RdS
RICERCA DI SISTEMA

ENEA
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Ricerca di Sistema elettrico

Analisi di soluzioni topologiche e predisposizione di un'infrastruttura di test per la validazione di protocolli ed apparati sviluppati per la cybersicurezza (LA1.2)

G. Adinolfi, A. Buonanno, R. Ciavarella, A. Merola, V. Palladino, M. Valenti

RdS_PTR 22-24_PR 2.1_LA1.2_066

ANALISI DI SOLUZIONI TOPOLOGICHE E PREDISPOSIZIONE DI UN'INFRASTRUTTURA DI TEST PER LA VALIDAZIONE DI PROTOCOLLI ED APPARATI SVILUPPATI PER LA CYBERSICUREZZA

G. Adinolfi, A. Buonanno, R. Ciavarella, A. Merola, V. Palladino, M. Valenti (ENEA)

Giugno 2023

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dell'Ambiente e della Sicurezza Energetica - ENEA
Piano Triennale di Realizzazione 2022-2024

Obiettivo: *Digitalizzazione ed evoluzione delle reti*
Progetto: *Progetto Integrato Cyber Security dei sistemi energetici*
Linea di attività: *LA1.2*
Responsabile del Progetto: *Maria Valenti*
Responsabile Linea di Attività: Giovanna Adinolfi
Mese inizio previsto: 1
Mese inizio effettivo: 1
Mese fine previsto: 18
Mese fine effettivo: 18

Indice

1 Risultati attesi

Lista dei risultati attesi come da capitolato vigente

Si riporta di seguito la lista dei risultati attesi come da capitolato vigente:

- Studio di almeno 2 topologie di reti e micro-reti elettriche
- Descrizione di dettaglio (almeno 4 apparati) dell'infrastruttura di ricerca predisposta presso il Laboratorio SGRE del Centro Ricerche ENEA per la conduzione delle attività di test e validazione sperimentali
- Due test di validazione funzionale (apparato e infrastruttura)

2 Risultati ottenuti

Lista dei risultati ottenuti *(Evidenziare in che misura il risultato è stato ottenuto ed il beneficio per il sistema elettrico nazionale e i suoi utenti. Aggiungere eventuali risultati ottenuti non previsti nel capitolato)*

Di seguito è riportato l'elenco dei risultati ottenuti:

- **Studio di almeno 2 topologie di reti e microreti elettriche**
  In una prima fase è stato condotto uno studio della letteratura scientifica finalizzato ad individuare i possibili elementi di vulnerabilità per le reti in funzione dei diversi tipi di attacco e, successivamente, è stata condotta un'analisi degli impatti sulle più comuni topologie delle reti elettriche di distribuzione. I risultati dello studio hanno consentito di identificare le topologie di interesse per la sperimentazione da condurre nelle LA1.6 e LA2.7.
- **Descrizione di dettaglio (almeno 4 apparati) dell'infrastruttura di ricerca predisposta presso il Laboratorio SGRE del Centro Ricerche ENEA per la conduzione delle attività di test e validazione sperimentali**
  Per validare sperimentalmente le topologie di rete individuate e gli apparati di progetto, si è proceduto alla progettazione di un'infrastruttura sperimentale presso il Laboratorio Smart Grid e Reti Energetiche (SGRE) del Centro Ricerche ENEA di Portici.
  Sono stati, quindi, definiti i requisiti del sistema di crittografia quantistica di tipo Quantum Key Distribution (QKD) da acquisire e si è proceduto alla predisposizione della documentazione tecnica di gara.
  Infine, sono stati descritti quattro apparati (3 già presenti nella nanogrid di laboratorio ed 1 da acquisire) del testbed sperimentale.
- **Due test di validazione funzionale (apparato e infrastruttura)**
  Per valutare gli impatti di cyber attacchi sul funzionamento dell'infrastruttura precedentemente definita, sono stati elaborati due scenari di test, rappresentativi di condizioni reali: uno scenario è stato definito per valutare l'impatto di un cyber attacco sul funzionamento dell'infrastruttura elettrica, l'altro per analizzare l'impatto di un cyber attacco sul funzionamento a livello di apparato e le relative conseguenze sul funzionamento dell'infrastruttura elettrica.

Le attività condotte hanno portato al pieno raggiungimento dei risultati attesi. Il testbed progettato (che verrà installato nel corso del II SAL) rappresenterà una infrastruttura avanzata per la sperimentazione della cybersecurity dei sistemi energetici su scala nano-, micro- rete e consentirà di sperimentare scenari attualmente sperimentati solo in ambiente di simulazione digitale. Ciò potrà incrementare il TRL della ricerca nel settore con evidenti benefici sia per il sistema energetico sia per i suoi utenti, per i quali la cybersecurity

diventa un tema sempre più rilevante, impattando sulla continuità del servizio e sulla protezione stessa dei dati.

3 Prodotti attesi

Lista dei prodotti hardware/software eventualmente attesi per la LA

Per la presente LA non sono attesi prodotti hardware/software.

4 Prodotti sviluppati

Lista dei prodotti hardware/software eventualmente sviluppati nella LA, illustrando, per il software, le modalità di accesso per gli utenti *(Aggiungere eventuali prodotti sviluppati non previsti nel capitolato)*

La LA1.2 non prevede lo sviluppo di prodotti hardware/software.

5 Analisi degli scostamenti su attività e risultati

(8000 caratteri max)

Descrivere le motivazioni di eventuali scostamenti tecnici/economici rispetto al preventivo e criticità riscontrate (*Evidenziare il contenuto in riferimento al piano di rischi presentato*)

Non si sono registrati scostamenti tecnico e/o economici nell'ambito della LA1.2.

6 Sintesi delle attività svolte

(1000 caratteri max)

Nella LA1.2 sono state svolte le seguenti attività: studio della letteratura di settore e dei documenti relativi alle cyber minacce perpetrate a danno delle infrastrutture energetiche, identificazione di soluzioni topologiche di reti e/o microreti elettriche utilizzabili come architetture test del progetto, progettazione dell'infrastruttura sperimentale da installare presso il Centro Ricerche ENEA di Portici per la predisposizione di un testbed per la conduzione delle attività sperimentali di progetto, definizione di scenari di test rappresentativi di cyber attacchi ad infrastrutture energetiche, predisposizione della documentazione tecnica della gara per l'acquisto di un sistema di crittografia quantistica, definizione di due procedure di test di validazione.

7 Dettaglio delle attività svolte

(15000 caratteri max)

Descrivere in dettaglio le attività svolte nella LA (*Evidenziare come si sono ottenuti i risultati. Descrivere brevemente anche le attività, per le quali si sono spese delle risorse, che tuttavia non hanno portato all'ottenimento dei risultati previsti al fine di permettere la corretta valutazione di congruità e pertinenza dei costi rendicontati.*)

Le attività svolte nella presente LA si sono articolate in diverse fasi, di seguito sinteticamente descritte.

Studio preliminare e individuazione delle topologie architetturali da implementare nelle successive LA sperimentali

In una prima fase è stato condotto uno studio della letteratura scientifica finalizzato ad individuare i possibili elementi di vulnerabilità per le reti in funzione dei diversi tipi di attacco e, successivamente, è stata condotta un'analisi degli impatti sulle più comuni topologie delle reti elettriche di distribuzione.
In generale, la vulnerabilità è definita come un elemento di debolezza del sistema mentre una minaccia come un potenziale danno al sistema stesso. I cyber-aggressori sfruttano le vulnerabilità delle infrastrutture di comunicazione, automazione, monitoraggio e controllo su cui sono basati gli attuali sistemi energetici per attaccare le reti fisiche. In particolare:

- **Infrastruttura di comunicazione**: i moderni sistemi energetici adottano diverse tecnologie di comunicazione (cablata, wireless). Le tecnologie wireless presentano sicuramente una maggiore vulnerabilità rispetto a quelle cablate in termini di potenziali intercettazioni e intrusioni che possono provocare diversi attacchi alla rete fisica (es. intrusioni nel canale di comunicazione tra il gestore di rete e la cabina di rete, intrusioni nel canale di comunicazione gestore di rete-utente).

  In particolare, le funzionalità compromesse possono riguardare: requisiti di riservatezza, gestione della privacy, requisiti di integrità, requisiti di disponibilità, interazione tra componenti e apparati, impossibilità di predire lo stato del sistema e/o delle sue risorse o errata predizione (es. alterazione dei dati).

- **Infrastruttura di automazione, controllo e monitoraggio**: i moderni sistemi energetici sono basati su un utilizzo significativo di dispositivi di automazione, controllo e monitoraggio distribuito (es. PLC, attuatori, misuratori, sensori, sistemi di monitoraggio di tipo informatico, ecc.). Questi, se da un lato facilitano un utilizzo più flessibile della rete e un migliore monitoraggio, dall'altro la rendono più cyber-vulnerabile; ciascun punto di automazione e monitoraggio diventa un potenziale punto di accesso esterno a possibili attacchi cibernetici.

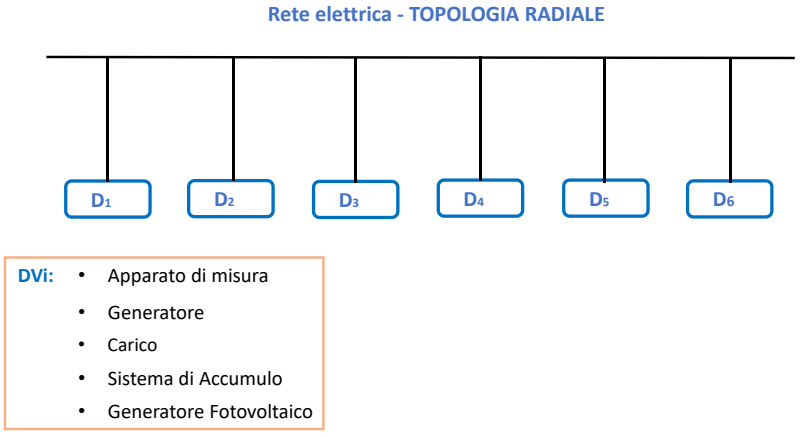
In Tabella 1 sono presentati, per i principali attacchi ai sistemi elettrici, il componente "sotto attacco", la funzionalità compromessa e la possibile azione di mitigazione.

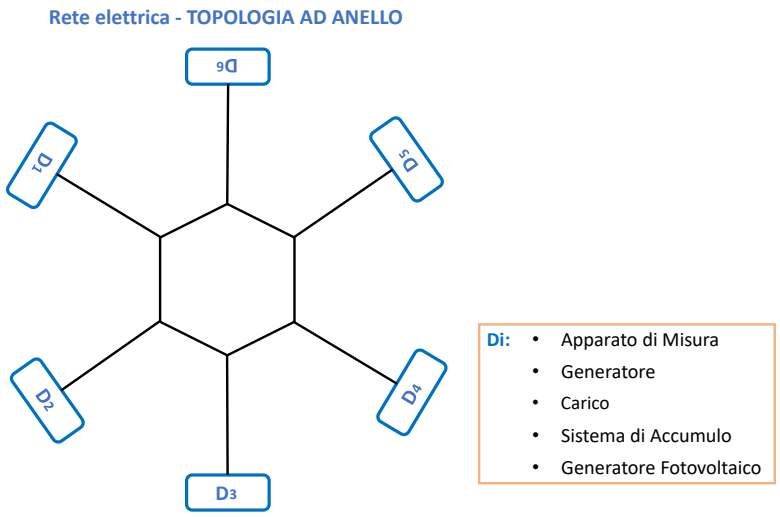
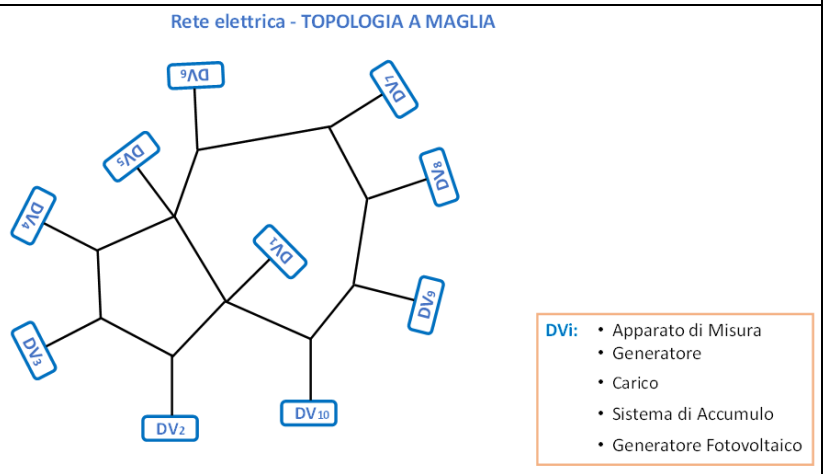
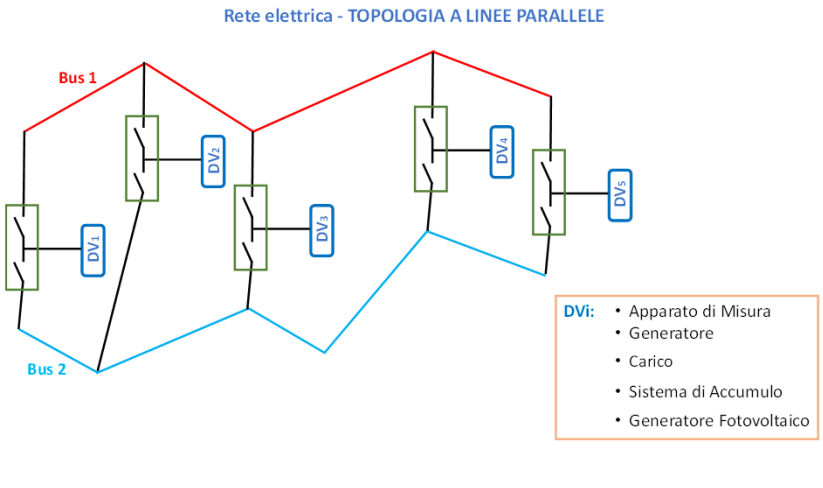
Tabella 1: Cyber attacchi alle microreti elettriche, loro impatto e contromisure.				
Tipo di Attacco	**Categoria dell'attacco**	**Componente sotto attacco**	**Funzionalità compromessa**	**Possibile azione di mitigazione**
INFRASTRUTTURA DI COMUNICAZIONE				
Reconnaissance (Ricognizione)	Analisi del traffico di rete	Protocolli: Modbus, DNP3	Riservatezza dei dati	Secure DNP3, PKI, TLS, SSL, Encryption, Authentication
Scanning	Scansione degli indirizzi IP, Porte, Servizi per sniffare i dati trasmessi			IDS (Sistema di detezione dell'intrusione), SIEM (Security Information and Event Management), Verifica automatica di conformità dei sistemi di sicurezza
INFRASTRUTTURA DI AUTOMAZIONE, MONITORAGGIO E CONTROLLO				
Exploitation (Qualsiasi attacco che sfrutta le vulnerabilità di applicazioni, reti, sistemi operativi o hardware)	Virus, worms, Trojan Horse	SCADA PMU, dispositivi di controllo	Integrità riservatezza dati, Disponibilità, Accountability	DLP (Data Loss Prevention), SIEM (Security Information and Event Management), Anti-virus, IDS (Intrusion Detection System)
	Denial of service (DoS)	AMI (Infrastruttura Avanzata di Misura), PMU, dispositive GGPS smart grid	Disponibilità	Analisi entropia flusso dati, SIEM (Security Information and Event Management), IDS (Intrusion Detection System), conteggio errori di trasmissione, metodi di riconfigurazione, etc.
	Violazione Privacy	Misuratori Smart (es. telecontatori)	Riservatezza dei dati	Secure DNP3, PKI, TLS, SSL, Encryption, Authentication
	Man-in-the-middle (MITM)	HMI, PLC, SCADA, AMI, DNP3	Integrità e riservatezza dati	Secure DNP3, PKI, TLS, SSL, Encryption, Authentication
	Replay attack	IED, SCADA, PLC, authentication scheme in AMI	Integrità dati	Secure DNP3, PKI, TLS, SSL, Encryption, Authentication
	Jamming channel	PMU, CRN in WSGN	Disponibilità	Anti-jamming
	Popping the HMI	SCADA, EMS, substations	Integrità riservatezza dati, Disponibilità, Accountability	DLP, SIEM, Anti-virus, automated security compliance checks, IDS
	Masquerade attack	PLC	Integrità riservatezza dati, Disponibilità, Accountability	DLP, Secure DNP3, PKI, SIEM, TLS, SSL, encryption, authentication, IDS

	Violazione integrità	Smart meter, RTU	Integrità e disponibilità dei dati	DLP, Secure DNP3, PKI, SIEM, TLS, SSL, encryption, authentication, IDS
	Backdoor	SCADA	Integrità e riservatezza dei dati, Disponibilità, Accountability	IDS, SIEM, Antivirus
Maintaining access	Backdoor	SCADA	Integrità e riservatezza dei dati, Disponibilità, Accountability	IDS, SIEM, Antivirus
Fonte: Jamil, N.; Qassim, Q.S.; Bohani, F.A.; Mansor, M.;Ramachandaramurthy, V.K." *Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research".* Appl.Sci. 2021, 11, 9812. https://doi.org/10.3390/app11219812				

In relazione, all'infrastruttura fisica, è stato condotto uno studio per valutare come i diversi attacchi alle infrastrutture di comunicazione, automazione, monitoraggio e controllo possano impattare sulle reti fisiche. In generale, la conoscenza della topologia della rete è fondamentale per poter attuare le opportune misure di mitigazione (es. isolare il nodo di rete interessato dall'attacco); non tutte le topologie, infatti, presentano la medesima flessibilità di intervento. In Tabella 2 si riportano le caratteristiche principali delle 4 topologie di rete più comuni.

Tabella 2: principali caratteristiche di 4 topologie di rete

La **topologia radiale** è caratterizzata dalla presenza di un bus singolo, un singolo punto di connessione, facilità di installazione, scalabilità e bassi costi. In caso di un cyber attacco che ha come conseguenza l'interruzione della fornitura di energia elettrica lungo una dorsale della rete, tutti gli utenti di quella dorsale, in caso di unico sistema di generazione vengono disalimentati.	

La **topologia ad anello** prevede un bus singolo ed ogni nodo della rete è connesso solo ai due vicini. Tale topologia è caratterizzata da facilità di installazione e una maggiore possibilità di isolamento in caso di guasti o problemi locali (isolamento del nodo). Ciò la rende anche più cyber-resiliente di quella radiale poiché in caso di un cyber attacco ad un nodo dell'anello, l'attacco può essere facilmente isolato senza inficiare la continuità di servizio. Di contro questa topologia è poco scalabile e presenta costi elevati legati all'estensione.	
La **topologia a maglie** prevede la presenza di bus multipli ed i nodi della rete sono interconnessi a più rami. Tale topologia è caratterizzata da complessità di installazione e costi elevati. Essa è costituita da anelli interdipendenti quindi, in caso di cyber attacco, conserva gli stessi vantaggi della topologia ad anello.	
La **topologia a linee parallele** presenta bus paralleli, una elevata affidabilità e ridondanza, ed è caratterizzata da costi elevati. Nella topologia a linee parallele viene raddoppiato il set di linee elettriche, che possono seguire anche percorsi diversi, per garantire la continuità del servizio. Quindi, per sua natura, tale topologia può essere considerata resiliente a cyber attacchi che hanno come conseguenza l'interruzione della fornitura di energia elettrica per una certa porzione di rete.	

Alla luce dell'analisi effettuata, sono state individuate la topologia di tipo radiale e la topologia di tipo ad anello quali topologie più idonee alla costruzione degli schemi sperimentali da implementare nella nanogrid ENEA per le attività sperimentali da condurre nell'ambito della LA2.7 e della LA1.6. La topologia radiale è stata scelta per la sua criticità intrinseca in caso di cyber attacchi e risulta quindi adatta per verificare l'efficacia degli schemi di protezione che verranno sviluppati nelle LA2.7 e LA1.6. La topologia ad anello, invece, è stata scelta in quanto, come evidenziato in precedenza, ad essa può essere ricondotta anche la topologia a maglie che è costituita da anelli interdipendenti. Infine, la topologia a linee parallele non è stata

ritenuta di interesse per le successive attività del progetto in quanto, per le sue caratteristiche intrinseche, risulta maggiormente cyber resiliente rispetto alle altre topologie.

Individuazione del sistema di crittografia quantistica di tipo Quantum Key Distribution (QKD) da acquisire e predisposizione della documentazione tecnica di gara

Al fine di condurre le attività sperimentali previste dal progetto si rende necessario dotare il laboratorio di un sistema integrato che includa apparati cifranti di rete e sistemi di trasmissione con tecnologia Quantum Key Distribution (QKD) per la comunicazione su canale quantistico in fibra ottica.

A valle dello studio dei sistemi disponibili in commercio, sono stati definiti i requisiti del sistema da acquisire. Si è, quindi, predisposto l'allegato tecnico per l'indizione (nel II SAL) della gara. Il sistema da acquisire, in particolare, dovrà essere dotato:

- 1 apparato di trasmissione e 1 apparato di ricezione di tipo bidirezionale (es: Alice e Bob) che utilizzano entrambi i canali di comunicazione classico e quantistico
- 2 sistemi cifranti, tutta la componentistica di interconnessione necessaria al funzionamento dell'infrastruttura (es. cavi ethernet, patch in fibra, switch, time tagger, SPAD, rack contenitori degli apparati forniti, ecc.)
- 1 piattaforma, modulare, scalabile e flessibile, dotata di interfaccia grafica per il monitoraggio e la gestione dei parametri operativi di tutti gli apparati del
- tutta la componentistica di interconnessione necessaria al funzionamento del sistema e alla sua interconnessione alla nanogrid ENEA, ovvero: cavi ethernet, patch in fibra, switch, time tagger, SPAD, rack contenitori degli apparati forniti, ecc.

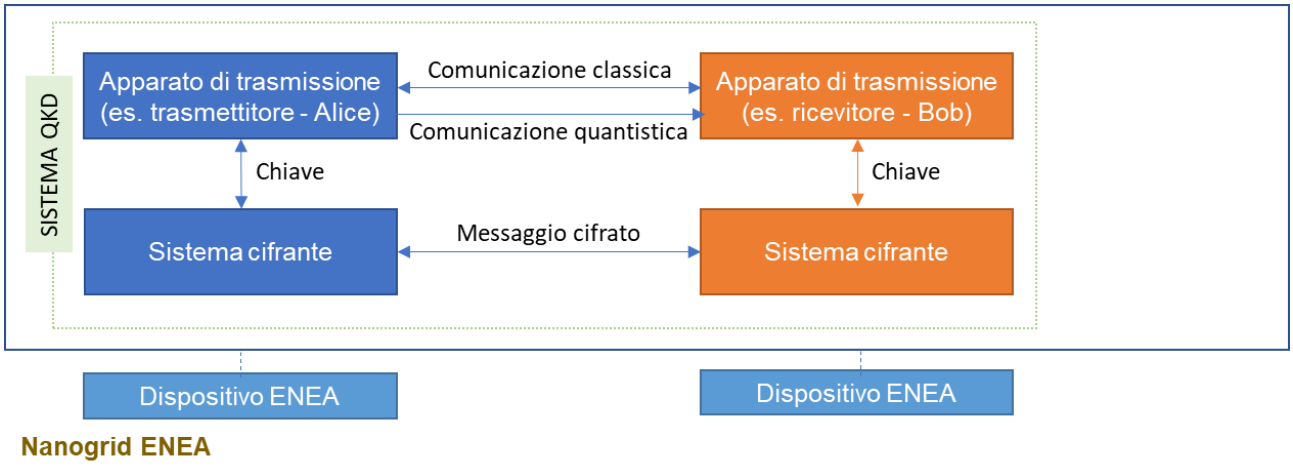


Figura 1: schema logico del sistema QKD da acquisire

Le specifiche tecniche di ciascun apparato/dispositivo del sistema richiesto sono riportate nelle seguenti tabelle (Tabelle 3-6).

Tabella 3: Specifiche tecniche apparati di trasmissione	
Canale di connessione Alice-Bob	Quantistico (fibra ottica) + Classico (servizio e sincronizzazione)
Laser Pulse Generator	Basato su FPGA
Bit rate	Non inferiore a 600MHz
Protocollo quantistico	BB84 e possibilità di utilizzo di protocolli sviluppati dall'utente
Key generation rate	(2-6) kbit/s
Distanza geografica coperta	> 80km
Connessione elettrica	Spina CEE
Simulatore di intercettazione (eavesdropper simulation)	Incluso nella fornitura del sistema integrato
Tipo di installazione	In armadi rack (19'')
Alimentatore per rete 230V e cavo di alimentazione elettrica con spina Shuko	Inclusi nella fornitura per tutti gli apparati di trasmissione

Tabella 4: Specifiche tecniche apparati cifranti	
Latenza	<= 1ms
Throughtput	>= 1Gbps
Sistema di accumulo per la memorizzazione delle chiavi quantistiche	Presente nella fornitura
Memory backup per chiavi quantistiche	>=10 giorni
Interfacce	Fibra ottica e/o rame
Sistema di protezione da manomissione	Sensori anti-tampering
Tipo di installazione	In armadi rack (19'')
Alimentatore per rete 230V AC e cavo di alimentazione elettrica con spina Shuko	Inclusi nella fornitura per tutti gli apparati di trasmissione

Tabella 5: Specifiche tecniche di componentistica di interconnessione	
Cavi Ethernet necessari per la connessione degli apparati del sistema integrato	Inclusi nella fornitura del sistema integrato
Patch in fibra necessari per la connessione degli apparati del sistema integrato	Inclusi nella fornitura del sistema integrato e di lunghezza non inferiore a 5 metri ciascuno
Moduli SFP	Idonei alla connessione con fibra del tipo Singlemode 1310nm – 10Gbps
Switch	N.2 switch, web managed, a 16 canali ciascuno, dotati di alimentatori e cavi di alimentazione elettrica con spina Shuko.
Time tagger	Implementato
SPAD	Inclusi nella fornitura del sistema integrato

Tabella 6: Specifiche tecniche piattaforma di monitoraggio e gestione	
Interfaccia grafica per le fasi di set, di controllo e di visualizzazione dei parametri operativi di tutti gli apparati del sistema integrato (cifranti + trasmettitori + canali)	Presente
Interfaccia web grafica	Presente
Software di monitoraggio delle chiavi e dei parametri operativi di tutti gli apparati del sistema	Presente
Key Management Software	Presente

Progettazione del testbed ENEA per le attività sperimentali del progetto

Il testbed sperimentale è stato definito in ottica di predisporre un ambiente di test che risponda alle esigenze di progetto in ottica di ampia configurabilità e di possibilità di integrazione con gli apparati preesistenti della nanogrid del Centro Ricerche ENEA di Portici. In particolare, l'infrastruttura definita dovrà consentire la validazione sperimentale delle tecnologie, delle topologie di rete precedentemente individuate e degli apparati di protezione del progetto.

L'infrastruttura sperimentale sarà costituita da diversi apparati elettronici già presenti nella nanogrid di laboratorio (sistemi di emulazione di generazione, carico e accumulo; sistemi di misura; 1 simulatore di rete; 1 software di gestione dell'architettura sperimentale) e il sistema QKD da acquisire (sezione precedente), come da schema concettuale in Figura 2.

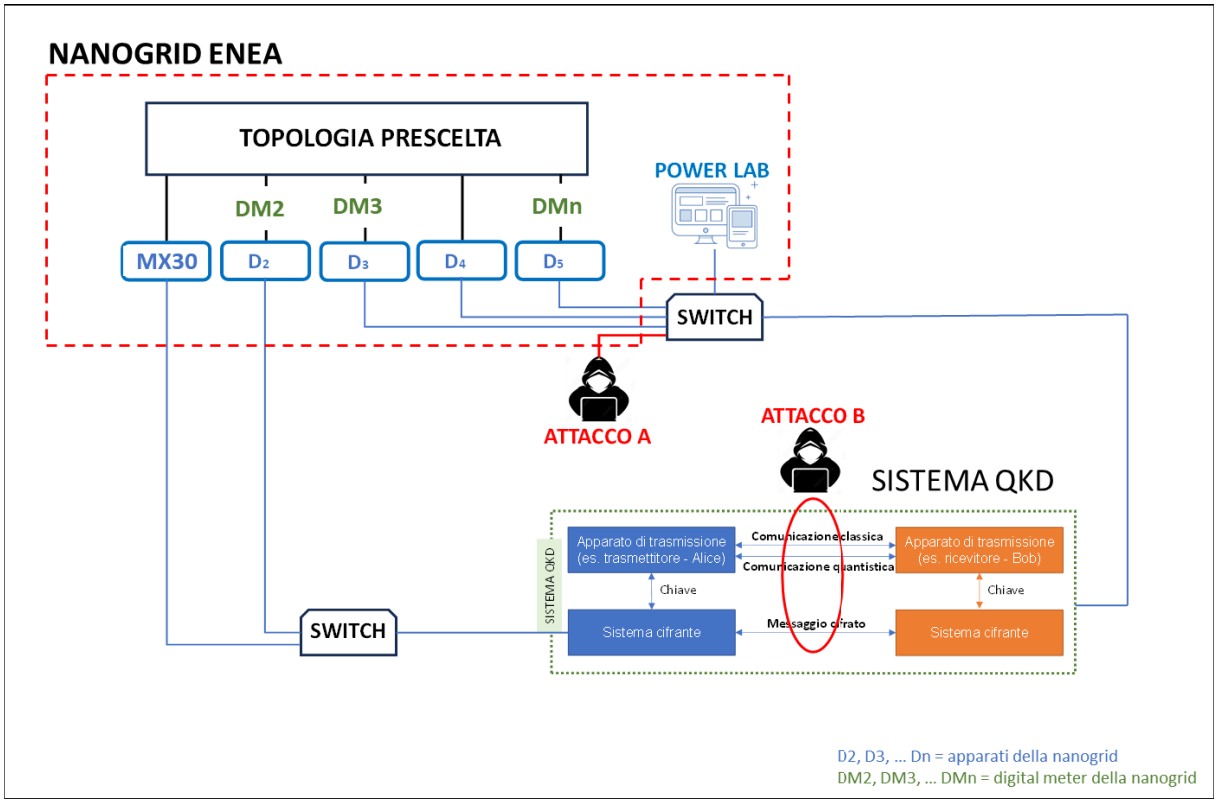


Figura 2: schema concettuale dei test

I diversi apparati saranno attivati e configurati in funzione delle diverse esigenze di test. Avendo già descritto nella precedente sezione il sistema QKD, di seguito, si riportano – come richiesto da capitolato – le caratteristiche di altri tre apparati: simulatore di rete trifase MX30-3Pi, Misuratori Digital Power Meter e software Powerlab.

Il **simulatore di rete trifase MX30-3Pi** è un generatore di potenza elettrica DC-AC, a quattro quadranti, avente una potenza di targa di 30kVA, una tensione massima di tipo AC di 300Vrms e una tensione massima DC di 400V. Questo apparato permette di simulare forme d'onda preconfigurate, oppure definite dall'utente. In particolare, è possibile simulare generazione di bassa/alta tensione DC, generazione di bassa/alta tensione AC monofase o trifase, funzionamento di tipo puramente generativo oppure misto generativo-rigenerativo. Per quanto riguarda l'isolamento tra la rete e le varie utenze, inoltre, il simulatore è dotato di un trasformatore di alimentazione di tipo isolato ad alta efficienza.

Al fine di rendere altamente accurato il monitoraggio in tempo reale della strumentazione di misura e il rilevamento dei parametri funzionali di interesse, sono stati predisposti dei misuratori a dati campionati ad alta velocità, denominati **Digital Power Meter** (WT333E per la rete trifase, WT310Eh per la monofase). Le misurazioni di tipo metrologico possono avvenire grazie all'interconnessione con la rete informatica di laboratorio, tramite canale Ethernet e al sistema HIL per la trasmissione delle grandezze elettriche, in tempo reale, all'ambiente di emulazione mediante interfaccia analogica. Da sottolineare l'accuratezza in potenza pari allo 0,1% ed il sampling rate pari a 100kS/s, che caratterizzano questi dispositivi di monitoraggio.

Per realizzare la comunicazione e il controllo tra i vari dispositivi che configureranno le reti benchmark durante le attività sperimentali di test e validazione, verrà adoperato un ambiente software **Powerlab**. Il software, progettato e sviluppato da ricercatori ENEA, consente di gestire – in real time – i diversi apparati di laboratorio come dispositivi di una rete elettrica. Il software, in particolare, è concettualmente costituito da 3 layer: gestione dei servizi, supervisione e controllo degli strumenti e dei meter (fungendo da sistema SCADA), e il terzo con i controllori locali degli strumenti di emulazione.

Definizione di due procedure per i test di validazione funzionale

Al fine di valutare gli impatti di cyber attacchi sul funzionamento dell'infrastruttura precedentemente definita, sono stati elaborati due scenari di test che saranno applicati per l'esecuzione delle prove sperimentali previste dal II SAL. Nello specifico, uno scenario è stato definito per valutare l'impatto di un cyber attacco sul funzionamento dell'infrastruttura elettrica (attacco A – Figura 2), l'altro per analizzare l'impatto di un cyber attacco sul funzionamento a livello di apparato e le relative conseguenze sul funzionamento dell'infrastruttura elettrica (attacco B – Figura 2). L'attacco B, in particolare, sarà orientato ad emulare un cyberattacco che compromette la riservatezza dei dati. Gli step per la realizzazione dei due test di validazione funzionale, ciascuno dei quali sarà effettuato per entrambe le topologie delle reti elettriche identificate in precedenza, sono di seguito riassunti.

Test n. 1
Il seguente test fa riferimento al caso studio dell'**attacco A** e ha lo scopo di effettuare una valutazione dell'impatto del cyber attacco sul funzionamento dell'infrastruttura elettrica.

1. Configurazione topologia elettrica della rete benchmark.
2. Setup degli apparati afferenti alla rete elettrica.
3. Avvio del funzionamento nominale della rete elettrica.
4. Monitoraggio e acquisizione dei parametri elettrici di funzionamento nominale della rete benchmark.
5. Verifica della capacità dei diversi dispositivi alla ricezione di un comando.

6. Verifica della capacità di riposta dei diversi dispositivi all'invio dei dati richiesti.
7. Verifica della capacità dei diversi dispositivi all'invio dei segnali di stato e/o allarme.
8. Avvio della procedura di iniezione del cyber attacco sulla rete elettrica.
9. Monitoraggio e acquisizione dei parametri elettrici di funzionamento nominale dopo il cyber attacco.
10. Verifica capacità dei diversi dispositivi di risposta alla ricezione di un comando dopo il cyber attacco.
11. Verifica della capacità dei diversi dispositivi all'invio dei dati richiesti dopo il cyber attacco.
12. Verifica della capacità dei diversi dispositivi all'invio dei segnali di stato/allarme dopo il cyber attacco.

Test n. 2
Il seguente test fa riferimento al caso studio dell'**attacco B** e ha lo scopo di effettuare una valutazione dell'impatto del cyber attacco sul funzionamento di uno specifico apparato le relative conseguenze sul funzionamento dell'infrastruttura elettrica.

1. Configurazione della rete benchmark.
2. Setup degli apparati afferenti alla rete.
3. Avvio del funzionamento nominale della rete.
4. Monitoraggio e acquisizione dei parametri caratteristici di funzionamento dell'apparato in esame.
5. Verifica della capacità dell'apparato alla diponibilità di ricezione di comandi.
6. Verifica della capacità di riposta dell'apparato alla richiesta di invio dati.
7. Verifica della capacità dell'apparato all'invio di segnali di stato e/o allarme.
8. Avvio della procedura di iniezione del cyber attacco verso l'apparato in esame.
9. Monitoraggio dei parametri caratteristici di funzionamento dell'apparato dopo il cyber attacco.
10. Verifica della capacità dell'apparato alla ricezione di comandi dopo il cyber attacco.
11. Verifica della capacità di riposta dell'apparato alla richiesta di invio dati dopo il cyber attacco.
12. Verifica della capacità dell'apparato all'invio di segnali di stato e/o allarme dopo il cyber attacco.

8 Contributo delle eventuali consulenze alle attività sopra descritte

L'attività non ha previsto il ricorso a consulenze.

9 Pubblicazioni scientifiche

Elenco delle pubblicazioni scientifiche eventualmente risultanti dall'attività svolta

L'attività svolta non è stata oggetto di pubblicazioni scientifiche nel SAL.

10 Eventi di disseminazione

Lista degli eventi di disseminazione eventualmente scaturiti dall'attività svolta

L'attività svolta non è stata oggetto di eventi di disseminazione specifici nel SAL.