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

Studio e valutazione di schemi di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche (LA2.2)

Giovanna Adinolfi, Maria Valenti

RdS_PTR 22-24_PR 2.1_LA2.2_067

STUDIO E VALUTAZIONE DI SCHEMI DI PROTEZIONE PER LA MITIGAZIONE DEGLI EFFETTI CONNESSI AI CYBER-ATTACCHI IN OTTICA DI INCREMENTO DELLA CYBER-RESILIENZA DELLE RETI E DELLE MICRORETI ELETTRICHE (LA2.2)

Giovanna Adinolfi, Maria 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: *Decarbonizzazione/Digitalizzazione ed evoluzione delle reti*
Progetto: *Tema di ricerca 2.1, Progetto integrato cyber security dei sistemi energetici*
Linea di attività: *2.2*
Responsabile del Progetto: Maria Valenti, ENEA
Responsabile Linea di Attività: Giovanna Adinolfi, ENEA
Mese inizio previsto: 1
Mese inizio effettivo: 1
Mese fine previsto: 18
Mese fine effettivo: 18

Indice

1 Risultati attesi

Viene, di seguito, riportata la lista dei risultati attesi come da capitolato vigente:

- studio di almeno due dispositivi di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche;

- schema architetturale di un dispositivo di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche.

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)

Le attività svolte nella presente LA hanno avuto inizio con lo studio della documentazione tecnica e normativa inerente ai dispositivi di protezione elettrica delle reti di distribuzione. Tale studio è stato condotto con il fine di analizzare gli schemi di coordinamento per la selettività in reti e microreti elettriche, i requisiti e le proprietà dei suddetti apparati.

Successivamente si è proceduto ad analizzare i rischi e le minacce di natura cibernetica cui le reti elettriche sono state sottoposte negli ultimi anni per l'individuazione delle vulnerabilità su cui lavorare per l'aggiornamento degli attuali schemi di protezione. Tale studio ha evidenziato che, negli ultimi anni, si è registrato un ingente numero di attacchi cibernetici condotti a danno delle infrastrutture strategiche e critiche. Nel contesto geopolitico attuale, la minaccia cyber è diventata una vera e propria arma di attacco che può avere impatti considerevoli sulla continuità dei servizi, sulla funzionalità di aziende, scuole ed uffici. Si pensi a quanti misuratori, sensori e controllori degli apparati collegati alle reti di distribuzione si avvalgono della rete dati pubblica per trasmettere informazioni, dati, misure e comandi necessari alle operazioni di monitoraggio, controllo e coordinamento.

In tale contesto, la definizione di nuovi schemi architetturali per dispositivi di protezione di nuova generazione, non solo in grado di proteggere un sistema, un apparato o un impianto da sovratensioni/sovracorrenti e temperature oltre i limiti, ma capace di rilevare e mitigare anche minacce cibernetiche, rappresenta un obiettivo fondamentale per garantire la difesa delle attuali e future reti elettriche da attacchi cibernetici.

È stato, a tal fine, proposto uno **schema architetturale di tipo multilayer** caratterizzato da uno strato dedicato allo stadio di potenza del sistema di protezione, uno strato per l'alimentazione del sistema elettronico e per la circuiteria di condizionamento e misura, un layer dedicato al sistema di controllo, uno al sistema di comunicazione e crittografia quantistica di dati e comandi e, infine, uno strato di set, segnalazione e visualizzazione delle principali grandezze operative.

Sulla base di tale architettura sono stati, quindi, definiti i layer di **due dispositivi di protezione elettrica e cibernetica**. Essi sono caratterizzati da interruttori allo stato solido realizzati anche mediante materiali di tipo Wide Band Gap. In dettaglio:

- il primo dispositivo proposto è dedicato a tutti gli impianti, apparati e sistemi collegati alle reti e/o microreti elettriche che si sviluppano in quelle zone con disponibilità di un mezzo trasmissivo in fibra ottica. Esso si avvale di tecniche di Quantum Key Distribution per la comunicazione di dati e comandi con apparati "gemelli". Ciò significa che le chiavi per crittografare i dati e comandi vengono scambiate mediante sequenze di fotoni opportunamente polarizzati e trasmessi sul canale quantistico in fibra ottica.

- il secondo dispositivo proposto è dedicato a tutti gli impianti, apparati e sistemi collegati alle reti e/o microreti elettriche che si sviluppano in quelle zone in cui non è disponibile un mezzo trasmissivo in fibra ottica per la realizzazione del canale quantistico. Questo secondo apparato si basa sul medesimo schema architetturale multilayer precedentemente presentato e si distingue dal precedente per il layer di comunicazione. In particolare, in assenza del mezzo trasmissivo in fibra ottica, si è deciso di sfruttare cammini liberi in aria per la ricezione e trasmissione di dati e comandi avvalendosi di tecniche Quantum Free Space. Potranno essere utilizzati telescopi o ricetrasmettitori innovativi.

In definitiva, nel presente SAL, sono stati raggiunti tutti i risultati previsti da capitolato e tabella integrativa inviata agli esperti. Tali risultati sono di seguito elencati:

- **Studio di schemi di coordinamento per la selettività in reti e microreti elettriche e dei requisiti e proprietà dei dispositivi di protezione**

  Studio dei dispositivi di protezione finalizzato all'analisi degli schemi di coordinamento per la selettività in reti e microreti elettriche, dei requisiti e delle proprietà dei suddetti apparati.

- **Schema architetturale di un dispositivo di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche.**

  È stato proposto uno schema architetturale di tipo multilayer e sono state descritte le funzionalità e le caratteristiche dei diversi layer che lo costituiscono.

- **Studio di almeno due dispositivi di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche**

  È stata portata a termine la definizione di due dispositivi di protezione elettrica e cibernetica per sistemi ed impianti collegati a reti e/o microreti elettriche in zone in cui risulta disponibile/non disponibile il mezzo trasmissivo in fibra ottica.

L'utilizzo dei dispositivi proposti potrà incidere non solo sulla continuità di servizio, che viene sempre più inficiata da eventi di tipo cyber, ma anche sulla riduzione dei rischi connessi all'impartizione di comandi dannosi. È semplice comprendere quali potrebbero essere le conseguenze di un comando malevolo in impianti d'utenza come le stazioni di ricarica dei veicoli elettrici, dei veicoli ad idrogeno, nonché nei grossi impianti di produzione da fonti rinnovabili (fotovoltaico, eolico, idrogeno). È evidente, quindi, che lo studio condotto e i risultati ottenuti costituiscono un beneficio per il sistema elettrico nazionale e i suoi utenti; i dispositivi proposti, infatti, contribuiscono ad incrementare la cyber-resilienza delle reti e delle microreti elettriche.

I risultati ottenuti sono propedeutici alla conduzione delle attività della LA2.7.

3 Prodotti attesi

La LA2.2 non prevede lo sviluppo di 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 LA2.2 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 LA2.2.

6 Sintesi delle attività svolte

(1000 caratteri max)

Sintesi delle attività svolte e dei risultati ottenuti in relazione ai risultati attesi.

Nella LA2.2 sono state svolte le seguenti attività: analisi della documentazione tecnica e normativa sui dispositivi di protezione elettrica per le reti di distribuzione, definizione di uno schema architetturale per la realizzazione di un apparato di protezione elettrica e cibernetica di nuova generazione, definizione di due dispositivi di protezione basati rispettivamente su tecniche Quantum Key Distribution e Quantum Free Space per la mitigazione degli effetti connessi ai cyber-attacchi in micro-reti e reti elettriche.

Lo schema ed i dispositivi proposti risultano propedeutici alla conduzione delle attività della LA2.7 "Implementazione di uno schema di protezione e sviluppo di un prototipo per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche".

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.

Nella LA2.2 sono stati analizzati la normativa ed i documenti tecnici di settore al fine di condurre uno studio dei sistemi di protezione con particolare riferimento alla cybersicurezza degli schemi di coordinamento tra protezioni attualmente adottati nelle reti italiane di distribuzione dell'energia elettrica.

In relazione alle **protezioni di tipo elettrico**, le attuali reti in Media e Bassa Tensione (MT e BT) sono generalmente dotate di protezioni di massima corrente, di massima corrente direzionale e omopolare, di massima corrente omopolare di terra, di minima e massima tensione, di massima corrente differenziale e di

protezioni di frequenza. Ciascuna di tali tipologie risulta caratterizzata da soglie e tempistiche d'intervento in conformità alla normativa di settore e sulla base delle specifiche della linea o dell'apparato da proteggere.
I dispositivi di protezione, inoltre, possono essere utilizzati come sistemi di protezione principale o come sistemi di protezione di riserva. I sistemi di protezione principale vengono impiegati per rilevare i guasti che si presentano in una certa area nel minor tempo possibile; quelli di riserva vengono attivati in caso di malfunzionamento del dispositivo principale. È evidente che si ricorre alle protezioni di riserva soltanto in sezioni vitali della rete elettrica in quanto i costi per ridondare la protezione principale sono giustificati dalla necessità di garantire elevate prestazioni.

I requisiti fondamentali dei sistemi di protezione sono riportati e descritti nella Tabella 1.

Tabella 1: Requisiti fondamentali dei sistemi di protezione

Requisito	Definizione
Sicurezza	un dispositivo è sicuro quando funziona correttamente, anche se è stato interessato da inattività per un periodo di tempo lungo
Affidabilità	un dispositivo è affidabile quando è alta la probabilità che esso svolga adeguatamente la funzione prevista (intervento richiesto/assenza di interventi intempestivi) per un determinato periodo di tempo o che esso funzioni in un ambiente definito senza presentare guasti
Sensitività	un dispositivo è sensibile se realizzato in maniera tale da rilevare anche esigui valori e contenute variazioni delle grandezze che interessano il sistema elettrico
Selettività	La selettività è la capacità di un sistema di protezioni di intervenire solo sulla porzione di rete dove si presenta il guasto, di isolarlo rapidamente, e di assicurare la continuità di servizio nelle porzioni non guaste della rete. In una rete elettrica, i dispositivi di protezione possono essere scelti in modo da garantire una delle seguenti tipologie di selettività: amperometrica, cronometrica, logica, energetica (valida solo in BT) e loro combinazioni. La selettività può essere richiesta nei confronti delle condizioni di sovraccarico, corto circuito e guasto a terra.

Con riferimento agli schemi di coordinamento tra protezioni elettriche, l'analisi condotta ha evidenziato che attualmente si utilizzano 3 tecniche di selettività: amperometrica, logica e cronometrica, sinteticamente descritte in Tabella 2.

Tabella 2: Tecniche di Selettività

Tecnica	Implementazione
Selettività Amperometrica	La selettività amperometrica viene ottenuta nelle reti e negli impianti definendo opportuni schemi di coordinamento tra protezioni collocate a livello gerarchico differente. Ciò significa identificare ed impiegare apparati di protezione delle sezioni a monte con soglie di intervento superiori a quelle delle protezioni collocate nelle porzioni a valle della rete, microrete o nell'impianto di interesse. In questo modo, al presentarsi di un guasto a valle, esso viene isolato dalla relativa protezione. Risulta, così, facilmente individuabile il sistema o la sottorete dove effettuare interventi di riparazione/manutenzione e, nello stesso tempo, è anche garantita la continuità di servizio delle sezioni a monte.
Selettività	La selettività di tipo cronometrico è basata sull'utilizzo di dispositivi caratterizzati da tempi di intervento "gradualmente" più lunghi a partire dalle porzioni di rete/impianto

Cronometrica	a valle fino a quelle a monte. Tali tempi sono regolabili in uno specifico range d'intervento basato sulla tipologia degli apparati considerati. A titolo di esempio, si tenga presente che per dispositivi di protezioni per reti di MT, il tempo di apertura è di circa 60 ms, il tempo di inerzia di tali apparati risulta di circa 20 ms, il massimo errore dell'intervento temporizzato è di circa 60 ms. Considerando, inoltre, un margine di sicurezza di circa 75 ms, appare chiaro che la selettività cronometrica tra due protezioni in serie richiede un ritardo tra i due interventi di circa 200-250 ms.
Selettività Logica	La selettività logica è basata sull'utilizzo di interruttori elettronici dotati di microprocessori ed installati in cascata. La presenza di cavi pilota tra due protezioni consente la trasmissione e ricezione dei segnali di blocco tra i due dispositivi[1]. Al presentarsi di un guasto di fase o di un guasto a terra, se le protezioni non fossero coordinate, scatterebbero tutti i dispositivi attraversati dalla corrente di guasto. L'implementazione di schemi di protezione basati sulla selettività logica fa sì che l'apparato di protezione collocato nella porzione più vicina al guasto inoltri un segnale di blocco a quello a monte inibendone l'intervento per 50 ms. In tal modo, esso isola il guasto e consente alle altre porzioni di rete di continuare a funzionare.

Più nello specifico, il **coordinamento degli interventi dei diversi dispositivi di protezione** viene ottenuto avvalendosi di tabelle di regolazione delle diverse soluzioni di protezione e dei diagrammi di selettività. In particolare, viene individuata e definita la sequenza di intervento dei diversi apparati di protezione in relazione a ciascun valore che assume la corrente nel circuito/impianto/porzione di rete o sottorete che si sta considerando.

Particolarmente critica per il coordinamento risulta la valutazione di eventuali interventi intempestivi di tali dispositivi. Questi ultimi risultano critici giacché, al loro verificarsi, non è possibile rilevare guasti e l'operatore di rete non possiede elementi utili per consentire il ripristino del servizio e per valutare le relative tempistiche.

Numerosi sono i dispositivi di protezione presenti in commercio. Accanto alle soluzioni di tipo tradizionale, come quelle elettromeccaniche, sono, attualmente, disponibili anche protezioni "intelligenti" e apparati di protezione virtuali.

Nel primo caso, si tratta di dispositivi dotati di interfacce di comunicazione basate su Modbus TCP ed Ethernet[2] e che presentano a bordo una logica programmabile.

Le protezioni virtuali[3] ricevono dati da misuratori collocati fisicamente su linee, trasformatori ed altri componenti di rete. Esse elaborano i dati ricevuti ed implementano algoritmi di protezione. Tali soluzioni inviano comandi ai relè perché interrompano il servizio in caso di guasto o per il riarmo necessario ad assicurare nuovamente il servizio dopo un intervento di riparazione o manutenzione. Esse sono propriamente software che possono essere utilizzati con apparati fisici (come i relè) prodotti da costruttori diversi. Essi si avvalgono di tecnologie di comunicazione di tipo digitale e sono conformi alla IEC 61850, standard internazionale per la realizzazione di reti di comunicazione e sistemi per l'automazione di utenze elettriche.

Con riferimento alle funzionalità di cybersicurezza, taluni apparati di protezione elettrica implementano strategie e tecniche per far fronte al pericolo cibernetico. In particolare, si tratta, più che di soluzioni integrate, di forme di autenticazione per l'accesso e la gestione del dispositivo (es. processo di autenticazione degli utenti, concessione di autorizzazioni solo a specifici utenti, identificazione di password di protezione,

[1] Guida tecnica Criteri di protezione delle reti elettriche di media tensione, ABB.

[2] PowerLogic™ P5 Protection Relay, Schneider Electric.

[3] Real-life pilot of virtualized protection and control – Experiences and performance analysis, White paper, ABB.

door endurance). In questo caso, la cybersicurezza nel coordinamento tra protezioni è demandata a sistemi di controllo degli accessi basati su autenticazione e autorizzazione degli utenti. Queste metodologie, però, non risultano del tutto efficaci a fronte di attacchi cibernetici che riescono ad aggirare l'accesso protetto da password tradizionale. Per ottenere un miglioramento della cybersicurezza del sistema occorre rivedere gli schemi di protezione, in maniera tale da integrare nei dispositivi stessi opportuni sistemi di rilevamento delle intrusioni che possano mitigare i rischi dei cyberattacchi.

Dispositivo di protezione avanzato: schema architetturale e caratteristiche del dispositivo (presenza di mezzo trasmissivo in fibra ottica)

L'analisi condotta nella prima fase di lavoro della LA ha evidenziato che occorre concentrare l'attenzione sullo sviluppo di apparati di protezione di nuova generazione che, oltre ad assolvere le tipiche funzionalità di protezione elettrica, possano rafforzare la capacità di impedire/mitigare interventi malevoli di natura cibernetica a danno di reti e microreti elettriche. Tali apparati potranno essere utilizzati per proteggere una linea elettrica o un componente di rete (meter, impianti di generazione, sistemi di storage, utenze) da condizioni anomale di funzionamento, quali sovratensioni, sovracorrenti e surriscaldamenti ma anche da minacce di tipo cyber.

Il dispositivo dedicato alla protezione di apparati connessi a microreti elettriche BT sarà progettato in maniera da gestire correnti di linea fino a 100 A (Tabella 3). Saranno impiegati Solid State Circuit Breaker (SSCB) pilotati opportunamente dai segnali di gate. A seconda dell'azione da intraprendere, il microcontrollore del sistema di controllo (layer 3 – Tabella 4) fornirà i segnali di gate per garantire continuità di servizio, per sezionare l'impianto, per coordinare selettivamente lo specifico dispositivo di protezione con un altro collocato nella microrete di interesse o per operazioni di "riarmo".

Il dispositivo, grazie all'adozione di uno schema architetturale a strati, presenterà un **elevato grado di configurabilità** (Tabella 3) sia in riferimento alle soglie delle principali grandezze, sia per le tempistiche degli interventi da portare a termine.
La possibilità di cambiare le soglie e le tempistiche d'intervento consente di:

- ottenere un livello di protezione customizzato sulle specifiche esigenze dell'apparato di interesse;
- riconfigurare il dispositivo, senza cambiarlo, nel rispetto dei rate massimi consentiti, in caso di interventi di potenziamento o aggiornamento degli impianti/sistemi che protegge.

Tabella 3: Specifiche elettriche del dispositivo di protezione

Grandezza elettrica	Valore
Tensione di fase AC in Bassa Tensione	230 V
Massima corrente di linea	100 A
Corrente nominale operativa	Configurabile
Corrente differenziale massima	Configurabile
Soglia di Over Voltage	Configurabile
Soglia di Under Voltage	Configurabile
Tempo di NON intervento	Configurabile
Temperatura operativa massima	Configurabile

Il dispositivo sarà dotato di interfaccia grafica di set e monitoraggio sia delle grandezze elettriche, sia dei dati e dei comandi ricevuti e/o trasmessi da/ad apparati coordinati.

Il coordinamento tra i diversi dispositivi sarà progettato in modo tale che ciascun apparato possa agire tempestivamente, nel caso in cui uno di essi risulti attaccato ciberneticamente, prevenendo così la propagazione della minaccia in reti e microreti elettriche. Infine, il dispositivo adotterà un controllo non basato su accesso con password tradizionale ma utilizzerà tecniche di crittografia quantistica avanzata per ottenere un sistema più cyber-resiliente.

In Tabella 4 si riporta descrizione delle funzioni dei diversi layer, successivamente descritti singolarmente.

Tabella 4: Dispositivo di protezione: layer dello schema architetturale

Layer	Funzione
Layer 1: Stadio di potenza del sistema di protezione a stato solido	Il primo strato è dedicato all'hardware dello stadio di potenza. Esso implementa una soluzione circuitale in grado di gestire flussi bidirezionali di potenza e di interromperli in presenza di anomalie e guasti di natura elettrica a monte o a valle del dispositivo. La topologia ed i relativi componenti saranno scelti e dimensionati in maniera tale da ottenere un apparato ad alta configurabilità in modo da personalizzare le tempistiche/le soglie di protezione in relazione allo specifico sistema o dispositivo da proteggere.
Layer 2: Alimentazione del sistema elettronico e circuiteria di condizionamento e misura	Il secondo layer è costituito dalla circuiteria per l'implementazione del sistema di alimentazione del dispositivo di protezione e per il condizionamento e la misura delle grandezze (tensioni, correnti, etc) ai terminali d'ingresso e d'uscita.
Layer 3: Sistema di controllo	Lo stadio di controllo del dispositivo di protezione risulta costituito da un dispositivo a microcontrollore, da un elemento di memoria e dalla componentistica ausiliaria necessaria per la generazione dei segnali di pilotaggio dei componenti switching del layer 1.
Layer 4: Sistema di comunicazione e crittografia quantistica di dati e comandi	Il layer 4 è costituito da un sistema per la ricezione di dati e comandi e la trasmissione degli stessi mediante un canale pubblico ed un canale quantistico. Le funzioni di comunicazione di questo strato si basano su strategie e tecnologie di Quantum Key Distribution[4].
Layer 5: Strato di set, segnalazione e visualizzazione	Il layer 5 del dispositivo di protezione proposto contiene LED per una visualizzazione rapida delle condizioni di funzionamento del dispositivo, pulsanti per impostare localmente soglie e tempistiche di intervento e display per la visualizzazione delle principali grandezze in tempo reale.

[4] Pelucchi, E., Fagas, G., Aharonovich, I. et al. The potential and global outlook of integrated photonics for quantum technologies. Nat Rev Phys 4, 194–208 (2022). https://doi.org/10.1038/s42254-021-00398-z.

Layer 1: Stadio di potenza del sistema di protezione a stato solido

Il primo strato del dispositivo di protezione sarà caratterizzato da dispositivi di commutazione allo stato solido SSCB, anche basati su materiali di tipo Wide Band Gap. Tali dispositivi saranno pilotati dai relativi segnali di gate (CTR_R, CTR_S, CTR_T e CTR_N) generati dal microcontrollore posizionato nel layer 3 dell'apparato di protezione.
In Figura 1 sono riportati lo schema di alto livello e la descrizione del layer 1.

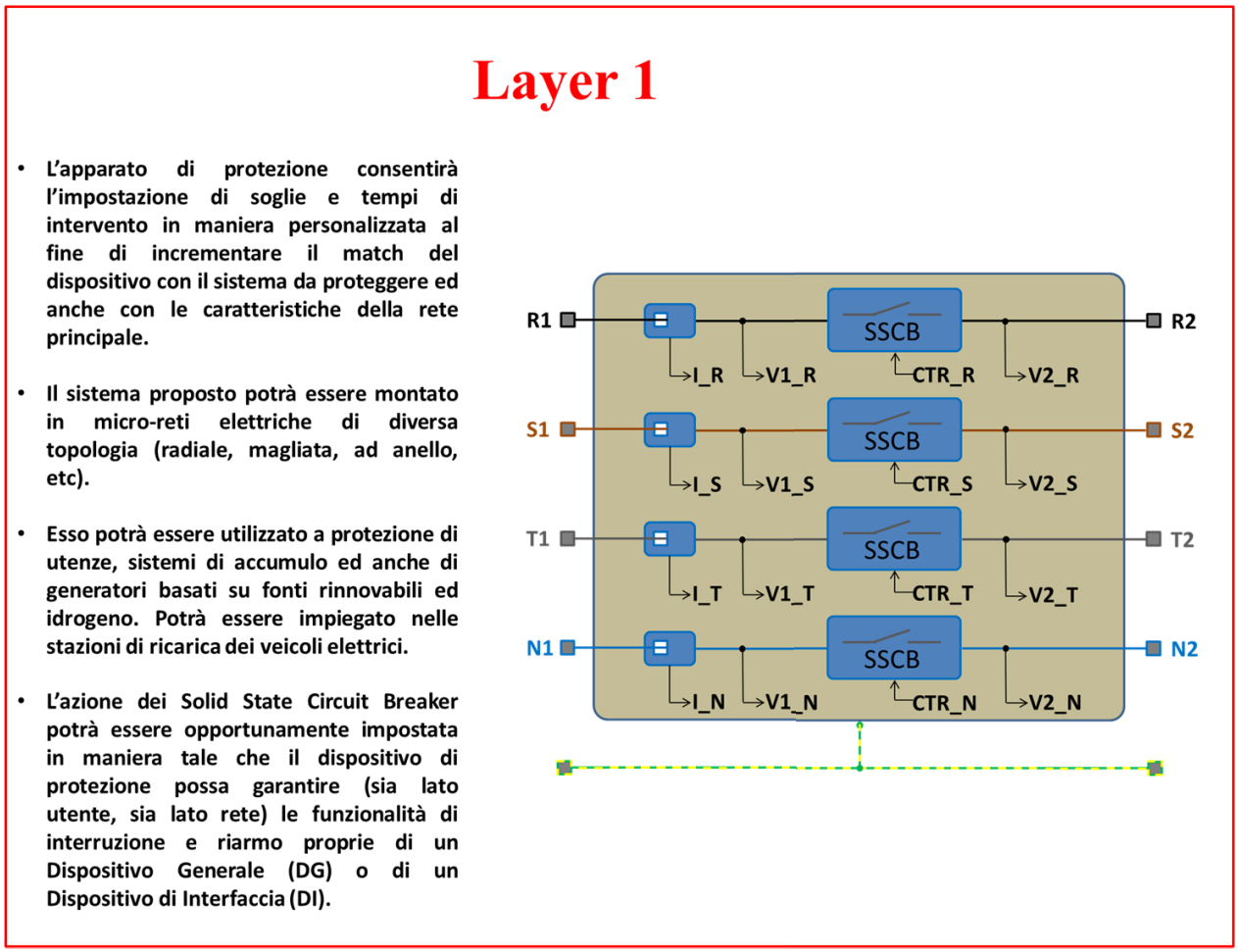

Figura 1: Layer 1 - stadio di potenza del dispositivo di protezione

Layer 2: Alimentazione del sistema elettronico e circuiteria di condizionamento e misura

Nel secondo strato saranno collocati i circuiti per l'alimentazione del dispositivo proposto (PS_1, PS_2), i trasduttori di misura e i componenti di condizionamento delle grandezze (tensioni, correnti ai terminali d'ingresso e d'uscita) in modo da renderle idonee ai canali d'ingresso (ADC) del microcontrollore (layer 3). In Figura 2 vengono riportati lo schema di alto livello e la descrizione del layer 2.

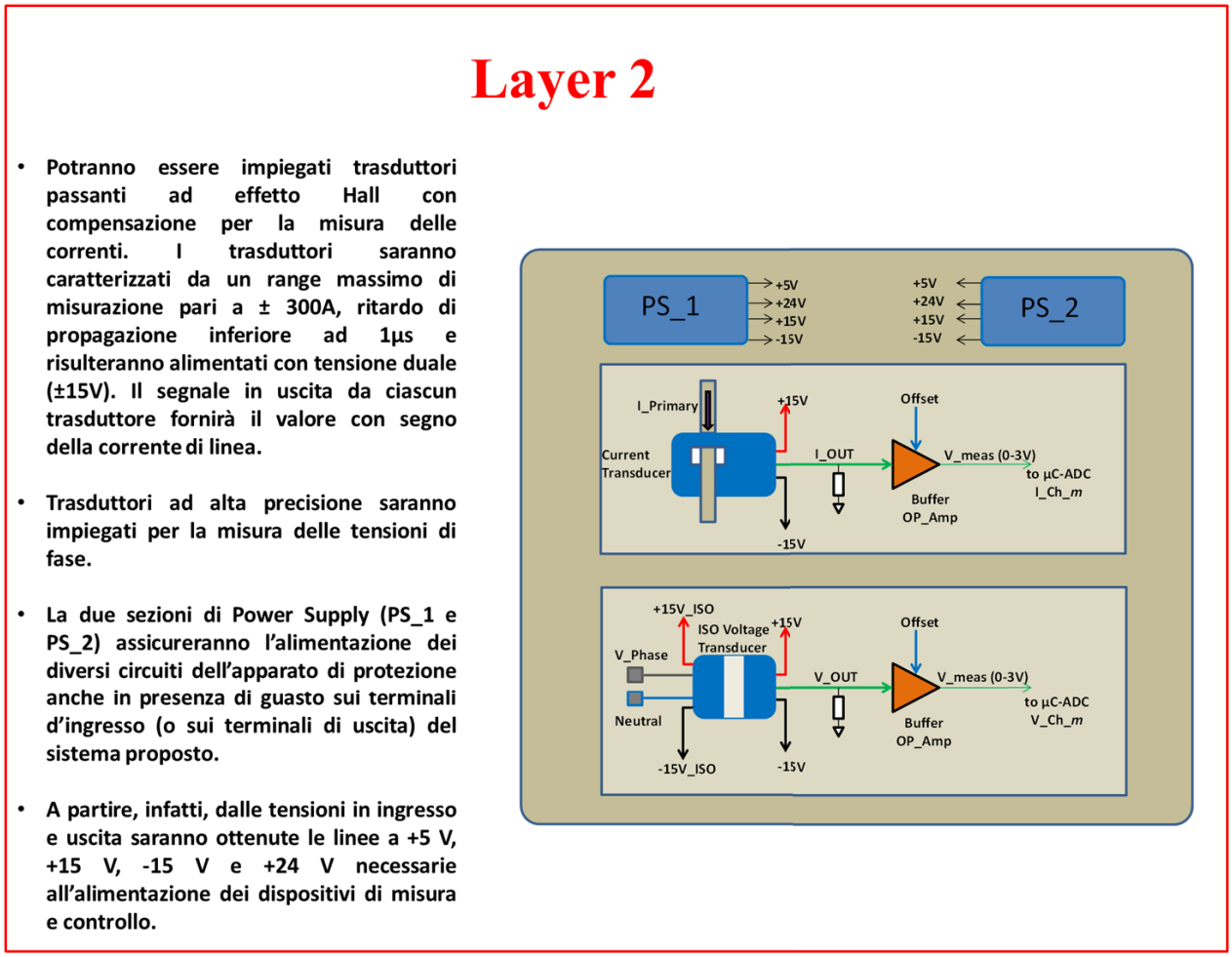

Figura 2: Layer 2 - stadio di alimentazione, condizionamento e misura del dispositivo di protezione

Layer 3: Sistema di controllo ed interfaccia utente del dispositivo di protezione

Lo stadio di controllo del dispositivo di protezione rappresenta il *core* dell'apparato. Esso sarà dotato dei componenti e della circuiteria ausiliaria necessaria all'implementazione e attivazione delle operazioni "elettriche" di interruzione e riarmo, nonché delle strategie e funzionalità per la cyber-resilienza delle micro-reti. L'apparato proposto viene schematicamente rappresentato in Figura 3.

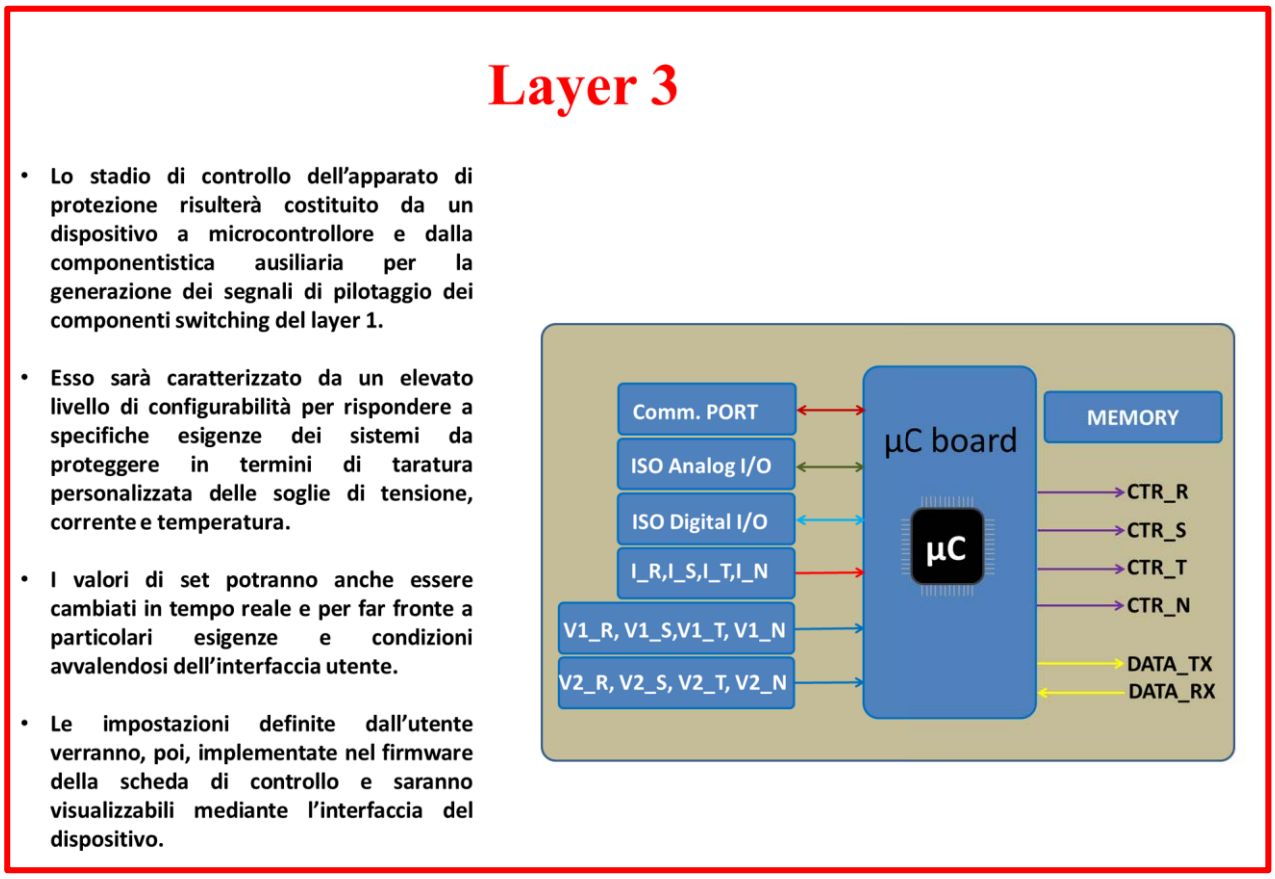

Figura 3: Layer 3 - stadio di controllo del dispositivo di protezione

A titolo di esempio vengono riportate, nelle seguenti figure, alcune schermate dell'interfaccia relativa al dispositivo di protezione ed i relativi contenuti.

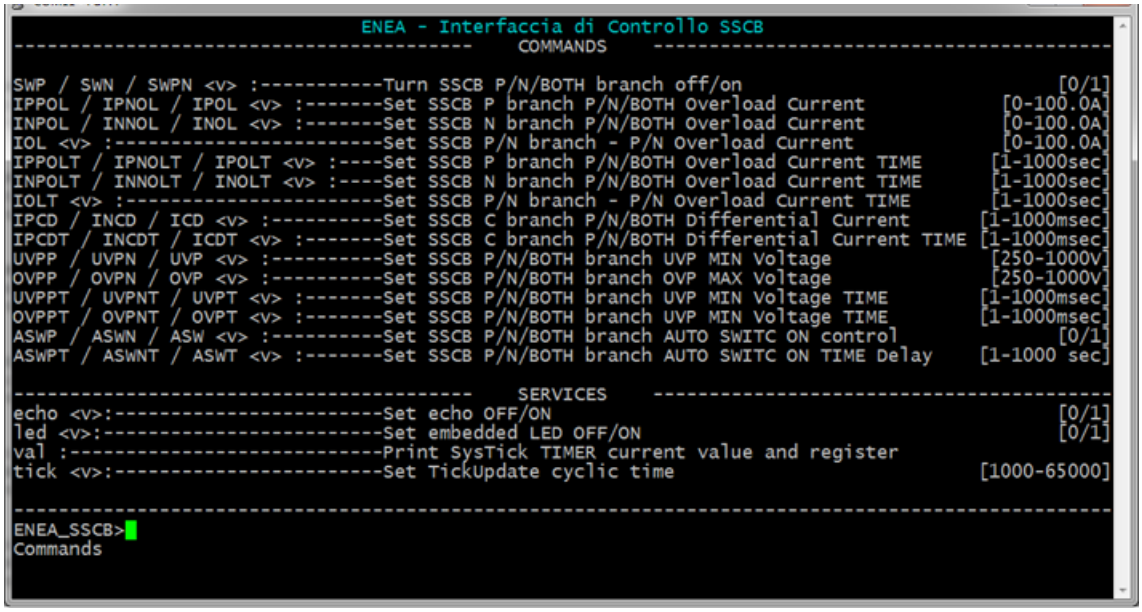

Figura 4: Esempio: schermata dell'interfaccia relativa al dispositivo di protezione

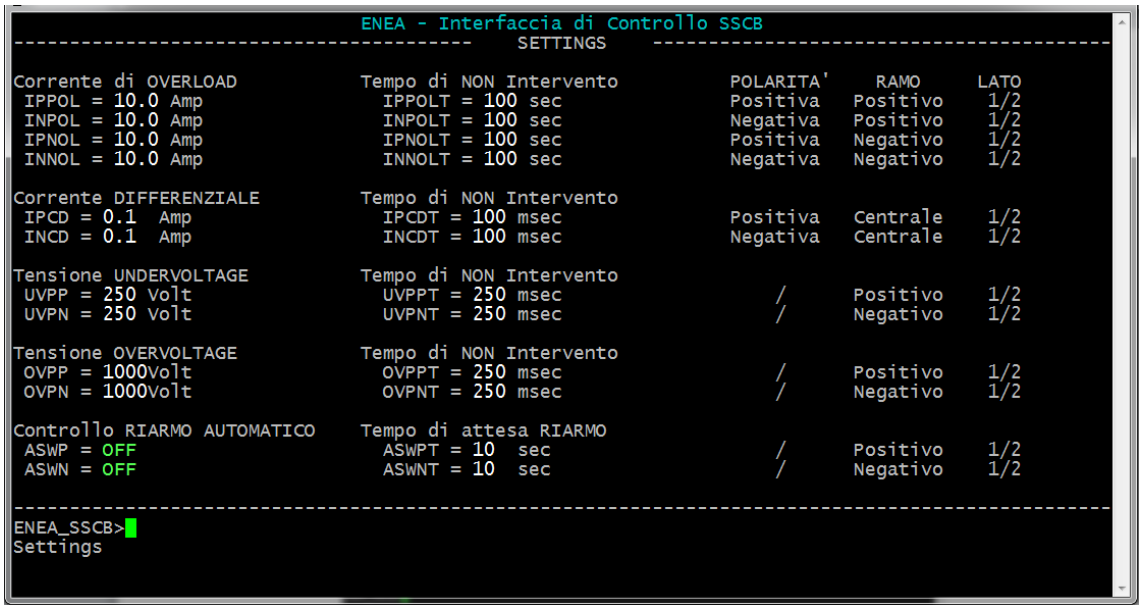

Figura 5: Esempio: schermata delle impostazioni del dispositivo di protezione

Un elemento di memoria sarà aggiunto al layer 3 per conservare le impostazioni ed il log delle condizioni operative del dispositivo di protezione.

Layer 4: Sistema di comunicazione e crittografia quantistica di dati e comandi

Il layer 4 è costituito da un sistema per la ricezione di dati e comandi e la trasmissione degli stessi da o verso altri apparati di protezione della rete microrete considerata. È importante tener presente che, nei sistemi di distribuzione locali (come le micro-reti) viene, sempre più frequentemente, cablata la fibra ottica, mezzo idoneo all'utilizzo come canale quantistico per la trasmissione dati.
Nel dispositivo di protezione descritto, lo strato 4 sarà basato su un sistema di comunicazione cifrata che si avvale della crittografia quantistica QKD (Quantum Key Distribution). Tale metodo si basa sulle leggi della meccanica quantistica e sfrutta il principio di indeterminazione di Heisenberg secondo cui la conduzione di una misura su una variabile quantistica (osservabile) provoca la perturbazione del sistema in esame. L'applicazione di tale principio alla comunicazione di dati comporta il notevole vantaggio di poter rilevare la presenza di un intercettatore (eavesdropper) sul canale di comunicazione.
La sicurezza nella trasmissione e ricezione di dati mediante crittografia quantistica richiede la presenza di due canali di comunicazione tra i dispositivi che si scambiano dati: uno di tipo classico (pubblico) ed uno di tipo quantistico (costituito da un apparato per la generazione di fotoni polarizzati, da un mezzo trasmissivo per il passaggio dei fotoni, come la fibra ottica, e da un analizzatore di polarizzazione). Nella crittografia di tipo classico, il sistema/apparato trasmettitore (denominato "Alice") e quello ricevitore (denominato "Bob") si avvalgono di un algoritmo pubblico che codifica il dato da scambiare con una chiave nota solo ad Alice e Bob. L'idea è quella di evitare possibili condizioni di rischio avvalendosi di una tecnica crittografica con scambio quantistico delle chiavi. In tal caso, lo scambio della chiave utilizzata da Alice per inviare un messaggio a Bob avviene immettendo una sequenza di bit quantistici, denominati "qubit", sul canale quantistico. Un qubit viene ottenuto mediante un fotone polarizzato orizzontalmente, verticalmente o in modo obliquo. Lo scambio di chiavi quantistiche avviene in accordo ad un protocollo stabilito.
In Figura 6 vengono riportate le fasi necessarie allo scambio di chiavi quantistiche in accordo al primo protocollo QKD sviluppato da Bennet e Brassard nel 1984 e denominato "BB84".

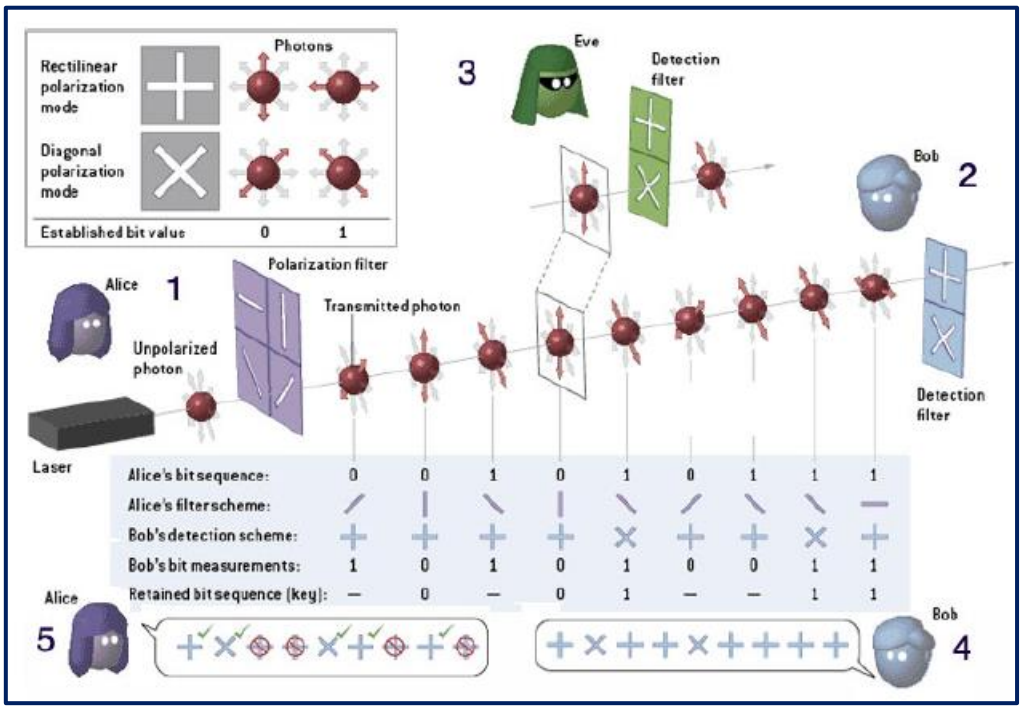

Figura 6: Scambio di chiavi quantistiche mediante il protocollo BB84 (i numeri indicano le diverse fasi del processo)[5]

[5]J. Lee, S. Kim et alii, Is Quantum State in BB84 Protocol Really Unclonable?, 2016.

1. In dettaglio, Alice dà il via alla trasmissione di un dato, scegliendo una stringa casuale di bit. Per ognuno di questi, Alice sceglierà ancora casualmente una base di trasmissione (o alfabeto) che ne identificherà la corrispondente tipologia di polarizzazione, come graficamente riportato in Figura 7.

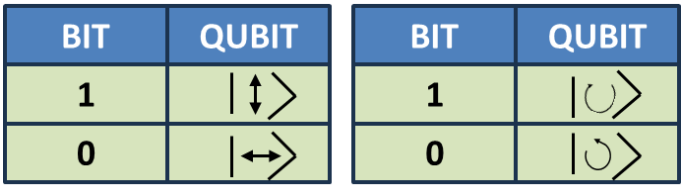

Figura 7: Basi o alfabeti di misura in trasmissione e ricezione (protocollo BB84)

2. Bob riceve ciascun qubit ed applica ad esso una base di misura scelta casualmente. Se quella scelta coincide con la base applicata da Alice, Bob riesce a misurare la polarizzazione che è stata applicata in trasmissione e riesce a comprendere correttamente il qubit trasmesso.

3. Nel caso in cui un intercettatore (Eve) si intromettesse sul canale quantistico, il processo di misurazione condotto sui qubit trasmessi perturberebbe il sistema. Ciò permetterebbe ad Alice e Bob di accorgersi dell'intercettazione.

4. Bob utilizza il canale pubblico per notificare ad Alice quali basi ha usato per misurare ciascun fotone.

5. Alice avvisa (su canale pubblico) Bob della corretta o erronea base utilizzata per ciascun fotone. Essi eliminano dalla sequenza quei qubit che Bob ha misurato con una base diversa da quella di Alice e, a questo punto, conoscono la stessa stringa di bit. Essi concordano, poi, su un sottoinsieme casuale della sequenza da confrontare per garantire la coerenza. A partire da tale sottoinsieme si ottiene la chiave segreta che Alice e Bob usano per crittografare e decrittografare il dato da trasferire.

   È bene sottolineare che le fasi 4 e 5 del processo descritto avvengono su canale tradizionale e richiedono un meccanismo sicuro di autenticazione.

   Il layer 4 (Figura 8) sarà costituito da componentistica sia per la trasmissione (TX) sia per la ricezione (RX), per la cifratura/decifratura dei messaggi e sistemi QKD per la generazione e la distribuzione di chiavi di tipo quantistico.

Layer 4

- Il layer 4 riceverà dati e comandi dal microcontrollore (layer 3) ed è in grado di trasmettere ad altri apparati di protezione della micro-rete. Esso sarà anche dotato di componentistica per la ricezione di dati e comandi da altri dispositivi di protezione e per l'elaborazione interna mediante invio al microcontrollore del layer 3.
- L'azione congiunta del layer 4 e del layer 3 consentirà l'attivazione di logiche preventive e mitigative di attacchi cyber.
- L'attività preventiva sarà assicurata mediante l'impiego di tecnologie quantistiche in cui la presenza di un eventuale intercettatore verrà rilevato con certezza dagli apparati che si scambieranno dati o comandi.
- Saranno implementati algoritmi per la gestione dell'evento "intercettazione" per cui, non appena l'apparato trasmettitore o ricevitore verificherà la presenza di "Eve", essi interromperanno lo scambio dati e attiveranno procedure di sicurezza stabilite a priori.
- Qualora l'attacco fosse veicolato mediante apparati diversi dal dispositivo di protezione, la presenza degli apparati proposti, utilizzati come DG, impedirà la propagazione della minaccia evitando aperture/chiusure fraudolente mediante azioni di segnalazione e messa in sicurezza.
- La segnalazione consisterà nell'invio di un "alert quantistico" ossia di una specifica sequenza di qubit agli altri dispostivi di protezione collegati. La ricezione di tale alert dovrà essere interpretata come una richiesta di attivazione di procedure di sicurezza.

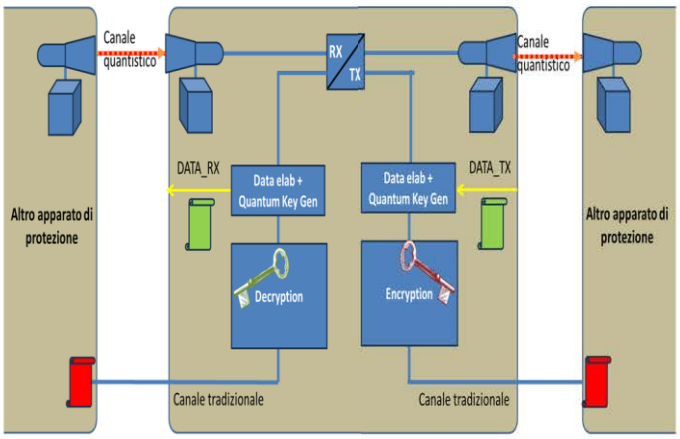

Figura 8: Layer 4 - stadio di comunicazione del dispositivo di protezione

Layer 5: Strato di set, segnalazione e visualizzazione

Il Layer 5 del dispositivo conterrà LED di diversi colori per una rapida valutazione delle condizioni operative del dispositivo (attivo/non attivo/guasto/anomalia).

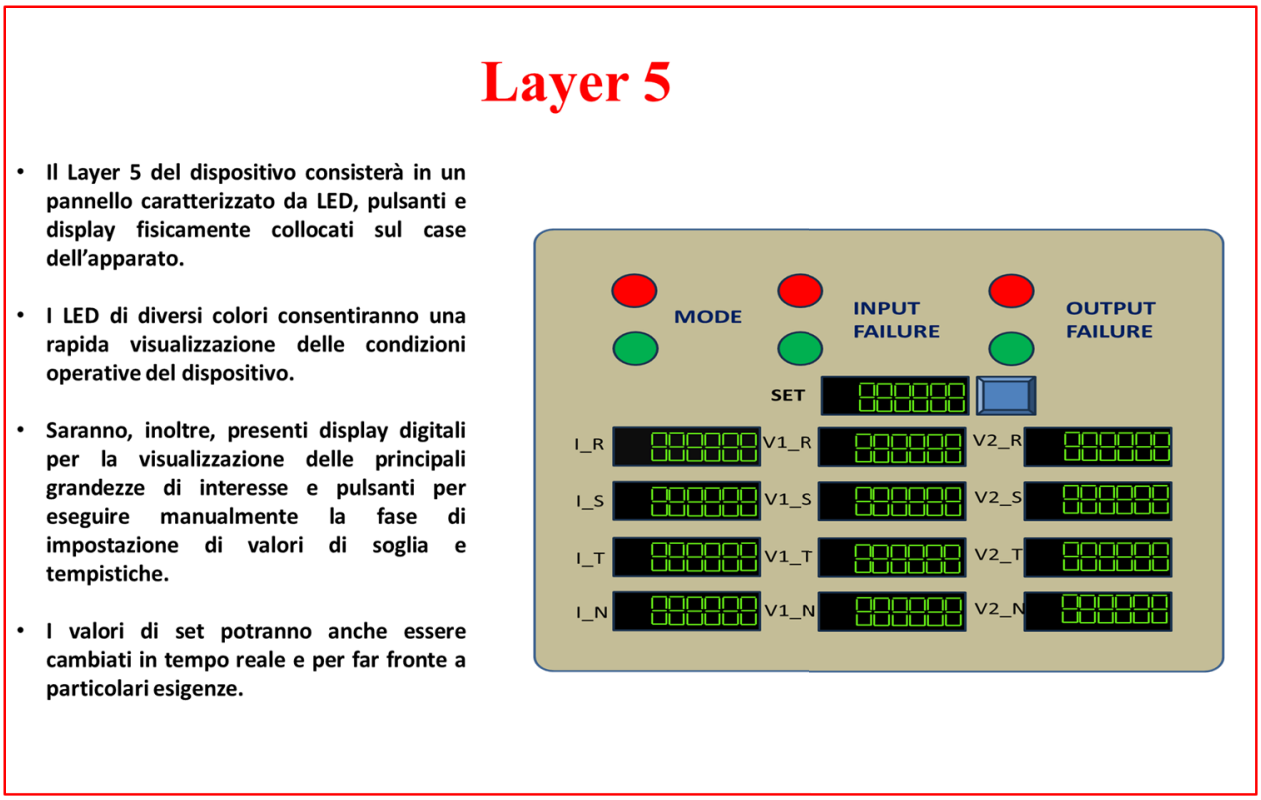

Figura 9: Layer 5 - Strato di set, segnalazione e visualizzazione

<u>Dispositivo di protezione avanzato: schema architetturale e caratteristiche del dispositivo (assenza di mezzo trasmissivo in fibra ottica)</u>

In ambiti come quelli delle reti di distribuzione in zone remote, il canale in fibra ottica potrebbe non essere presente. Il dispositivo di protezione presenterà lo stesso schema architetturale multilayer del primo dispositivo. In particolare, gli SSCB del layer 1 saranno definiti sulla base delle tensioni e delle correnti delle specifiche reti in MT o BT o dell'apparato di interesse. L'aspetto innovativo riguarderà il layer 4 per il quale il canale quantistico sarà ottenuto mediante cammini liberi in aria avvalendosi di tecniche Quantum Free Space[6]. Per la trasmissione dei qubit potranno essere, in tal caso, utilizzati telescopi o ricetrasmettitori innovativi.

[6] M. Ermini, V. Calà et alii Quantum Key Distribution Protocols for intrinsically secure communications on the Italian Railway Network, 13th World Congress on Railway Research, Birmingham 2022.

8 Contributo delle eventuali consulenze alle attività sopra descritte

(2000 caratteri max)

L'attività non ha previsto il ricorso a consulenze.

9 Pubblicazioni scientifiche

L'attività svolta è stata oggetto della seguente pubblicazione scientifica nel SAL:

G. Ferruzzi, V. Palladino, G. Adinolfi, M. Valenti and G. Graditi, "The role of protection systems in Smart Grids: the Protection Automation and Control application," 2023 International Conference on Clean Electrical Power (ICCEP), Terrasini, Italy, 2023, pp. 223-228, doi: 10.1109/ICCEP57914.2023.10247430.

10 Eventi di disseminazione

L'attività svolta è stata presentata alla conferenza International Conference on Clean Electrical Power (ICCEP) tenutasi a Terrasini (Palermo) dal 27 al 29 giugno 2023 in occasione della presentazione orale del lavoro "The role of protection systems in Smart Grids: the Protection Automation and Control application".