Cybersecurity OT: proteggere le Infrastrutture Critiche nell'era delle minacce persistenti

Omar Morando | Director of Cybersecurity OT, *EY Technology Consulting*
Chiara Ciurleo | Consigliere AIEA, *EY Technology Consulting*

Chiara Ciurleo
Consigliere AIEA,
Director EY Technology Consulting - Cybersecurity

Director nella practice di Cyber Security e Digital Protection di EY, a partire dal 2014 si occupa di attività in ambito Sicurezza delle informazioni e Data Protection con particolare focus sul mondo Security governance, risk e compliance. Responsabile di numerosi progetti nell'ambito della valutazione e gestione dei rischi IT&Security, di Audit nonché attività di Compliance Normativa sia per i Clienti della Pubblica Amministrazione che del Settore Privato, è membro del Consiglio Direttivo di AIEA dal 2022 e impegnata nell'erogazione delle attività dell'Associazione stessa.

AIEA - Associazione Italiana Information Systems Auditors – Chi siamo?

L' **Associazione Italiana Information Systems Auditors (AIEA),** fin da subito affiliata ad **ISACA,** è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

Promuovere un processo di **sensibilizzazione di tutti i livelli organizzativi** aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi

Ampliare la conoscenza ed esperienza dei suoi oltre 1000 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, **favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti**

Promuovere a livello nazionale la **partecipazione alle certificazioni** CISA, CISM, CRISC, CDPSE, CGEIT, COBIT, CCAK, CSX, CET e ITCA

AIEA - Associazione Italiana Information Systems Auditors – Le Iniziative

L´Associazione organizza le "**SESSIONI DI STUDIO**" su temi emergenti e/o d'attualità per i soci e per alcuni Ospiti portati dai soci. Tale sessioni rilasciano CPE per le certificazioni ISACA.

AIEA fornisce tramite AIEA **Formazione** sia cosi relativamente alle certificazioni ed agli standard sviluppati da ISACA, sia relativamente alle principali certificazioni e competenze necessarie per la pratica quotidiana dei professionisti chiamati a gestire l'IT o a governarne i requisiti di audit, compliance e sicurezza in organizzazioni complesse..

Il **convegno nazionale** dei propri associati, aperto anche ad esterni, che si sviluppa in più giornate ha, ogni anno, un tema principale di riferimento ed ospita relatori, anche stranieri, del mondo accademico, dell'industria e dei servizi.
.

Link Utili:

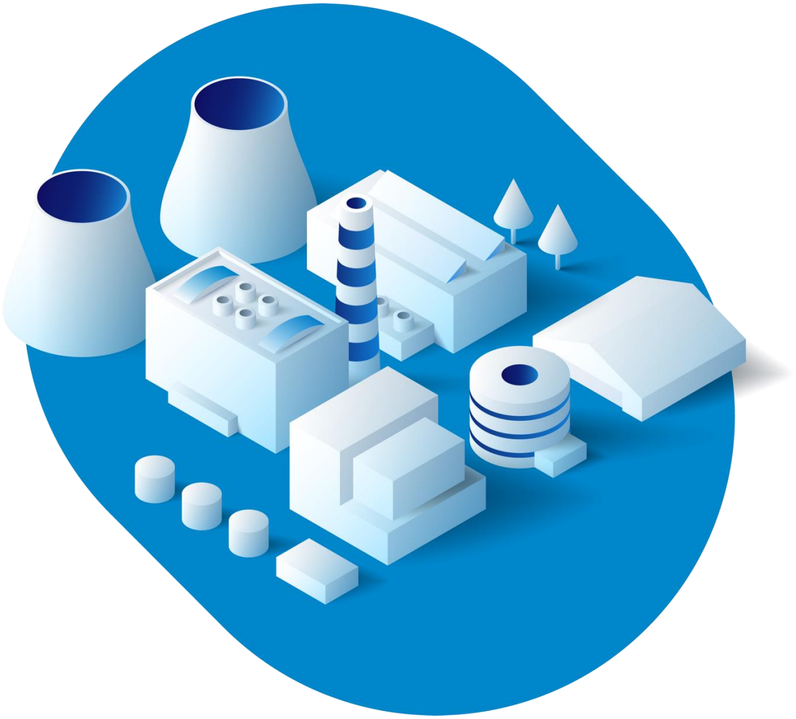
Sito AIEA: https://aiea.it/
Porale Sessioni Studio: https://portale.aiea.jed.st/
Linkedin: https://www.linkedin.com/company/aiea-associazione-italiana-information-systems-auditors/

Omar Morando
Director of Cybersecurity OT – EY Advisory SpA

- Esperto di cybersecurity OT, ricercatore, consulente e formatore.
- Oltre 20 anni di esperienza nel dominio dell'Automazione Industriale (SCADA, PLC, I/O remoto, fieldbus, reti).
- Cybersecurity Automotive applicata ai veicoli connessi.
- Relatore a conferenze italiane e internazionali, tra cui CSET, HackInBo, BSides, BlackHat Europe, SANS ICS Summit sulle tecniche offensive nel dominio OT.
- Blue team in esercitazioni internazionali di cybersecurity, supportando varie agenzie governative nella protezione delle Infrastrutture Critiche.

Perché parliamo di cybersecurity OT?

- I sistemi ICS sono ormai diventati un facile target degli APT!
- **Scopo?** Stabilità economica e sicurezza nazionale. Danni a strutture e persone.
- **Quali target?** Energia, trasporti, telecomunicazioni, trattamento acque e settore manifatturiero.



Non c’è soltanto…

Lo scenario continua a peggiorare

2016

Industroyer (CrashOverride)
Considerato uno dei primi malware specificamente progettati per attaccare le reti di distribuzione elettrica.

2017

Triton (Trisis)
Malware che ha come target i sistemi di protezione (SIS).

WannaCry
Pur non essendo rivolto esclusivamente all'OT ha avuto un impatto globale su diversi settori, compreso quello ospedaliero.

2018

VPNFilter
Malware sofisticato che ha colpito router e dispositivi di archiviazione, ha colpito anche i sistemi OT tramite dispositivi di rete infetti.

2019

LockerGoga
Ransomware che ha colpito le Industrie manifatturiere, tra cui Norsk Hydro.

2020

Ekans (Snake)
Malware ransomware progettato per i sistemi OT, in grado di interrompere i processi correlati a ICS prima di crittografare i file.

2022

Incontroller (Pipedream)
Malware sofisticato che prende di mira i sistemi ICS e le infrastrutture critiche.

Industroyer V2
Versione aggiornata e più sofisticata del suo predecessore.

2023

Gopuram
Malware di tipo backdoor che ha compromesso telecomunicazioni, enti governativi e aziende delle criptovalute.

Cosa c’è in un sistema ICS?

Sensori e Attuatori

Effettuano misurazioni di grandezze fisiche e agiscono direttamente nella catena produttiva.

Microcontrollore o PLC

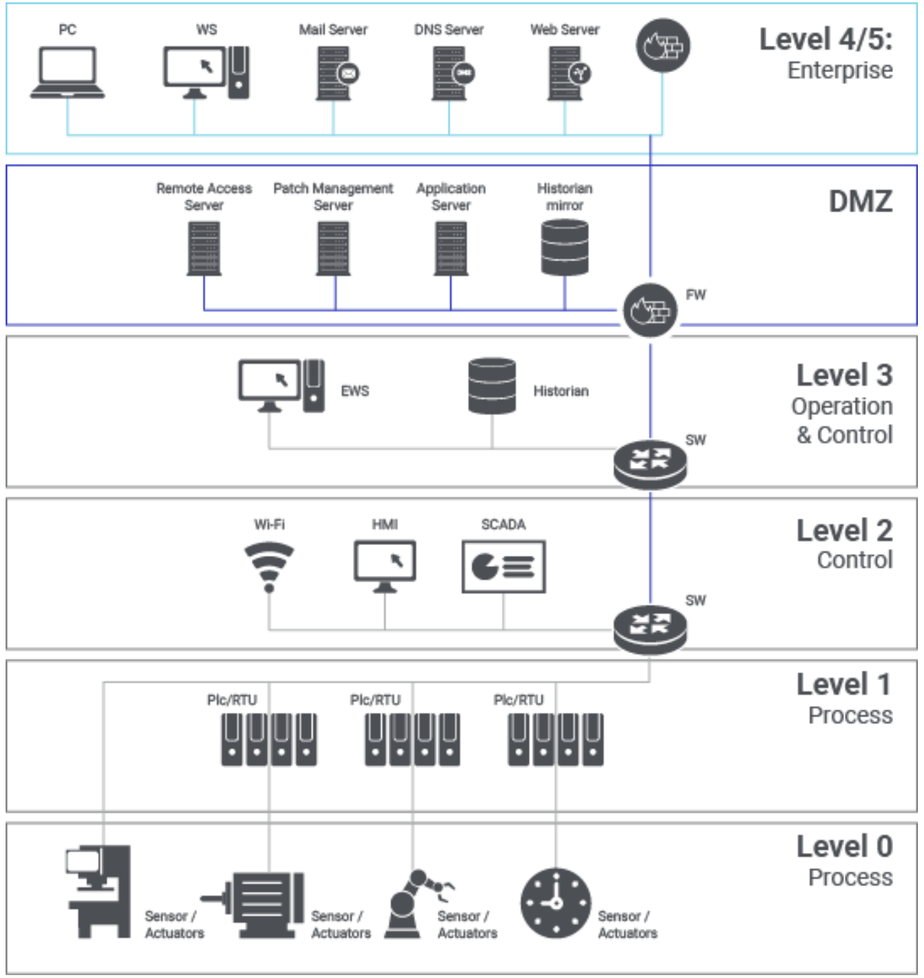
Ricevono dati dai sensori, azionano gli attuatori, comunicano con altri dispositivi (ad esempio PLC, HMI, SCADA, data logger).

HMI

Comunica con il PLC locale e consente all'operatore di visualizzare e immettere dati e comandi.

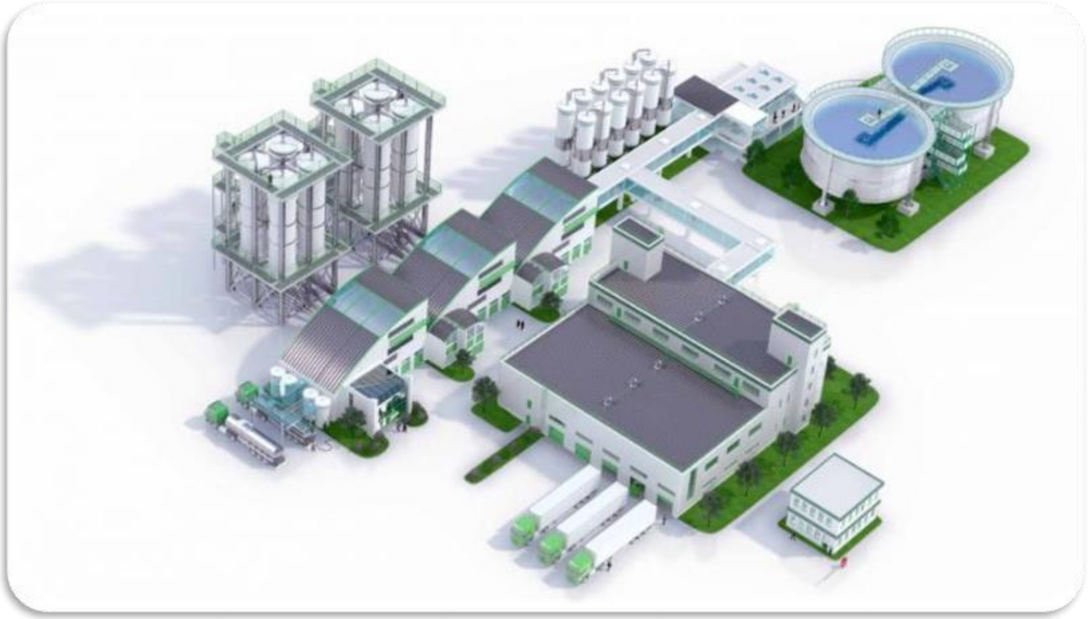
SCADA

Raccoglie i dati dai vari PLC, li elabora, li memorizza su database, gestisce la rappresentazione degli allarmi, visualizza il processo tramite sinottici grafici.



Perché i sistemi OT sono più a rischio?

- Hanno un ciclo di vita molto lungo: **10-30 anni**.
- Componenti obsoleti (hardware e software).
- Primo obiettivo: disponibilità = «**non toccare nulla se funziona**».
- Aggiornamenti eseguiti solo se necessari.
- Tecnologia IT non sicura.
- Protocolli proprietari deboli.
- Manutenzione remota non sicura.
- Uso di pratiche non sicure (es. dongle USB).



Building Automation & Smart City

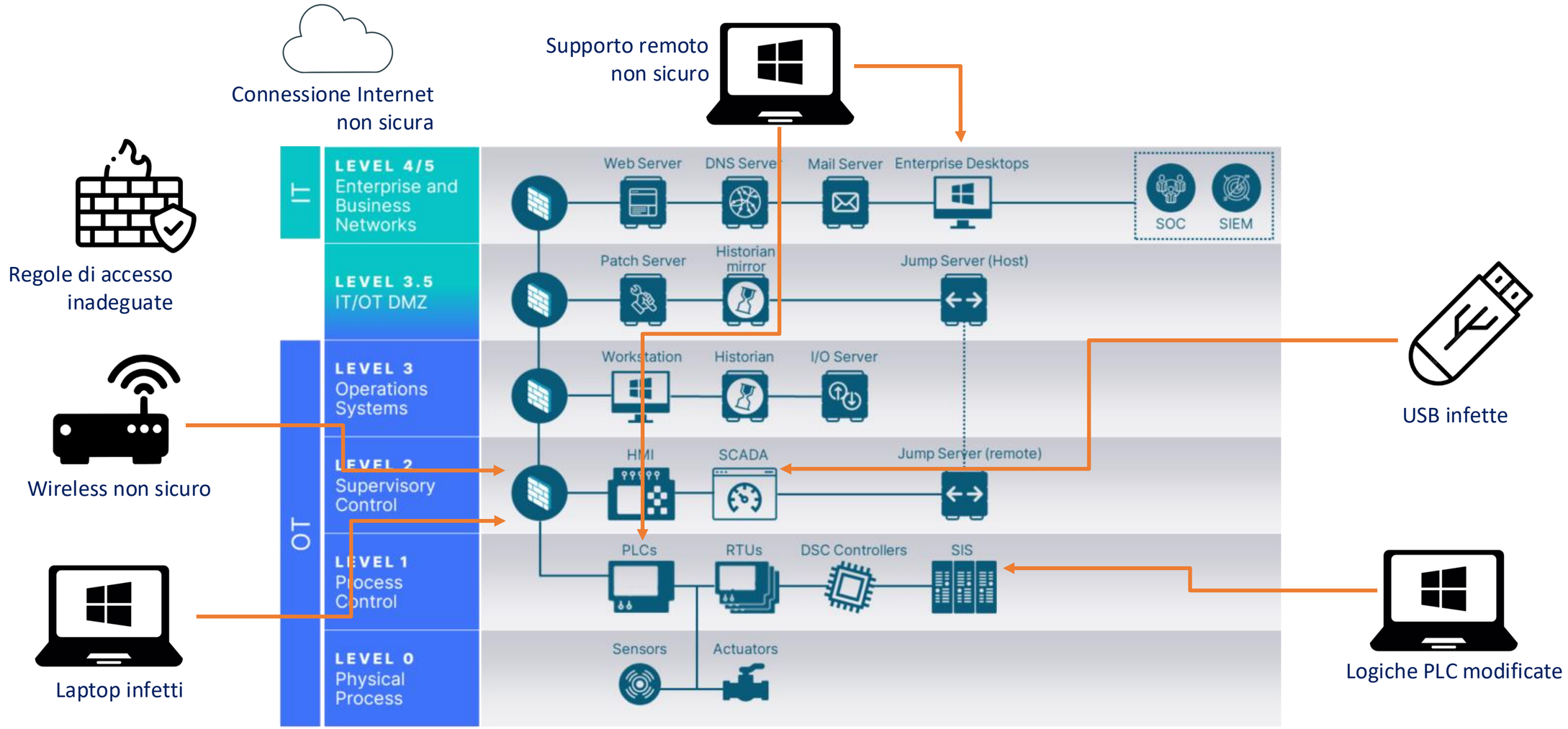
Automation Server

- Utilizzato negli edifici commerciali per controllare e automatizzare i numerosi sistemi tra cui condizionamento, illuminazione, sicurezza, ecc.
- Con una connessione remota tramite SSH si utilizzano le credenziali predefinite con privilegi di root.

Parking Charging Stations

- Stazioni di ricarica presenti in uffici, hotels, residence, aree di parcheggio.
- Individuate 3 vulnerabilità con un livello alto e medio (CVE-2018-7800).
- Le credenziali di root sono hardcoded e forniscono un accesso al sistema di Web interface.

Come posso attaccare un sistema OT?



Le principali linee guida della cyber OT

Il panorama normativo dell'OT sta subendo una trasformazione significativa.

1. Direttiva NIS 2
   Rafforzare la sicurezza delle infrastrutture critiche e dei sistemi OT.

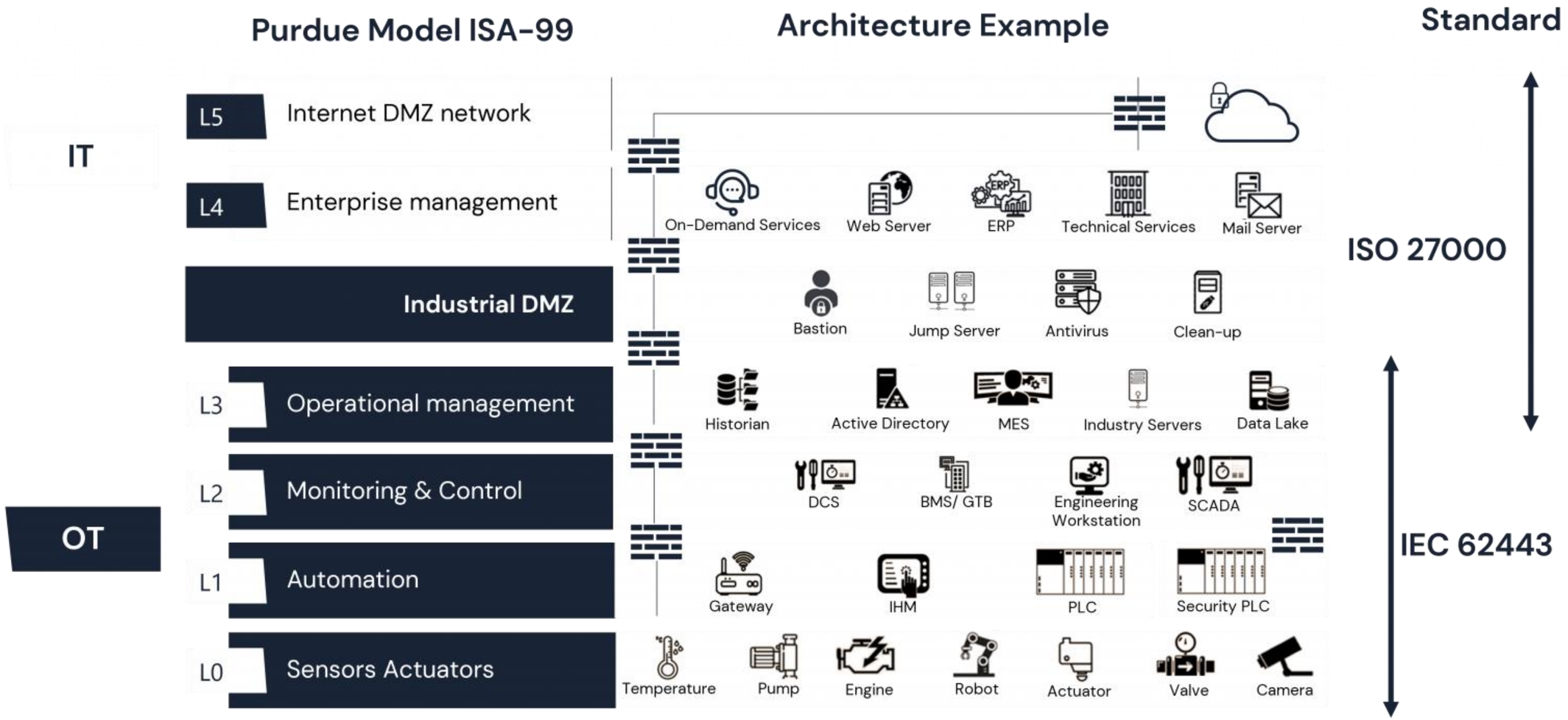
2. Regolamento Macchine
   Aumentare i requisiti di sicurezza per le macchine industriali connesse.

3. Cyber Resilience Act
   Garantire la sicurezza dei prodotti OT e IoT durante tutto il ciclo di vita.

Il Nuovo Regolamento Macchine

- Il **Regolamento Macchine** dell'UE 2023/1230 rappresenta un importante aggiornamento della precedente **Direttiva Macchine** 2006/42/CE, guidato dalla crescente trasformazione digitale e dall'avanzamento delle nuove tecnologie come l'IoT e l'AI.
- Questo nuovo regolamento mira a garantire la sicurezza e la tutela dei lavoratori in ambienti di lavoro sempre più collaborativi uomo-macchina.

Lo standard IEC 62443



Come possiamo difenderci?

La questione non è “se” il mio impianto verrà attaccato,
ma “quando”!

- I punti iniziali da memorizzare
- Individuare le risorse e i rischi.
- Segmentare l’architettura di rete.
- Analizzare il traffico.
- Controllare gli accessi a tutti i livelli.
- Proteggere i punti di ingresso delle reti.
- Adottare una politica di zero trust.

Questi step sono trattati in modo esaustivo nella IEC 62443.

La messa in sicurezza

Come operare

- Chi gestisce l’infrastruttura OT/ICS deve avere competenze specifiche.
- Da dove inizia la cyber OT: zone ICS? Enterprise?
- Training, formazione continua del personale.
- Assessment periodico, vulnerability scanning.

Gli step per la messa in sicurezza

- Definire il livello di rischio complessivo sostenibile.
- Identificare le funzioni di sicurezza per ciascuna minaccia.
- Definire i livelli di sicurezza (SL) per ciascun componente e per l’intero sistema.
- Audit della situazione attuale e dello scostamento dal target SL.
- Implementare le azioni correttive (tecniche, amministrative, formative).
- Determinare il rischio residuo.

La messa in sicurezza

Misure organizzative

- Security Assessment.
- Approccio orientato ai rischi cyber.
- Formazione specifica OT/ICS & Awareness.
- Gestione cyber dei fornitori.
- Secure Access Management, policies & procedures.

Misure tecniche

- Asset Inventory & Vulnerability Scanning.
- Network segmentation & monitoring.
- Endpoint protection & hardening.
- Secure programming dei PLC.
- Patching, backup, recovery plan.
- Accessi remoti sicuri.

CYBERSECURITY NATIONAL LABORATORY

NIST

IEC

SANS

MITRE ATT&CK for ICS

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier (Tor Project)

Q&A

Grazie!