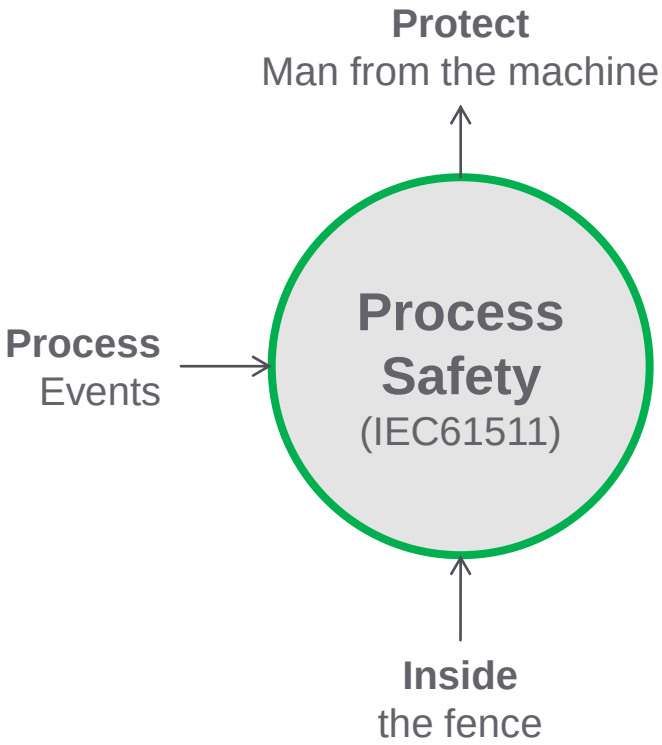
Cybersecurity: l’approccio nei sistemi di controllo industriali

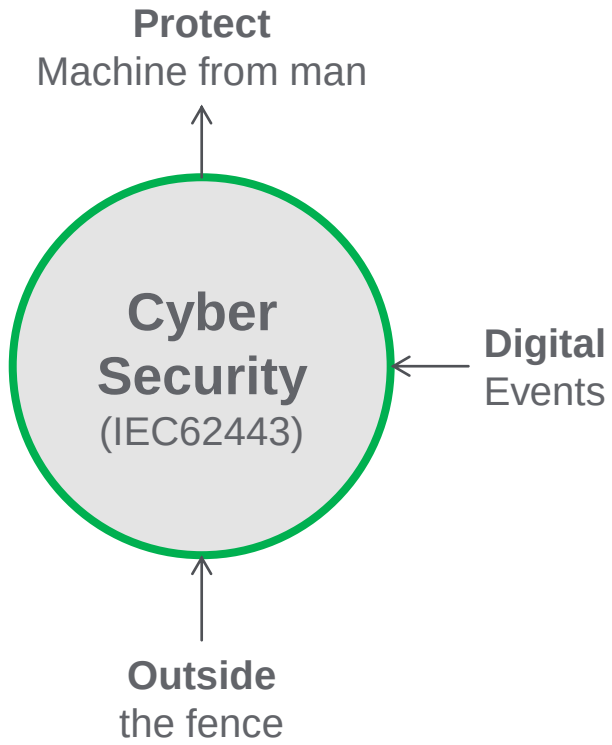
Elsa Carparelli

ISA/IEC 62443

E’ un insieme di 12 norme che coprono e definiscono diversi requisiti di sicurezza di un sistema ICS e si riferiscono a (partendo dal basso): COMPONENTI, SISTEMI, NORME E GESTIONE DEL SISTEMA, MISURE GENERALI di prevenzione e protezione.
Queste norme sono orientate alla necessità di progettare i sistemi di controllo industriali con buone pratiche di cybersecurity, in modo da rendere questi sistemi robusti e resilienti.

Security vs Safety



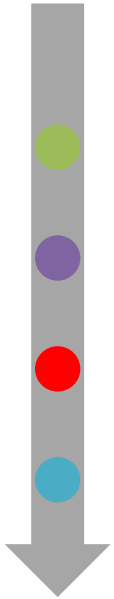


Security vs Safety

Security Profiles

Cyber Security

Security Level	Definition (IEC62443)
SL 1	Casual or coincidental violation
SL 2	**Intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	**Intentional violation** using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation



Most stringent

Safety

Safety Integrity Level	Safety	Probability of failure on demand
SIL 1	90% to 99%	1% to 10%
SIL 2	99 to 99.9%	0.1% to 1%
SIL 3	99.9% to 99.99%	0.01% to 0.1%
SIL 4	>99.99%	0.001% to 0.01%

IEC 62443.3.3 Security Level (SL)

SL/Protezione	Target	Abilità	Motivazione	Mezzi	Risorse
SL1	Casuale o violazione per coincidenza	Nessuna o bassa	Errore	Non intenzionale	Individuali
SL2	Cybercrimine/ hacker	Generica	Scarsa	Pochi e semplici	Scarse (individui isolati)
SL3	Attivisti/ Terroristi	Specifiche del sistema	Moderata	Sofisticati (attacco)	Moderate (gruppi di hacker)
SL4	Nazioni e Stati	Specifiche del sistema	Alta	Sofisticati (campagne)	Estese/condivise (gruppi multidisciplinari)

Industrial Cybersecurity vs IT Cybersecurity

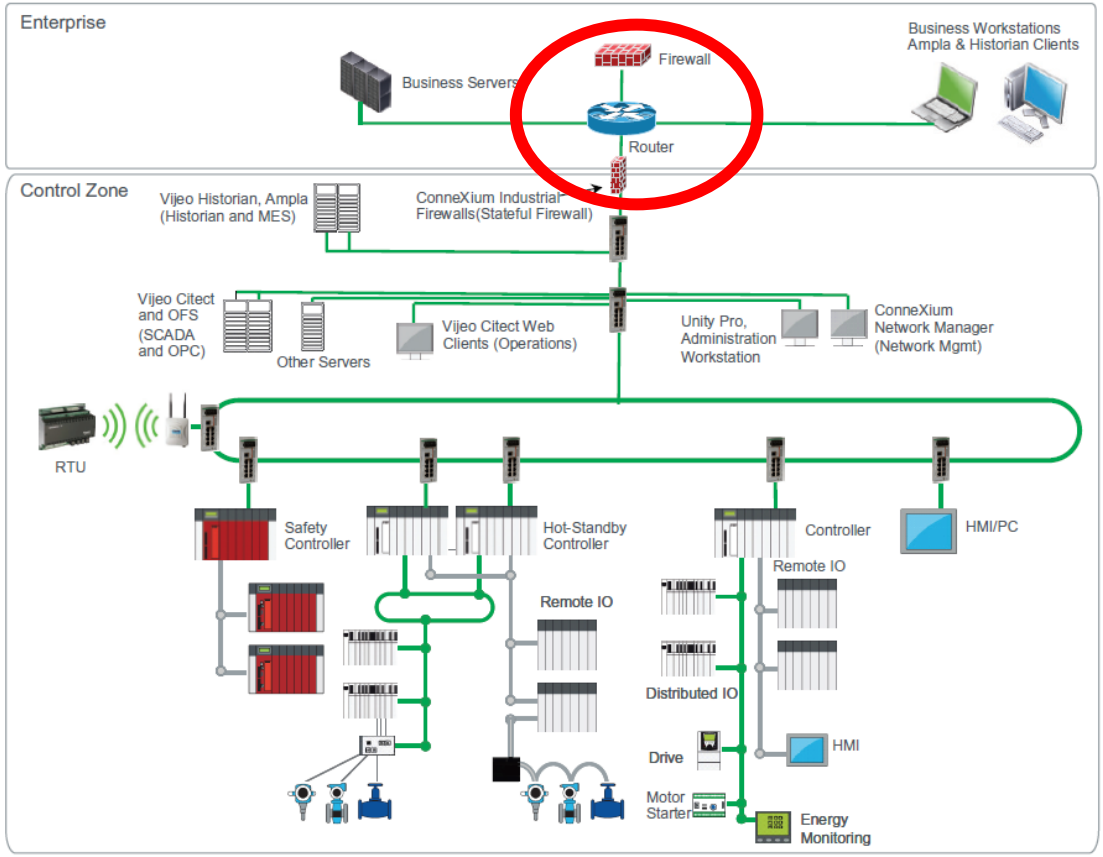
Quali sono le priorità?

OT Security	IT Security
Disponibilità	Riservatezza
Integrità	Integrità
Riservatezza	Disponibilità

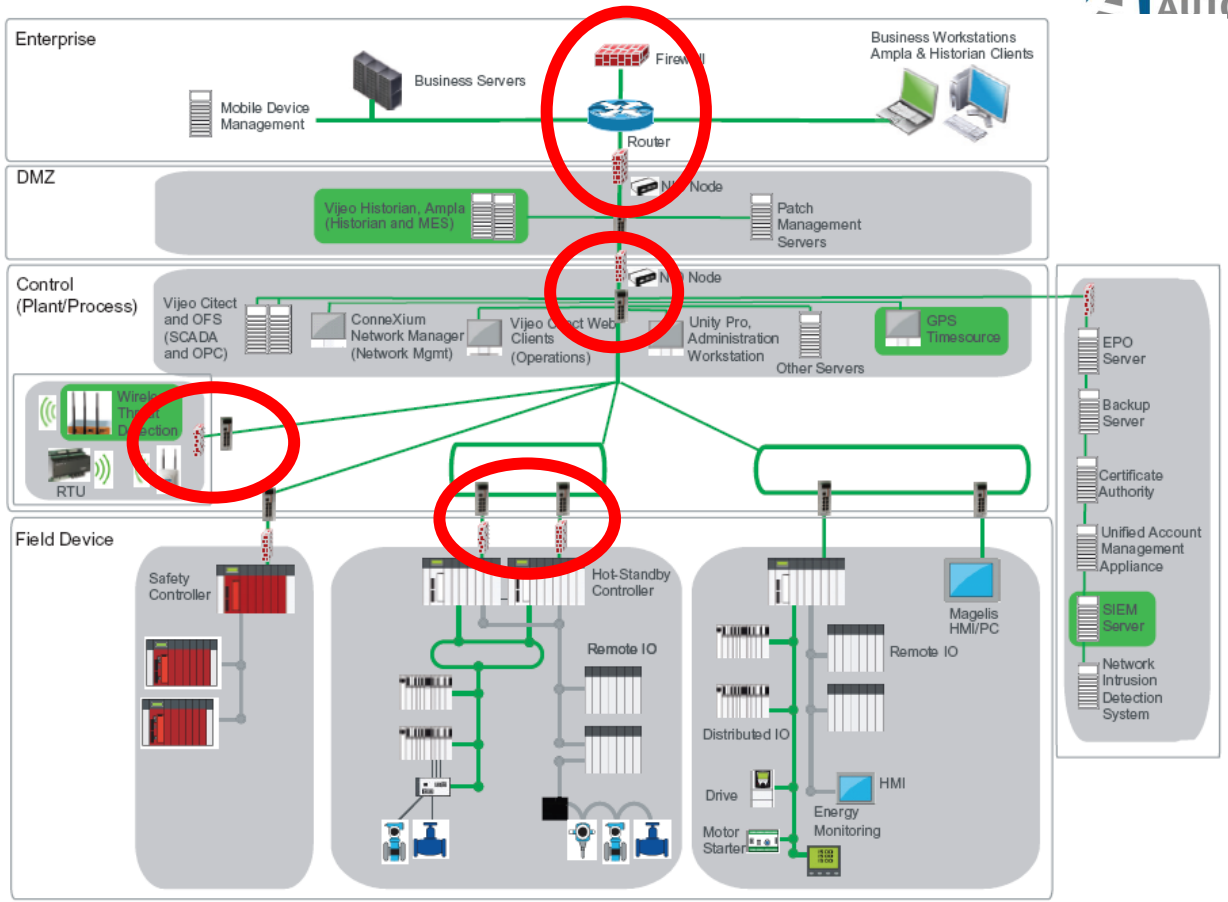
Alta affidabilità e disponibilità
Criticità di performance
Tempi di risposta veloci
Tipicamente sistema critico di sicurezza

Single Layer VS Defense in Depth

SL 0


Enterprise
Business Servers
Firewall
Router
Business Workstations
Ampla & Historian Clients
Control Zone
Vijeo Historian, Ampla
(Historian and MES)
ConneXium Industrial
Firewalls(Stateful Firewall)
Vijeo Citect
and OFS
(SCADA
and OPC)
Other Servers
Vijeo Citect Web
Clients (Operations)
Unity Pro,
Administration
Workstation
ConneXium
Network Manager
(Network Mgmt)
RTU
Safety
Controller
Hot-Standby
Controller
Remote IO
Controller
HMI/PC
Remote IO
Distributed IO
Drive
HMI
Motor
Starter
Energy
Monitoring

SL 3


Enterprise
Business Servers
Mobile Device Management
Firewall
Router
Business Workstations Ampla & Historian Clients
DMZ
Node
Vijeo Historian, Ampla (Historian and MES)
Patch Management Servers
Control (Plant/Process)
Node
Vijeo Citect and OFS (SCADA and OPC)
ConneXium Network Manager (Network Mgmt)
Vijeo Citect Web Clients (Operations)
Unity Pro, Administration Workstation
Other Servers
GPS Timesource
RTU
EPO Server
Backup Server
Certificate Authority
Unified Account Management Appliance
SIEM Server
Network Intrusion Detection System
Field Device
Safety Controller
Hot-Standby Controller
Remote IO
Magelis HMI/PC
Remote IO
Distributed IO
Drive
HMI
Energy Monitoring
Motor Starter

Cybersecurity Lifecycle

La risposta di Schneider-electric

M580 come strumento HW di sicurezza

ePAC certificato per essere CyberSicuro

RIO DIO Communicator Head

CommHeadRIODIO16L2
Channel 0

Security | IPConfig | RSTP | SNMP | NTP | ServicePort

Global policy

Enforce Security | Unlock Security

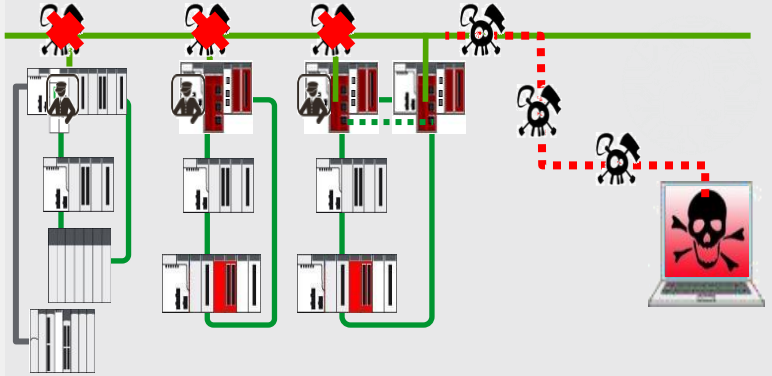
Services

FTP :	Disabled	DHCP / BOOTP :	Disabled
TFTP :	Disabled	SNMP :	Disabled
HTTP :	Disabled	EIP :	Disabled

Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
Yes	192.168.10.1	255.255.0.0	☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐

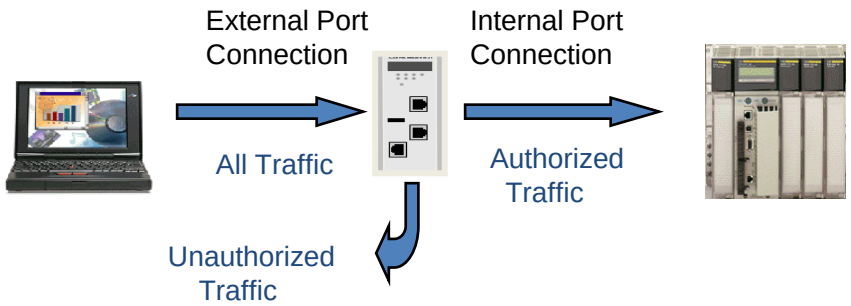


Certificazione di robustezza delle comunicazioni ed integrità di sistema

SE ConneXium Tofino – Advanced Firewall

Tofino è un firewall industriale che ha le seguenti principali caratteristiche:

- Lo strumento per controllare e monitorare il traffic tra due reti separate o tra due porzioni della stessa rete garantendo la protezione delle apparecchiature che si trovano al di là del firewall stesso
- La capacità di confrontare il flusso di traffico che passa attraverso il firewall confrontandolo con un set di regole impostate e bloccare gli scambi non omologati.
- Impostare un limite nel numero e nel tipo di traffico scambiato dai dispositivi.
- Log del traffico non conforme alle regole impostate.




Life Is On
Life Is On
Schneider Electric