

# Ricerca di Sistema elettrico



Prototipo di protezione elettrica e cibernetica per reti e/o microreti elettriche in zone con disponibilità di un mezzo trasmissivo in fibra ottica

Giovanna Adinolfi, Angelo Merola, Maria Valenti

Prototipo di protezione elettrica e cibernetica per reti e/o microreti elettriche in zone con disponibilità di un mezzo trasmissivo in fibra ottica

G. Adinolfi, A. Merola, M. Valenti (ENEA)

Dicembre 2024

Report Ricerca di Sistema Elettrico

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

Obiettivo 2: Digitalizzazione ed evoluzione delle reti

Progetto 2.1: Cybersecurity dei Sistemi Energetici

Linea di attività: 2.7

Responsabile del Progetto: M. Valenti

Responsabile Linea di Attività: G. Adinolfi

Mese inizio previsto: luglio 2023

Mese inizio effettivo: luglio 2023

Mese fine previsto: dicembre 2024

Mese fine effettivo: dicembre 2024

## Indice

|       |  |   |
|-------|--|---|
| 1     | Prototipo di protezione .....                              | 3 |
| 1.1   | Architettura del dispositivo di protezione .....           | 4 |
| 1.2   | Specifiche dell'apparato di protezione .....               | 5 |
| 1.3   | Sviluppo e assemblaggio del dispositivo di protezione..... | 7 |
| 1.4   | Funzionalità del dispositivo di protezione.....            | 8 |
| 1.4.1 | Protezione contro guasti elettrici .....                   | 8 |
| 1.4.2 | Protezione contro minacce cibernetiche .....               | 8 |
| 1.4.3 | Protezione contro eventi ibridi .....                      | 8 |

# 1 Prototipo di protezione

Le attività di ricerca della LA2.7 hanno fornito, come output, il prototipo del dispositivo CYber-electric PROtection over fiBER – **CYPROBER** – protezione elettrica e cibernetica (Figura 1) per per reti e/o microreti elettriche che si sviluppano in quelle zone con disponibilità di un mezzo trasmissivo in fibra ottica.

Si tratta di una protezione che si adatta a contesti e a topologie di rete diverse.

CYPROBER è stato concepito come un dispositivo altamente configurabile e settabile sia in fase d’installazione, sia durante le fasi operative. La customizzazione del funzionamento di tale protezione può essere effettuata localmente, mediante cavo USB, o da remoto, avvalendosi del mezzo trasmissivo in fibra ottica.

CYPROBER può essere utilizzato in schemi di protezione che prevedono il coordinamento (amperometrico, cronometrico o logico) con dispositivi “gemelli”.



Figura 1: CYber-electric PROtection over fiBER – **CYPROBER**: prototipo

## 1.1 Architettura del dispositivo di protezione

CYPROBER è caratterizzato dalla struttura multi-livello descritta in Tabella 1.

| Layer   | Funzione   |
|---|--|
| <b>Layer 1: Stadio di potenza del sistema di protezione a stato solido</b>                      | 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.   |
| <b>Layer 2: Alimentazione del sistema elettronico e circuiteria di condizionamento e misura</b> | 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.  |
| <b>Layer 3: Sistema di controllo</b>  | 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.   |
| <b>Layer 4: Sistema di comunicazione e crittografia quantistica di dati e comandi</b>           | <p>Il layer 4 è costituito da un sistema per la ricezione di dati e comandi e la trasmissione degli stessi. Le funzioni di comunicazione di questo strato si basano su strategie e tecnologie di Quantum Key Distribution (QKD).</p> <p>Il layer include gli apparati ALICE e BOB acquisiti nell'ambito della LA1.6 che, così integrati, consentono al prototipo di implementare la funzionalità di comunicazione e crittografia quantistica di dati e comandi. Essi rappresentano parte integrante del prototipo e non sono altrimenti utilizzabili poiché fisicamente collegati con gli altri layer del prototipo.</p> |
| <b>Layer 5: Strato di set, segnalazione e visualizzazione</b>                                   | Il layer 5 del dispositivo di protezione proposto contiene LED per una visualizzazione rapida delle condizioni di funzionamento del dispositivo.   |

Tabella 1: CYPROBER: layer dello schema architetturale

## 1.2 Specifiche dell'apparato di protezione

### Specifiche del layer 1 "Stadio di potenza del sistema di protezione a stato solido"

| Grandezza elettrica                          | Valore              |
|--|---------------------|
| Tensione di fase AC in Bassa Tensione        | 230 V <sub>LN</sub> |
| Massima corrente di linea                    | 100 A               |
| Corrente nominale operativa                  | Configurabile       |
| Corrente differenziale massima               | Configurabile       |
| Sovracorrente (sovraccarico, corto-circuito) | Configurabile       |
| Soglia di Over Voltage                       | Configurabile       |
| Soglia di Under Voltage                      | Configurabile       |
| Tempo di intervento                          | Configurabile       |
| Tempo di NON intervento                      | Configurabile       |

Tabella 2 - Specifiche del layer 1 "Stadio di potenza del sistema di protezione a stato solido"

### Specifiche del layer 2 "Alimentazione del sistema elettronico e circuiteria di condizionamento e misura"

| Layer  | Funzione   |
|--|--|
| Alimentazione del sistema di controllo           | Alimentazione della logica di controllo a microcontrollore: <ul style="list-style-type: none"> <li>tensione di alimentazione della logica: 5V</li> <li>tensione duale condizionamento segnale analogico: <math>\pm 15</math></li> <li>tensione di alimentazione interfacce: 24V</li> </ul> |
| Misura e condizionamento della corrente di linea | <ul style="list-style-type: none"> <li>Rilevamento e misura della corrente di linea con sensore di Hall</li> <li>Condizionamento e filtro attivo del segnale di misura</li> </ul>  |
| Misura e condizionamento della tensione di linea | <ul style="list-style-type: none"> <li>Rilevamento e misura della tensione di linea</li> <li>Condizionamento e filtro attivo del segnale di misura</li> </ul>  |
| Rilevamento della corrente di cortocircuito      | <ul style="list-style-type: none"> <li>Rilevamento mediante discriminatore a soglia veloce con isteresi</li> <li>Sistema di discriminatori a 2 oppure 3 soglie (2L/3L)</li> </ul>  |
| Rilevamento sovratensioni/sottotensioni          | <ul style="list-style-type: none"> <li>Rilevamento e misura della tensione di linea</li> </ul>   |

Tabella 3 - Specifiche del layer2 Alimentazione del sistema elettronico e circuiteria di condizionamento e misura"

### Specifiche del layer 3 "Sistema di controllo"

| Layer                             | Funzione  |
|-----------------------------------|---|
| <b>Tipologia microcontrollore</b> | Microcontrollore ARM-Cortex M0+, 48MHz, mod ATSAMD21J18   |
| <b>Alimentazione</b>              | Alimentazione singola 3,3V  |
| <b>Convertitore ADC</b>           | Interno, 12bit, 350kSpS, over sampling e decimazione a 16bit                                    |
| <b>Connessione I/O</b>            | Diretti del microcontrollore: interrupt, ingressi digitali, uscite digitali, ingressi analogici |

Tabella 4 - Specifiche del layer3 "Sistema di controllo"

### Specifiche del layer 4 "Sistema di comunicazione e crittografia quantistica di dati e comandi"

Il layer 4 è costituito da un sistema di trasmissione e ricezione di dati e comandi da o verso altri apparati di protezione della rete o della microrete. Esso si avvale delle tecnologie e dei protocolli di crittografia quantistica basati sullo scambio quantistico delle chiavi QKD. In tabella 5 sono riportate le specifiche tecniche dell'hardware necessario alla realizzazione del layer 4 mediante le apparecchiature QKD installate nell'ambito della LA1.6.

| Hardware per QKD   | Specifica              |
|--|------------------------|
| <b>Canale di connessione con altri apparati di protezione</b>              | In fibra ottica        |
| <b>Laser Pulse Generator</b>   | Basato su FPGA         |
| <b>Bit rate</b>  | 1GHz                   |
| <b>Protocollo quantistico</b>  | BB84 decoy code        |
| <b>Key generation rate</b>   | >2kbit/s @16dB         |
| Hardware per la cifratura  | Specifica              |
| <b>Latenza</b>   | 10µs a 1Gbps           |
| <b>Throughput</b>  | 1Gbps                  |
| <b>Sistema di accumulo per la memorizzazione delle chiavi quantistiche</b> | Presente               |
| <b>Memoria per il backup per chiavi quantistiche</b>                       | 10 giorni              |
| <b>Sistema di protezione da manomissione</b>                               | Sensori anti-tampering |

Tabella 5 - Specifiche del layer4 "Sistema di comunicazione e crittografia quantistica di dati e comandi"

## Specifiche del layer 5 "Strato di set, segnalazione e visualizzazione"

| Layer               | Funzione   |
|---------------------|--|
| Segnalazione locale | <ul style="list-style-type: none"> <li>• Segnalazione alimentazione interna regolare - gemma bianca</li> <li>• Segnalazione stato interruttore ON - gemma rossa</li> <li>• Segnalazione stato interruttore OFF - gemma verde</li> <li>• Segnalazione stato interruttore TRIP - gemma gialla</li> <li>• Segnalazione stato allarme Comunicazione Quantistica - gemma blu</li> </ul> |

Tabella 6- Specifiche del layer5 "Strato di set, segnalazione e visualizzazione"

### 1.3 Sviluppo e assemblaggio del dispositivo di protezione

A valle della fase di progettazione dell'apparato di protezione, i ricercatori ENEA sono stati impegnati nella prototipazione dello stesso.

L'idea è stata quella di sviluppare l'architettura multi-layer dell'apparato di protezione, proposto nella LA2.2, in maniera tale da collocarne le parti hardware in cassette standard per un'unità rack da 19 pollici.

A tal fine, le schede elettroniche (Figura 2) con i dispositivi elettronici, i trasduttori, il microcontrollore e tutta la componentistica necessaria allo sviluppo dei primi tre layer sono state implementate in modo da collocare tali Printed Circuit Board (PCB) nei cassette del rack, come mostrato in Figura 1.

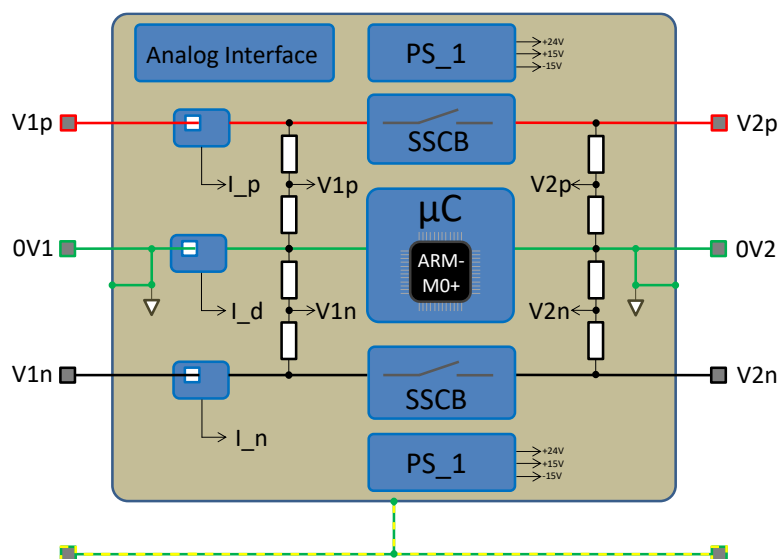


Figura 2: Collocazione dei componenti dei primi tre layer del dispositivo di protezione

Successivamente sono stati montati e saldati i componenti dei primi 3 layer.

Come descritto nel Rapporto Tecnico RdS\_PTR 22-24\_PR 2.1\_LA2.2\_067, il layer 4 della protezione è basato su un sistema di comunicazione che si avvale della crittografia quantistica QKD e su un sistema cifrante per la cifratura/decifratura dei dati e comandi ricevuti/trasmessi.

In questa prima realizzazione dell'apparato di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in reti e micro-reti elettriche, i ricercatori ENEA si sono avvalsi dei sistemi cifranti e di trasmissione/ricezione e crittografia quantistica dell'infrastruttura sperimentale realizzata presso il Centro Ricerche ENEA di Portici nell'ambito della LA1.6.

Il layer 5 del dispositivo di protezione è stato, infine, sviluppato sul pannello frontale del cassetto contenente l'hardware necessario alla realizzazione dei layer 1,2 e 3 (Figura 1).

Esso risulta costituito da gemme colorate. L'accensione delle diverse gemme avviene a seguito di una condizione specifica. In dettaglio, la gemma bianca viene accesa per segnalare che il dispositivo è installato ed alimentato. La gemma rossa si accende quando CYPROBER è nello stato ON. Nello stato OFF si accende, invece, la gemma verde, mentre quella gialla segnala che il dispositivo di protezione è nello stato TRIP. Si è verificato, quindi un guasto elettrico. Quando si accende la gemma blu è in corso un cyber attacco.

L'accensione di tali gemme è comandata dal microcontrollore a seconda delle condizioni operative. Esse sono alimentate mediante la circuiteria del layer 2 della protezione.

## 1.4 Funzionalità del dispositivo di protezione

### 1.4.1 Protezione contro guasti elettrici

CYPROBER è un dispositivo di protezione elettrica contro i seguenti guasti:

- Sovraccarico
- Corto-circuito
- Sovratensione
- Sottotensione

Specifiche strategie sono implementate nella protezione per ciascuna tipologia di guasto, come riportato in RdS\_PTR 22-24\_PR 2.1\_LA2.7\_136.

L'alta configurabilità del dispositivo consente la configurazione delle soglie e delle tempistiche d'intervento, nonché il tempo di riarmo ed il numero massimo di tentativi di riarmo consentiti a seguito di ciascun guasto.

### 1.4.2 Protezione contro minacce cibernetiche

CYPROBER è una protezione contro le azioni malevole di intercettatori non autorizzati dei dati trasmessi o ricevuti dal dispositivo. Esso si avvale di tecnologie QKD per la cifratura sicura dei dati e dei comandi. Continuamente CYPROBER esegue la valutazione del Quantum Bit Error Rate, ossia dell'indicatore delle prestazioni di un canale di comunicazione quantistica. Tale indice tiene conto degli errori nel collegamento ed è definito come il rapporto tra il numero (o la frequenza) di bit errati e il numero (o la frequenza) dei bit totali ricevuti. Il dispositivo invia dati solo se il valore di QBER risulta inferiore ad una soglia di sicurezza  $QBER_{max}$ . Valori superiori a tale soglia sono "sintomo" della presenza di un intercettatore sul canale. In tal caso, CYPROBER interrompe la comunicazione e vengono inibite le configurazioni da remoto del dispositivo. In tali condizioni, la protezione mette in sicurezza i dati interrompendo la comunicazione e inibendo le funzionalità di configurazione da remoto.

### 1.4.3 Protezione contro eventi ibridi

CYPROBER funge da protezione anche nel caso di eventi ibridi, ossia quelli in cui si verifica non solo un guasto di natura elettrica (sovracorrente, sovra/sottotensione), ma si presenta anche un attacco cibernetico.

In tali condizioni, il dispositivo di protezione attiva le logiche relative alla specifica tipologia di guasto elettrico ed interrompe la comunicazione e le configurazioni remote.

La logica sviluppata permette sia il riarmo dell'interruttore a seguito del guasto elettrico, sia il ripristino della comunicazione e delle configurazioni remote, quando la rete non è più sotto l'azione del cyber attacco.

CYPROBER può anche gestire i due ulteriori eventi ibridi:

- Riarmo elettrico, attacco cyber in corso
- Guasto elettrico in corso, rientro da un attacco cyber

Si segnala che il prototipo CYPROBER e tutti i suoi componenti/layer è un prodotto della Ricerca di Sistema Elettrico -progetto 2.1 e viene adoperato soltanto per le attività sperimentali del progetto stesso.