PIANO TRIENNALE DI REALIZZAZIONE 2022-2024 DELLA RICERCA DI SISTEMA ELETTRICO NAZIONALE

Presentazione dei progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

Tema di ricerca 2.1

Titolo del progetto

Progetto Integrato Cyber Security dei sistemi energetici

- Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile [ENEA]
- Consiglio Nazionale delle Ricerche [CNR]
- Ricerca sul Sistema Energetico [RSE]
- Dipartimento di Fisica ``Ettore Pancini'', Università degli Studi di Napoli Federico II [UNINA-FISICA]
- Dipartimento di Ingegneria - Università degli Studi del Sannio [DIG-UNISANNIO]
- Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche dell'Università Roma Tre [ROMA3-DICITA]
- Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni dell'Università La Sapienza [ROMA1-DIET]
- Padua Quantum Technologies Research Center [UniPD-QTech]
- Scuola IMT Alti Studi Lucca [Scuola IMT]
- Università degli Studi di Bari Aldo Moro [UNIBA]
- Università degli Studi di Firenze [UNIFI]
- Università degli Studi di Messina [UNIME]
- Università degli Studi di Palermo – Dipartimento di Ingegneria [UNIPA - DI]

Durata del progetto: 36 mesi

Costo proposto: 7.799.494,52 €

FASE: Trasmissione PTR rimodulato (ver. 0)

2. DATI GENERALI DEL PROGETTO

2.1 Dati progetto

Titolo del progetto
Progetto Integrato Cyber Security dei sistemi energetici
Durata del progetto
36 mesi

2.2 Descrizione progetto

Abstract del progetto

Il raggiungimento degli obiettivi energetici al 2030 stabiliti dal PNIEC (Piano Nazionale Integrato per l'Energia e il Clima) impone una trasformazione digitale del settore, che consenta la realizzazione di smart grid in grado di rispettare requisiti tecnici ed economici soddisfacendo con fonti rinnovabili la domanda energetica di una varietà di carichi, come impianti industriali, edifici commerciali e residenziali, smart home e veicoli elettrici.
In questo scenario evolutivo, la digitalizzazione delle infrastrutture energetiche diventa funzionale all'integrazione dei sistemi e supporta lo scambio dati tra operatori di trasmissione e distribuzione, servizi di rete più veloci ed efficienti, connessioni tra generatori distribuiti, tra sistemi di accumulo e generatori, una migliore connettività ed interazione tra consumatori e generatori, nonché le interazioni tra vettori energetici, quali reti elettriche, di gas, acqua e calore. Inoltre, va considerato che l'"internet delle cose elettriche/digitali" nel perimetro operativo dell'utente introduce requisiti di riservatezza dei dati personali.
Tale trasformazione digitale ha modificato in modo significativo il concetto di sicurezza dei sistemi energetici. Alla necessità di preservare l'adeguatezza e la sicurezza delle infrastrutture fisiche, si è aggiunta l'esigenza di prevedere misure di protezione delle tecnologie OT (Operational Technology), IT (Information Technology) e IIoT (Industrial Internet of Things) a tutela della sicurezza e della privacy dei dati e delle computazioni.
La dimensione della cybersecurity è destinata ad assumere un ruolo sempre più centrale nei prossimi anni se si considera che la digitalizzazione delle reti è un imprescindibile fattore abilitante della transizione energetica e che i sistemi energetici rappresentano infrastrutture critiche, il cui esercizio richiede adeguate misure di protezione e difesa dei sistemi di comunicazione e controllo.
Lo sviluppo e l'adozione di misure di cybersecurity adeguate al livello di rischio è una priorità riconosciuta dalle strategie di sviluppo e innovazione tecnologica del sistema paese, finalizzate a garantire un livello di maturità tecnologica allineato ai target di cybersecurity Europei (Direttiva NIS e Cybersecurity Act) e nazionali (Legge sul perimetro di sicurezza nazionale).
Il progetto integrato sulla cybersecurity dei sistemi energetici coinvolge i tre enti di ricerca italiani, RSE, ENEA e CNR (e le Università co-beneficiarie di ENEA e CNR), nel raggiungimento dell'obiettivo prioritario "Digitalizzazione ed evoluzione delle reti" dell'Accordo di Programma di Ricerca 2022-2024.
Le attività del progetto sono finalizzate alla sperimentazione di tecnologie di cybersecurity considerate mature in casi applicativi significativi per la transizione energetica e allo studio e valutazione di tecnologie e piattaforme innovative.
L'obiettivo delle sperimentazioni è fornire agli stakeholder coinvolti nel processo di digitalizzazione strumenti e valutazioni che facilitino l'adozione di misure di cybersecurity nei prodotti e nelle infrastrutture di controllo energetico.
Gli sviluppi relativi alle tecnologie innovative permetteranno di indirizzare l'ingegnerizzazione delle soluzioni in funzione della loro effettiva capacità di migliorare il livello di cybersecurity delle applicazioni energetiche, anche in relazione all'evoluzione degli attacchi cyber.

Abstract del progetto ENG

The achievement of the 2030 energy targets established by the PNIEC (the Italian Integrated Plan for Energy and Climate) requires a digital transformation of the sector, which allows the creation of smart grids capable of complying with technical and economic requirements by satisfying the energy demand of a variety of loads with renewable sources, such as industrial plants, commercial and residential buildings, smart homes and electric vehicles.
In this revolutionary scenario, the digitization of energy infrastructures becomes essential to the system integration and supports the data exchange between transmission and distribution operators, faster and more efficient grid services, connections between distributed generators, between storage systems and generators, a better connectivity and interaction between consumers and generators, and interactions between energy vectors, such as electricity, gas, water and heat networks. Furthermore, it should be considered that the

“Internet of electric/digital things” within the user's operational perimeter introduces privacy requirements for preserving the confidentiality of personal data.
This digital transformation has significantly changed the concept of energy system security. In addition to the need to preserve the adequacy and security of the physical infrastructures, there is the need to provide mechanisms for OT (Operational Technology), IT (Information Technology) and IIoT (Industrial Internet of Things) technologies to protect the security and privacy of data and computations.
The cybersecurity dimension will take an increasingly central role in the coming years if we consider that the grid digitization is an essential enabling factor of the energy transition and that energy systems represent critical infrastructures, whose operation requires adequate measures to protect and defend the communication and control systems.
The development and adoption of cybersecurity measures appropriate to the level of risk is a priority recognized by the development and innovation strategies of the Country, aimed at guaranteeing a technological maturity level aligned with the targets of European (NIS Directive and Cybersecurity Act) and National (Law on the National security perimeter) legislation.
The integrated project on the cybersecurity of energy systems involves the three Italian research institutions, RSE, ENEA and CNR (and the co-beneficiary universities of ENEA and CNR) in achieving the priority objective "Digitization and evolution of networks" of the Research Program Agreement 2022-2024.
The project activities are aimed at experimenting more mature cybersecurity technologies in significant application cases for the energy transition and at studying and evaluating innovative technologies and platforms.
The objective of the experimental track is to provide the stakeholders involved in the digitization process with tools and assessments that facilitate the adoption of cybersecurity measures in energy control devices and infrastructures.
The developments relating to the innovative technologies will make it possible to drive the solutions engineering according to their effective capability to improve the cybersecurity level of energy applications, also in relation to the cyber attack evolution.

2.3 TRL progetto

TRL iniziale: 2
TRL finale: 4

Le attività svolte nel triennio di ricerca consentiranno un incremento tecnologico da TRL 2 (Strumento o tecnologia formulata a livello di concetto) a TRL 4 (Strumento o tecnologia convalidata in laboratorio).
Le tematiche affrontate nel progetto sono caratterizzate da un elevato grado di interdisciplinarietà (conoscenza di sistemi di protezione, automazione e controllo, sistemi SCADA (Supervision, Control And Data Acquisition), sistemi di gestione dell’energia, tecnologie di comunicazione, tecnologie OT e IoT, cloud computing, virtualizzazione delle reti e degli IED (Intelligent Electronic Device), minacce cyber, vulnerabilità, tecniche di attacco, misure di cybersecurity) e, pertanto, il TRL generale di partenza per l’intero progetto è condizionato dal più basso valore di TRL nei diversi settori coinvolti (TRL 2).
Gli sviluppi indirizzati nel progetto comportano uno sforzo rilevante in termini di maturità tecnologica (disponibilità di software e dispositivi di mercato) e di grado di integrazione (disponibilità di infrastrutture energetiche cyber-fisiche digitalizzate e sicure).
L’incremento a TRL 4 si concretizza attraverso prodotti di ricerca applicati a casi d’uso significativi per la transizione energetica, validati in laboratori e infrastrutture energetiche di ricerca su scala ridotta.
In merito al dettaglio sulle motivazioni dell’attribuzione dei TRL iniziale pari a 2 e TRL finale pari a 4, si rimanda a quanto specificato per LA nel documento “Integrazioni_Commissione_2.1_Risposte.docx” (Tabella alle pagine 50- 55 del documento), inviato in data 15 giugno 2023 in risposta a specifica richiesta di integrazione formulata dalla Commissione.

2.4 Inquadramento del progetto nello stato dell'arte

a) Stato dell’arte nazionale e internazionale relativamente alle attività previste nel progetto

Di seguito, si riportano gli sviluppi di ricerca e lo stato delle soluzioni di mercato, suddivisi per obiettivi prioritari del progetto.

Cybersecurity delle comunicazioni

Lo standard di riferimento per le comunicazioni nei sistemi elettrici è la serie IEC 62351, la quale ha ormai raggiunto un discreto livello di maturità ed inizia ad essere supportata da dispositivi di mercato e da enti di certificazione.
I profili di sicurezza specificati in questa serie garantiscono riservatezza, integrità ed autenticità delle comunicazioni mediante protocolli

di scambio chiavi e algoritmi crittografici, quali RSA [1] e AES [2].
La gestione delle chiavi e dei certificati elettronici è tipicamente basata su Infrastrutture a Chiave Pubblica, o PKI. Di recente, la blockchain è emersa come un candidato promettente in grado di sostituire la PKI centralizzata, come testimoniato da una proliferazione di articoli su questo argomento, ad esempio [3], [4], [5].

La robustezza degli algoritmi crittografici attualmente in uso è strettamente legata alla complessità computazionale necessaria per l'individuazione delle chiavi. Per quanto riguarda la crittografia, una innovazione tecnologica è rappresentata dai protocolli di distribuzione di chiavi quantistiche (QKD) [6], in cui le chiavi vengono codificate in stati quantistici, intrinsecamente sicuri in quanto assicurano che una chiave segreta compromessa possa essere identificata e scartata prima dell'uso.
L'ETSI [7] [8], organizzazione leader nella standardizzazione in ambito ICT, ha creato il QKD Industry Specification Group (ISG) di livello mondiale per sviluppare standard per i sistemi QKD. L'obiettivo del gruppo è quello di combinare l'analisi della sicurezza QKD con i dettagli delle implementazioni pratiche per sviluppare standard che possano essere utilizzati dalle aziende che sviluppano prodotti QKD. L'obiettivo finale è sviluppare un quadro di certificazione che colmi il divario tra le prove di sicurezza teoriche e le implementazioni pratiche con dispositivi imperfetti. In alcuni casi, ciò ha stimolato ulteriori ricerche teoriche, al fine di rendere i presupposti teorici più facili da soddisfare nella pratica. In altri casi, consiste nel definire la migliore pratica ingegneristica per avvicinarsi alle ipotesi teoriche esistenti. Questo quadro di riferimento è considerato uno standard previsionale. La maggior parte delle norme si basa su una serie di metodi esistenti già in uso commerciale. Gli standard previsionali anticipano la tecnologia emergente e cercano di fornire le indicazioni operative, i metodi di prova e di verifica necessari per far progredire la nuova tecnologia verso un'ampia adozione commerciale [9].
La Raccomandazione dell'International Telecommunication Union (ITU) ITU-T Y.3803 fornisce assistenza per la progettazione, l'implementazione e il funzionamento della gestione delle chiavi di una rete di distribuzione di chiavi quantistiche (QKDN). Per implementare una QKDN e integrarla adeguatamente con la rete utente, la Raccomandazione ITU-T Y.3800 fornisce una panoramica delle tecnologie QKD, comprese le capacità della rete, la struttura concettuale, il modello a strati, le funzioni e i componenti di base e la relazione con la rete utente.
Attualmente risultano già disponibili prodotti commerciali e prototipi per la generazione di numeri casuali quantistici e la distribuzione quantistica delle chiavi (QKD). In Italia, l'attenzione è stata focalizzata sulla comunicazione quantistica mediante reti in fibra ottica (in free-space), sullo sviluppo di componentistica integrata e su protocolli avanzati. Presso il Centro di Tecnologie Quantistiche QTech dell'Università di Padova sono state avviate, da anni, diverse dimostrazioni sulle applicazioni della QKD.

Per quanto riguarda la consapevolezza delle minacce informatiche, molte organizzazioni producono, raccolgono e condividono informazioni per favorire il rilevamento precoce e una reazione efficace agli attacchi informatici. Il mercato attuale offre una varietà di piattaforme e metodi per consentire alle organizzazioni di condividere in modo sicuro e automatico le informazioni sugli attacchi informatici analizzati e sulle minacce, meglio noti come Cyber-Threat Intelligence (CTI) [10]. Alcune di queste, quale Malware Information Sharing Platform (MISP) [11], usano formati di dati specifici. Il MITRE [12] ha proposto la Structured Threat Information eXpression (STIX), che è diventato uno standard per molti strumenti e sistemi per la condivisione e l'analisi di CTI. Alcuni progetti Europei quali SPARTA e C3ISP hanno proposto approcci per la condivisione di queste informazioni in vari formati e meccanismi per passare da uno all'altro.

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978
[2] "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, United States National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Nov. 2001
[3] A. Singla, E. Bertino "Blockchain based PKI solution for IoT", IEEE 4th Intern. Conference on collaboration and Internet Computing, 2018
[4] D. Pavithran, K. Shaalan, "Towards Creating Public Key Authentication for IoT Blockchain", 2019 Sixth HCT Information Technology Trends (ITT), 2019
[5] A. Yakubov, W.M. Shbair, A. Wallbom, D. Sanda, R. State, "A blockchain-based PKI management framework", 2018 NOMS IEEE/IFIP Network Operations and Management Symposium, Taipei, 2018
[6] M. Kaur and S. Kalra, "Security in IoT-based smart grid through quantum key distribution," Adv. Intell. Syst. Comput., vol 554, pp. 523–530, Sep. 2017
[7] ETSI QKD-ISG, [online] Available: http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution
[8] T. Langer and G. Lenhart, "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD", New J. Phys., vol. 11, no. 055051, 2009
[9] ETSI Quantum-Safe-Crypto Workshop, Sep. 2013, [online] Available: http://www.etsi.org/news-events/past-events/648-crypto-workshop2013
[10] Johnson, Christopher, Mark Badger, David Waltermire, Julie Snyder e Clem Skorupka . Guida alla condivisione delle informazioni sulle minacce informatiche. N. Pubblicazione speciale NIST (SP) 800-150 (Bozza). Istituto nazionale di standard e tecnologia, 2016

[11] Funzionalità MISP, https://www.misp-project.org/features.html
[12] Mitre Common Vulnerability and Exposure, https://cve.mitre.org/

Cybersecurity e resilienza delle infrastrutture cyber-fisiche a fronte di cyber attacchi

Molteplici gruppi di ricerca hanno affrontato negli ultimi anni la tematica della sicurezza delle infrastrutture energetiche in termini di resilienza (in particolare a fronte di eventi con bassa probabilità di accadimento, ma ad alto impatto sulle risorse dell'infrastruttura) [1], sia per cause naturali che di attacchi malevoli [2]. Tali attacchi telematici possono essere diretti all'infrastruttura e/o al suo perimetro (ossia gli utenti finali) [3] [4]. Per esempio, in [5] è condotta un'analisi comparativa di attacchi cyber-fisici a micro-grid e sistemi di generazione e accumulo distribuito, basati su data injection.

Un ambito applicativo particolarmente critico per i sistemi elettrici è quello dei sistemi di protezione. Gli interruttori utilizzati come dispositivi di protezione nelle reti e micro-reti elettriche presentano diverse caratteristiche in relazione alle condizioni critiche (sovracorrenti, sovratensioni, etc) dalle quali devono proteggere i sistemi/apparati cui sono collegati, alla tecnologia costruttiva, all'ambito applicativo, alla tipologia e tempistica di intervento. Poichè tali dispositivi di protezione devono garantire tempi molto rapidi d'intervento, spesso utilizzano standard di comunicazione basati su traffico dati non criptato [6]. Ciò certamente assicura prestazioni in tempo reale, ma costituisce anche un elemento di vulnerabilità per tali interruttori e per tutta la rete elettrica, giacché essi potrebbero essere bersaglio di attacchi cibernetici.
Esempi di attacchi cyber a danno di dispositivi di protezione nelle reti elettriche sono descritti in [7], dove vengono considerate le criticità relative ai protocolli Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) della serie standard IEC 61850 [8] [9]. L'impatto che una minaccia di tale tipo può avere sulle reti elettriche può essere considerevole, basti pensare ai danni che possono provocare aperture non necessarie degli interruttori con possibile innesco di interventi a catena da parte degli altri dispositivi presenti, all'attivazione di procedure come il distacco dei carichi o la disconnessione dei generatori. In alcuni casi, si possono verificare condizioni di black-out e la conseguente interruzione della fornitura per un notevole numero di utenti.
Diverse sono le tecniche proposte per l'incremento della cyber resilienza nell'ambito delle reti elettriche [10], [11] e gli esperti del settore sottolineano la necessità di un approccio di tipo integrato [12]. Esso dovrebbe favorire l'identificazione e l'implementazione di soluzioni per la "cyber readiness", ossia la capacità di fronteggiare proattivamente un attacco cibernetico. In [12] ciò viene tradotto in un insieme di "controlli" intesi come contromisure tecniche o economiche per minimizzare le conseguenze di una minaccia cyber.

Un aspetto fondamentale per la resilienza delle infrastrutture energetiche sottolineato dalle recenti direttive europee e legislazioni nazionali è legato alla cybersecurity della supply chain e alla necessità di certificazioni di conformità di cybersecurity dei processi e dei prodotti.
Nell'ambito dei dispositivi di controllo e comunicazione indirizzati dal progetto, costituiscono un riferimento le certificazioni di conformità agli standard ISA/IEC 62443, IEC 62351 e 3GPP TS 33.117.

[1] Liu, J., Cao, X., Xu, Z., Guan, X., Dong, X., Wang, C., 2021. Resilient operation of multi-energy industrial park based on integrated hydrogen-electricity-heat microgrids. International Journal of Hydrogen Energy.; https://doi.org/10.1016/j.ijhydene.2020.11.229
[2] Liu, C.-C., Bedoya, J.C., Sahani, N., Stefanov, A., Appiah-Kubi, J., Sun, C.-C., Lee, J.Y., Zhu, R., 2021. Cyber–Physical System Security of Distribution Systems. FNT in Electric Energy Systems. https://doi.org/10.1561/3100000026
[3] Chen, T., Yin, X., Wang, G., 2021. Securing communications between smart grids and real users; providing a methodology based on user authentication. Energy Reports. https://doi.org/10.1016/j.egyr.2021.08.125
[4] Batiha, T., Krömer, P., 2020. Design and analysis of efficient neural intrusion detection for wireless sensor networks. Concurrency Computat Pract Exper. https://doi.org/10.1002/cpe.6152
[5] Husnoo, M.A., Anwar, A., Hosseinzadeh, N., Islam, S.N., Mahmood, A.N., Doss, R., 2023. False data injection threats in active distribution systems: A comprehensive survey. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2022.10.021
[6] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, 2020, pp. 247-254, doi: 10.1109/ISGT-Europe47291.2020.9248840
[7] M. Kabir-Querrec, S. Mocanu, J. Thiriet, and E. Savary, "A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks," in Proc IEEE Int Conf on Emerging Technologies and Factory Automation (ETFA), Berlin, Sep 2016, pp. 1-4
[8] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in in Proc 2012 IEEE Globecom Workshops, Anaheim, CA, Dec 2012, pp. 1508 ⬭ 1513
[9] T. A. Youssef, M. E. Hariri, N. Bugay, and O. A. Mohammed, "IEC 61850: Technology standards and cyber-threats," in Proc IEEE Int Conf on Environment and Electrical Engineering (EEEIC), Florence, Jun 2016, pp. 1-6
[10] A.D. Syrmakesis, C. Alcaraz, N.D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats", International Journal of Information Security, 21, 1189–1210 (2022). https://doi.org/10.1007/s10207-022-00594-7

[11] R. Ross, V. Pilliteri, R. Graubart, D. Bodeau, R. Mcquaid, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” in National Institute of Standards and Technologies (NIST) Special Publication (SP-800-160), 2019
[12] “Principi, Linee Guida e Good Practice per la gestione della Cyber security, Resilienza e Business Continuity,” Osservatorio Nazionale per la Cyber Security, 2018

Applicazioni di Intelligenza Artificiale per la cybersecurity dei sistemi energetici

Le applicazioni di AI a supporto della cybersecurity dell’ecosistema energia sono numerose ed hanno l’obiettivo e la potenzialità di migliorarne l’affidabilità e la robustezza.
Le performance dei modelli di Machine Learning (ML) dipendono fortemente dalla quantità e dalla qualità dei dati. Anche nei task di identificazione degli attacchi, come la classificazione o il clustering, ad esempio, i dati disponibili sono frequentemente soggetti ad uno sbilanciamento, ovvero la numerosità di campioni per ciascuna classe da identificare non è omogenea. Lo sbilanciamento dei dataset rappresenta un forte limite nella generazione di modelli che risultino efficaci.
Il clustering supervisionato, la Support Vector Machine (SVM) (singola o multi-classe), la fuzzy logic, le ANN (Artificial Neural Network) e le DNN (Deep Neural Network) sono tecniche comunemente utilizzate per il rilevamento degli attacchi nel traffico di rete. Queste tecniche analizzano i dati sul traffico in tempo reale per rilevare tempestivamente gli attacchi potenzialmente dannosi. Tuttavia, il rilevamento degli attacchi che considera solo i dati di rete e di host potrebbe non riuscire a rilevare attacchi più sofisticati, o i cosiddetti insider attacks. Uno degli ostacoli principali allo sviluppo di adeguati sistemi di cybersecurity basati sull’AI, secondo Sharafaldin et al. [1], sta proprio nella mancanza di set di dati adeguati su cui allenare gli algoritmi. Esistono numerosi set di dati, come DARPA98, KDD99, ISC2012 e ADFA13, che sono stati utilizzati dai ricercatori per valutare le prestazioni dei loro approcci di rilevamento e prevenzione delle intrusioni; tuttavia, sulla base dello studio illustrato in [1], su undici set di dati disponibili dal 1998 ad oggi, molti di questi dataset sono obsoleti e inaffidabili per essere utilizzati. Alcuni di questi set di dati soffrono della mancanza di diversità di traffico e volumi, alcuni di essi non coprono la varietà degli attacchi, mentre altri semplicemente non riflettono le tendenze attuali, oppure mancano di set di funzionalità e metadati. Nel loro articolo, Sharafakdn et al. producono un dataset affidabile (chiamato IDS20178), contenente flussi di rete benigni e sette famiglie aggiornate di attacchi comuni, che soddisfa i criteri del mondo reale ed è pubblicamente disponibile online. Infine, questo lavoro valuta le prestazioni di un insieme completo di features del traffico di rete e algoritmi di machine learning indicando il miglior insieme di features per rilevare determinate categorie di attacco. Gli algoritmi di cui si occupano Sharafaldin et al. sono tra i più comunemente utilizzati nella classificazione di attacchi con tecniche classiche di machine learning: K-Nearest Neighbors (KNN), Random Forest (RF), ID3, Adaboost, Multilayer perceptron (MLP), Naive-Bayes (NB), Quadratic Discriminant Analysis (QDA).

Di un’altra questione cruciale si occupano, invece, Jahromi et al. [2], secondo cui i modelli non supervisionati, che incorporano dati fisici o di processo, possono dare il loro contributo nel monitoraggio di un sistema poiché non si basano su una conoscenza troppo dettagliata e specifica delle minacce informatiche. Inoltre, la maggior parte degli approcci esistenti ignora il fatto che i dati provenienti dal sistema di controllo industriale (ICS) possono essere imbalanced, e dunque il rischio è di modellare solo il comportamento normale di un sistema. Jahromi et al. [2], hanno sviluppato un metodo innovativo di rilevamento degli attacchi a due fasi per set di dati ICS imbalanced, in grado di rilevare sia gli attacchi già noti, subiti in precedenza, che quelli sconosciuti.

In [3], Saharkhizan et al. utilizzano tecniche di deep learning per rilevare gli attacchi informatici contro i sistemi IoT. L’approccio, seguito da questi autori, integra un insieme di moduli avanzati di Recurrent Neural Network (RNN), di tipo Long Short-Term Memory (LSTM), in un insieme di rivelatori. Questi moduli vengono quindi uniti utilizzando un Decision Tree (DT) per arrivare a un output aggregato nella fase finale.

In [4] viene mostrato da Bland et al. come mappare le features di una rete di Petri in un framework di apprendimento per rinforzo. Le tipologie di attacco considerate sono: cross-site scripting (CAPEC 66) e spear phishing (CAPEC 163). Sebbene siano state scelte queste due tipologie in particolare, a detta degli autori le reti PNPSC sono in grado di modellare la maggior parte, se non tutti, gli schemi di attacco CAPEC.

In [5], Farivar et al. propongono un approccio di controllo classico per la compensazione degli attacchi su CPS (Cyber-Physical Systems). In questo articolo si ipotizza che il CPS stia subendo attacchi informatici. Il sistema di controllo progettato contiene un controller non lineare basato sul metodo Variable Structure (VS) e una Gaussian Radial Basis Function Neural Network (GRBFNN) come stimatore intelligente per stimare l'effetto dell'attacco. Il metodo VS è una tecnica di controllo robusta molto diffusa. Lo stimatore GRBFNN effettua la stima di possibili attacchi e il controller VS è progettato per compensare gli effetti di tali attacchi sul sistema fisico e per controllare le prestazioni per scopi di regolazione e tracciamento. I tipi di attacco considerati nell’articolo sono: deception attacks, denial of service (DoS), stealth attacks, replay attacks, covert attacks, false data injection attacks.

Avendo a che fare con il fog-to-things computing, occorre considerare soluzioni di tipo distribuito: è quello che fanno Abeshu et al. in [6]

proponendo un nuovo schema distribuito di deep learning per il rilevamento di attacchi cyber. La soluzione proposta consiste nell'utilizzo di un Autoencoder; si tratta di un modello di rete neurale, in ambito DL, attualmente fra i più utilizzati e che porta a risultati promettenti nell'apprendimento non supervisionato.

L' area tematica dell'Adversarial Machine Learning (AML), che include le soluzioni basate su GAN (Generative Adversarial Network), è quasi totalmente incentrata sullo studio dei sistemi e delle tecniche di attacco verso sistemi di ML e DL posti a difesa degli asset critici, come quelli dell'energia [7].
Con riferimento alle esperienze di utilizzo delle GAN nell'implementazione di sistemi di difesa degli asset dell'energia da attacchi cyber alla sicurezza, i contributi rilevati sono in numero più esiguo, a testimonianza del fatto che si tratta di un campo in cui la ricerca è ancora in fase quasi pioneristica e in cui la complessità dei sistemi di AML, abbinata a quella di un dominio, richiede nuove idee e nuovi paradigmi per essere ben sviluppata.
Un contributo degno di attenzione, nella prospettiva dell'impiego delle GAN per sistemi di difesa, è riportato in [8] in cui le GAN vengono impiegate per risolvere un problema di data generation e, dunque, di data augmentation, nel dominio dell'energia.
Tra i contributi che fanno uso esplicito di modelli basati su GAN per implementare attacchi ai sistemi energetici si può notare lo studio riportato in [7], in cui viene implementato un sistema di attacco basato su data poisoning, consistente nella generazione di dati falsi per raggiungere scopi fraudolenti. Il lavoro presentato in [9] discute le minacce di cybersecurity ai danni di sistemi energetici causate dallo sfruttamento dell'AML.

L'analisi del malware è un altro campo di ricerca molto attivo, con molte tecniche proposte negli ultimi tempi [10] per rilevare malware e mantenere il sistema sicuro. Inoltre, il numero di approcci proposti è aumentato seguendo la tendenza dell'intelligenza artificiale [11-12]. Il modello proposto da [13] utilizza due tecniche di apprendimento automatico, come KNN e SVM, e distingue tra software e malware osservando le chiamate di sistema API. Approcci più avanzati adottano i modelli di Deep Learning convertendo il malware in immagini e quindi classificandole [14-15]. Altri approcci interessanti sono basati su grafici e interazioni tra funzioni nel codice dannoso. Innanzitutto, disassemblano il codice dannoso e generano un grafico che riporta il comportamento e la sintassi dell'esecuzione (di solito, un grafico del flusso di controllo), quindi estraggono caratteristiche e attributi da questo grafico per classificare e rilevare il malware.

Infine, l'utilizzo di infrastrutture HPC (High Performance Computing) per la cybersicurezza sta diventando sempre più importante, sia a livello nazionale che internazionale. Questo è dovuto al crescente aumento delle minacce informatiche, che richiedono una risposta sempre più veloce ed efficiente per contrastarle. Inoltre, gli algoritmi di crittografia si stanno indirizzando verso le cosiddette tecnologie post-quantum, che garantiscono elevatissima robustezza, eventualmente implementate su hardware dedicato che permette l'istanziazione di profonde pipeline e l'utilizzo di parallelismo spaziale [16].

Relativamente all'aspetto puramente hardware, le architetture eterogenee in uso fanno ricorso a processori, acceleratori (sia FPGA che GPU), sistemi di storage e di interconnessione di ultima generazione. L'architettura proposta nel progetto supererà lo stato dell'arte integrando le infrastrutture tradizionali con l'Intelligenza Artificiale (processori Intel Sapphire Rapid / AMD Epyc Genoa, GPU H100, schede FPGA ALVEO (xilinx) o Agilex (Intel), firewalll con AI integrata, connessione su VPN dedicata, sistema di dischi ad alta banda/bassa latenza (NVMe)).

[1] I. Sharafaldin, A. H. Lashkari e A. A. Ghorbani, «Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization» in Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal, 2018
[2] A. N. Jahromi, H. Karimipour, A. Dehghantanha e K. -K. R. Choo, «Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems,» IEEE Internet of Things Journal, vol. 8, n. 17, pp. 13712-13722, Settembre 2021
[3] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo e R. M. Parizi, «An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic,» IEEE Internet of Things Journal, vol. 7, n. 9, pp. 8852-8859, Settembre 2020
[4] J. A. Bland, M. D. Petty, T. S. Whitaker, K. P. Maxwell e W. A. Cantrell, «Machine Learning Cyberattack and Defense Strategies,» Computers & Security, vol. 92, 2020
[5] F. Farivar, M. S. Haghighi, A. Jolfaei e M. Alazab, «Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT,» IEEE Transactions on Industrial Informatics, vol. 16, n. 4, pp. 2716-2725, Aprile 2020
[6] A. D. Abeshu e N. Chilamkurti, «Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing,» IEEE Communications Magazine, vol. 56, n. 2, pp. 169-175, Feb. 2018
[7] Marulli F, Visaggio CA. Adversarial deep learning for energy management in buildings. In: 2019 Summer Simulation Conference; 2019, no. 50
[8] Fekri, Mohammad Navid, Ananda Mohon Ghosh, and Katarina Grolinger. "Generating energy data for machine learning with recurrent generative adversarial networks." Energies 13.1 (2019): 130

[9] Bor, Martin C., et al. "Adversarial machine learning in smart energy systems." Proceedings of the Tenth ACM International Conference on Future Energy Systems, 2019
[10] Ucci, D., Aniello, L., & Baldoni, R. (2019). Indagine sulle tecniche di apprendimento au-tomatico per l'analisi del malware. Computer e sicurezza, 81, 123-147
[11] Mahdavifar, Samaneh e Ali A. Ghorbani. "Applicazione del deep learning alla sicurez-za informatica: un sondaggio". Neurocomputing 347 (2019): 149-176
[12] Kouliaridis, Vasileios , et al. "Un sondaggio sulle tecniche di rilevamento del malware mobile." Transazioni IEICE su informazioni e sistemi 103.2 (2020): 204-211
[13] Yuan, X. (2017, maggio). Forum di dottorato: rilevamento di malware in tempo reale basa-to sull'apprendimento approfondito con analisi in più fasi. Nel 2017 IEEE International Confer-ence on Smart Computing (SMARTCOMP) (pp. 1-2)
[14] Nguyen, MH, Le Nguyen, D., Nguyen, XM e Quan, TT (2018). Rilevamento automatico di malware sofisticati utilizzando il grafico del flusso di controllo lazy-binding e il deep learning. Computer e sicurezza, 76, 128-155
[15] Iadarola, G., Martinelli, F., Mercaldo, F., & Santone, A. (2020). Rilevamento della famiglia di malware basato su immagini: una valutazione tra tecniche di estrazione delle caratteristiche e di classificazione. In IoTBDS (pagg. 499-506)
[16] H. Li, Y. Tang, Z. Que and J. Zhang, "FPGA Accelerated Post-Quantum Cryptography," in IEEE Transactions on Nanotechnology, vol. 21, pp. 685-691, 2022

b) Attività svolte nel triennio precedente

Le attività della presente proposta progettuale si pongono in continuità con i seguenti progetti del Piano Triennale della Ricerca di Sistema 2019-2021:

• il Progetto 2.3 “Applicazione al sistema elettrico di tecnologie dell’informazione, internet delle cose, peer to peer – WP2 Incremento della sicurezza e resilienza del sistema”

• il Progetto 2.7 “Modelli e strumenti per incrementare l’efficienza energetica nel ciclo di produzione, trasporto, distribuzione dell’elettricità – WP1 Analisi delle problematiche di gestione per l’integrazione nelle attuali reti in AC di nuove reti in DC in MT/BT (Media Tensione/Bassa Tensione)”.

Nel seguito vengono riportati i prodotti del Progetto 2.3 sviluppati da RSE e i loro collegamenti con le attività della proposta di progetto.

• la Piattaforma Misurazione Prestazioni CyberSecurity verrà estesa ed integrata nella Piattaforma per misurazioni di impatto di servizi per la gestione centralizzata di chiavi e certificati nelle comunicazioni di telecontrollo

• il Sistema “Decentralized PKI for IoT Systems” verrà ulteriormente sviluppato nel progetto, dotandolo di funzionalità aggiuntive per la gestione delle chiavi

• le analisi di sicurezza della tecnologia 5G costituiranno un background per le attività di test delle reti 5G

• il modello probabilistico per l’analisi di scenari di attacco basato su evidenze sperimentali, lo strumento per l’emulazione di processi di attacco cyber ad infrastrutture energetiche e la Piattaforma Rilevamento Anomalie Cyber verranno ulteriormente estesi ed integrati nella Piattaforma di anomaly detection basata su AI e ML.

Nel Progetto 2.7 ENEA ha implementato un interruttore di protezione differenziale a stato solido per reti e micro-reti in DC (V=1000V, I=100A). Il dispositivo, altamente configurabile, è impostabile in maniera personalizzata in funzione delle specifiche esigenze di protezione (es. tensione, corrente, tempistica di interruzione, etc.). In continuità con tale attività del precedente piano triennale, ENEA studierà le nuove funzionalità da integrare nel prototipo per rispondere alle esigenze di cybersicurezza delle reti elettriche, progetterà i relativi schemi di protezione e li testerà nell’infrastruttura sperimentale dedicata.

c) Obiettivi scientifici e tecnologici e progressi attesi rispetto allo stato dell'arte

Di seguito, si riportano gli obiettivi scientifici e tecnologici e i progressi attesi rispetto allo stato dell'arte suddivisi per obiettivi prioritari del progetto.

Cybersecurity delle comunicazioni

Data l’importanza strategica delle infrastrutture energetiche e delle reti “smart” di ultima generazione, occorre sottolineare che queste sono caratterizzate da apparati che si scambiano dati ed interoperano coordinandosi e rispondendo a comandi e richieste da parte di controllori digitali. Un eventuale attacco cibernetico su uno degli apparati di rete non comporta criticità solo a livello del singolo sistema, ma può inficiare l’operatività di porzioni, anche estese, della infrastruttura energetica. In tale contesto, risulta sempre più indispensabile l’invio di dati, misure, stati e comandi in maniera sicura.

Lo sviluppo di piattaforme per valutazioni prestazionali di soluzioni di cybersecurity standard costituisce un supporto fondamentale per raggiungere l'obiettivo di migliorare il livello di cybersecurity by design delle applicazioni di controllo energetico. In particolare, gli sviluppi relativi all'integrazione di funzioni di gestione di chiavi e certificati digitali, in architetture centralizzate e decentralizzate, rappresentano un contributo essenziale alla cybersecurity di tutte le nuove applicazioni richieste dalla transizione energetica. Gli sviluppi previsti nel progetto costituiscono un avanzamento nell'applicazione ai sistemi energetici sia delle soluzioni più mature e standardizzate, sia delle soluzioni innovative oggetto di sviluppi di ricerca e di possibili attività di standardizzazione futura.

Gli sviluppi relativi all'implementazione di protocolli di autenticazione basati su QKD consentirà il conseguimento di progressi nel settore di interesse giacché, allo stato attuale, l'applicazione della crittografia quantistica ai sistemi energetici risulta, ancora, non esplorata a livello sperimentale. Le attività proposte nel progetto intendono andare oltre lo stato dell'arte mediante la sperimentazione dell'autenticazione di uno o più comandi operativi basata su scambio di chiavi crittografiche QKD, anche in contesti di tipo multiterminale. Si intende, in particolare, sfruttare le leggi della fisica (e non il risultato di algoritmi) per ottenere sequenze simmetriche e sicure di informazioni da trasmettere su un canale quantistico. Mettendo a sistema le competenze maturate in questi anni, si verificherà la potenziale efficacia dell'utilizzo della crittografia QKD nel settore energetico mediante l'infrastruttura di test realizzata per il progetto.

L'adozione della tecnologia Power Line Communication (PLC) che utilizza la rete elettrica come canale di comunicazione costituisce di per sé una infrastruttura di rete intrinsecamente sicura contro le minacce cyber in quanto generalmente di proprietà dell'operatore di distribuzione e difficilmente accessibile per ragioni di sicurezza. Nell'ambito delle attività del progetto si svilupperà una architettura di rete che utilizzi la power line communication come canale di comunicazione e l'impiego di prototipi di dispositivi elettronici intelligenti che sfruttano la comunicazione power line per monitorare la rete e controllare generatori distribuiti e sistemi di accumulo di energia. Ciò rappresenta un avanzamento applicativo rispetto allo stato dell'arte, in cui l'utilizzo della power line communication è limitato alla tele-lettura dei contatori.

Costituisce un avanzamento rispetto allo state dell'arte anche l'Osservatorio per aumentare la consapevolezza sulle minacce cyber nel settore energetico. Verranno migliorati gli strumenti per presentare e analizzare le vulnerabilità anche in maniera collaborativa.

Cybersecurity e resilienza delle infrastrutture cyber-fisiche a fronte di cyber attacchi

Nei documenti redatti da esperti del settore e organi competenti sulle soluzioni per lo sviluppo della "cyber readiness" si fa riferimento a contromisure tecniche o economiche per minimizzare le conseguenze di una minaccia cyber. Si fa, inoltre, riferimento alla definizione di metodi per l'identificazione dei componenti vulnerabili delle reti elettriche che necessitano di essere protetti. La successiva fase di protezione degli apparati identificati si basa su logiche di controllo e soluzioni di tipo software.
In questo progetto, si intendono proporre soluzioni che rappresentano un effettivo progresso rispetto allo stato dell'arte.
Si intende, in particolare, sviluppare dispositivi di protezione di nuova concezione per le reti elettriche. Tali apparati saranno ottenuti adottando un approccio di tipo integrato, organizzato su più layer che, partendo dalla sezione hardware del dispositivo di protezione, lo doterà di funzionalità software/trasmissione dati e comandi di tipo avanzato. I nuovi dispositivi saranno in grado di rilevare i potenziali attacchi mediante sensoristica ed intelligenza a bordo e saranno, altresì, in grado di interrompere i circuiti cui sono collegati e di comandare la messa in sicurezza degli apparati connessi alla stessa micro-rete elettrica. Tale tipologia di apparati non è disponibile a livello commerciale e costituisce, pertanto, un evidente avanzamento rispetto allo stato dell'arte.

Per quanto riguarda la cybersecurity della supply chain, gli sviluppi previsti nel progetto sulle analisi di conformità dei dispositivi di protezione, automazione, controllo e protezione utilizzati nelle infrastrutture energetiche, costituiscono un avanzamento significativo in quanto non esistono piattaforme commerciali con funzionalità analoghe.

Un'altra attività progettuale intende identificare e valutare tecniche di autenticazione e autorizzazione specifiche per l'ambito delle reti energetiche multi-vettore, in particolare utilizzando le grandezze fisiche tipiche di queste infrastrutture e le proprietà che possano portare a procedure di anomaly detection accurate (bassa percentuale di falsi positivi e/o falsi negativi). Pertanto, saranno individuati dei criteri per:
• la selezione delle variabili più adatte all'inclusione nelle procedure di autenticazione e anomaly detection da utilizzare nella progettazione delle future reti energetiche multi-vettore ad accesso distribuito
• le procedure da eseguire in caso di rilevamento di un attacco esterno.
Per quanto riguarda il primo punto, si identificheranno dei criteri di compatibilità tra singole variabili o raggruppamenti delle stesse (sottoinsiemi dell'intero set per la caratterizzazione dello stato della micro-rete) e delle soglie di attenzione per misurare le eventuali discrepanze tra stati attesi (in base alle misure della produzione e del carico reale) e quanto indicato dai sensori sul campo, per identificare possibili sensori e/o attuatori corrotti da attacchi esterni in base alle possibili combinazioni per la costruzione dei raggruppamenti di

variabili. Per esempio, diversi metodi basati su indicatori di comunicazione (quali la lunghezza, il numero e il rate dei pacchetti di informazioni), quindi sulla porzione IT della micro-rete, sono stati presentati per pacchetti singoli o su cluster di informazioni. Nella presente attività si vogliono applicare tecniche similari a quelle appena indicate, ma che vadano a osservare anche il contenuto dei pacchetti dal punto di vista della compatibilità con l'operatività energetica del sistema. Quindi si valuterà un benchmark che consisterà del modello energetico della smart grid in cui, dati i flussi di potenza elettrica e idrogeno attesi, si stimerà lo stato dei componenti in un determinato istante (o finestra temporale) e si confronterà l'insieme di misure acquisite da sensori in campo. Pertanto, sarà possibile individuare delle soglie di attenzione (o di confidenza) per la rilevazione di un attacco esterno su uno o più dispositivi.
In base alla quantità e qualità dei dati disponibili in letteratura ed eventuali prove sul campo, si potranno implementare procedure di rilevazione basate su modelli statistici e/o di machine learning fino alla possibilità di implementare una physics-informed neural network.
Per quanto riguarda le azioni da intraprendere in caso di rilevazione dell'evenienza di un attacco su uno o più dispositivi di campo, sarà necessario valutare la possibilità di isolare una porzione di smart grid rispetto allo svolgimento cooperativo di servizi (demand response, load shift, load smoothing o altri) per evitare la propagazione dell'attacco ad altri dispositivi di controllo della smart grid e quindi, in cascata, alle risorse energetiche controllate.
A questo scopo, si dovrà individuare una topologia di comunicazione tra i dispositivi di regolazione della potenza che possa essere meno soggetta ad attacchi esterni e/o che permetta di identificare rapidamente il dispositivo attaccato e rideterminare i servizi erogabili e la logica di controllo della parte di smart grid sana, una volta isolata la parte corrotta.

Costituiscono avanzamenti rispetto allo state dell'arte anche lo strumento per il calcolo del rischio dinamico basato su analisi automatica di vulnerabilità e modelli di monitoring di rete, e i modelli di digital twins per smart grids e analisi di resilienza.

Applicazioni di Intelligenza Artificiale per la cybersecurity dei sistemi energetici

L'applicazione di algoritmi di Intelligenza Artificiale e Machine Learning alle infrastrutture di scambio dati dei sistemi energetici costituisce, ad oggi, oggetto di attività di ricerca. Nonostante recenti prodotti commerciali (quali Elastic e Agger) includano algoritmi di Machine Learning, la loro capacità di analisi e detection di anomalie nelle infrastrutture energetiche non è ancora stata validata.
Gli sviluppi previsti nel progetto relativi a moduli di detection basati su algoritmi di intelligenza artificiale costituiscono un passo avanti rispetto allo stato dell'arte in diverse direzioni.

Un passo avanti delle piattaforme basate su AI sviluppate nel progetto è la possibilità di validazione delle capacità di detection di anomalie nelle comunicazioni per il controllo di carichi, generatori e sistemi di accumulo, sia stazionari che mobili, connessi a infrastrutture di rete in media e bassa tensione. L'applicabilità delle diverse classi di algoritmi di apprendimento automatico risultate più idonee per il rilevamento di anomalie da attacchi cyber applicazioni energetiche costituirà un significativo passo avanti in termini di affidabilità di queste tecnologie.

La modellazione di processi di attacco a infrastrutture energetiche costituirà un'evoluzione dello stato dell'arte per strumenti che combinano funzionalità di interfaccia con potenzialità di analisi probabilistiche basata su reti bayesiane dinamiche.

Al fine di rendere i modelli di ML ed AI maggiormente interpretabili all'interno del progetto saranno applicate tecniche basate sulla cosiddetta eXplainable Artificial Intelligence (XAI). Questi metodi permetteranno di comprendere i motivi alla base delle scelte effettuate dai modelli complessi.

Costituiscono avanzamenti rispetto allo state dell'arte anche l'infrastruttura distribuita, sicura e privacy preserving per edge data analytics e machine learning per data sovereignty, e il rilevamento di minacce a smart grids tramite algoritmi di meta-learning.

Per la prima volta verrà effettivamente realizzata una infrastruttura HW/SW che unisce le tecnologie di calcolo, comunicazione, storage allo stato dell'arte e le coniuga con algoritmiche, quali machine learning e post-quantum cryptography, per realizzare un prodotto cyber-resiliente in grado di supportare le attività di gestione e controllo previste dalle reti e micro-reti elettriche. Le piattaforme HPC devono essere loro stesse altamente sicure altrimenti diventerebbero l'anello debole della catena di protezione. La piattaforma sarà di tipo distribuito, risulterà connessa con un server ad alte prestazioni centralizzato dove verranno analizzati e conservati i dati.

d) Eventuali collegamenti con altri progetti relativamente alle attività previste nel progetto

Le attività previste nel presente progetto si collegano con altri progetti svolti dagli affidatari e dai loro co-beneficiari, come di seguito sinteticamente elencato:
1) Progetto Mission Innovation Smart Grid, in cui RSE sviluppa un dimostratore Cybersecurity In the Loop per test facility multi-energy

2) Progetto TEXTAROSSA (EuroHPC, coordinato da ENEA), in cui vengono sviluppate le tecnologie HW/SW per un nodo di classe Hexascale e basato su tecnologie eterogenee (processori x86 e Arm, acceleratori GPU e FPGA)
3) Complex networks; Machine Learning e Deep Learning; eXplainable Artificial Intelligence (XAI), nel quale i proponenti, nello scorso triennio, hanno condotto estensivamente ricerca su ambienti software e di programmazione
4) Progetto "Sperimentazione della crittografia quantistica sulla rete Internet in fibra" dell'Università di Padova
5) Progetto Europeo C3ISP (Horizon 2020) in cui CNR ha introdotto la tecnologia relativa agli approcci data-centric per la cybersecurity applicata a collaborative and confidential analytics
6) Progetto Europeo SPARTA (Horizon 2020), il quale ha proposto soluzioni che integrano strumenti per la protezione dei dati con la condivisione di informazioni relative alle minacce cibernetiche
7) Progetto Europeo OSMOSE (Horizon 2020), nel quale RSE ha sviluppato una metodologia di analisi di cybersecurity basata sullo strumento CSET (Cyber Security Evaluation Tool). La metodologia è stata applicata all'architettura ICT del pilota Terna per la gestione di risorse di flessibilità (generazione e carico) connesse alla rete di trasmissione
8) Progetti di ricerca REIPERSEI (PO-FESR Sicilia 2007-2013), I-SOLE (PO-FESR Sicilia 2014-2020) e SInERT (IEV CT Italie-Tunisie 2014-2020) in cui INM-CNR e UNIPA hanno affrontato l'utilizzo della tecnologia PLC per il controllo remoto degli impianti di generazione ed accumulo
9) Serie di progetti (uno finanziato dalla Regione Toscana ed un altro, E-CORRIDOR, dalla Comunità Europea) in cui si propongono ISAC (Information Sharing and Analysis Center) settoriali che permettano di aumentare la consapevolezza sulla tematica della cybersecurity di chi opera nel settore

2.5 Obiettivi e risultati

a) Obiettivi finali del progetto

La filiera energetica italiana assume un peso rilevante nella stabilità socioeconomica del sistema Paese. In tutte le economie avanzate, l'evoluzione del comparto energia comporta un'accelerazione dei processi di digitalizzazione e di gestione dei rischi di cybersecurity. Investire in ricerca per incrementare la Threat Intelligence nazionale, disporre di tecnologie di cyber-prevenzione e infrastrutture per il rilevamento e la risposta tempestiva ad eventi di crimine informatico risulta un ambito strategico per il Paese, come testimoniato dalla recente costituzione della Agenzia per la Cybersicurezza Nazionale.
Il progetto integrato Cyber Security dei Sistemi Energetici individua tre principali obiettivi prioritari per la trasformazione digitale dei sistemi energetici: i) garantire la sicurezza delle nuove tecnologie per le comunicazioni energetiche, ii) preservare la resilienza del sistema elettrico a fronte di attacchi cyber e iii) sfruttare le potenzialità delle tecnologie big data e intelligenza artificiale per sostenere la cybersecurity delle infrastrutture energetiche.
Le attività di ricerca del progetto hanno la capacità di coinvolgere diversi dipartimenti di ingegneria e informatica degli atenei italiani che hanno avviato progetti sul tema. Tra le categorie di industrie e imprese collegate agli sviluppi del progetto si annoverano, oltre ad operatori di infrastrutture e servizi energetici, anche fornitori di dispositivi OT, integratori di sistemi e fornitori di servizi di comunicazione e piattaforme digitali.
Le ricadute industriali degli output del progetto costituiranno un supporto per gli operatori di infrastrutture energetiche che implementano standard di cybersecurity, architetture IoT e reti locali 5G.
Gli sviluppi del progetto favoriranno anche le sperimentazioni delle funzioni di flessibilità erogabili dalle Infrastrutture di Ricarica per Veicoli Elettrici.
I risultati saranno fruibili da fornitori, enti di certificazione e laboratori di test quali il CVCN (Centro di Valutazione e Certificazione Nazionale) per le verifiche di conformità agli standard di cybersecurity dei prodotti commerciali.
Per quanto riguarda le ricadute normative, gli output del progetto saranno di supporto per la regolazione sulla osservabilità e controllabilità delle reti in bassa tensione, e per la standardizzazione nelle nuove tecnologie in funzione dei requisiti delle applicazioni energetiche.

b) Principali risultati attesi/deliverable

I principali risultati attesi dal progetto di ricerca sono, di seguito, sinteticamente raggruppati per obiettivo prioritario e tipologia.

Cybersecurity delle comunicazioni

Le attività finalizzate al miglioramento della cybersecurity delle comunicazioni produrranno Rapporti Tecnici, Protocolli e Piattaforme relativi a:

• Standard di cybersecurity per protocolli OT e relative valutazioni di impatto sulle prestazioni delle comunicazioni
• Architetture decentralizzate per l'autenticazione di dispositivi basata su Blockchain
• Protocolli quantistici di autenticazione e cyber difesa per reti/micro-reti elettriche
• Algoritmi di cifratura e autenticazione
• Valutazioni delle comunicazioni basate su tecnologia PLC in applicazioni di controllo di generatori distribuiti e sistemi di accumulo
• Osservatorio online per la condivisione di informazioni sulla cybersecurity dei sistemi energetici.

Cybersecurity e resilienza delle infrastrutture cyber-fisiche a fronte di cyber attacchi

Le attività finalizzate a preservare la resilienza dei sistemi energetici a fronte di attacchi cyber produrranno Rapporti Tecnici, Prototipi e Piattaforme relativi a:
• Schemi e dispositivi di protezione elettrica per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche
• Metodologie e Piattaforme per valutazioni di conformità di cybersecurity per dispositivi di controllo e comunicazione utilizzati in infrastrutture energetiche
• Metodologie e test di cybersecurity per reti di comunicazione 5G utilizzate in Test Facility energetiche
• Procedure di autorizzazione per un'architettura sicura di monitoraggio e controllo distribuito che integri sistemi di generazione, accumulo di energia e produzione di idrogeno
• Metodologie e strumenti per il calcolo del rischio dinamico basato su analisi automatica di vulnerabilità e modelli di monitoring di rete
• Modelli di digital twins per simulazioni di attacchi alle smart grids e analisi di resilienza.

Applicazioni di Intelligenza Artificiale per la cybersecurity dei sistemi energetici

Le attività finalizzate all'utilizzo di tecnologie big data e intelligenza artificiale per migliorare le capacità di risposta e difesa da attacchi cyber produrranno Rapporti Tecnici, Piattaforme, Infrastrutture e componenti Software relativi a:
• Metodi e modelli di apprendimento automatico per l'analisi e il rilevamento di anomalie in infrastrutture energetiche
• Dataset per sviluppo e test di algoritmi di anomaly detection
• Sistemi di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori e relative validazioni
• Metodologie e piattaforme di analisi di eventi e misure per il rilevamento di attacchi cyber a reti, micro-reti e applicazioni energetiche, che integrano modelli e algoritmi di AI, architetture di stream analytics, sistemi di raccolta, conservazione e analisi di flussi di dati OT
• Strumenti per il rilevamento automatico di vulnerabilità di cybersecurity di dispositivi di controllo connessi in internet
• Strumenti per la privacy dei dati di applicazioni energetiche, quali i sistemi per la ricarica di veicoli elettrici
• Infrastrutture di calcolo a basso consumo HPC per reti cyber-resilienti e relativi risultati sperimentali.

Diffusione

Le attività di diffusione produrranno Rapporti Tecnici, Pubblicazioni scientifiche, video, notizie ed eventi che permetteranno di raggiungere i potenziali utilizzatori dei risultati del progetto, sia del comparto ricerca che industriale.

Tutti i risultati sopra descritti contribuiranno al raggiungimento degli obiettivi di progetto e all'avanzamento rispetto allo stato dell'arte, come descritto nella sezione 2.4c.
La quantificazione delle prestazioni dei risultati non può essere stimata, a priori, rispetto a studi preesistenti data l'innovatività della tematica e l'assenza di dati di riferimento.
Il raggiungimento degli obiettivi di progetto sarà valutato e misurato mediante la predisposizione di opportuni indicatori in grado di valutare l'incremento di obiettivo dovuto ai protocolli, ai dispositivi, alle piattaforme e agli strumenti sviluppati nel progetto e di fornire un riscontro della bontà delle soluzioni proposte e una misura dell'avanzamento del progetto rispetto allo stato dell'arte.

I singoli risultati sono riportati nella Tabella della sezione 4 del PTR. Nella descrizione delle attività e nella Tabella della sezione 4 ogni Deliverable è identificato da un codice specifico secondo il metodo di codifica (simile ma non identico in quanto riflette la codifica prodotti utilizzata internamente da ciascun affidatario), illustrato nel seguito.

Codifica prodotti RSE
Rapporti Tecnici: RT-2.1-x.y-n_RSE
Piattaforme: PTF-2.1-x.y-n_RSE
dove:
x è il numero di WP
y è il numero progressivo di LA del WP

n è il numero progressivo di Deliverable della LA
Esempi: RT-2.1-1.5-1_RSE; SW-2.1-1.5-2_RSE

Codifica prodotti ENEA
Rapporti Tecnici: RT_LAx.y_ENEA_N
Protocolli: PRC_LAx.y_ENEA_N
Prototipi: PRT_LAx.y_ENEA_N
Infrastrutture: INF_LAx.y_ENEA_N
Piattaforme: PTF_LAx.y_N
Componenti software: SW_LAx.y_ENEA_N
dove:
x è il numero di WP
y è il numero progressivo di LA del WP
N la lettera maiuscola che identifica il Deliverable della LA
Esempi: RT_LA1.2_ENEA_A; PRC_LA1.7_ENEA_A; PRT_LA2.7_ENEA_A; INF_LA3.4_ENEA_A; PTF_LA3.7_ENEA_A; SW_LA3.13_ENEA_A

Codifica prodotti CNR
Rapporti Tecnici: RTx.y.n
Software: SWx.y.n
x è il numero di WP
y è il numero progressivo di LA del WP
n è il numero progressivo di Deliverable della LA
Esempi: RT1.3.1; SW3.14.2

2.6 Fattibilità tecnico-scientifica

a) Fattibilità tecnico-scientifica

Le attività del progetto, per loro natura, richiedono competenze trasversali al fine di applicare conoscenze di dettaglio sulle tecnologie digitali degli ambienti IT (sistemi distribuiti e reti di comunicazione), del contesto OT (sistemi SCADA, dispositivi di campo, applicazioni di protezione, automazione, controllo e gestione dell'energia) e di misure di cybersecurity ad infrastrutture energetiche in evoluzione. Le soluzioni che verranno sviluppate sono pertanto caratterizzate da un elevato grado di complessità funzionale, tecnologica e architetturale. Nel progetto tale complessità è sostenuta dal background maturato da affidatari e co-beneficiari nel corso di esperienze pregresse (vedi progetti riferiti nelle sezioni 2b e 2d) che da altri enti di ricerca che contribuiscono al progetto nell'ambito di appositi accordi e contratti di collaborazione scientifica.
In accordo con gli obiettivi esposti nella sezione 2.5a perseguiti dai tre affidatari RdS (RSE, ENEA e CNR) e dai loro co-beneficiari, i risultati sinteticamente introdotti nella sezione 2.5b saranno ottenuti attraverso quattro Work Package congiunti, per un numero complessivo di 45 Linee di Attività (LA).
Ciascuna LA ha una durata di 18 mesi e rappresenta una milestone del progetto di durata complessiva di 36 mesi. Tale tempistica permette di effettuare uno step di verifica intermedio sull'avanzamento del progetto e delle sinergie tra i risultati di LA collegate.
All'affidatario o al co-beneficiario responsabile della LA spetta il compito di monitorare l'avanzamento delle attività per garantire il raggiungimento dei risultati entro la fine della LA.
Durante lo svolgimento del progetto RSE, in qualità di coordinatore del progetto integrato, stabilirà interazioni e organizzerà incontri tra affidatari e co-beneficiari, calendarizzati in funzione dello svolgimento e delle esigenze del progetto (indicativamente su base semestrale), finalizzati a:
- verificare lo stato di avanzamento delle attività e il raggiungimento dei risultati attesi;
- identificare sinergie e collegamenti tra le attività;
- analizzare eventuali criticità emerse ed individuare azioni correttive;
- coordinare i contributi per la presentazione del piano di lavoro e dei risultati (ammissibilità, SAL I e SAL II);
- organizzare azioni di diffusione congiunte.
Le attività di diffusione prevedranno sia azioni di formazione e disseminazione tecnico-scientifica, sia partecipazioni e supporto ai tavoli tecnici istituiti dagli enti di normazione nazionali ed internazionali.
I prodotti della ricerca saranno testati nei laboratori e nelle infrastrutture di ricerca dei rispettivi affidatari, arricchendo il patrimonio di competenze e delle risorse disponibili per valutazioni e sperimentazioni di cybersecurity dei sistemi energetici.
I risultati delle attività verranno resi disponibili in rapporti tecnici e prodotti di ricerca che saranno accessibili tramite i siti web dei

rispettivi affidatari, in modo da renderli fruibili da un vasto pubblico.
I prodotti progettati e sviluppati dagli affidatari (metodologie, strumenti, piattaforme, prototipi), finalizzati al superamento dello stato dell'arte, costituiranno soluzioni innovative con funzionalità cruciali per gli scenari energetici futuri.
I benefici del progetto derivano dalle numerose ricadute sulla maturità di cybersecurity dei prodotti di mercato, del comparto industriale e della ricerca applicata ai sistemi energetici. Tali benefici contribuiranno al buon funzionamento delle infrastrutture energetiche e, considerata la rilevanza dei servizi energetici per tutti i servizi essenziali all'economia e ai cittadini, allo sviluppo socioeconomico del Paese.

2.7 Impatto sul sistema energetico e benefici attesi

a) Impatto e benefici sul sistema energetico

Gli sviluppi del progetto non hanno nessun impatto diretto sull'ambiente. Tuttavia, l'evoluzione delle reti elettriche verso sistemi energetici avanzati basati su apparati intelligenti è un prerequisito fondamentale della transizione energetica. La possibilità di integrare quote rilevanti di fonti energetiche di tipo rinnovabile nelle reti richiede, infatti, l'impiego di tecnologie abilitanti che applichino logiche di gestione, monitoraggio e comunicazione di tipo innovativo per l'esercizio dei sistemi energetici. Basate su architetture complesse che mettono in comunicazione apparati di diversa natura e funzionalità, tali tecnologie abilitanti introducono vulnerabilità che, se non opportunamente gestite, possono compromettere il livello di sicurezza del sistema energetico.
Le attività del progetto Cybersecurity mirano allo sviluppo di prodotti di ricerca hardware e software funzionali alla connessione di sistemi decarbonizzati e non inquinanti attraverso soluzioni cyber-resilienti.
Indirettamente le soluzioni di cybersecurity sviluppate nel progetto, in quanto parte integrante della componente smart delle infrastrutture energetiche previste dagli obiettivi del PNIEC, abilitano e contribuiscono ai miglioramenti ambientali derivanti, ad esempio, dalla gestione integrata di risorse energetiche rinnovabili, infrastrutture di ricarica di veicoli elettrici e carichi flessibili.

b) Benefici per gli utenti

Lo sviluppo di tecnologie abilitanti cyber-resilienti, agevolando l'integrazione di quote crescenti di fonti rinnovabili nelle reti, l'efficienza energetica, la sicurezza energetica e il mercato interno, favorisce la transizione energetica, con ricadute positive nel medio e lungo termine sull'economia e la salute degli utenti dei sistemi energetici.
Innanzitutto, i benefici per gli utenti sono una diretta conseguenza della riduzione dei rischi di malfunzionamento del sistema energetico dovuta all'applicazione di misure di cybersecurity. Come richiamato nella sezione 2.7a, in assenza di tecnologie cyber-resilienti, gli utenti potrebbero vedere compromesso l'attuale livello di continuità del servizio elettrico a seguito di attacchi informatici.
Le misure di sicurezza indirizzate dal progetto consentono di proteggere i sistemi dagli attacchi cyber, sia attraverso soluzioni preventive che difensive.
Ad esempio, piattaforme avanzate di anomaly detection, che rilevano tempestivamente la presenza di minacce cyber, consentono di evitare che il processo di attacco si propaghi sul sistema energetico, riducendo la possibilità di interruzioni del servizio agli utenti.
Soluzioni di gestione del sistema basate su logiche di riconfigurazione dinamica delle reti in risposta ad attacchi cyber consentono di preservare la sicurezza della rete, producendo così un beneficio al servizio degli utenti. La disponibilità di piattaforme Big Data cyber-resilienti è fondamentale per incrementare l'offerta di servizi energetici avanzati agli utenti finali, che potranno così beneficiare di un livello di servizio più elevato e/o di vantaggi economici.

c) Previsione delle ricadute applicative

Gli output della ricerca agevolano lo sviluppo della filiera industriale della componentistica elettronica, dei dispositivi di controllo e ICT.
In relazione al primo settore, il trasferimento alla filiera produttiva delle specifiche del prototipo di protezione progettato nel progetto, di cui saranno forniti i requisiti tecnici attraverso il rapporto tecnico e gli articoli di disseminazione, produrrà benefici per gli operatori dei sistemi di protezione, con potenziali ricadute positive per la relativa filiera. La caratterizzazione del prototipo a livello sperimentale, inoltre, fornirà ai potenziali produttori di questi dispositivi informazioni circa la validità della soluzione proposta, facilitando l'analisi costi-benefici connessa ad una eventuale industrializzazione del prodotto.
Le piattaforme di valutazione delle funzioni di cybersecurity hanno una ricaduta sulla disponibilità di dispositivi di controllo conformi a standard di cybersecurity, favorendo lo sviluppo di applicazioni che integrano tali dispositivi nelle infrastrutture energetiche previste dai nuovi mercati, locali e globali, basate sull'aggregazione di risorse flessibili distribuite.
Gli sviluppi di soluzioni avanzate di protezione e rilevamento di anomalie cyber hanno una ricaduta sugli sviluppi dei relativi standard di prodotto e piattaforme di mercato.

Un'altra ricaduta delle attività del progetto riguarda le competenze utili ai fini degli sviluppi normativi e regolatori in tema di cybersecurity dei sistemi energetici. La partecipazione ai gruppi di lavoro incaricati degli sviluppi normativi coinvolge una platea eterogenea di esperti, interessati a vario titolo agli sviluppi di cybersecurity, quali Autorità di Regolazione, comitati di standardizzazione internazionali e nazionali, operatori di rete (Terna e DSO), operatori di infrastrutture di ricarica, aggregatori, produttori di dispositivi, fornitori di servizi di comunicazione e di cybersecurity, laboratori di test e certificazione.

Non si riscontrano benefici economico-finanziari diretti per gli enti di ricerca proponenti derivanti dalle ricerche del progetto. L'incremento di competenze acquisite da affidatari e co-beneficiari aumenteranno le loro possibilità di accesso a finanziamenti di ricerca futuri su temi affini.

2.8 Verifica dell'esito del progetto

a) Oggetti e documentazione dei risultati finali

La verifica dell'esito del progetto sarà basata sui deliverable indicati nella Tabella riassuntiva della sezione 4, che includono Rapporti Tecnici, Protocolli, Prototipi, Piattaforme e Infrastrutture. E' di seguito sintetizzata la distribuzione per WP dei 71 prodotti complessivi del progetto:

- WP1: 17 Rapporti Tecnici, 1 Protocollo, 2 Piattaforme;
- WP2: 13 Rapporti Tecnici, 1 Prototipo, 2 Piattaforme;
- WP3: 21 Rapporti Tecnici, 1 Prototipo, 3 Piattaforme; 1 Infrastruttura, 2 Software;
- WP4: 6 Rapporti Tecnici.

Per la valutazione della qualità dei Rapporti Tecnici ci si potrà avvalere di opportuni indicatori. A titolo esemplificativo, nel seguito vengono indicati alcuni indicatori di qualità ritenuti significativi.

- Rispondenza dei contenuti alle attività previste nel PTR;
- Qualità del percorso logico della ricerca;
- Qualità dell'inquadramento del contesto;
- Qualità della descrizione dell'attività svolta;
- Grado di efficacia comunicativa;
- Rilevanza delle pubblicazioni effettuate.

La verifica di protocolli, prototipi, piattaforme e infrastrutture potrà avvalersi dei risultati delle valutazioni e dei test effettuati descritti nei relativi rapporti, o della loro presa visione presso le sedi degli affidatari.

Relativamente alle metriche e alle misurazioni dei singoli risultati si rimanda agli elementi di verifica inclusi nella Tabella della sezione 4.