PIANO TRIENNALE DI REALIZZAZIONE 2022-24 - RICERCA DI SISTEMA ELETTRICO NAZIONALE
Progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

AFFIDATARIO ENEA

Tema 2.1 – Cybersecurity dei sistemi energetici

Durata: 36 Mesi

Semestre n. 4 – Periodo attività: 01/07/2023 – 31/12/2023

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto "Cybersecurity dei sistemi energetici" svolte durante il quarto semestre di progetto.

Le attività di ricerca, previste dalla seconda annualità di progetto, hanno riguardato le seguenti Linee di Attività:

- ENEA (affidatario del progetto) per LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5;
- UniPD-QTech (cobeneficiario del progetto) per LA1.7 e LA1.8;
- UNINA-FISICA (cobeneficiario del progetto) per LA1.9 e LA1.10;
- ROMA1-DIET (cobeneficiario del progetto) per la LA1.11;
- ROMA3-DICITA (cobeneficiario del progetto) per LA3.9;
- UNIBA (cobeneficiario del progetto) per LA3.10;
- DIG-UNISANNIO (cobeneficiario del progetto) per LA3.12.

ATTIVITA' SVOLTE

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	Nell'ambito del presente semestre, ENEA ha condotto attività di ricerca relativamente alle seguenti linee di attività: LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5. Con riferimento alla **LA1.6** "**Valutazione della cyber-vulnerabilità di microreti elettriche dotate di apparati e tecnologie di comunicazione, monitoraggio, gestione e test degli interventi mitigativi**", sono state espletate, nel presente semestre, le fasi di gara per l'acquisizione del sistema Quantum Key Distribution (QKD) che sarà utilizzato per la distribuzione di chiavi crittografiche, tra un apparato trasmettitore ed uno ricevitore, mediante particelle di luce (fotoni) in accordo alle specifiche tecniche precedentemente definite nella LA1.2.

	Contestualmente è stata avviata la fase realizzativa dell'infrastruttura sperimentale e dell'ambiente di test che saranno impiegati per le fasi sperimentali del progetto. In particolare, i ricercatori del laboratorio Smart Grid e Reti Energetiche (SGRE) hanno predisposto, presso il Centro Ricerche ENEA di Portici, il locale, gli apparati hardware, il software e gli impianti per l'installazione del suddetto sistema QKD e di tutti i misuratori, sensori, attuatori e sistemi di supervisione, controllo e acquisizione dati necessari per la conduzione delle attività di progetto. Tale infrastruttura consentirà di condurre le attività di caratterizzazione sperimentale degli apparati di protezione che saranno realizzati nell'ambito della LA2.7. Essa permetterà anche di effettuare i test di validazione funzionale, definiti nell'ambito della LA 1.2, per ciascuna delle topologie delle reti elettriche identificate e riportate, in dettaglio, nel Rapporto tecnico "Analisi di soluzioni topologiche e predisposizione di un'infrastruttura di test per la validazione di protocolli ed apparati sviluppati per la cybersicurezza" (ENEA22_24-PR 2.1_LA1.2_066). È stato, a tal fine, necessario procedere con l'allocazione degli spazi e con la realizzazione di opportuni cablaggi e connessioni per l'integrazione dei nuovi apparati e sistemi nella nanogrid elettrica preesistente. Si è, inoltre, resa necessaria la predisposizione di un'opportuna interfaccia grafica per la gestione, in tempo reale, mediante software progettato e sviluppato da ricercatori ENEA. Per ciò che concerne la **LA2.7** "**Implementazione di uno schema di protezione e sviluppo di un prototipo per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche**", nel presente semestre è stata avviata la fase di progettazione dell'apparato di protezione proposto nella LA2.2 e dedicato alle reti di distribuzione in presenza di canale trasmissivo in fibra ottica. In accordo allo schema architetturale e alla definizione dei diversi layer dell'apparato, presentati nella LA2.2, sono stati identificati i dispositivi ed i sistemi hardware adeguati alla realizzazione del layer1 (stadio di potenza). L'attenzione è stata dedicata anche all'individuazione della componentistica necessaria agli altri layer dell'interruttore e, in particolar modo, ai diversi sistemi che costituiranno lo strato di comunicazione. Esso sarà costituito da sistemi per la generazione, polarizzazione, trasmissione e ricezione di fotoni. Tali particelle permetteranno di scambiare chiavi crittografiche in maniera sicura mediante tecniche QKD. Faranno parte del layer di comunicazione dell'apparato di protezione sistemi cifranti che consentiranno di crittografare (decrittografare) i messaggi e gli ordini da inviare (o quelli ricevuti da un altro apparato di protezione). Con riferimento alla **LA 3.4** "**Implementazione di una infrastruttura di calcolo a basso consumo per il controllo informatico delle reti elettriche intelligenti cyber-resilienti**", nel presente semestre si è proceduto ad acquisire tutti i componenti dell'infrastruttura identificati nella LA 3.2, tra cui il firewall PaloAlto 3260, lo storage server Supermicro SSG-6049P-E1CR24H, il server di calcolo Supermicro A+ Server 2024US-TRT e le schede FPGA Alveo U280 (AMD).

	È stata, poi, effettuata l'installazione di tutti i componenti hardware e risulta attualmente in corso l'installazione dello stack software previsto. Si è provveduto anche a predisporre e realizzare una Virtual LAN (VLAN) per ospitare i sensori, gli attuatori e gli smart meter e questa è stata opportunamente configurata all'interno dell'architettura della rete del Centro Ricerche ENEA Casaccia. Nel quarto semestre, i ricercatori ENEA si sono dedicati anche all'implementazione di un setup sperimentale per lo svolgimento delle attività di cifratura, di Machine Learning, e, più in generale, di stream analytics pianificate nelle LA 1.11, 3.8, 3.9, 3.10. In dettaglio, sono stati analizzati gli output del Traffic Analyzer "DarkTrace" e sono in fase di definizione le procedure di anonimizzazione dei dati per permetterne la condivisione, con i co-beneficiari di progetto, garantendo il rispetto delle normative relative alla privacy. È stata, inoltre, effettuata la configurazione di un server virtuale nel quale è stato installato il data base "ElasticSearch". Esso accetta gli output relativi al traffico (le informazioni sono a livello di protocollo, il payload del traffico non è considerato) generati da DarkTrace, permette di memorizzarli e di effettuare, su di essi, vari tipi di interrogazioni. Le attività della **LA3.7** "**Realizzazione e implementazione su un caso d'uso di una piattaforma di stream analytics e implementazione delle logiche di training e inference dei modelli di Machine Learning e Artificial Intelligence su acceleratori di varia natura (FPGA/GPU)**" sono state focalizzate, nel presente semestre, sull'implementazione del disegno architetturale precedentemente definito nella LA3.3, utilizzando una piattaforma virtualizzata per creare un ambiente di sviluppo flessibile e scalabile. In dettaglio, i ricercatori ENEA hanno predisposto un ambiente virtuale robusto, che consente agli sviluppatori di eseguire e testare le applicazioni di stream analytics e di Machine Learning (ML) in un contesto simulato e controllato. Ciò consente di gestire risorse e configurazioni in maniera flessibile. L'impiego della soluzione basata su Apache Kafka garantisce coerenza ed efficacia delle operazioni di stream analytics e di ML per la continuous intelligence. Le componenti hardware e software sono state integrate in modo sinergico per ottimizzare le prestazioni e garantire la scalabilità del sistema. A valle della fase implementativa, sono stati condotti i test preliminari per verificare non solo il corretto funzionamento dell'architettura, ma anche la precisione e l'affidabilità delle analisi e delle previsioni generate. Questo processo ha consentito di identificare e risolvere eventuali problemi o inefficienze, allineando le capacità della piattaforma alle necessità imposte dall'uso operativo. Ciò consentirà la conduzione degli esperimenti per il conseguimento degli obiettivi di progetto. Nell'ambito della **LA3.8** "**Test dell'infrastruttura di calcolo a basso consumo per il controllo informatico smart di reti cyber-resilienti**" i ricercatori ENEA hanno dedicato il quarto semestre alla fase di pianificazione di test-case preliminari relativi alla rilevazione di intrusioni nei sistemi informatici. A valle delle attività d'implementazione

	dell'infrastruttura di calcolo della LA3.4, il personale ENEA ha avviato la fase di conduzione degli esperimenti avvalendosi anche della piattaforma di stream analytics sviluppata nella LA3.7. In riferimento alla **LA3.13** "**Validazione ed Integrazione in piattaforma di un toolset di rivelazione attacchi nel contesto delle microreti elettriche**", nel presente semestre, sono state condotte attività di analisi dei requisiti per l'integrazione dei componenti nella piattaforma di analisi degli stream dati misurati. Nell'ambito dello sviluppo della piattaforma si è optato per la definizione e segregazione funzionale di un ambiente di validazione e test caratterizzato dal deployment di circa 100 apparati commerciali di tipo smart meter utilizzati per la misura delle grandezze elettriche relative a sistemi installati nel Centro Ricerche ENEA di Portici. L' acquisizione dati è stata concepita in maniera centralizzata ed il dispositivo di acquisizione sarà considerato come "edge" del sito di validazione. Un sistema di relay è stato disegnato e implementato per l'acquisizione, presso un broker MQTT, dei dati provenienti dagli smart meter. La **LA4.5 "Attività di diffusione II SAL"** ha come obiettivo la divulgazione dei risultati di progetto conseguiti da ENEA e dai relativi co-beneficiari. Nel presente semestre, i ricercatori ENEA e UniPD-QTech hanno preso parte alla manifestazione "Maker Faire Rome", evento europeo dedicato all'innovazione tecnologica, tenutosi a Roma dal 20 al 22 ottobre 2023. In tale contesto, particolare attenzione è stata dedicata ai temi della Ricerca di Sistema cui è stato riservato un apposito spazio espositivo dove i ricercatori hanno condotto esperimenti, in tempo reale, condividendo le proprie conoscenze e competenze con un ampio pubblico. Tale pubblico risultava costituito dagli studenti di istituzioni scolastiche e accademiche italiane, ma anche dal mondo dell'impresa e da innovatori nazionali ed internazionali. In dettaglio, ENEA e UniPD-QTech hanno predisposto il materiale e le attrezzature necessarie all'esecuzione di un esperimento di crittografia quantistica denominato "Quantum Future – combattiamo gli hacker a colpi di quanti!". Avvalendosi di un circuito ottico per l'implementazione di un generatore di numeri casuali e di un apparato per la crittografia, costituito da un trasmettitore (Alice), un ricevitore (Bob) e da un canale quantistico di comunicazione (fibra ottica), è stato possibile mostrare come le particelle di luce (fotoni) possano essere utilizzate per scambiare chiavi crittografiche in maniera sicura tra Alice e Bob. Notevole è risultato l'interesse che l'esperimento ha suscitato non solo negli studenti delle scuole secondarie di secondo grado ed universitari, ma anche negli imprenditori partecipanti alla manifestazione. Nel presente semestre, i ricercatori ENEA hanno anche preso parte alle attività di diversi comitati tecnici e tavoli di confronto confrontandosi con i membri di tali gruppi e condividendo conoscenze e competenze maturate nell'ambito di tale progetto.

UniPD-QTech	Nel periodo di riferimento, UniPD-QTech è stata impegnata nelle attività relative a LA1.7 e LA1.8. Con riferimento alla **LA1.7** "**Definizione e implementazione sperimentale di un protocollo quantistico di autenticazione di un comando a distanza con l'obiettivo di incremento della cyber-sicurezza delle reti energetiche**", nel presente semestre, le attività dei ricercatori UniPD-QTech sono state dedicate all'analisi dei comandi operativi e dei dati scambiati nell'ambito delle reti e microreti di distribuzione dell'energia elettrica al fine di procede con l'identificazione di quelli maggiormente rilevanti da utilizzare nelle fasi successive. Si è proceduto, poi, con la definizione di un processo di autenticazione di alcuni dei comandi operativi identificati, utilizzando lo scambio di chiavi crittografiche mediante tecniche QKD. Tale fase è stata eseguita con particolare attenzione a schemi di rete di tipo punto-punto caratterizzati da una distanza urbana. Per ciò che concerne la **LA1.8** "**Individuazione dei modelli di rete QKD appropriati per servire le necessità più rilevanti per le architetture di sistemi energetici**", nel quarto semestre di progetto, i ricercatori UniPD-QTech hanno concentrato l'attenzione sull'analisi delle diverse topologie delle reti e microreti di distribuzione dell'energia elettrica avviando la definizione di modelli di rete QKD idonei all'integrazione nelle architetture di tipo energetico. Tale fase risulta preliminare all'implementazione di protocolli di sicurezza multiterminale, basati su QKD, da utilizzare per la cifratura e l'autenticazione dei messaggi nelle reti e microreti elettriche.
UNINA-FISICA	Nel periodo di riferimento, UNINA-FISICA è stata impegnata nelle attività relative a LA1.9 e LA1.10. Con riferimento alla **LA1.9 "Progettazione e sviluppo di schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning"**, nel presente semestre, le attività di ricerca sono state dedicate all'analisi della letteratura esistente nel campo della difesa cyber-fisica e degli attacchi di quantum malware assistito da Quantum Machine Learning. Partendo dall'algoritmo di shadow estimation proposto nell'articolo "*Huang, H.-Y., Kueng, R. & Preskill J., Predicting many properties of a quantum system from very few measurements, Nat. Phys. 16, 1050–1057 (2020)*" e successive elaborazioni, i ricercatori UNINA-FISICA hanno proceduto all'integrazione di tale algoritmo con metodi di misurazione di processi di tipo t-doped Clifford. La bontà della tecnica utilizzata è testimoniata dalla maggiore efficienza dell'algoritmo implementato. Nel corrente semestre è stato anche elaborato un articolo sulla tematica "Learning t-doped stabilizer states". Il lavoro, sottomesso alla conferenza Quantum Techniques in Machine Learning, è stato presentato al CERN di Ginevra nel mese di novembre 2023. Le attività di ricerca sono state, poi, concentrate sulla misura di mappe quantistiche. I risultati ottenuti in questo ambito risultano promettenti, giacché una caratterizzazione efficiente di mappe quantistiche, operate da

	un attacker, permette di mitigare l'azione di quantum malware perpetrata ai danni di una rete. Per ciò che concerne la **LA1.10 "Emulazione e test degli schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning,** nel presente semestre, i ricercatori UNINA-FISICA hanno avviato l'applicazione di tecniche di Quantum Criptography a reti elettriche. Particolare attenzione è stata dedicata a sistemi di Quantum Machine Learning operanti su due livelli. Il primo di questi livelli ottimizza i parametri liberi della rete fisica per massimizzare la secure key rate scambiabile tra due nodi della rete. Il secondo livello è dedicato, invece, alla mitigazione degli effetti dovuti al quantum malware. In questo quarto semestre, le attività sono state dedicate, in particolare, al primo livello di un sistema di Quantum Machine Learning. In dettaglio, sono stati, analizzati diversi sistemi di ottimizzazione basati su QML applicati ad implementazioni pratiche di QKD.
ROMA1-DIET	Per ciò che concerne la **LA1.11** "**Implementazione efficiente su logiche programmabili di primitive crittografiche per la sintesi di funzioni di cifratura a flusso e autenticazione**", nel presente semestre, i ricercatori di ROMA1-DIET sono stati impegnati nell'analisi delle peculiarità e delle esigenze di sicurezza informatica delle reti e micro-reti elettriche. Particolare attenzione è stata dedicata anche agli strumenti di analisi della sicurezza della rete ed ai possibili strumenti per aumentarla. Tali fasi sono risultate propedeutiche all'avvio delle attività di selezione dell'algoritmo di cifratura più appropriato a garantire la protezione dei dati, trasmessi sulle reti elettriche di distribuzione, da attacchi sia fisici, sia matematici. Nel corso delle attività del quarto semestre sono stati analizzati anche i modelli simulativi delle reti elettriche che consentono non solo la valutazione dell'impatto degli attacchi fisici e matematici, ma anche dell'efficacia delle contromisure adottate per la sicurezza dei dati trasmessi.
ROMA3-DICITA	Per ciò che concerne la **LA3.9** "**Progettazione e implementazione di un sistema di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori**", nel presente semestre, l'attenzione è stata focalizzata sulle strategie per la memorizzazione e la pre-elaborazione di fonti di dati da analizzare mediante tecniche di ML. In particolare, sono stati approfondite le tecniche a supporto della preparazione dei dati basate su meccanismi per la raccolta della "provenienza" dei dati. Questi meccanismi sono in grado di suggerire spiegazioni dei risultati di un generico processo di data science aumentandone, in questo modo, il livello di trasparenza. A tale riguardo è stata preliminarmente svolta un'indagine sulle pipeline di machine learning disponibili online per identificare le caratteristiche più importanti delle operazioni tipiche svolte sui dati nella fase di pre-elaborazione. Da questa analisi è emerso che le operazioni utilizzate nella pratica possono essere implementate combinando un insieme piuttosto limitato di operatori di base. Questa osservazione ha guidato la definizione di uno strumento automatico per l'acquisizione, in maniera efficiente ed efficace, della

	provenienza dei dati nella fase di preparazione dei processi di machine-learning che verrà utilizzato per il raggiungimento degli obiettivi del progetto. Sulla base delle attività condotte nel quarto semestre, è stato redatto e sottomesso all'International Conference On Data Platform Design, Management, and Optimization (DATAPLAT 2024) che si terrà nel 2024, il seguente articolo: Gregori L., Missier P., Stidolph M., Torlone R, Wood A, Design and Development of a Provenance Capture Platform for Data Science, DATAPLAT 2024.
UNIBA	Per ciò che concerne la **LA3.10** "**Sviluppo ed implementazione di metodi di Machine Learning supervisionati e non supervisionati per lo studio delle anomalie**", nel presente semestre, i ricercatori UNIBA sono stati impegnati nell'analisi delle strategie metodologiche e implementative per l'identificazione delle anomalie che si possono presentare nelle reti elettriche. Tale attività ha riguardato lo studio di procedure di malware detection basate su differenti algoritmi di ML e di un sistema di detezione delle anomalie specifico per smart grid. Particolare attenzione è stata riservata all'analisi delle potenzialità legate all'applicazione, nell'ambito di riferimento, di reti neutrali di tipo Deep Convolutional Neural Network (DCNN) e di un sistema di rilevamento delle intrusioni basato su multi-convolutional neural network fusion. L'analisi condotta getta le basi per il prosieguo delle attività progettuali previste da capitolato.
DIG-UNISANNIO	Per ciò che concerne la **LA3.12 "Sviluppo e confronto prestazionale di algoritmi di rilevamento stocastico di cyber-attacchi nel contesto delle microreti elettriche"**, nel presente semestre, i ricercatori DIG-UNISANNIO si sono interfacciati con i colleghi ENEA per l'avvio delle attività relative alla selezione degli algoritmi ML da destinare alla detezione anomalie/attacchi di tipo FDI nello scenario microgrid. Nel quarto semestre l'attenzione è stata concentrata anche sull'analisi dei dataset di confronto e di quello di scenario (SmartMeter CR ENEA Portici). È stata, poi, avviata la fase di selezione dell'ambiente operativo e dei framework ML da utilizzare per lo sviluppo e per i successivi test. I ricercatori si sono dedicati, infine, allo sviluppo del set di algoritmi base, destinato a fornire il livello prestazionale di confronto, e all'implementazione di algoritmi avanzati per il prosieguo della fase implementativa.