

FORUM
INDUSTRIA
DIGITALE

MECCATRONICA
E SOFTWARE
PER L'INDUSTRIA

GEFRAN
BEYOND TECHNOLOGY

Il Cloud Non Basta. Il Ruolo di Edge Device e Controllori

Gefran S.p.A.
Giuseppe Cardovino

Promosso da



FORUMECCATRONICA

forum
Software
Industriale



ANIE
AUTOMAZIONE

In collaborazione con



Organizzato da

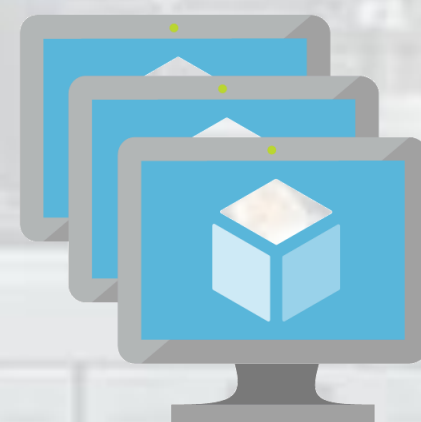
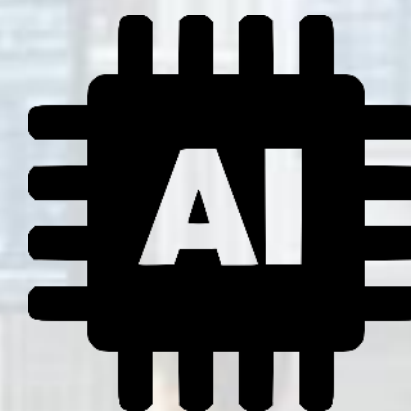


messe frankfurt

Interconnessioni e non solo

Le piattaforme di automazione di una macchina non gestiscono più il solo processo di produzione, ma diventano sistemi sempre più complessi da integrare al lavoro dell'operatore.

- Cybersecurity
- Intelligenza artificiale
- Personalizzazione
- Interoperabilità dei sistemi
- Virtualizzazione



Semplificare le interfacce, rendere il sistema Cyberfisico fruibile e utile anche all'operatore meno esperto, ma quanto tutto ciò impatta nella realizzazione di una macchina automatica?

Macchine connesse ad un mondo in evoluzione

Una macchina automatica, di serie o customizzata alle esigenze del cliente, per cosa viene valutata? Ovviamente per l'efficacia per lavoro che è chiamata a svolgere ma, è un dato di fatto, anche per le funzionalità aggiuntive di comunicazione con l'azienda e l'operatore

- La raccolta dei dati di produzione per i processi aziendali grazie ai protocolli standard di comunicazione è da tempo un concetto consolidato
- L'uso di device HMI in ambiente grafico in alternativa a comandi tradizionali quali pulsanti e tastiere, altrettanto.

Tutto bene quindi?



Un mondo in evoluzione ma meno sicuro

Le notizie di cyber attacchi, di presa in ostaggio dei dati sensibili o dell'intera capacità produttiva di aziende ovunque nel mondo non sono più eventi saltuari.

- Nel primo semestre del 2024, al mondo, si sono verificati in media 273 attacchi hacker rilevanti al mese, con il 5% di questi rivolti al settore manifatturiero (più di 3 a settimana).
Un terzo di tutti gli incidenti globali ha colpito l'Europa.
(Rapporto Clusit 2024 – Edizione di metà anno, ottobre 2024)
- Il Regolamento Macchine 2023/1230, in vigore dal 29 giugno 2023, mette l'accento sull'importanza della vulnerabilità dei controllori a salvaguardia della sicurezza e della continuità produttiva
- A partire dal 2027 il Cyber Resilience Act (CRA) imporrà i requisiti di cyber sicurezza per commercializzare prodotti HW/SW nell'EU



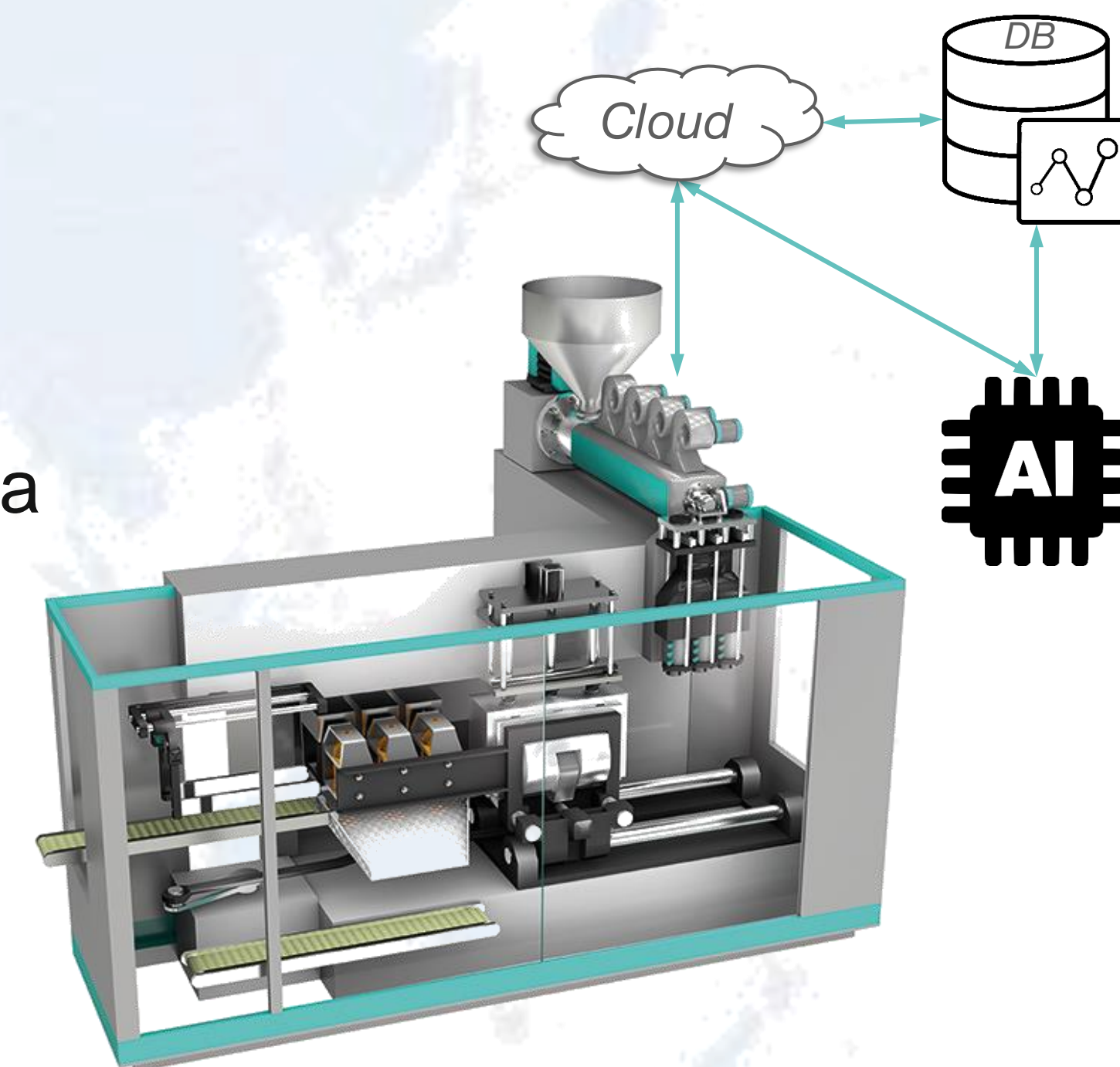
Semplificare la complessità dei sistemi di sicurezza limitando le vulnerabilità rappresenta un fattore chiave

Un mondo in evoluzione ma sempre più di corsa

Ridurre il downtime aumenta la produttività e, quanto rapidamente le funzioni di analisi dei dati e di diagnostica possano registrare e fornire indicazioni, diventa basilare

- L'analisi istantanea dei dati al momento in cui si verificano i problemi migliora la tempestività delle risposte operative
- Trasferire importanti volumi di dati è oneroso e deve essere minimizzato significativamente trasferendo solo i risultati dell'analisi locale
- L'interazione continua con strumenti di analisi evoluti, che sfruttino l'Intelligenza Artificiale, ottimizza le capacità diagnostiche e la capacità predittiva

Semplificare le ottimizzazioni significa aumentare la produttività



Un mondo in evoluzione ma che invecchia e perde competenze

La popolazione nelle economie avanzate, inclusa quella lavorativa, sta invecchiando e perdendo esperienze preziose. Tuttavia, il ricambio generazionale e la globalizzazione introducono nuove forze lavoro, abili con i dispositivi digitali ma da seguire attentamente perché ancora prive dell'esperienza necessaria.

- Gli operatori di macchine dei prossimi anni potrebbero affrontare problematiche che non riescono a risolvere a causa dell'inesperienza e della distanza da chi possa supportarli
- Questi automaticamente, cercheranno sostegno negli strumenti a loro già congeniali e che quotidianamente già usano, come smartphone o tablet

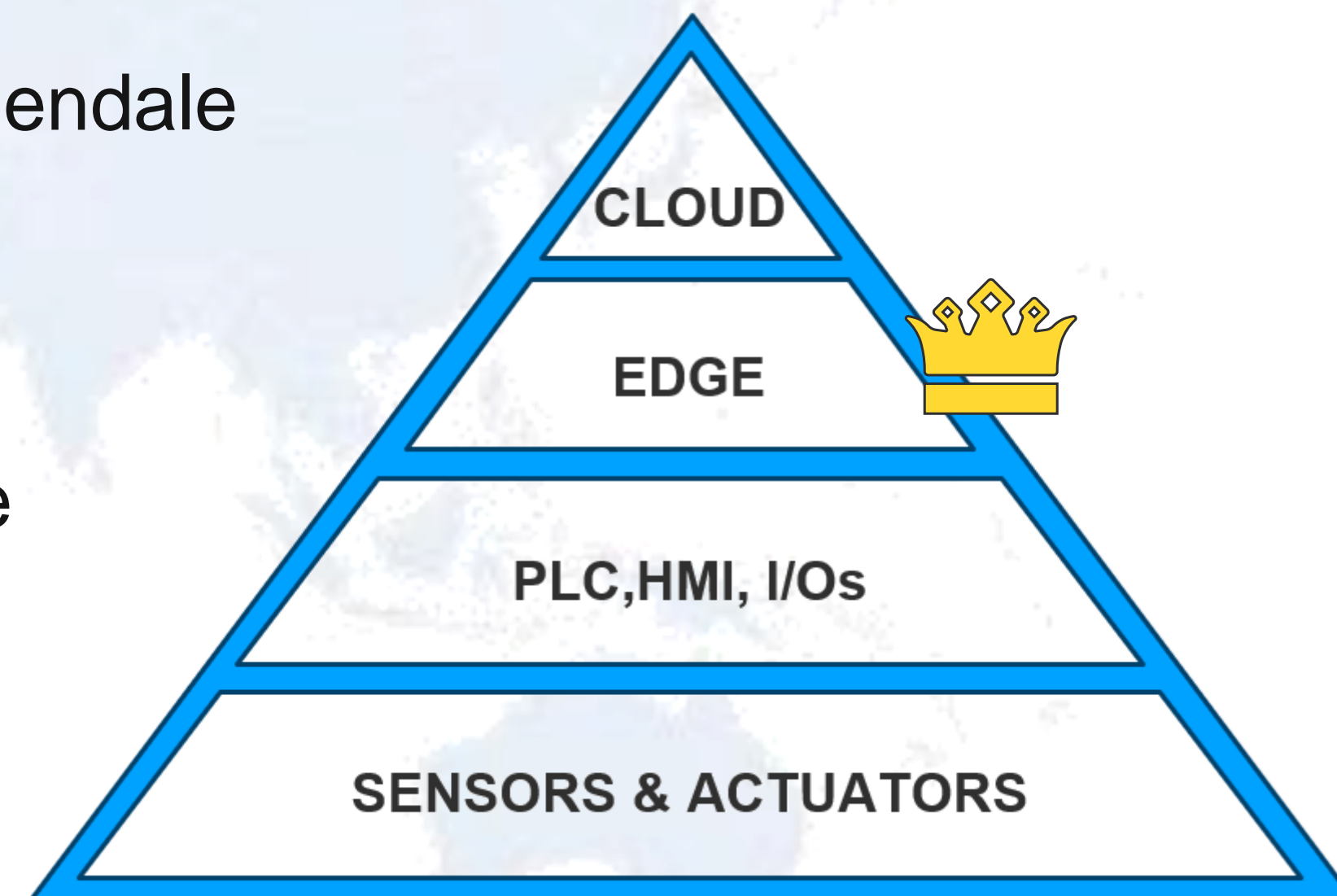


Semplificare la complessità dell'operatività degli operatori meno esperti rappresenta un fattore chiave

Come seguire questa evoluzione?

Affrontare le sfide delle piattaforme di automazione, specialmente quelle tradizionalmente gestite da PLC per la loro semplicità, implica garantire sicurezza, facilità di utilizzo personalizzabile dagli operatori, e apertura all'integrazione con avanzate soluzioni di Intelligenza Artificiale.

- Limitare gli accessi vulnerabili e al contempo garantire la connettività aziendale
- Utilizzo di software di diagnostica efficaci ma di facile integrazione
- Fornire tool intuitivi per agevolare gli utenti meno esperti
- Personalizzazione delle interfacce di comunicazione
- Agevolare questi ed altri plug-in assicurandosi che il sistema resti stabile

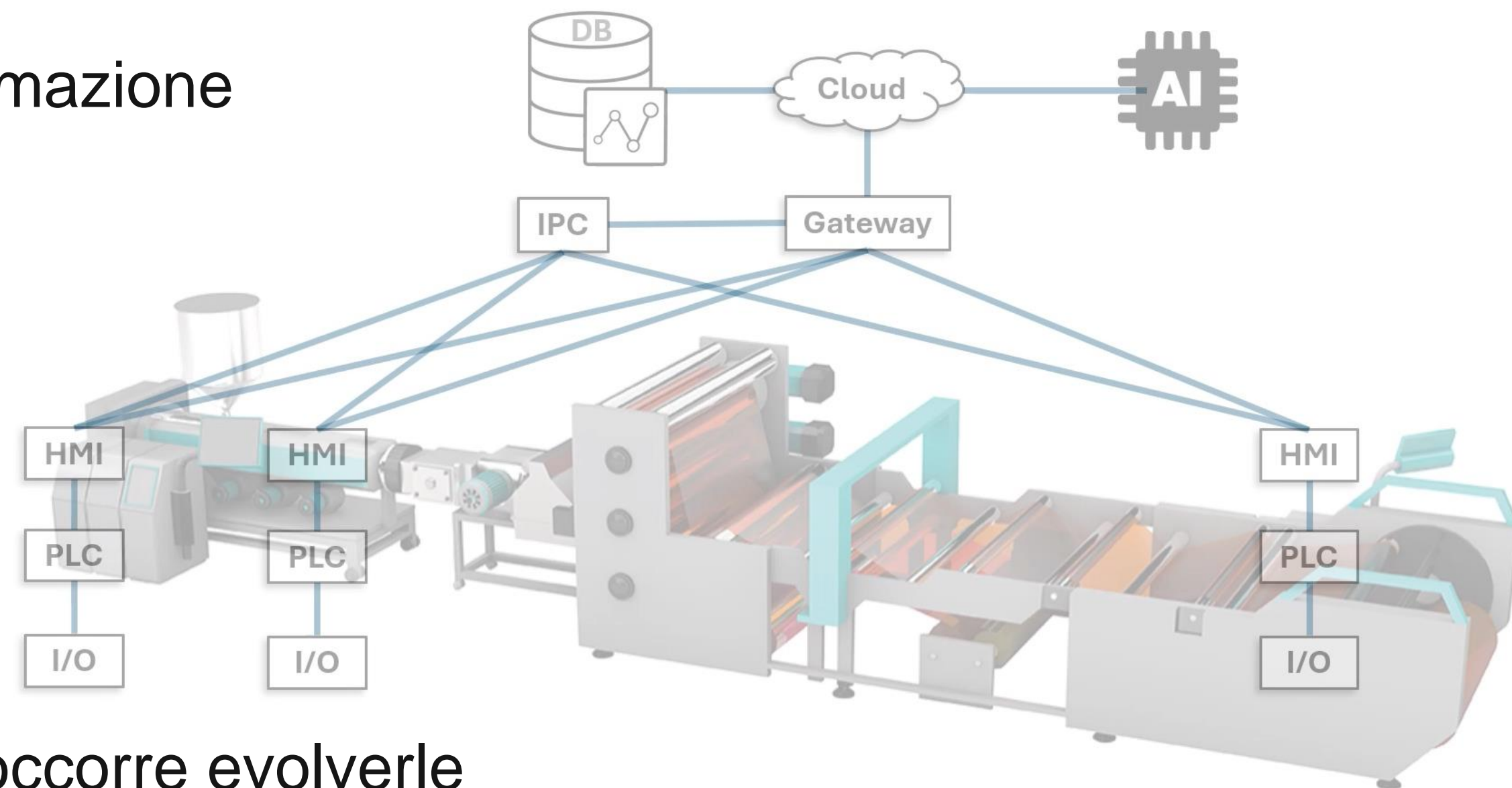


Molte delle risposte a questi quesiti possono trovare soluzione nell'Edge Computing

Edge Computing, obiettivo raggiunto

L'Edge computing permette di realizzare piattaforme ad alte prestazioni, mantenendo al contempo la semplicità tipica di un PLC, soprattutto nei sistemi meno complessi. Un'infrastruttura pensata cyber-resiliente, comunica con più dispositivi e virtualizza interfacce e personalizzazioni in un unico ambiente.

- PLC potenti e aperti con risorse riservate al processo di automazione
- Strumenti di interconnessione integrati (IOT, Gateway, VPN)
- Piattaforme che rispettino le direttive di sicurezza
- Dati di analisi elaborati a ridosso dell'applicazione per monitoraggio e intervento in tempo reale
- Visualizzazione flessibile su qualsiasi device
- Implementazioni di app tramite architetture Dockers o Snap



Adattarsi ai cambiamenti adattando le tecnologie non basta, occorre evolverle

FORUM INDUSTRIA
DIGITALE

MECCATRONICA
E SOFTWARE
PER L'INDUSTRIA

GRAZIE PER L'ATTENZIONE

Promosso da



FORUMECCATRONICA

forum
Software
Industriale



ANIE
AUTOMAZIONE

In collaborazione con



Organizzato da



messe frankfurt

La proposta di Gefran

La nuova piattaforma G-Mation di Gefran è la nostra idea di soluzione per questi quesiti

- CPU INTEL ATOM quad-core fino a 1,9 GHz con core dedicato al processo
- Interfaccia operatore HTML con Web Server integrato
- Comunicazione EtherCAT nativa
- Programmazione PLC standard IEC611331-3
- Compatibile per applicazioni Dockers
- Espandibile con moduli I/O
- Cybersecurity embedded



Simplifying Complexity

