How deep is your OT protection?

La protezione di ICS e SCADA è solo un problema teorico dell'IT o una vera criticità che impatta sulla business continuity, sino a che punto si deve sviluppare?

Mario Testino **MEng, EMBA**
Chief Operating Officer
ServiTecno

Organizzato da

Le architetture OT industriali (Purdue Model – ANSI/ISA95)

Level 4

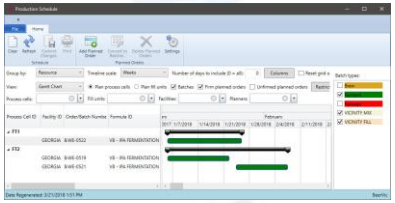
Business Planning & Logistics

Plant Production Scheduling, Operational Management, etc

4 - Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.

Time Frame

Months, weeks, days



Level 3

Manufacturing Operations Management

Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...

3 - Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process.

Time Frame

Days, Shifts, hours, minutes, seconds

Level 2

Batch Control

Continuous Control

Discrete Control

2 - Monitoring, supervisory control and automated control of the production process

Level 1

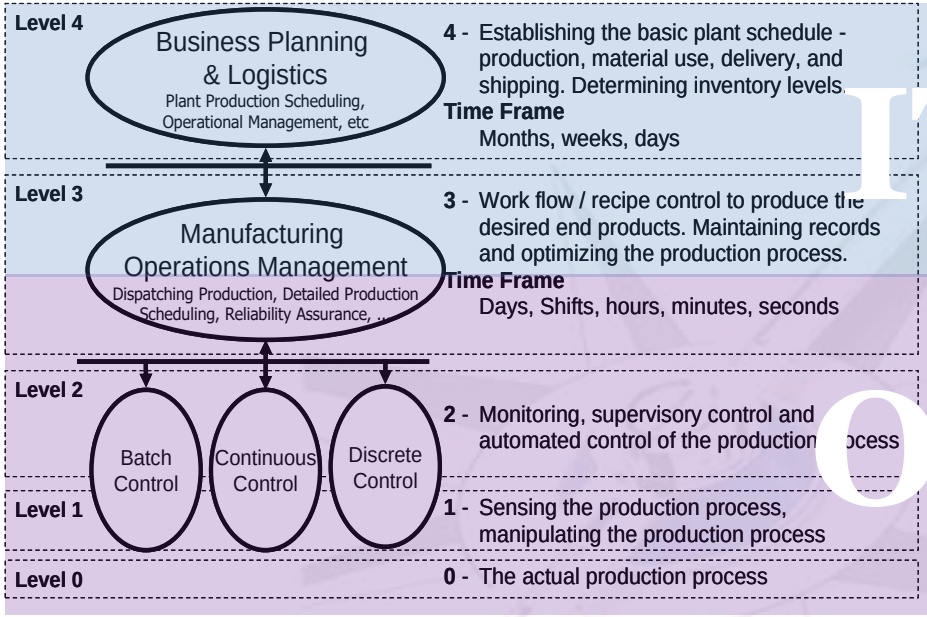
1 - Sensing the production process, oduction process

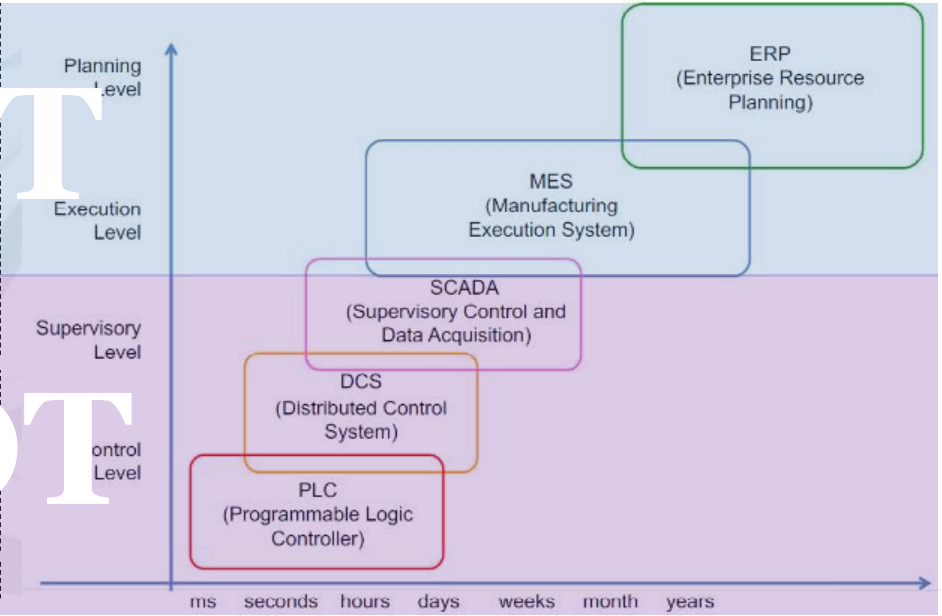
Level 0

0 - The actual production process

ISA 99/IEC 62443

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»
- Ciclo di Vita: anni

Requisiti Cogenti «Hot topics»
- Data Integrity
- Data Security
- Patent Infringment
- Business Continuity (management)

IT

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
- Ciclo di vita: decenni

Requisiti Cogenti «Hot Topics»
- People Safety
- Business Continuity (making)
- Service Continuity

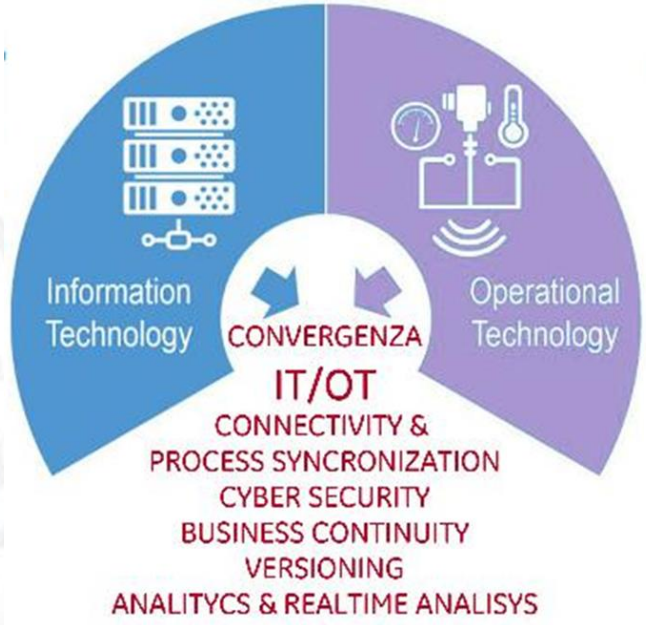
OT

Digitalizzazione

Convergenza IT - OT

Tutti gli standard informatici aziendali:

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

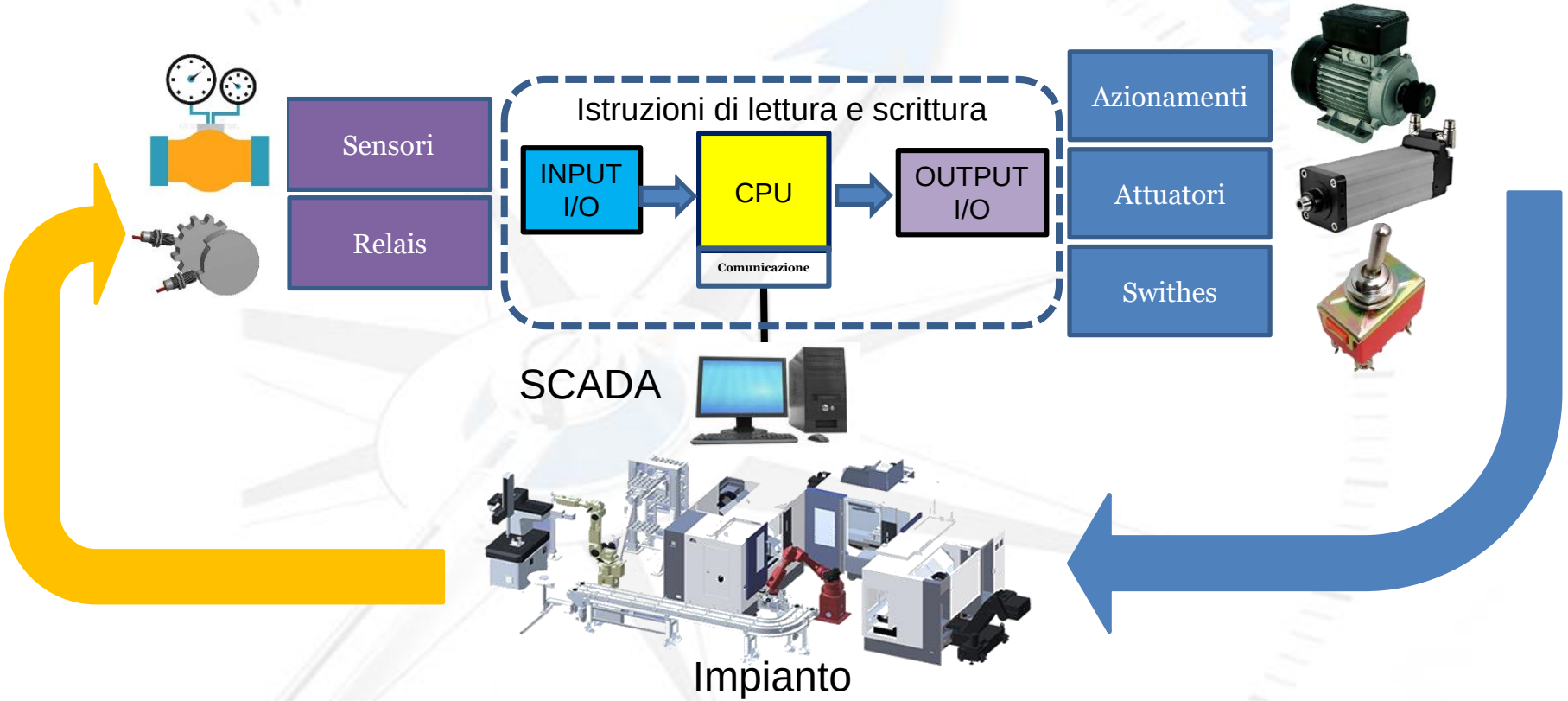


Tutti i sistemi di automazione, controllo, supervisione, storicizzazione, misura, analisi real-time di impianti, linee, macchine e in generale del processo produttivo:

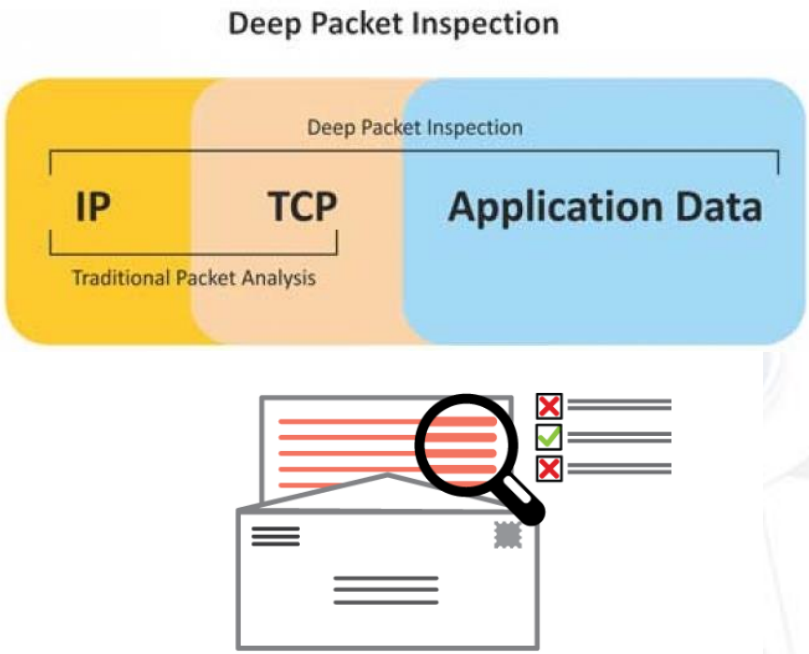
- PLC
- DCS
- CNC
- SCADA
- Robot
- Historian
- Sensori
- Attuatori

…

La «Fisica» del Controllore (PLC) e dei Protocolli di Comunicazione



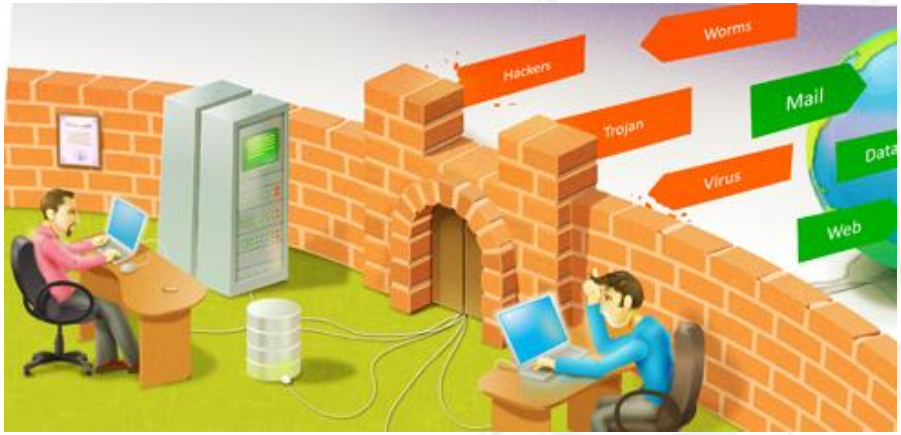
Protocol DPI (Deep Packet Inspection)

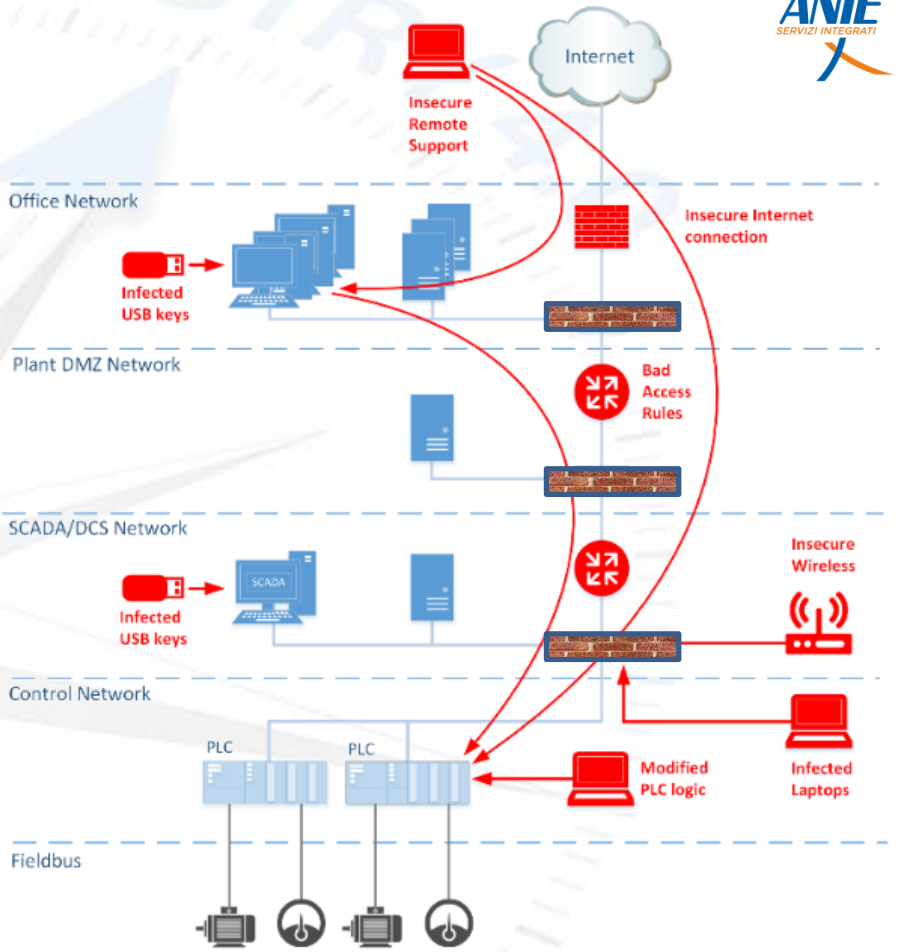


Function type			Function name
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs
		Internal Bits or Physical Coils	Read Coils
			Write Single Coil
			Write Multiple Coils
	16-bit access	Physical Input Registers	Read Input Registers
		Internal Registers or Physical Output Registers	Read 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

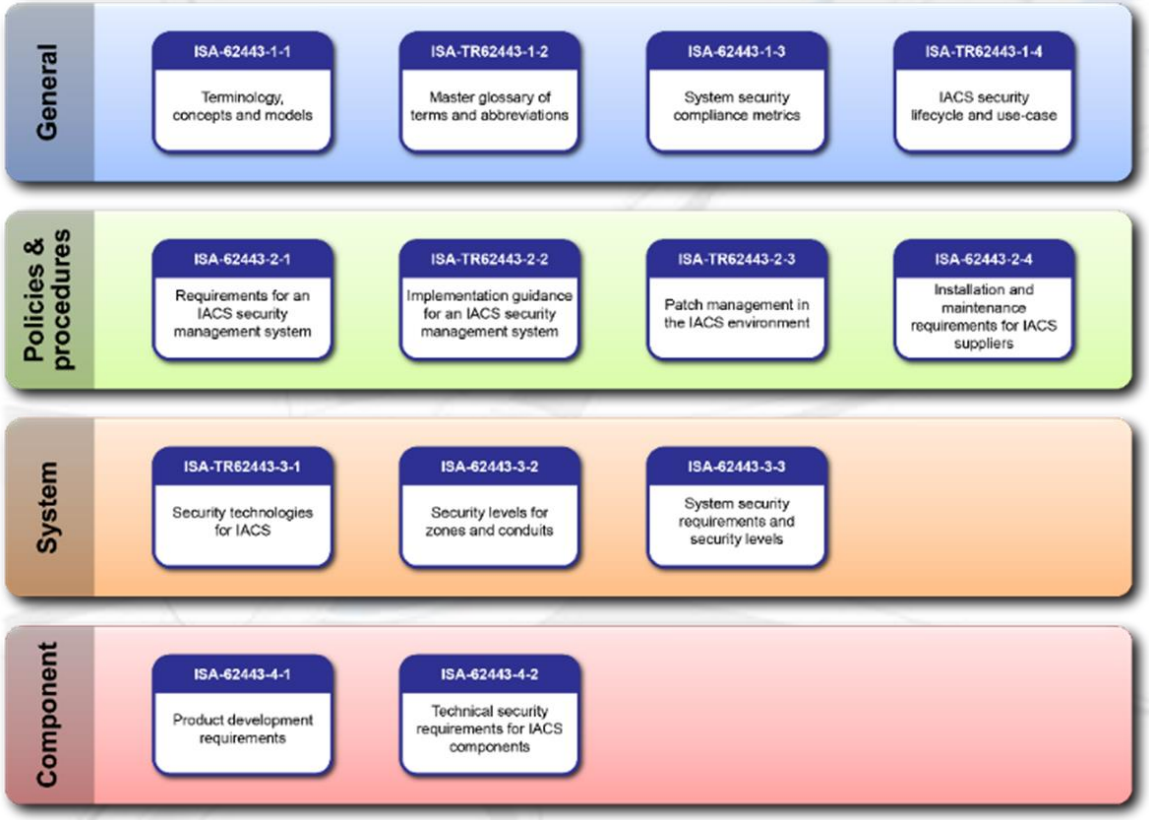
Attacchi e Incidenti informatici

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

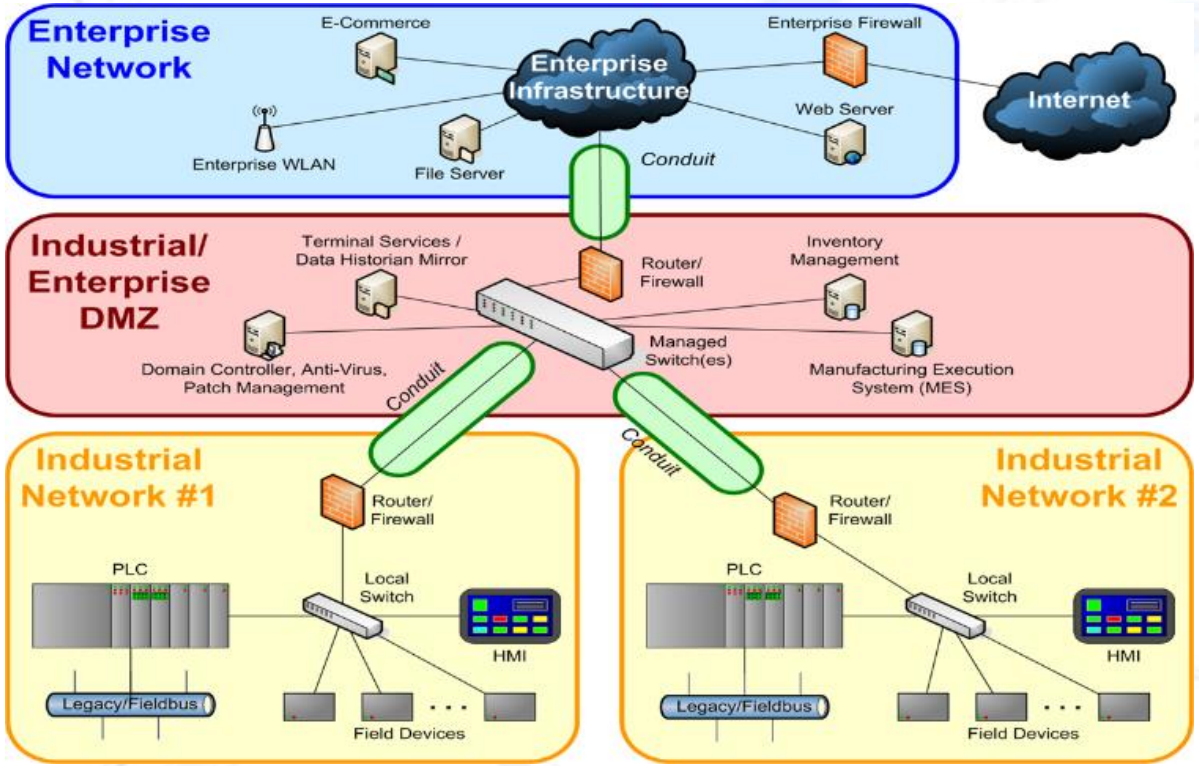




Lo standard di riferimento: IEC 62443 (ISA99)



IEC 62443 Architettura di sicurezza logica (Zones & Conduits)



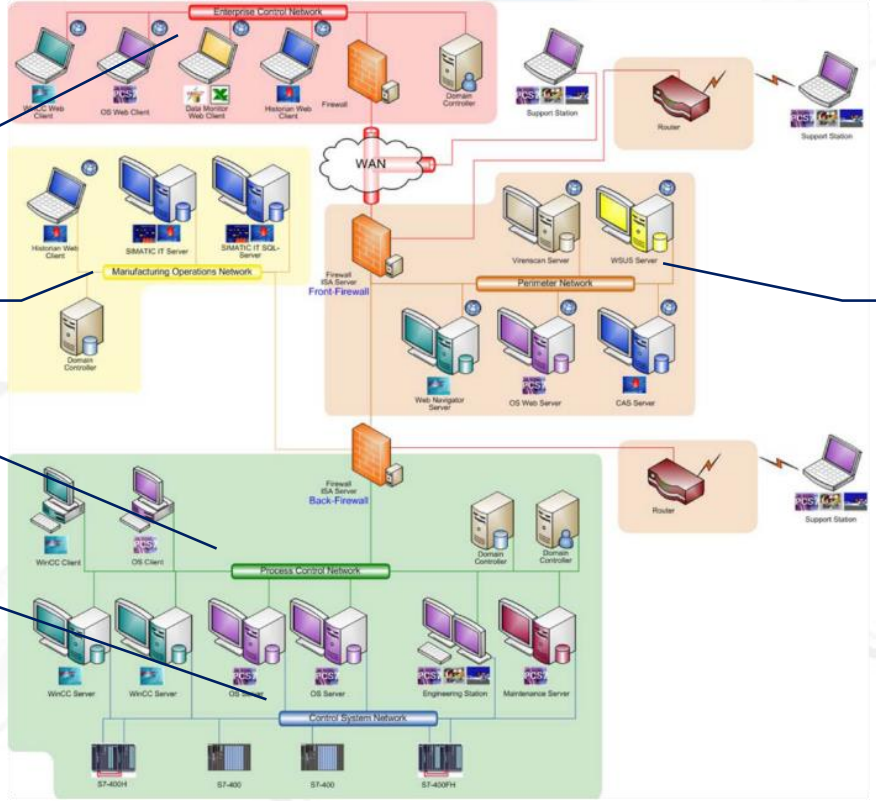
IEC 62443 Architettura di sicurezza logica (VLAN/DMZ)

Enterprise Control Network

Manufacturing Operations Network

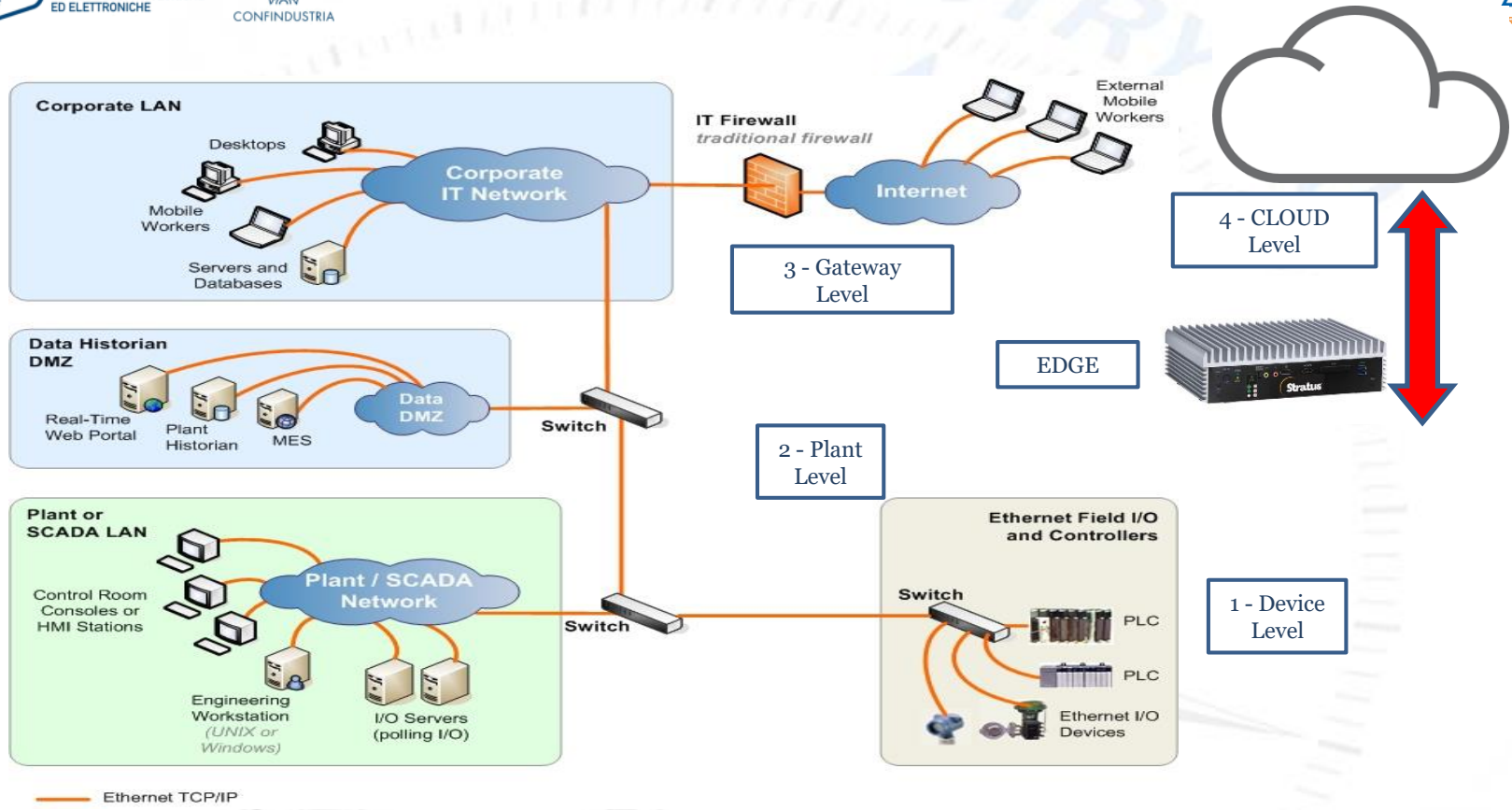
Process Control Network

Control System Network



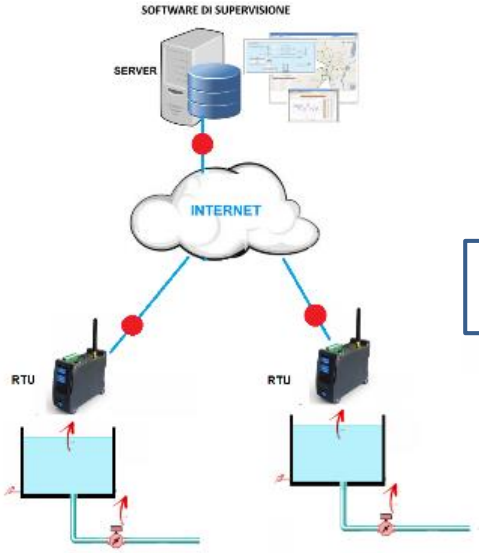
Perimeter Control Network

IEC 62443 Architettura di sicurezza logica

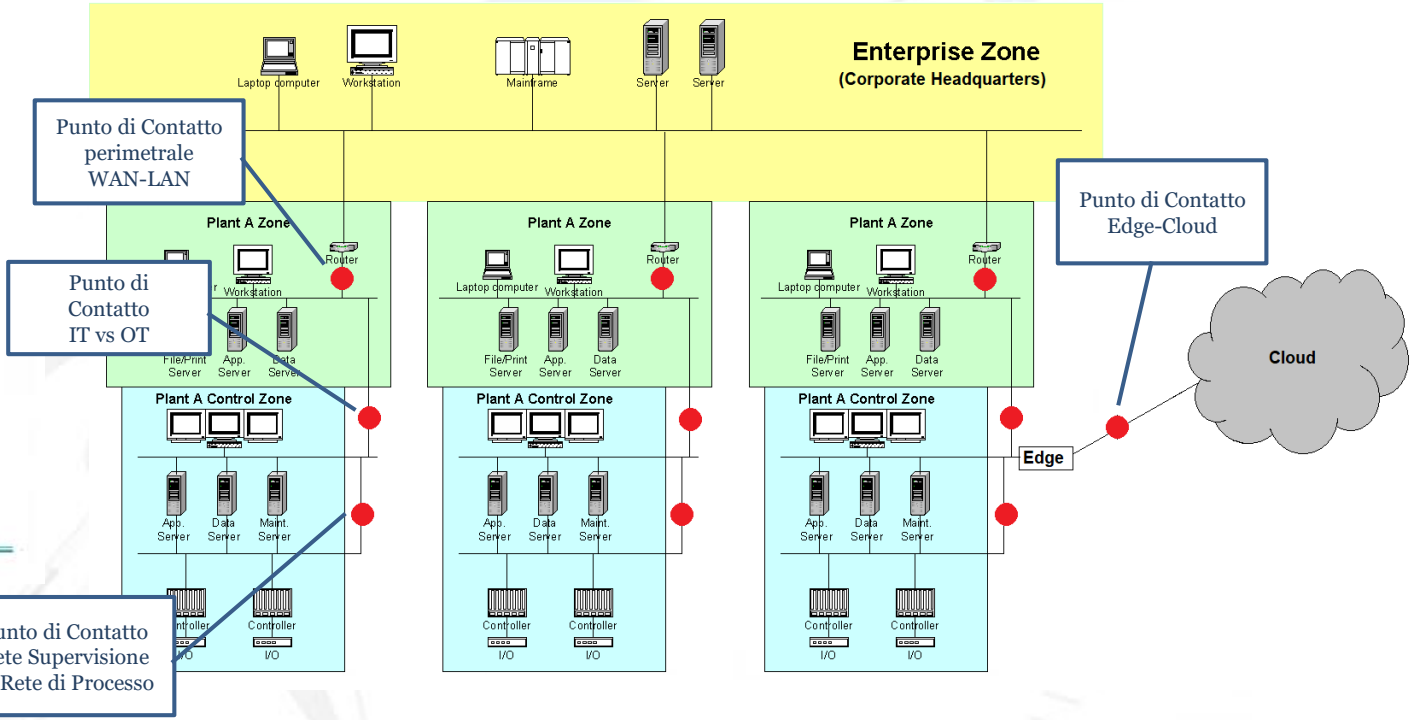


Criticità dei punti di Convergenza

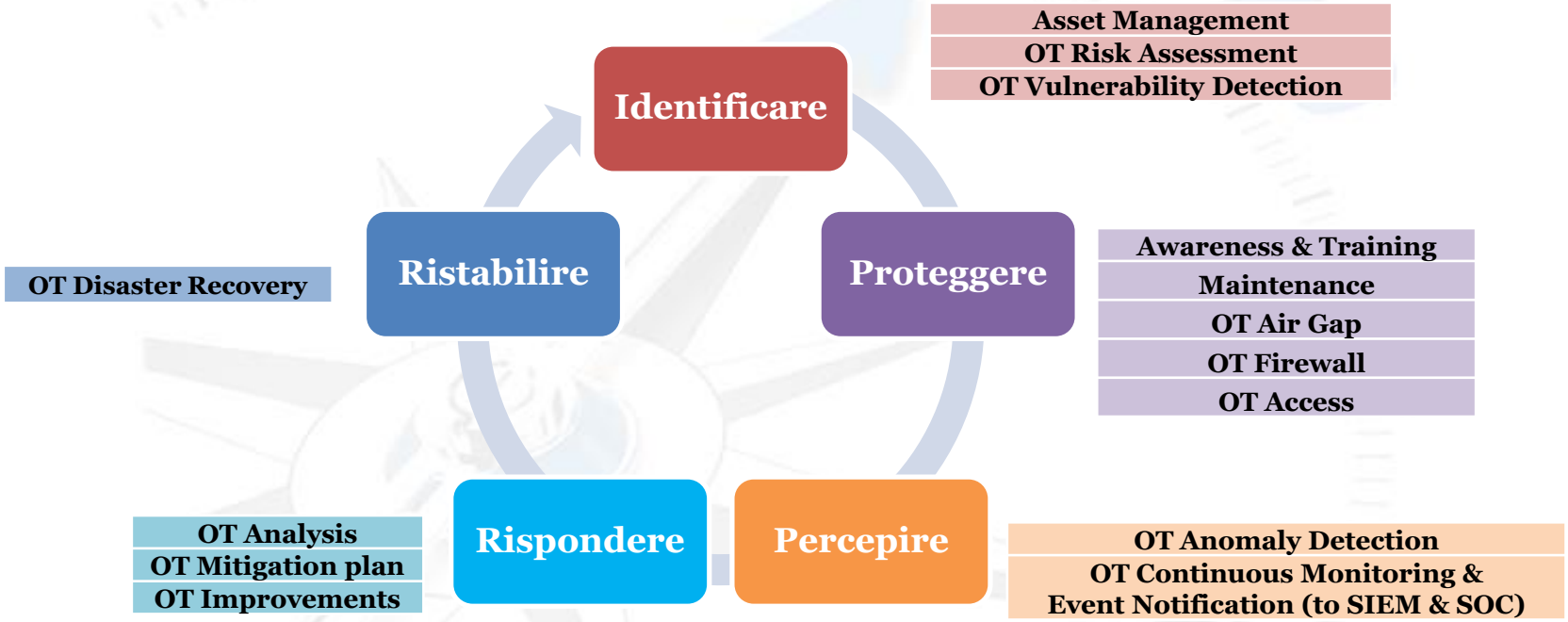
Sistema di Telecontrollo



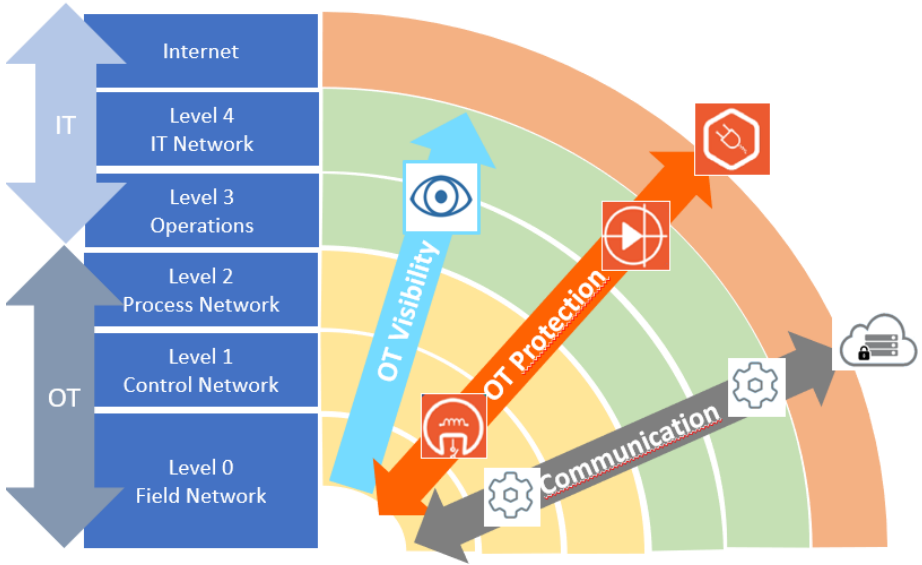
Sistema di rete azienda produttiva



Strategie di Protezione OT: La sicurezza un ciclo virtuoso



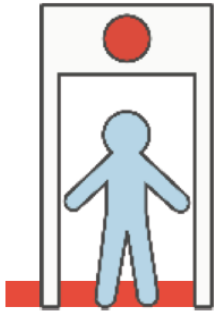
Strategie di Protezione OT: Layered Security (NIST)

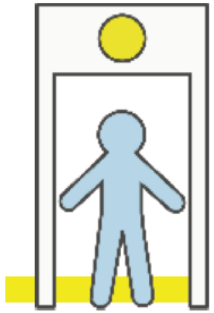


Assessment & Visibility	Identify (Asset Inventory & Intelligence)
	Assess (Vulnerability & Remediation)
	Detect (Anomaly & Threats)
	Act (Dashboard Alerts, Highlights & Notification)
Protection	Access On Site (VPN, High granular access policies)
	OT Segmentation (self configuration, DPI)
	AirGap bridge
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)

Strategie di Protezione OT: Layered Security (Esempio)

Last line of defense





STEP 03
Reinforced, locked cockpit door
Last line of defense / Endpoint protection

STEP 02
Only ticketed Passengers allowed on board
Segmentation (Authentication / Authorization enforcement)

STEP 01
ID check / Physical inspection
Perimeter protection

Continuità Operativa di Servizio (SLA)

Livello SLA Uptime [%]	Tempo annuo di Dowtime (Fermo)
99	3 giorni 15h 39m 29.5s
99.9	8h 45m 57.0s
99.99	52m 35.7s
99.999	5m 15.6s
99.9999	31.6s

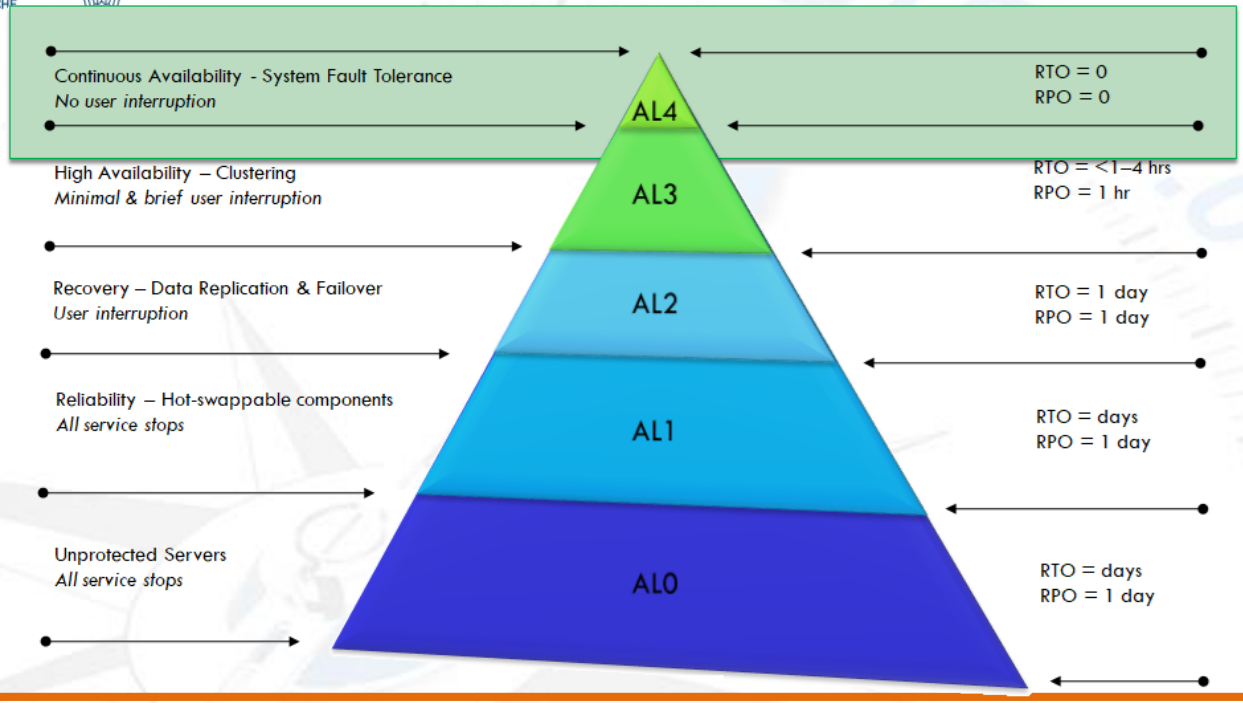
Sito Web

PC Office

OT

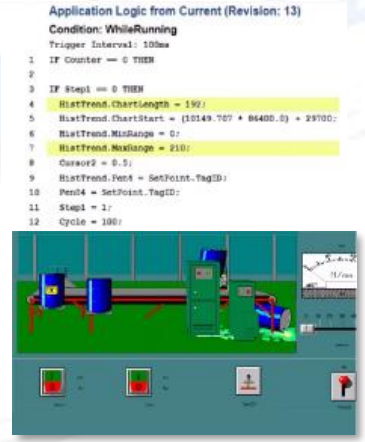
Server Fault Tolerant

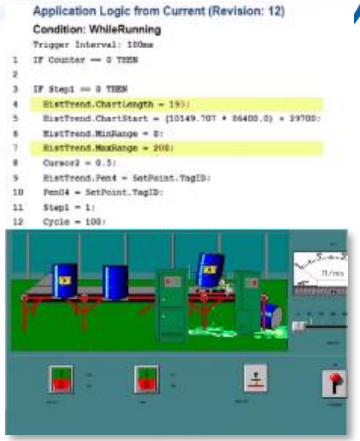
La piramide della Disponibilità

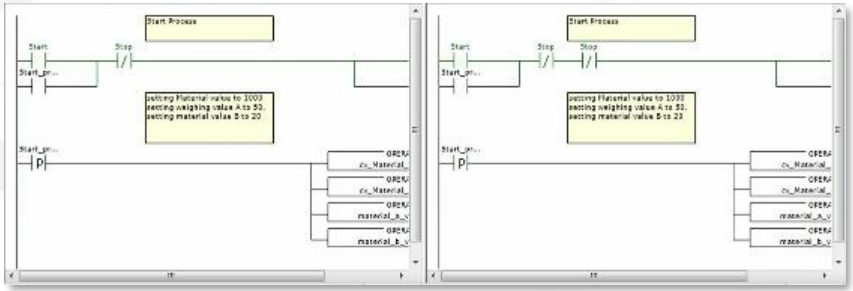


Il **Recovery Time Objective** (**RTO**) è il tempo necessario per il pieno recupero dell'operatività di un sistema. È in pratica la massima durata, prevista o tollerata, del downtime occorso.
Il **Recovery Point Objective** (**RPO**) è uno dei parametri usati nell'ambito delle politiche di disaster recovery per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua *messa in sicurezza* (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

Change Management & Control







Domande?

mtestino@servitecno.it