

PIANO DELLE ATTIVITÀ

- Progetto di ricerca correlato all'incarico di ricerca:

Il progetto di ricerca mira ad affrontare la crescente necessità di sviluppare sistemi di intelligenza artificiale non solo altamente performanti, ma anche sicuri, affidabili e conformi ai quadri normativi emergenti che ne disciplinano l'impiego, tra cui l'EU AI Act. L'attività si concentra sulla progettazione di metodologie ibride che integrino tecniche di machine learning con approcci simbolici e strumenti di ottimizzazione matematica, al fine di garantire il soddisfacimento di proprietà formali quali correttezza, robustezza, equità e verificabilità nei sistemi di AI data-driven. L'obiettivo è superare i limiti dei modelli puramente statistici, introducendo meccanismi di controllo e validazione formalmente fondati. Particolare attenzione sarà dedicata ai sistemi autonomi e agentici, specialmente quelli basati su Large Language Models, caratterizzati da elevata autonomia decisionale e da interazioni dinamiche con ambienti complessi. In tali contesti, la capacità di assicurare comportamenti prevedibili, controllabili e conformi a specifiche formali diventa cruciale. Il progetto intende quindi sviluppare strumenti teorici e computazionali per il monitoraggio, la verifica e l'enforcement delle proprietà desiderate, contribuendo alla realizzazione di sistemi di AI affidabili e responsabili.

- Descrizione delle attività di assistenza alla ricerca che saranno affidate al titolare dell'incarico:

Il titolare dell'incarico sarà coinvolto nelle attività di supporto scientifico e tecnico connesse allo sviluppo del progetto di ricerca. In particolare, collaborerà alla definizione e implementazione delle metodologie proposte, contribuendo all'analisi teorica, alla modellazione formale e alla sperimentazione computazionale.

Le attività includeranno:

- supporto alla progettazione e allo sviluppo di modelli e algoritmi;
- implementazione e validazione sperimentale delle soluzioni proposte;
- raccolta, organizzazione e analisi dei dati necessari alle attività di ricerca;
- redazione di report tecnici e contributo alla preparazione di pubblicazioni scientifiche;
- collaborazione all'organizzazione di incontri di progetto e alla disseminazione dei risultati.

Il titolare opererà in coordinamento con il responsabile scientifico, contribuendo al raggiungimento degli obiettivi progettuali nel rispetto delle tempistiche e delle linee guida definite.

- Piano delle attività:

L'attività di ricerca sarà articolata nelle seguenti fasi:

- 1) Analisi preliminare e definizione del quadro metodologico: studio dello stato dell'arte e individuazione delle proprietà formali e degli obiettivi di ricerca.
- 2) Progettazione e sviluppo: definizione di modelli e metodologie ibride, con integrazione di tecniche di machine learning, approcci simbolici e strumenti di ottimizzazione.

3) Implementazione e sperimentazione: sviluppo di prototipi, validazione sperimentale e analisi dei risultati.

4) Valutazione e diffusione: verifica delle prestazioni e delle proprietà garantite, redazione di report scientifici e preparazione di pubblicazioni.

Le attività saranno svolte in coordinamento con il responsabile scientifico, nel rispetto delle tempistiche previste dal progetto.

RESEARCH PLAN

- Research project related to the “incarico di ricerca”:

The research project aims to address the growing need to develop artificial intelligence systems that are not only highly performant, but also safe, reliable, and compliant with emerging regulatory frameworks governing their deployment, including the EU AI Act. The research activity focuses on the design of hybrid methodologies that integrate machine learning techniques with symbolic approaches and mathematical optimization tools, in order to guarantee the satisfaction of formal properties such as correctness, robustness, fairness, and verifiability in data-driven AI systems. The goal is to overcome the limitations of purely statistical models by introducing formally grounded mechanisms for control and validation. Particular attention will be devoted to autonomous and agentic AI systems, especially those based on Large Language Models, which are characterized by high degrees of decision-making autonomy and dynamic interaction with complex environments. In such settings, ensuring predictable, controllable, and specification-compliant behavior becomes crucial. The project therefore aims to develop theoretical and computational tools for monitoring, verification, and property enforcement, contributing to the advancement of trustworthy and responsible AI systems.

- Description of research assistance activities of the contract holder:

The appointee will be involved in providing scientific and technical support related to the development of the research project. In particular, they will collaborate in the definition and implementation of the proposed methodologies, contributing to theoretical analysis, formal modeling, and computational experimentation.

The activities will include:

- supporting the design and development of models and algorithms;
- implementing and experimentally validating the proposed solutions;
- collecting, organizing, and analyzing data relevant to the research activities;
- drafting technical reports and contributing to the preparation of scientific publications;
- assisting in the organization of project meetings and in the dissemination of research results.

The appointee will work under the supervision of the Principal Investigator, contributing to the achievement of the project objectives in accordance with the established timeline and guidelines.

- Research Activities Plan:

The research activity will be structured into the following phases:

- 1) Preliminary analysis and methodological framework definition: review of the state of the art and identification of formal properties and research objectives.
- 2) Design and development: definition of hybrid models and methodologies integrating machine learning techniques, symbolic approaches, and optimization tools.
- 3) Implementation and experimentation: development of prototypes, experimental validation, and analysis of results.
- 4) Evaluation and dissemination: assessment of performance and guaranteed properties, preparation of technical reports, and drafting of scientific publications.

All activities will be carried out in coordination with the Principal Investigator and in accordance with the project timeline.