DIGITAL FORENSICS PER DISPOSITIVI IIOT: SFIDE PROSPETTIVE E CASI REALI

A CURA DI FABRIZIO GIULIANI

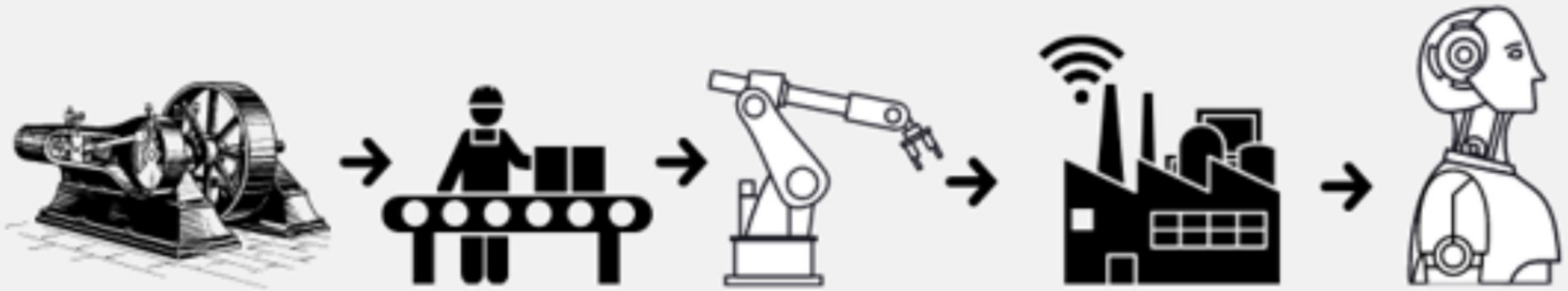
ONIF BARI 17 OTTOBRE 2025

CHI SONO

- Laureato in Ingegneria Meccanica presso l'Università La Sapienza di Roma
- Consulente Informatico Forense per privati, aziende ed Autorità Giudiziarie
- Iscritto Albo CTU Nazionale
- Perito ed Esperto C.C.I.I.A. di Roma
- Socio Ordinario ONIF Osservatorio Nazionale Informatica Forense
- Socio AIP Associazione Informatici Professionisti

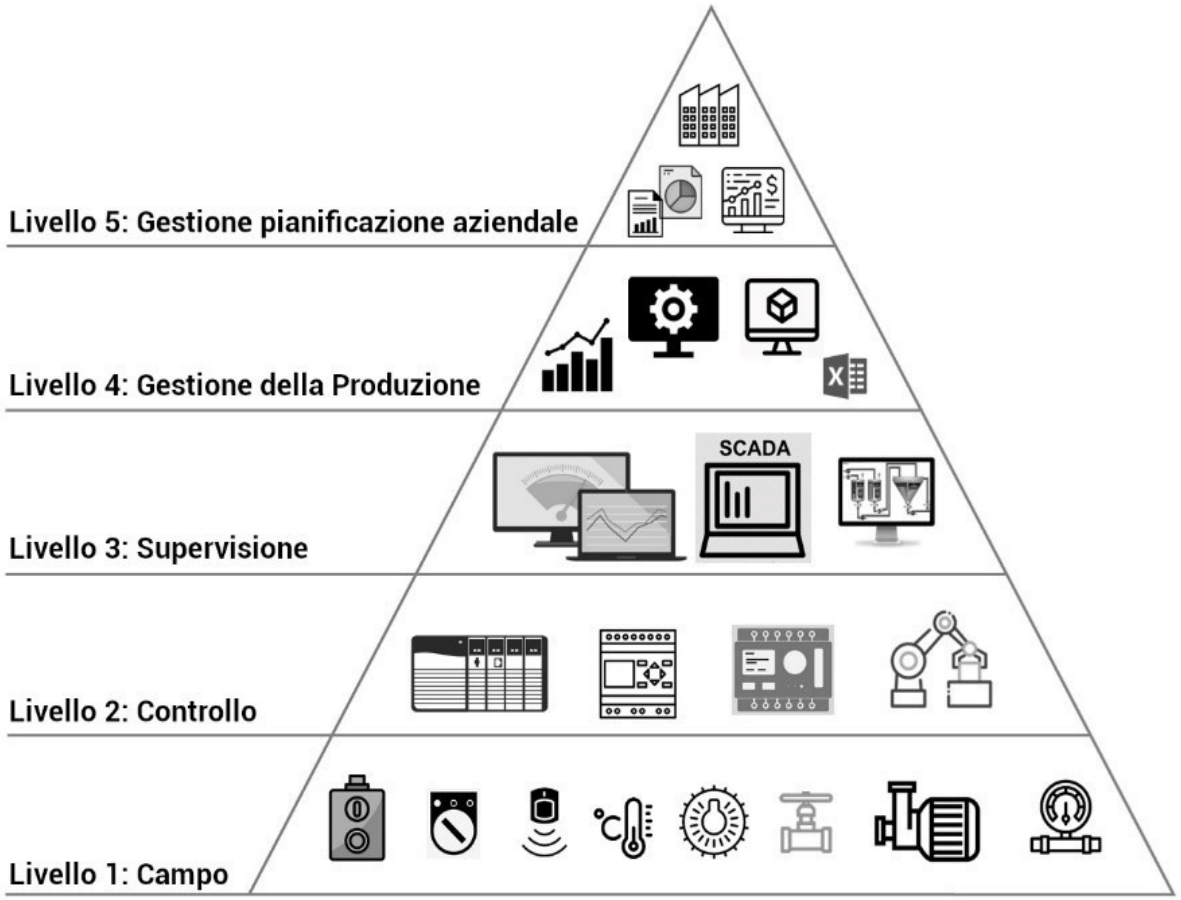
DISPOSITIVI IIOT

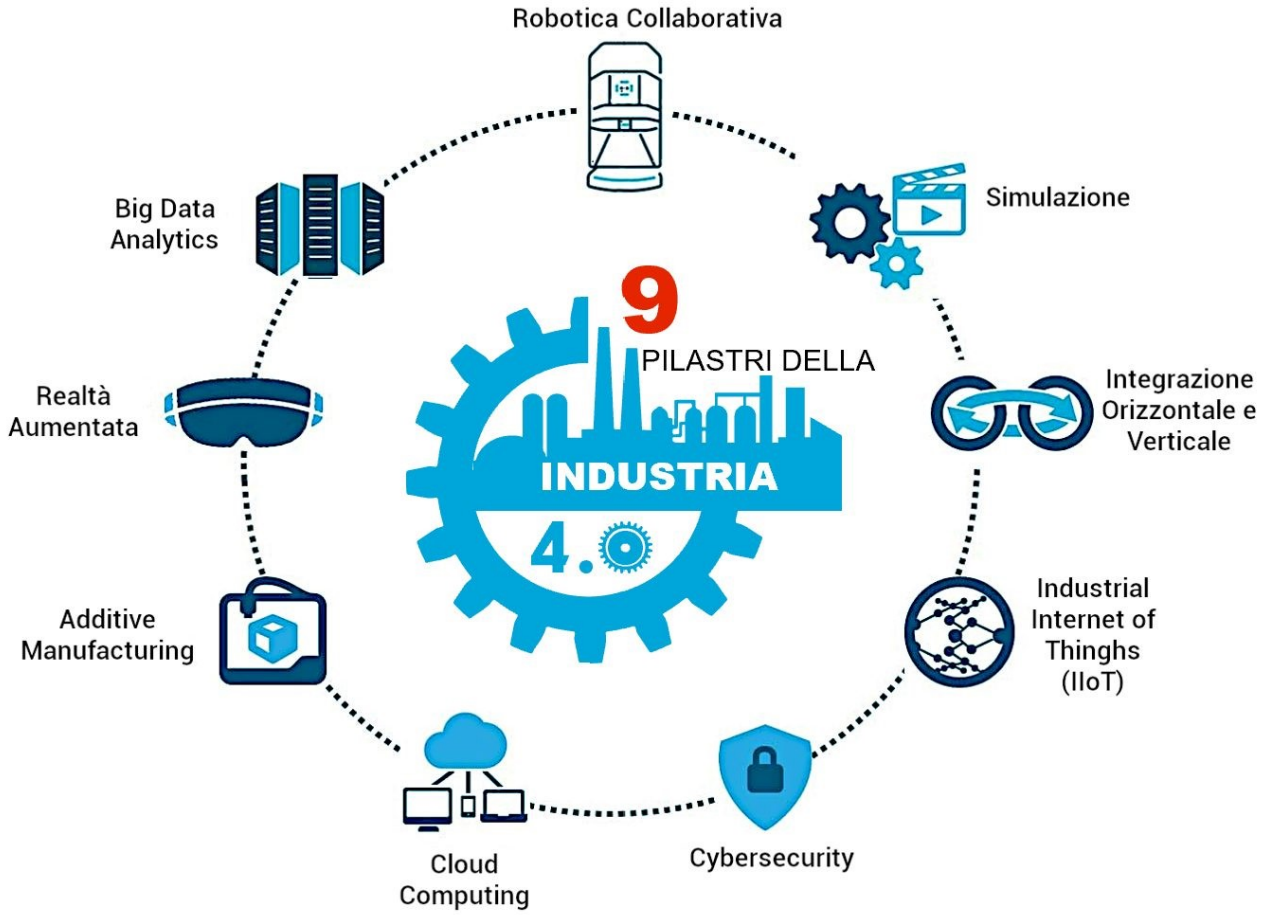
L'EVOLUZIONE DELL'INDUSTRIA



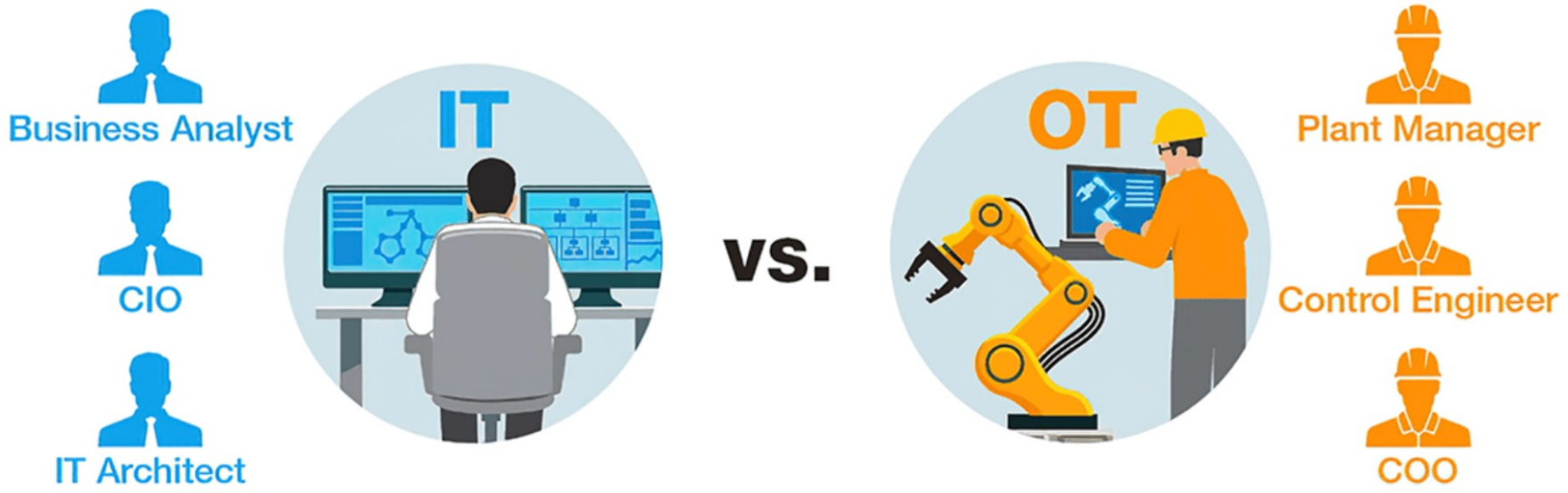
Industria 1.0	Industria 2.0	Industria 3.0	Industria 4.0	Industria 5.0
macchine, potenze di acqua e vapore	produzione di massa, energia elettrica, catena di montaggio	computer, produzione automatizzata, elettronica	sistemi cyber-fisici, IoT, networking, apprendimento automatico	collaborazione uomo-robot, sistemi cognitivi, personalizzazione
1800	1900	2000	2010	2020

INDUSTRIA 4.0





IT E OT: DIFFERENZE E INTERDIPENDENZE



No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

INNOVAZIONI NELL'INDUSTRIA 4.0

Miliardi di dati generati da sensori, smart meter, inverter, PLC, localizzatori ecc.

Analisi predittiva per anticipare domanda, produzione.

Ottimizzazione in tempo reale di produzione, reti, approvvigionamento.

Manutenzione predittiva e rilevamento anomalie (consumi, temperature, pressioni).

Tecnologie chiave: AI, machine learning, edge computing, digital twin, cloud.

DIGITAL FORENSICS: VULNERABILITÀ PER L'IIOT

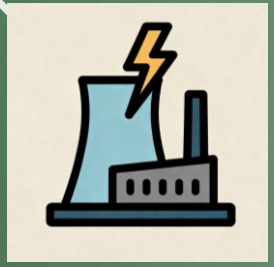
Dispositivi IoT poco sicuri
Firmware obsoleti, credenziali di default e assenza di aggiornamenti rendono sensori, smart meter, PLC facili bersagli.

Comunicazioni non cifrate
Protocolli come Modbus o DNP3 trasmettono comandi e dati senza protezione, esponendoli a intercettazioni o manomissioni.

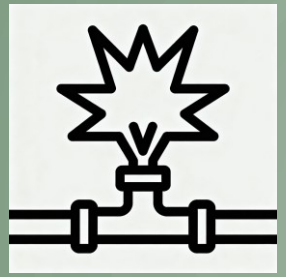
Accessi remoti vulnerabili
Inverter, edge computer, PLC, HMI, sono spesso accessibili da remoto senza adeguate misure di autenticazione e monitoraggio.

SCADA e sistemi industriali esposti
Software non aggiornati, mancanza di segmentazione e connessioni non protette mettono a rischio il cuore operativo.

Minacce dalla supply chain
Componenti di terze parti non verificati possono contenere backdoor o vulnerabilità nascoste.



Blackout diffusi per manipolazione di centrali elettriche o reti di distribuzione.



Sovrapressione o sabotaggio di gasdotti con possibili esplosioni.

Contaminazione dei prodotti (alterazioni nei processi alimentari o farmaceutici).

Rilascio ambientale di sostanze pericolose.

Manipolazione della segnaletica ferroviaria e semafori

Malfunzionamento intenzionale di sistemi medicali collegati

Contaminazione dell'acqua potabile e dell'ambiente .

STUXNET 2010

Un worm sfrutta le vulnerabilità di PLC Siemens per sabotare le centrifughe dell'arricchimento dell'uranio in Iran

UCRAINA 2015

Un attacco ai sistemi SCADA delle società di distribuzione interrompe la fornitura elettrica di 27 sottostazioni, creando un blackout per 225.000 utenti.

COLONIAL PIPELINE 2021

Un attacco ransomware colpisce Colonial Pipeline, il principale oleodotto degli Stati Uniti, bloccando i sistemi informatici aziendali e causando carenze di carburante e forti disagi sulla East Coast.

FLORIDA WATER TREATMENT 2021

Un attaccante accede da remoto al sistema di trattamento acque della città di Oldsmar, aumentando di 100 volte la quantità di idrossido di sodio, mettendo a rischio la sicurezza pubblica.

ULTIMISSIME

MATT BURGESS ECONOMIA 28.09.2025

Jaguar Land Rover, come un cyberattacco ha messo in ginocchio la filiera della casa britannica

La produzione della casa britannica è ferma da tre settimane, con perdite che ammontano a decine di milioni ed effetti a catena su tutta la linea di fornitura

Cyberattacco, colpiti aeroporti Bruxelles, Berlino e Londra. Ritardi su 200 voli. Evacuato scalo Dublino

Ritardi e cancellazioni colpiscono voli in Europa a causa di un attacco a un fornitore di sistemi aeroportuali

20 settembre 2025

MONDO | Venerdì 3 ottobre 2025

La birra più popolare in Giappone sta finendo

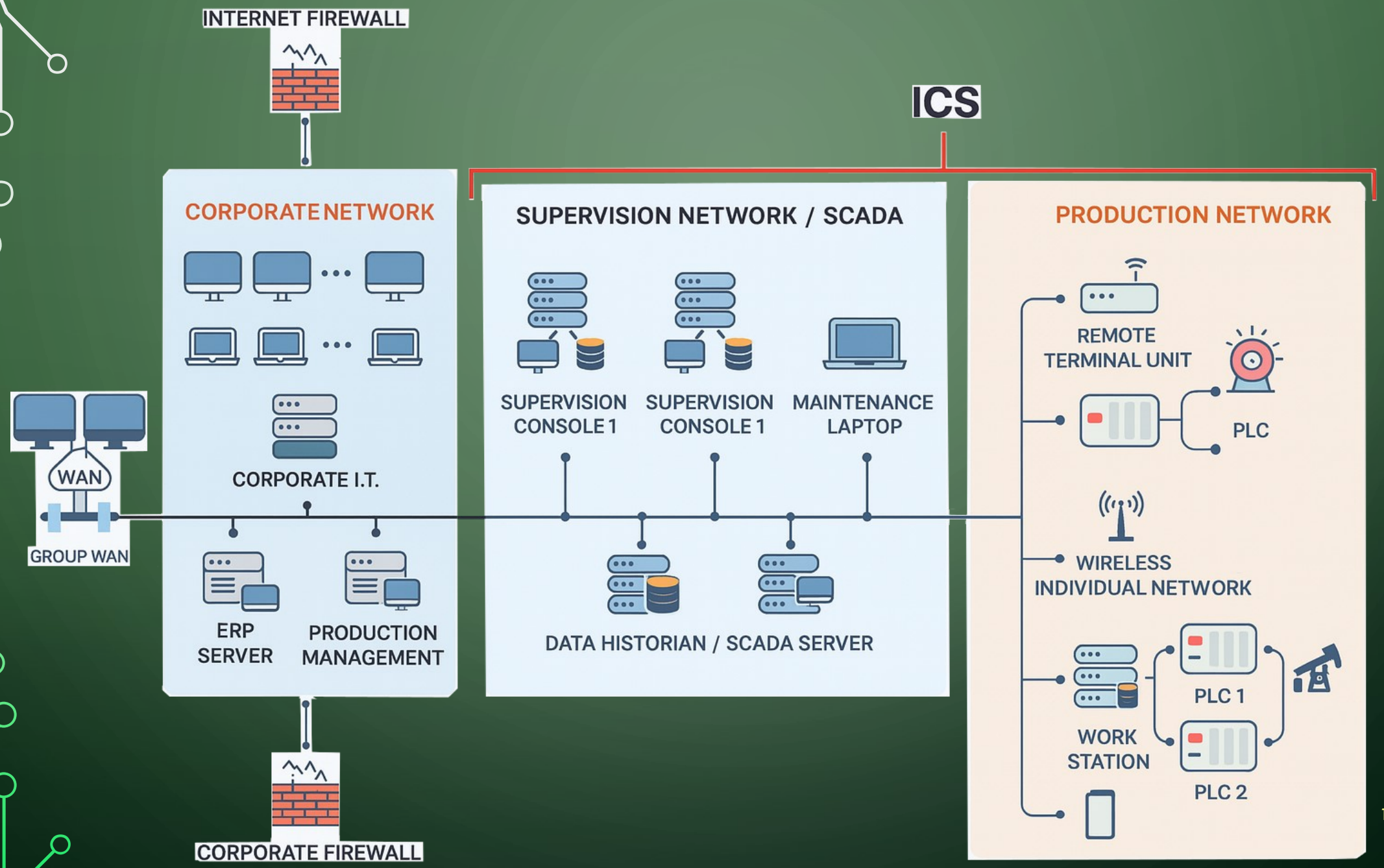
Da lunedì la Asahi ha interrotto la produzione a causa di un attacco informatico, e non si sa quando potrà ripartire

Infrastrutture Energetiche Nel Mirino! Gli Inverter Cinesi Sono Controllati Da Remoto

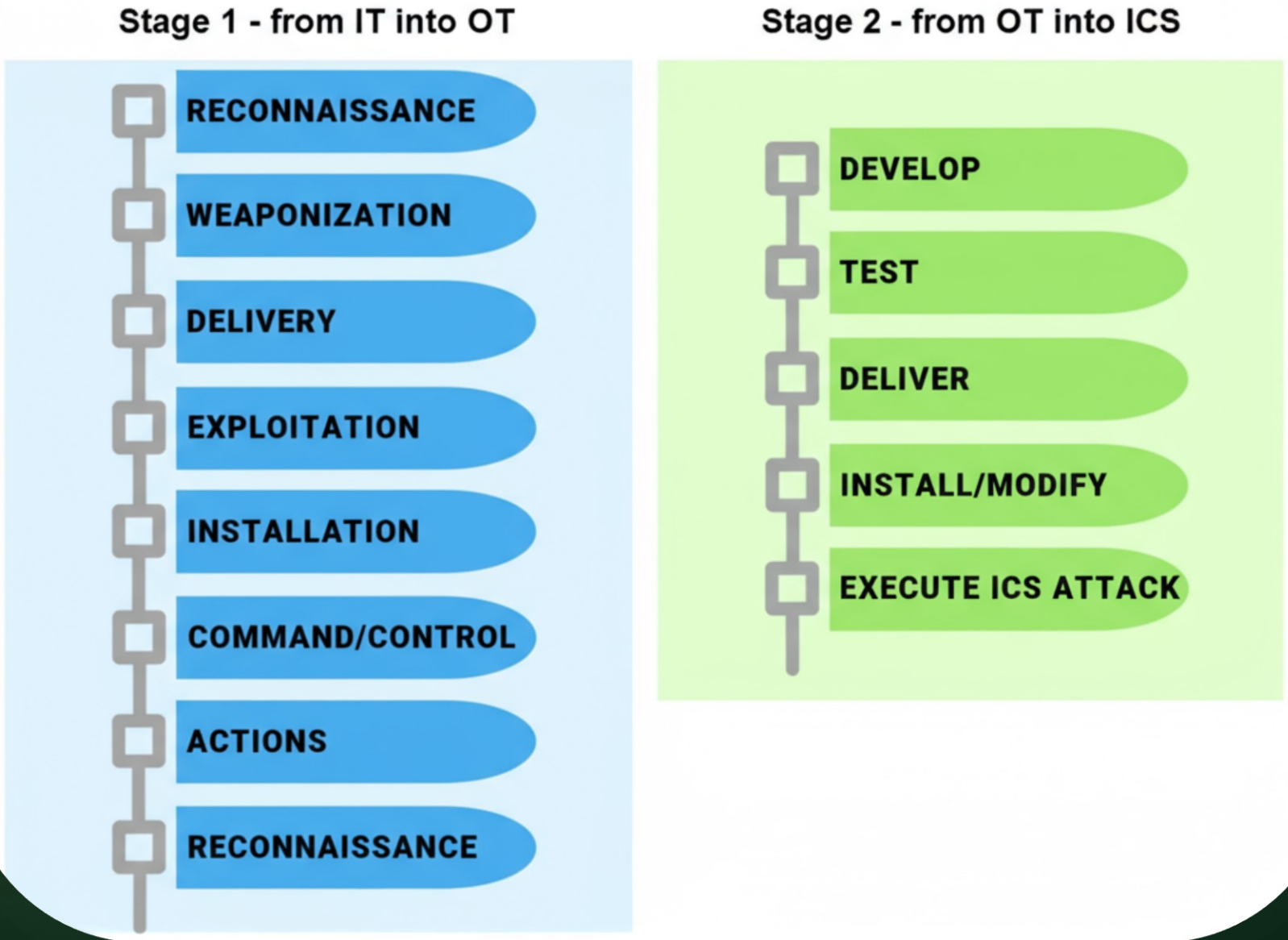
Redazione RHC : 14 Maggio 2025 20:26

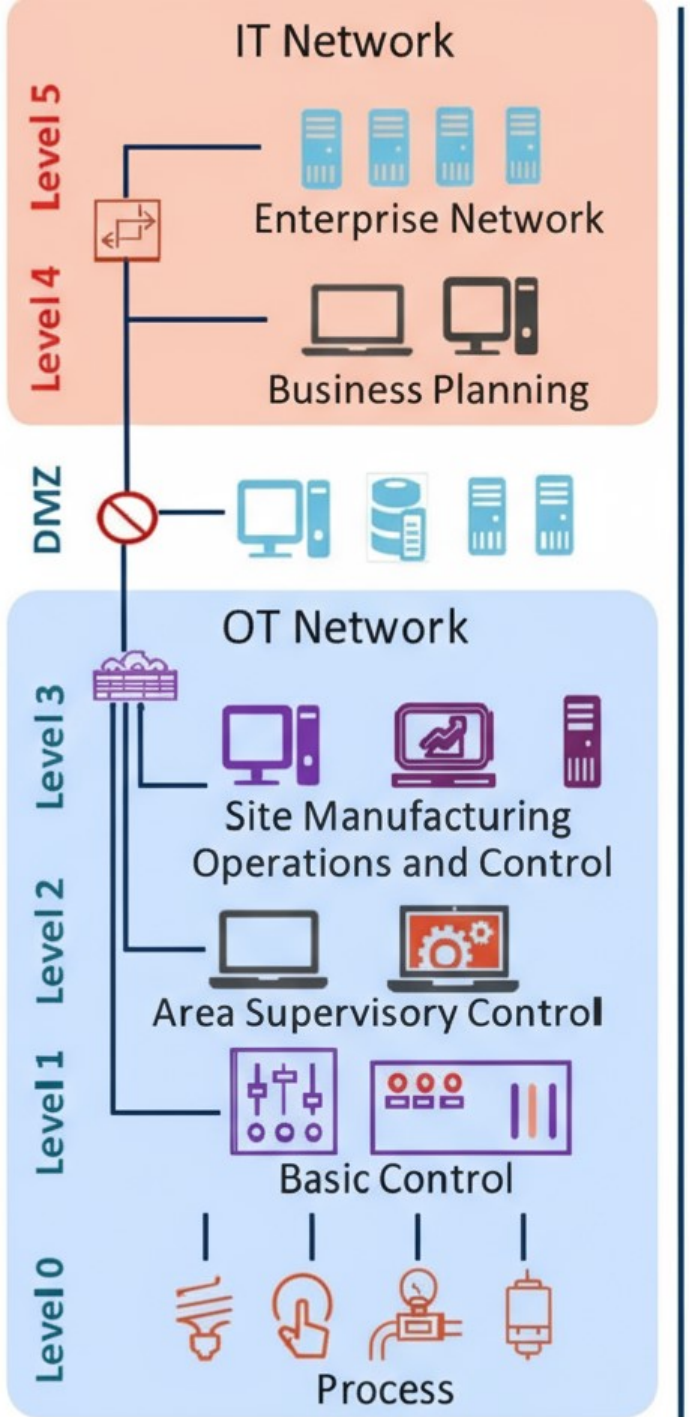
Bridgestone colpita da un sospetto attacco informatico, operazioni interrotte negli Stati Uniti e in Canada

News - Breaches & Ransoms


INTERNET FIREWALL
ICS
CORPORATE NETWORK
SUPERVISION NETWORK / SCADA
PRODUCTION NETWORK
WAN
GROUP WAN
CORPORATE I.T.
ERP SERVER
PRODUCTION MANAGEMENT
SUPERVISION CONSOLE 1
SUPERVISION CONSOLE 1
MAINTENANCE LAPTOP
DATA HISTORIAN / SCADA SERVER
REMOTE TERMINAL UNIT
PLC
WIRELESS INDIVIDUAL NETWORK
WORK STATION
PLC 1
PLC 2
CORPORATE FIREWALL

ICS Cyber Kill Chain

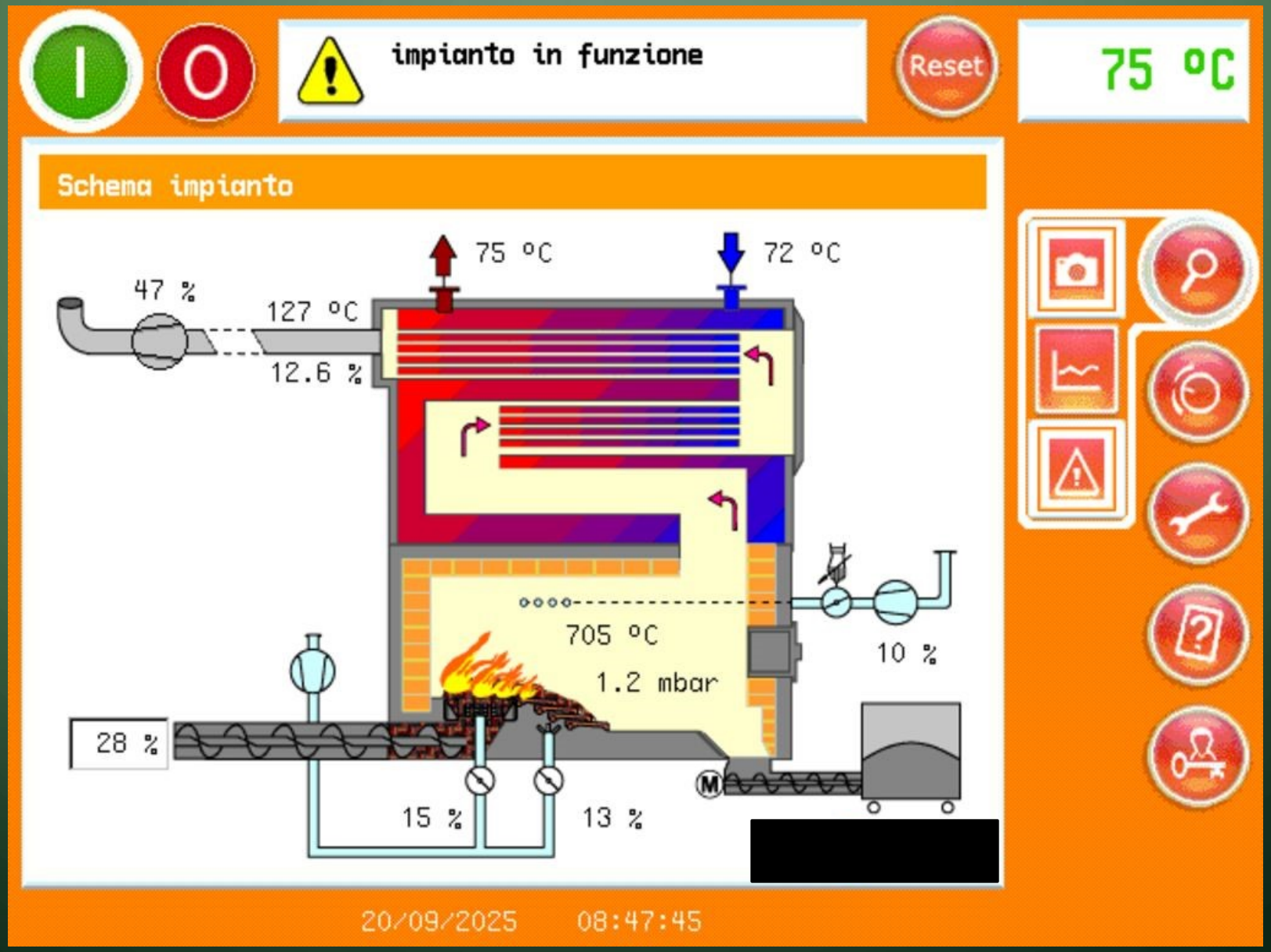


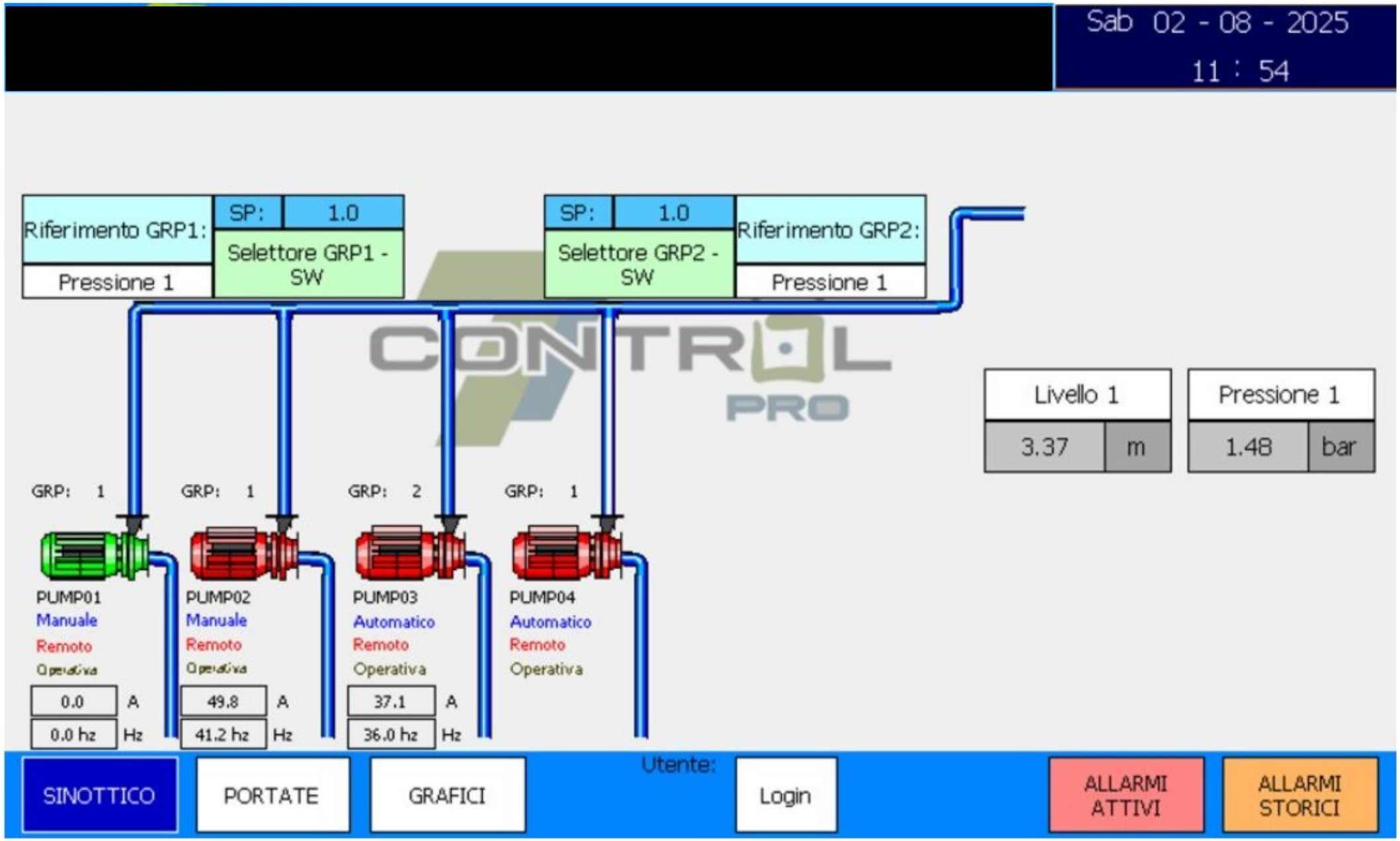


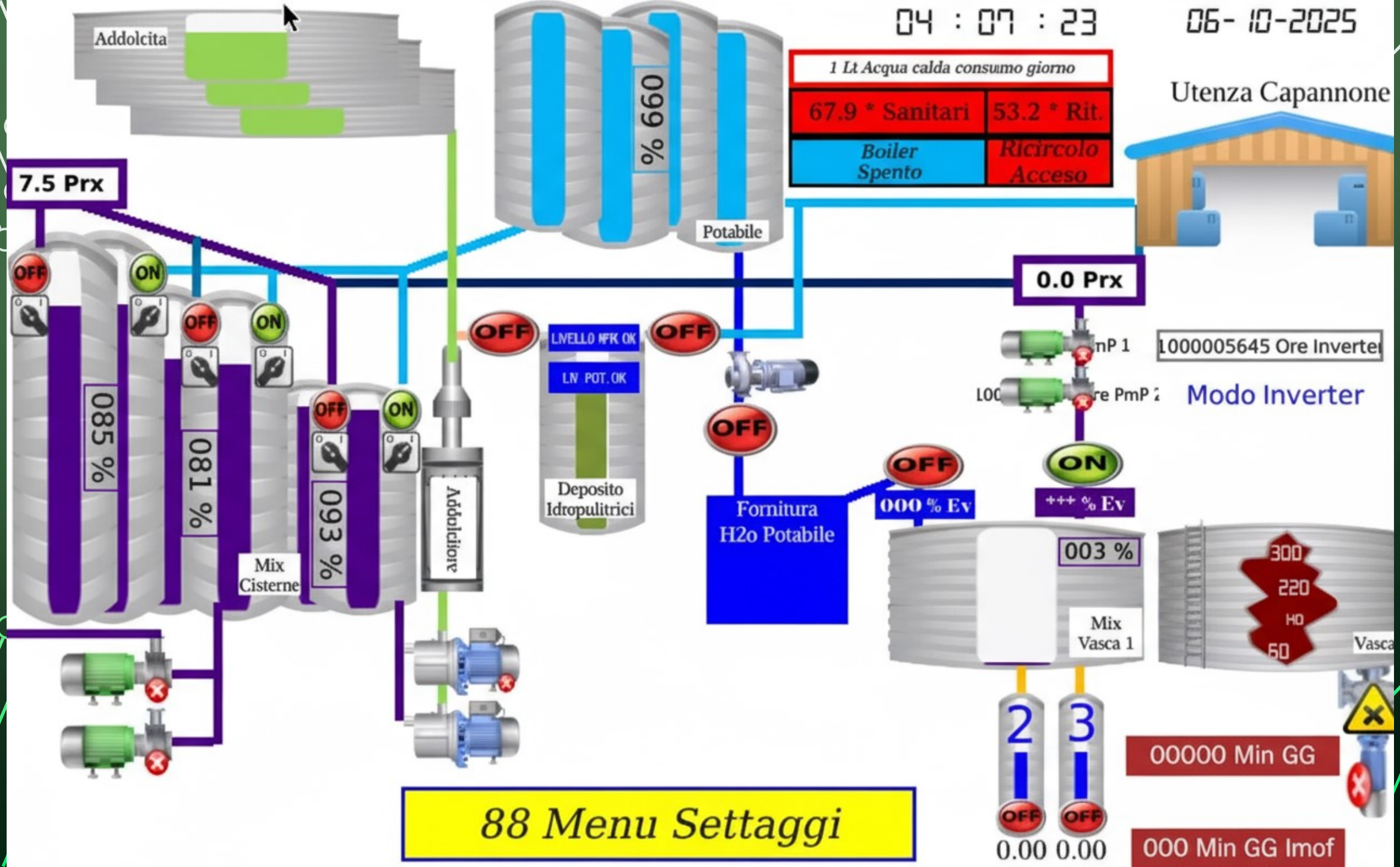
Planning		Reconnaissance
Preparation	Weaponization	Targeting
Cyber Intrusion	Attempt	Delivery
		Exploit
	Success	Install/Modify
Management & Enablement		C2
Sustainment, Entrenchment Development & Execution		Act
Attack Development & Tuning		Develop
Validation		Test
ICS Attack		Deliver
		Install/Modify
		Execute

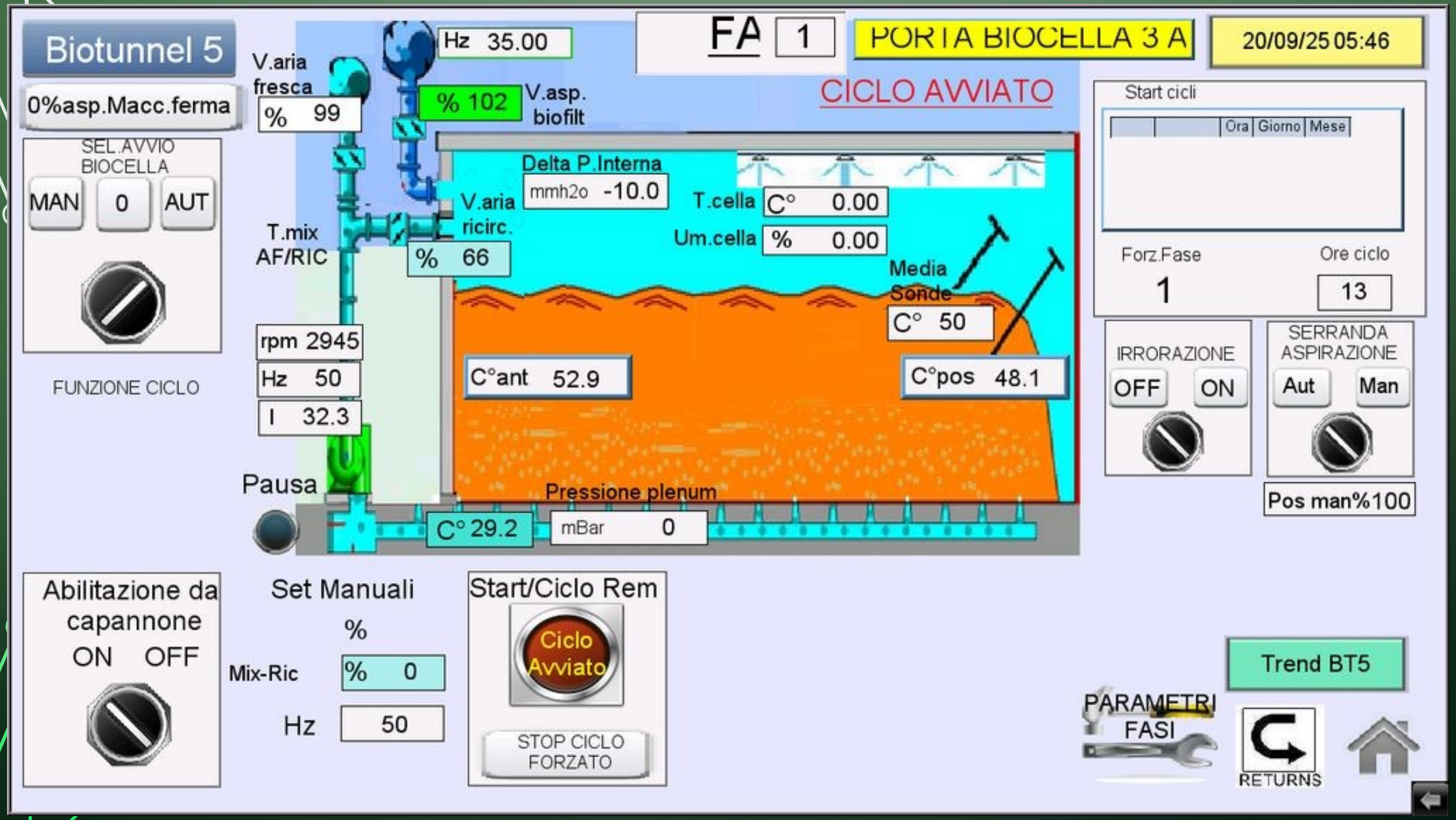
- Spear phishing
- Installazione Malware BlackEnergy 3
- Furto di credenziali
- Utilizzo (VPN) per entrare nella rete ICS
- Compromissione dispositivi comunicazione serial-ethernet
- Cancellazione mirata di alcuni log
- Attacco (denial-of-service) contro il call center

ESEMPI DI DISPOSITIVI IIOT ESPOSTI




Sab 02 - 08 - 2025
11 : 54
Riferimento GRP1:
Pressione 1
SP:
1.0
Selettore GRP1 - SW
SP:
1.0
Selettore GRP2 - SW
Riferimento GRP2:
Pressione 1
CONTROL PRO
Livello 1
3.37
m
Pressione 1
1.48
bar
GRP: 1
GRP: 1
GRP: 2
GRP: 1
PUMP01
Manuale
Remoto
Operativa
0.0
A
0.0 hz
Hz
PUMP02
Manuale
Remoto
Operativa
49.8
A
41.2 hz
Hz
PUMP03
Automatico
Remoto
Operativa
37.1
A
36.0 hz
Hz
PUMP04
Automatico
Remoto
Operativa
SINOTTICO
PORTATE
GRAFICI
Utente:
Login
ALLARMI ATTIVI
ALLARMI STORICI


04 : 07 : 23
06- 10-2025
Addolcita
% 660
Potabile
1 Lt Acqua calda consumo giorno
67.9 * Sanitari
53.2 * Rit.
Boiler Spento
Ricircolo Acceso
Utenza Capannone
7.5 Prx
0.0 Prx
OFF
ON
085 %
081 %
093 %
Mix Cisterne
Addolcitore
LIVELLO MFK OK
LN POT.OK
Deposito Idropulitrici
Fornitura H2o Potabile
1000005645 Ore Inverter
Modo Inverter
000 % Ev
+++ % Ev
003 %
Mix Vasca 1
300
220
HO
60
Vasca
2
3
0.00 0.00
00000 Min GG
000 Min GG Imof
88 Menu Settaggi


Biotunnel 5
0%asp.Macc.ferma
SEL.AVVIO BIOCELLA
MAN
0
AUT
FUNZIONE CICLO
V.aria fresca
% 99
Hz 35.00
% 102
V.asp. biofilt
FA 1
PORTA BIOCELLA 3 A
20/09/25 05:46
CICLO AVVIATO
Start cicli
Ora
Giorno
Mese
Delta P.Interna
mmh2o -10.0
V.aria ricirc.
% 66
T.mix AF/RIC
T.cella C° 0.00
Um.cella % 0.00
Media Sonde
C° 50
Forz.Fase
1
Ore ciclo
13
rpm 2945
Hz 50
I 32.3
C°ant 52.9
C°pos 48.1
IRRORAZIONE
OFF
ON
SERRANDA ASPIRAZIONE
Aut
Man
Pos man%100
Pausa
Pressione plenum
C° 29.2
mBar 0
Abilitazione da capannone
ON OFF
Set Manuali
%
Mix-Ric % 0
Hz 50
Start/Ciclo Rem
Ciclo Avviato
STOP CICLO FORZATO
Trend BT5
PARAMETRI FASI
RETURNS

DIGITAL FORENSICS: FONTI DI PROVA NELL'IIoT

SENSORI, SMART METER: log misurazioni, registri eventi, consumi.

CLOUD/EDGE: log transazioni, API call, file config.

PLC: log input/output, cronologia firmware.

SCADA/HMI: log accessi, allarmi, parametri, script.

RETE, FIREWALL: log accessi, pacchetti MQTT, Modbus, VPN.

SFIDE PER LA DIGITAL FORENSICS NELL'IIOT

ETEROGENEITÀ DEI DISPOSITIVI

VOLATILITÀ DEI DATI

LIMITAZIONI LOGISTICHE

CONTINUITÀ OPERATIVA

CRITICITÀ LEGALI E DI CONFORMITÀ

BEST PRACTICE

LOGGING AVANZATO FORMAZIONE

CORRELAZIONE IT-OT-FORENSICS E CYBERSECURITY

RESILIENZA PROGETTUALE FORENSICS BY DESIGN

VULNERABILITY ASSESSMENT PENETRATION TEST

BACKUP, SNAPSHOT, VERSIONING COMPLIANCE

PROSPETTIVE FUTURE

FORENSICS-AS-A-SERVICE (FAAS)

STANDARDIZZAZIONE DEI LOG

FORENSICS PREDITTIVA CON AI

MEMRISTORI

SICUREZZA POST-QUANTISTICA

GRAZIE PER L'ATTENZIONE

fgiuliani@fabriziogiuliani.com

www.fabriziogiuliani.com

www.linkedin.com/in/fabriziogiuliani