Codice concorso: ARIC/05_24

Tipologia di contratto	Ricercatore Universitario a tempo determinato tipo A
Regime di impegno	Tempo pieno
Oggetto del contratto *in italiano*	Sviluppo di metodologie per l'identificazione di minacce cyber o cyber-fisiche in scenari industriali
Oggetto del contratto *in inglese*	Development of Methodologies for Identifying Cyber or Cyber-Physical Threats in Industrial Environments
Programma di Ricerca *in italiano*	Il progetto si propone di sviluppare algoritmi avanzati di rilevamento e risposta alle anomalie ciber-fisiche per migliorare la sicurezza e la resilienza dei Sistemi di Controllo Industriale integrati in Industrial Cyber Physical Systems. Si intende proporre un framework "multi-formalismo" ibrido per combinare i risultati dei rilevatori di anomalie comportamentali non supervisionati applicati a dati derivanti dal traffico di rete e fisici utilizzando reti bayesiane. L'obiettivo sarà quello di saper discriminare minacce fisiche da minacce cyber ed identificare, inoltre, eventuali ripercussioni di una minaccia cyber sulle dinamiche fisiche del processo esaminato. I risultati della ricerca saranno testati in un ambiente reale costituito da un test range cyber-fisico caratterizzato dalla presenza di protocolli di rete industriali, hardware e software perfettamente in linea con reali impianti industriali. Infine, si intende realizzare un sistema di risposta alle minacce cyber in grado di minimizzare l'impatto della minaccia sulle dinamiche dell'impianto incrementandone la resilienza.
Programma di Ricerca *in inglese*	The project aims to develop advanced cyber-physical anomaly detection and response algorithms to enhance the security and resilience of Industrial Control Systems integrated into Industrial Cyber-Physical Systems. A hybrid "multi-formalism" framework will be proposed to combine the results of unsupervised behavior-based anomaly detectors applied to data derived from network traffic and physical processes using Bayesian networks. The objective is to distinguish physical threats from cyber threats and identify the potential repercussions of a cyber threat on the physical dynamics of the examined process. The research results will be tested in a real environment consisting of a cyber-physical test range characterized by the presence of industrial network protocols, hardware, and software perfectly aligned with real industrial plants. Finally, the project aims to develop a cyber threat response system capable of minimizing the impact of threats on plant dynamics, thereby increasing its resilience.
Dati del progetto	Il programma di ricerca è pienamente coerente con le tematiche previste dal PNR 2021-2027 di seguito specificate: Ambito 5.3.3 Cybersecurity Articolazione 3. Tecniche e metodologie per la protezione delle risorse
Gruppo Scientifico-Disciplinare	09/IINF-04 - Automatica
Settore Scientifico Disciplinare	IINF-04/A - Automatica
Durata del contratto	Durata triennale, rinnovabile ai sensi dell'art 3, comma 1, lettera a) del Regolamento di Ateneo

Facoltà Dipartimentale di afferenza	Ingegneria
Referente per l'attività di ricerca	Ing. Luca Faramondi
Obiettivi di produttività *in italiano*	Gli obiettivi di produttività scientifica si sostanziano in: pubblicazioni scientifiche su riviste internazionali indicizzate, partecipazioni a congressi nazionali ed internazionali come relatore, individuazione di linee di ricerca, avvio di collaborazioni scientifiche con Enti ed Istituzioni nazionali ed internazionali e realizzazione di attività nell'ambito della Terza Missione.
Obiettivi di produttività *in inglese*	The scientific productivity goals are embodied in: scientific publications in indexed international journals, participation in national and international conferences as a speaker, identification of research lines, initiation of scientific collaborations with national and international entities and institutions, and the execution of activities within the framework of the Third Mission.
Impegno didattico	L'impegno annuo complessivo (didattica frontale, integrativa e servizio agli studenti) è pari a 350 ore annue, di cui fino a un massimo di 80 ore di didattica frontale.
Numero massimo di pubblicazioni	12
Conoscenze e competenze linguistiche	Inglese
Titoli	Dottorato di ricerca nell'ambito dell'Ingegneria dell'Automazione o dell'Ingegneria Informatica o titolo equivalente

Documento firmato digitalmente