PIANO TRIENNALE DI REALIZZAZIONE 2025-27 - RICERCA DI SISTEMA ELETTRICO NAZIONALE
Progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

Obiettivo: Digitalizzazione ed evoluzione delle reti

Progetto 2.1 - Progetto Integrato Cyber Security dei sistemi energetici per la transizione energetica-digitale
Durata: 36 mesi
Periodo attività: 01/01/2025 - 31/12/2025

ABSTRACT ATTIVITA' ANNUALE:

Il presente documento descrive le attività di ricerca del Progetto Integrato "Cyber Security dei sistemi energetici per la transizione energetica-digitale" svolte durante la prima annualità di progetto.
Le attività di ricerca hanno riguardato le seguenti Linee di Attività:

- ENEA (affidatario del progetto) per LA1.2, LA1.3, LA2.2, LA3.2, LA3.3, LA3.4, LA3.5, LA4.2
- Università degli Studi di Foggia-Dipartimento di Scienze Agrarie, Alimenti, Risorse Naturali e Ingegneria per LA3.6
- Università degli Studi di Genova-Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi per LA1.5
- Università degli Studi di Napoli Federico II-Dipartimento di Ingegneria Industriale per LA2.4
- Università di Padova-Centro Interdipartimentale di Ricerca "Padua Quantum Technologies Research Center" per LA1.4
- Università degli Studi Roma Tre-Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche per LA2.3, LA3.7
- Università degli Studi di Trento-Dipartimento di Ingegneria e Scienza dell'Informazione per LA3.8

ATTIVITA' SVOLTE

WP1: Cybersecurity delle comunicazioni per le nuove applicazioni digitali dei sistemi energetici

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	La linea **LA1.2 "Definizione dei casi d'uso e dei requisiti di una infrastruttura sperimentale per test su reti energetiche dotate di servizi di comunicazione QKD in free space e su fibra"** ha come obiettivo l'estensione delle tecniche QKD (Quantum Key Distribution) alle reti e microreti elettriche prive di un mezzo trasmissivo in fibra. Nel precedente triennio di ricerca, infatti, l'indagine si era limitata ai sistemi

	elettrici già dotati di un'infrastruttura in fibra ottica, per il trasferimento di dati e comandi tra apparati, misuratori e controllori. Nella presente annualità, i ricercatori ENEA hanno inizialmente avviato la definizione dei requisiti della nuova infrastruttura sperimentale, concepita per configurare e condurre test di comunicazione QKD sia su fibra ottica sia in free space (cammini liberi in aria). Sulla base dei requisiti identificati, è stata condotta un'attività di scouting industriale e commerciale per individuare la strumentazione e gli apparati necessari alla realizzazione del laboratorio. Nel corso di tale attività, è emersa una criticità: gli apparati necessari alla comunicazione QKD in free space non risultano attualmente disponibili sul mercato. Si tratta, infatti, di tecnologie sviluppate e testate prevalentemente in contesti accademici o da spin-off di settore, non ancora ingegnerizzate per la commercializzazione su larga scala. Per superare tale limitazione, ENEA, in accordo con i ricercatori di UniPD-QTech, condurrà le attività di test avvalendosi della strumentazione prototipale sviluppata dall'Università di Padova. Infine, le attività si sono concentrate sulla definizione delle procedure di test per entrambe le modalità di trasmissione (fibra e aria) e sull'identificazione dei casi d'uso di specifico interesse per la validazione prestazionale delle strategie QKD, mirate alla cybersicurezza delle reti di distribuzione.
	La linea **LA1.3 "GOCYS: Governance Observatory of Cyber Security - progettazione dell'osservatorio e analisi di scenario"** ha come obiettivo la definizione di un approccio innovativo alla gestione della cybersecurity, replicabile in diversi contesti caratterizzati dalla necessità di gestire grandi quantità di dati, inclusi quelli sensibili, come avviene tipicamente nel settore energetico. Nel corso del primo anno, le attività si sono concentrate sull'identificazione e sulla definizione dei dataset necessari all'alimentazione dell'osservatorio. In coerenza con il piano operativo, l'analisi ha incluso la revisione dei dati pregressi, attraverso l'esame dei flussi derivanti dalla linea LA3.4 del precedente PTR 2022–2024, relativa a un'infrastruttura di calcolo a basso consumo per reti elettriche intelligenti. Parallelamente, è stata condotta un'attività di aggregazione e filtraggio dei dati, finalizzata a ottenere una valutazione olistica del traffico. Tale fase si è rivelata fondamentale per individuare ed eliminare i cosiddetti "segnali di disturbo" statistici, riconducibili in particolare alle limitate funzionalità di sicurezza nativa degli apparati IoT considerati. Dall'analisi è emerso che le informazioni originariamente disponibili non risultavano pienamente coerenti con gli obiettivi di analisi di scenario previsti per la linea LA1.3. Di conseguenza, si è resa necessaria una rimodulazione operativa che ha comportato la pianificazione di nuove modalità di acquisizione dei dati. In questo contesto, è stata definita una riconfigurazione degli apparati IoT, introducendo una diversa modalità di connessione finalizzata a garantire una maggiore granularità del dato, più adeguata alle esigenze di governance della sicurezza. Inoltre, è stato avviato un periodo di test dedicato, volto a validare la nuova architettura di rete e a verificare l'efficacia delle soluzioni adottate. Per il prosieguo delle attività, si prevede di valorizzare l'hardware acquisito nell'ambito della precedente linea LA3.4. In particolare, verrà

	utilizzata un'infrastruttura composta da due rack dotati di sensori e sistemi di controllo, tra cui due sensori di temperatura e quattro prese di corrente comandate tramite relais, in grado di assicurare un monitoraggio puntuale dei principali parametri elettrici, quali tensione e corrente. L'acquisizione dei dati dai sensori avverrà mediante interrogazione tramite protocollo HTTP, garantendo la piena integrazione con i sistemi di monitoraggio dell'osservatorio. A valle dell'identificazione e definizione dei dataset necessari all'alimentazione dell'osservatorio, l'attività è proseguita con la pianificazione delle azioni necessarie allo sviluppo di uno strumento di gestione integrato progettato per coniugare l'analisi dei dati operativi con la resilienza informatica, seguendo le linee guida ENISA per la protezione delle Smart Grids. In particolare, è stata definita l'architettura funzionale che permetterà di ottimizzare l'uso degli apparati IoT acquisiti nella precedente LA 3.4 del PTR 22-24. L'infrastruttura si articolerà nei seguenti moduli principali: • Gateway di Campo: unità centrale di elaborazione deputata all'interfacciamento diretto con i sensori di temperatura, tensione e corrente, nonché alla gestione degli attuatori (relais) del quadro elettrico. • Modulo Cyber Security: un motore dedicato all'identificazione in tempo reale di minacce note (signature matching) e alla rilevazione di comportamenti anomali del traffico. Il modulo genererà i log necessari ad alimentare la componente di Cyber Awareness, garantendo una piena consapevolezza situazionale del sistema. • Modulo Data Management: sistema ottimizzato per l'indicizzazione e la ricerca rapida dei dati provenienti dal campo. Questa architettura abilita la correlazione temporale tra eventuali anomalie elettriche ed eventi di rete potenzialmente malevoli, rendendo possibile una diagnostica integrata. Si evidenzia, infine, che, nel corso della prima annualità, le attività di indagine e scouting non hanno consentito di identificare un soggetto idoneo a cui affidare la consulenza specialistica prevista dal capitolato tecnico. Tale attività rimarrà pertanto oggetto di pianificazione per le fasi successive del progetto.
Università di Padova Centro Interdipartimentale di Ricerca "Padua Quantum Technologies Research Center"	La linea **LA1.4 "Studio e progettazione di una infrastruttura sperimentale per test su reti quantum free-space e relativi protocolli per network con cybersicurezza quantistica nella distribuzione dell'energia"** ha come obiettivo la progettazione di un dimostratore sperimentale per test su reti quantum free-space e relativi protocolli per network con cybersicurezza quantistica nella distribuzione dell'energia. Le attività svolte nella presente annualità possono essere così suddivise: 1. studio preliminare alla progettazione e verifica di componenti per le comunicazioni quantistiche in sistemi free-space. 2. sviluppo e realizzazione di due terminali ottici da poter integrare in una infrastruttura intermodale, in cui tratti di link free-space coesistono assieme a tratti di fibra ottica. L'obiettivo primario della prima attività è stato il design di terminali ottici ottimizzati per operare in scenari operativi dinamici, garantendo al contempo un'elevata efficienza di accoppiamento del segnale in fibra a

	singolo modo. Il sistema è stato dimensionato per operare stabilmente su link free-space in un range dell'ordine di qualche chilometro, minimizzando le perdite di inserzione e ottimizzando il budget di potenza ottica. Le componenti chiave dell'architettura, con particolare riferimento ai moduli per la Quantum Key Distribution (QKD) e ai sistemi di mitigazione degli effetti atmosferici, sono state testate in condizioni ambientali reali. I dispositivi di generazione delle chiavi sono stati testati su un reale link free-space. Nello specifico, è stato dimostrato che i fenomeni tipici della propagazione in free-space (come la scintillazione atmosferica) non costituiscono un fattore bloccante per il protocollo implementato. Il protocollo adottato è una versione efficient BB84 con codifica in polarizzazione, che ha mostrato di mantenere bassi i valori di quantum bit error rate (QBER) nonostante le fluttuazioni del canale dovute alla turbolenza. Parallelamente alla validazione free-space dei sistemi di QKD, il sistema di correzione degli effetti di turbolenza di tip-tilt è stato testato in un link free-space di 600 metri. La sperimentazione ha confermato l'efficacia dei meccanismi di compensazione, permettendo di mantenere un accoppiamento stabile della luce nel core della fibra ricevente e garantendo la continuità operativa del link di comunicazione anche in presenza di disturbi atmosferici diffusi durante le fasce orarie della giornata. La seconda attività rappresenta la naturale prosecuzione della fase precedente. Infatti, l'architettura dei prototipi integra un sistema di correzione attiva tip-tilt fondamentale per compensare dinamicamente le variazioni dell'angolo di arrivo del fascio indotte dalla turbolenza atmosferica, garantendo la stabilità del segnale necessaria per l'accoppiamento in fibra e la continuità del servizio. I terminali sono stati sottoposti a una fase di assemblaggio e caratterizzazione in ambiente controllato. I test di laboratorio hanno confermato l'integrità dell'architettura implementata, con particolare attenzione alla coesistenza di segnali quantistici e classici. Nello specifico, è stato verificato che i dispositivi di Quantum Key Distribution (QKD), interfacciati ai terminali tramite fibre ottiche a singolo modo, operassero correttamente per la generazione e distribuzione di chiavi quantistiche. Un risultato di rilievo riguarda la capacità del sistema di gestire, simultaneamente allo scambio quantistico, una comunicazione bidirezionale per i canali dati classici attraverso il medesimo link free-space. Il completamento della fase di laboratorio apre la strada alla validazione in ambiente esterno per testare la robustezza del sistema in scenari operativi reali. I terminali sviluppati sono pronti per essere installati in un'implementazione free-space di circa 100 metri presso il Centro Ricerche ENEA di Portici. La campagna sperimentale, programmata per il mese di maggio 2026, avrà l'obiettivo di misurare le prestazioni del sistema di correzione in presenza di turbolenza reale e di quantificare il secret-key rate ed il QBER, consolidando così i risultati ottenuti finora.
Università degli Studi di Genova Dipartimento di Informatica,	La linea **LA1.5 "Progettazione Architetturale e Implementazione di Componenti Digital Twin per l'analisi bidirezionale della comunicazione in sistemi energetici cybersicuri"** ha come obiettivo lo

Bioingegneria, Robotica e Ingegneria dei Sistemi	sviluppo di un'architettura per la creazione di gemelli digitali di sistemi energetici (Digital Twin) finalizzati all'analisi della cybersecurity. Nella presente annualità, le attività si sono focalizzate sull'analisi del contesto applicativo e dei casi d'uso di riferimento, finalizzata alla definizione dei requisiti del framework di Digital Twin per sistemi energetici cyber-fisici, e sul consolidamento della progettazione architetturale del framework di Digital Twin, mediante una più puntuale definizione dei livelli funzionali e dei relativi moduli, con particolare attenzione ai meccanismi di integrazione dei modelli digitali sviluppati nelle attività congiunte con la LA2.2. Di seguito le azioni compiute per ciascuna fase: • Fase 1: 1. **Analisi del contesto e dei casi d'uso**: sono stati analizzati scenari di riferimento quali microgrid, centro di controllo e sistemi IEEE test, al fine di individuare i principali componenti cyber-fisici, le relative interazioni e i flussi informativi rilevanti per l'analisi della cybersecurity. Da tale analisi è emersa una prima articolazione concettuale del framework in tre livelli funzionali: simulazione fisica, astrazione dei protocolli di comunicazione e rappresentazione informatica. 2. **Definizione dei requisiti di integrazione e interoperabilità**: sulla base dei possibili casi d'uso analizzati sono stati individuati i requisiti relativi a co-simulazione, emulazione di rete, supporto ai protocolli industriali e interfacciamento tra simulatori e componenti software tramite interfacce standard ed estensibili, ponendo le basi per la successiva progettazione architetturale del framework. All'interno del framework verranno integrati anche i gemelli digitali dei principali componenti delle microreti definiti nella LA2.2 di ENEA. • Fase 2: 1. **Definizione dei livelli e dei moduli del framework**: è stata ulteriormente dettagliata l'architettura del framework nei tre livelli di simulazione fisica, astrazione dei protocolli e rappresentazione informatica, specificandone i principali contenuti funzionali. In particolare, il livello di simulazione fisica è stato articolato in componenti per co-simulazione, catalogo di modelli dinamici, interfacciamento tramite Functional Mockup Interface e simulazione del power flow e dello stato elettrico; il livello di astrazione dei protocolli comprende moduli per emulazione di rete e simulazione di dispositivi e protocolli industriali; il livello di rappresentazione informatica comprende componenti SCADA, firewall, sistemi di supporto alle decisioni, applicazioni enterprise e security analytics. 2. **Approfondimento del layer di integrazione dei modelli**: alla luce della scelta del software Dymola e ad integrazione delle attività congiunte con la LA2.2, è stata dedicata particolare attenzione ai meccanismi di interoperabilità tra il framework e i modelli in corso di sviluppo. In tale ambito è stata approfondita l'adozione della Functional Mockup Interface, ritenuta una soluzione idonea sia all'integrazione dei modelli sviluppati in Dymola sia all'estensione della compatibilità verso simulatori

	alternativi, rafforzando così l'apertura e l'integrabilità complessiva del framework.

WP2: Cybersecurity nelle reti elettriche rinnovabili per infrastrutture energetiche più resilienti

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	La linea **LA2.2** "**Definizione di modelli digitali per la creazione di un Cyber Security Digital Twin di reti energetiche multivettore**" ha come obiettivo la definizione dei gemelli digitali dei principali componenti di una rete energetica multivettore. I modelli dei componenti creati in tale linea dovranno essere integrati nell'architettura complessiva (Digital Twin della rete) che verrà progettata e implementata nell'ambito della LA1.5. Durante la prima annualità, le attività si sono inizialmente concentrate su un'analisi di mercato mirata all'acquisto di un software specialistico per la modellazione di reti energetiche complesse e multivettore, individuato nella piattaforma Dymola. Successivamente, i lavori si sono focalizzati sulla definizione dei modelli per i sistemi di accumulo e di generazione fotovoltaica, procedendo nello specifico come segue: 1. Sistema di accumulo • Definizione del Framework Cyber-Fisico: Identificazione dei punti di compromissione nei flussi di dati tra campo e BMS. È stata definita la struttura del package Batteria e del blocco SOC_Attack, stabilendo come le variabili fisiche debbano essere alterate matematicamente (tramite le leggi di *Offset*, *Freeze* e *Drift*) per rappresentare un attacco cyber. • Modello Equivalente dello Storage: Definizione delle equazioni di stato per il modello Battery_packCycling con chimica NCM (Nichel-Cobalto-Manganese). Si tratta di una delle chimiche più diffuse per le batterie agli ioni di litio (Li-ion), utilizzata ampiamente sia nei veicoli elettrici che nei sistemi di accumulo stazionari per microgrid. L'attività si è focalizzata sulla mappatura dei parametri necessari a valutare le conseguenze energetiche (es. degradazione della capacità) derivanti da una gestione errata del SOC indotta da attacchi esterni. 2. Inverter fotovoltaico • Definizione del Digital Twin dell'Inverter: Sono stati definiti i modelli matematici per lo stadio di potenza e il controllo, individuando come la manipolazione dei segnali di fase e frequenza si traduca in stress termico sulla giunzione dei semiconduttori. • Logiche di Monitoraggio e Anomalia: Definizione dei requisiti per il CyberMonitor. È stata stabilita la metodologia per il calcolo dell'errore di fase tra riferimento e rete come indicatore di integrità del segnale, gettando le basi per la creazione di gemelli digitali in grado di "auto-rilevare" lo stato di compromissione.

Università degli Studi Roma Tre Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche	La linea **LA2.3 "Sviluppo di un software basato su tecniche di AI per il rilevamento di intrusioni in reti energetiche da integrare negli apparati di protezione ENEA"** ha come obiettivo di sviluppare un prototipo software basato su tecniche AI per il rilevamento di intrusioni informatiche nelle reti energetiche, da integrare nell'apparato di protezione che verrà sviluppato da ENEA nell'ambito della LA 2.9. Nel periodo di riferimento, le attività hanno riguardato sia la fase di analisi preliminare e di definizione del contesto applicativo, sia la identificazione e formalizzazione di uno scenario di deployment. Durante la fase preliminare è stata effettuata una ricognizione della documentazione tecnica ENEA relativa al caso d'uso di riferimento, con l'obiettivo di individuare possibili architetture di deployment in ambiente di produzione e di formalizzare i threat model applicabili all'infrastruttura energetica target. In parallelo, è stata condotta una revisione sistematica dello stato dell'arte, finalizzata alla selezione delle tecniche e dei modelli AI maggiormente idonei al dominio dell'intrusion detection. Nella seconda fase è stato identificato e formalizzato uno scenario di deployment, calibrato sull'infrastruttura reale di ENEA, che costituisce la base operativa per le successive fasi di sviluppo del prototipo. A partire da tale scenario, è stato elaborato il relativo threat model, attraverso un'analisi sistematica delle superfici di attacco e delle vulnerabilità applicabili al contesto infrastrutturale considerato. L'analisi ha portato alla catalogazione degli scenari di attacco rilevanti e alla mappatura delle relative strategie di mitigazione, con riferimento alle soluzioni allo stato dell'arte documentate in letteratura. Complessivamente, non sono state evidenziate particolari criticità.
Università degli Studi di Napoli Federico II Dipartimento di Ingegneria Industriale	La linea LA2.4 **"Analisi delle tecnologie di generazione energetica in riferimento agli attacchi informatici e definizione del cyber rischio su base scenario"** ha come obiettivo l'analisi delle vulnerabilità a cui sono soggette le tecnologie di generazione (impianti termoelettrici, impianti idroelettrici, impianti eolici, impianti solari e Multi-sources Hybrid Polygeneration Energy Systems) e il rischio associato a potenziali attacchi cibernetici. Le attività principali dell'annualità in questione sono state: 1) l'analisi preliminare delle architetture di controllo industriale applicate agli impianti energetici, con particolare attenzione agli Industrial Control Systems, ai sistemi SCADA, ai Distributed Control Systems e ai Programmable Logic Controllers; 2) l'identificazione delle superfici di attacco dei sistemi di controllo industriale e sulla classificazione delle minacce cyber applicabili agli impianti energetici. La prima attività ha avuto l'obiettivo di costruire una base conoscitiva tecnica utile alla successiva identificazione delle superfici di attacco e dei possibili scenari di compromissione cyber-fisica. In particolare, sono stati analizzati i principali livelli funzionali dell'architettura OT secondo una logica coerente con il modello Purdue/ISA-95, distinguendo tra livello di campo, livello di controllo, supervisione di impianto e interfacciamento con la rete entreprise. Tale analisi ha consentito di individuare i principali componenti coinvolti nella regolazione e supervisione degli impianti energetici, tra cui sensori, attuatori, PLC, DCS, HMI, workstation di ingegneria, server SCADA e sistemi historian.

	Una specifica attività di approfondimento è stata dedicata al ruolo dei PLC nei sistemi di generazione, evidenziandone la funzione di controllo locale su macchine e sottosistemi critici, quali pompe, valvole, turbine, generatori di vapore a recupero e quadri elettrici. Sono state analizzate le logiche di funzionamento ciclico dei PLC, basate sull'acquisizione degli ingressi, sull'elaborazione del programma di controllo e sull'aggiornamento delle uscite verso gli attuatori. A supporto dell'analisi è stato preso in considerazione un caso rappresentativo relativo alla regolazione PID del livello del drum di un generatore di vapore, utile per evidenziare il legame tra variabili di processo, set-point, errore di regolazione e segnale di comando verso gli attuatori. L'analisi ha permesso di mettere in evidenza come la compromissione di una misura, di un set-point o di un parametro di controllo possa generare effetti diretti sul comportamento fisico dell'impianto. Parallelamente, sono stati analizzati il ruolo del DCS e dello SCADA in impianti complessi e distribuiti. Il DCS è stato considerato come sistema di coordinamento e supervisione locale di sottosistemi energetici complessi, quali turbina a gas, HRSG, turbina a vapore, ausiliari di impianto e sistemi elettrici. Lo SCADA è stato invece analizzato come infrastruttura di supervisione e acquisizione dati, particolarmente rilevante nel caso di reti energetiche distribuite o infrastrutture geograficamente estese. Il principale risultato del semestre consiste nella definizione di una prima mappatura funzionale dell'architettura di controllo degli impianti energetici e nell'individuazione dei componenti cyber-fisici maggiormente rilevanti per l'analisi del rischio. Durante la seconda attività, a partire dall'analisi architetturale svolta nella fase precedente, sono state individuate tre principali classi di componenti potenzialmente vulnerabili: sensori, attuatori e controllori. I sensori sono stati analizzati come punti critici per la corretta acquisizione dello stato fisico dell'impianto, in quanto una loro compromissione potrebbe generare dati alterati verso PLC, DCS o SCADA, inducendo il sistema di controllo a operare sulla base di informazioni non coerenti con le reali condizioni operative. Gli attuatori, quali valvole, pompe, relè e dispositivi di regolazione, sono stati invece considerati come elementi attraverso cui un attacco informatico può produrre effetti fisici diretti sull'impianto. I controllori, infine, sono stati identificati come componenti particolarmente sensibili, poiché contengono logiche di regolazione, sequenze operative, interlock di sicurezza e parametri PID. L'attività ha previsto l'applicazione del modello STRIDE come metodologia di riferimento per la classificazione delle minacce. Sono state quindi analizzate le categorie di Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service ed Elevation of Privilege, declinandole nel contesto specifico degli impianti energetici. Lo spoofing è stato associato alla possibilità che un attaccante si presenti come operatore, workstation di ingegneria o dispositivo di campo legittimo, acquisendo la capacità di inviare comandi o set-point non autorizzati. Il tampering è stato ricondotto alla modifica non autorizzata di dati, comandi o logiche di controllo, anche attraverso attacchi Man-in-the-Middle su protocolli industriali. Le minacce di repudiation sono state analizzate in relazione alla possibile alterazione dei log e alla perdita di tracciabilità degli eventi, con conseguente difficoltà nel distinguere un guasto tecnico

	da un sabotaggio informatico. L'information disclosure è stata considerata come possibile fase preparatoria di un attacco, finalizzata all'acquisizione di configurazioni, variabili di processo, logiche di controllo e credenziali. Il Denial of Service è stato valutato in termini di perdita di disponibilità di reti, server, HMI o controllori, mentre l'elevation of privilege è stata associata alla possibilità di ottenere privilegi elevati su workstation di ingegneria o sistemi di controllo. Il principale risultato della presente annualità consiste nella definizione di una prima matrice concettuale tra minacce informatiche, componenti vulnerabili e possibili effetti operativi sull'impianto. Tale attività ha permesso di evidenziare che la valutazione del rischio cyber negli impianti di generazione non può essere limitata alla sola compromissione del dato o del dispositivo informatico, ma deve includere l'analisi degli effetti sul controllo del processo, sulla sicurezza operativa e sulla continuità di esercizio. Non sono state rilevate criticità metodologiche rilevanti; è emersa tuttavia la necessità di approfondire ulteriormente, nei successivi sviluppi della linea, la quantificazione degli impatti fisici e termodinamici associati ai diversi scenari di attacco.

WP3: Big Data e AI per la cybersecurity e la privacy nelle smart grids

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	La linea **LA3.2 "Sviluppo di un sistema innovativo per la modellazione e il rilevamento di intrusioni Adversarial ML in reti energetiche e di comunicazione"** mira a realizzare una soluzione avanzata per identificare e contrastare gli attacchi di tipo Adversarial Machine Learning (AML) all'interno delle infrastrutture energetiche e delle relative reti di telecomunicazione. Le attività della prima annualità si sono focalizzate su due macro-obiettivi: • L'analisi dello stato dell'arte del settore di riferimento. • L'analisi e l'elaborazione dei dati disponibili, finalizzate alla creazione di un dataset accurato per l'addestramento di un sistema automatico di Intrusion Detection (IDS). L'indagine è partita dallo studio delle vulnerabilità degli algoritmi di Machine Learning applicati all'Intrusion Detection, con un focus specifico sulle reti energetiche e di comunicazione, per poi approfondire la natura degli attacchi AML. Questi ultimi consistono in tecniche capaci di indurre alla misclassificazione un modello di ML già addestrato, degradandone drasticamente le prestazioni. Poiché i sistemi di ML sono intrinsecamente vulnerabili a perturbazioni dei dati progettate per ingannare l'algoritmo, lo sviluppo di una strategia di difesa richiede la simulazione di scenari d'attacco analoghi, così da preparare preventivamente il modello. Per tale ragione, la linea di attività analizza in modo sinergico sia le tecniche di offesa (AML attacks) sia le contromisure di mitigazione. Tra le minacce AML investigate, l'attenzione si è rivolta al poisoning attack – in cui il dataset viene contaminato in fase di training compromettendo le performance del modello – e all'evasion attack, in cui

	i dati vengono manipolati in fase di inferenza (inference) per eludere la classificazione sfruttando i punti deboli del modello. Sul fronte della difesa, la tecnica selezionata prevede la generazione di Adversarial Examples, ovvero set di dati perturbati ma verosimili rispetto a quelli reali, opportunamente etichettati (labeled) come malevoli. Tale approccio consente di addestrare l'algoritmo a riconoscere le anomalie, aumentandone la resilienza complessiva. A valle dello studio teorico, si è proceduto all'analisi dei dati reali. Il dataset attualmente disponibile mappa il traffico di rete di un centro ENEA, dal quale sono stati estratti i log di sessione HTTP relativi a un attacco controllato di tipo DDoS Slowloris. L'analisi ha riguardato i protocolli di comunicazione tra i componenti, basati sullo scambio di pacchetti tra mittenti e destinatari, configurando un setup che ricalca fedelmente le dinamiche di comunicazione delle reti energetiche. Le attività si sono poi concentrate sull'anonimizzazione e sulla generalizzazione dei dati, al fine di evitare che specifiche caratteristiche (features) potessero introdurre bias nell'algoritmo. È stata inoltre studiata la rappresentazione vettoriale dei dati per il successivo input in una rete neurale, valutando sia l'impiego di embedding basati su architetture Transformers, sia l'uso di embedding nativi in ambiente PyTorch. Infine, per riportare queste analisi all'interno delle reti elettriche, è stata avviata la ricerca di dataset specifici e di sistemi che permettono di creare dei dati fittizi che possano aiutare nella creazione di un nuovo set di dati che descriva maggiormente un sistema di connessioni di componenti di una rete elettrica.
	La linea **LA3.3 "Progettazione di ambiente prototipale per l'implementazione di attacchi massivi e risposta automatica in funzione di tecniche di AI per il rilevamento di intrusioni in reti energetiche"** ha come obiettivo la progettazione di un ambiente prototipale per il rilevamento delle intrusioni ed attacchi informatici nelle smart grid e la risposta automatica a tali eventi, basata su tecniche AI. Nel corso della prima annualità, le attività si sono concentrate inizialmente su una ricognizione della letteratura scientifica relativa alla sicurezza informatica delle smart grid. L'analisi ha dedicato particolare attenzione alle minacce tipiche dei sistemi cyber-fisici, alle vulnerabilità delle infrastrutture di comunicazione a supporto delle reti energetiche e alle metodologie di *intrusion detection* applicabili a contesti caratterizzati da una forte interdipendenza tra dominio fisico e digitale. Questo studio preliminare ha evidenziato come la progettazione di un ambiente prototipale richieda una profonda comprensione sia degli scenari di attacco, sia dei loro potenziali effetti sul funzionamento della rete energetica. Di conseguenza, si è proceduto a una classificazione generale delle principali famiglie di minacce descritte in letteratura, valutandone la rilevanza rispetto allo specifico contesto sperimentale. Parallelamente, tali tematiche sono state contestualizzate rispetto alla nanogrid dimostrativa disponibile presso il Centro ENEA di Portici. L'attività ha così permesso di avviare una selezione preliminare degli elementi infrastrutturali, logici e funzionali da integrare nel prototipo da sviluppare nella LA, con il vincolo fondamentale di operare in un ambiente controllato, riproducibile e isolato dai sistemi di produzione.

	Sulla base di questi presupposti, è stata formulata una prima ipotesi architetturale dell'ambiente prototipale, definendone a livello concettuale i componenti funzionali. Tale architettura è stata concepita per integrare l'ambiente di analisi e simulazione con la rete di laboratorio esistente, rispettandone i vincoli tecnici e garantendo la necessaria sicurezza operativa. Infine, nell'ottica di definire i requisiti complessivi del sistema, sono state avviate interlocuzioni preliminari con le Università co-beneficiarie coinvolte nello sviluppo dei moduli di analisi e rilevamento basati su tecniche di intelligenza artificiale. Questi confronti hanno permesso di far emergere l'esigenza di uno stretto coordinamento tra l'ambiente di simulazione, le procedure di generazione dei dati e le componenti AI.
	La linea **LA3.4 "Analisi e implementazione di una Blockchain per smart grid energetiche su architetture convenzionali"** ha come obiettivo l'implementazione di una blockchain programmabile basata su meccanismo di consenso proof-of-work e destinata ad operare in una rete energetica. Nella presente annualità sono state eseguite le seguenti attività: 1. impostazione di una prima versione della Blockchain 2. definizione un caso d'uso applicativo 3. preparazione dell'ambiente di sviluppo 4. Adattamento della blockchain per il consenso PoW. In particolare, è stata condotta un'analisi dello stato dell'arte della tecnologia Blockchain per la soluzione più adatta all'implementazione su sistemi convenzionali di un'applicazione per smart-grid energetiche. Sono stati considerati i vari requisiti, in particolare l'essere opensource e disporre di un ambiente e una community di sviluppo attiva per garantire elevati standard di interoperabilità e sicurezza. Inoltre, è stata considerata la possibilità di operare con il meccanismo di consenso Proof-of-Work (PoW) con eventuale possibilità di sostituzione con altri algoritmi di consenso. Ultimo requisito fondamentale considerato è la programmabilità dovendosi implementare smart-contract decentralizzati in modo da applicare logiche di interesse e casi d'uso nel campo delle reti energetiche. A valle dell'analisi condotta si è scelto di implementare un'istanza di Hyperledger Besu, blockchain sviluppata e mantenuta, tra gli altri, dalla Linux Foundation; Besu è opensource, basata su Java, supporta la Ethereum Virtual Machine (EVM) ed è progettata per l'uso enterprise sia su reti pubbliche che private. Da un punto di vista hardware la rete di server che ospita la blockchain è stata definita sull'infrastruttura virtuale ICT on-premise basata su VMWare Cloud. Tale scelta è compatibile con le iniziali scarse richieste di performance ed è scalabile all'occorrenza. Inoltre, tramite i sistemi di cui è composta la piattaforma (basata su VMware vSphere), è possibile gestire i nodi in modo trasparente e usufruire delle funzionalità tipiche dei servizi cloud più avanzati come l'alta affidabilità, backup, continuità operativa ecc. Sono stati quindi definiti e inizializzati 3 nodi virtuali con sistema operativo Linux Ubuntu 24.04.2 LTS. La blockchain Hyperledger Besu implementata è la versione 24.11 ultima disponibile che, nella forma attuale, implementa meccanismi di consenso

	di tipo Proof-of-Authority (PoA), in particolare Clique, installata all'interno del sistema di containerizzazione Docker che offre molti vantaggi, tra i quali portabilità, isolamento delle applicazioni e scalabilità. Per la scelta dello use-case, si è investigato quale potesse essere una buona applicazione, in ambito smart-grid energetica, che evidenziasse le potenzialità e funzionalità della blockchain e si è considerato il caso di ricarica ad una colonnina elettrica smart con relativo pagamento. La colonnina sarà presto presente nel centro ricerche di Portici e potrà essere testata per la comunicazione con uno smart-contract che si occuperà di registrare in blockchain, e quindi in maniera immutabile e non ripudiabile, l'avvenuta transazione energetica con informazioni relative al mix energetico di produzione, i costi e i dettagli del pagamento. Per lo sviluppo si è scelto il linguaggio Solidity di Ethereum, essendo Hyperledger Besu compatibile con l'Ethreum Virtual Machine (EVM), per l'implementazione dello smart-contract, Node.js come ambiente runtime e Hardat per lo sviluppo in ambito blockchain. È stata poi re-inizializzata una nuova blockchain Besu con meccanismo di consenso Proof-of-Work (PoW) in sostituzione dell'algoritmo PoA implementato precedentemente; per fare ciò si è dovuto passare ad una versione più vecchia di Besu, la 22.10, che utilizzava l'algoritmo Ethash come PoW. Ciò ha comportato una ripartenza da zero dei blocchi e la perdita di tutte le transazioni precedenti che comunque erano solo di test. Per la visualizzazione comoda delle transazioni, blocchi e smart-contract caricati sulla blockchain, nonché wallet utilizzati e relativi bilanci di token, si è ritenuto opportuno installare una piattaforma di esplorazione, un cosiddetto "block-explorer"; si è quindi scelto Chainlens, un sistema opensource navigabile tramite interfaccia web. Tale sistema è stato installato sui nodi della blockchain ed è interrogabile da qualsiasi browser che ha visibilità del network.
	La linea **LA3.5 ": Studio e selezione di tecniche GAN per la valutazione di resilienza di algoritmi di detezione FDI"** ha come obiettivo la selezione di tecniche avversariali per la valutazione di resilienza di algoritmi di detezione FDI. Nell'ambito della prima annualità è iniziata l'analisi della letteratura relativa alle intrusioni di tipo Adversarial ML con particolare focus sull' identificazione della componentistica oggetto di attacco FDIA, della tipologia di attacco, dell'obiettivo specifico e infine delle modalità di difesa da adottare. A causa del limitato numero di contributi presenti nel quinquennio considerato si è optato per l'allargamento della tipologia di architettura ML includendo anche tecniche non avversariali nell'analisi. Riassumendo i principali risultati ottenuti sono: • 70 Articoli già recensiti (2020-2026, numero limitatissimo di applicazioni di tecniche contrastive/ avversariali); • Censiti attacchi/rilevatori (non contrastivi) e tassonomizzati per: • Tipologia di attacco, Tipologia di sottosistema attaccato, Obiettivo principale, Tecnica utilizzata, Dataset ed eventuale disponibilità pubblica di dato e/o simulatore.

	Infine, si è avviato lo sviluppo di un SLR. Sono stati sviluppati i termini di ricerca che sono stati sottoposti ai principali motori di ricerca della letteratura (WoS, Scopus, Scholar). Gli articoli risultanti sono stati scaricati e depositati in un repository. Script appositi sono stati sviluppati per l'estrazione del contenuto testuale che attraverso prompt e .md specifici sono stati sottoposti ad un LLM. Nello specifico utilizzando ChatGpt 5.4 API sono stati in prima analisi tassonomizzati gli articoli selezionati. La tassonomia ottenuta è in corso di revisione al fine di informare la finalizzazione dell'articolo e del rapporto tecnico.
Università degli Studi di Foggia Dipartimento di Scienze Agrarie, Alimenti, Risorse Naturali e Ingegneria	La linea **LA3.6 "Implementazione e test di algoritmi di detezione FDI per la valutazione di resilienza"** ha come obiettivo lo sviluppo di algoritmi suscettibili di evoluzione tramite addestramento avversariale. Nella presente annualità, le attività svolte si sono focalizzate sulle seguenti tematiche: 1) analisi delle principali tecniche di detezione della FDI presenti nella letteratura scientifica al fine di costruire una tassonomia completa delle tecniche più efficaci e classificarle secondo le caratteristiche di maggiore interesse per il progetto; 2) studio delle architetture per l'addestramento avversariale. Per quanto riguarda la prima fase, è stata svolta un'analisi sistematica della letteratura scientifica di settore, con la finalità di individuare le tecniche che sono state studiate in letteratura e ottenerne informazioni riguardo: • L'efficacia in termini di capacità di alterare i dati e, al contempo, i maggiori punti di forza e di debolezza delle tecniche. Inoltre, questa analisi è servita anche a configurare gli strumenti e la pipeline tecnologica necessaria per la realizzazione dell'attacco. • La fattibilità dell'attacco, ovvero quali pre-requisiti siano necessari per effettuare gli attacchi, non solo in termini tecnologici e di capacità, ma anche in termini di conoscenza sia necessaria all'attaccante e quali asset l'attaccante deve possedere. • Le sperimentazioni effettuate e quindi quali evidenze sono disponibili in letteratura riguardo l'efficacia e la cost-effectiveness degli attacchi. Questa analisi ha avuto anche l'obiettivo di valutare la qualità delle sperimentazioni, ovvero la validità dei dati raccolti. Questa analisi ha perseguito un duplice scopo: • da un lato, è servita ad ottenere una mappatura delle tecniche esistenti, congiuntamente alla raccolta dei pre-requisiti indispensabili alla loro effettiva implementazione; • dall'altro è servita a realizzare una selezione delle tecniche più mature ed efficaci che potranno essere utilizzate per la definizione di test volti a misurare la resilienza rispetto a questi attacchi. Relativamente alla seconda fase, per il tipo di addestramento previsto devono essere utilizzate le Reti Generative Avversariali. Queste sono architetture di Reti Neurali che si basano sulla competizione di un generatore e di un discriminatore. In letteratura sono state rilevate diverse architetture. Nella prima annualità è stata effettuata prima una classificazione delle architetture proposte in letteratura, caratterizzandone punti di forza e di debolezza. Congiuntamente, sono stati definiti i criteri per la composizione del dataset di addestramento da imputare alla rete generativa al fine di creare i campioni avversariali. È stata quindi verificata

	l'adeguatezza dei campioni generati e la loro funzionalità in merito alle finalità del progetto. Non sono state ravvisate specifiche criticità se non quelle relative alla necessità di una potenza di calcolo adeguata al funzionamento di queste architetture che sono molto onerose in termini di potenza di calcolo.
Università degli Studi Roma Tre Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche	La linea **LA3.7 "Progetto di un sistema innovativo basato su tecniche di AI per il rilevamento e la risposta automatica a intrusioni in reti energetiche"** ha come obiettivo la progettazione un sistema innovativo basato su tecniche avanzate AI per il rilevamento e la risposta automatica a intrusioni informatiche in reti energetiche. Nel periodo di riferimento, in una prima fase le attività hanno avuto carattere esplorativo e di ricerca di base, articolandosi lungo le due direttrici progettuali principali: *detection* e *response*. Sul fronte della detection, le attività si sono concentrate sull'analisi della qualità dei dati di addestramento, elemento determinante per la costruzione di modelli AI robusti e con adeguate capacità di generalizzazione. È stata condotta una valutazione comparativa dei principali dataset, tecniche e metodologie di intrusion detection disponibili allo stato dell'arte. In tale contesto, è stata avviata una sperimentazione volta alla definizione di una metodologia e di un framework di Explainable AI a supporto del processo di addestramento di modelli di detection. Successivamente, è stata ultimata la definizione della metodologia e del framework XAI. È stata implementata una pipeline end-to-end finalizzata all'analisi e alla spiegazione degli errori di classificazione prodotti da modelli di intrusion detection addestrati su specifici dataset. La validazione è stata condotta attraverso una campagna sperimentale estensiva su molteplici dataset, i cui risultati hanno confermato la solidità dell'approccio proposto, mostrandosi in linea con le aspettative formulate in fase di progettazione. Sul fronte della response, le attività hanno riguardato lo studio delle tecniche e metodologie di intrusion response allo stato dell'arte. Inoltre, è stata effettuata una sperimentazione sull'impiego di Large Language Model per la risoluzione di problemi di ottimizzazione modellati mediante Attack-Defense Tree, con applicazione di tecniche di reinforcement learning. L'obiettivo è valutare la capacità degli LLM di approssimare le soluzioni ottime generate da model checker formali quali PRISM, con l'intento di abilitare scenari di risposta automatica online caratterizzati da maggiore efficienza computazionale rispetto agli approcci tradizionali. Sono state, quindi, avviate le attività riguardanti la formalizzazione del problema di ottimizzazione in una rappresentazione semanticamente adeguata all'elaborazione da parte di Large Language Model, garantendo che gli scenari sottoposti vengano formulati in modo corretto e privo di ambiguità.
Università degli Studi di Trento Dipartimento di Ingegneria e Scienza dell'Informazione	La linea **LA3.8 "Identificazione delle minacce nel controllo automatizzato di smart grid cloud-native"** ha come obiettivo la modellazione delle minacce informatiche (threat modeling) nel contesto delle smart grid. Nel presente periodo di riferimento le attività svolte sono state: 1. analisi preliminare delle minacce informatiche nel contesto delle smart grid cloud-native e sullo studio di possibili architetture di riferimento

	2. estensione dell'analisi preliminare delle architetture e delle minacce, con particolare attenzione ai confini di fiducia e all'identificazione delle risorse critiche. La prima attività si è focalizzata sui seguenti punti • Analisi del contesto e delle tecnologie cloud per smart grid: è stato analizzato il ruolo delle tecnologie cloud (IaaS, PaaS) nella gestione delle smart grid, con particolare attenzione agli aspetti di automazione, scalabilità e integrazione con sistemi distribuiti ed edge. • Studio di architetture cloud-native per smart grid: sono state esaminate possibili architetture basate su paradigma cloud-native, considerando la suddivisione in domini funzionali (TSO, DSO, AMI, GenCo) e l'utilizzo di tecnologie di containerizzazione e orchestrazione (Docker, Kubernetes). L'analisi ha portato all'identificazione di una prima architettura logica di riferimento. • Definizione preliminare dei flussi informativi e dei domini di fiducia: è stata sviluppata una prima rappresentazione dei data flow a livello logico (DFD L0), finalizzata all'individuazione dei componenti coinvolti, delle principali interazioni e delle superfici di attacco. In questa fase sono stati identificati i principali domini e i punti di interazione tra sistemi eterogenei. In relazione alla seconda attività le tematiche trattate sono state: • Identificazione preliminare delle risorse critiche: sono stati individuati i principali asset rilevanti ai fini della sicurezza, includendo componenti infrastrutturali cloud (cluster, container, API di gestione). • Avvio dell'analisi delle minacce informatiche: è stata avviata una prima attività di threat modeling, con particolare attenzione alle vulnerabilità introdotte da configurazioni cloud e processi automatizzati. Studio preliminare di tecniche di generazione automatizzata di configurazioni cloud: è stata avviata un'analisi di pipeline per la generazione automatica di manifest Kubernetes a partire da repository applicativi, al fine di valutarne l'applicabilità nello scenario considerato.

WP4: Attività di diffusione

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	Le attività della **LA4.2 "Diffusione SAL1"** ha come obiettivo la divulgazione delle attività svolte e dei risultati futuri del progetto, assicurandone la più ampia accessibilità e fruibilità da parte dei potenziali stakeholder e degli utenti interessati. Si riportano di seguito le attività di disseminazione svolte nel corso dell'annualità di riferimento: 1. Presentazione del progetto e dei risultati preliminari alla "Notte Europea dei Ricercatori e delle Ricercatrici" presso il C.R. ENEA di Portici (settembre 2025);

	2. Presentazione dei risultati del progetto ottenuti nel triennio 22-24 alla V edizione del CONVEGNO NAZIONALE DELLA RICERCA DI SISTEMA ELETTRICO - “Diffusione dei risultati e prospettive sulla Ricerca del Sistema Elettrico” (ottobre 2025); 3. Presentazione del progetto e dei risultati preliminari attraverso pubblicazione di un lavoro scientifico al 2025 IEEE INTERNATIONAL WORKSHOP ONTECHNOLOGIES FOR DEFENSE AND SECURITY ROME (novembre 2025). Parallelamente, le attività si sono concentrate sulla definizione delle basi tecnico-progettuali propedeutiche allo sviluppo del software di realtà immersiva per la divulgazione della ricerca su “Cybersecurity dei sistemi energetici”, previsto per il semestre successivo. A tal fine, è stato condotto uno studio preliminare volto a valutare le soluzioni disponibili sul mercato e sono stati avviati contatti con operatori del settore, con l’obiettivo di individuare il partner più idoneo rispetto ai requisiti progettuali e agli obiettivi di disseminazione. Successivamente è stata avviata la fase di predisposizione della documentazione per l’affidamento diretto all’Operatore Economico individuato. <u>Pubblicazioni ENEA:</u> Valenti M., Scafuri A., Merola A., Adinofli G., Graditi G. Evaluation of Cyber-Vulnerabilities in Commercial Microgrid Devices. 2025 IEEE INTERNATIONAL WORKSHOP ONTECHNOLOGIES FOR DEFENSE AND SECURITY ROME.