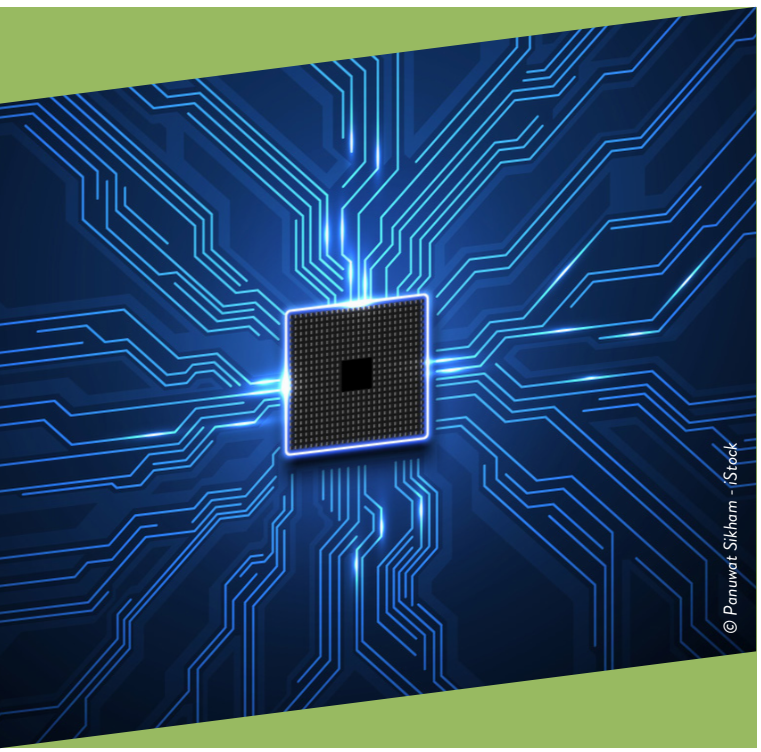
HARDWARE, LA CHIAVE DELLA QUALITÀ AI

di MARIA MORO



PER UNA MACCHINA ESSERE AFFIDABILE SIGNIFICA GARANTIRE UNA DISPONIBILITÀ CONTINUATA E DARE LA CERTEZZA DEL RISULTATO. LE POTENZIALITÀ DEI SISTEMI AUTONOMI ABILITATI DA INTELLIGENZA ARTIFICIALE SONO SUPERIORI ALLE CAPACITÀ DELLA PERCEZIONE UMANA DI RICONOSCERE FACILMENTE UN MALFUNZIONAMENTO, PER QUESTO RICHIEDONO UN'ESTREMA QUALITÀ DEI COMPONENTI CHE ABILITANO IL CALCOLO E L'INTERPRETAZIONE DELLE IMMAGINI

La possibilità di implementare soluzioni di intelligenza artificiale ha notevolmente aumentato negli ultimi due decenni il ricorso all'uso di sistemi autonomi intelligenti, capaci di affiancare l'essere umano migliorandone le prestazioni o di sostituire del tutto l'attività umana nello svolgimento di lavori. Nel primo caso, l'intelligenza artificiale migliora la precisione e la velocità di un dato lavoro, aumenta la capacità di calcolo, aiuta a interpretare situazioni. Nel secondo caso, trova applicazione, ad esempio, nei vari ambiti della robotica – lungo le linee di produzione industriale, in campo militare, in agricoltura… – e tende ad arrivare ai modelli più avanzati di veicoli a guida autonoma e a sistemi che siano in grado di interagire con altre macchine, con l'ambiente, con le persone e che siano capaci di apprendere, decidere, pianificare.

I sistemi autonomi sono spesso guidati da un'intelligenza artificiale basata sull'utilizzo di reti neurali, strutture che emulano i processi di apprendimento della mente umana e che vengono "addestrate" utilizzando enormi quantità di dati. La tecnologia che sostiene le capacità delle reti neurali è costituita da software e da dispositivi elettronici hardware, come i microprocessori.

Di fianco alle grandi risorse dei sistemi autonomi si sviluppano anche potenziali rischi, che riguardano in linea generale la capacità di fornire risposte corrette

agli ordini impartiti, la possibilità di causare danni al contesto in cui il sistema opera, l'esposizione ad attacchi cyber. In questo senso, e a garanzia della piena operatività, ai sistemi autonomi vengono richiesti requisiti di affidabilità, di *safety*, di sicurezza e di disponibilità, tanto più elevati quanto maggiore è il livello di autonomia.

Per affidabilità si intende la garanzia della continuità operativa; con safety, cioè la sicurezza nell'uso, si definisce la capacità di un sistema di mettersi in condizioni di sicurezza per non aggravare un rischio, ad esempio arrestandosi; il sistema deve poi garantire la sicurezza dei dati anche nell'eventualità di un malfunzionamento, e deve essere disponibile nella sua interezza quando se ne richiede l'utilizzo.

La complessità di elaborazione dei sistemi di intelligenza artificiale, eseguita in tempi rapidi e non paragonabili con le capacità umane, impone la necessità che i risultati siano certi e attendibili.

La realizzazione di tutti questi requisiti necessita di componenti hardware che devono essere progettati per garantire la più elevata affidabilità e sicurezza.

Il componente fisico che costituisce la parte hardware dell'intelligenza artificiale e ne permette l'implementazione può essere però vulnerabile a guasti che compaiano durante il suo funzionamento. Tale eventualità rischia di alterare l'esito dell'elaborazione del sistema intelligente, in una modalità che può essere colta o meno – e a diversi gradi di percezione – dall'uomo o dalle macchine stesse.

Un fenomeno tipico che può portare all'errore è l'invecchiamento dei componenti hardware, che può avere come effetto un rallentamento sensibile nell'esecuzione delle operazioni ma anche, nel caso di acceleratori hardware che eseguono reti neurali per il riconoscimento di immagini su sistemi autonomi, un'alterata interpretazione dell'immagine che si tradurrebbe in un comando errato alla macchina, eventualità potenzialmente molto dannosa.

IL RISULTATO DIPENDE DALL'AFFIDABILITÀ DEI COMPONENTI

Tutto ciò rende chiara l'esigenza di elevata affidabilità delle parti fisiche del sistema.

Una volta fabbricati, tutti i componenti hardware, e in modo particolare i microprocessori, vengono collaudati prima di essere immessi nel mercato, al fine di evitare la possibilità che vengano fornite parti malfunzionanti. Ciò nonostante, il componente hardware potrebbe guastarsi durante il suo funzionamento: "L'affidabilità di un sistema di intelligenza artificiale ha come presupposto il fatto che i componenti hardware che lo implementano continuino a dare il proprio contributo in modo corretto per un certo intervallo di tempo. Il livello qualitativo dei prodotti immessi in commercio è tale che non ci si attendono dei difetti di produzione", afferma **Cecilia Metra**, professoressa all'**Università di Bologna**, direttore **IEEE** 2022-2023 e già presidente nel 2019 della **IEEE Computer Society**, "ma nonostante il livello qualitativo elevato che le imprese di produzione forniscono, i componenti hardware potrebbero guastarsi sul campo a causa di guasti indotti dall'ambiente di utilizzo e di fenomeni di invecchiamento dei materiali".

Come per ogni tecnologia, quindi, anche la parte hardware dei sistemi di intelligenza artificiale può essere soggetta a deterioramento, con la conseguente emersione di un rischio di qualità dei risultati attesi. L'alterazione che ne deriva può manifestarsi in maniera più o meno percepibile e può dare origine a un malfunzionamento nell'operatività; "nel caso, ad esempio, di un sistema autonomo con intelligenza artificiale implementata con reti neurali per il riconoscimento delle immagini, potrebbe accadere che un'immagine venga interpretata erroneamente, di conseguenza, a seconda dell'utilizzo specifico in atto, gli esiti potrebbero raggiungere diversi livelli di gravità, soprattutto qualora venissero coinvolti esseri umani come può verificarsi nel caso di un'auto totalmente autonoma", spiega Cecilia Metra. Un fatto di questo tipo potrebbe verificarsi in molti contesti e potrebbe riguardare anche i sistemi robotizzati che operano nelle catene di produzione delle imprese.

I POTENZIALI RISCHI DI MALFUNZIONAMENTO

Ricorrere all'esecuzione di algoritmi estremamente complessi comporta necessariamente una "delega sulla fiducia" riguardo la correttezza dell'elaborazione, che trova fondamento nella elevata qualità dei componenti tecnologici.

La ricerca accademica sta approfondendo il tema, puntando a soluzioni che irrobustiscano i sistemi per far fronte a simili eventualità. In ogni caso, per ridurre ulteriormente il rischio, si sta lavorando ad aumentare la capacità di individuare un malfunzionamento degli elementi hardware.

Un segnale di possibile guasto è il rallentamento della performance, che può essere rilevato da monitor che avvertano un'anomalia; questa casistica in genere è collegata ad alcuni tipi di invecchiamento dell'elettro-

nica. “La prevenzione e il monitoraggio continuo del malfunzionamento – afferma Metra – sono oggetto di ricerca e sviluppo di tecniche apposite, ad esempio si sta lavorando sul monitoraggio di alcuni parametri il cui valore può destare allarme se si presenta al di sopra di determinate soglie. In più, va considerato che gli stessi sistemi di monitoraggio dei parametri fanno spesso uso di algoritmi di intelligenza artificiale, quindi il tema dell’affidabilità riguarda pure le tecnologie utilizzate per il controllo”.

Un eventuale deterioramento delle parti hardware potrebbe generare conseguenze anche sulla qualità, sulla sicurezza e sull’integrità degli archivi di dati.

In questi casi si tratta di guasti cosiddetti transitori, cioè variazioni momentanee dei valori di tensione nel circuito che possono causare errori soft. “Negli archivi di dati, gli errori possono colpire le celle di memoria in cui i dati sono immagazzinati; normalmente però le memorie sono protette con codici a correzione di errore”, spiega Metra. “Se le memorie – aggiunge – sono protette mediante codici opportuni, i dati letti dalla memoria, seppur alterati da errori, saranno corretti dal sistema. Sussiste comunque una quota di rischio legata al tipo di codici utilizzati e all’hardware che li implementa, ed è necessario che la ricerca approfondisca le tecniche di correzione ed elaborazione da usare in relazione al livello di autonomia del sistema”.

Un ulteriore esempio di possibile danno da errori soft riguarda il malfunzionamento di acceleratori hardware che implementino reti neurali per il riconoscimento di messaggi non autorizzati riconducibili ad attacchi cyber, eventualità che potrebbe causare una generale compromissione della disponibilità del sistema di sicurezza.

LE SFIDE DI AUTO AUTONOMA E METAVERSO

Uno degli ambiti più noti in cui vengono applicati sistemi di intelligenza artificiale basati sulle reti neurali per il riconoscimento delle immagini è quello dei veicoli autonomi. Come avviene in tutti i settori in cui è richiesto un elevatissimo livello di *safety*, nell’auto autonoma la risoluzione delle sfide di sicurezza nell’uso rappresenta l’istanza prioritaria.

In realtà, spiega Metra, “sulla tecnologia oggi disponibile sul mercato si è iniziato a lavorare molti anni fa, parimenti il livello attuale della ricerca in questo campo e la relativa applicazione sul prodotto in fase di test sono molto più avanti rispetto a quanto si trova in commercio; si può affermare che la ricerca, anche in termini di safety, sta attualmente operando su prodotti che saranno disponibili tra alcuni anni”. I processi di verifica dell’affidabilità sono costanti e “se e quando si giungerà a realizzare automobili con livello di autonomia pari a cinque, quindi totalmente autonome nella guida, vorrà dire che i componenti saranno stati progettati per avere un grado di affidabilità estremamente elevato in risposta alle regolamentazioni che saranno definite”. Attualmente si è ancora lontani da questo scenario.

Le tecniche per la progettazione di componenti hardware a elevata affidabilità e sicurezza nell’uso per i sistemi di intelligenza artificiale sono quindi al centro di una vasta attività di ricerca finalizzata alla crescita delle tecnologie autonome.

Guardando al futuro, più o meno prossimo, uno degli ambiti di utilizzo dell’intelligenza artificiale potrà essere il metaverso, in una modalità molto più immersiva rispetto a quella attuale, ancora oggi vicina ai modelli di realtà virtuale. Per la piena applicazione delle potenzialità del metaverso nei contesti industriali o sociali, commenta Metra, “una delle sfide principali riguarda proprio la parte hardware, necessaria alla realizzazione di forme di intelligenza artificiale affidabili e sicure che aumentino il livello di interazione con la realtà virtuale e aumentata, grazie alla capacità di riconoscere le immagini, il testo, il parlato e la gestualità; in una completa integrazione tra strumenti digitali e mondo reale”.