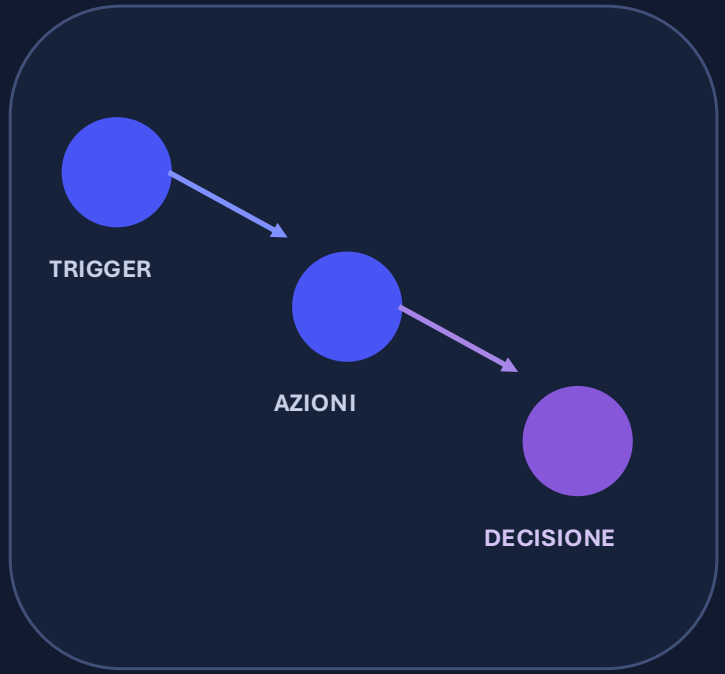
IA PER LA COMUNICAZIONE

Workflow e AI agentica

Dall’automazione deterministica ai sistemi che usano strumenti e prendono decisioni

Concetti, architetture, livelli di autonomia e human-in-the-loop



Prof.ssa Romina Eramo
Università degli Studi di Teramo
Dipartimento di Scienze della Comunicazione

Obiettivi della lezione

OVERVIEW

Costruire una mappa concettuale prima di passare agli strumenti.

1. Capire

Che cos'è un workflow e quali elementi lo compongono.

2. Distinguere

Automazione, AI workflow e AI Agent: non sono sinonimi.

3. Progettare

Capire dove inserire AI, decisioni, tool e controlli umani.

4. Valutare

Riconoscere quando un agente è utile e quando è eccessivo.

Messaggio chiave: prima si progetta il processo, poi si sceglie la tecnologia.

Perché oggi parliamo di sistemi agentici?

CONTESTO

Gli LLM non si limitano più a generare contenuti: possono usare strumenti e partecipare a processi multi-step.

Comprendere

testo, immagini, documenti, richieste non strutturate

Decidere

scegliere un'azione, una fonte, un tool o un percorso

Agire

chiamare API, cercare dati, aggiornare sistemi, produrre output

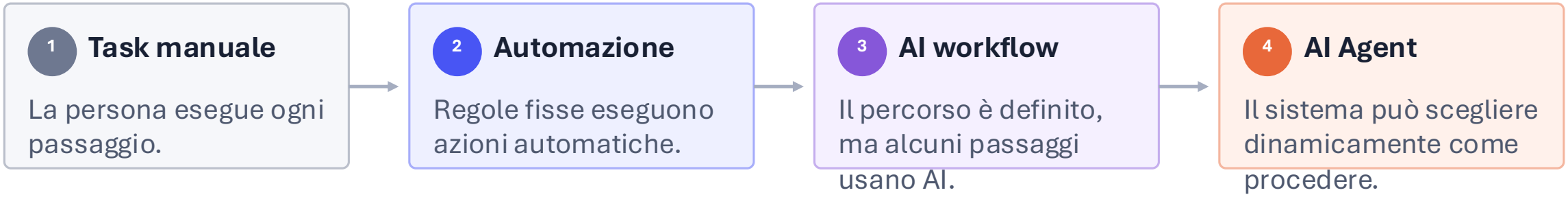
Verificare

osservare risultati, valutare errori e continuare o fermarsi

Dal "generare una risposta" al "portare avanti un compito".

Un continuum: dal task manuale all’agente

Non esiste un confine unico: cresce progressivamente la quota di decisione delegata al sistema.



Aumenta la flessibilità

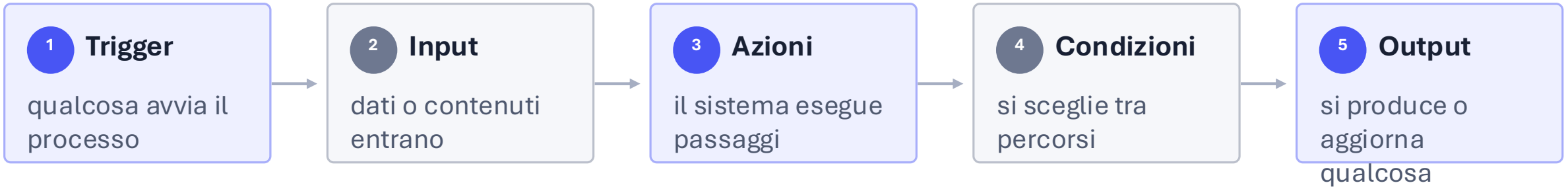
Aumentano anche variabilità, bisogno di controllo e rischio operativo

L’obiettivo non è arrivare sempre all’agente: è scegliere il livello di autonomia adatto al problema.

Che cos’è un workflow?

WORKFLOW

Una sequenza organizzata di attività che trasforma un input in un risultato.



Un workflow può essere completamente deterministico: stesso input + stesse regole → stesso percorso.

Esempio: invio di un modulo → salvataggio → notifica → archiviazione.

Anatomia di un workflow

DESIGN

Sei elementi da riconoscere prima ancora di scegliere una piattaforma.

Trigger

Quando parte?
nuovo form, nuova email, orario, evento

Input

Che cosa entra?
testo, file, dati, record, messaggio

Action

Che cosa accade?
crea, invia, trasforma, salva, chiama API

Condition

Quale percorso?
if/else, filtri, router, regole

Output

Che cosa ottengo?
documento, email, record, notifica

Control

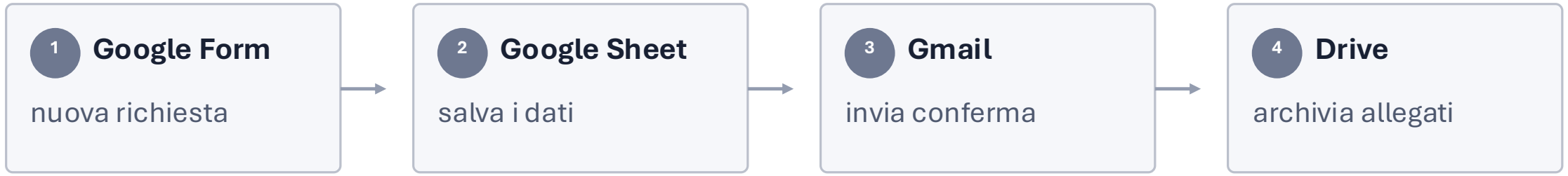
Come verifico?
log, errori, approvazione, metriche

Prima domanda progettuale: quali passaggi sono regole? quali richiedono interpretazione?

Automazione deterministica: un esempio

ESEMPIO

Il percorso è progettato in anticipo e non cambia in base a una decisione del modello.



PREVEDIBILE

RIPETIBILE

AUDITABILE

BASSO RISCHIO

Ottimo quando regole e percorso sono stabili.

Dove entra l’AI in un workflow?

AI WORKFLOW

L’AI è utile soprattutto dove il dato è ambiguo, non strutturato o richiede generazione.

Classificare

capire il tipo di richiesta, tema, urgenza, sentiment

Estrarre

ricavare dati da email, PDF, brief o conversazioni

Generare

produrre copy, sintesi, varianti, immagini, risposte

Valutare

confrontare output con criteri o policy

Trasformare

riscrivere, tradurre, adattare tono e formato

Supportare decisioni

proporre una categoria, priorità o azione successiva

AI workflow = percorso progettato + passaggi cognitivi affidati a un modello.

Pattern comuni di AI workflow

PATTERN

Schemi semplici e componibili sono spesso più efficaci di architetture inutilmente complesse.

Prompt chaining

Un output diventa input del passo successivo.
Analizza → sintetizza → adatta

Routing

L'AI classifica e indirizza verso un percorso.
Evento → social | stampa | newsletter

Parallelization

Più elaborazioni indipendenti lavorano in parallelo.
3 proposte → confronto

Evaluator–Optimizer

Un modello genera, un criterio valuta, poi si migliora.
Bozza → verifica → revisione

La complessità va aggiunta solo quando produce un vantaggio misurabile.

Attenzione: “usa un LLM” non significa “è un agente”

DISTINZIONE

L’elemento distintivo è chi controlla il percorso operativo.

AI workflow

Il percorso è definito dal sistema.

1. Classifica
2. Genera
3. Verifica
4. Invia in approvazione

Workflow: “segui questi passi”

AI Agent

DINAMICO

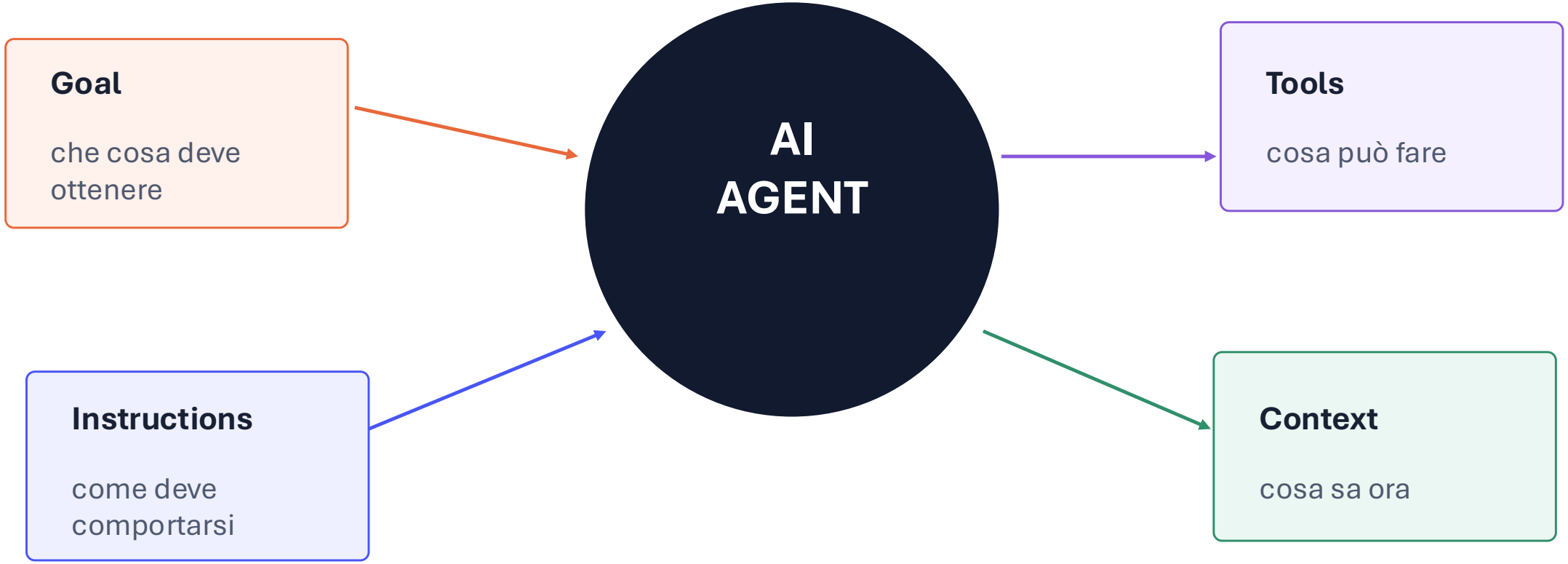
Riceve un obiettivo e può scegliere:

- quali tool usare
- in quale ordine
- quando cercare altri dati
- quando fermarsi o chiedere aiuto

Agent: “raggiungi questo obiettivo entro questi limiti”

Che cos’è un AI Agent?

Un sistema orientato a un obiettivo che combina modello, istruzioni e strumenti per eseguire azioni multi-step.



L’agente non è solo il modello: è l’intero sistema che lo rende capace di agire.

Anatomia di un agente

ARCHITETTURA

I componenti che trasformano un modello in un sistema operativo orientato a un obiettivo.

Model

interpreta, valuta opzioni, seleziona il prossimo passo

Instructions

obiettivi, ruolo, limiti, policy operative

Tools

API, ricerca, database, file, email, calendario…

Context / State

dati correnti, risultati precedenti, stato del task

Guardrails

vincoli, permessi, filtri, approvazioni

Evaluation

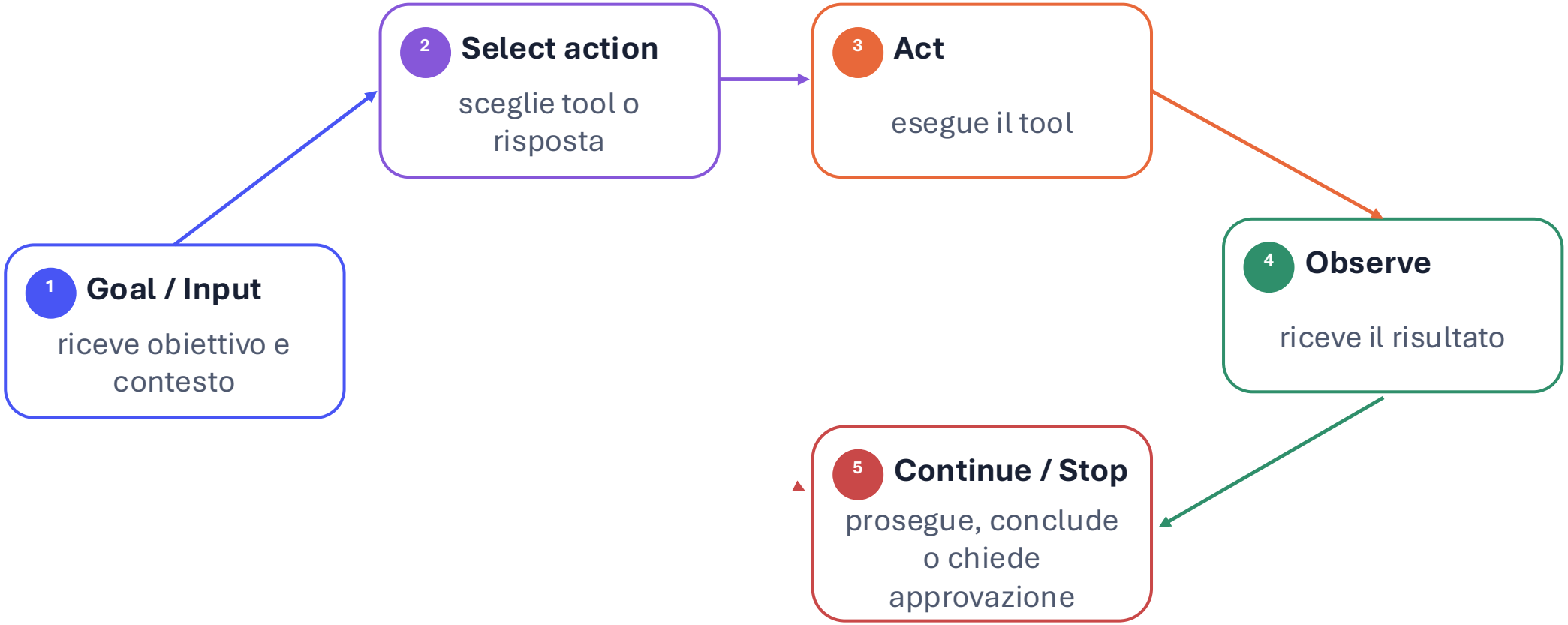
tracce, metriche, test e feedback sul comportamento

Progettare un agente significa progettare anche strumenti, permessi, stato e verifica.

Il ciclo agentico

AGENT LOOP

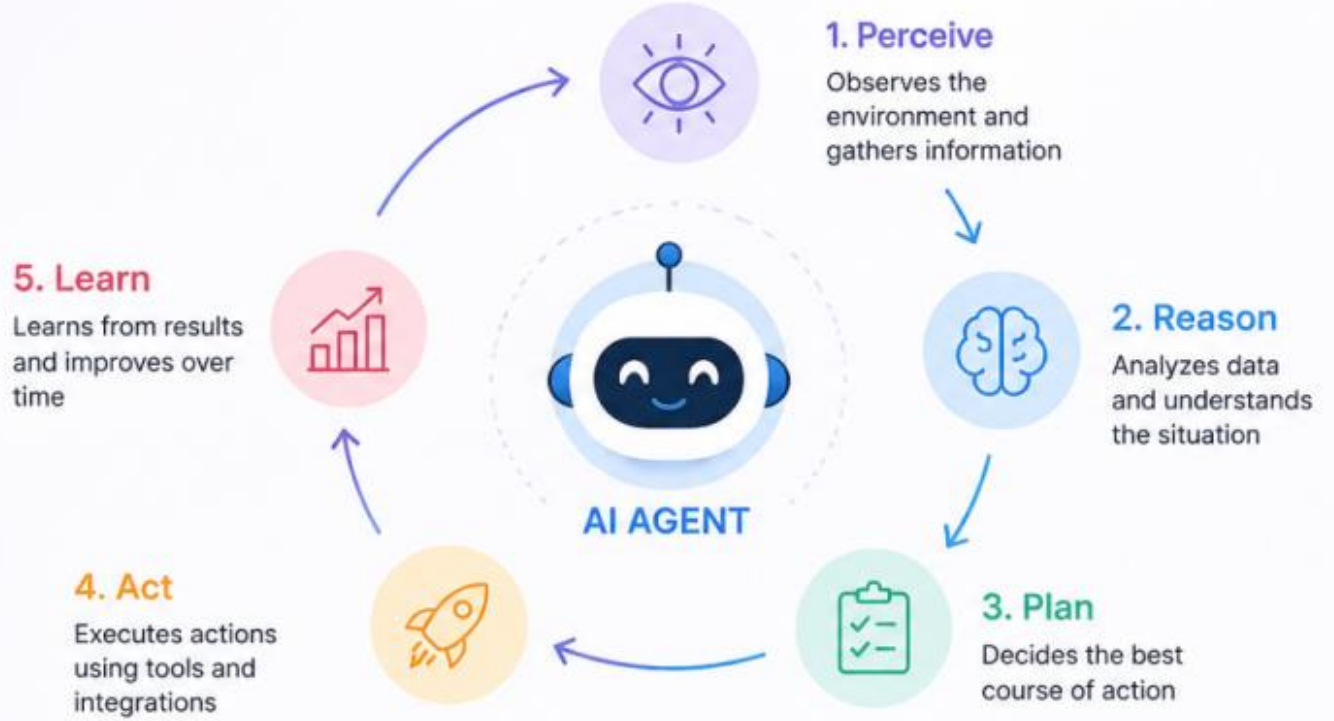
Il modello decide il prossimo passo sulla base dello stato e dei risultati ottenuti.



Il ciclo è limitato da strumenti disponibili, permessi, budget, criteri di arresto e approvazioni.

Agentic AI

AI That Thinks, Decides & Acts Independently



What It Can Do

- Understand Goals
- Make Decisions
- Use Tools
- Deliver Results Autonomously

Agentic AI powers the future of automation

- Smarter Workflows
- Higher Productivity
- Better Outcomes
- Continuous Improvement

hirist.tech

Workflow vs AI Agent

CONFRONTO

Due architetture diverse: scegliere in base alla variabilità del problema.

Dimensione	Workflow	AI Agent
Percorso	Predefinito	Dinamico entro limiti
Decisioni	Regole / router	Modello + istruzioni + stato
Tool	Invocati in punti stabiliti	Scelti in base al task
Prevedibilità	Alta	Più variabile
Controllo	Più semplice	Richiede guardrail e tracing
Ideale per	Processi stabili e ripetitivi	Task complessi e context-sensitive

Regola pratica: se puoi descrivere bene il percorso, inizia da un workflow.

Livelli di autonomia

“Agentico” non significa “senza supervisione”. L’autonomia può essere graduata.

Assistivo

propone, l’utente decide

Esempio:
Bozza di post

Supervisionato

agisce dopo approvazione

Esempio:
Invio newsletter

Bounded autonomy

agisce da solo entro regole e limiti

Esempio:
Classifica e aggiorna CRM

Alta autonomia

gestisce task lunghi e multi-step

Esempio:
Ricerca + azioni su più sistemi

Più aumenta l’autonomia, più diventano importanti permessi, logging, evaluation e rollback.

Single-agent e multi-agent

Più agenti non significa automaticamente un sistema migliore.

Single-agent

START HERE

Un agente gestisce il task e usa più strumenti.

Vantaggi:
- architettura più semplice
- meno coordinamento
- debugging più facile

Da preferire come punto di partenza.

Multi-agent

SPECIALISTS

Più agenti specializzati collaborano o si passano il controllo.

Utile quando:
- domini davvero distinti
- responsabilità separate
- handoff chiari
- task molto articolati

Complessità organizzativa e costi crescono rapidamente con il numero di agenti.

Connettere agenti, dati e strumenti

TREND

L’ecosistema sta convergendo su standard di interoperabilità.

MCP — Model Context Protocol

TOOLS & CONTEXT

Standard aperto per collegare applicazioni AI a sistemi esterni: dati, tool e workflow.

Idea chiave:
AI application ↔ tool / data source

A2A — Agent2Agent

AGENT COLLABORATION

Protocollo aperto per consentire a agenti differenti di collaborare e scambiarsi task.

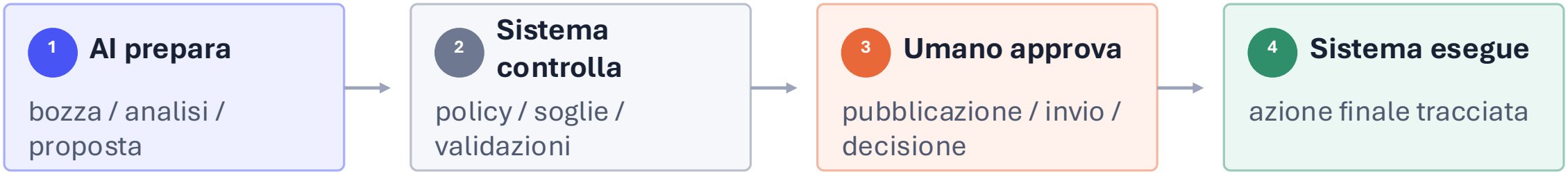
Idea chiave:
agent ↔ agent

Non serve implementarli nel corso: è utile capire la direzione del mercato.

Human-in-the-loop

GOVERNANCE

L’intervento umano non è un fallimento dell’automazione: è una scelta di governance.



Quando inserire un approval gate?

Azioni esterne • contenuti pubblici • dati sensibili • spese • modifiche irreversibili • messaggi a clienti / stakeholder

Rischi da progettare

RISK

L’autonomia aumenta la superficie di errore: servono limiti, test e osservabilità.

Errore / hallucination

informazione o decisione errata

Tool misuse

azione corretta eseguita nel contesto sbagliato

Prompt injection

input esterno tenta di deviare il comportamento

Privacy

dati sensibili passano a sistemi non appropriati

Loop / costi

l’agente continua più del necessario

Accountability

chi controlla e risponde dell’azione finale?

Mitigazioni: least privilege • approval gates • input validation • tracing • evaluation • fallback.

Workflow e agenti nella comunicazione

USE CASE

Esempi concreti: non tutti richiedono lo stesso livello di autonomia.

Adattare un comunicato a 3 canali	AI workflow
Classificare richieste stampa e inoltrarle	AI workflow
Generare report settimanale da fonti note	AI workflow
Gestire una richiesta complessa cercando dati e scegliendo tool	Agent
Preparare un media brief scegliendo autonomamente fonti e passi	Agent supervisionato
Pubblicare automaticamente sui social	Solo con forti approval gate

Criterio

Quanto è stabile il percorso?

Quanto è rischiosa l'azione?

Posso verificare il risultato?

Serve davvero decisione dinamica?

Caso: Teramo Future Fest

CASE STUDY

Lo stesso obiettivo può essere progettato come workflow o come agente.

A. AI workflow

Obiettivo: gestire nuove richieste di comunicazione.

Form → classificazione → generazione bozza → controllo → Google Sheet → email di approvazione

Il percorso è noto e ripetibile.

B. Agent supervisionato

PIÙ DINAMICO

Obiettivo: preparare il pacchetto settimanale di comunicazione.

L’agente consulta fonti, individua attività rilevanti, sceglie canali, genera bozze, segnala dati mancanti e propone il piano.

L’umano approva prima della pubblicazione.

Prima di scegliere l’agente chiediamoci: il workflow fisso è già sufficiente?

Quando NON serve un agente

DESIGN PRINCIPLE

Una buona architettura è la più semplice che soddisfa il requisito.

Percorso stabile

Le regole possono essere definite chiaramente.

Task breve

Una singola chiamata al modello è sufficiente.

Rischio alto

L'azione non è facilmente verificabile o reversibile.

Criteri deboli

Non sappiamo misurare se il task è riuscito.

Costi / latenza

Il ciclo agentico aggiunge chiamate e tempi.

Dati insufficienti

L'agente non può compensare fonti mancanti o non affidabili.

Principio: partire semplice → misurare → aggiungere autonomia solo dove serve.

Mini-esercizio: workflow o agente?

IN AULA

Per ogni scenario scegli l’architettura minima sufficiente e motiva la scelta.

1. Una nuova risposta Google Form deve essere salvata e notificata via email. ?

2. Un brief deve essere classificato e trasformato in tre varianti social. ?

3. Il sistema deve preparare un media brief cercando dati in più fonti e scegliendo autonomamente cosa approfondire. ?

4. Un contenuto deve essere pubblicato automaticamente dopo un controllo di conformità. ?

Domande guida: il percorso è noto? serve una decisione dinamica? qual è il rischio dell’azione?

Takeaway

RECAP

Prima di costruire, scegli il livello di autonomia adatto al processo.

1. Un workflow orchestra un percorso.
2. Un AI workflow usa modelli dentro un percorso progettato.
3. Un agente può decidere dinamicamente come raggiungere un obiettivo.
4. Tool, guardrail, stato e evaluation sono parte del sistema.
5. **Human-in-the-loop e autonomia limitata sono spesso la scelta professionale.**

Prossima lezione

Costruiamo un workflow in Make e inseriamo progressivamente AI, routing e controllo umano.