



Cybersecurity nei sistemi industriali

Gennaio 2020

Umberto Cattaneo
Cybersecurity CBC,
PMP, Sec+, IEC62443 Certified specialist

EMAIL
Umberto.cattaneo@se.com





Umberto Cattaneo

Cybersecurity Business Consultant

Biografia:

Dr. Fisica Cibernetica ,

Certificazioni: PMP, CompTIA Security +,

ISA99/IEC62443 Certified Specialist

Oltre 30 anni di esperienza nell'integrazione dei sistemi, Oil&Gas, SCADA, soluzioni di crittografia, implementazione di reti nazionali di comunicazione sicura, sistemi di comando e controllo, GMDSS, ITS, GIS

Occupazioni precedente:

Eni

AGUSTA –Leonardo Elicotteri

Sirti

Qnective AG (Svizzera)

Membro di: IEC, ANIE, ISA, Clusit, PMI©

Diversi articoli pubblicati su argomenti di cybersecurity per i sistemi industriali e le infrastrutture critiche



MOBILE

+39 335 5821626



EMAIL

Umberto.cattaneo@se.com

Cybersecurity nei sistemi industriali

- Differenze tra IT e OT
- Come proteggere un Sistema di Controllo Industriale
- Lo standard ISA99/IEC62443
- Leggi in Italia: DL NIS e succ.
- 10 Suggerimenti
- I 5 passi della Cybersecurity
- Case study
- Q&A

Quali sono i driver della digitalizzazione nell'industria?



CONNETTIVITA'

- Dispositivi connessi intelligenti (prodotti)
- Connettività standard-driven
- Minor costo di Misurazione



MOBILITA'

- Comunicazione pervasiva e conveniente
- Accesso remoto
- Interfacce user-driven



CLOUD

- Massiccia aggregazione di dati
- Accesso ai dati da parte di specialisti
- Eco-sistema di sviluppatori di applicazioni industriali



ANALYTICS

- Applicazioni cognitive
- Intelligenza artificiale che ottimizza le prestazioni a tutti i livelli

Top 10 Minacce 2020* (prima della crisi Covid-19)

Rank		Trend	2019
1	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	↑	2
2	Business interruption (incl. supply chain disruption)	↓	1
3	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	↑	4
4	Natural catastrophes (e.g. storm, flood, earthquake) ¹	↓	3
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	=	5
6	Fire, explosion	=	6
7	Climate change/increasing volatility of weather	↑	8
8	Loss of reputation or brand value	↑	9
9	New technologies (e.g. impact of artificial intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)	↓	7
10	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	↑	13

Cyber Threats in Industrial Control Systems are Growing Exponentially, Impacting Equipment Availability and Safety

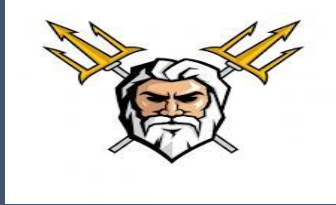
2010



Stuxnet
Iran nuclear plant

45,000 machines infected in Iran, Germany, France, India, Indonesia

2011



Zeus

"Zeus" malware, available for about \$1200, were able to steal over \$12 million from five banks in the US and UK.

2012



Shamoon
Saudi Aramco attack

30,000 Windows-based machines infected

2013



HaveX

Malware embedded into **vendor software**.
Gathered **OPC** tag data for later attack.

2014



German steel mill

Breakdowns of individual control components led to the uncontrolled **shutdown of a blast furnace**

2015



Ukraine

200K+ without power.
Remote control of SCADA.
Destruction of device firmware.

CAMPARI

LUXOTTICA

2016



Shamoon 2

Civil Aviation, KSA government agencies
Thousands of machines Wiped

2017



Triton

First attack targeted to Safety Instrumental Systems (SIS) in Middle East.

2017



NotPetya

Danish Shipping MAERSK port terminal attacked by ransomware: shut down for 2 days 300 Mil USD Loss

2018



Shamoon 3 SAIPEM

Saipem targeted with a modified version of the Shamoon virus, taking down hundred computers in the UAE, Saudi Arabia, Scotland, and India

2019



Venezuela power grid

Venezuelan power grid was out of services for 2 days due to suspicious cyber attack

2019



Norway aluminium plant

Ransomware LockerGoga blocked plants over 40 countries

2020

GEOX RESPIRA

enel

GARMIN.

Life Is On

Schneider Electric

I più comuni danni derivanti da attacchi cyber

**Violazione dati
confidenziali: segreti
industriali e dati sensibili**

Costo per contenimento danno
Violazione privacy
Danno reputazionale
Spese legali
Furto proprietà intellettuale
Responsabilità civile C-level

**Malfunzionamento reti
sistemi IT e OT**

Interruzione di esercizio
Risarcimento danni e/o multe
Danni a dipendenti
Danni all'ambiente
Danni fisici all'impianto
Danno reputazionale
Responsabilità civile C-level

**Cancellazione e
deterioramenti dati
Es.: Virus, Wiper, ...**

Costo per contenimento danno
Perdita dati
Spese legali
Responsabilità prodotti
Responsabilità civile C-level

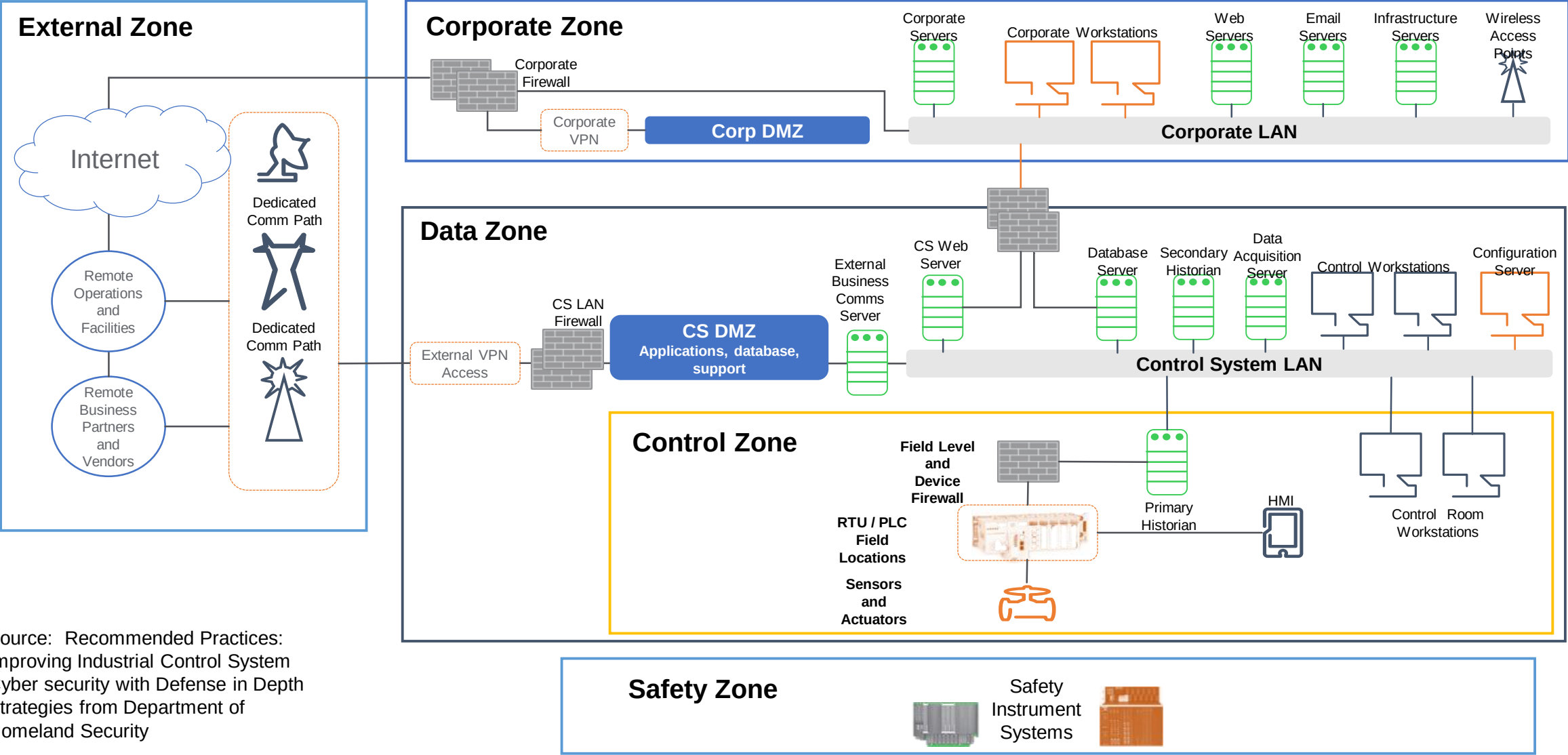
**Criptatura dati e
furto/Riscatto**

Costo per contenimento danno
Riscatto per estorsione dei dati
Frode finanziaria
Responsabilità civile C-level

Da dove vengono le minacce



Architettura di un Sistema di controllo (Purdue)



Source: Recommended Practices:
Improving Industrial Control System
Cyber security with Defense in Depth
Strategies from Department of
Homeland Security

Key concepts: Data Privacy & Cybersecurity

Cos'è la data privacy?



Data privacy si riferisce ai requisiti di protezione e confidenzialità, stabiliti per la manipolazione, la condivisione e la memorizzazione di informazioni personali (PII).

- Esempio: GDPR European regulation

Cos'è la cybersecurity?



Cybersecurity è l'arte di proteggere in modo sicuro reti, dispositivi, programmi e dati da accessi non autorizzati o uso criminale, garantendo al contempo la riservatezza, l'integrità e la disponibilità di informazioni.



GDPR, ISO 27001



NIS IEC62443, NIST, NERC

Operational Technology



I sistemi e le reti sono usati per far funzionare I processi produttivi negli impianti.

Le priorità sono la continuità operativa e la sicurezza di persone e ambiente.

Vs.

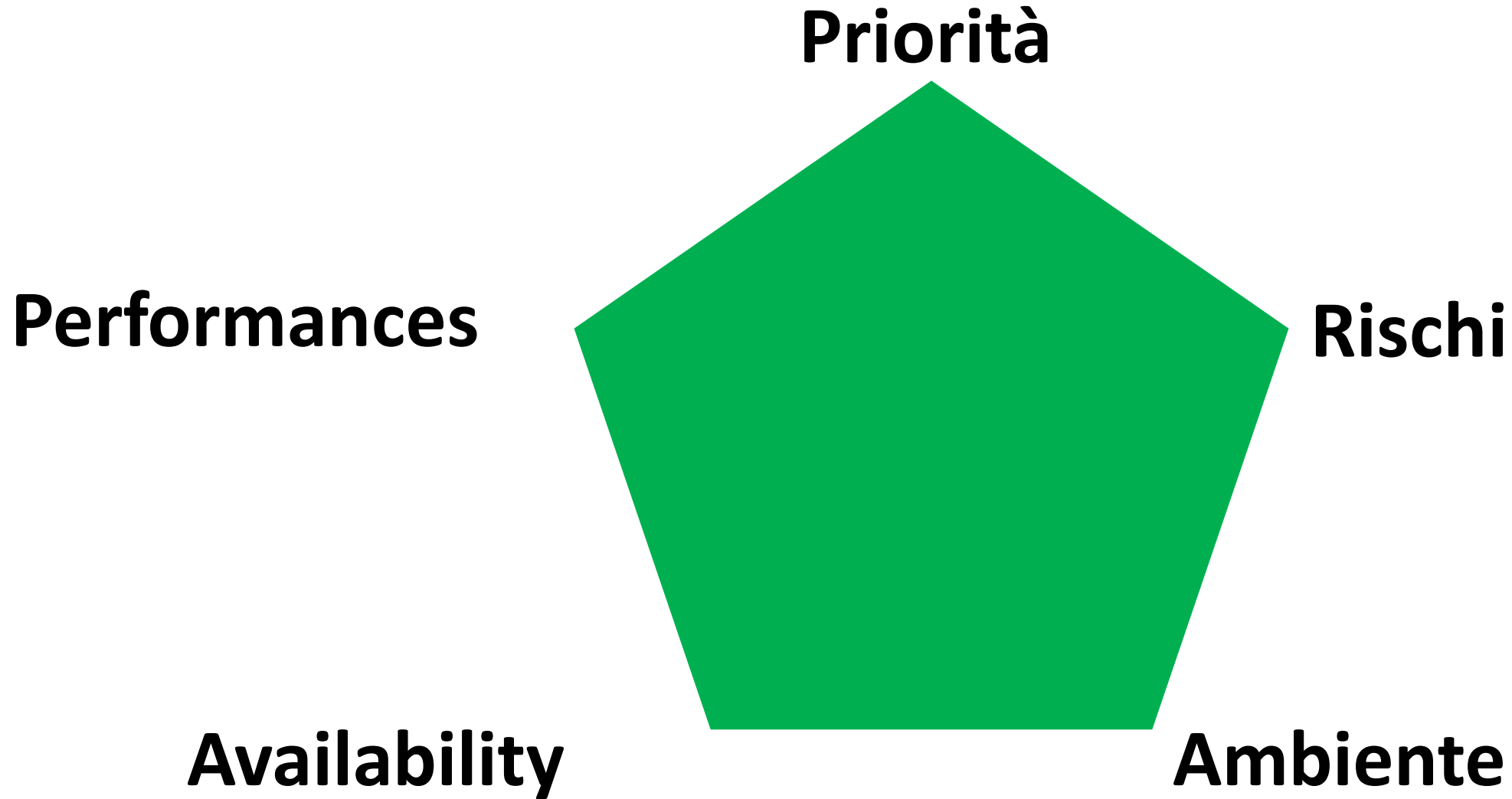
Information Technology



I sistemi e le reti sono usati per gestire processi di business e per la diffusione di informazioni (social media, siti web, e-commerce,...)

Le priorità sono la confidenzialità dei dati, la loro integrità e la continuità operativa.

Differenze tra IT e OT: le 5 aree



Differenze tra IT e OT



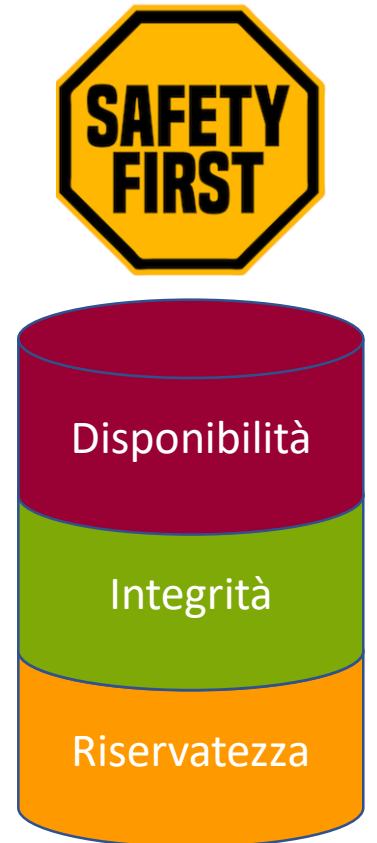
Priorità



IT



LAB

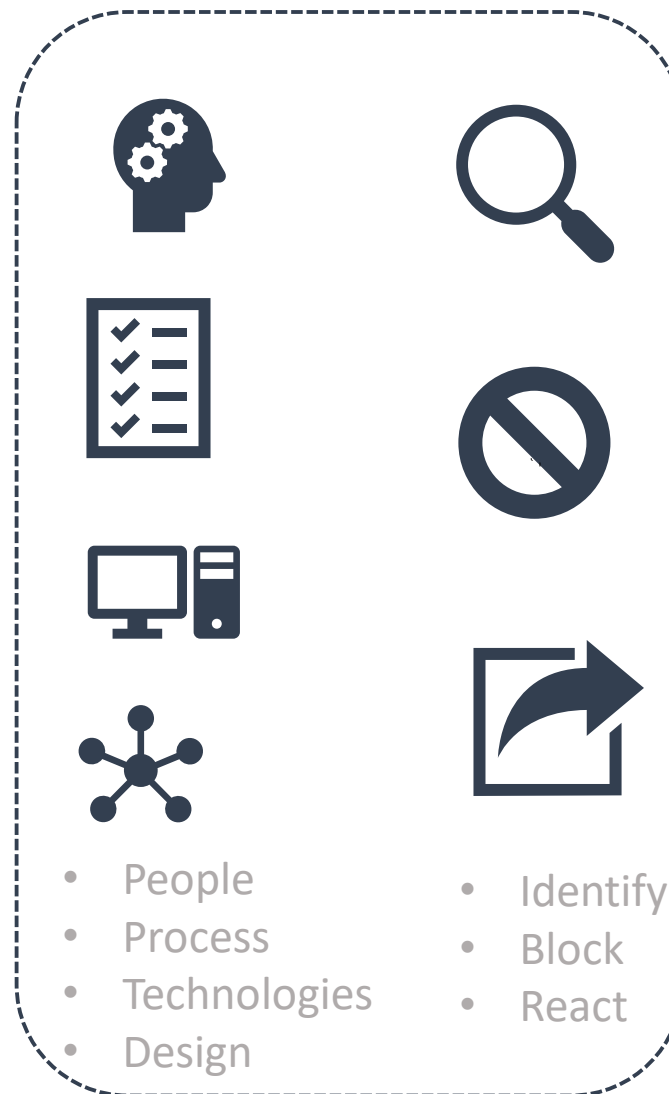


OT

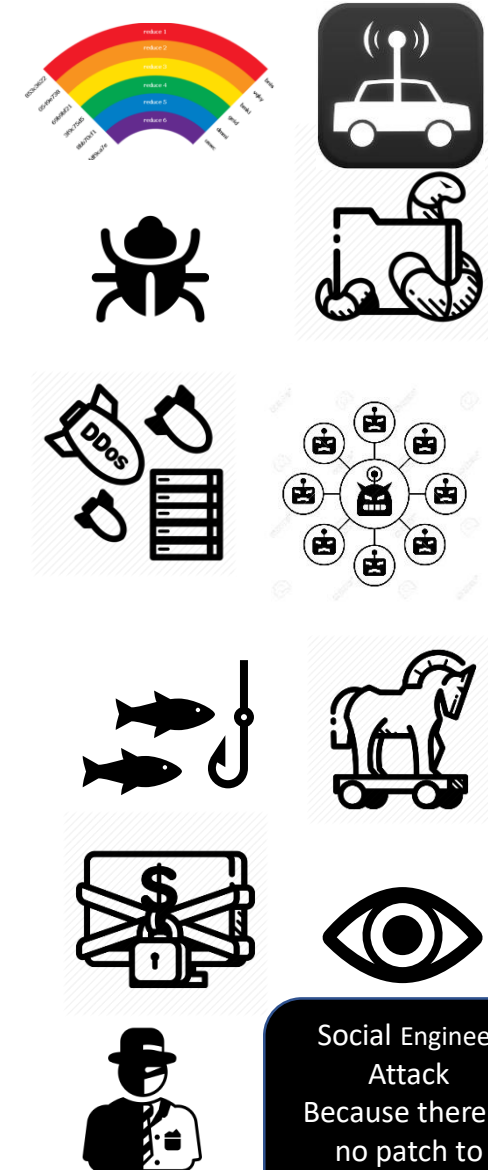
Scopo della Cybersecurity



Cosa proteggere



confidenziale



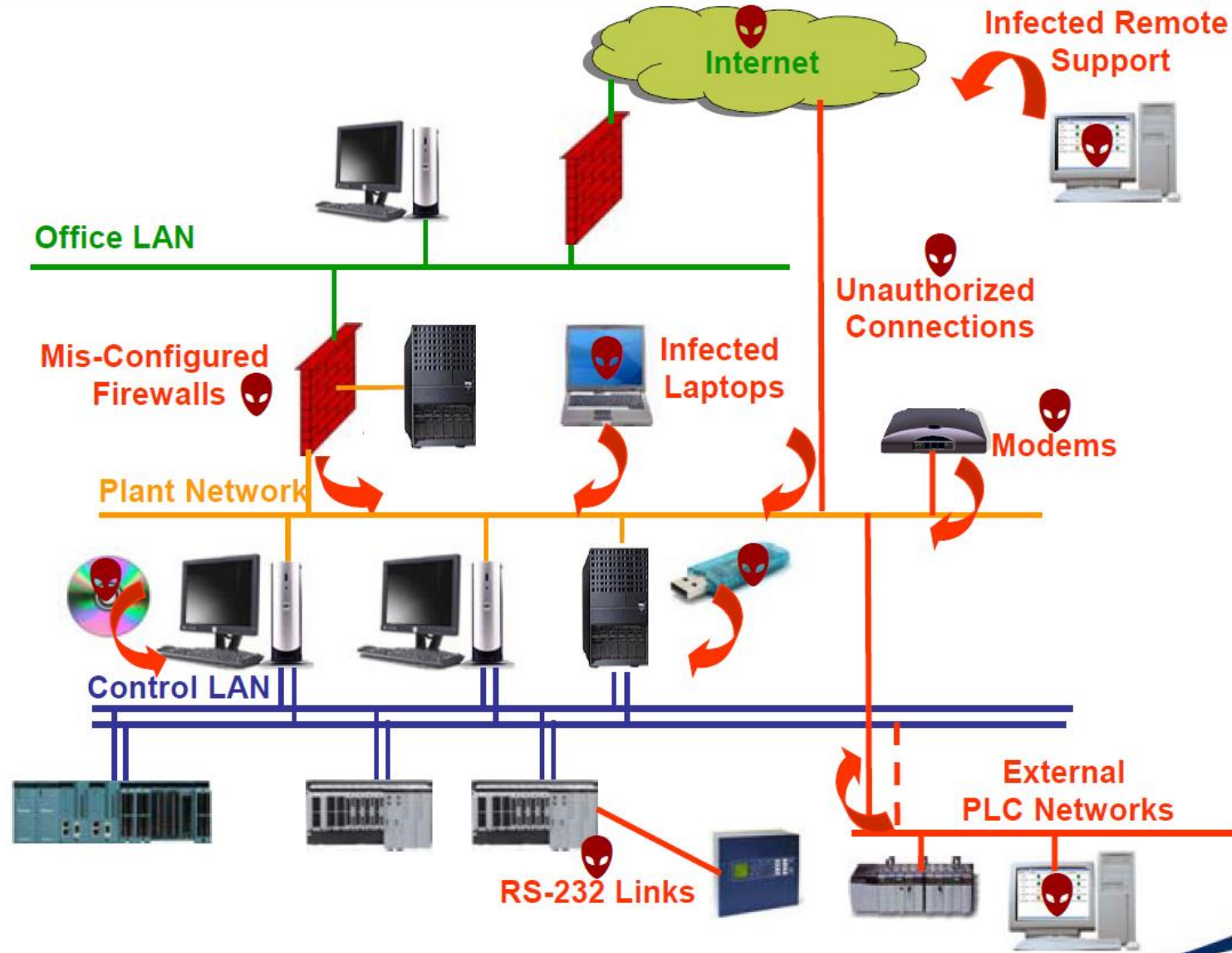
Social Engineer
Attack
Because there is
no patch to
human stupidity

Cyber Attacch: **Schneider Electric**

I 5 falsi miti sulla sicurezza industriale

- Mito 1 "Non siamo connessi a Internet..."
- Mito 2 I Sistemi di controllo sono dietro un firewall
- Mito 3 Gli hacker non capiscono i sistemi di controllo
- Mito 4 La nostra struttura non è un bersaglio
- Mito 5 I nostri sistemi di sicurezza ci proteggeranno

Falso mito 1: "Non siamo connessi a Internet..."



Falso mito 2: «Hackers Non capiscono i Sistemi di Controllo Systems»

IT & Software > Hardware > PLC

Learn 5 PLCs in a Day-AB, Siemens, Schneider, Omron & Delta

PLC Programming of Allen Bradley, Delta, Siemens, Omron & Schneider using LIVE Examples with HMI Interfacing

Bestseller 4.4 ★★★★★ (3,227 ratings) 15,452 students

Created by [Rajvir Singh](#), [Rajvir Singh](#)

⚙️ Last updated 9/2019 🌐 English 📺 English [Auto]

[Wishlist](#) [Share](#) [Gift this course](#)



Preview this course

€12.99 ~~€49.99~~ 74% off

 **Find the right course for you**
Answer a few questions to get personalized recommendations.

<https://www.udemy.com/course/nfi-plc-online-leaning/>

Falso mito 3: «La nostra struttura non è un obiettivo»

..attaccate nel 2020:

 **Bonfiglioli**
Forever Forward

 **GEFOX**
RESPIRA

 **GRUPPO HERA**

LUXOTTICA®

 **enel**

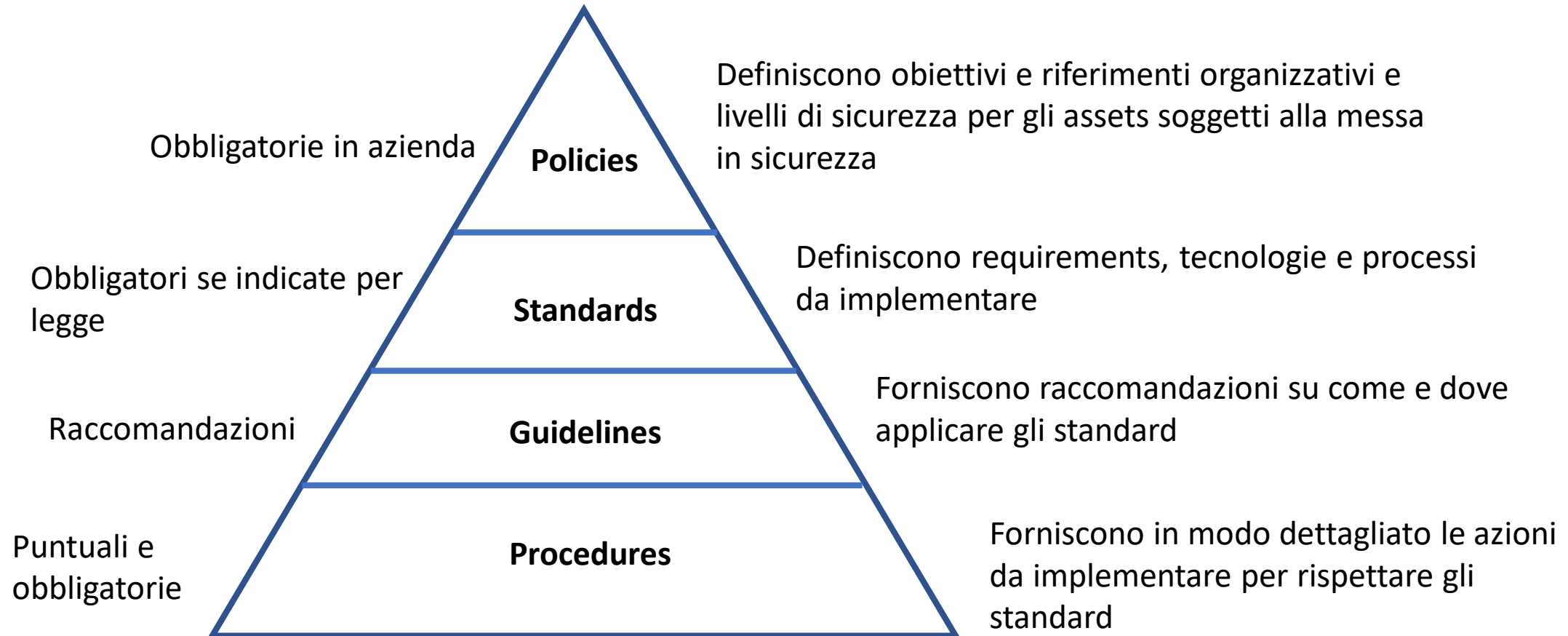
 **CAMPARI**

GARMIN®

 **HONDA**

Un approccio sistematico alla cybersecurity

Adapted from IEC62443-1-1
Gerarchie di controllo



International standards compliance



ISA99/IEC62443: Un approccio sistematico alla cybersecurity

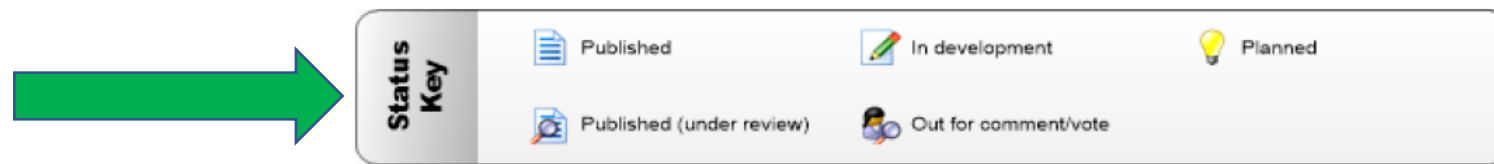
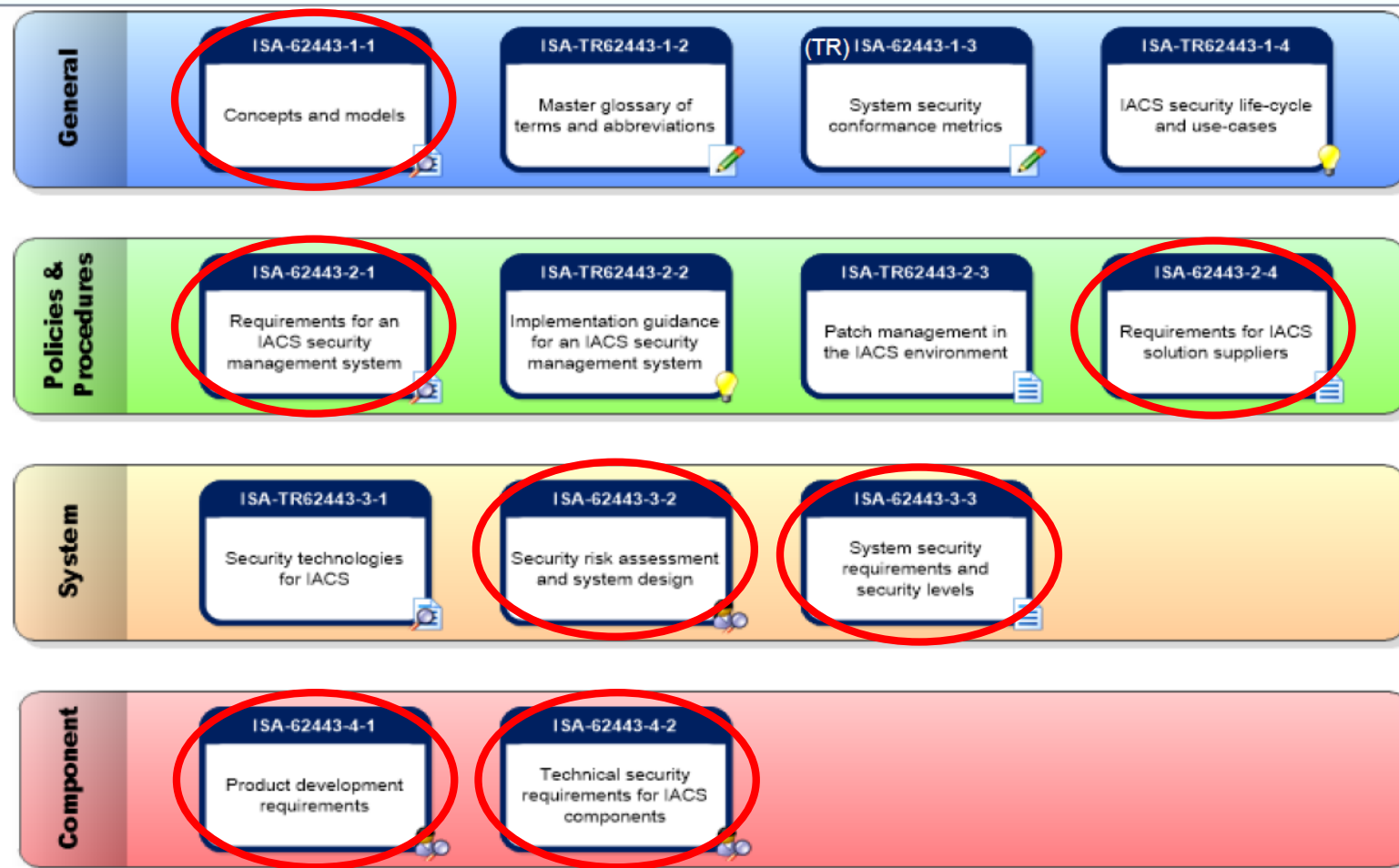
Overview

4 Livelli

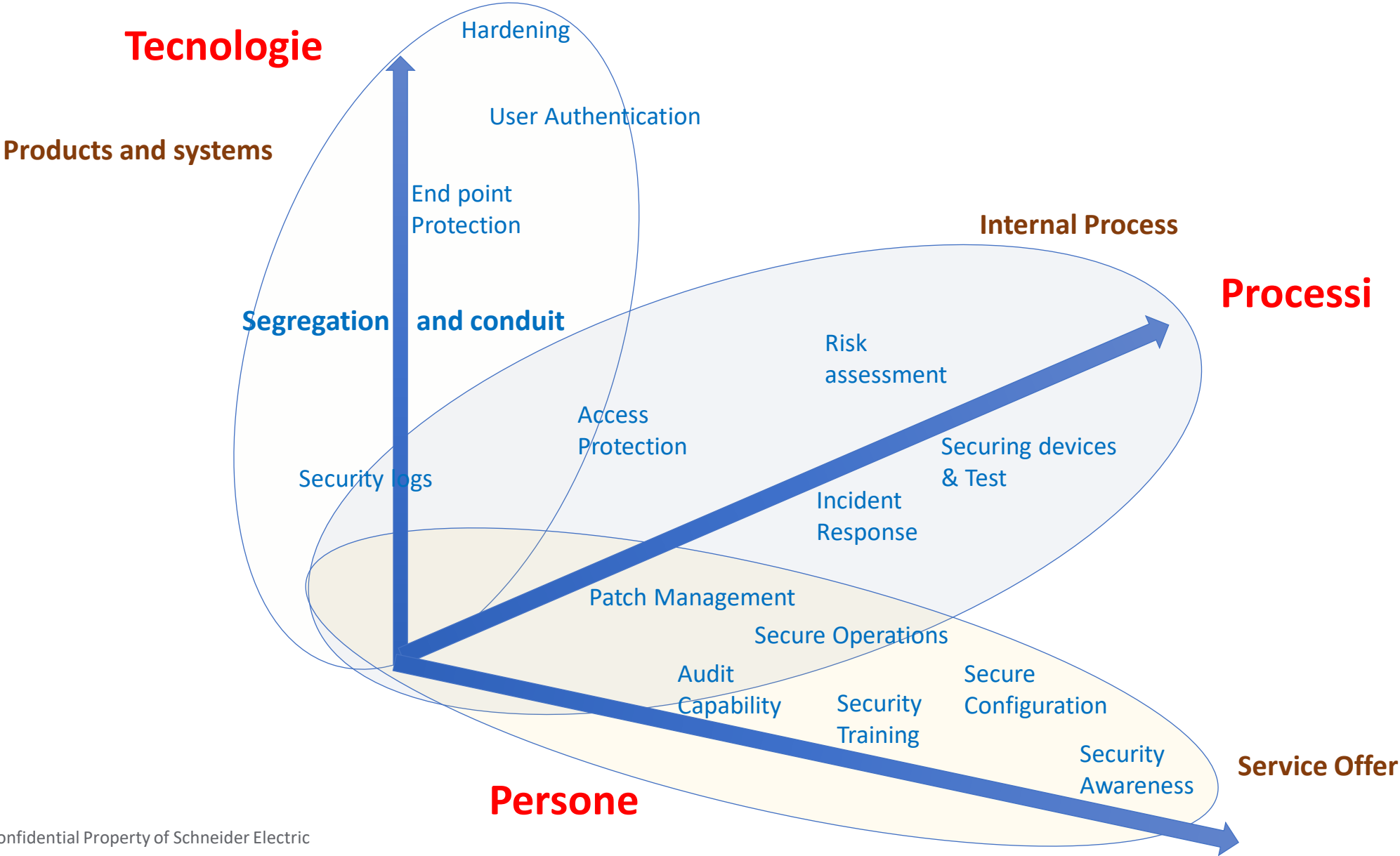
13 Pubblicazioni:

7 Standard

6 Technical Reports

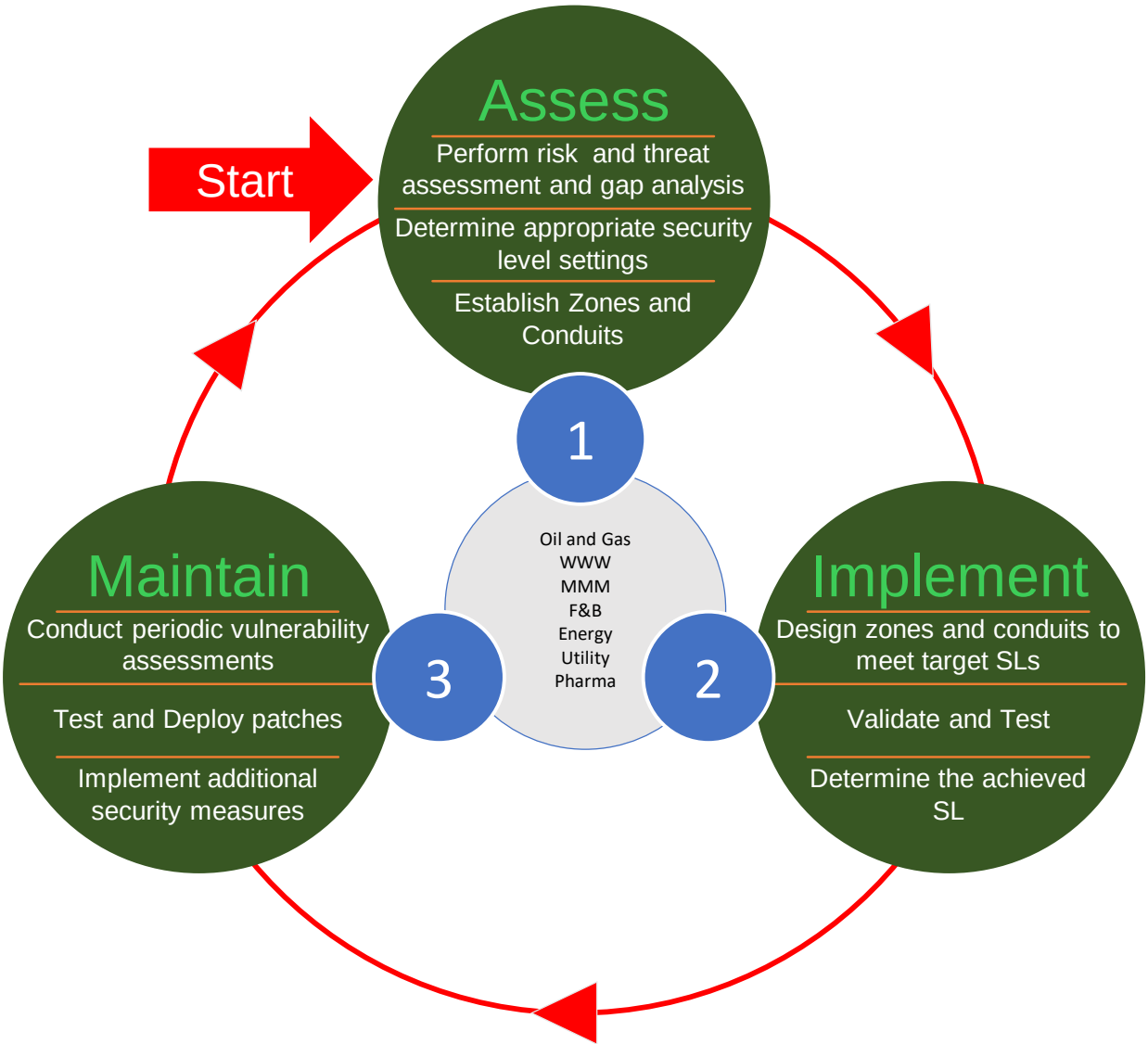


Linee Guida di Cybersecurity



Un approccio sistematico alla cybersecurity

Adapted from IEC62443-1-1

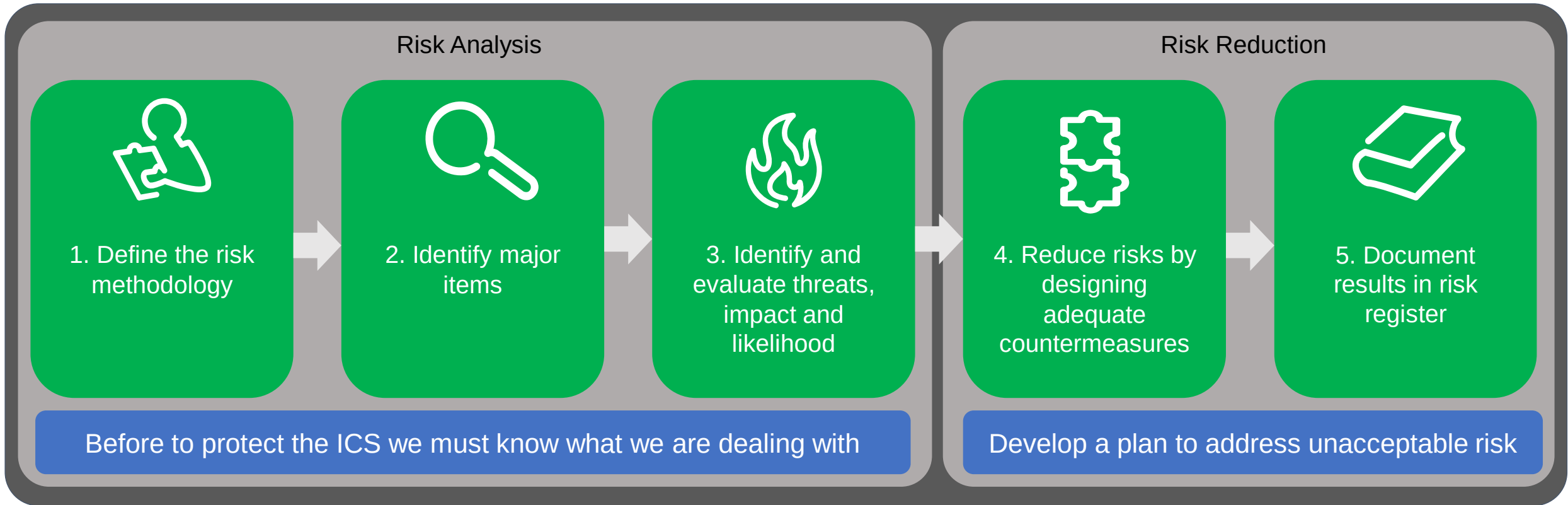




Assess

I rischi e le minacce

Cyber Security Risk Assessment



Each assessment must be site specific

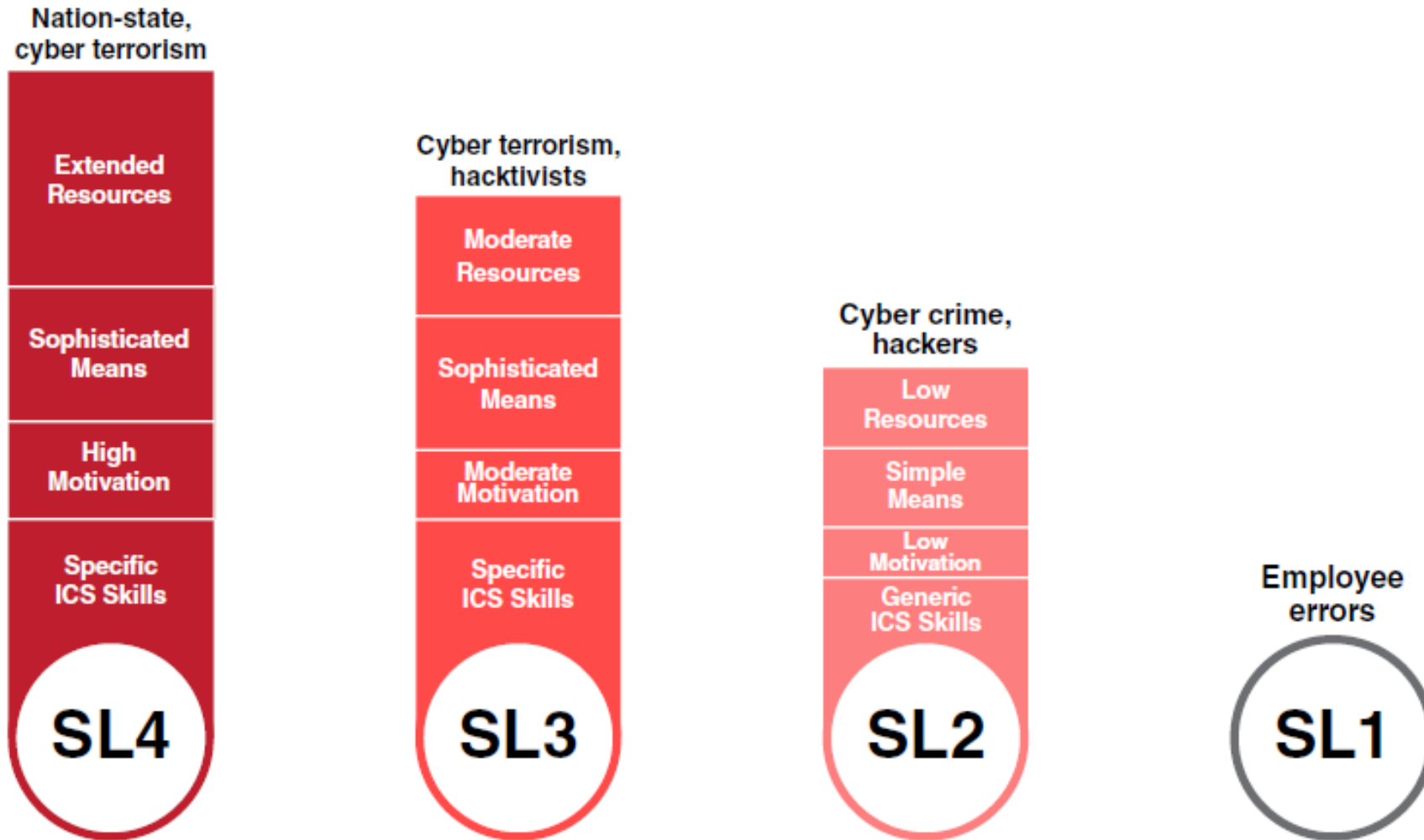


Sviluppare e implementare Defence in depth

Chi sono le minacce?

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hactivists usano computer e reti per promuovere le loro idee politiche e sciali	Individui e sofisticate organizzazioni criminali rubano informazioni personali e fanno estorsioni per soldi.	Insiders rubano informazioni e per ragioni personali, finanziarie ed ideologiche.	Organizzazioni nemiche conducono intrusioni informatiche per rubare segreti di stato e informazioni proprietarie da società private	Gruppi terroristici sabotano i sistemi informatici che gestiscono le nostre infrastrutture critiche come la rete elettrica.	Organizzazioni nemiche sabotano i sistemi di infrastrutture militari e critici per ottenere un vantaggio in caso di conflitto.

IEC 62443.3.3 Security Level (SL)



Quale modello di sicurezza applicare?

Single Layer



La maggioranza dei casi

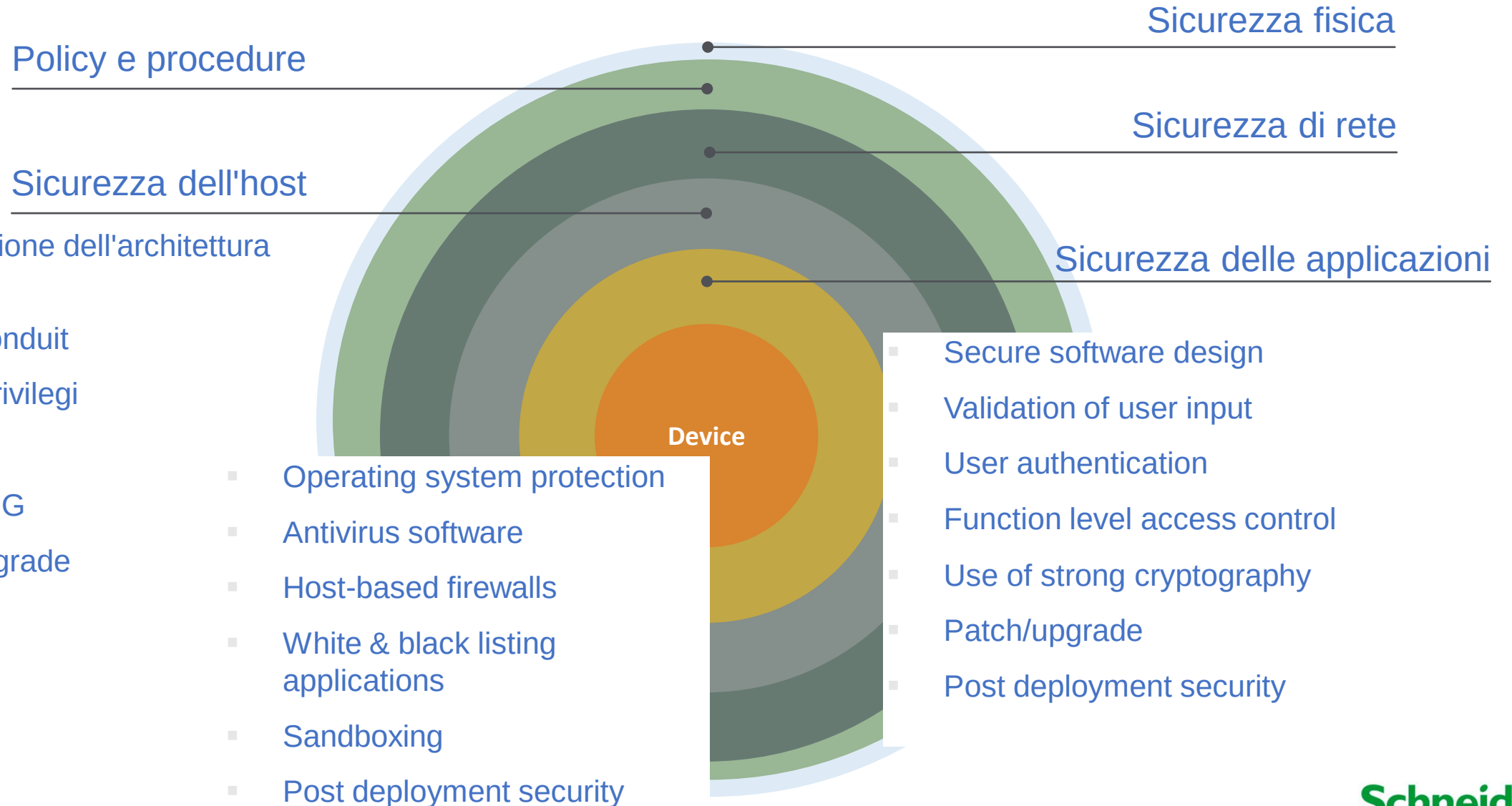
VS

Defense in depth



L'approccio corretto

Defense in depth



Elementi di valutazione dei Security Level per IACS

As per IEC 62443

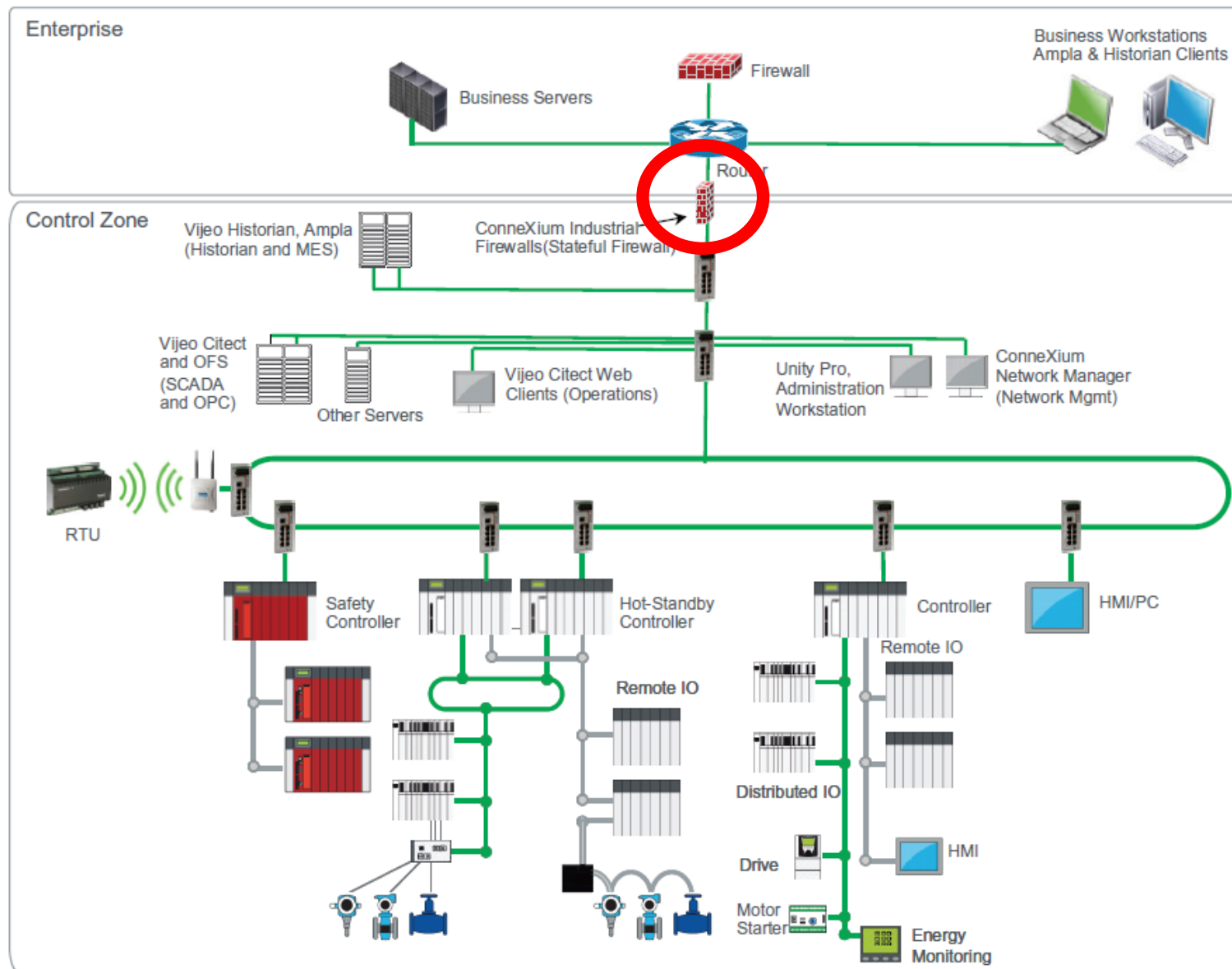
FR 1: Identification and authentication control (IAC)	FR 2: User Control (UC)	FR 3: System Integrity (SI)	FR 4: Data Confidentiality (DC)
Human user identification and authentication	Authorization enforcement	Communication integrity	Information confidentiality
Software process and device identification and authentication	Wireless use control	Malicious code protection	Information persistence
Account management	Use control for portable and mobile devices	Security functionality verification	Use of cryptography
Identifier management	Mobile code (e.g. javascript, Java ...)	Software and information integrity	
Authenticator management	Session lock	Input validation	
Wireless access management	Remote session termination	Deterministic output	
Strenght of password based authentication	Concurrent session control	Error handling	
Public Key Infrastructure (PKI) certificates	Auditable events	Session Integrity	
Strenght of public key authentication	Audit storage capacity	Protection of audit information	
Authenticator feedback	Response to Audit processing failure		
Unsuccesful login attempt (limitation)	Timestamp		
System use notification	Non repudiation		
Access via untrusted networks (monitor and control all methods of access)			

Elementi di valutazione dei Security Level per IACS

As per IEC 62443

FR 5: Restricted Data Flow (RDF)	FR 6: Timely Response to Event (TRE)	FR 7: System Availability (SA)
Network segmentation	Audit log accessibility	Denial of service protection
Zone boundary protection	Continuous monitoring	Resource management
General purpose person-to-person communication restrictions (email, social networks and so on...)		Control System Backup
Application partitioning		Control system recovery and reconstitution
		Emergency power
		Network and security configuration settings
		Control system component inventory

SL 0



Cybersecurity solutions portfolio – Level 1 (SL-1 compliant)



Access

- Authentication, Authorization, Accounting
- Network Segmentation



Protect

- Endpoint protection anti-virus, anti-malware,
- Patch Management



Detect

- Security Information & Event Management (SIEM)
- Network performance monitoring
- Anomaly Detection
- Intrusion Detection (NIPS)
- SOC / NOC



Respond

- Backup / Disaster Recovery

Cybersecurity solutions portfolio – Level 3 (SL-3 compliant)



Identify

- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security



Protect

- Endpoint protection anti-virus, anti-malware,
- DLP, HIPS, whitelisting
- Central Device Control
- CPU/PID Protection
- Patch Management



Detect

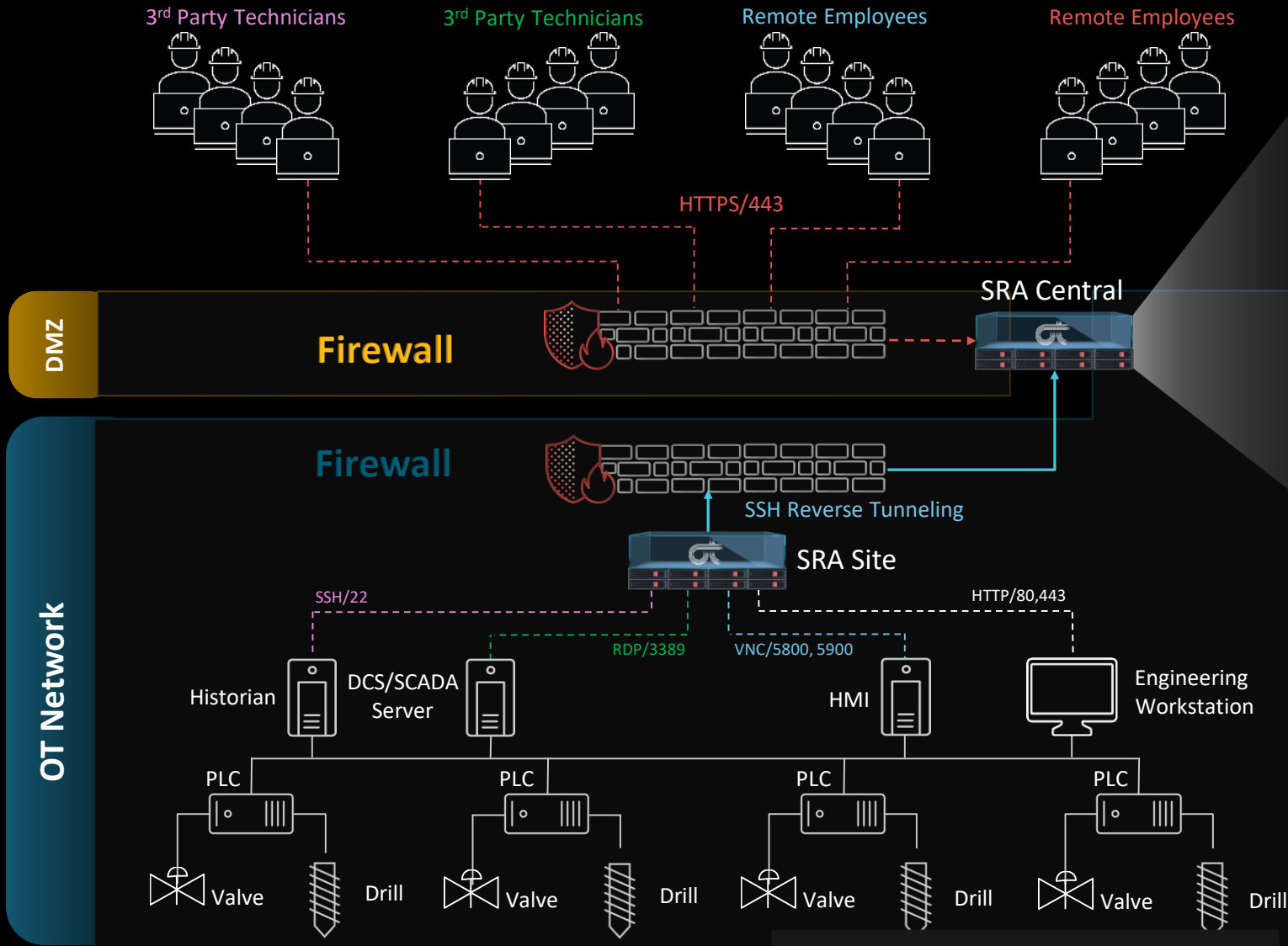
- Security Information & Event Management (SIEM)
- Network performance monitoring
- Anomaly Detection
- Intrusion Detection (NIPS)
- SOC / NOC



Respond

- Backup / Disaster Recovery

Secure Remote Access



SRA Admin



Control

- Granular user/asset access policy
- Enforce Auth. Policies (MFA) and Vault Passwords
- Manually approve remote connections



Monitor

- Real-time "over the shoulder" video viewing of session
- "Red Button" for immediate session termination



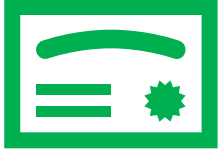
Audit

- Audit video session recordings
- Session integrity validation using CTD activity timeline

FW Open Ports

HTTP/S – 80 / 443

Certification



Use Certified Products

- Any embedded product with an interface and IP Stack now undergo Embedded Device Security Assurance (EDSA) certification.
- For long development cycles devices will undergo Achilles certification in the interim. Workstations will also be Achilles certified



Developed in certified development centres

- Follow the Secure Development Lifecycle
- All Policies, Practices & Procedures reviewed / updated every quarter.



By certified authorities

- For Process Automation we use exida and TÜV for Safety

Certification underpins cybersecurity technology



Mantenere
I più alti livelli di
protezione informatica

MANUTENZIONE: su misura

Gold



Silver



Bronze



Le normative sulla Cybersecurity in Italia

Classificazione delle Aziende



La Cybersecurity è un obiettivo Nazionale di sicurezza

Direttiva UE 2016/1148 del 6/7/2016 per la creazione di un alto livello di sicurezza nelle reti e nei sistemi informatici (NIS) in EU

In Italia

Decreto legge n. 65, del 16 maggio 2018

Il 9 giugno è andato in Gazzetta Ufficiale ed è in vigore dal 26 giugno 2018.

Operatori Servizi Essenziali (OSE)

Energia



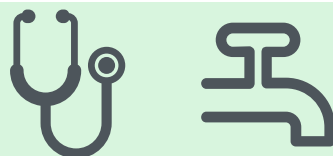
Elettricità – Petrolifere – Gas
Produzione, fornitura e distribuzione

Trasporti



Aeroporti – Ferrovie – Trasporto Acque
Strade (Utilities /Authorities)

Sanità e Acque



Ospedali – Cliniche
Fornitori - Distributori

Banche e finanza



Società di credito - Traders

Multe da 12.000 fino a 1.500.000 euro (riviste col DL 105/2019)

Obblighi

Gestione del rischio:

«Gli operatori di servizi essenziali devono adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi.»

Minimizzazione dell'impatto:

«Gli operatori di servizi essenziali devono adottare misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi..., al fine di assicurare la continuità dei servizi»

Notifica:

«Gli operatori di servizi essenziali devono notificare all' autorità competente o al CSIRT gli incidenti»

LEGGE 18 novembre 2019, n. 133

Perimetro di sicurezza nazionale cibernetica.

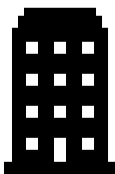
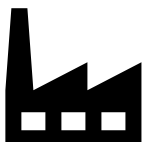
Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle:



**Amministrazioni pubbliche
Enti**



**Operatori nazionali pubblici e privati,
dal cui esercizio dipendono funzioni
essenziali e critiche per lo Stato**

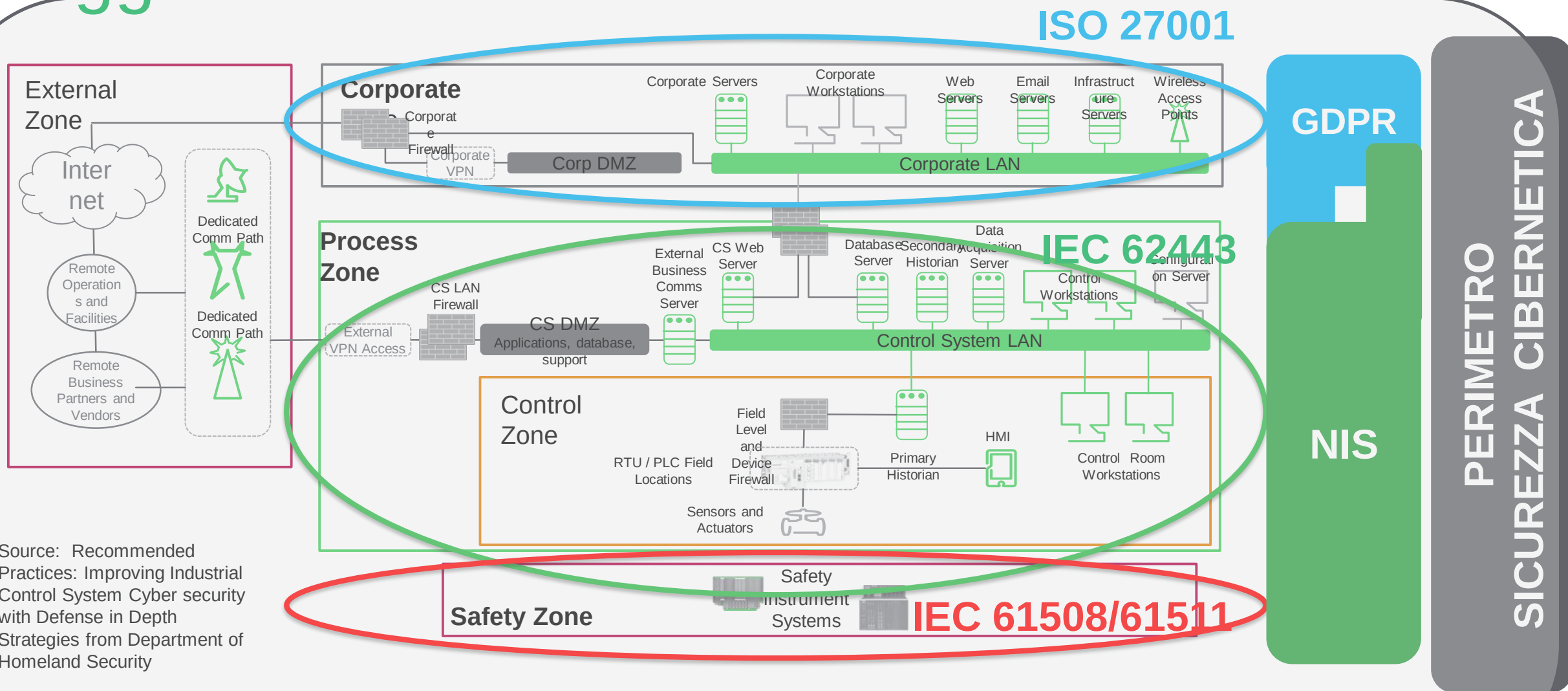


e' inoltre istituito il:

Centro di valutazione e certificazione nazionale (CVCN)

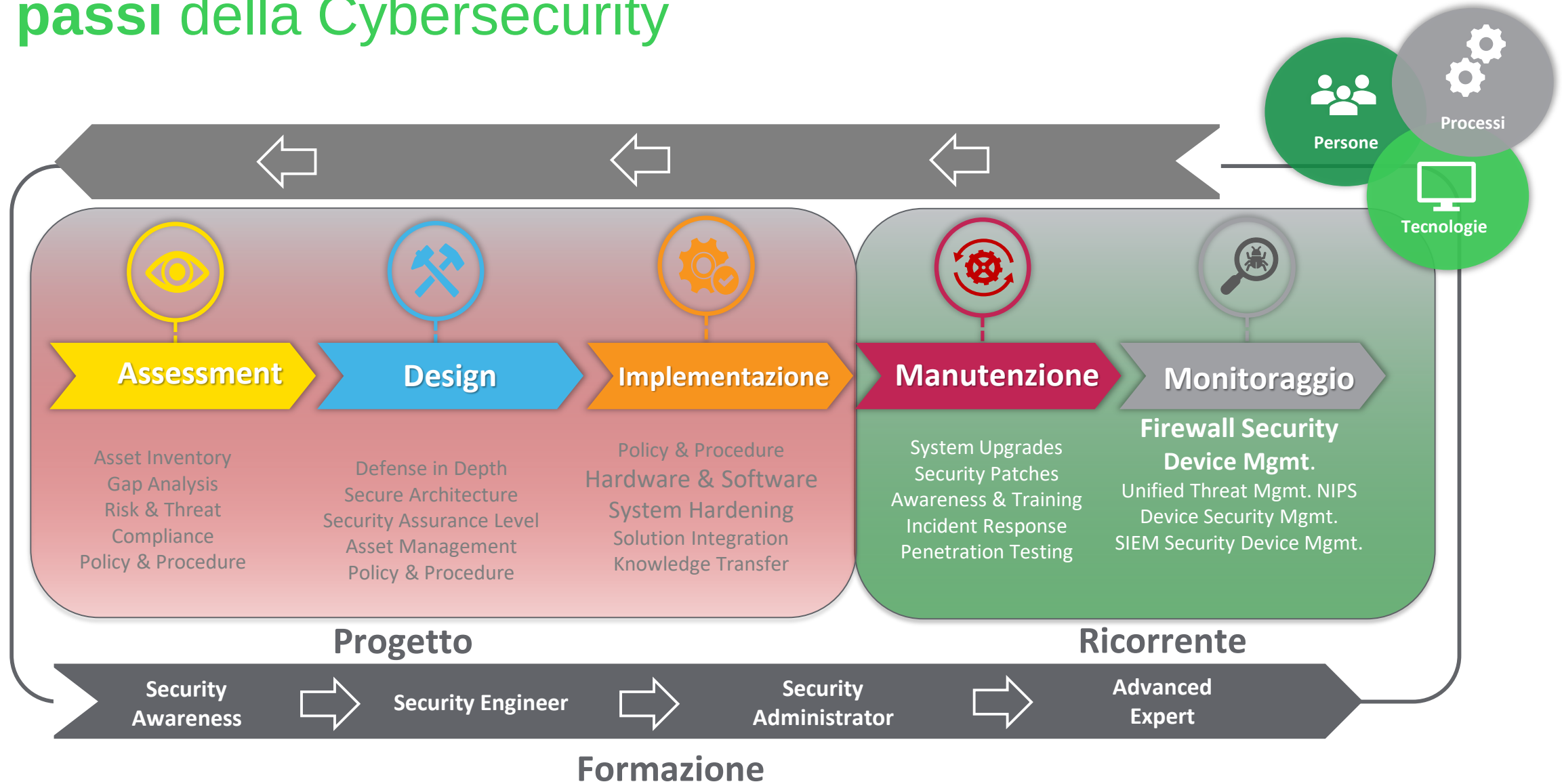


Leggi nel modello IACS



Source: Recommended Practices: Improving Industrial Control System Cyber security with Defense in Depth Strategies from Department of Homeland Security

I 5 passi della Cybersecurity





Cybersecurity nei sistemi industriali

- Differenze tra IT e OT
- Come proteggere un Sistema di Controllo Industriale
- Lo standard ISA99/IEC62443
- Leggi in Italia: DL NIS e succ.
- 10 Suggerimenti
- I 5 passi della Cybersecurity
- Case study
- Q&A

GRAZIE PER L'ATTENZIONE

umberto.cattaneo@se.com