

Adaptive Automation

Il paradigma SENECA di Automazione human-centric, interoperabile e sicura



Ideazione del paradigma: Manuel Moschin

Coordinamento: Armando Martin

Marzo 2026

Indice

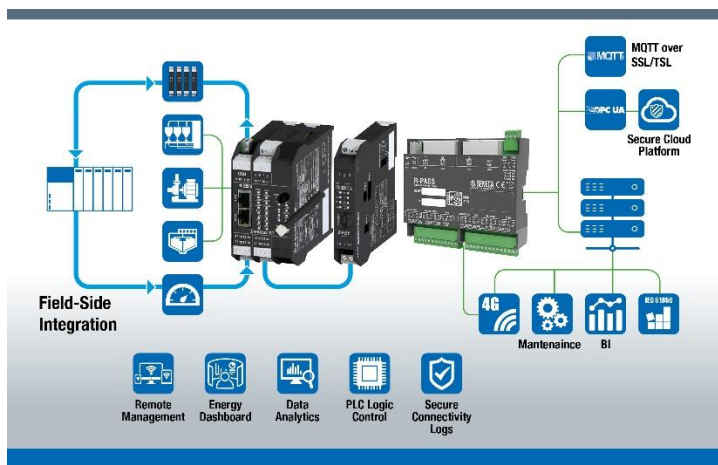
- 1. Introduzione**
- 2. Architettura del paradigma Adaptive Automation**
- 3. Pilastro 1. FLEX**
- 4. Pilastro 2. Firmware Unificato**
- 5. Pilastro 3. Sicurezza Distribuita**
- 6. Pilastro 4. EASY CLOUD**
- 7. Impatto industriale e benefici**
- 8. Glossario**
- 9. Bibliografia e Risorse**

1. Introduzione -Dalla complessità alla Adaptive Automation

Negli ultimi anni l'automazione industriale ha conosciuto una profonda trasformazione. Digitalizzazione, IoT, teleassistenza, energy management, cybersecurity e Intelligenza Artificiale hanno progressivamente stratificato le architetture di impianto. Il risultato è una crescente complessità: protocolli eterogenei, gateway dedicati, PLC separati, edge computer autonomi, sistemi cloud sovrapposti. Storicamente, ogni nuova esigenza ha generato un nuovo dispositivo. Serviva connettività? Si aggiungeva un gateway. Serviva accesso remoto? Un router VPN. Serviva registrazione dati? Un data logger. L'innovazione è stata prevalentemente additiva. Questo approccio ha prodotto impianti più sofisticati, ma anche più rigidi, più costosi da integrare e mantenere, più esposti a vulnerabilità cyber.

La trasformazione digitale, nata per semplificare, ha spesso aumentato la complessità sistemica. In questo scenario si inserisce il paradigma **Adaptive Automation**, sviluppato da **SENECA**, azienda italiana che da quasi quarant'anni progetta e realizza componenti e sistemi per l'automazione industriale. Il paradigma nasce all'interno del contesto tecnologico del **Made in Italy industriale**, storicamente caratterizzato da una forte integrazione tra progettazione elettronica, applicazioni di campo e capacità di adattamento alle esigenze reali degli impianti produttivi. Adaptive Automation non è un'ulteriore tecnologia, ma un cambio di prospettiva. L'obiettivo non è aggiungere funzioni, bensì ridurre la complessità strutturale dell'automazione attraverso quattro pilastri integrati: **FLEX, Firmware Unificato, Sicurezza Distribuita ed EASY CLOUD**. Il principio guida è chiaro: l'automazione deve essere configurabile, non sostituibile. Adaptive Automation integra in un unico nodo industriale funzioni tradizionalmente distribuite: controllo programmabile secondo IEC 61131-3, conversione multiprotocollo, data logging, HMI/Display Remoto, web server integrato, connettività IoT e mobile integrate, VPN industriale e gestione sicura delle comunicazioni. Non si tratta di una convergenza generica, ma di un'integrazione progettata per il campo, con segmentazione delle reti, cifratura dei dati e conformità ai principali standard di sicurezza (IEC 62443-4-2).

L'intelligenza viene collocata **close-to-the-field**, vicino alla macchina o al quadro elettrico. Questo riduce la latenza, aumenta la resilienza e consente di mantenere il controllo anche in assenza di connettività esterna. Il nodo edge diventa un elemento attivo dell'impianto, capace di eseguire logiche, registrare eventi, generare allarmi e dialogare con sistemi superiori in modo autonomo. Accanto alla dimensione tecnica, vi è una dimensione organizzativa. Adaptive Automation è un modello **human-centric**: la tecnologia non deve moltiplicare i punti di configurazione, ma semplificarli. Quando cambia il contesto operativo, si interviene sulla configurazione software, non sull'hardware. Si evolve il sistema senza ricostruirlo. Ridurre dispositivi, interfacce e livelli sovrapposti significa ridurre cablaggi, firmware, superfici di attacco e costi totali di proprietà. In un contesto in cui cybersecurity, continuità operativa e conformità normativa sono fattori strategici, la semplificazione architetturale diventa un vantaggio competitivo. Adaptive Automation non è un prodotto, ma un modello progettuale: un'automazione modulare, configurabile, sicura e architetturealmente evolutiva, capace di adattarsi all'impianto senza imporre continue sostituzioni tecnologiche.



Architettura IIoT con nodi adattativi SENECA Edge che concentra funzionalità PLC, Energy Controller, IIoT Gateway, Router 4G, unità di teleallarme, teleassistenza, datalogger

2. Architettura del paradigma Adaptive Automation

Adaptive Automation non è un prodotto ma un modello tecnico strutturato su quattro pilastri integrati: FLEX, Firmware Unificato, Sicurezza Distribuita e EASY CLOUD. È questa architettura coordinata a trasformare il dispositivo industriale da componente statico a nodo adattivo della rete.

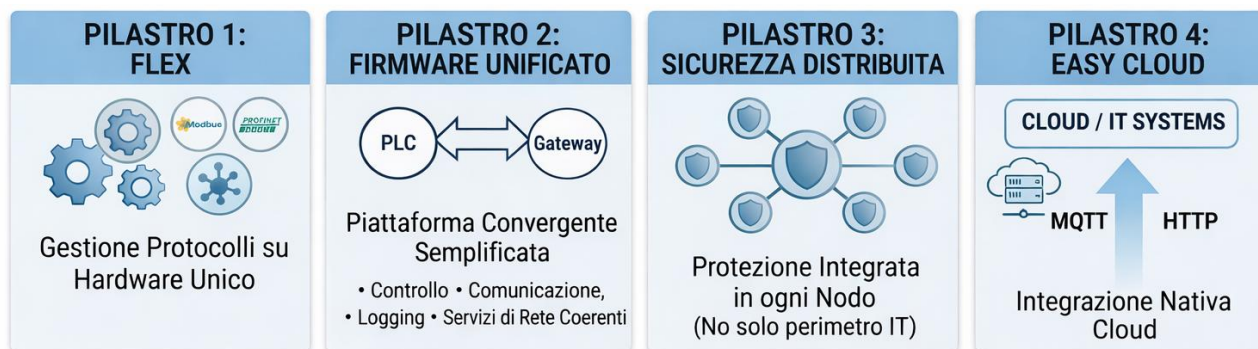
Il primo elemento è **FLEX**, ovvero la gestione e conversione dinamica dei protocolli di comunicazione su un unico hardware. Il principio è “configura, non sostituire”: lo stesso dispositivo può operare come gateway, analizzatore di rete o modulo I/O multiprotocollo, semplicemente variando configurazione. L’hardware resta invariato, cambia il ruolo funzionale.

Il secondo pilastro è il **Firmware Unificato**, piattaforma convergente PLC/Gateway/Edge che consente di semplificare aggiornamenti, modificare configurazioni in tempo reale e ridurre i costi di gestione. Controllo, comunicazione, logging e servizi di rete convivono in un ambiente coerente, con web server integrato, gestione centralizzata dei parametri e diagnostica locale. Non si sommano dispositivi: si evolve la piattaforma.

Il terzo pilastro è la **Sicurezza Distribuita**. La protezione non è concentrata nel perimetro IT, ma integrata in ogni nodo dell’architettura. Segmentazione LAN/WAN, VPN industriale, autenticazione avanzata, cifratura SSL/TLS e riferimenti a standard come IEC 62443 e NIS2 rendono la sicurezza una proprietà strutturale del sistema. Ogni dispositivo contribuisce attivamente alla resilienza complessiva, riducendo il rischio di propagazione laterale delle minacce.

Il quarto pilastro è **EASY CLOUD**. La connessione bidirezionale con i principali ambienti cloud è resa semplice da template di integrazione preconfigurati, basati soprattutto su MQTT, che consentono di adattare rapidamente il dispositivo alla piattaforma scelta. Il principio operativo è che il template collega il nodo edge a diversi cloud e, tramite configurazione o programmazione avanzata, la macchina si adatta al servizio selezionato senza gateway o middleware dedicati, rendendo l’automazione evolutiva e facilmente riconfigurabile.

In questo paradigma il dispositivo industriale non è più un elemento passivo, ma un nodo intelligente capace di adattarsi al contesto applicativo. L’innovazione non consiste nell’aggiungere funzioni, bensì nel coordinarle in una piattaforma unificata, configurabile, sicura ed evolutiva, riducendo complessità, superfici di attacco e costi complessivi di sistema.

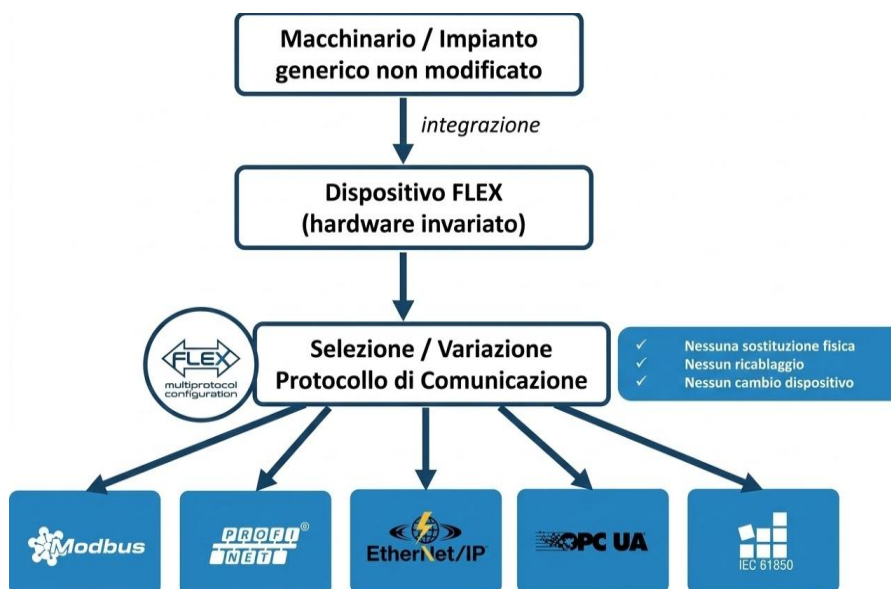


I pilastri dell'Adaptive Automation

4. Pilastro 1. FLEX

Il cuore adattivo del paradigma è la tecnologia proprietaria FLEX. FLEX rappresenta la soluzione sviluppata da SENECA per disaccoppiare in modo definitivo la funzione di comunicazione industriale dall'hardware fisico del dispositivo. Nei sistemi tradizionali ogni protocollo richiede un gateway dedicato, con conseguente moltiplicazione di varianti, firmware e componenti. Con FLEX questo schema viene superato: un unico hardware multiprotocollo gestisce in tempo reale Modbus RTU/TCP/ASCII, Profinet IO, Ethernet/IP, OPC UA, IEC 61850 e MQTT, senza sostituzione fisica del dispositivo.

Piattaforme come Z-KEY, R-KEY, R203, R204, modulo I/O integrano stack di comunicazione eterogenei su base hardware comune. FLEX agisce come livello di orchestrazione logica sopra questi stack, consentendo di selezionare via software il ruolo operativo del nodo: gateway Modbus RTU↔TCP, endpoint OPC UA, bridge Ethernet/IP, nodo Profinet, concentratore IEC 61850 o publisher MQTT verso piattaforme IIoT con logica locale (regole if then else). Il principio non è solo la coesistenza di più protocolli, ma la loro intercambiabilità senza impatto fisico sull'impianto. Il dispositivo mantiene la stessa base hardware mentre cambia il ruolo logico in funzione dell'architettura richiesta dal capitolato o dall'evoluzione del sistema. Questo elimina uno dei principali fattori di costo dell'automazione: il cambio architettura. Non è più necessario sostituire apparati quando si passa da uno standard di comunicazione a un altro; è sufficiente una riconfigurazione software tramite Web Server o ambiente di programmazione.



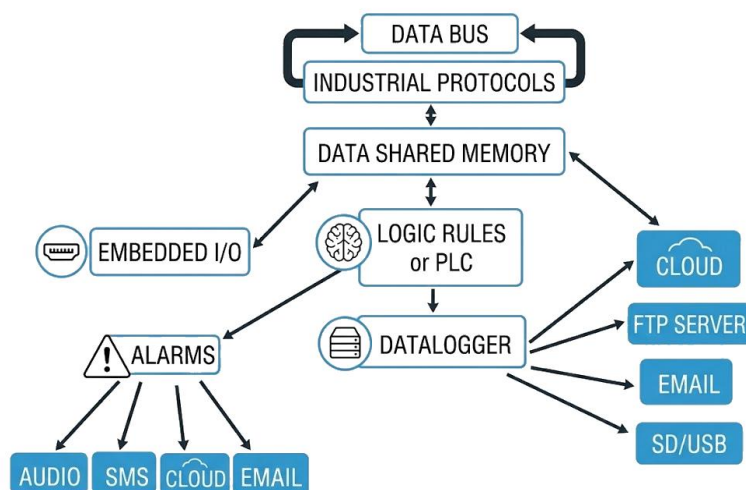
FLEX: selezione del protocollo di comunicazione senza modifiche hardware, ricablaggi o sostituzioni del dispositivo.

L'impatto tecnico è significativo. FLEX abilita retrofit di impianti esistenti senza riprogettazione completa, facilita l'adattamento a capitolati differenti tra clienti o mercati, consente la standardizzazione del magazzino riducendo il numero di codici da gestire, diminuisce il downtime legato a sostituzioni fisiche e rende possibile una migrazione progressiva verso architetture IIoT senza strappi tecnologici. La comunicazione industriale diventa una funzione adattiva e non un vincolo strutturale.

Inoltre, l'approccio non si limita alla conversione di protocollo. Edge e cloud sono integrati nativamente. I dispositivi supportano multi-cloud industriale, MQTT bidirezionale, configurazioni remote sicure via VPN e HTTPS. Il dato acquisito dai bus o dagli I/O non viene soltanto raccolto e inoltrato, ma contestualizzato direttamente in campo grazie alla shared memory e alle logiche locali. Può essere elaborato, filtrato, correlato e poi pubblicato verso sistemi superiori già arricchito di significato operativo. FLEX trasforma così il gateway da oggetto statico a piattaforma dinamica, coerente con l'Adaptive Automation: un'infrastruttura capace di evolvere nel tempo mantenendo stabile l'hardware e adattando via software la propria identità comunicativa.

4. Pilastro 2. Firmware Unificato.

Nel paradigma Adaptive Automation la convergenza delle funzioni non nasce da una semplice integrazione di prodotti eterogenei, ma da una precisa architettura software interna, fondata su memoria dati condivisa e servizi applicativi cooperanti. Nei dispositivi SENECA di ultima generazione – come le famiglie Z-PASS-RT, Z-TWS4-RT, R-PASS e Smart Display – i dati provenienti dai bus industriali (ModBUS RTU/TCP, CAN), dalle reti Ethernet LAN/WAN o dagli I/O integrati confluiscono in un'unica shared memory centrale. Questa memoria costituisce il modello informativo comune su cui operano simultaneamente logiche PLC IEC 61131-3 (Straton), funzioni di gateway multiprotocollo, servizi di datalogging, regole locali If-Then-Else, gestione allarmi, comunicazione MQTT/OPC UA verso cloud e piattaforme IIoT, oltre ai servizi VPN di teleassistenza e telecontrollo. Il principio chiave è la simultaneità operativa: controllo, acquisizione, analisi e trasmissione non sono più funzioni sequenziali affidate a dispositivi distinti, ma processi paralleli che insistono sullo stesso dato operativo. Un valore letto da un ingresso analogico o ricevuto via ModBUS può essere utilizzato nello stesso istante da una logica PLC, registrato su memoria flash o micro-SD, pubblicato via MQTT su broker remoto, esposto via OPC UA e reso disponibile su Web Server integrato, senza duplicazioni né conversioni intermedie. L'efficienza deriva proprio dall'unità del dato.

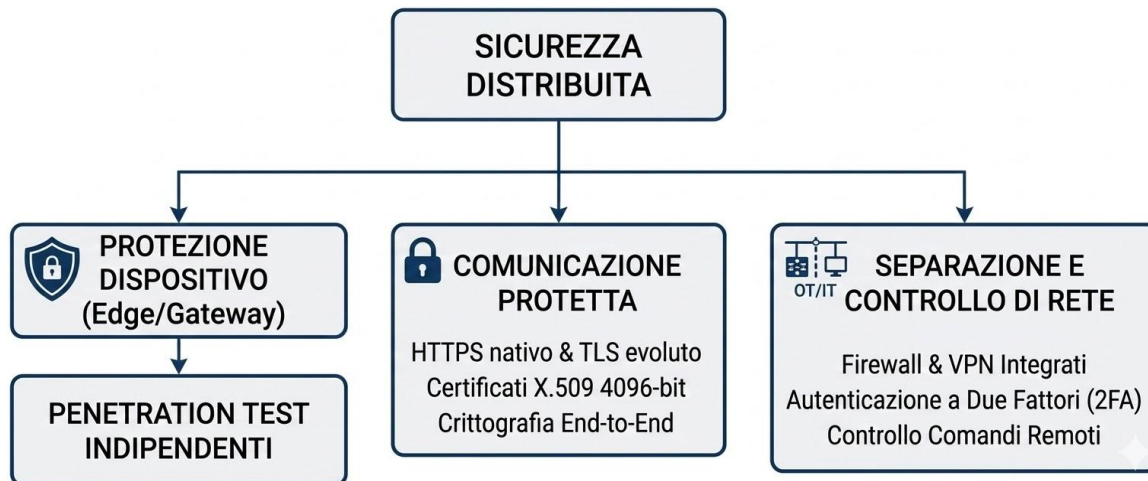


Architettura firmware unificata: comunicazione, logica, datalogging e gestione allarmi integrati in un'unica piattaforma.

Tradizionalmente l'architettura di impianto prevedeva ruoli ben separati: il PLC controllava, il gateway convertiva, il datalogger registrava, l'edge computer elaborava e il router garantiva la connettività remota. Nel modello Adaptive Automation queste funzioni non sono più vincolate all'hardware ma al firmware condiviso. La piattaforma unificata SENECA, comune alle famiglie RT, SSD e R-PASS, consente allo stesso dispositivo di operare come softPLC, gateway multiprotocollo, router LAN/WAN o 4G LTE con VPN, datalogger evoluto, concentratore IIoT o unità di teleallarme. Il comportamento è determinato dalla configurazione software e non dalla sostituzione fisica del prodotto. La sicurezza non è un modulo aggiuntivo ma un layer nativo della piattaforma poiché il dispositivo è sviluppato secondo i principi IEC 42443-4-2. I benefici ingegneristici sono rilevanti. La riduzione delle varianti hardware semplifica la progettazione e la gestione delle scorte; la continuità tecnologica garantisce coerenza lungo il ciclo di vita dell'impianto; l'aggiornamento firmware abilita nuove funzioni senza sostituire il dispositivo; la manutenzione si concentra su un'unica piattaforma software; l'interoperabilità tra dispositivi è intrinseca, perché condividono lo stesso modello dati e gli stessi strumenti di configurazione (Web Server, ambienti IEC 61131-3, tool di discovery e gestione). In questa prospettiva l'automazione non è più un insieme di apparati distinti collegati tra loro, ma una piattaforma software distribuita su nodi intelligenti, ciascuno capace di adattare dinamicamente il proprio ruolo operativo. Adaptive Automation significa esattamente questo: trasformare il dispositivo industriale da componente statico a nodo adattivo, in grado di evolvere con l'impianto, con le esigenze applicative e con l'ecosistema digitale di riferimento.

5. Pilastro 3. Sicurezza Distribuita

Nel paradigma Adaptive Automation la cybersecurity non è un layer aggiuntivo né una funzione delegata esclusivamente al perimetro IT: è un requisito architetturale intrinseco al dispositivo. L'approccio adottato è coerente con i principi di Security by Design e Security by Default, in cui protezione hardware, firmware e comunicazioni sono integrate fin dalla progettazione, in linea con i riferimenti tecnici della IEC 62443 e con il quadro normativo europeo NIS2 e Cyber Resilience Act.



Sicurezza distribuita: protezione del dispositivo, comunicazioni cifrate e controllo sicuro della rete OT/IT.

I dispositivi Edge IIoT e i gateway industriali implementano autenticazione avanzata con gestione dei privilegi, protezione contro attacchi brute force e controllo granulare degli accessi per operatori, manutentori e sistemi di teleassistenza.

La comunicazione è protetta tramite HTTPS nativo, TLS evoluto e certificati X.509 fino a 4096 bit, garantendo crittografia end-to-end dei dati in transito e protezione delle credenziali.

Il firmware è firmato digitalmente per impedirne la modifica non autorizzata, riducendo il rischio di compromissioni persistenti del dispositivo.

Accanto ai meccanismi software sono previste protezioni hardware degli accessi, il controllo dei comandi remoti e la separazione strutturale tra ambienti LAN/WAN e tra domini OT e IT, con integrazione di firewall, VPN e autenticazione a due fattori. I dati sensibili sono conservati in partizioni criptate del dispositivo. Questa segmentazione riduce drasticamente la superficie di attacco e limita l'esposizione dei sistemi di campo verso reti esterne. I dispositivi sono inoltre sottoposti a penetration test indipendenti secondo metodologie riconosciute (CWE, OWASP, CVSS, IEC 62443-4-2), con esiti integrati nel processo di miglioramento continuo.

Il modello adottato è quello di sicurezza distribuita. Invece di concentrare la protezione nel firewall perimetrale o nel data center, ogni nodo è progettato per essere intrinsecamente sicuro. Logging locale avanzato, monitoraggio degli eventi (audit log forensici) e gestione controllata degli aggiornamenti consentono di mantenere resilienza operativa anche in contesti remoti o con connettività limitata.

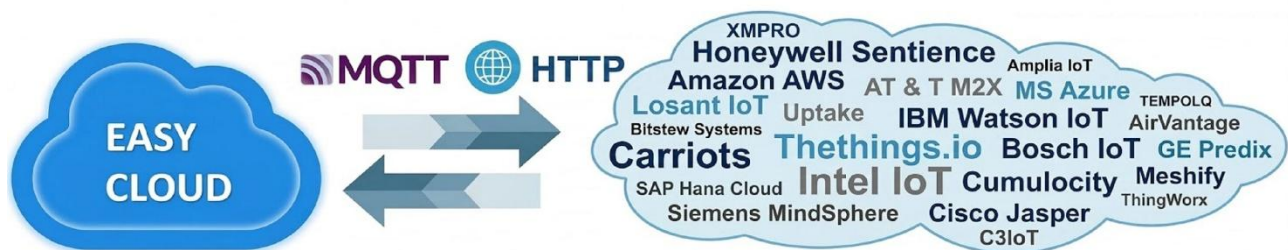
Gli aggiornamenti firmware avvengono tramite meccanismi sicuri e pianificabili, evitando impatti sulla continuità di servizio. Questo approccio riduce uno dei rischi tipici degli impianti industriali: la propagazione laterale dell'attacco. Se un nodo viene compromesso, la segmentazione e i controlli locali impediscono la diffusione automatica verso altri dispositivi OT. La sicurezza non è quindi solo centralizzata (ad esempio tramite server syslog), ma replicata e radicata in ogni elemento dell'architettura.

Nel paradigma Adaptive Automation la sicurezza diventa quindi una proprietà strutturale del sistema: non un costo accessorio, ma una condizione abilitante per resilienza, continuità operativa e conformità regolatoria lungo l'intero ciclo di vita dell'automazione.

6. Pilastro 4. EASY CLOUD.

Il quarto pilastro dell'Adaptive Automation integra connettività, modularità e sviluppo applicativo in un unico principio: l'automazione deve poter evolvere nel tempo senza essere riprogettata. Questo approccio si concretizza nell'integrazione nativa tra Edge e Cloud, nella flessibilità operativa dei dispositivi e in un modello di ingegneria orientato alle esigenze reali di campo.

La connettività è abilitata dalla tecnologia Easy Cloud, che consente una connessione bidirezionale immediata verso i principali servizi cloud tramite template di integrazione preconfigurati, basati principalmente su MQTT e HTTP. Il nodo edge dialoga direttamente con i sistemi superiori senza richiedere architetture intermedie complesse o gateway aggiuntivi. I dispositivi integrano Web Server nativo, aggiornamento remoto e funzioni di configurazione via interfaccia web, permettendo la gestione distribuita dell'infrastruttura. Nei modelli dotati di connettività mobile sono disponibili modem 4G, gestione VPN e diagnostica di rete integrata, garantendo continuità operativa anche in siti remoti o non presidiati. Sono inoltre disponibili connettori e template pronti per l'integrazione con diverse piattaforme cloud.



Easy Cloud: integrazione semplice con piattaforme IoT tramite protocolli standard come MQTT e HTTP.

La flessibilità operativa non riguarda solo la comunicazione ma l'intero ciclo di vita dell'impianto. Dispositivi come gateway, RTU e HMI integrano funzioni di logging, PLC, VPN e I/O su piattaforme compatte. Questo approccio riduce componenti separati, cablaggi e punti di guasto, semplificando retrofit, ampliamenti e adattamenti a capitolati differenti, con benefici anche in termini di consumi ed efficienza energetica. La modularità hardware consente inoltre l'aggiunta di moduli opzionali o varianti funzionali senza sostituire l'architettura di base, favorendo la standardizzazione di magazzino e manutenzione.

Il dato non viene solo raccolto e inviato al cloud: viene prima contestualizzato in campo. L'elaborazione locale su processori ARM con memoria dedicata consente l'esecuzione di logiche, script, normalizzazione dei segnali e gestione degli allarmi direttamente a livello edge. Questo approccio riduce latenza, traffico dati e dipendenza dalla connettività continua, mantenendo autonomia decisionale sul campo.

Grazie a Easy Cloud, la connessione con i principali ambienti cloud è semplificata da template di integrazione che permettono di adattare rapidamente il dispositivo alla piattaforma scelta. Il principio operativo è che il template collega il nodo edge a diversi cloud e, attraverso configurazione o programmazione avanzata, la macchina si adatta al servizio selezionato senza richiedere gateway o middleware dedicati.

In questo modo Easy Cloud, modularità e ingegneria di campo convergono in un unico concetto: evoluzione operativa continua, dal sensore al cloud, senza fratture architetturali e senza sostituzioni disruptive.

7. Impatto Industriale e benefici

L'impatto industriale dell'Adaptive Automation non si misura soltanto in termini di funzionalità introdotte, ma nella trasformazione strutturale del modo in cui un impianto viene concepito, gestito e fatto evolvere nel tempo e nei relativi benefici.

- 1) **Riduzione della complessità.** Meno dispositivi significano meno configurazioni, meno varianti hardware, meno punti di errore, minore energia consumata. La concentrazione di più funzioni in un'unica piattaforma adattiva riduce la frammentazione architettuale tipica degli impianti tradizionali, semplifica la documentazione tecnica e diminuisce il rischio di incompatibilità tra componenti. La complessità non viene spostata altrove: viene assorbita dall'architettura.
- 2) **Estensione del ciclo di vita dell'impianto.** In un modello statico, il cambio di protocollo o di sistema supervisore comporta spesso la sostituzione fisica dei gateway o dei dispositivi di interfaccia. Nel paradigma adattivo, invece, l'hardware non diventa obsoleto al mutare del requisito: evolve tramite configurazione. Questo disaccoppiamento tra funzione logica e componente fisico preserva l'investimento iniziale e riduce il costo totale di proprietà.
- 3) **Resilienza operativa.** L'architettura resta funzionante anche quando l'infrastruttura IT si evolve, quando vengono introdotti nuovi standard o quando cambia il sistema di raccolta dati. L'impianto non subisce interruzioni strutturali: si adatta progressivamente. La continuità non è garantita da sovradimensionamento, ma da flessibilità intrinseca.
- 4) **Cybersecurity.** Il modello supera la logica esclusivamente perimetrale. La protezione non è concentrata in un unico punto di frontiera, ma distribuita sui nodi. Ogni dispositivo diventa parte attiva della difesa, riducendo il rischio di propagazione laterale degli attacchi. La sicurezza non è un'aggiunta esterna, ma una proprietà strutturale del sistema.
- 5) **Sostenibilità tecnica.** Meno sostituzioni significano meno rifiuti elettronici, meno logistica, meno interventi invasivi. La possibilità di aggiornare e riconfigurare senza smantellare contribuisce a un modello industriale più coerente con i principi di durabilità e responsabilità tecnologica.

Questo insieme di effetti definisce il passaggio dal paradigma tradizionale a quello adattivo. L'automazione industriale classica è statica: quando cambia il requisito, si cambia il dispositivo. L'automazione adattiva è dinamica: quando cambia il requisito, si cambia la configurazione. È un ribaltamento concettuale che introduce un nuovo livello architettuale: dal dispositivo programmabile al sistema adattivo.

Adaptive Automation non rappresenta quindi una semplice evoluzione funzionale, ma un cambiamento nel rapporto tra hardware, software, rete e operatore. L'impianto non è più una struttura rigida da sostituire nel tempo, ma una piattaforma evolutiva configurabile. L'innovazione non è soltanto tecnologica: è architettuale. Questo approccio riflette una tradizione ingegneristica tipica del Made in Italy industriale, in cui l'innovazione nasce dalla capacità di integrare elettronica, software e applicazioni di campo. In questo contesto SENECA, costruttore italiano di componenti e sistemi per l'automazione da quasi quarant'anni, ha sviluppato il paradigma Adaptive Automation come sintesi di questa esperienza applicativa.

L'automazione smette di imporre vincoli al processo e diventa essa stessa capace di adattarsi al processo. Ed è proprio questa inversione di prospettiva a costituire il valore tecnico distintivo dell'Adaptive Automation.

Glossario

Adaptive Automation

Modello architetturale SENECA basato su configurabilità, interoperabilità, sicurezza strutturale ed evoluzione dell'impianto senza sostituzioni hardware.

Close-to-the-Field Engineering

Approccio progettuale basato su esigenze reali di campo, sviluppo incrementale e verticalizzazioni applicative.

Configurabilità vs Sostituzione

Principio guida del paradigma: quando cambia il requisito si modifica la configurazione software, non il dispositivo.

Cyber Resilience Act (CRA)

Regolamento europeo che introduce requisiti obbligatori di cybersecurity per prodotti digitali connessi.

CWE (Common Weakness Enumeration)

Catalogo standardizzato delle vulnerabilità software utilizzato nei processi di analisi sicurezza.

CVSS (Common Vulnerability Scoring System)

Sistema di classificazione e punteggio delle vulnerabilità informatiche.

EASY CLOUD

Tecnologia che consente ai dispositivi edge di collegarsi direttamente a piattaforme cloud tramite template MQTT/HTTP preconfigurati, senza gateway intermedi.

Edge Computing Industriale

Elaborazione locale dei dati sul nodo di campo prima dell'invio verso sistemi cloud o supervisor.

Firmware Unificato

Piattaforma software convergente che integra PLC, gateway, logging, VPN e servizi IIoT su memoria condivisa.

FLEX

Tecnologia proprietaria che consente la gestione dinamica e intercambiabile dei protocolli industriali su un unico hardware.

Human-Centric Automation

Modello che semplifica configurazione e gestione, riducendo complessità tecnica e punti di intervento.

IEC 61131-3

Standard internazionale per la programmazione dei PLC.

IEC 62443

Standard internazionale per la sicurezza dei sistemi di automazione e controllo industriale.

Multi-protocollo

Capacità di gestire protocolli eterogenei (Modbus, Profinet, Ethernet/IP, OPC UA, IEC 61850, MQTT) su un'unica piattaforma.

NIS2

Direttiva europea sulla resilienza cyber delle infrastrutture critiche e dei soggetti essenziali.

Nodo Industriale Adattivo

Dispositivo edge capace di modificare il proprio ruolo operativo tramite configurazione software.

OWASP (Open Web Application Security Project)

Framework e linee guida per test e sicurezza applicativa.

Penetration Test

Test indipendenti di vulnerabilità condotti secondo metodologie strutturate.

Retrofit Evolutivo

Aggiornamento funzionale di impianti esistenti senza sostituzione massiva dei dispositivi.

Security by Default

Configurazione di sicurezza attiva per impostazione predefinita.

Security by Design

Integrazione della sicurezza fin dalle fasi di progettazione hardware e firmware.

Segmentazione OT/IT

Separazione strutturale tra rete operativa industriale (OT) e rete informatica aziendale (IT).

Shared Memory

Memoria dati centralizzata su cui operano simultaneamente PLC, gateway, logging e servizi cloud.

Sicurezza Distribuita

Modello in cui ogni nodo dell'architettura è intrinsecamente protetto, riducendo la dipendenza dal solo perimetro IT.

Bibliografia e Risorse

Documentazione tecnica prodotti

- Dispositivi Edge IIoT multifunzione: https://www.seneca.it/media/6849299/0099_seneca_edge_iiot-it-2025_it.pdf
- Industrial IoT Edge Devices (R-PASS): https://www.seneca.it/media/4151/0224-seneca_r-pass_it.pdf
- HMI Gateway PLC multifunzione (SSD): https://www.seneca.it/media/6848723/feb_25iiot-edge-hmi-multifunzione-it.pdf
- Manuale Utente Dispositivi Edge IIoT <https://www.seneca.it/media/6849479/mi00557-26-it.pdf>
- R-PASS – IIoT Edge Controllers https://www.seneca.it/media/6849366/flyer_r-pass-s-en-2210-ps.pdf
- Gateway Edge IIoT con supporto VPN https://www.seneca.it/media/6849714/flyer_zpass1-rt_23070it.pdf
- Gateway Edge IIoT / Router 4G con supporto VPN https://www.seneca.it/media/6849718/flyer_zpass2_rt_2307_it.pdf
- Controllore Edge IIoT 4G https://www.seneca.it/media/6849724/flyer_z-pass2-rt-s_2307it.pdf

Normative e Standard Tecnici

- IEC 62443 – Industrial Communication Networks – IT Security for Networks and Systems
- IEC 61131-3 – PLC Programming Languages
- Direttiva NIS2 (UE 2022/2555)
- Cyber Resilience Act (Regolamento UE 2024)
- NIST SP 800-115 – Technical Guide to Information Security Testing
- OWASP Testing Guide
- CVSS – Common Vulnerability Scoring System
- CWE – Common Weakness Enumeration

Riferimenti Web istituzionali

- <https://www.seneca.it>
- <https://www.iec.ch>
- <https://www.enisa.europa.eu>
- <https://digital-strategy.ec.europa.eu>
- <https://owasp.org>
- <https://nvd.nist.gov>



SENECA s.r.l.

Via Austria, 26 - 35127 Padova

Tel. +39 049 8705359

Web: www.seneca.it

Email: info@seneca.it