10/2019 Cybersecurity nella transizione energetica e digitale

DOSSIER

Digitalizzazione della filiera energetica, fonti rinnovabili e prosumer

La sicurezza energetica è vitale per il buon funzionamento delle società e delle economie moderne, sottolinea la IEA - Agenzia Internazionale dell'Energia. Le tecnologie energetiche sono sempre più connesse alle reti digitali. Questa crescente digitalizzazione rende il sistema energetico più intelligente, garantendo benefici agli operatori e agli utilizzatori in termini di servizi energetici innovativi ed efficienti.

Al tempo stesso, segnala la Commissione Europea, la digitalizzazione crea rischi significativi, in quanto una maggiore esposizione a minacce cyber mina la sicurezza dell'approvvigionamento energetico e la riservatezza dei dati degli utenti.

Che gli operatori energetici siano vulnerabili e subiscano i danni causati dagli attacchi informatici ormai è un rischio accertato. Il rapporto "Cyber challenges to the energy transition" del World Energy Council [1] stima che i gruppi legati alla criminalità informatica identificati come attaccanti delle società di energia sia in continua crescita, con numeri raddoppiati nell'arco di quattro anni (Figura 1).

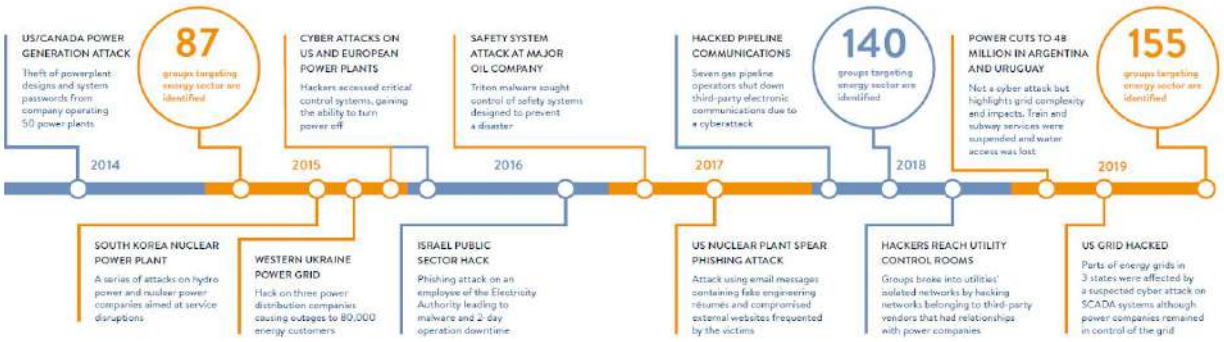

Figura 1: Gli incidenti informatici aumentano sia in frequenza che in impatto [1]

Tra i casi realmente accaduti, il blackout avvenuto a Dicembre 2015 in Ucraina che ha coinvolto tre società di distribuzione, provocando il distacco di 27 stazioni elettriche disalimentando 230.000 utenze per diverse ore, ha segnato la storia del crimine informatico verso le utility elettriche. Come evidenziato dall'analisi dei casi di attacco reale (Figura 2), l'azione malevola verso i sistemi OT (Operational Technology) spesso

viene veicolata da un'intrusione iniziale in una rete informatica aziendale e, attraverso le connessioni di rete, si sviluppano nell'infrastruttura di controllo del sistema elettrico.

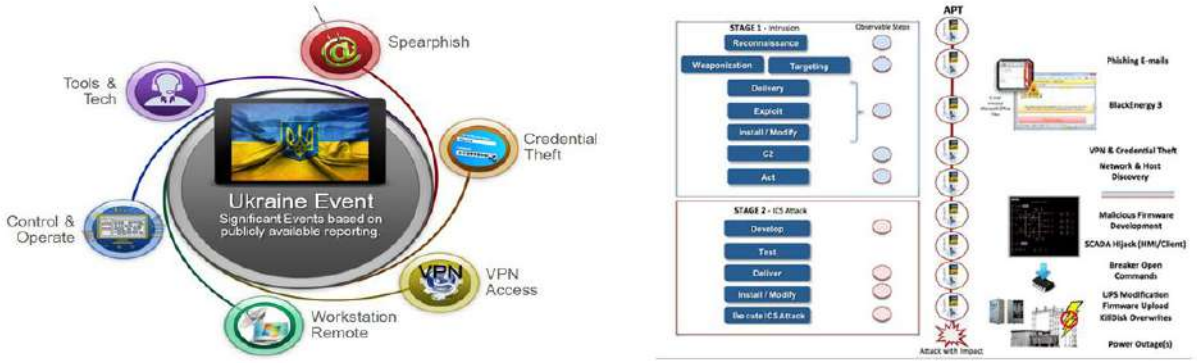

Figura 2: Attacco alla rete elettrica Ucraina [2]

I rischi da affrontare sono sostanzialmente legati al processo di digitalizzazione delle infrastrutture, richiesto dalla transizione energetica che caratterizzerà il prossimo decennio. Ci riferiamo, in particolare, ai sistemi riguardanti l'esercizio degli impianti, come le stazioni elettriche o gli impianti di generazione e di carico che comprendono impianti di grossa taglia e risorse energetiche distribuite connesse in media e bassa tensione, in particolare risorse di generazione da fonti rinnovabili, infrastrutture di ricarica e di accumulo dei veicoli elettrici caratterizzate da un profilo elettrico impredicibile dovuto alla mobilità dei veicoli, sistemi di gestione flessibile della domanda o che forniscono servizi ancillari all'operatore di rete, funzionali alla gestione in sicurezza di un sistema energetico sostenibile.

I big player concordano sul fatto che la cybersecurity è una dimensione irrinunciabile per il business dell'energia e il welfare della nazione, che necessita cooperazione tra operatori energetici, fornitori di prodotti e di servizi digitali. Per i grandi operatori il metodo è tracciato: occorre procedere con la classificazione degli asset, la scelta delle misure di sicurezza organizzative e tecniche commisurate al livello di rischio, le richieste di conformità agli standard di cybersecurity e di certificazione verso i fornitori di prodotti e servizi.

In un mercato energetico in evoluzione la cybersecurity diventa normativa

A livello istituzionale, la Strategia Energetica Nazionale (SEN) [3] fa riferimento allo schema nazionale di cybersecurity, partendo dal Decreto della Presidenza del Consiglio dei Ministri (DPCM Gentiloni del 17 febbraio 2017) che ne definisce l'architettura e i ruoli delle istituzioni preposte alla sua implementazione in collaborazione con i fornitori dei servizi essenziali. Il Decreto Gentiloni ha anche promosso la costituzione di un Centro di Valutazione e Certificazione Nazionale (CVCN) per la verifica dell'affidabilità della componentistica ICT utilizzata nelle infrastrutture critiche e strategiche, e affidato la gestione del Centro al Ministero dello Sviluppo Economico.

In tema di regolamentazione di cybersecurity per il settore energia un primo riferimento è il decreto-legge n. 65, entrato in vigore il 24 Giugno 2018, il quale

costituisce l'attuazione italiana della Direttiva europea NIS (EU 2016/1148) sulla sicurezza delle reti e dei sistemi digitali, praticamente gemella del regolamento GDPR (EU 2016/679) sulla protezione dei dati sensibili, la cui entrata in vigore non è certamente passata inosservata a nessuno di noi. Un primo fondamentale provvedimento stabilito dal decreto n.65 è relativo all'identificazione degli operatori classificati come fornitori di servizi essenziali, quali quelli energetici, soggetti agli obblighi in materia di sicurezza e notifica degli incidenti indicati dall'Art. 14, e alle relative sanzioni amministrative in caso di inadempienza di cui all' Art. 21. Il decreto stabilisce che tali obblighi non si applicano alle micro imprese e alle piccole imprese che in base alla definizione contenuta nella raccomandazione della Commissione europea n.2003/361/CE, sono tutte quelle imprese che occupano meno di 50 persone e realizzano un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di euro.

Il più recente decreto-legge n. 105, approvato il 21 Settembre 2019 dal Consiglio dei Ministri, modificato e convertito dal decreto per la legge di conversione n.133 entrato in vigore il 21 Novembre 2019, introduce disposizioni urgenti in materia di "*perimetro di sicurezza nazionale cibernetica*". Esso riguarda tutte le infrastrutture critiche, private e pubbliche aventi una sede nel territorio nazionale, che assicurano un servizio essenziale per le attività civili, sociali o economiche fondamentali per la nazione, e che per la fornitura di tale servizio si avvalgono di reti, sistemi informativi e servizi informatici dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.
Secondo quanto stabilito dall' Art.1, entro quattro mesi dall'entrata in vigore della legge di conversione è richiesta l'individuazione delle amministrazioni, degli enti e degli operatori inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto degli obblighi stabiliti dalla legge.
Entro dieci mesi dall'entrata in vigore della legge di conversione il Ministero dello Sviluppo Economico definisce le procedure che i soggetti privati del settore energia devono seguire per la notifica degli incidenti cyber al gruppo di intervento per la sicurezza informatica (CSIRT) già prevista dal D.L. n.65. Vengono, inoltre, stabilite le misure organizzative, di gestione del rischio e di mitigazione e gestione degli incidenti che garantiscono elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici tenendo conto degli standard definiti a livello internazionale ed europeo.
I soggetti individuati che intendono approvvigionarsi di beni, sistemi e servizi ICT devono darne comunicazione al CVCN, unitamente alla valutazione del rischio associato all'oggetto della fornitura in relazione all'ambito di impiego. Entro al massimo sessanta giorni dalla comunicazione, il CVCN può effettuare verifiche preliminari e imporre condizioni e test di hardware e software da effettuare in collaborazione con i soggetti individuati secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Tali condizioni e test di hardware e software condizionano i relativi bandi di gara e contratti al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. L'onere dell'effettuazione delle attività di test risulta a carico dei soggetti inclusi nel perimetro di sicurezza nazionale.
In particolare il CVCN assume il compito di elaborare le misure di sicurezza che riguardano l'affidamento di forniture di beni, sistemi e servizi ICT, definisce le metodologie di verifica e di test, effettua le verifiche avvalendosi di laboratori

accreditati dallo stesso CVCN e, se necessario, elabora ed adotta nuovi schemi di certificazione cibernetica tenendo conto degli standard definiti a livello internazionale ed europeo[1].
Il mancato adempimento da parte dei soggetti inclusi nel perimetro degli obblighi previsti dalla legge comporta sanzioni amministrative e pecuniarie fino a 1 milione e 800 mila euro.

Quali sono gli standard di cyber security di riferimento?

La strategia di sicurezza informatica a livello nazionale utilizza il NIST Cybersecurity Framework [4] come riferimento per definire le misure di resilienza dei sistemi cyber-fisici. Il framework enumera un elenco di requisiti per identificare, proteggere, rilevare, rispondere e recuperare gli effetti delle minacce informatiche all'interno di un'organizzazione che opera in un'infrastruttura critica.
Per guidare gli operatori energetici nell'attuazione della loro strategia di resilienza informatica, la Task Force sulla sicurezza informatica del comitato di sistema IEC Smart Energy ha selezionato una serie di standard internazionali che si applicano agli ambienti operativi smart energy.

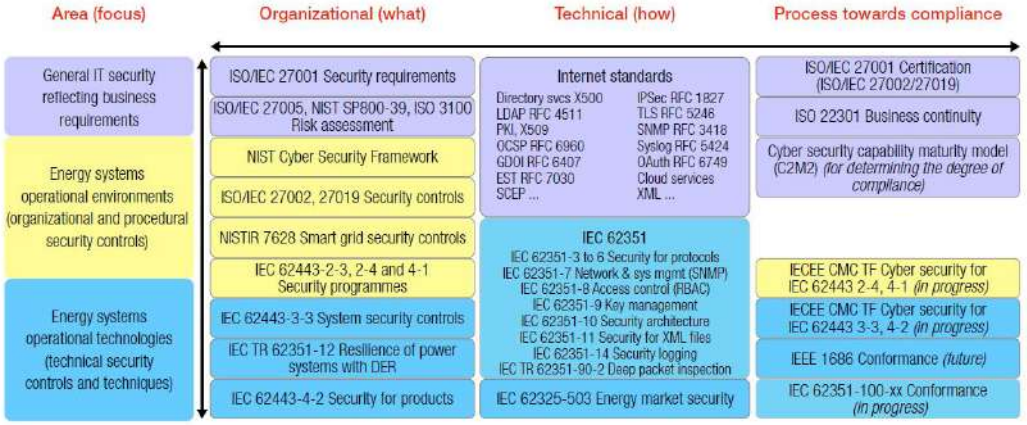

Figura 3: cyber security standards e guidelines [5]

Come si può notare dalla serie di standard riferiti in Figura 3, controlli di sicurezza di tipo organizzativo devono essere combinati con controlli tecnici implementati sia a livello di sistema, sia a livello di prodotto da integratori di sistemi e produttori di dispositivi. Ogniqualvolta possibile la specifica della serie di standard IEC 62351 (terza colonna in Figura 3) riferisce gli standard Internet esistenti, specificando dei profili adeguati ai vincoli di disponibilità, integrità e confidenzialità dell'ambiente operativo energetico. Un esempio tra tutti è rappresentato dallo standard IEC 62351-3, il quale utilizza lo standard TLS (Transport Layer Security) sviluppato da IETF per definire il profilo da utilizzare per l'implementazione di un livello di trasporto sicuro in tutti i protocolli di scambio dati energetici, basati su TCP/IP. Ciò dimostra la convergenza delle tecnologie IT (Information Technology) e OT (Operational Technology) e la necessità di renderle interoperabili, un problema ancora più rilevante in futuro, con

[1] Il 27 giugno 2019 è entrato in vigore il regolamento europeo EU 2019/881 noto come Cyber Security Act, che stabilisce il nuovo mandato dell'ENISA, l'agenzia europea per la cyber security, per la definizione del quadro europeo di certificazione della cyber sicurezza.

l'utilizzo di piattaforme aperte basate su tecnologie IoT (Internet of Things) e servizi edge e cloud.

Di riferimento per gli schemi di certificazione della sicurezza per i sistemi energetici è la serie di standard IEC 62443 (quarta colonna in Figura 1) e i relativi programmi di valutazione della conformità offerti da enti quali IECEE, i quali forniscono certificati di conformità ad integratori di sistemi e sviluppatori di prodotti, secondo gli schemi indicati nel rapporto del rapporto dell'Expert Group 2 della Smart Grid Task Force [6].

Per i servizi di connettività e di certificato digitale utilizzati dai sistemi energetici, Expert Group 2 raccomanda di applicare uno schema di certificazione basato sulla serie ISO/IEC 27000.

Secondo le buone pratiche raccomandate da standard e linee guida, i requisiti di sicurezza per autenticazione, autorizzazione, integrità e tracciabilità si basano principalmente su algoritmi crittografici e richiedono sistemi di gestione di chiavi e certificati elettronici, mentre i requisiti di disponibilità sono principalmente gestiti mediante tecniche di segregazione delle reti, sistemi di analisi del traffico (firewall), protezioni antivirus e tecniche di ingegneria dei sistemi per la gestione della ridondanza. Complementari alle misure di prevenzione della sicurezza, sono le pratiche di monitoraggio della sicurezza basate sull'utilizzo di sistemi IDS per il rilevamento delle intrusioni e di sistemi SIEM per la gestione degli eventi di sicurezza.

Il futuro che ci attende

Quali e quanti produttori di energia, prosumer o aggregatori rientreranno nella categoria piccola impresa esente dagli obblighi di cybersecurity imposti dal D.L. n.65? Ma soprattutto, che impatto provocherebbe un eventuale incidente cyber in termini di megawatt non forniti al sistema elettrico o di carico non assorbito? Quanti e quali utenti subirebbero un disservizio prolungato a causa di un attacco sufficientemente distribuito in termini di superficie cyber?

Riguardo alla possibilità che questi sistemi subiscano gli effetti di un attacco cyber, se guardiamo alla casistica delle vulnerabilità note possiamo rilevare dati inquietanti: i risultati estraibili dai motori di ricerca rilevano che diversi impianti sono piuttosto esposti, visibili e controllabili da Internet senza alcun grado di protezione. La strada per l'attaccante è praticamente tracciata (Figura 4).

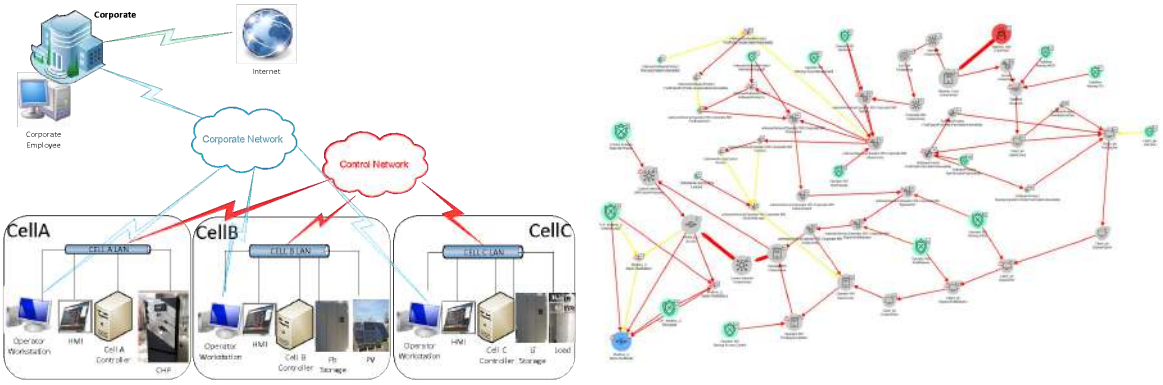

Figura 4: percorsi di attacco alle celle di una microrete [7]

Si ravvisa una disparità di livello di sicurezza tra i sistemi di controllo dell'infrastruttura elettrica e quelli degli impianti di potenziali fornitori di servizi di flessibilità. E' più che plausibile supporre che il livello di maturità in termini di sicurezza cyber degli impianti attuali sia inferiore al livello medio utilizzato per la gestione dei rischi cyber dagli operatori di rete.

Il rapporto dell' Expert Group 2 [6] pone un'attenzione specifica alla cybersecurity di tutti gli operatori energetici, indipendente dalla loro potenza installata e capacità.
L'Autorità per l'energia ARERA, attualmente impegnata nella definizione della normazione per l'implementazione del Regolamento Europeo 2017/1485 (Guideline on Electricity Transmission System Operation) relativo agli scambi informativi tra operatori di trasmissione, di distribuzione e utenti di rete significativi, riconosce la necessità di includere nel regolamento i requisiti di sicurezza cyber, da applicare anche per l'adeguamento dei 3000 impianti di generazione di potenza superiore al megawatt già connessi alla rete in media tensione.
Il riferimento per l'adeguamento di questi impianti e la connessione di quelli nuovi previsti dal PNIEC [8] è rappresentato dalla norma italiana CEI 0-16 [9], pubblicata ad Aprile 2019, che definisce le regole tecniche per la connessione di utenti attivi alle reti in alta e media tensione. Tale norma dovrà essere estesa al fine di recepire i requisiti di comunicazione e cyber security previsti dal regolamento per la messa in sicurezza delle comunicazioni tra il controllore dell'impianto e i soggetti esterni che vi possono accedere da remoto.

I contributi della ricerca e gli obiettivi futuri

La stessa SEN [3] nel capitolo dedicato alla cyber security sottolinea la necessità di svolgere attività di ricerca e sviluppo, riferendo il programma di ricerca RSE, finanziato dal fondo della Ricerca di Sistema (RdS) e finalizzato a produrre strumenti di valutazione dei rischi e misure di sicurezza idonee all'esercizio di sistemi energetici eterogenei sia dal punto di vista elettrico che digitale [10] (Figura 5).

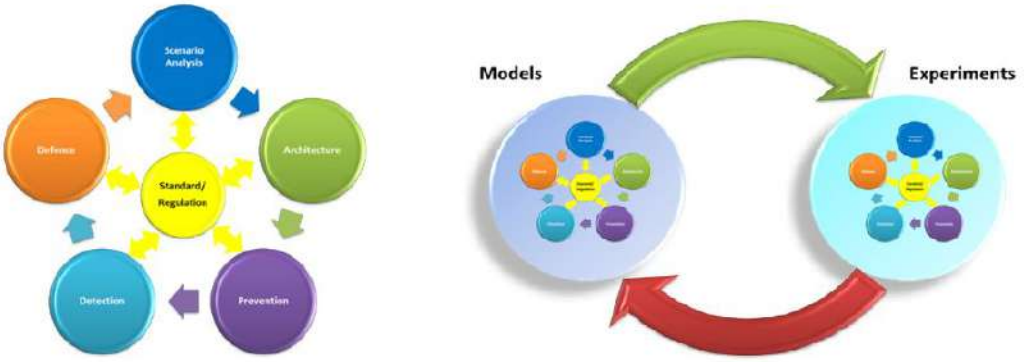

Figura 5 - Il framework di analisi della resilienza dei sistemi cyber-fisici

Il piano RdS di RSE affronta aspetti di cyber security negli scenari energetici futuri, che comprendono impianti di generazione da fonti rinnovabili, aggregatori, prosumer, valutando la resilienza dei nuovi schemi di controllo, l'integrazione di nuove tecnologie e standard di cyber security per fornire una risposta adeguata ad eventuali nuove minacce (Figura 6).

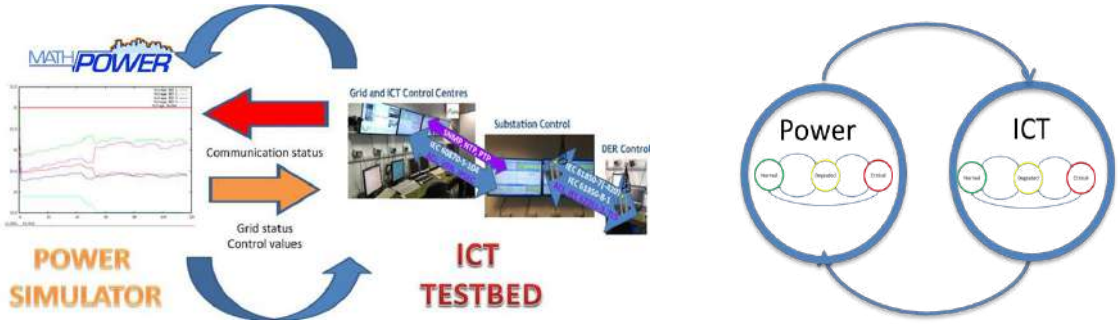

Figura 6 - Scenari di resilienza cyber-power

Gli asset della ricerca includono:

- strumenti per la specifica e la valutazione della sicurezza informatica [11] (Figura 7)

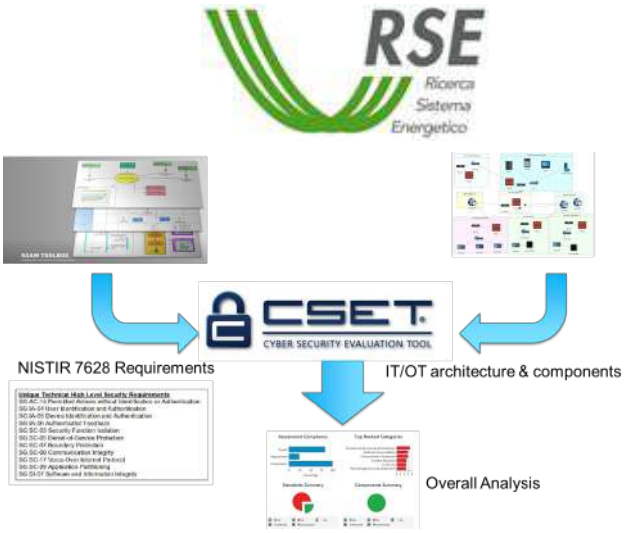

Figura 7 - Valutazione dei requisiti di sicurezza

- piattaforme sperimentali IT/OT/IoT per la sicurezza end-to-end delle comunicazioni su tecnologie di rete eterogenee [12], [13], [14] (Figura 8 e Figura 9) e di nuova generazione come il 5G

Figura 8 - Laboratorio RSE PCS-ResTest (Power Control Systems – Resilience Testing)

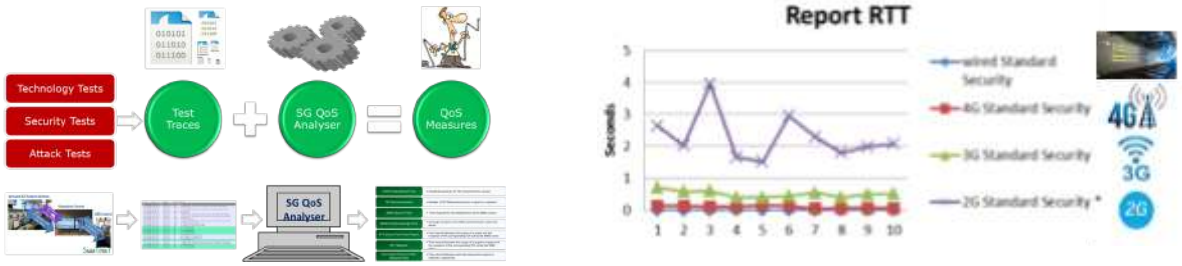

Figura 9 - Valutazioni prestazionali della sicurezza end-to-end

- sistemi di monitoraggio della sicurezza in tempo reale e rilevamento delle anomalie [15], funzioni di recovery integrate in scenari di controllo elettrico [16]. Relativamente al riconoscimento tempestivo di anomalie cyber, sono in corso di sviluppo modelli di simulazione e piattaforme evolute di raccolta e analisi di dati basate sull'applicazione di tecniche di machine e deep learning (Figura 10).

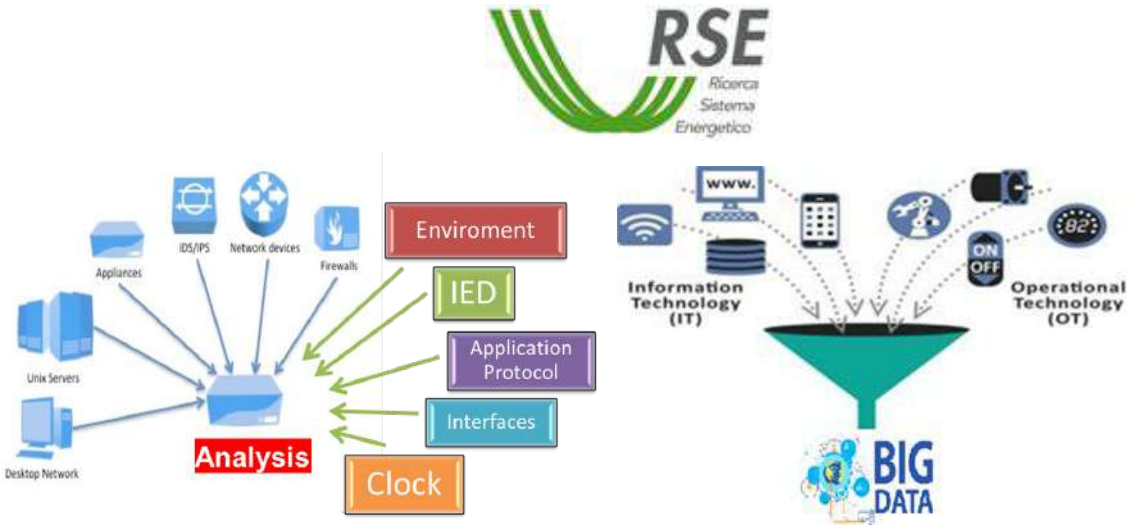

Figura 10 - Raccolta e analisi di dati e eventi di sicurezza

Gli strumenti e i risultati della ricerca sono destinati agli operatori energetici, ai fornitori di servizi digitali e di telecomunicazione (Figura 11), per consentire loro di accelerare il processo di innovazione tecnologica richiesta dalla transizione energetica. Il percorso di collaborazione in atto con le principali imprese nazionali ha reso possibile l'adozione di principi e pratiche derivate dalle analisi e dalla sperimentazione, in un ciclo sinergico tra innovazione industriale e risultati della ricerca, tenendo conto degli opportuni feedback.

Un contributo fondamentale del piano di ricerca è relativo all'evoluzione degli standard per le comunicazioni del settore energetico, proseguendo nell'azione di trasferimento dei risultati sperimentali ai Comitati che sviluppano la normativa tecnica, alla loro implementazione e certificazione in prodotti e soluzioni IT/OT/IoT, competenze di cui si sono avvalsi anche i regolatori dell'energia e i decisori politici a livello europeo e nazionale.

Bibliografia

[1] World Energy Council, "Cyber challenges to the energy transition", 2019

[2] E-ISAC | Analysis of the Cyber Attack on the Ukrainian Power Grid | March 18, 2016

[3] Ministero dello Sviluppo Economico, Strategia Energetica Nazionale, 10 Novembre 2017, https://www.mise.gov.it/images/stories/documenti/Testo-integrale-SEN-2017.pdf
[4] NIST Cybersecurity Framework Version 1.1, Aprile 2018, https://www.nist.gov/cyberframework/framework

[5] IEC Technology Report, "Cyber security and resilience guidelines for the smart energy operational environment", 2019

[6] Smart Grid Task Force-Expert Group 2-Cybersecurity , «Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management,» 2019

[7] R. Terruggia, G. Dondossola, M. Ekstedt, "Cyber security analysis of Web-of-Cells energy architectures", 5th International Symposium for ICS and SCADA Cyber Security Research 2018, Hamburg, August 2018

[8] Ministero dello Sviluppo Economico, Proposta di piano nazionale integrato per l'energia e il clima, 31 Dicembre 2018, https://www.mise.gov.it/images/stories/documenti/Proposta_di_Piano_Nazionale_Integrato_per_Energia_e_il_Clima_Italiano.pdf

[9] Norma CEI 0-16, "Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica", 17 aprile 2019

[10] G. Dondossola, "Cyber Security of Electrical Systems – Italian R&D priorities" Cyber Security Workshop, G7-Energy, Rome, 23 June 2017

[11] R. Terruggia, G. Dondossola, "Cyber security standard and architectural assessment for a new digitalized power infrastructure", CIGRE SC D2 Colloquium 2019, Helsinki 12-13 June 2019

[12] M.G. Todeschini, G. Dondossola, R. Terruggia, "Impact evaluation of IEC 62351 cyber security on IEC 61850 communications performance" CIRED 2019, Madrid 3-6 June 2019

[13] G. Dondossola, R. Terruggia, "Mobile secure communications in smart grid control", 2nd EAI International Conference on Smart Grid Inspired Future Technologies, London (UK), 27-28 March 2017

[14] H-P. Schwefel, G. Dondossola, R. Terruggia et al., "Impact of communication network performance on voltage control and energy balancing", Cigré Science and Engineering, February 2018

[15] G. Dondossola, R. Terruggia, "A monitoring architecture for smart grid cyber security", Cigré Science and Engineering, February 2018

[16] G. Dondossola, R. Terruggia, "Evaluation of Smart Grid Control Scenarios in a Communication Security Platform" International colloquium "building smarter substations" - CIGRÉ Mexican National Committee and Study Committees B3, B5 and D2 – Mexico City , 14-16 November 2016.