PIANO TRIENNALE DI REALIZZAZIONE 2025-2027 DELLA RICERCA DI SISTEMA ELETTRICO NAZIONALE

Presentazione dei progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

Tema di ricerca 2.1

Titolo del progetto

Progetto Integrato Cyber Security dei sistemi energetici per la transizione energetica-digitale

- Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile [ENEA]
- Consiglio Nazionale delle Ricerche [CNR]
- Ricerca sul Sistema Energetico [RSE]
- Padua Quantum Technologies Research Center [UniPD-QTech]
- Scuola Alti Studi Lucca- IMT [IMT]
- UNITRENTO - Dipartimento di Ingegneria e Scienza dell'Informazione [UniTN]
- Università degli Studi di Foggia - Dipartimento di Scienze Agrarie, Alimenti, Risorse Naturali e Ingegneria [DAFNE]
- Università degli Studi di Genova - Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi [UNIGE]
- Università degli Studi di Napoli Federico II - DIPARTIMENTO DI INGEGNERIA INDUSTRIALE [UNINA-DII]
- Università del Molise- Dipartimento di Medicina e di Scienze della Salute "Vincenzo Tiberio" [UNIMO]
- Università della Calabria - Dipartimento di ingegneria informatica, modellistica, elettronica e sistemistica -DIMES [UNICA]
- Università di Firenze- Dipartimento di Matematica e Informatica 'Ulisse Dini' [UNIFI]
- UNiversità di Messina - Dipartimento di Ingegneria [UNIME]

FASE: Trasmissione PTR rimodulato (ver. 7)

- Università Roma Tre - Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche [ROMA3-DICITA]

Durata del progetto: 36 mesi

Costo proposto: 8.813.275,00 €

2. DATI GENERALI DEL PROGETTO

2.1 Dati progetto

Titolo del progetto
Progetto Integrato Cyber Security dei sistemi energetici per la transizione energetica-digitale
Durata del progetto
36 mesi

2.2 Descrizione progetto

Abstract del progetto
Nella transizione energetica in atto, la digitalizzazione delle infrastrutture è funzionale ad una loro sempre più spinta osservabilità, automazione, controllo ed efficientamento e supporta lo scambio dati tra diverse entità (quali operatori di rete, produttori, gestori di infrastrutture di ricarica per veicoli elettrici, comunità energetiche, aggregatori) e le interazioni tra diversi vettori e reti energetiche (quali reti elettriche, di gas, idrogeno, acqua e calore) tramite connessioni tra sistemi eterogenei (quali generatori distribuiti, sistemi di accumulo, consumatori passivi e attivi) garantendo servizi energetici più efficienti. In futuro le reti energetiche saranno sempre più di tipo multivettore, integrate con le reti di trasmissione dati e con sistemi intelligenti di gestione per abilitare l'impiego massivo delle fonti rinnovabili, l'elettrificazione di consumi (soprattutto in settori come la mobilità e il condizionamento ambientale) e il coinvolgimento attivo degli utenti. La presenza del layer di comunicazione dati in tali infrastrutture le rende al tempo stesso intrinsecamente più vulnerabili agli attacchi cibernetici ed esposte a rischi che possono compromettere la continuità del servizio e l'incolumità dei cittadini (si pensi ad esempio ad un cyberattacco che "altera" in maniera indesiderata i dati operativi di funzionamento di una centrale di gestione di una rete gas o, nel futuro, di una rete idrogeno). Conseguentemente, appare evidente come la cybersecurity assuma un ruolo strategico nei sistemi energetici e divenga fondamentale investigare, soprattutto in ottica di sviluppo futuro delle reti energetiche, per le diverse tipologie di attacchi, le potenziali conseguenze sulle reti multienergetiche e le tecnologie e i dispositivi di rilevamento e difesa di cui dotare le reti sia in ottica "difensiva" (es. tecnologie per la rilevazione delle minacce cibernetiche) che "riparativa" (es. tecnologie per la messa in sicurezza di impianti ed apparati in caso di attacco cibernetico). Va inoltre considerato che l'internet delle cose "elettriche/digitali" nel perimetro dell'utente o i servizi ad accesso pubblico, come le infrastrutture di ricarica per veicoli elettrici, introducono requisiti di riservatezza dei dati personali che devono essere gestiti da opportune misure di privacy.
Tale trasformazione digitale del settore energetico ha modificato in modo significativo il concetto di sicurezza del sistema. Alla necessità di preservare l'adeguatezza e la sicurezza delle infrastrutture fisiche in ambito OT (Operational Technology), si è aggiunta l'esigenza di prevedere azioni e meccanismi di protezione delle tecnologie IT (Information Technology) a tutela della cybersecurity e della privacy dei dati e delle elaborazioni. La tematica è destinata ad assumere un ruolo sempre più centrale nei prossimi anni se si considera che la digitalizzazione delle reti è un imprescindibile fattore abilitante della transizione energetica e che i sistemi energetici rappresentano infrastrutture critiche, il cui esercizio richiede misure di difesa in tutti i settori tecnologici (IT/OT/IoT).
Il progetto integrato sulla cybersecurity dei sistemi energetici coinvolge i tre enti di ricerca italiani, RSE, ENEA e CNR (e le Università co-beneficiarie di ENEA e CNR), nel raggiungimento dell'obiettivo prioritario "Digitalizzazione ed evoluzione delle reti" dell'Accordo di Programma di Ricerca 2025-2027.
Il progetto indirizza i malfunzionamenti delle infrastrutture digitali per il controllo energetico causati da minacce informatiche. Il piano di ricerca è finalizzato alla messa in sicurezza degli scambi informativi necessari per il monitoraggio e controllo di reti e impianti energetici secondo gli sviluppi previsti al 2030 dal Piano Nazionale Integrato Energia e Clima (PNIEC), in allineamento ai recenti regolamenti sulla cybersecurity, quali la Direttiva UE 2022/2555 NIS2 e il Codice di Rete NCCS, ed i conseguenti aggiornamenti della Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Agenzia per la Cybersicurezza Nazionale e della legislazione nazionali (DL 2024/138).
Le attività del progetto studiano e valutano misure e tecnologie di gestione dei rischi e di segnalazione degli incidenti di cibersicurezza adeguate a garantire elevati gradi di disponibilità, integrità e confidenzialità ai dati e ai processi digitali delle infrastrutture energetiche funzionali al PNIEC.
Nel progetto vengono specificamente indirizzati standard di cybersecurity basati su crittografia e infrastrutture di gestione di chiavi pubbliche e certificati digitali, riconosciuti a livello internazionale, al fine di valutarne l'applicabilità e l'impatto prestazionale in specifici scenari di controllo energetico.
Allo scopo di preparare il settore all'avvento del quantum computing, viene considerata l'evoluzione degli standard necessaria per l'adozione di algoritmi di crittografia in grado di resistere ad attacchi effettuati con computer quantistici e l'impatto dell'utilizzo di chiavi quantistiche sulle infrastrutture di gestione delle chiavi.

Per il rilevamento tempestivo delle anomalie cyber, vengono sviluppate piattaforme innovative che sfruttano le potenzialità dei migliori algoritmi di intelligenza artificiale e generativa e garantiscono la privacy dei dati attraverso l'applicazione di tecniche di anonimizzazione.
Le valutazioni e i test di cybersecurity, effettuati in laboratori digitali e infrastrutture energetiche sperimentali, indirizzano test di conformità agli standard di cybersecurity, favorendo lo sviluppo di schemi di certificazione di cybersecurity di dispositivi di controllo energetico. I test di cybersecurity utilizzano architetture digitali fisiche e virtualizzate, basate su interfacce e reti di comunicazione di nuova generazione per impianti, comunità energetiche, operatori della flessibilità e prosumer distribuiti sul territorio nazionale.
Al fine di presidiare l'evoluzione dei processi di attacco e proteggere le infrastrutture dagli effetti dei processi più insidiosi, il progetto utilizza lo strumento dei digital twin che metteranno a disposizione ambienti verosimili per l'analisi approfondita degli attacchi, del loro impatto sui processi fisici e dell'efficacia delle misure di protezione e difesa.
Le attività si avvalgono di collaborazioni di ricerca con stakeholder in modo da accelerare il trasferimento tecnologico e il time to market di servizi di identità digitale e di certificazione di cybersecurity e di dispositivi di controllo energetico certificati e il loro utilizzo nelle infrastrutture energetiche del sistema paese.
Grazie ai numerosi contatti accademici, il progetto riserva un'attenzione specifica alla formazione sulla cybersecurity attraverso lo svolgimento di stage, tesi di laurea, borse di dottorato, seminari e lezioni nell'ambito dei programmi di lauree triennali, magistrali, master di primo e secondo livello.

Abstract del progetto ENG

In the ongoing energy transition, the digitalization of infrastructures is functional to their increasingly advanced observability, automation, control, and efficiency. It supports data exchange between different entities (such as grid operators, energy producers, operators of electric vehicle charging infrastructures, energy communities, aggregators) and interactions among different energy vectors and grids (such as electrical, gas, hydrogen, water, and heat grids) through connections between heterogeneous systems (such as distributed generators, storage systems, consumers and prosumers), ensuring more efficient energy services. In the future, energy grids will increasingly be multi-vector, integrated with data transmission networks and intelligent management systems to enable the massive use of renewable sources, the electrification of consumption (especially in sectors such as mobility and environmental conditioning), and the active involvement of users. The presence of the data communication layer in such infrastructures makes them inherently more vulnerable to cyberattacks and exposed to risks that can compromise service continuity and citizen safety (consider, for example, a cyberattack that "alters" the operational data of a gas grid management centre or, in the future, a hydrogen grid). Consequently, it is evident that cybersecurity assumes a strategic role in energy systems and becomes essential to investigate, especially with a view to the future development of energy grids, the different types of attacks, the potential consequences on multi-energy grids, and the detection and defense technologies and devices to equip the data networks with both a "defensive" perspective (e.g., technologies for detecting cyber threats) and a "remedial" perspective (e.g., technologies for securing plants and equipment in case of a cyberattack). It should also be considered that the "electrical/digital" internet of things within the user perimeter or public access services, such as electric vehicle charging infrastructures, introduce personal data confidentiality requirements that must be managed by appropriate privacy measures.
This digital transformation of the energy sector has significantly changed the concept of system security. In addition to the need to preserve the adequacy and security of physical infrastructures in the OT (Operational Technology) domain, there is also the need to foresee actions and protection mechanisms for IT (Information Technology) domains to protect cybersecurity and data privacy. The topic is destined to assume an increasingly central role in the coming years, considering that the digitalization of networks is an indispensable enabling factor for the energy transition and that energy systems represent critical infrastructures, whose operation requires defense measures in all technological sectors (IT/OT/IoT).
The integrated cybersecurity project for energy systems involves the three Italian research entities, RSE, ENEA, and CNR (and the universities co-beneficiaries of ENEA and CNR), in achieving the priority objective "Digitalization and evolution of networks" of the 2025-2027 Research Program Agreement.
The project addresses malfunctions of digital infrastructures for energy control caused by cyber threats. The research plan aims to secure the information exchanges necessary for monitoring and controlling energy grids and plants according to the developments foreseen by the National Integrated Energy and Climate Plan (PNIEC) by 2030, in alignment with recent cybersecurity regulations, such as the EU Directive 2022/2555 NIS2 and the NCCS Network Code, and the consequent updates of national strategies and legislation (DL 2024/138).
The project's activities study and evaluate risk management measures and cybersecurity incident reporting technologies adequate to ensure high levels of availability, integrity, and confidentiality of data and digital processes of energy infrastructures functional to the PNIEC.
The project specifically addresses cybersecurity standards based on cryptography and public key infrastructure and digital certificates, recognized internationally, to evaluate their applicability and performance impact in specific energy control scenarios.
To prepare the sector for the advent of quantum computing, the evolution of standards necessary for the adoption of cryptographic algorithms capable of withstanding attacks carried out with quantum computers and the impact of using quantum keys on key management infrastructures are considered.
For the timely detection of cyber anomalies, the project develops innovative platforms that exploit the potential of the best artificial

intelligence and generative algorithms and ensure data privacy through the application of anonymization techniques.
Cybersecurity assessments and tests, carried out in digital laboratories and experimental energy infrastructures, address compliance tests with cybersecurity standards, promoting the development of cybersecurity certification schemes for energy control devices.
Cybersecurity tests use physical and virtualized digital architectures, based on new generation communication interfaces and networks for plants, energy communities, flexibility operators, and prosumers distributed throughout the national territory.
To monitor the evolution of attack processes and protect infrastructures from the effects of the most insidious processes, the project uses digital twin tools that will provide realistic environments for in-depth analysis of attacks, their impact on physical processes, and the effectiveness of protection and defense measures.
The activities benefit from research collaborations with stakeholders to accelerate the technological transfer and time to market of digital identity and cybersecurity certification services and certified energy control devices and their use in the country's energy infrastructures.
Thanks to numerous academic contacts, the project pays specific attention to cybersecurity training through internships, theses, doctoral scholarships, seminars, and lectures within the framework of bachelor's, master's, first and second level master's degree programs.

2.3 TRL progetto

TRL iniziale: 3
TRL finale: 4

Allo stato dell'arte, la tematica della cybersecurity è in una fase di sviluppo più avanzato nel settore delle reti di telecomunicazione e delle tecnologie IT, mentre si trova ad un livello di maturità inferiore nelle infrastrutture energetiche e nelle tecnologie OT (TRL 2-4). Il TRL è ancora più ridotto (TRL <3) nel settore delle reti energetiche di tipo multivettore, o delle reti di tipo "non elettrico" (es. reti idrogeno), considerata l'attuale ridotta diffusione di queste ultime, destinate a diventare anch'esse prioritarie negli scenari energetici futuri.
In considerazione dei risultati degli studi e degli sviluppi ottenuti nel progetto integrato 2.1 del PTR 2022-2024 della Ricerca di Sistema e nel progetto MI-SG, dell'evoluzione dello stato dell'arte e della tecnologia, le attività svolte nel triennio di ricerca consentiranno un incremento tecnologico da TRL 3 (Prova di concetto sperimentale) a TRL 4 (Strumento o tecnologia convalidata in laboratorio).
Le tematiche affrontate nel progetto sono caratterizzate da un elevato grado di interdisciplinarità (conoscenza di sistemi di protezione, automazione e controllo, sistemi SCADA (Supervision, Control And Data Acquisition), sistemi di gestione dell'energia, tecnologie di comunicazione, Operational Technology e Internet of Things, cloud computing, virtualizzazione delle reti e degli IED (Intelligent Electronic Device), minacce cyber, vulnerabilità, tecniche di attacco, misure di cybersecurity, protocolli di crittografia, crittografia post-quantistica e quantistica, strumenti di simulazione elettrica e informatica, tecniche e algoritmi di Intelligenza Artificiale e apprendimento automatico. Pertanto, il TRL iniziale per l'intero progetto è condizionato dal più basso valore di TRL nei diversi settori coinvolti (TRL 3).
Gli sviluppi indirizzati nel progetto comportano uno sforzo rilevante in termini di maturità tecnologica (disponibilità di software e dispositivi di mercato) e di grado di integrazione (disponibilità di infrastrutture energetiche cyber-fisiche digitalizzate e sicure).
L'incremento a TRL 4 si concretizza attraverso prodotti di ricerca applicati a casi d'uso significativi per la transizione energetica e validati in laboratori e infrastrutture energetiche di ricerca su scala ridotta.

2.4 Inquadramento del progetto nello stato dell'arte

a) Stato dell'arte nazionale e internazionale relativamente alle attività previste nel progetto
La cybersecurity dei sistemi energetici è un tema multidisciplinare che coinvolge diversi ambiti di ricerca. Le potenziali minacce possono riguardare la produzione-trasmissione-distribuzione dell'energia, ovvero le reti di comunicazione, o ancora i network informatici e le applicazioni software. Un attacco ai diversi livelli può comportare interruzioni nell'erogazione dell'energia con evidenti impatti negativi sulla corretta fornitura del servizio alle utenze, siano esse residenziali, commerciali e/o industriali.
Lo storico degli attacchi ai sistemi energetici include una casistica diversificata di processi malevoli che hanno provocato conseguenze significative sul servizio energetico. Nel 2010 è stato scoperto Stuxnet, un processo di attacco sofisticato che, attraverso interfacce locali e di rete, è riuscito a compromettere dispositivi di controllo programmabili con lo scopo di disabilitare le centrifughe dell'impianto di arricchimento dell'uranio di una centrale nucleare in Iran. Sfruttando vulnerabilità del sistema operativo ancora inedite (0-day), l'attacco si propagava verso il software di programmazione del controllore di impianto. Il virus si era poi diffuso al di fuori della centrale iraniana, colpendo principalmente aziende in Giappone, USA ed Europa, finendo sotto i riflettori dei media di tutto il mondo. Un secondo caso di attacco rilevante è avvenuto a dicembre 2015 in Ucraina ed ha coinvolto tre società di distribuzione provocando il distacco di 27 stazioni elettriche e la disalimentazione di 230.000 utenze per diverse ore. Un caso di attacco informatico coordinato molto recente è quello che l'11 maggio 2023 si è verificato contro numerose società energetiche danesi. Sfruttando una vulnerabilità nei firewall utilizzati per proteggere gli accessi alle reti di impianto, gli aggressori hanno colpito selettivamente i firewall vulnerabili prendendone il controllo. Casi

recenti di attacchi cyber al settore energia nel mondo (es. nel 2018 attacchi informatici hanno interrotto il servizio di cinque gasdotti/società negli USA; nel 2019, in Messico, la Petroleos Mexicanos ha bloccato le attività per settimane per un attacco ransomware) dimostrano che sono richiesti sforzi ulteriori, nei diversi ambiti infrastrutturali (reti energetiche, reti di comunicazione, reti informatiche) per lo sviluppo di strumenti e l'adozione di tecnologie che preservino la cybersecurity, prevedano soluzioni di backup e minimizzino gli impatti di cyber-attacchi sul sistema fisico.
Nell'attuale scenario geopolitico, la minaccia cyber è sempre più utilizzata come arma di attacco; i cyberattacchi, infatti, sono in grado di compromettere la continuità dei servizi anche primari di una nazione, con conseguenze sia sulla sicurezza delle infrastrutture e delle persone, che di carattere economico e sociale. Ad esempio, nel 2022, in seguito all'invasione dell'Ucraina, è stata scoperta una variante del malware Industroyer già utilizzato nel 2016 allo scopo di generare un blackout sempre in Ucraina.
L'adozione delle nuove tecnologie digitali IT/OT/IoT in infrastrutture energetiche che abilitano servizi di flessibilità e nuovi mercati comporta un'evoluzione delle misure di sicurezza cyber in funzione delle esigenze operative proprie dei servizi energetici e di potenziali nuove minacce ad estese superfici di attacco.
A livello internazionale ed Europeo la tematica della cybersecurity per i sistemi energetici è oggetto di cospicui programmi di ricerca, sviluppo e innovazione tecnologica (vedi DoE, DHS, EPRI, Horizon Europe), ed è considerata una priorità di agenzie ed iniziative atte alla condivisione di informazioni ed esperienze (IEA, Set-Plan, ENISA, ENCS, EE-ISAC, etc.).
Di seguito, si riportano gli sviluppi di ricerca e lo stato delle soluzioni di mercato, suddivisi per obiettivi prioritari del progetto.

OB1: garantire l'adeguatezza delle tecnologie di cybersecurity nelle applicazioni digitali per il controllo energetico

La sicurezza delle reti energetiche dipende dall'affidabilità dei protocolli di comunicazione. Protocolli come il DNP3 (Distributed Network Protocol) e l'IEC 61850, utilizzati per la comunicazione tra stazioni elettriche e centri di controllo, sono stati aggiornati per includere meccanismi crittografici robusti.
Nel 2023, l'IEC ha aggiornato la serie di standard IEC 62351, una suite di specifiche di sicurezza progettata per proteggere i protocolli di comunicazione utilizzati nelle reti energetiche, introducendo tecniche di autenticazione crittografica e cifratura end-to-end per prevenire attacchi di tipo Man-in-the-middle, manipolazioni e repliche dei contenuti.
La serie di standard IEC 62351 ha ormai raggiunto un discreto livello di maturità ed inizia ad essere supportata da dispositivi di mercato e da enti di certificazione. I profili di sicurezza specificati in questa serie garantiscono riservatezza, integrità ed autenticità delle comunicazioni mediante protocolli di scambio chiavi e algoritmi crittografici, quali RSA [1] e AES [2].
La gestione delle chiavi e dei certificati elettronici è tipicamente basata su Infrastrutture a Chiave Pubblica, o PKI. Gli standard di riferimento per l'implementazione delle PKI in ambito elettrico sono IEC 62351-9 e ISO 15118-20 che descrive l'utilizzo di infrastrutture PKI per la realizzazione di una comunicazione sicura tra veicoli elettrici e stazioni di ricarica.
I certificati digitali e le chiavi crittografiche assicurano infatti l'identità delle parti coinvolte nella comunicazione (es. veicoli e stazioni di ricarica) e offrono gli strumenti per l'integrità e la riservatezza delle informazioni scambiate. In uno scenario futuro caratterizzato da una diffusione massiccia della mobilità elettrica, è prevedibile l'utilizzo di molteplici PKI, con conseguenti potenziali problemi di interoperabilità. Anche su questo fronte, lo standard ISO 15118-20 fornisce linee guida specifiche per la garanzia della compatibilità tra le diverse PKI.
La robustezza degli algoritmi crittografici attualmente in uso è strettamente legata alla complessità computazionale necessaria per l'individuazione delle chiavi. Per quanto riguarda la crittografia, una innovazione tecnologica è rappresentata dai protocolli di distribuzione di chiavi quantistiche (QKD) [3], in cui le chiavi vengono codificate in stati quantistici, intrinsecamente sicuri in quanto assicurano che una chiave segreta compromessa possa essere identificata e scartata prima dell'uso. L'attività del progetto si inserisce in un contesto di ricerca molto ricco e attuale, con obbiettivi europei fissati al 2030 per l'utilizzo di comunicazioni quantistiche e tavoli di lavoro IEC e CENELEC sulla gestione delle chiavi quantistiche e sull'utilizzo della crittografia post-quantistica. In ambito IEC è in preparazione il rapporto tecnico IEC TR 62351-90-4 ED1 "Power systems management and associated information exchange - Data and communications security - Part 90-4: Migration of cryptographic algorithms" che prende in considerazione alcune tematiche considerate nel progetto.
L'ENISA (European Union Agency for Cybersecurity) già nel 2020 dichiarava la crittografia post-quantistica come uno strumento fondamentale per raggiungere la resilienza nell'ambito della cybersecurity e da allora ha pubblicato diversi documenti sullo stato dell'arte e sull'utilizzo della crittografia post-quantistica.
Nell'aprile 2024 la Commissione dell'Unione ha emesso il documento "Raccomandazione relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica" con la quale invita gli stati membri a iniziare a studiare la migrazione delle proprie infrastrutture verso la crittografia post-quantistica, che determinerà un cambiamento radicale degli algoritmi, dei protocolli e dei sistemi crittografici.
Dal punto di vista delle comunicazioni quantistiche, a livello europeo è in fase di realizzazione un'infrastruttura di comunicazioni quantistiche (EuroQCI) in grado di distribuire chiavi quantistiche intrinsecamente sicure, affiancata in Italia dal progetto Italian Quantum Backbone (IQB) dove sono stati avviati esperimenti in campo reale di comunicazione quantistica con protocolli di Quantum Key

Distribution.
A livello internazionale il NIST, che già evidenzia la concretezza del rischio correlato alla presenza di tecnologie quantistiche, è punto di riferimento per delineare le strategie di sicurezza informatica e per definire le misure di resilienza dei sistemi cyber-fisici.
Un documento di riferimento sullo stato dell'arte della crittografia quantum-safe e quantistica è il rapporto pubblicato da ACN a Luglio 2024 [4].
A livello globale, diversi paesi stanno implementando soluzioni crittografiche avanzate per proteggere le loro reti energetiche.
L'Energy Sector Cybersecurity Framework sviluppato dal NIST ha incluso linee guida specifiche per l'uso della crittografia nelle reti elettriche. Nel 2023, l'ente di regolazione FERC (Federal Energy Regulatory Commission) ha richiesto l'implementazione obbligatoria di crittografia per tutte le comunicazioni tra le apparecchiature di rete per ridurre il rischio di cyberattacchi.
In Europa, la Direttiva NIS2 (Network and Information Security Directive) aggiornata nel 2022 ha introdotto requisiti di sicurezza informatica più rigorosi per le infrastrutture critiche, comprese quelle energetiche. Questa direttiva incoraggia l'uso di crittografia avanzata e di tecnologie come la crittografia omomorfica per proteggere i dati sensibili durante il loro trattamento.
La Cina sta investendo pesantemente nella protezione delle sue reti energetiche con l'uso di crittografia quantistica. Il progetto "QuantumCTek" ha già implementato canali crittografici quantistici in alcune delle sue reti elettriche di distribuzione per proteggere i dati strategici dalle minacce informatiche. Queste soluzioni combinano QKD con protocolli di sicurezza tradizionali per garantire la protezione dei dati più sensibili.
Numerosi progetti internazionali stanno lavorando per migliorare la sicurezza crittografica delle reti energetiche. Iniziative come il progetto europeo SDN-microSENSE puntano ad integrare tecnologie di crittografia avanzata con le architetture di rete SDN (Software-Defined Networking) per migliorare la risposta agli attacchi cibernetici in tempo reale.

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978
[2] "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, United States National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Nov. 2001
[3] M. Kaur and S. Kalra, "Security in IoT-based smart grid through quantum key distribution," Adv. Intell. Syst. Comput., vol 554, pp. 523–530, Sep. 2017
[4] ACN, "Crittografia post-quantum e quantistica. Preparazione alla Minaccia Quantistica", Luglio 2024, [online] Available: https://www.acn.gov.it/portale/documents/20119/85999/ACN_Crittografia_Quantum_Safe.pdf/d7eb595c-ee7f-848b-6c14-abf64cafb310?t=1721310015826
[5] G. Ciaramella, F. Martinelli, F. Mercaldo, A. Santone "Exploring Quantum Machine Learning for Explainable Malware Detection". IJCNN 2023: 1-6

OB2: preservare la resilienza del sistema elettrico da attacchi cyber

Un ambito applicativo particolarmente critico per i sistemi elettrici è quello dei sistemi elettronici di misura, controllo e automazione che pervadono le reti e microreti elettriche. Un attacco a tali sistemi può comportare danni che vanno dal furto di dati, all'invio di comandi fraudolenti fino all'interruzione del servizio. Diviene, pertanto, fondamentale per proteggere le reti, agire su due livelli: sull'infrastruttura informatica, integrando misure di protezione e di rilevamento degli attacchi; sull'infrastruttura fisica, applicando strategie che confinino i disservizi a valle di un possibile attacco che ha superato le misure di primo livello.
Con riferimento al primo ambito, una interessante review dello stato dell'arte sulla cyber-resilienza a livello di elettronica di potenza presente ai diversi livelli di tensione dei sistemi elettrici è riportata in [1].
In relazione ai dispositivi di "piccola taglia" presenti nelle reti di distribuzione elettrica (es. dispositivi IoT a bassa potenza), il NIST ha avviato la selezione di algoritmi di "crittografia leggera" per la loro protezione. Poiché le reti di distribuzione elettrica sono sempre più popolate da dispositivi IoT a bassa potenza, l'uso di algoritmi di crittografia leggera è diventato essenziale. Algoritmi come SPECK e SIMON, sviluppati dalla NSA, sono progettati per dispositivi con risorse limitate, come sensori e attuatori, offrendo protezione senza compromettere le prestazioni della rete. Questi algoritmi stanno vedendo un'ampia adozione nelle reti di distribuzione per proteggere i dati critici e garantire la sicurezza operativa.
Con riferimento al secondo ambito, una possibile misura di intervento per limitare i disservizi all'utente finale, potrebbe riguardare la possibilità di riconfigurare le connessioni delle reti elettriche in corrispondenza di cyberattacchi in aree specifiche delle reti di distribuzione. Attualmente, l'optimal network reconfiguration è prevalentemente applicato per ottimizzare le prestazioni dei sistemi di distribuzione elettrica. Questo approccio mira a ridurre al minimo le perdite di potenza e a migliorare il profilo di tensione, garantendo così un'efficienza energetica superiore e una maggiore affidabilità del servizio. In ottica evolutiva, esso potrebbe essere applicato anche per innalzare il livello di cyber-resilienza delle reti.
Il progetto affronta l'obiettivo della resilienza da attacchi cyber sviluppando ambienti cyber-fisici o Digital Twin, rappresentazioni digitali dettagliate di componenti, sistemi o processi reali. Proprio dal mondo reale il digital twin attinge le informazioni per aggiornare il suo

stato. Per mezzo di questa replica digitale è possibile studiare il comportamento del sistema o del fenomeno di interesse attraverso simulazioni, analisi e valutazioni considerando differenti scenari. Ambienti di potenziale interesse presenti in letteratura sono CP-SyNet [2] e Wattson [3].

[1] J. Hou, C. Hu, S. Lei, Y. Hou, “Cyber resilience of power electronics-enabled power systems: A review”, Renewable and Sustainable Energy Reviews, Volume 189, Part B, 2024, 114036, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2023.114036
[2] L. Wang, J. Halvorsen, S. Pannala, A. Srivastava, A. H. Gebremedhin, N. N. Schulz “CP-SyNet: A tool for generating customised cyber-power synthetic network for distribution systems with distributed energy resources”, IET Smart Grid, 2022 https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.12088
[3] L. Bader, Ö. Sen, J. Filter, M. Serror, D. van der Velde, E. Padilla, O. Lamberts, I. Hacker, M. Henze “Comprehensively Analyzing the Impact of Cyberattacks on Power Grids”, 2023.

OB3: sfruttare le tecnologie di intelligenza artificiale per la cybersecurity dei servizi energetici

L’Intelligenza Artificiale sta trasformando la cybersecurity attraverso diversi approcci avanzati. I sistemi IA analizzano grandi volumi di dati per individuare minacce e anomalie in tempo reale, migliorando la prevenzione degli attacchi. Monitorano anche il comportamento degli utenti e il traffico di rete per rilevare attività sospette. L’IA automatizza la risposta agli incidenti e gestisce la sicurezza con maggiore efficienza. Uno degli aspetti più critici della cybersecurity è la continua capacità dei cybercriminali di applicare nuove tecniche che costringono ad un continuo aggiornamento delle strategie e delle tecnologie difensive adottate per proteggere le infrastrutture. In tal senso, è fondamentale adottare modelli di Machine Learning (ML) progettati per “autoproteggersi” adottando strategie come: machine learning contradditorio; rilevamento continuo delle possibili anomalie e verifica/validazione, attraverso un monitoraggio continuo dei dati in ingresso e previsionali per identificare comportamenti insoliti che potrebbero indicare tentativi di manipolazione; meccanismi di difesa adattiva che implementino sistemi di feedback per aggiornare e migliorare automaticamente le difese in risposta a nuove minacce identificate.
Le performance dei modelli di Machine Learning dipendono fortemente dalla quantità e dalla qualità dei dati. Anche nei task di identificazione degli attacchi, come la classificazione o il clustering, ad esempio, i dati disponibili sono frequentemente soggetti ad uno sbilanciamento, ovvero la numerosità di campioni per ciascuna classe da identificare non è omogenea. Lo sbilanciamento dei dataset rappresenta un forte limite nella generazione di modelli che risultino efficaci.
Negli ultimi anni, l'uso degli LSTM Autoencoder per la rilevazione di anomalie in ambito cybersecurity ha suscitato un crescente interesse nella comunità scientifica. Gli LSTM (Long Short-Term Memory) sono una variante delle reti neurali ricorrenti (RNN) particolarmente adatta all'analisi di dati sequenziali, grazie alla loro capacità di catturare dipendenze a lungo termine. Gli Autoencoder, d'altra parte, sono reti neurali progettate per apprendere una rappresentazione compressa dei dati, utile per identificare pattern normali e rilevare deviazioni significative. Combinando queste due architetture, gli LSTM Autoencoder sono stati applicati con successo nella rilevazione di anomalie in vari contesti legati alla cybersecurity.
Ad esempio, Wei et al. in [1] hanno proposto un modello basato su LSTM Autoencoder per la rilevazione di attacchi DDoS, dimostrando un'accuratezza molto elevata nel rilevare tali minacce. Un ulteriore esempio è costituito da Yuan et al. in [2] in cui viene introdotto "DabLog", un metodo basato su Autoencoder per la rilevazione di anomalie in log di eventi discreti, migliorando la capacità di identificare attività sospette nei sistemi informatici.
Questi studi evidenziano l'efficacia degli LSTM Autoencoder nella rilevazione di anomalie in ambito cybersecurity, offrendo soluzioni promettenti per la protezione dei sistemi informatici da minacce sia esterne che interne.
Con riferimento alle esperienze di utilizzo delle GAN (Generative Adversarial Network) nell’implementazione di sistemi di difesa degli asset dell’energia da attacchi cyber, i contributi rilevati sono in numero più esiguo, a testimonianza del fatto che si tratta di un campo in cui la ricerca è ancora in fase quasi pioneristica e in cui la complessità dei sistemi di AML (Adversarial Machine Learning), abbinata a quella di un dominio, richiede nuove idee e nuovi paradigmi per essere ben sviluppata. Il concetto di Generative Adversarial Networks (GAN) è apparso per la prima volta nel 2014 come un'idea rivoluzionaria del ricercatore di Google Brain Ian J. Goodfellow [3]. Radford et al. [4] hanno introdotto una nuova classe di reti CNN, chiamate Deep Convolutional Generative Adversarial Networks (DCGAN), che migliora le performance delle reti GAN e le rende stabili per l'addestramento.
Tra le tipologie di GAN ci sono le Time-series Generative Adversarial Networks (T-GAN), una classe di reti neurali progettate per modellare e generare dati sequenziali che si sviluppano nel tempo. La caratteristica distintiva delle T-GAN rispetto ad altre GAN risiede nella loro abilità di cogliere relazioni temporali e dipendenze tra i punti di una sequenza, avvalendosi di strati di tipo LSTM o fondati su meccanismi di attenzione. Tuttavia, le T-GAN possono essere difficili da addestrare poiché soggette ad instabilità durante la fase di addestramento. A tal proposito, sono state introdotte delle architetture di tipo WGAN (Wasserstein GAN) da Arjovski et al. in [5], che utilizzano la metrica di Wasserstein per stabilizzare il processo di ottimizzazione delle curve di apprendimento.
Il lavoro presentato in [6] discute le minacce di cybersecurity ai danni di sistemi energetici causate dallo sfruttamento dell’AML. Un primo tentativo di impiego delle GAN per risolvere un problema di data generation e, dunque, di data augmentation in comunicazioni basate su

protocolli tipici dell'ambito energetico è riportato in [7].
Le GAN rappresentano una frontiera emergente nella cybersecurity esplorata nel progetto, offrendo sia opportunità per migliorare le difese sia sfide legate al loro potenziale uso malevolo. La ricerca continua in questo campo è fondamentale per sviluppare strategie efficaci che sfruttino i benefici delle GAN, mitigandone al contempo i rischi associati.

[1] Yuanyuan Wei, Julian Jang-Jaccard, Fariza Sabrina, Wen Xu, Seyit Camtepe, Aeryn Dunmore. 2023. Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data. Cryptography and Security. https://arxiv.org/abs/2305.09475
[2] Lun-Pin Yuan, Peng Liu, and Sencun Zhu "Recompose Event Sequences vs. Predict Next Events: A Novel Anomaly Detection Approach for Discrete Event Logs", In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21). Association for Computing Machinery, New York, NY, USA, 336–348, 2021, https://doi.org/10.1145/3433210.3453098
[3] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y., "Generative adversarial nets", Advances in neural information processing systems, 27, 2014
[4] L. Metz, A. Radford, S. Chintala "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks", arXiv preprint arXiv:1511.06434, 2018
[5] Arjovsky, M., Chintala, S. & Bottou, L.. (2017). Wasserstein Generative Adversarial Networks. Proceedings of the 34th International Conference on Machine Learning, in Proceedings of Machine Learning Research 70:214-223 Available from https://proceedings.mlr.press/v70/arjovsky17a.html
[6] Bor, Martin C., et al. "Adversarial machine learning in smart energy systems", Proceedings of the Tenth ACM International Conference on Future Energy Systems, 2019
[7] F. Marulli, F. Lancellotti, P. Paganini, G. Dondossola, R. Terruggia "Towards a novel approach to enhance cyber security assessment of industrial energy control and distribution systems through generative adversarial networks", Journal High Speed Networks, 2024, https://doi.org/10.1177/0926680124129140
[8] P. Bountakas et. al. SYNAPSE "An Integrated Cyber Security Risk & Resilience Management Platform, With Holistic Situational Awareness, Incident Response & Preparedness Capabilities", SYNAPSE. ARES 2024: 128:1
[9] O. Osliak, A. Saracino, F. Martinelli, P. Mori, "Cyber threat intelligence for critical infrastructure security", Concurr. Comput. Pract. Exp. 35(23) (2023)-128:10

b) Attività svolte nel triennio precedente
Le attività del progetto si pongono in continuità con il Progetto Integrato 2.1 Cybersecurity dei sistemi energetici del Piano Triennale della Ricerca di Sistema 2022-2024 e si basano sui suoi output riportati nel seguito:

- Standard di cybersecurity per protocolli OT e relative valutazioni di impatto sulle prestazioni delle comunicazioni
- Protocolli quantistici di autenticazione e cyber difesa per reti/micro-reti elettriche
- Algoritmi di cifratura e autenticazione
- Schemi e dispositivi di protezione elettrica per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche
- Metodologie e valutazioni di conformità di cybersecurity per dispositivi di controllo e comunicazione utilizzati in infrastrutture energetiche
- Procedure di autorizzazione per un'architettura sicura di monitoraggio e controllo distribuito che integri sistemi di generazione, accumulo di energia e produzione di idrogeno
- Metodologie e strumenti per il calcolo del rischio dinamico basato su analisi automatica di vulnerabilità e modelli di monitoring di rete
- Modelli di digital twins per simulazioni di attacchi alle smart grids e analisi di resilienza
- Metodi e modelli di apprendimento automatico per l'analisi e il rilevamento di anomalie in infrastrutture energetiche
- Dataset per sviluppo e test di algoritmi di anomaly detection
- Sistemi di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori e relative validazioni
- Metodologie e piattaforme di analisi di eventi e misure per il rilevamento di attacchi cyber a reti, micro-reti e applicazioni energetiche, che integrano modelli e algoritmi di AI, architetture di stream analytics, sistemi di raccolta, conservazione e analisi di flussi di dati OT
- Strumenti per la privacy dei dati di applicazioni energetiche, quali i sistemi per la ricarica di veicoli elettrici
- Prototipo di dispositivo di protezione, basato su apparati di crittografia quantistica, per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle micro-reti elettriche
- Componenti integrabili di ML per il rilevamento di anomalie in reti/microreti elettriche
- Infrastruttura di calcolo HPC a basso consumo per il controllo informatico di reti intelligenti cyber-resilienti.

In particolare, l'attività RSE relativa al framework per la valutazione di soluzioni di cybersecurity si ricollega in parte ai risultati delle LA 1.5 e 2.6 del triennio 2022-2024. Nel triennio 2025-2027 verranno consolidate ed estese le funzionalità di misurazione delle prestazioni e valutazione di conformità in un unico ambiente di test.
Si prevede di proseguire la collaborazione con il progetto RdS "Mobilità sostenibile e interazione con il sistema energetico" per quanto

riguarda le comunicazioni di telecontrollo e la cybersecurity delle infrastrutture di ricarica dei veicoli elettrici, cui si intende applicare le funzionalità del framework sviluppato nel progetto 2.1. Proseguirà il contributo alla sperimentazione del CIR e agli eventuali aggiornamenti della norma CEI PAS 57-127 che si dovessero verificare nel triennio 2025-2027.
Per la progettazione dei cybersecurity twin, le attività RSE si baseranno ed estenderanno i modelli simulativi ICT sviluppati nella LA 3.6 del progetto del PTR 2022-2024, considerando anche le valutazioni della LA 2.11.
Lo strumento SecuriDN sviluppato nella LA 3.6 del PTR 2022-2024 verrà esteso in termini di capacità di modellazione e la piattaforma di monitoraggio e detection verrà ampliata con nuovi moduli sviluppati a partire da quelli esistenti. Le attività di detection svolte da RSE in questo triennio considereranno scenari di attacco più complessi rispetto a quelli indirizzati nella LA 3.11 del triennio precedente. Inoltre, i dataset considerati per l'addestramento e la validazione dei modelli afferiranno pienamente all'ambito elettro-energetico e di preferenza verranno estratti da ambienti sperimentali reali e non da simulazioni. La piattaforma di raccolta dati farà uso di strumenti di data streaming estendendo l'infrastruttura descritta nella LA 3.3 del PTR 2022-2024 in termini di sorgenti dati e di maggiore caratterizzazione delle informazioni all'ambito energetico. A partire dall'ambiente di detection basato su AI sviluppato nella LA 3.6 del PTR 2022-2024, in questo triennio si consolideranno i moduli di generazione dei dataset ottenuti da ambienti sperimentali e per mezzo di tecniche di AI generativa, di maggiore dimensione e rappresentatività. Questo permetterà di poter raffinare i modelli di anomaly detection basati su LSTM Autoencoder implementati. Al fine di accrescere le capacità di detection real time, si migliorerà l'integrazione dei moduli di generazione dei dati con i moduli basati su AI di identificazione di azioni malevole, creando opportune pipeline tra lo stack ELK, in cui sono raccolti i dati, e i modelli multivariati di detection in linea con quanto fatto per il modello univariato nel PTR 2022-2024.
In relazione alle attività ENEA e dei relativi co-beneficiari, le attività del presente triennio relative all'utilizzo delle tecniche di crittografia quantistica a protezione delle reti elettriche consentiranno di estendere i risulti delle LA1.7, LA1.8, LA1.2, LA1.6 e LA2.7 del PTR 2022-2024, sviluppando soluzioni che rendono l'utilizzo della crittografia quantistica idoneo anche alle reti non dotate di mezzo trasmissivo in fibra. Le attività ENEA connesse allo studio di eventi e misure per il rilevamento e la difesa da attacchi cyber a reti, micro-reti e applicazioni energetiche sviluppate nell'ambito del WP3 nel presente PTR utilizzeranno l'infrastruttura HPC realizzata nel corso del PTR 2022-2024 (WP3).
Le attività CNR e dei suoi co-beneficiari permetteranno di rendere utilizzabili i risultati sull'osservatorio (LA 1.12 del PTR 2022-2024) ed i servizi per la cyber security nella continuazione di questa linea di attività del presente triennio; così come i risultati ottenuti per gli aspetti della sicurezza dei veicoli elettrici nel triennio 2022-2024 (LA 3.14) si espanderanno in questo triennio acquisendo una loro specifica rilevanza in una nuova LA.
Si continueranno a portare avanti le linee di ricerca sulla explainable AI, applicate al malware e alle reti, partendo da risultati iniziali della LA 3.14 del PTR 2022-2024. Inoltre, verrà aperto un nuovo filone di quantum machine learning, con interesse anche sugli aspetti di explainability. Anche idee per la gestione dinamica del rischio sviluppate nella LA 2.4 del precedente triennio verranno sviluppate nelle LA del presente triennio.

c) Obiettivi scientifici e tecnologici e progressi attesi rispetto allo stato dell'arte
Di seguito, si riportano gli obiettivi scientifici e tecnologici e i progressi attesi rispetto allo stato dell'arte suddivisi per obiettivi prioritari del progetto.

OB1: garantire l'adeguatezza delle tecnologie di cybersecurity nelle applicazioni digitali per il controllo energetico

Data l'importanza strategica delle infrastrutture energetiche e delle reti "smart" di ultima generazione, occorre sottolineare che queste sono caratterizzate da apparati che si scambiano dati ed interoperano coordinandosi e rispondendo a comandi e richieste da parte di controllori digitali. Un eventuale attacco cibernetico su uno degli apparati di rete non comporta criticità solo a livello del singolo sistema, ma può inficiare l'operatività di porzioni, anche estese, della infrastruttura energetica. In tale contesto, risulta sempre più indispensabile l'invio di dati, misure, stati e comandi in maniera sicura.
Lo sviluppo di un framework integrato per valutazioni prestazionali e di conformità di soluzioni di cybersecurity standard costituisce un supporto fondamentale per raggiungere l'obiettivo di migliorare il livello di cybersecurity by design delle applicazioni di controllo energetico. L'integrazione di funzioni di gestione di chiavi e certificati digitali rappresenta un contributo essenziale alla cybersecurity di tutte le nuove applicazioni richieste dalla transizione energetica. Gli sviluppi previsti nel progetto costituiscono un avanzamento nell'applicazione ai sistemi energetici sia delle soluzioni più mature e standardizzate, sia delle soluzioni quantum-safe oggetto di sviluppi di ricerca e di possibili attività di standardizzazione futura.
Gli sviluppi relativi all'implementazione di protocolli di autenticazione basati su QKD consentirà il conseguimento di progressi nel settore di interesse giacché, allo stato attuale, l'applicazione della crittografia quantistica ai sistemi energetici risulta, ancora, non esplorata a livello sperimentale. Le attività proposte intendono andare oltre lo stato dell'arte della crittografia, sfruttando le leggi della fisica (e non il risultato di algoritmi) per ottenere sequenze simmetriche e sicure di informazioni da trasmettere su un canale quantistico. Mettendo a sistema le competenze maturate in questi anni, si verificherà la potenziale efficacia dell'utilizzo della crittografia QKD nel settore energetico mediante l'infrastruttura di test realizzata per il progetto, che verrà opportunamente estesa con apparati che consentiranno di

sperimentare la crittografia quantistica anche per reti energetiche non dotate di fibra ottica per la comunicazione dati.
Grazie al framework che sarà sviluppato le valutazioni di conformità agli standard di cybersecurity saranno effettuabili sia su dispositivi di protezione, automazione, controllo degli impianti di generazione connessi alle reti elettriche in media tensione, sia su dispositivi gateway e controllori commerciali economici più adatti alla implementazione di servizi di flessibilità di aggregati di utenti residenziali e comunità energetiche connesse alle reti in bassa tensione. Il framework faciliterà le attività di test e certificazione di cybersecurity di competenza dei laboratori accreditati, in linea con le Direttive NIS2 e Cyber Resilience Act.

OB2: preservare la resilienza del sistema elettrico da cyber attacchi

L'approccio digital twin per analisi dei sistemi elettrici non è concettualmente nuovo. Gli ambienti e le tecnologie per la stima dello stato sono utilizzati nell'operatività dei centri di controllo degli operatori di rete per la pianificazione e l'esercizio in sicurezza del sistema elettrico. In questo progetto si intendono proporre soluzioni di cybersecurity twin, utili anche all'analisi bidirezionale della cybersicurezza, che rappresentano un effettivo progresso rispetto allo stato dell'arte che risulta limitato sia in termini di scenari energetici e di attacco.

OB3: sfruttare le tecnologie di intelligenza artificiale per la cybersecurity dei servizi energetici

L'applicazione di algoritmi di Intelligenza Artificiale e Machine Learning alle infrastrutture di scambio dati dei sistemi energetici costituisce, ad oggi, oggetto di attività di ricerca. Nonostante recenti prodotti commerciali includano algoritmi di Machine Learning, la loro capacità di analisi e detection di anomalie nelle infrastrutture energetiche non è ancora stata validata.
Gli sviluppi previsti nel progetto relativi a moduli di detection basati su algoritmi di intelligenza artificiale costituiscono un passo avanti rispetto allo stato dell'arte in diverse direzioni.
Un passo avanti è la possibilità di validazione delle capacità di detection di anomalie nelle comunicazioni per il controllo di carichi, generatori e sistemi di accumulo, sia stazionari che mobili, connessi a infrastrutture di rete in media e bassa tensione. L'applicabilità delle classi di algoritmi di apprendimento automatico, risultate nel PTR 2022-2024 più idonee per il rilevamento di anomalie da attacchi cyber applicazioni energetiche, permetterà di compiere un significativo passo avanti in termini di affidabilità di queste tecnologie.
La modellazione di processi di attacco a infrastrutture energetiche costituirà un'evoluzione dello stato dell'arte per strumenti che semplificano le analisi probabilistiche di cybersecurity attraverso funzionalità di interfaccia grafica, ontologie di cybersecurity, traduttori di grafi di attacco in reti bayesiane.
Lo sviluppo di metodologie di explainable AI per l'analisi delle intrusioni e delle minacce nel settore energetico sarà un valore aggiunto delle ricerche del progetto integrato, in cui verranno unite a soluzioni innovative per quantum machine learning.

d) Eventuali collegamenti con altri progetti relativamente alle attività previste nel progetto
1) Progetto MISSION Smart Grid (Multivector Integrated Smart Systems and Intelligent microgrids for accelerating the energy transitiON, https://mission-innovation.it/smart-grid/), in cui RSE sviluppa funzionalità di "Cybersecurity In the Loop" per test facility multi-energy ed ENEA si occupa dello sviluppo connesso alla realizzazione delle infrastrutture energetiche e di comunicazione della smart energy microgrid multivettore.
2) Partenariato esteso SERICS, ovvero SEcurity and RIghts in the CyberSpace (www.serics.eu) finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), in cui 25 istituzioni (incluso CNR) ed industrie italiane collaborano su tematiche che non riguardano specificamente le infrastrutture energetiche, ma si focalizzano su aspetti e tecnologie core della cybersecurity ed aspetti legali e giuridici.
3) Progetto Europeo EU-DREAM (Home - EU Dream) in cui ENEA collabora allo sviluppo di un assistente energetico intelligente, basato su tecniche di AI, capace di ottimizzare le impostazioni energetiche in base alle preferenze individuali, e un intermediario che utilizzerà tecniche di elaborazione del linguaggio naturale (NLP) che semplifica la terminologia tecnica, migliorando l'interazione con l'utente e facilitando la gestione dell'energia.
4) Progetto Rome Technopole (https://ripi.iss.it/ripi/it/progetti-pnrr-rome-technopole/), finanziato nell'ambito del PNRR, il quale si focalizza sui processi di innovazione orientati allo sviluppo sostenibile, alla 'smart specialization', alla riqualificazione e al rilancio del settore industriale, con focus specifico su tre aree tematiche: Transizione Energetica, Transizione Digitale. In Rome Technopole ENEA si occupa di realizzare un digital twin di reti e microreti elettriche.
5) Progetto Europeo NEST – Network 4 Energy Sustainable Transition (https://fondazionenest.it/), finanziato dall'Unione Europea – NextGenerationEU, in cui ENEA si occupa di realizzare un digital twin di reti e microreti elettriche multivettore e multienergy.
6) Progetto SYNAPSE (https://www.synapse-project.eu/), il quale fornisce una piattaforma integrata di gestione del rischio e resilienza nella sicurezza informatica basata su tre pilastri: situation awareness, risposta agli incidenti e preparazione. Per raggiungere questo obiettivo, vengono ampiamente considerate tecnologie, tecniche, strumenti per promuovere una gestione dinamica del rischio, una rilevazione proattiva, il monitoraggio e il tracciamento degli attacchi, e una risposta contro le potenziali minacce, offrendo garanzie di continuità operativa in ogni momento.

2.5 Obiettivi e risultati

a) Obiettivi finali del progetto

La filiera energetica italiana assume un peso rilevante nella stabilità socioeconomica del sistema Paese. In tutte le economie avanzate, l'evoluzione del comparto energia comporta un'accelerazione dei processi di digitalizzazione e di gestione dei rischi di cybersecurity. Investire in ricerca per incrementare la Threat Intelligence nazionale, disporre di tecnologie di cyber-prevenzione e infrastrutture per il rilevamento e la risposta tempestiva ad eventi di crimine informatico risulta strategico per il Paese, come testimoniato dal Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 pubblicato dall' Agenzia per la Cybersicurezza Nazionale.
Il progetto integrato Cyber Security dei Sistemi Energetici per la transizione energetica individua tre principali obiettivi prioritari per la trasformazione digitale dei sistemi energetici:
OB1) garantire l'adeguatezza delle tecnologie di cybersecurity nelle applicazioni digitali per il controllo energetico,
OB2) preservare la resilienza del sistema elettrico a fronte di attacchi cyber,
OB3) sfruttare le tecnologie di intelligenza artificiale per migliorare la cybersecurity delle infrastrutture energetiche.
Le attività di ricerca del progetto hanno la capacità di coinvolgere diversi dipartimenti di ingegneria, fisica e informatica degli atenei italiani che hanno in corso progetti sul tema. Tra le categorie di industrie e imprese collegate agli sviluppi del progetto si annoverano autorità di regolazione, quali ARERA e ACN, operatori di reti elettriche ed energetiche, operatori di infrastrutture di ricarica di veicoli elettrici, operatori dei servizi di flessibilità e aggregatori di risorse energetiche, micro-reti e comunità energetiche, fornitori di dispositivi OT e IoT, fornitori di reti e servizi di comunicazione, fornitori di piattaforme digitali e servizi di sicurezza informatica, fornitori di servizi di identità digitale, enti accreditati di certificazione.
Le ricadute industriali degli output del progetto costituiranno un supporto per gli operatori di infrastrutture energetiche che devono garantire livelli elevati di cybersecurity ai loro servizi.
Gli sviluppi del progetto favoriranno anche le sperimentazioni delle funzioni di flessibilità erogabili dalle diverse tipologie di utenti energetici, anticipando quando previsto dal TIDE (Testo Integrato del Dispacciamento Elettrico) di ARERA e dal Codice di Rete Europeo su Demand Response di prossima emanazione.
Per quanto riguarda le ricadute normative, gli output del progetto saranno di supporto per la regolazione sulla osservabilità e controllabilità delle reti in bassa tensione, e per la standardizzazione nelle nuove tecnologie in funzione dei requisiti delle applicazioni energetiche.

b) Principali risultati attesi/deliverable

L'articolazione del progetto integrato Cybersecurity per la transizione energetica secondo i driver richiamati nella sezione 2.5a consente ai tre affidatari RdS (CNR, ENEA e RSE) di affrontare il tema della cybersecurity considerando le problematiche connesse alla trasformazione digitale dei sistemi energetici con l'intento di fornire strumenti di prevenzione e rimedio alle cyber-minacce connesse ai servizi digitali ed energetici. Più in dettaglio i tre affidatari:

- attraverso le attività del WP1 "Tecnologie di cybersecurity per le nuove applicazioni digitali di controllo energetico", intendono focalizzare l'attenzione sulla gestione dei rischi delle applicazioni energetiche interconnesse, proponendo soluzioni per la sicurezza preventiva nei nuovi protocolli e vettori di telecomunicazione che interconnettono operatori e prosumer energetici;
- attraverso le attività del WP2 "Cybersecurity per infrastrutture energetiche cyber-fisiche più resilienti", intendono sviluppare strumenti e tecnologie per mitigare la vulnerabilità di reti elettriche definendo strategie, azioni e schemi di protezione che le rendano cyber-resilienti;
- attraverso le attività del WP3 "AI per la cybersecurity e la privacy dei servizi energetici", intendono sviluppare strumenti e ambienti che permettono di sfruttare le potenzialità dell'AI per il rilevamento di nuove minacce di cybersecurity, preservando al contempo la privacy dei dati e delle computazioni. Gli algoritmi di intelligenza artificiale sviluppati saranno robusti, in grado di resistere ad attacchi e, ove possibile, "spiegabili".

Di seguito sono sinteticamente indicati gli output attesi del progetto integrato, raggruppati per obiettivo prioritario e tipologia.

OB1: garantire l'adeguatezza delle tecnologie di cybersecurity nelle applicazioni digitali per il controllo energetico

Le attività finalizzate al miglioramento della cybersecurity delle comunicazioni produrranno Rapporti Tecnici e Software relativi a:

- Protocolli post-quantum e quantistici di autenticazione e cifratura per reti energetiche (LA 1.1, 1.7, 1.10, LA 1.11)
- Piattaforma per valutazioni di impatto di standard di cybersecurity sulle prestazioni delle comunicazioni OT e di conformità di cybersecurity per dispositivi di controllo e comunicazione utilizzati in infrastrutture energetiche (LA 1.1, LA 1.7, LA 1.11)
- Infrastruttura sperimentale per test su reti con canali trasmissivi in fibra e in aria per network con cybersicurezza quantistica nella distribuzione dell'energia (LA 1.2, LA 1.4, LA 1.8)
- Progetto pilota GOCYS: Governance Observatory of CYber Security (LA 1.3, LA 1.9)

OB2: preservare la resilienza del sistema elettrico da cyber attacchi

Le attività finalizzate a preservare la resilienza dei sistemi energetici a fronte di attacchi cyber produrranno Rapporti Tecnici e Software relativi a:
- Modelli di digital twins per simulazioni di attacchi alle smart grids e analisi di resilienza (LA 2.1, LA 2.2, LA 2.7, LA 2.8, LA 2.12, LA 2.14)
- Studi di cyber vulnerabilità delle tecnologie di generazione delle reti elettriche e test sulle smart grid anche mediante infrastruttura sperimentale dotata di sistema crittografico basato su comunicazione mista fibra e in aria (LA 2.4, LA 2.9, LA 2.11)
- Ambiente di simulazione di un software basato su tecniche di AI per il rilevamento di intrusioni in reti energetiche da integrare negli apparati di protezione ENEA (LA 2.10)
- Soluzioni di sicurezza, privacy e fiducia per comunità energetiche (LA 2.13)
- Infrastruttura decentralizzata, trustless e post-quantum per la raccolta e l'analisi dei dati per la gestione di Federated Smart Grids (LA 2.15)

OB3: sfruttare le tecnologie di intelligenza artificiale per la cybersecurity dei servizi energetici

Le attività finalizzate all'utilizzo di tecnologie di intelligenza artificiale per migliorare le capacità di risposta e difesa da attacchi cyber produrranno Rapporti Tecnici e Software relativi a:
- Dataset per sviluppo e test di algoritmi di anomaly detection (LA 3.1, LA 3.12)
- Tecniche GAN per la generazione di dataset e la valutazione di algoritmi di rilevamento intrusioni (LA 3.1, LA 3.5, LA 3.6, LA 3.12, LA 3.16, LA 3.17)
- Metodi e modelli di apprendimento automatico per l'analisi e il rilevamento di anomalie in infrastrutture energetiche (LA 3.1, LA 3.8, LA 3.12, LA 3.19)
- Sistema di mitigazione di attacchi adversarial ML per la risposta automatica e la resilienza in contesti reali (LA 3.2, LA 3.3, LA 3.7, LA 3.13)
- Ambiente prototipale per la mitigazione di minacce informatiche tramite isolamento automatico di porzioni di reti di comunicazione (LA 3.14)
- Blockchain per smart grid energetiche (LA 3.4, LA 3.15)
- Sistema innovativo basato su tecniche di AI per il rilevamento e la risposta automatica a intrusioni in reti energetiche (LA 3.18)
- Quantum machine learning per smart grid (LA 3.24)
- Metodologie e piattaforme di analisi di eventi e misure per il rilevamento di attacchi cyber a reti, micro-reti e applicazioni energetiche, che integrano modelli e algoritmi di AI, architetture di stream analytics, sistemi di raccolta, conservazione e analisi di flussi di dati OT (LA 3.12, LA 3.25).

È, inoltre, prevista una attività di diffusione (WP4) i cui output saranno contenuti in Rapporti Tecnici, Pubblicazioni scientifiche, notizie ed eventi e permetteranno di raggiungere i potenziali utilizzatori dei risultati del progetto, sia del comparto ricerca che industriale.
Tutti gli output sopra descritti contribuiranno al raggiungimento degli obiettivi di progetto e all'avanzamento rispetto allo stato dell'arte, come descritto nella sezione 2.4c.
Gli output (risultati e prodotti) attesi dalle singole LA del progetto sono riportati nella sezione descrittiva di ciascuna di esse e riassunti nella sezione "Tabella riassuntiva prodotti della ricerca ed elementi di verifica del progetto", cui si rimanda.

2.6 Fattibilità tecnico-scientifica

a) Fattibilità tecnico-scientifica
Le attività del progetto necessitano di competenze trasversali per applicare conoscenze specifiche nelle diverse tecnologie digitali degli ambienti IT (sistemi distribuiti, reti di comunicazione, architetture virtualizzate), nel contesto OT (sistemi SCADA, dispositivi di campo, applicazioni di protezione, automazione, controllo e gestione dell'energia) e nelle analisi dei sistemi elettrici (es. Optimal Network Reconfiguration). Le soluzioni da sviluppare saranno caratterizzate da una notevole complessità funzionale, tecnologica e architetturale, sia per l'innovatività della tematica che per la vulnerabilità intrinseca delle soluzioni proposte connessa alla capacità di aggiornamento continua dei cybercriminali.
Questa complessità è supportata dal background acquisito dagli affidatari e dai co-beneficiari attraverso esperienze pregresse riportate nelle sezioni 2.4b e 2.4d) e dalla collaborazione con altri enti di ricerca con i quali verranno stipulati accordi scientifici specifici.
Gli obiettivi progettuali descritti nella sezione 2.5a saranno conseguiti dai tre affidatari (RSE, ENEA e CNR) e dai loro co-beneficiari attraverso le ricerche oggetto delle Linee di Attività (LA) che afferiscono Work Package in cui il progetto si articola:

- WP1 Tecnologie di cybersecurity per le nuove applicazioni digitali di controllo energetico
- WP2 Cybersecurity per infrastrutture energetiche cyber-fisiche più resilienti
- WP3 AI per la cybersecurity e la privacy dei servizi energetici
- WP4 Diffusione.

Il progetto prevede un totale di 58 LA, la cui durata individuale è stata definita in modo tale da garantire la possibilità di una verifica intermedia sull'avanzamento del progetto e sulle sinergie tra le LA correlate. In particolare, per RSE ogni LA ha una durata di 12 mesi, mentre per ENEA e CNR e i loro co-beneficiari ogni LA ha una durata di 18 mesi.
Durante lo svolgimento del progetto RSE, in qualità di coordinatore del progetto integrato, stabilirà interazioni e organizzerà incontri tra affidatari e co-beneficiari, calendarizzati in funzione dello svolgimento e delle esigenze del progetto (indicativamente a M14, M20 e M26), finalizzati a verificare lo stato di avanzamento delle attività, identificare sinergie e collegamenti, analizzare eventuali criticità ed individuare azioni correttive, organizzare azioni di diffusione congiunte.
I risultati della ricerca saranno testati nei laboratori e nelle infrastrutture di ricerca dei rispettivi affidatari, arricchendo il patrimonio di competenze e risorse disponibili per la valutazione e sperimentazione della cybersecurity nei sistemi energetici.
Le attività di diffusione prevederanno sia azioni di formazione e disseminazione tecnico-scientifica rivolte agli stakeholder, sia partecipazioni e supporto ai tavoli tecnici istituiti dagli enti di normazione nazionali ed internazionali.
I risultati saranno documentati in rapporti e pubblicazioni tecnico-scientifiche che, analogamente ai prodotti della ricerca saranno resi accessibili tramite i siti web degli affidatari. Gli strumenti progettati e sviluppati (metodologie, strumenti, modelli, piattaforme, prototipi) offriranno soluzioni innovative con funzionalità cruciali per i futuri scenari energetici. I benefici del progetto influenzeranno positivamente la maturità della cybersecurity nei prodotti di mercato, nel settore industriale e nella ricerca applicata ai sistemi energetici, contribuendo al comportamento resiliente delle infrastrutture energetiche e, di conseguenza, allo sviluppo socioeconomico sempre più energivoro.

2.7 Impatto sul sistema energetico e benefici attesi

a) Impatto e benefici sul sistema energetico
Le attività del progetto mirano allo sviluppo di prodotti di ricerca hardware e software funzionali alla connessione di sistemi decarbonizzati e non inquinanti attraverso soluzioni cyber-resilienti. Indirettamente le soluzioni di cybersecurity sviluppate nel progetto, in quanto parte integrante della componente smart delle infrastrutture energetiche previste dagli obiettivi del PNIEC, abilitano e contribuiscono ai miglioramenti ambientali derivanti, ad esempio, dalla gestione integrata di risorse energetiche rinnovabili, infrastrutture di ricarica di veicoli elettrici e pompe di calore.

b) Benefici per gli utenti
Gli obiettivi di decarbonizzazione, elettrificazione dei consumi ed efficienza energetica della transizione energetica presuppongono un coinvolgimento diretto degli utenti finali. La partecipazione degli utenti finali ai mercati della flessibilità consentirà loro di beneficiare dei vantaggi finanziari derivanti dall'autoconsumo e dall'ottimizzazione delle risorse delle comunità energetiche.
I benefici per gli utenti sono una diretta conseguenza della riduzione dei rischi di malfunzionamento dei servizi energetici grazie all'applicazione di misure di cybersecurity. In assenza di tecnologie cyber-resilienti, gli utenti finali potrebbero subire anomalie del servizio a causa di attacchi informatici ai sistemi di controllo delle reti e delle risorse energetiche distribuite. Le misure di cybersecurity e privacy indirizzate dal progetto consentono di proteggere tali sistemi dagli attacchi cyber, sia attraverso soluzioni preventive che difensive. In quanto tali, esse abilitano e agevolano l'integrazione di quote crescenti di fonti rinnovabili nelle reti, l'efficienza energetica, la sicurezza energetica e il mercato interno, con ricadute positive nel medio e lungo termine sull'economia e la salute degli utenti dei sistemi energetici.

c) Previsione delle ricadute applicative
I risultati del progetto sperimentano sia tecnologie di cybersecurity considerate mature in casi applicativi significativi per la transizione energetica, sia tecnologie e piattaforme innovative.
L'applicazione di tecnologie mature di cybersecurity a infrastrutture energetiche permetterà a fornitori e sviluppatori di integrare tali tecnologie in dispositivi e prodotti di mercato, quali controllori di impianti di generazione e di infrastrutture di ricarica.
Le valutazioni delle funzioni di cybersecurity contribuiranno allo sviluppo di applicazioni sicure di scambio dati che coinvolgono operatori di rete, proprietari di impianti di generazione, di infrastrutture di ricarica, aggregatori.
Gli sviluppi sui test di conformità contribuiranno alla competitività del mercato dei dispositivi OT e IoT, utilizzati nelle reti energetiche per funzioni di protezione, automazione, controllo e comunicazione, favorendo la loro certificazione di conformità a standard di cybersecurity riconosciuti a livello internazionale. Gli sviluppi di soluzioni avanzate di protezione e rilevamento di anomalie cyber hanno una ricaduta sugli sviluppi dei relativi standard di prodotto e piattaforme di mercato.

I risultati relativi alle tecnologie innovative di cybersecurity permetteranno di indirizzare l'ingegnerizzazione delle soluzioni in funzione della loro effettiva capacità di migliorare il livello di cybersecurity delle applicazioni energetiche, in relazione all'evoluzione degli attacchi cyber. L'implementazione di interventi mitigativi, anche basati su scambio di chiavi quantistiche, potrà avere ricadute applicative rilevanti per i fornitori di apparati elettronici, digitali (es. smart meter), gli operatori di rete, gli sviluppatori di software di cybersecurity.
Un'altra ricaduta delle attività del progetto riguarda le competenze utili ai fini degli sviluppi normativi e regolatori in tema di cybersecurity dei sistemi energetici. La partecipazione ai gruppi di lavoro incaricati degli sviluppi normativi internazionali e nazionali coinvolge una platea eterogenea di esperti, interessati a vario titolo agli sviluppi di cybersecurity, quali Autorità di Regolazione, operatori di rete, operatori di infrastrutture di ricarica, aggregatori, produttori di dispositivi, fornitori di servizi di comunicazione e di cybersecurity, laboratori di test e certificazione.
Non si riscontrano benefici economico-finanziari diretti per gli enti di ricerca proponenti derivanti dalle ricerche del progetto.
L'incremento di competenze acquisite da affidatari e co-beneficiari aumenteranno le loro possibilità di accesso a finanziamenti di ricerca futuri su temi affini.

2.8 Verifica dell'esito del progetto

a) Oggetti e documentazione dei risultati finali
La verifica dell'esito del progetto potrà essere effettuata sulla base degli elementi di metrica e misurazione specificati nella sezione "Tabella riassuntiva prodotti della ricerca ed elementi di verifica del progetto" per connotare le diverse tipologie di prodotti progettuali previsti (quali ad esempio: Rapporti Tecnici, Prototipi, Software, Database, Piattaforme, Pubblicazioni Scientifiche).
Per la valutazione della qualità dei Rapporti Tecnici ci si potrà avvalere di opportuni indicatori. A titolo esemplificativo, nel seguito vengono indicati alcuni indicatori di qualità ritenuti significativi.

- Rispondenza dei contenuti alle attività previste nel PTR;
- Qualità del percorso logico della ricerca;
- Qualità dell'inquadramento del contesto;
- Qualità della descrizione dell'attività svolta;
- Grado di efficacia comunicativa;
- Rilevanza delle pubblicazioni effettuate.

La verifica del software potrà avvalersi dei risultati delle valutazioni e dei test descritti nei relativi Rapporti Tecnici, o della loro presa visione presso le sedi degli affidatari.