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. 3 – Periodo attività: 01/01/2023 – 30/06/2023

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto "Cybersecurity dei sistemi energetici" svolte durante il terzo 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	Nell'ambito del presente semestre, 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"**, nell'ambito del presente semestre si è proceduto alla progettazione del testbed ENEA per le attività sperimentali del progetto. Il testbed sperimentale è stato definito in ottica di predisporre un ambiente di test che risponda alle esigenze di progetto in ottica di ampia configurabilità e di possibilità di integrazione con gli apparati preesistenti della nanogrid del Centro Ricerche ENEA di Portici. In particolare, l'infrastruttura definita dovrà consentire la validazione sperimentale delle tecnologie, delle topologie di rete precedentemente individuate e degli apparati di protezione del progetto. L'infrastruttura sperimentale sarà costituita da diversi apparati elettronici già presenti nella nanogrid di laboratorio (sistemi di emulazione di generazione, carico e accumulo; sistemi di misura; 1 simulatore di rete; 1 software di gestione dell'architettura sperimentale) e il sistema QKD da acquisire (sezione precedente). Successivamente alla definizione del testbed, si è proceduto ad elaborare due scenari di test che saranno applicati per l'esecuzione delle prove sperimentali previste dal II SAL. Nello

	specifico, uno scenario è stato definito per valutare l'impatto di un cyber attacco sul funzionamento dell'infrastruttura elettrica, l'altro per analizzare l'impatto di un cyber attacco sul funzionamento a livello di apparato e le relative conseguenze sul funzionamento dell'infrastruttura elettrica. L'attacco B, in particolare, sarà orientato ad emulare un cyberattacco che compromette la riservatezza dei dati. Nel semestre, si è, quindi, proceduto alla redazione del Rapporto Tecnico riepilogativo dei risultati della LA1.2: "Analisi di soluzioni topologiche e predisposizione di un'infrastruttura di test per la validazione di protocolli ed apparati sviluppati per la cybersicurezza" (RdS_PTR 22-24_PR 2.1_LA1.2_066). 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 alla definizione di un apparato di protezione elettrica e cibernetica per sistemi ed impianti collegati a micro-reti elettriche in zone in cui non è disponibile il mezzo trasmissivo in fibra ottica. Sulla base dello schema architetturale proposto nel primo semestre delle attività di ricerca, sono stati definiti i diversi layer di tale apparato. Particolare attenzione è stata dedicata alla definizione del layer di comunicazione. In assenza del mezzo trasmissivo in fibra ottica, è stato necessario analizzare soluzioni in grado di sfruttare cammini liberi in aria per la ricezione e trasmissione di dati e comandi avvalendosi di tecniche Quantum Free Space. È stato, a tal fine, proposto l'impiego di telescopi o di ricetrasmettitori innovativi. In accordo al cronoprogramma di progetto, nel presente semestre, si sono concluse le attività della LA2.2. I risultati conseguiti risultano in linea con gli output di progetto. Nel semestre, si è, quindi, proceduto alla redazione del Rapporto Tecnico riepilogativo dei risultati della LA2.2: "Studio e valutazione 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" (RdS_PTR 22-24_PR 2.1_LA2.2_067). 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 state concretizzate le attività preparatorie svolte nel primo anno del progetto e si è portata a termine la configurazione della architettura della infrastruttura di calcolo a basso consumo per il controllo informatico di reti elettriche intelligenti cyber-resilienti. Sulla base delle analisi fatte precedentemente, sono stati selezionati i dispositivi che dovranno costituire la infrastruttura di calcolo. In particolare, • Sono stati individuati gli acceleratori basati su schede FPGA AMD U280, scelte per la loro elevata banda di memoria (dispongono sia di 2 banchi di memoria DDR che due banchi di memoria HBM (High Bandwidth Memory) e per l'elevato numero di risorse hardware messe a disposizione (DSP, moduli di memoria BRAM, Look-Up Tables);

	• Sono stati selezionati un server di calcolo e uno storage server, entrambi prodotti da SuperMicro, in grado di offrire le prestazioni richieste, in termini di spazio di memorizzazione, sicurezza dei dati memorizzati, velocità di accesso allo storage, capacità di calcolo; • È stato scelto un Firewall di ultima generazione in grado di fornire i richiesti requisiti di sicurezza, adottando algoritmi di intelligenza artificiale per riconoscere potenziali attacchi alla rete dati; • Sono stati selezionati ed acquisiti alcuni sensori/attuatori per introdurre nella rete del centro ENEA Casaccia dei dispositivi IoT che possano essere inseriti nella VLAN che sarà definita per ospitare i sensori ed i server di storage e di elaborazione; • È stata individuato lo stack SW necessario a gestire l'infrastruttura di calcolo a basso consumo. Come risultato delle suddette attività si è prodotta l'architettura di dettaglio della infrastruttura di calcolo a basso consumo per il controllo informatico di reti elettriche intelligenti cyber-resilienti. Tale architettura è descritta in dettaglio nel Rapporto tecnico di sintesi della LA: "Definizione dei requisiti di una infrastruttura di calcolo HPC a basso consumo per il controllo informatico di reti intelligenti cyber-resilienti" (RdS_PTR 22-24_PR 2.1_LA3.2_068). 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 si è lavorato alla definizione della piattaforma di stream processing. Una piattaforma di stream processing è un sistema informatico progettato per elaborare e analizzare dati in tempo reale, mentre vengono generati. Questi dati possono provenire da una vasta gamma di fonti, come sensori IoT e log di firewall, in questo caso strettamente connessi alle reti elettriche. L'obiettivo principale di una piattaforma di stream processing è consentire alle organizzazioni di trarre informazioni significative e agire rapidamente sui dati mentre sono ancora rilevanti. La piattaforma di stream processing riceve costantemente flussi di dati in ingresso, li processa istantaneamente e fornisce risposte in tempo reale. Questo processo può includere il filtraggio, l'aggregazione, l'arricchimento e l'analisi dei dati. Gli eventi rilevanti possono essere identificati e analizzati immediatamente, consentendo alle organizzazioni di prendere decisioni tempestive e informate. Le piattaforme di stream processing sono caratterizzate da una serie di componenti chiave, tra cui: 1. Ingestion Layer: Questo componente è responsabile della ricezione e dell'acquisizione dei dati provenienti dalle diverse fonti. Può includere connettori specifici per la sorgente dati 2. Processing Engine: È il motore centrale della piattaforma, responsabile dell'elaborazione dei dati in tempo reale. Utilizza principalmente algoritmi di intelligenza artificiale per analizzare i dati, applicare trasformazioni e generare risultati. 3. Storage: In alcune piattaforme, i dati possono essere temporaneamente memorizzati per consentire analisi ulteriori o per scopi di archiviazione. Tuttavia, nelle applicazioni di stream processing, il focus principale è sulla velocità e sull'analisi in tempo

	quasi reale, quindi lo storage deve essere ottimizzato per l'efficienza. 4. Output/Action Layer: Una volta elaborati, i risultati dell'analisi possono essere inviati a destinazioni specifiche come dashboard di monitoraggio in tempo reale, sistemi di notifica, sistemi decisionali o possono attivare azioni automatiche come avvisi, correzioni di processo o aggiornamenti di database. I risultati dell'analisi sono riassunti nel Rapporto Tecnico di sintesi della 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" che illustra le caratteristiche della piattaforma di stream processing/continuous intelligence da realizzare nell'ambito della cybersecurity delle reti elettriche (RdS_PTR 22-24_PR 2.1_LA3.3_069). 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, sono state analizzate le basi di dati utilizzate in letteratura e, in particolare, la metodologia di raccolta degli stessi. Nello specifico, sono stati esaminati dataset simulati, ottenuti da sistemi di simulazione in tempo reale anche di tipo Hardware In Loop (HIL), e dataset ottenuti utilizzando, almeno in parte, misure in campo su sottosistemi rilevanti di microgriglia reali. Infine, sono state identificate le architetture tipiche di microgriglia tipicamente utilizzate in questi studi e, in particolare, in quelli in cui si simulavano queste architetture in tempo reale. Nel semestre, si è proceduto alla redazione del Rapporto Tecnico riepilogativo dei risultati della LA3.11: "Studio di modelli di ML per la detezione di cyber-attacchi in sistemi energetici attraverso l'analisi statistica del dato misurato su nodi cyber-fisici" (RdS_PTR 22-24_PR 2.1_LA3.11_070) e al rilascio del "Datalake per sviluppo e test di algoritmi di anomaly detection nel contesto delle cybersecurity nelle reti elettriche" (RdS_PTR 22-24_PR 2.1_LA3.11_091). Con riferimento alla **LA4.2 "Attività di diffusione I SAL",** nel presente semestre, si è organizzata, insieme al co-beneficiario UniPD-QTech, la partecipazione alla Fiera Maker Faire 2023 e, in particolare, è stata predisposta la scheda di presentazione dell'esperimento da mostrare ed è stata avviata l'organizzazione della partecipazione prevista ad ottobre 2023 nello stand della Ricerca di Sistema. Nel semestre, si è, quindi, proceduto alla redazione del Rapporto Tecnico riepilogativo dei risultati della LA4.2: "Attività di diffusione I SAL" (RdS_PTR 22-24_PR 2.1_LA4.2_070).