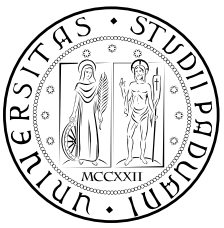

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI TECNICA E GESTIONE DEI SISTEMI INDUSTRIALI
CORSO DI LAUREA TRIENNALE IN INGEGNERIA MECCATRONICA

TESI DI LAUREA TRIENNALE

Stato dell'arte sulle microreti elettriche e relativi temi sulla sicurezza informatica

Relatore: Tommaso Caldognetto

Laureando: Samuele Visentin
1168731-IMC

ANNO ACCADEMICO: 2021-22

SOMMARIO

Il seguente lavoro inizia con un breve esposizione del panorama energetico mondiale, portando l'attenzione sui temi dell'energia elettrica e di come questa venga distribuita ed utilizzata nel mondo. Considerando l'inquinamento apportato dalla generazione attraverso i metodi tradizionali e le possibili evoluzioni per una distribuzione sempre maggiore di fonti rinnovabili all'interno del sistema elettrico mondiale.

Si passa alla descrizione del sistema microrete, dove viene posto nei sistemi di distribuzione e quali fonti energetiche sfrutta. Si identificano le topologie di funzionamento più comuni in cui l'energia elettrica viene distribuita, considerando poi i metodi di controllo delle variabili principali (tensione, frequenza, corrente,potenza attiva e reattiva) per le topologie di rete considerata. Identificando, verso la fine del capitolo, la parte fisica della microrete che implementa i controlli e la gestione dell'energia. Come ultimo sottocapitolo si descrivono i relativi problemi della sicurezza elettrica nelle microreti, identificando anche qui le diverse strategie adottate a causa delle differenti topologie presenti.

Infine si discute della sicurezza informatica delle microreti, dove data la loro natura fisica e informatica possono essere soggette a problemi di questo tipo. Partendo con la descrizione della struttura informatica e fisica in una MR si passa poi a definire le principali violazioni a cui è soggetta e si considerano i loro effetti sul sistema. L'ultimo paragrafo discute i metodi per implementare le difese e alcuni tipi di architetture che ne fanno uso.

RINGRAZIAMENTI

Ringrazio la mamma Vittorina, il papà Renato e il fratello Matteo
i quali mi hanno sempre sostenuto nei momenti di profonda difficoltà
durante il mio percorso di vita e universitario.

INDICE

1 Introduzione 1
2 Scenario energetico mondiale 3
2.1 Consumi energetici futuri 3
2.1.1 Consumi energetici nelle economie avanzate 4
2.2 Accesso all'elettricità 5
2.3 Fonti produzione energia elettrica 6
2.3.1 Fonti non rinnovabili 8
2.4 Sicurezza nella transizione energetica 9
2.4.1 Reti elettriche 12
3 microreti elettriche 15
3.1 Topologia e caratteristiche delle microreti 15
3.2 struttura delle microreti 17
3.2.1 Introduzione 17
3.2.2 La Microrete 18
3.2.3 Richiamo alle nanoreti 22
3.3 Classificazione delle microreti: C.A. e C.C. e relativi sistemi di funzionamento 23
3.3.1 Microreti in corrente alternata e relativi controlli 24
3.3.2 Microrete in corrente continua e relativi controlli 27
3.3.3 Altri tipi di microrete 29
3.4 Approfondimento su modalità e controlli delle microreti 31
3.5 Sicurezza elettrica nelle Microreti 34
3.5.1 Sistemi di sicurezza nelle reti in CA 35
3.5.2 Sistemi di sicurezza nelle reti in CC 37
4 Sicurezza informatica nelle microreti 39
4.1 Aumento del rischio per la sicurezza informatica 39
4.2 Struttura informatica di una microrete 40
4.2.1 Architettura informatica di una microrete 42
4.3 Tipi di attacchi informatici e relative conseguenze 43
4.4 Architetture e strategie di protezione 49
4.4.1 Architetture di protezione delle Microreti 51
Conclusioni 55

Appendici
A Appendice 59
A.1 Definizioni 59
A.2 Riferimenti figure 60

Bibliografia 63

ELENCO DELLE FIGURE

Figura 2.1 Popolazione globale per regioni senza accesso all'elettricità : *Rosa*: Africa sub-sahariana *Arancione*: regione Asiatica in via di sviluppo *Grigio*: resto del mondo *Linea blu*: totale della popolazione mondiale senza elettricità. `Nota`: asse delle ordinate abbiamo la popolazione in milioni 6

Figura 2.2 Popolazione globale per regioni senza accesso a fonti di cottura pulite: *Rosa*: Africa subsahariana *Arancione*: regione Asiatica in via di sviluppo *Grigio*: resto del mondo *Linea blu*: totale della popolazione mondiale senza fonti di cottura pulite. `Nota`: asse delle ordinate abbiamo la popolazione in milioni 7

Figura 2.3 Generazione Eolica e Solare (FV) per scenario 2020-2030 *Grigio*: storico degli anni precedenti. *Azzurro*: STEPS *Giallo*: APS *Verde*: NZE `Nota`: asse ordinate abbiamo TeraWatthour [TWh] 9

Figura 2.4 Aumenti di capacità delle rinnovabili negli scenari APS e NZE,2020-2030 *Azzurro*: economie avanzate e Cina. *Blu*: Resto del mondo `Nota`: asse delle ordinate abbiamo la potenza in GigaWatt [GW] 10

Figura 2.5 Quote a bassa emissione di generazione elettrica nello scenario NZE, 2020-2030 `Nota`: asse delle ascisse abbiamo la percentuale di quota di elettricità pulita 11

Figura 3.1 topologia di una microrete e smart grids[17] 16

Figura 3.2 Architettura microrete[12] 19

Figura 3.3 Architettura microrete[2] 20

Figura 3.4 Architettura microrete[3] 20

Figura 3.5 Architettura microrete[2] 21

Figura 3.6 Architettura microrete[4] 23

Figura 3.7 Architettura microrete in corrente alternata (AC)[17] 25

Figura 3.8 Architettura microrete in corrente continua (DC)[17] 28

Figura 3.9 Architettura microrete in corrente alternata ad alta frequenza[2] dove abbiamo: Unified Power Quality Conditioner (UPQC), Universal Power Line Conditioner (UPLC) 30

Figura 3.10 Architettura microrete di tipo ibrido (AC & DC)[17] 31

Figura 3.11 Tipico scenario di una MR con un inverter collegato alla rete. Distribuzione degli inverter connessi alla rete che sono coordinati tra loro con un controllo gerarchicamente organizzato a livelli[14] 32
Figura 3.12 Protezione di una microrete in CA con funzionalità Plug&Play[2] 36
Figura 3.13 Sistema di protezione centralizzato nella MR in CA[11], *MGCC: Microgrid Central Controller*, *MCB: Miniature Circuit Breakers* 37
Figura 4.1 Architettura di una rete informatica e fisica per un sistema a MR[1]. Microgrid Controller Center: è il controllore centrale della microrete. 42
Figura 4.2 Classificazione dei Vettori d'attacco. Da sinistra verso destra abbiamo: *esplorazione*, *compromissione del dispositivo* , *compromissione della rete*, *attacchi all'integrità* e *attacchi d'interruzione del servizio* [1] 48
Figura 4.3 Componenti di sicurezza della microrete [6] 50
Figura 4.4 Applicazioni della tecnologia SOAR [6] 52
Figura 4.5 Categorie d'applicazione della sicurezza basata su ML [6] 53
Figura 4.6 Processo della Blockchain [6] 54

ELENCO DELLE TABELLE

LISTINGS

ACRONYMS

IEEE Institute of Electrical and Electronics Engineers

IEA International Energy Agency

NZE Net Zero Emission
VRE Variable Renewable Energy
STEPS Stated Policies Scenario
APS Announced Policies Scenario
DER Distributed Energy Resource
MR microrete
POI Point of Interconnession
PCC Point of Common Coupling
CA Corrente Alternata
RES Renewable Energy Sources
CC Corrente Continua
FDI False Data Injection

1 INTRODUZIONE

La crescita costante della domanda energetica e il peggioramento delle condizioni ambientali hanno spinto la ricerca verso una visione di produzione energetica rinnovabile. Ad oggi la diffusione di queste fonti non è sufficiente per soddisfare la domanda, benché l'aumento e la distribuzione di queste sorgenti rinnovabili aumenti ogni anno.

In questo elaborato si presenta inizialmente il problema legato alla distribuzione dell'energia elettrica e la sua produzione, concentrandosi sul problema generale dell'elettrificazione. Considerando innanzitutto i dati forniti dalla International Energy Agency (IEA) ho descritto un panorama del consumo energetico per poi passare ai piani adottati per raggiungere una quasi totale emancipazione dall'uso delle fonti fossili. Per arrivare al livello di zero emissioni nette, in cui la produzione di gas climalteranti è bilanciata dalla quantità di gas che viene tolta dall'atmosfera, gli sforzi intrapresi fino ad ora non sono sufficienti. E le scelte politiche per portare il mondo verso questo obbiettivo sono altrettanto insufficienti. Lo sfruttamento delle infrastrutture presenti per la generazione e distribuzione dell'energia elettrica non saranno in grado di soddisfare il continuo aumento della domanda energetica, mentre il classico sistema di generazione, trasmissione e distribuzione centralizzato non è adatto al nuovo tipo di mercato energetico che si sta affacciando negli ultimi anni. Quindi, per questo motivo, sono richieste delle nuove metodologie di generazione e distribuzione che permettano ai nuovi utenti di accedere ad un minimo di energia elettrica, anche senza una connessione diretta alla rete principale. E a garantire ai vecchi utenti un metodo per generare la propria energia in modo affidabile, benché connessi alla rete principale.

Nel capitolo seguente si presenta la struttura di una microrete come possibile metodo per la generazione e distribuzione dell'energia elettrica. Inizialmente, si discute partendo dalla collocazione che può avere in una rete elettrica tradizionale, definendo poi le caratteristiche che la differenziano. Dopodiché, si identifica la struttura interna della microrete con le principali componenti che ne fanno parte, dando in seguito la definizione di microrete secondo gli standard internazionali. Si discutono le due topologie principali di microrete in Corrente Alternata (CA)/Corrente Continua (CC), con i relativi metodi di controllo e gestione dell'energia, presentando infine alcune topologie di rete simili alle principali descritte. Verso la fine del capitolo si da uno sguardo al dispositivo di potenza per la gestione e il controllo della microrete (e le sue sotto reti), indicando sommariamente la struttu-

ra e l'implementazione di questo. Infine, non si poteva tralasciare un sottocapitolo sulla sicurezza elettrica della microrete, dove anche qui, si suddividono i sistemi di sicurezza in base alle due topologie in CC e CA. Per poi osservare le principali differenze e difficoltà legate al tipo di corrente (alternata o continua) che viene utilizzata per la distribuzione all'interno della microrete.

L'ultimo capitolo presenta il problema della sicurezza informatica nelle microreti. Si evidenzia il fatto della loro forma fisica e informatica che permette un utilizzo "intelligente" della rete, amplificando le caratteristiche di comunicazione e gestione dell'energia generata. Ovviamente dall'altro lato, questa digitalizzazione porta con se la maggior parte dei problemi legati alla sicurezza informatica. Perciò, sempre in questo capitolo si descrive la struttura informatica della microrete, considerando alcuni dei protocolli di comunicazione in uso. Si passa alla descrizione delle principali violazioni con i rispettivi tipi di vettori d'attacco informatico, passando poi per i problemi che possono generare questi attacchi se vanno a segno nel sistema informatico della microrete. Infine si descrivono i metodi per contrastare questi attacchi con le relative architetture di protezione/mitigazione.

La maggior parte delle informazioni utilizzate per la scrittura di questa tesi, principalmente per i capitolo 3 e 4, sono state reperite nei documenti redatti dall'Institute of Electrical and Electronics Engineers (IEEE). Mentre, per il capitolo 2, la quasi totalità delle informazioni provengono dai report della IEA.

2 SCENARIO ENERGETICO MONDIALE

In questo breve capitolo si vuole presentare l'andamento energetico mondiale della domanda, consumo e infine produzione dell'energia elettrica negli ultimi anni e successivi. Dove i temi riguardanti l'aumento dei consumi, la maggiore elettrificazione, l'uso di fonti rinnovabili e la decarbonizzazzine sono i principali discussi, vista la scadenza entro il 2030 di non superare la temperatura mondiale di 1,5°C.
Quindi, ritengo che una parentesi sullo sfruttamento delle fonti di energia elettrica rinnovabile e non sia doverosa.

Denotando il fatto che le microreti si inseriscono in questo ambito come una delle principali soluzioni al problema energetico mondiale, sia dal lato produzione sia dal lato elettrificazione e vista la loro capacità intrinseca nello sfruttare l'energia elettrica in modo flessibile 3.

2.1 CONSUMI ENERGETICI FUTURI

Benché il Covid-19 sia stato traumatizzante per il sistema energetico globale la parte elettrica è stata la più resiliente tra le sorgenti energetiche, difatti la domanda globale per l'energia elettrica si è abbassata solamente del 1% durante il 2020, mentre nel 2021 si è visto un rimbalzo sopra i livelli del 2019 con un continuo aumento nel 2022 grazie al riprendersi delle economie incentivate dallo stimolo della spesa.

Le previsioni per i prossimi anni definisco una continua crescita nel consumo di energia elettrica come fonte primaria della domanda energetica, la quale supererà le altre fonti energetiche nei prossimi 25 anni[1].

Per il consumo energetico mondiale gli scenari presentati dalla IEA prevedono che nello Stated Policies Scenario (STEPS) ci sarà un aumento della fornitura energetica totale a livello globale del 1,3% annuo dal 2020 al 2030. Raggiungendo così una generazione totale di 670 exajoule ($ExaJoule = EJ = 10^{18}J = 277,778TWh(TeraWatthour)$) di energia. Mentre, nello scenario di tipo Announced Policies Scenario (APS), si prevede una crescita annua dell' 1% nei prossimi anni arrivando a produrre un massimo di 650 EJ. Dove entrambi gli scenari si discostano da quello che è lo Net Zero Emission (NZE), in cui si ha una previsione di crescita dello 0,7% annuo con un massimo di produzione previsto a 550 EJ entro il 2030.

Per quanto riguarda il consumo totale finale di energia abbiamo, secondo gli scenari presentati, che crescerà in media ogni anno del

1 https://www.iea.org/areas-of-work/promoting-digital-demand-driven-electricity-networks

1,7% dal 2020 al 2030 nello scenario STEPS, mentre la crescita nel caso APS sarà del 1,4%. Secondo queste previsioni il consumo finale entro il 2030 nello scenario APS sarà inferiore del 3% rispetto allo STEPS. Questa differenza presente tra gli scenari considerati è da considerarsi in gran parte causata dalla mancanza di un adeguata elettrificazione e alla minore efficienza energetica generale. Infine, negli anni a seguire le direttive correnti e quelle annunciate definiscono uno scenario in cui la domanda di energia elettrica sarà in continuo aumento. Infatti, negli STEPS si prevede una crescita del 30% da 23 300TWh (*TeraWattora*) di potenza nel 2020 a praticamente 30 000TWh entro il 2030 (la domanda prevista entro il 2050 dovrebbe avvicinarsi intorno ai 42 000TWh, pressoché oltre l'80% dei livelli odierni).

Principalmente, questo aumento della domanda è dovuto agli utenti finali del sistema di distribuzione elettrico. Ovvero, all'aumento delle abitazioni e dei dispositivi che utilizzano questo tipo di energia (si pensi all'aumento dei veicoli elettrici in questi anni). Si vedrà poi, nei prossimi paragrafi, come l'utente finale può essere parte della soluzione del problema energetico, diventando a sua volta produttore per soddisfare la propria richiesta energetica e in parte quella altrui, si parlerà in questo caso di prosumatore A.1.

Nei prossimi paragrafi, si pone l'attenzione su come le politiche energetiche adottate dagli stati europei e non, attraverso gli scenari presentati dalla IEA, hanno intenzione di affrontare le problematiche dovute a questa crescita della domanda di energia elettrica.

2.1.1 *Consumi energetici nelle economie avanzate*

Per quanto riguarda le economie avanzate abbiamo un aumento della domanda di energia elettrica dopo un periodo statico, in cui la domanda è rimasta quasi uguale per alcuni anni. I principali promotori di questo aumento della domanda sono i trasporti su strada e il riscaldamento. Questi fautori dell'aumento della richiesta energetica, utilizzando sempre di più fonti elettriche, tendono a spostare nel tempo i combustibili fossili sempre di più in secondo piano come fonte di energia primaria[7]. Per quanto riportato in [5] l'elettrificazione stessa può contribuire ad un abbassamento della domanda, perché molte delle tecnologie utilizzate per la gestione dell'energia elettrica sono significativamente più efficienti delle loro controparti a combustibili fossili. Si riporta l'esempio dei i veicoli elettrici di oggi in cui si usano in media meno del 70% di energia per percorrere un chilometro, rispetto alle convenzionali macchine con motori a combustione interna. Mentre, riguardo il riscaldamento degli edifici, attraverso l'uso delle pompe di calore la generazione di calore può essere più efficiente di tre o quattro volte dei rispettivi boiler convenzionali.

Nello scenario APS, l'espansione dell'elettrificazione permette di arrivare a ridurre la richiesta energetica di 10 EJ nel 2030, che equi-

valgono al 2,5% della domanda odierna, confrontata con l' 1,5% della richiesta energetica attuale negli STEPS.

2.2 ACCESSO ALL'ELETTRICITÀ

Da un punto di vista della distribuzione dell'energia elettrica mondiale l' obbiettivo è quello di raggiungere un elettrificazione totale entro il 2030. Dove nello scenario NZE questo obbiettivo è definito chiaramente, mentre negli scenari STEPS e APS non è ancora previsto questo traguardo.

Nello STEPS le politiche correntemente adottate e quelle previste non sono sufficienti a raggiungere una elettrificazione mondiale e un accesso alle fonti pulite per cucinareA.1. Si stima che circa 2,5 miliardi di persone non hanno un accesso a questo tipo di servizio e, come per l'elettricità, la crisi generata dal Covid-19 ha rovesciato i progressi fatti di recente per un accesso universale a questo tipo di servizi entro il 2030 2.2. Riguardo i problemi derivanti dalla mancanza di fonti per il *clean coocking system* [A.1], abbiamo un dato sconcertante, ovvero questa assenza provoca 2,5 milioni di morti premature all'anno, un rallentamento nello sviluppo economico e sociale con una fortificazione della disuguaglianza di genere.

Proseguendo nella trattazione abbiamo che le economie emergenti sono tuttora nel percorso che le porterà a soddisfare la richiesta per un elettrificazione totale. Ma questo non si può dire altrettanto per le economie in via di sviluppo dell'Africa sub-sahariana e Asia [5], le quali non riusciranno a soddisfare entro i limiti previsti l'obbiettivo di portare una fonte di energia elettrica o una soglia minima di questa fonte, per alimentare dei pacchetti base di servizi energetici[2] a tutti gli utenti finali.

Le cause principali che hanno rallentato questo sviluppo sono da imputare alla pandemia di Covid-19 e alla crisi energetica derivante dalla guerra scoppiata in Ucraina nell'ultimo anno, perciò, a questo tasso di velocità si prevede di raggiungere il 92% dell'elettrificazione mondiale entro il 2030. Quindi, per questo motivo è necessario accelerare il processo di elettrificazione totale, visto che oggigiorno ancora 770 milioni di persone non hanno accesso ad una fonte di energia elettrica. Come evidenziato poco fa, molte di queste si trovano nella zona sub-sahariana dell'Africa 2.1.

Per far fronte a questo problema e raggiungere un elettrificazione totale entro il 2030 sono richiesti degli investimenti di oltre 35 miliardi USD[3] , dove solo il 15% di quello che è realmente richiesto

2 Questi pacchetti base di servizi energetici sono definiti dalla IEA, mentre per l'accesso ad una soglia minima di fonte energetica non si ha una definizione univoca, si rimanda per un approfondimento a https://www.iea.org/articles/defining-energy-access-2020-methodology

3 si parla di circa 43 miliardi USD anno per riuscire nell'obbiettivo di un'elettrificazione totale entro il 2030 [7].

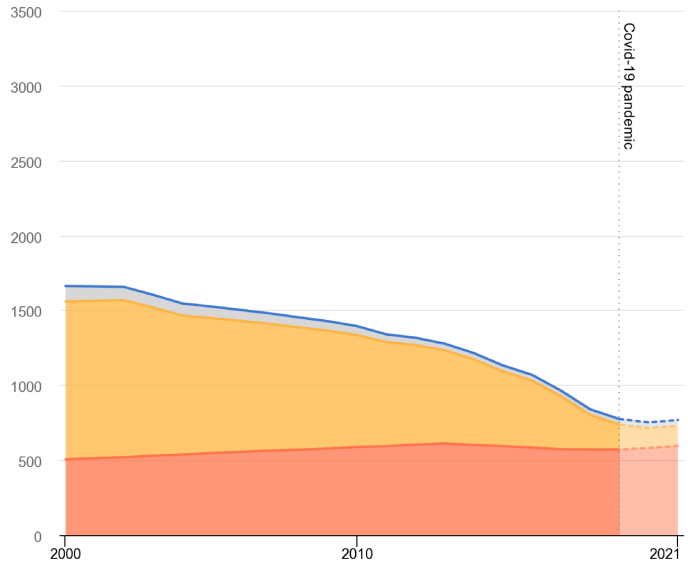

Figura 2.1: Popolazione globale per regioni senza accesso all'elettricità :
Rosa: Africa sub-sahariana
Arancione: regione Asiatica in via di sviluppo
Grigio: resto del mondo
Linea blu: totale della popolazione mondiale senza elettricità.
`Nota`: asse delle ordinate abbiamo la popolazione in milioni

viene tuttora investito nell'Africa sub-sahariana. Per quanto riguarda lo scenario più ambizioso proposto dalla IEA, ovvero lo NZE, questo disegna un percorso per portare l'energia elettrica a tutti entro il 2030. Nel quale meno della metà delle abitazioni avranno una connessione alla rete principale mentre, le mini-reti [3] saranno il 30% del totale delle reti utilizzate per distribuire l'energia elettrica agli utenti, infine il restante 25% sarà gestito dai sistemi autonomi.

2.3 FONTI PRODUZIONE ENERGIA ELETTRICA

Visto l'aumento del consumo di energia elettrica, con conseguente crescita della domanda, è richiesto un altrettanto aumento della produzione di energia elettrica. Dove, secondo quanto riferito in [5], il settore dell'elettricità ha il potenziale per rimodellare la domanda e l'approvvigionamento dell'energia, attraverso l'elettrifica degli utenti finale, l'utilizzo di energie rinnovabili e con altre forme di sorgenti energetiche a basse emissioni (ad esempio il biogas).

Comunque, ad oggi, il settore della produzione di energia elettrica è la maggiore fonte di **emissioni di CO_2**, queste in ogni scenario presentato dalla IEA, sono destinate a diminuire nella prossima decade. Tuttavia, le previsioni non sono cosi rosee, difatti per il 2030 si parla di una diminuzione delle emissioni del 10% negli STEPS e appena

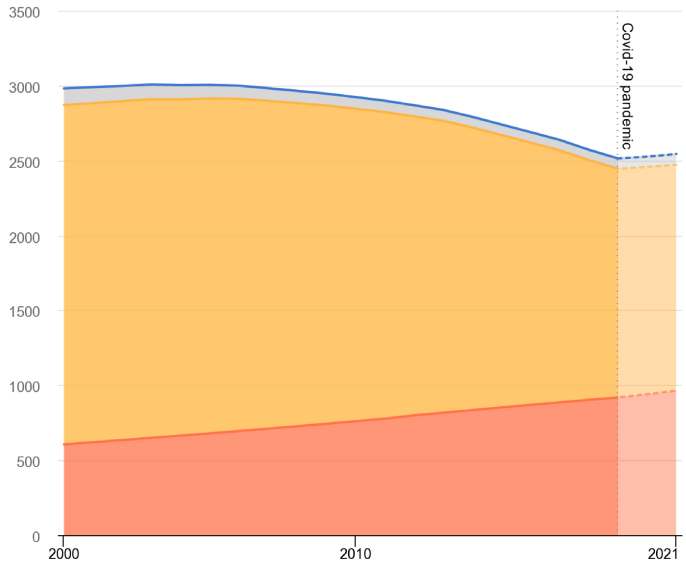

Figura 2.2: Popolazione globale per regioni senza accesso a fonti di cottura pulite:
Rosa: Africa sub-sahariana
Arancione: regione Asiatica in via di sviluppo
Grigio: resto del mondo
Linea blu: totale della popolazione mondiale senza fonti di cottura pulite.
`Nota`: asse delle ordinate abbiamo la popolazione in milioni

il 20% negli APS, comparato allo scenario lungimirante dello NZE che prevede di scendere al 60%. L'ultimo scenario indicato, identifica proprio l'elettricità stessa come mezzo per aprire la strada e a permettere di ridurre l'impatto ambientale negli altri settori, attraverso una maggiore diffusione dell'elettrificazione.

Come si è già visto, il fabbisogno elettrico aumenta costantemente nello scenario STEPS dove è presente un modesto allontanamento dalla fonte fossile del carbone, con un aumento del 30% delle fonti rinnovabili nel 2020 fino ad arrivare sopra il 40% nel 2030. Nello scenario NZE, molto più ambizioso, raddoppia la crescita della domanda energetica rispetto a quello annunciato nello STEPS, tagliando in maniera repentina lo sfruttamento delle centrali a carbone e aumentando al 60% la quota delle energie rinnovabili entro il 2030 (si veda figura 2.5).

Riguardo alle fonti rinnovabili, nel 2020 si è aggiunta alla fornitura mondiale di elettricità una quantità record di energia solare (fotovoltaico) e capacità eolica, anche se a causa della pandemia la domanda è diminuita leggermente. Per questo motivo la quota di combustibili fossili utilizzati per la generazione elettrica e scesa al minimo negli ultimi 20 anni, e la generazione di energia nelle centrali a carbone ha raggiunto la quota più bassa negli ultimi 50 anni. Purtroppo, la continua espansione nell'utilizzo delle risorse rinnovabili, non è sta-

ta sufficiente a compensare l'aumento dell'impiego dei combustibili fossili per soddisfare la richiesta crescente di elettricità, portando così alla ripresa delle emissioni di CO_2 nel 2021.[5]

Nella decade successiva, **la forte crescita delle rinnovabili è destinata a continuare in tutti gli scenari**, difatti, le politiche attuali portano ad un integrazione delle capacità combinate (si parla di fotovoltaico ed eolico) dalla quantità record di 248 GW nel 2020 a 310 GW nel 2030, questo nello scenario STEPS. Mentre, sono richieste delle misure di attuazione supplementari, per espandere l'implementazione della potenza generata dalle rinnovabili a quasi 470 GW nel 2030 nello scenario APS, dove la maggior parte di questa crescita deve essere raggiunta all'esterno della Cina, la quale si trova ad affrontare un lacuna di attuazione [A.1] relativamente piccola rispetto gli stati europei (ad oggi la Cina è il più grande mercato per il fotovoltaico e l'eolico, perciò hanno una difficoltà minore a reperire i generatori di "energia rinnovabile"). Infine, nello scenario NZE, è richiesto un aumento entro il 2030 di oltre 1000 GW della potenza combinata solare ed eolica (si veda 2.4).

Quindi, nello scenario STEPS, le fonti rinnovabili appena descritte andranno a soddisfare i tre quarti della domanda in crescita fino il 2030, mentre nell'APS coprirà il 90%, infine, nell'ambizioso scenario dello NZE si supererà facilmente la domanda in crescita. Questo significa che la percentuale di energia solare ed eolica nella fornitura di elettricità nel 2030 salirà dal 10% (2020) al 23% negli STEPS, del 27% nell'APS e del 40% nello scenario NZE. Si vedano gli andamenti2.3.

2.3.1 *Fonti non rinnovabili*

Riguardo alla fonte combustibile del **carbone**, per la generazione di energia elettrica, le previsioni verso il 2030 dei tre scenari variano di molto tra loro. In ogni caso è stata la risorsa principale per la generazione di energia elettrica nel 2020, ed è anche la colpevole di tre quarti delle totali emissioni di CO_2 provenienti dalla generazione elettrica.

Nelle economie avanzate, il carbone, continua ad essere la risorsa in maggior disuso nei tre scenari indicati. Il vero problema è nei mercati emergenti e nelle economie in via di sviluppo, dove la vera sfida è quella di rallentare e fermare la crescita dell'utilizzo del carbone prima che si inneschi un declino a lungo termine.

Per il **Gas naturale** nel settore energetico mondiale, abbiamo un incremento tra il 5% e 10% procedendo in direzione del 2030 per, rispettivamente, lo scenario STEPS e quello APS, anche se la quota di generazione dell'energia elettrica attraverso questa fonte sarà in declino nei prossimi anni. Inoltre in entrambi gli scenari, per quello che riguarda la generazione di energia elettrica, fornirà un essenziale flessibilità di sistema e un servizio di rete. Secondo [5] il gas naturale è la risorsa di maggior utilizzo per l'elettricità nelle economie avanzate

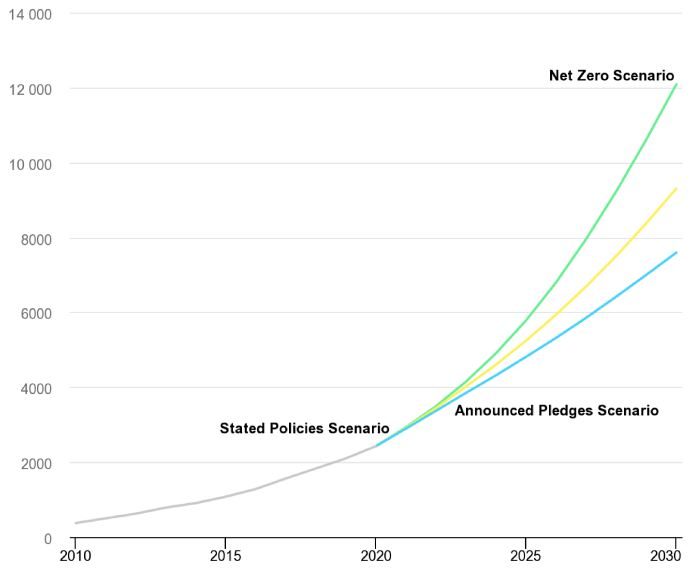

Figura 2.3: Generazione Eolica e Solare (FV) per scenario 2020-2030 *Grigio*: storico degli anni precedenti.
Azzurro: STEPS
Giallo: APS
Verde: NZE
`Nota`: asse ordinate abbiamo TeraWatthour [TWh]

e i suoi livelli di utilizzo rimarranno pressoché uguali nella prossima decade. Mentre, nei mercati emergenti e nelle economie in via di sviluppo, l'utilizzo del gas aumenterà di circa un terzo contribuendo a moderare l'uso del carbone come fonte primaria per la produzione di energia elettrica. Infine, nello scenario NZE, il gas naturale fornisce un ponte per diminuire le emissioni di CO_2 in modo sostanziale, spostando la necessità dalle centrali elettriche a carbone per produrre energia. Comunque, fino ad oggi i generatori termici a disposizione come le centrali elettriche (carbone o a gas) sono state le principali fonti di generazione,ma, grazie agli impegni presi, tutto questo sta rapidamente cambiando mentre la loro quota di mercato diminuisce.

2.4 SICUREZZA NELLA TRANSIZIONE ENERGETICA

Secondo quanto riportato in [7], la sicurezza elettrica è spesso definita come *la capacità del sistema di assicurare una disponibilità continua di elettricità* (in poche parole "tenere le luci accese"). Spesso, nel passato, ci si focalizzava sul garantire un adeguato sistema di approvvigionamento (sia di generazione che distribuzione) per affrontare una domanda variabile e aleatoria nel tempo, insieme alla flessibilità di far fronte ad un serie di interruzioni rilevanti. Ma, con l' aumento dell'utilizzo delle fonti rinnovabili (generazione eolica e solare), il paradigma della sicurezza, come lo conoscevamo, sta cambiando man mano che la

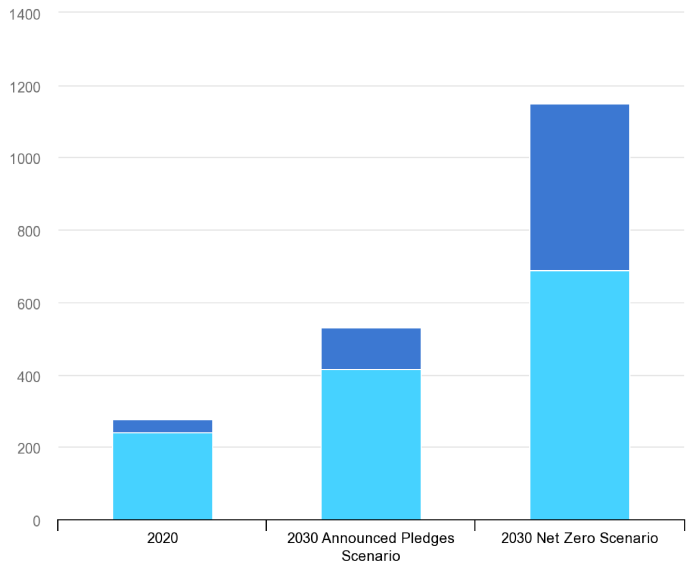

Figura 2.4: Aumenti di capacità delle rinnovabili negli scenari APS e NZE,2020-2030 *Azzurro*: economie avanzate e Cina. *Blu*: Resto del mondo
`Nota`: asse delle ordinate abbiamo la potenza in GigaWatt [GW]

generazione di energia elettrica diventa più variabile. Una possibile soluzione, a queste nuove sfide sulla sicurezza elettrica, può arrivare dall'utente stesso che genera la domanda [A.1], vedremo poi nel 3 come questo può avvenire.

Ancora di più, in [7], si riportano i fatti degli ultimi eventi atmosferici estremi nel mondo. Questi fenomeni hanno evidenziato come i rischi generati dai cambianti climatici sono parte della sicurezza energetica, e per questo motivo devono essere inclusi degli "stress test" negli studi di progettazione delle reti del futuro. Queste prove, oltre a presupporre degli eventi climatici estremi nella fase di design della rete, devo garantire un minimo di protezione dai malfunzionamenti della rete causati dalle crescenti minacce alla sicurezza informatica 4. Riguardo all'ultimo punto si nota, sopratutto negli ultimi anni, una digitalizzazione sempre maggiore dei sistemi di alimentazione. Questa apporta benefici a tutti i livelli, partendo da una migliore gestione della generazione e distribuzione di energia elettrica, fino ad arrivare alla nascita di nuove funzionalità e servizi per una ampia gamma di risorse, incluso il lato della domanda. Ma, l'aumento della digitalizzazione comporta dei maggiori e nuovi rischi alla sicurezza informatica. Dove un attacco informatico in grado di colpire il mio apparato di potenza può innescare una perdita del controllo dei dispositivi e dei processi svolti al suo interno, che a sua volta può causare dei danni fisici alle apparecchiature con una conseguente interruzione del servizio diffuso sui sistemi elettrici [4].

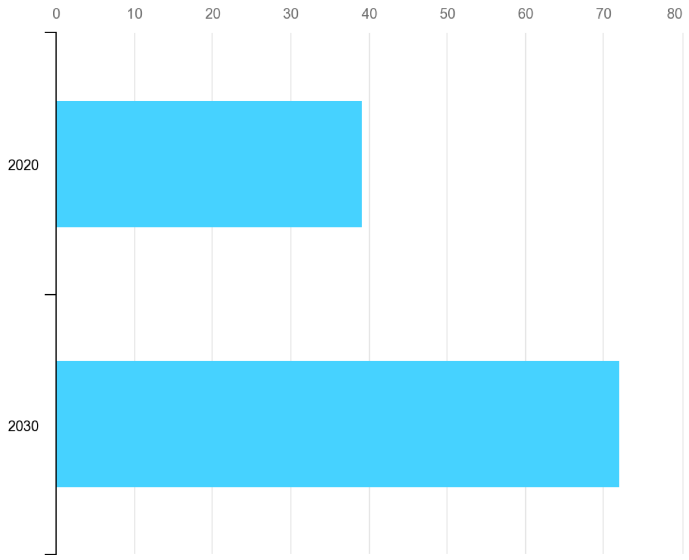

Figura 2.5: Quote a bassa emissione di generazione elettrica nello scenario NZE, 2020-2030
Nota: asse delle ascisse abbiamo la percentuale di quota di elettricità pulita

Nel [5] si fa riferimento al fatto che la flessibilità[4] dei sistemi elettrici è sempre più centrale nella sicurezza elettrica, dove i sistemi elettrici richiederanno una maggiore flessibilità da minuto a minuto, ad ora per ora e persino da stagione a stagione nella prossima decade. Il motivo della necessità di questa crescita della flessibilità a breve termine è da imputare allo scambio sempre maggiore delle quote di energia eolica e solare, che sono di loro natura variabile, e al cambio dei modelli della domanda elettrica. Sempre in [5], si evidenzia che nelle prossime decadi, nello scenario STEPS e in quello APS il fotovoltaico e l'eolico sono destinati a raddoppiare la loro quota combinata attuale di energia elettrica, pressoché il 10%, mentre si quadruplicherà nello scenario NZE. Persistentemente l'aumento dell'elettrificazione dei mezzi di trasporto, il riscaldamento degli edifici,i processi industriali e la comparsa della produzione elettrolitica dell'idrogeno; tutti questi assieme hanno la facoltà di rimodellare la curva di carico della richiesta di elettricità, e di conseguenza, aggravare le sfide per i sistemi elettrici in transizione. Come accennato prima entro il 2030 questi utenti finali nascenti sono destinati a far aumentare la loro quota di domanda elettrica per il 14% nello scenario STEPS, del 16% in quello APS e infine per lo NZE del 25%.

L'intermittenza della produzione e la natura variabile di queste tec-

4 La flessibilità è definita come *la capacità del sistema di alimentazione di gestire in modo affidabile ed economico la variabilità e l'incertezza presente nella richiesta energetica, e di fornirla su tutte le scale temporali rilevanti per assicurare una stabilità istantanea del sistema di alimentazione, in grado così di sostenere una sicurezza a lungo termine dell'alimentazione.*

nologie, basta sulle fonti rinnovabili, richiedono un'ulteriore flessibilità dei sistemi. Così questi saranno in grado di poter bilanciare in modo continuo l'erogazione di energia elettrica, soddisfare la domanda e mantenere una stabilità della rete di distribuzione. Infine, si può affermare che è in atto una transizione nella flessibilità delle reti elettriche, dove, in [5], sono presentate quattro sorgenti principali che contribuiranno ad assicurare l'equilibrio del fabbisogno elettrico e dell'approvvigionamento dalle risorse in qualsiasi momento:

- Centrali elettriche
- Tecnologie di stoccaggio
- Rimodulazione
- Reti elettriche

2.4.1 *Reti elettriche*

Per quanto detto in [5], le reti elettriche sono le fondamenta di un sistema elettrico affidabile ed accessibile, e per questo motivo, le rende delle infrastrutture critiche in tutte le economie moderne. Ad oggi ci sono circa 80 km di reti elettriche al mondo, ma si prevede che nella prossima decade saranno necessari degli ulteriori investimenti nella rete elettrica per la necessità di; aumentare sostanzialmente i sistemi di gestione, il miglioramento dell'affidabilità delle rete, il supporto alla transizione alle energie "pulite" e infine garantire un accesso all'elettricità a tutti nel mondo [2.2].

Nei soliti scenari analizzati dalla IEA abbiamo che; negli STEPS gli investimenti previsti nella rete di distribuzione e trasmissione salgono da meno di 300 miliardi (USD), in media all'anno, negli ultimi cinque anni ad oltre 370 miliardi nella prossima decade, con la maggior parte degli aumenti diretti nella distribuzione energetica. Mentre, nello scenario APS si prevede un aumento marginale negli investimenti nella rete entro il 2030. Infine nello scenario più ambizioso, lo NZE, gli investimenti entro il 2030 saranno in media di 630 miliardi (USD) per anno, un aumento importante, soprattutto nei settori in cui i nuovi progetti coprono un decennio o più.

Come abbiamo già visto prima, il principale catalizzatore degli investimenti per consolidare ed ampliare la rete elettrica è la continua crescita della domanda di elettricità. Modernizzare ed estendere l'infrastruttura della rete elettrica, (dalle linee di trasmissione e distribuzione alle sottostazioni o ad altre apparecchiature) costituisce la sfida principale per i proprietari e gli operatori dei servizi di distribuzione&trasmissione. Delle nuove linee di trasmissione saranno necessarie per connetter su larga scala le centrali eoliche e fotovoltaiche ai centri di domanda, qualche volta anche attraverso lunghe distanze. Mentre, delle nuove linee di distribuzione saranno necessarie per

gestire la potenza distribuita del fotovoltaico, il quale si quasi quadruplicherà entro il 2030 nello scenario APS e aumenterà di quasi sei volte nello scenario NZE.

Concludendo, per aggiungere nella rete sezioni nuove di strutture e/o rimpiazzarne altre, sono necessari degli investimenti nelle reti intelligenti e nei componenti digitali (che le compongono). Non da ultimo, per contribuire a garantire che l'espansione dei volumi del fotovoltaico e eolico possano essere ospitati in modo da perseguire un ottima stabilità e affidabilità della rete sono necessari altrettanti investimenti. Tutte le città del mondo hanno la particolare opportunità di accelerare il progresso verso le zero emissioni nette prendendo i vantaggi delle nuove opportunità proposte dalla digitalizzazione. Perciò un azione tempestiva è necessaria per tenere il passo con la transizione energetica, sapendo che i progetti delle reti elettriche, tendenzialmente, ci mettono più anni rispetto ai progetti delle energie rinnovabili, quindi un progresso inadeguato dello sviluppo può portare alla potenziale creazione di "colli di bottiglia" nell'assorbimento da parte della rete elettrica delle crescenti fonti di energie elettriche rinnovabili.

3

MICRORETI ELETTRICHE

Riprendendo dal capitolo precedente, si è visto come le difficoltà che il mondo sta affrontando in questa ultima decade e quella successiva, riguardo al panorama dell'energia elettrica, hanno reso le energie rinnovabili la prima scelta da perseguire per raggiungere l'ambizioso scenario del NZE.

Oltre l'aumento della domanda di energia elettrica, è presente la difficoltà di distribuire a tutti questa fonte primaria di sostentamento. Un possibile metodo per portare il mondo ad un elettrificazione totale è dare all'utente finale la possibilità di collegarsi alla rete principale su larga scala, ovviamente quando questo è possibile, ma è presente anche un altro metodo più fine. Ovvero, insieme all'utilizzo della rete principale, si hanno delle reti elettriche parzialmente autonome di minore dimensione e portata che permettono il normale funzionamento, anche quando la mia "sottorete" (che poi definiremo come *microreti*) è isolata dalla rete principale, così d'avere una continuità del servizio al mio utente finale [1].

In questo capitolo si andranno ad analizzare le principali strutture presenti in letteratura della microrete (MR), con le loro classificazioni e implementazioni in alcuni casi reali. Si vedranno i metodi più utilizzati per garantire la stabilità di tensione e corrente ai carichi connessi alla rete, si vedranno i metodi di funzionamento delle rete nei vari contesti in cui si trovano, infine si farà un breve cenno ai metodi per garantire la sicurezza elettrica all'interno di queste reti.

3.1 TOPOLOGIA E CARATTERISTICHE DELLE MICRORETI

Negli ultimi anni si inizia a vedere un cambiamento nel paradigma della generazione centralizzata dell'energia, con la conseguente trasmissione e infine distribuzione a tutti gli utenti finali. La generazione centralizzata è stata nominata per secoli come unica soluzione per soddisfare la richiesta di energia elettrica, ma facendo riferimento a quanto riportato in [2, 16, 17], si discute del fatto che questo tipo di approccio nei prossimi anni non sarà più in grado di sostenere la domanda di energia elettrica in constante crescita.

Per questo motivo la microrete [MR], in un prossimo futuro, si può individuare in un contesto più ampio. La quale è collegata ai limiti della rete elettrica 3.1 con i propri carichi,generatori indipendenti e

1 ad esempio molte nazioni utilizzano dei sistemi fotovoltaici per portare energia elettrica anche in luoghi dove è estremamente difficile collegare una o più abitazioni alla rete elettrica principale [7]

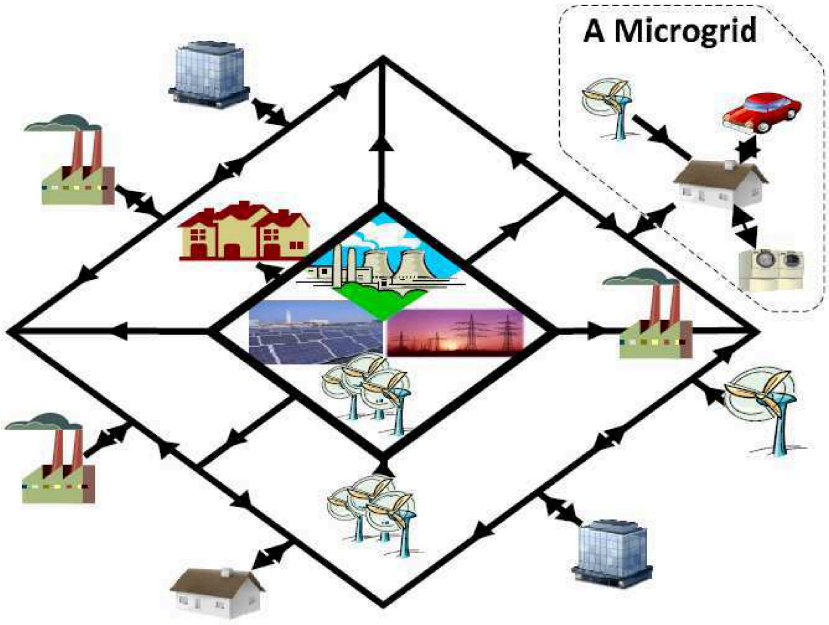

Figura 3.1: topologia di una microrete e smart grids[17]

accumulatori (che vanno sotto il nome di Distributed Energy Resource (DER)), permettendogli così di funzionare collegata o scollegata dalla rete di distribuzione principale. Si può pensare alla MR come ad una versione in scala ridotta del sistema elettrico centralizzato predominante. Questo perché come la rete elettrica ha i suoi sistemi di generazione, regolazione e accumulo la MR possiede le capacità di regolare il flusso di elettricità richiesto dal consumatore il tutto a livello locale, in cui possono essere presenti più utenti collegati.

Sempre in [17] si introduce il fatto che, dato un gruppo di vari generatori distribuiti, stoccaggi di energia e dispositivi di elettronica di potenza e regolatori, una MR può lavorare come una cella autogestita di un sistema elettrico più grande, ed essere in grado di controllare i suoi componenti interni per ridurre al minimo gli effetti negativi sulla rete esterna e tutelare l'utente nel caso di interruzioni della rete di distribuzione .

Si noti ancora come la figura 3.1 descriva un concetto topologico futuro, in cui una microrete residenziale di piccole dimensione con i propri carichi e DERs, si collega ad una rete intelligente di distribuzione. Dove è presente al centro il solito sistema di generazione e distribuzione centralizzato, con all'esterno, il concetto di microrete evidenziato dal tratteggio per identificare la sua non stretta appartenenza alla griglia principale.

Un'interessante lista di caratteristiche d'importanza delle microreti la troviamo in [2], dove si elencano le seguenti funzioni che dovrebbe garantire la MR:

- La normale alimentazione fornita nell'area di interesse della

MG deve essere garantita durante i disastri naturali, interruzioni di servizio, etc...

- I costi per le perdite attraverso la trasmissione e distribuzione della rete di alimentazione vengono salvate se la MG è in grado di soddisfare la domanda interna.
- Con la sempre crescente domanda di energia elettrica la creazione di MR può andare a differire la spesa per l'espansione della trasmissione e distribuzione del sistema elettrico tradizionale.
- Le MR utilizzano per lo più tecnologie rinnovabili ecocompatibili per la generazione di energia, le quali hanno quasi emissioni zero, quindi deve avere un basso impatto ambientale.
- L'affidabilità e la qualità dell'energia ricevuta dal cliente è notevolmente migliorata mediante la creazione di una MR grazie ai suoi sistemi di gestione e controllo dell'energia.
- Il costo per unità di energia si riduce notevolmente creando una MR, ad esempio attraverso l'utilizzo di una fonte disponibile localmente di energia rinnovabile nelle località remote e con la cogenerazione[2] nei centri di carico delle città.
- A lungo termine, le strutture delle MR saranno interessanti per le piccole attività che finirà per valorizzare l'economia locale e creare dei nuovi posti di lavoro locali.

Oltre queste importanti caratteristiche, ma generalizzate, in [14] troviamo una raffigurazione che andremo qui sotto a esemplificare e descrivere. In questo caso si rappresentano le quattro **funzionalità fondamentali** di una microrete, queste sono identificate come segue:

1. **Stabilità:** avere negli stati stazionari e nelle modalità operative transitorie dei margini di stabilità sufficienti.
2. **Flessibilità:** avere la possibilità di riconfigurare il sistema online durante i guasti disconnettendo la MR dalla rete elettrica.
3. **Scalabilità:** possibilità di rimuovere o aggiungere unità energetiche agevolmente.
4. **Supporto rete:** averla capacità di fornire servizi ausiliari.

3.2 STRUTTURA DELLE MICRORETI

3.2.1 *Introduzione*

Già all'inizio del nuovo secolo intorno agli anni 2000 in [15] si discute della difficoltà di portare avanti il paradigma della generazione elettrica centralizzata tradizionale e del suo sistema di erogazione. Con

2 Nei testi ci si riferisce con *Combined Heat and Power Generation*

i quali, la produzione e distribuzione diventerebbe troppo stretta e incompatibile a livello di costo per riuscire a soddisfare la domanda sempre crescente di energia elettrica.

Contemporaneamente, la ricerca tecnologica ha notevolmente migliorato il reparto della elettronica di potenza permettendo così il collegamento di fonti energetiche asincrone alla rete. Ovvero, l'esistenza di una quantità significante di risorse distribuite lungo la rete a bassa tensione, permette di creare un sistema di generazione e distribuzione che è nettamente diverso da quello che abbiamo visto svilupparsi negli ultimi 100 anni. Ovviamente, da questa nuova visione della rete elettrica si sono fatte spazio delle nuove sfide per l'ingegneria e altrettante nuove proposte di ricerca nel campo elettrico, però da questo possono nascere delle nuove forme di rapporti elettrici ed economici, tra i clienti e la rete tradizionale di distribuzione e, persino, tra i clienti stessi.

Sempre nel sommario [15] si porta una preliminare definizione di MR; vista come un piccolo gruppo di fonti, sistemi di accumulo e carichi che insieme si presentano alla rete principale come una legittima singola entità autosufficiente. Infine si parla del concetto che si trova al cuore della microrete, che è la nozione di un interfaccia flessibile ma controllabile di elettronica che si interpone tra la MR e il classico sistema di distribuzione più ampio, dove questa *"interfaccia"* a livello essenziale, isola i due lati della rete elettricamente. Tuttavia li collega economicamente permettendo la consegna e ricezione dell'energia elettrica e dei servizi accessori.

3.2.2 *La Microrete*

Per un primo paradigma di microrete troviamo in [12] un semplice esemplificazione del concetto, che la definisce come; *un gruppo di carichi e microfonti operanti come un unico sistema controllabile che fornisce potenze e calore entrambi nella sua area locale di utilizzo*. Dove guardandola da un altro punto di vista, la microrete, può essere concepita come una cella controllata del sistema di alimentazione.

Dopodiché si presenta sempre in [12] una struttura base, nella quale abbiamo una prima indicazione sulle componentistiche che la costituiscono; si parla delle microsorgenti come scelta primaria per tipo di sorgente, le quali sono piccole unità con un interfaccia elettronica di potenza che vengono posizionate dall'utente stesso [3]. Dopodiché riguardo l'elettronica di potenza, questa trova largo utilizzo nelle microreti perché fornisce il controllo e la flessibilità richiesta dal concetto stesso di MR, difatti una corretta progettazione di questa, con l'utilizzo dei controlli adatti, assicura che la microrete sia in grado di

3 queste fonti hanno solitamente un costo contenuto, una bassa tensione, con una buona affidabilità e basse emissioni (microturbine,pannelli fotovoltaici e cella a combustibile)

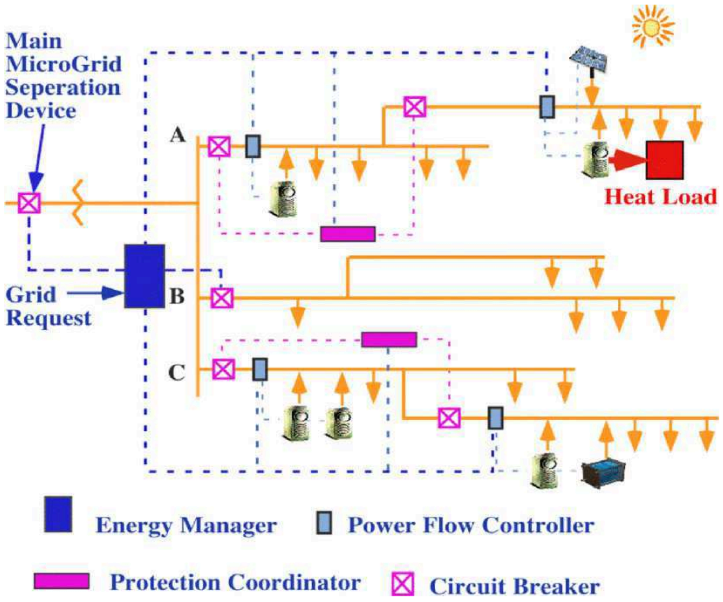

Figura 3.2: Architettura microrete[12]

soddisfare i bisogni energetici dei propri utenti, così come le esigenze di utilità.

Si presenta una prima raffigurazione base 3.2 dell'architettura di una MR in [12], dove si assume che il sistema sia radiale con tre alimentazioni A,B e C insieme ad una raccolta di carichi. Questo sistema radiale è connesso alla rete di distribuzione tramite un dispositivo di separazione, solitamente un commutatore di tipo statico. Si noti che ogni alimentazione ha un interruttore e un controllore per il flusso di potenza, quest'ultimo, dato il livello prescritto dall'*Energy Manager*, regola il flusso di potenza dell'alimentazione. Infine, man mano che i carichi si abbassano le microfonti locali aumentano e diminuiscono la loro potenza per mantenere costante il flusso di potenza 3.2.

In modo altrettanto simile in [2] (dopo una decina d'anni dall'uscita di [12]) si ha un concetto base di microrete molto simile a quello trovato in [12]. Dove identificano la MR come una singola unità controllata in un sistema di alimentazione, che può essere utilizzata come un singolo carico aggregato. Dopodiché questa MR è composta da generatori, stoccaggi di energia, controlli di carico e interfacce elettroniche di alimentazione come gli inverter. Evidenziano, infine, i due componenti critici della MR, ovvero; l'interruttore statico e le microsorgenti (che consistono in generatori, accumulatori e inverter). Si ha una disposizione della microrete in 3.3 molto simile a quella che abbiamo visto precedentemente in 3.2.

Anche in [3] troviamo una struttura generalizzata con dei potenziali elementi topologici di una microrete. Raffigurati in 3.4, abbiamo che, non tutti i componenti presenti sono da utilizzare e la combinazione tra l'utilizzo e non di questi elementi vanno a definire poi la capacità della MR di soddisfare oppure no alcuni tipi richiesti di

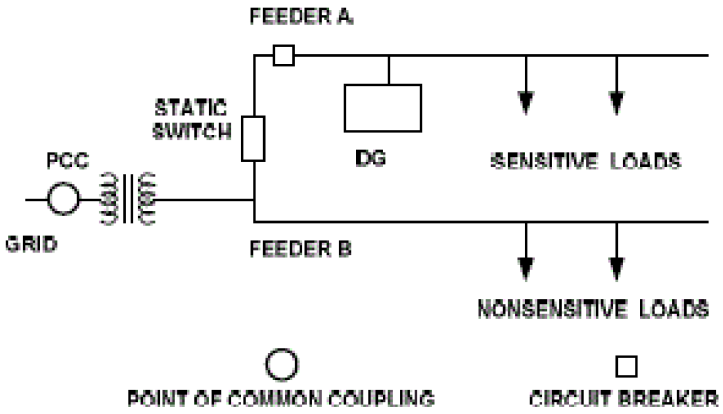

Figura 3.3: Architettura microrete[2]

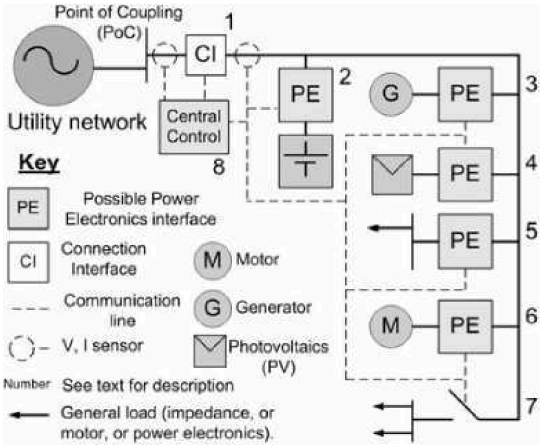

Figura 3.4: Architettura microrete[3]

necessita dell'utente. Infine, per generare il comportamento migliore richiesto da una microrete, rispetto ad un sistema convenzionale di distribuzione, sono necessari hardware e software aggiuntivi per controllare i flussi di tensione e corrente (quindi di potenza) nel sistema aggregato.

Dopo tutte queste descrizioni di MR intermedie, alla fine, si è arrivati allo standard IEEE 2030.7^{TM} – 2017 [10], dove abbiamo la definizione di microrete come;

> **un gruppo di carichi interconnessi e risorse di energia distribuita con confini elettrici chiaramente definiti, che permette di agire come una singola entità controllabile rispetto alla rete principale e può connettersi/disconnettersi dalla rete per consentirgli di operare sia in modalità connessa alla rete che in modalità isola (o isolata).**

Si vede riferito in figura 3.5 la struttura di una microrete in cui si possono individuare le componenti che ne fanno parte. Queste, presentate in [10], sono descritti come segue;

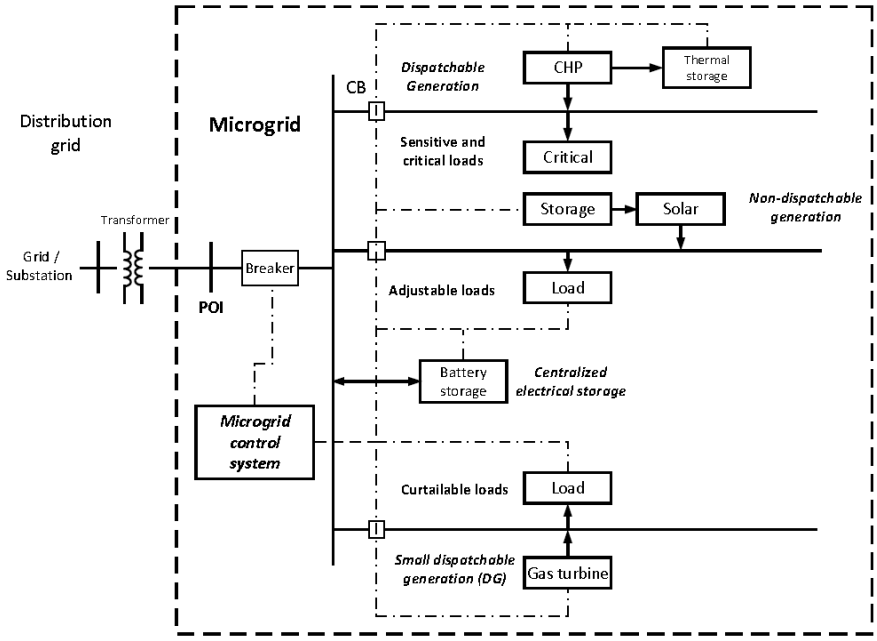

Figura 3.5: Architettura microrete[2]

CARICHI: I carichi all'interno di una microrete sono categorizzati in diverse tipologie. Nei termini di criticità e controllabilità abbiamo:

- *Carichi critici:* questi devono essere serviti in tutte le modalità operative della microrete e solitamente non possono essere ridotti.
- *Carichi prioritari:* si tratta di carichi che possono essere ridotti se è necessario.
- *Carichi controllabili:* questi tipi di carichi possono essere interrotti periodicamente oppure impostati a vari livelli di carico.
- *Carichi interrompibili*: Si tratta di carichi che possono essere sparsi o interrotti in qualsiasi momento per consentire la generazione di soddisfare la domanda.
- *Deviazioni o carichi di deposito:* questi sono usati quando è disponibile un eccesso di generazione e ridurre questa non è possibile, oppure dove c'è un vantaggio economico per utilizzare l'energia deviata.
- *Carichi indefiniti:* altri carichi non definiti sopra, compresi quelli con caratteristiche non definite.

RISORSE ENERGETICHE DISTRIBUITE: Le (DER) comprendenti la generazione e lo stoccaggio includono quanto segue:

- *Generazione distribuita:* Queste è categorizzata in due tipi:

1. unità spendibili; che possono essere controllate dal sistema di controllo della MRMe che sono soggette a vincoli tecnici.
2. unità non spendibili; che non possono essere controllate dal sistema di controllo della MR in quanto la fonte d'ingresso è incontrollabile per sua stessa natura. Queste sono principalmente le risorse rinnovabili che forniscono una potenza in uscita variabile ed intermittente.

Riguardo l'ultimo punto abbiamo che le caratteristiche delle unità non spendibili hanno un impatto negativo sulla capacità di generazione, le quali aumentano l'errore di previsione. Perciò queste unità vengono comunemente rinforzate con i sistemi distribuiti di stoccaggio e generazione di energia (ad esempio: macchine elettriche sincrone e rotanti a induzione azionate meccanicamente, cogeneratori, sistemi basati su inverter che convertono la corrente continua in corrente alternata,)

- *Stoccaggio di energia distribuita:* l'applicazione principale di questo sistema consiste nel coordinarsi con le generazioni distribuite per consentire l'adeguatezza della generazione di energia delle MR.
- *Risorse energetiche distribuite indefinite:* altri tipi di queste fonti che producono energia elettrica e non sono state definite sopra.

ELEMENTI DI CONTROLLO: Dove gli elementi di controllo includono i seguenti componenti

- *Sistemi di controllo della MR:* il controllore locale della MR è un software e/o hardware decisionale della microrete che fornisce la programmazione delle risorse nella modalità connessa alla rete o isolata. Questi permettono di controllare la frequenza e la tensione all'interno della MR decidendo quale carichi spostare o limitare.
- *sensori aggiuntivi, comunicazione ed elementi di controllo:* questi includono interruttori intelligenti, reti di comunicazione, etc...

3.2.3 *Richiamo alle nanoreti*

Solitamente una microrete può essere formata da altrettante sotto reti che vanno sotto il nome di nanoreti (tradotto da *"nanogrids"*). Queste definite in [4] come *un sistema di distribuzione di energia per una singola casa oppure un piccolo edificio, con la possibilità di connettersi o disconnettersi da altre entità di alimentazione tramite un passaggio (gateway).*

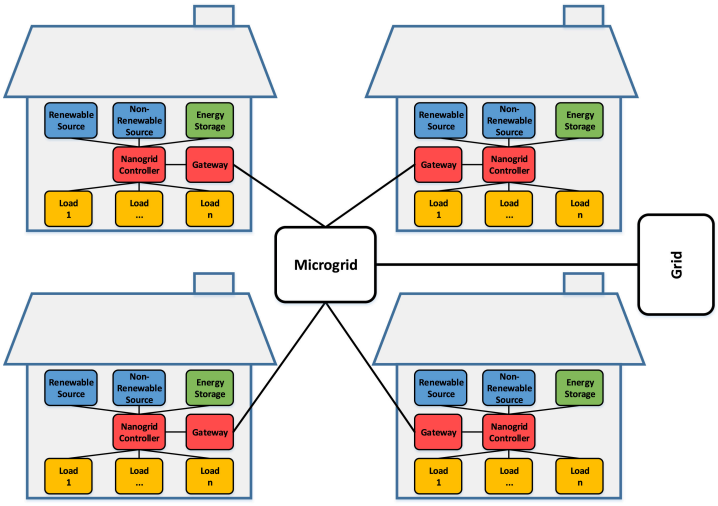

Figura 3.6: Architettura microrete[4]

Questa consiste nella produzione locale di energia elettrica che serve per alimentare i carichi locali, con la possibilità di utilizzare un sistema di stoccaggio energetico e/o un sistema di controllo.

Sempre in [4] si incoraggia la distinzione tra nanoreti e microreti. Ma, sempre in [4], si spiega che i due non si escludono necessariamente a vicenda, perché la natura modulare delle nanoreti offre la possibilità di collegarle insieme(ovviamente devono essere presenti più di due nanoreti), così da generare una microrete che può collegarsi alla rete esterna di distribuzione. Si vede in figura 3.6 come questo tipo di raggruppamento può essere realizzato.

3.3 CLASSIFICAZIONE DELLE MICRORETI: C.A. E C.C. E RELATIVI SISTEMI DI FUNZIONAMENTO

Abbiamo identificato la struttura di una microrete con le sue componenti principali, ma un'altra grande distinzione che si può fare delle MR è attraverso il tipo di output energetico fornito ai carichi. Questo può essere in CA o CC.

Come evidenziato in [2, 16, 17], nell'ultimo secolo si è visto come la generazione, trasmissione e infine distribuzione di energia elettrica dalla centrale all'utente finale sia stata in forma di CA. Questo è avvenuto per il semplice motivo che le reti in corrente alternata sono quelle che più si adattavano ai carichi presenti nell'epoca scorsa, dove per esempio, la maggior parte di questi carichi erano motori elettrici (asincorni) nelle nostre fabbriche e lampade ad incandescenza nelle abitazioni. Anche la generazione stessa dell'energia elettrica in forma di CA era resa (ed è tuttora) di semplice implementazione, visto le capacità intrinseche delle macchine rotanti alimentate a energia fossile di generare un flusso costante a richiesta di CA. Poi, per quello che riguarda la trasmissione e distribuzione dell'energia, queste non

incontra grosse difficoltà. Visto che è facile trasformare la corrente alternata in vari livelli di tensione, per essere utilizzata da vari tipi di applicazioni, oppure per essere trasmessa su lunghe distanze.

Perciò, dalla fine del 19° secolo in poi, la rete elettrica centralizzata ha seguito questo andamento creando un mercato dominante per le reti e i carichi in corrente alternata. Ma ad oggi tutto questo sta cambiando, dove descrivendo il fatto già esposto precedentemente, il paradigma per cui l'energia elettrica viene generata dal concetto di grandi generatori centralizzati è sempre meno diffuso. Questo perché i sistemi centralizzati sono insufficienti e non fattibili in un prossimo futuro; visto l'aumento dei costi energetici, un fondo limitato per la costruzione di nuove grandi centrali e linee di trasmissione a lunga distanza, l'invecchiamento delle attuali infrastrutture del sistema elettrico, etc. . . che vanno a vincolare la possibilità di soddisfare la crescente domanda di energia elettrica[5].

Infine, con la nascita di moderne e migliori soluzioni per la generazione e distribuzioni come; l'aumento del numero di carichi in corrente continua basate su fonti rinnovabili, sistemi di stoccaggio dell'energia, sistemi flessibili per la trasmissione di corrente alternata e continua, gestione attiva della domanda, strategie di controllo avanzate basate sulle tecnologie dell'informazione e della comunicazione, etc. . . quindi, *a causa del progresso tecnologico nell'elettronica di potenza*, rivelano che la modernizzazione del corrente sistema di generazione,trasmissione e distribuzione è inevitabile. Sottolineando il fatto che le MR di oggi sono concepite per essere il più possibile flessibili, cioè che possono operare in entrambe le modalità.

Vediamo le descrizioni di queste MR nei prossimi sottocapitoli.

3.3.1 *Microreti in corrente alternata e relativi controlli*

La microrete in CA è la forma più comune esistente, in quanto la sua caratteristica di facile integrazione con i sistemi di alimentazione esistenti e i rispettivi carichi, la rendono di più facile implementazione. Mentre uno svantaggio significativo di questa MR è la sincronizzazione con il sistema di distribuzione principale rispetto la sua controparte in CC, dove la frequenza, l'angolo di fase e la tensione devono essere necessariamente abbinate con la griglia principale che andrà ad ospitare la mia MR. Per quanto detto, i requisiti di alimentazione della MR in CA sono più alti rispetto alla sua controparte in CC dove la tensione del bus è l'unica variabile ad essere controllata, mentre la sincronizzazione dei carichi è di facile implementazione. Infine, la complessità dell'architettura della microrete in CA è maggiore rispetto alla topologia in CC, poiché sono necessarie più conversioni tra i tipi di energia forniti dai generatori distribuiti nella microrete. Dove, tutto questo, porta ad una diminuzione generale dell'affidabilità del sistema.

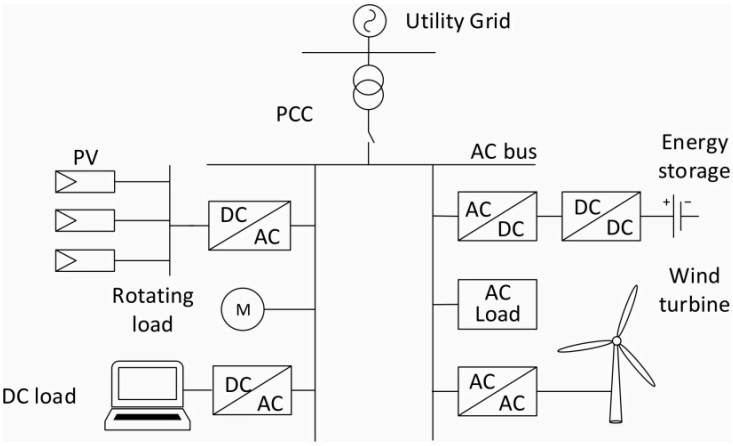

Figura 3.7: Architettura microrete in corrente alternata (AC)[17]

La figura 3.7 rappresenta un esempio di infrastruttura, dove la MR in corrente alternata, come parte del sistema di distribuzione, può collegarsi e scollegarsi dalla rete di pubblica utilità attraverso il Point of Interconnession (POI) (nella figura individuato come *PCC: point of common coupling*) così permettendo un passaggio tra le due modalità di connessione alla rete e isolata. Le DERs (identificate in [2] come microsorgenti) possono produrre o un'uscita elettrica in CC, oppure, una fonte energetica che in uscita ha una frequenza non compatibile con la rete di distribuzione. Per esempio, i generatori fotovoltaici richiedono un inverter CC-CA per connettersi al bus in CA, oppure i generatori di CA, come la turbina eolica, posso collegarsi al bus in CA grazie ad un convertitore CA-CA visto che solitamente questi tipi di generatori generano tensioni ad una frequenza variabile.

Sempre in figura 3.7 abbiamo l'accumulo di energia (*Energy Storage*); vitale nelle architetture delle MR, vista la capacità di assorbire l'energia in eccesso e di fornirla ai carichi quando i generatori distribuiti non sono sufficienti a soddisfare la richiesta energetica dei carichi presenti. Per far si che questo avvenga, sono necessari dei convertitori bidirezionali CC-CC in grado di fornire un flusso di potenza stabile per la carica o la scarica degli accumulatori ed infine si ha un inverter CC-CA per collegarsi al bus in corrente alternata. Mentre per i carichi in CA come i motori elettrici (asincroni) possono collegarsi direttamente al bus in CA le loro controparti in CC avrebbero bisogno di almeno un convertitore a stadio singolo come ad esempio un raddrizzatore.

Un altra caratteristica delle microreti in CA (ma anche di quelle in CC) è la capacità di funzionare in diverse modalità. Ancora in [2, 3, 17] si afferma che la topologia degli elementi presenti in una MR dipende fortemente dallo stato di lavoro in cui si trova e questa può operare principalmente in due stati stazionari:

MODALITÀ CONNESSA: La microrete scambia energia con la rete

elettrica esterna supportandola. In questa modalità la frequenza della MR è mantenuta dalla rete esterna e si presenta come un carico aggregato controllabile dalla rete esterna, per questo motivo è necessario controllare al POI la quantità di armoniche e corrente continua che vengo iniettate nella rete principale [2].

Un modo per gestire il tutto è la tecnica di controllo della modalità connessa alla rete, in cui sono presenti diverse funzioni di controllo della microrete. In questa modalità di controllo ci sono principalmente tre categorie di generatori distribuiti: [17]:

- grid-forming
- grid-feeding
- grid-supporting

MODALITÀ ISOLATA: L'interconnessione con la rete principale non è più presente e ho una disconnessione fisica dalla rete di distribuzione principale. Mentre nella modalità connessa alla rete la MR estrae o fornisce energia alla rete principale in base al mescolarsi della generazione dei carichi e delle politiche di mercato implementate, in questa modalità, la MR può separarsi dalla rete principale ogni volta che si verifica un evento sulla "qualità" dell'energia nella rete principale [2]. Purtroppo in questo tipo di modalità la MR si trova ad affrontare una serie di problemi che elenchiamo di seguito:

- Regolazione di Tensione e Frequenza
- Bilanciare domanda e generazione
- Qualità dell'energia
- Questioni centrali sulle microsorgenti
- Comunicazioni tra le microsorgenti

Qui le tecniche di controllo per la modalità isolata sono le seguenti (ulteriori approfondimenti in [17]):

1. Controllo Master-Slave: quando la MR passa dalla modalità connessa a quella isolata una microsorgete si comporterà come il regolatore principale di tensione e frequenza attraverso un metodo di controllo della tensione, mentre fornisce i riferimenti alle altre microsorgenti che funzionano attraverso il metodo di controllo in corrente.
2. Controllo Peer-to-Peer: diversamente dal controllo precedente, tutti i generatori distribuiti agiscono nello stesso ruolo. Ciascuna fonte esegue un controllo locale in base alle proprie caratteristiche di caduta(drop characteristics). Quando una fonte è collegata o scollegata dal sistema, la MR funzionerà continuamente senza alcuna configurazione aggiuntiva, ottenendo una funzione *"Plug and Play"*.

3. Controllo Gerarchico: questo metodo contiene tre livelli, il primo controllo avviene al livello del convertitore. Il secondo serve a compensare la frequenza e le deviazioni di tensione, ed assicura una buona sincronizzazione con la rete principale. Infine il terzo tiene conto degli interessi economici e determina quando vendere o acquistare energia dalla o verso la rete principale.
4. Controllo Sistema Multy-agent: è una tecnologia emergente che utilizza il sistema Multi Agente Consente ad ogni microsorgente o carico di rappresentarsi come agente e di scambiare informazioni con gli agenti vicini per collaborare ad un obbiettivo reciproco. Questo può essere classificato nella famiglia dei metodi *Peer-to-Peer* con controllo decentralizzato [4].

3.3.2 *Microrete in corrente continua e relativi controlli*

Le MR in corrente continua sono una tecnologia emergente a causa di un continuo aumento negli ultimi anni del numero di DER. Le quali, per la maggior parte di loro, la fonte di energia erogata è di natura continua. Oltretutto, anche il numero di carichi che assorbono questo tipo di energia è in aumento. Si pensi all'energia fotovoltaica fornita da pannelli fotovoltaici o l'energia immagazzinata e poi restituita dagli accumulatori, oltre a questi, la maggior parte dei nuovi dispositivi domestici (i.e: televisori, personal computer, console, etc...), grazie all'evoluzione dei semiconduttori, sono alimentati da forme di energia in corrente continua. Ancora di più nell'ultimo periodo si è visto come la vendita dei veicoli elettrici è aumentata e sarà destinata ad aumentare (si guardi [5]), portando così ad un ulteriore aumento di dispositivi con una richiesta elevata di energia elettrica in CC dalla MR e di conseguenza dalla rete principale.

Ancora in [17], e nella figura 3.8, abbiamo che la MR in CC mostra il suo vasto potenziale. Simile alla MR in CA, quella in CC si connetta alla rete ospite attraverso il POI (i.e Point of Common Coupling (PCC)) che gli permette le transizioni di collegamento e scollegamento. Poi, le DER in CC presenti nella rete possono facilmente collegarsi al bus passando attraverso dei convertitori CC-CC (o *buck/boost*) Mentre per i generatori, o carichi in CA (per esempio le macchine rotanti e le turbine eoliche), si richiede un raddrizzatore con controllo per essere integrate al bus CC.

Alcuni vantaggi delle MR in CC, presentati nei [2, 17], sono i seguenti:

4 Un esempio di questo sistema lo abbiamo in [9] dove si parla dell' *Intelligent Load Controllers (ILCs)* che funge da principale controllore locale, utilizzato per monitorare lo stato di una linea elettrica, dove acquisisce le misure di tensione, corrente e frequenza.

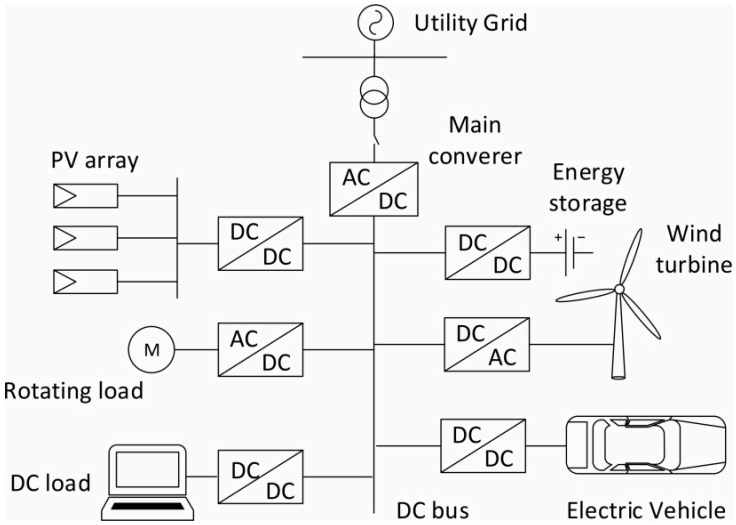

Figura 3.8: Architettura microrete in corrente continua (DC)[17]

- La riduzione delle perdite derivanti dalla conversione dell'energia elettrica tra i carichi in CC e le uscite in CC rendono l'efficienza della MR in CC superiore. Questa riduzione di perdite è accentuata rispetto ad una MR in CA se si utilizzano dei sistemi di accumulo energetico, oltretutto con meno processi di conversione rispetto la controparte in CA la rende più affidabile e con una topologia di rete più semplice.
- I requisiti per la compensazione della potenza reattiva e sincronizzazione con la griglia principale non sono presenti.
- La microrete in CC ha la capacità di passare attraverso i guasti della rete da sola, quando si ha un calo di tensione oppure un guasto alla rete principale. Questi non hanno un effetto diretto nel bus in CC continua a causa dell'energia accumulata dalle batterie o dai condensatori.

Mentre alcuni svantaggi, delle reti in CC sono:

- Per l'utilizzo di una MR basata sulla CC devono essere posate delle infrastrutture di distribuzione private. Mentre per quella in CA sono già presenti tutte le infrastrutture, quindi è necessaria una ristrutturazione generale della rete di distribuzione.
- Poiché nella tensione in CC non esiste un punto di attraversamento dello zero, la protezione in questi sistemi è più difficile rispetto a quella in CA3.5.
- Alcuni carichi devono essere adattati per l'alimentazione in corrente continua
- La standardizzazione delle MR in CC è un'altra questione che deve essere migliorata.

Quindi come visto poco fa, le MR in CC iniziano ad essere popolari grazie al fatto che; hanno una maggiore efficienza e sono in grado di fornire una qualità migliore di energia. Oltretutto, con l'assenza di problemi riguardanti frequenza e potenza reattiva, le tecniche di controllo sono più semplici da implementare. Di seguito vediamo alcuni metodi per il controllo della MR (senza la distinzione tra modalità isolata e collegata a rete, ulteriori approfondimenti in [17]:

Droop Control: il metodo *Droop control* può essere utilizzato per bilanciare la condivisione della corrente di carico tramite la regolazione della tensione d'uscita.

Controllo Gerarchico: simile a quello introdotto per la MR in CA, anche questo ha tre livelli di controllo; il primo ha due anelli, quello più interno ha un controllo di tensione e corrente mentre quello più esterno ha un circuito di controllo dell'impedenza virtuale. Mentre il secondo livello mira a compensare le deviazioni della tensione. Infine il terzo livello di controllo, che gestisce il flusso di potenza con la rete esterna, ha il compito di supervisionare l'integrazione tra più MR. Va evidenziato che questo metodo nelle MR in CC è più semplice da implementare rispetto alle MR in CA.

Controllo ad Isteresi: comunemente usato negli inverter connessi alla rete principale o nelle applicazione per la correzione del fattore di potenza, grazie alla velocità della caratteristica dinamica di risposta che assicura una buona qualità dell'energia elettrica ai cariche e alla rete.

Controllo della modalità di Tensione: è un controllo in retroazione a singolo anello, il quale può regolare il rapporto di lavoro del convertitore per adeguare la tensione d'uscita al valore obbiettivo

Controllo ad Inseguimento del Massimo Punto di Potenza: ovvero la tecnica *Max Power Point Tracking (MPPT)*, è comunemente utilizzata nella generazione di energia rinnovabile come il fotovoltaico e le turbine a generazione eolica dovuta alla loro natura stocastica. Questo tipo di tecnica nelle MR è generalmente usata a livello di conversione locale.

3.3.3 *Altri tipi di microrete*

Oltre alle due principali categorie di MR in CC e CA si affacciano al mondo altre tipologie di MR che rispettano dei canoni leggermente diversi.

Un tipo di MR praticamente uguale a quella in CA è la **Microrete con collegamento a corrente alternata ad alta frequenza** [2]. In

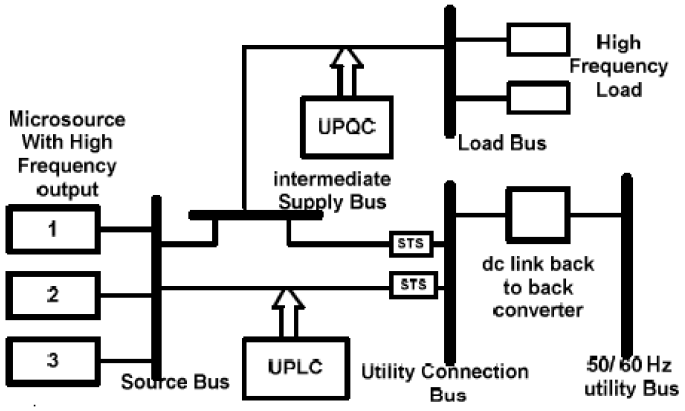

Figura 3.9: Architettura microrete in corrente alternata ad alta frequenza[2] dove abbiamo: Unified Power Quality Conditioner (UPQC), Universal Power Line Conditioner (UPLC)

questo caso, per l' inserimento delle varie DERs si utilizza un collegamento ad alta frequenza. Questo tipo di distribuzione viene già implementata nelle applicazioni aerospaziali e nei veicoli elettrici. I più grandi vantaggi che si hanno in questo tipo di sistema sono le dimensioni ridotte della rete e la densità elevata di potenza con una buona modularità.

Nella figura 3.9 abbiamo uno schema a blocchi generale della microrete in alta frequenza, dove si può notare il blocco UPQC (*Unified Power Quality Conditioner*) necessario per compensare le armoniche e la potenza reattiva presente nella rete. Questo perché i carichi non lineari, come i convertitori di potenza, introducono delle armoniche nella rete causando distorsioni di tensione. Mentre per il controllo del flusso di potenza, fondamentale nelle MR, è presente il blocco UPLC (*Universal Power Line Conditioner*) che mantiene il controllo del flusso di potenza tra la MR e la rete principale.

Un altro tipo di microrete è la MR di tipo **Ibrido** (Si trova un esauriente spiegazione nel libro [13]). Questa specie di microrete è composta da sub microreti in CA e CC, la quale può essere una forma particolare di MR in CA con una sub rete in CC dove, nel complesso, l'efficienza dell'architettura è migliore rispetto alla singola MR in CA. Tipicamente la topologia della rete prevede che la parte in CA si colleghi direttamente alla rete principale attraverso il POI, mentre la sotto rete in CC si collega al bus in CA attraverso un inverter CA-CC bidirezionale.

Come vediamo in figura 3.10, l'inverter presente tra la parte in CA e quella in CC, si comporta da principale punto di scambio tra le due reti gestendo il flusso di potenza tra i due sotto sistemi insieme alla tensione del bus in CC. Inoltre, la coordinazione del controllo tra i vari inverter è fondamentale nelle MR ibride, al fine di raggiungere la stabilità e l'efficienza della microrete.

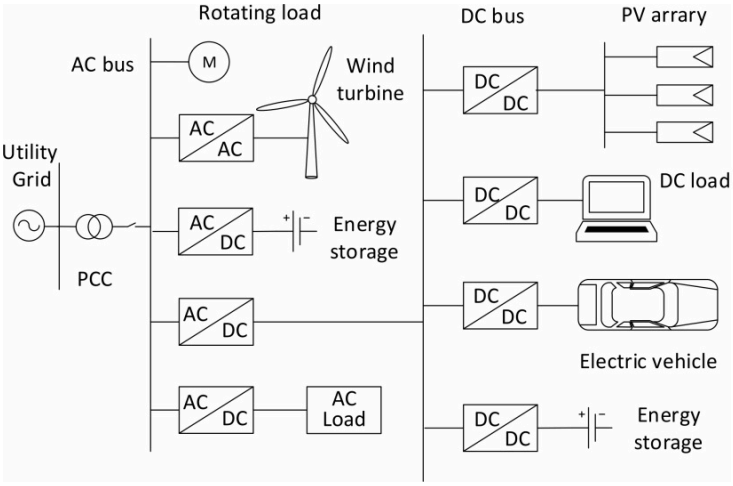

Figura 3.10: Architettura microrete di tipo ibrido (AC & DC)[17]

3.4 APPROFONDIMENTO SU MODALITÀ E CONTROLLI DELLE MICRORETI

I convertitori di potenza giocano un ruolo fondamentale nelle microreti, poiché permettono il collegamento fra le diverse risorse energetiche e trasferiscono facilmente l'energia tra le componenti della microrete, indipendentemente che siano di natura continua o alternata. Ma, non solo convertono e trasferiscono l'energia, questi convertitori con dei controlli adeguati riescono a mantenere il livello di qualità dell'energia all'obbiettivo previsto dalla MR.

Il motivo della necessità di questi controlli nasce dalla difficoltà di prevedere la produzione di energia dalle fonti rinnovabili (come ad esempio i pannelli fotovoltaici e le turbine eoliche, appunto chiamate Variable Renewable Energy (VRE)) che sono per loro natura stocastiche. Poi, il flusso di potenza tra la MR e la rete di distribuzione principale deve essere controllato nella modalità connessa, per assicurare una transizione fluida nel caso fosse necessaria. Mentre, nel caso in cui la MR è nella modalità isolata, dovrebbe avere la capacità di sopravvivere dopo la disconnessione dalla rete principale [17].

Anche in [14] si afferma che la peculiarità delle microreti intelligenti è quella di essere un sistema di potenza flessibile, controllabile e programmabile, le quali posso operare connesse come pure sconnesse dalla rete a monte, dove tutto questo è reso possibile dall'elettronica di potenza.

Nella figura 3.11, possiamo identificare uno scenario rappresentativo nel quale i convertitori di potenza elettronici sono applicati in maniera diffusa come interfaccia tra i diversi domini elettrici. Nel nostro caso particolare, gli inverter connessi alla rete, sono usati per interfacciarsi con; la rete principale in CA, delle semplici fonti in CC oppure dei sistemi più complessi di risorse energetiche e carichi, che possono comporre da soli delle piccole microreti in CC chiamate nanoreti 3.2.3.

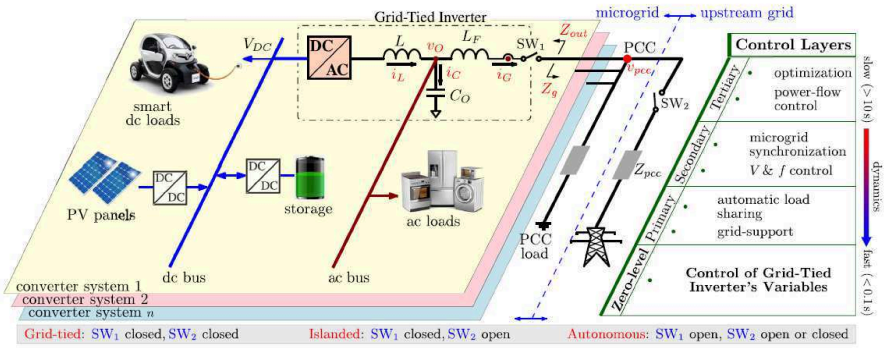

Figura 3.11: Tipico scenario di una MR con un inverter collegato alla rete. Distribuzione degli inverter connessi alla rete che sono coordinati tra loro con un controllo gerarchicamente organizzato a livelli[14]

Sempre nel caso esposto in [14], e quello precedentemente descritto in [17], generalizzando si identificano tre modalità diverse di funzionamento della microrete. Dove facendo riferimento alla figura 3.11, si hanno tre modalità operative differenti che sono permesse dagli stati degli interruttori SW_1 e SW_2, gestiti dall'inverter connesso alla rete oppure da remoto dal gestore del sistema di distribuzione:

1. **Modalità Connesso alla Rete:** gli interruttori SW_1 e SW_2 sono entrambi chiusi, mentre la rete a monte impone la tensione laddove ogni inverter connesso si comporta come una sorgente di corrente o potenza.

2. **Modalità Isolata:** nel caso di guasti la disconnessione della MR può essere rilasciata dai dispositivi di protezione ed attuata aprendo gli interruttori di linea Questi rappresentati dal commutatore SW_2. In questo caso gli inverter di linea possono supportare le operazioni della MR.

3. **Modalità Autonoma:** gli inverter connessi alla rete posso scollegarsi intenzionalmente dal POI (nella figura abbiamo il PCC) in qualsiasi momento con l'apertura dell'interruttore SW_1. In questo caso opera autonomamente come fonte di tensione controllata in grado di alimentare solamente i carichi in CA.

Perciò, gli inverter connessi alla rete giocano più ruoli; accoppiano i bus di distribuzione delle linee in CC e CA, contribuiscono ad alimentare i carichi locali in CA e forniscono alla rete principale l'energia prodotta dalle sorgenti locali, dove tutto ciò è conforme alle norme regolamentari applicabili.

Sempre nella revisione dei controlli delle MR fatta in [14], si affronta il problema tramite delle strutture di controllo gerarchico, e come

evidenziato 3.11, questo è composto dal livello zero, dal primario, secondario e infine terziario. Considerando solamente il livello zero, dove troviamo il controllo delle variabili che appartengono all'inverter connesso alla rete, si identificano delle strutture di controllo a cascata che possono essere categorizzate come segue:

1. **Singolo anello:** questo metodo è attuato quando solo una variabile è rilevata e regolata.

2. **Doppio anello:** quando più di una variabile è reimmessa la struttura del controllore guadagna una maggiore flessibilità. Tipicamente quando due variabili di controllo vengono restituite viene stabilita una strutture di controllo a cascata. Perciò, nel caso dei convertitori di potenza, il controllo con più variabili e quasi sempre costruito con una disposizione a cascata.

3. **Triplo anello:** il controllo a triplo anello è l'ultima struttura che viene proposta nella letteratura, questo è più complesso da analizzare e implementare rispetto alle soluzioni a doppio e singolo anello. In particolare, con tre anelli a cascata, è difficile ottenere una larghezza di banda ampia sull'anello più esterno, perché ogni singola larghezza di banda d'anello è limitata dal ritardo di risposta del ciclo interno.

Si lasciano ulteriori approfondimenti al lettore in [14] Perciò, con lo sviluppo delle microreti sono state proposte molte funzionalità riguardante i controlli e altrettanti requisiti identificativi per gli inverter connessi alla rete, i quali hanno reso la standardizzazione un imperativo.

Vista la natura delle MR, il tipo di risorse che utilizza e i diversi stati di funzionamento, queste sono tenute a presentare delle caratteristiche specifiche in materia di: stabilità, flessibilità, scalabilità e capacità di supporto alla rete. Vediamo di seguito gli obbiettivi e le caratteristiche che dovrebbero avere i controlli adottati in una microrete (ulteriori approfondimenti in [14, 17])

- Funzionalità *"Plug and Play"* quando si inserisce/disinserisce una sorgente o un carico dalla MR.

- Controllare il flusso di potenza attiva e reattiva dalla rete che ospita la MR oppure il carico in base alla richiesta dalla rete ospite nella modalità connessa alla rete.

- Condivisione dinamica dei carichi, nel momento in cui iniziano ad aumentare o diminuire i carichi nella modalità isolata.

- Garantire la qualità della potenza fornita alla MR, mantenendo la tensione, le fluttuazioni della frequenza e l'angolo di fase entro certi limiti desiderati.

- Capacità di mantenere la stabilità della rete di lavoro durante i periodi di transizione o quando si verifica un disturbo, quindi presentare degli adeguati margini di stabilità sia nello stato stazionario sia nelle condizioni transitorie.
- Transizioni fluide dalla modalità connessa alla rete a quella isolata, nel caso di disconnessioni intenzionali o non dalla rete principale, garantendo la reazione automatica ai guasti per consentire il ripristino tempestivo delle normali condizioni operative per carichi e fonti.
- Fornire dei servizi accessori come; supporto alla rete di distribuzione, programmazione della fornitura di energia, registrazione dei dati e diagnostica dei sistemi da remoto.

Nel loro complesso, l'insieme di queste funzionalità può essere classificato facendo riferimento a quattro circostanze di funzionamento, descritte dalle seguenti modalità: *connessa alla rete*, *isolata o autonoma*, *di transizione da connessa alla rete a isolata/autonoma*, *di transizione da autonoma a connessa alla rete/isolata*.[14]

3.5 SICUREZZA ELETTRICA NELLE MICRORETI

Una delle maggiori sfide nel funzionamento delle MR è la protezione del sistema nei suoi stati di funzionamento. Dove i relè di protezione devono essere progettati in modo che possano operare nella modalità connessa alla rete nonché nella modalità isolata. Per questo motivo la struttura dei relè di protezione per una MR collegata ad un sistema di alimentazione, è diversa da quella utilizzata per una rete con un sistema di distribuzione ordinario. Le tre ragioni principali da considerare sono [2]:

1. Quando una DER si aggiunge alla mia MR l'energia elettrica può scorrere in entrambe le direzioni, mentre il sistema di protezione ordinario è stato progettato per il flusso unidirezionale.
2. Una differenza significante della capacità di corto circuito si presenta nel momento in cui si commuta dalla modalità connessa alla rete a quella isolata.
3. Le correnti di guasto nella MR connessa alla rete e quella isolata sono notevolmente differenti. [11]

Appunto per questi motivi, nella modalità connessa alla rete, la protezione fornita dai relè isola la MR dalla griglia principale il prima possibile per proteggere i vari generatori e carichi distribuiti. Mentre, nella modalità isolata, i relè operano per individuare ed isolare la più piccola parte del sistema MR durante la compensazione dei guasti.

Allo stesso modo, molte DER sono connesse alla MR attraverso dei convertitori elettronici di potenza, in grado di sopportare delle correnti di guasto che sono limitate intorno a 2-3 volte la corrente nominale del dispositivo. Perciò molti metodi convenzionali di protezione dalle sovracorrenti potrebbero essere inefficaci per salvaguardare questi dispositivi. Quindi e richiesto un adeguato coordinamento tra le unità di generatori distribuiti, dispositivi di protezione e carichi per garantire alla MR di operare in sicurezza.

Oltretutto, si consiglia (in [11]) che le impostazioni dei dispositivi di protezione siano sempre aggiornate, tenendo conto della modalità di funzionamento della MR Mentre il controllo centrale della MR comunica con tutti i relè e i controlli dei generatori per registrare; il loro stato di ACCESO o SPENTO, la corrente nominale e quella di guasto. Infine la comunicazione con i vari relè è necessaria per aggiornare la corrente di normale funzionamento e determinare la direzione della corrente di guasto per poi mitigarne il suo effetto.

Fondamentalmente, ci sono due aspetti principali che devono essere studiati attentamente per poter ottenere un schema generale di protezione efficacie per una MR.

1. La quantità di fonti distribuite presenti nel sistema MR.
2. La disponibilità di un livello sufficiente di corrente di cortocircuito nella modalità isolata della MR è molto importante, in quanto questo livello di sicurezza può scendere sostanzialmente dopo l'isolamento dalla rete principale.

Nella progettazione degli schemi di protezione, la sicurezza e l'analisi dei guasti ricoprono un ruolo fondamentale, dove un corretto modello di sicurezza fornisce un adeguato livello di fiducia nel sistema di protezione. Sia nella progettazione dei sistemi di sicurezza delle reti CA che DC alcuni parametri devono essere considerati, per esempio, questi sono la; *Sensibilità*, *Selettività*, *Velocità di risposta*, *Livello di sicurezza*. Che sono solamente alcuni degli aspetti da considerare.

Vediamo ora le differenze presenti nei sistemi di sicurezza delle reti in CA e CC.

3.5.1 *Sistemi di sicurezza nelle reti in CA*

Nel tempo sono stati proposti diversi metodi per proteggere le microreti in Corrente Alternata, grazie anche ad un'ampia varietà di apparecchiature che sono tutt'ora utilizzate nella reti convenzionali di distribuzione in CA.

Questi particolari dispositivi di protezione dipendono dai componenti dei sistemi che devono proteggere e dal livello di tensione in cui lavorano, vediamo quelli più utilizzati nei sistemi di distribuzione in CA:

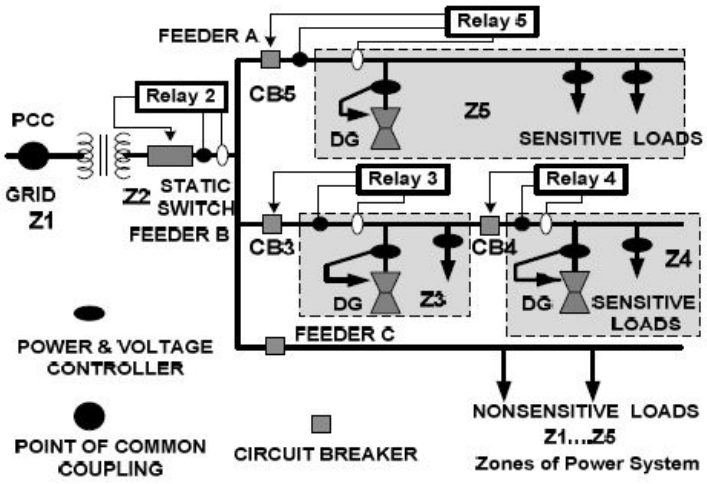

Figura 3.12: Protezione di una microrete in CA con funzionalità Plug&Play[2]

- rele di sovracorrente
- richiusori
- sezionatori
- Interruttori miniaturizzati
- fusibili

Uno schema di protezione che troviamo applicato nelle MR in CA che viene presentato in [2, 11] e rappresentato 3.12, è quello di configurare ogni unità di generazione distribuita con il proprio relè e di operare in modo decentralizzato. Questo approccio è il più efficiente per i singoli guasti tra fase-terra e fase-fase, mentre è limitato per i guasti con impedenze limitate.

Nella figura 3.12 viene mostrato il sistema di protezione autonomo con funzionalità *Plug&Play* di una MR: l'interruttore statico (Static Switch) si apre per qualsiasi causa di guasto, indipendentemente dal modo di funzionamento, dopodiché il guasto all'interno della MR viene eliminato con tecniche che non si basano sulle grandi correnti di guasto. Per esempio, se il guasto avviene nella Zona 4 (Z4) l'interruttore statico si apre seguito poi dall'interruttore di circuito 4, mentre gli interruttori 3 e 5 rimangono chiusi. Anche la DER in zona 4 verrà spenta.

Un altro schema di protezione in tensione che troviamo sempre in [2, 11] è di tipo centralizzato che vediamo in figura 3.13 . Le fasi di tensione sono trasformate negli assi d-q-o e vengono confrontate con un rifermento di tensione attraverso il controllore centrale della MR (MGCC) che è dotato di una unità centrale di protezione. Quando si verifica un cambiamento di tensione oltre la portata accettabile, il

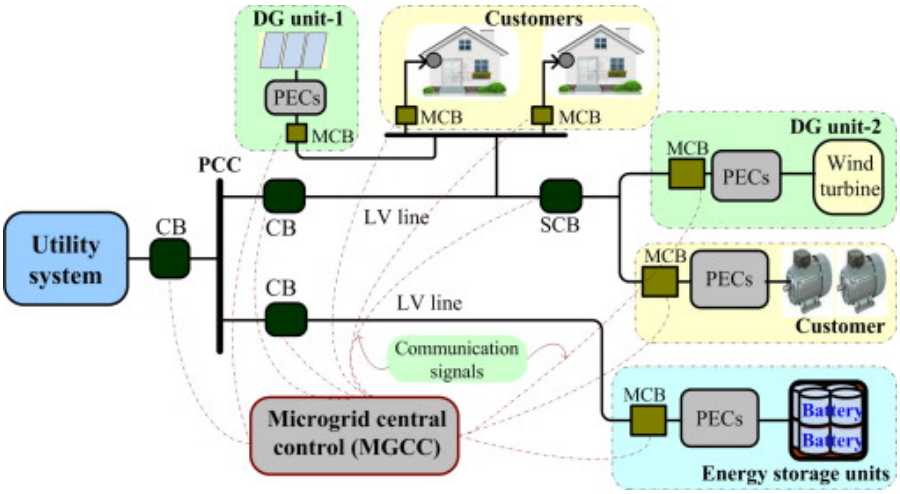

Figura 3.13: Sistema di protezione centralizzato nella MR in CA[11], *MGCC: Microgrid Central Controller, MCB: Miniature Circuit Breakers*

dispositivo di intervento (i.e, gli MCB in figura, che stanno per interruttori miniaturizzati o sezionatori) è azionato per isolare adeguatamente la sezione difettosa inviando il segnale al relè appropriato o al dispositivo di commutazione. Tutto questo è rappresentato nella figura 3.13. Oltre a queste funzionalità indicate sopra, l'unità di controllo centrale raccoglie le informazioni sullo stato dell'interruttore statico (i.e, se la MR è collegata alla rete o se è isolata).

3.5.2 *Sistemi di sicurezza nelle reti in CC*

Le sfide principali nella progettazione dei sistemi di protezione delle microreti in corrente continua si focalizza sugli inverter finali a lato cliente, i guasti di rete, i transitori di commutazione degli inverter e le situazioni in cui abbiamo dei doppi guasti tra reti di natura diversa (cioè reti Ibride 3.3.3).

I comuni sistemi di sicurezza con fusibili e relè automatici sono molto difficili da utilizzare con i convertitori di potenza, perché questi non riescono a produrre delle correnti di cortocircuito per tutto il tempo necessario alla reazione di protezione dei fusibili. Perciò per quanto detto, si utilizza un approccio diverso per la progettazione dei sistemi di sicurezza per le MR in CC, con un metodo differente di rilevamento dei guasti e messa a terra.

Nel caso delle MR in CC i sistemi di protezione consistono in; dispositivi d'interruzione della corrente, relè di protezione, apparecchiature di misura e sistemi di messa a terra. Oltretutto, sono presenti delle categorie di protezione per questo tipo di MR. Queste sono cinque, dove abbiamo la:

1. protezione utenza.
2. protezione convertitore.

3. protezione unità di generazione distribuita
4. protezione alimentatore
5. protezione sistemi di sbarre

Queste categorie possono essere utilizzate con sistemi centralizzati/-decentralizzati in un modo simili come nel caso delle protezioni nella microrete in CA.

Ciononostante, la capacità della corrente di cortocircuito degli inverter deve soddisfare gli "interruttori utlizzati" o altri requisiti di protezione adottati, vale a dire che, i convertitori di potenza di carico non possono essere dimensionati in base alla loro potenza effettiva. Bensì è la loro corrente di cortocircuito che determina le loro dimensioni, difatti, in una situazione di cortocircuito l'inverter è in grado di operare fino a 2-3 volte la sua corrente nominale, ma con una protezione basata su fusibili tradizionali per una rete in CA a bassa tensione questa richiederebbe una corrente più alta per funzionare correttamente, e perciò, non ha senso utilizzarla. Ecco perché, i convertitori di potenza devono essere sovradimensionati rispetto alla richiesta della capacità di alimentazione, dove i fusibili devono essere sostituiti da relè di protezione molto più veloci nel caso in cui si richieda l'utilizzo di convertitori più piccoli. Ancora una volta, nei convertitori di potenza CA/CC i guasti di commutazione possono essere protetti con delle funzioni di protezione integrate in esso e con dei relè di cortocircuito.

Infine, per le MR in CC i guasti sono coperti con la combinazione delle protezioni di sovracorrente e cortocircuito, insieme alla protezione dei guasti a terra. Oltretutto, la difesa contro i cortocircuiti in questo tipo di reti, può essere fatta con dispositivi che includono degli interruttori in CC, i quali sono più convenienti rispetto ai fusibili e relè di sovracorrente.

Perciò, tenendo conto di tutte le possibilità come lo stato operativo di ogni componente connesso all'interno del dato sistema della MR, la tecnica selezionata per le operazioni e il controllo della modalità operativa nella MR e i requisiti della microrete per rispondere ai guasti della rete, si può ottenere un adeguato schema di protezione per le MR in CC[5].

5 Questo sotto capitolo sulla sicurezza in CC segue quanto indicato in [11].

4

SICUREZZA INFORMATICA NELLE MICRORETI

In quest'ultimo capitolo si considera uno dei principali problemi presenti nelle microreti intelligenti, ovvero la loro sicurezza informatica.

Queste per loro natura sono composte da una parte hardware per gestire la componente energia elettrica (tensione,frequenza, corrente, etc...) e la comunicazione tra le varie MR, insieme ad una parte software in cui gli algoritmi delle modalità di controllo e gestione sono implementati. Visto l'elevato e continuo scambio di dati tre le varie microreti e la rete principale, con altrettante comunicazioni all'interno della microrete stessa (i.e: sensori che rilevano grandezze elettriche, comunicazione con i vari generatori distribuiti, relè di sicurezza collegati all'unità centrale di controllo, etc...) il campo di scelte per un probabile attacco informatico è estremamente ampio.

Oltretutto,se uno dei possibili attacchi informatici riuscisse ad andare a segno, questo non provoca problemi al solo apparato informatico, bensì può generare danni di una certa entità anche all'apparato fisico, creando così: sovratensioni, sovracorrenti, cambi nella frequenza e angolo di fase, acquisti energetici impropri... Arrivando a minacciare la sicurezza dei sistemi di protezione del sistema MR, causando problemi al cliente finale.

Quindi, si andranno ad analizzare i principali tipi di attacco informatico che può subire una microrete e in quali punti può accedere un probabile malintenzionato per colpire il sistema MR, con i conseguenti metodi per mitigare o bloccare del tutto questi tipi di minaccia.

4.1 AUMENTO DEL RISCHIO PER LA SICUREZZA INFORMATICA

Innanzitutto, la digitalizzazione offre molti benefici per i consumatori e il sistema elettrico, difatti per facilitare il funzionamento e la gestione della rete, il settore elettrico ha iniziato ad usare le tecnologie digitali dagli inizi del 1970. Da quel punto in poi, le società elettriche hanno costantemente adottato livelli crescenti di automazione e capacità di controllo, poiché i costi per le tecnologie digitali sono diminuiti drasticamente negli ultimi anni. Oltre a questo, dal 2010 al 2019 la velocità delle connessioni a internet sono aumentate di 10 volte, mentre i costi di archiviazione dei dati e sensori IoT (*IoT: Internet of Things*) sono diminuiti rispettivamente del 70% e 54%. Perciò, attraverso il sistema elettrico, le tecnologie digitali offrono una serie di opportunità per migliorare le prestazioni a beneficio delle singole aziende, del sistema nel suo complesso, dei consumatori di energia e dell'ambiente. Riguardo all'ultimo punto, la digitalizzazione può con-

tribuire ad accelerare le transizioni ad un energia pulita sbloccando più opportunità di risposta alla domanda, integrando maggiori quote di fonti rinnovabili variabili (VRE) e facilitando la ricarica intelligente dei veicoli elettrici[8].

Mentre la digitalizzazione offre molti vantaggi aumentando così l'automazione e la connettività in tutto il sistema elettrico, questa può anche aumentare i rischi per la sicurezza informatica lungo tutta la catena del valore dell'elettricità. Dove, gli attacchi informatici, sono tra i primi dieci rischi globali in termini di probabilità e impatto secondo il *World Economic Forum Global Risk Report 2020* ed è proprio per questo che i governi stanno prestando maggiore attenzione alla sicurezza informatica. In particolare, per la criticità dell'infrastruttura, in cui quasi la metà delle strategie nazionali di sicurezza informatica a livello globale sono state sviluppate o aggiornate dal 2017.[8]

Come evidenziato in [5], la preoccupazione più imminente è l'aumento del rischio per la sicurezza informatica. Dove un attacco informatico riuscito, potrebbe portare alla perdita di controllo su dispositivi e processi nei sistemi elettrici, causando danni fisici e interruzioni diffuse del servizio per i consumatori e le imprese. Sempre in [5] si indica ancora che, la digitalizzazione offre molti vantaggi per i consumatori e i sistemi elettrici, ma a discapito di una maggiore connettività e automazione in tutto il sistema, aumentano i rischi per la sicurezza informatica. Mentre la piena prevenzione dagli attacchi informatici non è possibile, allora è necessario che i sistemi elettrici divengano più resilienti a questi tipi di attacchi. Ciò significa mettere in atto un sistema di rete e protocolli di gestione della sicurezza sempre più robusti, insieme a tecnologie e strumenti di sicurezza informatica al fine di rilevare, resistere,adattarsi e recuperare rapidamente da incidenti e attacchi, preservando la continuità delle operazioni nelle infrastrutture critiche.

Infine, la digitalizzazione, solleva un ulteriore preoccupazione riguardante privacy e sicurezza dei dati del consumatore. Questo perché le reti intelligenti e le tecnologie di risposta alla domanda si basano su grandi quantità di dati sull'utilizzo dell'elettricità in tempo reale specifici per i consumatori, così sollevando questioni importanti sulla privacy e proprietà dei dati.

Perciò viste tutte queste opportunità e problematiche introdotte dalla digitalizzazione, i responsabili delle politiche devono bilanciare le preoccupazioni in materia di privacy con le esigenze operative dei servizi di pubblica utilità e l'ampio potenziale della trasformazione digitale dell'elettricità.

4.2 STRUTTURA INFORMATICA DI UNA MICRORETE

Nelle reti intelligenti, e in particolare nelle microreti, il sistema informatico e il processo fisico sono strettamente accoppiati. A causa delle

vulnerabilità del sistema informatico degli eventuali incidenti informatici possono avere un impatto economico e fisico sul funzionamento delle reti intelligenti. Così come nelle MR, in cui abbiamo un'elevata presenza di DERs basate su convertitore, dove una possibile violazione della loro sicurezza informatica può essere molto dannosa per gli utenti e la MR stessa [13] .

Rispetto alla eredita delle vecchie centrali elettriche centralizzate e alla rete di distribuzione tradizionale, sia le reti intelligenti che le MR sono sistemi più complessi che incorporano delle tecnologie operative e dell'informazione per la generazione efficiente, distribuzione e consumo dell'energia elettrica. Dove, nel sistema informativo delle MR abbiamo la raccolta, trasmissione ed elaborazione dei dati per controllare il funzionamento del sistema fisico. Per questo motivo il flusso di dati nel sistema informatico dovrebbe essere efficiente, affidabile e tempestivo per governare al meglio le operazioni di processo fisico all'interno della MR. Tuttavia, la digitalizzazione che è responsabile della loro stessa "intelligenza" le rende più vulnerabili alle minacce informatiche [6, 13].

In [1] si espone brevemente la struttura di controllo in una microrete, dova la si classifica in tre categorie di controllo:

1. *Controllo Primario:* questi controlli locali sono condotti a livello dispositivo in base alle misure raccolte localmente (intenso come controllo locale o come livello zero in figura 3.11).

2. *Controllo Secondario:* il sistema di controllo distribuito o il sistema di gestione dell'energia all'interno della MR funge da controllo secondario (sempre in 3.11 lo troviamo nel primo e secondo livello).

3. *Controllo Terziario:* sono quelle azioni condotte dal livello superiore di un'organizzazione, come il gestore del sistema di distribuzione. Questo livello di controllo è principalmente incaricato delle operazioni economiche e del coordinamento dello scambio di energia tra i gestori del sistema di distribuzione e le microreti presenti.

Sempre in [1], si evidenzia il fatto che i livelli di controllo secondario e terziario hanno la necessità di utilizzare delle reti di comunicazione e la loro implementazione è gerarchica. Tutto questo significa che se avviene un fallimento dei canali di comunicazione, tra i centri di controllo e i dispositivi sul campo (i.e: convertitori o inverter), questo causerebbe vari malfunzionamenti dei dispositivi che potrebbero portare ad altri guasti in cascata e problemi a livello di sistema. Oltretutto, tali relazioni gerarchiche possono causare incidenti di sicurezza catastrofici, come il compromesso del livello superiore può comportare il danneggiamento dell'intero sistema fino ai livelli più bassi.

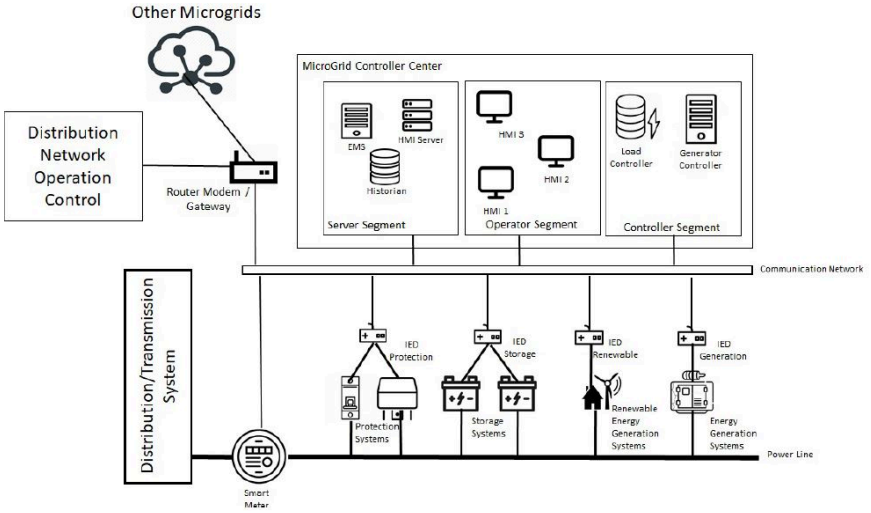

Figura 4.1: Architettura di una rete informatica e fisica per un sistema a MR[1].
Microgrid Controller Center: è il controllore centrale della microrete.

4.2.1 *Architettura informatica di una microrete*

Infine abbiamo in figura 4.1 una tipica architettura di sistema e topologia di rete per un sitema di tipo MR. Vediamo che il sistema è diviso sostanzialmente in due reti principali: La prima è una rete ad ampia area o rete di quartiere composta da connessioni di MR con il gestore del sistema di distribuzione (se la MR è su larga scala allora può essere collegata al gestore del sistema di trasmissione) ed altre microreti. Mentre la seconda rete, è di tipo locale o domestica, composta dal centro di controllo della MR, dispositivi elettronici intelligenti, contatori intelligenti e router-modem/gateway.

In questa architettura, il controllore centrale (che funziona come il livello di controllo secondario), costituisce una sottorete che può essere ulteriormente suddivisa in tre segmenti di rete separati tra loro:

- Server: questo segmento ospita i componenti di sistema utilizzati per il controllo secondario dell'intero complesso della MR, che sono: il sistema di gestione dell'energia, lo Human Machine Interface Server e il database storico .
- Operatori: è dedicato alle console d'interfaccia accessibili dagli operatori. Questo segmento può essere composto da altri sotto segmenti situati in diverse parti della struttura a seconda delle dimensioni, della posizione e dell'infrastruttura di rete.
- Controllori: questo segmento ospita i server di controllo che collegano i dispositivi elettronici intelligenti e il sistema di gestione dell'energia

Dopodiché, esistono tre livelli di architettura in una tipica rete di sottostazioni, essenzialmente abbiamo: il livello *centrale* che contiene i componenti del controllo di supervisione e acquisizione dati (ovvero lo *SCADA:Supervisory Control And Data Acquisition*), poi abbiamo il livello *baia* che ospita i dispositivi elettronici intelligenti e infine il livello di *processo* che include i sensori/attuatori. Questo tipo di architettura è composta da due bus di rete, un bus centrale e infine un bus di processo. Il primo collega gli elementi presenti nel livello baia al livello centrale, mentre il secondo fornisce dei collegamenti diretti di rete dai dispositivi al livello di baia e processo. Nella figura 4.1 la rete di comunicazione (*Communication Network*) corrisponde al bus centrale, anche se non è incluso, il bus di processo questo può essere aggiunto quando necessario.

Per completare questa spiegazione sull'architettura informatica, si introducono brevemente i protocolli di rete più utilizzati nelle MR, [1]:

1. IEEE 1815 (*DNP*3): è il protocollo di comunicazione usato per le comunicazioni SCADA. Mentre il *DNP*3, è un protocollo aperto e ottimizzato, sviluppato per interagire tra il master e le sottostazioni insieme ad applicazioni a supporto delle loro operazioni.

2. IEC 61850: è il modello internazionale d'informazione e protocollo di comunicazione con le DER e l'automazione della distribuzione.

3. IEEE 2030.5 (*SEP*2): è un nuovo protocollo sviluppato basandosi sul IEC 61850 per le reti in area domestica, anche se viene usato per altre applicazioni come le interazioni d'utenza con i sistemi DER tra le reti intelligenti e i consumatori.

4. OPENADR: è un protocollo sviluppato per le applicazioni di risposta alla domanda nella fornitura dei dati sui prezzi.

4.3 TIPI DI ATTACCHI INFORMATICI E RELATIVE CONSEGUENZE

Riguardo alle violazioni nella sicurezza informatica delle MR abbiamo una classificazione riportata in [13]. Queste violazioni sul flusso dati delle MR che compromette il suo funzionamento è suddivisa in tre tipi:

1. *Violazione sulla Disponibilità dei dati:* il sistema informatico dovrebbe garantire che i dati siano tempestivi ed accessibili. Questo è cruciale per i controlli dei convertitori elettronici di potenza nelle reti intelligenti, specialmente nella modalità isolata e nei transitori. Gli attacchi informatici il cui obbiettivo primario è il blocco o il ritardo delle comunicazioni dati vengono definiti attacchi sulla disponibilità dati. L'interruzione di servizio

(*DoS: Denial of Service*) e l'interruzione di servizio distribuita (*DDos: Distributed Denial of Service*) sono esempi di violazioni alla sicurezza informatica sulla disponibilità dei dati.

2. *Violazione sull'integrità dei dati:* insieme alla disponibilità, i dati nei sistemi informatici dovrebbero essere accurati ed affidabili nel loro intero ciclo di utilizzo e sotto ogni condizione operativa. Qualsiasi violazione che compromette l'integrità dei dati, modificando le informazioni che fluiscono nel sistema informatico, vengono definiti attacchi sull'integrità dei dati. Queste violazioni possono essere fatte corrompendo le misure o i segnali di comando nella rete di comunicazione e possono portare a malfunzionamenti nelle MR e influenzare il suo controllo. Un tipico esempio di violazione che compromette l'integrità dei dati, e una delle minacce più impegnative per le microreti, è l'attacco informatico basato sull'iniezione di dati falsi (*FDI: False Data Injection*)

3. *Violazione sulla riservatezza dei dati:* La riservatezza dei dati stabilisce che i dati devono essere protetti dall'accesso e dalla comprensione da parte di soggetti non autorizzati. Le violazioni della sicurezza informatica, che compromettono la riservatezza dei dati scambiati, permetto ai malintenzionati di spiare la rete di comunicazione per carpire le informazioni riguardanti i suoi clienti (ad esempio, identità e consumi di elettricità) insieme ai funzionamenti e le strategie di controllo della MR. Sebbene questo tipo di violazioni non hanno un forte impatto sulle operazioni della MR, le informazioni scoperte possono essere usate dagli hackers per attaccare efficacemente la disponibilità e l'integrità dei dati.

Date queste tre tipologie principali di violazione dei dati, in [1] troviamo una ulteriore suddivisione dei vettori d'attacco con la loro classificazione. Si identificano cinque categorie principali di tipi d'attacco: [esplorazione], [compromissione del dispositivo] , [compromissione della rete], [attacchi all'integrità] e [attacchi d'interruzione del servizio]. Solitamente, in molti casi applicativi, le attività di esplorazione e compromissione di dispositivo/rete, le quali hanno proprie procedure tecniche e di approccio, costituiscono dei prerequisiti per tutti gli attacchi indipendentemente dal loro impatto effettivo. Comunque, ogni categoria d'attacco è ulteriormente suddivisa in sotto categorie che sono per lo più definite in base alle variazioni dell'obbiettivo o della tecnica d'attacco. Vediamo quanto segue nello schema, che viene poi rappresentato nella figura 4.2:

ATTACCHI ESPLORATIVI. Un attore malintenzionato ha sempre la necessità di informazioni dettagliate sul sistema al fine di prepararsi all'attacco. Mentre si affronta un sistema informatico-

fisico, come una microrete, l'attaccante deve dedicare uno sforzo maggiore rispetto ai tradizionali attacchi della sicurezza di rete, in quanto deve concentrarsi su entrambi i livelli fisico e informatico.

1. *Esplorazione del livello fisico:* La topologia fisica del sistema di alimentazione mirato costituisce un input significativo per gli attacchi d'iniezione di dati falsi (False Data Injection (FDI)). Delle intrusioni passate o da ex dipendenti di società di servizi pubblici, si possono fornire dei dati riguardanti la topologia della rete Dove questo viene definito come un metodo di raccolta dati offline, considerando che gli aggressori possono utilizzare metodi online come la distribuzione dei propri sensori e delle unità di misura fasori.
2. *Esplorazione del livello informatico:* Ottenere dei dati riguardanti la topologia della rete nel livello informatico è una pratica molto conosciuta nel settore della sicurezza informatica. L'aggressore può ricorrere a metodi passivi come la raccolta di dati da risorse a partire dalle informazioni sulle minacce informatiche o dei metodi attivi attraverso l'uso dei scanner di sicurezza e rete.

COMPROMISSIONE DEI DISPOSITIVI. A questo livello abbiamo cinque tipi di attacco che possono passare attraverso il dispositivo.

1. *Compromissione del Firmware:* Il firmware dei dispositivi incorporati potrebbe essere compromesso come prerequisito per il lancio di altri attacchi, come quello sull'integrità dei dati o d'interruzione del servizio. Questi dispositivi solitamente svolgono l'esecuzione del codice in un anello a "unica trama" senza la necessità di un sistema operativo. Perciò, gli hacker possono colpire l'integrità dell'esecuzione del codice e prendere il controllo del dispositivo.
2. *Compromissione Fisica:* Un avversario può ricorre a mezzi fisici per accedere ai dipositivi sul campo (ad esempio, sensori, attuatori, dispositivi elettrici intelligenti) e sostituirli con quelli che possono controllare in remoto, oppure distribuiscono dei malware sul dispositivo.
3. *Malware:* I botnets consisto in bot computers che sono controllati da un gruppo di aggressori per lanciare un attacco informatico sui loro obbiettivi principali.
4. *Compromissione delle Credenziali:* Gli attori malintenzionati possono accedere ai dispositivi di destinazione fisicamente o in remoto e mirano ad ottenere le credenziali utente o amministratore.

5. *Vulnerabilità dei Servizi e delle Applicazioni:* Le vulnerabilità del servizio di rete o le applicazioni che possono essere raggiunte da remoto sono solitamente utilizzate dagli hackers per compromettere le attività del sistema.

COMPROMISSIONE DELLA RETE. Nella rete, i protocolli, sono fondamentali per la comunicazione tra i vari dispositivi presenti, ma permetto una possibile porta d'ingresso per i malintenzionati. Vediamo di seguito i quattro tipi di attacco.

1. *Dirottamento delle Comunicazioni:* Questo vettore d'attacco consente all'avversario di prendere il controllo della comunicazione tra diverse entità nella rete. Tuttavia, questo vettore, richiede che l'attore malintenzionato abbia un punto d'appoggio nella rete di destinazione, posizionando un dispositivo corrotto o compromettendone uno esistente.
2. *Falsificazione (Spoofing):* I protocolli di controllo industriali non forniscono l'autenticazione delle entità comunicanti e dei messaggi. Pertanto, una volta che un utente malintenzionato ottiene un punto d'appoggio nella rete pertinente, gli sarà facile falsificare l'indirizzo MAC di ogni dispositivo obbiettivo e condurre un attacco di rete nel secondo livello.
3. *Intercettazione:* Questo è un tipo di attacco passivo nel quale un avversario ascolta il canale di comunicazione della rete e ottiene i messaggi scambiati tra i nodi. In questo caso i metodi di crittografia forniscono una contromisura contro i dispositivi d'intercettazione.
4. *Man-In-The-Middle:* Questo si riferisce ad una categoria di attacchi d'impersonificazione in cui un intruso si inserisce tra due dispositivi per impersonare o intercettare le comunicazioni tra dispositivi. Quindi, un utente malintenzionato potrebbe utilizzare le informazioni acquisite per condurre attività dannose come la manomissione dei dati informativi trasferiti nei pacchetti dati.

ATTACCHI ALL'INTEGRITÀ. Questi attacchi violano le proprietà di integrità dei dati di controllo o misura, per indurre cambiamenti comportamentali in sensori o attuatori, raggiungendo così scopi di interruzione o distruzione. Questi sono principalmente di due tipi.

1. *Ripetizione:* In questo tipo di attacco, gli attori malintenzionati mirano a danneggiare la funzione energetica bersaglio raccogliendo dati di controllo e misurazione per poi rispedirli al momento pertinente, nel senso che, la parte modificata è in un aspetto temporale piuttosto che nella modifica dei dati stessi.

2. ***Iniezione di Dati Falsi (FDI):*** Questa categoria di attacco mira all'integrità dei dati di misura raccolti dai sensori o dei dati di controllo presi tra i diversi strati di controllo, al fine di creare danni distruttivi a varie funzioni di gestione dell'energia critiche come la stima dello stato, il controllo della tensione e della frequenza ed anche la protezione del sistema. In [1] abbiamo una descrizione più approfondita di questo attacco, mentre in [13] lo si considera uno degli attacchi più distruttivi e per questo motivo viene evidenziato più degli altri tipi d'attacco presentati in questo testo. Nei testi in inglese si trova spesso l'acronimo FDI.

ATTACCHI D'INTERRUZIONE DEL SERVIZIO. Questo tipi di attacco costituiscono la componente principale di una rete energetica, vale a dire, la disponibilità garantita dai dispositivi elettronici intelligenti per lo scambio dati di consumo, aggiornamenti e tariffe elettriche da parte delle società di servizi. La rete di comunicazione è soggetta ad attacchi canalizzati attraverso l'infrastruttura di rete utilizzata per la trasmissione e il controllo dei dati. Queste sono suddivise in sei tipi diversi di attacco.

1. *Manipolazione dei Protocolli d'Instradamento:* Le reti intelligenti, in generale, e i sistemi delle microreti, in particolare, possono beneficiare di vari tipi di reti (intese come reti di comunicazione), tra cui includono le topologie wirless-mesh, che esegue protocolli d'instradamento notevolmente complessi. Un attore malintenzionato può indirizzare il traffico di routing invece della comunicazione dei dati reali per poi interrompere la connettività in tali reti dinamicamente formate.
2. *Alla Sincronizzazione dei Tempi:* I sistemi della rete intelligente dipendono da severi requisiti in tempo reale che richiedono una gestione accurata e tempestiva dei dati temporali. Gli attacchi alla sincronizzazione dei tempi possono causare ritardi nella trasmissione dei dati temporali o finire con gravi violazioni dell'integrità sui valori del timestamp (marca temporale) dei dati di misurazione.
3. *Interferenza (Jamming):* Questa è una classe d'attacco DOS nelle applicazioni del sistema fisico-informatico. Queste utilizzano il livello di comunicazione fisica dei protocolli wirless come mezzo di attacco, dove le prestazioni delle reti possono essere degradate o bloccate attraverso l'emissione di un segnale d'interferenza che interrompe il controllo tra i vari dispositivi.
4. *Perdita Pacchetti(Packet Drop):* In questo attacco un avversario compromette un nodo, un gateway oppure un dispositivo di routing nella rete di destinazione, e intenzionalmente,

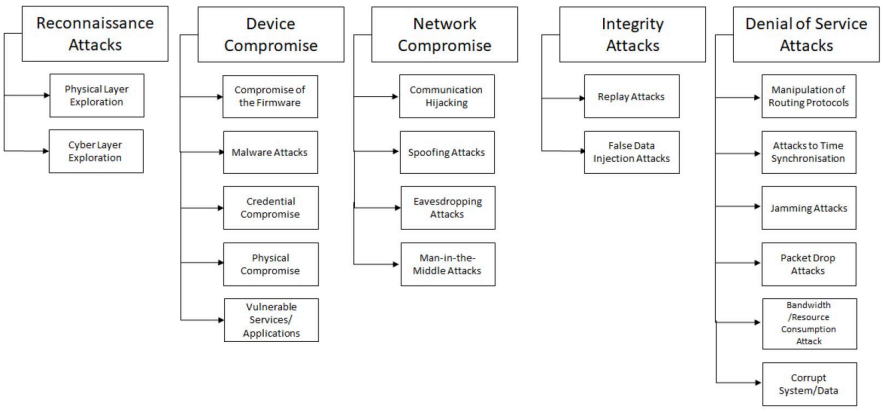

Figura 4.2: Classificazione dei Vettori d'attacco. Da sinistra verso destra abbiamo: *esplorazione*, *compromissione del dispositivo* , *compromissione della rete*, *attacchi all'integrità* e *attacchi d'interruzione del servizio* [1]

fa cadere o ritarda le comunicazioni di rete che passano su quel nodo compromesso.

5. *Consumo Risorse o Larghezza di Banda:* Uno degli attacchi più comuni di tipo DOS che possono essere applicati anche alle microreti è il riempimento della larghezza di banda del sistema di destinazione con richieste di comunicazione eccessive. Mentre, alcuni tipi di attacco possono mirare a un uso eccessivo delle risorse locali del dispositivo (per esempio la RAM, CPU, limiti del sistema operativo,...).
6. *Corruzione di Sistema o Dati:* L'attaccante può mirare a corrompere il sistema operativo, firmware o i dati del sistema di destinazione una volta che ha l'accesso fisico o remoto alla rete di comunicazione della MR.

Infine, si discute in [13] l'impatto di queste violazioni nelle microreti. Il primo fattore discusso è quello *economico*, dove una violazione della sicurezza informatica potrebbe causare dei significanti problemi economici nelle microreti, specialmente in quelle che si trovano nella modalità connessa alla rete con un elevata diffusione di risorse energetiche rinnovabili. La maggior parte dei mercati dell'elettricità liberalizzati consiste in un mercato *"day-ahead"(del giorno prima)* e in uno *"real-time" (in tempo reale)*. In quello day-ahead, il carico è previsto e un problema di ottimizzazione viene risolto per avere una spesa al minimo il costo. Dal momento che gli attacchi informatici basati sulla iniezione di dati falsi possono influire sulla previsione del carico, questo tipo di mercato è vulnerabile a tali violazioni. Mentre nel real-time si utilizza la stima dello stato per valutare la potenza generata e il carico su ciascun bus, che viene utilizzato per calcolare il flusso di potenza attraverso ogni linea. Pertanto, anche qui, gli attacchi informatici basati sull'iniezione di dati falsi che modifichino lo

stato stimato hanno un impatto sul mercato in real-time. Dopodiché, oltre agli impatti economici, le violazioni della sicurezza informatica attraverso gli FDI2 possono avere degli impatti *fisici e tecnici* sulle microreti. In generale, le violazioni degli FDI possono influire sulla stabilità transitoria e stazionaria delle microreti. In termini di stabilità dello stato stazionario, le violazioni formate dalle FDIs possono influire sul controllo della tensione, nei sistemi di gestione dell'energia e della domanda di potenza/corrente. Inoltre, la stabilità transitoria e dinamica delle microreti può essere influenzata dagli attacchi FDI. Per esempio, le violazioni di quel tipo possono impattare sul controllo della frequenza, nella stabilità dell'angolo di rotore e nei sistemi di protezione della microrete.

4.4 ARCHITETTURE E STRATEGIE DI PROTEZIONE

Una microrete, per diventare più resiliente contro gli attacchi informatici, deve integrare la sua infrastruttura distribuita di risorse con le informazioni informatiche presenti nella MR. In generale, una MR implementerà le caratteristiche di sicurezza informatica che riportiamo qui sotto [6]:

- Firewall di Perimetro.
- Hardware rinforzato.
- Controllori di Supporto.
- Crittografia dati.
- Protocolli di Autenticazione/Autorizzazioni.
- Monitoraggio delle Comunicazioni Interne/Processi .

Tutte le precedenti sono indicate in figura 4.3

Dopodiché, in [13], si trovano le principali strategie difensive contro gli attacchi informatici. Queste possono essere classificate nelle strategie basate sulla protezione e rilevamento/mitigazione, vediamole di seguito:

Strategie difensive basate sulla protezione: i Contatori/Sensori dovrebbero essere tutti protetti contro gli attacchi informatici, poiché sono presenti molti sensori intelligenti nelle MR emergenti, proteggere tutti i misuratori non è fattibile economicamente. Perciò, solo un insieme di sensori critici e le misure corrispondenti sono solitamente protette, quindi in questo tipo di protezione il numero di sensori protetti (e l'ubicazione) può essere raggiunto considerando il budget e la sensibilità del sistema.

Strategie difensive basate sul rilevamento/mitigazione: I dati misurati sono analizzati per rilevare degli attacchi informatici e

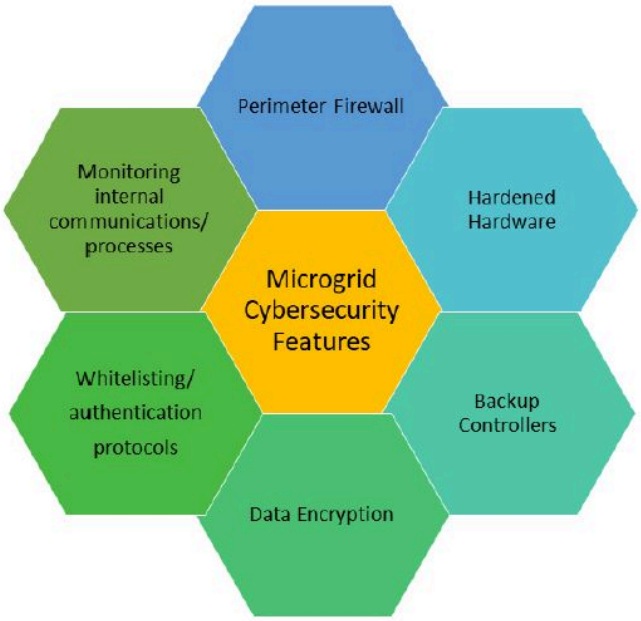

Figura 4.3: Componenti di sicurezza della microrete [6]

mitigati/ridurre i loro effetti avversi sulle operazioni della MR. In generale, le strategie di rilevamento possono essere suddivise in statiche e dinamiche:

- *Rilevatori statici di attacchi informatici:* le strategie di difesa che riconoscono le violazioni nello stato stazionario vengono chiamate rilevatori statici. Uno di questi ben noti è il rilevatore di attacchi sulla stima dello stato. Ad oggi, sono state sviluppate diverse strategie per individuare/mitigare le violazioni da parte dei FDI mirate alla stima dello stato.

  Si pone l'attenzione sul fatto che, le strategie utilizzate per recuperare le informazioni sullo stato delle MR in CC e adatte per gli attacchi FDI nella stima dello stato in CC, nei modelli di stima delle reti in CA, che vengono utilizzati nella maggior parte dei sistemi di alimentazione reali, le loro prestazioni non sono sufficienti. Perciò, vengono utilizzati dei metodi diversi per rilevare gli attacchi di FDI nella stima dello stato delle reti in CA.

  Le strategie di difesa, contro gli attacchi mirati alle regolazioni della tensione nelle microreti, possono essere classificate come rilevatori statici, dove l'algoritmo di rilevamento può essere integrato nel sistema di controllo dei convertitori come un anello di controllo supplementare oppure può monitorare i cambiamenti negli insiemi degli invarianti dei candidati inferiti.

- *Rilevatori dinamici di attacchi informatici:* L'informazione sulla dinamica del sistema è utilizzata nel metodo del rile-

vamento dinamico per individuare gli attacchi informatici. Diversi rilevatori dinamici si concentrano principalmente sui sistemi lineari, i quali non possono efficacemente riconoscere gli attacchi nel mondo reale a causa della loro non linearità.

Il rilevamento delle violazioni FDI che mirano al controllo della frequenza nella microrete e la stabilità dei transitori nei sistemi di alimentazione, sono classificati come metodi per il rilevamento dinamico.

4.4.1 *Architetture di protezione delle Microreti*

Di seguito si riportano le architetture descritte in [6] per la protezione o il rilevamento/mitigazione delle violazioni informatiche. Abbiamo la descrizione delle tre architetture con le loro implementazioni nel seguito di questo sotto paragrafo.

4.4.1.1 *SOAR Security Orchestration, Automation and Response*

L'architettura di tipo *SOAR Security Orchestration, Automation and Response*(tradotto come:*"Orchestrazione della Sicurezza, Automazione e Risposta"*) è una pila di programmi software compatibili tra loro. Questi servono per raccogliere dati sulle minacce fisiche e digitali da più risorse e facilitare la risposta automatizzata agli eventi di sicurezza a basso livello.

L'ecosistema della tecnologia SOAR supporta le seguenti funzioni:

- L'orchestrazione della sicurezza, o la gestione delle minacce e vulnerabilità, facilità la raccolta di informazioni. Cioè, dato un gran numero di minacce alla sicurezza e avvisi provenienti da più fonti informative, questo va a consolidare i dati che in un secondo momento verranno utilizzati per ulteriori analisi. Dopodiché si rivolge alla vulnerabilità correlando i dati di registro con le informazioni della minaccia e utilizza dei processi definiti, delle funzionalità di segnalazione e delle condivisioni di informazione per allarmare il sistema.

- Le operazioni di sicurezza automatica agevolano le analisi sugli eventi informatici e poi, a seconda della complessità in cui si trova gli eventi, agisce utilizzando degli interventi manuali oppure dei playbook (questi sono un insieme di regole e politiche definite a priori).

- La risposta agli incidenti di sicurezza utilizza delle funzionalità automatizzate che impostano i flussi di lavoro automatizzati in risposta agli eventi per i tipi più comuni di incidenti di sicurezza.

Come illustrato in 4.4 la pila SOAR consiste nelle seguenti applicazioni, chiamate *Network di analisi*, *Gestione del flusso*, *Gestione incidenti*, [Informazioni sulle minacce] e [Gestione delle conformità]. Utilizzando queste applicazioni, l'ecosistema SOAR automatizza i processi di gestione degli eventi fornendo in tempo reale una mitigazione delle minacce informatiche.

Figura 4.4: Applicazioni della tecnologia SOAR [6]

Per quanto riguarda l'implementazione del SOAR nelle microreti, questa può essere utilizzata per raccogliere automaticamente avvisi di eventi dagli elementi della rete, per utilizzare poi la correlazione degli eventi, contestuale con l'analisi di sicurezza, per fornire una visione consolidata della posizione di sicurezza della microrete. Il sistema SOAR può essere utilizzato anche per verificare automaticamente la moltitudine di impostazioni della sicurezza sui dispositivi della MR e garantirne il continuo rinforzo.

4.4.1.2 *Artificial Intelligence/Machine Learning*

I termini *Artificial Intelligence* (tradotto come *Intelligenza artificiale*) e*Machine Learning* (tradotto come *apprendimento automatico*) sono spesso usati in modo intercambiabili ma sono di fatto due concetti diversi. L'AI è la scienza che automatizza le attività umane utilizzando sistemi automatici che sono in grado di imitare il comportamento umano. Mentre, il ML, un sottosistema della AI, è un approccio al concetto di AI utilizzando un sistema che riconosce i modelli, prende le decisioni basate sui dati disponibili e regola il relativo comportamento secondo le decisioni prese precedentemente. I sistemi di IA possono rispondere agli attacchi informatici, ma il ML facilita le attività associate con la risposta all'evento effettivo.

I compiti della sicurezza informatica sono generalmente classificati in: *previsione*, *prevenzione*, *monitoraggio*,*rilevazione* e *risposta*. Alcune

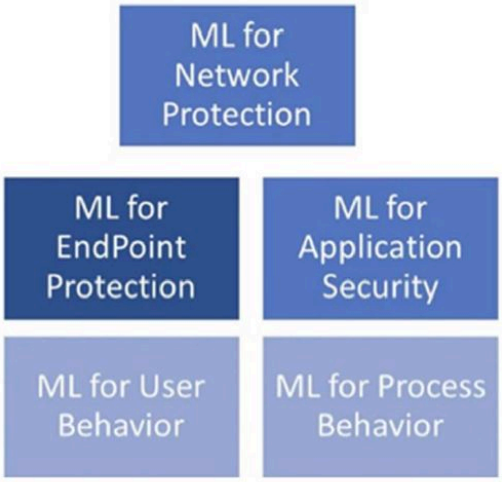

Figura 4.5: Categorie d'applicazione della sicurezza basata su ML [6]

tecniche per cui il ML viene utilizzato, all'interno dell'ambito della sicurezza informatica, sono mostrate in 4.5

Infine, l'architettura basata sul ML può essere applicata alle seguenti funzioni di sicurezza informatica:

- Protezione Network
- Protezione degli Endpoint
- Sicurezza delle Applicazioni
- Comportamento Utenti
- Comportamento Processi

Riguardo l'utilizzo del AI/ML nelle microreti abbiamo innanzitutto che queste MR possono essere vulnerabili a principalmente due minacce informatiche: le prime sono tutte quelle che influenzano i sistemi hardware e i dispositivi connessi, mentre le seconde, sono quelle che colpiscono i sistemi internet della microrete. Le tecniche algoritmiche basate sul ML/AI possono essere usate dalle utenze per insegnare ai sistemi come delle normali attività vengono viste, in questo modo possono individuare le anomalie e generare degli avvertimenti quando un attacco informatico colpisce la MR.

4.4.1.3 *Blockchain*

Innanzitutto, una blockchain è un registro crittografico condiviso che viene mantenuto da una rete di computer. La tecnologia Blockchain o tecnologia *Distributed Ledger*, è un database distribuito aperto e in continua crescita che permette ai membri della rete blockchain di; mantenere una replica del registro digitale, aggiornarlo utilizzando il

protocollo di consenso, distribuire e memorizzare i dati. In figura 4.6 è illustrato il processo di una blockchain.

La tecnologia blockchain è considerata sicura attraverso il collegamento e la protezione di blocchi dati utilizzando la crittografia che rende difficile la modifica dei registri. Perciò, dal momento che le transazioni dei registri delle blockchain sono esaminati e visibili a tutti i membri della rete blockchain, le possibilità di utilizzo non autorizzato dell'energia o frodi energetiche sono ridotte.

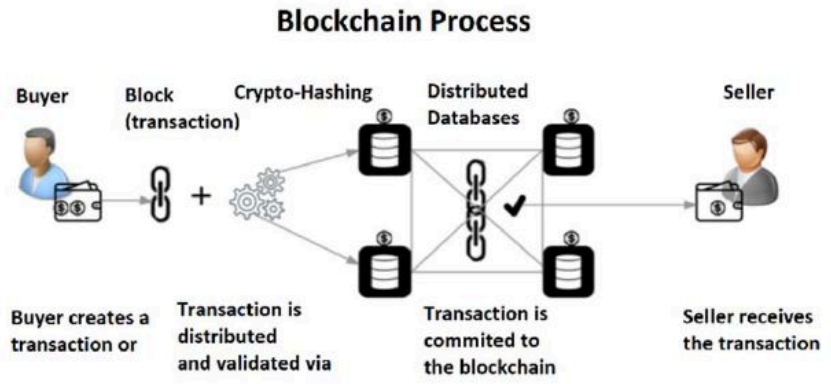

Figura 4.6: Processo della Blockchain [6]

Al giorno d'oggi le reti di collegamenti tra piccoli generatori distribuiti di potenza, inclusi quelli che utilizzano le DER, sono collegati alla rete elettrica principale. Quindi queste microreti permettono ai residenti comunitari di impegnarsi a scambiare il loro surplus di energia tra loro, così fornendo una maggiore efficienza nella gestione del processo. Purtroppo, quando sono presenti tutte queste transazioni di dati, ci possono essere altrettanti criminali informatici con l'obbiettivo di carpire più informazioni possibili .

Ecco allora che l'utilizzo della tecnologia blockchain nelle MR può essere utilizzata in modo che le reti di prosumatori [A.1] possano collegarsi in sicurezza alle altre microreti e scambiare un insieme di dati condivisi. Oltretutto, questa tecnologia può fornire una piattaforma di scambio Peer-to-Peer che protegge una MR di prosumer, in quanto condividono dati transazionali in modalità anonima, in modo sicuro. Perciò, la generazione decentralizzata dell'energia e il sistema di distribuzione della MR combinati con; lo scambio distribuito di grossi volumi di dati digitali connessi all'energia in tempo reale, attraverso le transazioni di dati nella blockchain crittograficamente sicura con i dati transazionali trasparenti per tutti i prosumatori, possono aiutare a proteggere la sicurezza e l'integrità dell'infrastruttura critica della microrete.

CONCLUSIONI

Partendo dall'esposizione della situazione elettrica mondiale riguardante la generazione e distribuzione dell'energia, in cui si riassumono i principali problemi derivanti dalle fonti rinnovabili e quelle a base di combustibili fossili. Passando poi alla descrizione delle microreti in base alla loro; posizione topologica nelle reti odierne, topologia strutturale, funzionamenti/controlli e infine sicurezza elettrica. Evidenziando in fine le difficoltà presenti nell'apparato informatico della microrete che la espone ad una larga varietà di minacce in grado di destabilizzare il suo corretto funzionamento.

La possibilità dell'uso dei generatori distribuiti di fonti rinnovabili attraverso le microreti è una obbiettivo da perseguire con forza. Queste hanno la possibilità di ridurre notevolmente il carico dalla rete principale, riuscendo comunque a soddisfare gli utenti connessi fornendo una fonte di energia affidabile. D'altronde, la principale difficoltà nella diffusione di nuovi sistemi, è l'impatto del costo iniziale dove la maggior parte dei paesi in via di sviluppo non riescono ad affrontare un costo di questo tipo. Inoltre i problemi legati alla sicurezza non sono da sottovalutare, visto la posizione critica che ricopre la microrete.

Si sono tralasciate volutamente le informazioni riguardanti la costruzione di un attacco informatico verso una microrete, perché si è preferito portare una visione sui tipi di attacco e i metodi di protezione delle microreti. Per quanto riguarda i convertitori di potenza e le architetture di controllo e gestione, ne abbiamo una breve discussione senza entrare troppo nel dettaglio per evitare di perdere il continuo dell'elaborato visto che l'argomento è estremamente ampio. Così come per i metodi di sicurezza elettrica, dove per le reti in CC lo sviluppo di questi metodi è in crescita visto il loro scarso utilizzo in passato e il nuovo interesse che stanno riscuotendo nel panorama elettrico mondiale. Mentre le reti in CA vengono utilizzati i metodi già presenti nelle reti di distribuzione tradizionali.

Praticamente ogni componente presente nella microrete ha subito degli sviluppi negli anni, sistemi di accumulo, generatori di energia da fonti rinnovabili, convertitori di potenza e sistemi informatici per citarne alcuni. Perciò come sistema, la microrete ha ampie possibilità di miglioramenti nel tempo visto che ogni suo dispositivo è soggetto ad un continuo sviluppo tecnologico.

APPENDICI

A

APPENDICE

A.1 DEFINIZIONI

Allo scopo di rendere più scorrevole la lettura del corpo dell'elaborato, ho deciso di mettere delle definizioni per aiutare il lettore a famigliarizzare con i termini introdotti nel testo.

INTERNATIONAL ENERGY AGENCY: IEA tradotto come "*Agenzia Internazionale dell'Energia*" nata con la crisi del petrolio nel 1973-1974 aveva lo scopo di coordinare le politiche energetiche e la sicurezza di queste. Oggigiorno è il cuore delle discussioni internazionali dell'energia, fornendo statistiche e analisi autorevoli riguardo i temi legati all'energia.

NET ZERO EMISSION: NZE tradotto come "*Zero Emissioni Nette*" è lo scenario normativo fornito dalla IEA per il settore energetico globale, dove delinea un percorso per raggiungere le zero emissioni nette di CO_2 entro il 2050.
Si guardi anche:https://www.iea.org/reports/world-energy-model/net-zero-emissions-by-2050-scenario-nze

STATED POLICIES SCENARIO: STEPS tradotto come "*Scenario delle Politiche Dichiarate*" rappresenta le politiche/scelte energetiche già intraprese o in via di sviluppo dei governi. Fornisce un banco di prova più conservativo, perché non è garantito che i governi riescano a raggiungere gli obbiettivi prefissati dagli altri scenari.

ANNOUNCED POLICIES SCENARIO: APS tradotto come "*Scenario degli Impegni Annunciati*" rappresenta l'insieme delle politiche/-scelte energetiche che ogni stato deve intraprendere per raggiungere gli obbiettivi prefissati di zero emissioni nette nelle scadenze prefissate.

IMPLEMENTATION GAP: tradotto come "*Divario di attuazione*" è analizzato come il divario tra i traguardi dello scenario STEPS e quello APS [5].

CLEAN COOKING SYSTEM: soluzioni di preparazione pietanze che rilasciano meno stanze inquinanti nocive, sono più ecosostenibili ed efficienti rispetto i sistemi tradizionali di cottura che fanno uso di biomasse solide (come un fuoco da campo),carbone o kerosene. Questo tipo di sistema si riferisce a migliorare il tipo di cottura con biomasse solide sicure, sistemi a biogas o biodigestori, fornelli elettrici, gas di petrolio liquefatti (GPL)

e gas naturali oppure fornelli ad etanolo[5]. Si guardi anche https://cleancooking.org/.

VARIABLE RENEWABLE ENERGY: VRE tradotto come "*Energie Variabili Rinnovabili* ", si riferiscono a tutte quelle tecnologie la cui produzione massima in ogni momento dipende dalla fluttuazione della disponibilità delle risorse energetiche rinnovabili. Le VRE includono un ampia gamma di tecnologie tra cui l'eolico, fotovoltaico solare,idroelettrica ad acqua fluente, concentrazione di energia solare(dove nessun accumulo termico è inserito) e marittime (attraverso onde e maree).

ADVANCED ECONOMIES: tradotto come "*Economie avanzate*", sono il gruppo regionale OCSE (Organizzazione per la cooperazione e lo sviluppo economico) e la Bulgaria, Croazia, Cipro, Malta e Romania. Le troviamo in [5].

DISTRIBUTED ENERGY RESOURCE: Le DERs tradotto come "*Riosrse Energetiche Distriubuite*", vengono definite in [10] come le fonti e gruppo di fonti di energia elettrica che non sono direttamente collegate al sistema di alimentazione globale; queste comprendo sia i generatori che le tecnologie di stoccaggio dell'energia elettrica in grado di esportare energia. Un sottoinsieme di queste sono le Renewable Energy Sources (RES) che utilizzano fonti rinnovabili come la generazione solare tramite pannelli fotovoltaici, energia geotermica ed eolica, fuel-cell ad idrogeno (con estrazione dell'idrogeno tramite energia rinnovabile), generatori a biomasse o biogas, etc...

PROSUMATORE: consumatore che è a sua volta produttore di energia elettrica (cioè, produttore + consumatore).

POINT OF INTERCONNESSION: POI tradotto come *"Punto di Interconnessione"* è il punto di connessione elettrica dalla quale la microrete si connetta alla, o si disconnette dalla, rete di distribuzione principale [10]. Molto spesso viene indicato con PCC.

A.2 RIFERIMENTI FIGURE

Alcune immagini utilizzate nella scrittura di questa tesi hanno una maggiore descrizione e interattività nel sito della IEA. Riporto di seguito i localizzatori uniformi di risorse (URL) delle immagini:

- Riferito alla figura 2.1 abbiamo: global population without access to electricity.
- Riferito alla figura 2.2 abbiamo: global population without access to clean cooking.
- Riferito alla figura 2.3 abbiamo: solar pv and wind generation

- Riferito alla figura 2.4 abbiamo: capacity additions of renewables in the announced pledges and net zero scenarios.

BIBLIOGRAFIA

[1] Hayretdin Bahsi, Henry Ochieng' Dola, Shaymaa Mamdouh Khalil e Tarmo Korõtko. «A Cyber Attack Taxonomy for Microgrid Systems». In: *2022 17th Annual System of Systems Engineering Conference (SOSE)*. 2022, pp. 324–331. DOI: 10.1109/SOSE55472.2022.9812642.

[2] Ambarnath Banerji, Debasmita Sen, Ayan K. Bera, Debtanu Ray, Debjyoti Paul, Anurag Bhakat e Sujit K. Biswas. «Microgrid: A review». In: *2013 IEEE Global Humanitarian Technology Conference: South Asia Satellite (GHTC-SAS)*. 2013, pp. 27–35. DOI: 10.1109/GHTC-SAS.2013.6629883.

[3] Mike Barnes, Junji Kondoh, Hiroshi Asano, Jose Oyarzabal, Giri Ventakaramanan, Robert Lasseter, Nikos Hatziargyriou e Tim Green. «Real-World MicroGrids-An Overview». In: *2007 IEEE International Conference on System of Systems Engineering*. 2007, pp. 1–8. DOI: 10.1109/SYSOSE.2007.4304255.

[4] Daniel Burmester, Ramesh Rayudu, Winston Seah e Daniel Akinyele. «A review of nanogrid topologies and technologies». In: *Renewable and Sustainable Energy Reviews* 67 (2017), pp. 760–775. ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2016.09.073. URL: https://www.sciencedirect.com/science/article/pii/S1364032116305640.

[5] Laura Cozzi, Tim Gould et al. *World Energy Outlook 2021*. report. International Energy Agency (IEA), 2022. URL: https://www.iea.org/reports/world-energy-outlook-2021.

[6] Sarmistha De Dutta e Ramjee Prasad. «Cybersecurity for Microgrid». In: *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*. 2020, pp. 1–5. DOI: 10.1109/WPMC50192.2020.9309494.

[7] Directorate of Energy Markets Security (EMS), Keisuke Sadamori et al. *Security of Clean Energy Transitions 2022*. report. International Energy Agency (IEA), 2022. URL: https://www.iea.org/reports/security-of-clean-energy-transitions-2022.

[8] Edwin Haesen, Enrique Gutierrez, George Kamiya, Grecia Sofía Rodríguez e Jason Elliott. *Enhancing cyber resilience in electricity systems*. report. International Energy Agency (IEA), 2021. URL: https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems.

[9] Nikos Hatziargyriou, Aris Dimeas, Nasos Vasilakis, Dimitrios Lagos e Alkistis Kontou. «The Kythnos Microgrid: A 20-Year History». In: *IEEE Electrification Magazine* 8.4 (2020), pp. 46–54. DOI: 10.1109/MELE.2020.3026439.

[10] «IEEE Standard for the Specification of Microgrid Controllers». In: *IEEE Std 2030.7-2017* (2018), pp. 1–43. DOI: 10.1109/IEEESTD.2018.8340204.

[11] Jackson John Justo, Francis Mwasilu, Ju Lee e Jin-Woo Jung. «AC-microgrids versus DC-microgrids with distributed energy resources: A review». In: *Renewable and Sustainable Energy Reviews* 24 (2013), pp. 387–405. ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2013.03.067. URL: https://www.sciencedirect.com/science/article/pii/S1364032113002268.

[12] R.H. Lasseter. «MicroGrids». In: *2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*. Vol. 1. 2002, 305–308 vol.1. DOI: 10.1109/PESW.2002.985003.

[13] Yunwei Ryan Li, Farzam Nejabatkhah e Hao Tian. «Cyber-security in Smart Hybrid Microgrids». In: *Smart Hybrid AC/DC Microgrids: Power Management, Energy Management, and Power Quality Control*. 2023, pp. 170–182. DOI: 10.1002/9781119598411.ch5.

[14] Qing Liu, Tommaso Caldognetto e Simone Buso. «Review and Comparison of Grid-Tied Inverter Controllers in Microgrids». In: *IEEE Transactions on Power Electronics* 35.7 (2020), pp. 7624–7639. DOI: 10.1109/TPEL.2019.2957975.

[15] Chris Marnay, F Javier Rubio e Afzal S Siddiqui. «Shape of the microgrid». In: (nov. 2000). URL: https://www.osti.gov/biblio/843057.

[16] Bruce Nordman e Ken Christensen. «DC Local Power Distribution with microgrids and nanogrids». In: *2015 IEEE First International Conference on DC Microgrids (ICDCM)*. 2015, pp. 199–204. DOI: 10.1109/ICDCM.2015.7152038.

[17] Yang Zhou e Carl Ngai-Man Ho. «A review on Microgrid architectures and control methods». In: *2016 IEEE 8th International Power Electronics and Motion Control Conference (IPEMC-ECCE Asia)*. 2016, pp. 3149–3156. DOI: 10.1109/IPEMC.2016.7512799.

Don’t wait until you reach your goal to be proud of yourself.
Be proud of every step you take