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. 1 – Periodo attività: 01/01/2022 – 30/06/2022

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto "Cybersecurity dei sistemi energetici" svolte durante il primo 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, è stato condotto uno studio della letteratura tecnico-scientifica finalizzato ad individuare i possibili elementi di vulnerabilità per le reti in funzione dei diversi tipi di attacco e, successivamente, è stata condotta un'analisi degli impatti sulle più comuni topologie delle reti elettriche di distribuzione. I risultati dello studio hanno consentito di identificare le topologie di interesse per la sperimentazione da condurre nelle LA1.6 e LA2.7. Più nello specifico, nella prima fase di analisi sono stati analizzati, per i principali attacchi ai sistemi elettrici, il componente "sotto attacco", la funzionalità compromessa e la possibile azione di mitigazione. Successivamente, per quattro topologie di rete (topologia radiale, topologia ad anello, topologia a maglie, topologia a linee parallele) sono state indagate le principali caratteristiche e la resilienza intrinseca ai cyber attacchi.

	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 primo semestre delle attività, si è proceduto ad analizzare la normativa ed i documenti tecnici di settore relativi ai sistemi di protezione da adottare nelle reti italiane di distribuzione dell'energia elettrica. Identificate le tipologie di apparati di protezione necessari (protezioni di massima corrente, di minima e massima tensione, ecc.), l'attenzione è stata focalizzata sulle tecnologie utilizzate, sulla presenza di eventuali interfacce di comunicazione, sulle soglie e tempistiche d'intervento degli apparati disponibili in commercio (elettromeccanici, intelligenti e virtuali). I ricercatori ENEA hanno, poi, analizzato le diverse tecniche di selettività (amperometrica, cronometrica, ecc.) utilizzate nelle reti di distribuzione al fine di attivare meccanismi di coordinamento degli interventi dei diversi dispositivi di protezione. Questo studio preliminare ha consentito di comprendere punti di forza e di debolezza delle soluzioni esistenti. Tale attività ha gettato le basi per la definizione dello schema architetturale di un dispositivo per proteggere sistemi ed apparati da criticità di natura elettrica (sovracorrenti, sovratensioni) e per mitigare degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche. È stato, infine, proposto uno schema architetturale di tipo multilayer e sono state identificate le funzionalità e le caratteristiche dei diversi layer che lo costituiscono. 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: • È stato condotto lo studio della tipologia di attacchi al layer informatico e di scambio dati delle reti elettriche e alle tipologie di approccio che possono essere seguite per mitigare il rischio derivante da tali attacchi. Sono, inoltre, state analizzate le procedure di cifratura che possono venire usate per aumentare la robustezza delle reti elettriche. • È stato avviato un confronto con i partner accademici, coinvolti nel progetto a partire dal quarto semestre, le cui attività sono logicamente connesse alla LA3.2 (Università di Roma1, Università Roma3, Università di Bari) per recepire le esigenze, dal punto di vista del calcolo e della comunicazione, che potranno scaturire dalle attività che li vedranno coinvolti. Le attività condotte hanno consentito di individuare le classi di algoritmi, di cifratura e di machine learning, che dovranno essere implementate nella infrastruttura di calcolo da definire nell'ambito del progetto. 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 proceduto a esaminare approfonditamente i requisiti di sicurezza informatica e a identificare le lacune che si possono identificare nei sistemi attuali. Inoltre, sono state condotte delle prime analisi dei flussi di informazioni volte ad individuare potenziali minacce e vulnerabilità nel contesto della cybersecurity. Sono stati avviati degli studi

	sui protocolli e metodologie per la raccolta continua, l'analisi e monitoraggio dei dati, al fine di garantire una risposta tempestiva ed efficace agli eventi di sicurezza. Parallelamente, sono state valutate soluzioni avanzate di continuous intelligence e stream analytics per migliorare la capacità di rilevamento e mitigazione delle minacce informatiche in tempo reale quasi reale. Questo studio preliminare ha consentito di comprendere punti di forza e di debolezza delle soluzioni esistenti e di porre le basi per la scelta delle tipologie di infrastrutture che dovranno essere implementate nella piattaforma di stream analytics e continuous intelligence. 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, è stato condotto uno studio selettivo di algoritmi di anomaly detection su nodi cyber fisici di architetture a microgriglia. Gli algoritmi, le tecnologie e le architetture proposti dalla letteratura, sono stati analizzati in chiave critica ponendo in risalto le proposte più recenti basate fondamentalmente su tecniche statistiche e machine learning. Con riferimento alla **LA4.2** "**Attività di diffusione del I SAL"**, nel presente semestre, si è proceduto a identificare riviste di interesse scientifico e divulgativo, di rilevanza nazionale e internazionale per la successiva disseminazione dei risultati del progetto.