PIANO TRIENNALE DI REALIZZAZIONE 2019-21 - RICERCA DI SISTEMA ELETTRICO NAZIONALE
Progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

AFFIDATARIO 1

Tema 2.3 – Applicazione al sistema elettrico, come atteso in evoluzione (tema 2.2) e anche per migliorare sicurezza e resilienza, di tecnologie dell'informazione, internet delle cose, peer to peer

Durata: 36 mesi

Semestre n. 4 – Periodo attività: 01/07/2020 – 31/12/2020

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento riporta, in forma sintetica, i risultati ottenuti nel corso del secondo semestre 2020 dal progetto di Ricerca di Sistema per il Tema 2.3. Nel semestre sono state completate le attività delle 12 linee avviate ad inizio anno con la realizzazione di strumenti software e piattaforme dimostrative di tecnologie ICT. Sono stati prodotti 14 rapporti tecnici di cui 2 per le attività di diffusione e di supporto alla normativa e alla regolazione. Sono stati sviluppati alcuni collegamenti con altri progetti RdS maggiormente focalizzati sul sistema elettro-energetico e con i progetti europei correlati, svolgendo alcune attività in sinergia. Alle collaborazioni in essere con soggetti industriali è stato aggiunto un accordo di collaborazione con un DSO e con un costruttore di dispositivi utente in grado di ricevere direttamente i dati dei contatori di seconda generazione. Grazie a tali accordi si è potuto avere accesso ad informazioni e dati utili per la ricerca, relativi alle reti elettriche esistenti e al comportamento energetico reale di utenze residenziali. Le collaborazioni stabiliscono inoltre un'interazione diretta con gli operatori del settore che consente una efficace diffusione dei risultati del progetto.

ATTIVITA' SVOLTE	
AFFIDATARIO / COBENEFICIARIO	***SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE, RISULTATI CONSEGUITI E RICADUTE SUL SETTORE PRODUTTIVO***
RSE	Le attività svolte nel secondo semestre hanno portato al raggiungimento degli obiettivi delle Linee di Attività 2020. In particolare: Per le architetture emergenti di Fog/Edge/Cloud computing è stata completata la realizzazione della piattaforma sperimentale dimostrativa di base con l'installazione e la configurazione di ulteriori dispositivi di rete e comunicazione e nodi edge. Sono stati predisposti gli applicativi per il test dei casi d'uso di Controllo di Microreti e di monitoraggio della rete mediante PMU ed un sistema per la collezione dei dati di funzionamento dei componenti della piattaforma durante i test. In vista della sperimentazione sono stati anche valutati strumenti open source per l'orchestrazione di fog computing e per il controllo di reti di comunicazione configurate via software. • Sul tema dei modelli semantici si è conclusa l'integrazione nella piattaforma Smart Grid Semantic Platform (SGSP) di funzioni provenienti dagli applicativi di ricerca SARA e MAPS sviluppando microservizi utili allo scopo. Per ottenere il Digital Twin di una rete elettrica a partire dalla sua descrizione standard si è operata la trasformazione dell'architettura della SGSP in una versione basata sui container. Per le applicazioni al

	settore multi-energy sono state studiate le modalità applicabili per integrare fra loro differenti ontologie e si è realizzato un primo modello per la gestione del profilo geografico di una rete di teleriscaldamento. In relazione al progetto EU PlatOne è stato sviluppato un processo di trasformazione dal formato Digsilent al formato IEC CIM per reti di media tensione. • In ambito ICT per gli utenti finali è stata completata la prima versione di un emulatore di utenze residenziali in grado di riprodurre il comportamento e gli scambi informativi verso un gestore comune di un numero configurabile di utenti. In relazione con il progetto EU Interconnect, sono stati individuati i dati di interesse del laboratorio RSE PREVO che è possibile descrivere tramite l'ontologia SAREF. Per le tecnologie blockchain è stata realizzata una piattaforma dimostrativa per la tracciatura certificata delle emissioni prodotte da impianti termici di produzione elettrica. • Per le tecnologie Low Power WAN è stata realizzata un'architettura LoRaWAN che gestisce sensori di monitoraggio delle linee elettriche aeree installati in campo e sensori per cavi interrati. L'architettura comprende un sistema di visualizzazione e archiviazione delle misure raccolte ed integra anche sensori in tecnologia NB-IoT. • Relativamente alle tecniche di Intelligenza Artificiale e Big Data è stato effettuato uno studio e una valutazione di tecniche di clustering di serie temporali. In ambiente Big Data, sono state utilizzate soluzioni basate sui grafi per sviluppare e verificare algoritmi per il calcolo del power flow e, in collaborazione con il Politecnico di Milano, per applicare alle reti elettriche tecniche di analisi dei grafi, esaminando alcune reti reali. Si è realizzata un'architettura big data streaming di test applicata al calcolo della probabilità di occupazione di colonnine di ricarica di auto elettriche. Per i dati diagnostici provenienti dal sistema di monitoraggio LANPRIS si è sviluppato un algoritmo di elaborazione Deep Learning di immagini/video in grado di riconoscere eventi di scarica elettrica sugli isolatori. Per l'elaborazione dei dati di power quality è stata completata la realizzazione di un sistema automatico per l'estrazione di eventi dal data base del sistema di monitoraggio di Power Quality QuEEN. L'applicativo ha permesso una verifica intensiva delle prestazioni del classificatore di buchi di tensione DELFI su un numero elevato di forme d'onda. In sinergia col progetto 2.2 sono stati effettuati confronti con le prestazioni della funzione di validazione dei buchi di tensione implementata in QuEEN. L'applicativo sviluppato integra altre analisi automatiche di Power Quality, quali la classificazione dei buchi di tensione secondo la norma CEI EN 50160, il calcolo di indici sintetici e la classificazione in Cluster. • Per il test di tecnologie di protezione cibernetica sono state completate le funzionalità di gestione dei set point dei moduli client e server della piattaforma, sono state sviluppate le funzionalità per la gestione concorrente di molteplici DER da parte del connections-manager e sono state implementate le prime funzionalità di logging di eventi rilevanti per la sicurezza. La piattaforma di test è stata integrata nell'architettura di telecontrollo del laboratorio PCS-ResTest di RSE. In relazione con il progetto europeo OSMOSE è stata sviluppata una versione semplificata di ambiente di test IEC 62351 per comunicazioni IEC 60870-5-104 utilizzato per calcolare un primo set di KPI. • Per il riconoscimento di anomalie in infrastrutture ICT di comunicazione e controllo del settore energetico si è sviluppato un modello grafico probabilistico basato su reti bayesiane per l'analisi di possibili percorsi di attacco, per la valutazione delle probabilità di attacco e delle soluzioni che ottimizzano l'efficacia di protezione e per la pianificazione di misure di sicurezza, anche considerando la dimensione temporale. Si sono sviluppate analisi preliminari di tecniche di anomaly detection attraverso l'uso di differenti algoritmi di machine learning e deep learning, • Sul tema della resilienza dei sistemi cyber-power è proseguita la valutazione dei requisiti di cybersecurity del dimostratore Terna del progetto OSMOSE e la generazione di test di sicurezza per la prima versione dell'architettura ICT del demo. Il laboratorio PCS-ResTest è stato dotato di funzionalità di monitoring e logging della sicurezza delle comunicazioni per il telecontrollo DER, di generazione di processi di attacco e di anomaly detection. In collaborazione con il progetto 2.5, è stato sviluppato con securiCAD un modello probabilistico per l'analisi di processi di attacco al sistema

	automatico di distacco carichi della rete di trasmissione. Il modello è stato utilizzato per simulare alcuni scenari di attacco e calcolare la distribuzione di probabilità dell'evento *substation_trip_failure,* utilizzata nel progetto 2.5 come input allo strumento RELIEF per calcolare indici di resilienza ad attacchi cyber. • Riguardo alla sicurezza delle architetture emergenti Cloud/Fog e IoT si è estesa con nuovi moduli ed agenti la piattaforma sperimentale di monitoraggio dello stato dell'infrastruttura ICT. Si è sviluppata nella piattaforma una prima versione degli strumenti di emulazione dei processi di attacco e delle funzionalità per l'individuazione delle anomalie cyber. • Per il supporto alla normativa si è contribuito principalmente alle attività CEI e IEC del CT 57 "Scambio informativo associato alla gestione dei sistemi elettrici di potenza" e alle TF del CEI CT316 per gli aspetti di sicurezza del Controllore Centrale Impianto e del Controllore Infrastruttura Ricarica dei veicoli elettrici. A supporto di ARERA, a completamento del lavoro svolto nel 2019 riguardante le architetture ICT per l'osservabilità del sistema elettrico, si è contribuito ad una valutazione dei costi richiesti per l'adeguamento degli impianti esistenti degli utenti di rete significativi. Si è inoltre fornito un contributo significativo alle attività CIGRE SC D2.
FUB	Le attività svolte nel secondo semestre hanno portato al raggiungimento degli obiettivi delle Linee di Attività 2020. In particolare: • Per le reti 5G, si sono effettuate valutazioni tramite approcci sia simulativo che emulativo considerando casi d'uso tipici per applicazioni energetiche. Le valutazioni di copertura radio per comunicazioni 5G al di sotto di 6 GHz si sono concentrate soprattutto per le comunicazioni eMBB, per servizi che richiedono elevate capacità in termini di velocità trasmissiva, e comunicazioni mMTC, per servizi che richiedono una copertura estesa. Le analisi hanno riguardato contesti applicativi con dispositivi collocati in linea di vista (LOS) e non (NLOS). In quest'ultimo caso sono stati introdotte nelle simulazioni anche caratteristiche orografiche del territorio per fornire una stima più realistica delle prestazioni. Sono state affrontate anche analisi di prestazioni per comunicazioni 5G sopra i 6 GHz considerando il caso uRLLC, per applicazioni che richiedono stringenti requisiti di latenza. Infine, le valutazioni con l'emulatore di rete Mininet delle prestazioni di una rete SDN orientata alla gestione di traffico dati IoT, sono state estese a soluzioni di "Fog Computing" per verificarne l'applicabilità per rispondere ai requisiti prestazionali (QoS) di servizi per il settore energetico. • Relativamente ai motori di ricerca IoT è stata svolta un'attività sperimentale per incrociare dati energetici e dati di altro tipo, limitatamente ad alcune banche dati pubblicate in formato aperto ed utilizzando la piattaforma di *Data Analytics* proprietaria predisposta in ambiente Spark. In particolare è stato utilizzato il TIM Big Data Challenge, focalizzato su dati di consumi elettrici e altri dati temporali e georeferenziati associati, quali il traffico della rete mobile di telecomunicazione e di *internet* riscontrando una moderata correlazione tra consumi elettrici e consumi di telefonia mobile e di internet. Si è inoltre avviata un'attività che riguarda gli strumenti per il censimento e l'analisi dei dispositivi accessibili connessi a Internet. In particolare, è stata valutata l'utilizzazione di Shodan come motore di ricerca *IoT* primario, per ottenere dati grezzi sui quali basare analisi più approfondite, ed è stata predisposta una piattaforma *Big Data* per l'acquisizione, l'indicizzazione e l'analisi dei dati così ottenuti. Utilizzando tali strumenti, sono stati condotti alcuni test focalizzandosi sui dispositivi di tipo *ICS (Industrial Control Systems)* che, nella grande varietà dei dispositivi censiti, sembrano al momento fra quelli più interessanti per il settore energetico. • Per gli aspetti di sicurezza dei sistemi 5G è stata eseguita una prima analisi delle problematiche di sicurezza connesse ai concetti di Network Function Virtualization (NFV) e Network Slicing; è stata completata l'analisi della metodologia 3GPP SECAM e del corrispondente schema implementativo GSMA NESAS per la valutazione di sicurezza dei prodotti di rete, coprendo anche gli aggiornamenti (in fase di sostanziale sviluppo lato 3GPP) per i prodotti di rete non virtualizzati; per le specifiche 3GPP è stata inoltre aggiornata l'analisi della letteratura specialistica dedicata alle vulnerabilità. • Per la certificazione di sicurezza dei sistemi SCADA è stata aggiornata l'analisi della

	normativa di riferimento (D.L. 105/2019 – Perimetro di sicurezza nazionale cibernetica e norme successive norme) ed approfondita ed estesa l'analisi delle vulnerabilità tipiche dei sistemi SCADA. Dall'esame delle metodologie di analisi dei rischi utilizzate o proposte per sistemi SCADA si è arrivati a definire, in versione preliminare, una metodologia adeguata per l'acquisizione di (componenti di) questi sistemi nel rispetto dei vincoli previsti nel Perimetro di sicurezza nazionale cibernetica. • Per l'applicazione di tecnologie blockchain alla gestione di chiavi di sicurezza nel contesto IoT è stata estesa l'esplorazione della letteratura specialistica riguardante sia soluzioni classiche per l'autenticazione di chiavi pubbliche, quali l'uso di certificati digitali e PKI (Public Key Infrastructure), sia l'autenticazione mediante Blockchain delle chiavi pubbliche di dispositivi. Sono state esaminate in dettaglio alcune delle soluzioni proposte per l'autenticazione di dispositivi basate su sistemi Blockchain e sono stati definiti alcuni criteri per la valutazione preliminare delle soluzioni considerate.