



«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
**I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della
cybersecurity**

Milano, 30 Maggio 2018

Auditorio TECNIMONT

Thinking security to ensure productivity

La strategia di Siemens per la sicurezza degli impianti industriali



Digitalization changes everything

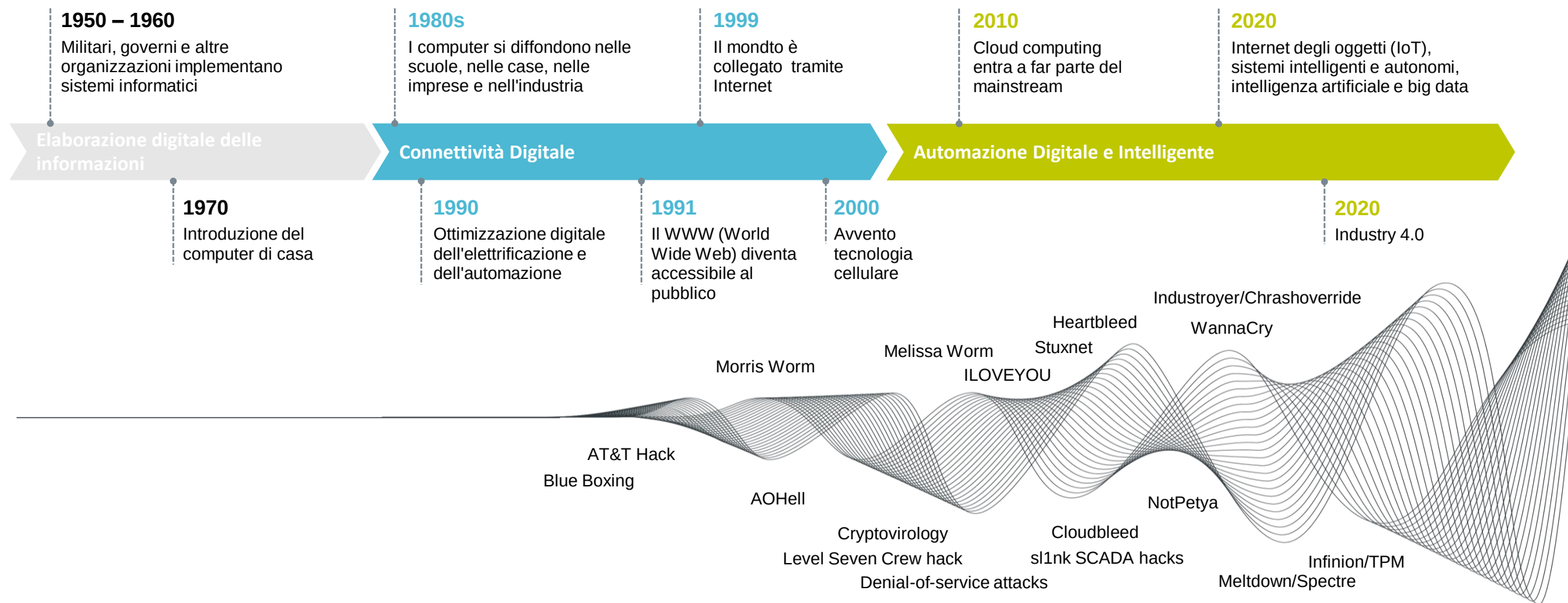
- L'intelligenza artificiale (AI) e l'analisi di grandi dati stanno rivoluzionando il modo in cui prendiamo le decisioni
- E miliardi di dispositivi sono collegati dall'Internet Of Things e interagiscono su un livello e una scala completamente nuovi
- La Cyber Security è fondamentale per il successo dell'economia digitale

SIEMENS

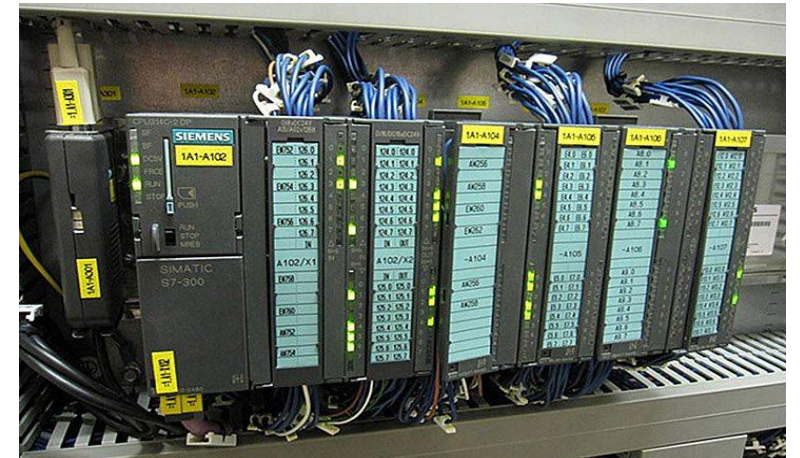
Ingenuity for life

Industrial Security

Il rischio all'esposizione di attacchi sta crescendo esponenzialmente



Certe cose non sono fatte per essere collegate “as is” ad Internet...



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

SHODAN

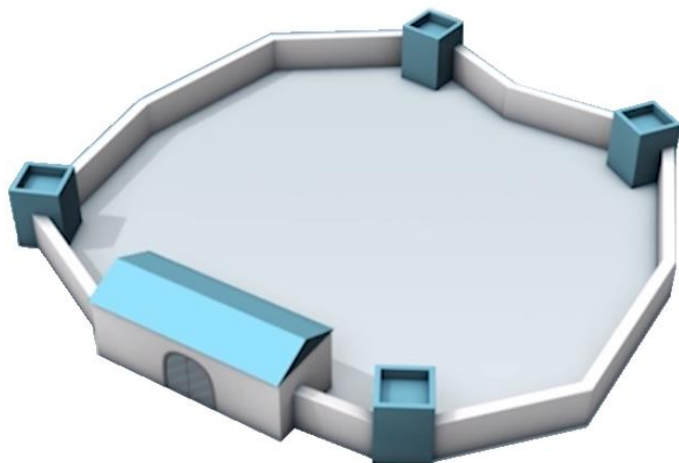
20.69.105
50.87.75.184
104.18.61.231

The banner features a dark background with a grid of IP addresses and red virus-like icons. The Shodan logo is prominently displayed on the right.

Come difendersi in ambito OT?

Cyber attack – Ucraina 2015

Singola Barriera

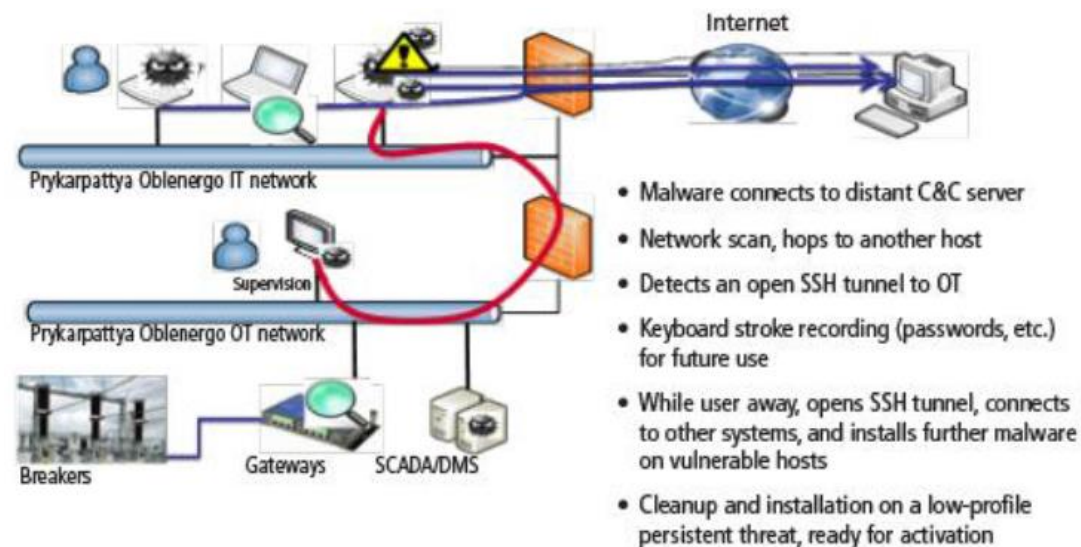


- Singolo livello di protezione
- Singolo punto di attacco
- Muro impenetrabile

Spear Phishing

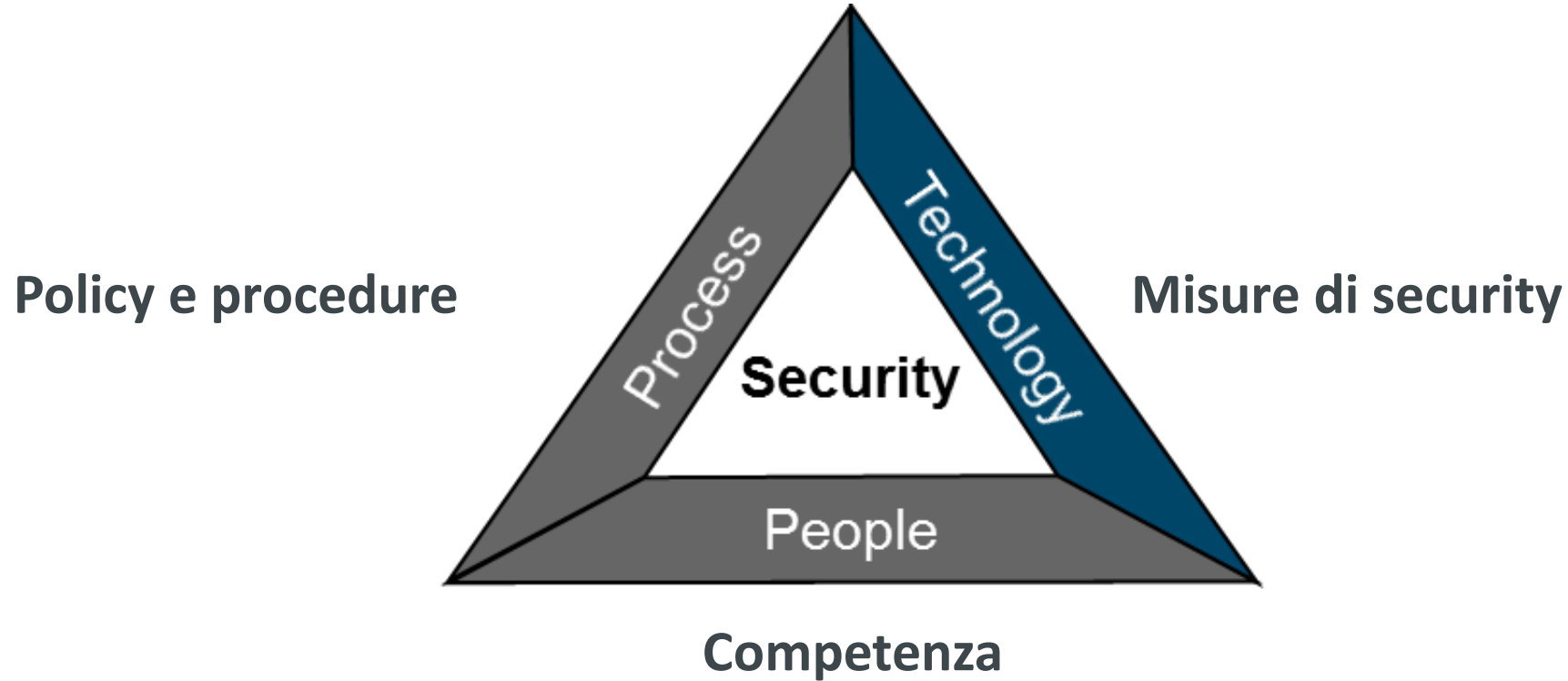
Intrusione nella rete e raccolta informazioni

Upload del FW corrotto e attacco sullo SCADA



Source <https://www.isa.org/templates/news-detail.aspx?id=152995>

In primis, la security è legata a...

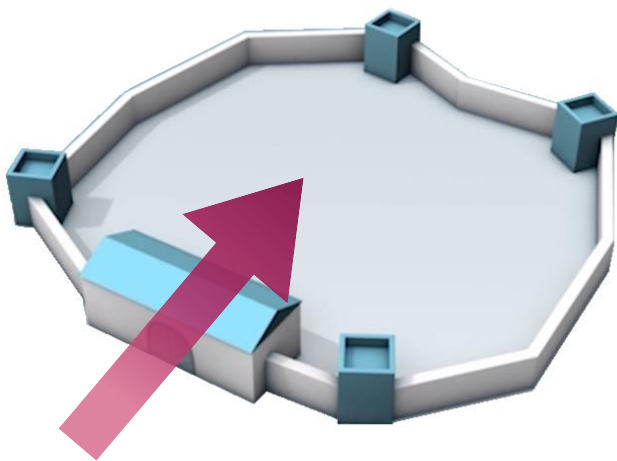


Un approccio olistico per la security è un concetto che include:
tecnologie, processi e persone

Defense in Depth

Principio

Singola Barriera



- Singolo livello di protezione
- Singolo punto di attacco
- Muro “**apparentemente**” impenetrabile

Defense In Depth



- Protezione su più livelli
- Ogni livello protegge gli altri livelli
- Un attaccante deve spendere tempo ed effort per ogni transizione

La protezione è ottimizzata solo implementando simultaneamente più misure complementari

IEC 62443

Security per OT (Operation Technology)

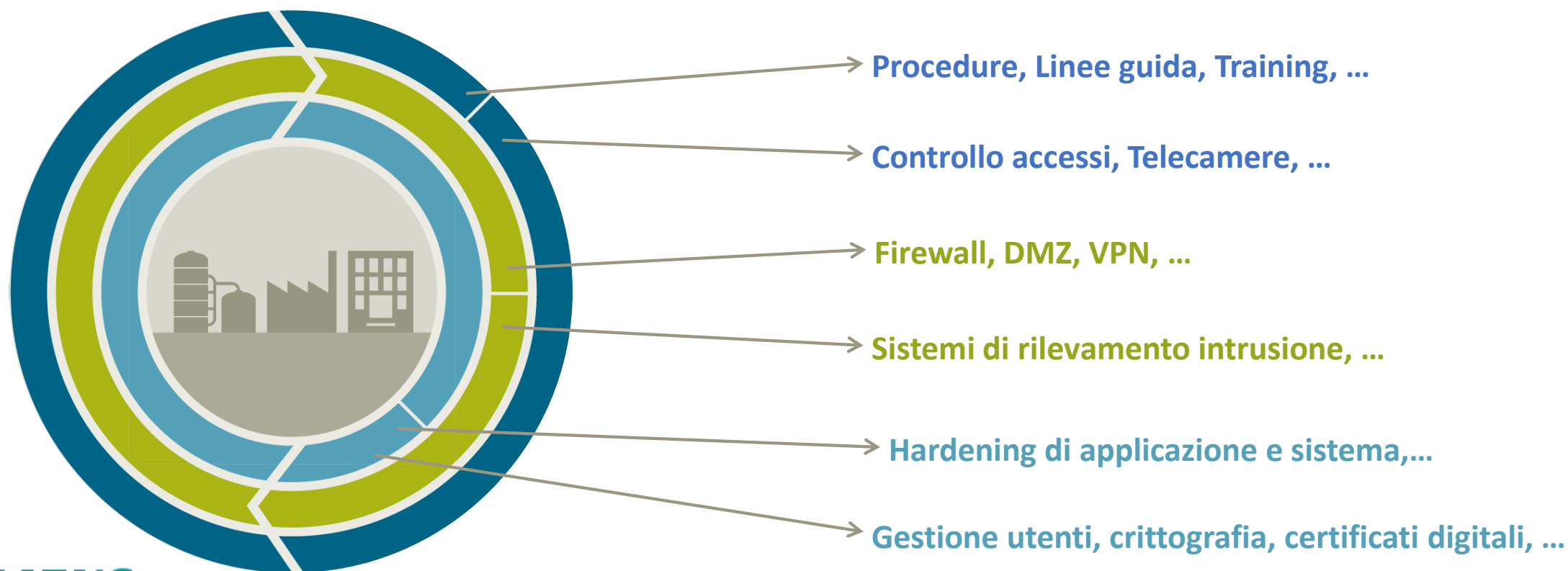


Associazione Italiana
Strumentisti



Italy
Section

IEC 62443: standard security in ambito IACS – Industrial Automation and Control System - basato sul principio “Defense in depth” → protezione su più livelli



SIEMENS

Ingenuity for life

Protection Level

Proposta Siemens per estensione IEC 62443-2-2

Security Level

- Valutazione delle **funzionalità** di security
- Basati su IEC 62443-3-3

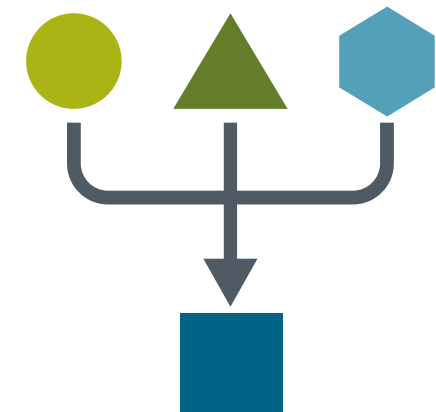
Maturity Level

- Valutazione dei **processi** di security
- Basati su IEC 62443- 2-4 and ISO27001

Protection Level (PL)

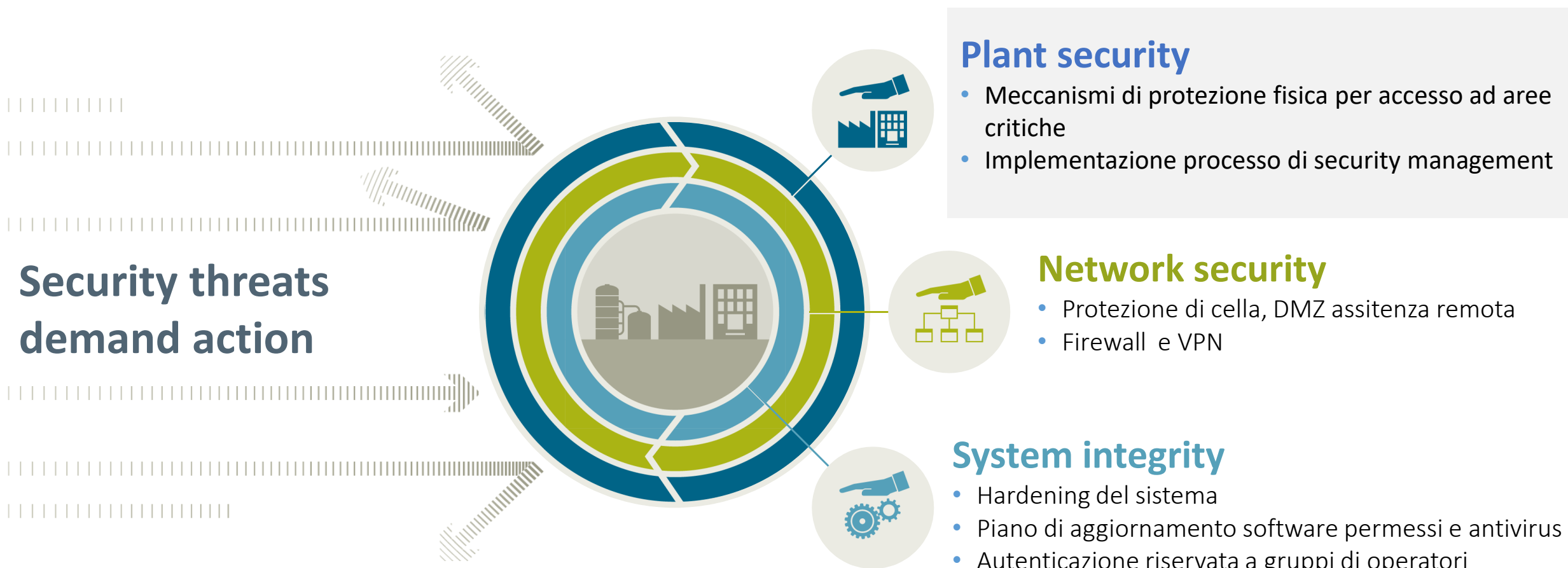


Maturity Level	4				PL 4
	3			PL 3	
	2		PL 2		
	1	PL 1			
		1	2	3	4
		Security Level			



Industrial Security - Introduzione

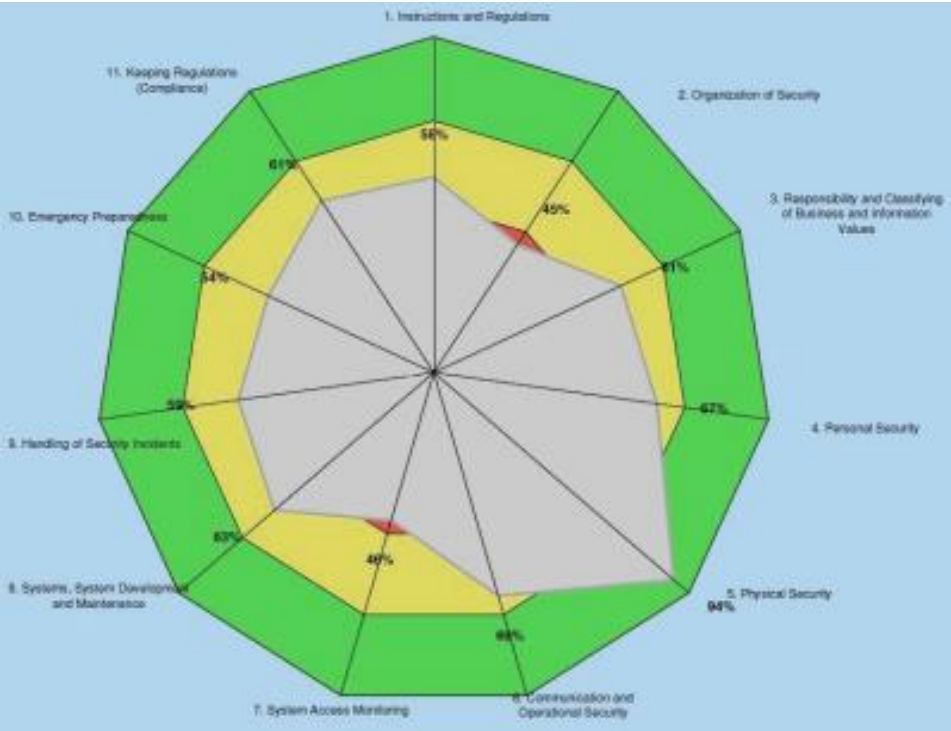
Concetto “Defense in Depth” – ISA 99 / IEC 62443



Plant Security Services

Indentificazione rischi e misure di mitigazione

- **Assessment** della sicurezza della fabbrica in funzione dello standard **ISO 27001** e **IEC 62443**



- **Risk & Vulnerability Assessment:** identificazione, classificazione e valutazione per un programma basato sulla metodologia del rischio

Vulnerability	Risk Score
Flat network architecture / No DMZ available	8,1
Flat network architecture / No network segmentation	8,1
Unsecure / Not controlled remote activities	7,4
No system hardening / Unneeded applications and services installed	7,1
Unpatched operating systems	6,8
Obsolete anti-virus database	6,6
Windows firewall not active	5,6
Uncontrolled USB interfaces	4,8

Table 1: Risk Scoring (direct risks) according to CVSS

- **Red [7,5-10]** – Unacceptable risk; Urgent action is necessary
- **Orange [5-7,5]** – Unacceptable risk; Action is required
- **Yellow [2,5-5]** – Acceptable risk; Subject to management approval
- **Green [0-2,5]** – Acceptable risk; No action required



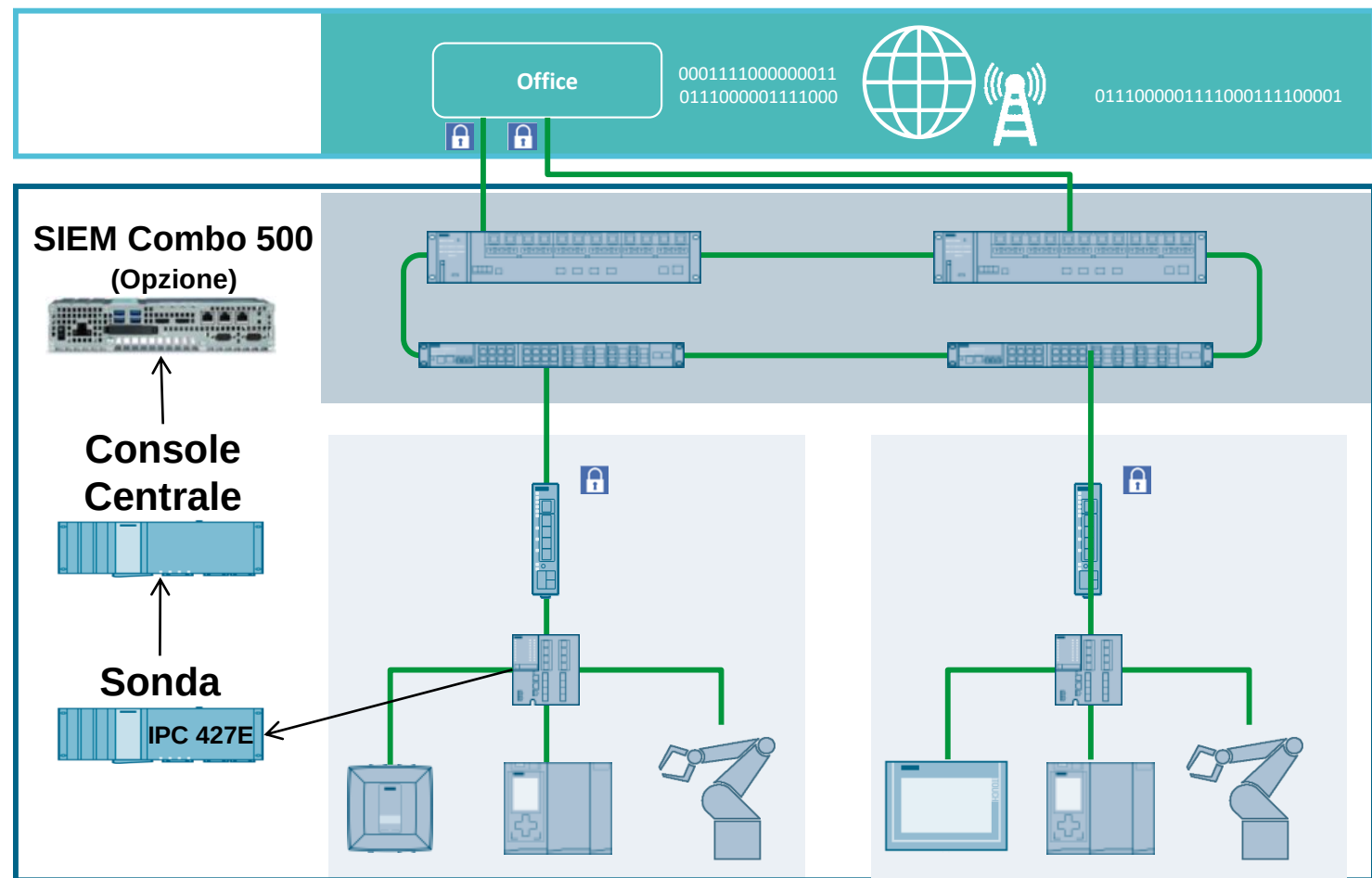
Industrial Anomaly Detection

Trasparenza della rete industriale

Sistema in grado di fornire un **monitoraggio continuo delle reti industriali**

- **Monitoraggio passivo** al 100%
- **Discovery automatica** degli asset fisici e di comunicazione semplificato per facilitare l'analisi e la mitigazione del rischio
- **Analisi continua** delle attività di **traffico** e reporting in caso di riscontro di eventuali anomalie (tramite tecniche di machine learning)
- **Supporto** di dispositivi **3rd party**

Massima trasparenza

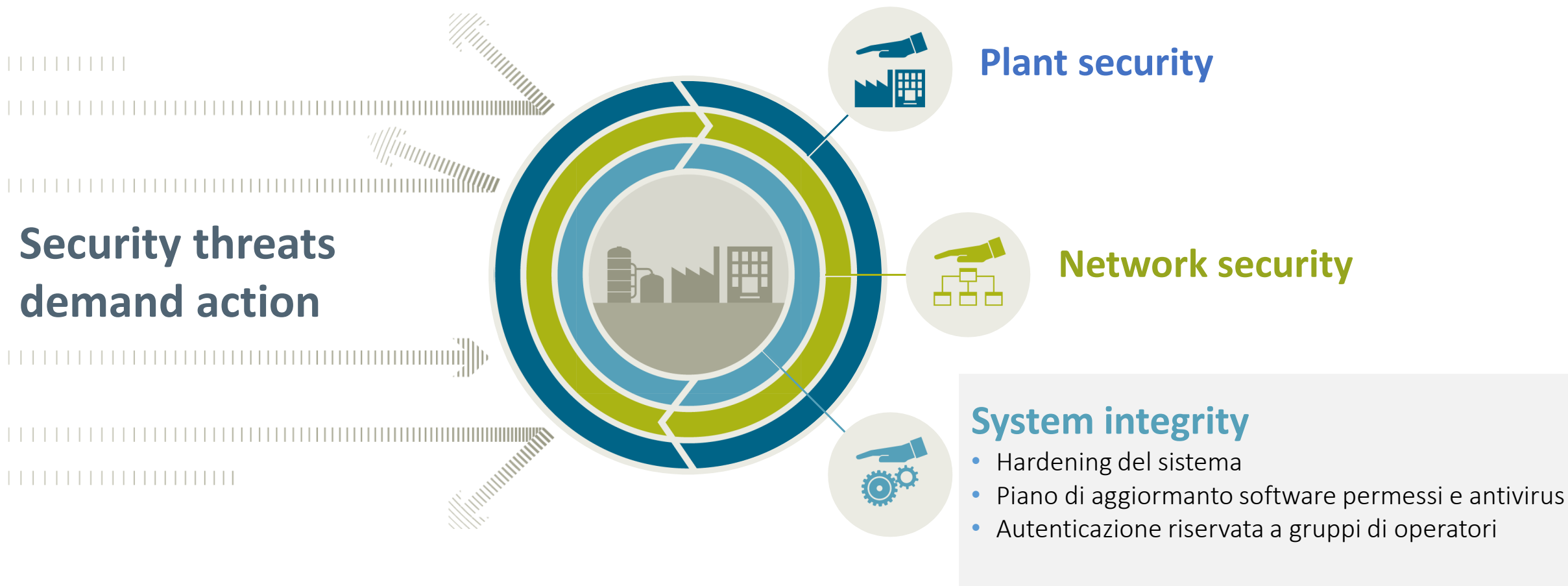


SIEMENS

Ingenuity for life



Defense in Depth System Integrity



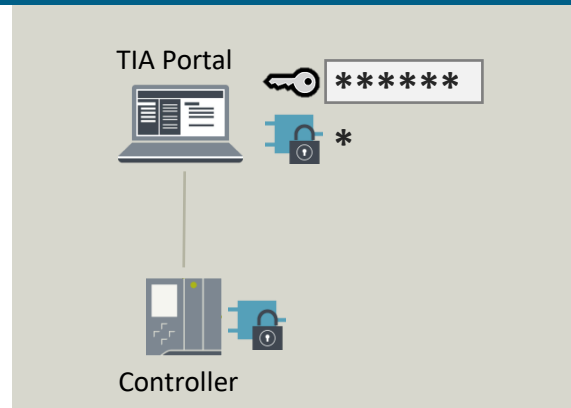
System Integrity

Security use cases – controllori industriali

Protezione Know-how

Protezione della proprietà intellettuale del codice di programmazione

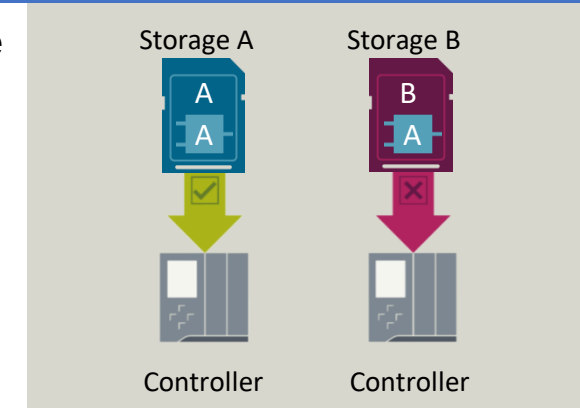
- Protezione Know-how per blocchi programmazione PLC



Protezione copia programma

Protezione contro duplicazione non autorizzata del codice runtime

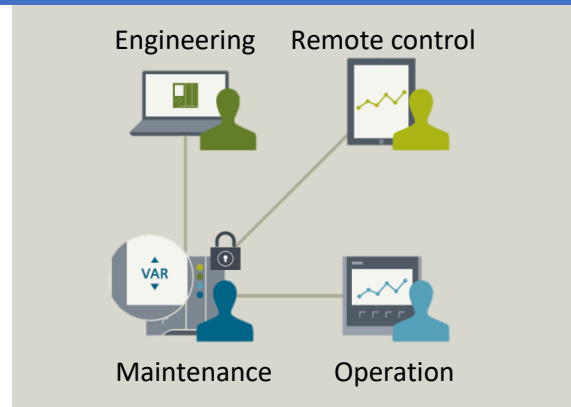
- Blocchi di programma con riconoscimento del serial number (CPU or SD card)



Protezione accesso

Protezione contro accesso e cambi di configurazione indesiderati

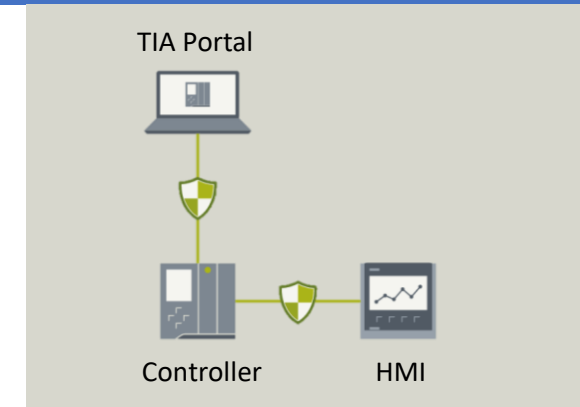
- Concept di protezione su diritti di accesso su più livelli



Integrità della comunicazione

Rilevamento di dati manipolati

- Comunicazione tra il SW, il controllore e l'HMI con security integrata



Industrial Security

RFID per autenticarsi in modo semplice

Necessità

Controllo di accesso alle macchine e sistemi di automazione in funzione dei diritti dell'utente/operatore tramite utilizzo di badge

Soluzione

Smart Reader per fornire il controllo di accesso alla macchina di automazione tramite badge standard (ISO 14443A/B e ISO 15693).

- Login con badge RFID card (one-time)
- Login con badge (permanente)
- Login with user name, password and RFID card

SIEMENS

Ingenuity for life

Login locale
direttamente sul
pannello HMI



Login allo Scada - IPC

Win7 x64
(esempio IPC 677D)



RFID API

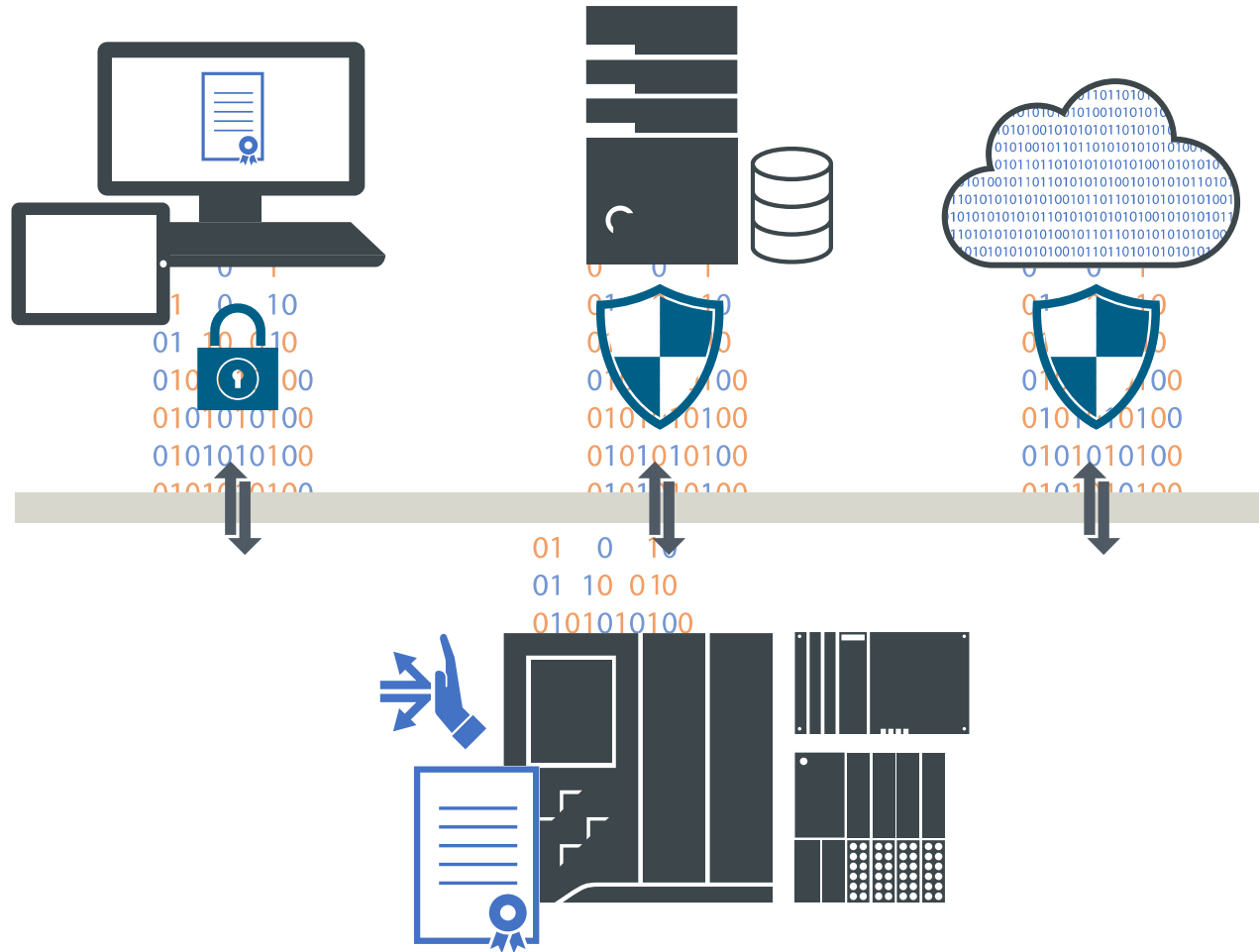
HID driver

USB



OPC UA

Comunicazione con sicurezza integrata



OPC UA Security



Policy di security in funzione dell'utente sia sul controller che il client



Autenticazione di dispositivi/applicazione sulla base di certificati



Comunicazione crittografata e protezione dell'integrità

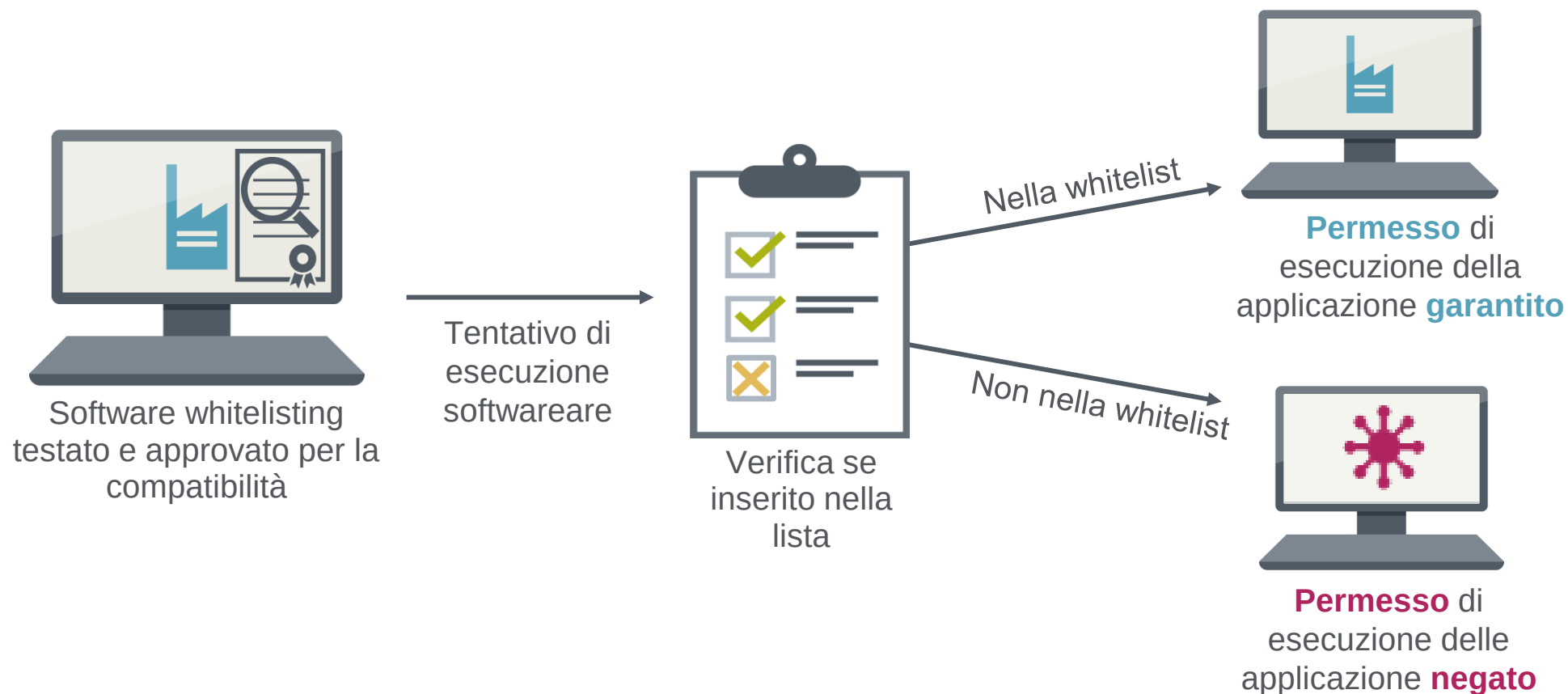


Autenticazione di utenti e accesso con restrizioni alle tag dei PLC

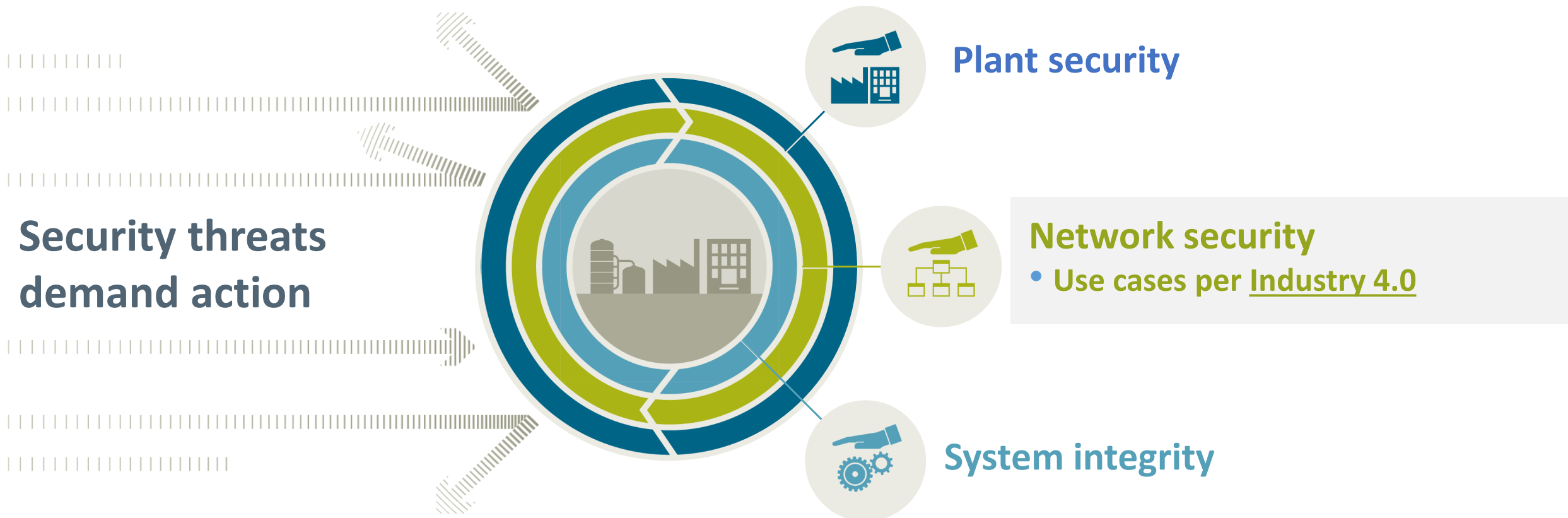


Whitelisting & Antivirus

Controllo delle applicazioni per la protezione da malware e applicazioni indesiderate



Defense in Depth Network Security



Network Security

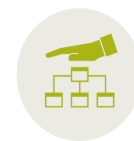
Switch managed - “Go Managed”

- Sfruttare **protocolli** per **ridondanza**
- Usare **Password**
- Usare **VLAN**
- Abilitare **ACL**
- **Limitare** Broadcast (DoS)
- **Disabilitare porte** non utilizzate e **Loop Detection**
- Abilitare **SNMP V3**



SIEMENS

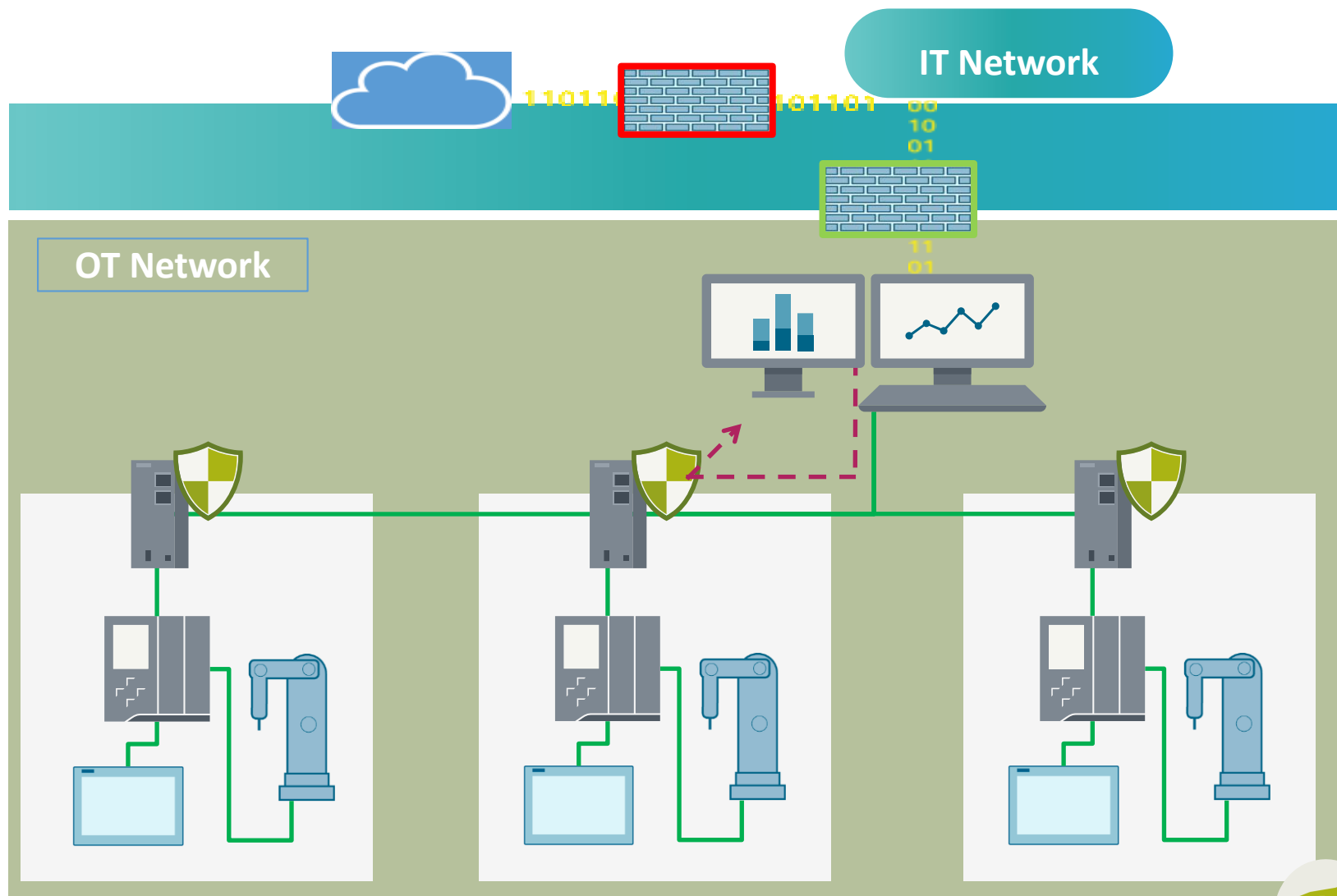
Ingenuity for life



Network Security

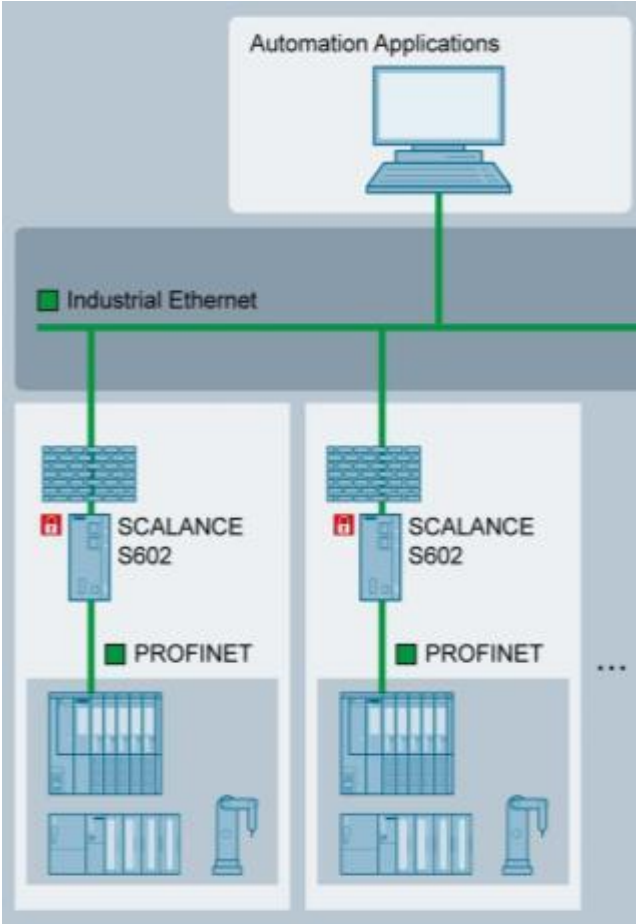
Firewall: Protezione e segmentazione della rete

- Separazione della rete OT in **celle di protezione**
- Connessioni autorizzate tramite **Firewall**
- Separazione fisica per mezzo di **Dispositivi dedicati**



Deep Packet Inspection Firewall

Standard Firewall: Filtering basato su L3/L4

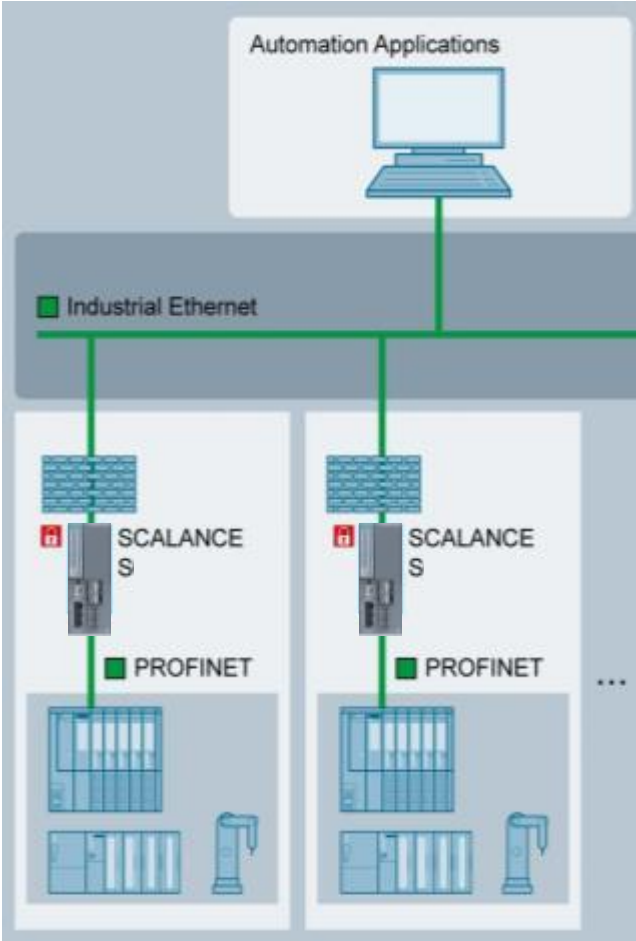


Permesso



- S7 Comm
- set commands
 - read commands
 - diagnostic access
 - ...

DPI: Filtering in funzione del livello applicativo



Negato



- S7 Comm
- „set PLC time“

Permesso



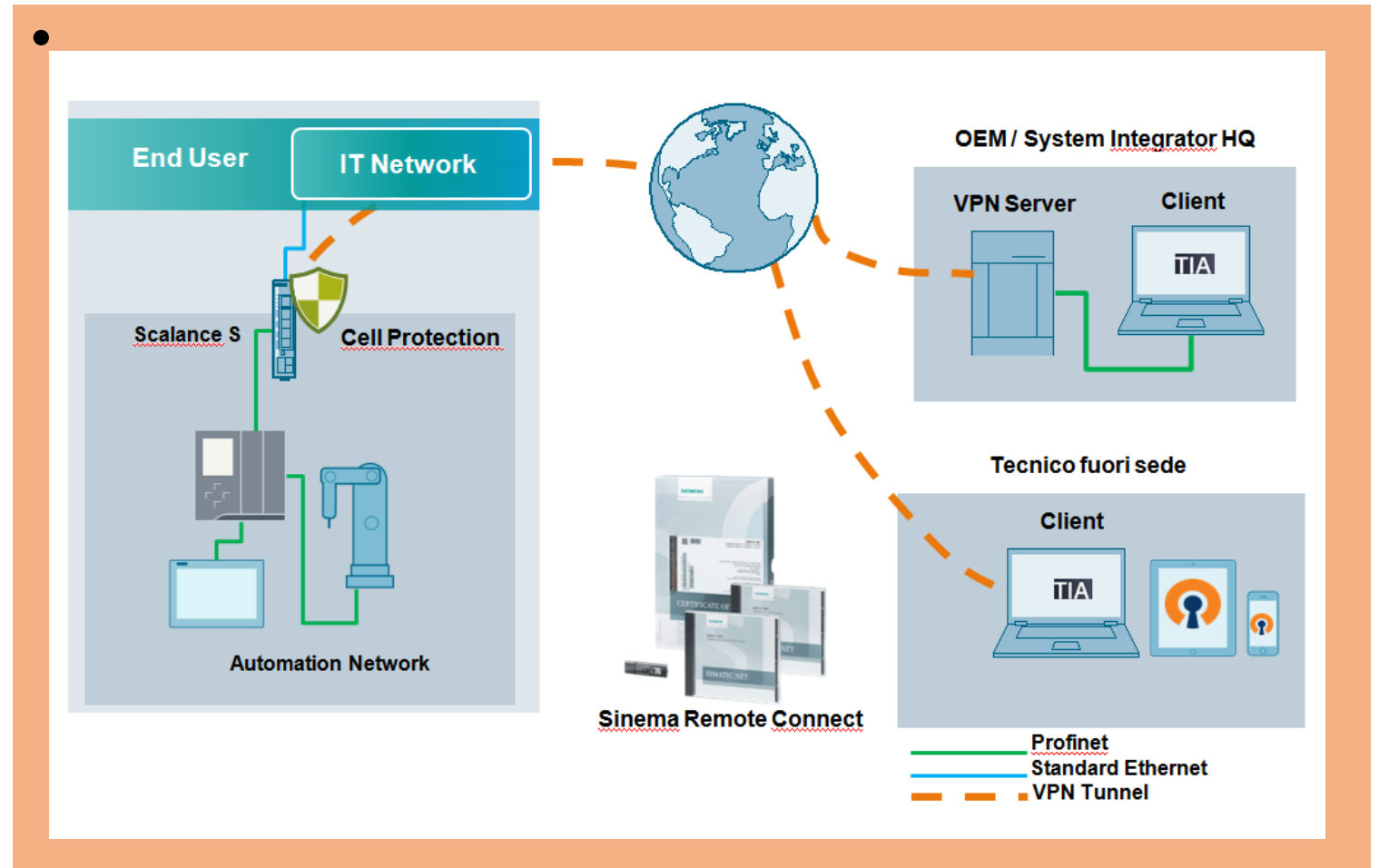
- S7 Comm
- „read PLC status“



Accesso Remoto

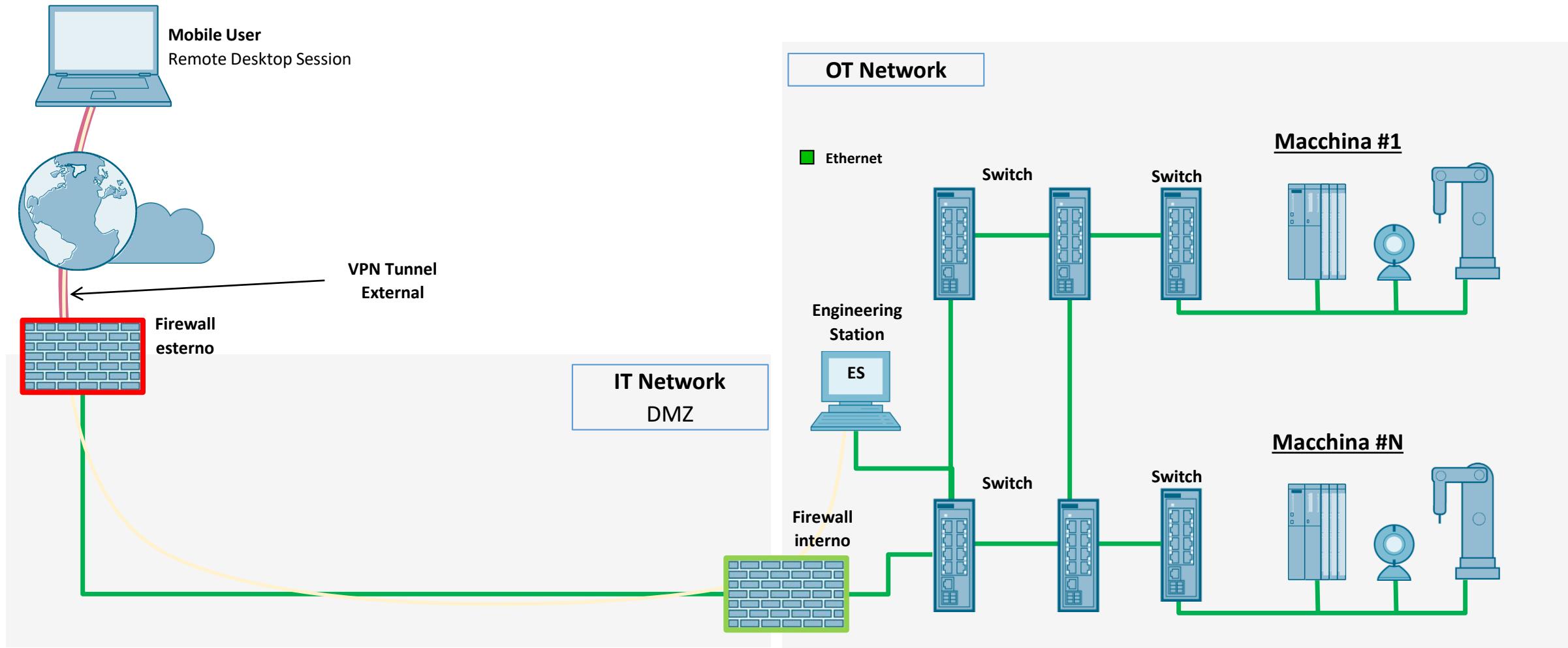
La soluzione per una teleassistenza sicura

- Connessioni VPN di dispositivi e utenti tramite gestione centralizzata
- Comunicazione crittografata con tecnologia **OpenVPN**
- Attivazione VPN tramite **digital input**
- Autenticazione a due fattori (password e PKI)



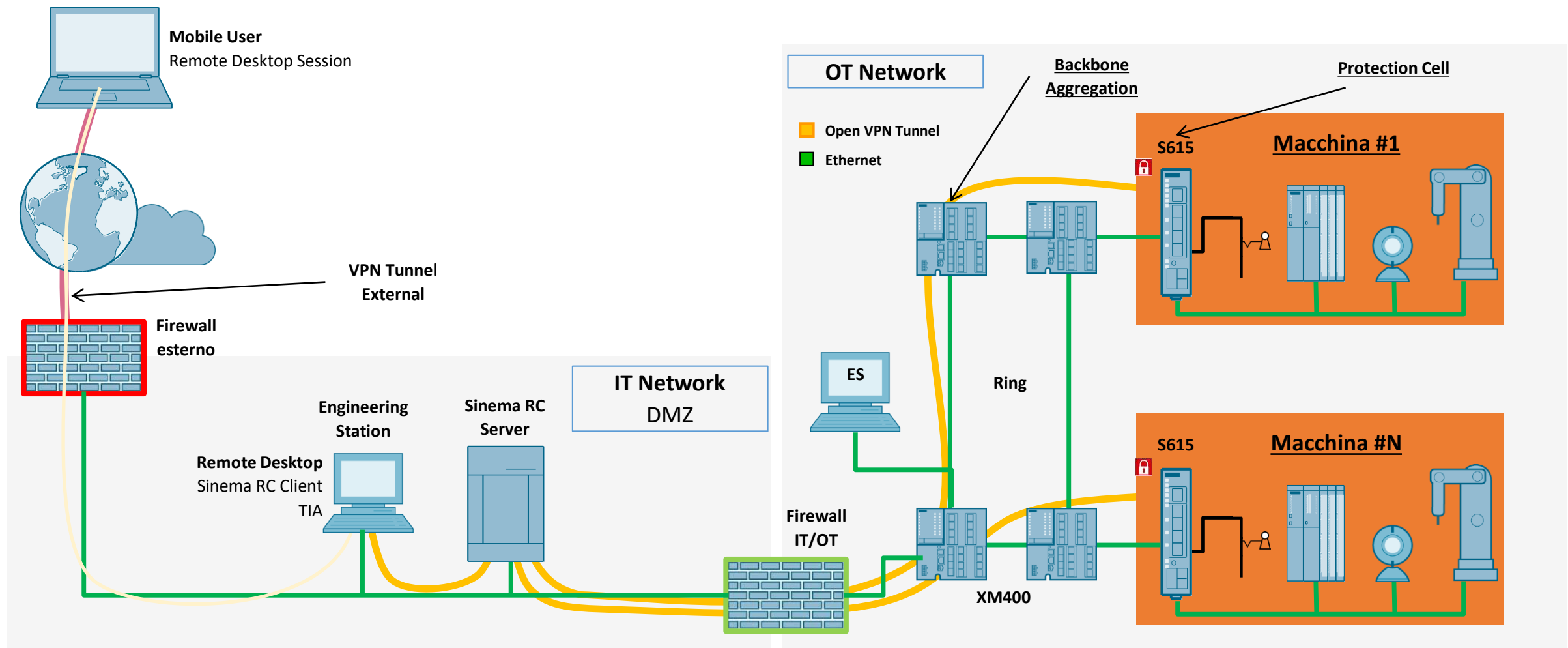
Teleassistenza End User

Situazione tipica



Teleassistenza End User

Backbone Aggregation e Jump Host



Referenze Industrial Security

Festo AG, Automation

Informazioni Progetto	- Festo AG è un fornitore globale nel mondo dell'automazione - Per gli stabilimenti di produzione, FESTO ha predisposto una nuova piattaforma di security nella propria fabbrica in Germania (Scharnhausen). Funzioni come firewall e VPN forniscono un incremento di protezione dei dati sigillando le reti di produzione da accessi esterni ed interni indesiderati.
Obiettivi Cliente	- Le reti di produzione dovevano essere più sicure e amministrate centralmente. - Non esisteva uno standard IT per segmentare e separare le reti di ufficio e di produzione. - Si doveva gestire l'accesso alla rete da parte di personale di servizio interno ed esterno alle macchine
Soluzione di Siemens	Segmentazione di cella e accesso remoto sicuro - Soluzione di manutenzione remota efficiente grazie alla piattaforma di gestione SINEMA Remote Connect e SCALANCE S615. - Funzione rubrica disponibile con SINEMA RC Client per l'identificazione chiara di macchinari e attrezzature nella fabbrica tecnologica e la loro selezione per l'accesso remoto a Internet e intranet.
Valore per il Cliente	- Il tempo richiesto per l'integrazione della rete di nuove macchine è stato ridotto da due settimane a poche ore; l'hardware e il software possono essere utilizzati immediatamente. Un software user-friendly rende possibile la parametrizzazione delle appliance di sicurezza anche per utenti inesperti. - I conflitti di indirizzi IP vengono eliminati dalla funzione NAT di SINEMA RC Client e SCALANCE S.



“Abbiamo implementato una soluzione che garantisce un accesso remoto sicuro alle nostre macchine e ai nostri impianti di produzione.

” ”

Albrecht Salm, Chief Information Security Officer at the Festo AG in Esslingen, Germany

Referenze Industrial Security

Siemens Amberg



Profilo

Elektronikwerk Amberg è uno dei **primi esempi di fabbrica digitale**. La fabbrica usa le tecnologie più innovative per produrre approssimativamente **quindici milioni di prodotti SIMATIC ogni anno**.

Sfida

- Processi controllati da dati IT molto sensibili
- Ambiente di automazione totalmente collegato in rete
- Flusso dei dati e database omnicomprensivi
- Protezione contro spionaggio industriale, manipolazione e attività di hacker

Soluzione

- **Implementazione di Defense in Depth** con S7-1500 e SCALANCE S usando TIA Portal
- **Monitoraggio di eventi** relativi alla **security**
- **Report mensile dello status** della produzione e della **security** del sistema
- Raccomandazioni per ottimizzare il livello di protezione

Vantaggi per il cliente

- **Protezione delle reti** e componenti TIA secondo i concetti della security **Defense-in-Depth**
- Notifiche precise e puntuali grazie a **Security Information and Event Management (SIEM)**
- **Continua ottimizzazione** del concetto di security

SIEMENS

Ingenuity for life

Referenze Industrial Security

Pohjolan Voima (PVO)



Profilo

Voima Pohjolan è stata fondata nel 1943 e produce energia elettrica e calore per i suoi clienti mediante fonti idroelettriche e termiche

Sfida

- Il sistema esistente non soddisfa i moderni standard di sicurezza informatica
- Nessun aggiornamento regolare delle routine nei vecchi sistemi quando sono stati implementati nuovi sistemi.
- Evitare malfunzionamenti intenzionali e non intenzionali causati da minacce alla sicurezza.
- Protezione contro il phishing di informazioni preziose e lo spionaggio

Soluzione

- **Effettuata la valutazione per individuare vulnerabilità** in materia di sicurezza e le misure di attenuazione dei rischi in base alla **norma IEC 62443**.
- Indagine sulle proprietà tecnologiche del sistema di sicurezza informatica: **gestione degli utenti e degli accessi**, registri operativi, procedure di back-up, **crittografia dei dati**
- analisi dei processi e delle istruzioni in materia di sicurezza informatica, come la capacità di reagire alle minacce

Vantaggi per il cliente

- Prospettive diverse rispetto alle valutazioni interne effettuate da un esperto esterno
- Conformità ai requisiti di sicurezza stabiliti per l'azienda
- Raggiungere il livello di maturità desiderato di sicurezza industriale più elevato

SIEMENS

Ingenuity for life

Referenze Industrial Security

Raffineria Sinopec a Qingdao



Profilo

- La raffineria Sinopec di Qingdao è un enorme complesso petrolchimico e di raffinazione con una capacità di distillazione di 10 milioni di tonnellate all'anno
- Produce benzina, kerosene, gasolio, GPL, polipropilene e stirene

Sfida

- Funzionamento senza disturbi
Protezione contro tutti i tipi di virus
- Implementazione rapida e indolore
- **Il più grande progetto di industrial security stand alone in tutto il mondo**

Soluzione

- Sviluppo di una soluzione di security per l'ambiente di PCS 7 incluse **DMZ, Firewall, Anti-Virus, Patch Management, User Management e System hardening**
- 2 settimane di implementazione durante il fermo impianto

Vantaggi per il cliente

- **Protezione continua dell'impianto:**
riduce i rischi e mantiene la disponibilità della produzione
- Zero incidenti o infezioni dopo il progetto: 18 mesi di funzionamento sicuro
- Riferimento per clienti cinesi nel settore petrolchimico

Certificazione IEC 62443-4-1

Product Development Lifecycle



Siemens è stata la **prima azienda al mondo con**
Certificazione TÜV SÜD IEC 62443-4-1 per i processi **R&D**
Siemens DF & PD (Product Development Lifecycle based
on IEC 62443-1)

SIEMENS	
Security by design	✓
Security verification and validation testing	✓
Security update management	✓

Per ulteriori informazioni:

<http://www.siemens.com/press/en/pressrelease/?press=/en/pressrelease/2016/digitalfactory/pr2016080373dfen.htm>



**Charter
of Trust**

**We sign for
cybersecurity!
We sign the
Charter of Trust.**

SIEMENS AES AIRBUS Allianz  AtoS enel

DAIMLER IBM Munich Security Conference  NXP SGS T..

**Creare una “foundation” affidabile per instaurare
fiducia per un mondo digitale connesso**

Grazie dell'attenzione



Niccolò Spinola Ferrari

Product Manager Industrial Security

E-Mail: spinola_ferrari@siemens.com

www.siemens.com/industrial-security