

Capire e governare l'IA: strumenti, LLM e Agenti per l'ingegnere

ing Roberto Magnani

Ente Nazionale per l'intelligenza Artificiale ENIA® - Technical & Scientific Committee
Consigliere Ordine Ingegneri prov. di Lecco



Contenuto dei webinar 13 -21 ottobre

	INTERVENTO 1	INTERVENTO 2
Titolo	Capire e governare l'IA: strumenti, LLM e Agenti per l'ingegnere	Machine Learning per l'ingegneria: dati, previsione e ottimizzazione
1	IA generativa vs IA tradizionale	Oltre gli LLM
2	Machine Learning e LLM	Modelli predittivi
3	Prompt Engineering e RAG	Algoritmi ML
4	Agenti IA	Manutenzione predittiva
5	Human-in-the-Loop	Ottimizzazione progettuale
6	GDPR, AI Act e responsabilità	ML + CAD + BIM
7	Governance dell'IA	Digital Twin e roadmap
	Sapere cosa usare e come governarlo	Sapere come trasformare i dati in modelli e decisioni

Le tre aree da approfondire



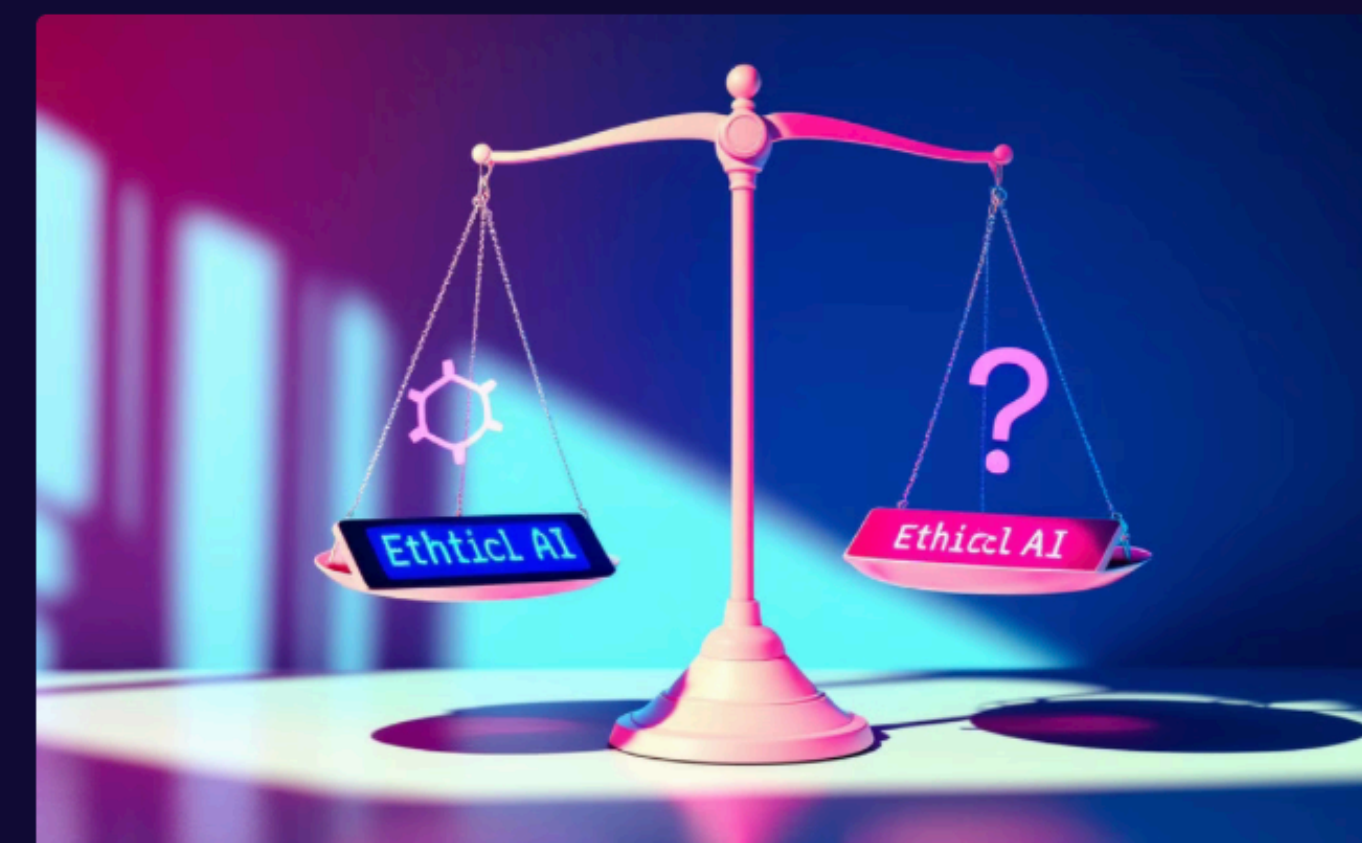
1) La tecnologia: comprenderne i Fondamenti

Conoscere i principi base dell'IA per valutarne correttamente le potenzialità e i limiti



2) Come usarla in pratica: Le componenti base dell'IA per creare Applicazioni

Scoprire come integrare l'IA nei processi quotidiani per aumentare efficienza e produttività



3) Come gestire: la governance e l'e Considerazioni Etiche

Riconoscere le implicazioni etiche per un utilizzo responsabile e sostenibile delle tecnologie IA

Ci porta via il lavoro dell'Ingegnere?

○ NO ma lo cambia

estratto dalla lista dell'articolo ...lista parziale

- **Professioni intellettuali:** molte figure white-collar (es. data scientist, ingegneri, manager) svolgono compiti comunicativi e di coordinamento: difficilmente automatizzabili perché implicano fiducia e responsabilità.
- **Lavoro accademico:** docenza e mentoring sono attività irriducibili all'automazione, basate su relazioni, esperienza, curiosità e adattamento individuale.
- **Tecnologia come complemento:** l'IA può essere utile per assistere, ma non per sostituire integralmente. Il valore umano resta nel giudizio, nella relazione e nella creatività.
- **La persistenza dei mestieri:** i lavori più antichi (es. falegname, insegnante, pescatore) tendono a durare nel tempo, mentre quelli recenti (es. social media manager) potrebbero scomparire prima.
- **L'arte e l'autenticità:** la creazione artistica ha senso per l'esperienza personale che esprime, non per la quantità di immagini generate.



Yann LeCun • Following
VP & Chief AI Scientist at Meta
4h •

Yeah, most tasks for most jobs can't be automated.

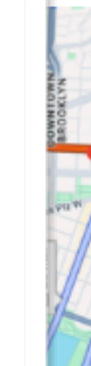


Julian Togelius • 2nd
Associate Professor of Computer ...
1d •

[+ Follow](#)

I wrote something. I'm afraid it's about AI again.

<https://lnkd.in/e7fwN-VN>

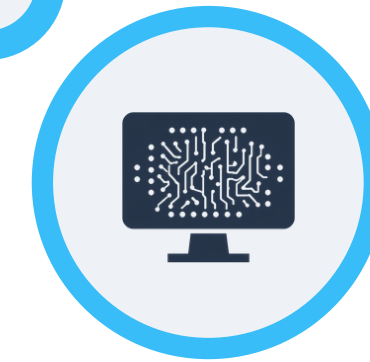
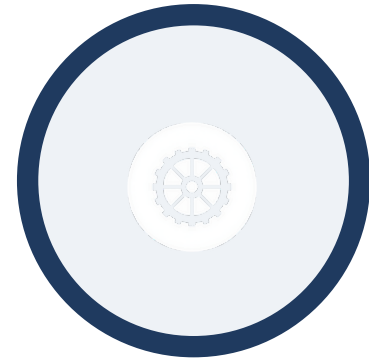


What is automatable and who is replaceable?...

togelius.blogspot.com

Perché questa trasformazione è diversa

Le rivoluzioni industriali hanno sempre ridefinito il ruolo dell'ingegnere. La quarta è diversa: riguarda l'intelligenza stessa.



1^a Rivoluzione Industriale

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

2^a Rivoluzione Industriale

Elettricità e produzione di massa. Nasce l'ingegneria industriale e la catena di montaggio.

3^a Rivoluzione Industriale

Informatica e automazione. Software, CAD e sistemi digitali trasformano il progetto.

4^a Rivoluzione Industriale

IA e collaborazione uomo-macchina. L'ingegnere supervisiona l'intelligenza artificiale.

Le forze del cambiamento

Le principali tecnologie dirompenti che stanno ridefinendo il ruolo dell'ingegnere.

IA Generativa

Crea contenuti, progetti e soluzioni autonomamente, accelerando processi creativi e tecnici.

Robotica

Sistemi fisici autonomi e collaborativi che operano in ambienti industriali e civili complessi.

Digital Twin

Replica digitale in tempo reale di asset fisici per simulazione, monitoraggio e ottimizzazione.

Agenti IA

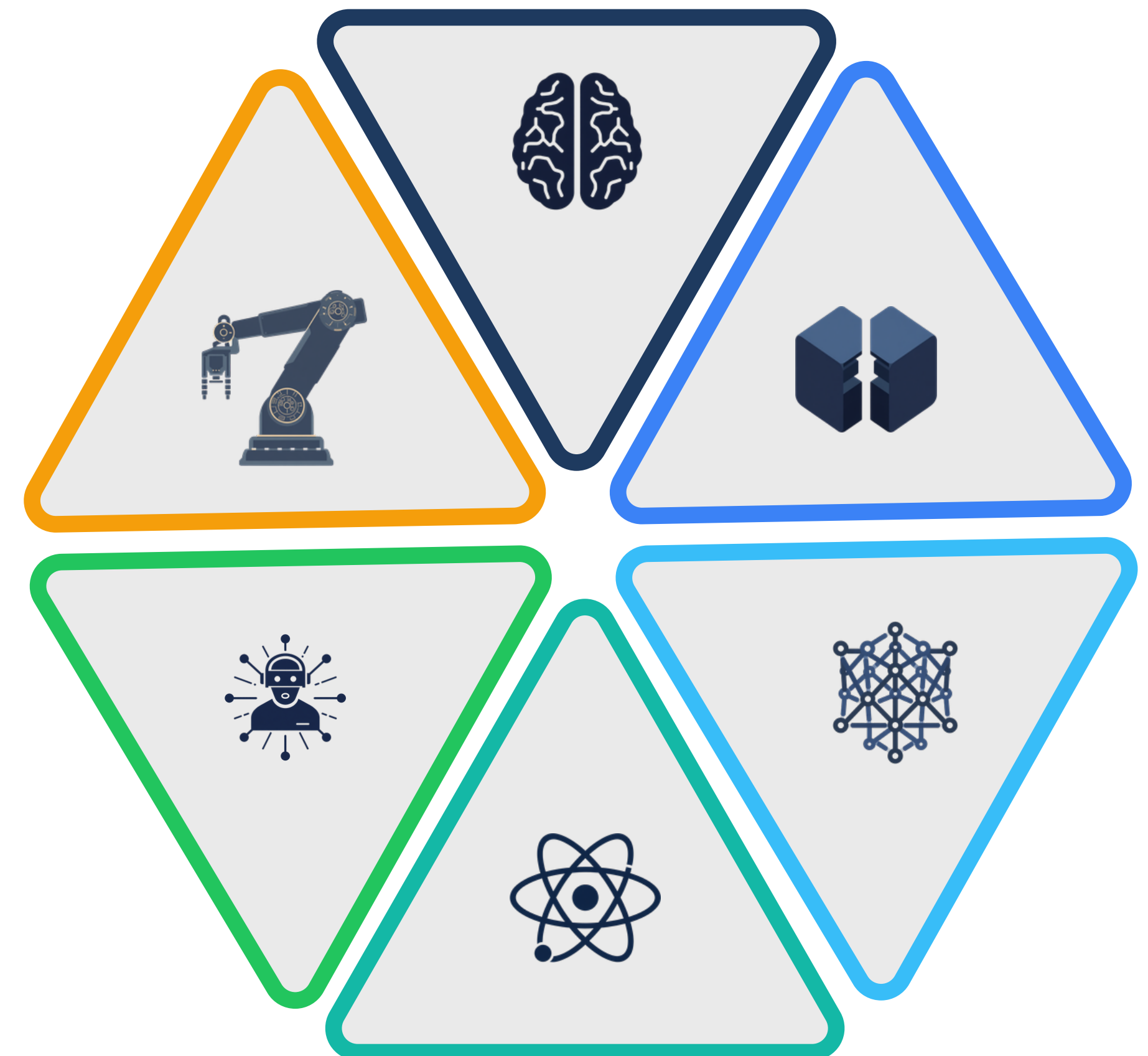
Entità software autonome capaci di pianificare, decidere e agire per raggiungere obiettivi complessi.

Quantum Computing

Potenza computazionale esponenziale per ottimizzazione, simulazione molecolare e crittografia.

Nuovi materiali

Materiali intelligenti, auto-riparanti e programmabili che trasformano progettazione e produzione.



Dal CAD all' *AI Engineering*

L'evoluzione tecnologica dell'ingegnere: dal disegno manuale agli agenti intelligenti.



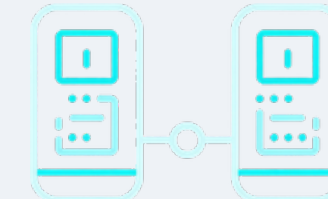
Disegno → CAD

Dal disegno manuale ai primi strumenti CAD: nasce la progettazione digitale 2D e 3D.



BIM → Cloud

Il BIM integra dati e collaborazione; il Cloud abilita accesso globale e lavoro distribuito.



Digital Twin

Il gemello digitale replica l'asset reale in tempo reale, abilitando simulazione e monitoraggio continuo.



IA → Agenti IA

L'IA genera soluzioni progettuali autonome; gli Agenti AI orchestrano processi complessi end-to-end.

L'evoluzione del ruolo dell'ingegnere

Come cambia il profilo professionale dell'ingegnere nel tempo: Ieri, Oggi e Domani.



Ieri

Disegna
Calcola
Produce



Oggi

Coordina
Verifica
Integra



Domani

Decide
Supervisiona IA
Governa
ecosistemi

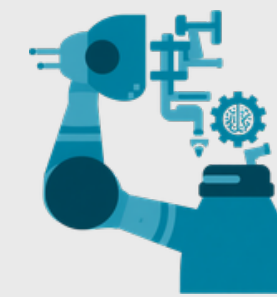


Cosa farà l'IA

Divisione dei compiti tra intelligenza artificiale e ruolo umano dell'ingegnere

Automatizzato dall'IA — 80%

Relazioni strutturali, computi metrici, disegni esecutivi e verifiche normative saranno gestiti autonomamente dall'IA.



Attività IA: esempi

Calcolo strutturale automatizzato, generazione di tavole CAD/BIM, computo preventivi, controllo conformità normativa.

Non Automatizzato — 20%

Decisioni strategiche, responsabilità professionale, creatività progettuale e leadership restano prerogativa esclusiva dell'ingegnere.



Ruolo umano: esempi

Scelte etiche e di progetto, firma e responsabilità legale, visione creativa, gestione del team e relazione con il cliente.

L'ingegnere aumentato

L'ingegnere al centro di un ecosistema di agenti IA specializzati che amplificano le sue capacità.



AI Designer

Genera disegni, modelli 3D e layout ottimizzati su richiesta dell'ingegnere.

Normativa IA

Verifica automaticamente conformità a norme, codici e regolamenti tecnici vigenti.

Costi IA

Elabora computi metrici, analisi costi e ottimizzazione del budget in tempo reale.

Sicurezza con IA

Identifica rischi, analizza vulnerabilità e propone misure preventive di sicurezza.

Simulazione con IA

Esegue simulazioni strutturali, energetiche e di scenario con modelli predittivi avanzati.

AI Project Manager

Pianifica attività, gestisce risorse, monitora avanzamento e ottimizza la schedulazione.

Evoluzione settore Civile

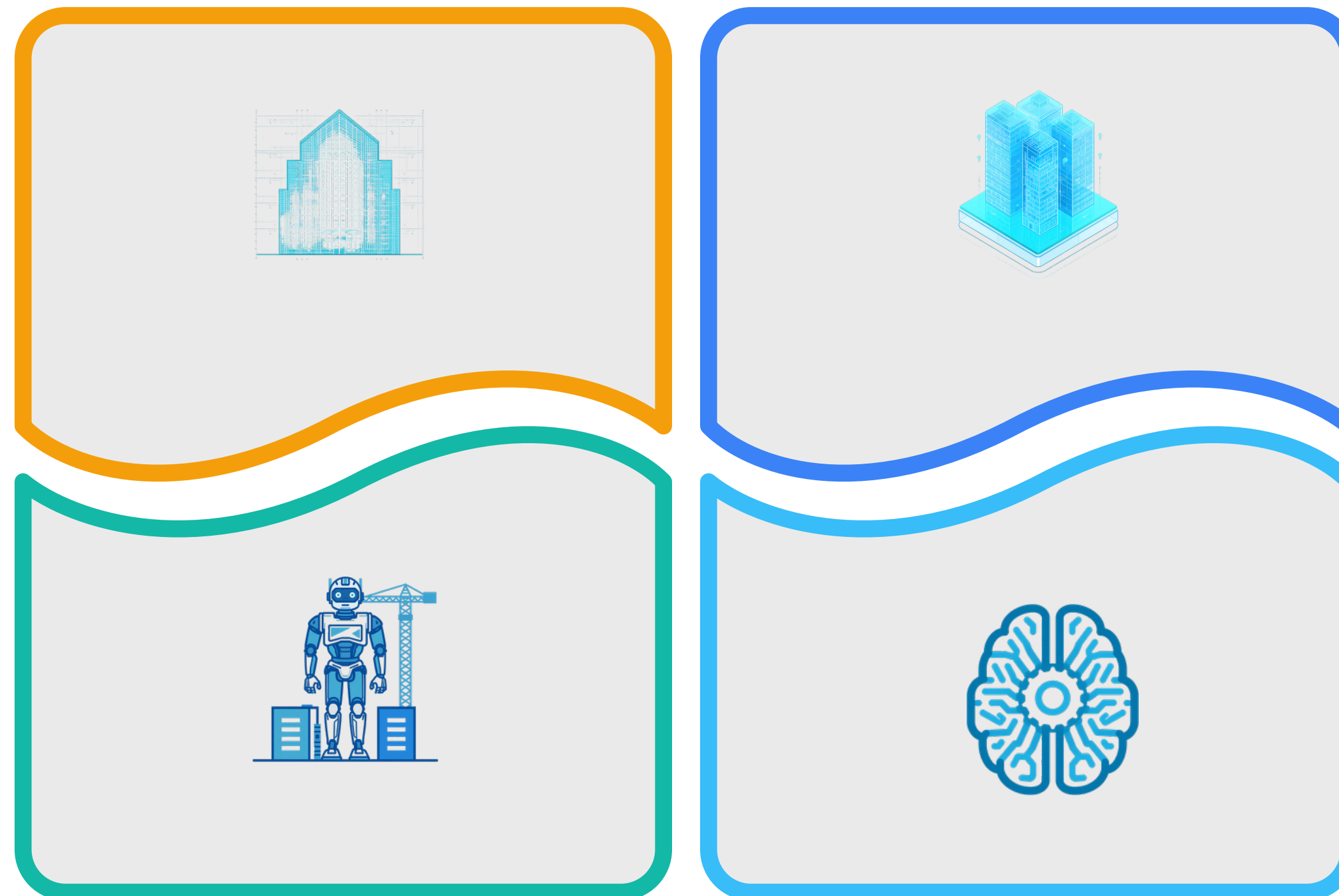
Dal progetto tradizionale alla supervisione intelligente di infrastrutture digitali e robot di cantiere.

Oggi

Progetta edifici e infrastrutture con strumenti tradizionali e CAD. Il ruolo è centrato sul disegno tecnico e sul calcolo strutturale.

2045

Utilizza IA generativa per progettazione automatica. Controlla robot di cantiere e monitora infrastrutture in tempo reale tramite AI.



2035

Supervisiona Digital Twin permanenti degli edifici. Gestisce edifici intelligenti connessi e coordina team ibridi uomo-macchina.

Competenze Chiave

AI Literacy, Digital Twin Management, Supervisione robotica, Gestione dati in tempo reale, Governance di sistemi autonomi.

Evoluzione settore Industriale

Trasformazione del settore industriale dall'ingegneria tradizionale all'automazione intelligente.

Oggi

Progettazione manuale, calcolo strutturale tradizionale, processi produttivi standardizzati.

2035

Materiali intelligenti e adattativi, manutenzione predittiva autonoma con sensori IoT.



Transizione

Progettazione generativa assistita da IA, prototipazione rapida con stampa 3D avanzata.

2045

Robot collaborativi, gemelli digitali di fabbrica, ottimizzazione continua dei processi produttivi.

Evoluzione settore Gestionale

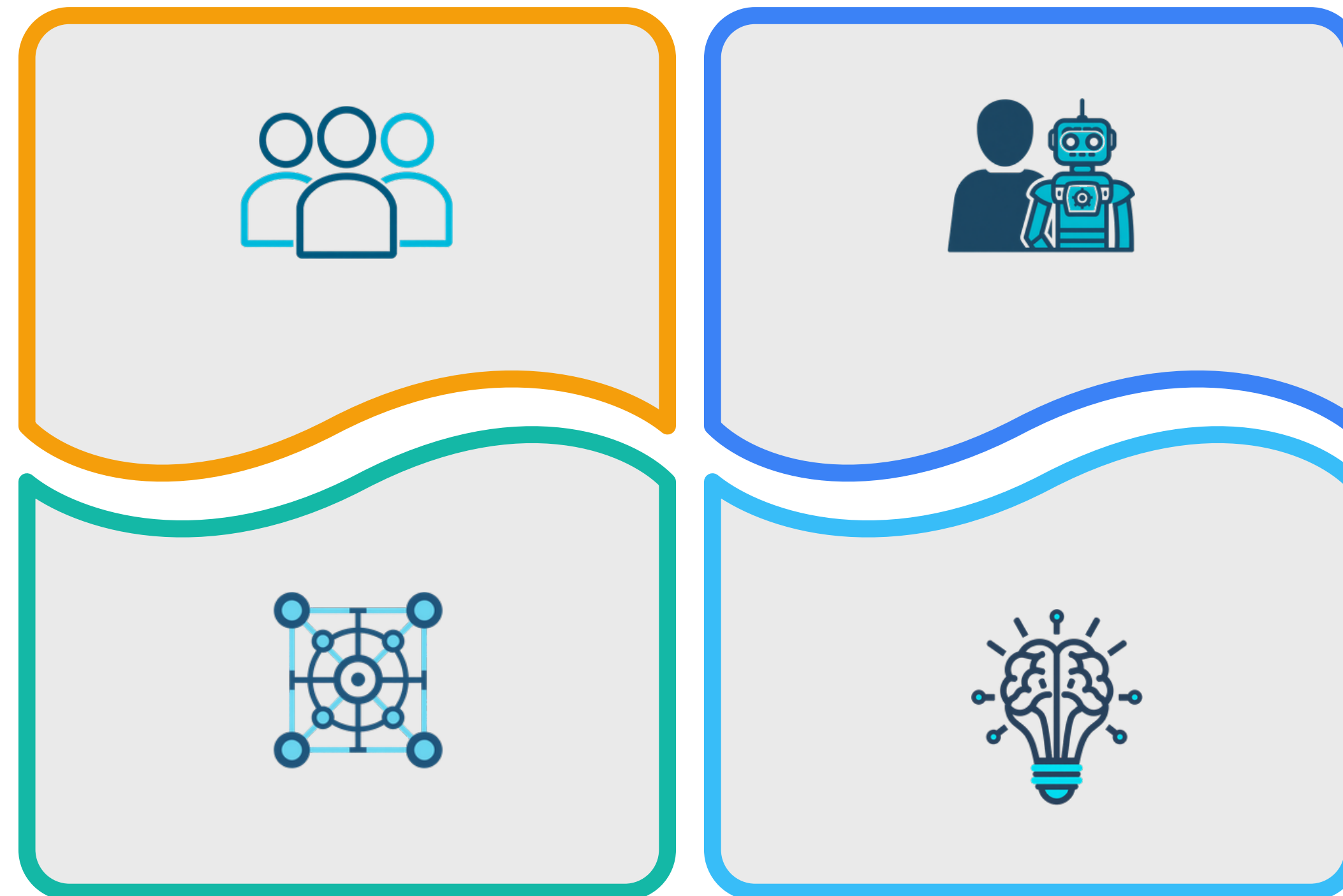
Trasformazione del ruolo gestionale: dal coordinamento tradizionale all'orchestrazione di ecosistemi autonomi.

Oggi

Coordinamento base di team e processi. Gestione manuale di progetti, risorse e fornitori con strumenti tradizionali.

2045

Gestore di supply chain autonome e sistemi decisionali complessi. Orchestrazione di ecosistemi intelligenti in tempo reale.



2035

Coordina IA, persone e robot. Gestione ibrida di team umani e agenti automatizzati in ambienti digitalizzati.

Competenze Chiave

Leadership, AI Literacy, pensiero sistemico, gestione del cambiamento e governance di processi autonomi.

Evoluzione settore Informatica

Trasformazione del ruolo dell'ingegnere informatico: da programmatore a orchestratore di ecosistemi intelligenti.

Oggi

Programmazione software tradizionale, sviluppo applicazioni, gestione database e infrastrutture IT classiche.

2045 — AI Engineering

AI Engineering, Model Governance, Edge AI, Federated Learning, Human-AI Interaction e sistemi autonomi distribuiti.

2035

Progettazione di ecosistemi intelligenti, integrazione di modelli AI, architetture cloud-native e piattaforme dati avanzate.

2045 — Governance & Safety

AI Safety, gestione del rischio algoritmico, compliance normativa AI, supervisione di agenti autonomi e sistemi decisionali complessi.



Evoluzione settore Elettronica

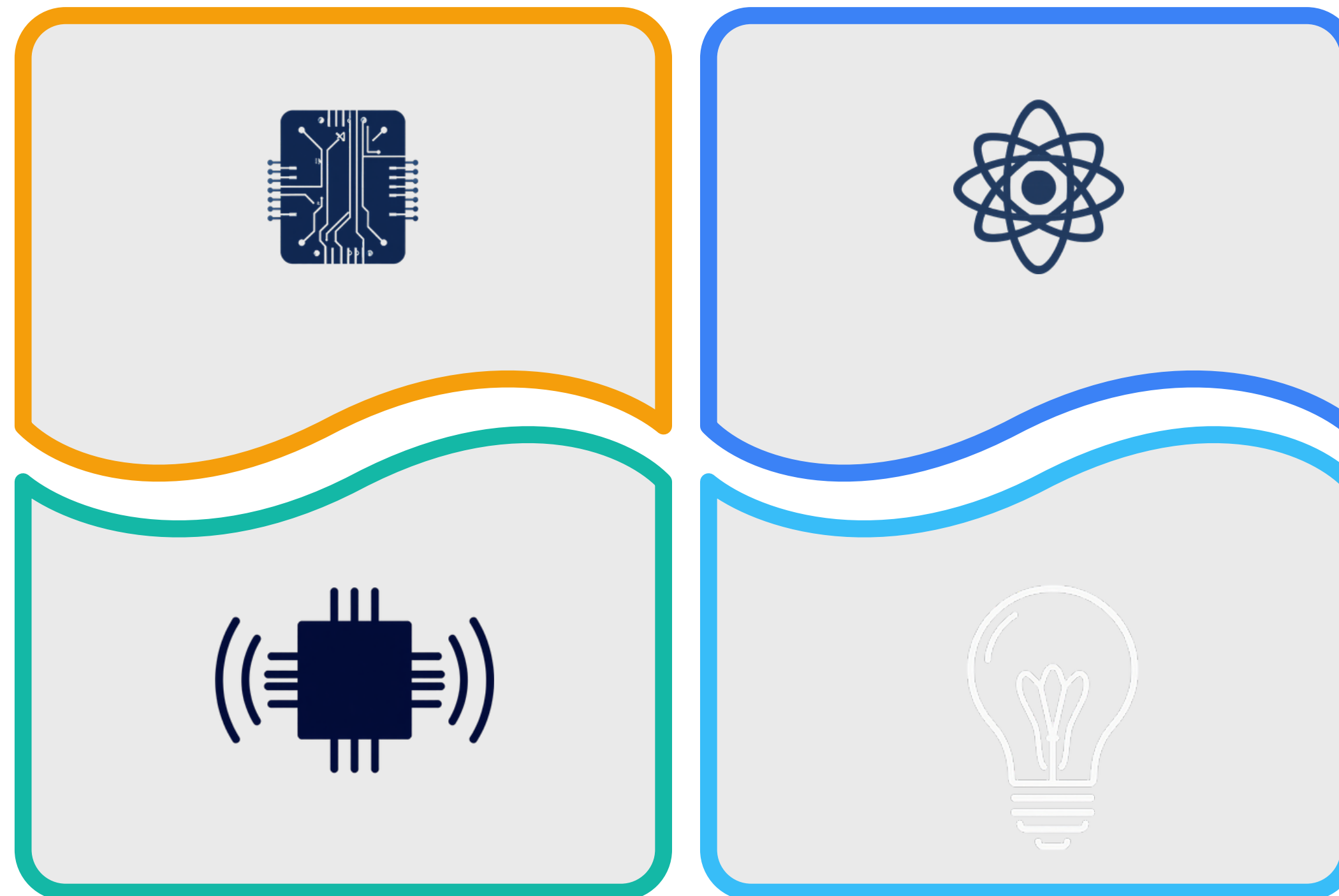
Trasformazione del settore elettronico: da circuiti tradizionali a sistemi autonomi e quantum devices.

Oggi

Progettazione di circuiti tradizionali, sistemi embedded e componenti elettronici standard.

2045

Sistemi autonomi, robotica avanzata, quantum devices e architetture neuromorfe di nuova generazione.



2035

Sensori intelligenti, semiconduttori avanzati, IoT pervasivo e integrazione AI nei dispositivi.

Impatto Chiave

L'ingegnere elettronico governa ecosistemi intelligenti, garantendo sicurezza, efficienza e innovazione continua.

Evoluzione settore Meccanica ed Energetica

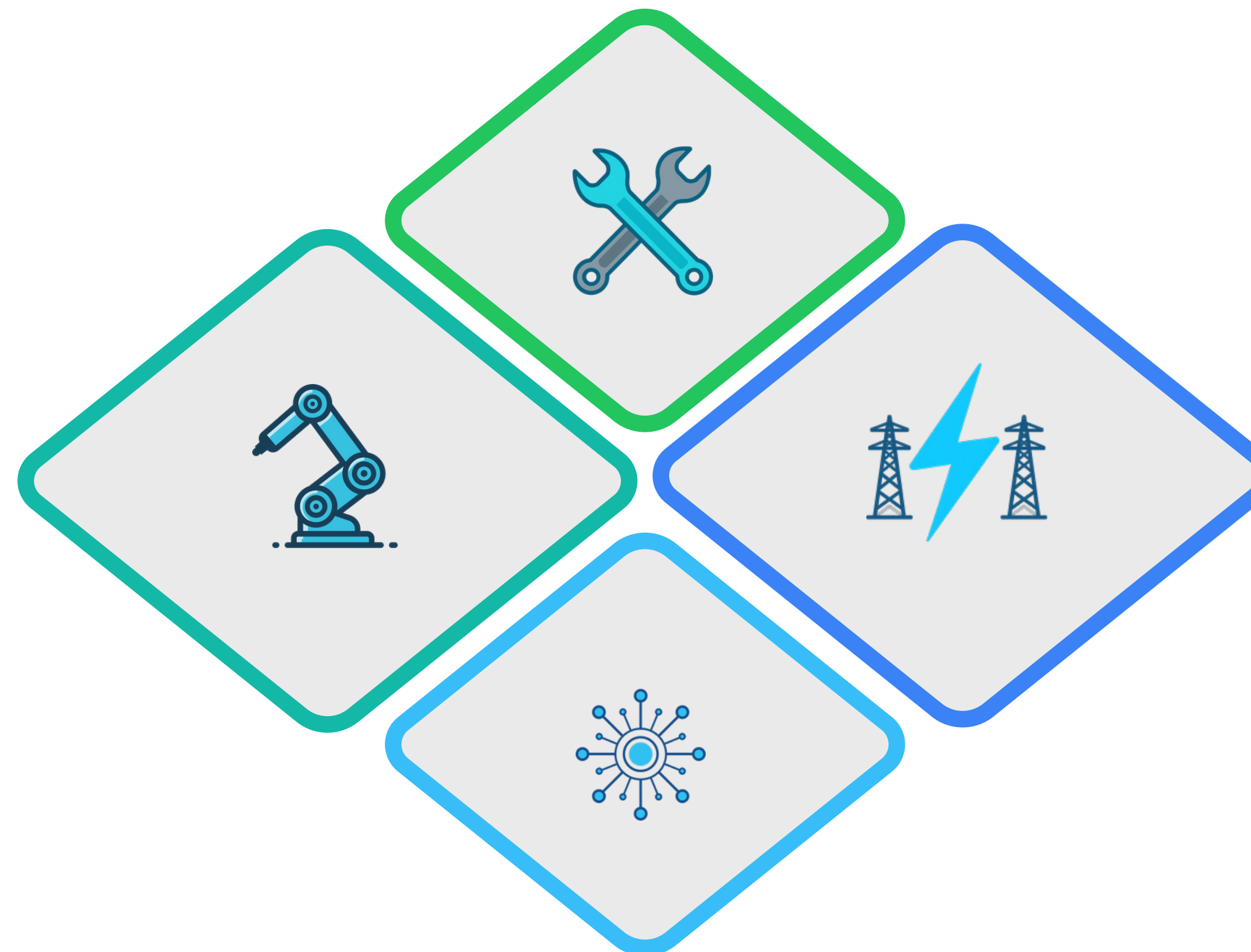
Confronto temporale: Oggi → 2035 → 2045 per i settori Meccanica ed Energetica

Meccanica – Oggi & 2035

Oggi: progettazione meccanica tradizionale. 2035: progettazione generativa assistita da IA, stampa 3D avanzata.

Meccanica – 2045

Robot collaborativi in produzione, materiali intelligenti e adattativi, manutenzione predittiva automatizzata.



Energetica – Oggi & 2035

Oggi: gestione manuale delle reti energetiche. 2035: reti autonome, IA per ottimizzare produzione e consumo.

Energetica – 2045

Strategie energetiche integrate con IA, gestione di micro-reti distribuite, ottimizzazione in tempo reale.

Le competenze che cresceranno

Le 8 competenze chiave per l'ingegnere del futuro nell'era dell'intelligenza artificiale.

AI Literacy

Comprendere e governare i modelli di intelligenza artificiale, prompt engineering e gestione degli agenti AI.

Leadership & Pensiero Critico

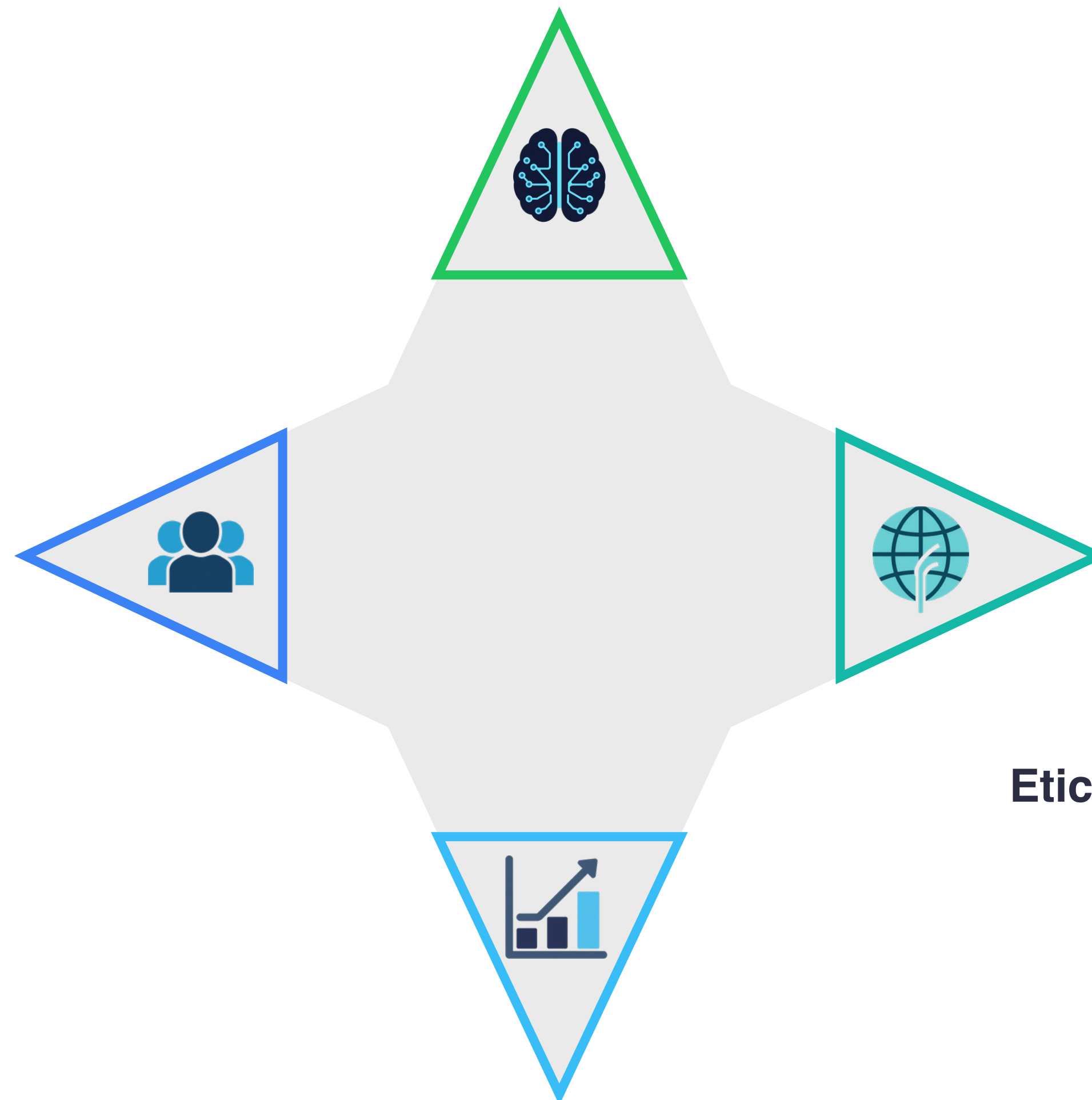
Guidare team ibridi uomo-macchina, prendere decisioni complesse e valutare criticamente gli output dell'IA.

Data Science & Cybersecurity

Analizzare dati strutturati e non strutturati, proteggere infrastrutture digitali e garantire la sicurezza dei sistemi.

Etica, Sostenibilità & Comunicazione

Applicare principi etici all'IA, integrare criteri ESG nei progetti e comunicare efficacemente con stakeholder diversi.



Nuove Professioni

Le figure emergenti nell'ingegneria aumentata dall'intelligenza artificiale.

AI Engineering Manager

Coordina team ibridi uomo-macchina, supervisiona pipeline di sviluppo AI e garantisce l'allineamento tecnico-strategico.

AI Safety Engineer

Identifica rischi nei sistemi AI, definisce protocolli di sicurezza e garantisce il rispetto degli standard etici e normativi.

Digital Twin Architect

Progetta e gestisce repliche digitali di infrastrutture fisiche per simulazione, monitoraggio e ottimizzazione in tempo reale.

Prompt Engineer

Progetta istruzioni e flussi di interazione con modelli AI per massimizzare l'accuratezza e l'utilità degli output generati.

Human-AI Coordinator

Facilita la collaborazione tra operatori umani e agenti AI, ottimizzando processi decisionali e flussi di lavoro integrati.

AI Compliance Engineer

Assicura la conformità dei sistemi AI alle normative vigenti (es. EU AI Act), gestendo audit, documentazione e governance.



Il nuovo workflow

Dal brief del cliente alla consegna digitale: il processo ingegneristico aumentato dall'IA.



Richiesta del cliente

Il cliente definisce obiettivi, vincoli e requisiti del progetto.

Agenti con IA

Gli agenti AI elaborano il brief e generano fino a 100 alternative progettuali in automatico.

Simulazioni

Le alternative vengono simulate e valutate su parametri strutturali, energetici e di costo.

Scelta dell'ingegnere

L'ingegnere analizza i risultati, applica il giudizio critico e seleziona la soluzione ottimale.

Firma digitale

L'ingegnere valida e certifica il progetto con firma digitale, assumendosi la responsabilità professionale.

Digital Twin

Il progetto viene consegnato come Digital Twin permanente, aggiornabile e monitorabile in tempo reale.

Rischi

Principali rischi legati all'integrazione dell'IA nel ruolo dell'ingegnere.

Deskilling

La dipendenza eccessiva dall'IA può erodere le competenze tecniche fondamentali dell'ingegnere nel lungo periodo.



Dipendenza dall'IA

Affidarsi ciecamente ai sistemi automatizzati senza comprensione critica dei processi sottostanti.

Cybersecurity

Sistemi connessi e digitali espongono infrastrutture critiche a vulnerabilità e attacchi informatici.



Errori sistemici & Bias

Modelli AI possono amplificare errori sistematici e bias nei dati, con conseguenze su decisioni ingegneristiche critiche.

TROPPO PRESTO PER FISSARE BUSINESS MODEL DEFINITIVI, SIAMO ALL'INIZIO DI UN'EVOLOUZIONE

**Ne va tenuto conto ogni volta che si imposta l'implementazione di sistemi con IA all'interno di
un'organizzazione**

Fa parte di un primo approccio etico

La definizione di IA dall'Unione Europea

- Le “intelligenze artificiali”

Prima legge al mondo rilasciata sulle Intelligenze artificiali

Basata sulla valutazione del rischio

Promuove la tecnologia

Protegge i cittadini

INTELLIGENZA ARTIFICIALE O SISTEMI DI IA

Si tratta di] sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato.

I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente.

Come disciplina scientifica, l'IA comprende diverse approcci diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici).

Commissione Europea, *Orientamenti etici per un'IA affidabile*, 2018 | cfr.: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>



AI Act: la mappa del rischio per l'ingegneria

Regolamento UE 2024/1689 · In vigore dal 1° agosto 2024 · Scadenze operative: 2026-2027

VIETATO

Riconoscimento biometrico realtime · Social scoring · Manipolazione subliminale

Nessuna applicazione tipica in ingegneria — ma attenzione ai sistemi di controllo accessi biometrici

ALTO RISCHIO —

Allegato III Sistemi di controllo infrastrutture critiche · Macchinari autonomi in ambienti di lavoro · Sistemi di sicurezza

Civile: AI per verifica sicurezza strutture critiche · Industriale: robot collaborativi, SCADA su reti energetiche

RISCHIO LIMITATO

Chatbot e assistenti virtuali · Sistemi di raccomandazione · Deep fake — obbligo di trasparenza

LLM usati per assistenza tecnica, generazione documentazione, verifica normativa

RISCHIO BASSO

Filtri spam, correttori, ottimizzazione percorsi standard, strumenti di calcolo con ML non critico

La maggior parte degli usi di Claude/ Gemini per relazioni tecniche rientra qui

Per i professionisti tecnici: il ruolo chiave è distinguere se si è **FORNITORE** (sviluppa/personalizza il sistema) o **DEPLOYER** (usa il sistema nel proprio incarico). Gli obblighi sono molto diversi.

CIVILE

Strutture critiche, ponti, dighe → verificare Allegato III

INDUSTRIALE

Robot collaborativi, SCADA critici → verificare Allegato III

GESTIONALE

AI decisionali su personale/contratti → verificare Allegato III

Nascita dell'IA (1956)

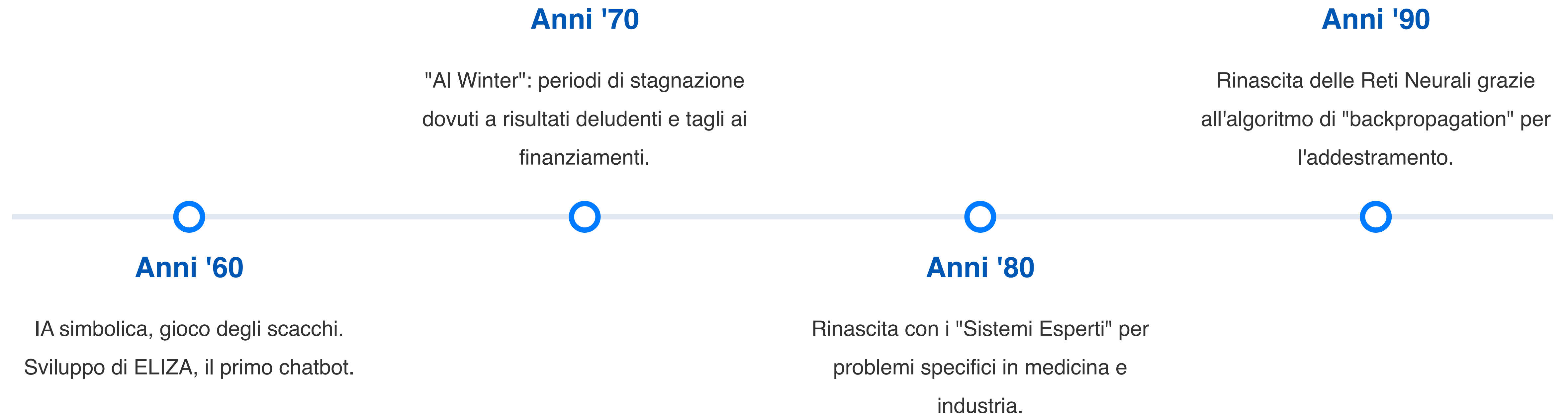
Conferenza al Dartmouth College

Considerato l'evento fondante della disciplina. Fu organizzata da ricercatori e specialisti tra cui: John McCarthy, Marvin Minsky, Claude Shannon e Nathaniel Rochester.

L'obiettivo: esplorare come far compiere alle macchine funzioni tipiche dell'intelligenza umana, come apprendere, ragionare e risolvere problemi.



Evoluzione dell'IA: Dal Simbolismo al Connessionismo



Il Cambio di Paradigma nell'Informatica

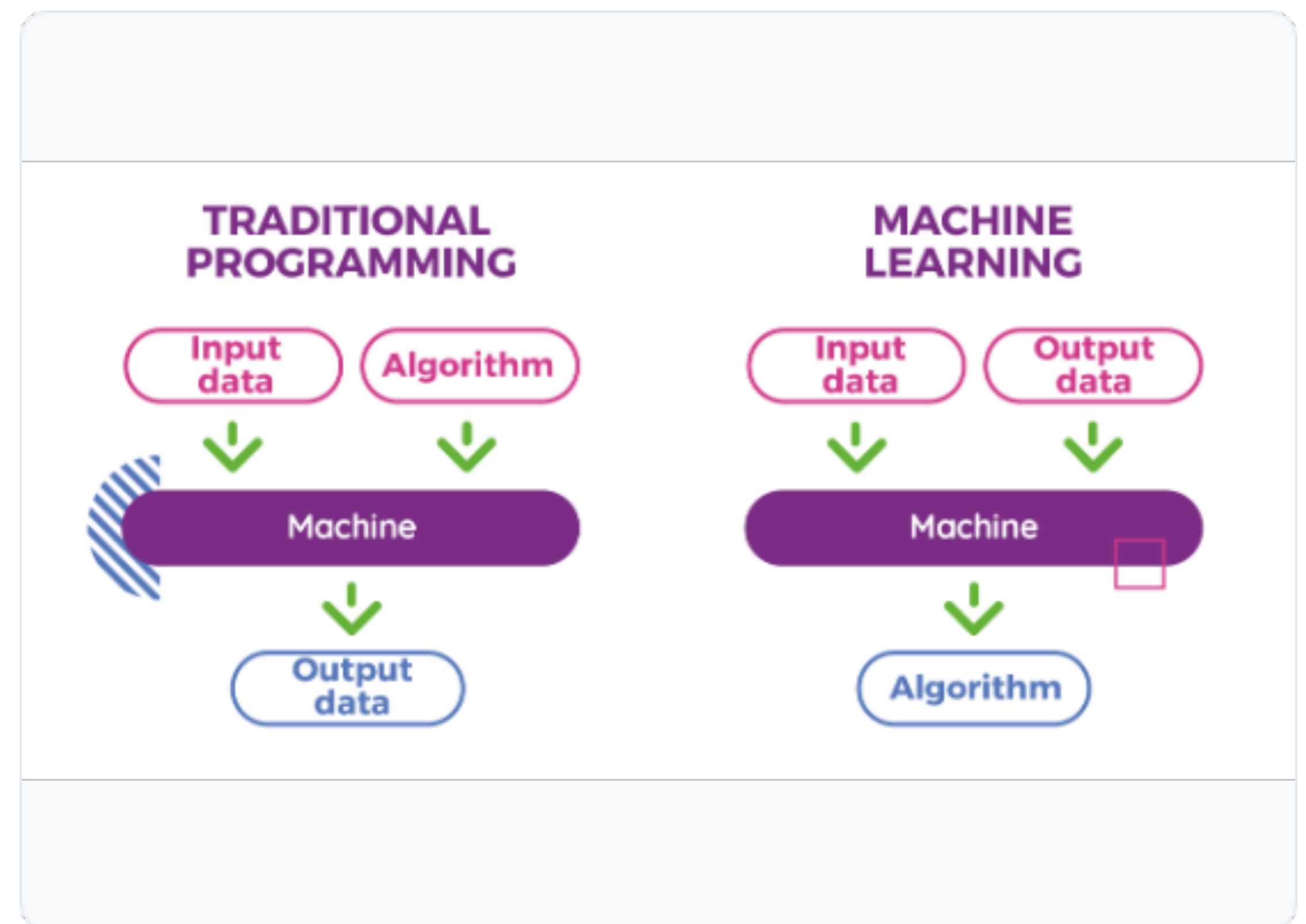
Dall'Algoritmo che Esegue all'Algoritmo che Impara

Programmazione Tradizionale: Uno sviluppatore crea un algoritmo (Programma SW) che esegue azioni specifiche.

Machine Learning: Un modello ML impara dai dati per eseguire azioni. I dati sono l'elemento fondamentale.

Umano: Esperienza → Elaborazione → Decisione

Macchina: Dati → Elaborazione → Decisione

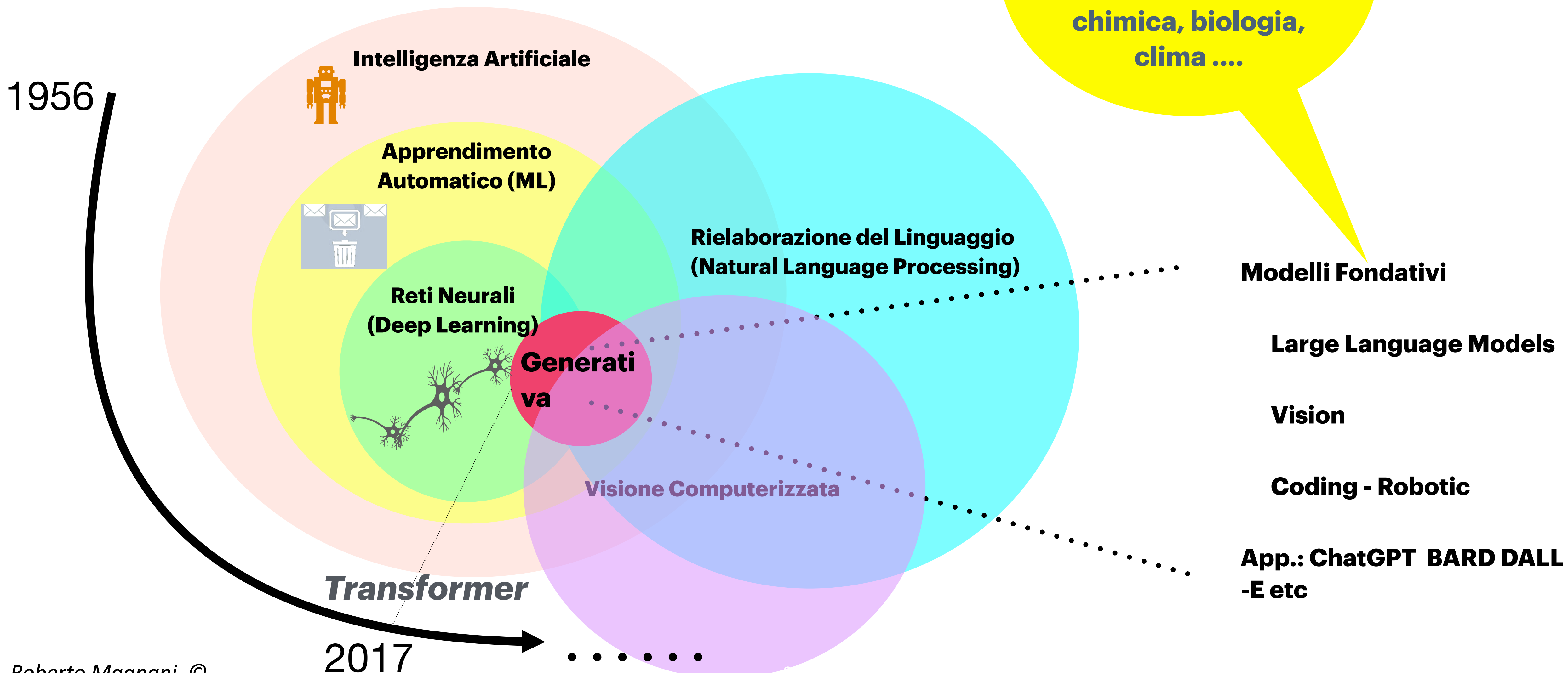


Intelligenza Artificiale

Un mondo variegato

Sui modelli
fondativi si
possono sviluppare
modelli dedicati a
chimica, biologia,
clima

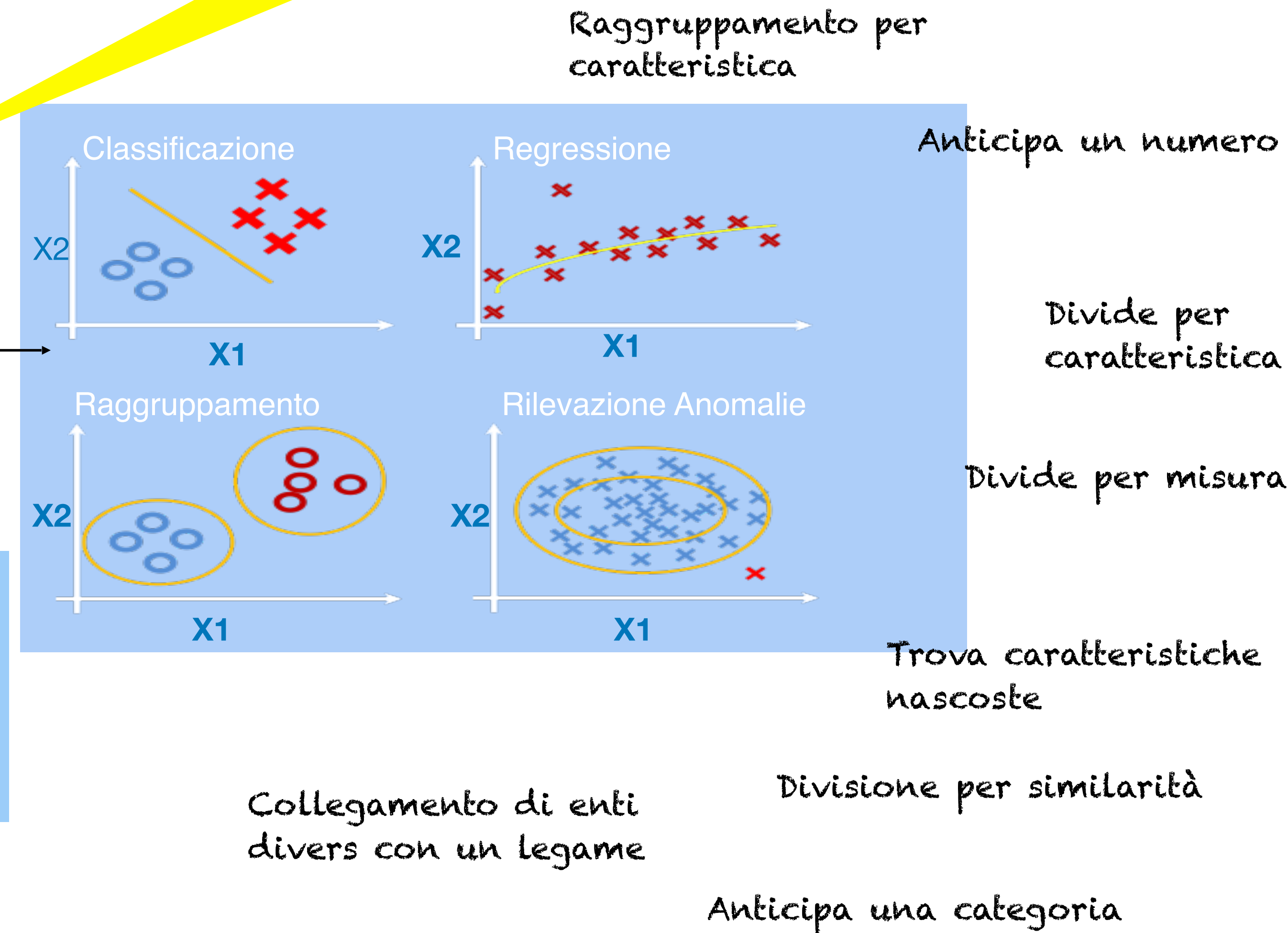
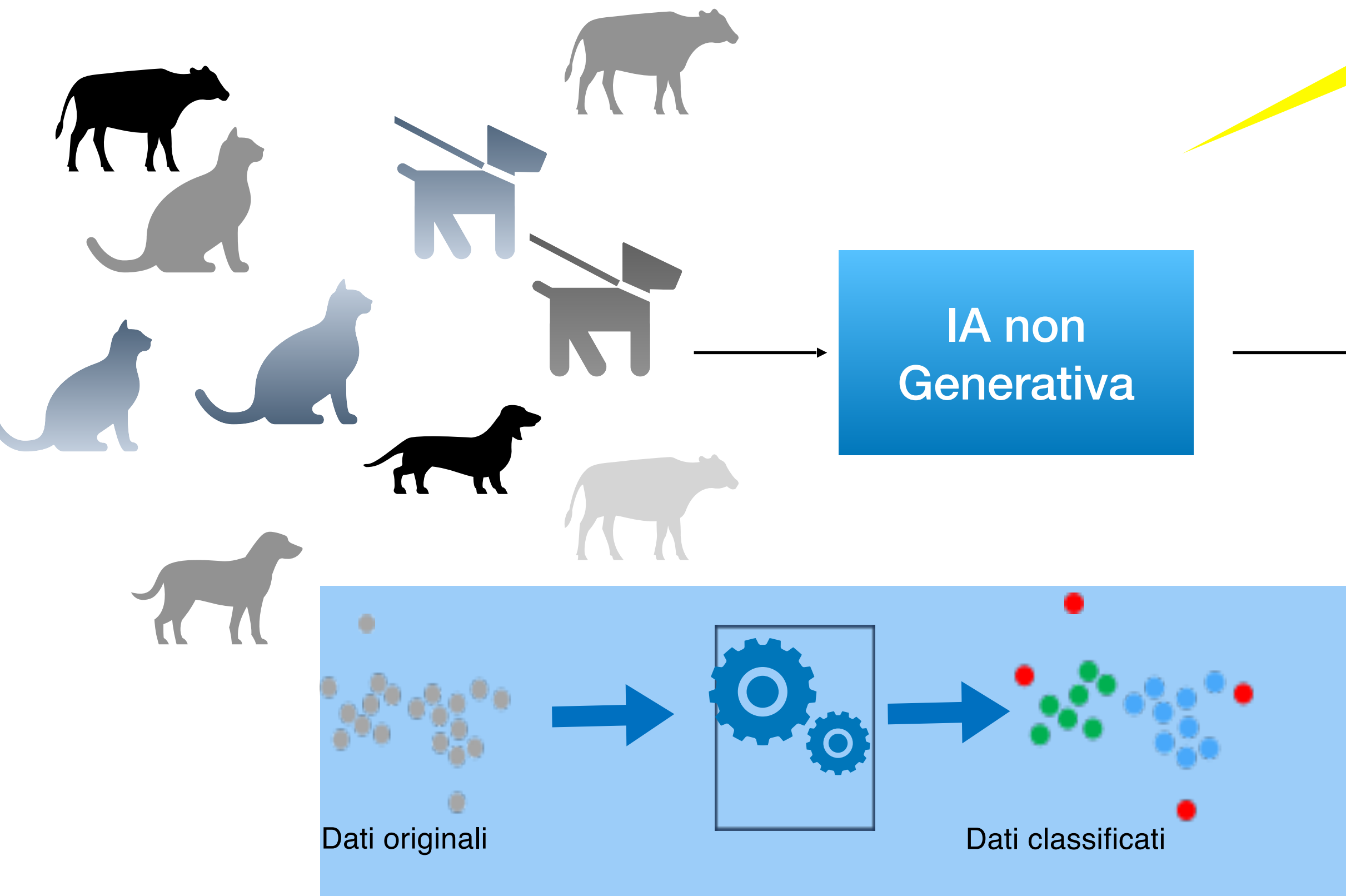
Fine Tuning



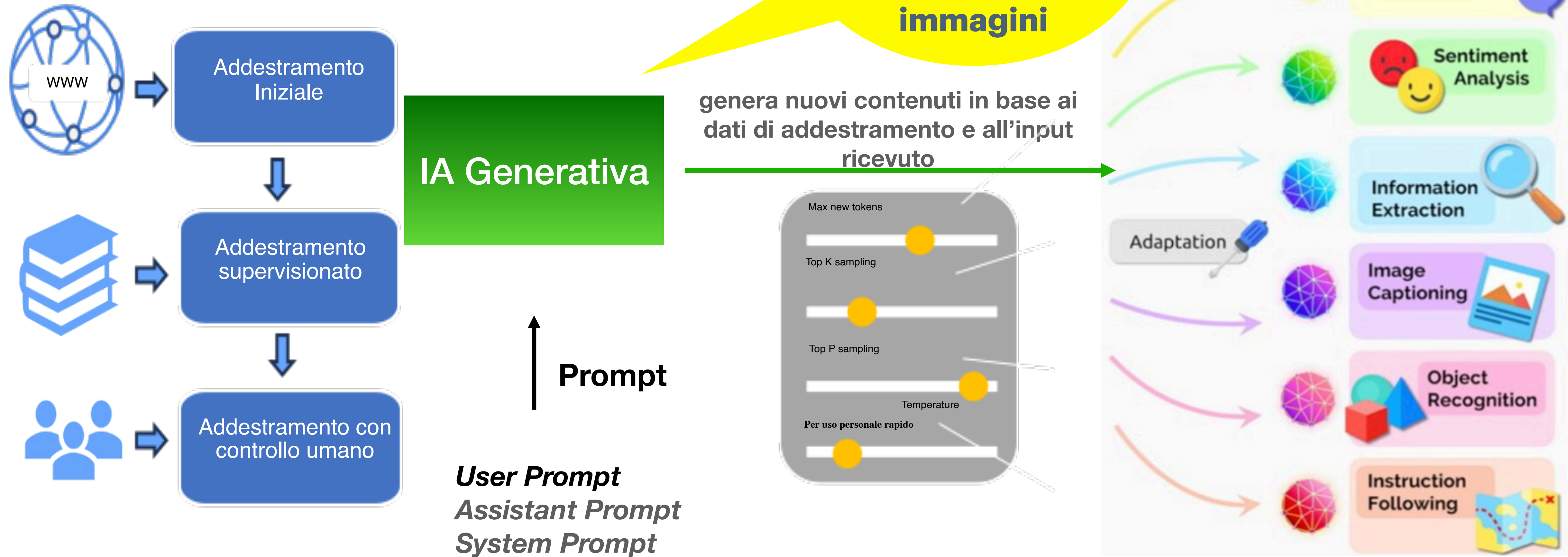
Le IA non generative

Machine Learning

Focus su compiti
specifici come
classificazioni o
regressioni



Le IA generative



IA Generativa

Foundation Model (Pre-addestrato)

Un grande modello (come un LLM) viene addestrato su terabyte di dati in modo non supervisionato, creando una vasta base di conoscenza.

Fine-Tuning e Prompting

Il Foundation Model viene poi specializzato (fine-tuning) per compiti specifici. L'IA Generativa può creare "dati sintetici" per addestrare modelli non generativi, riducendo la necessità di grandi dataset iniziali.

IA Generativa vs. IA Analitica (Discriminativa)

IA Analitica (Non Generativa)

Elabora i dati di ingresso per differenziare, classificare, identificare modelli e trarre conclusioni.

Compiti: Classificazione, Regressione, Raggruppamento.

Esempi: Riconoscimento immagini, diagnosi medica, previsione del tempo, rilevamento anomalie.

IA Generativa

Crea nuovi contenuti (testi, musica, immagini) che sono simili ai dati su cui è stata addestrata.

Compiti: Creazione contenuti, generazione dati sintetici.

Esempi: Generazione di nuove immagini, chatbot avanzati, composizione musicale.

Cosa sono le Reti Neurali?

Ispirate ai Sistemi Biologici

Le Reti Neurali Artificiali (ANN) sono basate su un modello matematico del neurone biologico.

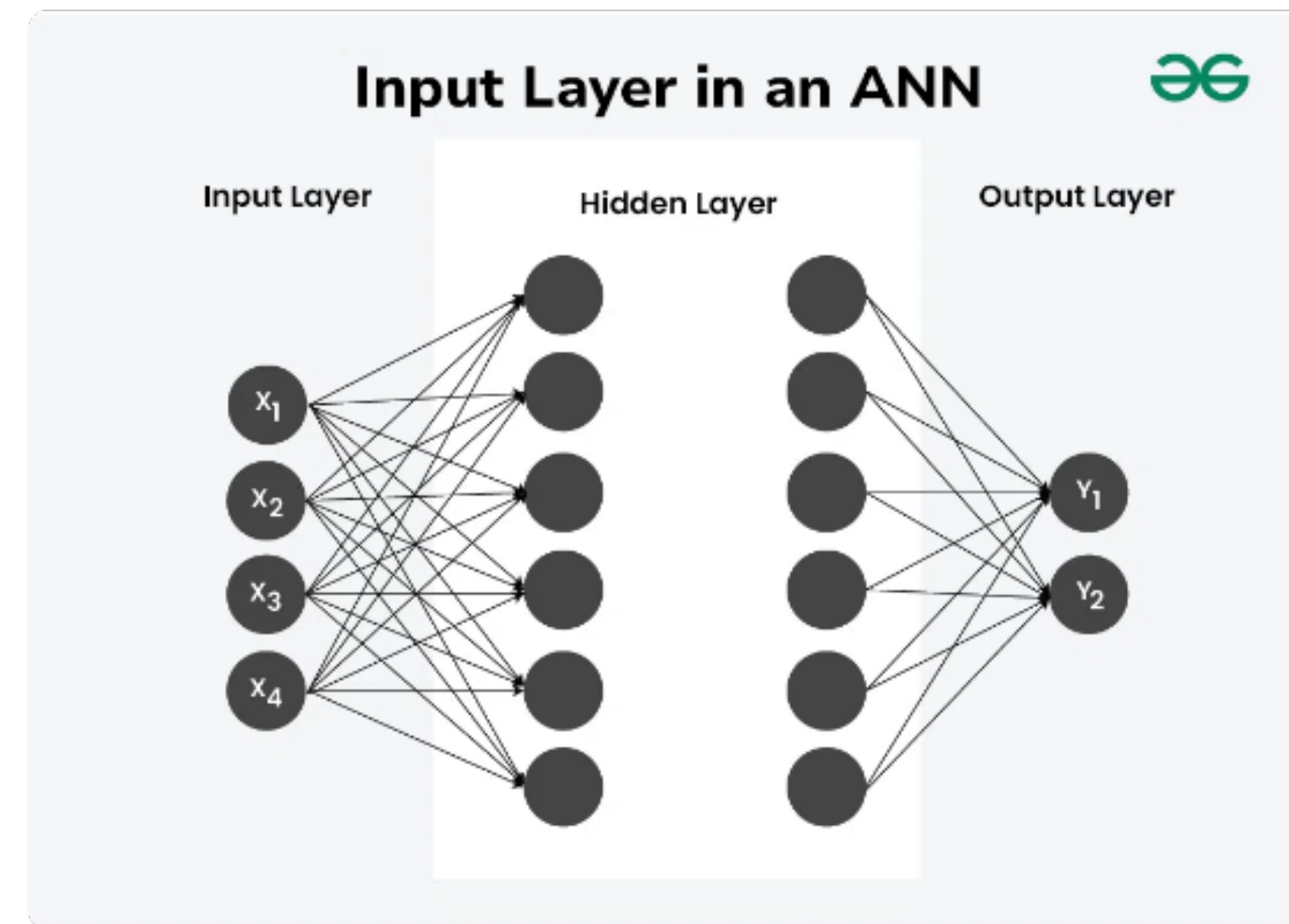
- **Neurone Artificiale:** Riceve input (I), applica dei pesi (w), somma i valori (net) e applica una funzione di attivazione (f) per produrre un output (U).
- **Rete Neurale:** Un'architettura a più strati (ingresso, strati nascosti, uscita) il cui comportamento è determinato dalla topologia e dai valori dei pesi.

Neurone Artificiale

Costituito da due stadi:

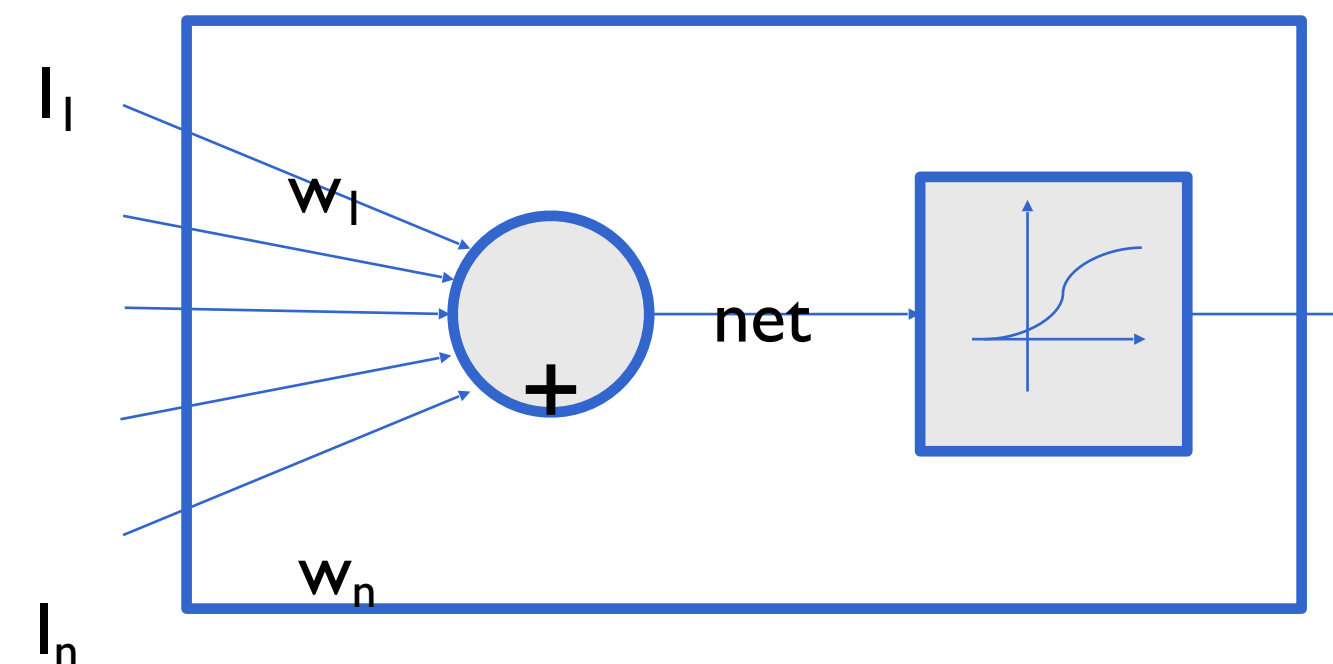
sommatore **lineare** $\text{net} = \sum_j W_j i_j + \text{bias}$ $W_j = \text{peso}$

funzione di attivazione f **non lineare** a soglia $U = f(\text{net})$



Il comportamento di una rete neurale è determinato:

- dal numero dei neuroni
- dalla topologia
- dai valori dei pesi associati alle connessioni



Ad ogni ingresso è associato un **peso**, utilizzato nel sommatore che costituisce il primo stadio del neurone che *riceve* dati attraverso la connessione.

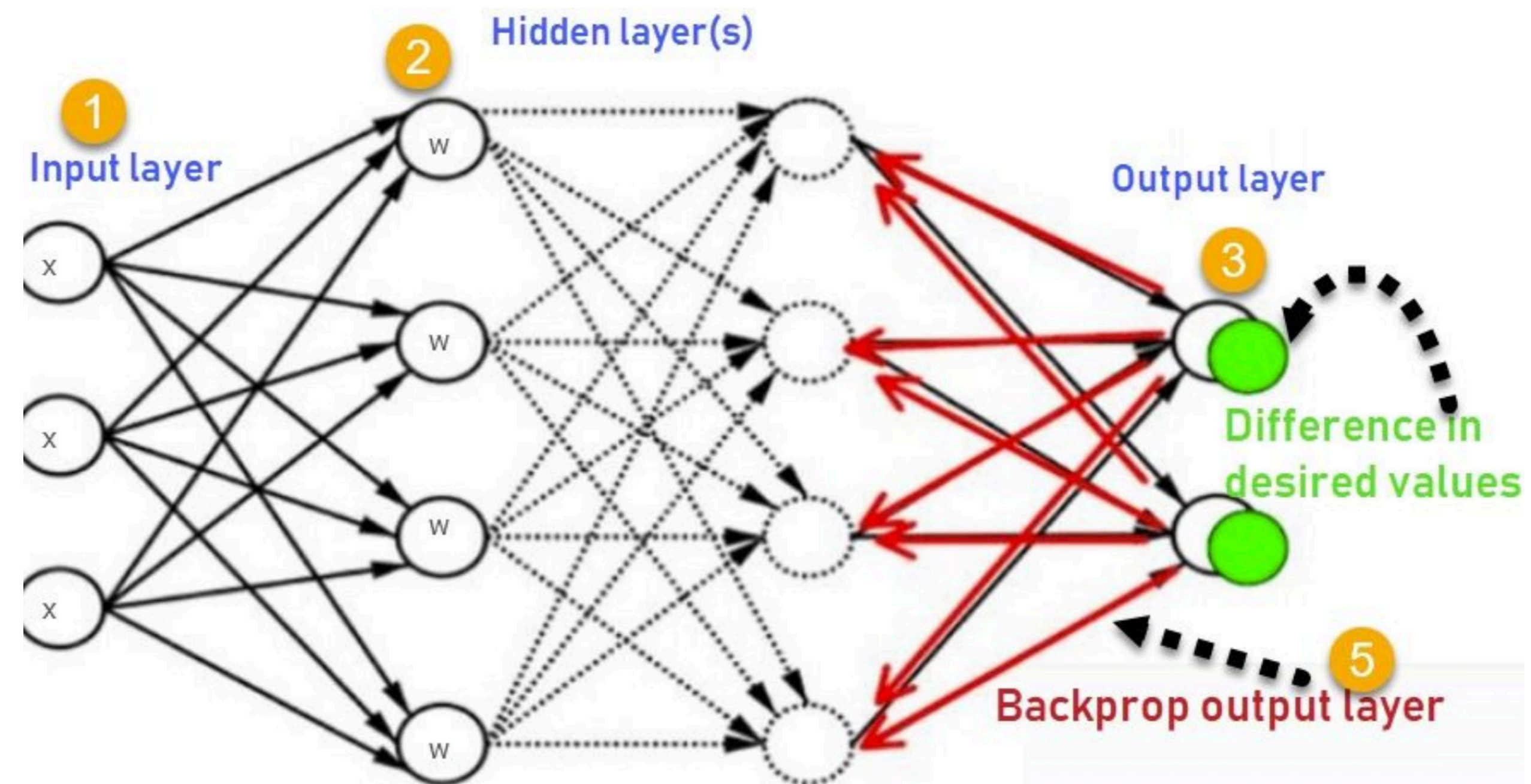
L'errore che insegna. Come l'IA impara davvero

Backpropagation

- intuizione nata negli anni '80
- aggiusta i pesi interni della rete in base all'errore commesso

1. L'output viene confrontato con il valore atteso: si calcola l'errore.

2. Questo errore viene “retropropagato” all'indietro lungo tutti i livelli della rete, per aggiornare i pesi e ridurre gradualmente lo scarto nei successivi tentativi.



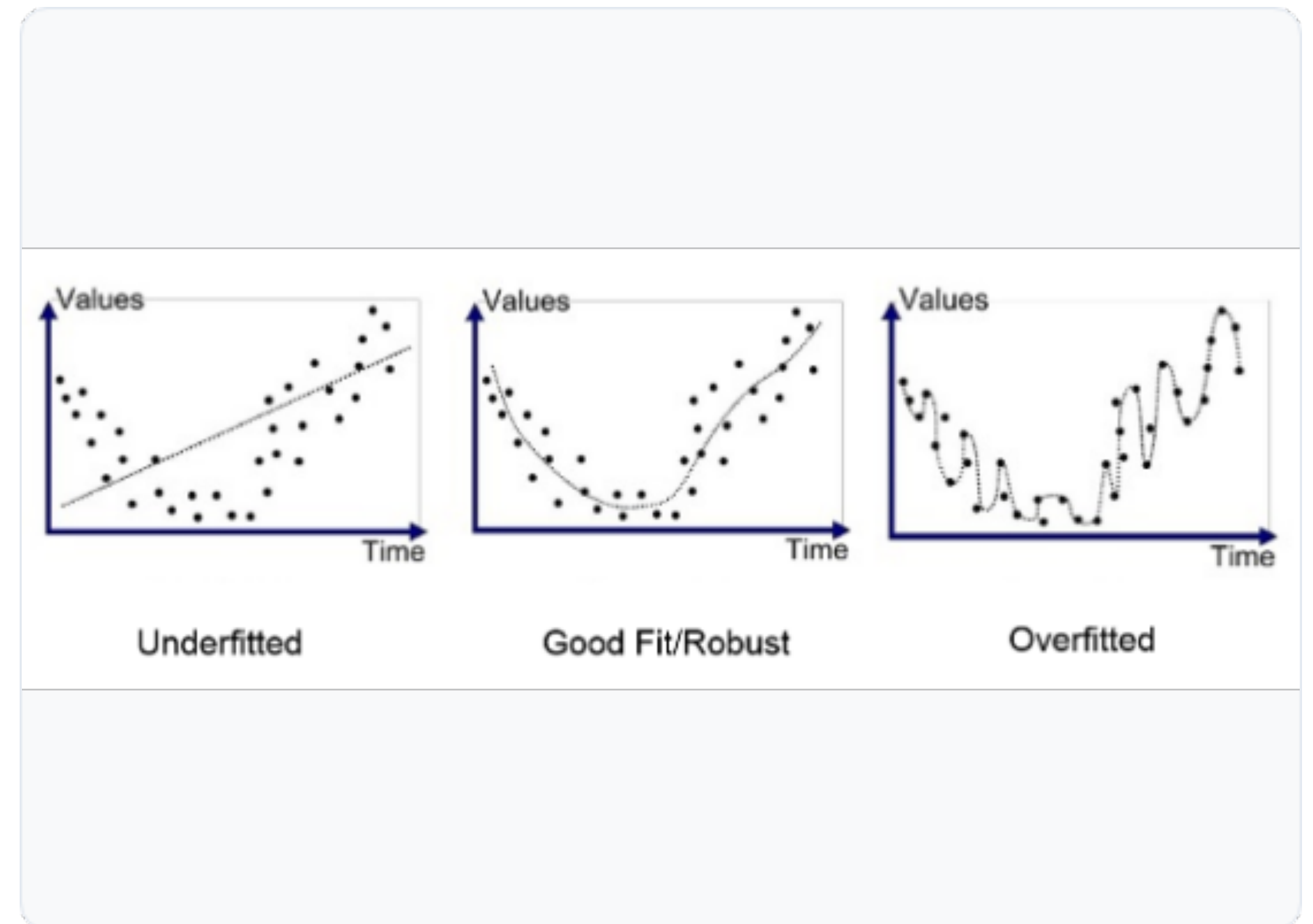
Senza la backpropagation, oggi non esisterebbero né il riconoscimento vocale, né la traduzione automatica, né i modelli generativi. È l'algoritmo che ha insegnato alle macchine a imparare... sbagliando

Addestramento di una Rete Neurale

Trovare il Giusto Equilibrio

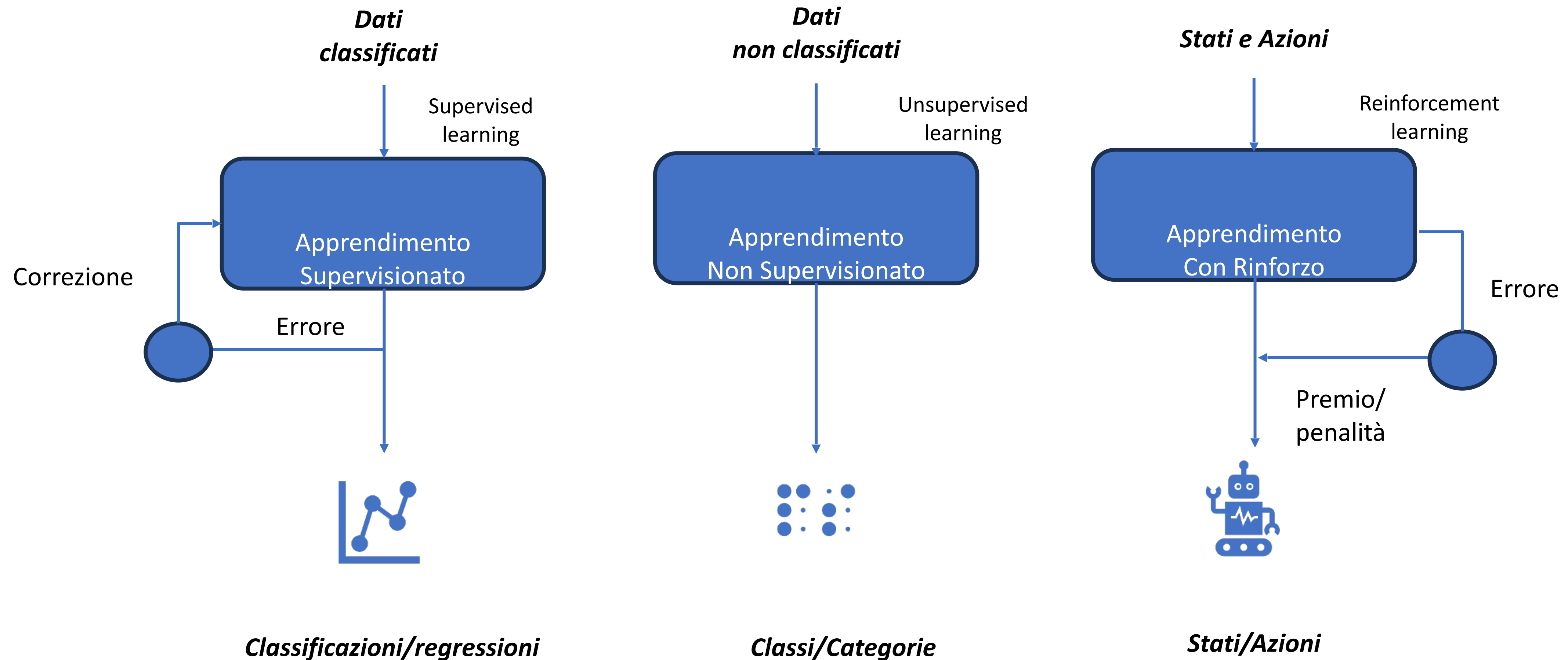
L'addestramento è un processo di ottimizzazione. La rete confronta il suo output con i "valori attesi", calcola un "Errore" e usa la backpropagation per aggiornare i pesi e ridurre l'errore.

- **Underfitting:** Il modello è troppo semplice, non cattura il trend dei dati.
- **Good Fit:** Il modello generalizza bene.
- **Overfitting:** Il modello impara a memoria i dati di addestramento (incluso il rumore) e non è capace di generalizzare su nuovi dati.

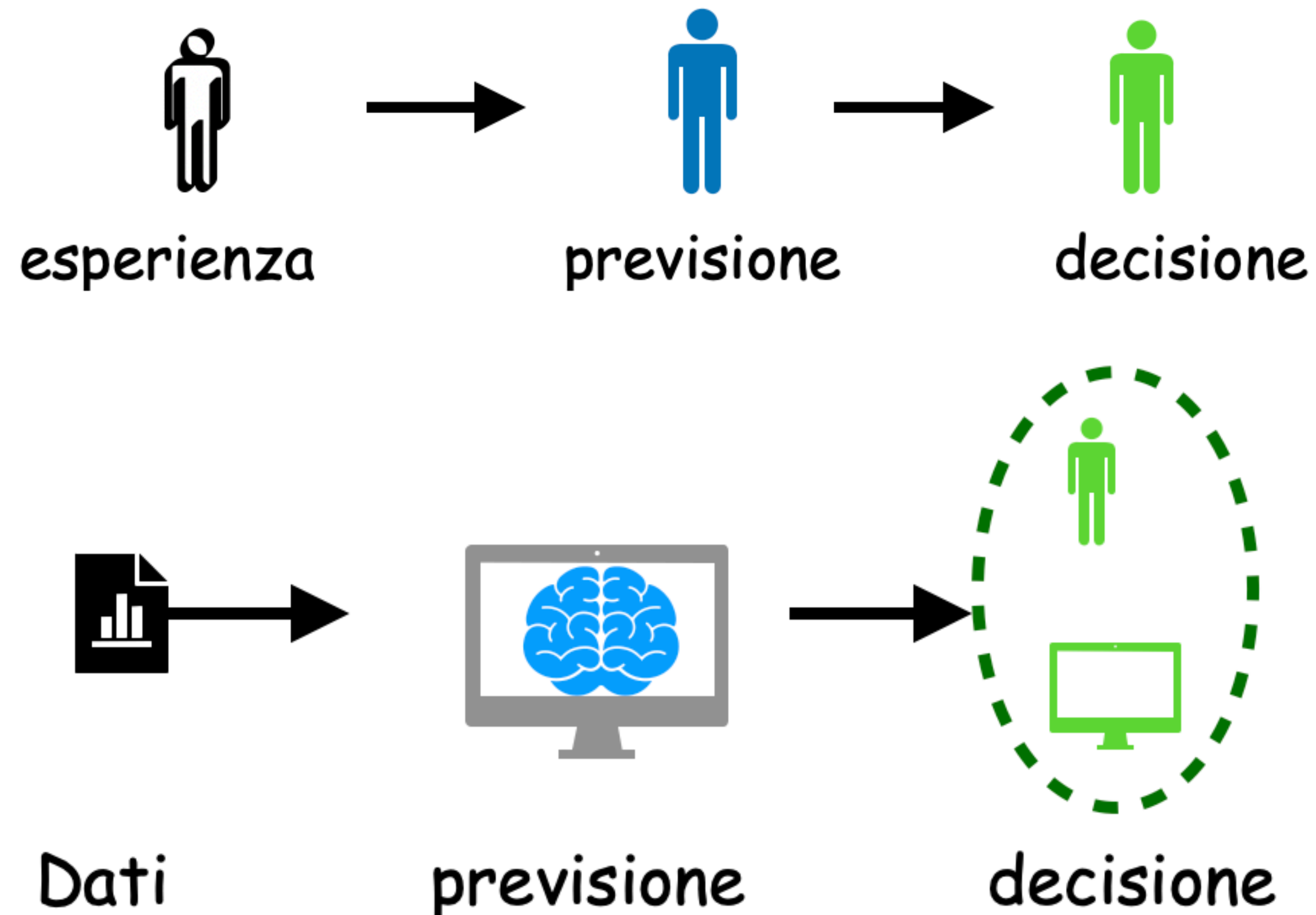


Le metodologie per l'apprendimento nell'IA

Sono le metodologie più diffuse in campo industriale



Apprendimento automatico



l'apprendimento automatico è semplicemente imparare dai dati e trasformarli in previsioni.

Proprio come impariamo dall'esperienza, la macchina impara dai dati

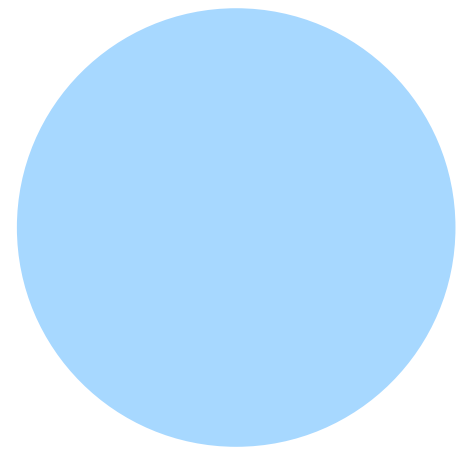
Da "Intelligenza Artificiale per le professioni" stesso autore

Il Machine Learning è il cuore dell'intelligenza artificiale moderna, permettendo di estrarre “insight” dai dati e supportare decisioni intelligenti.

Conoscere gli algoritmi principali è fondamentale per ogni Data Scientist: consente di costruire modelli predittivi robusti, interpretare fenomeni complessi e sviluppare sistemi intelligenti capaci di adattarsi a problemi reali.

Dall'apprendimento supervisionato al rinforzo, ogni paradigma offre strumenti potenti per trasformare i dati in valore concreto.



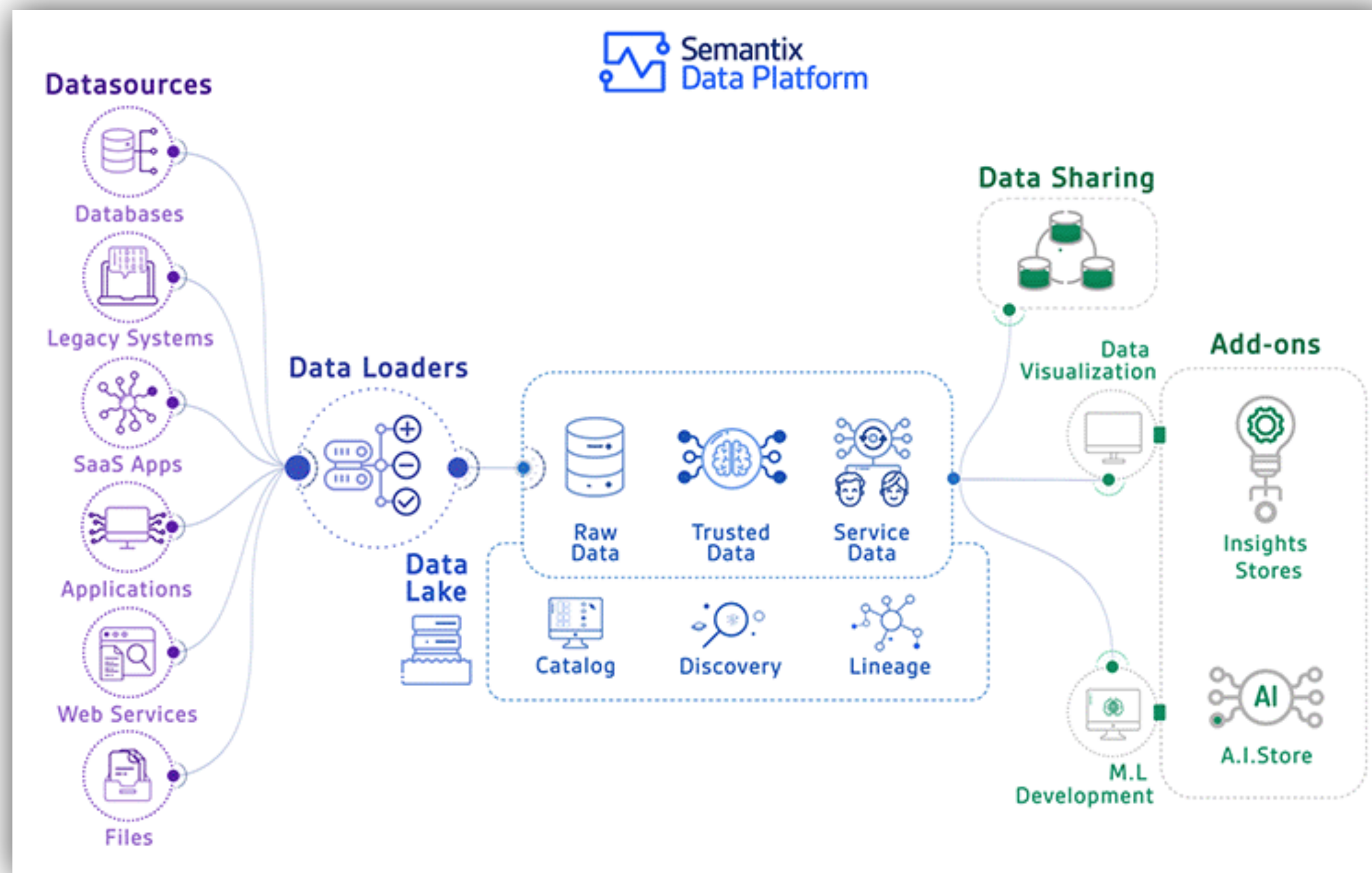


PERCHÉ CONOSCERE GLI ALGORITMI?

1. Costruire modelli predittivi robusti: padroneggiare gli algoritmi di Machine Learning ti permette di sviluppare soluzioni affidabili per classificazione, regressione e previsione su dati reali.
 2. Scoprire pattern nascosti e rilevare anomalie: tecniche non supervisionate e di rilevamento anomalie consentono di estrarre insight preziosi e migliorare la qualità dei dati.
 3. Creare sistemi intelligenti: una solida conoscenza degli algoritmi è la base per una carriera di successo in Data Science e AI, affrontando problemi reali con soluzioni innovative.
-

L'importanza della gestione dei dati in ingresso

Il tipo di dati disponibili e l'obiettivo determinano la modellazione del sistema con IA



MODELLAZIONE



- Selezione delle caratteristiche
- Selezione del tipo di modello
- Impostazione degli iperparametri
- Training del modello
- Validazione del modello
- Ottimizzazione del modello

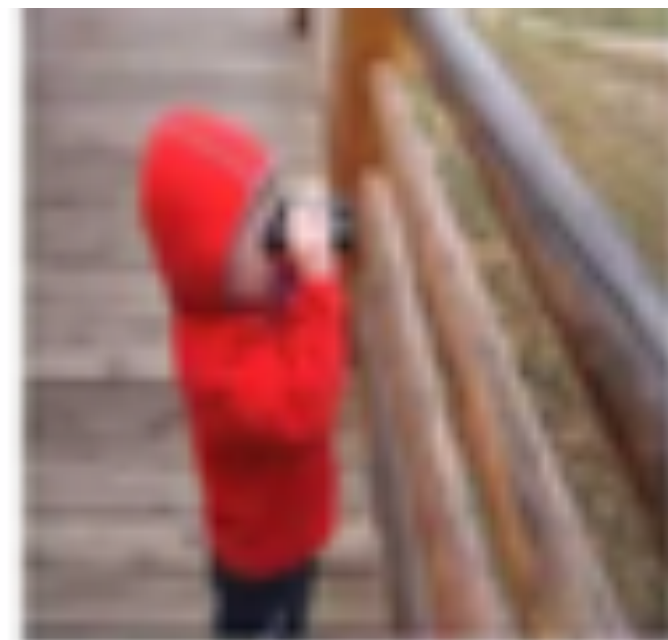
Web source - da seminario "Costruiamoci il futuro: l'uso dell'intelligenza artificiale nell'ingegneria e nell'industria" CNI Gennaio 2024

Criticità per la visione computerizzata

creare un **dataset** sufficientemente ampio per l'addestramento dell'algoritmo

insegnare all'algoritmo a comprendere l'immagine anche in presenza di **trasformazioni** (es. condizioni di luminosità non ottimale, deformazione o copertura parziale del soggetto, variazioni di scala) — —> IA generative

Bimbo con binocolo
Sotto la pioggia



Filtraggio di pixel
in archivio

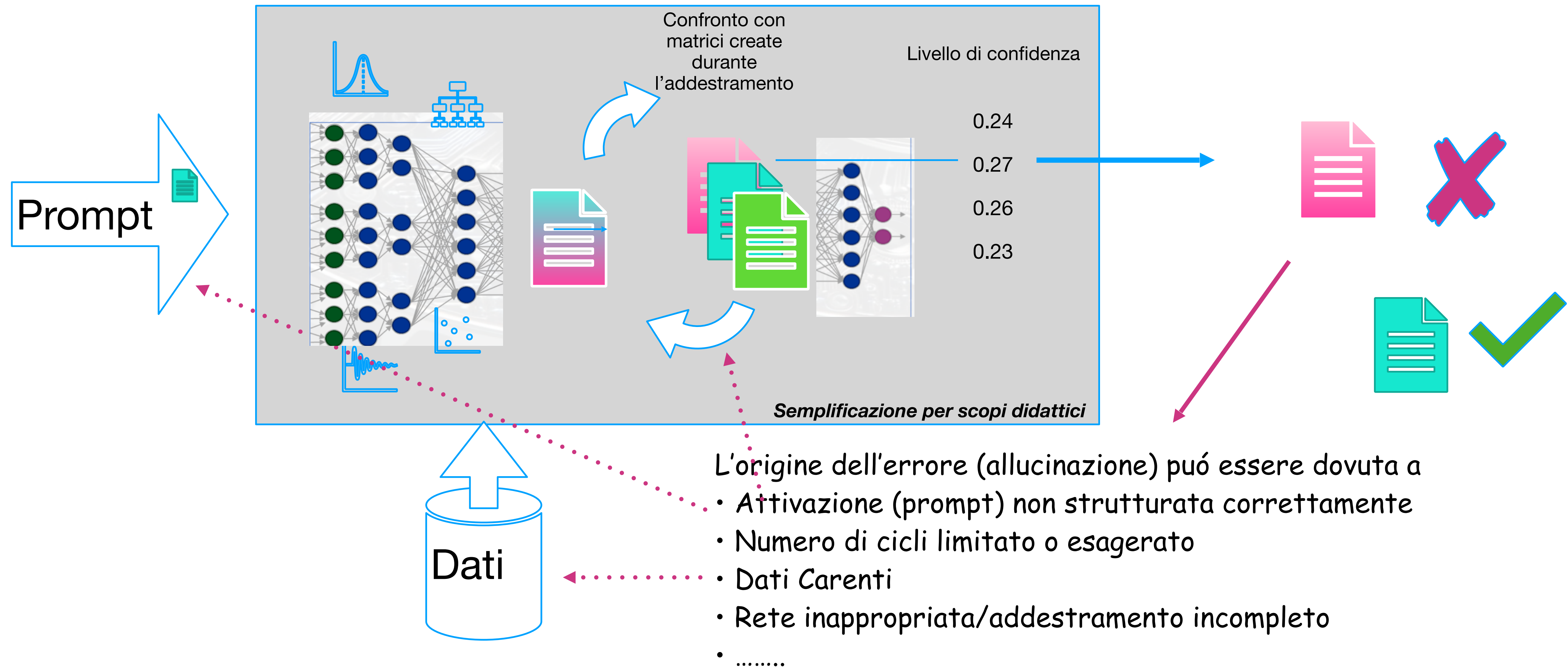


Bimbo confuso con
zoccolo rosso

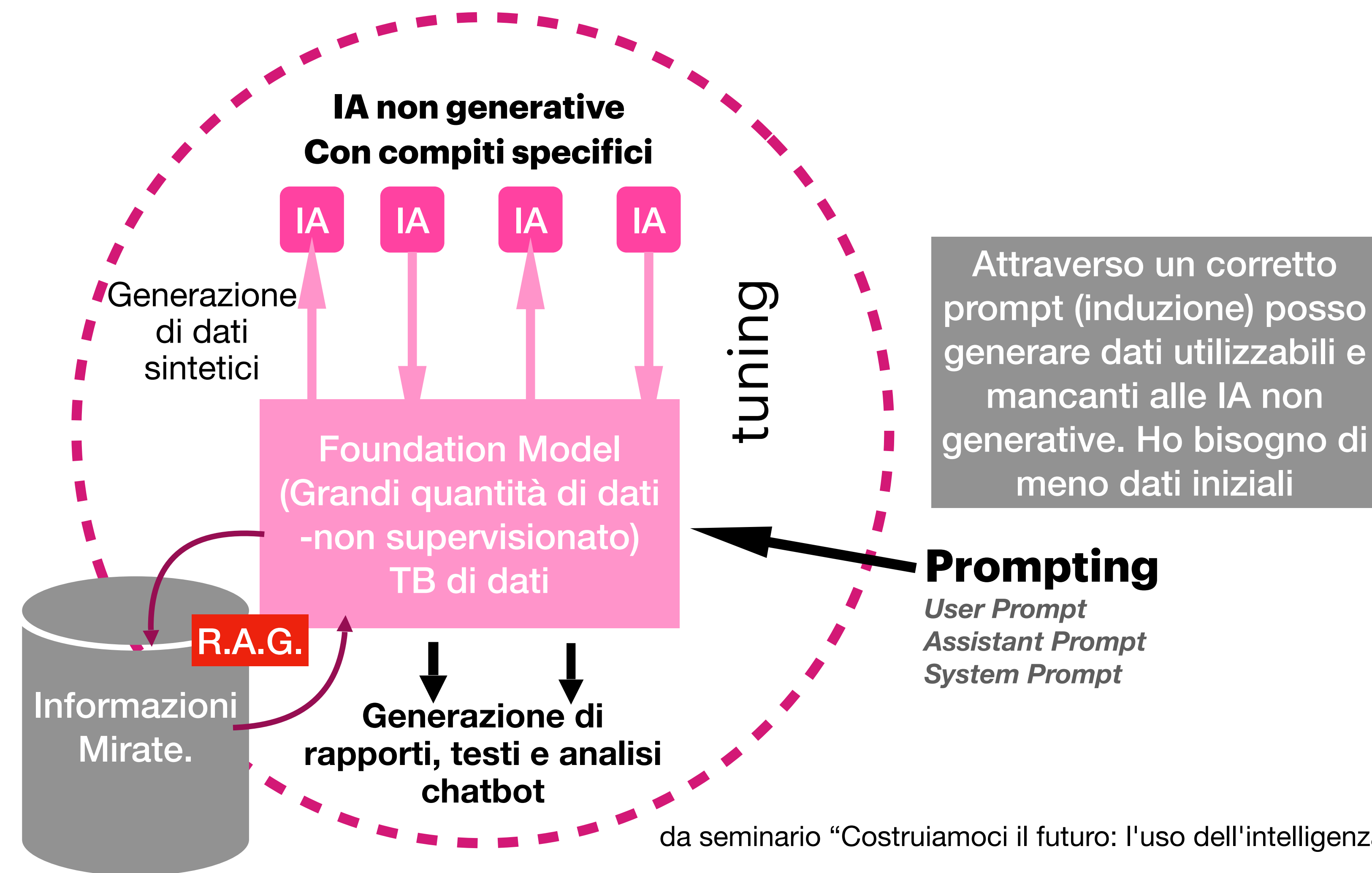


IA, statistica e allucinazioni

Determinazione dell'immagine o della prossima parola/frase del testo



La combinazione Gen/non Gen



Vantaggi

- Prestazioni
- Produttività

Svantaggi

- Costi computazionali
- Fiducia (allucinazioni)

Protezioni vs allucinazioni

- Tecniche RAG

Retrieval-Augmented Generation

da seminario "Costruiamoci il futuro: l'uso dell'intelligenza artificiale nell'ingegneria e nell'industria" CNI Gennaio 2024

R.A.G. = Retrieval Augmented Generation

Prompt Engineering



Zero-Shot

La richiesta viene data senza esempi.
L'IA deve capire il compito solo
dall'istruzione.



Few-Shot

Vengono forniti alcuni esempi (da 1 a
5) per mostrare all'IA il formato di
output desiderato.



Chain-of-Thought (CoT)

Si usano esempi che includono
domanda, risposta e lo schema di
ragionamento (i passaggi) per arrivare
alla risposta.

Le 5 componenti del prompt professionale per l'ingegnere

Struttura universale — adattabile a qualsiasi settore e tipo di elaborato

1**RUOLO**

Definisci chi sei e il contesto professionale

«Sei un ingegnere strutturale che assiste un professionista italiano iscritto all'Albo in un progetto di adeguamento sismico»

2**CONTESTO**

Il background specifico del progetto

«L'edificio è un capannone industriale anni 70 in zona sismica 2, categoria suolo C, con struttura in c.a. non duttile»

3**COMPITO**

Cosa vuoi esattamente — più preciso, più utile

«Redigi il paragrafo 4.1 della relazione di calcolo che descrive la strategia di intervento per l'adeguamento sismico»

4**VINCOLI**

Formato, lunghezza, norma, tono

«Stile tecnico formale, max 300 parole, cita NTC 2018 §7.4 e Circ. 2019, struttura in: obiettivo / approccio / interventi previsti»

5**OUTPUT**

Come vuoi ricevere la risposta

«Produci il testo del paragrafo direttamente inseribile nella relazione, senza preamble, con citazioni normative tra parentesi quadre»

Prompt debole vs prompt professionale: tre casi reali

Un prompt vago produce output inutile. Un prompt strutturato produce valore diretto.

ING. CIVILE — Relazione di calcolo sismica

✗ Prompt debole:

"Scrivi la relazione sismica dell'edificio"

✓ Prompt professionale:

"«Sei un ing. strutturale italiano. Edificio: c.a. anni 80, zona sismica 2A, suolo C, Vs30=280 m/s, uso: uffici. Redigi il par. 2.3 'Azione sismica di progetto' citando NTC 2018 §3.2.3 e Circ. Min. 2019 §C3.2. Max 200 parole, stile tecnico formale.»"

ING. INDUSTRIALE — Manuale tecnico macchinario

✗ Prompt debole:

"Scrivi il manuale del macchinario"

✓ Prompt professionale:

"«Sei un ing. meccanico italiano. Macchina: pressa idraulica 200t, PED 2014/68/UE, Dir. Macchine 2006/42/CE. Redigi §3.2 'Limiti d'uso', in italiano tecnico, max 150 parole, con tabella parametri (pressione max, temp. fluido, cicli/ora).»"

ING. GESTIONALE — Report KPI logistica

✗ Prompt debole:

"Analizza i dati di logistica e scrivi un report"

✓ Prompt professionale:

"«Sei un consulente logistico. Dati: lead time medio 4,2gg (target 3,5gg), OTD 87% (target 95%), rotazione scorte 8x (settore: 12x). Redigi par. 2 'Analisi scostamenti' per il CdA: max 200 parole, evidenzia le 2 priorità di intervento, stile executive summary.»"

- Ogni riferimento a prodotti e procedure nel prosieguo della presentazione ha un puro scopo didattico e non costituisce in nessun modo una loro comparazione e ancor meno una promozione nell'uso professionale

L'IA è già nel vostro software — probabilmente lo usate già

Esempi concreti per i tre profili · Classificazione AI Act inclusa

Software	Settore	Componente AI	Rischio AI Act
Autodesk Revit / BIM 360	CIVILE	Clash detection automatica, energy analysis predittiva, generazione layout strutturale con AI generativa	Basso
ETABS / SAP2000 AI modules	CIVILE	Ottimizzazione automatica sezioni, analisi modale con AI per strutture sismiche, verifica NTC assistita	Basso→Medio
Siemens TIA Portal / WinCC	INDUSTRIALE	Anomaly detection su PLC, manutenzione predittiva integrata, ottimizzazione automatica parametri di processo	Alto*
MATLAB / Simulink + ML Toolbox	INDUSTRIALE	Identificazione sistemi, controllo predittivo MPC, ottimizzazione parametri di regolazione automatica	Medio
SAP S/4HANA AI / Oracle SCM	GESTIONALE	Demand forecasting, ottimizzazione scorte, rilevamento anomalie nei processi di acquisto e logistica	Medio
Power BI / Tableau con AutoML	GESTIONALE	Dashboard predittive, anomaly detection su KPI, suggerimenti automatici di azioni correttive	Basso

* Siemens TIA su infrastrutture critiche (reti elettriche, impianti produzione continua) → Allegato III AI Act, alto rischio con obblighi specifici

ORA 1

Mappa dei dati sensibili e governance

Non tutti i dati sono uguali. Sapere quale dato può andare in cloud e quale deve restare off-line è il primo atto di governance professionale.

- Classificazione dei dati tecnici per livello di sensibilità
- Il Registro dei Trattamenti GDPR come strumento attivo (non solo adempimento)
- Policy interna per l'uso degli strumenti AI: struttura in 5 articoli

CIVILE

Dati strutturali · Geotecnica · Vulnerabilità edifici · Cantiere

INDUSTRIALE

Codici PLC · Layout impianto · Parametri processo · Segreto ind.

GESTIONALE

Dati ERP · Contratti logistici · KPI aziendali · Offerte gara

I dati del vostro studio: cosa è davvero sensibile?

Non tutti i dati richiedono lo stesso livello di protezione — sapere la differenza protegge voi e il committente

DATI PERSONALI — GDPR art. 4

- ✗ Dati anagrafici di committenti, lavoratori, residenti coinvolti nel progetto
- ✗ Immagini da telecamere di cantiere con volti o targhe identificabili
- ✗ Dati GPS di lavoratori o mezzi con orari e percorsi ricostruibili
- ✗ Dati biometrici di accesso a cantieri o impianti produttivi

DATI RISERVATI CONTRATTUALI

- ✗ Offerte economiche, prezzi unitari, stime di commessa sotto NDA
- ✗ Elaborati tecnici coperti da clausole di riservatezza contrattuale
- ✗ Documentazione di gara in corso (pre-aggiudicazione)
- ✗ Verbali riservati con enti pubblici o committenti privati

DATI TECNICI A RISCHIO SPECIFICO

- ✗ Codici sorgente PLC e SCADA, parametri di processo produttivo riservati
- ✗ Layout precisi di impianti critici (energetici, idrici, infrastrutture)
- ✗ Vulnerabilità strutturali rilevate in sopralluogo e non ancora risolte
- ✗ Planimetrie con sistemi di sicurezza non ancora approvati o pubblicati

DATI NON SENSIBILI — liberi per AI cloud

- ✓ Norme e riferimenti tecnici pubblici (NTC, Eurocodici, ISO, UNI)
- ✓ Dati aggregati e anonimizzati di misura senza riferimenti identificativi
- ✓ Testi descrittivi tecnici senza luoghi, persone o commesse identificabili
- ✓ Template e modelli di relazione non ancora compilati con dati reali

Il Registro dei Trattamenti: da adempimento a mappa operativa

Con l'AI, il Registro non è più un documento annuale: diventa la bussola per decidere cosa va in cloud e cosa no

Trattamento	Piano AI	Uso principale	Dati ammessi	Dati vietati	Resp.
Relazioni tecniche strutturali	Claude Teams	Redazione, analisi normativa NTC	Testi anonimizzati, norme pubbliche	Vulnerabilità strutturali, dati catastali ID	[Ing.]
Verifica normativa NTC/EC	Claude Projects	Verifica conformità articoli	Testi normativi pubblici, descrizioni	NDA, dati progetto identificativi	[Ing.]
Gestione documentale commessa	Claude Teams MCP	Ricerca semantica, versioning	Documenti commessa (Teams DPA)	Offerte economiche, documenti gara	[Ing.]
Codice PLC e parametri processo	Ollama locale	Analisi, commenti, refactoring	Qualsiasi (rimane in locale)	Non applicabile — tutto off-line	[Ing.]
Report KPI logistica/produzione	Gemini Workspace	Dashboard, sintesi, analisi	KPI aggregati anonimizzati	Dati personali lavoratori, segreto ind.	[Ing.]
Immagini cantiere/impianto	SLM locale o anon.	Analisi visiva, documentazione	Solo dopo anonimizzazione volti/targhe	Immagini con persone/targhe ID	[Ing.]
[Aggiungere...]					

Policy interna AI: struttura in 5 articoli

Una pagina, firmata dal titolare/responsabile, distribuita a tutti i collaboratori — non un documento da archiviare

Art. 1 — Strumenti autorizzati

Claude.ai Teams, Gemini for Workspace Business+, Ollama locale. Ogni strumento non in elenco richiede autorizzazione scritta del Responsabile AI prima dell'uso su commesse reali.

Art. 2 — Dati non inseribili in cloud AI

Codici PLC/SCADA e parametri di processo riservati · Documenti sotto NDA · Vulnerabilità strutturali non risolte · Layout impianti critici · Offerte economiche · Dati personali non anonimizzati · Documenti di gara in corso.

Art. 3 — Anonimizzazione obbligatoria

Prima di caricare qualsiasi documento su strumenti cloud AI: sostituire nomi propri con [COMMITTENTE-XX], coordinate con [SITO-XX], codici commessa con [COMMESSA-XX], dati identificativi con codici neutri. Il professionista attesta l'avvenuta anonimizzazione.

Art. 4 — Log e supervisione

Ogni output AI usato in un elaborato firmato deve essere registrato nel Log AI di commessa (strumento, data, input sintetico, revisore). La firma dell'elaborato attesta la supervisione umana ai sensi dell'AI Act art. 14.

Art. 5 — Formazione e aggiornamento

Ogni collaboratore completa il percorso di alfabetizzazione AI (o equivalente) prima di usare strumenti AI su commesse reali. Il Registro IA e la Policy sono aggiornati entro 30 giorni dall'adozione di ogni nuovo strumento.

Non basta scegliere lo strumento giusto: va configurato correttamente prima di usarlo su dati professionali

Claude.ai Teams / Enterprise

- ✓ Zero training sui dati: i prompt non vengono usati per addestrare il modello
- ✓ DPA (Data Processing Agreement) incluso nel contratto Teams/Enterprise
- ✓ Retention dati: 30 giorni di default, configurabile su Enterprise fino a zero
- ✓ API Anthropic: zero retention per default — migliore per workflow automatizzati
- ✗ Claude free e Pro consumer: dati su server USA, possibile uso per training — NON usare per dati professionali

Azione
impostazioni:
Settings → Privacy →
Disattiva 'Use my
data to train Claude'
(solo su Teams/
Enterprise)

Google Gemini for Workspace Business+

- ✓ Data residency EU configurabile: EU Processing Add-on disponibile su Business/Enterprise
- ✓ Zero training: i dati Workspace non vengono usati per il training del modello base
- ✓ DPA incluso nel contratto Google Workspace — verificare versione e data di firma
- ✓ Separazione account: Gemini Advanced personale non accede ai dati Workspace aziendali
- ✗ Gemini consumer (account Google personale): NESSUN DPA, zero garanzie — mai per dati professionali

Azione
impostazioni:
Google Admin
Console → Dati e
Privacy → attivare
'Gemini for
Workspace' con DPA
verificato

Regola d'oro: leggere il DPA del proprio fornitore PRIMA di caricare i dati di una commessa. Se non c'è DPA — non usare per dati professionali.

Confronto tra Motori di Ricerca e IA Generativa

Caratteristica	Motori di Ricerca	AI Generativa
Tipo di output	Link a pagine web esistenti	Testo, immagini o codice generato
Fonte dei dati	Indicizzazione del web	Modelli addestrati su dataset preesistenti
Aggiornamento	Quasi in tempo reale	Dipende dall'addestramento o accesso ad API
Elaborazione della richiesta	Ricerca parole chiave e ranking	Comprensione semantica e generazione

Confronto tra alcuni chatbot con IA e alcuni motori di ricerca con IA

Ogni strumento è progettato per scopi specifici:

Perplexity AI eccelle nella ricerca rapida,

NotebookLM nella gestione delle note personali,

ChatGPT nella versatilità conversazionale

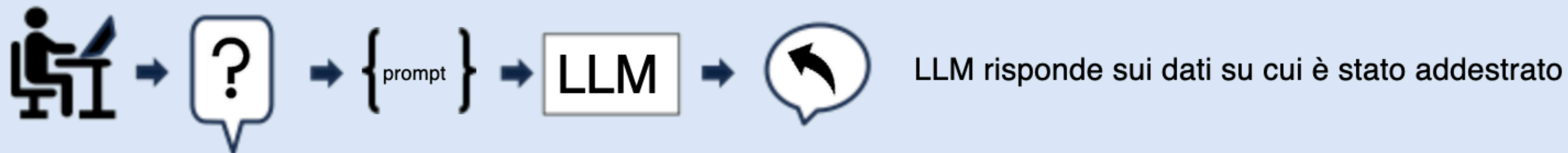
Gemini punta a combinare creatività con analisi avanzata.



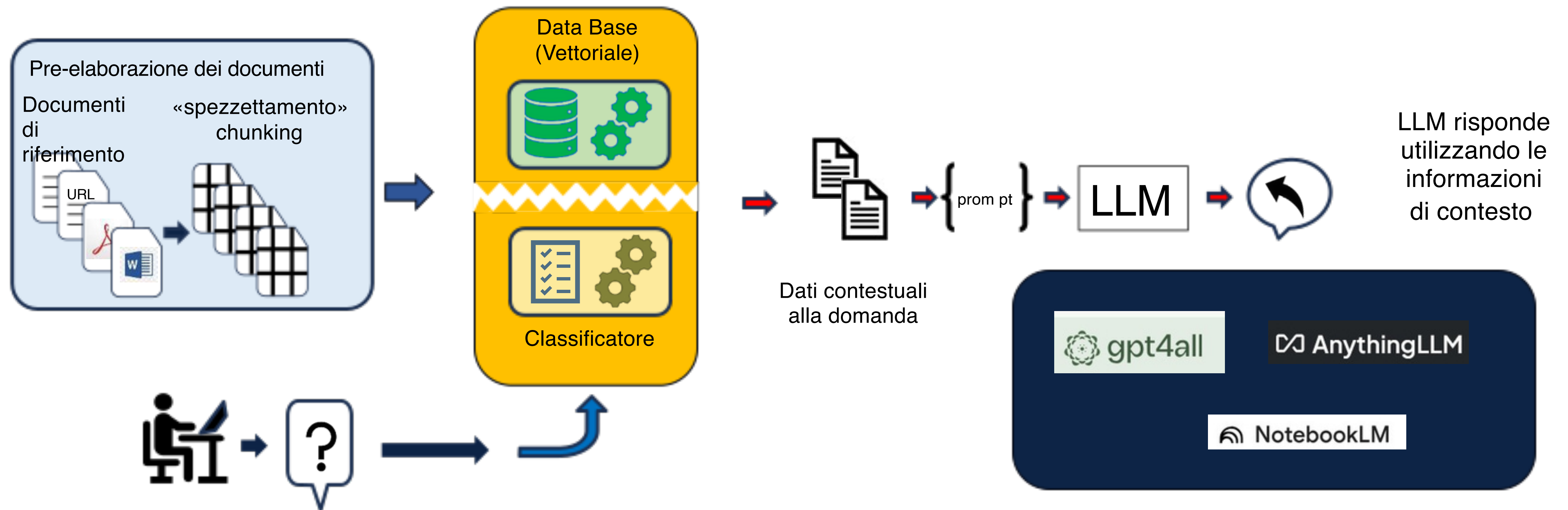
Confronto Principale				
Caratteristica	Perplexity AI	NotebookLM	ChatGPT	Gemini
Tipo di utilizzo	Ricerca conversazionale	Gestione delle note	Conversazioni generali	Conversazioni + analisi
Fonti aggiornate	Sì	Solo dati utente	Statiche/dinamiche	Sì
Personalizzazione	Limitata	Alta	Media	Alta
Applicazioni principali	Informazione rapida	Organizzazione documenti	Generazione testi	Creatività + analisi

Per assicurarsi risposte appropriate - Retrieval Augmented Generation

Interrogazione di LLM canonica



Interrogazione di LLM tramite RAG



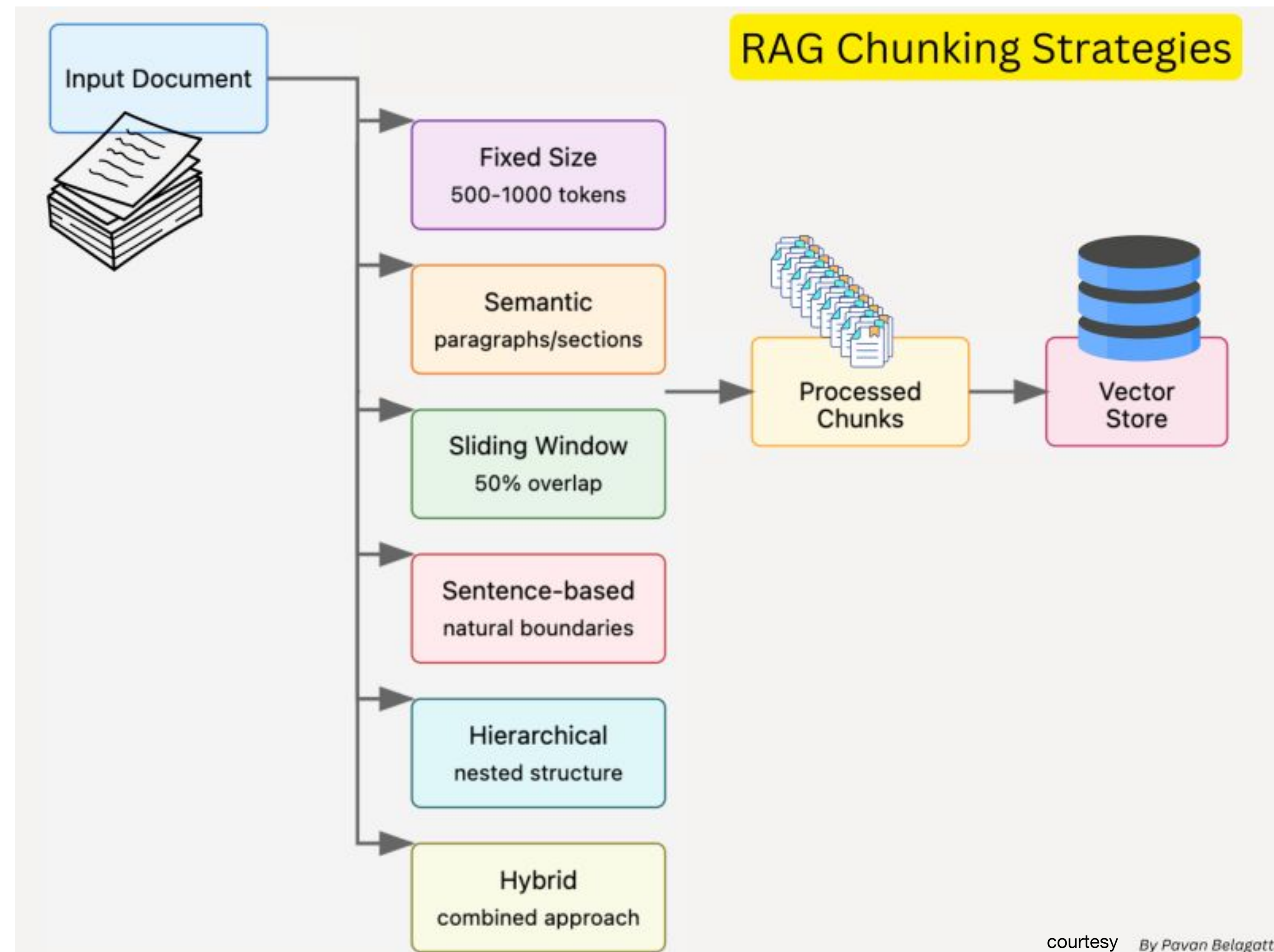
Tecniche di frammentazione per RAG

Funzionamento base: I sistemi RAG cercano in "chunks" (frammenti) di documenti anziché in documenti interi per trovare informazioni rilevanti.

Vantaggi del chunking: Migliora efficienza e precisione del recupero delle informazioni, accelerando il processo e migliorando la qualità delle risposte.

Limitazioni delle strategie base: Il chunking ingenuo che divide il testo in frammenti di dimensione fissa non è sempre efficace.

Processo finale: I frammenti elaborati vengono vettorizzati e memorizzati in database vettoriali per un recupero efficiente durante la fase di generazione.



courtesy By Pavan Belagatti

Caratteristica / Criterio	AnythingLLM	NotebookLM (Google)
Natura del Software	Piattaforma open-source focalizzata su privacy, multi-utenza ed esecuzione locale.	Web app cloud-native sviluppata da Google, ottimizzata per lo studio e la ricerca basata su fonti.
Privacy e Sicurezza dei Dati	Totale (Local-first): i dati possono risiedere interamente sul tuo dispositivo o su un server di tua proprietà (Self-hosted). Nessun dato viene inviato a terzi se si usano modelli locali.	Cloud Google: i dati risiedono sui server cloud di Google. Per gli account Workspace i dati non vengono usati per l'addestramento dei modelli, ma non è una soluzione offline o "air-gapped".
Modelli Linguistici (LLM)	Estremamente flessibile: supporta decine di provider. Puoi usare modelli locali via Ollama/LM Studio (Llama, Mistral, ecc.) o API cloud (OpenAI, Anthropic, Gemini, DeepSeek, ecc.).	Esclusivo Google Gemini: utilizza nativamente i modelli avanzati della famiglia Gemini messi a disposizione da Google (senza possibilità di cambiarli o eseguirli in locale).
Gestione dei Documenti	Illimitata: organizza i file in <i>Workspace</i> isolati. Accetta PDF, DOCX, TXT, fogli di calcolo, presentazioni, codice sorgente, audio (con trascrizione) e scraping web.	Basata su Notebook (fino a 50 fonti per taccuino): accetta PDF, Google Docs/Slides, link web, video YouTube e testo copiato.
Database Vettoriale	Configurabile: usa nativamente LanceDB (integrato), ma permette di passare a Pinecone, Chroma, Milvus, Qdrant, Weaviate, ecc.	Gestito internamente da Google: l'utente non deve configurare né gestire alcun database vettoriale.
Funzioni di Sintesi e Studio	Focalizzato su chat avanzate, flussi di agenti (Agent Flows), comandi rapidi e integrazione con strumenti esterni (es. protocollo MCP).	Molto avanzate per l'apprendimento: genera automaticamente panoramiche audio (Podcast AI), panoramiche video, guide allo studio, FAQ e mappe mentali.
Utilizzo Offline	Sì: l'app desktop funziona completamente offline se abbinata a un motore locale come Ollama.	No: richiede una connessione a Internet attiva essendo un servizio basato su cloud.

Quando scegliere l'uno o l'altro?

- **AnythingLLM se:** necessità assoluta di mantenere i dati offline o sui tuoi server, vuoi testare diversi modelli open-source (es. Llama o Mistral) senza costi di API, o desideri costruire agenti di automazione e flussi di lavoro. [anythingllm.com+ 1](#)
- **Scegli NotebookLM se:** obiettivo principale è studiare, fare ricerche, riassumere grandi volumi di documenti accademici o aziendali e desideri sfruttare strumenti unici come la generazione automatica di podcast audio interattivi senza doverti preoccupare della configurazione tecnica.

DAL PROMPT ENGINEERING AL CONTEXT ENGINEERING

Il nuovo paradigma dell'intelligenza artificiale

Come il modo di progettare l'AI sta
cambiando radicalmente il futuro del
lavoro





PERCHÉ STIAMO CAMBIANDO PARADIGMA

Il prompt engineering ha rappresentato il primo passo nell'interazione con i modelli AI. Tuttavia, istruzioni singole e isolate non bastano più: i sistemi moderni richiedono contesti ricchi, strutturati e dinamici. L'evoluzione verso il Context Engineering nasce dalla necessità di superare i limiti di approcci troppo semplici, per ottenere risposte più precise, coerenti e realmente utili.

DAL PROMPT AL CONTESTO

Un cambio di paradigma fondamentale:
dall'istruzione singola alla costruzione
di ambienti informativi ricchi e
strutturati.



L'Era del Prompt Engineering

Si scrivevano istruzioni precise e dettagliate per guidare il modello. Il focus era sulla formulazione della domanda giusta.



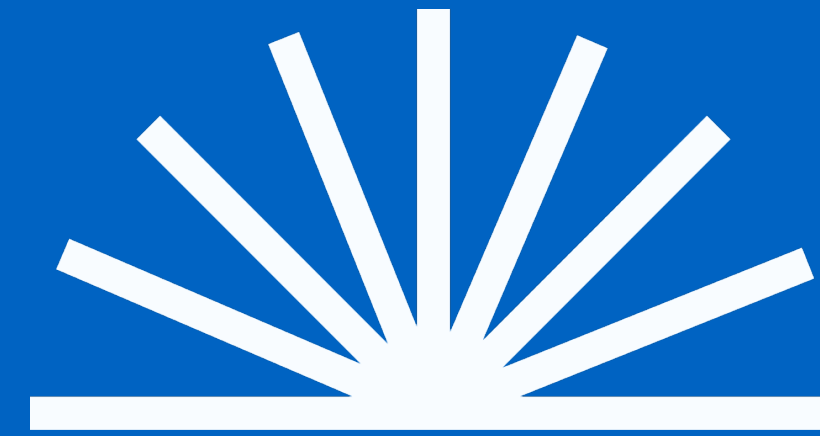
Il Limite dell'Approccio Classico

I prompt singoli non bastano per task complessi: manca memoria, contesto aziendale, dati aggiornati e regole specifiche.



La Svolta: Context Engineering

Oggi si progetta l'intero ecosistema informativo che circonda il modello: documenti, esempi, memoria e strumenti integrati.



CONTEXT ENGINEERING

Il Context Engineering è la disciplina che consiste nel progettare e strutturare l'ambiente informativo completo fornito a un modello AI. Non si tratta solo di scrivere un prompt: significa costruire un sistema coerente di istruzioni, dati, esempi, memoria e regole che guidano il comportamento dell'AI in modo preciso, affidabile e scalabile.

COMPONENTI DEL CONTESTO



DOCUMENTAZIONE



Manuali, guide e specifiche tecniche

ESEMPI & MEMORIA



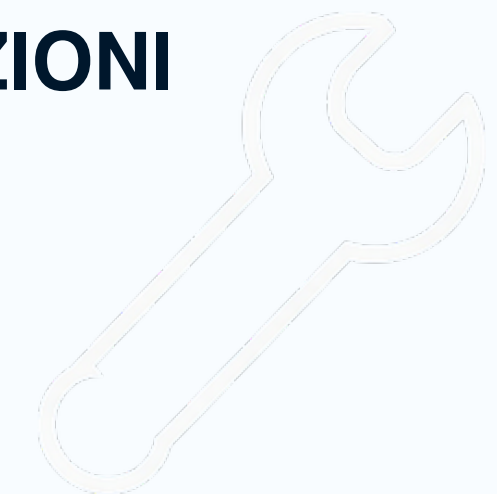
Few-shot examples e storico conversazioni

REGOLE & DATI



Vincoli, policy e dati strutturati

TOOL & INTEGRAZIONI



API, funzioni e sistemi esterni

PERCHÉ ORA

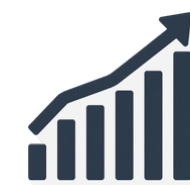
Le soluzioni IA. richiedono precisione, coerenza e scalabilità.

Il Context Engineering è la risposta a queste esigenze.



Precisione e Affidabilità

Un contesto ben strutturato riduce errori e allucinazioni, rendendo le risposte dell'AI coerenti e verificabili.



Scalabilità dei Sistemi con IA

Gestire il contesto in modo sistematico consente di scalare le soluzioni AI su processi complessi e team distribuiti.



Vantaggio Competitivo Reale

Le aziende che padroneggiano il Context Engineering ottengono risultati superiori, riducendo costi e tempi di sviluppo.



IL FUTURO APPARTIENE A CHI SA PROGETTARE IL CONTESTO



Non basta scrivere prompt



Progetta il contesto. Guida l'AI.



Dal Prompt al Context Engineering

Concetto di *Reasoning* nell'Intelligenza Artificiale

Il ragionamento (*reasoning*) è il processo attraverso il quale un'IA analizza informazioni e genera inferenze logiche. Esistono diversi tipi di reasoning:

- **Deduttivo**: parte da regole generali per arrivare a conclusioni specifiche.
- **Induttivo**: parte da esempi specifici per formulare regole generali.
- **Abduttivo**: cerca la spiegazione più probabile per un'osservazione.



Dai LLM agli agenti - caratteristiche e differenze

LLM

L'utente fornisce un input (un "prompt") e il modello genera un output

- **Mancanza di accesso a dati privati:** Gli LLM non hanno accesso intrinseco ai dati personali dell'utente (calendari, email, file), a meno che non venga loro concesso esplicitamente attraverso integrazioni o strumenti specifici collegati.
- **Natura passiva:** Questi modelli sono reattivi. Attendono un input diretto dall'utente per attivarsi e generare una risposta. Non agiscono di propria iniziativa.

Flussi - RAG

flussi di lavoro AI, spesso definiti "*AI Workflows*". Aggiunta di livello di istruzione e automazione.

esegue una sequenza di passaggi specifici, definiti esplicitamente dall'utente o dallo sviluppatore. Questo insieme di istruzioni passo-passo è noto come "logica di controllo"

è l'essere umano a prendere tutte le decisioni sulla struttura del processo, sugli strumenti da utilizzare e sull'ordine delle operazioni.

Esempio: Retrieval Augment Generation - RAG nei chatbot di relazione cliente

AGENTE

Agisce collegando gli strumenti necessari (es. fogli di calcolo, motori di ricerca, altri modelli AI). Deve

- **Ragionare:** Qual è il modo migliore per raccogliere informazioni rilevanti? Quale strumento è più adatto,?
- **Agire:** Quale modello AI da usare per effettuare il compito? Ho bisogno di altro? Quale modello è migliore per questo compito specifico?".

Il modello deve pensare al prossimo passo logico e poi eseguirlo autonomamente. Spesso secondo la sequenza Reason Act

caratteristica distintiva degli agenti è **l'iterazione**



L'uso di agenti con l'IA

I LLM generano output basandosi sugli input ricevuti, senza iniziativa autonoma o persistenza.

IA agentic

L'IA basata sugli agenti è più autonoma e proattiva:

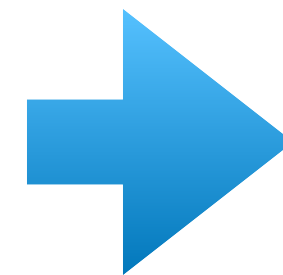
- **Autonomia decisionale:** può decidere quali azioni intraprendere per raggiungere un obiettivo
- **Persistenza:** mantiene uno stato e una memoria nel tempo tra diverse interazioni
- **Pianificazione:** elabora strategie multi-step per completare compiti complessi
- **Uso di strumenti:** interagisce attivamente con software, API, database e altri strumenti esterni
- **Apprendimento continuo:** migliora le proprie capacità in base ai feedback e alle esperienze
- **Iniziativa:** può avviare azioni e conversazioni quando appropriato
- **Adattamento:** modifica il proprio comportamento in base al contesto e ai cambiamenti dell'ambiente

Agenti di cosa parliamo

Di fatto

Definizione di Agente Autonomo

- Un agente IA è un sistema che agisce in modo indipendente con la possibilità di prendere decisioni autonome per raggiungere obiettivi
 - Si distingue dai chatbot reattivi
 - Proattivo
 - indipendenza decisionale.



Uso Strategico degli Agenti

- Contesti specifici caratterizzati da decisioni complesse,
- regole intricate o dati non strutturati,
- Richiesta di una valutazione mirata dei casi d'uso.

- Sono **applicazioni** che utilizzano **modelli di IA generativa** per agire verso degli obiettivi, utilizzando strumenti e interagendo con il mondo.
- **Ricevono un obiettivo** dall'utente e ragionano su come raggiungerlo, utilizzando strumenti e interagendo con il mondo.
- Hanno una **varietà di strumenti a loro disposizione** e possono ragionare su come utilizzarli.
- Possono **risolvere problemi oltre le capacità di un tipico LLM**, analizzando situazioni e prendendo decisioni informate.
- Sono **adattivi, auto-diretti** e capaci di gestire flussi di lavoro complessi.

Sistemi Multiagenti

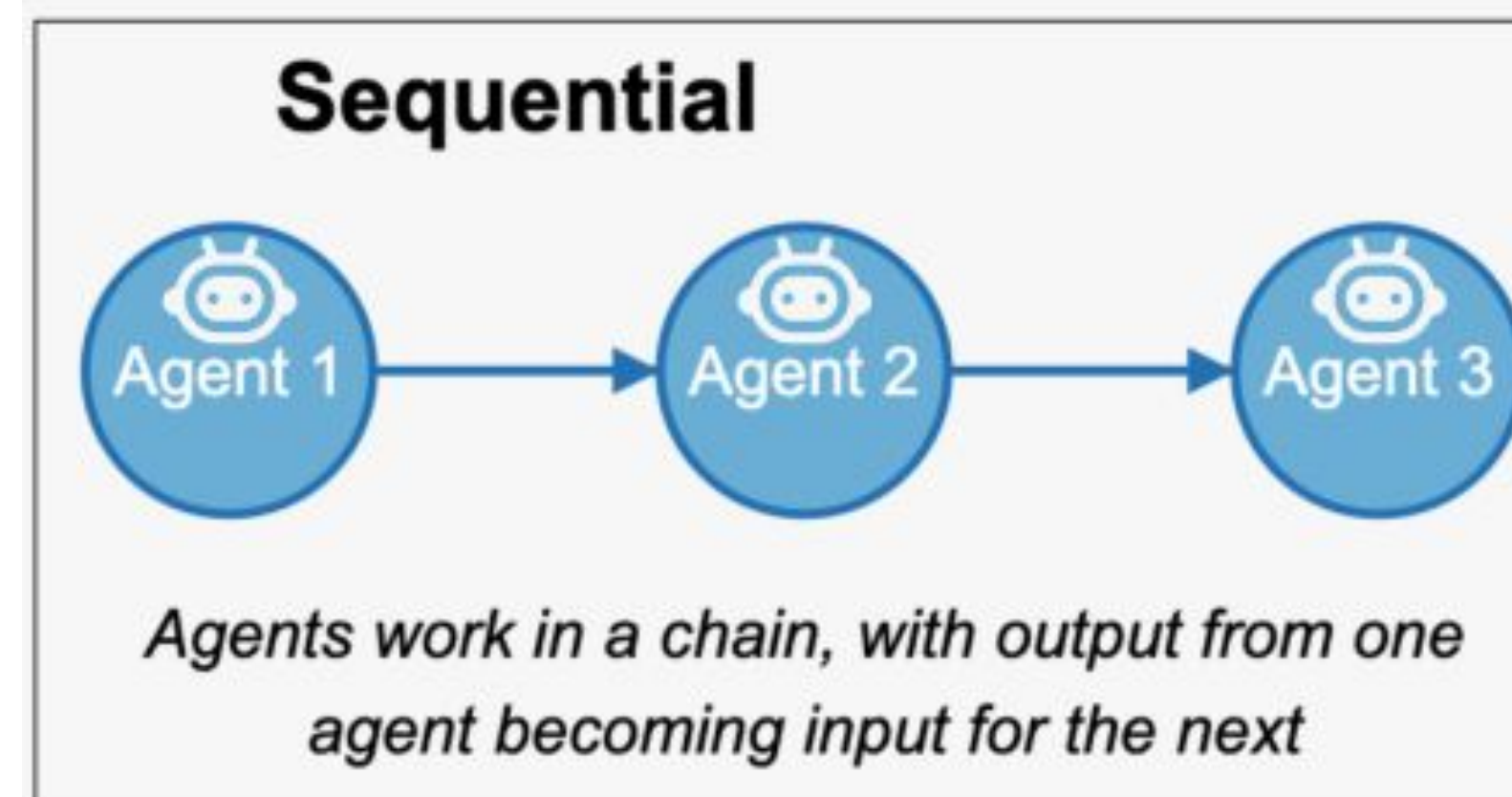
Definizione: Un Sistema Multi-Agente è costituito da un gruppo di agenti (o "Crew") con competenze e capacità specializzate uniche.

Scopo: Gli agenti collaborano risolvendo compiti semplici per raggiungere insieme un obiettivo comune più complesso.

Comunicazione: Gli agenti interagiscono inviando l'output dei loro compiti ad altri agenti che lo utilizzano come base per il proprio lavoro.

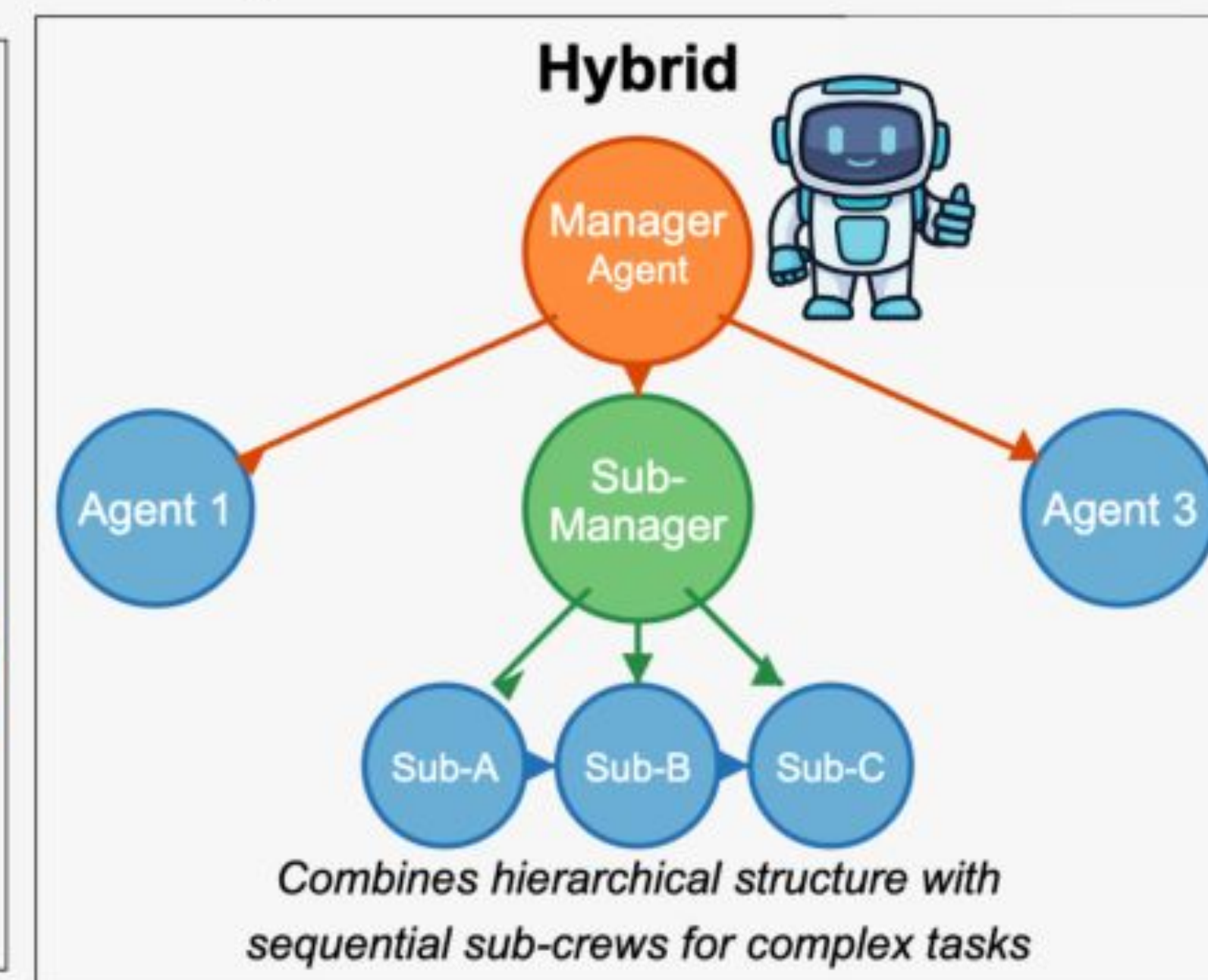
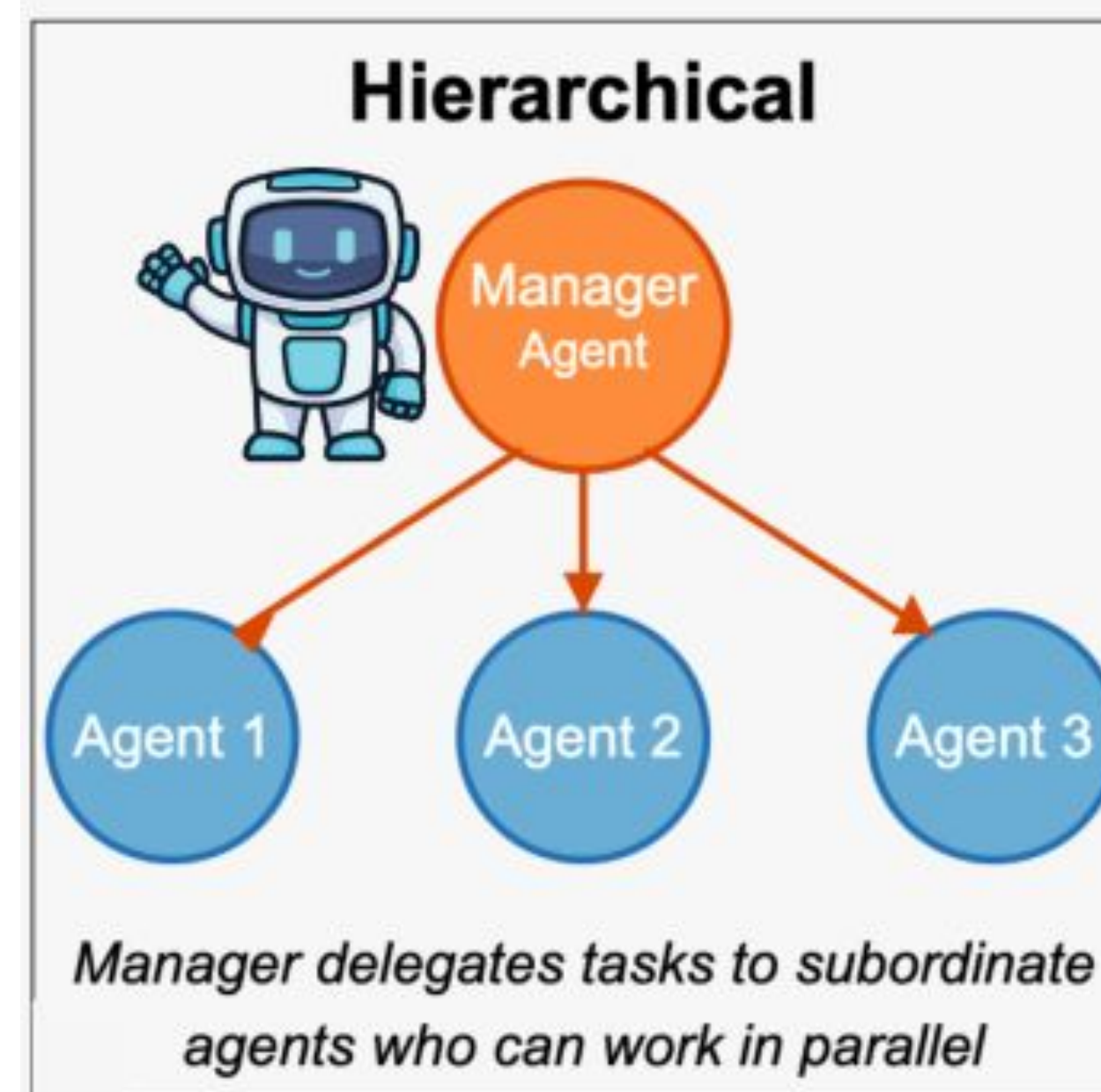
Strutture di organizzazione:

- **Sequenziale:** Gli agenti lavorano in catena, dove l'output di un agente diventa l'input del successivo
- **Gerarchica:** Comprende un manager e più subordinati; il leader pianifica e delega mentre i subordinati eseguono (consente l'esecuzione simultanea di compiti)
- **Ibrida:** Combina elementi sequenziali e gerarchici, permettendo ad alcuni agenti di creare "sotto-crew" diventando leader di queste mentre rimangono subordinati nella crew originale



Multi-Agent System

Crew Structure Types



Strutture tipiche di IA basata su Agenti

Struttura	Caratteristiche Principali	Funzionamento	Esempio
Agenti Singoli	• Autonomi • Indipendenti • Specializzati	Operano autonomamente senza dipendere da altri sistemi	Assistenti virtuali (Siri, Alexa)
Agenti Multi-Componente	• Modulari • Integrati • Specializzati per funzione	Combinano moduli specializzati in un sistema unificato	Claude Code (pianificazione, coding, debugging)
Multi-Agenti Cooperativi	• Collaborativi • Comunicativi • Orientati all'obiettivo comune	Si dividono compiti complessi in sotto-compiti	Sistemi di ricerca scientifica automatizzata
Multi-Agenti Competitivi	• Competitivi • Adattivi • Auto-migliorativi	Interagiscono in modo competitivo per ottimizzare performance	Trading algoritmico nei mercati finanziari
Reti Gerarchiche	• Struttura piramidale • Coordinamento centralizzato • Esecuzione distribuita	Agenti di livello superiore coordinano quelli inferiori	Sistemi di gestione supply chain
Architetture Ibride Uomo-AI	• Collaborativi con umani • Complementari • Supervisionati	L'umano guida strategicamente mentre l'AI esegue operazioni specifiche	Sistemi di supporto decisionale in medicina

Perché l'Autonomia è Fondamentale

- **Ambiente aziendale globale:** velocità, complessità, incertezza
- Limitazioni dei sistemi tradizionali: supervisione umana costante
- Vantaggi degli agenti autonomi:
 - Decisioni contestuali senza intervento umano
 - Adattamento in tempo reale
 - Coordinamento tra dipartimenti



Come funziona un agente con IA: il ciclo percezione → azione

Non è magia: è un ciclo che si ripete — e il professionista deve sapere dove può intervenire



↻ se l'obiettivo non è raggiunto: ricomincia dal passo 1 — autonomamente, senza chiedere approvazione

ING. CIVILE — Agente verifica normativa NTC

PERCEPISCE → legge le tavole strutturali della commessa · PIANIFICA → identifica gli articoli NTC 2018 applicabili · AGISCE → verifica paragrafo per paragrafo e genera il report di conformità · VERIFICA → controlla che tutti i requisiti siano stati analizzati, altrimenti segnala gap

ING. INDUSTRIALE — Agente anomaly detection su linea

PERCEPISCE → legge i log SCADA degli ultimi 7 giorni · PIANIFICA → identifica i parametri fuori tolleranza · AGISCE → genera alert per manutenzione preventiva con priorità e finestra temporale consigliata · VERIFICA → confronta con storico degli interventi, aggiusta la priorità

ING. GESTIONALE — Agente report settimanale KPI

PERCEPISCE → scarica i dati ERP della settimana · PIANIFICA → calcola scostamenti vs target per ogni KPI · AGISCE → genera la bozza del report executive con grafici e commento automatico · VERIFICA → controlla che tutti i KPI richiesti siano presenti, invia email al team

AI Act art. 14: supervisione umana 'effettiva, non meramente formale'

Cosa significa concretamente per un ingegnere che usa un agente su un progetto professionale

Monitoraggio attivo

Non basta definire l'obiettivo e aspettare il risultato. Il deployer (voi) deve poter intervenire, modificare o fermare l'agente in qualsiasi momento durante l'esecuzione.

Stop di emergenza obbligatorio

Ogni agente in produzione deve avere un meccanismo di interruzione immediata. Chi può fermarlo? Come? In quanto tempo? Se non lo sapete — non è ancora pronto per l'uso professionale.

Log obbligatorio delle azioni

Ogni azione dell'agente deve essere registrata con timestamp. Il log non è un optional tecnico: è documentazione professionale che dimostra la supervisione richiesta dall'AI Act.

Revisione umana dell'output firmato

Per sistemi ad alto rischio: ogni output deve essere revisionato da un ingegnere prima di essere incluso in un elaborato firmato. La firma non è solo formalità — attesta la revisione.

CIVILE

Relazioni strutturali firmate: revisione umana sempre obbligatoria

INDUSTRIALE

Output SCADA su sicurezza impianto: log + stop di emergenza hardware

GESTIONALE

Report automatici per CdA: revisione prima della distribuzione

Responsabilità, log e laboratorio

*La domanda non è se l'agente sbaglierà. La domanda è:
chi risponde, come lo scoprite, e cosa fate — e poi costruiamolo insieme.*

- Tipologie di errori negli agenti: prevedibili e imprevedibili
- Responsabilità professionale e output AI: il quadro giuridico per l'ingegnere
- Il log come strumento di tutela professionale (non solo compliance)
- Lab no-code: costruite il vostro primo flusso agente dal vivo

CIVILE

Responsabilità DL · Collaudo con
AI · Fascicolo tecnico

INDUSTRIALE

Responsabilità fabbricante ·
Fascicolo CE · Manutenzione

GESTIONALE

Responsabilità logistica · SLA ·
Audit supply chain

Come sbaglia un agente con IA — e come accorgersene

Gli errori di un agente sono più insidiosi di quelli di un chatbot: avvengono in sequenza autonoma

Errore di input

L'agente legge un file malformato o dati fuori range. Produce analisi numericamente corrette su dati sbagliati.

Caso reale: Le misure di deformazione del sensore erano in millimetri, il file era in pollici. L'agente ha calcolato correttamente — su dati sbagliati. Errore scoperto alla firma della relazione.

Errore di ragionamento

L'agente usa la formula o il riferimento normativo sbagliato per il contesto specifico.

Caso reale: Ha verificato la resistenza al fuoco con la norma EN 1995 (legno) invece di EN 1992 (c.a.). Output coerente internamente — sbagliato nella sostanza.

Errore di propagazione

Un piccolo errore al passo 1 si amplifica nei passi successivi producendo un output apparentemente coerente ma sbagliato.

Caso reale: Il baseline per le anomalie di manutenzione era calcolato su 3 settimane invece di 4: tutte le 'anomalie' segnalate erano in realtà nella norma.

Errore di contesto

L'agente non ha le informazioni necessarie e non lo segnala. Lavora sul contesto parziale che ha.

Caso reale: L'agente ha verificato la conformità NTC ma non sapeva che il Comune aveva un regolamento edilizio locale con norme aggiuntive. La verifica era incompleta senza segnalazione.

Chi risponde quando sbaglia l'agente?

La risposta del diritto italiano è univoca: il professionista che ha firmato l'elaborato.

Art. 2229 Codice Civile

La responsabilità professionale non è delegabile a uno strumento. L'ingegnere risponde dell'elaborato firmato indipendentemente da come è stato prodotto. L'AI è uno strumento — non è un coautore e non è un responsabile.

L. 132/2025 art. 13

Se non avete dichiarato l'uso dell'AI al committente, la responsabilità si aggrava. La non-disclosure è una violazione deontologica autonoma rispetto all'eventuale errore tecnico dell'agente.

AI Act art. 14 (deployer)

'Non sapevo cosa stesse facendo l'agente' non è una difesa — è un'ammissione di mancata supervisione. Come deployer di un sistema AI (anche semplice), rispondete della supervisione umana.

Assicurazione RC professionale

La maggior parte delle polizze RC professionale non copre esplicitamente i danni da output AI non supervisionato. Verificare con il proprio broker prima di usare agenti su progetti con alto impatto.

CIVILE

Firma DL: attesta supervisione · Perizia: responsabilità personale

INDUSTRIALE

Marcatura CE: responsabilità fabbricante su macchina con AI

GESTIONALE

Contratto logistico: SLA e penali non trasferibili all'agente

Il log dell'agente: documentazione professionale, non solo tecnica

Il log dimostra che la supervisione umana era effettiva — non solo dichiarata

STRUTTURA MINIMA DEL LOG — Agente con iAlper commesse di ingegneria	
Campo	Esempio / Valore
Data e ora avvio	2025-09-15 08:12:44
Agente / strumento	Claude Projects 'Verifica NTC 2018' v2.1
Input utilizzati	Relazione strutturale_rev3_ANONIMIZZATA.pdf
Norma di riferimento	NTC 2018 cap. 7 + Circ. Min. 2019
Output prodotto	Report_verifica_NTC_15set.docx (bozza)
Anomalie rilevate	Art. 7.4.3: dato mancante — segnalato
Revisore umano	[Nome Ing.] · Data revisione: 15/09/2025
Modifiche post-AI	Integrata verifica art. 7.4.3 con calcolo manuale
Versione finale	Report_verifica_NTC_15set_REV1.docx — firmato

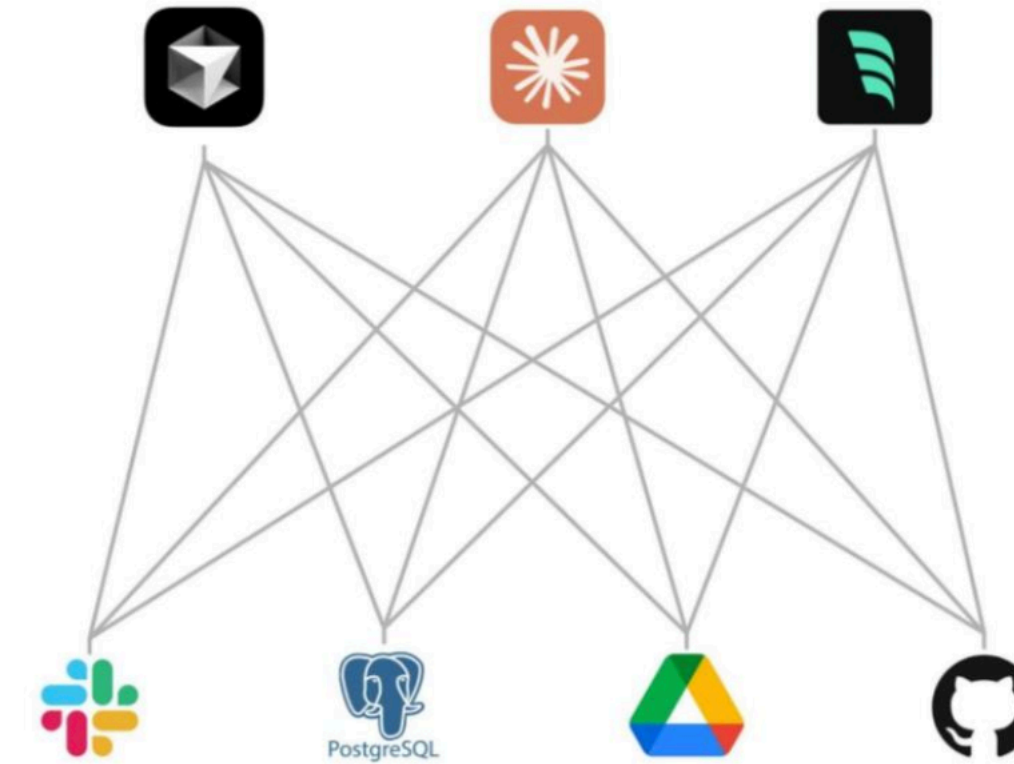
- Conservare per tutta la durata dell'incarico + 10 anni (termine prescrizione responsabilità)
- Il log deve essere leggibile da un non-tecnico: usato in caso di contestazione o audit
- Non è sufficiente il log tecnico del software: serve anche la traccia della revisione umana
- Conservare il log separato dai file di progetto: backup indipendente dall'archivio commessa

Il Ruolo del Model Context Protocol (MCP)

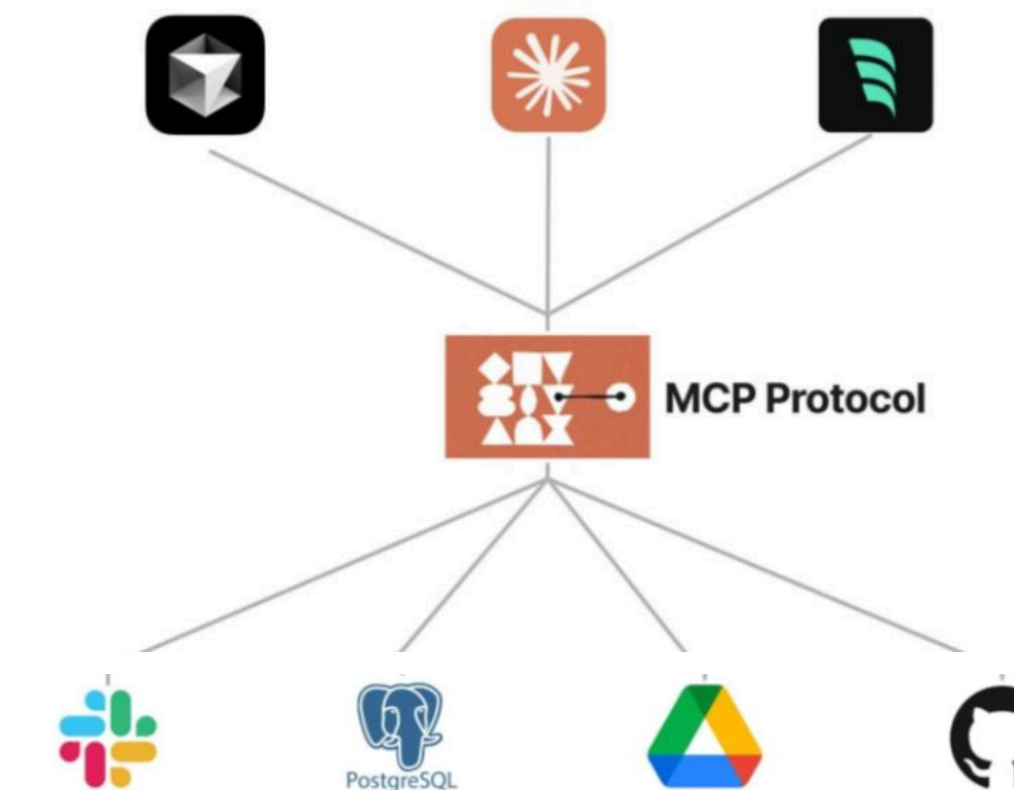
sviluppato e reso liberamente accessibile da Anthropic
Sistema di regole aperto che permette ai chatbot di interfacciarsi con diversi servizi esterni

- Spina dorsale operativa per ambienti di agenti con IA
- Standardizza le interazioni tra:
 - Agenti IA
 - Dati
 - Strumenti
 - Altri agenti

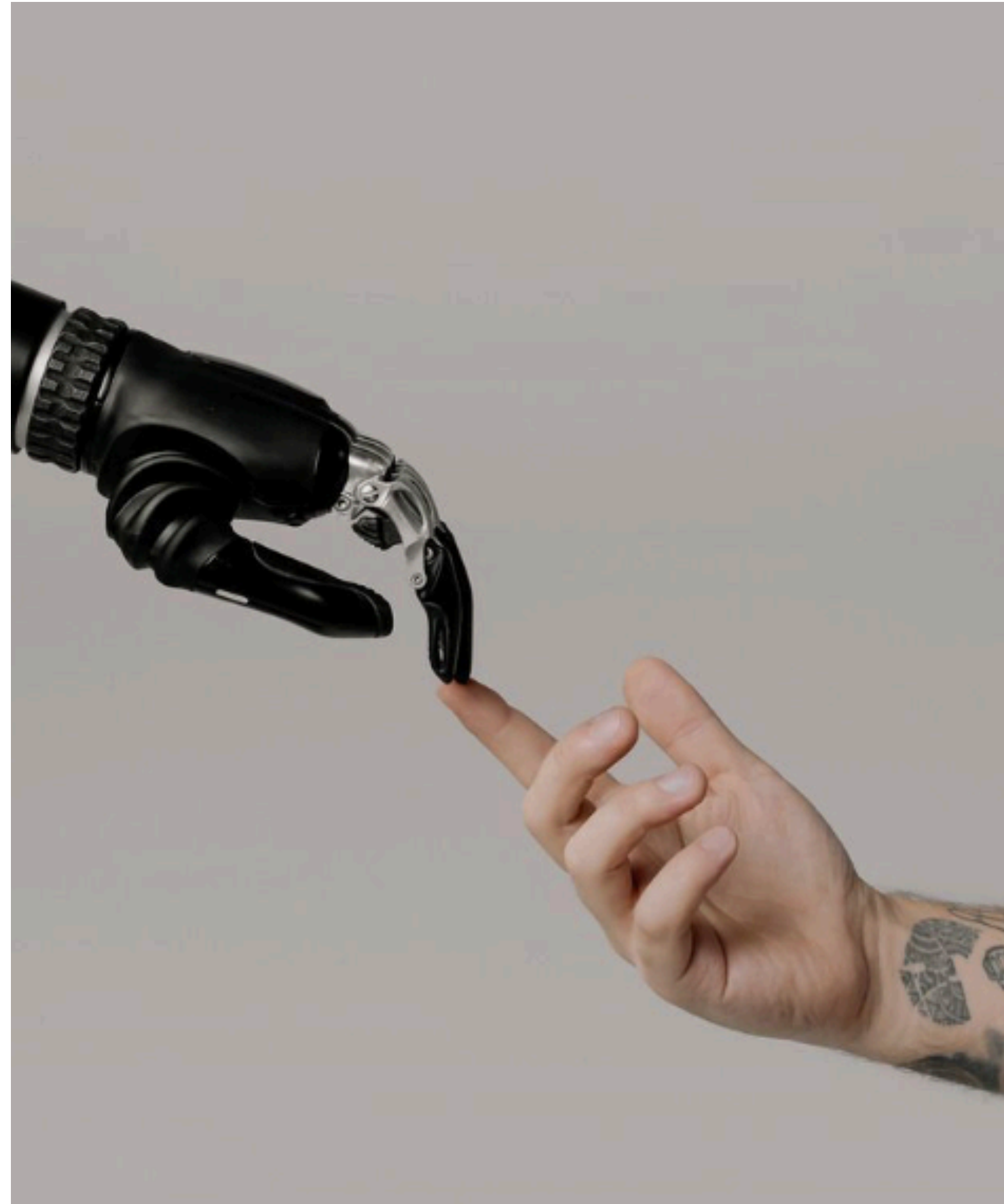
Senza Protocollo di Controllo del modello



con Protocollo di Controllo del modello



Trasformazione del Ruolo Umano



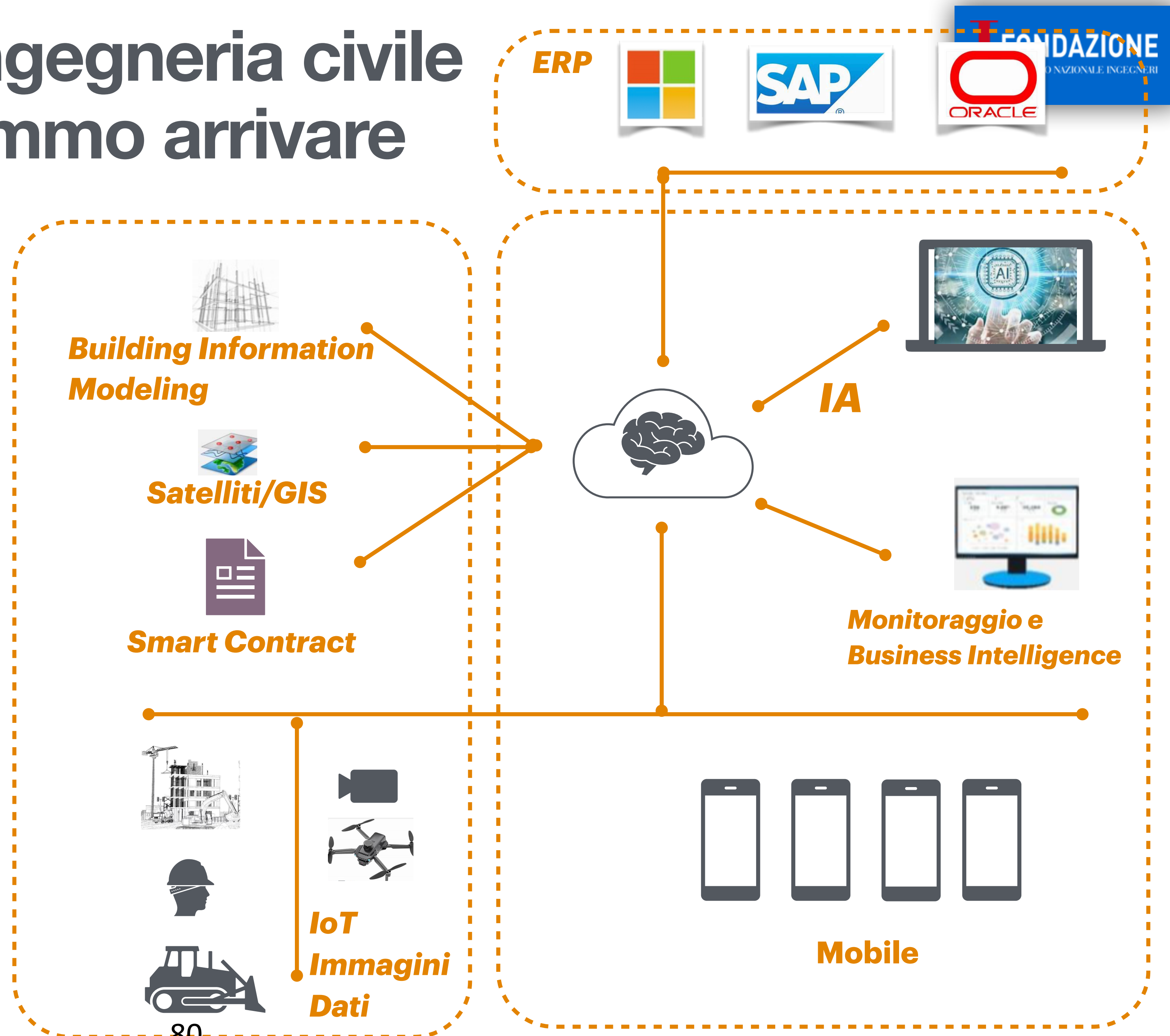
Da “Intelligenza Artificiale Per Le Professioni” ed EBS stesso autore

- Da operatori a decisori strategici
- Focus su:
 - Supervisione
 - Gestione delle eccezioni
 - Innovazione

Esempio di ingegneria civile Dove vorremmo arrivare

- **Centralità dei dati**
- **Integrazione di diverse tecnologie**
- **Collaborazione e condivisione**

L'integrazione di BIM, GIS, IoT, IA e altre tecnologie permette di creare progetti più efficienti, sostenibili e personalizzati, migliorando la collaborazione tra tutti gli attori coinvolti e ottimizzando l'intero ciclo di vita della costruzione.



Come si mette in funzione un agente

Due strade percorribili: adottare soluzioni già pronte sul mercato o costruire un agente su misura

Agenti IA già pronti



Piattaforme di Customer Service

Aziende come **Zendesk**, **ServiceNow**, **Salesforce** e **Freshdesk** hanno integrato agenti IA nelle loro soluzioni, capaci di rispondere alle FAQ, instradare ticket e risolvere problemi comuni.



Chatbot e assistenti virtuali

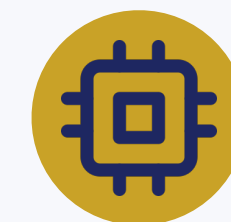
Molti fornitori offrono chatbot IA addestrabili con i dati specifici dell'azienda (manuali tecnici, guide utente, registri di problemi risolti) per un supporto immediato ai clienti.



Assistenti telefonici

Esistono agenti IA specializzati che gestiscono chiamate in entrata, rispondono a domande tecniche e creano ticket di supporto.

Costruire un agente IA ad hoc



Piattaforme di sviluppo

Strumenti come **Microsoft Copilot Studio**, **Google Workflow** e **Azure Databricks** offrono ambienti per creare, testare e distribuire agenti IA personalizzati.



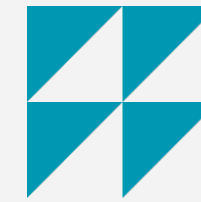
Integrazione con database

Un agente costruito ad hoc può essere collegato direttamente ai database interni, ai sistemi CRM e alle basi di conoscenza tecniche dell'azienda, per risposte più precise e contestualizzate.



Apprendimento continuo

Un agente personalizzato può essere addestrato per apprendere continuamente dalle nuove interazioni, migliorando la capacità di risolvere problemi complessi e di adattarsi a nuove sfide tecniche.

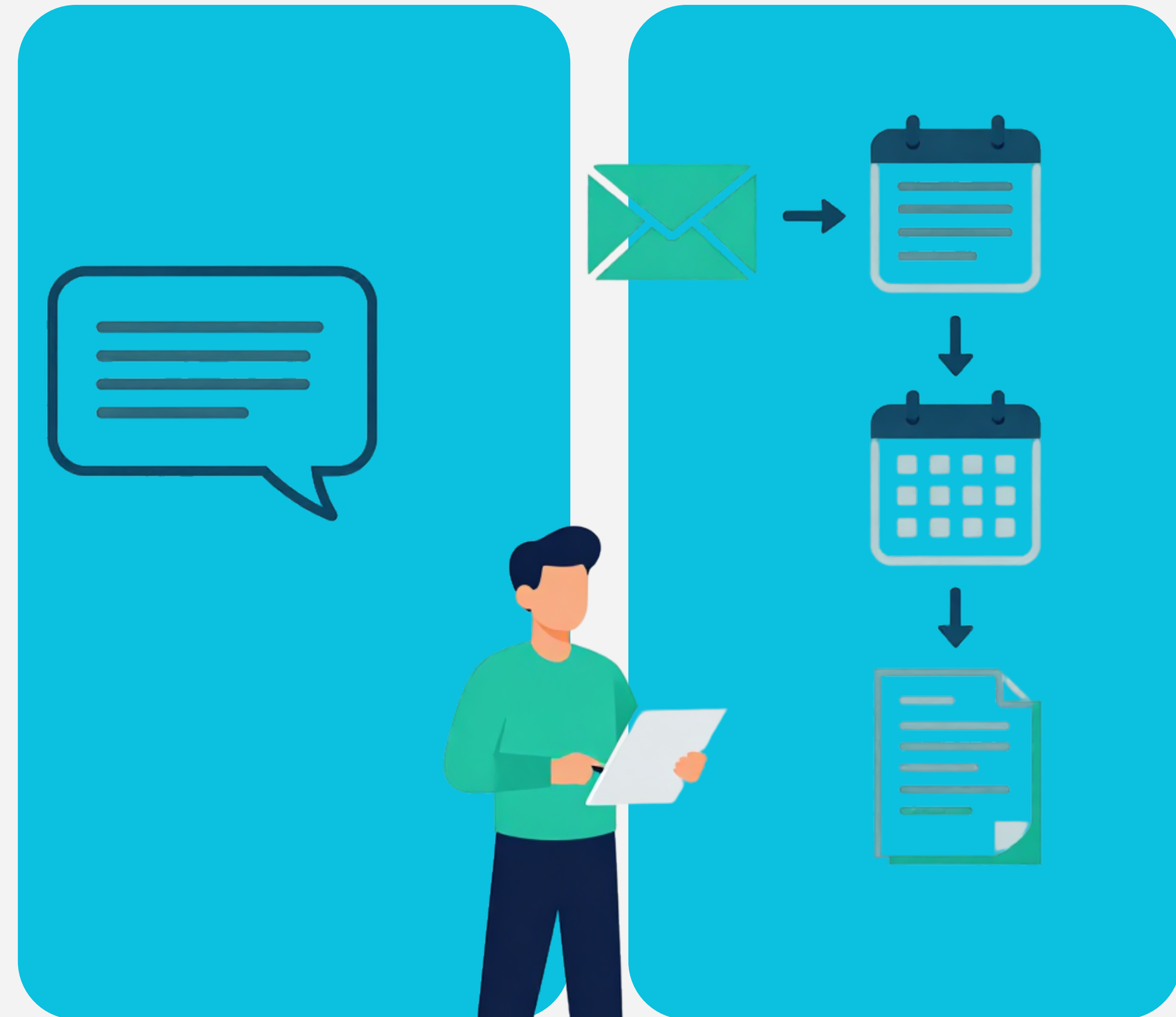


Assistente vs Agente: la differenza chiave

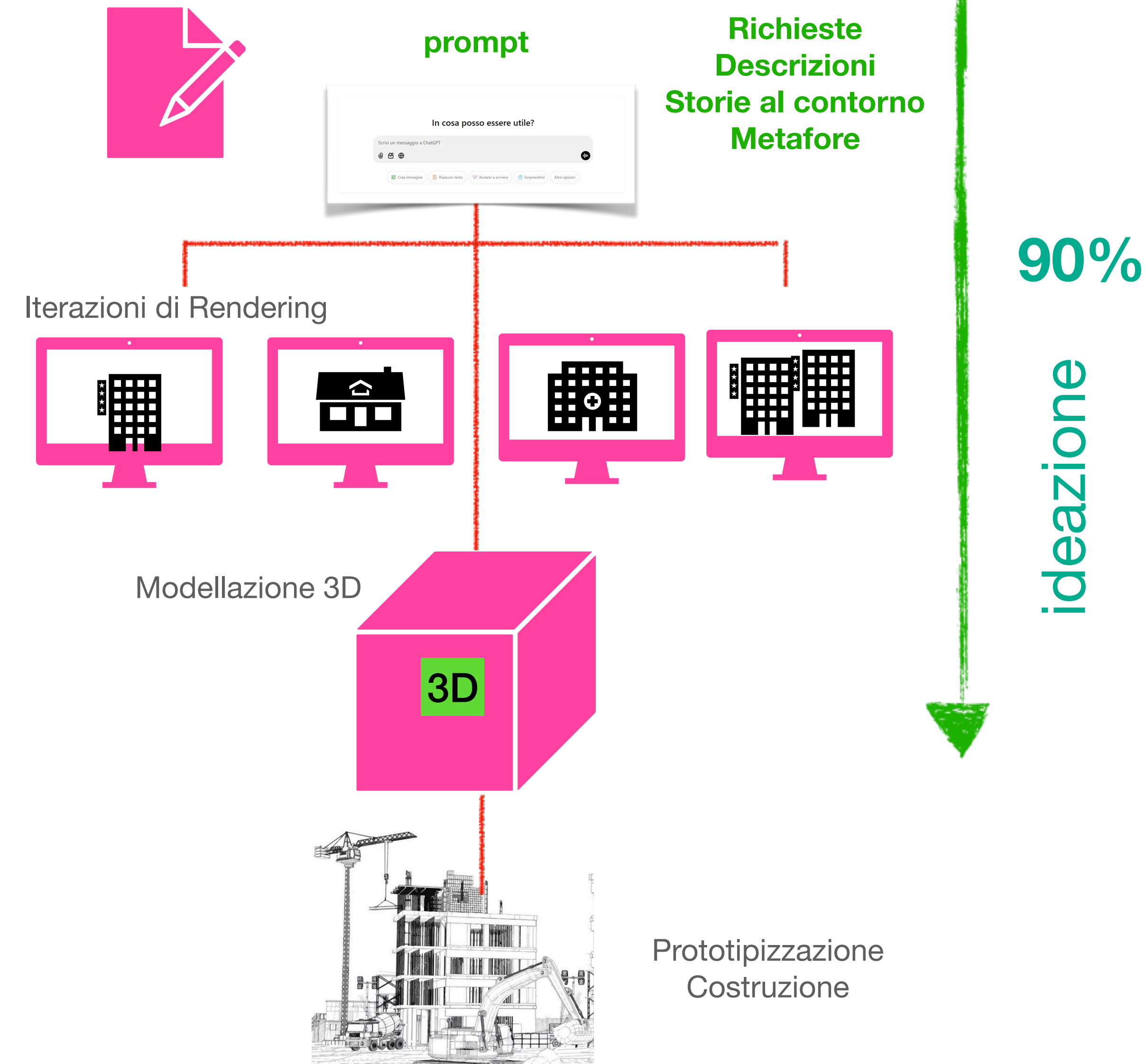
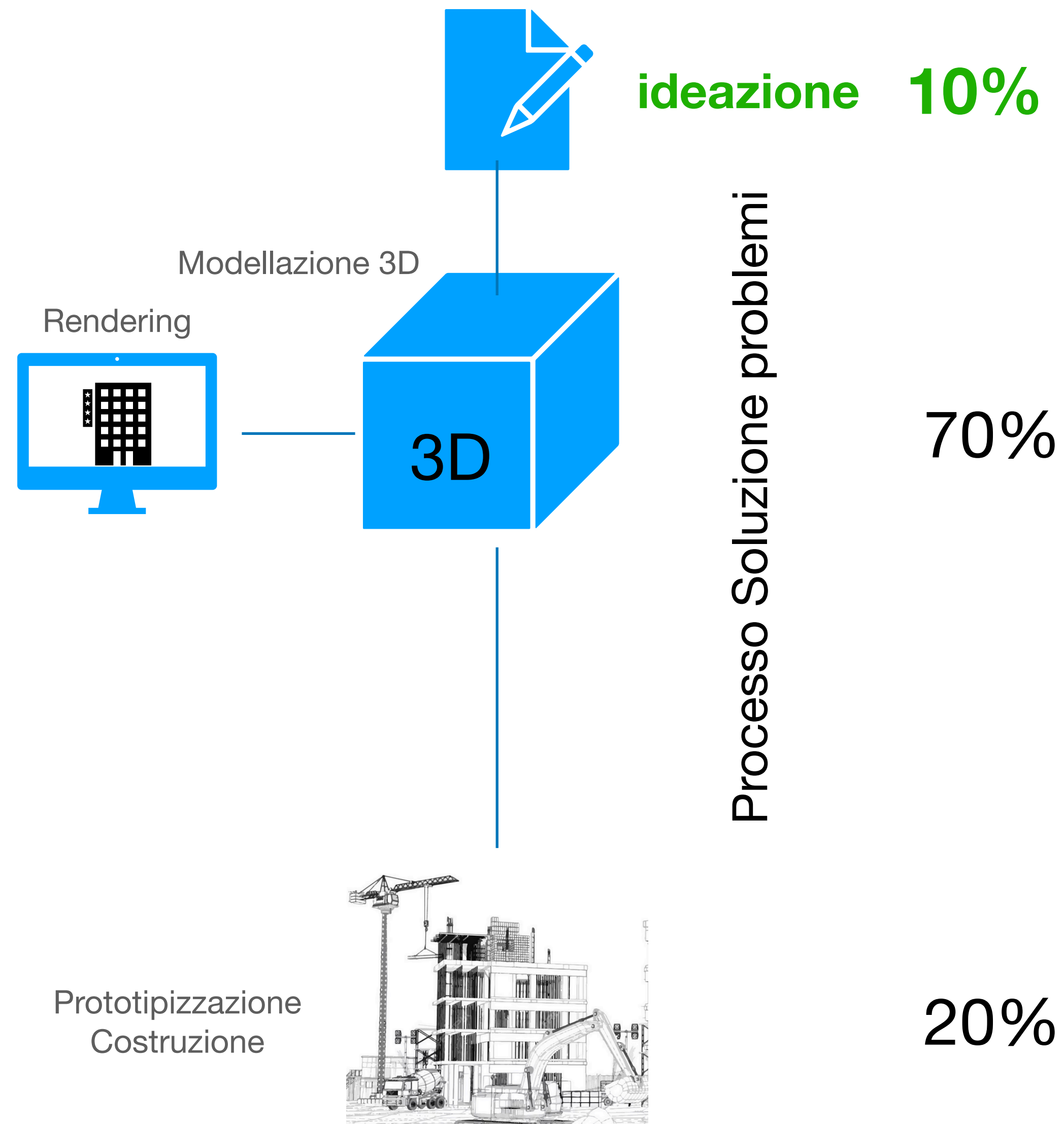
Principio guida: l'agente prepara, l'ingegnere decide e firma

Assistente in chat: risponde a singole domande, opera solo sul testo, conoscenza limitata al momento della conversazione.

Agente intelligente: riceve obiettivi, accede a posta, calendario e documenti, esegue sequenze di azioni in autonomia.



Da tradizionale a progettazione Generativa con IA



uso dell'IA generativa nella progettazione grafica

Strumento IA	Ideale per	Perché sceglierlo
Autodesk Fusion (con Generative Design e AI integrata)	<i>Progettazione meccanica avanzata, ingegneria di precisione e ottimizzazione dei vincoli di produzione (es. fresatura a 5 assi o stampa 3D)</i>	Integra algoritmi di generative design e assistenti IA in grado di suggerire geometrie ottimizzate per specifiche esigenze strutturali, riducendo drasticamente i tempi di sviluppo.
Strumenti Text-to-CAD (es. Zoo.dev, AdamCAD)	<i>Modellazione 3D rapida tramite prompt testuali e prototipazione preliminare</i>	Permettono di generare modelli tridimensionali modificabili direttamente da descrizioni in linguaggio naturale, rendendo l'ingegneria accessibile e accelerando l'ideazione.
SOLIDWORKS Aura / PTC Creo AI / Siemens NX Copilot	<i>Progettazione parametrica, gestione di assemblaggi complessi e automazione delle attività ripetitive</i>	I principali software CAD di settore integrano assistenti intelligenti ed agenti IA per automatizzare la creazione di disegni, la gestione delle tolleranze e l'analisi dei componenti.
PhysicsX (Simulation Workbench)	<i>Simulazione fisica avanzata e analisi predittiva delle performance fluidodinamiche e strutturali</i>	Sostituisce o affianca i solutori tradizionali con modelli di inferenza basati su IA, consentendo di testare migliaia di varianti in tempo reale con una precisione validata fisicamente.
Adobe Firefly, Canva AI e Runway	<i>Grafica tecnica, concept art, visualizzazioni commerciali e documentazione multimediale</i>	Offrono un'interfaccia user-friendly integrata nei flussi creativi per la rapida generazione di asset visivi, presentazioni e materiali di comunicazione per i clienti.

Le informazioni riportate non costituiscono comparazione né valutazione, tabella a puro uso didattico

Vibe coding - - Cosa sapere

◆ Cos'è il Vibe Coding?

- Traduzione di descrizioni in linguaggio naturale in codice funzionante grazie all'uso di modelli linguistici avanzati (LLM).
- Permette di creare software con semplici istruzioni verbali.

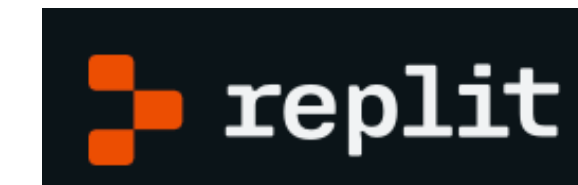


✓ Vantaggi

- Maggiore accessibilità alla programmazione.
- Prototipazione rapida ed efficace.

◆ Evoluzione

💡 **Notevole Potenziale**, da valutare l'affidabilità a lungo termine.



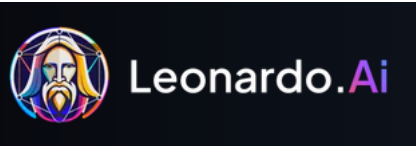
✗ Sfide

- Qualità del codice generato e rischi di sicurezza.
- Necessità di supervisione e competenze tecniche per risultati affidabili.

🧑‍💻 **Competenze necessarie:** Visione architetturale, sicurezza e controllo umano sono essenziali.



Generazione di video alcuni strumenti



Categoria	Nome Strumento	Piano Gratuito	Interfaccia/Facilità d'uso	Ideale Per	Caratteristiche Aggiuntive
Generazione Video Text-to-Video / Image-to-Video	OpenAI Sora	Accesso tramite piani avanzati / API (disponibilità variabile)	Interfaccia guidata e intuitiva	Creazione di video fotorealistici ad alta risoluzione (fino a 60 secondi) partendo da prompt testuali complessi	Comprensione avanzata della fisica del mondo reale e consistenza temporale elevata
Generazione Video Text-to-Video	Runway Gen-3 Alpha	Versione di prova gratuita con crediti limitati	Interfaccia professionale ma accessibile	Generazione di sequenze cinematografiche, animazioni e motion graphics di altissima qualità	Controllo avanzato della cinepresa, motion brush e blending fluido tra i fotogrammi
Generazione Video & Cinematic	Luma Dream Machine / Kling AI	Piano gratuito con generazioni giornaliere limitate	Semplice e immediata via web	Produzione rapida di concept video, loop visivi ed effetti speciali realistici	Ottima gestione dei movimenti dinamici e della coerenza dei personaggi
Editing e Post-produzione Video	Adobe Premiere Pro (con Firefly Video AI)	Incluso nell'abbonamento Creative Cloud (con prove gratuite)	Familiare per i professionisti del montaggio	Estensione di clip video, aggiunta o rimozione di oggetti tramite IA direttamente in timeline	Generazione di b-roll automatica, text-based editing e miglioramento audio intelligente
Video Editing AutomATIK & Sottotitoli	Descript / CapCut Web	Piano gratuito con esportazioni base	Estremamente user-friendly	Editing video basato su testo, rimozione automatica dei silenzi e sottotitolazione smart	Clonazione vocale, traduzione video automatica e template virali per i social media

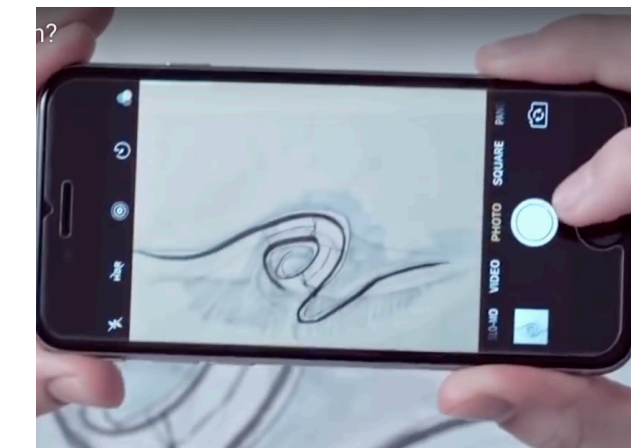
Le informazioni riportate non costituiscono comparazione né valutazione, tabella a puro uso didattico

Predictive design software

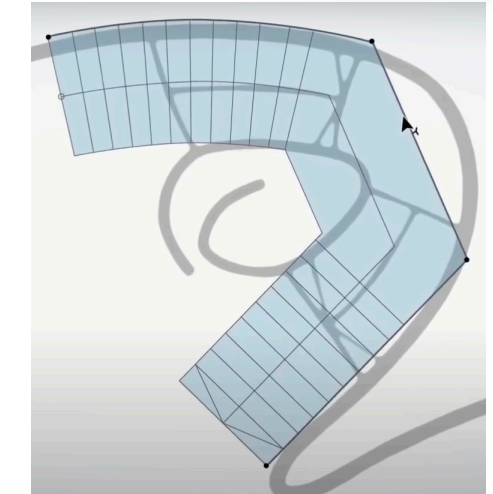


Inserendo semplici limiti
IA propone soluzioni
Considera storia
Considera norme
Suggerisce soluzioni

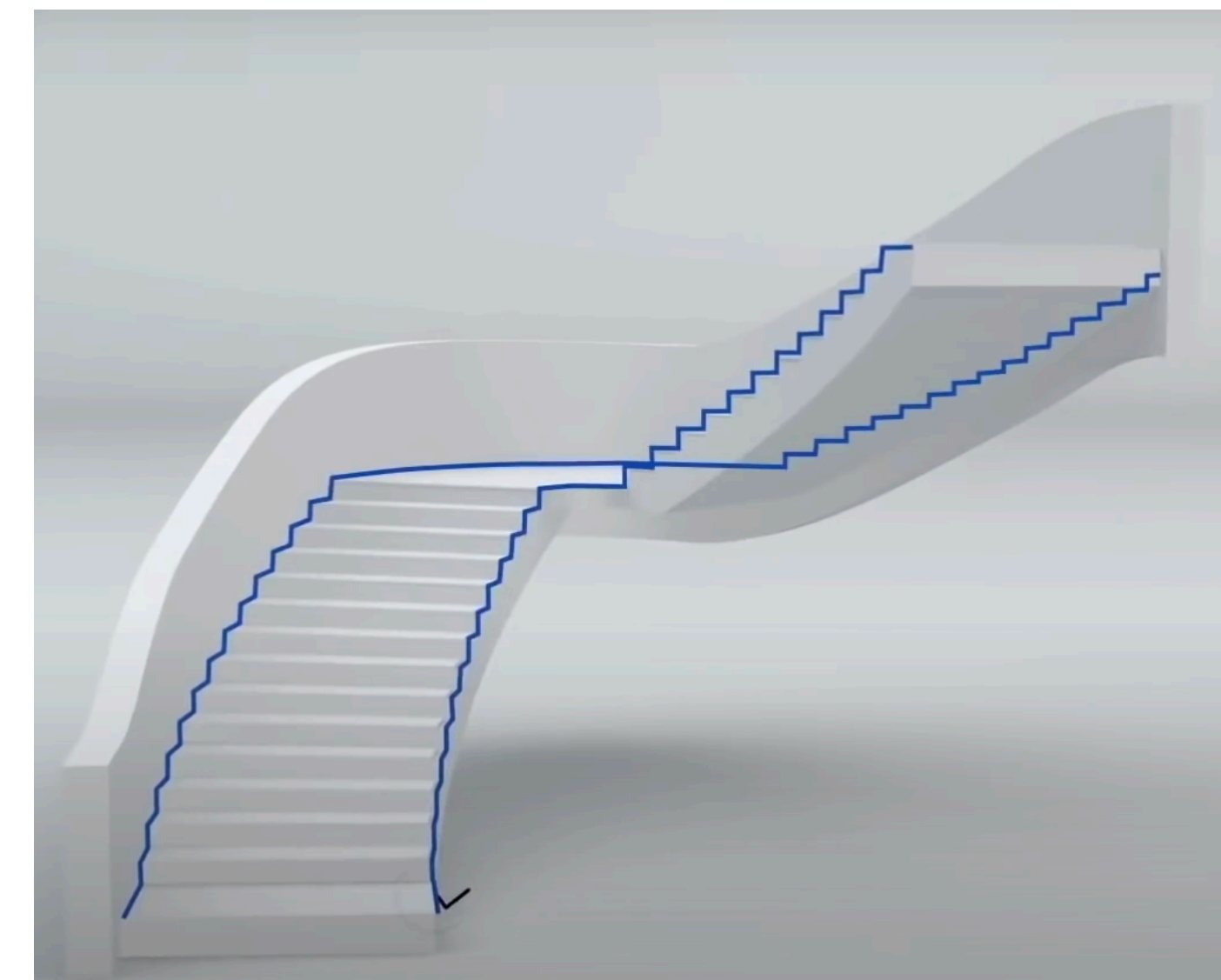
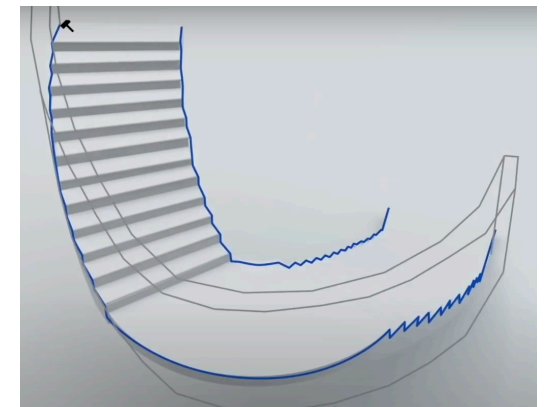
1



2



3



Come attuare un monitoraggio remoto

- 1. Analisi del Flusso:** analisi delle metodologie con cui ogni dato o pacchetto software viene processato, dalla fase di acquisizione dell'immagine fino alla sua presentazione all'utente finale.
- 2. Ottimizzazione:** individuare nodi critici o rallentamenti nel flusso dei dati. (Six Sigma)
- 3. Scelta delle rete**
- 4. Allenamento della rete neurale**
- 5. Generazione delle maschere**
- 6. Offuscamento**

IA non generativa

- CNN (Convolutional Neural Networks):**
- 1. Pro:** efficaci nell'identificare schemi visivi con minimi preprocessamenti. Hanno rivoluzionato il riconoscimento di immagini.
 - 2. Contro:** non ottimali per problemi che vanno oltre la classificazione di immagini semplici.

- SSD (Single Shot Multibox Detector):**
- 1. Pro:** effettua rilevamenti in un solo passaggio, veloce.
 - 2. Contro:** non sempre accurato

- YOLOv8**, è particolarmente potente per la sua capacità di identificare oggetti in tempo reale con alta precisione,
- 1. Pro:** accuratezza, rilevamento di piccoli oggetti e riduzione di falsi positivi..
 - 2. Contro:** considerevole potenza di calcolo per l'allenamento

Data Augmentation aumenta artificialmente la dimensione del dataset di allenamento attraverso rotazione, zoom, capovolgimento, variazione di luminosità e colore, tra le altre. Modello più robusto

Transfer Learning sfrutta un modello pre-addestrato (spesso su un ampio dataset come ImageNet) come punto di partenza per un nuovo compito specifico. Si inizia con pesi che hanno già una certa "intuizione" sulle caratteristiche delle immagini. Solo gli ultimi strati vengono poi ri-allenate sul nuovo dataset specifico.

Ogni maschera deve essere accurata per garantire che solo le parti sensibili dell'immagine siano offuscate e rilevato quanto necessario.

L'offuscamento (es blurring), bilancia l'anonimizzazione con la conservazione della qualità complessiva dell'immagine. Prima dell'offuscamento l'immagine è analizzata e vengono estrapolati i dati e le informazioni necessarie.

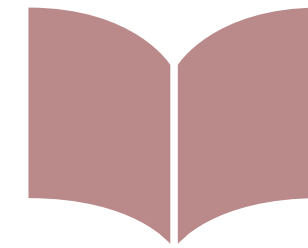


Le normative europee a protezione dei cittadini



DATA ACT

Regola l'accesso e l'utilizzo dei dati non personali
Permette agli utenti di accedere ai propri dati generati
Facilita il cambio tra servizi cloud
Protegge i dati sensibili delle aziende
Stabilisce standard per l'interoperabilità

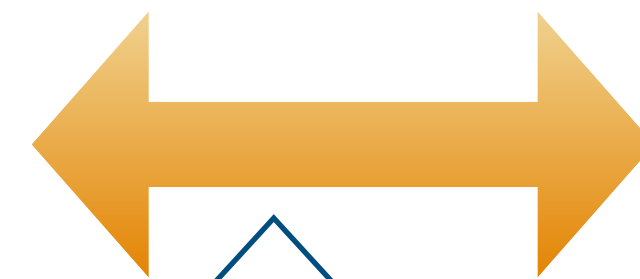


Digital Markets Act (DMA)

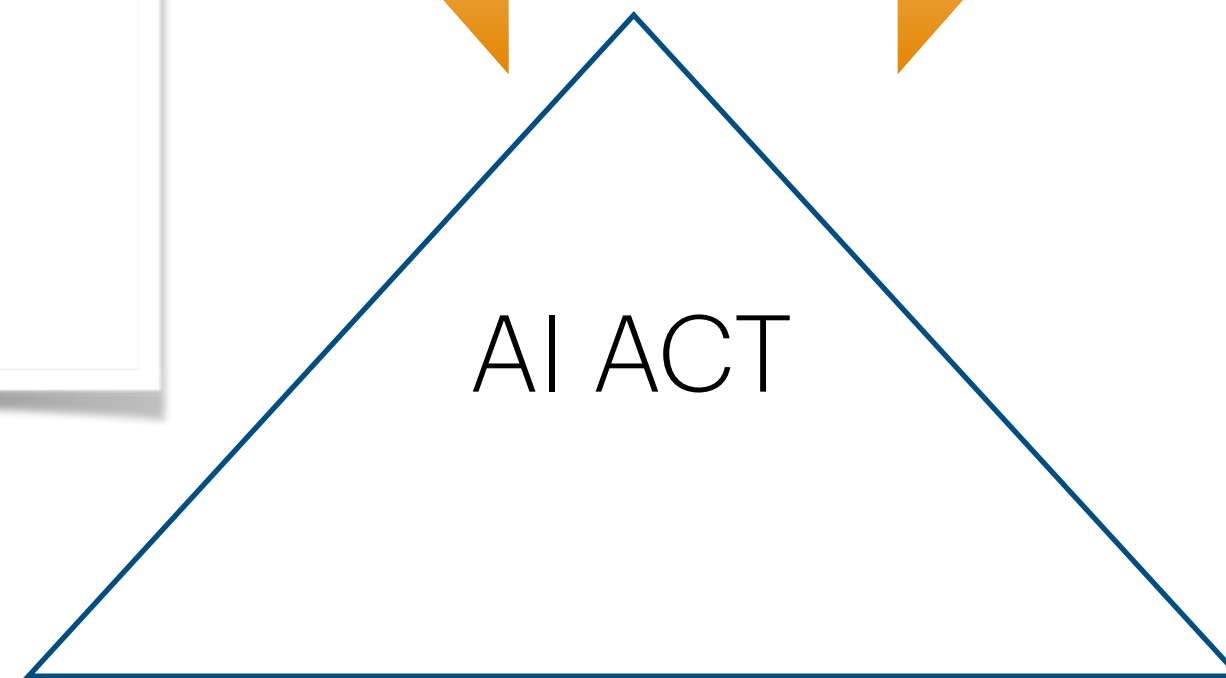
- Regola le grandi piattaforme digitali ("gatekeeper")
- Criteri per identificare i gatekeeper:
 - Fatturato > €7.5 miliardi in EU
 - 45 milioni di utenti mensili
 - Posizione stabile e duratura

Obblighi:

- Interoperabilità
- Accesso ai dati per business users
- Divieto di self-preferencing



AI ACT



Digital Services Act (DSA)

Principi Fondamentali

- Responsabilità delle piattaforme online
- Protezione dei diritti fondamentali online
- Trasparenza degli algoritmi
- Moderazione dei contenuti

Obblighi Chiave

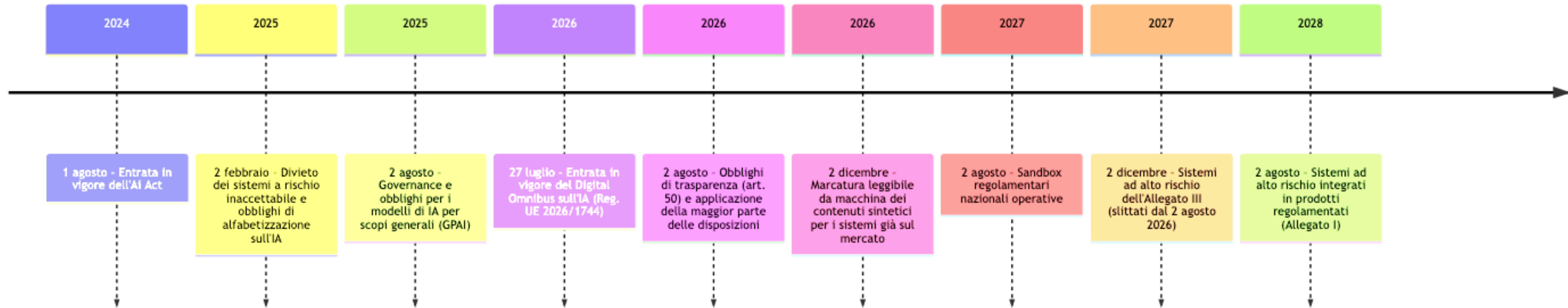
- Rimozione rapida contenuti illegali
- Tracciabilità dei commercianti online
- Valutazione dei rischi sistemici
- Audit indipendenti

Supervisione e Sanzioni

- Coordinatori nazionali servizi digitali
- Commissione Europea per piattaforme molto grandi
- **Multe fino al 6% del fatturato globale**

Tappe più prossime dell'AI Act

AI Act (Reg. UE 2024/1689) - calendario aggiornato al Digital Omnibus



- **Entrata in vigore:** L'AI Act è entrato in vigore il 1° agosto 2024.
- **+ Dal 2 agosto 2026** si applicano gli obblighi di trasparenza dell'art. 50 (chatbot, contenuti generati) e la supervisione è operativa
- **+ Nuova scadenza intermedia:** 2 dicembre 2026 per la marcatura leggibile da macchina dei contenuti sintetici generati da sistemi già immessi sul mercato

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

Roberto Magnani ©

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689

Linee guida pratiche

Studi

- Valutazione etica prima dell'adozione di strumenti IA
- Politiche di trasparenza con clienti e collaboratori
- Formazione continua del personale
- Diversificazione delle competenze
- Monitoraggio degli impatti



Professionisti

- Sviluppo di competenze complementari all'IA
- Approccio critico agli strumenti utilizzati
- Valorizzazione dell'apporto umano unico
- Comunità di pratica per condivisione esperienze
- Bilanciamento tra innovazione e tradizione



Committenti/Clienti

- Domande da porre sui processi IA utilizzati
- Diritti sui dati e sulla proprietà intellettuale
- Valutazione degli impatti etici dei progetti
- Inclusione di diversi stakeholder
- Criteri di sostenibilità oltre l'ottimizzazione



Agenti AI per lo studio di ingegneria

Come passare da un primo assistente a un sistema agentico su misura: metodo, strumenti già disponibili ed esempi che si attivano in pochi giorni.

Per titolari, responsabili di commessa e segreteria

Ottobre 2026

Usa i tasti freccia per scorrere

Un agente non si limita a rispondere: lavora

La differenza sta negli strumenti. Un agente può leggere posta, calendario e documenti, eseguire passaggi e consegnare un risultato pronto da verificare.

Agenti AI per lo studio di ingegneria

Assistente in chat

- Risponde a una domanda alla volta
- Conosce solo ciò che gli incolla
- Produce testo da copiare a mano

Agente

- Riceve un obiettivo, non solo una domanda
- Accede a posta, calendario e archivio tramite connettori
- Esegue una sequenza di passaggi e prepara bozze o azioni
- Si ferma e chiede conferma prima di agire

Principio guida dello studio: l'agente prepara, l'ingegnere decide e firma.

Dove lo studio perde ore ogni settimana

Prima di scegliere strumenti, si mappano i punti di attrito.
Questi otto sono i candidati più frequenti.

Posta e PEC

Smistare, capire cosa è urgente, preparare risposte.

Scadenze

Pratiche, integrazioni, collaudi, stati di avanzamento.

Verbalì e relazioni

Da appunti di sopralluogo a documento ordinato.

Ricerca interna

Capitolati, procedure, progetti simili già fatti.

Offerte e preventivi

Bozze coerenti con lo storico dello studio.

Commesse

Ore, avanzamento, margini, ritardi.

Fatturazione

Promemoria, solleciti, controllo incassi.

Archivio

Nomi file, versioni, documenti dispersi.

Esercizio da 10 minuti: ogni persona dello studio segna le tre attività più ripetitive della propria settimana.

Come scegliere il primo agente

Un buon candidato soddisfa tutti e cinque i criteri.

- **Frequente:** si ripete ogni giorno o ogni settimana
- **Regolare:** segue un criterio che si sa spiegare a voce
- **Verificabile:** il risultato si controlla in pochi minuti
- **A basso rischio:** un errore costa poco e si corregge
- **Con dati accessibili:** posta, calendario o file già in formato digitale

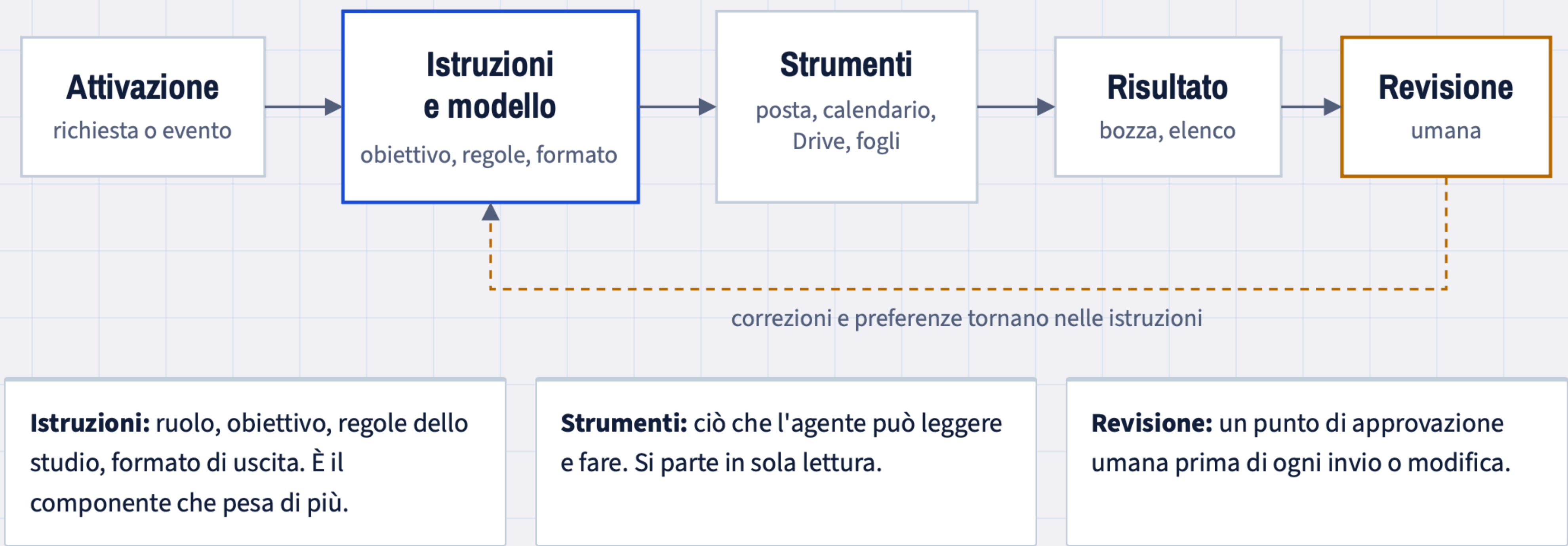
Da cui partire

- Riepilogo del mattino su posta e agenda
- Estrazione scadenze dalle email
- Bozza di verbale da appunti

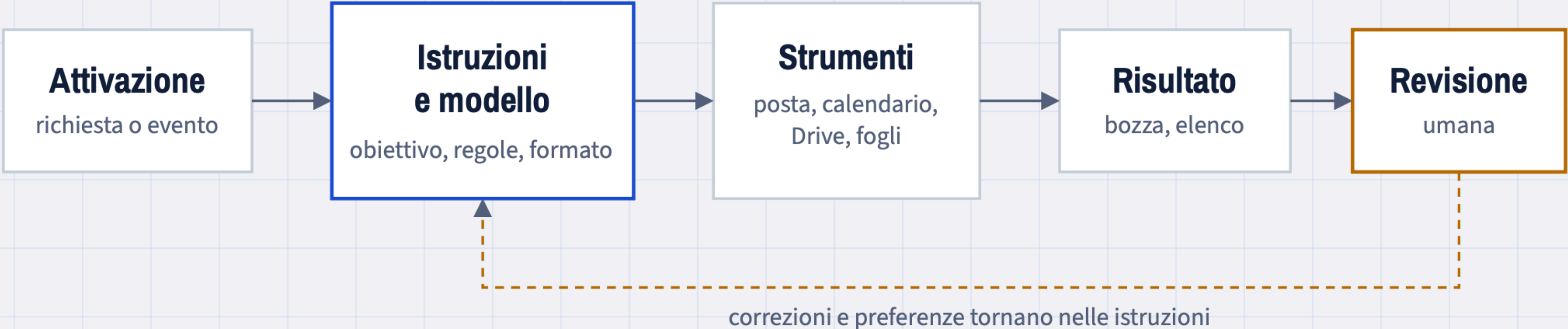
Da non automatizzare all'inizio

- Calcoli strutturali e verifiche di sicurezza
- Asseverazioni e firme
- Invio automatico a enti e clienti

Anatomia di un agente: cinque componenti



Anatomia di un agente: cinque componenti



Istruzioni: ruolo, obiettivo, regole dello studio, formato di uscita. È il componente che pesa di più.

Strumenti: ciò che l'agente può leggere e fare. Si parte in sola lettura.

Revisione: un punto di approvazione umana prima di ogni invio o modifica.

Quattro livelli: si cresce per gradi

Ogni livello porta valore da solo. Non serve costruire il sistema completo per iniziare.

Livello 1, pochi giorni

Assistente in chat

Uso quotidiano per testi, riassunti, revisione di bozze.
Nessuna integrazione.

Livello 2, una settimana

Assistente dello studio

Istruzioni fisse e documenti dello studio caricati: capitolati, modelli, procedure.

Livello 3, 2-4 settimane

Agente con connettori

Legge posta, calendario e Drive, e prepara bozze e promemoria.

Livello 4, 2-3 mesi

Sistema di agenti

Più agenti specializzati, coordinati, con registro delle attività e regole condivise.

I tempi sono stime per uno studio di piccole e medie dimensioni, con una persona di riferimento che dedica qualche ora a settimana.

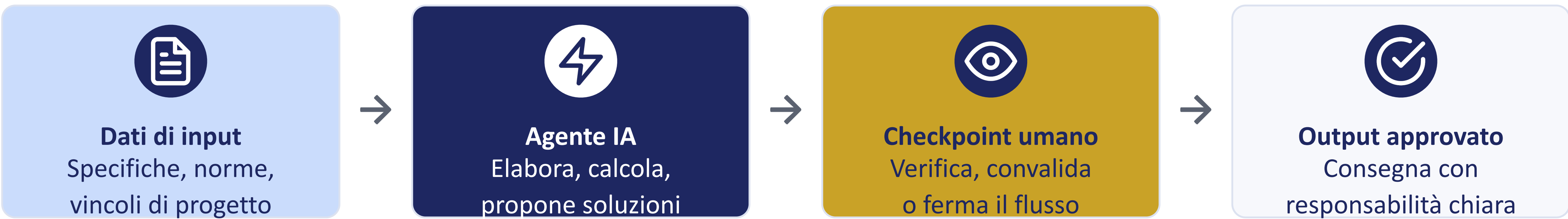
Strumenti già disponibili, per esigenza

Esigenza	Prodotti da valutare
Assistente con istruzioni e documenti dello studio	Claude con i Projects; ChatGPT con Projects e GPT personalizzati; Gemini con i Gems
Agente che legge posta, calendario e Drive	Claude con i connettori Gmail, Google Calendar e Google Drive; Microsoft 365 Copilot per Outlook, Teams e SharePoint; Gemini in Google Workspace
Flussi automatici con attivazione a evento	Zapier, Make, n8n; Copilot Studio per agenti in ambiente Microsoft; Comandi Rapidi di macOS
Lavoro su file locali del Mac	Claude Cowork, app desktop per attività con i file; Claude Code per chi scrive script
Dati riservati che non devono uscire	Modelli piccoli (SLM) in locale con Ollama o LM Studio

Funzioni, piani e costi cambiano spesso. Prima di scegliere, verificare disponibilità e condizioni sui siti dei fornitori. Regola pratica: usare lo strumento della suite che lo studio usa già (Google Workspace o Microsoft 365) riduce attriti e permessi.

Perché serve il Human-in-the-Loop

Un sistema IA che assiste calcoli, disegni o verifiche non elimina la necessità del giudizio ingegneristico: lo sposta.



Il principio guida

Human-in-the-Loop non significa “un umano legge il risultato finale”, ma progettare consapevolmente i punti in cui il controllo umano è obbligatorio, quali segnali lo attivano e quali competenze deve avere chi lo esercita.

Definire le soglie di autonomia dell'agente

Non tutte le attività IA richiedono lo stesso livello di supervisione: la soglia va calibrata sul rischio e sulla reversibilità dell'azione.

L0	Assistenza passiva	L'IA suggerisce, l'ingegnere decide e agisce interamente da solo (es. ricerca normativa, bozze di documenti).	Rischio minimo
L1	Automazione supervisionata	L'IA esegue un compito delimitato (calcolo, disegno); ogni output è validato prima dell'uso (es. verifica strutturale preliminare).	Rischio contenuto
L2	Autonomia condizionata	L'IA esegue sequenze di azioni entro parametri prefissati, con checkpoint obbligatori a soglie critiche (es. dimensionamento impianti).	Rischio moderato
L3	Autonomia estesa	L'IA opera su più fasi con intervento umano solo su eccezione o allarme; richiede audit trail continuo e reversibilità garantita.	Rischio elevato

Quando intercettare il flusso

Audit continuo ed errori a cascata: fermare l'azione automatica prima che un errore si propaghi

Segnali che devono fermare l'agente



Deviazione dai parametri di progetto

L'output esce dai limiti normativi o dai margini di sicurezza attesi.



Bassa confidenza del modello

Il sistema segnala incertezza, dati mancanti o ambigui.



Impatto su sicurezza o costi critici

La decisione incide su elementi strutturali, safety o budget rilevanti.



Input non validati

I dati a monte non hanno superato un controllo di qualità.



Audit ed errori a cascata

Un errore non intercettato in una fase iniziale (es. un dato di carico sbagliato) si propaga alle fasi successive, amplificandosi:

- Errore nel dato di input
- Calcolo derivato non valido
- Disegno esecutivo errato
- Decisione operativa a rischio

→ *L'audit trail deve tracciare ogni checkpoint per isolare il punto di origine dell'errore.*

02

Responsabilità legale

e deontologica

Chi risponde quando un sistema IA sbaglia? Come tutelarsi sul piano giuridico, contrattuale e assicurativo

Di chi è la responsabilità?

Quando un sistema IA commette un errore in un calcolo o in una perizia, la responsabilità si distribuisce lungo la catena di soggetti coinvolti



Ingegnere firmatario

Responsabilità professionale e civile per l'atto firmato: l'uso di IA non trasferisce l'obbligo di verifica e la responsabilità dell'elaborato finale.



Sviluppatore / fornitore del sistema IA

Responsabilità da prodotto per difetti del software, limiti dichiarati non conformi o mancata informazione sui rischi d'uso.



Committente / datore di lavoro

Responsabilità organizzativa se impone l'uso di IA senza formazione, tempo di verifica adeguato o procedure di controllo.

Principio operativo: la responsabilità civile resta tipicamente in capo a chi firma e convalida l'elaborato — l'IA è uno strumento, non un soggetto di diritto.

Come tutelarsi

Sul piano contrattuale e assicurativo: misure concrete per limitare l'esposizione al rischio



Tutela contrattuale

- Clausole che definiscono l'uso dell'IA come supporto e non come sostituto della validazione professionale
- Obbligo contrattuale di tracciabilità: conservare prompt, output e versioni del modello utilizzato
- Definizione esplicita dei limiti di responsabilità del fornitore del sistema IA
- Procedure interne documentate di revisione umana per ogni output critico



Tutela assicurativa

- Verificare che la polizza di responsabilità civile professionale copra esplicitamente errori originati da strumenti IA
- Dichiarare l'uso di sistemi IA all'assicuratore: l'omissione può invalidare la copertura
- Valutare estensioni specifiche per rischio cyber e data-liability
- Documentare il processo di controllo qualità come prova di diligenza professionale

Framework operativo di sintesi

Cinque azioni per governare l'IA nella pratica ingegneristica quotidiana

	1	Classificare il rischio	Assegnare ad ogni task IA una soglia di autonomia coerente con impatto e reversibilità.
	2	Presidiare i checkpoint	Fissare i punti di controllo umano obbligatori e i segnali che fermano il flusso automatico.
	3	Tracciare ogni passaggio	Mantenere un audit trail che permetta di risalire all'origine di un errore a cascata.
	4	Verificare, non fidarsi	Trattare ogni output IA come un'ipotesi da validare, specie dati numerici e riferimenti normativi.
	5	Formalizzare la tutela	Aggiornare contratti e polizze assicurative per riflettere l'uso reale di strumenti IA.

GRAZIE PER L'ATTENZIONE

I'Autore

Roberto Magnani



Ingegnere elettronico, sviluppa la sua carriera nel settore IT nei laboratori di multinazionali in Italia, Francia, USA, Svizzera, Spagna e Irlanda. Dal 2012 ha condotto un team dedicato al Public Cloud per l'Europa in un **Campus tecnologico di Dublino, Irlanda**, per poi assumere la responsabilità di progetti digitali per Healthcare e Life Science sul mercato EMEA, **con utilizzo di intelligenza artificiale**.

Dal 2021 è consulente indipendente e consigliere di AEIT Milano - Associazione italiana elettronica elettrotecnica informatica e telecomunicazioni, e dal 2024 è un componente del Comitato Tecnico Scientifico per l'Intelligenza Artificiale ENIA®, **focalizzandosi sulla penetrazione dell'Intelligenza Artificiale nell'industria e curando anche gli aspetti etici e normativi in combinazione con l'introduzione del Quantum computing**.

È autore di articoli e interventi in Italia e all'estero sugli stessi argomenti, di una pubblicazione dedicata all' "**Intelligenza artificiale per le professioni**" (2023) edito da EBS, e dei saggi "**Costruiamoci il Futuro. Intelligenza Artificiale: un approccio etico**" (2023 - seconda edizione 2026) edito da EthosJob come "**Valutazione della prontezza all'IA per PMI**" (2026) e "**Intelligenza Artificiale. Guardiamo oltre**" (2025), "**Gli effetti dell'Intelligenza Artificiale nel quotidiano**" (2025) Edizioni Messaggero, "**Intelligenza Artificiale e Sostenibilità**". Ed **Castelvecchi 2025**

<https://www.linkedin.com/in/robertomagnani/>