

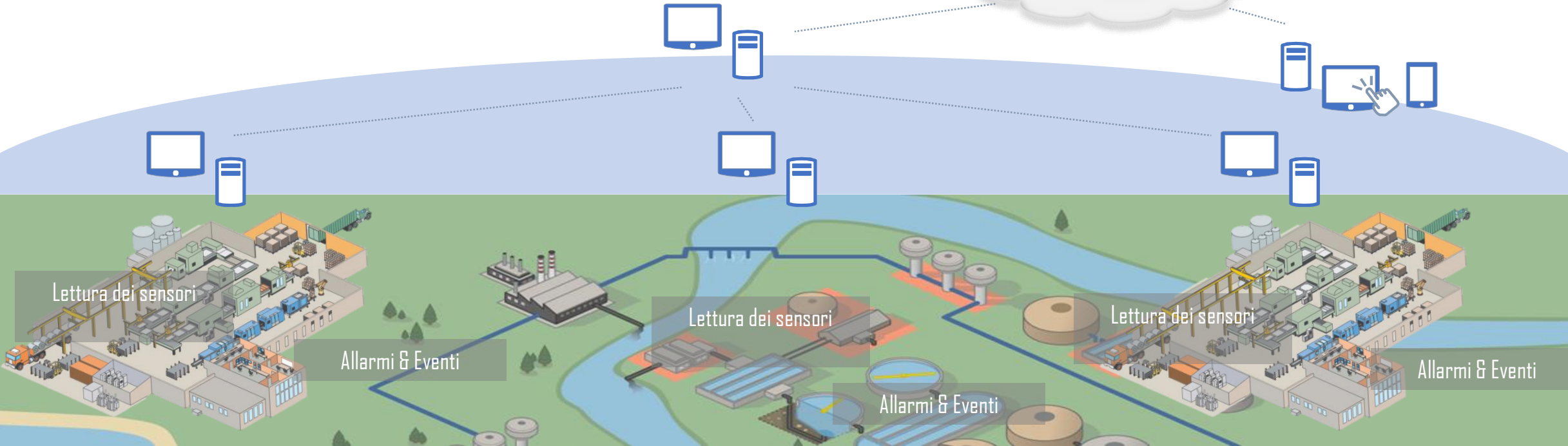
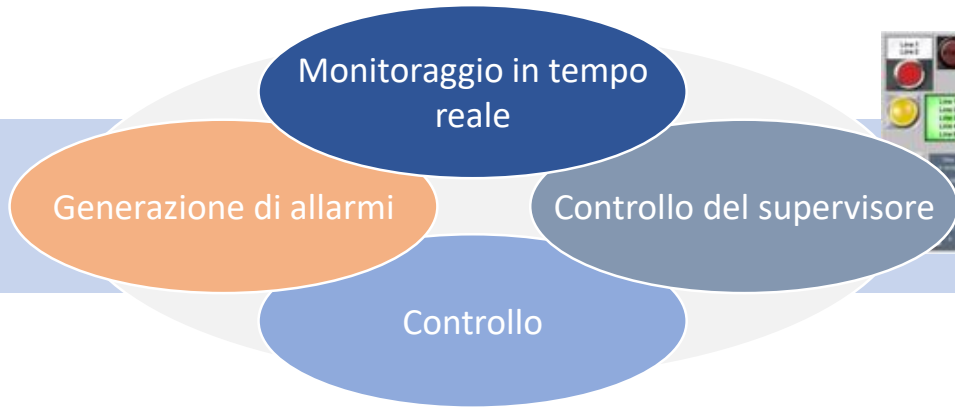
Strategie per uno SCADA SICURO

Luglio 2020

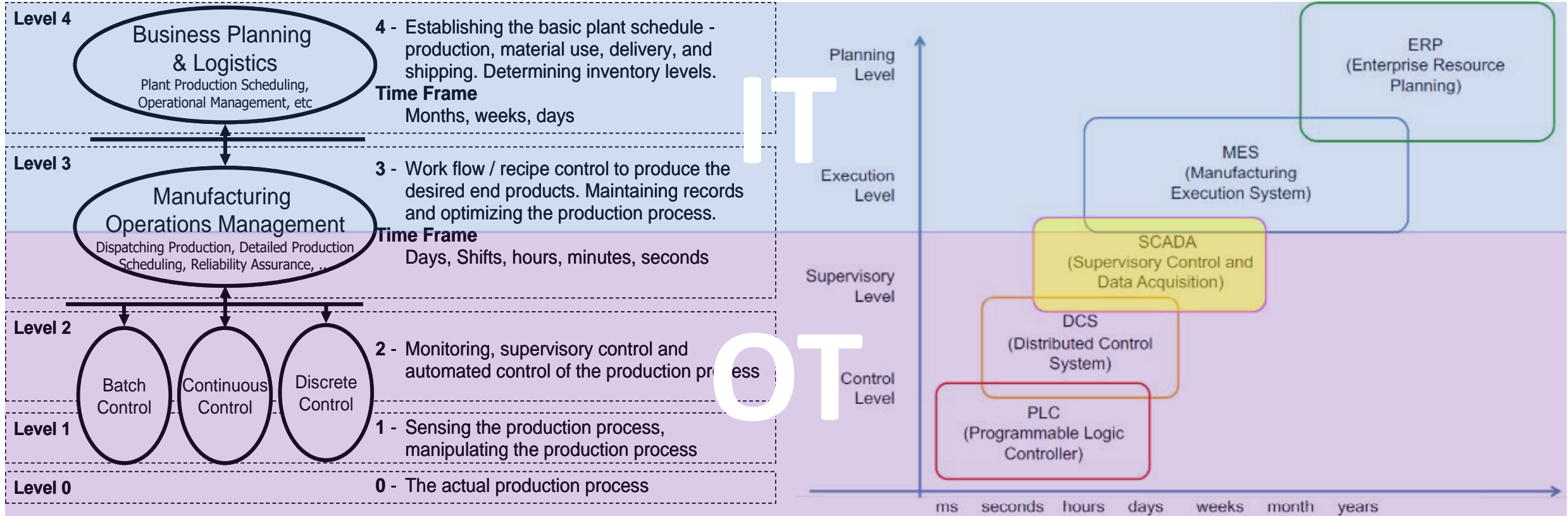


Mario Testino EMBA, MEng
C.O.O.
ServiTecno

SCADA: il perno dell'Internet Industriale



Cos'è IT e cos'è OT



IT vs OT paradigmi differenti

Obiettivi organizzativi

Standardizzazione prevalente

Skills del personale

Informatici, networking, amministrativi e gestionali

Tecnologia

Scenario non-deterministico

Sistemi non-real-time o al massimo near realtime

Propensione verso sistemi cloud-based

Protocolli informatici (livello 7 applicazione)

Sviluppo dei progetti

Progetto coordinato dall'interno, con risorse esterne

Progetto globale «corporate»

Requisiti Cogenti «Hot topics»

Data Integrity

Data Security

Patent Infringement

Business Continuity (management)



Obiettivi organizzativi

Integrazione Multi-brand

Skills del personale

Elettrici, meccanici, conduzione di processo

Tecnologia

Sistemi prevalentemente deterministici

Sistemi strettamente real-time

Propensione verso sistemi «ibridi»

Protocolli «fisici» industriali

Sviluppo dei progetti

Progetto completamente esternalizzato

Progetto locale: Impianto, linea, macchina

Requisiti Cogenti «Hot Topics»

People Safety

Business Continuity (making)

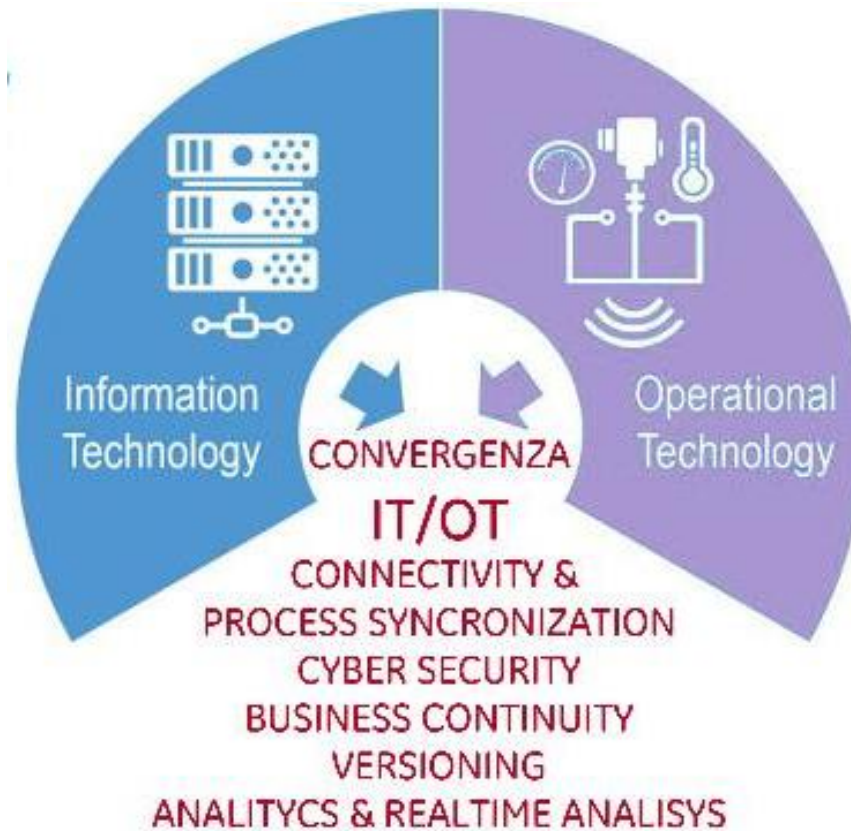
Service Continuity

Digitalizzazione

Convergenza IT - OT

Tutti gli standard informatici aziendali:

- Web,
- Networking,
- Cloud,
- Gestionale (ERP, MRP, MES)
- Cyber Security
- ...

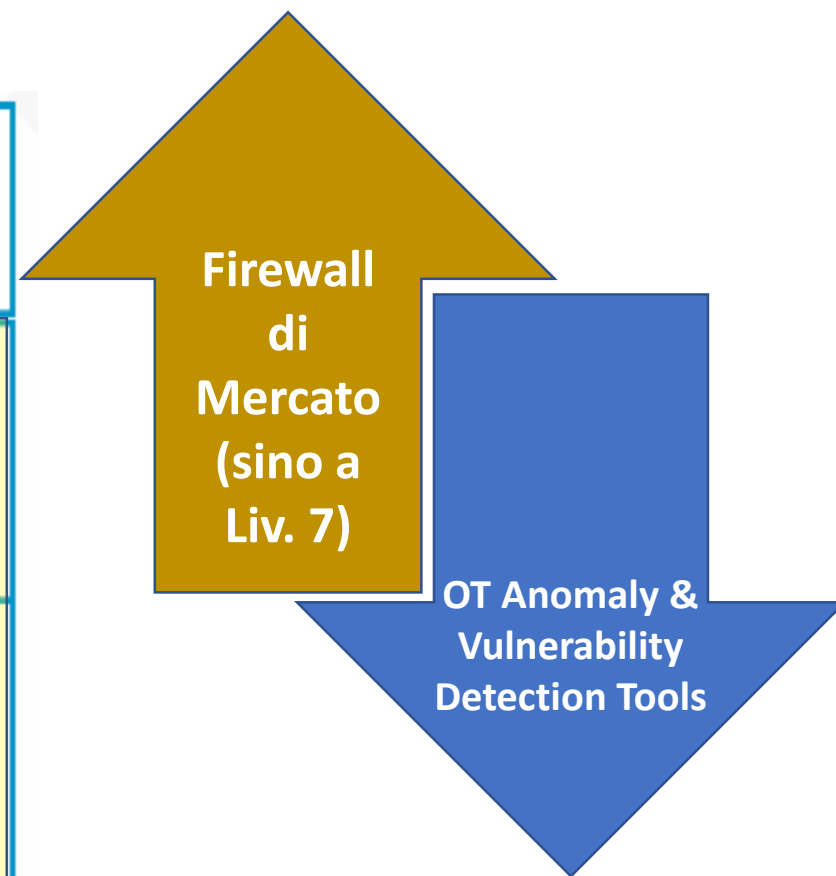
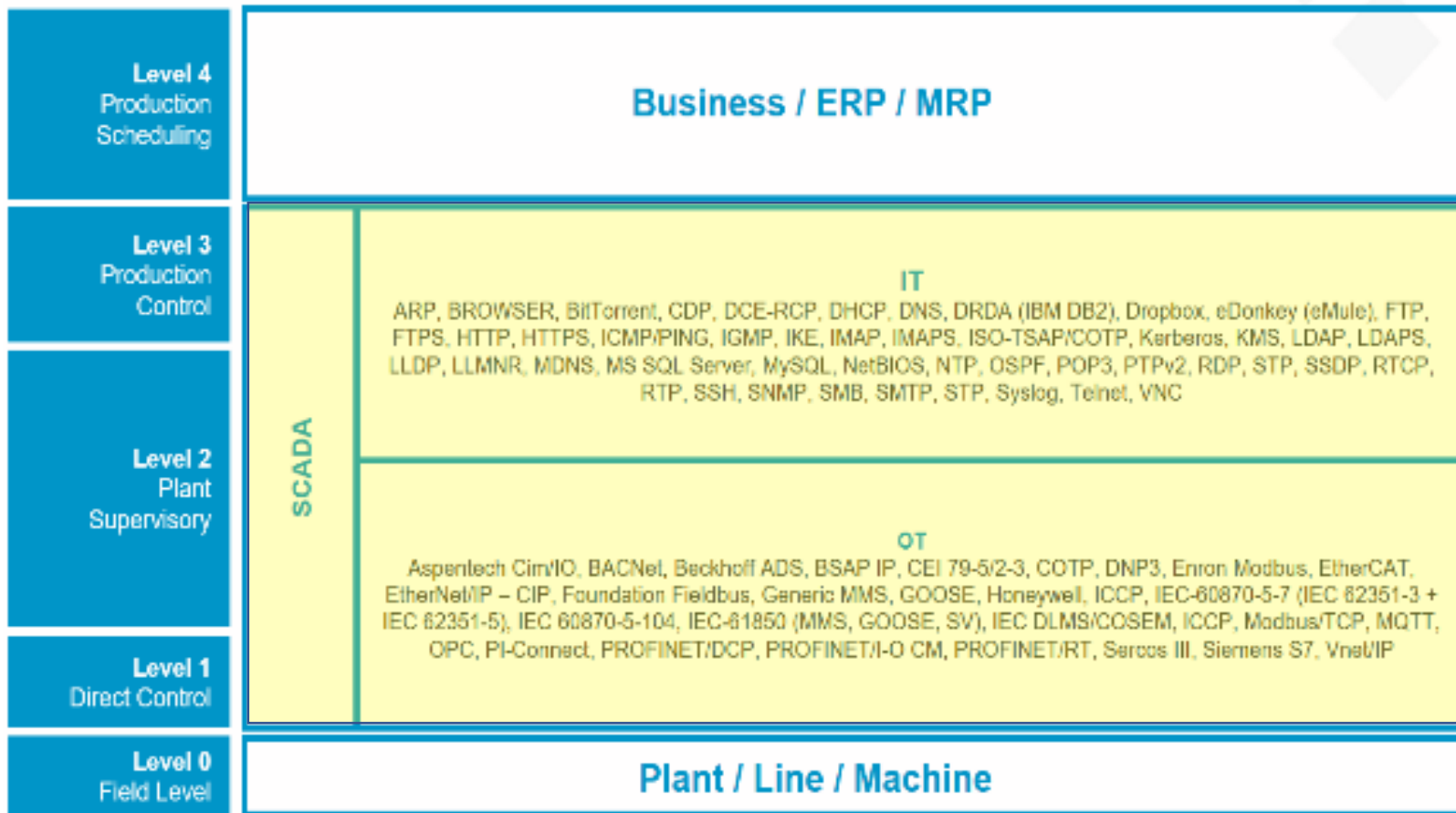


Tutti i sistemi di automazione, controllo, supervisione, storicizzazione, misura, analisi real-time di impianti, linee, macchine e in generale del processo produttivo:

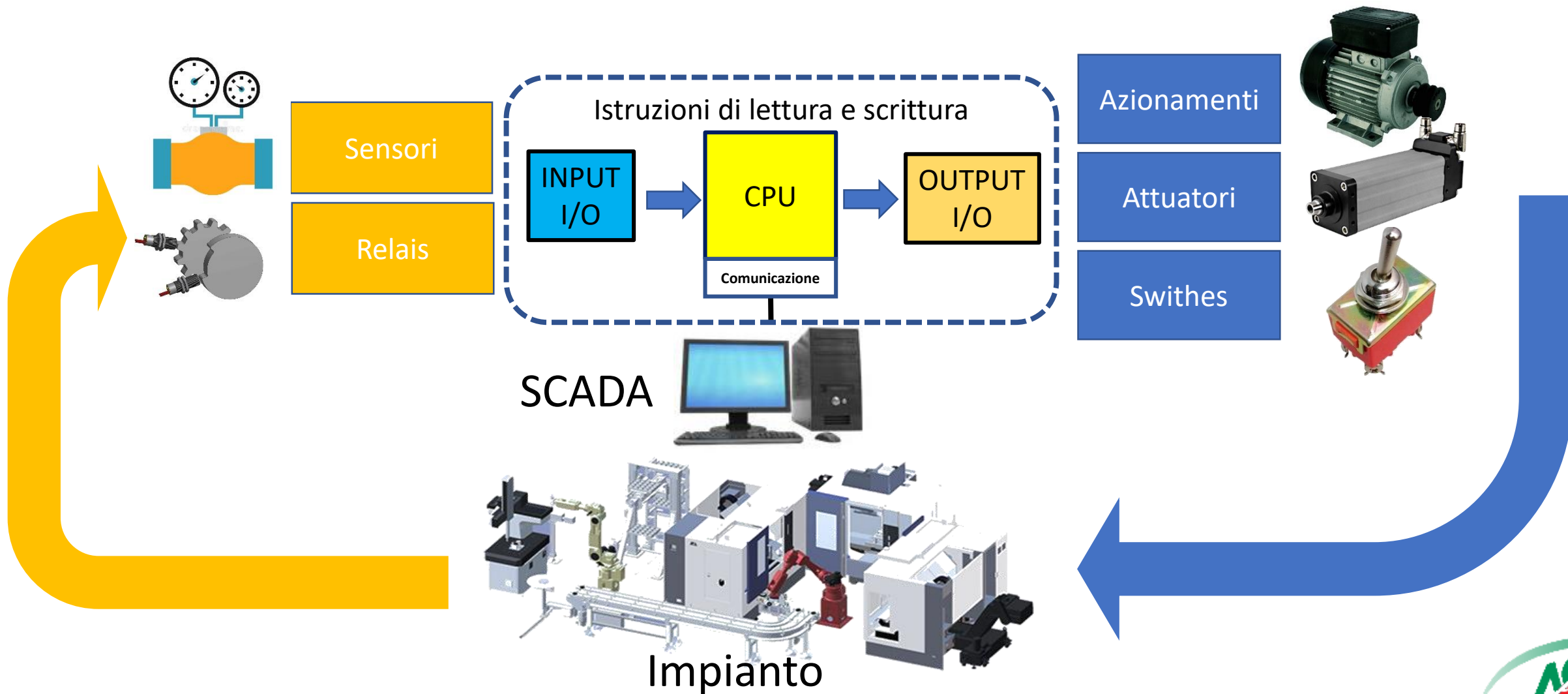
- PLC
- DCS
- CNC
- SCADA
- Robot
- Historian
- Sensori
- Attuatori
- ...



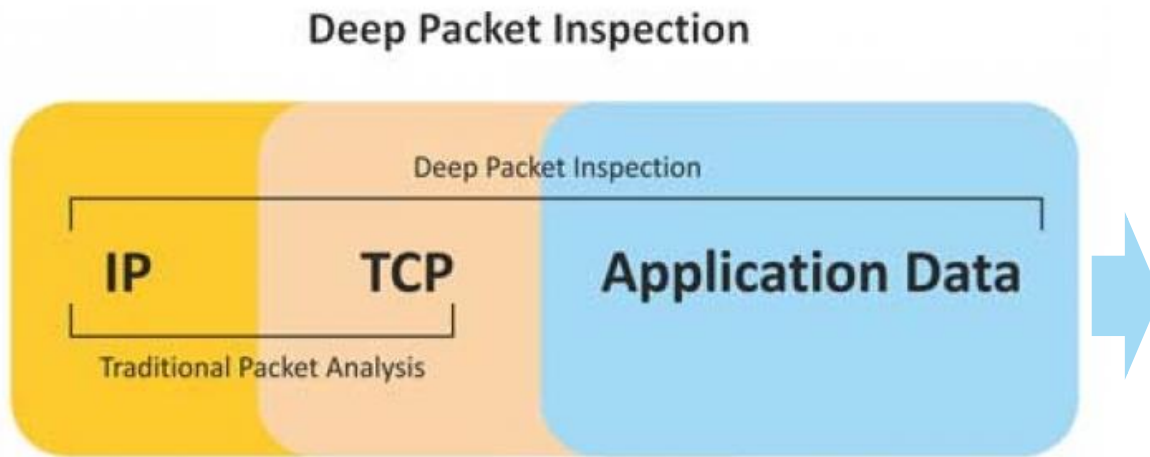
Lo SCADA è Border Line



La «Fisica» di SCADA e PLC



DPI (Deep Packet Inspection): TCP/IP non basta!

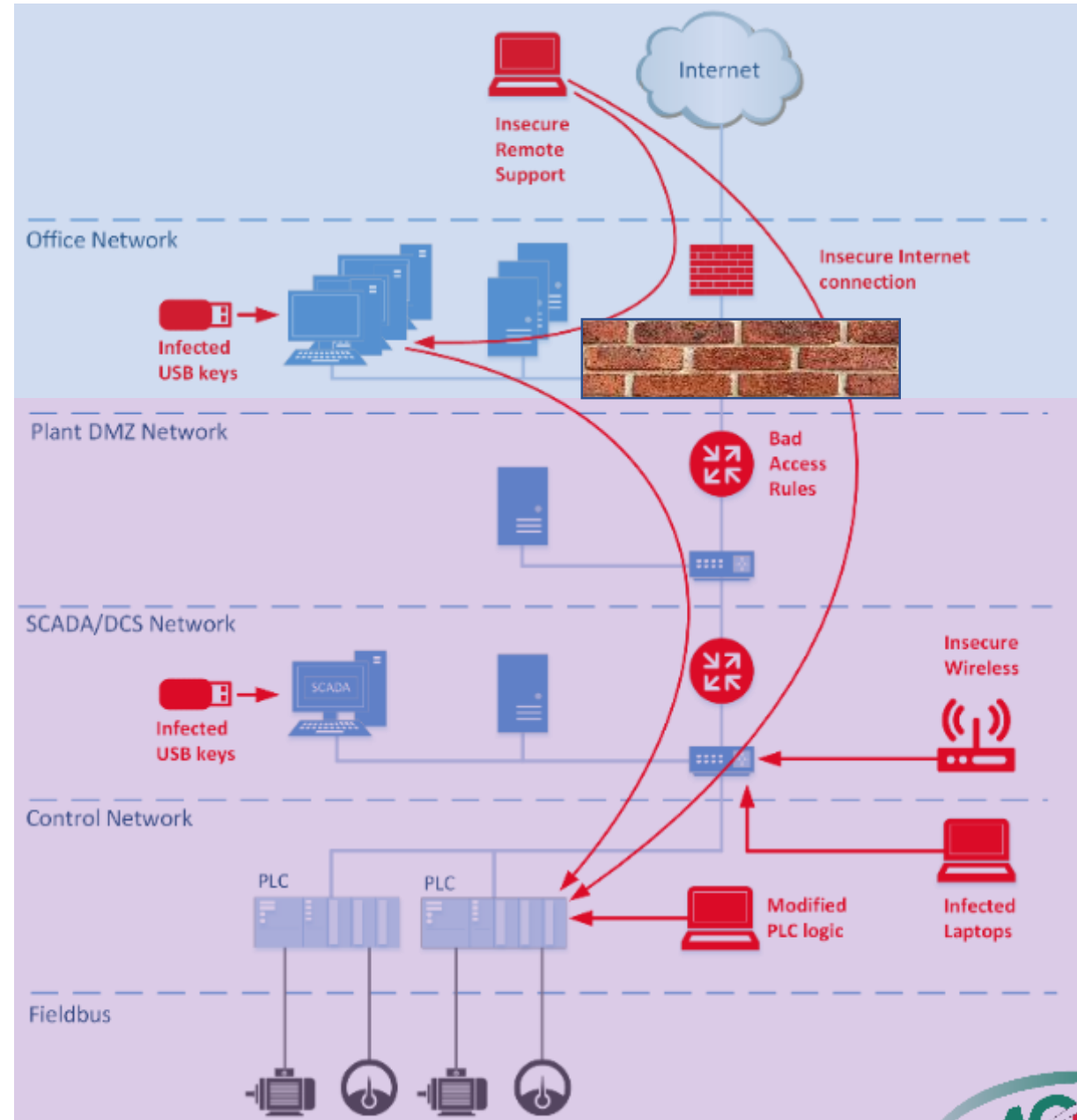


Function type		Function name	
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs
		Internal Bits or Physical Coils	Read Coils
			Write Single Coil Write Multiple Coils
	16-bit access	Physical Input Registers	Read Input Registers
		Internal Registers or Physical Output Registers	Read Multiple Holding Registers
			Write Single Holding Register
			Write Multiple Holding Registers
			Read/Write Multiple Registers
			Mask Write Register
			Read FIFO Queue
File Record Access	Read File Record		
	Write File Record		

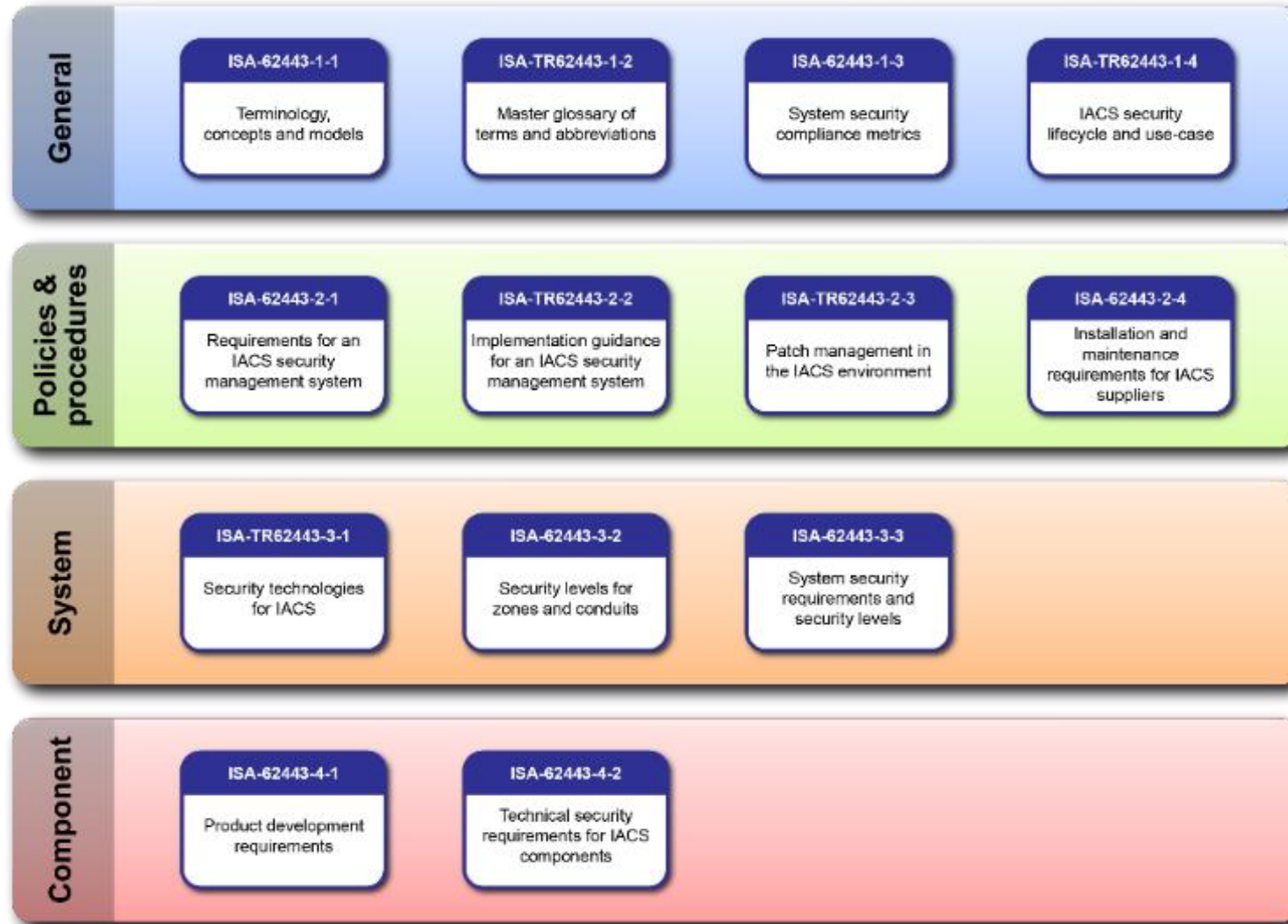


Attacchi e Incidenti informatici

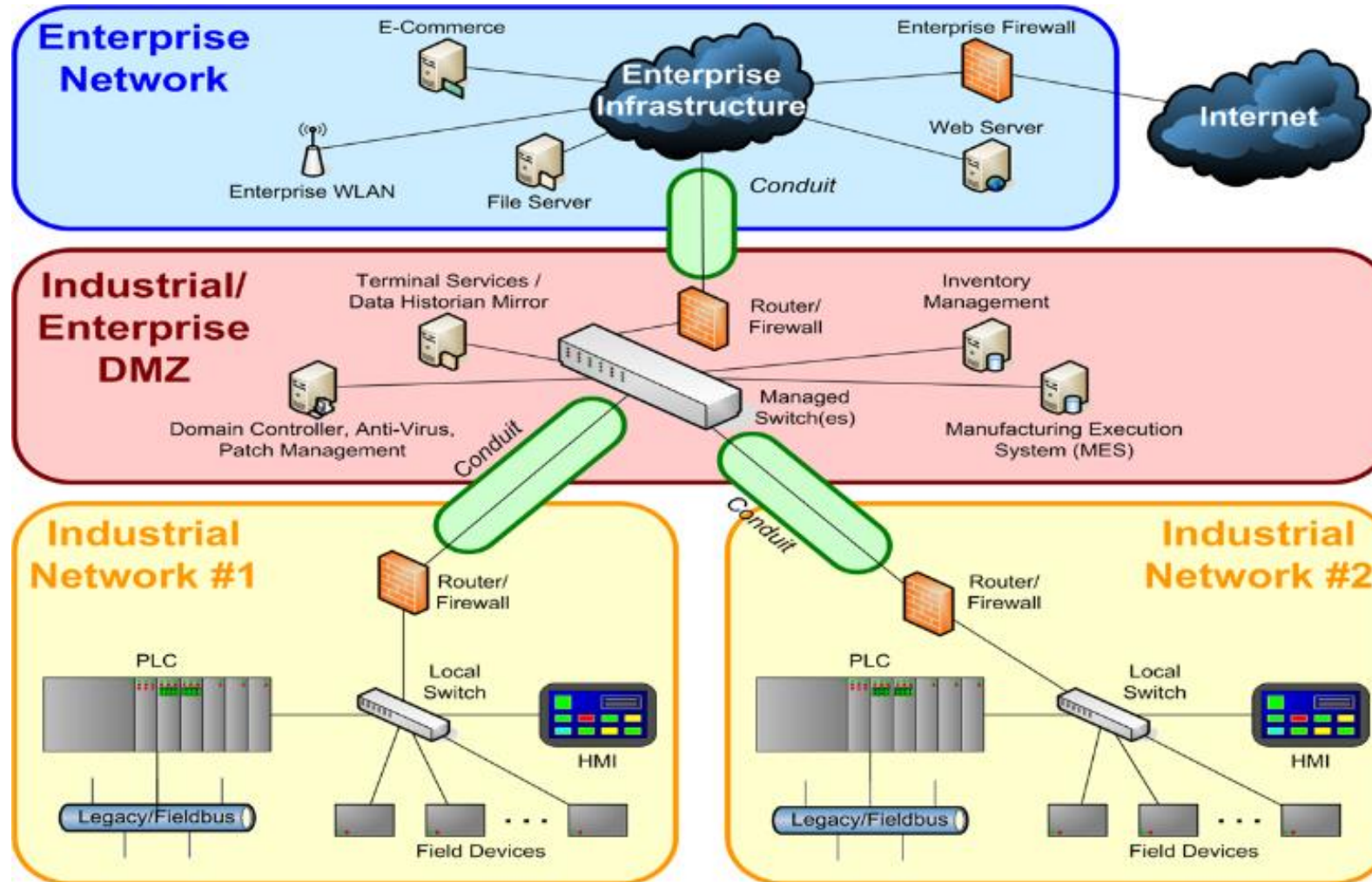
Non ho mai avuto problemi!
Quindi sono a posto...o no?



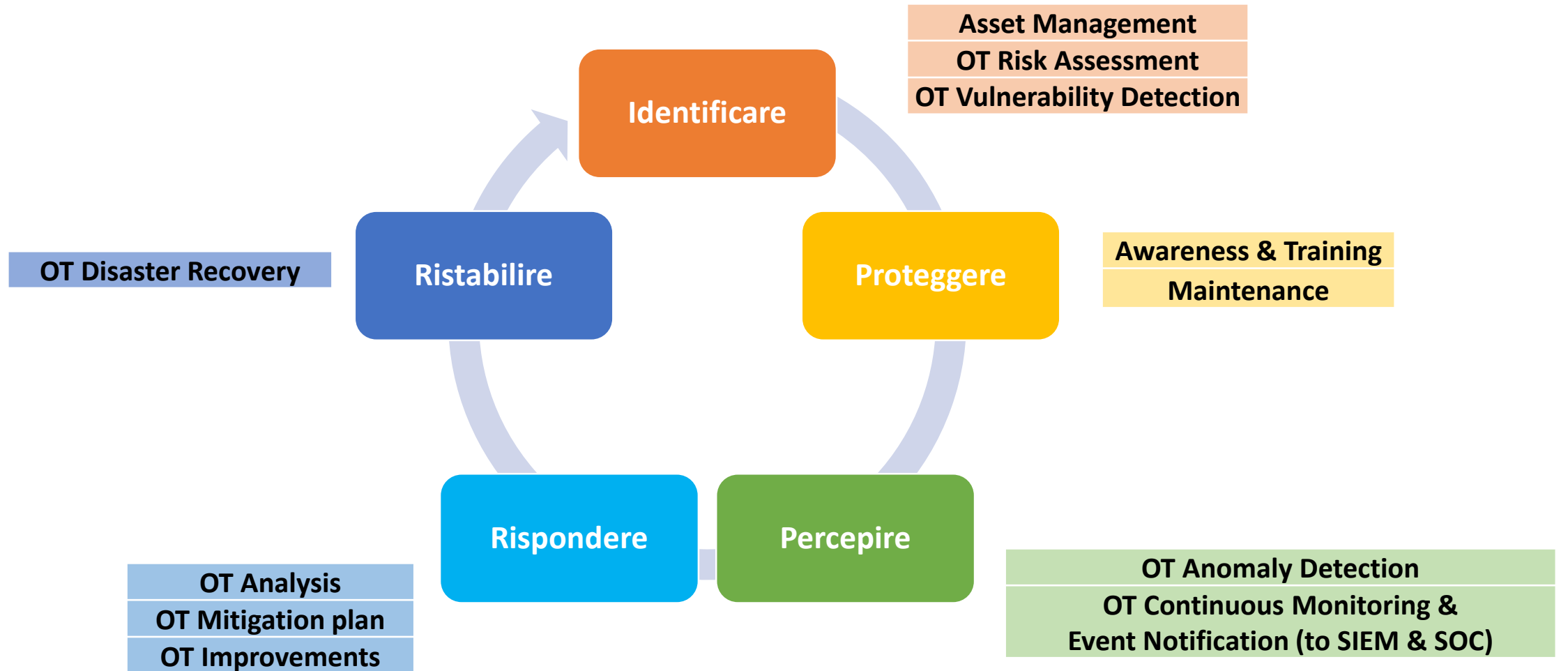
Lo standard di riferimento: IEC 62443 (ISA99)



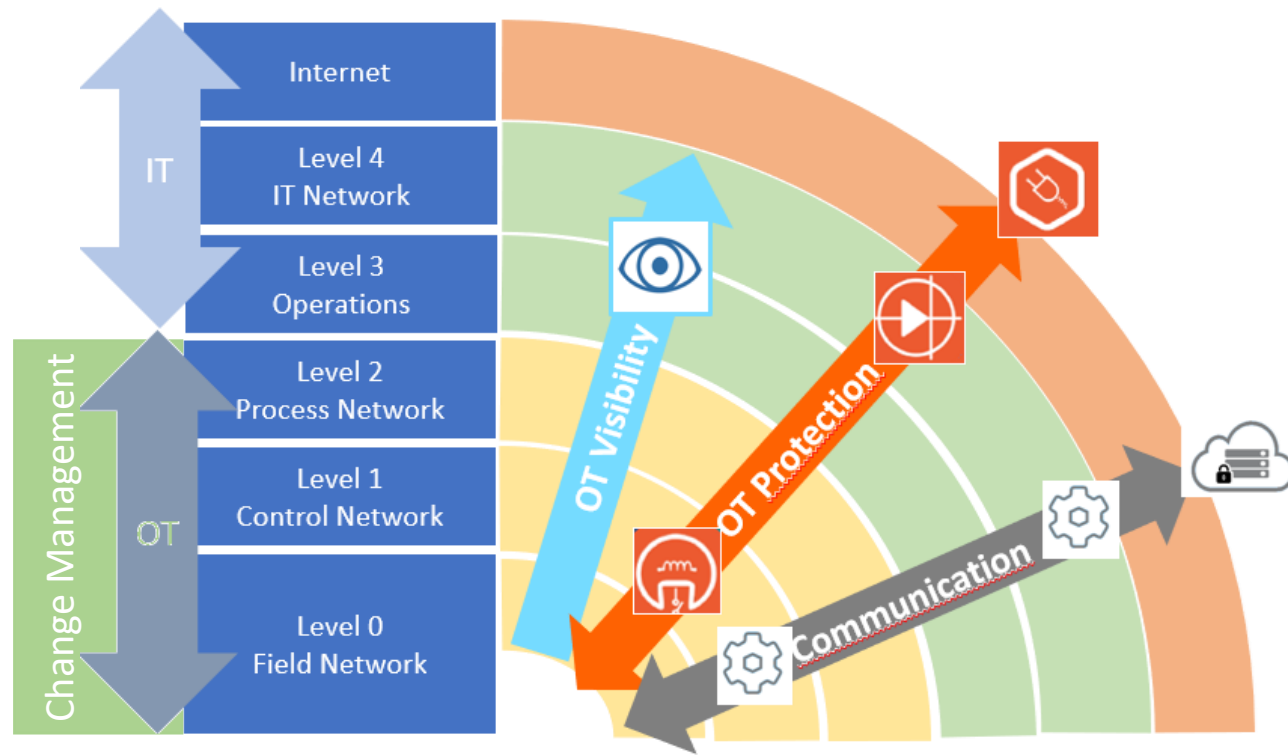
IEC 62443 Architettura di sicurezza logica (Zones & Conduits)



Strategie di Protezione OT: La sicurezza un ciclo virtuoso



Strategie di Protezione OT: Layered Security (NIST)



Assessment & Visibility	Identify (Asset Inventory & Intelligence)
	Assess (Vulnerability & Remediation)
	Detect (Anomaly & Threats)
	Act (Dashboard Alerts, Highlights & Notification)
Protection	Access On Site (VPN, High granular access policies)
	OT Segmentation (self configuration, DPI)
	AirGap bridge
Secure Streaming of Data	Data Tunneling (OPC DA/UA, Modbus)
	Data Bridge (OPC DA<->UA, OPC DA/UA<->Modbus)
	Data Gateway (OPC DA/UA, ModBus, MQTT)
	Data Logging (OPC DA/UA, Modbus to SQL)
	Cloud Secure Streaming (VPN)
Change Management & Control	PLC, ICS, SCADA versioned back-up
	SW & configuration scheduled consistency control
	Disaster Recovery

Strategie di Protezione OT: Layered Security (Esempio)

Last line of defense



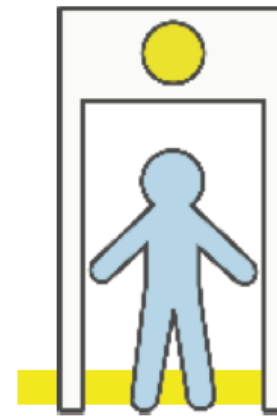
ID check / Physical inspection
Perimeter protection

STEP
01



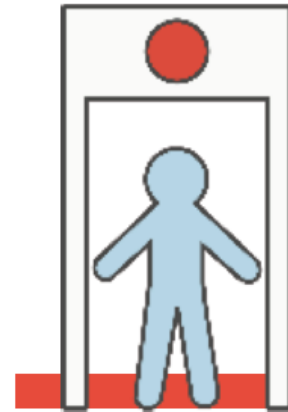
STEP
02

Only ticketed Passengers
allowed on board
Segmentation (Authentication /
Authorization enforcement)



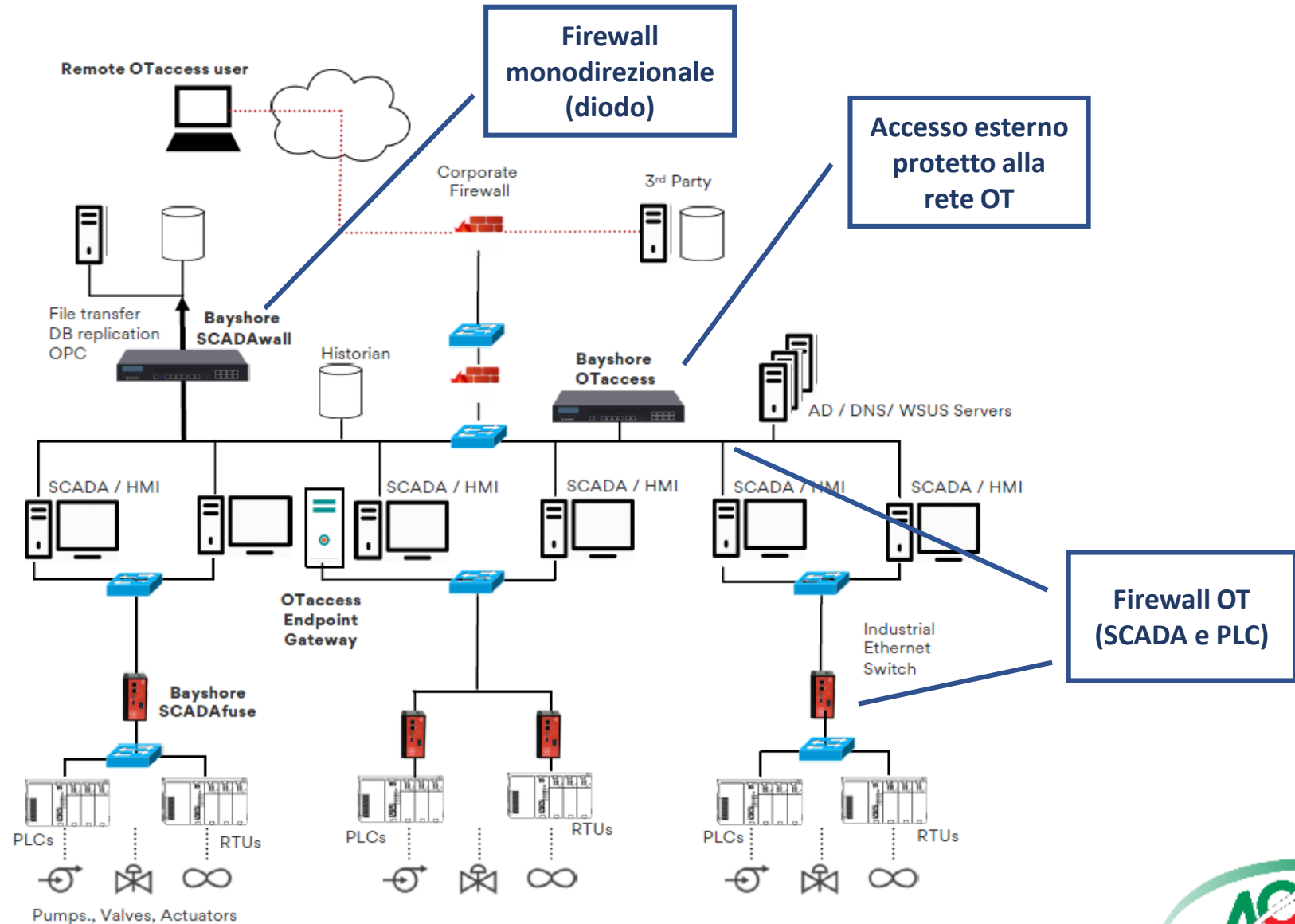
STEP
03

Reinforced, locked cockpit door
Last line of defense / Endpoint protection

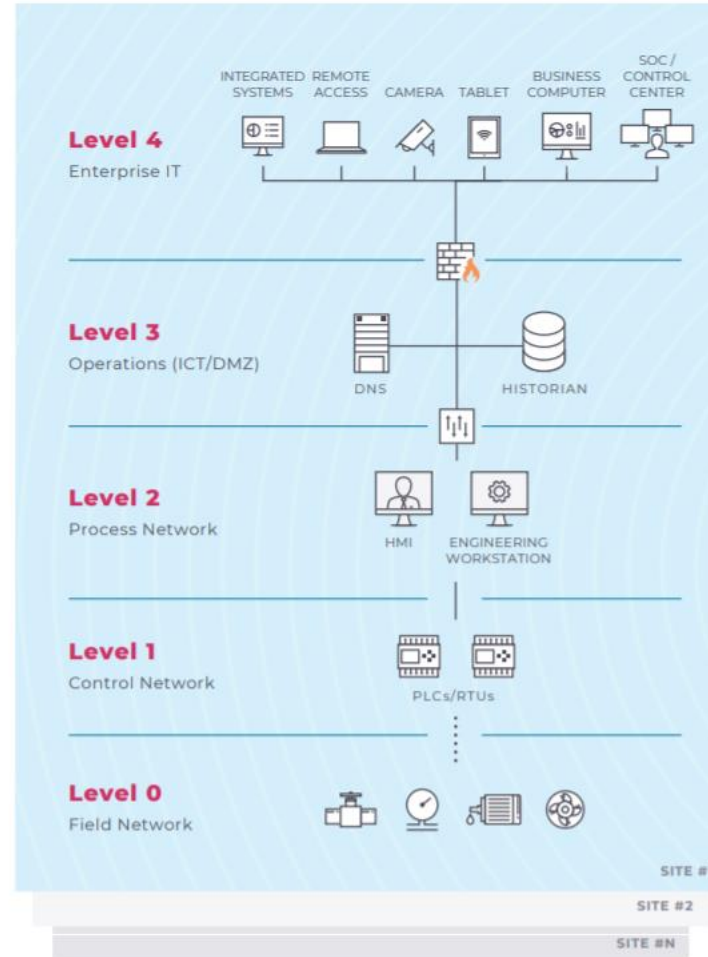
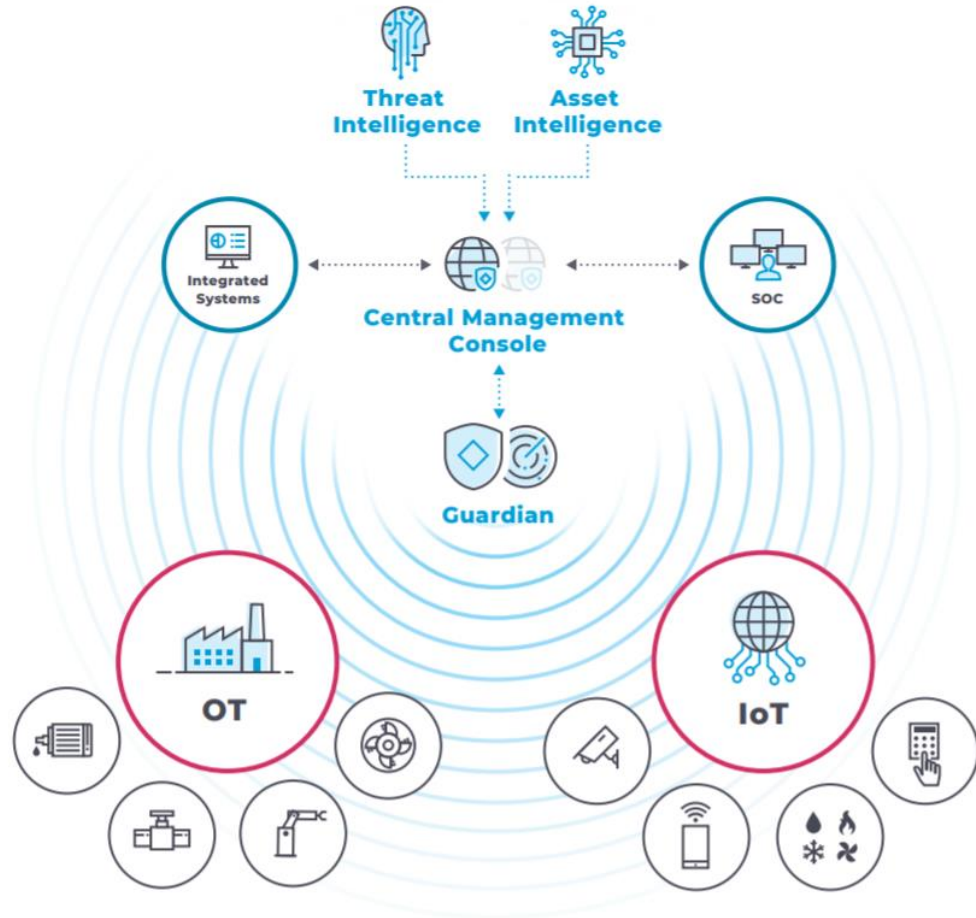


La strategia di Protezione nell'Architettura di Rete

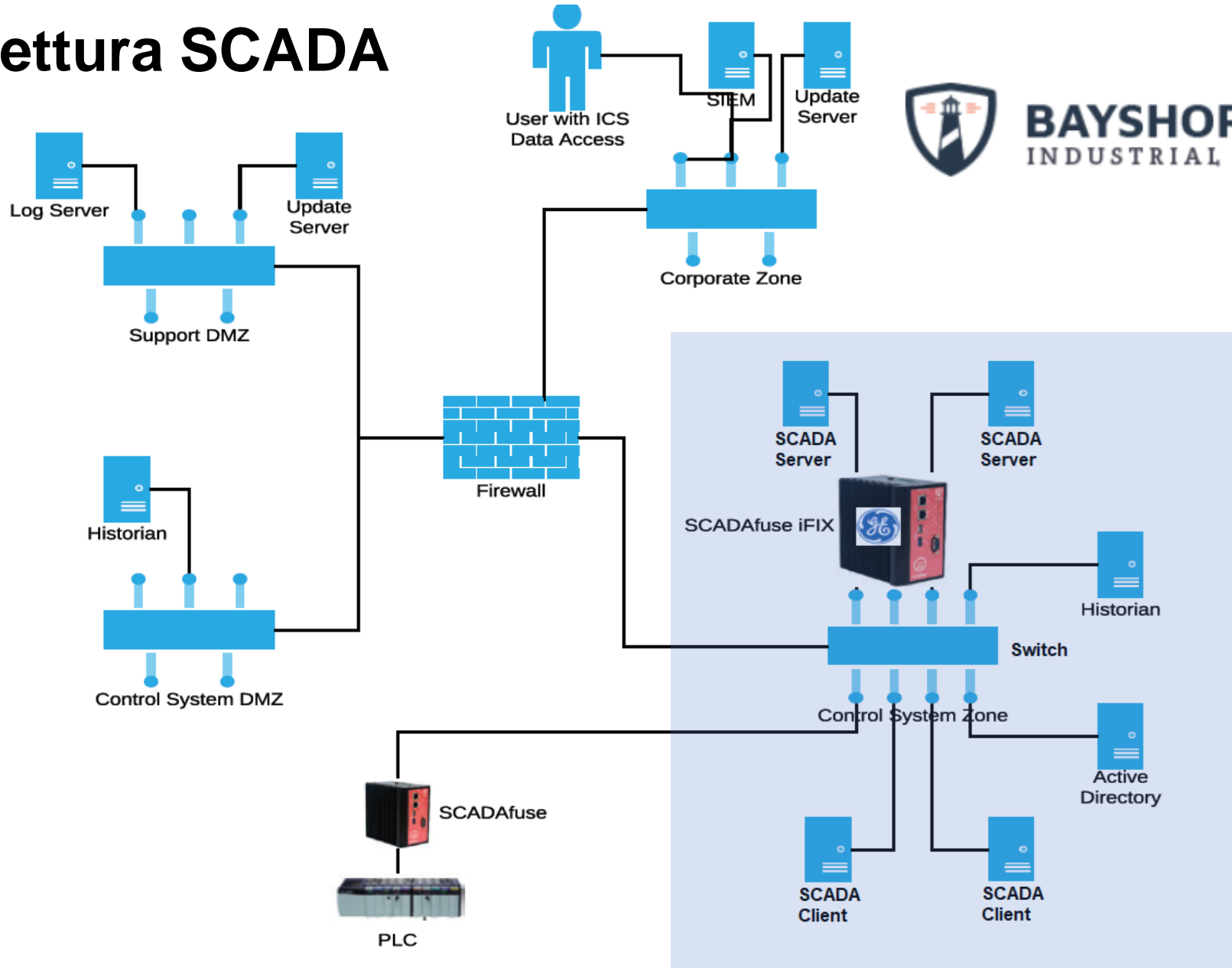
- Internet
- Level 4
IT Network
- Level 3
Operations
- Level 2
Process Network
- Level 1
Control Network
- Level 0
Field Network



OT & IoT Security & Visibility

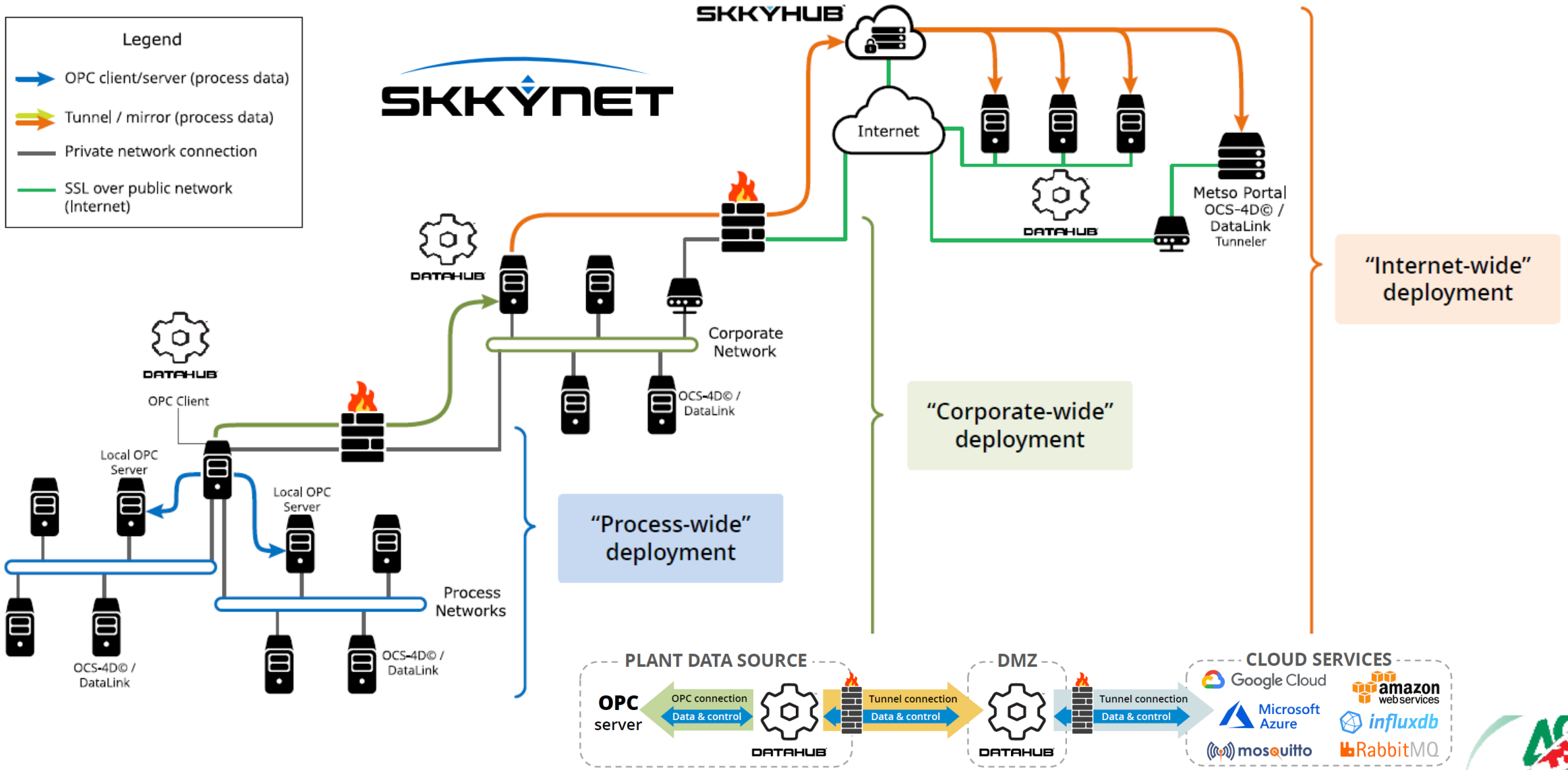


Architettura SCADA



BAYSHORE NETWORKS
INDUSTRIAL NETWORK SECURITY

La strategia di Trasferimento Dati nell'Architettura Corporate



Criteri di Sicurezza nella Configurazione dello SCADA

Connettività Client-Server Criptata

Integrazione user accounts con Windows user accounts

Server Ridondati a Caldo

Server Fault Tolerant

Protocolli con Certificato di Sicurezza (OPC UA)

Historian integrato in Mirroring

Uso tecnologie Edge



GE Digital

GE Digital IFIX
GE Digital Cimplicity



Dispositivi Automaticamente Configurabili

SCADAFuse Monitoring Mode Events 51 IP 192.168.100.13/24 BRANCH SCAD-396

Quick Navigation...

Dashboard
Events
Configuration
System Log
Device Manual
Diagnostics
Advanced

Traffic Dashboard

Graph **Table** Idle/Edit Learn **Monitor** Protect Action

Show 10 entries

Source IP	Destination IP	Destin	Learn	Monitor	Protect	Schedule	Action
192.168.100.21	TEST (192.168.100.23)	2010				Permanent	ACCESS
192.168.100.213	TEST (192.168.100.23)	22				Permanent	
192.168.100.102	TEST (192.168.100.23)	22				Permanent	
192.168.100.21	TEST (192.168.100.23)	22				Permanent	
192.168.100.21	TEST (192.168.100.23)	50000				Permanent	
10.10.10.10	20.20.20.20	555				Permanent	

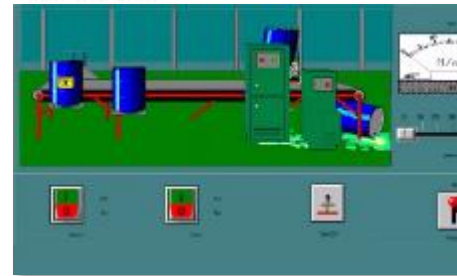
L'apprendimento automatico (facilitato da un ambiente deterministico) permette di abbattere l'onere di configurazione

Change Management & Control



```

Application Logic from Current (Revision: 13)
Condition: WhileRunning
Trigger Interval: 100ms
1 IF Counter == 0 THEN
2
3 IF Step1 == 0 THEN
4 HistTrend.ChartLength = 192;
5 HistTrend.ChartStart = (10149.707 + 86400.0) + 29700;
6 HistTrend.MinRange = 0;
7 HistTrend.MaxRange = 210;
8 Cursor2 = 0.5;
9 HistTrend.Pen4 = SetPoint.TagID;
10 Pen04 = SetPoint.TagID;
11 Step1 = 1;
12 Cycle = 100;
    
```



```

Application Logic from Current (Revision: 12)
Condition: WhileRunning
Trigger Interval: 100ms
1 IF Counter == 0 THEN
2
3 IF Step1 == 0 THEN
4 HistTrend.ChartLength = 192;
5 HistTrend.ChartStart = (10149.707 + 86400.0) + 29700;
6 HistTrend.MinRange = 0;
7 HistTrend.MaxRange = 200;
8 Cursor2 = 0.5;
9 HistTrend.Pen4 = SetPoint.TagID;
10 Pen04 = SetPoint.TagID;
11 Step1 = 1;
12 Cycle = 100;
    
```

