







UNIVERSITÀ  
DI TRENTO

Dipartimento di Ingegneria e Scienza dell'Informazione

Corso di Laurea in  
Ingegneria Informatica, delle Comunicazioni ed Elettronica

ELABORATO FINALE

MODELLAZIONE DI MINACCE  
INFORMATICHE IN AMBIENTE SMART GRID  
CLOUD-NATIVE

Supervisore

Prof. Domenico Siracusa

Laureando

Berardo Cristiano - 234428

Anno accademico 2024/2025



# Ringraziamenti

*Ringrazio la mia famiglia, papà Giacomo, mamma Elena e sorella Ilaria, di avermi dato la possibilità di intraprendere questo ricco percorso accademico.*

*Ringrazio i miei nonni, nonno Renato e nonna Laura, che mi hanno sempre spronato a dare il meglio di me.*

*Ringrazio Elena che mi ha supportato in questo cammino tortuoso, aiutandomi nelle decisioni più complesse.*

*Ringrazio gli amici di università per aver condiviso assieme esperienze e traguardi. Un ringraziamento particolare a Jacopo e Nicola per il confronto e l'aiuto reciproco.*



*Ai miei nonni Gabriele e Marta,  
che sarebbero fieri di questo traguardo, vi voglio bene.*

*A mia sorella Ilaria,  
che questo possa essere fonte di ispirazione nel raggiungimento degli obiettivi futuri.*



# Indice

<b>Sommario</b>	<b>2</b>
<b>1 Smart Grid: Architettura e componenti</b>	<b>3</b>
1.1 Introduzione alla Smart Grid . . . . .	3
1.2 Componenti principali della Smart Grid . . . . .	4
1.2.1 Dominio del consumatore . . . . .	4
1.2.2 Dominio operazionale . . . . .	8
<b>2 Il Paradigma Cloud-Native per le Infrastrutture Smart Grid</b>	<b>15</b>
2.1 Un Modello Architetturale Cloud-Native per la Smart Grid . . . . .	15
2.1.1 Logica di Disaccoppiamento: Componenti Centralizzati e Distribuiti . . . . .	15
2.1.2 Architettura a Cluster Federati e Trusted Boundaries . . . . .	15
2.1.3 Descrizione tecnica dei cluster Kubernetes . . . . .	17
<b>3 Modellazione delle Minacce Informatiche: Metodologie e Framework Applicativi</b>	<b>18</b>
3.1 Esigenze e ambiti applicativi . . . . .	18
3.2 Il Processo di Threat Modeling . . . . .	19
3.3 Le Fasi del Processo di Threat Modeling . . . . .	20
3.3.1 Modellazione del sistema . . . . .	20
3.3.2 Identificazione delle minacce . . . . .	21
3.3.3 Mitigazione delle Minacce . . . . .	22
3.3.4 Validazione delle Mitigazioni . . . . .	22
3.4 Il framework utilizzato: STRIDE . . . . .	23
<b>4 Applicazione del Threat Modeling all'Architettura Proposta</b>	<b>24</b>
4.1 Definizione del Data Flow Diagram . . . . .	24
4.1.1 Definizione dell'Ambito di Analisi . . . . .	25
4.1.2 Identificazione degli Asset Critici . . . . .	26
4.2 Analisi delle Minacce con il Framework STRIDE . . . . .	27
4.3 Strategie di Mitigazione e Contromisure di Sicurezza . . . . .	29
4.4 Approcci alla Validazione delle Contromisure . . . . .	30
<b>5 Conclusioni e sviluppi futuri</b>	<b>31</b>
<b>Bibliografia</b>	<b>31</b>
<b>A Glossario</b>	<b>35</b>
<b>B L'Architettura della Filiera Elettrica Italiana</b>	<b>37</b>
B.1 Dalla produzione alla distribuzione dell'energia elettrica . . . . .	37
<b>C Il paradigma tecnologico del Cloud Computing e i suoi principali vantaggi</b>	<b>43</b>
C.1 Introduzione al Cloud Computing . . . . .	43



# Sommario

La transizione globale verso un paradigma energetico sostenibile ha accelerato l'evoluzione delle reti elettriche tradizionali in Smart Grid. Questa trasformazione, caratterizzata dall'integrazione di fonti rinnovabili e dalla partecipazione attiva dei consumatori (*prosumer*), impone requisiti di scalabilità, resilienza e capacità di elaborazione dati che le architetture IT convenzionali faticano a soddisfare. In risposta, le infrastrutture critiche stanno adottando sempre più il paradigma *Cloud-Native*, che promette agilità, efficienza e robustezza attraverso tecnologie come la containerizzazione e l'orchestrazione con Kubernetes.

Tuttavia, se da un lato l'adozione del *cloud* offre vantaggi significativi, dall'altro introduce nuove e complesse superfici di attacco, esponendo le operazioni della rete energetica a minacce informatiche sofisticate. La sicurezza di tali sistemi diventa, quindi, una priorità non negoziabile.

Il presente elaborato si pone l'obiettivo di analizzare e modellare sistematicamente le minacce informatiche in un'architettura Smart Grid progettata secondo i principi *Cloud-Native*. Il lavoro si articola in tre fasi principali:

1. **Analisi del Dominio:** Viene presentata un'analisi dettagliata dell'architettura della Smart Grid, dai componenti di produzione fino al dominio del consumatore e operazionale, evidenziando le tecnologie chiave come AMI, SCADA, EMS e DMS.
2. **Proposta Architetturale:** Viene definito un modello architetturale *Cloud-Native* per la Smart Grid, basato su una federazione di cluster Kubernetes isolati (*Trusted Boundaries*) che gestiscono i diversi domini funzionali (AMI, DMS, EMS), garantendo robustezza e autonomia operativa.
3. **Modellazione delle Minacce:** Viene applicata la metodologia formale del *Threat Modeling*. Utilizzando un Diagramma di Flusso dei Dati (DFD) per rappresentare l'architettura, si applica il framework STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*) per identificare, classificare e analizzare sistematicamente le potenziali minacce.

L'analisi ha permesso di individuare vulnerabilità critiche, come attacchi di *Tampering* ai dati provenienti dai PMU, *Denial of Service* contro i sistemi SCADA ospitati nel *cloud* e attacchi di *Elevation of Privilege* e per il controllo coordinato di dispositivi remoti. Per ciascuna minaccia significativa, vengono proposte strategie di mitigazione e contromisure di sicurezza specifiche per il contesto *Cloud-Native*, tra cui l'uso di database WORM, la segmentazione dei privilegi tramite RBAC e l'adozione di *best practice* per la sicurezza dei container e dei cluster.

Il contributo principale di questa tesi risiede nell'applicazione strutturata di una metodologia di sicurezza proattiva ("Secure by Design") a un'infrastruttura critica moderna, fornendo un modello concreto per l'analisi dei rischi in sistemi ciber-fisici complessi e distribuiti.



# 1 Smart Grid: Architettura e componenti

## 1.1 Introduzione alla Smart Grid

Il paradigma energetico contemporaneo è caratterizzato da una trasformazione radicale, spinta dalla crescente integrazione di Fonti Energetiche Rinnovabili (FER). Tale transizione ha favorito la proliferazione della generazione distribuita (DER): impianti di piccola taglia, spesso di proprietà degli stessi consumatori, che immettono energia in rete. Questa dinamica trasforma il ruolo del consumatore passivo in quello di *Prosumer*<sup>1</sup>, un attore attivo capace sia di consumare che di produrre energia.

Di conseguenza, il modello tradizionale di flusso energetico, storicamente monodirezionale dalla centrale all'utente, è stato soppiantato da un modello complesso e bidirezionale [34]. In questo scenario, la rete elettrica tradizionale mostra i propri limiti strutturali. La risposta a questa sfida è la Smart Grid, o Rete Intelligente: un'evoluzione dell'infrastruttura elettrica che, integrando tecnologie avanzate di sensoristica, comunicazione e controllo, è progettata per gestire i flussi energetici in modo efficiente, sicuro e resiliente [7].

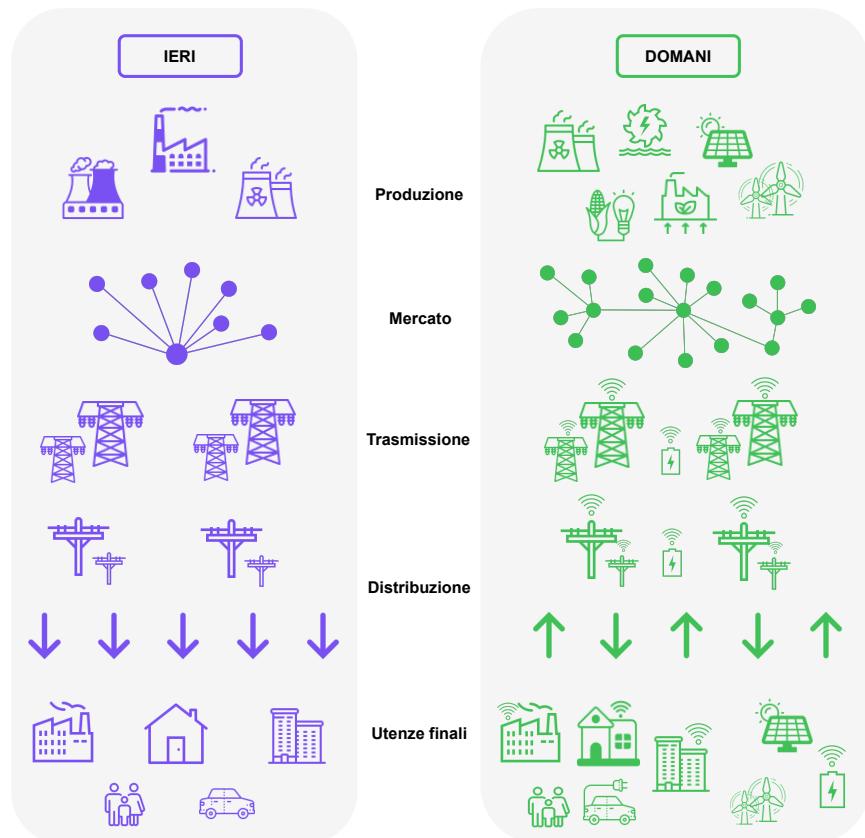


Figura 1.1: Confronto rete tradizionale e rete intelligente

Come si può vedere nella Figura 1.1 la Smart Grid si compone di 5 parti fondamentali: la Produzione, il Mercato<sup>2</sup>, la Trasmissione, la Distribuzione e infine le Utenze.

Nell'Allegato B viene approfondita tutta la filiera dell'energia, dal Produttore al Consumatore.

<sup>1</sup>Prosumer: Unione di *Consumer* (consumatore) e *Producer* (Produttore)

<sup>2</sup>Non trattato in questa tesi

## 1.2 Componenti principali della Smart Grid

La Smart Grid è un'infrastruttura complessa e stratificata, la cui comprensione richiede una scomposizione analitica nei suoi domini funzionali principali.

Questa sezione si propone di analizzare i componenti fondamentali della Smart Grid, concentrando su due aree macroscopiche ma profondamente interconnesse:

1. Il **Dominio del Consumatore** (*Customer Domain*): Rappresenta l'interfaccia diretta tra la rete e l'utente, abilitando una gestione attiva e consapevole dei consumi. Le tecnologie chiave di questo dominio, che verranno analizzate nel dettaglio, includono le Infrastrutture di Misurazione Avanzata (AMI) e i sistemi di gestione energetica domestica (HEMS).
2. Il **Dominio Operazionale** (*Operations Domain*): Costituisce il nucleo operativo della rete, responsabile della governance di generazione, trasmissione e distribuzione. In questo ambito operano sistemi di controllo e monitoraggio critici, come le piattaforme SCADA e le tecnologie di misurazione fasoriale (PMU).

La disamina di questi due domini è propedeutica all'identificazione delle superfici di attacco e delle vulnerabilità specifiche di ciascun livello, aspetti centrali per la modellazione delle minacce informatiche oggetto di questa tesi.

### 1.2.1 Dominio del consumatore

Il Dominio del Consumatore rappresenta il fulcro dell'interazione tra l'utente finale e la Smart Grid. La sua funzione primaria è trasformare il ruolo del consumatore da semplice fruitore passivo di energia a partecipante attivo (*Prosumer*), capace di prendere decisioni informate, gestire i propri carichi e interagire con la rete.

Questo è reso possibile da un ecosistema di tecnologie interconnesse che operano a livello locale, all'interno dell'edificio, e comunicano con i sistemi centrali del DSO. I componenti chiave di questo dominio, che verranno analizzati nei paragrafi seguenti, sono:

1. I sistemi di gestione energetica locale, come HEMS e BEMS.
2. L'infrastruttura di comunicazione e misurazione, nota come *Advanced Metering Infrastructure* (AMI), che a sua volta comprende elementi come *Smart Meter* (SM), *Data Concentrator* (DC), *Head-End System* (HES) e *Meter Data Management System* (MDMS).

### Home e Building Energy Management Systems (HEMS/BEMS)

I sistemi HEMS, per contesti residenziali, e BEMS, per edifici commerciali o terziari, sono piattaforme integrate, composte da hardware e software, progettate per monitorare, analizzare e controllare i flussi energetici all'interno di un edificio [16].

Le loro funzionalità principali sono:

- **Monitoraggio:** Raccolgono dati in tempo reale sul consumo degli elettrodomestici e sulla produzione di eventuali impianti locali, come ad esempio il fotovoltaico.
- **Controllo e Ottimizzazione:** Consentono di gestire attivamente i carichi, ad esempio posticipando l'avvio di dispositivi ad alto consumo (come lavatrici o veicoli elettrici in carica) nelle fasce orarie più costose o durante i picchi di richiesta della rete.

L'obiettivo di questi sistemi è duplice: da un lato, ottimizzare i consumi per generare un risparmio economico per l'utente e aumentare la sostenibilità dell'edificio; dall'altro, abilitare la partecipazione a programmi di *Demand Response* (DR), contribuendo così alla stabilità e all'efficienza della rete elettrica nel suo complesso.

Un esempio di implementazione in ambito BEMS è la piattaforma EcoStruxure<sup>TM</sup><sup>3</sup> di Schneider Electric, un'architettura che integra i vari dispositivi e sistemi di un edificio, centralizzandone la gestione. In ambito residenziale, HEMS, la stessa azienda propone soluzioni come Schneider Home<sup>4</sup>.

<sup>3</sup><https://www.se.com/it/it/work/products/product-launch/building-management-system/>

<sup>4</sup><https://shop.se.com/us/en>

## **Advanced Metering Infrastructure (AMI)**

L'AMI rappresenta l'infrastruttura di comunicazione e dati che abilita il dialogo bidirezionale tra l'utente finale e il DSO. Costituisce un'evoluzione cruciale rispetto ai precedenti sistemi di *Automatic Meter Reading* (AMR), che consentivano unicamente la telelettura unidirezionale dei consumi. L'AMI, invece, trasforma il contatore in un *gateway* intelligente, capace di ricevere comandi, inviare dati in tempo quasi reale (*Near Real Time - NRT*) e supportare servizi energetici avanzati.

L'architettura AMI è tipicamente stratificata e segue un percorso dati ben definito, che connette il dominio domestico (Home Area Network - HAN) ai sistemi centrali del DSO attraverso reti di quartiere (Neighborhood Area Network - NAN) e reti geografiche estese (Wide Area Network - WAN). Il flusso dei dati coinvolge una catena di componenti specializzati: lo *Smart Meter* (SM), il *Data Concentrator* (DC), l'*Head-End System* (HES) e il *Meter Data Management System* (MDMS) [2].

### **Smart Meter (SM)**

Lo SM, o Contatore Elettronico (CE), è il dispositivo terminale dell'architettura AMI, installato presso ogni punto di prelievo (POD) dell'utente finale. Sebbene la sua funzione primaria rimanga la misurazione del consumo energetico, in *kWh*, ai fini della fatturazione, il suo ruolo nella Smart Grid è molto più strategico: esso agisce come un vero e proprio sensore di rete intelligente, un nodo pervasivo capace di raccogliere dati granulari e abilitare servizi avanzati.

L'evoluzione di questi dispositivi è normata a livello europeo (Direttiva 2012/27/UE) e recepita in Italia dal D. Lgs. 102/2014<sup>5</sup>, che ha imposto la sostituzione dei contatori di prima generazione (1G) con i più moderni modelli di seconda generazione (2G). Questa transizione, che E-Distribuzione ha dichiarato conclusa a fine 2024 [10] e altri DSO come Ireti prevedono di completare entro il 2026 [26], non è un semplice aggiornamento tecnologico, ma un cambio di paradigma verso una gestione più attiva e sicura della rete.

### **Funzionalità Avanzate dei Contatori di Seconda Generazione CE 2G**

I contatori 2G introducono un ventaglio di funzionalità innovative che ne espandono notevolmente le capacità. Basandosi sulle specifiche tecniche [11][13][8], queste possono essere raggruppate nelle seguenti categorie:

#### **1. Comunicazione e Interoperabilità:**

- Canale di comunicazione dedicato all'utente, commercializzato con il nome di *Chain 2*: Utilizza la tecnologia *Power Line Communication* (PLC)<sup>6</sup> in banda C (125 – 140 kHz)<sup>7</sup> per dialogare con i dispositivi dell'utente (es. HEMS, *display in-home*), abilitando una reale gestione consapevole dei consumi.
- Canale di comunicazione verso il concentratore, *Chain 1*<sup>8</sup>: Oltre al canale PLC primario, è previsto un canale di backup su Radio Frequenza (RF) a 169 MHz, che garantisce resilienza e permette l'invio in tempo reale di segnalazioni critiche (es. interruzione di tensione).

#### **2. Dati e Misure Avanzate:**

- Registrazione delle curve di carico quartorarie: Il contatore registra e rende disponibili i dati di consumo e immissione con una granularità di 15 minuti, permettendo analisi dettagliate e nuovi modelli di tariffazione.
- Rilevamento della potenza massima giornaliera: Fornisce dati precisi sui picchi di potenza, utili al DSO per la pianificazione e la gestione della rete.

<sup>5</sup><https://www.gazzettaufficiale.it/eli/id/2014/07/18/14G00113/sg>

<sup>6</sup>*Power Line Communication* o anche chiamata a Onde Convogliate

<sup>7</sup>PLC-banda C CENELEC, con trasmissione almeno pari a 4,8 kbit/s

<sup>8</sup>Utilizzando la rete pubblica GPRS/UMTS/LTE

### **3. Sicurezza Integrata (*Security by Design*):**

- Crittografia avanzata: Implementa l'algoritmo di cifratura simmetrica *Advanced Encryption Standard (AES)* con chiavi a 128/256 bit per proteggere la confidenzialità e l'integrità dei dati scambiati sia con il concentratore che con i dispositivi utente.
- Autenticazione robusta: Gestisce processi di autenticazione per garantire che solo i dispositivi autorizzati possano comunicare con il contatore.

### **4. Gestione e Controllo Remoto:**

- Modifica remota della potenza: Consente al DSO di variare a distanza la potenza disponibile per l'utente, ad esempio per gestire clienti morosi senza intervento fisico.
- Comunicazioni al cliente: Permette al venditore o al distributore di inviare messaggi di testo personalizzati direttamente sul display del contatore.

## **Data Concentrator (DC)**

Il DC, o Concentratore, è un dispositivo intermedio che funge da ponte, *gateway*, tra la NAN e la WAN. Installato tipicamente nelle cabine di trasformazione secondarie (MT/BT), il suo ruolo è cruciale per la scalabilità e l'efficienza dell'infrastruttura AMI.

Esso aggrega le comunicazioni provenienti da centinaia o migliaia di SM, riducendo il traffico di rete e fungendo da primo livello di elaborazione e gestione dei dati sul campo.

Questo dispositivo è un elemento chiave del sistema di Telegestione, termine che descrive la capacità del DSO di monitorare e comandare la rete di bassa tensione da remoto.

## **Caratteristiche e Funzionalità Principali del Concentratore 2G**

Le specifiche tecniche [11] dei concentratori moderni riflettono il loro duplice ruolo di comunicazione e gestione. Le funzionalità possono essere suddivise come segue:

### **1. Comunicazione con gli Smart Meter (Interfaccia NAN):**

- Supporto Multi-Tecnologia: È dotato di modem PLC multi-modulazione, operante in banda A per garantire la retrocompatibilità con i contatori di prima generazione (1G), e di modem RF a 169 MHz per comunicare con i contatori 2G, utilizzando quest'ultimo anche come canale di backup.

### **2. Comunicazione con il Sistema Centrale (Interfaccia WAN):**

- Connattività Resiliente: Supporta molteplici canali di comunicazione verso l'Head-End System, inclusa la connattività mobile (3G/4G/5G) e una porta Ethernet per il collegamento a router in fibra ottica, garantendo alta affidabilità [5].
- Sicurezza del Canale: Implementa la cifratura del canale di comunicazione verso il sistema centrale secondo standard internazionali, assicurando la confidenzialità e l'integrità dei dati aggregati.

### **3. Gestione dei Dati e degli Eventi:**

- Raccolta Massiva e Aggregazione: È programmato per raccogliere in modo massivo i dati di misura (es. curve di carico, picchi di potenza) dagli Smart Meter e aggregarli prima dell'invio.
- Gestione di Eventi in Tempo Reale: Rileva e inoltra immediatamente al sistema centrale eventi critici provenienti dalla rete di bassa tensione, come l'assenza o il ripristino della tensione su un contatore 2G, permettendo al DSO di reagire prontamente a guasti o anomalie.

## **Head End System (HES)**

L'HES è il cuore software dell'infrastruttura AMI. Esso funge da interfaccia strategica, un *gateway* centralizzato che media la comunicazione tra i sistemi informativi aziendali del DSO e l'intero ecosistema di dispositivi distribuiti sul campo, ovvero i DC e, attraverso di essi, gli SM.

Il suo ruolo è quello di orchestrare e gestire tutte le interazioni con la rete di misurazione. Le sue funzioni principali possono essere sintetizzate come segue:

- **Gestione delle Comunicazioni:** Stabilisce, mantiene e protegge le sessioni di comunicazione con migliaia di DC simultaneamente.
- **Acquisizione Dati e Telegestione:** Esegue le operazioni di lettura massiva dei dati di misura (curve di carico, eventi) e invia comandi di telegestione verso i dispositivi periferici (es. aggiornamenti firmware, modifiche contrattuali, comandi di Demand Response).
- **Validazione e Normalizzazione:** Riceve i dati "grezzi" dal campo, li valida per verificarne la correttezza formale e li normalizza in un formato standardizzato, pronto per essere inoltrato ai sistemi di livello superiore.

L'HES ha un'importanza critica nel garantire il rispetto dei rigorosi parametri prestazionali imposti dalla normativa, come la delibera ARERA 87/2016<sup>9</sup>, in termini di volumi di dati processati e tempistiche di risposta. Per soddisfare tali requisiti, le implementazioni moderne di HES devono essere caratterizzate da un'elevata scalabilità e affidabilità. Questo obiettivo, come evidenziato in [12], è raggiungibile in modo efficace principalmente attraverso l'adozione di architetture cloud-native, un aspetto che espone questi sistemi a specifici vettori di minacce informatiche.

## **Meter Data Management System (MDMS)**

L'MDMS è la piattaforma software di back-end che agisce come repository centrale e motore analitico per tutti i dati di misura raccolti dall'infrastruttura AMI. Una volta che l'HES ha acquisito e normalizzato i dati provenienti dal campo, li inoltra all'MDMS, che diventa la "*single source of truth*" (unica fonte di verità) per tutte le informazioni relative ai consumi e allo stato della rete di bassa tensione.

Il ciclo di vita del dato all'interno dell'MDMS si articola in diverse fasi cruciali:

1. **Validazione, Stima e Modifica (VEE - Validation, Estimation, and Editing):** I dati grezzi vengono sottoposti a un processo rigoroso di VEE per identificare anomalie, correggere valori mancanti o palesemente errati attraverso algoritmi di stima, e preparare un *dataset* pulito e affidabile.
2. **Archiviazione a Lungo Termine:** I dati validati vengono memorizzati e archiviati in modo sicuro, garantendo la loro disponibilità per analisi storiche, dispute di fatturazione e obblighi normativi. La gestione dell'Alta Affidabilità (HA) e del *Disaster Recovery* (DR) di questi dati critici è spesso affidata ai meccanismi nativi delle piattaforme cloud su cui questi sistemi sono implementati.
3. **Analisi e Aggregazione:** L'MDMS aggrega i dati granulari per creare profili di carico, eseguire previsioni sui consumi futuri (*forecasting*) e calcolare i dati necessari per i processi di fatturazione.
4. **Integrazione e Condivisione:** Agisce come un hub centrale che espone i dati elaborati, in formati strutturati, ad altri sistemi aziendali critici. Ad esempio, fornisce dati aggregati al *Distribution Management System* (DMS) per ottimizzare le operazioni sulla rete di media/bassa tensione, o all'*Energy Management System* (EMS) per analisi a livello di rete di trasmissione.

In sintesi, se l'HES è il "motore" della comunicazione, l'MDMS è il "cervello" analitico che trasforma la mole di dati grezzi in informazioni di valore, abilitando decisioni operative e strategiche sia per il DSO che il TSO.

---

<sup>9</sup>Delibera 08 marzo 2016 87/2016/R/eel - <https://www.arera.it/atti-e-provvedimenti/dettaglio/16/87-16>

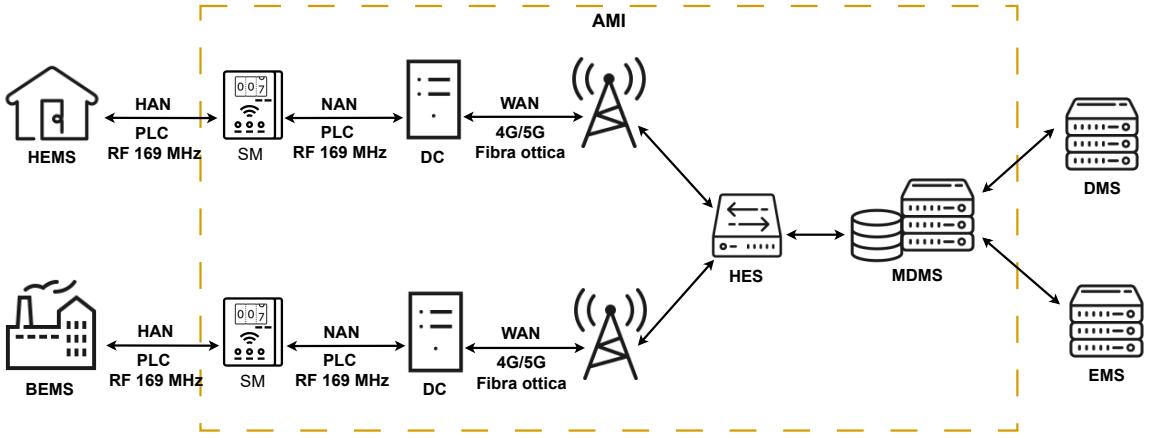


Figura 1.2: Dominio del consumatore

### 1.2.2 Dominio operazionale

Il Dominio Operazionale rappresenta il centro di controllo nevralgico della Smart Grid, l'insieme dei sistemi e delle tecnologie responsabili della gestione, del monitoraggio e della protezione dell'infrastruttura fisica di generazione, trasmissione e distribuzione dell'energia.

A differenza del Dominio del Consumatore, focalizzato sull'utente finale, questo dominio è di competenza esclusiva degli operatori di rete: il TSO per la rete di alta e altissima tensione e il DSO per le reti di media e bassa tensione.

L'obiettivo di questo dominio è garantire che l'energia sia prodotta, trasportata e consegnata in modo stabile, efficiente e sicuro, mantenendo in ogni istante l'equilibrio tra domanda e offerta. Per raggiungere questo scopo, si avvale di una complessa architettura tecnologica, i cui componenti principali possono essere raggruppati in tre categorie funzionali:

1. Sistemi di Monitoraggio Sincronizzato (WAMS): tecnologia utile per una visione in tempo reale dello stato della rete, basata su: *Phasor Measurement Unit* (PMU) e *Phasor Data Concentrator* (PDC)
2. Sistemi di Gestione Avanzata: le piattaforme software di alto livello per l'ottimizzazione e la gestione della rete, che includono: *Energy Management System* (EMS) per la rete di trasmissione, il *Distribution Management System* (DMS) per la rete di distribuzione e *Generation Management System* (GMS) per la programmazione della generazione.
3. Sistemi di Controllo e Acquisizione Dati (SCADA): la spina dorsale del controllo operativo, composta da: *Supervisory Control and Data Acquisition* (SCADA) e dispositivi di campo come *Remote Terminal Unit* (RTU) e *Intelligent Electronic Device* (IED).

Nei paragrafi seguenti, ciascuno di questi componenti verrà analizzato nel dettaglio per comprenderne il ruolo specifico e le interazioni all'interno dell'architettura operativa.

#### Phasor Measurement Units (PMU)

Il PMU, o unità di misura fasoriale, è un dispositivo di monitoraggio avanzato che rileva in tempo reale i fasori di tensione e corrente della rete elettrica. La caratteristica distintiva del PMU è la sua capacità di associare a ogni misura un marcitore temporale (*timestamp*) di altissima precisione, ottenuto tramite segnali di sincronizzazione da GPS o protocolli di rete come il *Precision Time Protocol* (PTP - IEEE 1588) [37].

Questa sincronizzazione temporale permette di confrontare istantaneamente le misure provenienti da punti diversi e geograficamente distanti della rete, creando una fotografia dinamica e coerente dello stato del sistema. I dati così ottenuti, noti come sincrofasori, sono fondamentali per analizzare fenomeni dinamici come le oscillazioni di potenza e per prevenire instabilità. Infatti, un disallineamento

fasoriale tra diverse aree della rete è un indicatore precoce di stress sistematico, che, se non gestito, può portare a disservizi o blackout.

I PMU sono i sensori alla base dei *Wide Area Monitoring Systems* (WAMS), sistemi di monitoraggio ad area estesa che offrono una visibilità in tempo reale sullo stato della rete. Grazie ai dati forniti dai PMU, gli operatori di rete possono:

- Eseguire un'analisi della stabilità del sistema in tempo reale.
- Rilevare con estrema rapidità l'insorgere di disturbi e anomalie.
- Migliorare l'efficacia delle procedure di protezione e controllo della rete.

Data la loro importanza strategica e il costo, i PMU sono installati prevalentemente nella Rete di Trasmissione Nazionale (RTN), su linee AT/AAT, e nei punti di connessione degli impianti di generazione di taglia significativa,  $\geq 50$  MVA, dove l'impatto sul sistema è maggiore [39]. Sebbene il loro impiego nelle reti di distribuzione (MT/BT) sia tecnicamente possibile e potenzialmente utile per gestire l'intermittenza delle fonti rinnovabili distribuite (DER), la loro diffusione in questo ambito è attualmente limitata da considerazioni economiche e dalla natura più localizzata dei fenomeni di instabilità a questo livello.

### Phasor Data Concentrator (PDC)

Il PDC è il componente centrale dell'architettura WAMS, agendo come nodo di aggregazione e sincronizzazione per i flussi di dati provenienti dai PMU. La sua funzione primaria è quella di raccogliere i dati dei sincrofasi da molteplici PMU, allinearli temporalmente in un unico *dataset* coerente e inoltrarli ai sistemi di gestione di livello superiore, come l'EMS o piattaforme SCADA avanzate.

I PDC sono spesso organizzati in un'architettura gerarchica: PDC di livello inferiore possono raccogliere dati direttamente dalle PMU, mentre PDC di livello superiore (o "Super PDC") aggregano i dati provenienti da altri PDC, permettendo una visione consolidata di intere regioni o dell'intera rete nazionale [15]. Figura 1.3.

Le capacità di un PDC possono essere riassunte nelle seguenti funzioni chiave:

- **Aggregazione e Sincronizzazione Dati:** Colleziona flussi di dati da più fonti, li ordina in base al loro timestamp e crea un set di dati unico e cronologicamente coerente, essenziale per un'analisi accurata dello stato della rete.
- **Elaborazione e Monitoraggio in Tempo Reale:** Oltre all'aggregazione, i PDC moderni possono eseguire calcoli e analisi in tempo reale sui dati ricevuti (es. controllo della qualità dei dati, rilevamento di eventi), fornendo riscontri immediati agli operatori.
- **Garanzia di Interoperabilità:** Un ruolo cruciale del PDC è quello di garantire l'interoperabilità tra dispositivi di diversi fornitori. Per questo, supporta una vasta gamma di protocolli standardizzati per il trasferimento dei sincrofasi, tra cui IEEE C37.118 (nelle sue varie revisioni) e IEC 61850-90-5. Questo permette al PDC di ricevere, interpretare e, se necessario, convertire dati tra diversi formati [1].
- **Comunicazione Robusta:** Per la trasmissione dei dati, i PDC utilizzano canali di comunicazione affidabili, tipicamente basati su reti Ethernet e protocolli standard come TCP/IP (sia IPv4 che IPv6), assicurando una connettività sicura e performante verso i sistemi centrali.

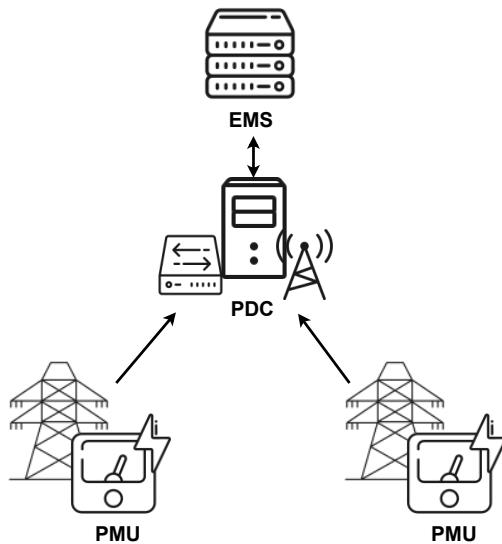


Figura 1.3: Esempio di connessione tra PMU e PDC [15]

### Energy Management System (EMS)

L'EMS<sup>10</sup> è la piattaforma software di alto livello che funge da "cervello" operativo e decisionale per la gestione della rete di trasmissione, AT e AAT. Mentre i sistemi SCADA si occupano primariamente dell'acquisizione dati e del controllo in tempo reale dei singoli apparati, l'EMS opera a un livello superiore: utilizza i dati provenienti da SCADA, PMU e altre fonti per eseguire analisi complesse e applicazioni di ottimizzazione, con l'obiettivo di garantire una gestione della rete sicura, affidabile ed economicamente efficiente [17, 46].

Le funzioni strategiche di un EMS sono finalizzate al mantenimento costante dell'equilibrio tra generazione e carico. Tra le sue principali responsabilità si includono:

- **Gestione del Bilanciamento (*Load-Frequency Control*):** L'EMS monitora costantemente la frequenza della rete, un indicatore diretto dell'equilibrio tra produzione e consumo. Attraverso algoritmi di controllo, regola automaticamente la produzione delle centrali per mantenere la frequenza entro i limiti di sicurezza stabiliti.
- **Dispacciamento Economico (*Economic Dispatch*):** Determina la ripartizione ottimale della produzione tra le diverse centrali disponibili, minimizzando i costi totali di generazione. Questo processo considera fattori come il costo del combustibile, l'efficienza degli impianti e i vincoli di rete.
- **Integrazione delle Fonti Rinnovabili:** Gestisce l'intrinseca variabilità e intermittenza delle fonti energetiche rinnovabili (FER), come l'eolico e il solare. Utilizza modelli previsionali per stimare la produzione da FER e coordina le risorse convenzionali e i sistemi di accumulo per compensarne le fluttuazioni.

In sintesi, l'EMS è un'infrastruttura critica che integra il monitoraggio in tempo reale con l'analisi avanzata, abilitando sia processi di controllo automatizzato sia il supporto alle decisioni per gli operatori umani ("human-in-the-loop"), indispensabili per il governo di un sistema complesso come la rete di trasmissione [17].

---

<sup>10</sup>In questo contesto si può parlare anche di Utility Energy Management Systems (UEMS) - destinato alle aziende di servizi pubblici che si concentrano a livello di distribuzione e trasmissione dell'energia di rete.

## Distribution Management System (DMS)

Il DMS è la piattaforma software di alto livello utilizzata dai *Distribution System Operator* (DSO) per il monitoraggio, il controllo e l'ottimizzazione delle reti di media e bassa tensione (MT/MB). Esso può essere considerato la controparte dell'EMS per il dominio della distribuzione: se l'EMS si concentra sulla stabilità e l'economia del sistema di trasmissione, il DMS è progettato per affrontare le sfide operative specifiche delle reti di distribuzione, come la gestione dei guasti, la regolazione della tensione e l'integrazione dei *Distributed Energy Resources* (DER).

Come l'EMS, anche il DMS si appoggia a un sistema SCADA per l'acquisizione dei dati e l'esecuzione dei comandi in campo. Tuttavia, le sue applicazioni analitiche sono specializzate per le caratteristiche delle reti di distribuzione. Le funzionalità chiave includono [20]:

- **Monitoraggio e Ottimizzazione della Rete:** Il DMS fornisce una visione completa dello stato della rete di distribuzione, analizzando i dati in tempo reale per identificare sovraccarichi, cadute di tensione e altre condizioni anomale. Sulla base di queste analisi, può suggerire o eseguire azioni correttive, come la riconfigurazione della rete o la regolazione dei trasformatori.
- **Gestione Automatica dei Guasti (FLISR):** Una delle applicazioni più critiche del DMS è la funzione di *Fault Location, Isolation, and Service Restoration* (FLISR). In caso di guasto, il sistema è in grado di:
  1. **Localizzare** automaticamente la sezione di rete interessata.
  2. **Isolare** il guasto comandando a distanza l'apertura degli interruttori appropriati.
  3. **Ripristinare** il servizio al maggior numero di utenze possibile, riconfigurando la rete per alimentare le sezioni sane da percorsi alternativi, il tutto in pochi secondi o minuti e prima dell'intervento fisico delle squadre tecniche.

Piattaforme commerciali come eXPert DMS<sup>11</sup> di SDI Automazione S.p.A. implementano queste funzionalità avanzate per migliorare significativamente l'affidabilità e la resilienza delle reti di distribuzione.

## Generation Management System (GMS)

Il GMS è una piattaforma software specializzata, utilizzata dalle società di generazione (GenCo) per la gestione ottimale del proprio portafoglio di impianti di produzione. Sebbene operi in stretto coordinamento con l'EMS del TSO, il suo focus è nettamente distinto: mentre l'EMS ha l'obiettivo di garantire la stabilità dell'intera rete, il GMS si concentra sull'ottimizzazione tecnico-economica degli asset di generazione, siano essi centrali convenzionali (termoelettriche, idroelettriche) o parchi di energia rinnovabile [18].

L'obiettivo principale del GMS è massimizzare la redditività e l'efficienza degli impianti, rispettando al contempo i vincoli tecnici e i segnali provenienti dal mercato dell'energia e dal TSO. Per raggiungere questo scopo, un GMS svolge diverse funzioni critiche:

- **Programmazione della Produzione (*Unit Commitment*):** Sulla base delle previsioni di prezzo del mercato elettrico e della domanda, il GMS determina quali centrali avviare o spegnere (*commitment*) e a quale livello di produzione farle operare (*dispatch*) nelle ore o nei giorni successivi per massimizzare i profitti.
- **Gestione delle Offerte sul Mercato:** Automatizza la preparazione e la sottomissione delle offerte di vendita di energia sui diversi mercati elettrici (es. Mercato del Giorno Prima, Mercato Infragiornaliero), basandosi su strategie commerciali complesse.
- **Monitoraggio delle Prestazioni degli Asset:** Controlla in tempo reale lo stato di salute e l'efficienza di ogni impianto di generazione, pianificando le attività di manutenzione in modo da minimizzare le perdite di produzione e i costi.

---

<sup>11</sup><https://sdiautomazione.com/prodotto/expert-dms/>

- **Gestione del Combustibile e delle Risorse:** Ottimizza l'approvvigionamento, lo stoccaggio e l'utilizzo delle risorse primarie (come gas naturale, carbone o riserve d'acqua per l'idroelettrico), un fattore cruciale per il controllo dei costi operativi.

In sintesi, il GMS agisce come il centro di comando strategico per un'azienda di generazione, traducendo gli obiettivi commerciali in piani operativi concreti per il proprio parco centrali.

### **Supervisory Control and Data Acquisition (SCADA)**

Il sistema SCADA rappresenta la spina dorsale per il controllo e il monitoraggio in tempo reale delle infrastrutture elettriche. Più che un singolo dispositivo, è un'architettura di automazione industriale progettata per raccogliere dati dal campo e fornire agli operatori gli strumenti per controllare a distanza gli apparati di rete.

### **Architettura di un Sistema SCADA**

Un'architettura SCADA tipica si articola su tre livelli gerarchici:

- Master Station (o *Master Terminal Unit* - MTU): Il centro di controllo centrale dove risiede il software SCADA. Qui, gli operatori umani monitorano lo stato della rete attraverso un'interfaccia grafica (*Human-Machine Interface* - HMI) e inviano comandi.
- Rete di Comunicazione: L'infrastruttura (es. fibra ottica, radio, reti cellulari) che collega la Master Station ai dispositivi sul campo.
- Dispositivi di Campo (RTU e IED): Le unità periferiche installate nelle sottostazioni o lungo le linee. Le *Remote Terminal Unit* (RTU) e gli *Intelligent Electronic Device* (IED) sono i "sensi" e le "braccia" del sistema: raccolgono dati dai sensori locali (misure di tensione, corrente, stato degli interruttori) e attuano i comandi ricevuti dalla Master Station.

### **Funzioni Operative**

Attraverso questa architettura, un sistema SCADA permette agli operatori di eseguire una serie di azioni di controllo fondamentali per la gestione della rete, come:

- Aprire e chiudere interruttori e sezionatori.
- Regolare la tensione attraverso la modifica dei *tap*<sup>12</sup> dei trasformatori.
- Commutare banchi di condensatori per la regolazione della potenza reattiva.

### **Posizione nella Gerarchia dei Sistemi di Controllo**

È cruciale comprendere la posizione dello SCADA rispetto a sistemi come EMS e DMS. Lo SCADA è il sistema di controllo operativo diretto. L'EMS e il DMS sono sistemi di gestione e ottimizzazione di livello superiore che si interfacciano con lo SCADA. Essi analizzano lo stato complessivo della rete e possono inviare comandi di alto livello (es. "ottimizza il profilo di tensione in quest'area"), che vengono poi tradotti dallo SCADA in azioni di controllo specifiche sui singoli apparati [21].

Piattaforme commerciali come eXPert SCADA<sup>13</sup> di SDI Automazione S.p.A. forniscono questo tipo di funzionalità integrate.

---

<sup>12</sup>I *tap* dei trasformatori, o commutatori di prese, sono dispositivi che permettono di variare il rapporto di trasformazione di un trasformatore, modificando così la tensione in uscita.

<sup>13</sup><https://sdiautomazione.com/product/expert-scada/>

## Remote Terminal Units (RTU)

Come anticipato, la RTU è il dispositivo di campo che funge da interfaccia diretta tra il sistema SCADA e gli apparati fisici della rete (es. interruttori, trasformatori). È un dispositivo a microprocessore, progettato per operare in ambienti elettricamente ostili e con elevata affidabilità.

Il suo ruolo operativo si articola in tre funzioni fondamentali:

- **Acquisizione Dati:** Raccoglie dati dallo stato degli impianti attraverso i suoi ingressi. Acquisisce sia segnali digitali (es. stato aperto/chiuso di un interruttore) sia misure analogiche (es. valori di tensione, corrente, temperatura), che vengono poi convertite in formato digitale.
- **Esecuzione Comandi:** Esegue i comandi ricevuti dalla Master Station SCADA attraverso le sue uscite. Un comando digitale, ad esempio, può provocare l'apertura o la chiusura di un interruttore automatico.
- **Comunicazione:** Gestisce la comunicazione con la Master Station, trasmettendo i dati raccolti e ricevendo i comandi, utilizzando protocolli SCADA specifici.

Tradizionalmente, la RTU è stata concepita come un raccoglitrice di dati e un esecutore di comandi con capacità di elaborazione limitate. Questa caratteristica la distingue dagli *Intelligent Electronic Devices* (IED), che integrano funzionalità di elaborazione e automazione più avanzate.

## Intelligent Electronic Devices (IED)

L'IED rappresenta l'evoluzione della RTU e il mattone fondamentale per l'automazione avanzata delle sottostazioni elettriche moderne. A differenza di una RTU tradizionale, che agisce principalmente come collettore di dati e attuatore di comandi, un IED integra capacità di elaborazione, comunicazione e controllo avanzate direttamente a livello di campo.

Esempi tipici di IED includono i relè di protezione digitali, i controllori di interruttori, i regolatori di tensione e i misuratori di qualità dell'energia. Le loro capacità distintive sono:

- **Elaborazione e Decisione Locale:** Un IED può eseguire autonomamente funzioni complesse, come rilevare un guasto sulla base di algoritmi interni e decidere di aprire un interruttore, senza attendere un comando esplicito dalla Master Station SCADA. Questa capacità di elaborazione locale riduce i tempi di reazione e aumenta l'affidabilità della protezione.
- **Dati di Alto Livello:** Invece di trasmettere solo dati grezzi (come una misura di corrente), un IED può elaborarli per fornire informazioni di valore aggiunto (es. "rilevato un picco di sovraccorrente", "calcolata la distorsione armonica totale").
- **Comunicazione Peer-to-Peer:** Gli IED moderni sono progettati per comunicare non solo "verticalmente" con il sistema SCADA, ma anche "orizzontalmente" tra di loro (*peer-to-peer*). Questa comunicazione diretta è fondamentale per schemi di protezione e automazione distribuiti e veloci, ed è normata dallo standard internazionale IEC 61850.

L'adozione diffusa degli IED segna un cambiamento di paradigma nell'automazione delle reti elettriche: si passa da un modello di controllo puramente centralizzato, tipico delle architetture basate su RTU, a un modello di intelligenza distribuita, dove le decisioni critiche possono essere prese in modo più rapido e autonomo direttamente sul campo.

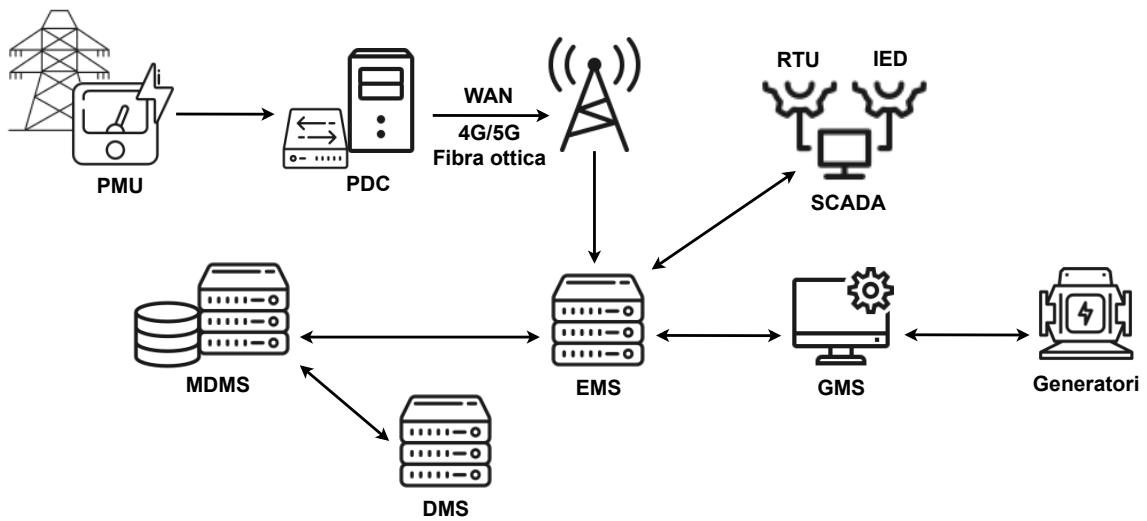


Figura 1.4: Dominio operazionale

# 2 Il Paradigma Cloud-Native per le Infrastrutture Smart Grid

Nel capitolo precedente è stata delineata l'architettura fondamentale della Smart Grid descrivendo i componenti tecnologici chiave dei domini del consumatore e operazionale. Questa analisi ha evidenziato come sistemi quali HES, MDMS ed EMS/DMS richiedano un'elevata capacità di calcolo, scalabilità e gestione di enormi volumi di dati. La risposta tecnologica a queste esigenze emergenti risiede nel *Cloud Computing*. Nell'Allegato C, come approfondimento, vengono presentati i concetti fondamentali e i principali vantaggi in termini di flessibilità, resilienza ed efficienza del *Cloud Computing*.

Questa sezione si propone di esplorare un modello architettonico per una Smart Grid basata su un approccio *Cloud-Native* decentralizzato, analizzando come tale implementazione possa rispondere alle sfide operative della rete moderna e, al contempo, introdurre nuove superfici di attacco e problematiche di sicurezza informatica.

## 2.1 Un Modello Architettonico Cloud-Native per la Smart Grid

Sulla base dei principi del *Cloud Computing* in questa sezione viene proposto un modello architettonico per l'implementazione di una Smart Grid secondo un paradigma *Cloud-Native*. L'obiettivo è illustrare come le moderne tecnologie *cloud* possano essere applicate per creare un'infrastruttura flessibile, scalabile e resiliente, superando i limiti dei sistemi monolitici tradizionali.

### 2.1.1 Logica di Disaccoppiamento: Componenti Centralizzati e Distribuiti

La prima scelta architettonica consiste nel separare i componenti in base alla loro funzione e ai loro requisiti operativi.

**Componenti Centralizzati (*Cloud*):** I sistemi caratterizzati da un'elevata intensità di calcolo, dalla necessità di gestire grandi volumi di dati e da requisiti di scalabilità elastica sono i candidati ideali per essere implementati come applicazioni *Cloud-Native*. In questo modello, rientrano le piattaforme software di alto livello: HES, MDMS, DMS, EMS, GMS, i SCADA Master e i PDC di alto livello. Questi sistemi beneficiano direttamente dell'agilità e della potenza di un'infrastruttura *cloud*.

**Componenti Distribuiti (*Edge*):** I dispositivi che interagiscono direttamente con il mondo fisico, che richiedono bassissima latenza o che devono garantire un funzionamento basilare anche in assenza di connettività, rientrano nel panorama dell'*Edge Computing*. Questi includono: *Smart Meter* (SM), *Data Concentrator* (DC), PMU, RTU e IED. Essi costituiscono i "sensi" e le "braccia" della rete, operando ai margini dell'infrastruttura.

### 2.1.2 Architettura a Cluster Federati e Trusted Boundaries

Come illustrato nella Figura 2.1 l'architettura proposta non si basa su un unico cloud monolitico, ma su una federazione di cluster Kubernetes indipendenti, ciascuno dedicato a un dominio funzionale e gestito dal relativo operatore. Questa scelta di progettazione, basata su Trusted Boundaries, persegue due obiettivi strategici:

1. **Robustezza e Sicurezza (*Isolation*):** L'isolamento dei cluster impedisce che un incidente di sicurezza o un malfunzionamento in un dominio (es. DMS) possa propagarsi direttamente e compromettere gli altri (es. EMS). Ogni cluster rappresenta un dominio di guasto e di sicurezza separato.

2. **Autonomia Operativa e di Governance:** Ogni operatore di rete (TSO, DSO, o potenziali terze parti per l'AMI) mantiene il pieno controllo sulla propria infrastruttura, gestendo autonomamente le proprie policy di sicurezza, gli aggiornamenti e le operazioni.

I principali cluster identificati sono:

- **Advanced Metering Infrastructure (AMI):** Contiene le applicazioni HES e MDMS. Potrebbe essere gestito dal DSO o da un operatore terzo specializzato.
- **Distribution Management System - BT/MT:** Di competenza del DSO, ospita le applicazioni DMS e lo SCADA Master per la rete di distribuzione.
- **Energy Management System - AT/AAT:** Di competenza del TSO, ospita EMS, GMS e lo SCADA Master per la rete di trasmissione.

La comunicazione sicura tra questi cluster indipendenti è garantita da tunnel VPN inter-cluster, come indicato nello schema.

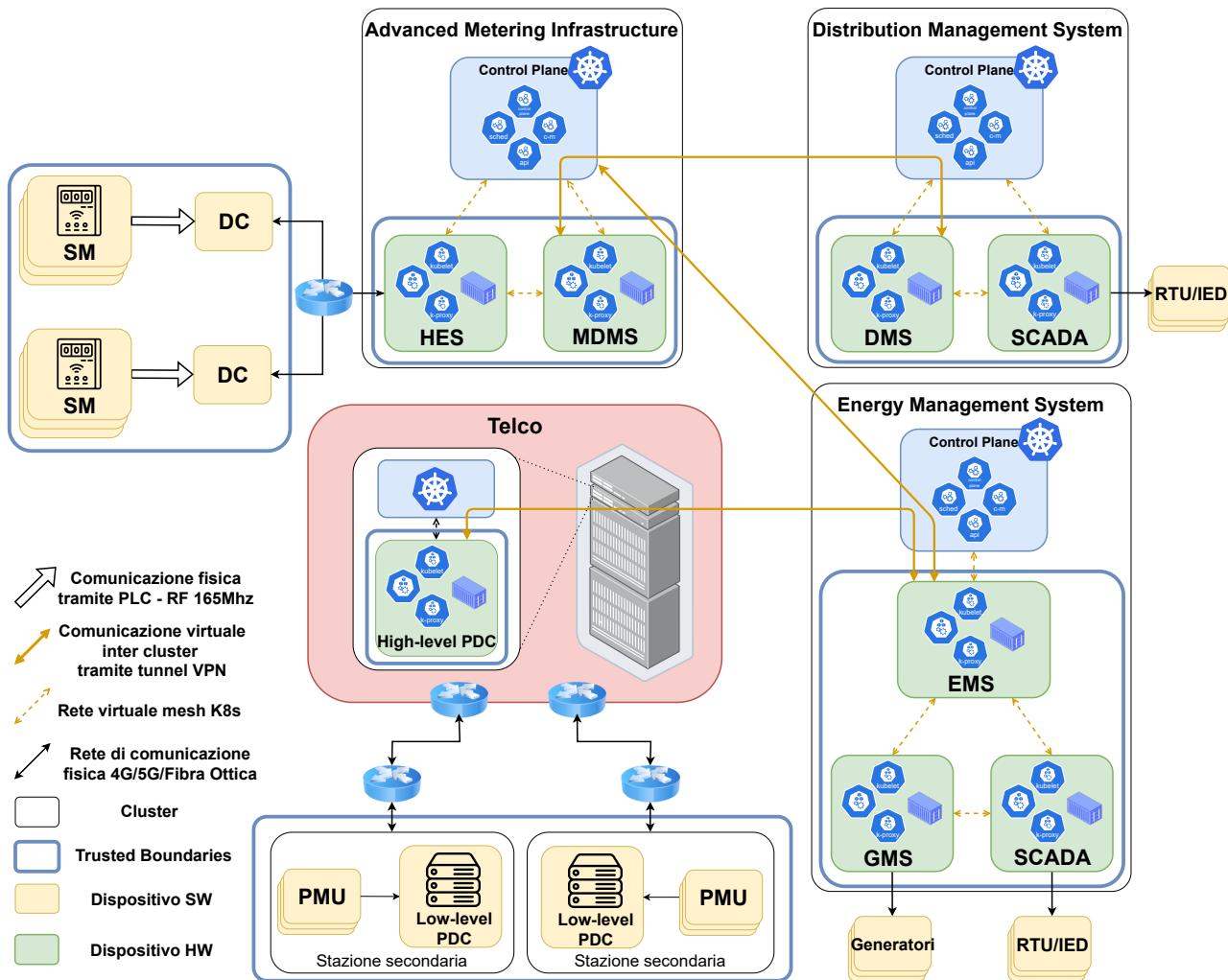


Figura 2.1: Architettura cloud native Smart Grid

### 2.1.3 Descrizione tecnica dei cluster Kubernetes

Come illustrato nel modello architetturale, ogni dominio funzionale è implementato come un cluster Kubernetes (K8s) autonomo. Un cluster K8s è composto da un insieme di macchine, chiamate nodi, che si dividono in due ruoli: nodi del *Control Plane* e nodi *Worker*.

#### 1. Il *Control Plane*

Il *Control Plane* è il cervello del cluster e ne gestisce lo stato globale. I suoi componenti principali, rappresentati schematicamente nella Figura 2.1, sono:

- *kube-apiserver*: Espone l'API di Kubernetes, fungendo da punto di ingresso per tutte le operazioni di gestione del cluster.
- *etcd*: Un database chiave-valore consistente e ad alta disponibilità, utilizzato per memorizzare in modo persistente tutti i dati di configurazione e lo stato del cluster.
- *kube-scheduler*: Assegna i nuovi Pod (le unità di esecuzione delle applicazioni) ai nodi *Worker* disponibili, in base ai requisiti di risorse e alle policy definite.
- *kube-controller-manager* (c-m): Esegue i controller che regolano lo stato del cluster, assicurando che lo stato attuale corrisponda a quello desiderato.

#### 2. *Worker Nodes*

I nodi *Worker* sono le macchine (virtuali o fisiche) dove le applicazioni containerizzate vengono effettivamente eseguite. Ogni nodo *Worker* esegue due agenti fondamentali:

- *kubelet*: L'agente primario che comunica con il *Control Plane* e si assicura che i container descritti nei Pod siano in esecuzione e in buono stato.
- *kube-proxy*: Un proxy di rete che gestisce la comunicazione di rete sui singoli nodi, implementando le regole che permettono ai servizi di essere raggiungibili.

Le applicazioni, come ad esempio l'EMS, vengono scomposte in microservizi e impacchettate in uno o più container, che vengono poi eseguiti all'interno dei Pod. Questa architettura a microservizi, sebbene più complessa, offre vantaggi significativi in termini di scalabilità selettiva, resilienza e isolamento dei guasti.

### Comunicazione all'interno e tra i Cluster

- **Intra-Cluster:** All'interno di un singolo cluster, Kubernetes fornisce una rete virtuale flat (rete a mesh) che permette a tutti i Pod di comunicare direttamente tra loro, indipendentemente dal nodo su cui si trovano. Questo facilita lo scambio di dati ad alta velocità tra i microservizi che compongono un'applicazione.
- **Inter-Cluster:** La comunicazione tra cluster diversi e isolati (es. tra il cluster DMS e il cluster EMS) è un'operazione controllata e sicura. Viene gestita esponendo servizi specifici attraverso l'API server e, come proposto nel modello, incanalando il traffico attraverso un tunnel VPN (*Virtual Private Network*). Questo approccio garantisce il rispetto della triade della sicurezza (Confidenzialità, Integrità, Disponibilità - *CIA Triad*), proteggendo i dati scambiati tra i domini fidati [32].



# 3 Modellazione delle Minacce Informatiche: Metodologie e Framework Applicativi

Nel capitolo precedente è stata presentata un'architettura per la Smart Grid basata su un paradigma *Cloud-Native* decentralizzato. È stato dimostrato come tale approccio offra significativi vantaggi in termini di scalabilità, resilienza e agilità. Tuttavia, la transizione da sistemi on-premise a infrastrutture distribuite e basate su cloud altera profondamente il panorama delle minacce, introducendo nuove superfici di attacco e vettori di compromissione.

Pertanto, una valutazione proattiva e sistematica di queste nuove vulnerabilità diventa un'attività indispensabile per garantire la sicurezza e l'affidabilità dell'intera infrastruttura. Questo capitolo costituisce il nucleo metodologico della tesi, fornendo gli strumenti concettuali per la modellazione delle minacce (*Threat Modeling*), un processo strutturato per identificare, analizzare e mitigare i rischi di sicurezza fin dalla fase di progettazione di un sistema.

La trattazione seguirà un percorso logico:

1. Inizialmente, verrà definito il processo di *Threat Modeling* e i suoi ambiti applicativi.
2. Successivamente, verranno illustrati i passi fondamentali che compongono questa metodologia.
3. Verrà poi introdotto in dettaglio il framework STRIDE, la metodologia scelta per la classificazione sistematica delle minacce in questo studio.
4. Infine, verranno esaminate le tipologie di minacce specifiche delle architetture *cloud*, preparando il terreno per l'applicazione pratica di questi concetti al modello di Smart Grid proposto nel capitolo successivo.

## 3.1 Esigenze e ambiti applicativi

Il panorama della sicurezza informatica è oggi caratterizzato da un'escalation costante di attacchi rivolti alle applicazioni software, con conseguenze che vanno dall'indisponibilità dei servizi a gravi danni economici e reputazionali. Per affrontare questa sfida, l'industria si sta spostando da un approccio puramente reattivo (rispondere agli incidenti dopo che si sono verificati) a un approccio proattivo, basato sul principio del *Secure by Design*.

Questo paradigma impone di integrare la sicurezza in ogni fase del ciclo di vita dello sviluppo del software (SDLC), partendo dal presupposto che le vulnerabilità sono una conseguenza inevitabile della complessità dei sistemi. Le loro origini, infatti, sono molteplici e possono derivare da [35]:

- Errori di programmazione introdotti dal team di sviluppo.
- Debolezze nelle policy di sicurezza aziendali.
- Vulnerabilità ereditate da componenti di terze parti, *framework* o librerie *open-source*.

In questo contesto, la modellazione delle minacce (*Threat Modeling*) emerge come lo strumento metodologico chiave per implementare il *Secure by Design*. Esso è un processo strutturato che, attraverso l'astrazione e l'analisi del sistema, consente di identificare e ragionare sulle potenziali minacce prima che queste possano essere sfruttate.

L'obiettivo finale del *Threat Modeling* non è solo creare una lista di possibili attacchi, ma fornire le informazioni necessarie per una corretta gestione del rischio. Per ogni minaccia identificata, l'organizzazione può infatti prendere una decisione strategica informata, scegliendo se il rischio debba essere:

- **Mitigato:** applicando una contromisura;
- **Eliminato:** rimuovendo la componente o la funzionalità vulnerabile;
- **Trasferito:** attraverso un'assicurazione o delegando a terzi;
- **Accettato:** se il costo della mitigazione supera il potenziale danno.

## 3.2 Il Processo di Threat Modeling

*"La modellazione delle minacce è un processo strategico<sup>1</sup> volto a prendere in considerazione i possibili scenari di attacchi e vulnerabilità all'interno di un ambiente applicativo proposto o esistente allo scopo di identificare chiaramente i livelli di rischio e di impatto."* [43]

L'adozione di questa metodologia offre vantaggi tangibili durante tutto il ciclo di vita dello sviluppo [36]:

- **Identificazione Precoce dei Difetti:** Permette di individuare vulnerabilità di progettazione nelle fasi iniziali dello sviluppo, riducendo drasticamente i costi di correzione rispetto a un loro rilevamento in fasi successive o dopo il rilascio del prodotto;
- **Definizione dei Requisiti di Sicurezza:** Aiuta a chiarire e a completare i requisiti di sicurezza, evidenziando aspetti inizialmente non considerati;
- **Miglioramento della Progettazione:** Conduce a un'architettura più robusta e sicura, minimizzando la necessità di costose riprogettazioni;
- **Analisi dei Rischi Logici:** A differenza di strumenti automatici che trovano bug<sup>2</sup> nel codice, il *Threat Modeling* è in grado di identificare difetti logici e di progettazione che nessun'altra tecnologia può rilevare;

Sebbene il processo possa avvalersi di tecniche collaborative come il *brainstorming*, esso viene tipicamente guidato da uno dei seguenti approcci metodologici [36]:

1. **Approccio Centrato sugli Asset (*Asset-centric*):** Il processo inizia con l'identificazione e la classificazione degli asset critici del sistema (es. dati sensibili, funzionalità chiave). Successivamente, si analizzano le minacce che potrebbero compromettere ciascun asset.
2. **Approccio Centrato sull'Attaccante (*Attacker-centric*):** Questo approccio si concentra sulla profilazione dei potenziali attaccanti, analizzandone le motivazioni, le capacità e gli obiettivi. Si cerca quindi di simulare le loro possibili azioni contro il sistema. Sebbene utile, questo metodo presenta il rischio che il team di sviluppo proietti le proprie conoscenze e i propri bias nel modello, sottostimando o ignorando le reali tattiche degli avversari.
3. **Approccio Centrato sul Software (*Software-centric*):** Considerato spesso il più efficace in contesti di sviluppo, questo approccio parte da una rappresentazione del sistema stesso, tipicamente attraverso diagrammi di flusso dei dati (DFD). Analizzando come i dati si muovono attraverso i componenti del sistema e superano i confini di fiducia (*trust boundaries*), il team può identificare sistematicamente le potenziali vulnerabilità.

<sup>1</sup>Si riferisce alla capacità di anticipare le minacce attraverso modelli di attacco simulati.

<sup>2</sup>Un bug è un errore nel codice di un programma che causa malfunzionamenti o comportamenti inaspettati, e può rappresentare una vulnerabilità sfruttabile per attacchi informatici.

### 3.3 Le Fasi del Processo di Threat Modeling

Il processo di modellazione delle minacce (*Threat Modeling*) è un'attività iterativa che può essere scomposta in quattro fasi fondamentali. Ciascuna fase è progettata per rispondere a una domanda chiave, guidando il team di analisi dalla comprensione del sistema alla validazione delle contromisure implementate [36, 35].

Di seguito vengono introdotte le quattro fasi, che saranno analizzate in dettaglio nei paragrafi successivi.

#### 1. Modellazione del Sistema (Risponde a: "Cosa stiamo costruendo?")

La prima fase consiste nel comprendere e rappresentare formalmente il sistema oggetto di analisi. Questo implica la definizione dei suoi componenti, dei confini di fiducia (*trust boundaries*), delle interfacce e, soprattutto, dei flussi di dati (DFD). Un modello accurato è il prerequisito fondamentale per una corretta identificazione delle minacce.

#### 2. Identificazione delle Minacce (Risponde a: "Cosa potrebbe andare storto?")

Una volta definito il modello, la seconda fase si concentra sull'identificazione sistematica delle potenziali minacce. Utilizzando framework strutturati come STRIDE, si analizza ogni elemento del modello per enumerare le vulnerabilità che potrebbero comprometterne la sicurezza. L'obiettivo è creare un elenco completo di possibili scenari di attacco.

#### 3. Mitigazione delle Minacce (Risponde a: "Cosa possiamo fare al riguardo?")

In questa fase, per ogni minaccia identificata, si definisce una strategia di gestione del rischio. Ciò comporta la progettazione e la prioritizzazione di contromisure di sicurezza (mitigazioni) volte a ridurre la probabilità o l'impatto della minaccia. Le strategie possono includere la modifica della progettazione, l'implementazione di controlli di sicurezza o la revisione delle policy.

#### 4. Validazione delle Mitigazioni (Risponde a: "Abbiamo fatto un buon lavoro?")

La fase finale chiude il ciclo verificando che le minacce siano state adeguatamente affrontate. Questo include la revisione delle contromisure implementate, l'esecuzione di test di sicurezza per validarne l'efficacia e l'aggiornamento della documentazione. Questo step garantisce che il processo abbia effettivamente ridotto il livello di rischio del sistema.



Figura 3.1: Le Fasi del Processo di Threat Modeling

#### 3.3.1 Modellazione del sistema

La prima e fondamentale fase del processo di *Threat Modeling* consiste nel creare una rappresentazione astratta ma accurata del sistema da analizzare. L'obiettivo è comprendere a fondo i suoi componenti, le interazioni e, soprattutto, come i dati fluiscano e vengono trattati al suo interno.

Lo strumento standard per questa attività è il *Data Flow Diagram* (DFD). Introdotto originalmente negli anni '70, il DFD è una tecnica di rappresentazione grafica che visualizza il flusso di

informazioni all'interno di un sistema. Invece di mostrare la logica di controllo (come farebbe un *flowchart*), un DFD si concentra esclusivamente sul movimento e sulla trasformazione dei dati.

Un DFD è composto da quattro elementi fondamentali:

1. **Entità Esterne (*External Entities*)**: Rappresentano gli attori, sia umani che altri sistemi, che interagiscono con il sistema inviando o ricevendo dati, ma che si trovano al di fuori del suo controllo (es. un utente, un'API di terze parti).
2. **Processi (*Processes*)**: Sono le componenti del sistema che elaborano o trasformano i dati. Ogni processo prende dei dati in input e produce dei dati in output.
3. **Archivio dati (*Data Store*)**: Rappresentano i luoghi in cui i dati vengono archiviati, sia in modo temporaneo (es. una cache) che permanente (es. un database).
4. **Flussi di Dati (*Data Flows*)**: Sono le frecce che collegano gli altri elementi del diagramma, indicando la direzione in cui i dati si muovono.

Per l'analisi di sicurezza, i DFD sono stati arricchiti con un quinto elemento cruciale: i Confini di Fiducia (*Trust Boundaries*). Questi confini sono linee tratteggiate che delimitano le aree del sistema con diversi livelli di privilegio o fiducia. Un flusso di dati che attraversa un trust boundary rappresenta un punto di ingresso critico (*entry point*) e una potenziale superficie di attacco che richiede un'analisi particolarmente attenta [30].

La costruzione di un DFD costringe il team a rispondere a domande essenziali: quali sono gli asset da proteggere? Chi sono gli attori che interagiscono con il sistema? Quali sono i punti di ingresso e come vengono validati i dati che li attraversano? Questo modello diventa così la mappa su cui, nella fase successiva, verranno sistematicamente identificate le minacce.

### 3.3.2 Identificazione delle minacce

Una volta ottenuto un modello chiaro del sistema attraverso il DFD, la seconda fase del processo consiste nell'identificare sistematicamente le minacce. Questa attività, spesso definita "*threat enumeration*", ha lo scopo di rispondere alla domanda: "Cosa potrebbe andare storto?". Si analizza ogni componente del DFD (processi, flussi di dati, data store) per individuare le potenziali vulnerabilità.

Per guidare questa analisi in modo strutturato e ripetibile, sono stati sviluppati numerosi framework e metodologie. Tra i più noti si includono:

- **STRIDE**: Un modello di classificazione delle minacce sviluppato da Microsoft, focalizzato sulle proprietà di sicurezza che un software dovrebbe garantire.
- **Attack Trees**: Una tecnica che scomponete un potenziale attacco in una struttura ad albero, mappando i passaggi necessari per raggiungere un obiettivo malevolo.
- **PASTA (Process for Attack Simulation and Threat Analysis)**: Una metodologia completa in sette fasi che allinea le minacce agli obiettivi di business.
- **CVSS (Common Vulnerability Scoring System)**: Sebbene non sia una metodologia di *threat modeling*, è un sistema di punteggio utilizzato per valutare la gravità delle vulnerabilità una volta identificate.
- **LINDDUN**: Un framework specifico per l'identificazione di minacce alla privacy.

Per l'analisi condotta in questa tesi, è stato scelto il framework STRIDE. Questa decisione è motivata dalla sua stretta integrazione con la modellazione basata su DFD e dalla sua efficacia nell'identificare un'ampia gamma di minacce a livello di progettazione software. La sua natura sistematica lo rende particolarmente adatto ad analizzare sistemi complessi e distribuiti come l'architettura Smart Grid *Cloud-Native* proposta. Il framework STRIDE verrà descritto in dettaglio nella sezione seguente.

### 3.3.3 Mitigazione delle Minacce

Una volta completata l'identificazione delle minacce, la terza fase del processo si concentra su come affrontarle. Non è sufficiente avere una lista di potenziali attacchi; è necessario valutarli, prioritizzarli e definire contromisure adeguate. Questo processo si articola in tre attività principali.

1. **Valutazione del Rischio (Risk Assessment):** Per ogni minaccia identificata, viene effettuata una valutazione del rischio associato. Questo non si basa solo sulla natura della minaccia stessa, ma su una combinazione di due fattori chiave:

- **Probabilità (Likelihood):** La probabilità che la vulnerabilità possa essere effettivamente sfruttata da un attaccante.
- **Impatto (Impact):** Il danno potenziale (operativo, finanziario, reputazionale) che si verificherebbe in caso di successo dell'attacco.

Molte metodologie, come DREAD, assegnano un punteggio a questi fattori per calcolare un livello di rischio complessivo per ogni minaccia.

2. **Prioritizzazione delle Minacce:** Sulla base del livello di rischio calcolato, le minacce vengono classificate in ordine di priorità, da quelle più critiche a quelle meno gravi. Questo permette al team di concentrare le risorse e l'attenzione sulla risoluzione dei problemi che rappresentano il maggior pericolo per il sistema.

3. **Definizione delle Contromisure:** Per le minacce prioritarie, si passa alla progettazione delle contromisure (o mitigazioni). L'obiettivo è applicare controlli di sicurezza che riducano la probabilità o l'impatto della minaccia a un livello accettabile. Come già discusso nel contesto della gestione del rischio, le opzioni non si limitano alla mitigazione; il team può decidere di eliminare una funzionalità, trasferire il rischio o accettarlo consapevolmente.

### 3.3.4 Validazione delle Mitigazioni

La fase finale del processo di Threat Modeling chiude il ciclo, assicurando che il lavoro svolto abbia effettivamente migliorato la postura di sicurezza del sistema. Questa fase di validazione ha un duplice obiettivo: verificare la completezza dell'analisi e l'efficacia delle contromisure implementate. Le attività principali includono:

1. **Revisione del Modello e delle Contromisure:** Si riesamina l'intero modello di minaccia per confermarne l'accuratezza e la completezza. Il team si assicura che tutte le minacce identificate siano state associate a una strategia di gestione del rischio e che le contromisure progettate siano state implementate correttamente secondo le specifiche.

2. **Analisi del Rischio Residuo:** È raro che tutte le minacce possano essere eliminate completamente. Per le minacce che sono state mitigate (ma non eliminate) o accettate, si valuta il rischio residuo, ovvero il livello di rischio che permane nel sistema dopo l'applicazione dei controlli di sicurezza. È compito dei responsabili del rischio (*risk owner*) determinare se tale rischio residuo rientri nella soglia di tolleranza definita dall'organizzazione.

3. **Test di Sicurezza e Validazione Pratica:** Per verificare empiricamente l'efficacia delle mitigazioni, si ricorre a test di sicurezza. Questi possono includere:

- **Penetration Testing:** Viene eseguito un attacco simulato da parte di "ethical hacker" per tentare di sfruttare le vulnerabilità del sistema. I risultati vengono poi confrontati con le minacce identificate nel modello per verificarne la copertura.
- **Security Test Case:** Vengono creati casi di test specifici per validare che ogni singola contromisura funzioni come previsto (es. "verificare che un input malizioso venga correttamente rigettato dal sistema di validazione").

Solo al termine di questa fase di validazione si può considerare concluso un ciclo di *Threat Modeling*. Il modello, tuttavia, non è un documento statico: deve essere rivisto e aggiornato ogni volta che il sistema subisce modifiche significative.

### 3.4 Il framework utilizzato: STRIDE

Sviluppato originariamente da Microsoft, STRIDE è un modello di classificazione delle minacce che aiuta gli analisti a identificare sistematicamente un'ampia gamma di vulnerabilità di sicurezza. Il suo scopo è fornire un approccio mnemonico e strutturato per ragionare sulle possibili minacce contro ogni componente di un sistema, mappando ogni minaccia a una specifica proprietà di sicurezza che viene violata [30, 36].

L'acronimo STRIDE rappresenta sei categorie di minacce:

- ***Spoofing*** (Falsificazione dell'identità): Si verifica quando un aggressore si finge illegittimamente un altro utente, componente o sistema. Viola la proprietà di Autenticazione.
- ***Tampering*** (Manomissione): Consiste nella modifica non autorizzata di dati, sia in transito su una rete che archiviati in un data store. Viola la proprietà di Integrità.
- ***Repudiation*** (Ripudio): Si riferisce alla capacità di un utente di negare di aver compiuto un'azione, in assenza di prove che dimostrino il contrario. Viola la proprietà di Non Ripudio.
- ***Information Disclosure*** (Rivelazione di informazioni): Consiste nell'esposizione di informazioni sensibili a soggetti non autorizzati. Viola la proprietà di Confidenzialità.
- ***Denial of Service*** (DoS - Negazione del servizio): Si verifica quando un attaccante rende un sistema o una risorsa non disponibile per gli utenti legittimi. Viola la proprietà di Disponibilità.
- ***Elevation of Privilege*** (EoP - Acquisizione di privilegi): Avviene quando un utente con privilegi limitati riesce a ottenere accessi o permessi superiori a quelli che gli sono stati assegnati. Viola la proprietà di Autorizzazione.

La forza di STRIDE risiede nella sua applicazione sistematica a un *Data Flow Diagram*. Una volta creato il DFD, la modellazione delle minacce basata su STRIDE può essere eseguita in due modi:

- STRIDE per-elemento: per ogni minaccia coperta da STRIDE, ogni componente del sistema viene analizzato per verificare se può essere soggetto a questa minaccia.
- STRIDE-per-interazione: i componenti del sistema sono considerati in tuple (origine, destinazione e interazione) e la loro interazione viene analizzata per verificare se può essere soggetta a una o più minacce coperte da STRIDE.

# 4 Applicazione del Threat Modeling all’Architettura Proposta

Nei capitoli precedenti sono stati definiti i tre pilastri concettuali di questa tesi: il concetto di Smart Grid con la sua architettura e componenti (Capitolo 1), un’implementazione di una Smart Grid basata su un paradigma *Cloud-Native* (Capitolo 2) e la metodologia formale del *Threat Modeling* per l’analisi della sicurezza dei sistemi (Capitolo 3).

Questo capitolo rappresenta il punto di convergenza di questi tre elementi, costituendo il contributo centrale della ricerca. L’obiettivo è applicare sistematicamente il processo di *Threat Modeling*, e in particolare il framework STRIDE, al modello architettonico proposto, al fine di identificare e classificare le principali minacce informatiche che lo caratterizzano.

L’analisi seguirà fedelmente le quattro fasi metodologiche descritte in precedenza:

1. **Modellazione del Sistema:** Verrà presentato e discusso in dettaglio il *Data Flow Diagram* (DFD) dell’architettura.
2. **Identificazione delle Minacce:** Ogni componente del DFD verrà analizzato attraverso la lente di STRIDE per enumerare le potenziali minacce.
3. **Mitigazione delle Minacce:** Per le minacce più significative, verranno proposte delle contromisure di sicurezza specifiche per il contesto *Cloud-Native*.
4. **Validazione:** Verrà discusso un piano di validazione delle minacce.

## 4.1 Definizione del Data Flow Diagram

In questa sezione si avvia l’applicazione pratica del processo di *Threat Modeling* all’architettura Smart Grid *Cloud-Native* proposta. Il primo passo fondamentale, come descritto dalla metodologia, consiste nella modellazione del sistema attraverso un DFD.

La Figura 4.1 presenta un DFD di Livello 0 che astrae l’architettura, evidenziandone i componenti principali, i flussi di dati e, soprattutto, i confini di sicurezza. In questo modello sono stati identificati i seguenti elementi:

- **Entità Esterne:** Componenti che interagiscono con il sistema ma si trovano al di fuori del suo controllo diretto, come lo *Smart Meter*, l’RTU/IED e il sistema PMU/PDC.
- **Processi:** I componenti software che elaborano i dati, come l’AMI, il DMS e l’EMS.
- **Archivi Dati:** I luoghi di memorizzazione dei dati, rappresentati dai *Cloud Store*.

Per l’analisi di sicurezza, sono stati definiti due tipi di confini (*boundaries*), ciascuno con un significato preciso:

1. **Trust Boundary (confine rosso):** Rappresenta un confine logico che separa componenti con diversi livelli di fiducia. Qualsiasi flusso di dati che attraversa un *Trust Boundary* deve essere considerato potenzialmente ostile e quindi soggetto a rigorose procedure di autenticazione, autorizzazione e validazione. Questi confini definiscono la superficie di attacco di ciascun servizio.
2. **Machine Boundary (confine blu):** Rappresenta un confine fisico o a livello di dispositivo. Esso isola i componenti che operano sul campo (*Edge*), come il *Data Concentrator* o il *Phasor Data Concentrator*, dal loro ambiente fisico e dalla rete locale. Questo confine è rilevante per analizzare minacce di accesso fisico (manomissione) o attacchi diretti al dispositivo, che bypasserebbero i controlli a livello di applicazione.

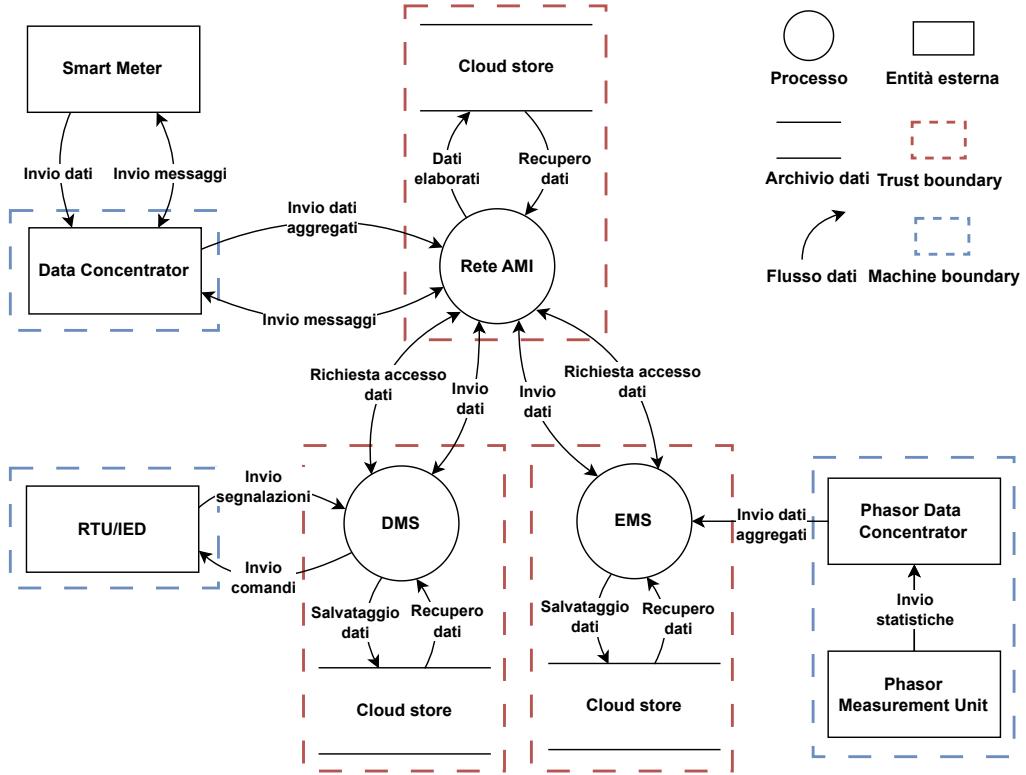


Figura 4.1: Data flow diagram - Smart Grid Cloud-Native

#### 4.1.1 Definizione dell'Ambito di Analisi

Prima di procedere con l'analisi delle minacce, è essenziale definire con precisione il perimetro (*scope*) di questo studio. Data la vastità dell'ecosistema Smart Grid, l'analisi si concentrerà specificamente sulle vulnerabilità introdotte dalla sua implementazione in un'architettura *Cloud-Native*.

Di conseguenza, verranno prese in considerazione le minacce relative ai componenti software centralizzati e ai canali di comunicazione che li collegano al campo.

La Tabella 4.1 riassume formalmente questa suddivisione, elencando gli elementi considerati oggetto di analisi (*In Scope*) e esclusi dall'analisi (*Out of Scope*).

Tabella 4.1: Definizione dell'ambito di analisi

	Oggetto in analisi	Oggetto fuori dall'analisi
Componenti software:	SM, HES, MDMS, DMS, EMS, SCADA, GMS, High-level PDC	Sicurezza dei dispositivi hardware: DC, RTU/IED, Generatori, low-level PDC, PMU
Canali di comunicazione:	PLC/RF 169 MHz, 4G/5G, Fibra, VPN	Sicurezza della cabina Telco
Infrastruttura cloud:	Kubernetes e container	

#### 4.1.2 Identificazione degli Asset Critici

Successivamente alla definizione della struttura del sistema tramite il DFD, è cruciale identificare gli asset, ovvero gli elementi di valore all'interno dell'architettura la cui compromissione causerebbe un danno significativo. Sapere cosa si sta proteggendo è un prerequisito fondamentale per poter valutare l'impatto reale di una minaccia. Un'analisi completa considera che gli asset non sono limitati ai soli dati, ma includono anche i processi e i componenti infrastrutturali che li gestiscono. Per questa tesi, gli asset sono stati classificati in tre tipologie principali:

1. **Dati:** Rappresentano le informazioni sensibili o critiche gestite dal sistema. La loro compromissione può portare a violazioni della privacy, frodi o perdita di controllo sulla rete. Esempi includono i dati di consumo dei clienti, le statistiche di rete delle PMU e le credenziali di accesso come token e chiavi API.
2. **Processi:** Sono le funzioni operative e di elaborazione chiave del sistema. Un attacco a un processo può corrompere i dati, causare un'interruzione del servizio o portare a decisioni errate nella gestione della rete. Esempi includono l'elaborazione dei dati da parte dell'MDMS o il monitoraggio della rete da parte dell'EMS.
3. **Infrastruttura Logica:** Costituisce la base tecnologica su cui poggia l'intera architettura. La compromissione di questi componenti può avere un impatto a cascata su tutti i servizi ospitati. Esempi includono i cluster Kubernetes, le immagini dei container e l'infrastruttura VPN che garantisce la comunicazione sicura.

La Tabella 4.2 presenta una sintesi dei principali asset identificati per l'architettura in esame, classificati secondo queste tre tipologie.

Tabella 4.2: Identificazione degli Asset Critici

Dati	Processi	Infrastruttura logica
Statistiche del cliente	Dati collezionati da HES	Cluster K8s
Fatturazione consumi (MDMS)	Elaborazione dei dati MDMS	Immagini container
Statistiche di rete (PMU)	Monitoraggio della rete EMS/DMS	Infrastruttura VPN
API, credenziali, token	Dati collezionati da high-level PDC	Cloud storage

## 4.2 Analisi delle Minacce con il Framework STRIDE

Dopo aver modellato il sistema, si procede ora con la fase di identificazione delle minacce, il cuore di questa analisi. Come anticipato, questa fase verrà condotta applicando sistematicamente il framework STRIDE e utilizzando come riferimento il *Data Flow Diagram* Figura 4.1.

L'approccio utilizzato sarà quello di STRIDE-per-elemento: per ogni componente del DFD (processi, *data store*, flussi di dati ed entità esterne), verranno considerate le categorie di minaccia STRIDE pertinenti. Questo metodo garantisce una copertura completa e strutturata, riducendo il rischio di tralasciare vulnerabilità significative.

Tabella 4.3: Minacce informatiche

ID Mi- naccia	Elemento	Categoria STRIDE	Descrizione minaccia	Possibile attaccante
S-01	Smart Me- ter	Spoofing	Una mancanza di risorse e memoria limitata su SM e dispositivi di campo, possono impedire l'implementazione di tutte le funzionalità di sicurezza e l'aggiornamento del firmware, rendendoli più vulnerabili ad attaccanti esperti che riescono a sfruttare queste vulnerabilità minando l'affidabilità dei dati inviati ai DC. [38]	Attaccante esterno
T-01	Flusso dati PDC	Tampering	Un attaccante non si limita ad un possibile DoS bloccando i dati inviati dai PDC su rete 4G/5G, bensì cerca di intercettare il traffico e modificare leggermente e costantemente tutti i dati prima che essi raggiungano l'EMS. Questo attacco simula un carico fantasma o una falsa instabilità di frequenza. L'EMS che si fida di questi dati reagisce automaticamente ridirigendo l'energia o sezionando la zona, causando gravi disagi. [38]	Attaccante esterno
R-01	Dati consu- matori	Repudiation	Un attaccante esterno, riuscendo ad avere accesso privilegiato con permessi di lettura e scrittura al <i>cloud store</i> dell'infrastruttura AMI, riesce a modificare i dati contenuti nel database con conseguente impatto sulle misure fino ad ora effettuate e possibili previsioni future.	Attaccante esterno
I-01	Software di gestione	Information Disclosure	Un attaccante può sfruttare le vulnerabilità scoperte nei software <i>open source</i> , come ad esempio OpenEMS, per compromettere i sistemi EMS delle aziende che li utilizzano. Alternativamente, l'attaccante può inserire codice malevolo nel progetto <i>open source</i> , che successivamente utilizzerà per condurre attacchi mirati all'esfiltrazione dei dati dell'azienda.	Attaccante esterno

ID Minaccia	Elemento	Categoria STRIDE	Descrizione minaccia	Possibile attaccante
D-01	Disponibilità servizio	Denial of Service	L'attaccante riesce ad accedere alle cabine secondarie del DSO e si collega tramite uno <i>switch</i> tra il <i>gateway</i> e la RTU. Questa posizione privilegiata gli consente di intercettare il traffico di rete e identificare il server SCADA presente nel DMS. Una volta individuato il target, l'attaccante può lanciare un attacco DoS (magari utilizzando un software come <i>hping</i> ) contro il servizio cloud che ospita il cluster Kubernetes, saturando il canale di trasmissione e causando latenze significative ( <i>Bottleneck</i> ). Queste latenze compromettono gravemente l'invio tempestivo dei dati di telemetria, delle segnalazioni e dei comandi di controllo provenienti dallo SCADA Master, causando potenziali disfunzioni operative nella rete di distribuzione. [19]	Attaccante esterno
E-01	Invio comandi	Elevation of Privilege	Una volta ottenuto il controllo di un cluster Kubernetes del DMS sfruttando l'endpoint API utilizzato per l'invio delle segnalazioni da parte di RTU/IED, un attaccante può evitare di causare un singolo e vistoso disservizio, optando invece per sfruttare le capacità del DMS di controllare migliaia di dispositivi sul campo (RTU/IED) per lanciare un attacco distribuito e coordinato. L'attaccante può inviare comandi di apertura e chiusura degli interruttori o regolare la tensione dei trasformatori, causando oscillazioni di frequenza e tensione su tutta la rete di distribuzione, con effetti che possono propagarsi fino a perturbare la rete di alta tensione.	Attaccante esterno con aiuto da insider

## 4.3 Strategie di Mitigazione e Contromisure di Sicurezza

Tabella 4.4: Mitigazione delle minacce

ID Minaccia	Descrizione minaccia	Mitigazione proposta	Categoria mitigazione
S-01	Impersonificazione di SM	Durante la fase di acquisto dei dispositivi da utilizzare per centinaia di migliaia di dispositivi, il DSO deve imporre requisiti di sicurezza minimi obbligatori durante il bando di gare. L'utilizzo di pattern statistici e algoritmi di <i>Anomaly Detection</i> da parte dell'AMI, può essere d'aiuto per valutare eventuali dispositivi compromessi.	Mitigare
T-01	Manomissione dati in transito	L'utilizzo di crittografia e autenticazione <i>End-to-End</i> può rendere la manomissione dei dati difficile. L'EMS non si dovrebbe fidare ciecamente bensì deve tutelarsi incrociando dati da altri dispositivi utilizzando pattern statistici di correlazione. [38]	Mitigare
R-01	Furto e/o modifica dei dati AMI	I dati una volta validati devono essere archiviatati in un database <i>WORM</i> ( <i>Write-Once, Read-Many</i> ) garantendo la non mutabilità del dato. Nessuna singola persona, a prescindere dal ruolo, dovrebbe avere i permessi per leggere, modificare e cancellare dati sensibili, sia di utenti sia aziendali.	Mitigare
I-01	Inserimento di codice malevolo	Verificare attraverso <i>code review</i> l'utilizzo delle <i>Best Practices</i> di sicurezza, implementative e le ulteriori librerie open-sorce utilizzate	Accettare
D-01	Minare il funzionamento dello SCADA Master	La simulazione ha rivelato che il collo di bottiglia delle prestazioni durante un attacco DoS erano i router, la cui CPU veniva utilizzata al 100%, rendendoli irresponsabili sia tramite interfaccia web che CLI. Al contrario, il dispositivo di monitoraggio (che simula il server SCADA) ha mostrato un impatto minimo sull'utilizzo di CPU e RAM. Questo suggerisce che se il router è il punto debole, una parte significativa del traffico d'attacco può essere bloccata a quel livello, impedendo che raggiunga il server SCADA e potenzialmente l'intera rete attraverso l'impostazione di regole firewall appropriate [19]	Mitigare
E-01	Attacco distribuito MT/BT	Nessun singolo processo deve avere la possibilità di controllare tutti i dispositivi di campo. I privilegi di comando devono essere segmentati geograficamente e/o per dispositivo, seguendo il modello RBAC. Inoltre per comandi ad alto impatto deve essere predisposto almeno una seconda approvazione da parte del personale.	Mitigare

## 4.4 Approcci alla Validazione delle Contromisure

La fase finale del ciclo di *Threat Modeling*, la validazione, è essenziale per garantire che le contromisure proposte siano efficaci e che la sicurezza complessiva del sistema sia stata effettivamente migliorata. Sebbene un'implementazione e una validazione empirica completa dell'architettura proposta esulino dall'ambito di questa tesi, è possibile delineare un piano di validazione strutturato.

Questo piano si baserebbe su una combinazione di revisioni di progettazione e test di sicurezza pratici, mirati a verificare le mitigazioni suggerite.

### 1. Revisione e Analisi del Rischio Residuo:

Il primo passo consisterebbe in una revisione formale delle contromisure progettate per ogni minaccia. Per ciascuna, si dovrebbe valutare il rischio residuo, ovvero il livello di rischio che permane anche dopo l'implementazione della mitigazione. L'obiettivo è assicurarsi che tale rischio sia sceso al di sotto della soglia di accettabilità definita dagli *stakeholder* del sistema.

### 2. Test di Sicurezza a Livello di Infrastruttura Cloud-Native:

Per validare le contromisure legate alla configurazione di Kubernetes e dei container, si potrebbero eseguire le seguenti attività:

- Scansione delle Immagini dei Container: Utilizzare strumenti come Trivy o Clair per scansioneare le immagini dei container (HES, DMS, etc.) alla ricerca di vulnerabilità note in librerie e dipendenze.
- Analisi della Configurazione del Cluster (*IaC Scanning*): Impiegare strumenti come Kube-bench o Checkov per analizzare i file di configurazione di Kubernetes (*Infrastructure as Code*) e verificare che siano conformi alle *best practice* di sicurezza del CIS (*Center for Internet Security*).

### 3. Test di Sicurezza a Livello Applicativo e di Rete:

Per verificare le contromisure a livello di servizio, si potrebbero pianificare test più attivi:

- *Penetration Testing* mirato: Eseguire test di penetrazione focalizzati sui punti più critici emersi dall'analisi STRIDE. Ad esempio, si potrebbe tentare di sfruttare una debolezza nelle API esposte dal cluster EMS o di effettuare un attacco di *Tampering* sui dati scambiati tramite la VPN inter-cluster.
- Creazione di *Security Test Case*: Sviluppare test automatici che verifichino specifiche contromisure. Ad esempio, un test potrebbe simulare una richiesta con un token di autenticazione invalido per assicurarsi che venga correttamente respinta, validando così una mitigazione contro lo *Spoofing*.

L'esecuzione di queste attività di validazione fornirebbe un feedback concreto sull'efficacia delle strategie di mitigazione proposte e completerebbe il ciclo iterativo del *Threat Modeling*, trasformando l'analisi teorica in una base solida per un'implementazione sicura.



# 5 Conclusioni e sviluppi futuri

Questo lavoro di tesi ha affrontato le implicazioni di sicurezza derivanti dalla convergenza tra le reti elettriche di nuova generazione, le Smart Grid, e il paradigma architetturale *Cloud-Native*. Partendo da questo presupposto, l'obiettivo del presente elaborato è stato duplice: in primo luogo, delineare un'architettura moderna e scalabile per una Smart Grid, basata su una federazione di cluster Kubernetes; in secondo luogo, applicare in modo sistematico il framework STRIDE di modellazione delle minacce per analizzare proattivamente le vulnerabilità che un simile sistema si troverebbe ad affrontare.

Il percorso di ricerca ha seguito una logica progressiva. Si è partiti da una definizione dei componenti fondamentali della Smart Grid (Capitolo 1) per poi analizzare il paradigma *Cloud-Native* (Capitolo 2), evidenziandone il ruolo cruciale nelle moderne applicazioni distribuite. Successivamente, è stata introdotta la metodologia formale del *Threat Modeling* con le sue quattro fasi (Capitolo 3). Questa preparazione metodologica è culminata nella definizione di un *Data Flow Diagram* per l'architettura proposta e nella conseguente analisi delle minacce (Capitolo 4). Questa applicazione metodica si è rivelata cruciale per andare oltre le vulnerabilità più evidenti, facendo emergere minacce specifiche legate all'interazione tra i componenti *cloud* e i dispositivi sul campo, che aggiungono un valore significativo all'analisi della sicurezza.

L'analisi ha confermato che l'ecosistema Smart Grid presenta sfide di notevole complessità, soprattutto dal punto di vista della sicurezza informatica. Come evidenziato, è indispensabile un'attenta e continua analisi dei rischi, supportata da piani di mitigazione e risposta agli incidenti. La posta in gioco è altissima: l'energia elettrica è un'infrastruttura critica per qualsiasi nazione moderna, e un guasto o un attacco mirato alla rete nazionale comporterebbe gravissime perdite economiche per le imprese e profondi disagi per i cittadini.

In sintesi, il contributo principale di questo elaborato risiede nell'applicazione di un approccio *"Secure by Design"* a un'infrastruttura ciber-fisica complessa. Sono state identificate minacce concrete come attacchi di *Tampering* ai flussi di dati, *Denial of Service* contro i sistemi di controllo centrali e campagne coordinate di *Elevation of Privilege* per manipolare la rete. Per ciascuna di esse, sono state proposte strategie di mitigazione adeguate al contesto *Cloud-Native*, dimostrando come un'analisi proattiva sia fondamentale per costruire sistemi resilienti.

## Limiti e Sviluppi Futuri

Il focus di questo elaborato è stato principalmente l'identificazione di minacce a livello architettonico. Di conseguenza, il naturale e più importante sviluppo futuro consisterebbe nel testare e validare empiricamente l'architettura proposta e le minacce identificate.

In conclusione, la messa in sicurezza delle infrastrutture energetiche del futuro è un percorso iterativo e una sfida tecnologica costante. Questo lavoro si pone come un passo in tale direzione, fornendo una metodologia e un'analisi concreta per affrontare tale complessità con rigore e proattività.



# Bibliografia

- [1] Ieee guide for phasor data concentrator requirements for power system protection, control, and monitoring. *IEEE Std C37.244-2013*, pages 1–65, 2013.
- [2] Ammar Albayati, Nor Fadzilah Abdullah, Asma Abu-Samah, Ammar Hussein Mutlag, and Rosdiadee Nordin. A serverless advanced metering infrastructure based on fog-edge computing for a smart grid: A comparison study for energy sector in iraq. *Energies*, 13(20), 2020.
- [3] Arera. Elenco delle società di distribuzione dell'energia elettrica sul territorio nazionale. [https://www.arera.it/area-operatori/ricerca-operatori?tiporicerca=PER\\_ATTIVITA&listaAttivititaPerCerca=4](https://www.arera.it/area-operatori/ricerca-operatori?tiporicerca=PER_ATTIVITA&listaAttivititaPerCerca=4).
- [4] Areti. I nostri numeri. <https://www.areti.it/conoscere-areti>.
- [5] Areti. La comunicazione dei consumi al fornitore. <https://www.areti.it/gestione-rete/contatore-2g-smart-meter/come-si-usa>.
- [6] GSE – Gestore dei Servizi Energetici. Composizione del mix iniziale nazionale utilizzato per la produzione dell'energia elettrica immessa nel sistema elettrico italiano nel 2023. <https://www.gse.it/servizi-per-te/news/fuel-mix-pubblicata-la-composizione-del-mix-energetico-relativo-agli-anni-2022-e-2023>.
- [7] Jianguo Ding, Attia Qammar, Zhimin Zhang, Ahmad Karim, and Huansheng Ning. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, 15(18), 2022.
- [8] Set Distribuzione. Chain 2. <https://www.setdistribuzione.it/attivita/smarthemeter/chain-2.html#:~:text=La%20Chain%202%20permette%20la,di%20consumo%20in%20tempo%20reale>.
- [9] E-Distribuzione. Bilancio esercizio e-distribuzione 2024. [https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/e-distribuzione/Bilancio\\_esercizio\\_2024.pdf](https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/e-distribuzione/Bilancio_esercizio_2024.pdf).
- [10] E-Distribuzione. Open meter. <https://www.e-distribuzione.it/open-meter/open-meter--il-contatore-2-0.html>.
- [11] E-Distribuzione. Open meter - piano di messa in servizio del sistema di smart metering 2g (pms2). <https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/open-meter/pms/PMS2-2dicembre2016.pdf>.
- [12] E-Distribuzione. Open meter - piano di messa in servizio del sistema di smart metering 2g (pms2) - edizione aggiornata. [https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/open-meter/pms/PMS2aggiornato\\_31-05-2017.pdf](https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/open-meter/pms/PMS2aggiornato_31-05-2017.pdf).
- [13] E-Distribuzione. Open meter - risposte ai quesiti pervenuti relativi al piano di messa in servizio del sistema di smart metering 2g. [https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/open-meter/pms/Risposta quesiti\\_PMS2.pdf](https://www.e-distribuzione.it/content/dam/e-distribuzione/documenti/open-meter/pms/Risposta quesiti_PMS2.pdf).
- [14] Edyna. I nostri numeri. <https://www.edyna.net/chi-siamo/dati-principali.html>.

- [15] Janaka B. Ekanayake. *Smart grid : technology and applications*. Wiley, Chichester, 2012.
- [16] Schneider Electric. Cos'è un home energy management system? <https://www.se.com/ww/en/home/inspirations/save.jsp>.
- [17] Enel-X. Energy management per aziende. <https://www.enelx.com/it/it/aziende/sostenibilita/consulenza-energetica/energy-management>.
- [18] Hitachi. Grid and generation management. <https://www.hitachienergy.com/products-and-solutions/grid-and-generation-management-network-manager>.
- [19] Filip Holik, Lars Halvdan Flå, Martin Gilje Jaatun, Sule Yildirim Yayilgan, and Jørn Foros. Threat modeling of a smart grid secondary substation. *Electronics*, 11(6), 2022.
- [20] SDI Automazione Industriale. Distribution management system - dms. [https://www.sdiautomazione.com/2022/assets/mktd\\_expertdms\\_it\\_22\\_02.pdf](https://www.sdiautomazione.com/2022/assets/mktd_expertdms_it_22_02.pdf).
- [21] SDI Automazione Industriale. expert scada. <https://sdiautomazione.com/product/expert-scada/>.
- [22] Inrete. I nostri numeri. <https://www.inretdistribuzione.it/chi-siamo-la-nostra-attivita-di-distribuzione>.
- [23] Investopedia. Operating expense (opex) definition and examples. [https://www.investopedia.com/terms/o/operating\\_expense.asp](https://www.investopedia.com/terms/o/operating_expense.asp).
- [24] Ireti. I nostri numeri. [https://www.ireti.it/servizi/distribuzione-energia-elettrica/sviluppo-reti.html?\\_gl=1\\*1iiyy8o\\*\\_up\\*MQ..\\*\\_ga\\*MzE50TYyMDA0LjE3NDk1NTg0MTM.\\*\\_ga\\_PQDCRB8YF0\\*cze3NDk1NTg0MTMkbzEkZzEkdDE3NDk1NTg0NTMkajIwJGwwJGgw](https://www.ireti.it/servizi/distribuzione-energia-elettrica/sviluppo-reti.html?_gl=1*1iiyy8o*_up*MQ..*_ga*MzE50TYyMDA0LjE3NDk1NTg0MTM.*_ga_PQDCRB8YF0*cze3NDk1NTg0MTMkbzEkZzEkdDE3NDk1NTg0NTMkajIwJGwwJGgw).
- [25] Ireti. I nostri numeri. <https://www.setdistribuzione.it/societa/chi-siamo.html>.
- [26] Ireti. Nuovi contatori 2g. <https://www.ireti.it/servizi/distribuzione-energia-elettrica/clienti-finali/nuovi-contatori-2g.html>.
- [27] Borsa Italiana. Capital expenditures. <https://www.borsaitaliana.it/borsa/glossario/capital-expenditures.html>.
- [28] CEI Comitato Elettrotecnico Italiano. Cei en 50160. <https://mycatalogo.ceinorme.it/cei/item/0000019447>.
- [29] CEI – Comitato Elettrotecnico Italiano. Regola tecnica di riferimento per la connessione di utenti attivi e passivi alle reti bt delle imprese distributrici di energia elettrica. <https://static.ceinorme.it/strumenti-online/doc/18309.pdf>.
- [30] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. Stride-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pages 1–6, 2017.
- [31] Azure Microsoft. What is cloud computing? <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing>.
- [32] NIST National Institute of Standard and Technology. Cia triad. <https://www.nist.gov/image/cia-triad>.
- [33] NIST National Institute of Standard and Technology. The nist definition of cloud computing. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
- [34] Enel – Ente Nazionale per l'Energia Elettrica. Smart grid: cosa sono, come funzionano, vantaggi. <https://www.enel.com/it/azienda/servizi-energetici/enel-grids/smart-grid>.

- [35] AgID Agenzia per l'Italia Digitale. Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design. [https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/linee\\_guida\\_modellazione\\_minacce\\_e\\_individuazione\\_azioni\\_di\\_mitigazionev1.0.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/linee_guida_modellazione_minacce_e_individuazione_azioni_di_mitigazionev1.0.pdf).
- [36] Adam Shostack. *Threat Modeling - Designing for security*. John Wiley and Sons, 2014.
- [37] SIEMENS. Phasor measurement unit (pmu). <https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/protection-relays-and-control/general-protection/phasor-measurement-unit-pmu.html>.
- [38] Husam Suleiman, Israa Alqassem, Ali Diabat, Edin Arnautovic, and Davor Svetinovic. Integrated smart grid systems security threat model. *Information Systems*, 53:147–160, 2015.
- [39] Terna. Accesso alla rete di trasmissione nazionale. [https://download.terna.it/terna/Capitolo%201\\_Nuova%20sezione%201C\\_8d787c66135589d.pdf](https://download.terna.it/terna/Capitolo%201_Nuova%20sezione%201C_8d787c66135589d.pdf).
- [40] Terna. Glossario dei termini. <https://download.terna.it/terna/0000/0107/42.pdf>.
- [41] Terna. Rapporto mensile sul sistema elettrico 2024. [https://download.terna.it/terna/Rapporto\\_Mensile\\_Dicembre\\_24\\_8dd358635ce3ac2.pdf](https://download.terna.it/terna/Rapporto_Mensile_Dicembre_24_8dd358635ce3ac2.pdf).
- [42] Terna. Sito pubblicazioni rapporti mensili del sistema elettrico nazionale. <https://www.terna.it/it/sistema-elettrico/pubblicazioni/rapporto-mensile>.
- [43] Tony Ucedavélez and Marco M. Morana. *RISK CENTRIC THREAT MODELING -Process for Attack Simulation and Threat Analysis*. John Wiley and Sons, first edition, 2015.
- [44] Uniareti. I nostri numeri. <https://www.unareti.it/it/servizi/elettricità/distribuzione-infrastrutture>.
- [45] V-reti. I nostri numeri. <https://www.v-reti.it/v-reti>.
- [46] GE Vernova. Ems (energy management system). <https://www.gevernova.com/power-conversion/product-solutions/EMS-Energy-Management-System>.
- [47] Wikipedia. Failover. <https://it.wikipedia.org/wiki/Failover>.

# Allegato A Glossario

Tabella A.1: Acronimi e Descrizione

<b>Acronimo</b>	<b>Acronimo Esteso</b>	<b>Descrizione</b>
<b>AAT</b>	Altissima Tensione	Tensione nominale di valore superiore a $220\text{ kV}$ .
<b>ARERA</b>	Autorità di Regolazione per Energia Reti e Ambiente	Autorità indipendente italiana che regola i servizi di pubblica utilità nei settori dell'energia elettrica, del gas e del ciclo idrico.
<b>AT</b>	Alta tensione	Tensione nominale di valore superiore a $35\text{ kV}$ e inferiore o uguale a $220\text{ kV}$ .
<b>BT</b>	Bassa Tensione	Tensione nominale di valore inferiore o uguale ad $1\text{ kV}$ .
<b>CP</b>	Cabina Primaria	Stazione elettrica con apparecchiature, organi di manovra e trasformazione AT/MT.
<b>DER</b>	Distributed Energy Resources	Risorse energetiche distribuite come pannelli solari, batterie e generatori localizzati vicino al punto di consumo.
<b>DFD</b>	Data Flow Diagram	Diagramma che rappresenta il flusso di dati attraverso un sistema, mostrando processi, archivi dati e flussi informativi.
<b>DR</b>	Demand Response	Programmi che permettono alla rete elettrica di richiedere automaticamente la riduzione dei consumi domestici durante i picchi di domanda, in cambio di incentivi economici. Il sistema di domotica riduce temporaneamente l'uso di elettrodomestici non essenziali per stabilizzare la rete.
<b>DSO</b>	Distribution System Operator	Gestore del sistema di distribuzione elettrica a media e bassa tensione, responsabile della consegna dell'energia elettrica agli utenti finali.
<b>FER</b>	Fonti di Energia Rinnovabili	Fonti rinnovabili tra cui: Idrico, Biomasse, Geotermico, Eolico e Fotovoltaico.
<b>HAN</b>	Home Area Network	Rete locale domestica che connette dispositivi intelligenti e sistemi di automazione all'interno di un'abitazione.
<b>MT</b>	Media Tensione	Tensione nominale di valore superiore a $1\text{ kV}$ e inferiore o uguale a $35\text{ kV}$ .
<b>NAN</b>	Neighborhood Area Network	Rete di comunicazione che collega più edifici o utenze in un'area geografica limitata.

<b>Acronimo</b>	<b>Acronimo Esteso</b>	<b>Descrizione</b>
<b>POD</b>	Point of Delivery	Identifica in modo certo il punto di prelievo, ovvero il punto fisico dove l'energia elettrica viene consegnata dal venditore e prelevata dal cliente finale. Non viene modificato se si cambia fornitore.
<b>RBAC</b>	Resource Base Access Control	Sistema di controllo degli accessi che assegna permessi agli utenti in base ai loro ruoli organizzativi.
<b>RF</b>	Radio Frequenza	Gamma di frequenze elettromagnetiche utilizzate per trasmissioni wireless, tipicamente da $3\text{ kHz}$ a $300\text{ GHz}$ .
<b>RTN</b>	Rete di Trasmissione Nazionale	Insieme delle infrastrutture che permettono la trasmissione dell'energia elettrica su tutto il territorio.
<b>TSO</b>	Transmission System Operator	Gestore del sistema di trasmissione elettrica ad alta tensione, responsabile del trasporto dell'energia e dell'equilibrio della rete. In Italia questo compito è stato assegnato a Terna.
<b>WAN</b>	Wide Area Network	Rete di telecomunicazioni che copre un'ampia area geografica, connettendo reti locali distanti tra loro.
<b>WORM</b>	Write-Once, Read-Many	Tecnologia di storage che permette la scrittura dei dati una sola volta ma consente letture multiple, garantendo integrità e immutabilità.



# Allegato B L'Architettura della Filiera Elettrica Italiana

## B.1 Dalla produzione alla distribuzione dell'energia elettrica

Il presente allegato fornisce un inquadramento dettagliato della filiera dell'energia elettrica in Italia, descrivendo l'architettura e i processi fondamentali dalla generazione fino all'utenza finale. Questa panoramica è propedeutica alla comprensione del contesto operativo in cui si inseriscono le minacce informatiche analizzate nel corpo della tesi.

La trattazione è articolata nelle seguenti sezioni:

1. **Produzione dell'Energia:** Si analizza il mix energetico nazionale, con un focus sul trend di crescita delle fonti rinnovabili nel periodo 2006-2024.
2. **Trasmissione e Dispacciamento:** Vengono descritte le responsabilità del *Transmission System Operator* (TSO) e i parametri tecnici fondamentali (frequenza, tensione) che governano la stabilità della rete.
3. **Distribuzione dell'Energia:** Si esamina l'architettura delle reti di Media e Bassa Tensione e il ruolo dei principali *Distribution System Operator* (DSO) sul territorio.
4. **Utenze Finali:** Si illustra l'evoluzione del ruolo dell'utente, da consumatore passivo a nodo attivo e interattivo della Smart Grid.

### B.1.1 Produzione dell'Energia: il Mix Energetico

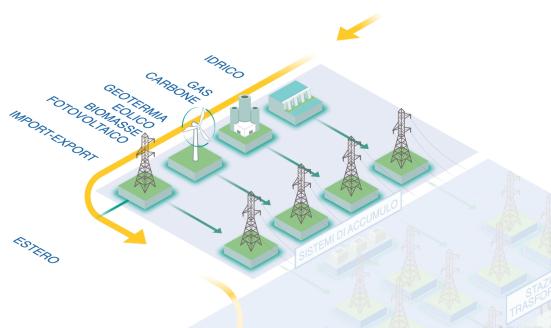


Figura B.1: Fonte immagine: Terna - Produzione

La generazione di energia elettrica, sia nei sistemi tradizionali che nelle Smart Grid, si fonda su un mix energetico che bilancia Fonti Energetiche non Rinnovabili (non-FER) e Fonti Energetiche Rinnovabili (FER), Tabella B.1. Questo equilibrio è un fattore chiave per la stabilità e la sostenibilità del sistema elettrico nazionale.

<b>Fonti primarie utilizzate</b>	<b>%</b>
Fonti rinnovabili	46
Gas naturale	43
Carbone	5
Altre fonti	5
Prodotti petroliferi	1

Tabella B.1: Composizione del mix iniziale nazionale immessa nel anno 2023 [6]

Analizzando il contesto italiano, i dati più recenti del "Rapporto Mensile sul Sistema Elettrico" di Terna per il periodo Gennaio-Dicembre 2024 [41] offrono un quadro preciso della situazione. A fronte di un assorbimento totale di energia elettrica di  $312\text{ TWh}$ , la produzione nazionale netta si è attestata a  $261\text{ TWh}$ . La composizione di tale produzione evidenzia un contributo quasi paritetico tra fonti rinnovabili e non rinnovabili. In particolare,  $132\text{ TWh}$  (51%) della produzione è derivato da fonti non-FER, mentre  $129\text{ TWh}$  (49%) è stato generato da FER, a testimonianza del progresso della transizione energetica. Il fabbisogno è stato infine completato da un saldo netto di importazioni dall'estero per  $51\text{ TWh}$ , principalmente da Francia e Svizzera.

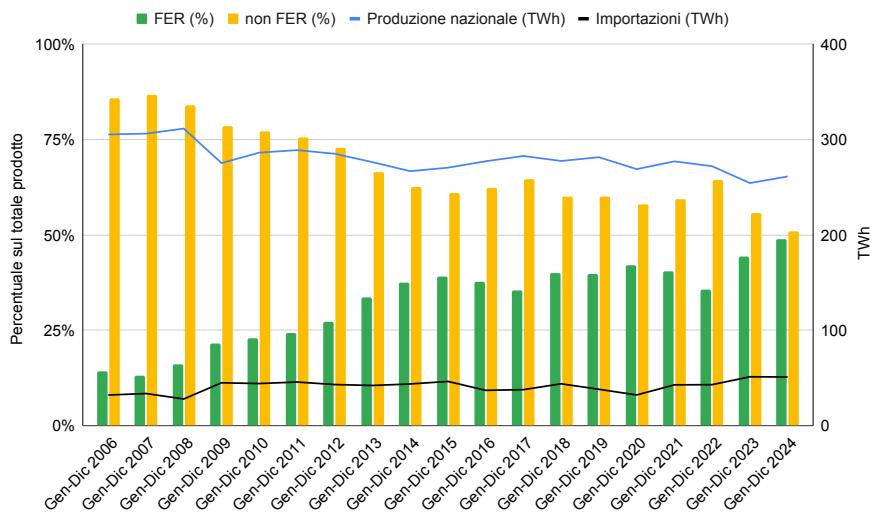


Figura B.2: Produzione nazionale annuale suddivisa tra FER e non FER [42]

La crescente rilevanza delle fonti rinnovabili non è un fenomeno recente, ma il risultato di un trend consolidato. Come evidenziato nella Figura B.2, il periodo dal 2006 al 2024 ha visto un incremento costante e significativo della produzione da FER, fino a raggiungere quasi un punto di pareggio con le fonti convenzionali nell'ultimo anno di rilevazione. L'analisi disaggregata di questa crescita, Figura B.3, rivela che i principali motori di questa trasformazione sono stati l'espansione del settore fotovoltaico, a partire dal 2009, e lo sviluppo continuo e progressivo dell'energia eolica.

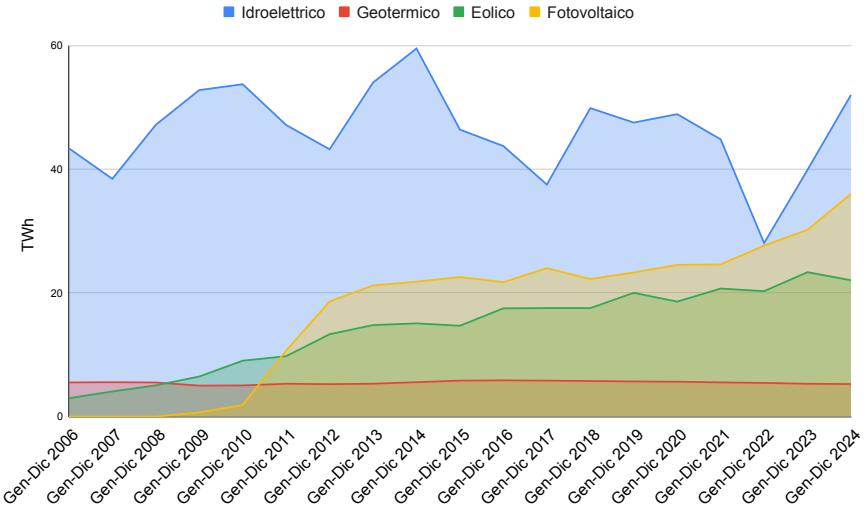


Figura B.3: Suddivisione delle principali FER in Italia [42]

### B.1.2 La Trasmissione e il Dispacciamento dell'Energia

La fase di trasmissione costituisce il sistema nervoso della rete elettrica, incaricata di trasportare l'energia su lunghe distanze, dalle centrali di produzione alle reti di distribuzione. In Italia, questa infrastruttura strategica, nota come Rete di Trasmissione Nazionale (RTN), è gestita in regime di monopolio naturale da Terna, che opera in qualità di *Transmission System Operator* (TSO). Tale modello di governance, diffuso in gran parte d'Europa, è considerato ottimale per garantire l'efficienza, la sicurezza e lo sviluppo coordinato dell'intera infrastruttura elettrica nazionale.

#### Funzioni del TSO: Il Dispacciamento

Il ruolo di Terna non si limita alla manutenzione fisica della rete, ma include la complessa attività di dispacciamento: la gestione e il controllo in tempo reale dei flussi energetici per assicurare costantemente l'equilibrio tra energia prodotta e consumata.

Le principali responsabilità del dispacciamento includono:

- il **monitoraggio** continuo dei flussi di potenza e la loro deviazione per soddisfare i picchi di assorbimento regionali;
- l'attuazione di **procedure operative** per il controllo coordinato di tutti gli elementi del sistema (centrali, linee, stazioni);
- la **pianificazione** delle manutenzioni, dell'allacciamento di nuove linee e della gestione delle indisponibilità programmate o accidentali di porzioni della rete;

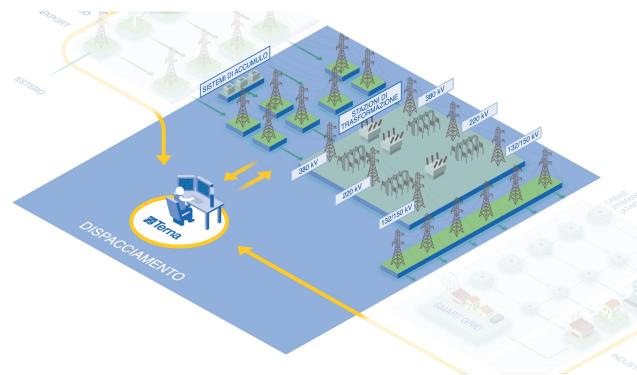


Figura B.4: Fonte immagine: Terna - Trasmissione

- la **previsione** del fabbisogno energetico nazionale con un dettaglio orario, fondamentale per la programmazione della produzione.

### Parametri Tecnici della Rete di Trasmissione

Per garantire la stabilità e la qualità della fornitura, l'energia elettrica in corrente alternata deve rispettare parametri tecnici rigorosi in ogni punto della rete europea. I due principali indicatori sono la frequenza e la tensione.

- **Frequenza:** La frequenza nominale ( $f_n$ ) del sistema è fissata a  $50\text{ Hz}$ . Deviazioni da questo valore indicano uno squilibrio tra produzione e consumo. In condizioni operative normali, la rete è progettata per funzionare a tempo indeterminato entro un intervallo di tolleranza compreso tra  $47,5\text{ Hz}$  e  $51,5\text{ Hz}$ , con limiti eccezionali di breve durata fuori dalle precedenti soglie [39] [28].
- **Tensione:** A livello di utenza finale, la tensione nominale ( $U_n$ ) è di  $230\text{ V}$  per le forniture monofase e  $400\text{ V}$  per quelle trifase, con una tolleranza ammessa di  $\pm 10\%^1$  [29]. Tuttavia, per minimizzare le perdite di energia per effetto Joule ( $P = R \cdot I^2$ ) durante il trasporto su lunghe distanze, la trasmissione avviene a livelli di tensione molto più elevati. La RTN, infatti, opera prevalentemente in Alta Tensione (AT), tra  $35\text{ kV}$  e  $220\text{ kV}$ , e in Altissima Tensione (AAT), oltre i  $220\text{ kV}$  [40].

### B.1.3 La Distribuzione dell'Energia

La fase di distribuzione rappresenta il segmento finale della filiera elettrica, con il compito di prelevare l'energia dalla Rete di Trasmissione Nazionale (RTN) e consegnarla capillarmente agli utenti finali. A differenza della trasmissione, gestita da un singolo operatore nazionale, Terna, il servizio di distribuzione in Italia è frammentato e liberalizzato, operato su base territoriale da diversi *Distribution System Operator* (DSO).

Attualmente, sul territorio nazionale operano circa 114 aziende di distribuzione [3]. Sebbene il numero sia elevato, il mercato è fortemente concentrato. I principali DSO, che servono collettivamente la quasi totalità della popolazione italiana, sono elencati in Tabella B.2, la quale riporta per ciascuno il gruppo di appartenenza, il numero di utenti e l'area geografica di competenza. Tra questi, spicca E-Distribuzione, società del gruppo Enel, che da sola gestisce oltre 31 milioni di utenze [9].

### Architettura della Rete di Distribuzione

Il DSO è responsabile del trasporto, della trasformazione e della consegna dell'energia elettrica su reti in Media Tensione (MT), con tensioni tipicamente comprese tra  $1\text{ kV}$  e  $35\text{ kV}$ , e in Bassa Tensione (BT), con tensioni inferiori a  $1\text{ kV}$ .

---

<sup>1</sup>Monofase: da  $207\text{ V}$  a  $253\text{ V}$  e Trifase: da  $360\text{ V}$  a  $440\text{ V}$



Figura B.5: Fonte immagine: Terna - Distribuzione

DSO	Gruppo di Appartenenza	Utenti Serviti in mln.	Principali	Fonti
			aree geografiche	
E-Distribuzione	Enel	31,1	Tutto il territorio nazionale	[9]
Areti	Acea	2,8	Roma e Formello	[4]
Unareti	A2A	1,2	Brescia, Milano e Bergamo	[44]
Ireti	Iren	0,7	Parma, Torino e Vercelli	[24]
Set Distribuzione	Dolomiti Energia	0,3	Provincia autonoma di Trento	[25]
V-reti	AGSM AIM	0,3	Verona e Vicenza	[45]
InRete	Hera	0,3	Emilia-Romagna e Toscana	[22]
Edyna	Alperia	0,2	Alto Adige	[14]

Tabella B.2: Principali Distributori di Energia Elettrica in Italia

Il processo di trasformazione della tensione avviene in più passaggi:

1. Nelle Cabine Primarie, l'energia viene prelevata dalla rete di trasmissione in Alta Tensione (AT) e trasformata a un livello di Media Tensione (es. 15 kV o 20 kV). Queste cabine fungono da nodo di interconnessione tra la rete del TSO e quella del DSO.
2. L'energia in Media Tensione viene quindi distribuita attraverso una rete di cavi (spesso interrati nei centri urbani) fino a raggiungere le Cabine Secondarie.
3. All'interno delle Cabine Secondarie, un ulteriore trasformatore abbassa la tensione da Media a Bassa Tensione, portandola ai valori standard per l'utenza finale: 400 V per le forniture trifase e 230 V per quelle monofase.

#### B.1.4 Le Utenze Finali: da Consumatori Passivi a Nodi Attivi della Rete

Nell'architettura della Smart Grid, il ruolo dell'utente finale subisce una profonda trasformazione, evolvendo da semplice consumatore passivo a nodo attivo e interattivo dell'ecosistema energetico. Se nel mercato tradizionale la scelta si limita alla selezione di un venditore di energia – un processo oggi facilitato da strumenti istituzionali come "Il portale delle offerte"<sup>2</sup> di ARERA – nella Smart Grid l'utente diventa un partecipante dinamico grazie a nuove tecnologie e funzionalità.

Questa evoluzione è abilitata principalmente da due fattori:

1. **Le Infrastrutture di Misurazione Avanzata (AMI)**: attraverso i contatori intelligenti (*Smart Meter*), i DSO possono non solo raccogliere i dati di consumo in tempo reale, ma anche inviare segnali di prezzo o comandi di gestione all'utente, creando un canale di comunicazione bidirezionale.
2. **L'Emergere del "Prosumer"**: come anticipato nella Sezione 1.1, gli utenti dotati di impianti di generazione distribuita (es. fotovoltaico) possono produrre e immettere energia in rete, invertendo il flusso tradizionale di potenza e interagendo attivamente con il sistema.

Inoltre, l'utente può ottimizzare i propri consumi attraverso sistemi di gestione dei carichi (*Demand Response*) e dispositivi di automazione domestica come gli *Home Energy Management Systems* (HEMS).

Questa crescente digitalizzazione e interconnessione del dominio utente, se da un lato promette maggiore efficienza e sostenibilità, dall'altro introduce nuove superfici di attacco e significative sfide di

<sup>2</sup><https://www.ilportaleofferte.it/portaleOfferte/>

sicurezza informatica. La compromissione di *Smart Meter*, HEMS o altri dispositivi connessi potrebbe infatti avere ripercussioni non solo sul singolo utente, ma sulla stabilità dell'intera rete di distribuzione.

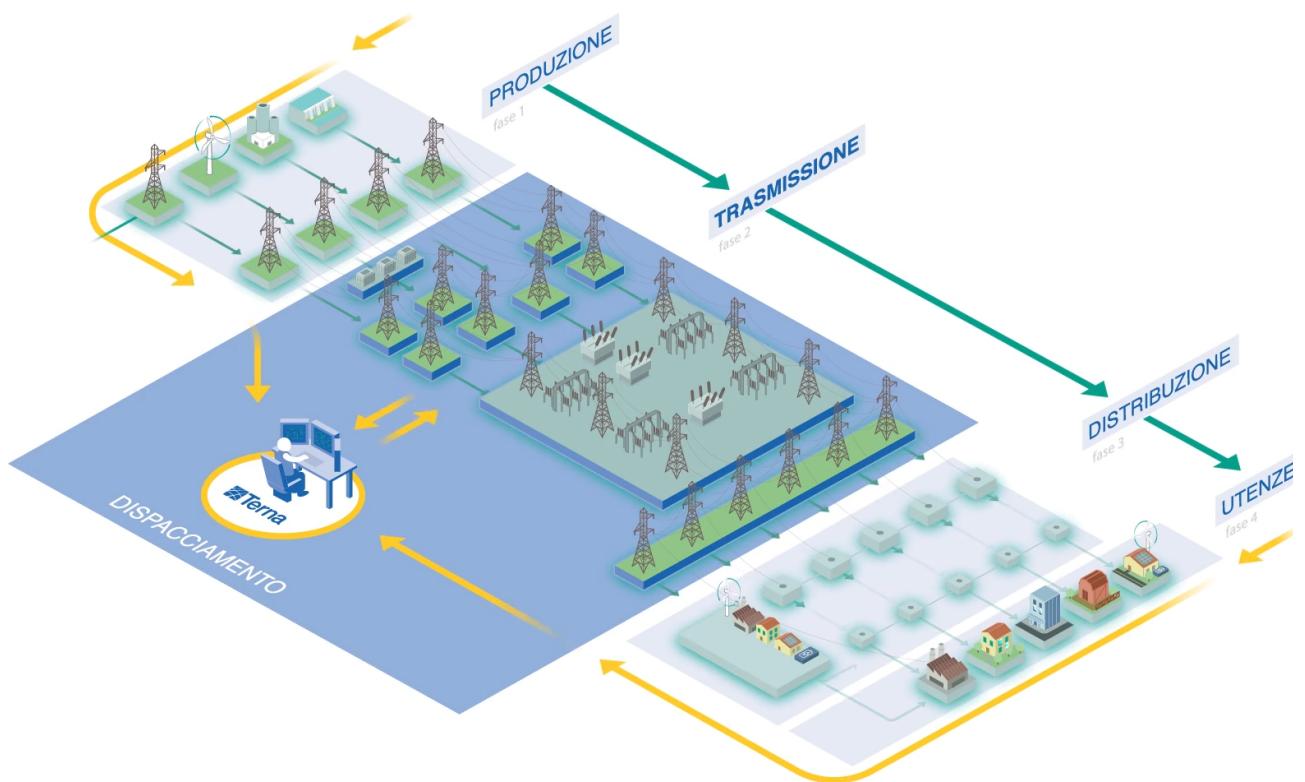


Figura B.6: Fonte immagine: Terna - Sistema Elettrico

# Allegato C Il paradigma tecnologico del Cloud Computing e i suoi principali vantaggi

## C.1 Introduzione al Cloud Computing

Negli ultimi due decenni, il *Cloud Computing* si è affermato come il paradigma dominante per l'erogazione di servizi informatici, una transizione accelerata dalla maturità di piattaforme leader come Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

Formalmente, il *National Institute of Standards and Technology* (NIST) definisce il *Cloud Computing* come "un modello per abilitare un accesso di rete *on-demand*, conveniente e ubiquo a un pool condiviso di risorse di calcolo configurabili (es. reti, server, storage, applicazioni e servizi) che possono essere rapidamente approvvigionate e rilasciate con un minimo sforzo di gestione o interazione con il fornitore di servizi" [33]

In termini più semplici, il *Cloud Computing* permette a organizzazioni e individui di accedere a risorse IT via Internet ("il *Cloud*"), astraendo la complessità della gestione fisica e logica dell'infrastruttura sottostante. L'analogia più calzante, particolarmente pertinente per questa tesi, è quella con la rete elettrica pubblica: un'azienda non ha bisogno di costruire e mantenere la propria centrale elettrica privata per alimentare le proprie attività. Al contrario, si connette alla rete nazionale e paga solo per l'energia effettivamente consumata (modello *pay-per-use*).

allo stesso modo, il *Cloud Computing* consente di delegare a un fornitore specializzato la gestione, la manutenzione, la sicurezza e la scalabilità dell'infrastruttura IT, trasformando un ingente costo fisso iniziale (CAPEX)<sup>1</sup> in un costo operativo variabile (OPEX)<sup>2</sup>, proporzionale all'utilizzo effettivo delle risorse.

### C.1.1 Modelli di Deployment del Cloud Computing

La scelta di un'architettura *cloud* dipende dalle specifiche esigenze di un'organizzazione in termini di sicurezza, controllo, scalabilità e costi. Secondo la classificazione del NIST [33], esistono quattro principali modelli di *deployment* (o implementazione) del *cloud*.

#### Public Cloud

L'infrastruttura *cloud* è di proprietà di un fornitore terzo (*Cloud Service Provider* - CSP), come AWS, Microsoft Azure o GCP, che la rende disponibile al pubblico generale via Internet. In questo modello, le risorse (calcolo, *storage*, rete) sono condivise tra più clienti (*multi-tenancy*), sebbene logicamente isolate. Il cliente non ha alcuna visibilità o controllo sull'infrastruttura fisica, ma beneficia di un'enorme scalabilità, di un modello di costo *pay-per-use* e della delega totale della gestione hardware al provider.

<sup>1</sup>*Capital Expenditure*: rappresentano flussi di cassa in uscita per la realizzazione di investimenti in attività immobilizzate di natura operativa. [27]

<sup>2</sup>*Operating Expenses*: è un costo che un'azienda sostiene attraverso le sue normali attività, incluse spese come l'affitto che sono tipicamente deducibili dalle tasse. [23]

## Private Cloud

L'infrastruttura *cloud* è utilizzata in modo esclusivo da una singola organizzazione. Può essere di proprietà, gestita e operata dall'organizzazione stessa (*on-premises*) oppure da una terza parte, e può essere ospitata sia internamente che esternamente. Il vantaggio principale del *Private Cloud* è il maggiore controllo sulla sicurezza, sulla governance dei dati e sulla personalizzazione dell'infrastruttura, pur mantenendo i benefici tipici del *cloud* come l'automazione e l'elasticità delle risorse.

## Hybrid Cloud

Questo modello combina due o più infrastrutture *cloud* distinte (*private*, *community* o *public*) che rimangono entità uniche ma sono legate insieme da tecnologie standardizzate che permettono la portabilità di dati e applicazioni (es. *"cloud bursting"* per la gestione dei picchi di carico). Un'organizzazione potrebbe, ad esempio, mantenere i dati sensibili su un *Private Cloud* e utilizzare un *Public Cloud* per le applicazioni meno critiche o per gestire carichi di lavoro variabili, ottenendo un equilibrio tra controllo e flessibilità.

## Community Cloud

L'infrastruttura *cloud* è condivisa da diverse organizzazioni che hanno interessi comuni (es. requisiti di sicurezza, policy, conformità normativa). Può essere gestita dalle organizzazioni stesse o da una terza parte. Un esempio potrebbe essere un *cloud* condiviso da diverse agenzie governative o da aziende dello stesso settore industriale (es. finanziario, sanitario o energetico) per ridurre i costi pur mantenendo standard di sicurezza elevati.

### C.1.2 Tecnologie Abilitanti per le Architetture Cloud-Native

La transizione verso il *Cloud Computing* non riguarda solo dove le applicazioni vengono eseguite, ma anche come vengono progettate, "impacchettate" e gestite. Le architetture *Cloud-Native* si basano su un insieme di tecnologie che consentono di costruire sistemi resilienti, scalabili e flessibili. Di seguito viene presentata la traiettoria evolutiva di queste tecnologie, che saranno richiamate nell'analisi dell'architettura Smart Grid proposta.

#### 1. Virtualizzazione tramite Virtual Machine (VM)

La virtualizzazione tradizionale, basata su *Virtual Machine* (VM), è stato il primo passo per astrarre l'hardware fisico. Una VM emula un intero computer, includendo un sistema operativo ospite (*Guest OS*) completo, che viene eseguito sopra un *hypervisor*. Questo approccio, noto come *Infrastructure as a Service* (IaaS), offre un eccellente isolamento e permette di migrare applicazioni *legacy* (*"lift-and-shift"*) nel *cloud* con poche o nessuna modifica. Tuttavia, ogni VM comporta un significativo *overhead* di risorse, poiché deve caricare un intero sistema operativo, risultando in tempi di avvio più lenti e una minore densità di applicazioni per host fisico.

#### 2. Containerizzazione

La containerizzazione rappresenta un passo evolutivo verso una maggiore efficienza e portabilità. A differenza delle VM, un container non emula l'hardware, ma virtualizza il sistema operativo. Tutti i container in esecuzione su un *host* condividono lo stesso kernel del sistema operativo ospitante (*Host OS*), "impacchettando" solo l'applicazione e le sue dipendenze (library, file di configurazione). Tecnologie come Docker e containerd hanno reso questo approccio popolare. I vantaggi sono notevoli:

- **Efficienza:** Avendo un *overhead* minimo, i container sono leggeri, si avviano in pochi secondi e consentono una maggiore densità di *deployment*.
- **Portabilità:** Un container funziona in modo identico su qualsiasi ambiente che supporti un *container runtime*, dal laptop dello sviluppatore al *cloud* pubblico.

- **Abilitazione dei Microservizi:** La leggerezza e l'isolamento dei container li rendono la tecnologia ideale per implementare architetture a microservizi, dove un'applicazione complessa viene scomposta in piccoli servizi indipendenti e autonomi.

### 3. Orchestrazione di Container con Kubernetes

Se i container risolvono il problema di come impacchettare e distribuire un'applicazione, l'orchestrazione risolve il problema di come gestirne centinaia o migliaia in un ambiente di produzione. Kubernetes (K8s) è diventata la piattaforma di orchestrazione *de facto*. Essa automatizza il ciclo di vita delle applicazioni containerizzate, gestendo compiti complessi come:

- **Deployment e Scaling:** Distribuisce i container sui nodi di un cluster e ne scala automaticamente il numero in base al carico.
- **Service Discovery e Load Balancing:** Espone i container come servizi di rete e distribuisce il traffico tra di essi.
- **Self-healing:** Riavvia automaticamente i container che si bloccano, li sostituisce e gestisce i *failover*<sup>3</sup>.

Kubernetes è il pilastro delle moderne applicazioni *Cloud-Native*, fornendo l'automazione e la resilienza necessarie per operare sistemi distribuiti su larga scala.

#### C.1.3 Principali Vantaggi del Cloud Computing

L'adozione del *Cloud Computing* offre vantaggi strategici che ne hanno guidato la rapida diffusione. I principali possono essere riassunti come segue [31]:

- **Efficienza Economica:** Sostituisce i grandi investimenti iniziali in hardware (CAPEX) con costi operativi variabili (OPEX), basati su un modello a consumo (*pay-as-you-go*). Questo, unito alle economie di scala dei provider, riduce significativamente i costi totali dell'IT.
- **Agilità e Scalabilità:** Le risorse possono essere approvvigionate in pochi minuti e scalate automaticamente (elasticità) per rispondere in tempo reale alle fluttuazioni del carico di lavoro. Ciò accelera l'innovazione e garantisce prestazioni ottimali.
- **Affidabilità e Sicurezza:** I provider cloud offrono infrastrutture globali con elevati livelli di ridondanza, garantendo alta affidabilità e semplificando le strategie di *Disaster Recovery*. Inoltre, investono in misure di sicurezza avanzate che superano le capacità della maggior parte delle singole organizzazioni.

In sintesi, il cloud permette alle aziende di delegare la complessità della gestione infrastrutturale per concentrarsi sul proprio core business, beneficiando di un'infrastruttura più efficiente, scalabile e sicura.

---

<sup>3</sup>si intende la tecnica che prevede in caso di guasto o interruzione anomala nel funzionamento di un server, un componente hardware o una rete, la commutazione automatica a una struttura analoga ridondante o in *standby* [47]





