



# **IA, Cybersecurity nell'era di Industry 4.0: Affrontare le Sfide del Futuro**

## ***AI Applicata alla Smart Factory***

***Ing. Serena Proietti***

*Phd candidate Università di Roma Tor Vergata, Next Gen-AI  
commission E.N.I.A*

*Ordine degli Ingegneri della Provincia di Roma*

*Roma, 18 giugno 2025*



# Introduzione



Se esistesse un rapporto tra quanto si parla di Industry 4.0 e quanto effettivamente si applica, il risultato sarebbe deludente.



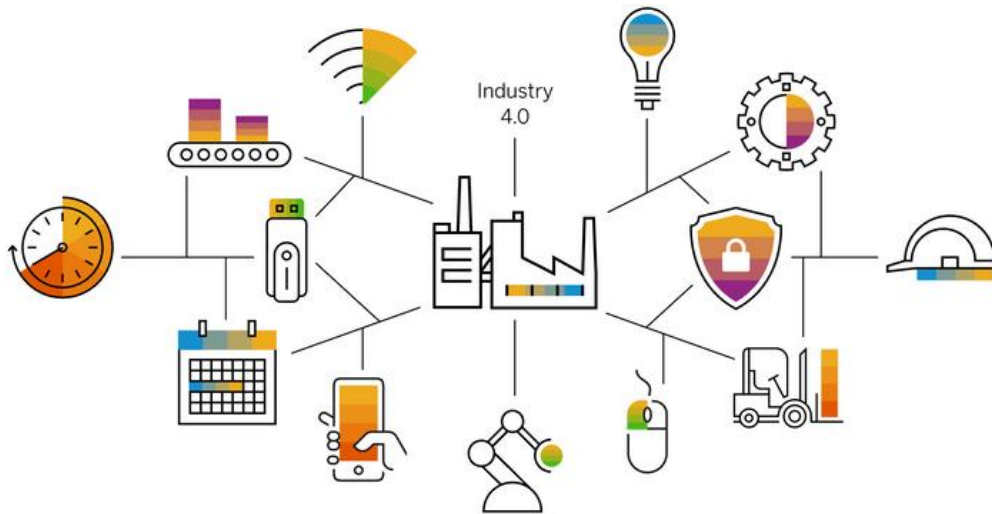
Non perché le aziende non ottengano risultati, ma perché nella maggior parte dei casi sono ben lontane dalla visione ingegneristica della fabbrica completamente automatizzata.

Una delle cause plausibili di questa scarsa adozione è la **confusione** tra i manager su cosa sia davvero Industry 4.0 e quale impatto possa avere sui risultati aziendali.

# Industry 4.0

L'Industry 4.0 può essere definita come l'**integrazione delle tecnologie digitali intelligenti** nei processi produttivi e industriali.

Comprende una serie di tecnologie che includono **reti IoT industriali, AI, Big Data, robotica e automazione.**



L'Industry 4.0 consente la produzione intelligente e la creazione di fabbriche intelligenti.

L'Industry 4.0 ha reinventato il modo in cui le aziende progettano, producono e distribuiscono i loro prodotti.



# Industry 4.0

Alcune delle tecnologie al centro di Industry 4.0:



IoT



Cloud



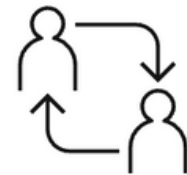
AI e apprendimento  
autonomo



Edge  
Computing



Cybersecurity



Digital  
Twin

Le aziende e le supply chain utilizzano già alcune di queste tecnologie avanzate, ma il **pieno potenziale** dell'Industry 4.0 prende vita quando queste tecnologie vengono utilizzate insieme.



# Industry 4.0

## Internet Of Things

La maggior parte degli aspetti fisici dell'Industry 4.0 (dispositivi, robot, macchinari, apparecchiature, prodotti) utilizza sensori e tag RFID per fornire dati in tempo reale sulle loro condizioni, prestazioni o posizione.

## Cloud Computing

La piena realizzazione della produzione intelligente richiede connettività e integrazione di ingegneria, supply chain, produzione, vendita, distribuzione e assistenza. Il cloud rende tutto questo possibile e consente di elaborare in modo più efficiente ed economico grandi quantità di dati.

## AI e Machine Learning

Aiutano a prevedere e automatizzare operazioni e processi aziendali. Ad esempio, le macchine industriali sono soggette a guasti durante il processo di produzione. L'utilizzo dei dati raccolti da questi asset può aiutare le aziende a eseguire la manutenzione predittiva basata su algoritmi di apprendimento automatico.



# Industry 4.0

## Edge computing

Nella produzione, alcune analisi devono avvenire localmente per garantire risposta immediata. L'edge computing riduce la latenza, evita dipendenze dal cloud e migliora sicurezza e reattività su problemi critici come qualità o sicurezza.

## Cybersecurity

Le aziende manifatturiere non hanno sempre considerato l'importanza della cybersecurity o dei sistemi cyber-fisici. Tuttavia, la stessa connettività delle apparecchiature operative in fabbrica o sul campo (OT), che consente processi di produzione più efficienti, espone anche nuove vie d'accesso ad attacchi dannosi e malware.

## Digital Twin

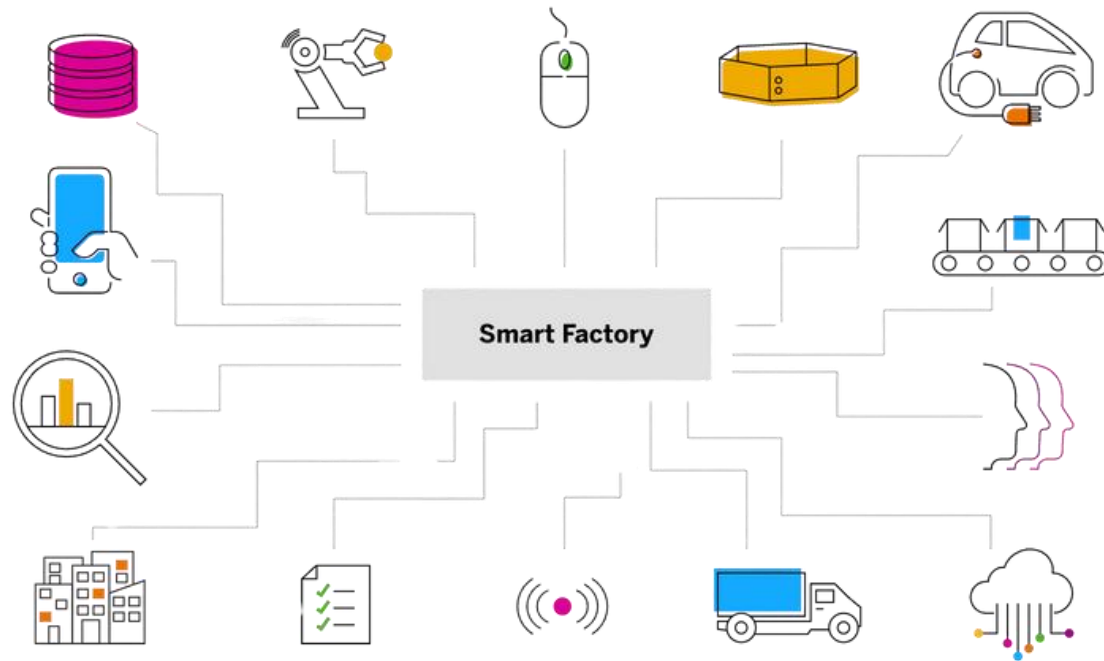
I gemelli digitali sono repliche virtuali di processi, linee di produzione, fabbriche e supply chain. Un gemello digitale viene creato estraendo dati da sensori, dispositivi, PLC e altri oggetti IoT connessi a internet. Simulando un processo di produzione, ad esempio, i produttori possono testare le modifiche al processo per trovare modi per ridurre al minimo i tempi di inattività o migliorare la capacità.



# Smart Factory

Si parla spesso di processi automatizzati come se fossero prerogativa unica della smart factory, quando di fatto l'automazione e la robotica sono in uso da decenni nelle attività produttive.

**Ma in una fabbrica tradizionale questi dispositivi non sono interconnessi!**





# Smart Factory

## Fabbrica Tradizionale

*Automazione frammentata*

- Tecnologie in uso da decenni: robot, scanner, fotocamere
- Sistemi e persone non interconnessi
- Richiede intervento manuale per coordinare impianti e dati

## Fabbrica Intelligente

*Ecosistema connesso e intelligente*

- Integrazione tra macchine, persone e Big Data
- I sistemi apprendono dai dati (machine learning)
- Prevedono eventi, ottimizzano processi e si autocorreggono
- Evolvono in modo continuo verso produttività e sicurezza

**La fabbrica digitale intelligente funziona integrando macchine, persone e Big Data in un unico ecosistema connesso in rete.**

# Smart Factory



## 1) Acquisizione dati:

Le tecnologie consentono la raccolta di dati eterogenei. Attraverso sensori e gateway, l'IoT permette alle macchine connesse di far confluire dati nel sistema.

## 2) Analisi dati:

il machine learning e i sistemi aziendali intelligenti sfruttano l'analisi avanzata e le moderne soluzioni di gestione dei dati per dare un senso a tutti i dati disparati raccolti.

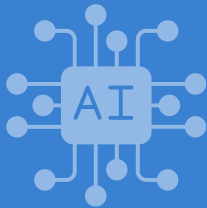
## 3) Automazione della fabbrica intelligente:

una volta compiute l'acquisizione e l'analisi dei dati, vengono stabiliti i flussi di lavoro e inviate istruzioni alle macchine e ai dispositivi all'interno del sistema.



# Tra ambizione e realtà

Oggi l'industria manifatturiera è sempre più alimentata dall'informazione. Vaste quantità di dati provengono da tutto il business e in tutto il mondo, in tempo reale, tutto il giorno.



L'AI è al centro della quarta rivoluzione industriale, consentendo alle aziende manifatturiere di raccogliere non solo tutti i dati, ma anche di utilizzarli per analizzare, prevedere e comprendere.

**BUT..**

La fattibilità tecnica non implica però automaticamente benefici di business.

Le aziende che hanno tentato trasformazioni radicali spesso hanno fatto marcia indietro.



Il risultato: **isole di alta tecnologia in mezzo a sistemi ancora tradizionali.**



# Industry 5.0



Integra l'attuale approccio "Industry 4.0" mettendo specificamente la ricerca e l'innovazione al servizio della transizione verso un'industria europea **sostenibile, incentrata sull'uomo e resiliente.**

## Come realizzarla?

- Adottare un approccio incentrato sull'uomo per le tecnologie digitali, inclusa l'Intelligenza Artificiale.
- Aggiornamento e riqualificazione dei lavoratori europei, in particolare delle competenze digitali
- Promuovendo industrie moderne, efficienti sotto il profilo delle risorse e sostenibili e transizione verso un'economia circolare
- Accelerando gli investimenti in ricerca e innovazione



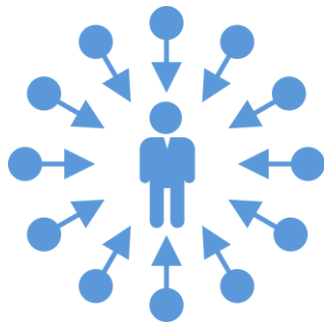
# Human-in-the-Loop

Le aziende cercano di testare nuove tecnologie, ma spesso si rendono conto di un fattore cruciale: il ruolo degli esseri umani.

I lavoratori coinvolti nei processi produttivi, spesso dotati di conoscenza tacita, non accolgono l'automazione con lo stesso entusiasmo.



**Progetti abbandonati al primo confronto con la realtà del lavoro umano.**



Progettare soluzioni che mantengano l'essere umano al centro, secondo il principio human-in-the-loop, è essenziale per garantire non solo l'efficacia tecnica, ma anche il rispetto dei **valori umani e sociali**.



# Cybersecurity

Oltre alla progettazione di soluzioni che tengano conto del fattore umano, c'è un altro aspetto da tenere in considerazione: la **sicurezza**.

La crescente connettività e l'adozione di tecnologie **digitali aumentano la superficie d'attacco**.

Infatti, l'iperconnessione delle **Smart Factory** crea una superficie di attacco molto ampia per i cybercriminali.

Gli attacchi possono riguardare:

- ❖ la compromissione di macchinari
- ❖ la manipolazione dei processi produttivi
- ❖ la fuga di dati sensibili e la interruzione delle attività.



**La cybersecurity non è solo protezione del dato, ma difesa della continuità operativa.**



# Cybersecurity

L'**AI Act** introduce una classificazione del rischio per i sistemi di AI e molte applicazioni in ambito industriale potranno ricadere in categorie **high-risk**.

L'articolo 15 richiede che i sistemi AI ad alto rischio garantiscano tra le altre cose:

*“adeguati livelli di cybersecurity per resistere a tentativi di manipolazione”, inclusi attacchi che mirano a influenzare il comportamento del sistema.*

Esempio:

Un chatbot **integrato nel sistema di interfaccia uomo-macchina** che fornisce comandi, suggerimenti operativi in tempo reale, o istruzioni che influenzano **comportamenti critici** (es. avviare procedure pericolose, configurare parametri di sicurezza), potrebbe rientrare nei sistemi ad alto rischio?





# Cybersecurity



Se da un lato l'iperconnettività della fabbrica intelligente ha ampliato la superficie di attacco e i rischi per la cybersecurity



dall'altro tecnologie emergenti come l'AI generativa possono diventare un potente alleato per rafforzare la resilienza dei sistemi industriali.

I team di sicurezza informatica possono sfruttare l'IA generativa per creare **attacchi altamente realistici** (es. phishing, social engineering, malware simulato) con cui testare l'efficacia dei processi difensivi e la preparazione del personale.

Questo approccio consente di **identificare e correggere vulnerabilità prima che vengano sfruttate da attaccanti reali**.

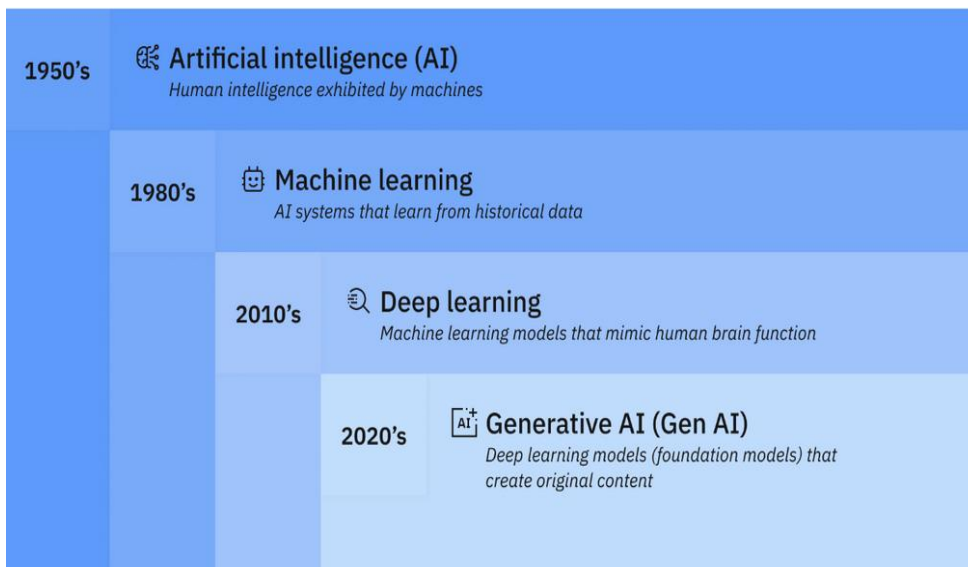
Inoltre, l'IA generativa può essere utilizzata per **simulare ambienti operativi complessi e scenari di attacco realistici**, permettendo di testare a fondo i sistemi di sicurezza aziendali e rafforzarne le difese.



# Intelligenza artificiale

Se da un lato dobbiamo proteggere un ecosistema digitale sempre più complesso, dall'altro abbiamo l'opportunità di renderlo più **intelligente** e **proattivo**.

L'**Intelligenza Artificiale**, insieme a tecnologie come IoT, Blockchain, e Digital Twin etc., è oggi una delle leve principali per il **ripensamento dei processi industriali**.



## Cos'è l'AI?

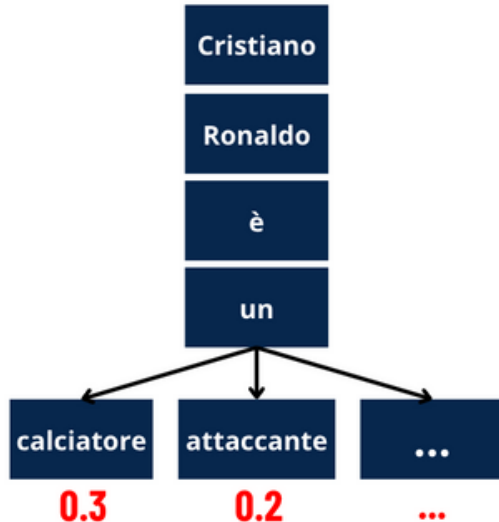
L'intelligenza artificiale (AI) è una tecnologia che consente ai computer e alle macchine di simulare l'apprendimento umano, la comprensione e la risoluzione dei problemi.



# Intelligenza artificiale Generativa

L'AI generativa, talvolta chiamata “**gen AI**”, si riferisce a modelli di deep learning in grado di creare contenuti originali complessi, come testi, immagini, video o audio.

I Modelli Generativi sono quindi algoritmi che, data una serie di esempi, imparano a generare nuovi dati simili agli esempi osservati.



Un modello generativo come ChatGPT non fa altro che prevedere quale parola seguente è la più probabile.



## LEGAME CON LA PROBABILITA'

I modelli generativi utilizzano la **probabilità** per generare dati in base alla distribuzione osservata.



# Retrieval Augmented Generation

Un'opzione per migliorare le prestazioni di un'applicazione di gen AI è la **Retrieval Augmented Generation (RAG)**, una tecnica che consente di estendere il foundation model all'utilizzo di fonti pertinenti al di fuori dei dati di addestramento per una maggiore precisione o pertinenza.

La **Retrieval-Augmented Generation (RAG)** è quindi un sistema che aiuta a dare risposte migliori e più pertinenti.

Come?

**1. Retrieval** (Ricerca): L'IA cerca informazioni rilevanti in un database o una fonte di conoscenza esterna.



**2. Generation** (Generazione): Utilizza i dati trovati durante la ricerca per generare risposte più accurate.





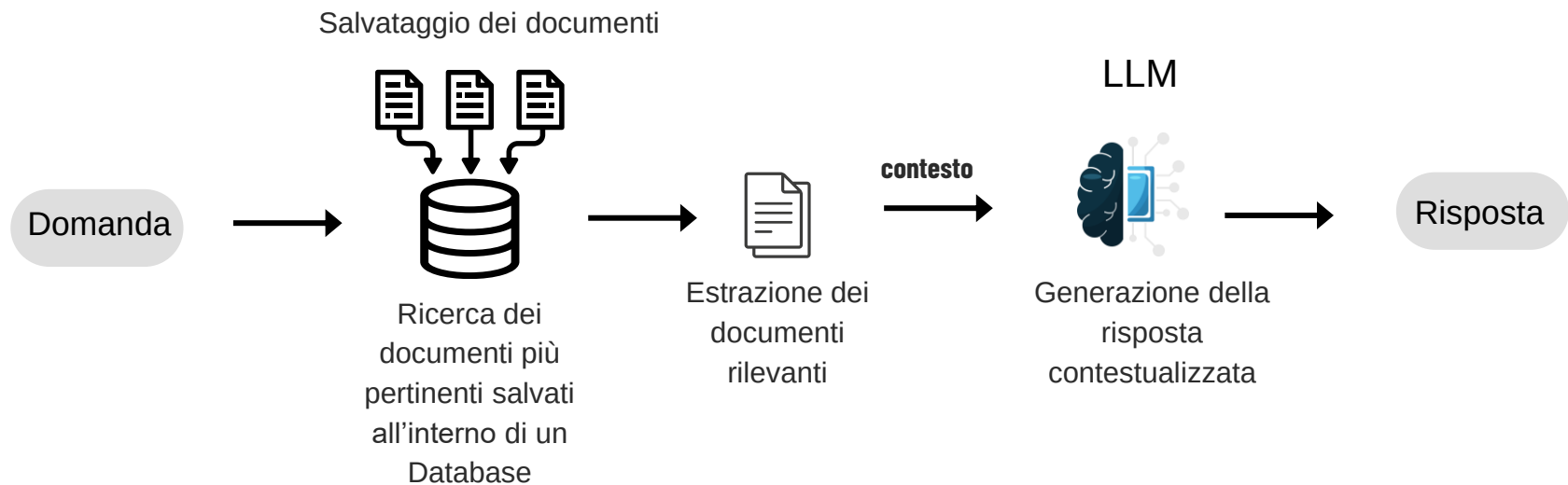
# Retrieval Augmented Generation



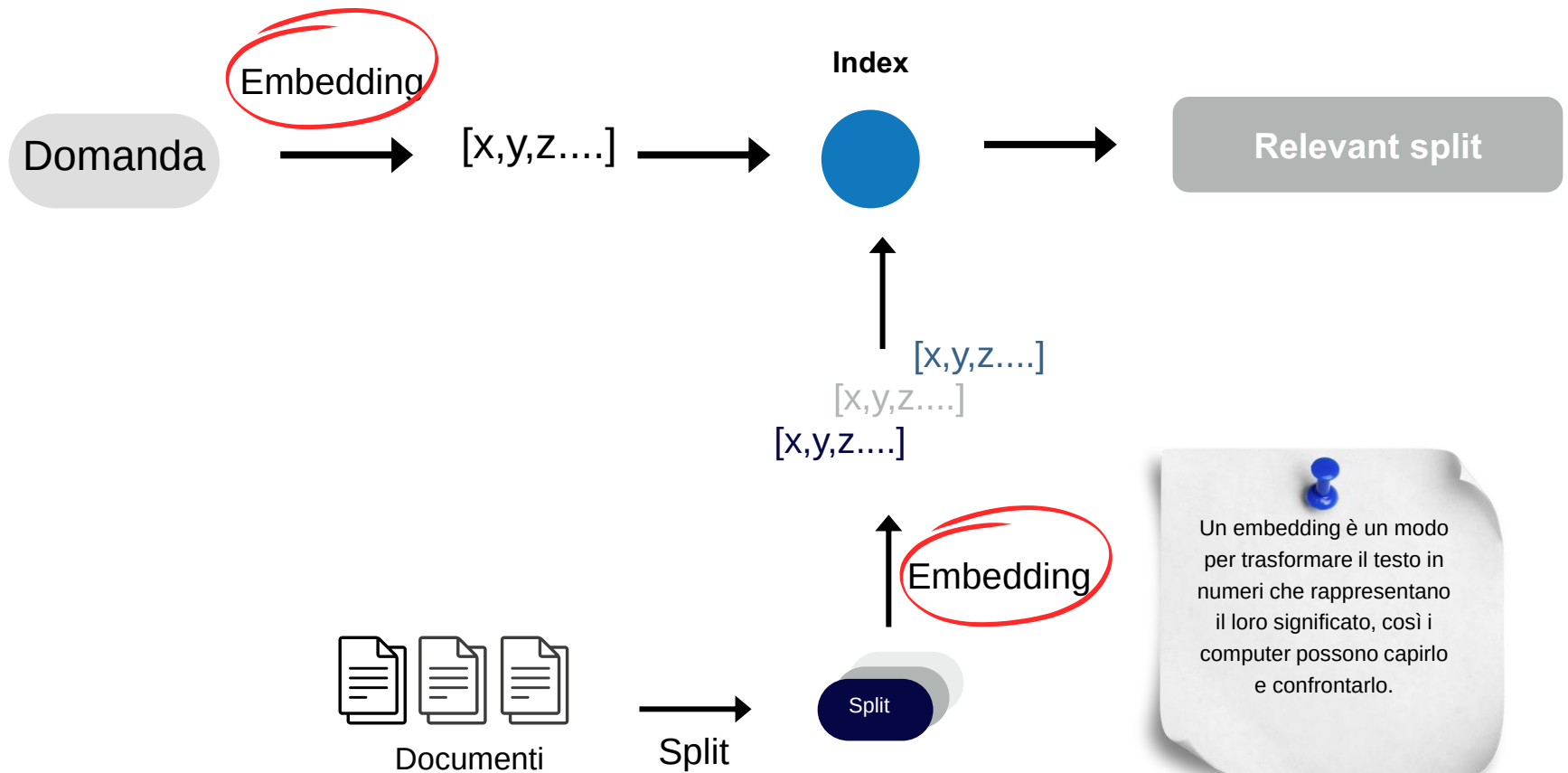
**Risposta tradizionale (AI senza RAG):** L'IA usa solo ciò che sa dal suo addestramento.



**Risposta con RAG:** L'IA cerca informazioni aggiornate per dare risposte migliori.



# Retrieval Augmented Generation





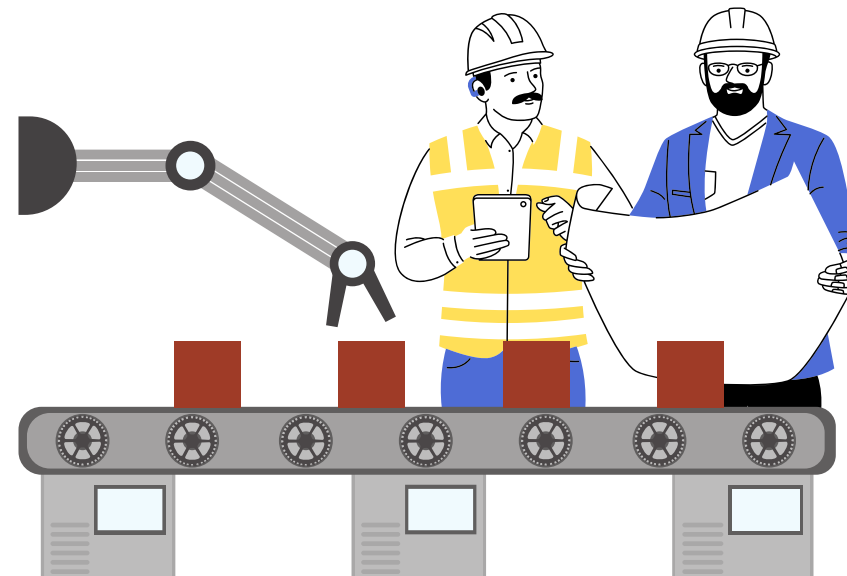
# Perchè la GenAI in fabbrica?

Gli operatori di linea si trovano spesso a dover:

- Consultare manuali tecnici complessi durante l'attività operativa, rallentando l'intervento.
- Gestire **anomalie** senza istruzioni immediate e contestuali
- Lavorare in ambienti dove un errore operativo può avere impatti sulla **sicurezza personale** e sul processo produttivo
- Dipendere da **documentazione dispersa**



Tempi di fermo più lunghi  
Conoscenza tecnica poco accessibile  
Riduzione della sicurezza operativa



# Assistente all'operatore di linea

Un assistente intelligente che:

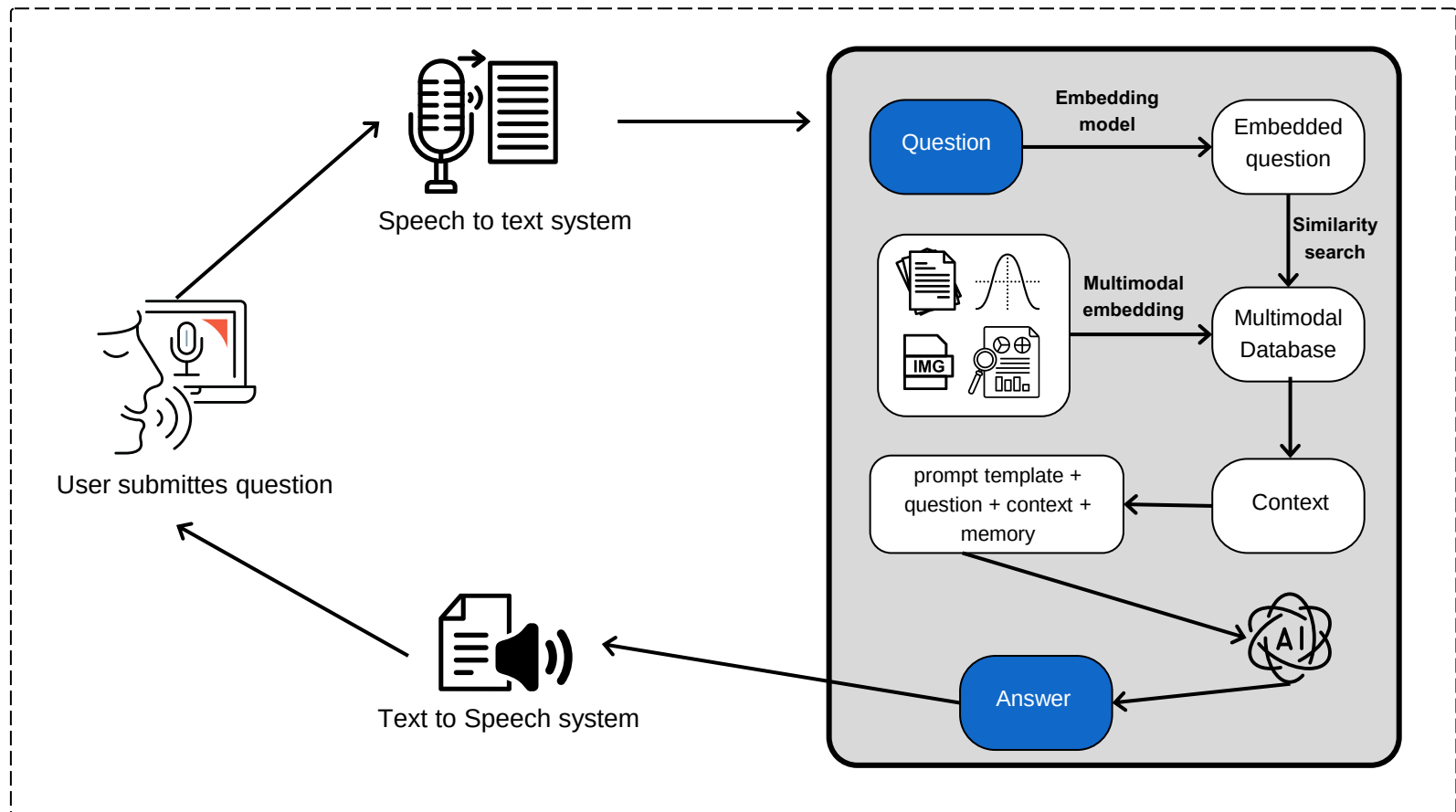
- Risponde in tempo reale a domande su manuali, procedure, parametri e anomalie.
- Comprende il linguaggio naturale, anche tecnico  
Accede alla documentazione aziendale (PDF, database, note operative).
- Si integra con la linea per fornire risposte contestuali.
- Aumenta la sicurezza riducendo gli errori legati a interpretazioni sbagliate.
- Supporta l'autonomia e la formazione continua dell'operatore.





# Assistente all'operatore di linea

È davvero possibile realizzare tutto questo?





# Integrazione tra AI predittiva e assistenza operativa





# Sfide nell'uso dell'AI in campo industriale

- Limiti tecnici nell'ingestion di documentazione complessa (tipica del settore industriale);
- In ambito HSE, manutenzione o controllo qualità, un errore della GenAI può causare **danni fisici, economici o ambientali!**
- L'addestramento o l'uso della GenAI su dati aziendali solleva domande su **riservatezza, proprietà intellettuale e consenso;**
- Attenzione al controllo del **bias nei dati** (es. manutenzione trascurata in certi impianti o operatori meno esperti penalizzati).



# Conclusioni

Come ingegneri abbiamo un ruolo fondamentale in questa evoluzione: non solo progettare tecnologie avanzate, ma contribuire a costruire soluzioni che siano efficaci, sicure e soprattutto **antropocentriche**.

- **Integrare le tecnologie, non solo installarle**  
Le tecnologie hanno senso solo quando dialogano fra loro, con i processi e l'organizzazione aziendale.
- **Progettare con approccio human-in-the-loop**  
Le soluzioni devono valorizzare il contributo umano e rispettare i principi etici e sociali.
- **Garantire la sicurezza come requisito abilitante**  
La cybersecurity non è opzionale: è un pilastro fondamentale nella realizzazione di tali sistemi.



# GRAZIE PER L'ATTENZIONE

 **Serena Proietti**  
 [serena.proietti@uniroma2.it](mailto:serena.proietti@uniroma2.it)