degli accessi (ACL) vengono utilizzati per applicare rigide policy di comunicazione e garantire che solo il traffico autorizzato possa spostarsi tra le zone. "

Difesa in profondità: la segmentazione supporta la sicurezza a strati separando i diversi zone in base alla funzione, al livello di esposizione e al livello di fiducia. "

Microsegmentazione: nelle implementazioni più avanzate, la segmentazione può avvenire a livello di applicazione o di carico di lavoro, riducendo ulteriormente la superficie di attacco.

Cyber-In

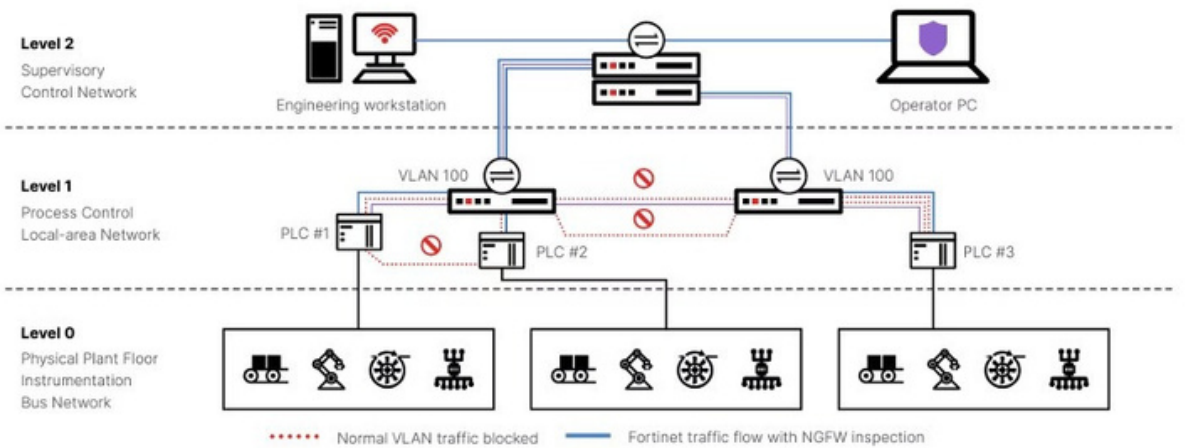
Che cos’è una rete DMZ?



Una DMZ o zona demilitarizzata è una rete perimetrale che protegge e aggiunge un ulteriore livello di sicurezza alla rete locale interna di un’azienda dal traffico non attendibile.

L’obiettivo finale di una DMZ è consentire a un'azienda di accedere a reti non attendibili, come Internet, garantendo al contempo che la sua rete privata o LAN rimanga sicura. Le organizzazioni in genere archiviano nella DMZ servizi e risorse rivolti verso l’esterno, nonché server per il **Domain Name System (DNS),** il **File Transfer Protocol (FTP),** la posta, il proxy, il Voice over Internet Protocol (VoIP) e i server Web.

Questi server e risorse sono isolati e dispongono di un accesso limitato alla rete LAN, per garantire che sia possibile accedervi tramite Internet, ma la LAN interna non può farlo. Di conseguenza, un approccio DMZ rende più difficile per un hacker ottenere l9accesso diretto ai dati e ai server interni di un9azienda tramite Internet. Un’azienda può ridurre al minimo le vulnerabilità della sua rete locale, creando un ambiente sicuro dalle minacce e garantendo al contempo che i dipendenti possano comunicare in modo efficiente e condividere informazioni direttamente tramite una connessione sicura.



Vantaggi della segmentazione della rete:

- **Contenimento degli attacchi:** impedisce a malware, ransomware o intrusi di muoversi lateralmente attraverso la rete.
- **Visibilità e monitoraggio migliorati:** ogni segmento può essere monitorato in modo indipendente, consentendo un rilevamento e una risposta alle minacce più accurati.
- **Applicazione granulare delle policy:** i segmenti consentono agli amministratori di applicare policy univoche regole per diversi tipi di traffico e sistemi.
- **Conformità semplificata:** la segmentazione è in linea con i quadri normativi e le normative di settore come NIST 800-82, ISA/IEC 62443 e ISO 27001

Segmentazione: barriera tra IT e OT

Internet

Ambiente esterno non affidabile

Firewall & DMZ

Zona demilitarizzata di controllo

Rete IT

Sistemi informativi aziendali

Gateway Sicuro

Controllo accessi rigido

Rete OT

Sistemi di controllo industriale

Conclusione: Proteggere il Futuro dell'Automazione

Centralità dei PLC

I PLC sono il cuore pulsante dell'industria moderna, ma la loro sicurezza è spesso trascurata o sottovalutata.

Difesa Strategica

Cybersecurity e segmentazione sono strumenti essenziali per garantire continuità operativa, sicurezza e affidabilità dei processi.

Investimento Necessario

Formazione continua del personale, monitoraggio proattivo e strategie di difesa a più livelli sono la chiave per un'industria resiliente e sicura.

> "La sicurezza OT non è un costo, ma un investimento nella continuità e nel futuro della produzione industriale."

Co-funded by the European Union