FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

ANIE AUTOMAZIONE

Connected, Intelligent, Secure: la nuova frontiera dell'automazione industriale



Davide Travaglia
Senior Solution Consultant

Rockwell Automation

expanding **human possibility**®

Perché “oltre l’Edge”?

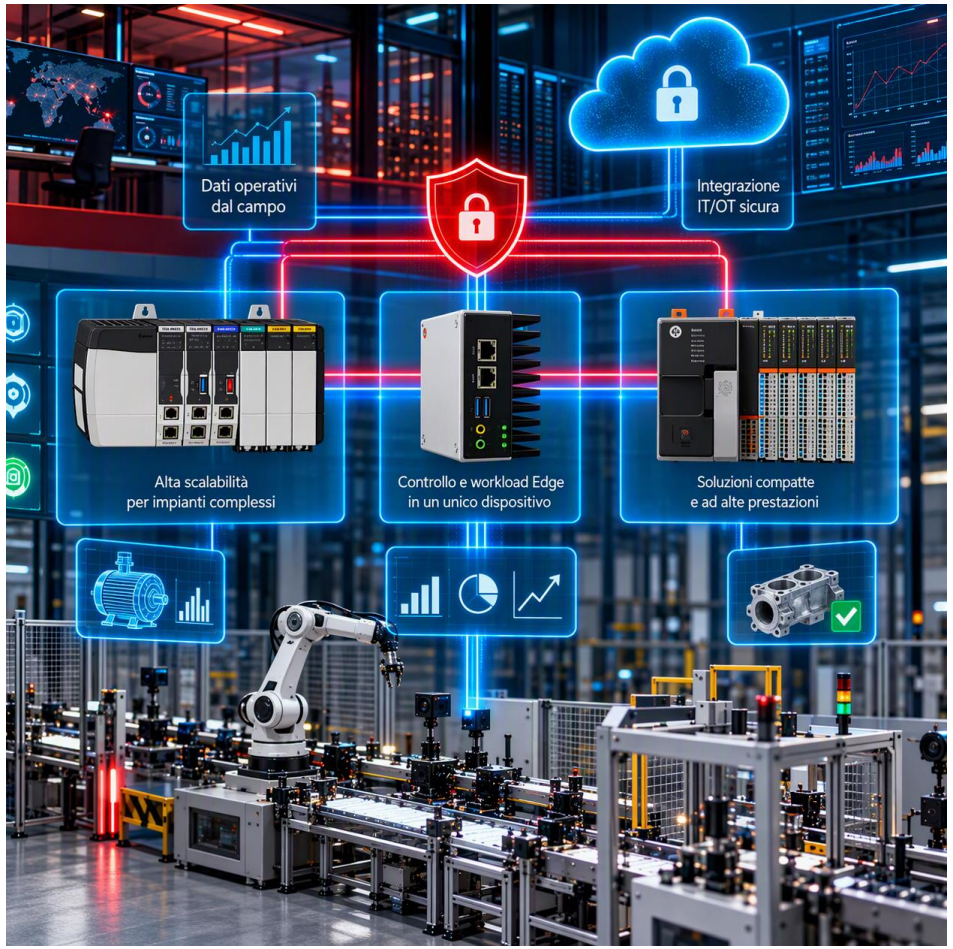
Connessione, intelligenza e sicurezza devono diventare una sola architettura operativa.

CONNETTERE Sistemi PAC e di terze parti

CONTESTUALIZZARE Trasformare segnali in informazioni

DECIDERE Portare analytics e AI vicino al processo

PROTEGGERE Applicare security by design



Dal dato grezzo a un’azione affidabile

Software-Defined Automation

Controllo deterministico e workload Edge convergono in un’architettura software-centrica.

CONTROLLO + COMPUTE

Un’unica piattaforma per logica di controllo e applicazioni Edge

WORKLOAD FLESSIBILI

Analytics, visualizzazione e servizi eseguiti vicino al processo

ARCHITETTURA APERTA

OCI Containers, API e protocolli standard per integrare domini OT e IT

SECURITY BY DESIGN

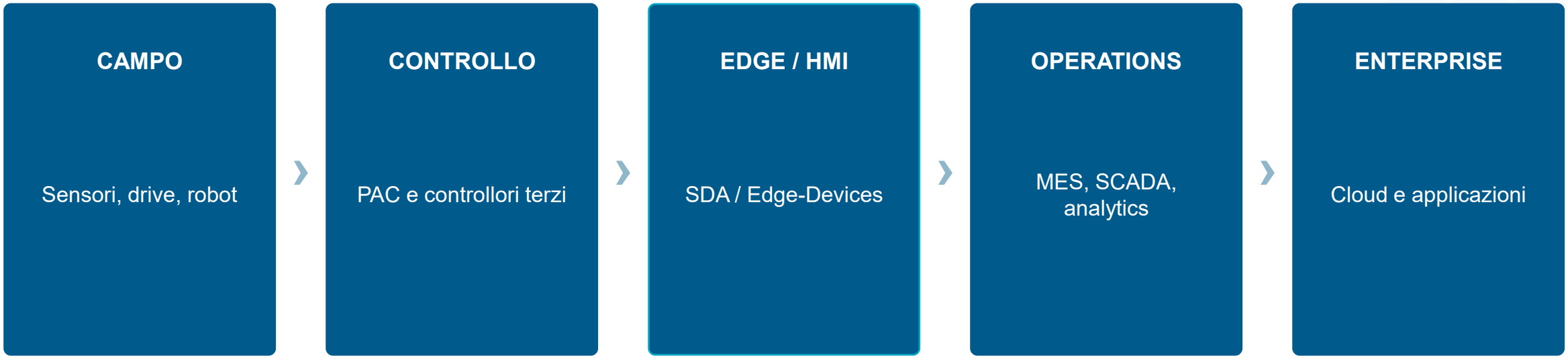
Identità, segmentazione, comunicazioni protette e gestione del ciclo di vita



Dal dispositivo al sistema: più flessibilità di deployment, meno hardware dedicato, dati disponibili dove generano valore.

CONNECTED | Interoperabilità dal campo all’enterprise

Un’architettura aperta rende il dato riutilizzabile lungo tutta la catena del valore.



OPC UA • MQTT • REST API • driver nativi • modelli informativi

Il punto non è spostare più dati, ma renderli comprensibili e disponibili dove servono.

INTELLIGENT | L’AI industriale parte dal contesto

Dall’assistenza all’ingegneria fino alle decisioni operative, mantenendo la governance.



1. DATI AFFIDABILI — Connettività e qualità del dato

2. CONTESTO — Modelli, asset e relazioni

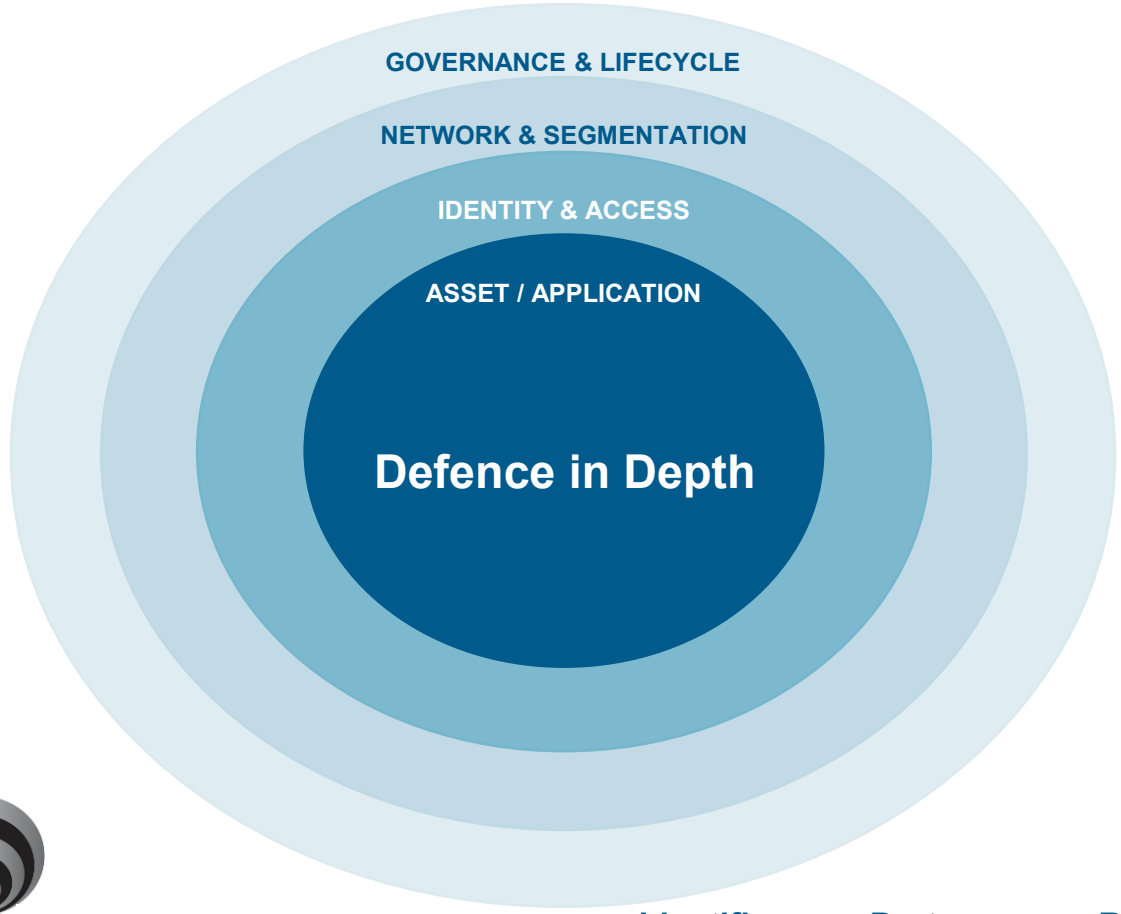
3. AI APPLICATA — Anomaly detection, assistenza, ottimizzazione

4. AZIONE GOVERNATA — Decisione umana o automazione controllata

AI utile = problema chiaro + dato contestualizzato + governance

SECURE | Cybersecurity by design, non come add-on

La resilienza richiede protezione multilivello, segmentazione e gestione continua.





Identificare • Proteggere • Rilevare • Rispondere • Ripristinare

DUE CASI D’USO | Dal dato all’azione

Due esempi di convergenza tra interoperabilità, AI all’edge e cybersecurity.



01 CONDITION MONITORING

Rilevare comportamenti anomali prima che diventino un fermo

Dati macchina › Contesto asset › AI / anomaly › Intervento

Obiettivo: manutenzione più tempestiva e maggiore disponibilità

02 QUALITY INSPECTION

Individuare difetti vicino alla linea e governare la risposta

Immagine › AI all’edge › Esito contestuale › Scarto / verifica

Obiettivo: controllo più rapido e decisione tracciabile

Interoperabilità per accedere ai dati. AI per interpretarli. Cybersecurity per rendere affidabile l’azione.

QUALITY INSPECTION | Esempio applicativo



CONNECTED + INTELLIGENT + SECURE

Una roadmap pragmatica per trasformare tecnologia in risultati operativi.

CONNETTI

Parti dal caso d’uso

CONTESTUALIZZA

Definisci asset e modelli

APPLICA AI

Misura e governa

PROTEGGI

Security dall’architettura

SCALA

Replica su linee e siti

La nuova frontiera è un’architettura aperta, intelligente e resiliente.

Dalla macchina all’enterprise, con valore misurabile e sicurezza integrata.