PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5264 di Mercoledì 26 ottobre 2022

Sicurezza dei sistemi di IA

Come verificare la sicurezza funzionale e operativa di sistemi con intelligenza artificiale a cui non è possibile applicare alcun metodo di valutazione convenzionale poiché eccessivamente complessi, se non addirittura in grado di evolversi autonomamente?

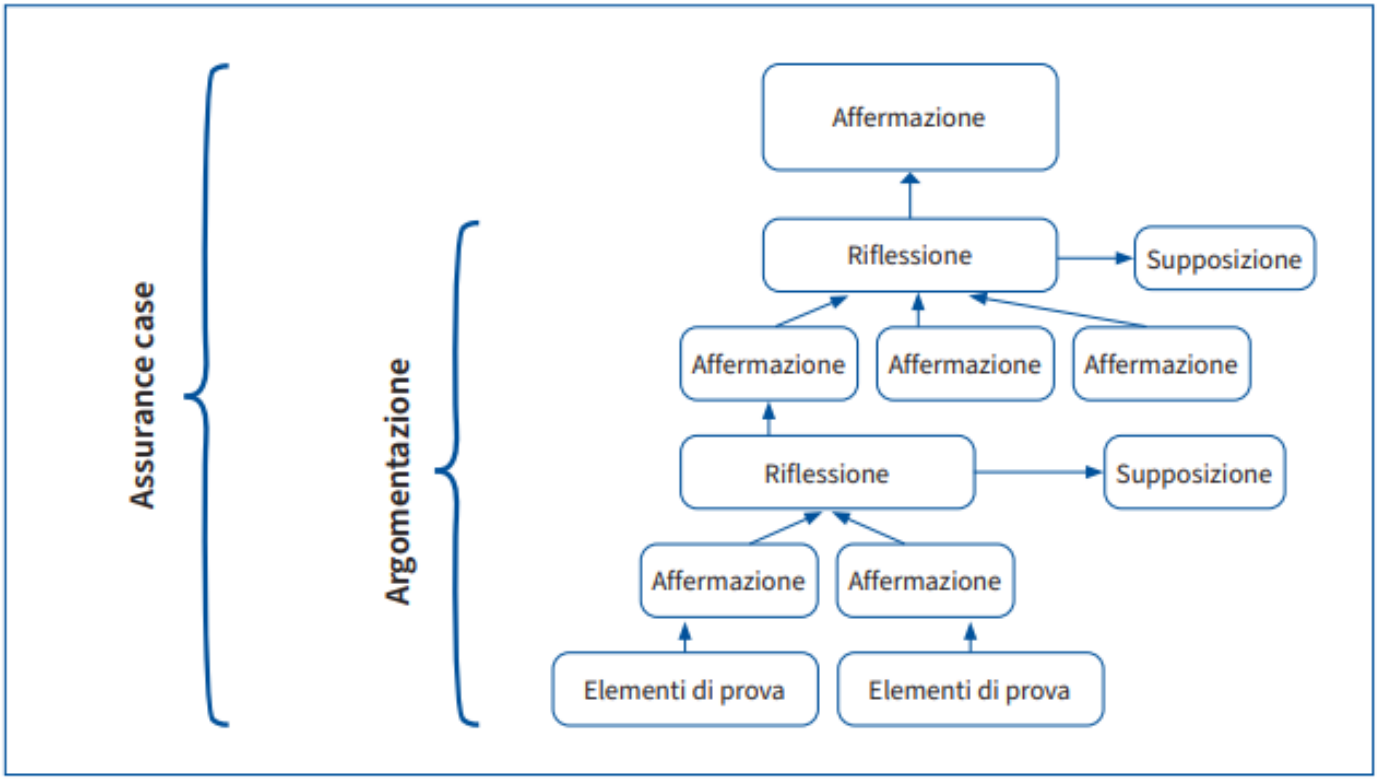
Nonostante anni di discussioni nell'ambito della normazione e regolamentazione, ad oggi non vige ancora un consenso circa una definizione di "sistema di IA". A livello di regolamentazione europea i più sono d'accordo nell'affermare che un sistema di Intelligenza Artificiale consiste in un determinato tipo di software. È invece poco chiaro in che modo quest'ultimo vada distinto da un software classico.

Nel caso dei sistemi autonomi e parzialmente autonomi le procedure normate per la valutazione della sicurezza si scontrano sempre più spesso con i loro limiti. Laddove si automatizzino dei compiti complessi in ambienti di utilizzo complessi, anche uno schema di sicurezza per quanto possibile semplice può farsi molto articolato. Varie misure ? p. es. la gestione dei fattori d'incertezza nel caso del riconoscimento ambientale ? si compenetrano dando luogo a diversi livelli di protezione ("Layers of Protection Architecture"). Gli ambienti di utilizzo e i compiti dei sistemi autonomi o parzialmente autonomi che s'intende automatizzare possono essere molto complessi. Ciò presuppone che i relativi livelli di protezione si basino su un software che, ai sensi della proposta di regolamentazione europea, è considerato essere un sistema di IA.

Argomentazione sulla sicurezza tramite assurance case

Nel caso di schemi di sicurezza così complessi occorre procedere a un'argomentazione sulla sicurezza in grado di garantire che l'intero schema regga davvero a lungo. Un approccio in tal senso adeguato sembra essere quello degli assurance case definiti nella ISO/IEC 15026 (Systems and software assurance). Questi sono generalmente considerati adatti laddove, in relazione a una determinata tecnologia, non sia ancora stata maturata un'esperienza sufficiente all'interno del contesto critico in termini di sicurezza?.

In via di principio un assurance case comprende un'affermazione, ancora da dimostrare, circa il livello di sicurezza che s'intende raggiungere e la relativa argomentazione, che si fonda su una serie di elementi e prove favorevoli.



Struttura logica di un assurance case

Come illustrato dall'immagine, l'argomentazione può essere impostata in modo gerarchico esplicitando singole riflessioni. Ciascuna riflessione collega un'affermazione da dimostrarsi (p. es.: il prodotto è sicuro) a delle premesse (p. es.: il rischio elettrico è sotto controllo). Al livello successivo queste fungono a loro volta da nuove affermazioni e vengono collegate ad altre premesse in ulteriori riflessioni (p. es.: nessun danno al cavo di alimentazione <- l'isolamento è sufficiente).

Spesso la conclusione logica che, partendo da determinate premesse, porta a un'affermazione, vale solo nel caso di determinate supposizioni, p. es. quella di un certo contesto di utilizzo (p. es.: l'utilizzatore ha esperienza / le correnti elettriche sono inferiori a...). Tali supposizioni vengono definite in fase di sviluppo ed esplicitamente documentate nell'assurance case. Ogni affermazione non ulteriormente approfondita deve essere corroborata da elementi di prova quali documentazioni o esiti di verifiche.

Un assurance case elaborato offre una serie di vantaggi. Riunisce in maniera modulare tutti i necessari elementi (artefatti) per l'argomentazione sulla sicurezza e, attraverso speciali moduli di programma (Digital Dependability Identities), può essere integrato nel software del sistema complessivo. Durante l'utilizzo è così possibile verificare che importanti supposizioni e affermazioni risultino soddisfatte, in modo da individuare precocemente eventuali punti deboli dell'assurance case, perfezionare di continuo quest'ultimo e modificarlo in funzione dei cambiamenti nell'ambiente di utilizzo . Gli assurance case offrono però soprattutto un alto grado di flessibilità per quel che riguarda la strutturazione dell'argomentazione. Ciò permette di considerare le particolarità dell'impiego concreto e delle tecnologie utilizzate.

Possibilità di attuazione pratica

Per gestire questa flessibilità in modo produttivo, vi sono degli ausili pratici. Il metodo AMLAS , p.es., descrive delle procedure generiche per la strutturazione di un'argomentazione sulla sicurezza. L'AMLAS, tuttavia, non stabilisce cosa significhi l'espressione "sufficientemente sicuro" nel caso di un sistema di Intelligenza Artificiale.

Nell'ambito del progetto ExamAI è stata elaborata una proposta su come potrebbero essere impostati i metodi di prova per sistemi di IA. Tale proposta si basa su due linee argomentative indipendenti?6 : la prima mira a dimostrare che, per quanto possibile nella pratica, il rischio per la sicurezza è stato ridotto scegliendo una combinazione di misure di protezione

possibilmente efficace e implementandola nel miglior modo possibile dopo aver soppesato i costi e benefici del caso. La seconda punta invece a dimostrare in termini quantitativi che la riduzione del rischio ottenuta è sufficiente.

Nel quadro del progetto di ricerca LOPAAS?7 si stanno attualmente riunendo questi e altri approcci elaborati da ricercatori. I partner di progetto fanno inoltre confluire il consenso scientifico in attività di standardizzazione e normazione come la regola di applicazione per sistemi cognitivi autonomi VDE-AR-E 2842-61, il rapporto tecnico 5469 di ISO e IEC sull'IA e la sicurezza funzionale o la BSI PAS 8800 per l'IA critica dal punto di vista della sicurezza nel settore automobilistico.

Raccomandazioni operative

Innanzitutto nell'ambito della regolamentazione e della normazione andrebbero elaborate delle definizioni coerenti dei concetti di "sistema di IA" e "sistema autonomo". Solo così sarà possibile comprendere e colmare le lacune riscontrabili nella regolamentazione e nella normazione in materia di sicurezza e altri beni giuridici. In secondo luogo occorrerebbe incentivare la ricerca in fatto di assurance case ? e con essa la partecipazione dei ricercatori alle attività di normazione e standardizzazione ? e diffondere tra i soggetti interessati il know-how maturato relativamente agli assurance case. In terzo luogo sarebbe necessario formulare i requisiti regolamentari in maniera tale che offrano un buon punto di partenza per l'elaborazione e applicazione di norme sugli assurance case. Detti requisiti regolamentari dovrebbero concentrarsi sulle affermazioni indispensabili per la sicurezza, che solitamente sono riportate nella parte alta del testo di un assurance case. Possono invece risultare problematici i requisiti a valle che, a seconda del tipo di argomentazione o del caso applicativo, non devono necessariamente essere parte di un'argomentazione valida sulla sicurezza. Dei requisiti regolamentari su dettagli del genere potrebbero limitare inutilmente i margini di attuazione o causare un'inutile mole di lavoro.

Rasmus Adler
Michael Kläs

Fonte: KanBrief, 3/2022
