SIEMENS
Ingegno per la vita

Cyber Security

Gruppo Este 16.05.2019

SIEMENS
Ingenuity for life

La Cyber Security è fondamentale per il successo dell'economia digitale

SIEMENS
Ingenuity for life

Difendersi nell’ Era della digitalizzazione

Il Cyber crimine è sempre più diffuso e I costi per l’economia globale sono stimati in 400 miliardi di $ all’anno.[1]
Gli attacchi Cyber impattano le compagni di ogni dimensione in tutti I mercati.

1 Stima di Strategic and International Studies, Washington, D.C.

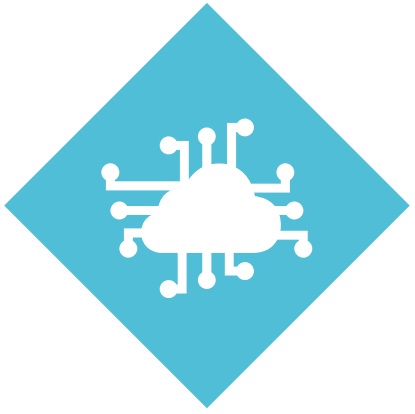
Uno scenario in continua evoluzione

SIEMENS
Ingenuity for life

Professionisti
Hacker

Vulnerabilità

Internet of Things



Leggi su Cybersecurity e
Normative

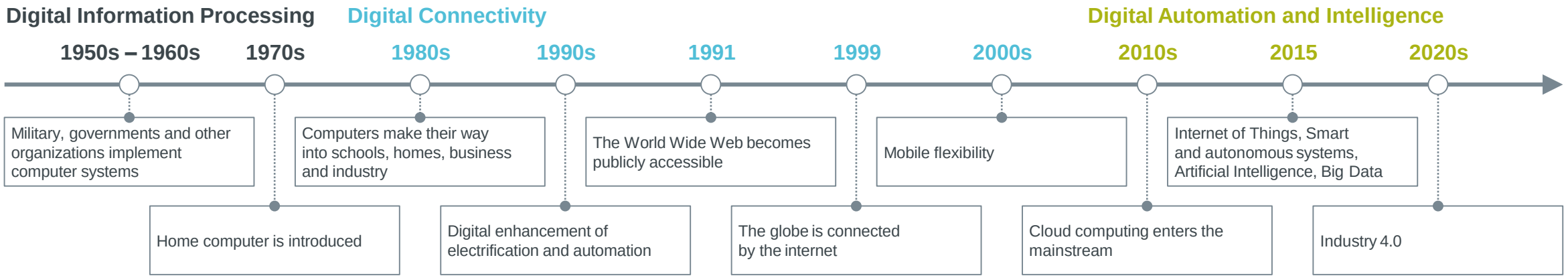
E oggi…

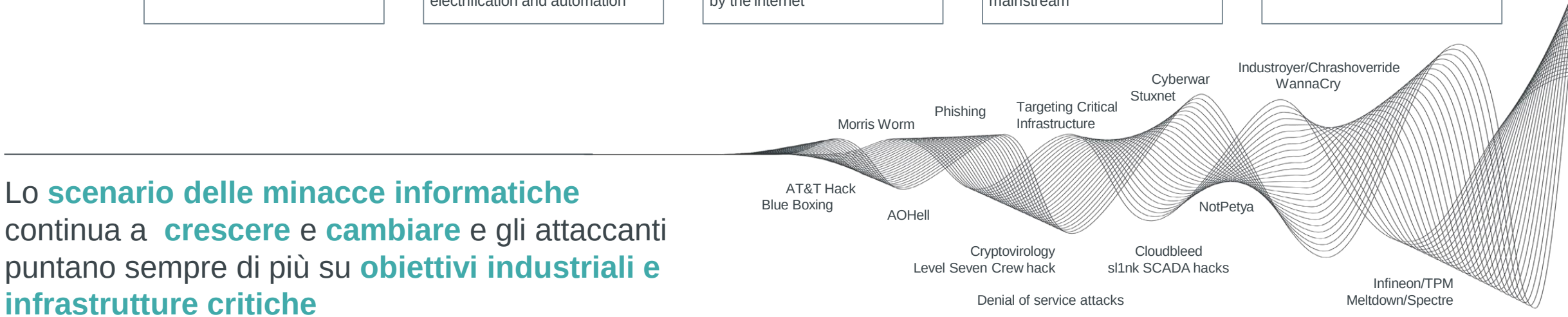
SIEMENS
Ingenuity for life

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Minacce informatiche: evoluzione dello scenario

SIEMENS
Ingenuity for life





Lo **scenario delle minacce informatiche** continua a **crescere** e **cambiare** e gli attaccanti puntano sempre di più su **obiettivi industriali e infrastrutture critiche**

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

SIEMENS
Ingenuity for life

https://www.**shodan**.io/

Le sfide sono simili ma la realtà è molto diversa fra IT Security e Industrial Security

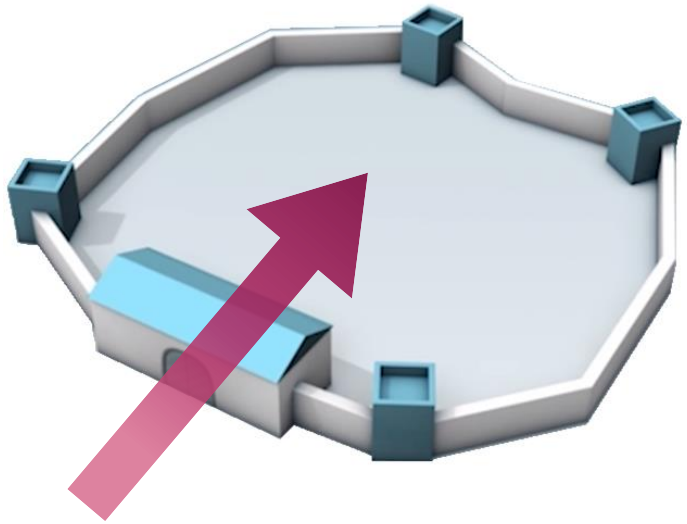
SIEMENS
Ingenuity for life

IT Security		Industrial Security
3-5 anni	**Ciclo di vita dei prodotti**	20-40 anni
Migrazione obbligata (es:PC, smart phone)	**Ciclo di vita software**	Uso fintanto che si hanno parti di ricambio
Alta (> 10 “agents” sui PC office)	**Opzioni per aggiungere SW**	Bassa (occhio alle prestazioni)
Bassa (~2 generazioni, Windows 7 and 10)	**Eterogeneità**	Alta (da Windows 95 fino a 10)
Standard (agents & patching)	**Concetto di protezione**	Specifica a seconda del rischio

Defense in depth
Il principio degli strati

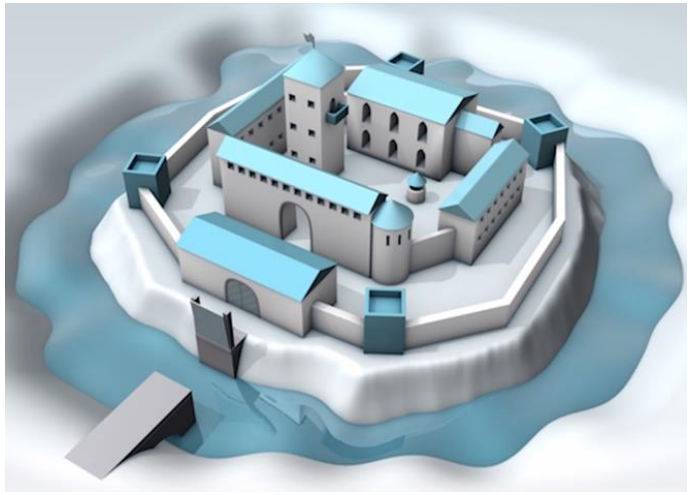
SIEMENS
Ingenuity for life

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)

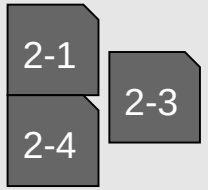
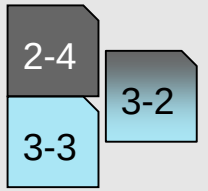
IEC 62443: standard security in ambito IACS – Industrial Automation and Control System - **basato sul principo "Defense in depth"** → protezione su più livelli

- Policies, Procedures, Training
- Access Control Cards, Cameras, Locks
- Firewall, IPSec, Network Intrusion Detection
- System Hardening, Intrusion Detection
- Application Layer FW , Application Hardening
- Access Controls, Encryption, Digital Rights

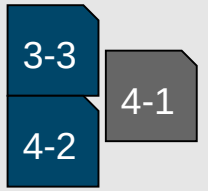
IEC 62443
Definizione dei ruoli

SIEMENS
Ingenuity for life

On site

Chi	Cosa	IEC62443
End User	**Produzione e manutenzione**	
System Integrator / OEM	**Progettazione ed implementazione**	

Off site

Chi	Cosa	IEC62443
Produttore	**Sviluppo prodotti**	

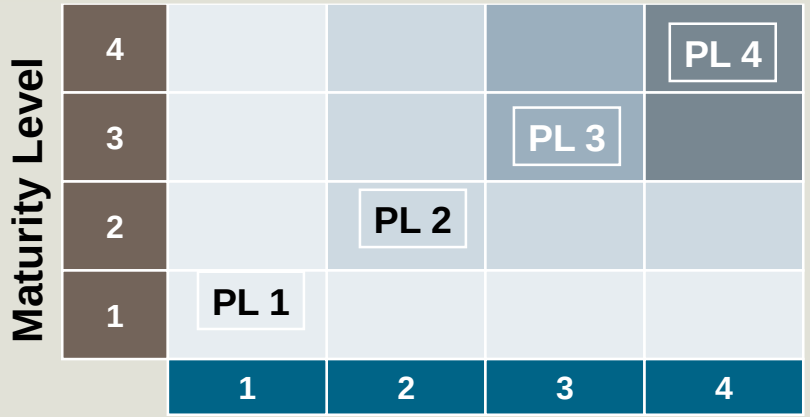
Protection Level
Estensione IEC 62443

SIEMENS
Ingenuity for life

Security Level

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

Protection Level (PL)

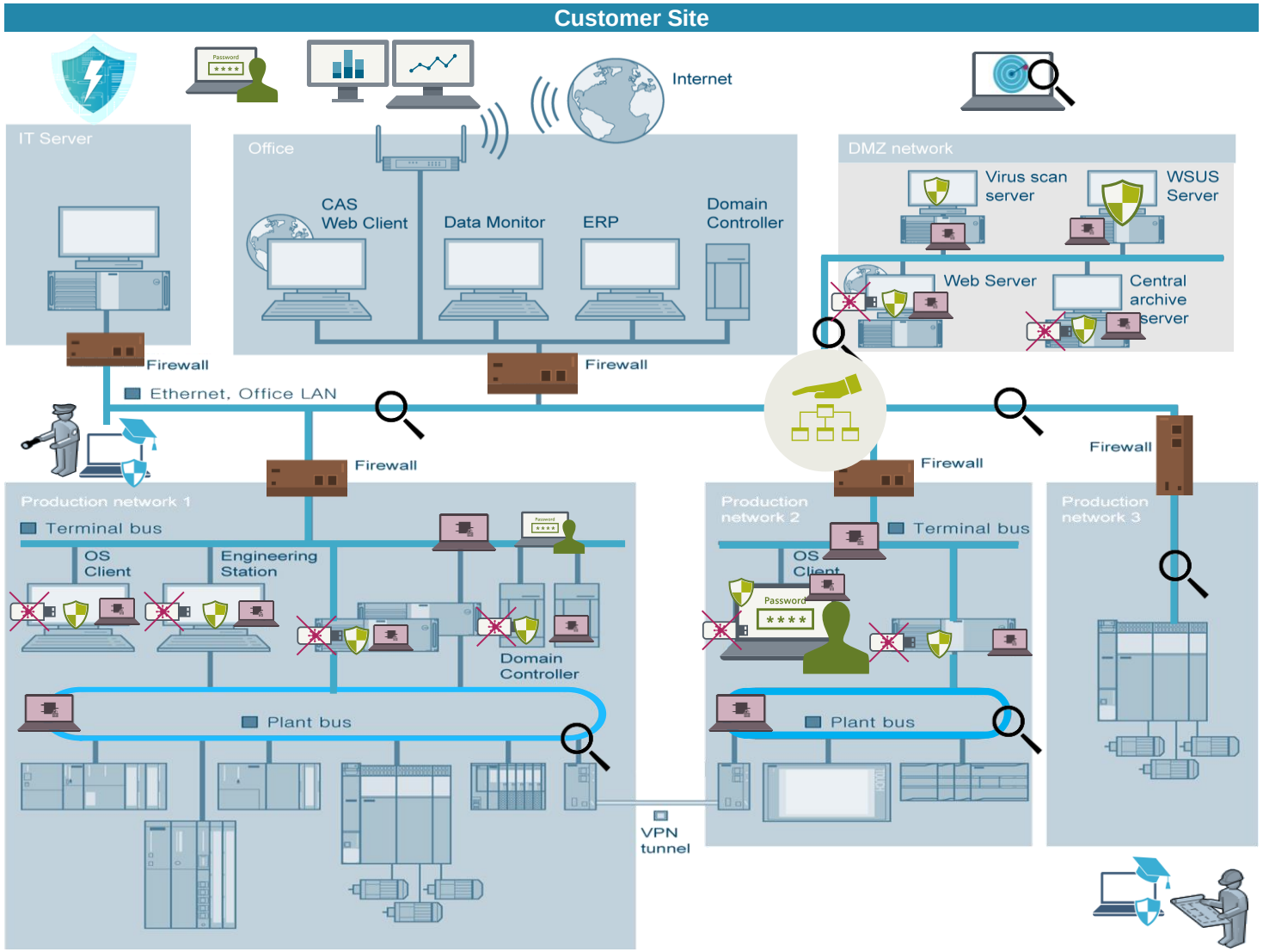


Maturity Level

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

Industrial Security Service Portfolio

SIEMENS
Ingenuity for life



Industrial Security Services

- **Security Awareness Training, Policy e Procedure**
- **Antivirus e Application Whitelisting**
- **System Hardening**
- **Identity and Access Management**
- **Firewalls and VPN**
- **Segmentazione di rete e DMZ**
- **Windows Patch**
- **Security Vulnerability Management**
- **Industrial Anomaly Detection**
- **Security Monitoring**

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

SIEMENS
Ingenuity for life

Security threats demand action

Plant security
- Meccanismi di protezione fisica per accesso ad aree critiche
- Implementazione processo di security management

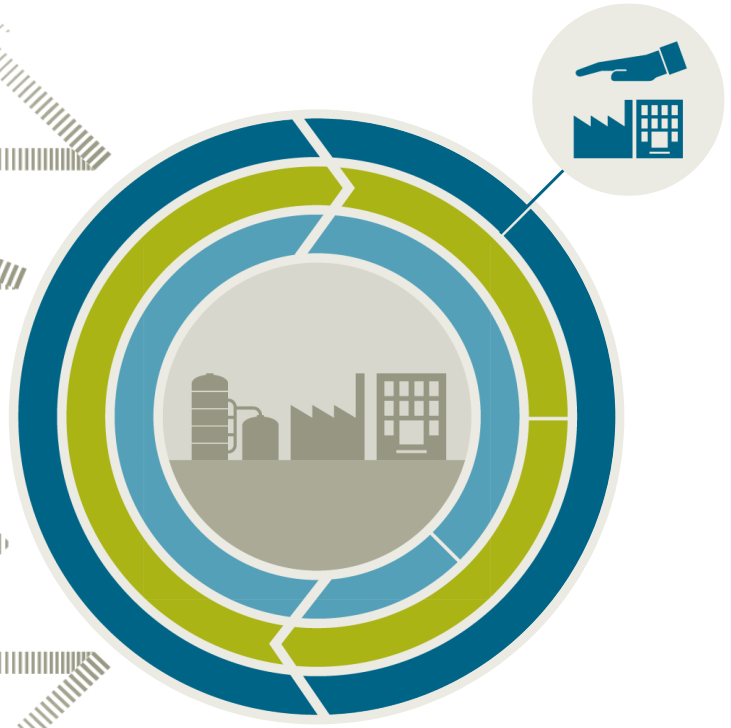
Network security
- Protezione di cella, DMZ assitenza remota
- Firewall e VPN

System integrity
- Hardening del sistema
- Piano di aggiornamento software permessi e antivirus
- Autenticazione riservata a gruppi di operatori

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

SIEMENS
Ingenuity for life

Defense in Depth



Plant security

- Meccanismi di protezione fisica per accesso ad aree critiche
- Implementazione processo di security management

Industrial Security Services
Assessment

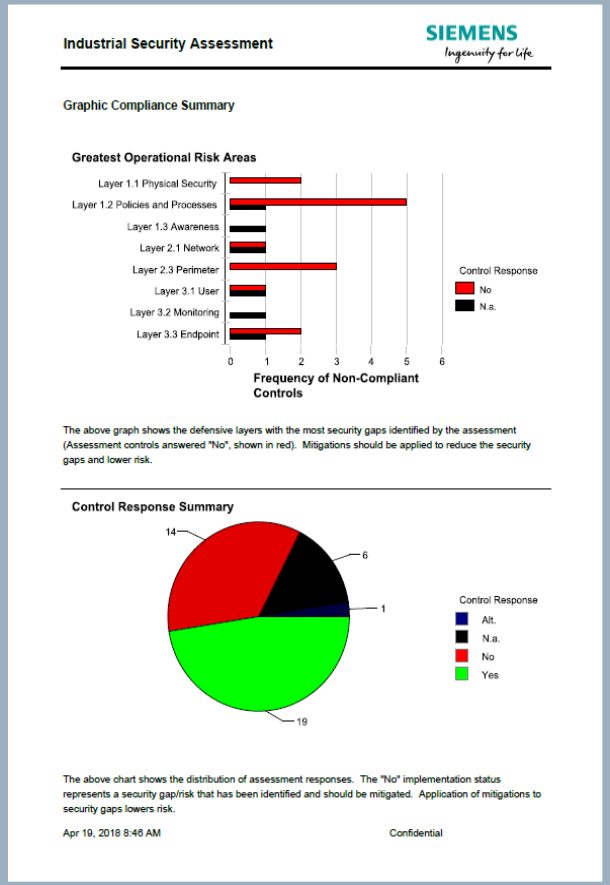
SIEMENS
Ingenuity for life

Industrial Security Check
derivato dallo standard IEC62443 e basato sul concetto di Defense-In Depth

Assessment IEC 62443
(e ISO 27001) per la sicurezza della fabbrica in funzione degli standard

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

Servizi di Scanning
per ottenere la trasparenza sugli asset e software usati nell'ambiente di automazione



Industrial Security Assessment SIEMENS Ingenuity for life

Graphic Compliance Summary

Greatest Operational Risk Areas

The above graph shows the defensive layers with the most security gaps identified by the assessment (Assessment controls answered "No", shown in red). Mitigations should be applied to reduce the security gaps and lower risk.

Control Response Summary

The above chart shows the distribution of assessment responses. The "No" implementation status represents a security gap/risk that has been identified and should be mitigated. Application of mitigations to security gaps lowers risk.

Apr 19, 2018 8:46 AM Confidential

Vulnerability	Risk score
Flat network architecture/ No DMZ available	x.x
Flat network architecture/ No network segmentation	x.x
Unsecure/ Not controlled remote activities	x.x
No system hardening/Unneeded applications and services installed	x.x
Unpatched operating system	x.x
Obsolete Antivirus database	x.x
Windows firewall not active	x.x
Uncontrolled USB interfaces	x.x

Red (7.5 – 10) = Unaccaptable risk; Urgent action is necessary
Orange (5 – 7.5) = Unaccaptable risk; Acrtion is required
Yellow (2.5 – 5) = Accaptable risk; Subject to management approval
Green (0 – 2.5) = Accaptable risk; No action required

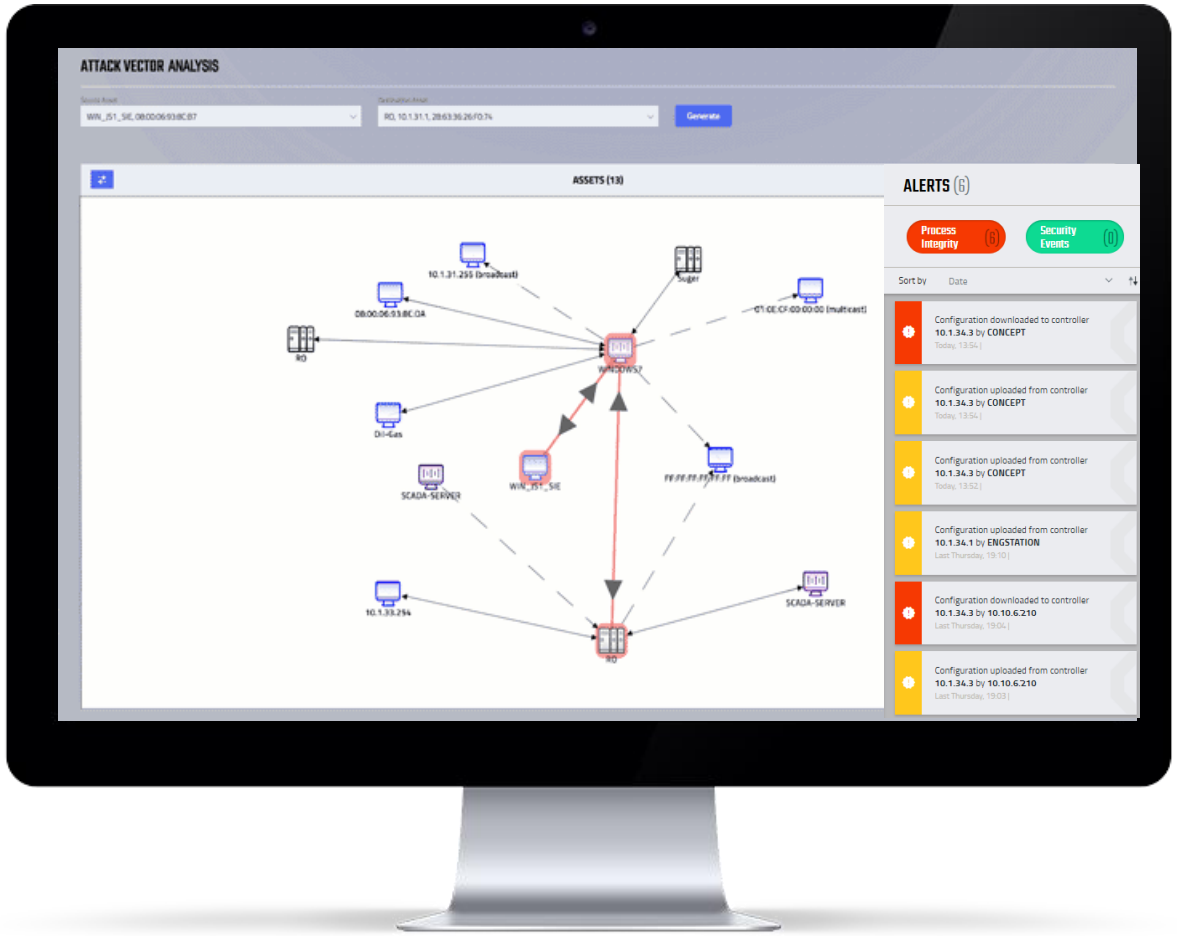
Industrial Anomaly Detection (IAD)
Cos'è e cosa fa?

SIEMENS
Ingenuity for life

Monitora la security in modo totalmente passivo e automatico!!!

1. Rileva i dispositivi (PLC, PC, drives…) **e le loro caratteristiche** (versione software, …)

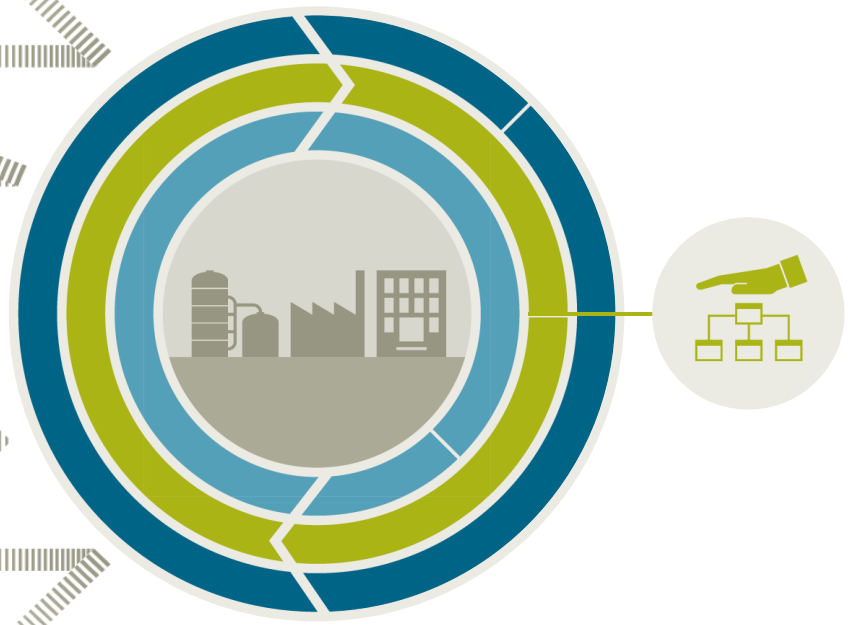
2. Avvisa in caso di attività ritenute anomale (es. PLC che inizia mandare comandi "strani")



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

SIEMENS
Ingenuity for life

Defense in Depth



Network security

- Protezione di cella, DMZ assitenza remota
- Firewall e VPN

Switch managed
"Go Managed!!!"

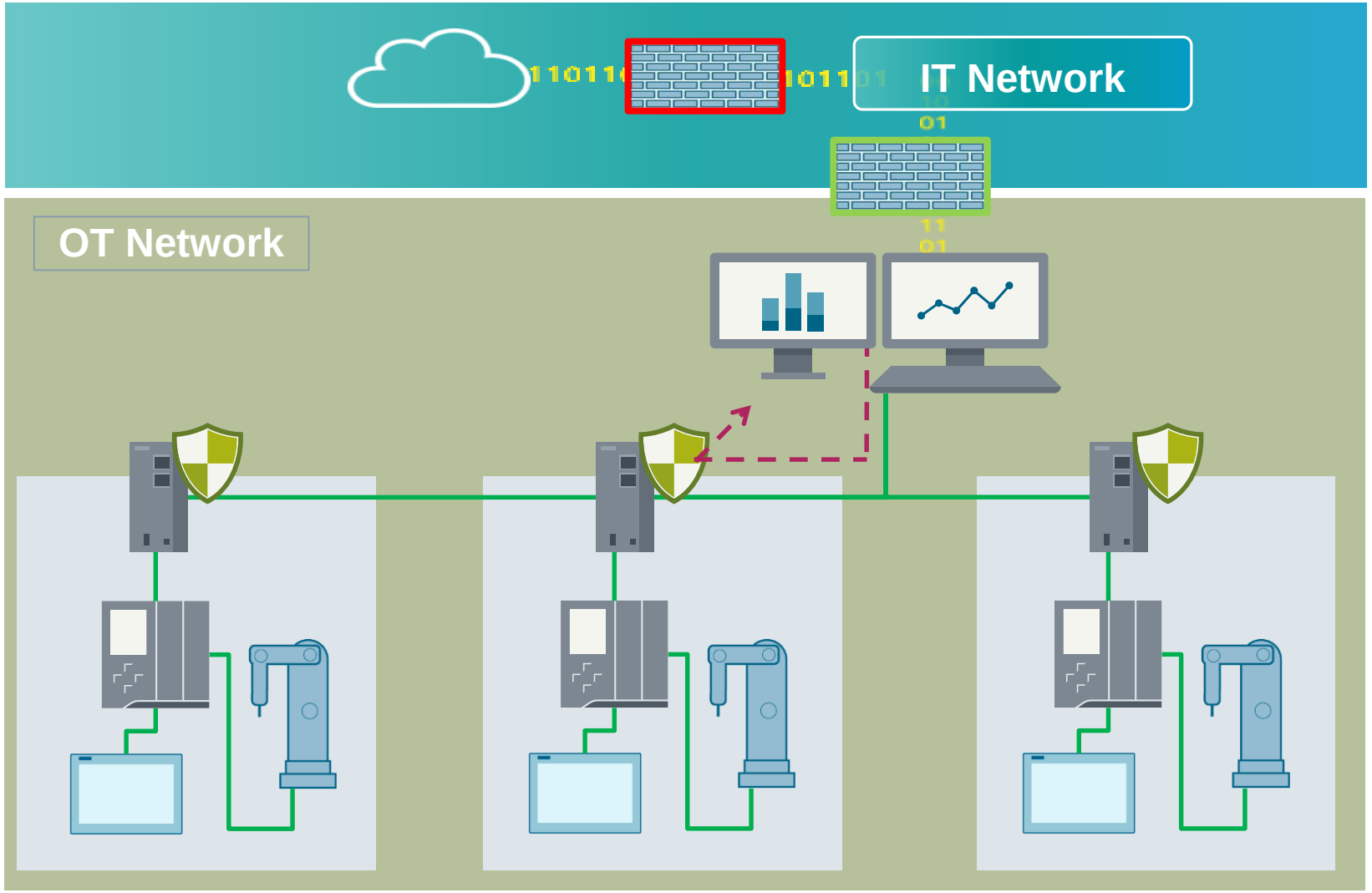
SIEMENS
Ingenuity for life

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

Network Security
Firewall: Protezione e segmentazione della rete

SIEMENS
Ingenuity for life

- Separazione della rete OT in **celle di protezione**
- Connessioni autorizzate tramite **Firewall**
- Dispostivi **CP** con **Security Integrated** e **Scalance S**



Network Security
SCALANCE S: Industrial security appliance

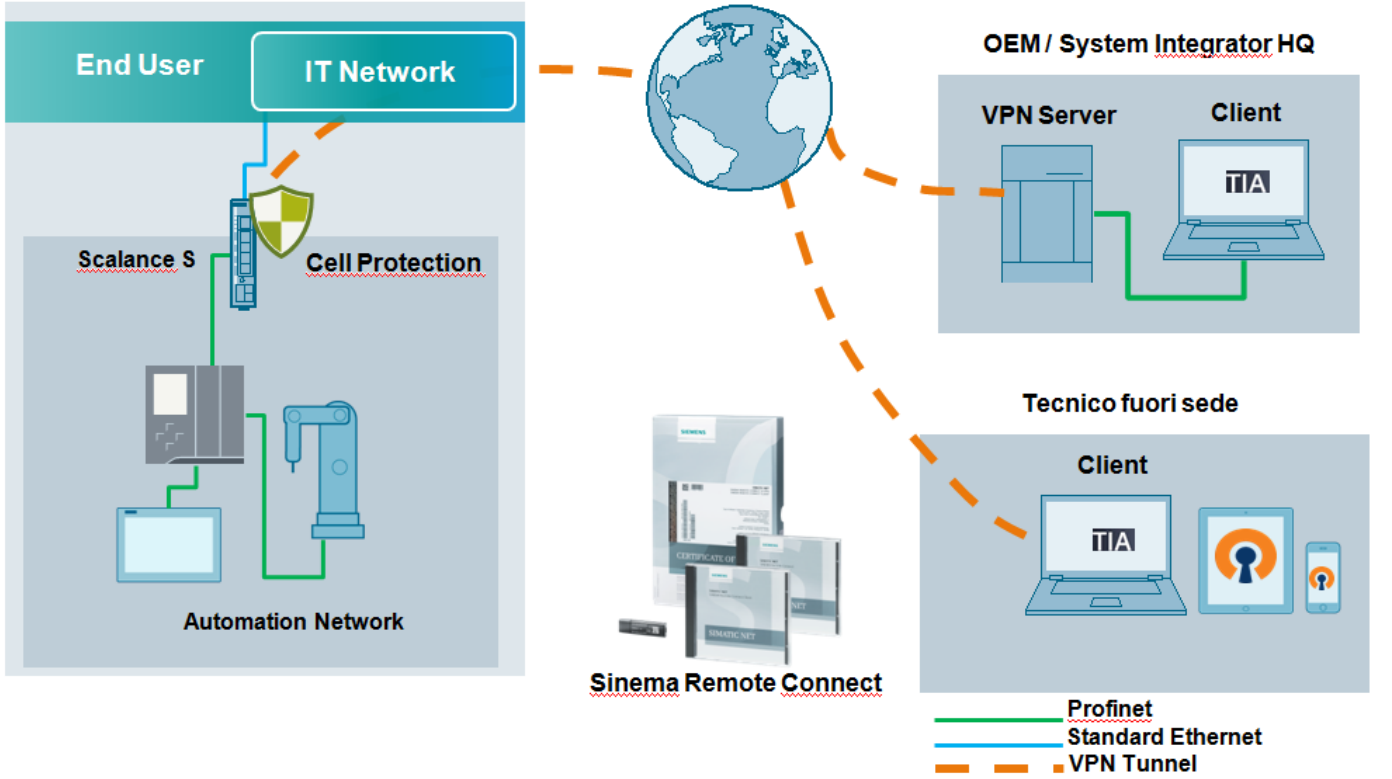
Scalance SC e Scalance S615

Funzionalità
• Gigabit Firewall (Scalance SC) • Creazione di celle di sicurezza tramite VLAN
• Stateful Inspection **Firewall** • **Bridge** Firewall (SC) • Firewall su base utente
• **VPN con SINEMA RC**
• Instaurazione del tunnel **VPN** tramite **Digital input**
• Configurazione automatica di Sinema RC
• **Integrazione** completa in **TIA portal**

SINEMA Remote Connect
La soluzione per una teleassistenza sicura

SIEMENS
Ingenuity for life

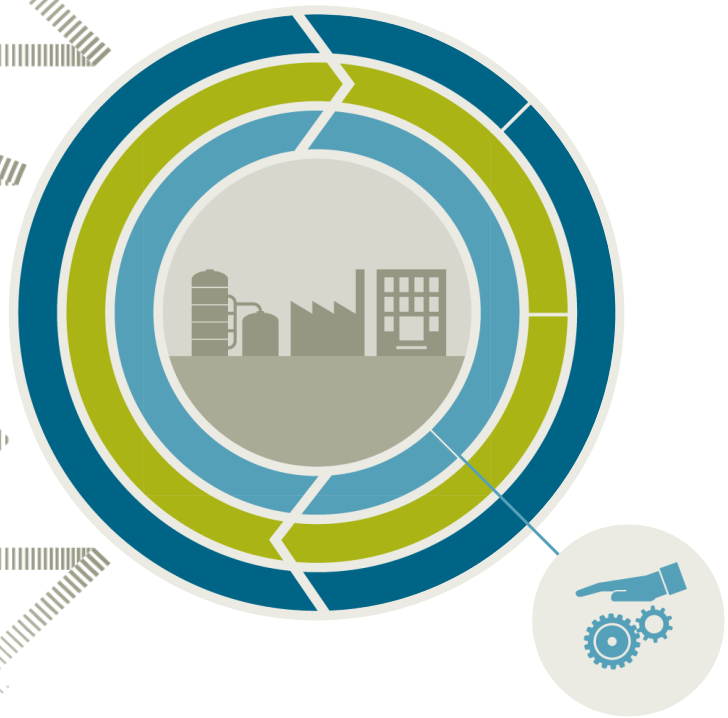
- **Connessioni VPN** di **dispositivi** e **utenti** tramite gestione centralizzata
- Comunicazione crittografata con tecnologia **OpenVPN**
- Attivazione VPN tramite **digital input**
- **Autenticazione a due fattori** (password e PKI)



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

SIEMENS
Ingenuity for life

Defense in Depth



System integrity

- Hardening del sistema
- Piano di aggiormanto software permessi e antivirus
- Autenticazione riservata a gruppi di operatori

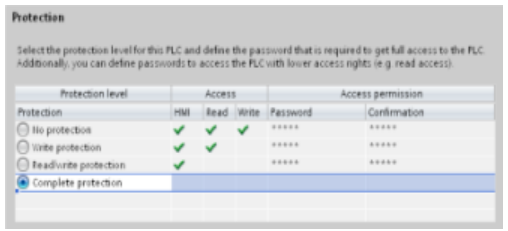
System Integrity
Nuovi Controllori SIMATIC

SIEMENS
Ingenuity for life

Protezione accesso fisico

Protezione del know-how

Protezione accesso utenti



Protezione della copia

Firma digitale su firmware

OPC UA

Web Server (HTTPS)

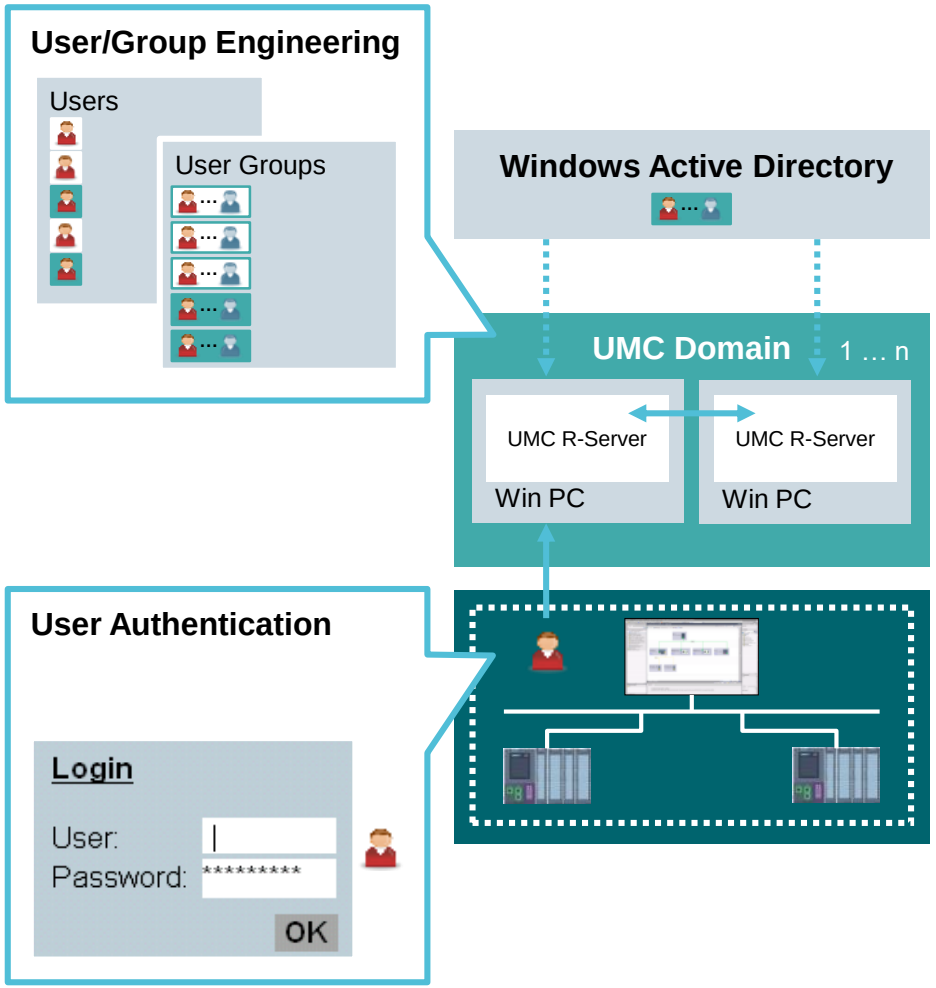
Secure Open User Communication (TLS)

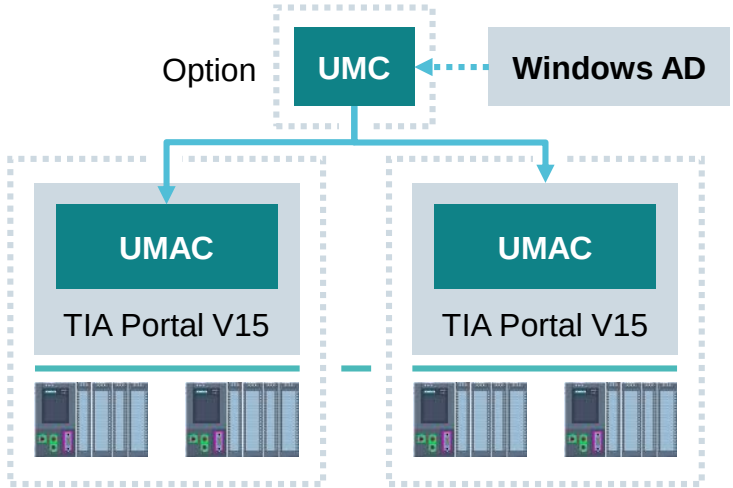
Opzioni TIA Portal

Gestioni utenti su tutto il sistema con UMC

SIEMENS
Ingenuity for life

UMC = User Management Component

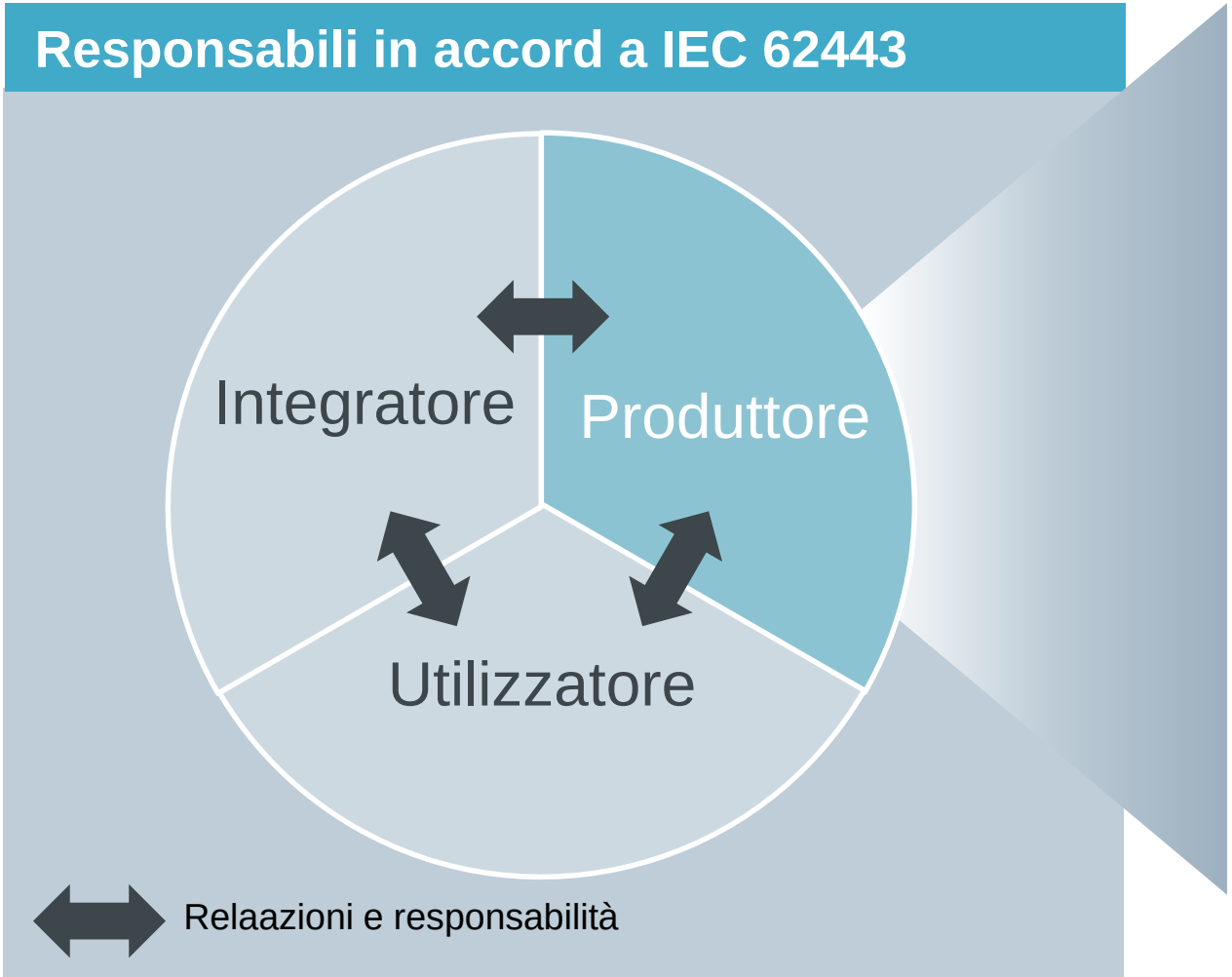




Certificazione IEC 62443-4-1
Product Development Lifecycle

SIEMENS
Ingenuity for life

Responsabili in accord a IEC 62443



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

Keep in mind!

Keep your business, your business!

SIEMENS
Ingenuity for life