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. 2 – Periodo attività: 01/07/2022 – 31/12/2022

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto "Cybersecurity dei sistemi energetici" svolte durante il secondo semestre di progetto dall'affidatario ENEA. Le attività dei co-beneficiari sono, infatti, programmate, da Gantt di progetto, a partire dal quarto semestre.

ATTIVITA' SVOLTE

AFFIDATARIO / COBENEFICIARIO	*SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO*
ENEA	Nel presente semestre, come da Gantt di progetto, ENEA ha condotto attività di ricerca nell'ambito delle seguenti linee di attività: LA1.2, LA2.2, LA3.2, LA3.3; LA3.11; LA4.2. Con riferimento alla linea **LA1.2 "Definizione delle soluzioni topologiche, progettazione e realizzazione di un'infrastruttura di test per la validazione di protocolli ed apparati sviluppati per la cybersicurezza di reti e microreti elettriche"**, nel presente semestre, si è proceduto alla progettazione delle specifiche tecniche del sistema di crittografia quantistica da acquisire per le attività previste dal progetto. Più nello specifico, al fine di condurre le attività sperimentali previste dal progetto, come indicato nel capitolato di progetto, si rende necessario dotare il laboratorio di un sistema integrato che includa apparati cifranti di rete e sistemi di trasmissione con tecnologia Quantum Key Distribution (QKD) per la comunicazione su canale quantistico in fibra ottica. Nel presente semestre, a valle dello studio dei sistemi disponibili in commercio, sono stati definiti i requisiti del sistema da acquisire e, in particolare, le specifiche tecniche richieste per: gli apparati di trasmissione e ricezione di tipo bidirezionale (Alice e Bob) basati su canali di comunicazione classico e quantistico; i sistemi cifranti; la componentistica di interconnessione necessaria al funzionamento dell'infrastruttura (es. cavi ethernet, patch in fibra, switch, time tagger, SPAD, rack contenitori degli apparati forniti, ecc.); la piattaforma, modulare, scalabile e flessibile,

	dotata di interfaccia grafica per il monitoraggio e la gestione dei parametri operativi di tutti gli apparati del sistema. A valle della definizione, si è, quindi, proceduto a predisporre la relativa documentazione tecnica di gara da eseguire nei successivi semestri. Per ciò che concerne la **LA2.2** "**Studio di schemi di protezione 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, si è proceduto a definire i layer di un dispositivo di protezione elettrica e cibernetica per sistemi ed impianti collegati a micro-reti elettriche in zone in cui risulta disponibile il mezzo trasmissivo in fibra ottica. A partire dallo schema architetturale del dispositivo definito nel semestre precedente è stata proposto un apparato di tipo multilayer caratterizzato da uno strato dedicato allo stadio di potenza del sistema di protezione, uno strato per l'alimentazione del sistema elettronico e per la circuiteria di condizionamento e misura, un layer dedicato al sistema di controllo, uno al sistema di comunicazione e crittografia quantistica di dati e comandi e, infine, uno strato di set, segnalazione e visualizzazione delle principali grandezze operative. Si tratta di un dispositivo che si avvale di componenti allo stato solido realizzati anche mediante materiali di tipo Wide Band Gap per la realizzazione dello stadio di potenza. Per il secondo ed il terzo layer dell'apparato sono stati identificati il microcontrollore ed i circuiti ausiliari e di alimentazione. È stato, poi, necessario definire i componenti e sistemi per lo sviluppo dello stadio di comunicazione in maniera tale che le chiavi crittografiche siano scambiate mediante sequenze di fotoni opportunamente polarizzati e trasmessi sul canale quantistico in fibra ottica (tecniche di Quantum Key Distribution). In riferimento all'ultimo layer dell'apparato, sono stati identificati pulsanti, LED e display necessari per la visualizzazione delle condizioni operative del dispositivo di protezione e per la segnalazione di allarmi. La descrizione dettagliata dei diversi strati dell'apparato di protezione sarà riportata nel Rapporto tecnico finale della LA, redatto nel III semestre. Con riferimento alla **LA3.2** "**Definizione dei requisiti di una infrastruttura di calcolo a basso consumo per il controllo informatico di reti elettriche intelligenti cyber-resilienti**", nel presente semestre sono stati analizzati i requisiti che la infrastruttura di calcolo dovrà possedere. In particolare, sono stati presi in considerazione: • I nodi di calcolo che saranno costituiti sia da server di ultima generazione, dotati di processori multi-core di fascia alta per garantire rapidità di risposta ai vari eventi che si presenteranno, che da dispositivi acceleratori basati su schede FPGA che, per la loro flessibilità architetturale, consentono di ottenere elevate velocità di calcolo sia grazie alla banda di memoria interna estremamente elevate che permette di evitare il collo di bottiglia indicato con il termine "memory wall" che alla possibilità di definire in maniera dinamica architetture di calcolo parallelo che rispecchiano la struttura dell'algoritmo che si deve implementare (sia esso un algoritmo di cifratura o un'implementazione di una rete neurale);

	• Le necessità di storage connesse alla implementazione di un data base che contenga i dati di traffico raccolti nel normale funzionamento della rete dati (si fa riferimento alla rete dati del Centro Ricerche ENEA Casaccia); tali dati saranno usati per il training di reti neurali finalizzate al riconoscimento di attacchi e, più in generale, di situazioni anomale potenzialmente pericolose; • I requisiti di sicurezza che la rete dovrà fornire rispetto i potenziali tentativi di intrusione di tipo malevolo. A valle di tale analisi è stata definita la struttura che dovrà possedere l'architettura di calcolo a basso consumo per il controllo informatico di reti elettriche intelligenti cyber-resilienti. Tale architettura sarà descritta in dettaglio nel Rapporto tecnico di sintesi della LA nel terzo semestre. Con riferimento alla **LA3.3** "**Studio e definizione di componenti per l'analisi dei flussi di informazioni relativi alla cybersecurity e predisposizione di sistemi di continuous intelligence/stream analytics**", nel presente semestre, le attività sono state focalizzate sull'individuazione della soluzione tecnologica in grado di supportare il training nei sistemi di continuous intelligence. In particolare, si è strutturata una piattaforma basata su una appliance appositamente formulata per i workflow di intelligenza artificiale, in grado di gestire il training e il deployment degli algoritmi di machine learning che devono essere integrati nella piattaforma di stream analytics. La piattaforma consente di rendere disponibili in modalità virtualizzata unità di elaborazione eterogenee per l'analisi dei dati e per il training dei modelli, in architetture ad alto parallelismo capaci di supportare il calcolo matriciale. L'approccio implementato permette di ottenere risultati significativi, con l'acquisto di hardware GPU specifico, il quale è stato integrato in una appliance formulata per la sua gestione in maniera intelligente ed efficace. il risultato finale è quello di potenziare le capacità di analisi e di risposta nel campo della cybersecurity delle reti elettriche. La nuova piattaforma di stream analytics sarà focalizzata sulla rilevazione e la prevenzione delle minacce informatiche in tempo reale, garantendo una protezione avanzata e proattiva per le infrastrutture critiche del settore energetico. Con riferimento alla **LA3.11 "Studio di modelli di Machine Learning per la detezione di cyber-attacchi in sistemi energetici attraverso l'analisi statistica del dato misurato su nodi cyber-fisici"**, nel presente semestre, si è proceduto ad identificare e studiare i tipi di attacchi riportati come più frequenti o pericolosi in base alle analisi di rischio effettuate in letteratura. Si è studiata l'applicabilità delle proposte algoritmiche in termini di implementazione fog/edge. Non si sono riscontrate particolari criticità da questo punto di vista in quanto lo spettro di strumenti individuato copre agevolmente il range di carico computazionale di differenti dispositivi riscontrabili nelle architetture a microgriglia. Con riferimento alla **LA4.2 "Attività di diffusione I SAL",** nel presente semestre, si è avviata la redazione di un articolo scientifico di divulgazione da sottomettere nel terzo semestre di progetto (deadline della conferenza)

	alla conferenza internazionale ICCEP 2023 (International Conference on Clean Electrical Power 2023).