

---

# Smart Grid

***Marco Amoruso, Daniele Anello, Francesco Farina,  
Iolanda Rinaldi***

*Università degli Studi di Salerno*

---

Last edit: 9 dicembre 2015

# Indice

<b>Indice</b>	<b>1</b>	
<b>1</b>	<b>Introduzione</b>	<b>4</b>
<b>2</b>	<b>Smart Grid: panorama attuale e definizione</b>	<b>6</b>
2.1	Panorama energetico attuale . . . . .	6
2.2	Cenni storici . . . . .	7
2.3	Perché la Smart Grid? . . . . .	10
2.4	Cos'è la Smart Grid? . . . . .	13
2.5	Requisiti di una Smart Grid . . . . .	14
2.6	Tecnologie coinvolte . . . . .	17
<b>3</b>	<b>Architettura</b>	<b>19</b>
3.1	Smart Grid Framework . . . . .	20
3.1.1	Wide-area network . . . . .	22
3.1.2	Field-area network . . . . .	22
3.1.3	Home-area network . . . . .	23
3.2	Generazione di energia rinnovabile . . . . .	23
3.3	Smart meter e Advanced Metering Infrastructure . . . . .	24
3.4	Conservazione dell'energia . . . . .	26
3.5	Veicoli elettrici . . . . .	27
3.6	Microgrid . . . . .	28
3.7	Smart substation . . . . .	29
3.7.1	IED . . . . .	31
3.7.2	Sensori . . . . .	31
3.7.3	SCADA . . . . .	32
3.8	Sistemi di trasmissione . . . . .	40
3.9	Sistemi di distribuzione . . . . .	42
3.9.1	Distribution Management System . . . . .	43

<b>4 Smart Grid Cybersecurity</b>	<b>46</b>
4.1 Un caso esemplare di attacco: Stuxnet . . . . .	47
4.2 Definire la sicurezza . . . . .	50
4.2.1 Confidentiality . . . . .	50
4.2.2 Integrity . . . . .	51
4.2.3 Availability . . . . .	52
4.2.4 Control . . . . .	52
4.2.5 Authenticity . . . . .	52
4.2.6 Usability . . . . .	53
4.2.7 Analisi dei rischi . . . . .	53
4.3 Building blocks . . . . .	53
4.3.1 Layered Security Model . . . . .	54
4.3.2 Authentication . . . . .	55
4.3.3 Authorization . . . . .	55
4.3.4 Auditing . . . . .	56
4.3.5 Key Management . . . . .	56
4.3.6 Message Integrity . . . . .	56
4.3.7 Network Integrity . . . . .	57
4.3.8 System Integrity . . . . .	57
4.4 Threats and Impacts . . . . .	58
4.4.1 Consumers threats . . . . .	58
4.4.2 Utility companies threats . . . . .	61
<b>5 Standard e tecnologie</b>	<b>67</b>
5.1 Tecnologie di comunicazione . . . . .	68
5.1.1 IEEE 802 . . . . .	68
5.1.2 Power line . . . . .	76
5.2 Standard per lo scambio di informazioni . . . . .	78
5.2.1 Standard per Smart Meter . . . . .	78
5.2.2 Modbus . . . . .	79
5.2.3 ISO/IEC 61850 . . . . .	79
5.3 Standard per la sicurezza . . . . .	87
5.3.1 ISO/IEC 62351 . . . . .	87
<b>6 Principali vulnerabilità delle Smart Grid: attacchi e contro-misure</b>	<b>90</b>
6.1 Open Smart Grid Protocol . . . . .	91
6.1.1 Setup . . . . .	92
6.1.2 Communication with authenticated encryption . . . . .	92
6.1.3 Analisi . . . . .	99

6.2	Attacking Smart Meters and Smart Devices . . . . .	102
6.2.1	Open Source Security Testing Methodology Manual .	102
6.3	False Data Injection . . . . .	110
6.3.1	Stima dello stato e Bad Data Injection . . . . .	111
6.3.2	Bad Data Detection . . . . .	113
6.3.3	Stealth Bad Data Injection . . . . .	114
6.3.4	Meccanismo Difensivo . . . . .	114
6.3.5	Strategia di attacco . . . . .	116
6.4	Disconnect Attack . . . . .	118
6.4.1	Modellare attacchi di Remote Disconnect su AMI . .	118
6.4.2	Contromisura Delayed Disconnect . . . . .	120
6.4.3	Impatto del delay sui tempi di operazioni RCD . .	121
6.4.4	Progettazione delle contromisure di delay . . . . .	123
6.5	Jamming . . . . .	127
6.5.1	Strategia di attacco . . . . .	128
6.5.2	Contromisure . . . . .	128

**Bibliografia** **129**

# **Capitolo 1**

## **Introduzione**

L'infrastruttura elettrica attuale, non subisce modifiche da circa un centinaio d'anni: le componenti della rete, organizzate in una struttura gerarchica, sono vicine alla fine della loro vita.

Mentre la rete invecchia sempre più, la richiesta di energia elettrica aumenta gradualmente e l'attuale organizzazione è troppo complessa e poco adatta per soddisfare i bisogni del 21-esimo secolo.

Tra le mancanze dell'infrastruttura corrente vi sono: mancanza di analisi automatizzate, tempi di risposta lenti, mancanza di consapevolezza della situazione, ecc. A tali fattori, si uniscono anche l'aumento della popolazione sul pianeta e la conseguente richiesta di energia, il cambiamento del clima globale, i fallimenti delle apparecchiature che costituiscono la rete, i problemi di conservazione dell'energia, capacità limitata della generazione di energia, comunicazione unidirezionale, diminuzione di combustibili fossili e scarse capacità di recupero in caso di guasti.

È facile capire, analizzando tutti questi fattori, che vi è un bisogno urgente di una nuova infrastruttura elettrica in grado di risolvere tutti questi problemi.

L'attuale rivoluzione dei sistemi di comunicazione, particolarmente stimolata anche dalla crescita di Internet, offre la possibilità di migliorare il monitoraggio e, in generale, le funzionalità dei sistemi energetici e di rendere, quindi, le operazioni più efficaci e flessibili ma, allo stesso tempo, meno costose.

La **Smart Grid** è l'opportunità per utilizzare le novità introdotte dall'ICT (*Information and Communication Technology*) al fine di rivoluzionare il sistema energetico. Tuttavia, a causa delle grandi dimensioni sia del sistema che dell'entità degli investimenti che sono stati fatti nel corso degli anni, qualsiasi cambiamento significativo sarà costoso e richiederà un'attenta giustificazione.

La Smart Grid è una rete elettrica moderna che offre migliore efficienza, affidabilità e sicurezza, permettendo anche una facile integrazione di nuove fonti di energia rinnovabile. In confronto ai sistemi precedenti, la Smart Grid è concepita per integrare pienamente, all'interno di milioni di dispositivi, tecnologie che permettano comunicazioni veloci e bidirezionali e che permettano di formare un'infrastruttura dinamica ed interattiva con nuove e migliori capacità di gestione dell'energia. Tuttavia, una dipendenza così forte dal *networking* di informazioni, inevitabilmente sottopone la Smart Grid ad una serie di potenziali vulnerabilità associate ai sistemi di comunicazione e di rete. Ciò, in pratica, aumenta il rischio di compromettere l'affidabilità e la sicurezza delle operazioni dell'infrastruttura che costituiscono gli obiettivi principali della Smart Grid. Per esempio, una potenziale intrusione nella rete da parte di un individuo non autorizzato, potrebbe portare ad una serie di conseguenze negative che vanno dall'*information leakage* alla generazione di fallimenti in cascata, come ad esempio un blackout totale e la distruzione dell'intero sistema. Pertanto, lo scopo di questa survey è analizzare i problemi legati alla **sicurezza** della Smart Grid, che è critica nella progettazione delle reti di comunicazione ed è considerata una delle più alte priorità nello sviluppo della rete elettrica moderna.

La survey è strutturata nel seguente modo:

- Capitolo 2, *Smart Grid: panorama attuale e definizione*, in cui si introducono i concetti base relativi alla Smart Grid (definizione, requisiti, tecnologie), insieme al contesto attuale e alle motivazioni che hanno portato all'evoluzione della corrente infrastruttura elettrica;
- Capitolo 3, *Architettura*, in cui vengono descritti i principali sistemi, dispositivi e componenti che costituiscono la Smart Grid;
- Capitolo 4, *Smart Grid Cybersecurity*, in cui si descrivono i requisiti che una Smart Grid deve soddisfare dal punto di vista della sicurezza, gli strumenti che permettono di realizzare ciò, e le minacce che può subire;
- Capitolo 5, *Standard e tecnologie*, in cui si descrivono gli standard e le tecnologie utilizzate attualmente all'interno della Smart Grid, in particolare per la comunicazione e la sicurezza;
- Capitolo 6, *Principali vulnerabilità delle Smart Grid: attacchi e contromisure*, in cui si analizzano in dettaglio le vulnerabilità della Smart Grid e gli attacchi a cui essa può essere sottoposta.

## Capitolo 2

# Smart Grid: panorama attuale e definizione

### 2.1 Panorama energetico attuale

La rete elettrica attuale è il risultato di una rapida urbanizzazione e di un rapido sviluppo di infrastrutture in varie zone del mondo. Sebbene tali reti esistano ormai in molte aree geografiche diverse, le aziende generalmente tendono ad adottare tecnologie molto simili tra di loro. Ciononostante, restano altri fattori di varia natura (economica, politica, geografica) legati allo sviluppo energetico che si diversificano a seconda dell'azienda.

In generale però, pur tenendo in considerazione le differenze portate da tali fattori, la topologia base della rete elettrica attuale è rimasta immutata.

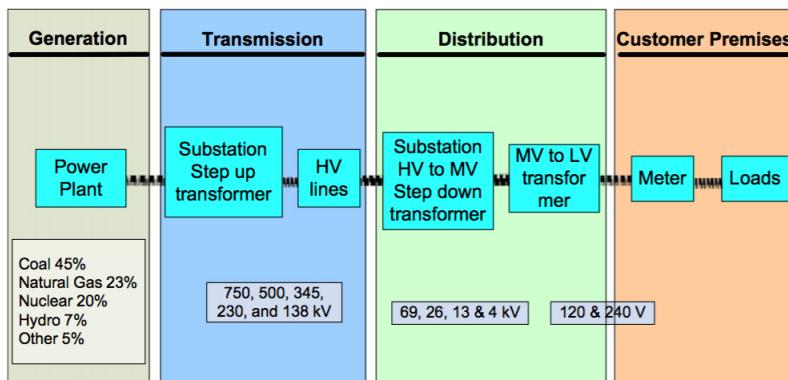


Figura 2.1: La rete elettrica attuale

La struttura della rete attuale è una struttura strettamente gerarchica. La figura 2.1 mostra l'esistenza di tre sottosistemi distinti: generazione, trasmissione e distribuzione [4].

Le centrali elettriche sono composte da generatori elettromeccanici i quali, durante la fase di **generazione**, spinti dal flusso dell'acqua corrente o da motori termici alimentati da combustioni chimiche, generano energia. Tale energia viene successivamente inviata ai trasformatori del livello di **trasmissione**, i quali la convertiranno in energia ad alto voltaggio per permetterne la diffusione a lunga distanza. Dopo tale step, si passa alla **distribuzione**, in cui si applica prima una trasformazione a medio e basso voltaggio e, in seguito, si procede all'erogazione agli utenti finali.

Tale sistema è basato sostanzialmente su una comunicazione *unidirezionale* in cui la sorgente non ha nessuna informazione real-time circa le necessità degli ultimi punti della catena. Pertanto si tende a sovraccaricare la rete, facendole raggiungere a priori i picchi massimi di carico; poiché è raro che le richieste degli utenti raggiungano tali valori, questo approccio porta a rendere la rete elettrica un meccanismo inefficiente.

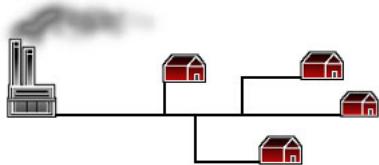
Inoltre, le reti elettriche attuali sono interconnesse tra loro a formare reti regionali o nazionali con lo scopo di fornire rotte ridondanti e alternative per il flusso della corrente in caso di problemi.

La distribuzione dell'energia è gestita da un *controllore centralizzato* che ha il compito di amministrare diverse regioni da un'unica posizione centrale.

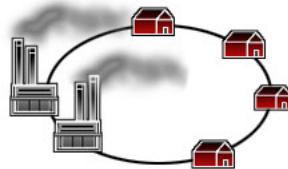
## 2.2 Cenni storici

Le tecnologie relative alle reti elettriche hanno radici che risalgono alla fine del XIX secolo: la *corrente continua* di Thomas Edison e la *corrente alternata* di Nikola Tesla continuano ad essere utilizzate tutt'ora. Oggi, infatti, l'energia viene trasmessa utilizzando la corrente alternata, mentre quella continua ha applicazioni specifiche, solitamente all'interno di plessi residenziali e commerciali.

In accordo a [1], le principali topologie di rete elettrica attualmente in uso sono: **radial grid**, **mesh grid**, e **looped topology**. La radial grid (Figura 2.2) è la più economica da costruire ed è ampiamente utilizzata in zone scarsamente popolate. Questa topologia prevede che per un gruppo di utenti ci sia solo una fonte di energia; pertanto un fallimento, un corto-circuito o un abbattimento della linea elettrica interromperebbero l'erogazione di tutto il sistema che deve essere riparato prima di ristabilire la corrente.



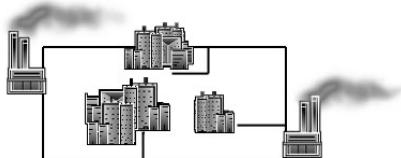
**Figura 2.2:** Radial grid



**Figura 2.3:** Looped topology

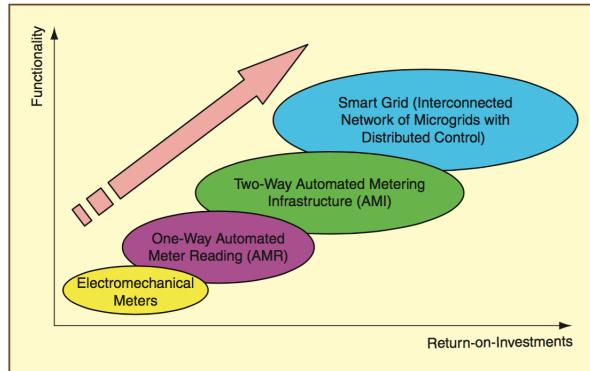
La looped topology (Figura 2.3), come suggerisce il nome, prevede che ci sia un ciclo che attraversi tutta l'area in cui si eroga il servizio fino a ritornare al punto d'origine. Tale *loop* è solitamente connesso ad una sorgente alternativa di energia: posizionando degli switch nelle giuste locazioni, si può fornire corrente all'utente da entrambe le direzioni. Se una sorgente presenta dei guasti, si attivano gli switch (manualmente o automaticamente) e la corrente può arrivare ai consumatori dall'altra fonte.

La looped topology fornisce una continuità del servizio migliore rispetto alla radial grid, poiché ci sono solo brevi interruzioni dovute allo switching. In caso di fallimenti causati da guasti sulle linee, la compagnia che si occupa di erogare il servizio deve solo trovare il punto in cui si è verificato il guasto e ripristinare il servizio; anche la riparazione stessa può essere effettuata riducendo al minimo le interruzioni ai clienti. La looped topology è, però, più costosa della radial grid perché sono richiesti una serie di switch e di conduttori, ma il sistema migliore che ne viene fuori vale la spesa.



**Figura 2.4:** Mesh grid

Vi è poi la terza topologia, la mesh grid (Figura 2.4), che è la più complicata e consiste di looped topology collegate. Un dato cliente può essere, pertanto, servito da due, tre, quattro o più fonti diverse; il grande vantaggio di tale topologia è, quindi, un'affidabilità ulteriore che, però, rende la mesh grid la più costosa tra le tre. Per tale ragione, questa topologia è utilizzata solo in aree altamente congestionate, con alta densità di popolazione o in centri cittadini.



**Figura 2.5:** L'evoluzione della smart grid

La Figura 2.5 mostra che gli investimenti degli ultimi anni si sono focalizzati principalmente sull'aspetto della rete elettrica che riguarda le misurazioni (*metering*). I primi progetti in questo settore hanno visto la nascita dei sistemi di **automated meter reading** (AMR) all'interno del sistema di distribuzione [1].

L'infrastruttura AMR, nata nel 1977, ha introdotto l'automazione nella rete elettrica. Attraverso una combinazione di tecnologie, incluse reti wireless e wired, AMR ha permesso alle compagnie di leggere le misurazioni da remoto, di ottenere le informazioni quasi in real-time e di fornire agli utenti bollette basate sui loro consumi reali (in precedenza le compagnie emettevano le bollette basandosi sulle stime dei consumi del cliente).

Inoltre, grazie a questo meccanismo di recupero informazioni tempestivo, le aziende sono state capaci di migliorare la produzione di energia attraverso un maggiore controllo durante periodi di alta e bassa richiesta.

Sebbene la tecnologia AMR all'inizio abbia attirato molta attenzione, le aziende presto si sono rese conto che non risolve il loro problema principale: la gestione demand-side. A causa della sua comunicazione unidirezionale, le capacità di AMR sono ridotte alla sola lettura dei dati e non è permesso, per esempio, modificare il comportamento della rete a seconda delle informazioni ricevute.

Pertanto AMR ha avuto vita breve; le aziende, piuttosto che continuare ad investire su di essa, hanno preferito spostarsi verso l'**advanced metering infrastructure** (AMI).

L'AMI (di cui si parlerà in dettaglio nel Capitolo 3), è un'architettura che permette la comunicazione automatizzata e bidirezionale tra uno smart me-

ter e una società di servizi. L'obiettivo è quello di fornire a tali società informazioni real-time circa i consumi energetici e permettere agli utenti di fare scelte consapevoli sull'utilizzo dell'energia basate sui costi all'istante di utilizzo.

Il passo successivo nell'evoluzione della distribuzione della corrente elettrica è costituito dalla **Smart Grid**, che utilizza l'AMI come componente core per il recupero delle informazioni circa lo stato della rete e i consumi utente.

## 2.3 Perché la Smart Grid?

Le industrie del settore dei servizi pubblici di tutto il mondo attualmente cercano di risolvere numerosi problemi, tra cui

- Diversificazione della generazione di energia;
- Gestione delle richieste utente;
- Conservazione dell'energia;
- Riduzione globale dell'emissione di anidride carbonica.

È evidente che tali problemi non possono essere risolti facendo affidamento sulla rete elettrica esistente.

Come detto in precedenza, la natura della comunicazione della rete attuale è unidirezionale. Essa, inoltre, converte solo un terzo di energia in elettricità, senza preoccuparsi del calore disperso. Circa l'8% della corrente prodotta, viene dissipata poi attraverso i cavi elettrici, mentre il 20% viene riservata ad eventuali picchi di carico di richieste utente (ed è in uso solo il 5% delle volte).

In aggiunta a tali problemi, vi è l'inadeguatezza della struttura gerarchica della rete. A causa di tale organizzazione, infatti, si ha un *effetto domino dei guasti*, in cui un fallimento verificatosi all'interno di uno dei tre sottosistemi può influire significativamente sugli altri.

La rete elettrica di nuova generazione, la Smart Grid, si propone di occuparsi delle maggiori carenze della rete attuale. A partire dal 2005, c'è stato un interesse sempre più crescente verso le Smart Grid. Il riconoscere che l'ICT (*Information and Communication Technology*) offre significative opportunità per modernizzare il funzionamento delle reti elettriche unito alla consapevolezza che la produzione di energia può essere migliorata solo con un continuo

Existing Grid	Intelligent Grid
Electromechanical	Digital
One-Way Communication	Two-Way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-Monitoring
Manual Restoration	Self-Healing
Failures and Blackouts	Adaptive and Islanding
Manual Check/Test	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

**Figura 2.6:** Differenze tra la rete elettrica attuale e la Smart Grid

ed efficiente monitoraggio, ha fatto sì che si muovessero i primi passi verso la Smart Grid. In aggiunta a tali fattori, ci sono anche altre motivazioni a favore del passaggio verso una rete elettrica moderna [3]:

- *Strutture non più adeguate:* in molte zone del mondo (per esempio in USA e in alcuni paesi dell'Europa), i sistemi si sono rapidamente espansi a partire dal 1950; le strutture relative alla trasmissione e alla distribuzione che furono installate a quel tempo non sono più adatte e devono essere sostituite. Il bisogno di rinnovare tali componenti è un'ovvia opportunità di innovazione e, quindi, di introduzione di nuovi modelli e pratiche operative. A ciò si aggiunge il fatto che, in molti paesi, i circuiti elettrici hanno bisogno di adattarsi ai carichi sempre più crescenti e all'introduzione di nuove fonti di energia rinnovabili. Ciò richiede, quindi, metodi più intelligenti sia per aumentare la capacità di trasmissione dell'energia, sia per reindirizzare il flusso di corrente verso circuiti meno carichi;
- *Vincoli termici:* si riferiscono ai limiti dei sistemi di trasmissione e distribuzione relativamente alla loro capacità di diffusione dell'energia. Quando le attrezzature trasportano la corrente eccedendo la loro potenza termica, si surriscaldano e i materiali atti all'isolamento si deteriorano rapidamente. Ciò comporta una riduzione della vita delle attrezzature e un aumento di possibilità di fallimenti.  
I vincoli termici dipendono molto dalle condizioni dell'ambiente esterno,

che cambiano durante gli anni. Pertanto l'uso di rate di trasmissione e distribuzione dinamici può aumentare la capacità del circuito;

- *Vincoli operativi*: qualsiasi sistema opera all'interno di predefiniti vincoli di voltaggio e frequenza. Se il voltaggio eccede il limite, i materiali isolanti dei componenti del sistema e le attrezzature degli utenti possono essere danneggiate e causare corto-circuito.

Per quanto riguarda la frequenza invece, si tende a mantenerla all'interno di un range molto piccolo e, quando varia, intervengono dei servizi appositi che hanno il compito di riportarla nell'intervallo prestabilito. La generazione di energia rinnovabile, però, ha un output variabile che non può essere previsto con certezza in anticipo. Pertanto mantenere il bilancio erogazione-richiesta e la frequenza del sistema nei limiti risulta essere un compito arduo. Per tale motivo si è sempre alla ricerca di nuovi servizi per la gestione della frequenza.

Si pensa che in futuro l'utilizzo delle Smart Grid in vari ambiti, per esempio domestico e automobilistico, porterà ad avere carichi sempre più flessibili; ciò aiuterà nel mantenere la stabilità della rete;

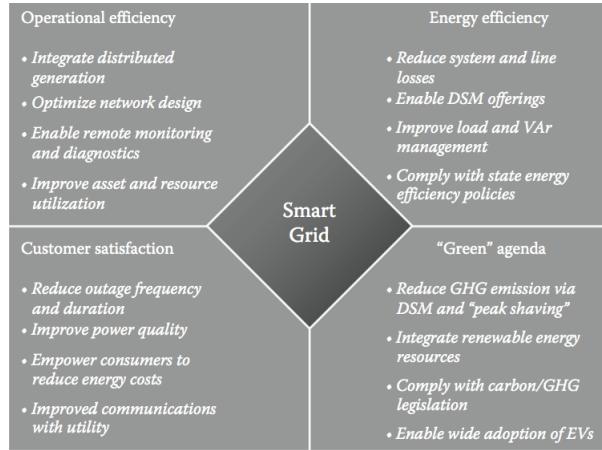
- *Sicurezza delle forniture*: la società moderna richiede che la fornitura di energia sia sempre più affidabile, man mano che carichi sempre più critici vengono connessi alla rete. L'approccio tradizionale per migliorare l'affidabilità, come visto in precedenza, era quello di installare cammini ridondanti, con notevole impatto sia sui costi che sull'ambiente.

L'approccio della Smart Grid in caso di guasti, invece, prevede l'utilizzo di intelligenti meccanismi di riconfigurazione, in modo tale da mantenere costante la fornitura ai clienti ma evitando i costi addizionali portati da ulteriori circuiti;

- *Iniziative nazionali*: molti governi nazionali incoraggiano le iniziative delle Smart Grid poiché le considerano un meccanismo redditizio ma, allo stesso tempo, economico per rinnovare le loro infrastrutture e introdurre risorse rinnovabili.

La figura 2.7 mostra i vantaggi introdotti dall'utilizzo delle Smart Grid. Lo sviluppo di tale rete moderna non dovrebbe essere basato solo su "soluzioni abilitanti", ma anche su "soluzioni integrate" che rispondano ai problemi operativi e aziendali e che forniscono benefici significativi, misurabili e durevoli agli utenti, al servizio pubblico, all'economia e all'ambiente.

Di estrema importanza nell'implementazione delle soluzioni proposte dalla Smart Grid sono i seguenti aspetti:



**Figura 2.7:** Benefici introdotti dalla Smart Grid

- Migliorare l'affidabilità dell'energia dei servizi pubblici, le performance operative e la produttività generale;
- Aumentare l'efficienza energetica e diminuire le emissioni di anidride carbonica;
- Permettere agli utenti di gestire i loro consumi energetici risparmiando energia ma, allo stesso tempo, senza modificare il loro stile di vita;
- Ottimizzare l'integrazione di energie rinnovabili.

## 2.4 Cos’è la Smart Grid?

Il concetto di Smart Grid mette insieme una serie di tecnologie e soluzioni per gli utenti finali e affronta, inoltre, concetti politici e normativi.

Non esiste una singola definizione chiara e precisa; in [3] è possibile trovare una serie di caratterizzazioni.

L’European Technology Platform definisce la Smart Grid nel seguente modo:

*“Una Smart Grid è una rete elettrica che può integrare intelligentemente le azioni di tutti gli utenti connessi ad essa - generatori, consumatori - in modo da fornire efficientemente un’alimentazione elettrica che sia sostenibile, economica e sicura.”*

In accordo all’US Department of Energy:

*“Una Smart Grid utilizza la tecnologia digitale per migliorare l'affidabilità, la sicurezza e l'efficienza (sia economica che energetica) del sistema elettrico, a partire dalla generazione su larga scala, attraverso il sistema di distribuzione, fino ai consumatori, ed attraverso un numero crescente di risorse di storage e di generazione distribuita.”*

Secondo *Smarter Grids: The Opportunity*, invece, la Smart Grid è definita come:

*“Una Smart Grid utilizza sensing, embedded processing e comunicazioni digitali per far sì che la rete elettrica sia osservabile (capace di essere misurata e visualizzata), controllabile (capace di essere manipolata ed utilizzata), automatizzata (capace di adattarsi ed autoripararsi), pienamente integrata (pienamente interoperabile con sistemi esistenti e con la capacità di incorporare un insieme di diverse sorgenti energetiche).”*

[3] suggerisce, inoltre, i seguenti attributi per una Smart Grid:

- Permette la gestione “demand side” sia attraverso l'integrazione di smart meter, elettrodomestici intelligenti, micro-generazione e conservazione dell'energia sia fornendo agli utenti informazioni circa i loro utilizzi e i prezzi;
- Facilita l'introduzione di fonti di energia rinnovabile e di generazione distribuita, riducendo così l'impatto ambientale dell'intero settore energetico;
- Assicura e migliora l'affidabilità e la sicurezza delle forniture, resistendo agli attacchi, ai disturbi e ai disastri naturali, anticipando e affrontando i problemi del sistema e migliorando le funzionalità di trasferimento dell'energia;
- Mantiene alta la qualità della fornitura di energia elettrica per soddisfare le apparecchiature sempre più sofisticate che aumentano con l'economia digitale.

## 2.5 Requisiti di una Smart Grid

Monitoraggio/*sensing*, comunicazione e controllo sono i tre *building block* fondamentali che convertono un sistema di distribuzione di energia in una



Smart Grid. Le componenti di monitoraggio/sensing devono essere capaci di rilevare malfunzionamenti o deviazioni dal normale range operativo della rete elettrica. Inoltre, poiché in una Smart Grid un punto di consumo elettrico può diventare anche un punto di generazione, il processo di sensing deve essere strettamente collegato al processo di *metering*.

I sistemi di comunicazione devono permettere che l'input dei sensori raggiunga gli elementi di controllo della Smart Grid, i quali genereranno dei messaggi con il compito di assicurarsi che la trasmissione nei vari punti della rete sia conforme alle aspettative. Ci sono, inoltre, altri requisiti importanti per le infrastrutture di comunicazione, di cui si discutono i dettagli nel resto di questo paragrafo [5].

*Quality of Service*: è necessario garantire la *QoS* per le tecnologie di comunicazione e di rete utilizzate all'interno della Smart Grid, partendo dalla generazione dell'energia, passando per trasmissione e distribuzione e finendo alle applicazioni utente. In particolare, ci si focalizza su due parametri: *latenza* e *larghezza di banda*.

Per quanto riguarda la latenza, la comunicazione in una Smart Grid è caratterizzata dal fatto che la maggior parte delle interazioni devono avvenire in tempo reale. Per scopi di sensing/misurazione, i messaggi di lettura dovrebbero essere trasmessi all'interno di un *frame temporale* molto piccolo. Per esempio, il tempo massimo di trasmissione ammesso è nel range dei 12-20 ms. I valori misurati non dovrebbero essere generati da più di 15 secondi quando arrivano al centro di controllo.

Per quanto riguarda la larghezza di banda, durante l'evoluzione di una Smart Grid, mediante l'aggiunta ad essa di elementi sempre più intelligenti, l'infrastruttura di comunicazione dovrebbe essere capace di trasmettere un numero sempre più crescente di messaggi simultaneamente, senza grave impatto sulla

latenza. La banda di rete deve aumentare più rapidamente rispetto alla richiesta di tali elementi intelligenti nella rete.

*Interoperabilità:* si riferisce all'abilità delle diverse parti di una Smart Grid di lavorare insieme, di utilizzare componenti compatibili, di scambiarsi informazioni tra di loro e lavorare in maniera cooperativa per completare i task. Tale requisito rende effettiva l'integrazione e la comunicazione bidirezionale tra i tanti elementi interconnessi della rete.

Il *NIST* ha sviluppato un framework che include protocolli e standard per la gestione delle informazioni, in modo da raggiungere l'interoperabilità tra i dispositivi della Smart Grid e i sistemi. Maggiori dettagli in [9].

*Scalabilità:* è necessaria per facilitare l'inserimento all'interno della Smart Grid sia di tanti nuovi dispositivi e servizi, che di tanti meccanismi di monitoraggio real-time dell'interazione dell'utente finale.

[5] propone una rete *IP-based* come soluzione efficace per i bisogni dell'infrastruttura di comunicazione.

*Sicurezza:* in accordo all'*Electric Power Research Institute (EPRI)*, uno dei requisiti emergenti dello sviluppo delle Smart Grid è relato alla **cyber security** dei sistemi. Come indicato nel loro report [5], la sicurezza informatica del sistema di comunicazione è un problema critico, a causa dell'aumento del potenziale degli attacchi e degli incidenti che si verificano in esso.

La cyber security deve occuparsi non solo di attacchi deliberati, come quelli provenienti, ad esempio, da dipendenti non contenti, da spionaggio industriale e da terroristi, ma anche di manomissioni involontarie dell'infrastruttura di informazione dovute ad errori degli utenti, fallimenti delle attrezzature e disastri naturali. Le vulnerabilità potrebbero permettere, infatti, ad un attaccante di penetrare nella rete, ottenere accesso al software di controllo e alterare le condizioni di carico per destabilizzare la rete.

Attualmente, molte organizzazioni lavorano sullo sviluppo dei requisiti di sicurezza nella Smart Grid, tra cui North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), IEEE, National Infrastructure Protection Plan (NIPP), e NIST.

Denominatore comune di tutti gli standard in via di sviluppo è il seguente concetto: la sicurezza delle comunicazioni nella Smart Grid dipenderà fortemente da autenticazione, autorizzazione e tecnologie per la *privacy*.

Tutte le tecnologie sviluppate, poggiano su una sorta di gestione della chiave. Considerando il fatto che la Smart Grid conterrà milioni di dispositivi, diffusi tra tante organizzazioni, i sistemi di gestione della chiave utilizzati dovranno

no essere altamente scalabili e garantire i livelli massimi possibili di efficienza.

*Standardizzazione:* la Smart Grid coinvolge al suo interno una serie di standard come, ad esempio, nella generazione dell'energia, nella distribuzione e nel controllo oltre che nella comunicazione. IEEE recentemente ha preso l'iniziativa per definire questi standard e linee guida su come la Smart Grid dovrebbe operare utilizzando le ultime tecnologie nell'ingegnerizzazione dell'energia, controllo, comunicazione e informazione; il gruppo che è stato creato prende il nome di IEEE P2030 group [5].

Per quanto riguarda l'ingegnerizzazione dell'energia, ci si focalizza sui requisiti di interoperabilità. Per quanto riguarda l'informazione, invece, si affrontano problemi relativi alla privacy, sicurezza, integrità dei dati, interoperabilità e interfacce. Per la comunicazione, infine, si definiscono i requisiti per l'interazione tra i dispositivi e si stabiliscono limiti per generazione, distribuzione e trasmissione in collaborazione con i clienti.

## 2.6 Tecnologie coinvolte

Per soddisfare tutti i requisiti della Smart Grid, è necessario sviluppare ed implementare le seguenti tecnologie [3]:

1. *Tecnologie per l'informazione e la comunicazione*, che includono

- Meccanismi per la comunicazione bidirezionale tra le varie componenti del sistema;
- Architetture aperte per il collegamento e l'utilizzo semplice di elettrodomestici e veicoli elettrici;
- Componenti hardware e software necessari per fornire ai clienti sempre più informazioni;
- Software per garantire la sicurezza delle informazioni e standard per fornire scalabilità e interoperabilità tra i sistemi di informazione e comunicazione.

2. *Tecnologie per misurazioni, sensing, controllo ed automazione*, che includono

- *Intelligent Electronic Devices* (IED) per fornire inoltro, misurazioni e memorizzazione di fallimenti ed eventi per il sistema energetico in maniera avanzata;

- *Phasor Measurement Units* (PMU) e *Wide Area Monitoring, Protection and Control* (WAMPAC) per garantire la sicurezza del sistema;
- Sistemi integrati di sensing, misurazione, controllo ed automazione e tecnologie per l'informazione e la comunicazione per fornire rapide diagnosi e risposte tempestive a qualsiasi evento in qualsiasi parte della rete;
- Elettrodomestici, comunicazione, controllo e monitoraggio più intelligenti per massimizzare la sicurezza, il comfort e il risparmio energetico delle abitazioni;
- Smart meter e tutti i software che permettano ai clienti di avere una maggiore scelta e un maggiore controllo sull'utilizzo di elettricità e gas. Tali meccanismi permetteranno, inoltre, di fornire ai clienti bollette più accurate e informazioni real-time più precise sui loro consumi.

### 3. *Tecnologie per la conservazione dell'energia*, che includono

- *High Voltage Direct Current* (HVDC) e *Flexible Alternate Current Transmission Systems* (FACTS) per abilitare le trasmissioni a lungo raggio e l'integrazione delle energie rinnovabili;
- Differenti interfacce e differenti dispositivi per fornire una connessione efficiente delle risorse rinnovabili e dei dispositivi per la conservazione dell'energia;
- Dispositivi per fornire un maggiore controllo sui flussi di energia nella rete a corrente alternata;
- HVDC e FACTS in unione ad altri filtri, integrati nei meccanismi di comunicazione e controllo per assicurare una maggiore affidabilità e flessibilità del sistema e una migliore qualità dell'energia.

# Capitolo 3

## Architettura

L'odierna rete elettrica è stata progettata come un sistema centralizzato, in cui l'energia elettrica fluisce attraverso linee unidirezionali di trasmissione e distribuzione dai generatori fino ai clienti finali. La logica applicativa è concentrata in una zona centrale e solo parzialmente nelle *substation*, mentre le componenti restanti sono quasi totalmente passive. Una Smart Grid, mostrata dal punto di vista strutturale, in Figura 3.1, fornisce una più elevata ed ampia intelligenza distribuita incorporata nei dispositivi locali, comunicazione e scambio bidirezionale di informazioni ed elettricità.

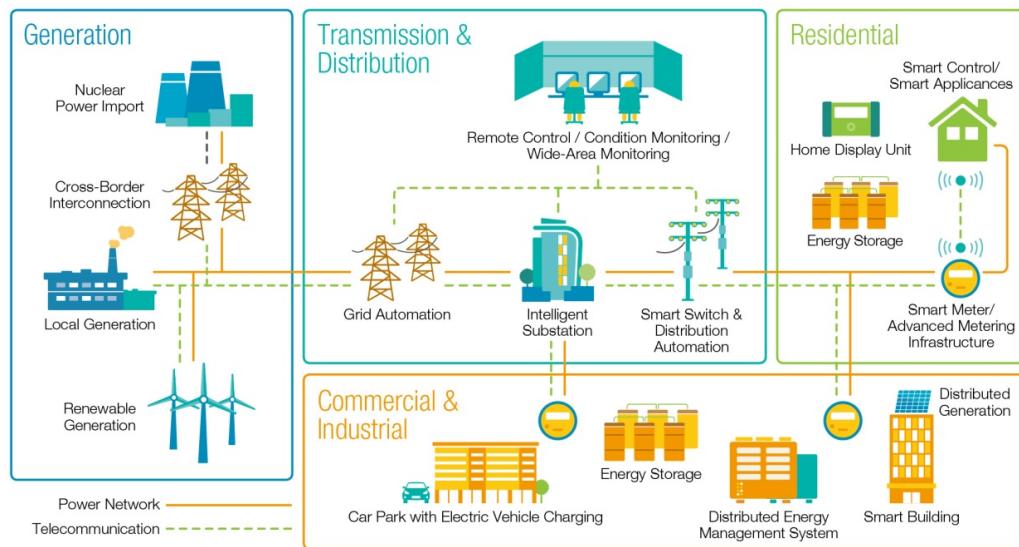


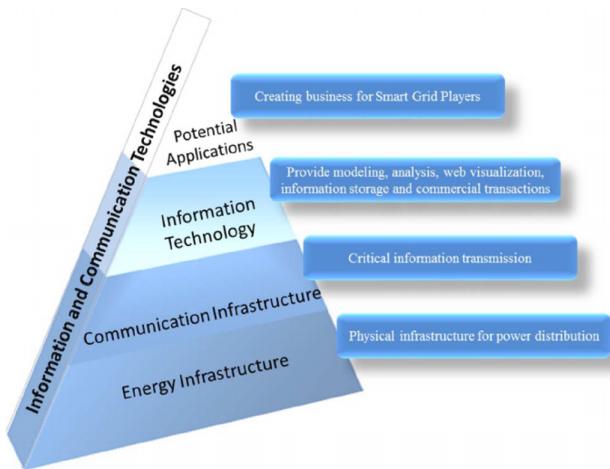
Figura 3.1: *Smart Grid*

### 3.1 Smart Grid Framework

Le Smart Grid richiedono sia una complessa infrastruttura di comunicazione, che sofisticate tecnologie di comunicazione e computazione. Entrambe consentono la conservazione di parte dell'energia prodotta e l'introduzione di nuovi metodi di gestione della domanda energetica, per adottare politiche di bilanciamento del carico, controllare instabilità energetiche causate dalla natura delle risorse rinnovabili e prevenire la diffusione di fallimenti in cascata nella rete [10].

La Figura 3.2 riassume le principali tematiche relative alle Smart Grid:

- *Energy infrastructure*, rappresenta la base fisica ed organizzativa necessaria per la generazione, trasmissione e distribuzione dell'energia;
- *Communication infrastructure*, è responsabile del trasferimento di informazioni critiche attraverso la rete;
- *Information technology*, fornisce modelli, analisi, visualizzazioni web e transazioni commerciali;
- *Potential applications*, offre tecniche di generazione, gestione, automatizzazione e rilevamento per l'intero sistema.



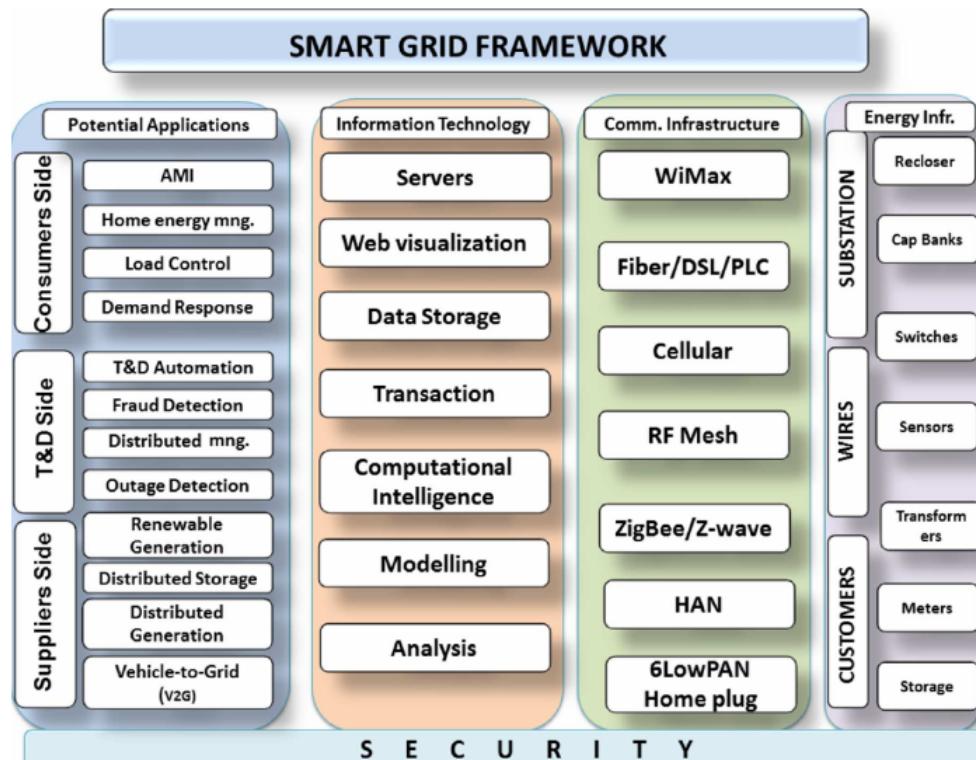
**Figura 3.2:** *Smart Grid framework*

La communication infrastructure svolge un ruolo cruciale, ossia collegare tutte le componenti della rete collezionando informazioni sulle loro condizioni,

per scopi di controllo, monitoraggio e manutenzione. Eventuali problemi legati all'energy infrastructure possono essere evitati se vengono adottate determinate contromisure con l'aiuto della communication infrastructure. Differenti tecnologie di comunicazione posso essere usate per diversi scopi, in base all'applicazione. L'information technology fornisce una piattaforma comune di scambio di informazioni provenienti da differenti attività legate alla Smart Grid, che permette l'integrazione di informazioni da diversi livelli, dando sostegno alla raccolta di informazioni, all'analisi e al loro utilizzo per applicazioni avanzate.

Le tecniche dell'application layer generalmente mirano a ridurre il consumo energetico dei clienti, cambiando i loro comportamenti di consumo, dotandoli di strumenti di monitoraggio.

La Figura 3.3 mostra le componenti della Smart Grid, illustrate dall'energy infrastructure al potential applications.



**Figura 3.3:** Smart Grid framework

Il concetto di Smart Grid mira a realizzare un sofisticato sistema, integrando information technology e communication infrastructure all'attuale sistema di alimentazione e il nuovo sistema di generazione distribuito, in modo da sfruttare pienamente l'uso di risorse rinnovabili e di massimizzare l'efficienza energetica. Da una prospettiva leggermente diversa, una Smart Grid può essere considerata come una rete di comunicazione di dati che riesce, grazie al supporto di specifici dispositivi di gestione dell'energia, a far collaborare le diverse componenti della rete in maniera flessibile e senza discontinuità, per un utilizzo efficiente dell'energia.

La comunicazione consiste di tre categorie di trasmissione, con relativi standard e protocolli (vedi Capitolo 5):

- *Wide-area network* (WAN);
- *Field-area network* (FAN);
- *Home-area network* (HAN).

### **3.1.1 Wide-area network**

La WAN consente la comunicazione fra le entità che forniscono energia e le substation; deve estendersi su tutte le substation, strutture di distribuzione, generazione e conservazione dell'energia, per poter essere efficace e scalabile. Essa è una rete di comunicazione bidirezionale ad alta larghezza di banda, che gestisce le trasmissioni a lunga distanza dei dati con avanzate applicazioni di misurazione e monitoraggio. La comunicazione remota fra le *utility* e gli smart meter è essenziale per lo scambio di importanti informazioni, quali prezzi e tariffe dei clienti. Le reti cellulari, WiMAX e comunicazioni cablate, e in particolare comunicazioni basate su fibra ottica e microwave, sono i migliori candidati come tecnologie per WAN (vedi Capitolo 5).

Il sistema di distribuzione agisce da punto di aggregazione fra FAN e WAN, come ad esempio una substation o una torre di comunicazione, che colleziona tutte le informazioni prodotte dagli smart meter e le trasferisce alla rete di comunicazione principale. Oltre che da punto di aggregazione, tali dispositivi possono fungere da punti di conservazione dell'energia per eventuali interruzioni o guasti.

### **3.1.2 Field-area network**

La FAN può essere descritta come una rete di comunicazione per aree di distribuzione dell'energia e che mette in contatto l'automazione della

distribuzione e dispositivi di controllo alle sedi dei consumatori. Essa agisce, quindi, come un intermediario fra le substation e le sedi dei clienti, con nodi intelligenti in grado di raccogliere e controllare i dati da remoto. Tali nodi sono connessi ad un gateway, il quale è alimentato costantemente in modo da poter trasmettere i dati raccolti. I canali a bassa larghezza di banda della FAN sono altamente robusti per la trasmissione affidabile di dati.

La scelta delle tecnologie di comunicazione variano per la FAN in base alle esigenze della Smart Grid: fibra ottica per avere bassa latenza e performance di comunicazione superiori, oppure WiMAX se le reti cellulari non riescono a coprire l'area di interesse, ma l'attuale orientamento ricade sull'utilizzo dello standard ISO/IEC 61850 (vedi Sezione 5.2.3), il quale fornisce interoperabilità e comunicazione fra i dispositivi elettronici intelligenti.

### 3.1.3 Home-area network

Gli smart meter riescono a connettersi alla HAN, in modo tale che i consumatori siano in grado di conoscere l'importo da pagare e gestire il loro consumo ed avere il controllo dei propri elettrodomestici intelligenti, attraverso display presenti in casa e interfacce web. Le migliori tecnologie di comunicazione per HAN sono ZigBee, Wi-Fi, HomePlug, Z-wave e M-Bus (vedi Capitolo 5).

Nelle sezioni successive vengono presentate le tecnologie e le infrastrutture abilitanti di una Smart Grid, a partire dalla generazione e conservazione dell'energia fino ad arrivare alla trasmissione e distribuzione.

## 3.2 Generazione di energia rinnovabile

Le risorse di energia rinnovabile sono state sviluppate in molti paesi per ridurre l'inquinamento e fornire energia elettrica sostenibile. A differenza delle tradizionali fonti di energia, che creano inquinamento, le risorse di energia rinnovabile non esauriscono risorse naturali nel processo di creazione di energia e sono adattabili ovunque, in base alle dimensioni a partire dall'applicazione su una singola casa fino a dimensioni su larga scala [2].

Le più comuni risorse di energia rinnovabile sono:

- *Sistemi fotovoltaici*, i quali convertono l'energia solare direttamente in elettricità, attraverso pannelli esposti al sole. Tali pannelli sono costituiti da celle solari che contengono materiale fotovoltaico, le quali trasmettono elettroni tra diverse bande all'interno del materiale ge-

nerando differenza di potenziale fra due elettrodi, che consente alla corrente continua di fluire;

- *Sistemi per l'energia solare termica*, che convertono energia solare in calore. Esistono tre tipi di raccoglitori in base alla temperatura, da bassa per riscaldare piccoli spazi ad alta per l'utilizzo nella produzione di energia elettrica;
- *Vento*, la cui energia viene convertita tramite turbine in elettricità. Il principale aspetto negativo deriva dall'intermittenza del vento, specularmente per i sistemi basati sull'energia solare;
- *Biomasse*, ovvero la produzione di elettricità a partire da elementi naturali morti, anche se questa causa inquinamento atmosferico;
- *Sistemi che sfruttano la potenza dell'acqua*, sia che essa sia generata artificialmente che naturalmente, grazie alle onde e alle maree.

### 3.3 Smart meter e Advanced Metering Infrastructure

Uno *smart meter* è un dispositivo elettronico che registra consumi di energia elettrica in intervalli di un'ora o meno e comunica tali informazioni per scopi di fatturazione e monitoraggio [11]. Gli smart meter consentono una comunicazione bidirezionale fra essi ed i sistemi di controllo. A differenza dei display energetici posizionati nelle case, gli smart meter possono inviare in remoto i dati raccolti.

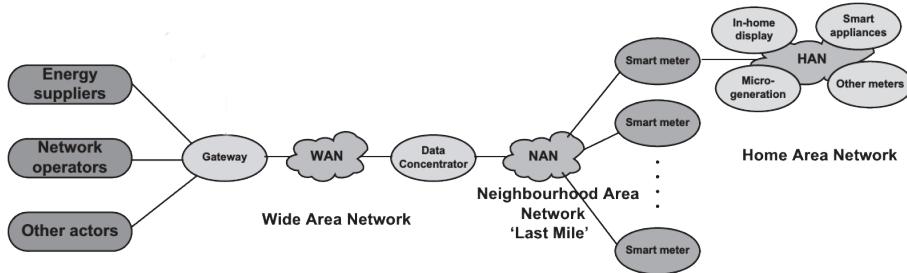
Per quanto riguarda la comunicazione bidirezionale esistono diversi protocolli:

- ANSI C12.18, C12.19 e C12.21, utilizzati principalmente nel nord America;
- ISO/IEC 61107 e 62056, usati nell'Unione Europea;
- *Open Smart Grid Protocol* (vedi Sezione 6.1), famiglia di specifiche pubblicata dall'European Telecommunications Standards Institute, usato in congiunzione con ISO/IEC 14908.

Gli smart meter consentono di ottenere informazioni specifiche, ciò consente alle aziende di introdurre diversi prezzi sul consumo, in base al periodo del giorno e alla stagione. Dal punto di vista dei clienti, gli smart meter permettono di conoscere il proprio consumo e potersi regolare di conseguenza. Uno studio accademico sulla base di studi esistenti ha mostrato che il consumo

di energia elettrica dei proprietari di abitazione, in media, si riduce di circa il 3-5% [12]. Le misurazioni degli smart meter vengono spesso aggregate da un dispositivo elettronico, chiamato *data concentrator* (vedi Figura 3.4), il quale:

- Si occupa di gestire gli smart meter ad esso collegati, in particolare le loro condizioni;
- Spedisce le misurazioni aggregate alle substation e ai centri di controllo che sfruttano tali informazioni;
- Punto di interazione fra i fornitori di servizi ed i consumatori.

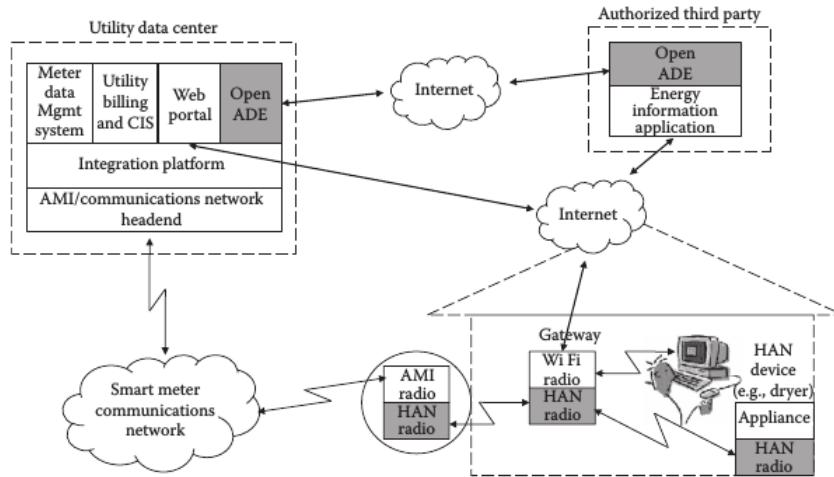


**Figura 3.4: Data concentrator unit**

*Advanced Metering Infrastructure* è una tecnologia che non coinvolge soltanto gli smart meter, ma è anche un'infrastruttura di comunicazione, applicazioni ed interfacce per lo scambio di dati. Un tipico sistema AMI (vedi Figura 3.5) è composto da una centralina AMI per la comunicazione, una piattaforma integrata, un *meter data management system* (MDMS), una rete di comunicazione AMI e terminali AMI, inclusi gli smart meter. I collegamenti di comunicazione con i clienti avviene mediante HAN, attraverso un'interfaccia che comunica con i termostati, elettrodomestici ed altri dispositivi. La centralina monitora, controlla e gestisce i protocolli di comunicazione e lo scambio dei dati con la rete. Inoltre, la centralina permette agli operatori remotamente di monitorare e gestire la rete AMI. Il MDMS colleziona i dati degli smart meter, effettua conservazione dei dati e li gestisce.

Fra i principali benefici dei sistemi AMI:

- Dati preziosi per il rilevamento di interruzioni, che sono integrati con l'OMS;



**Figura 3.5: Architettura AMI**

- Rilevamento e notificazione, in caso di manomissioni o furti;
- Aspetto chiave, per programmi di gestione della domanda energetica;
- Maggiori informazioni sui clienti per compagnie.

Alcuni svantaggi potenziali dei sistemi AMI:

- Problemi di privacy, in quanto le informazioni sull'utilizzo di energia sono disponibili per ciascun cliente e si possono trarre informazioni personali;
- Maggiore possibilità per una terza parte non autorizzata di poter accedere ai dati;
- Aumento dei rischi per la sicurezza di rete o l'accesso remoto.

### 3.4 Conservazione dell'energia

Il principale problema con l'energia elettrica è che deve essere utilizzata non appena viene generata, o in caso contrario, deve essere convertita in altre forme di energia. Durante i periodi in cui non è richiesta la loro assistenza, i sistemi di stoccaggio accumulano energia. Successivamente, l'energia immagazzinata viene inviata nel sistema di alimentazione in determinati periodi di tempo, riducendo pertanto la richiesta di generazione e assistendo il sistema

quando necessario [2]. Tali sistemi di conservazione dell'energia vengono sfruttati per diversi scopi:

- Mitigare fluttuazioni e perdite momentanee di potenza;
- Gestire cambiamenti frequenti di richiesta energetica per garantire la stabilità del sistema;
- Sostenere l'intermittenza e la mancanza di controllabilità nella generazione di energia rinnovabile, fornendo l'energia mancante e sottraendo quella in eccesso rispetto alla domanda;
- Conservare energia in determinati periodi, ad esempio quando la domanda oppure il prezzo sono bassi e fornirla quando conviene.

Storicamente le centrali idroelettriche sono state le più comuni applicazioni di stoccaggio dell'energia, tuttavia negli ultimi decenni sono state introdotte nuove tecnologie in tale ambito:

- Batterie, in grado di immagazzinare energia durante le fasi di carico/-scarico;
- Pile a combustibile, che permettono di ottenere energia mediante reazioni chimiche, senza che avvenga alcun processo di combustione termica, a partire da ossigeno ed idrogeno;
- Volani, i quali possono accumulare energia cinetica in masse rotanti e rilasciarla rallentandone la rotazione;
- Superconduttori magnetici, capaci di raccogliere energia in campi magnetici, che vengono creati attraverso il passaggio di corrente continua in super bobine.

### 3.5 Veicoli elettrici

Le Smart Grid ed i relativi miglioramenti in affidabilità, sostenibilità, sicurezza ed economia della rete elettrica consentono la partecipazione attiva di veicoli alla Smart Grid. I trasporti elettrici sono sempre stati collegati alla tradizionale rete elettrica, in maniera più o meno contigua per alimentare tali veicoli. L'introduzione di meccanismi di conservazione di energia hanno permesso l'uso di veicoli non strettamente legato alla rete. Sono presenti due tipologie di veicoli elettrici:

- *Plug-in*, i quali possono conservare energia grazie a batterie ricaricabili ed utilizzano un motore elettrico per la propulsione;
- *Ibidi*, che combinano i motori convenzionali e treni a trazione elettrica per fornire la forza motrice da entrambi i carburanti a combustione interna o energia immagazzinata nelle batterie.

Esistono due categorie di interazioni energetiche fra i veicoli e la rete elettrica:

- *Grid-to-vehicle*, che consiste nella fornitura di energia da parte della rete ai veicoli del tipo plug-in, mediante una presa per la carica;
- *Vehicle-to-grid*, in cui il veicolo possiede gli strumenti per fornire energia verso la rete elettrica, considerato come distributore di energia e risorsa di alimentazione nella Smart Grid.

Siccome i veicoli non seguono dei meccanismi deterministici e non forniscono una quantità paragonabile a quelle delle classiche tecnologie, rappresentano una sfida per l'integrazione nelle Smart Grid, anche a causa dei costi infrastrutturali [13]. I veicoli elettrici possono essere usati sia come dispositivi di memorizzazione distribuiti, che per fornire l'energia conservata nelle batterie alla rete elettrica o altrettanto alle case. Quindi tali mezzi possono fornire aiuto nel bilanciamento del carico, immagazzinando energia la notte e fornendola di giorno alla rete. Essi per il 95% del tempo sono parcheggiati, fornendo così l'opportunità di usare la loro energia, in modo da ridurre costi del sistema elettrico.

### 3.6 Microgrid

Una microgrid è un sistema energetico locale, che offre integrazione di risorse energetiche distribuite con le risorse che usufruiscono di tale energia, che può operare sia con la Smart Grid che in maniera isolata per fornire un livello personalizzato di affidabilità e resilienza [3]. Fra i principali vantaggi delle microgrid:

- Costituiscono un passo avanti economico ed efficiente per portare elettricità nelle zone rurali;
- Offrono una soluzione per alleviare la pressione dovuta alla saturazione della rete in determinate aree, senza grandi sforzi economici;
- Isolano determinati e sensibili consumatori, come basi militari e ospedali;

- Possono contribuire nella gestione della domanda energetica delle risorse rinnovabili;
- Sono in grado di contribuire nella conservazione dell'energia, nel miglioramento della stabilità e affidabilità delle reti elettriche.

Il maggior numero di tipi di microgrid sono istituzionali (ospedali, università o zone militari), seguiti da commerciali (fattorie, server farm, centri commerciali) ed infine di comunità (gruppi di case o appartamenti). Una microgrid è formata da componenti disponibili sul mercato, quali:

- *Sensori*, che determinano quali criteri adottare, se di isolamento o connessione alla rete elettrica;
- *Switch e contatori intelligenti*, che consentono rapide riconfigurazioni e monitoraggio in tempo reale;
- *Generatori di energia e dispositivi per la conservazione dell'energia*.

### 3.7 Smart substation

Una substation elettrica è un punto di riferimento dei sistemi di generazione, trasmissione e distribuzione, dove il voltaggio viene trasformato da alto a basso e viceversa mediante trasformatori. La corrente elettrica scorre attraverso diverse substation fra impianti di generazioni e clienti. Ci sono diversi tipi di substation: trasmissione, distribuzione, raccolta, smistamento. Le funzioni generali includono:

- Trasformazione del voltaggio;
- Punto di connessione delle linee energetiche di trasmissione e distribuzione;
- Centro di smistamento delle configurazioni dei sistemi di trasmissione e distribuzione;
- Zona di monitoraggio per il centro di controllo;
- Protezione per gli apparecchiature e linee elettriche;
- Comunicazione con le altre substation e i centri di controllo.

Le substation sono le fonti dei dati in tempo reale fondamentali per il funzionamento efficiente e sicuro della rete. I dati reali sono valori istantanei dei sistemi di alimentazione e vengono usati per la protezione, monitoraggio e controllo delle apparecchiature di tali sistemi. Vi è anche una ricchezza di dati non in tempo reale disponibile dalle apparecchiature, generalmente segnalazioni, che aiuta a rendere il funzionamento e la gestione delle attività di sistema più efficiente e affidabile [14].

Il concetto di smart substation, che si basa sulle tecnologie automatiche delle substation, consente monitoraggio più affidabile ed efficiente, funzionamento, controllo, protezione e manutenzione delle attrezzature e apparecchiature installate nelle sottostazioni. Tali obiettivi vengono raggiunti grazie alle caratteristiche principali delle smart substation, che sono:

- *Digitalizzazione*, un'unica e compatibile piattaforma per la rilevazione, misurazione, comunicazione, controllo, protezione e manutenzione, che comunica con i centri di controllo;
- *Autonomia e coordinazione*, il funzionamento non dipende da altre substation o centri di controllo, ma possono comunicare per incrementare l'efficienza e la stabilità della trasmissione elettrica. Anche all'interno stesso della smart substation, i singoli componenti devono essere autonomi;
- *Autoconfigurazione*, abilità nel configurarsi autonomamente in maniera dinamica, per ristabilirsi da attacchi, blackout, fallimenti delle componenti oppure disastri naturali.

Le funzioni essenziali di una smart substation comprendono:

- *Rilevamento e misurazione smart*, tutti i segnali misurati vengono etichettati con alta accuratezza grazie a sistemi di posizionamento (GPS);
- *Comunicazione*, ogni smart substation ha una LAN con alta larghezza di banda, che lega tutte le unità di misurazione e le applicazioni locali insieme, ed interfacce di connessione per diversi tipi di comunicazione. Il protocollo di comunicazione di una smart grid dovrebbe essere *open* e standardizzato ed una buona opzione è lo standard *ISO/IEC 61850* (vedi Sezione 5.2.3);
- *Controllo autonomo*, controllori decentralizzati vengono usati per l'autoripristino, per intraprendere azioni correttive o di previsione e ottimizzazione. I tradizionali controller *volt/VAr*, i quali permettono di

regolare e gestire in maniera dinamica il voltaggio, basati sulle informazioni di misurazione locali vengono coordinati da centri di controllo. Condizioni di instabilità valutati più velocemente dalle informazioni dei *PMU* [15], [16];

- *Gestione e visualizzazione dei dati*, applicazioni decentralizzate richiedono un appropriato sistema di gestione di dati distribuito, il quale gestisca e condivida i dati con le altre substation e che comunichi con i centri di controllo. Tutti i dati provenienti dai PMU (vedi Sezione 3.7.3), i ritardi, i resoconti di fallimenti devono essere visualizzati in tempo reale, per fornire una chiara visione dello stato della substation.

### 3.7.1 IED

*Intelligent Electronic Devices* (IED) sono dei dispositivi basati su microprocessore, che hanno la capacità di scambiare dati e segnali di controllo con altri dispositivi, come altri IED, misuratori elettrici, controller e sistemi SCADA (vedi Sezione 3.7.3), mediante canali di comunicazione. Gli IED svolgono funzioni di protezione, monitoraggio, controllo e acquisizione di dati nelle stazioni di generazione, substation ed alimentatori. Essi sono largamente usati nelle substation per diversi scopi e vengono utilizzati anche separatamente per ottenere funzioni individuali. Gli IED sono una componente chiave di integrazione e di automazione delle substation, le quali comportano l'integrazione delle funzioni di protezione, controllo e acquisizione dei dati, in modo da ridurre i costi operativi e di capitale, eliminando apparecchiature ridondanti e riducendo al minimo l'intervento umano. Tali dispositivi sono totalmente compatibili con lo standard ISO/IEC 61850 (vedi Sezione 5.2.3), hanno dimensioni ridotte e combinano varie funzioni in un'unica struttura robusta, consentendo una riduzione delle dimensioni dell'intero sistema, un aumento dell'efficienza e di robustezza, fornendo soluzioni estendibili basati su tecnologie di comunicazione tradizionali.

### 3.7.2 Sensori

La principale funzione dei sensori è quella di raccogliere i dati provenienti da apparecchiature di alimentazione e portarle alle componenti delle substation, in particolare trasformatori, interruttori e linee elettriche. Con l'introduzione delle tecnologie digitali e ottiche, nuovi sensori sono diventati disponibili per acquisire diversi tipi di informazioni relative a determinate risorse. L'apparato analogico basato su fili di rame può essere sostituito da fibra ottica per

misurazione e monitoraggio.

I vantaggi più importanti di tali sensori sono:

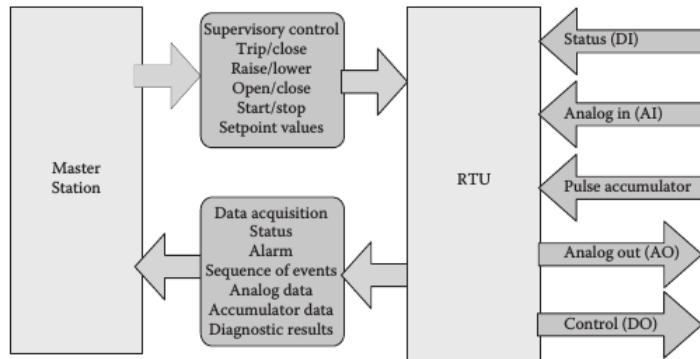
- Maggiore precisione;
- Nessuna saturazione;
- Dimensioni e peso ridotti;
- Sicuri e non dannosi per l'ambiente;
- Prestazioni e larghezza di banda elevate;
- Bassa manutenzione.

### 3.7.3 SCADA

*Supervisory Control And Data Acquisition* (SCADA) si riferisce a un sistema o una combinazione di sistemi che raccoglie i dati provenienti da vari sensori in un impianto o in altre posizioni remote e che invia questi dati ad un elaboratore centrale, che poi gestisce i dati e controlla da remoto i dispositivi. SCADA è un termine che viene utilizzato ampiamente per rappresentare soluzioni di controllo e di gestione in una vasta gamma di settori. Il settore elettrico ha un insieme specifico di requisiti che si applicano ai sistemi SCADA. Lo scopo principale di un sistema SCADA elettrico è quello di acquisire dati in tempo reale provenienti dai dispositivi situati nelle centrali elettriche, substation di trasmissione e di distribuzione, alimentatori per distribuzione, fornire il controllo delle apparecchiature e presentare le informazioni al personale operativo.

I sistemi SCADA sono globalmente accettati come mezzo di monitoraggio e controllo di sistemi di alimentazione elettrica, in particolare sistemi di generazione e trasmissione in tempo reale. Gli *RTU* (vedi Sezione 3.7.3) vengono utilizzati per raccogliere i dati analogici e lo stato di telemetria dai dispositivi, e di trasmettere comandi di controllo a tali dispositivi. Tali sistemi installati in una posizione centrale, come ad esempio il centro di controllo, includono apparecchiature di acquisizione dati, interfacce grafiche per gli operatori, applicazioni che agiscono sui dati e altri componenti.

Tipicamente apparecchiature di controllo di acquisizione dati comprendono almeno una *master station* (vedi sezione 3.7.3), uno o più RTU e un sistema di comunicazione. La master station di solito è collocata al centro di controllo dell'energia, mentre gli RTU sono installati nelle centrali elettriche, substation di trasmissione e distribuzione e attrezzature di alimentazione (Figura 3.6).



**Figura 3.6:** Architettura SCADA relativa al data flow

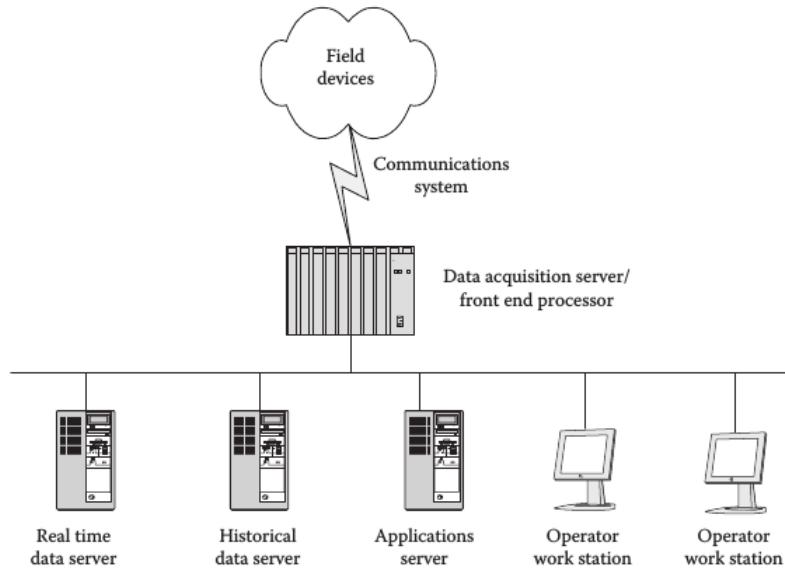
### Master station

Una master station è responsabile per la comunicazione delle apparecchiature e fornisce un’interfaccia uomo macchina (HMI) nella sala di controllo. In sistemi SCADA molto grandi, la master station può includere server ridondanti, applicazioni distribuite e meccanismi di ripristino. Una grande master station per l’impianto elettrico o *energy management system* (EMS), in Figura 3.7, generalmente ingloba:

- Uno o più server di acquisizione dati che si interfacciano con i dispositivi, mediante il sistema di comunicazione;
- Server di dati in tempo reale, il quale contiene una base di dati dedicata;
- Server che funge da storico;
- Server per le applicazioni dell’EMS;
- Postazioni operative con HMI.

All’interno dei EMS, le componenti hardware sono connesse mediante LAN. Ci sono diversi tipi di master station, che dipendono dal tipo di funzionalità:

- SCADA master station, che effettuano:
  - Acquisizione dei dati;
  - Controllo remoto;
  - Interfaccia utente;



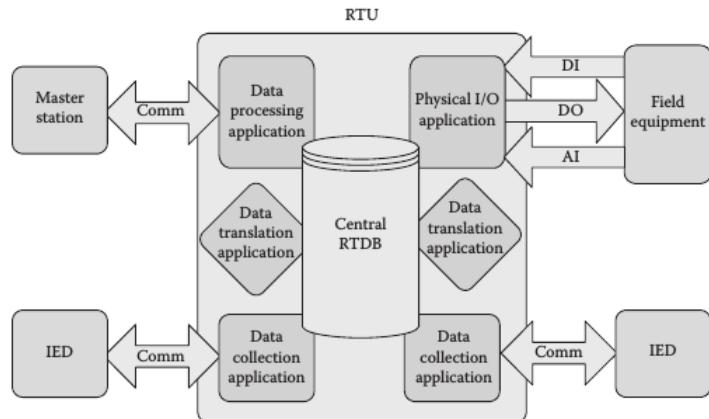
**Figura 3.7:** Architettura di un EMS

- Analisi dei dati;
- Produttore di report;
- SCADA master station con controllo di generazione automatico, in aggiunta alla categoria precedente:
  - Controllo di gestione automatico;
  - Economic dispatch;
  - Scheduling per le transazioni;
- EMS:
  - Configurazione e topologia di rete;
  - Stima dello stato;
  - Analisi delle contingenze;
  - *Optimal power flow*;
- *Distribution management system* (DMS):
  - Interfaccia per la gestione automatizzata per attrezzature o sistema di informazioni geografiche;

- Interfaccia per il sistema di informazioni dei clienti;
  - Interfaccia per la gestione delle interruzioni;
- *Distribution automation master:*
    - Comunicazioni bidirezionali distribuite;
    - Identificazione, isolamento e ripristino da fallimenti;
    - Riduzione del voltaggio;
    - Gestione dei dispositivi che utilizzano energia elettrica;
    - Controllo del *power factor*;
    - Previsione a breve termine della potenza che sarà consumata.

### Remote Terminal Unit

Un RTU è un dispositivo basato su microprocessore, che interfaccia un sistema SCADA trasmettendo dati di telemetria alla master station e che cambia lo stato dei dispositivi connessi, in base ai messaggi di controllo ricevuti dalla master station o da comandi generati dallo stesso RTU. Tale dispositivo fornisce dati alla master station e gli consente di emettere comandi per i dispositivi di campo. Tipicamente un RTU ha input fisici alle interfacce dei dispositivi di campo ed una più porte di comunicazione (Figura 3.8).



**Figura 3.8:** Architettura software di un RTU

Diversi RTU processano i dati in modi differenti, ma in generale contengono moduli software comuni fra di essi:

- Server per i dati real-time;
- Applicazioni per l'I/O fisico, che acquisisce i dati dei dispositivi mediante porte;
- Applicazioni per l'elaborazione dei dati, da inoltrare ad una master station o HMI;
- Applicazioni per la traduzione dei dati, che manipolano i dati prima di presentarli ad una master station.

Le generazioni precedenti di sistemi SCADA generalmente utilizzavano un RTU per ogni substation. Con tale architettura, tutti i cavi delle apparecchiature di campo dovevano terminare all'RTU, il quale offriva capacità limitate di espansione. Per gli ingressi analogici, l'RTU aveva bisogno di un trasduttore per convertire alti livelli di tensione e corrente da CT e PT (*Current e Potential Transformation*) in milliamper e volt. La maggior parte di RTU avevano una singola porta di comunicazione ed erano capaci di comunicare con una singola master station. La comunicazione fra un RTU e la sua master station era tipicamente ottenuta mediante protocolli proprietari orientati ai bit. Con l'avanzamento della tecnologia, gli RTU sono diventati più piccoli e flessibili. Questo ha permesso un approccio verso un'architettura distribuita, con un piccolo RTU per una o più parti dell'attrezzatura di una substation. Questo ha portato una riduzione dei costi di installazione, abbassando i requisiti legati al cablaggio. Questa architettura offre migliori capacità di espansione, mediante l'aggiunta di RTU. Inoltre, la nuova generazione di RTU è capace di accettare direttamente input con alti livelli di corrente alternata, eliminando la necessità di trasduttori e permettendo un collegamento diretto fra CT e PT all'interno degli RTU. Questo ha consentito un aumento delle funzionalità degli RTU, quali registrazione dei guasti e monitoraggio della qualità dell'energia.

Un avanzamento nelle capacità comunicative è stato raggiunto con l'aggiunta di porte disponibile per la comunicazione con gli IED. Tuttavia, il passo avanti più effettivo è stato l'introduzione di protocolli di comunicazione open. La disponibilità di un protocollo di comunicazione open e standard ha offerto la possibilità di scegliere un'attrezzatura che fosse indipendente dal venditore per i sistemi SCADA. Lo standard di fatto per i sistemi SCADA per impianti elettrici nel Nord America è diventato DNP3.0, un altro protocollo per l'ambiente manifatturiero industriale è MODBUS. L'ultimo standard di comunicazione adottato è ISO/IEC 61850 (vedi Capitolo ).

Per i sistemi SCADA cruciali sono le comunicazioni dei dati della rete.

L'architettura SCADA basata su protocolli di comunicazione seriali pone limitazioni sulle capacità del sistema, in quanto:

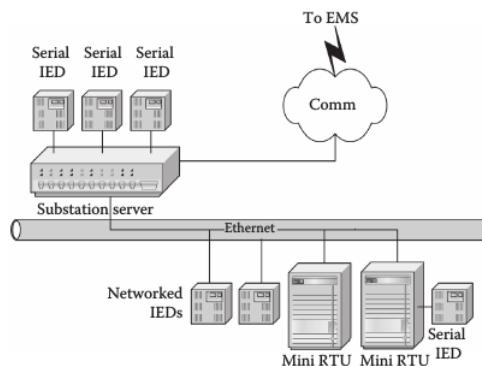
- Esiste un percorso statico tra la componenti che limita la connettività dei dispositivi;
- Protocolli seriali per SCADA non permettono l'utilizzo di più protocolli su un singolo canale;
- Sono presenti problemi con lo scambio di dati con nuove sorgenti;
- La gestione della configurazione deve essere eseguita attraverso una porta dedicata alla manutenzione.

L'architettura basata sulla rete offre numerosi vantaggi:

- Incremento significativo nella velocità e connettività, una LAN basata su Ethernet incrementa la larghezza di banda disponibile per la comunicazione e i protocolli di rete forniscono un collegamento diretto ai dispositivi presenti nella rete;
- Disponibilità di canali logici, protocolli di rete supportano canali logici multipli fra più dispositivi;
- Abilità di utilizzare nuove sorgenti di dati, ogni IED può fornire un nuovo numero di porta del protocollo per file o un trasferimento di dati ausiliare, senza disturbare altri processi e aggiungere ulteriore hardware;
- Miglioramento della gestione per la configurazione, eseguita mediante la rete.

Tale architettura offre dei tempi di risposta migliori, consente di accedere a dati importanti e riduce i tempi di gestione e configurazione del sistema. Prendendo in esame i passati sistemi SCADA, questi erano semplici sistemi di monitoraggio e controllo remoto che comunicavano mediante link a bassa velocità. Mentre, grazie alla proliferazione di IED basati su microprocessore, è diventato possibile avere informazioni direttamente dagli IED, RTU o dalle componenti del sistema di controllo delle substation. Ciò è stato possibile attraverso le capacità di comunicazione degli IED, in grado di comunicare direttamente con gli RTU, concentratori di dati o direttamente con la master station. Mentre sempre più IED sono stati installati presso le substation, è divenuto possibile integrare funzionalità di protezione, controllo

e acquisizione dati. Molte informazioni precedentemente estratte dagli RTU ora sono fruibili dagli IED. Tuttavia non è pratico avere una comunicazione diretta fra master station con i numerosi IED in tutte le substation. Per consentire tale passaggio di dati, si utilizza un *server* per la substation. Quest'ultimo comunica con tutti gli IED di una substation, conserva tutte le informazioni degli IED, e comunica con la master station. Siccome gli IED utilizzano diversi protocolli di comunicazione, il server della substation deve avere la capacità di comunicare mediante tali protocolli, così come con il protocollo della master station. Tale server permette ad un sistema SCADA di accedere ai dati da diversi IED della substation, il quale prima era possibile solo localmente. Con l'architettura SCADA basata su server di substation (Figura 3.9), tutti gli IED (inclusi gli RTU) sono interrogati dal server della substation, mediante la connessione LAN. Con tale architettura, la master

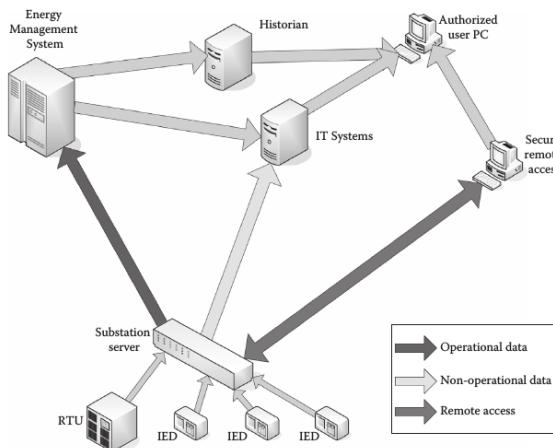


**Figura 3.9:** Architettura di controllo di una substation basata su server

station può comunicare direttamente con il server della substation invece che con i RTU e IED. Inoltre, le capacità di comunicazione del server sono superiori rispetto a quelle degli IED, e anche il ridotto numero di dispositivi collegati alla master station contribuisce al miglioramento delle performance di comunicazione. I dati disponibili nelle substation possono essere di due tipi:

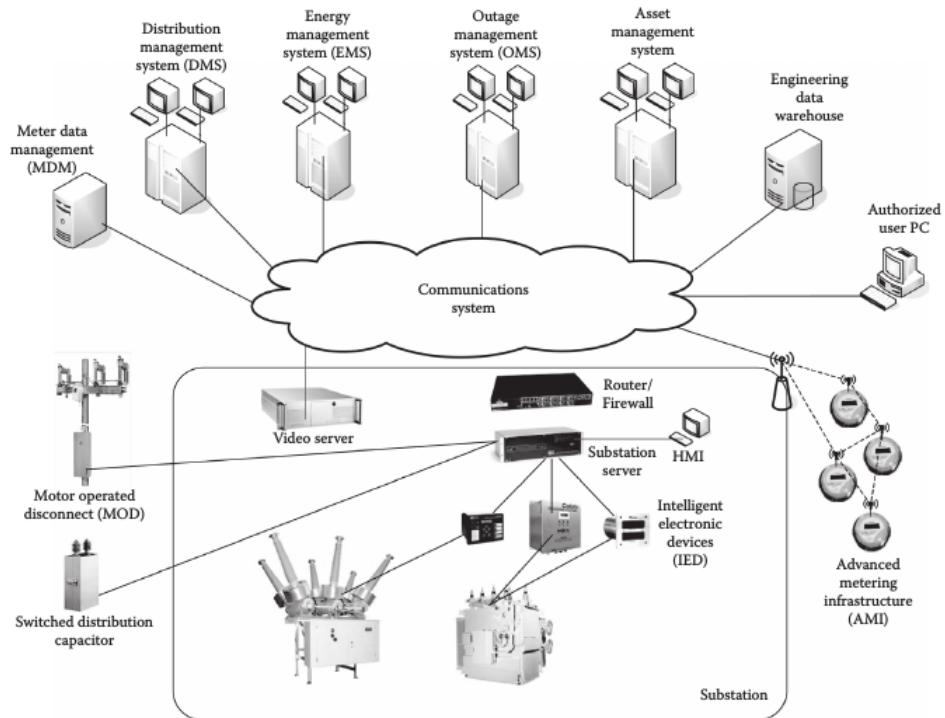
- Operazionali o in tempo reale, richiesti per il funzionamento di sistemi di alimentazione e per utilizzare applicazioni di EMS. Tali dati sono memorizzati dalle applicazioni dell'EMS e disponibili come dati appartenenti allo storico;
- Non operazionali, sono dati appartenenti allo storico ed in generale quei dati usati per analisi, manutenzione e pianificazione.

I moderni IED, come sistemi di protezione elettrica e misuratori, hanno una quantità enorme di informazioni. Una tipica master station non è progettata per processare questi dati, tuttavia queste informazioni possono essere estremamente utili per utenti diversi. Per poter trarre vantaggio da questi dati, un meccanismo di estrazione indipendente dalla master station deve essere implementato. I dati operazionali e non hanno meccanismi di raccolta dati diversi, per cui devono esistere due percorsi logici per i dati (Figura 3.10) uno per gli operazionali che connetta la substation all'EMS, ed un altro per quelli non operazionali dalla substation a sistemi di information technology. Con tutti gli IED connessi ai concentratori di dati delle substation ed



**Figura 3.10:** Scambio di dati delle substation

un'infrastruttura di comunicazione locale, è diventato possibile avere una connessione sicura per gli IED, in modo da effettuare manutenzione remota. Un'architettura di integrazione di substation (Figura 3.11) offre maggiori funzionalità, traendo vantaggio da un'architettura basata sulla rete, permettendo agli utenti di accedere ad informazioni importanti da tutti i componenti connessi alla rete. Tuttavia, introduce rischi di sicurezza addizionali all'interno del sistema di controllo. Per mitigare tali rischi, una attenzione speciale deve essere rivolta nella progettazione della rete, concentrandosi sulla sicurezza, autenticazione, autorizzazione e gestione degli utenti.



**Figura 3.11:** *Smart substation nell'architettura di una Smart Grid*

### 3.8 Sistemi di trasmissione

I sistemi di trasmissione si occupano dell'erogazione di energia elettrica. Essi forniscono milioni di megawatt di energia ogni giorno. La domanda di energia sempre crescente ha portato all'evoluzione dei sistemi di trasmissione dovendo fronteggiare, ad esempio, problemi legati alla variabilità dell'energia prodotta dalle risorse rinnovabili, alle eccessive richieste di energia e all'integrazione con altri sistemi. Sono presenti diverse tecnologie di controllo e monitoraggio che garantiscono efficienza, sicurezza ed affidabilità delle operazioni per quanto riguarda la trasmissione. Alcune di queste tecnologie intraprendono azioni automatiche di controllo della rete ed hanno effetto localmente al punto di connessione, mentre altre possono hanno un ambito operativo che può estendersi fino al centro di controllo. Queste tecnologie offrono controllo dinamico, non solo della fornitura di energia, ma anche della stabilità, voltaggio, frequenze della rete ed altri aspetti.

Una funzione di base delle reti elettriche è che la quantità di energia prodotta

in qualsiasi momento deve corrispondere alla quantità di energia consumata, e questo è compito dell'infrastruttura di trasmissione. Il flusso di energia elettrica attraverso il sistema di trasmissione segue le leggi fondamentali della fisica. Per una data tensione e impedenza di linea, si può calcolare la quantità di corrente che fluirà. Questo flusso di corrente può essere più (sovraffatto) o meno (sottoutilizzato) di quanto desiderato per la trasmissione. Un dispositivo di trasmissione che è in grado di modificare la risposta del sistema elettrico ad una data condizione è ovviamente un elemento utile nella creazione di una Smart Grid. L'aggiunta di un simile apparecchio non è sufficiente per ottenere una Smart Grid, ma sono necessari strumenti che consentono di controllare il flusso reale di energia, voltaggio e frequenza. Tali dispositivi in grado di mantenere il controllo sul reale flusso di corrente in una linea o nodo o addirittura regione di una rete sono i seguenti:

- *Condensatori sincroni*, in grado di controllare la tensione attraverso l'iniezione o l'assorbimento di potenza nei punti chiave del sistema di trasmissione, consentendo un controllo più preciso del flusso di potenza;
- *Flexible AC Transmission Systems* (FACTS), sistema che fornisce il controllo di uno o più parametri del sistema di trasmissione AC per migliorare la controllabilità e aumentare la capacità di trasferimento dell'energia;
- *High-Voltage Direct Current* (HVDC), sistema di trasmissione di energia elettrica in corrente continua, utilizzato su lunghe distanze. Esso può effettuare un controllo preciso sul flusso di informazioni interno ed esterno, in quanto tramite esso passano informazioni dettagliate ai centri remoti per monitoraggio, protezione e controllo. Tali sistemi sono in grado di rispondere agli eventi e alle anomalie più velocemente degli operatori, permettendo al sistema di stabilizzarsi e recuperare più velocemente.

Questi dispositivi sono in grado di implementare gli aspetti del controllo intelligente, sotto condizioni operative stazionarie, così come in caso di guasti, e a seconda della loro velocità di risposta, possono essere in grado di prevenire o accelerare il recupero automatico da situazioni di errore. In particolare, FACTS e HVDC forniscono caratteristiche che evitano problemi nei sistemi di alimentazione sovraccarichi; aumentano efficientemente la stabilità e capacità di trasmissione del sistema e aiutano a prevenire disturbi e alterazioni in cascata. Con l'aumento del carico e dei cambiamenti, alcuni elementi del sistema possono andare in contro ai loro limiti termici, e il commercio di energia per ampie aree con diversi modelli di carico contribuisce

ad aumentare la congestione [17], [18]. Inoltre, vincoli ambientali, come la minimizzazione delle perdite e riduzione di CO<sub>2</sub>, avranno un ruolo sempre più importante. Di conseguenza, i progettisti di rete devono affrontare conflitti tra la sicurezza delle forniture, sostenibilità ambientale, nonché l'efficienza economica. FACTS e HVDC giocano un ruolo importante nelle Smart Grid, permettono infatti di avere reti ibride efficienti di AC/DC e con basse perdite, le quali assicurano migliori gestione del flusso di corrente e prendono parte nel processo di gestione di disturbi e blackout.

In aggiunta a questi sistemi relativamente complessi, ci sono altre dispositivi di costo inferiore che aggiungono funzionalità alla Smart Grid, quali monitoraggio dei trasformatori e interruttori, in modo da determinarne l'usura e quindi prevedere i guasti. Tali sistemi prendono il nome di *Wide Area Monitoring, Protection And Control*, che includono l'utilizzo di misurazioni sincronizzate di ampie aree, reti di comunicazione affidabili e ad alta larghezza di banda e schemi di controllo e di protezione avanzati [19]. Un *Phasor Measurement Unit* è il building block principale di un sistema WAMPAC, il quale converte i segnali semplici dei sistemi di alimentazione in fasori, ovvero rappresentazioni della corrente e del voltaggio, che vengono comparati per ottenere informazioni sullo stato di stress della rete o eventuali alterazioni. Per cui attraverso tali informazioni si riescono ad individuare velocemente alterazioni dei segnali e dove si verificano in maniera accurata, per adottare successivamente misure adeguate.

### 3.9 Sistemi di distribuzione

Il sistema di distribuzione è il cuore di una Smart Grid. I progressi nelle tecnologie di controllo e comunicazione hanno consentito il funzionamento remoto automatico e/o semi-automatico delle componenti del sistema di distribuzione, che nel passato poteva essere azionato solo manualmente [20]. La necessità di lavori manuali da parte degli operatori nelle substation di distribuzione fu eliminata dall'applicazione di IED, sistemi SCADA e logger automatici di dati. In seguito, furono aggiunti strumenti, indicati come *fault location isolation and service restoration* (FLISR), per il ripristino energetico per far fronte a corti circuiti e malfunzionamenti temporanei. Successivamente, per il controllo e monitoraggio remoto degli alimentatori furono sviluppati sistemi con controllo del *volt/VAr* e sistemi SCADA basati su FLISR, in modo da migliorare l'affidabilità e ridurre le perdite di energia. Anche se la maggior parte dell'energia veniva fornita da grandi generatori centrali, un numero crescente di generatori distribuiti faceva il suo ingresso nel sistema

di distribuzione, tra cui le risorse energetiche rinnovabili e nello stesso periodo furono introdotti i sistemi *AMR*, in grado di effettuare comunicazioni unidirezionali.

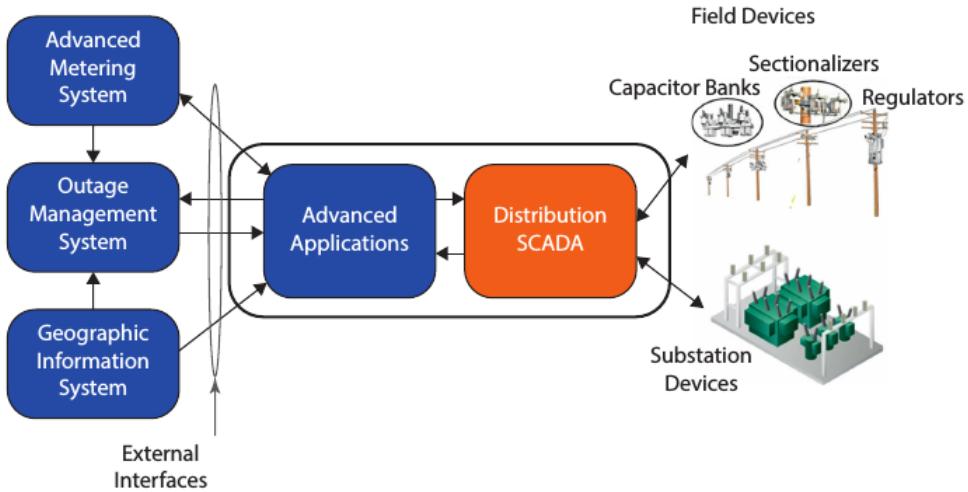
Le risorse energetiche rinnovabili costituiscono attualmente un importante aspetto della Smart Grid. Il sistema di distribuzione, infatti, deve fronteggiare l'alta variabilità delle risorse rinnovabili. Ad esempio, l'alta nuvolosità e la scarsa potenza del vento causano una riduzione dell'energia prodotta, che deve essere compensata mediante condensatori e regolatori di voltaggio. Inoltre per contrastare le variabilità della generazione energetica distribuita, le unità di quest'ultima sono equipaggiate di convertitori di corrente da diretta ad alternata per fornire in maniera reattiva energia, riducendo l'energia persa e migliorando il *power factor*, ovvero il rapporto tra potenza necessaria per compiere lavoro e quella erogata. La generazione di energia distribuita unita alla conservazione dell'energia e ai sistemi di controllo avanzati consentono alle microgrid di continuare a servire i clienti nelle comunità locali, sia quando se esse si separano dalla rete che si verifica una mancanza di corrente.

Il sistema di distribuzione si avvale di un *distribution management system* (DMS), per la propria gestione e prendere decisioni, e di sistemi con comunicazione bidirezionale basati su *Advanced Metering Infrastructure* (AMI), per supportare una vasta gamma di applicazioni collegate al fatturato e fornire informazioni in tempo reale sul consumo dei clienti e sulle condizioni delle apparecchiature elettrice di distribuzione. I sistemi AMI permettono programmi di *Demand-Side Management* (DSM), come ad esempio per la gestione di picchi energetici. I sistemi AMI e sensori intelligenti dentro e fuori le substation consentono di ottenere una grande quantità di informazioni proveniente dalle componenti del sistema di distribuzione, tramite comunicazioni che sfruttano l'alta larghezza di banda. In aggiunta alle informazioni in tempo reale da collezionare, è presente una moltitudine di informazioni geospatiali, che vengono memorizzati in *Geographic Information System* (GIS). Tale abbondanza di dati contiene informazioni che aiutano nella gestione del sistema di distribuzione ed è complessa da analizzare, per cui non vengono utilizzati strumenti tradizionali, ma strumenti per l'analisi dei dati specifici.

### 3.9.1 Distribution Management System

Il sistema di distribuzione della Smart Grid si affida ad un sistema con una visione completa sulle condizioni dei sistemi di alimentazione, ossia il distribution management system (Figura 3.12).

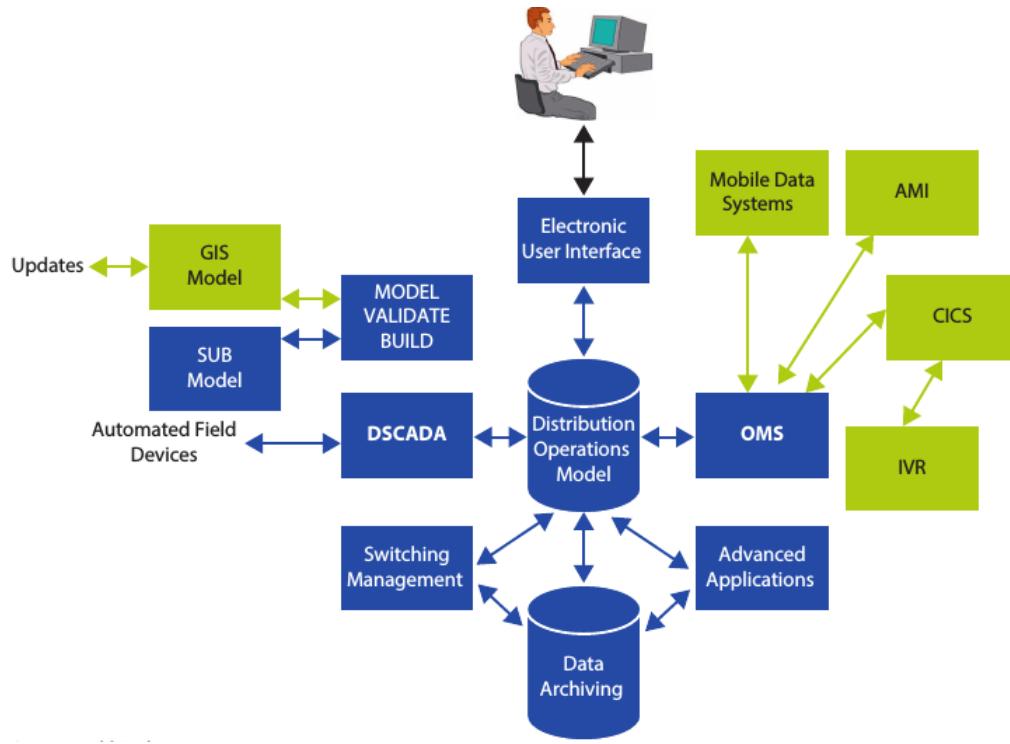
Un DMS integra il monitoraggio, l'analisi di rete e le applicazioni di controllo in un sistema decisionale, in grado di gestire le complessità del sistema



**Figura 3.12:** Configurazione ad alto livello di un Distribution Management System

di distribuzione, sia in condizioni stazionarie che di emergenza. Migliorare l'affidabilità e la qualità del servizio in termini di riduzione delle interruzioni. Inoltre, esso minimizza il tempo di interruzione, mantenendo i livelli di frequenza e di tensione accettabili. La figura 3.13 mostra l'architettura di un DMS.

Uno dei sistemi chiave nel sistema di distribuzione è l'*Outage Management System* (OMS), che assiste nella gestione del sistema di distribuzione elettrica nel rilevare interruzioni di alimentazione, determinare la posizione approssimativa della causa principale dell'interruzione, stimare il tempo di ripristino, valutare i danni e attività di restauro, e lo sviluppo di statistiche relative alle interruzioni. Il DMS deve essere in grado di rappresentare tutti gli aspetti della rete di distribuzione, inclusi conduttori, trasformatori, interruttori manuali o automatici e tutti gli altri dispositivi che operano nel sistema di distribuzione. Per poter effettuare politiche di bilanciamento del carico e gestire le variabilità energetiche nel sistema di distribuzione, un algoritmo *load-flow*, il quale permette di calcolare i parametri della rete in ogni punto della rete, deve essere eseguito su dati telemetrici, resi disponibili dai sistemi SCADA e la telemetria mediante la tecnologia AMI e l'OMS. Risulta cruciale, avendo un modello di rete complesso e quantità significative di dati telemetrici e calcolati, fornire strumenti per la visualizzazione dei risultati. Un DMS deve mostrare i dati della rete in viste geografiche, come mappe, schemi e diagrammi. La *Demand response* è una funzione chiave per



**Figura 3.13:** Architettura di un *Distribution Management System*

il DMS per ridurre i picchi di consumo energetico. Per modificare le abitudini dei consumatori, soprattutto nelle ore di punta, le società di servizi offrono diverse politiche di pagamento, incentivando i clienti ad usufruire dell'energia nelle ore notturne. Siccome questo approccio non fornisce sufficienti riduzioni, il DMS può aiutare in questa direzione riducendo la tensione erogata tra il 3 e 7%, grazie alle funzionalità dei volt/VAr, senza che i clienti ne siano consapevoli.

## Capitolo 4

# Smart Grid Cybersecurity

Il termine “**sicurezza**” si riferisce alle tecniche, ai processi e ai provvedimenti adottati per proteggere dati, reti di comunicazione, tecnologie informatiche e sistemi di calcolo da attacchi o da accessi non autorizzati.

L’approccio tradizionale prevede che la maggior parte delle risorse a disposizione per mettere in sicurezza il sistema si focalizzi sulle componenti più cruciali e che le protegga dalle minacce più grandi e più note; questo meccanismo fa sì che le componenti secondarie siano indifese e, inoltre, non protette da attacchi meno pericolosi. Tale approccio, però, risulta inefficiente nell’ambito della Smart Grid.

Per adattarsi al nuovo sistema, le organizzazioni promuovono un metodo più proattivo ed adattivo: il NIST, per esempio, ha recentemente pubblicato delle linee guida che consigliano uno spostamento verso il continuo monitoraggio e verso valutazioni real-time [2].

La sicurezza della Smart Grid, in relazione al suo sviluppo, è un tema fortemente discusso: tutti concordano nel sostenere che la Smart Grid dovrebbe avere un modello di sicurezza robusto; il problema è che ci si trova dinanzi a due sfide: come poter rispondere ai requisiti richiesti e come poter applicare le numerose alternative esistenti quando si cerca di rendere sicuro un ambiente complesso come la Smart Grid.

Quando si sente parlare di “nuova tecnologia”, di “interconnessione” e di “condivisione dei dati”, subito ci si focalizza sui benefici e sulle nuove funzionalità che tali concetti portano con loro. C’è da considerare, però, anche i nuovi rischi che queste nuove funzionalità introducono all’interno del sistema.

Per questo motivo, lo scopo della sicurezza è quello di garantire che le funzionalità del sistema operino correttamente e siano protette da abusi. È importante sottolineare, però, che non esistono applicazioni, reti o sistemi completamente sicuri e le Smart Grid non sono un'eccezione. Sebbene ogni componente della nuova rete elettrica porti con sé numerosi miglioramenti operazionali o funzionali, introduce anche nuove vulnerabilità e rischi addizionali che, se non propriamente gestiti, possono portare il sistema ad essere esposto ad attacchi di varia natura.

## 4.1 Un caso esemplare di attacco: Stuxnet

Stuxnet è un noto worm di 500 Kbyte scoperto nel 2010 da VirusBlokAda, una società di sicurezza bielorussa. Un *worm* è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus ma, a differenza di questo, si diffonde spedendosi direttamente agli altri computer, ad esempio tramite e-mail o in una rete. Stuxnet ha infettato il software di almeno 14 siti industriali in Iran, tra cui un impianto di arricchimento dell'uranio. Questo pezzo di codice maligno ha attaccato in tre fasi. In primo luogo attaccava macchine Windows e reti, replicandosi ripetutamente. Poi passava alla ricerca del software Siemens Step7 che è Windows-based e utilizzato per programmare sistemi di controllo industriale e infine comprometteva i programmable logic controller. La Figura 4.1 mostra il modo in cui opera Stuxnet.

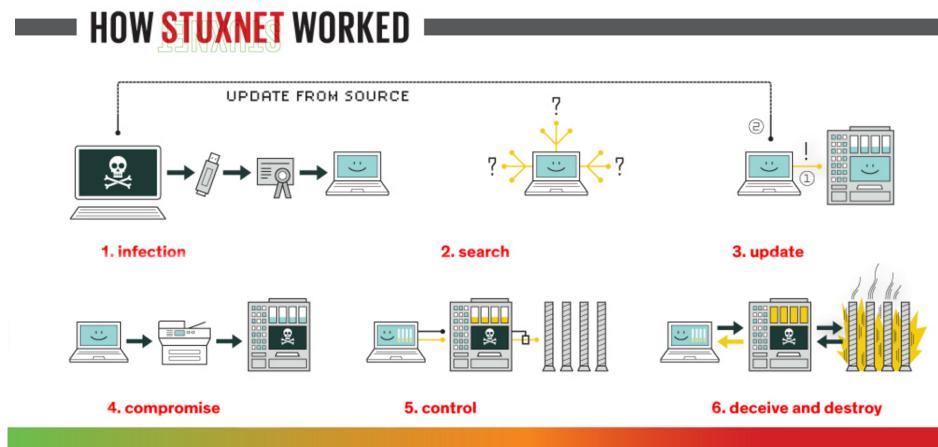
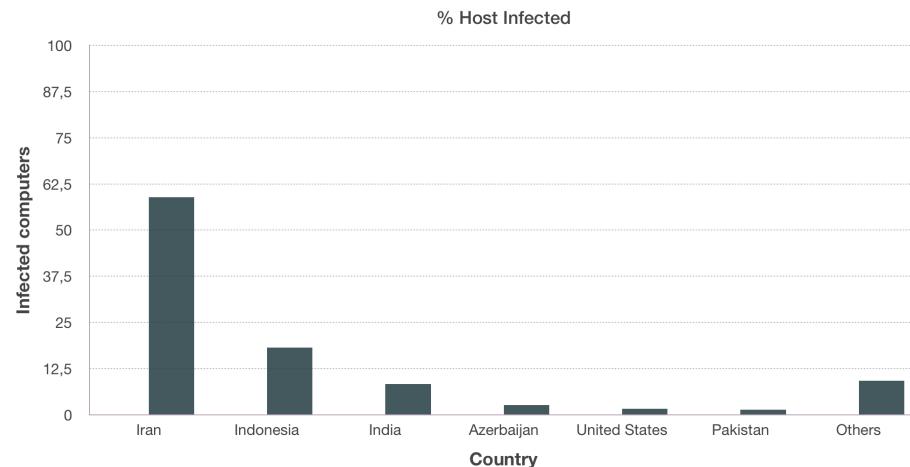


Figura 4.1

1. *Infection*: stuxnet entra nel sistema attraverso il collegamento di una penna USB e procede con l'infettare tutte le macchine su cui gira Microsoft Windows. Grazie all'utilizzo di un certificato digitale che lo fa sembrare affidabile, il worm è in grado di eludere sistemi di automated-detection;
2. *Search*: stuxnet verifica se una macchina è parte del sistema di controllo industriale creato da Siemens;
3. *Update*: se il sistema non è target, Stuxnet non fa niente; in caso contrario, il worm prova ad accedere ad Internet e scaricare una versione più recente di se stesso.
4. *Compromise*: il worm quindi compromette i controllori logici del sistema target, sfruttando la vulnerabilità “zero day”;
5. *Control*: in principio, si spiano le operazioni del sistema target. Successivamente, si usano le informazioni raccolte per prendere il controllo delle centrifughe, portandole al deterioramento;
6. *Deceive and Destroy*: fornisce false informazioni ai controllori, assicurando che questi ultimi non si accorgessero del problema fin quando non sarà troppo tardi per fare qualsiasi cosa.

Stuxnet è stato creato dal governo USA in collaborazione col governo Israeleiano e diffuso nella centrale iraniana di Natanz, allo scopo di sabotare la centrifuga della centrale tramite l'esecuzione di specifici comandi da inviarsi all'hardware di controllo industriale responsabile della velocità di rotazione delle turbine allo scopo di danneggiarle. Stuxnet si diffondeva velocemente sulle macchine che utilizzavano Windows, pur non essendo collegati ad Internet. Un operaio che inseriva una penna USB in una macchina infetta poteva propagare inconsapevolmente il worm sulla macchina che leggeva successivamente dalla stessa penna. Data la facile diffusione, gli esperti temevano che il malware poteva propagarsi anche su scala mondiale. L'azione di Stuxnet ha distrutto tra le 900 e le 1000 centrifughe (circa il 10% di quelle totali), nonostante l'intento di distruggere tutte. Uno studio da parte di Symantec relativo alla diffusione di Stuxnet mostra la percentuale di host infetti nei giorni successivi all'attacco (vedi Figura 4.2).



**Figura 4.2**

Gli autori di Stuxnet non sono stati identificati ma dalla sua scoperta gli ingegneri di sicurezza informatica stanno combattendo contro altre cyberarmi che sono state considerate varianti rispetto all'originale Stuxnet, fra queste Duqu e Flame. Mentre Stuxnet aveva lo scopo di “distruggere”, lo scopo di Flame era solo quello di “spiare”. Una volta che Flame aveva compromesso una macchina, era in grado di cercare delle keyword su file PDF top-secret e/o trasmettere parti del documento, il tutto senza essere scoperti. Inoltre, Flame non trasmetteva le informazioni raccolte tutte in una volta al suo server, in quanto il network manager poteva notare questo grande flusso improvviso di dati. L’idea, era quindi, quella di spedire i dati in blocchi di piccola dimensione per evitare di monopolizzare la larghezza di banda disponibile per troppo tempo. Siemens, dopo qualche tempo ha messo a disposizione uno strumento per il rilevamento e la rimozione di Stuxnet. Ha richiesto inoltre agli utenti di evitare l’utilizzo di penne USB non sicure all’interno della rete anche nel periodo successivo alla rimozione del virus. Uno strumento gratuito per la rimozione di Stuxnet è messo a disposizione da BitDefender sul suo sito dedicato [MalwareCity.com](http://MalwareCity.com).

## 4.2 Definire la sicurezza

La sicurezza tradizionale fa affidamento sulla cosiddetta **CIA triad**, che ne costituisce il cuore. La CIA triad comprende tre concetti: *confidentiality*, *integrity* ed *availability*.

Una concezione più moderna, e più adatta all'ambiente della Smart Grid, prevede l'utilizzo del **Parkerian hexad**, figura 4.3, proposto da Parker nel 2002. Tale modello propone, in aggiunta ai tre classici concetti precedenti, altri tre principi: *control* (o *possession*), *authenticity* ed *usability* (o *utility*). All'interno di questi sei pilastri, è possibile trovare tutti i problemi relativi alla Smart Grid [2].



Figura 4.3: Parkerian hexad

### 4.2.1 Confidentiality

Tale concetto porta con sé una serie di problemi e di preoccupazioni relative alla trasmissione e alla memorizzazione di dati ricavati dalle operazioni della Smart Grid. Questo tipo di dati, infatti, è spesso ritenuto *confidenziale*, nel senso che se fosse noto, avrebbe tutto il potenziale per causare danni alla sicurezza delle operazioni di tutto il sistema.

La confidenzialità, inoltre, può essere intesa anche in un'altra accezione: se i dati fossero noti alla concorrenza, per esempio, quest'ultima potrebbe trarre un notevole vantaggio in uno specifico settore o in tutto il mercato.

A tali fattori si aggiungono altre nuove problematiche legate alla *privacy del consumatore* e, quindi, dei suoi dati, che vengono fuori da meccanismi di metering quali l'AMI. Gli utenti, infatti, si aspettano che i consumi relativi

alle loro abitazioni private rimangano confidenziali; se così non fosse, la disponibilità di tali informazioni insieme alla capacità di fare data mining, avrebbe il potenziale per creare significative preoccupazioni sulla privacy.

I punti della Smart Grid che introducono rischi per la confidenzialità, sono costituiti da tutte le locazioni in cui sono memorizzati i dati e da tutti i meccanismi di trasmissione delle informazioni. Per quanto riguarda i dati memorizzati, questi potrebbero essere letti, copiati e distribuiti a soggetti diversi dai destinatari. Per quanto riguarda la trasmissione, invece, sia su reti private che su reti pubbliche come Internet, i dati potrebbero essere intercettati, copiati e distribuiti.

La soluzione a tali problemi risiede nelle funzioni di *cifratura dei dati* e di *controllo degli accessi*. Fornendo l'appropriato livello di cifratura delle informazioni, quest'ultime possono essere protette da chiunque non sia il diretto destinatario.

Il controllo degli accessi, prevede che i dati siano protetti da coloro che hanno l'autorizzazione per accedere al sistema ma che, allo stesso tempo, non hanno bisogno di tali dati per svolgere il loro lavoro.

#### 4.2.2 Integrity

L'integrity si riferisce all'abilità del sistema di evitare che le informazioni possano essere modificate da persone o da sistemi non autorizzati.

Se si rendono possibili meccanismi di modifica volontari quali la manipolazione dei dati, o anche involontari quali la loro corruzione, i sistemi riceveranno informazioni non accurate; a lungo andare ciò potrebbe avere un impatto negativo su tutte le operazioni e, in casi estremi, portare ad instabilità o compromettere del tutto la Smart Grid.

I punti della nuova rete elettrica che introducono rischi per l'integrità, sono tutti quei punti che consentono il passaggio dei dati da un sistema ad un altro. Pertanto, la sicurezza di tali meccanismi di transizione è importante, ma ancora più importante è come il sistema che riceve i dati possa assicurarsi della validità di quest'ultimi: se i dati subiscono manipolazioni mentre sono in viaggio tra i due sistemi, il ricevente potrebbe prendere decisioni basate su tali informazioni (che risultano essere errate); se, invece, i dati sono soggetti a corruzione durante la loro transizione, ci si potrebbe trovare di fronte ad un comportamento inaspettato del ricevente. In entrambi i casi, è evidente che l'integrità dei dati sia cruciale per assicurare la stabilità delle operazioni. Le risposte ai problemi di integrità, possono essere trovate nei meccanismi di *auditing*, di *authorization*, di *nonrepudiation*, e di *message-signing*, che saranno trattati in seguito (vedi Paragrafo 4.3).

### **4.2.3 Availability**

Molto spesso si tende ad utilizzare i concetti di reliability ed availability in maniera intercambiabile; in realtà, tali concetti hanno due significati diversi. La reliability, infatti, risponde alle seguenti domande: “quanto spesso fallisce il sistema?”, “quanto è elastico?”; l’availability, invece, indica la disponibilità del sistema e, quindi, la capacità di compiere il lavoro che gli è stato assegnato, *nel momento in cui se ne ha bisogno*.

Una porzione del sistema potrebbe essere attiva, eseguendo e processando i comandi, il 100% del tempo, e pertanto molto affidabile ma, se le performance non sono adeguate ai bisogni della rete e operazioni critiche vengono ritardate o mancano, non si può dire che il sistema sia disponibile.

I punti della Smart Grid che introducono rischi per la disponibilità sono troppi per poterli elencare: qualsiasi sistema, rete, dispositivo che gestisce le comunicazioni, processo per la gestione dei messaggi, e qualsiasi servizio invocato a qualsiasi livello applicativo e il suo sistema operativo sottostante sono un rischio per la disponibilità quando si trovano a dover gestire l’inoltro di un comando da un’estremità del sistema ad un’altra. Risolvere tale rischio è quasi tanto complicato quanto identificare le componenti del sistema che hanno il potenziale per impattare sulla disponibilità. La maggior parte delle soluzioni si affida a tecniche di ridondanza (clustering, bilanciamento del carico); il costo di tali metodologie, però, cresce in maniera proporzionale ai punti di fallimento che si identificano nel sistema.

### **4.2.4 Control**

La capacità di controllare le informazioni che necessitano protezione è essenziale per assicurare la loro integrità e la loro usabilità a lungo termine. Ciò ha diverse implicazioni per tutti quei sistemi che si affidano al meccanismo di controllo per scopi di vario genere (legali, normativi o commerciali): se le informazioni utilizzate per calcoli finanziari, come ad esempio i dati ricavati da meccanismi di metering, non fossero controllate, potrebbero compromettere tutti i sistemi che le forniscono e le trasmettono; di conseguenza, la provenienza di tali informazioni non potrebbe essere più garantita, portando una diminuzione dell'affidabilità di quest'ultime.

### **4.2.5 Authenticity**

Tale termine è spesso utilizzato per descrivere la certezza della provenienza. Il processo di verifica dell'autenticità è simile al processo utilizzato per verificare l'integrità: assicurarsi che la fonte dei dati e i dati stessi, siano autentici.

#### **4.2.6 Usability**

Questo aspetto del Parkerian hexad si preoccupa di assicurare che i dati siano utilizzabili.

Consideriamo un flusso di dati opportunamente cifrato: quest'ultimo garantisce la sicurezza delle informazioni, ma rende molto difficile far sì che queste ultime siano utili. L'usabilità è il fattore che, in definitiva, fornisce valore a livello aziendale e pertanto deve essere preservato e trattato come il requisito con più alta priorità.

#### **4.2.7 Analisi dei rischi**

Quale sarebbe il rischio per l'intero sistema Smart Grid se il sistema stesso, o qualsiasi sua componente, fosse compromessa? Tale rischio e il suo potenziale costo, guidano il lato economico delle decisioni per la progettazione dei meccanismi di sicurezza.

Come determinare l'accettazione dei rischi è, pertanto, una decisione legata al business e non una decisione tecnica. Un'azienda che sceglie di adottare una particolare metodologia per l'analisi dei rischi, avrà come input le proprie variabili che guidano le decisioni; tali variabili sono solitamente legate ad un rischio finanziario che l'azienda assume basandosi su una propria analisi competitiva del mercato o su condizioni regolamentari sotto le quali opera. Ci sono altre motivazioni, oltre a quelle finanziarie, che possono guidare l'accettazione dei rischi, come ad esempio fattori legislativi o legati a normative industriali: tali fattori possono portare ad adottare comportamenti che garantiscono la sicurezza anche in assenza di forti incentivi economici, per aggiungere ulteriori capacità di protezione del sistema.

È importante riconoscere che nessuna decisione riguardante la sicurezza dovrebbe essere presa senza prima aver considerato i rischi: "dove sono i rischi nel sistema?", "Quanto costerà un fallimento del sistema?", "Quanto costerà un fallimento della sicurezza del sistema?". Un'azienda dovrebbe essere in grado di capire i rischi e dovrebbe essere capace di fare scelte informate ed intelligenti su come risolvere tali problemi.

### **4.3 Building blocks**

Nel paragrafo precedente, sono state descritte una serie di potenziali minacce e funzioni di sicurezza che sono importanti per sistemi complessi ed interdipendenti come le Smart Grid.

In questo paragrafo, si esaminerà una possibile architettura di sicurezza che

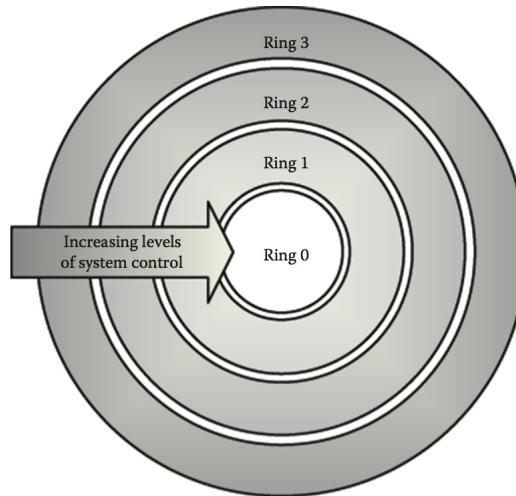
comprende tutte le funzioni precedentemente analizzate e che cerca di creare una struttura adatta a risolvere tutte le vulnerabilità descritte nel Paragrafo 4.2.

#### 4.3.1 Layered Security Model

Il concetto di modello di sicurezza *stratificato* non è un concetto nuovo: i sistemi operativi ed i microprocessori, infatti, lo utilizzano da tempo per controllare gli accessi a risorse privilegiate.

Immaginare tale concetto applicato ad una Smart Grid non è difficile.

Dalla figura 4.4 è possibile vedere che la struttura di tale modello è una struttura ad anello in cui la comunicazione tra gli strati del sistema è sicura. In generale, uno strato esterno non può avere libero accesso alle risorse presenti su uno strato più interno; inoltre, le richieste per le risorse non dovrebbero essere in grado di “saltare” i vari anelli: una richiesta che parte dal terzo anello, non dovrebbe poter accedere direttamente alla risorsa del primo, ma gli accessi sono regolati da opportune interfacce progettate in modo tale da assicurare la sicurezza di tutto il sistema.



**Figura 4.4:** *Layered security model*

Una Smart Grid ben progettata, dovrebbe essere in grado di offrire una simile protezione: i sistemi e le risorse poste agli estremi, come ad esempio dispositivi HAN (home area network) o smart meter, non dovrebbero avere la possibilità di accedere direttamente agli strati operativi (ring 0) della Smart Grid e, in più, i dati che passano per il sistema dovrebbero attraversare

opportune interfacce che ne assicurino l'integrità prima di procedere verso strati più interni.

Indipendentemente dal meccanismo specifico utilizzato per separare gli strati, ci sono diversi principi architetturali chiave che dovrebbero essere considerati nel percorso dei dati tra gli anelli: il primo e il più importante è assicurarsi che un fallimento in uno strato non abbia impatto né in uno strato più basso né in qualsiasi sistema dello stesso strato. Con il termine “impatto” ci si riferisce al fatto che nessuna tra confidentiality, integrity, o availability degli strati sottostanti debba essere colpita. È importante notare, però, che il viceversa non è vero: molto spesso danni ai livelli più bassi si propagano verso gli strati superiori e ciò è dovuto alla natura gerarchica del sistema.

Nelle prossime sezioni si analizzano le principali funzioni che costituiscono le componenti di sicurezza di alto livello che la Smart Grid dovrebbe avere per assicurare la protezione del sistema.

### 4.3.2 Authentication

L'autenticazione è il processo di verifica dell'identità di una persona o di un servizio che richiede l'accesso ad una risorsa.

Un meccanismo di autenticazione robusto potrebbe richiedere un certo numero di componenti, ognuna delle quali offre una particolare funzione di tutto il processo.

Spesso si tende a pensare all'autenticazione in termini di username e password, il che è corretto, ma non è solo questo: vi può essere autenticazione anche tra sistemi, processi o componenti hardware. Ci sono due componenti base per un meccanismo di autenticazione:

- *Identity Database*, contiene le informazioni necessarie per determinare chi e cosa sta tentando di accedere al sistema;
- *Identity Management System*, repository centrale di tutte le risorse che richiedono servizi di autenticazione.

### 4.3.3 Authorization

L'autorizzazione è il processo che verifica ciò che la persona o il servizio autenticato può fare all'interno del contesto del sistema.

Spesso i sistemi più semplici prevedono solo due modalità: “read-write” e “write-only”; i sistemi più complessi, invece, dovrebbero fornire regole di autorizzazione più specifiche, includendo la possibilità di indicare quali

campi si possono modificare e quali no, solo ad un certo orario del giorno e solamente se autenticati su specifiche macchine.

#### 4.3.4 Auditing

Il cuore di una qualsiasi analisi dei rischi è costituito dal programma di controllo. Senza revisioni periodiche dell'efficacia dei meccanismi di sicurezza che sono in atto nella Smart Grid, non ci sarebbe nessuna garanzia che il sistema sia sicuro.

Un buon programma di controllo dovrebbe essere eseguito periodicamente e dovrebbe testare quelle componenti che sono ritenute essenziali dall'azienda per mettere in sicurezza le operazioni del sistema. Tra i meccanismi più utili per eseguire tali revisioni, vi sono i seguenti:

- *Logging*: utilizzare file di log e memorizzare al loro interno tutti gli accessi critici al sistema e tutti i cambiamenti avvenuti;
- *Time Synchronization*: in un sistema unificato come una Smart Grid, è essenziale che tutti i dispositivi condividano lo stesso tempo.

#### 4.3.5 Key Management

È il processo che gestisce le emissioni delle chiavi per utenti, applicazioni e dispositivi. Tali chiavi sono utilizzate per stabilire l'identità e per assicurare l'integrità dei messaggi quando si inviano comandi tra sistemi.

Se consideriamo centinaia di chiavi, la loro gestione è relativamente semplice; ma quando ci si trova di fronte a centinaia di migliaia, o addirittura milioni, di dispositivi, la gestione diventa più complessa. Ogni chiave nel sistema sia relativa ad applicazioni, al sistema, ad un dispositivo o ad una persona, dovrebbe poter essere modificata o revocata su richiesta.

Per fare ciò, si utilizza la ben nota *Public Key Infrastructure* (PKI) [3].

#### 4.3.6 Message Integrity

Per trattare l'integrità dei messaggi, consideriamo tre meccanismi: signing, nonrepudiation ed encryption.

Per quanto riguarda il meccanismo di *signing*, quando un messaggio viene inviato da un sistema ad un altro, vi è prima un processo di autenticazione per dimostrare un'identità, seguito da un processo di autorizzazione, per verificare ciò che l'identità può fare. Una volta effettuati questi due controlli, può iniziare lo scambio di messaggi tra i due sistemi. Ci sono due motivazioni

principali per cui conviene firmare un messaggio: la prima è assicurare che il contenuto del messaggio non sia stato modificato durante la trasmissione tra i sistemi; la seconda è permettere di verificare l'identità del mittente indipendentemente dal processo di autenticazione.

La *nonrepudiation* entra in gioco quando il mittente di un messaggio necessita di essere riconosciuto (o confermato). Tale termine, infatti, si riferisce alla capacità di fornire una prova inconfutabile, ad una terza parte, di chi ha iniziato una certa azione nel sistema, anche se la persona in questione non sta partecipando al momento.

Il termine *encryption* porta con sé una serie di problematiche e di discussioni ampiamente trattate in letteratura, pertanto è impossibile riassumerlo in poche righe. Si può, però, riassumere il suo scopo: assicurarsi che un messaggio non possa essere letto da una persona o da un sistema che non sono i diretti destinatari dell'informazione. Ciò può essere messo in pratica attraverso innumerevoli algoritmi di cifratura, i quali fanno affidamento sul preservare l'integrità della chiave utilizzata per cifrare i dati; pertanto se tale chiave viene compromessa, lo sarà anche il messaggio.

#### 4.3.7 Network Integrity

Vi è un'infinità di modi per garantire l'integrità di rete, ognuno dei quali dipende dai dispositivi che la compongono e dalle loro necessità. Infatti, poiché ogni rete ha bisogni diversi, non vi è una configurazione che sia adatta a tutte quante.

Due dei meccanismi principali sono i seguenti:

- *Firewall*, utilizzato per restringere il traffico sulla rete ad uno specifico insieme di regole. Per esempio, potrebbe limitare il traffico a specifici canali di comunicazione tra un dispositivo e un insieme noto di altri dispositivi;
- *Rilevamento e prevenzione delle intrusioni*, messo in atto analizzando il traffico della rete per identificare specifici pattern di dati che corrispondono ad attacchi noti.

#### 4.3.8 System Integrity

- *Protezione da malware*, o più comunemente nota come protezione antivirus: ogni sistema dovrebbe avere una strategia che lo protegga da questo tipo di minacce; una protezione robusta, infatti, non solo

può evitare che file maliziosi vengano memorizzati, ma può anche far sì che si possa avvisare un operatore del ritrovamento del malware;

- *Gestione della configurazione del sistema:* le specifiche su come un sistema è configurato possono impattare enormemente sulla sua sicurezza. La gestione è necessaria per assicurarsi che il sistema non cambi rispetto alle basi di funzionamento stabilite;
- *Validazione e testing:* essenziali per garantire l'integrità del sistema. Prima di effettuare qualsiasi cambiamento e di distribuire nuovi sistemi, bisogna valutare le nuove modifiche e capire che impatto hanno sull'intero sistema. I cambiamenti devono essere testati per sicurezza e per garantire che non abbiano conseguenze negative sull'affidabilità di tutto il sistema.

## 4.4 Threats and Impacts

Analizziamo ora le minacce a cui una Smart Grid può essere sottoposta e l'impatto che esse hanno sull'infrastruttura, focalizzandoci principalmente su due attori del sistema: gli utenti e le società di servizi. Maggiori dettagli possono essere trovati in [1].

### 4.4.1 Consumers threats

Il fatto che gli utenti si trovino ad affrontare le minacce poste dalle nuove tecnologie non è un qualcosa di nuovo. Essi, infatti, si sono già trovati di fronte a problemi simili introdotti dai personal computer, dai cellulari e dall'attuale rete elettrica: mano che aumenta la dipendenza dalla tecnologia, aumenta anche la dipendenza dalla corrente elettrica per alimentare la tecnologia. Nel momento in cui ad una persona, però, viene sottratto un apparecchio tecnologico, riuscirà a sopravvivere anche senza; ma, se alla stessa persona viene negato l'accesso alla corrente elettrica, il danno che essa ne subirà sarà sicuramente maggiore.

Gli utenti di una Smart Grid possono essere sottoposti ad una serie di pericoli di varia natura, partendo dalla privacy fino ad arrivare a situazioni che rischiano di mettere in pericolo la loro stessa vita:

- *Minacce naturali.* In accordo al *NERC Disturbance Analysis Working Group* (DAWG) [1], i disastri metereologici e naturali (quali venti, tempeste, tornadi, terremoti, ecc.) sono la causa di più del 50% dei disturbi del sistema elettrico e, in particolare, degli utenti. La Smart

Grid si propone di affrontare tali minacce ma è importante notare che eliminare totalmente i danni causati dai frequenti disastri atmosferici e naturali non è fattibile in maniera semplice nel prossimo futuro. Poichè non si può fermare il verificarsi di tali calamità, i programmi di aiuto in caso di incidenti continueranno ad essere di critica importanza, in risposta ai fenomeni naturali distruttivi;

- *Minacce provenienti da singoli o da organizzazioni.* L'AMI e gli altri componenti della Smart Grid, permettono agli operatori di amministrare da remoto i dispositivi situati nelle case degli utenti; in più gli *smart device*, permettono ai consumatori e alle società di servizi di controllare in maniera remota anche i consumi energetici. Numerose sono le motivazioni che possono spingere persone e organizzazioni ad abusare delle funzionalità di questi dispositivi; la possibilità di ottenere il controllo di tali componenti, può portare ad attaccare la Smart Grid e, quindi, i suoi utenti. Varie possono essere le figure coinvolte in tali situazioni:
  - *Ladri e stalker.* Uno degli obiettivi della Smart Grid, come detto nei capitoli precedenti, è quello di rendere gli utenti più consapevoli dei propri consumi e, in questo modo, aiutarli a cambiare i propri comportamenti energetici allo scopo di ridurre i costi delle bollette. Ma, l'accesso a tali informazioni, può far sì che altre persone possano compiere azioni maliziose: supponiamo che un ladro riesca a monitorare il consumo elettrico di una certa abitazione; tale persona può rendersi conto, in base agli orari di attività e inattività della corrente e ai consumi in ciascun orario, delle abitudini quotidiane degli inquilini di tale abitazione. Se riesce a monitorare questi comportamenti per un periodo di tempo ampio, riuscirà ad individuare quando le persone non sono in casa e potrà, quindi, compiere un furto all'interno dell'abitazione, oppure, riuscendo ad individuare i momenti di utilizzo di energia settimanali e giornalieri, potrà utilizzare la loro corrente per i suoi scopi. Uno stalker, analogamente, analizzando i consumi di un veicolo elettrico di una determinata donna, può essere in grado di individuare i suoi spostamenti e le sue abitudini;
  - *Hacker.* I motivi per “hackerare” una Smart Grid possono essere vari. Tra i principali ci sono sicuramente motivi non maliziosi: una persona potrebbe essere semplicemente curiosa di capire come funziona un determinato dispositivo, oppure potrebbe utilizzare la

Smart Grid come un mezzo per ottenere gratificazione personale o per egoismo; sebbene tali motivazioni non siano maliziose, possono comunque arrecare danno all'infrastruttura. Un'altra causa che spinge ad hackerare la rete potrebbe essere un semplice test per verificare la robustezza del programma di sicurezza e per indentificare, quindi, le potenziali vulnerabilità. Le persone che effettuano tali test, ovviamente fanno il possibile per evitare che il loro lavoro abbia conseguenze negative sul sistema elettrico. In aggiunta a tali motivazioni, però, esistono giustificazioni per l'attacco della rete tutt'altro che non maliziose: guadagno economico, desiderio di potere, sete di vendetta e volontà di distruggere il sistema;

- *Terrorismo.* A prescindere dalle motivazioni e dalla categoria di attacco, le Smart Grid sono considerate potenziali target per i terroristi. Attaccando la rete elettrica, i terroristi potrebbero colpire enormi quantità di persone e, come risultato, spostare verso di loro un'attenzione massiva;
- *Governo.* Il governo è sia un consumatore, che una minaccia per i consumatori: dai semafori stradali ai laboratori di ricerca, le agenzie governative consumano una grande quantità di energia e, pertanto, sono anche loro suscettibili ai pericoli visti in questo paragrafo. Nonostante ciò, il governo può anche rappresentare una minaccia per gli utenti, in particolare su due aspetti: la guerra e le attività illegali. Per quanto riguarda la guerra, è normale pensare che paralizzare un'infrastruttura critica nazionale come la rete elettrica possa ostacolare le capacità della nazione stessa di operare; per questo motivo la Smart Grid è uno dei target durante la guerra. Per quanto riguarda le attività illegali, come ad esempio la produzione di droga, spesso queste fanno uso di energia elettrica per poter andare avanti. Utilizzando una rete intelligente, è possibile, monitorando i consumi di tali attività, riuscire ad individuare le operazioni illegali che effettuano, localizzare dove esse avvengono e arrestare i colpevoli;
- *Società di servizi.* Tali società, o più precisamente i suoi agenti, possono essere una minaccia per i consumatori attraverso azioni intenzionali e non intenzionali. A partire dagli incidenti fino alle minacce interne, tali persone possono continuare ad essere la causa di interruzioni di corrente, *privacy leak*, fatturazioni improprie e altro.

## **Impatti**

Le minacce e i problemi visti nel paragrafo precedente, possono comportare una serie di danni e di conseguenze differenti; i principali sono:

- *Impatto sui consumatori.* In questo caso è la privacy che, in particolare, subisce le maggiori conseguenze: nell'implementazione dell'AMI, gli smart meter collezionano in maniera autonoma un grande ammontare di dati e lo trasportano alle società di servizi, al cliente e ai fornitori di servizi di terze parti. Tali dati includono anche informazioni personali identificative che possono, quindi, compromettere la privacy del cliente. Pertanto un tale dettaglio nel resoconto dei consumi di una persona, può far sì che altre persone e organizzazioni riescano a tracciare un profilo delle abitudini. Se tali informazioni giungono ad un hacker, come detto in precedenza, potrà utilizzarle per scopi maliziosi; se, invece, giungono nelle mani di servizi di terze parti affidabili, quali agenzie pubblicitarie, esse ne potranno fare un uso più legittimo;
- *Impatto sull'availability.* Al di là di tutte le nuove funzionalità e delle nuove caratteristiche introdotte, l'obiettivo principale di una Smart Grid rimane quello di rendere la corrente sempre disponibile ai clienti. Pertanto, la maggior parte dei pericoli analizzati precedentemente, può incidere sulla disponibilità di energia. Gli impatti che ciò può avere sul sistema variano dall'alterare i termostati che regolano riscaldamento e aria condizionata, fino a limitare, o addirittura impedire, servizi di emergenza;
- *Impatto finanziario.* I pericoli sopra descritti possono avere serie conseguenze sulle finanze dei clienti: corrompere i dati che nascono dagli smart meter, può portare al calcolo di bollette non accurate che, di conseguenza, comporta un pagamento da parte degli utenti maggiore del loro effettivo consumo.

### **4.4.2 Utility companies threats**

Alcuni dei pericoli a cui le società di servizi possono essere esposte sono simili alle minacce riguardanti i consumatori, altri sono unici, ma la cosa certa è che attaccare tali compagnie, le aziende e i governi avrà un impatto più grande degli attacchi contro gli utenti.

In questo paragrafo, verranno analizzate le minacce che impattano sulle componenti della *CIA triad* relative alle società, mostrando per ognuna di esse uno scenario ipotetico e le conseguenze.

## Confidentiality

Come detto nel paragrafo 4.2, si soddisfa il requisito di *confidentiality* nel momento in cui si proteggono i dati da accessi non autorizzati: la perdita tale requisito arreca un grande danno ai consumatori, ma rende anche le società di servizi un *target* molto appetibile per gli hacker, in quanto tali società effettuano aggregazione di informazioni personali. Gli attacchi possibili riguardano i seguenti ambiti:

- *Privacy del consumatore.* Le società di servizi raccolgono e memorizzano varie informazioni personali dei clienti (e.g. nome, indirizzo, dati relativi ai consumi), informazioni che ci si aspetta restino confidenziali. Fare breccia nella confidenzialità per accedere a tali dati è l'obiettivo di molti hacker; tuttavia, non sono solo loro a poter desiderare tali informazioni. Le nuove tecnologie introdotte dalla Smart Grid permettono agli utenti di interagire più frequentemente con le loro società di servizi attraverso Internet e le *Web application*. Le forze dell'ordine potrebbero trarre vantaggio da tali tecnologie e, quindi, ricavarne i dati necessari per eseguire il loro lavoro (ad esempio fare delle indagini), allo stesso modo in cui utilizzano le tecnologie cellulari e il GPS. Consideriamo, ora, due possibili scenari:
  - *Personally identifiable information (PII).* Consideriamo una società di servizi e un hacker in grado di compromettere il suo database di clienti; tale hacker potrebbe operare sfruttando una vulnerabilità *Structured Query Language* (SQL) all'interno del sito Web della società utilizzato dai clienti per gestire i loro account, monitorare i loro consumi ed effettuare pagamenti. Tale operazione renderebbe possibile agli hacker ottenere le PII di tutti gli utenti (e.g. dati personali, numero di carta di credito), i quali potrebbero venderle ad altre società interessate.
  - *Consumption data.* Nel sottoparagrafo precedente, abbiamo visto come i governi (in particolare le forze dell'ordine che agiscono per loro) possono utilizzare le informazioni circa i consumi degli utenti di una società di servizi per determinare se stanno producendo droga; essi, però, possono utilizzarle anche per identificare la locazione dei sospettati durante i crimini. Le forze dell'ordine potrebbero, per esempio, analizzare lo storico dei consumi dei sospettati per determinare la probabilità che questi ultimi fossero in casa mentre avveniva il crimine. Le reazioni dei clienti al presunto abuso d'utilizzo delle loro informazioni personali potrebbero, però,

causare dei problemi alla società di servizi e, pertanto, portare dei rallentamenti nell'adozione delle nuove tecnologie della Smart Grid.

- *Informazioni proprietarie.* Un esempio di informazione proprietaria è sicuramente un *segreto aziendale*, il tipo di *target* che attrae gli hacker che pensano di poterlo vendere alle aziende competitive, ai governi o ai gruppi terroristi.

Consideriamo un possibile scenario: supponiamo che ci sia un governo straniero stanco di particolari sanzioni riguardanti l'energia. Esso potrebbe ingaggiare degli hacker e ottenere accesso ad alcuni segreti che gli permettono di aumentare le sue capacità di generazione dell'energia nonostante le sanzioni imposte. Ciò può essere realizzato attraverso l'utilizzo di un *malware* che si installa sui sistemi degli impiegati delle società *target* nel momento in cui visitano il sito Web delle loro aziende. In questo modo gli hacker ottengono l'accesso alla rete interna e riescono a rubare i segreti di cui hanno bisogno. Un attacco del genere ad una società di servizi fa sì che esse perdano il loro vantaggio competitivo, andando incontro ad un calo notevole dei profitti.

## Integrity

Un sistema risponde al requisito di integrità nel momento in cui le informazioni in esso contenute sono protette da modifiche non autorizzate. Una perdita di tale garanzia ha l'impatto più forte sulle società di servizi; tali minacce possono riguardare:

- *Frode.* I clienti dell'azienda fornitrice di servizi, possono accedere agli smart meter installati nelle loro case o nelle loro società. Sebbene sia doveroso implementare meccanismi di antimanomissione, potrebbe essere facile reperire su Internet informazioni su come manomettere tali dispositivi; una volta che tali informazioni sono pubbliche, sono facilmente accessibili alle masse (dagli hacker ai semplici curiosi), le quali avranno le conoscenze giuste per truffare la propria società di servizi. Consideriamo due possibili scenari:
  - *Service theft.* Consideriamo un cliente in grado di hackerare i suoi smart meter e di modificare, quindi, le informazioni circa i suoi consumi che vengono spedite alla società. Ciò è realizzabile attraverso l'installazione all'interno del *meter* di un driver relativo ad un dispositivo di rete che permette l'esecuzione remota di

codice. Tale comportamento malevolo rende i consumatori capaci di sottostimare i propri consumi e, quindi, di ottenere bollette più basse a totale insaputa delle società di servizi.

- *Net metering.* Consideriamo, ora, uno scenario inverso al precedente: un cliente capace di modificare le informazioni relative alla sua produzione di energia che verranno inviate alla società di servizi. Una persona può facilmente manomettere tali dati semplicemente installando all'interno del suo device un programma scaricato da Internet. È facile immaginare le conseguenze di tale atto: i consumatori sono capaci di sovrastimare la propria produzione di energia che forniscono all'azienda e di ricevere, quindi, compensi maggiori.
- *Manipolazione dei dati dei sensori.* Gli smart meter includono i sensori che permettono alle società di servizi di compiere una miriade di operazioni (e.g. analisi forense, ristabilimento dell'energia, monitoraggio); tuttavia, se si compromette l'integrità dei dati raccolti, il risultato sarà disastroso. Un possibile scenario in questo caso è il seguente: consideriamo una persona molto curiosa di sapere come funziona l'intero sistema Smart Grid, e consideriamola anche capace di mettere mano all'interno del proprio smart meter e di creare un programma per falsificare i dati inviati dal suo intero vicinato. Supponiamo che tale utente, sfruttando il fatto che i dati sono inviati in maniera non cifrata, riesca a manomettere le informazioni dei vicini, ad analizzare il traffico di rete (ottenendo gli indirizzi IP dei device) e ad indicare alla società di servizi che il suo intero vicinato è senza corrente elettrica. Quest'ultima, manda una squadra sul posto per investigare ma, arrivati lì, i tecnici si rendono conto che in realtà non c'è nessun guasto. L'azienda, pertanto, sottostima il problema e dà semplicemente la colpa ad un malfunzionamento del sistema. L'utente malevolo, nel frattempo, può ripetere il processo più volte senza essere scoperto, costringendo la società a sprecare tempo e denaro.

## Availability

Si soddisfa il requisito di *availability* nel momento in cui il servizio offerto dalle società di servizi è protetto da interruzioni non autorizzate. Una negligenza in tale requisito comporta una serie di problemi sia per la società, sia per coloro che fanno affidamento su di essa (clienti, organizzazioni, aziende e governi). Gli obiettivi di questo tipo di attacco possono essere diversi:

- *Clienti.* In tal caso gli attacchi riguardano le abitazioni, e possono provenire principalmente da persone conosciute ai clienti stessi. Consideriamo il seguente scenario: supponiamo ci sia un cliente che ha installato all'interno della propria abitazione uno smart meter e supponiamo che tale persona abbia un nemico; consideriamo, poi, che quest'ultimo sia capace di manomettere il dispositivo per creare un blackout locale a quella casa. L'attaccante potrebbe realizzare ciò attraverso la configurazione di default del router Wireless dell'abitazione, in particolare riuscendo ad accedere alla rete Wireless e connettendosi al *front-end* Web dello smart meter. Una volta ottenuto l'accesso, si potrebbe cambiare la password di default e spegnere la corrente in casa. Le cause di tale attacco malevolo, ovviamente, portano l'inquilino a rimanere senza corrente e senza possibilità di ripristinarla.
- *Organizzazioni.* Sebbene gli attacchi indirizzati agli utenti e alle loro abitazioni molto spesso possono essere considerati non malevoli, gli attacchi diretti alle organizzazioni sono da ritenersi quasi sempre maliiziosi e con secondi fini (ad esempio, l'estorsione). Consideriamo i seguenti scenari:
  - Supponiamo ci sia un hacker che, per prestigio personale e per acquisire maggiore notorietà, vuole danneggiare la più grande società di servizi del suo paese e causare un'interruzione di corrente così importante da farne parlare i notiziari. A tale scopo, l'attaccante inizia a studiare l'infrastruttura della Smart Grid e riesce a trovare il suo obiettivo; sfruttando, poi, le debolezze della sicurezza fisica della postazione di gestione della società di servizi, riesce ad ottenere accesso alla rete interna. Da qui, l'hacker può eseguire un *Denial-of-Service attack* contro tutte le stazioni di gestione. Come pianificato in anticipo dall'hacker stesso, le unità cadono nel momento in cui la società raccoglie i dati di utilizzo dei clienti; pertanto il processo di emissione delle bollette subisce dei ritardi e i clienti vengono avvisati attraverso i notiziari.
  - Un ex dipendente di una stazione di servizio locale vuole vendicarsi del suo recente licenziamento. Supponiamo che, durante il suo impiego, era responsabile del pagamento delle bollette della stazione e consideriamolo anche esperto di computer: egli è in grado di interrompere l'alimentazione di corrente al suo ex datore di lavoro. Per fare ciò, può utilizzare la *Web application* messa a disposizione dalla società di servizi per i pagamenti che permette,

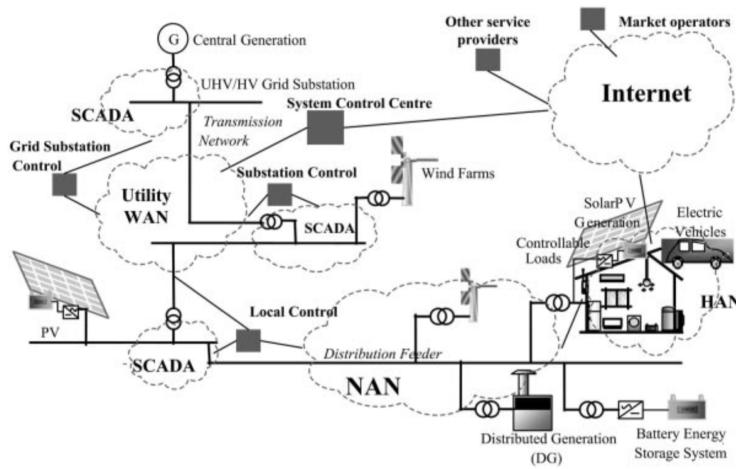
inoltre, ai clienti di chiudere i loro account senza verifiche addizionali. Pertanto l'ex dipendente, semplicemente utilizzando login e password che utilizzava quando lavorava ancora lì, fa richiesta per cancellare l'account. Un tale attacco fa sì che la stazione resti senza corrente nel giro di una settimana e che la società di servizi contemporaneamente perda dei guadagni.

- *Manipolazione del mercato.* Il guadagno economico continua ad essere uno dei principali motori dietro gli attacchi informatici: gli hacker, infatti, sono interessati a scoprire le debolezze della Smart Grid soprattutto per ricevere un compenso in denaro o, nei casi peggiori, per estorcere denaro alle società. Consideriamo il seguente scenario: gli hacker, individui spinti da tornaconti finanziari, mettono le loro abilità a servizio di gruppi i cui membri non sono tecnici del mestiere. L'unione di queste persone con un team di esperti di mercati finanziari, può facilmente sfruttare l'adozione delle nuove tecnologie portate dalla Smart Grid per ottenere significative quantità di denaro in un breve periodo di tempo.

# Capitolo 5

## Standard e tecnologie

L'infrastruttura di comunicazione consiste tipicamente di sistemi SCADA con canali di comunicazione dedicati da e verso il centro di controllo del sistema e di una Wide Area Network (WAN). I sistemi SCADA collegano tutte le principali strutture operative del sistema mentre la WAN è prevalentemente usata per azioni di mercato. Uno sviluppo importante per la Smart Grid (vedi Figura 5.1) è quello di estendere la comunicazione a tutto il sistema di distribuzione e di stabilire una comunicazione bidirezionale con i clienti attraverso le Neighbourhood Area Network (NANs) che coprono le zone servite dalle sottostazioni di distribuzione. I clienti avranno la necessità di una Home Area Network (HAN) a cui saranno connessi gli smart device.



**Figura 5.1:** Una possibile infrastruttura di comunicazione per la Smart Grid

Le sotto-reti di comunicazione che andranno a comporre la Smart Grid utilizzano diverse tecnologie (vedi Figura 5.2) e di particolare interesse è il modo in cui quest'ultime possono essere integrate in maniera efficace. Le Smart Grid possono utilizzare diverse tecnologie di comunicazione wired e wireless (cellulare, satellitare, microwave, WiMAX etc.). Le tecnologie di comunicazione wireless short range, come WiFi e ZigBee, sono tipicamente utilizzate nelle HAN. In questo capitolo, saranno descritte alcune tecnologie di comunicazione associate ai livelli inferiori del modello di riferimento ISO/OSI.

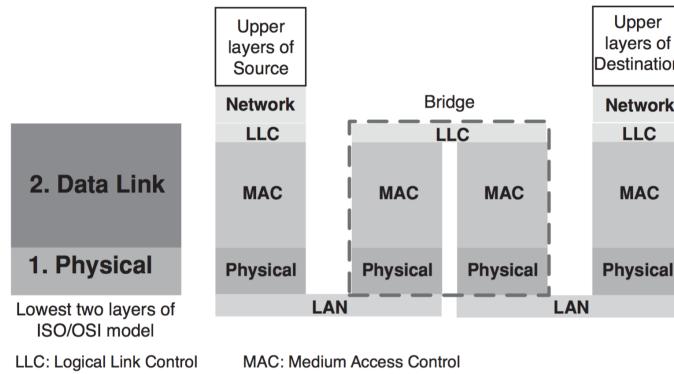
Sub-network	Communication technologies
HAN	Ethernet, Wireless Ethernet, Power Line Carrier (PLC), Broadband over Power Line (BPL), ZigBee
NAN	PLC, BPL, Metro Ethernet, Digital Subscriber Line (DSL), EDGE, High Speed Packet Access (HSPA), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE), WiMax, Frame Relay
WAN	Multi Protocol Label Switching (MPLS), WiMax, LTE, Frame Relay

**Figura 5.2:** *Tecnologie usate nelle differenti sottoreti*

## 5.1 Tecnologie di comunicazione

### 5.1.1 IEEE 802

IEEE 802 è una famiglia di standard sviluppati per il supporto alle reti locali (LAN). Facendo riferimento alla Smart Grid, tali standard sono applicabili alle reti LAN in sistemi SCADA, NAN per le reti di distribuzione e HAN nei locali dei clienti. La Figura 5.3 mostra come l'architettura IEEE 802 è incentrata sui due livelli inferiori del modello ISO/OSI. Nella Figura in esame è mostrata la connessione di due LAN attraverso l'utilizzo di un Bridge. Tale connessione è comune in molte organizzazioni che hanno più LAN. Un pacchetto dalla sorgente va nel sottostrato Logical Link Control (LLC) che funge da interfaccia tra il livello di rete e il sottostrato MAC. LLC è definito da IEEE 802.2 e fornisce i meccanismi di controllo del flusso, multiplexing e di controllo degli errori. Il pacchetto passa poi nel sottostrato MAC in cui un header ed un trailer vengono aggiunti al pacchetto (a seconda della LAN cui il pacchetto entra). Poi si passa attraverso il livello fisico e nel canale di comunicazione e si raggiunge il Bridge. A livello MAC del Bridge, header e trailer vengono rimossi, recuperando così il pacchetto originale che passa al sottostrato LLC del Bridge. Successivamente il pacchetto viene elaborato

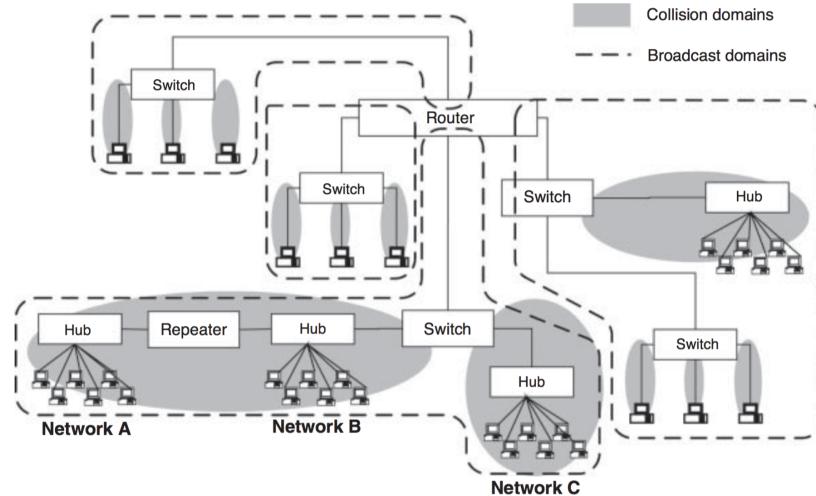


**Figura 5.3: Architettura IEEE 802**

dal sottostrato MAC (aggiungendo header e trailer appropriati) in base alla LAN a cui si trasmette. L'utilizzo del Bridge è essenziale in quanto LAN diverse utilizzano dimensioni del frame e velocità (e.g. IEEE 802.3 utilizza un frame di 1500 byte, mentre IEEE 802.4 ne utilizza uno di 8191 byte[21]).

### Ethernet

Ethernet è diventata la tecnologia di rete più utilizzata per le LAN cablate grazie alla sua semplicità, affidabilità, facilità di manutenzione e la capacità di integrare nuove tecnologie. Essa ha un basso costo di installazione ed è facile farne l'upgrade. Si tratta di una tecnologia di comunicazione frame-based che si basa sullo standard IEEE 802.3. Ethernet utilizza un mezzo condiviso che può portare a collisioni tra i frame trasmessi dai vari host. Il problema delle collisioni è gestito da un protocollo chiamato Carrier Sense Multiple Access/Collision Detect (CSMA/CD). Un set di host connessi ad una rete in modo tale che la trasmissione simultanea da due host nel set porta a collisioni, crea un *dominio di collisione*. Inoltre, le LAN Ethernet trasportano anche frame di broadcast il cui dominio raggiungibile è chiamato *dominio di broadcast*. Le prestazioni della rete, in caso di traffico, sono influenzate dal modo in cui i domini di collisione e di broadcast sono posizionati e pertanto l'idea è quella di isolarli per aumentare le prestazioni della rete. La Figura 5.4 mostra tali domini su una tipica LAN Ethernet.



**Figura 5.4:** LAN Ethernet

I Bridge limitano i domini di collisione mentre i Router limitano entrambi i domini. In Figura 5.4 è mostrato come un pacchetto inviato dalla rete A può collidere con uno della rete B, ma non con uno inviato da C.

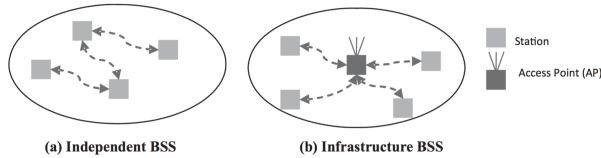
## Wireless

IEEE 802.11 definisce un insieme di standard per le Wireless LAN (WLAN). L’interoperabilità dei dispositivi IEEE 802.11 è certificata dalla Wi-Fi Alliance. Una LAN Wireless è costituita dai seguenti componenti:

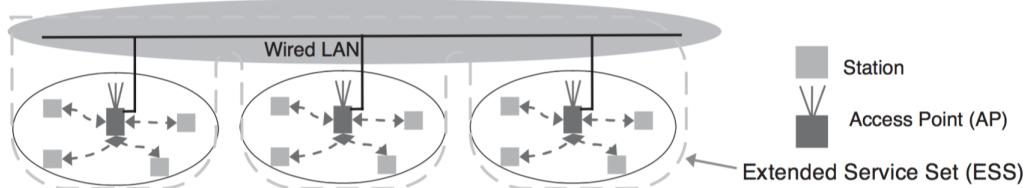
- *Station*: descrive qualsiasi dispositivo che comunica tramite una rete WLAN, ad esempio, un computer portatile, o cellulari che supportano WiFi. Nelle reti Ad-hoc questi dispositivi possono comunicare tra loro, creando una rete mesh (vedi Figura 5.5a). L’insieme di station che formano la rete Ad-hoc è chiamato Independent Basic Service Set (IBSS);
- *Access Point (AP)*: consente ad una stazione di comunicare con un’altra facendo da tramite. Necessita il doppio della larghezza di banda necessaria se la stessa comunicazione avvenisse direttamente tra le stazioni comunicanti. Gli AP rendono il sistema scalabile e consentono la connessione cablata con altre reti. In presenza di AP (vedi Figura 5.5b) l’insieme delle station è chiamato Infrastructure BSS;

- *Distribution System*: interconnette Infrastructure BSS attraverso gli AP, come mostrato nella Figura 5.6. Facilita la comunicazione tra gli AP, l'inoltro del traffico da un BSS ad un altro ed il movimento di mobile station tra BSS. Un insieme di Infrastructure BSS è chiamato Extended Service Set (ESS).

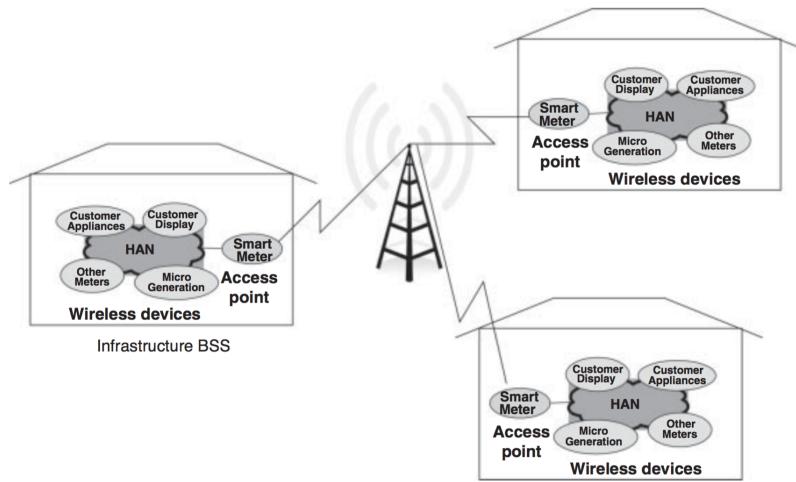
La famiglia di reti LAN Wireless 802.11 utilizza il protocollo CSMA/CA per l'accesso al mezzo trasmissivo. Sono noti vari standard identificati da 802.11a/b/g/n/ac con variazioni a livello fisico. Una tipica applicazione di 802.11 nelle Smart Grid è mostrata in Figura 5.7.



**Figura 5.5:** Architetture BSS di WLAN



**Figura 5.6:** *Distribution System*



**Figura 5.7:** Applicazione di WLAN 802.11 in una Smart Grid

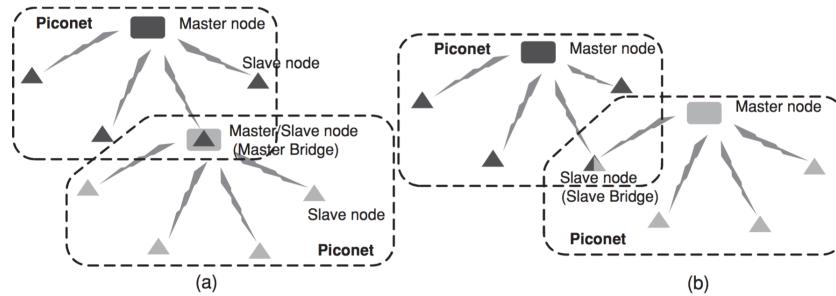
### Bluetooth

Bluetooth, definito dallo standard IEEE 802.15.1, è una tecnologia LAN wireless progettata per collegare i dispositivi mobili o fissi con bassi consumi, un corto raggio d'azione (fino a 100 metri di copertura) e un basso costo di produzione per i dispositivi compatibili. Bluetooth definisce due architetture di rete denominate Piconet e Scatternet. La Piconet è costituita da un dispositivo *Master* e fino a sette dispositivi *Slave*. Altri dispositivi possono sincronizzarsi col Master ma non possono partecipare alla comunicazione. Si dice che tali dispositivi sono in un parked state. Un device in parked state può passare in active state se il numero di Slave della Piconet è inferiore a sette. Le Piconet possono essere interconnesse attraverso un Bridge che può essere Slave per una Piconet e Master per un'altra oppure Slave per due Piconet che sono interconnesse come in Figura 5.8a e 5.8b. Un insieme di Piconet forma una Scatternet.

Per il trasferimento dei dati è possibile creare due tipi di collegamenti bluetooth:

- Synchronous Connection Orientated (SCO) link
- Asynchronous Connectionless Link (ACL)

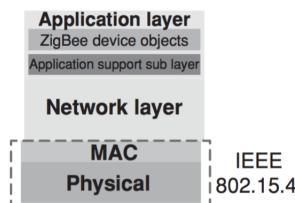
SCO è utilizzato quando la consegna tempestiva è più importante della consegna senza errori mentre ACL è utilizzato nel caso inverso.



**Figura 5.8: Piconet e Scatternet**

### ZigBee and 6LoWPAN

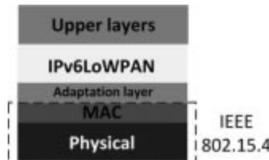
ZigBee e 6LoWPAN sono due tecnologie di comunicazione basate su IEEE 802.15.4 per Wireless Personal Area Network (WPAN) dato il basso consumo, l'alta flessibilità ed i bassi costi. L'architettura protocollare di un device ZigBee è mostrata nella Figura 5.9 in cui i due strati inferiori sono definiti da IEEE 802.15.4. Application Support e Network Layer per la rete ZigBee sono definiti dalla ZigBee Alliance[22].



**Figura 5.9: Architettura Protocollare di ZigBee**

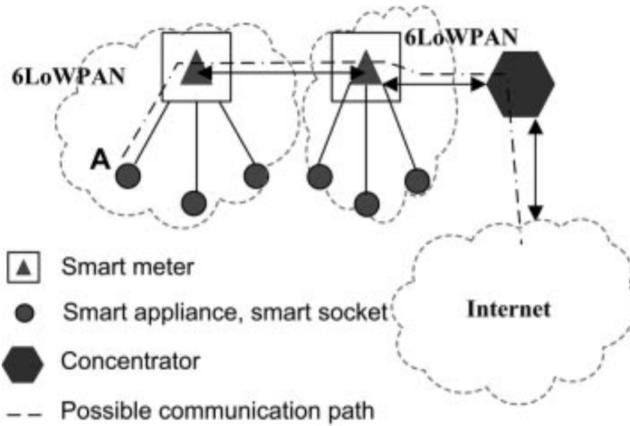
Un device ZigBee può essere un Full Function Device (FFD) o un Reduced Function Device (RFD). Una rete avrà almeno un FFD, che fungerà da coordinatore della WPAN. Il FFD può funzionare in tre modalità: coordinatore, router o device. Un RFD può funzionare solo come device. Un FFD può interagire sia con un altro FFD che con un RFD, mentre un RFD può parlare solo con un FFD. La tecnologia ZigBee è considerata come una buona opzione per il metering e per la gestione dell'energia ideale in implementazioni Smart Grid data la semplicità, mobilità, robustezza e i bassi costi di sviluppo. Offre anche programmi di pricing e monitoraggio del sistema real-time. ZigBee presenta però alcuni vincoli relativi alle basse capacità di elaborazione, alla piccola dimensione della memoria e alle interferenze tra i vari apparecchi che condividono lo stesso mezzo trasmissivo. Tali problematiche, in condizioni di rumore, aumentano la possibilità di danneggiare il canale di comunicazione a causa delle interferenze. Schemi di interference detection/avoidance e protocolli di routing energy-efficient estendono il tempo di vita della rete e forniscono una performance di rete affidabile e ad alta efficienza dal punto di vista energetico.

6LoWPAN è un protocollo che consente l'invio e la ricezione di pacchetti IPv6 nelle reti basate su IEEE 802.15.4. In tale protocollo è stato inserito un Adaptation Layer (vedi Figura 5.10) per il collegamento tra lo strato MAC e il Network Layer IPv6.



**Figura 5.10:** Architettura di rete 6LoWPAN

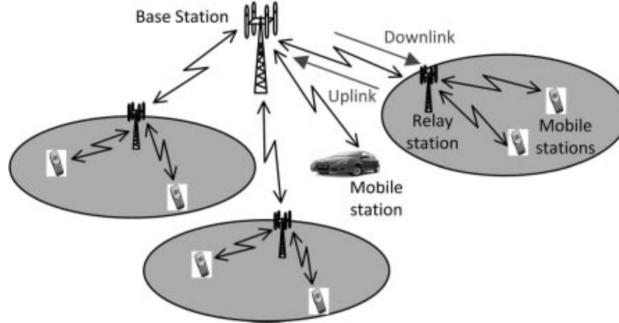
Quando un RFD in una 6LoWPAN vuole inviare un pacchetto di dati ad un dispositivo che si trova al di fuori del dominio 6LoWPAN, invia inizialmente il pacchetto ad un FFD nella stessa WPAN. Il FFD che agisce da router, inoltrerà il pacchetto dati di hop in hop fino al gateway 6LoWPAN. Il gateway 6LoWPAN potrà quindi inoltrare il pacchetto al dispositivo di destinazione utilizzando l'indirizzo IP (vedi Figura 5.11).



**Figura 5.11:** Comunicazione in una rete 6LoWPAN

## WiMax

Worldwide Interoperability for Microwave Access (WiMAX) è una tecnologia wireless conforme allo standard IEEE 802.16. Risulta superiore rispetto a Wi-Fi per velocità di trasmissione e range di copertura delle celle, per cui è adatto ad una trasmissione sia di tipo urbano che rurale. Inoltre, implementa diverse tecniche di crittografia, sicurezza ed autenticazione. WiMAX è una tecnologia in grado di integrarsi con quelle presenti, soddisfacendo diverse specifiche imposte da una tipica Smart Grid tra cui la massima accessibilità ed interoperabilità, tempi di latenza inferiori ai 50ms e larghezza di banda di 5MHz. Fornisce sia connettività fissa che mobile usando una tecnica chiamata Orthogonal Frequency Division Multiple Access (OFDMA). Una tipica rete WiMax è mostrata in Figura 5.12. La copertura di WiMax si estende fino ai 50 km con una velocità di trasmissione dati pari a 75 Mbps per i collegamenti fissi e fino a 15 Mbps per le connessioni mobili. È ottimizzato per supportare dispositivi mobili fino ad una velocità di 10 km/h. Anche se supporta veicoli in movimento fino a 120 km/h, le sue prestazioni degradano con l'aumentare della velocità del veicolo[23].



**Figure 3.19** WiMax network

**Figura 5.12:** Una rete WiMax

### 5.1.2 Power line

La Power Line Communication (PLC) rappresenta una delle tecnologie di rete proposte per la trasmissione in ambiente Smart Grid in quanto l'infrastruttura esistente ne riduce i costi di installazione. Se, da un lato non è richiesta la realizzazione di nuove strutture, da un altro lato vi è un limite dovuto alla presenza di disturbi che possono corrompere le informazioni, non garantendo più la continuità del servizio. PLC trasporta i dati utilizzando i conduttori e le linee elettriche esistenti. Fornisce servizi di comunicazione per Automatic Meter Reading (AMR), AMI e HAN ma anche l'accesso ad internet all'utente finale. In una tipica rete PLC, gli smart meter sono collegati al data concentrator (che colleziona le informazioni ricevute dai vari meter) attraverso power line e i dati vengono trasferiti al data center tramite tecnologie di rete cellulare. La tecnologia PLC è infatti scelta per la comunicazione tra gli smart meter e il data concentrator, mentre la tecnologia GPRS è utilizzata per trasferire i dati dal concentrator al data center.

L'ENEL, nota azienda multinazionale produttrice e distributrice di energia elettrica, ha scelto la tecnologia PLC per trasferire i dati degli smart meter al data concentrator più vicino e la tecnologia GSM per inviare i dati al data center. La topologia di rete, il numero/tipo dei dispositivi collegati e la distanza trasmettitore/ricevitore compromettono la qualità del segnale.

Le sensibilità di PLC ai disturbi e alla qualità del segnale sono gli svantaggi che rendono la tecnologia non adatta alla trasmissione dei dati. Tuttavia, ci sono state alcune soluzioni ibride in cui la tecnologia PLC si combina con altre, ad esempio, GPRS o GSM, per fornire una connettività non possibile generalmente con PLC.

Inizialmente, la velocità di trasmissione in questo tipo di reti era molto limitata, fino a pochi kbps. Successivamente, grazie al progresso tecnologico e con l'introduzione di broadband PLC (BB-PLC), un'applicazione della tecnologia PLC a banda larga che fornisce l'accesso a Internet tramite linee elettriche ordinarie, la velocità di trasmissione ha raggiunto anche i 200 Mbps. Sono utilizzate tre tecnologie di comunicazione che prendono il nome di *narrowband transmission*, *spread-spectrum transmission* e *DSP-processed narrowband transmission*. La Figura 5.13 mostra alcuni vantaggi e svantaggi relativi a PLC in ambito Smart Grid. Tra gli standard e i protocolli maggiormente utilizzati troviamo IEEE P1901 e HomePlug.

Advantages	Disadvantages
Wide Coverage	High noise sources over power lines
Cost	Capacity
Flexibility and Range	Problem of open circuits
Mobility	Attenuation and distortion of the signal
Easy Installation	Inadequacy of the regulations for broadband PLC
Stability	Lack of interoperability

**Figura 5.13:** Vantaggi e Svantaggi di PLC in ambito Smart Grid

## **IEEE P1901**

Il gruppo IEEE P1901 è stato formato nel 2005 con lo scopo di sviluppare una tecnologia per la trasmissione di voce o dati che utilizzasse la rete di alimentazione elettrica come mezzo trasmittivo. Lo standard permette una comunicazione ad alta velocità tra i device che prendono il nome di BPL (Broadband over Power Line). Lo standard utilizza frequenze inferiori a 100 MHz ed è di supporto ai device BPL utilizzati per i collegamenti first-mile/last-mile così come quelli utilizzati nelle reti LAN all'interno di edifici. Inoltre, tali device possono essere utilizzati all'interno di smart energy application, autoveicoli e in altre applicazioni per la distribuzione dei dati.

## **HomePlug**

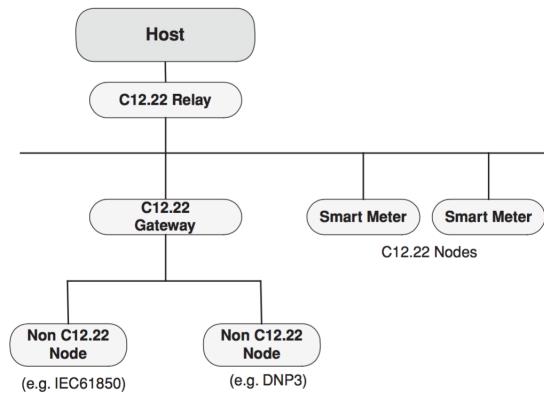
HomePlug è una tecnologia broadband non standardizzata e specificata dalla HomePlug Powerline Alliance, i cui membri sono le principali aziende nel settore della comunicazione e dell'energia. Il protocollo gestisce vari sottocanali suddividendo la larghezza di banda disponibile. La velocità di trasmissione varia da 1 a 14 Mbps e i nodi sono in grado di adattarsi al data rate ottimale in maniera automatica. Le collisioni sono evitate grazie al CSMA/CD. Lo standard HomePlug 1.0 per la connessione di dispositivi nelle case (1-10 Mbps) fa uso della tecnica di Orthogonal Frequency Division (OFDM), utilizzata anche da DSL, IEEE 802.11a e IEEE 802.11g. Il rumore, comune in ambiente power line, è superato per mezzo di forward error correction e data interleaving. La HomePlug Powerline Alliance ha definito ulteriori standard come HomePlug AV/AV2 che forniscono banda sufficiente per applicazioni come HDTV e VoIP, HomePlug CC e HomePlug BPL.

## **5.2 Standard per lo scambio di informazioni**

### **5.2.1 Standard per Smart Meter**

Gli smart meter possono essere utilizzati in vari modi portando a differenti requisiti dal punto di vista del sistema di comunicazione. Con Automated Meter Reading (AMR) si richiede una trasmissione occasionale dei dati energetici registrati (circa una volta al mese), viceversa con Advanced Metering Infrastructure (AMI) si richiedono frequenti comunicazioni bidirezionali (ad esempio ogni 30 minuti). ISO/IEC 62056 e ANSI C12.22 sono due famiglie di standard che descrivono sistemi di comunicazione per gli smart meter. ISO/IEC 62056 definisce Transport e Application Layer per lo smart metering nell'ambito di una serie di specifiche chiamate COSEM (Companion

Specification for Energy Metering). ANSI C12.22 (vedi Figura 5.14) specifica l'invio e la ricezione dei dati registrati da e verso sistemi esterni ed è possibile utilizzarlo su qualsiasi rete di comunicazione.



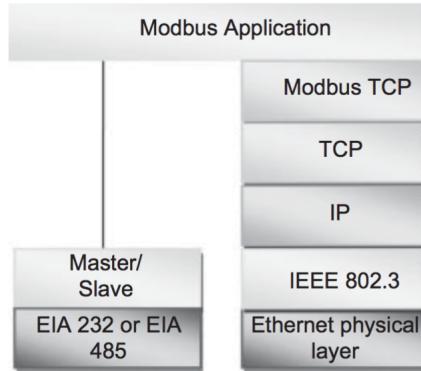
**Figura 5.14:** Architettura ANSI C12.22

### 5.2.2 Modbus

Modbus è un protocollo di messaggistica che risiede nell'Application Layer e consente la comunicazione tra i dispositivi collegati su diversi bus e reti. Può essere implementato tramite Ethernet o utilizzando la trasmissione seriale asincrona su EIA 232, EIA 422, EIA 485 e fibra ottica. Di questi, l'applicazione più comune è Modbus su EIA485. La Figura 5.15 mostra come l'Application Layer Modbus è connesso agli altri layer del modello OSI. Modbus su EIA 485 è ampiamente utilizzato nell'automazione delle sottostazioni. La comunicazione è avviata dal Master con una query. Il Master è l'unico che può inviare query destinate al singolo Slave o di broadcast. Uno Slave monitora continuamente la rete riconoscendo solo le query destinate ad esso. All'arrivo di una query, lo Slave eseguirà un'azione o risponderà. Tra i problemi del protocollo spiccano il limitato supporto alle varie tipologie di dati e la non garanzia di sicurezza.

### 5.2.3 ISO/IEC 61850

ISO/IEC 61850 è uno standard per la progettazione dei sistemi di automazione per le sottostazioni elettriche. È una sovrastruttura che coordina e gestisce protocolli e tecnologie esistenti garantendo l'interoperabilità. Gene-



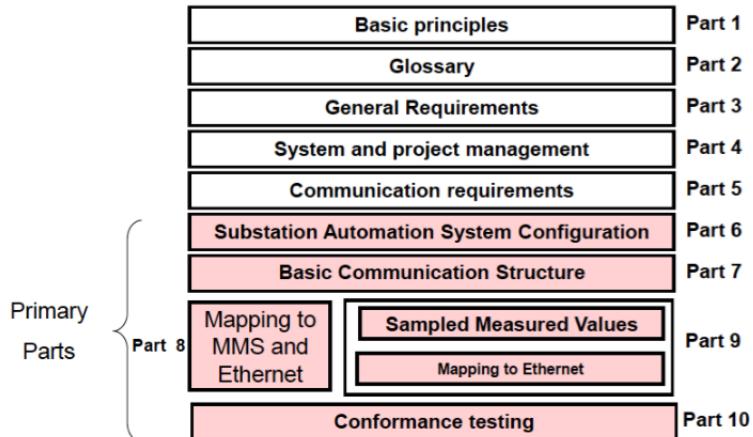
**Figura 5.15:** Modbus stack

ralmente, questi protocolli girano su reti TCP/IP o LAN con switch Ethernet molto performanti per rispondere ai requisiti stringenti dei dispositivi, che necessitano di tempi di risposta inferiori a 4-5 millisecondi.

I principali vantaggi dello standard ISO/IEC 61850:

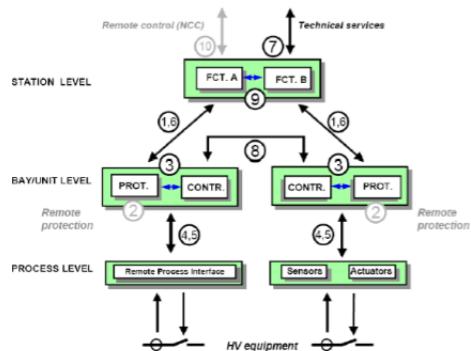
- Coordina la complessità di tante unità indipendenti;
- Si integra con i sistemi preinstallati in rete;
- È scalabile e facilita l'integrazione di apparati diversi;
- Si basa il più possibile su standard esistenti;
- È aperto e supporta i *self descriptive device* eliminando problemi di configurazione manuale;
- Si basa sui *data object* e standardizzazione degli elementi tipici di una rete elettrica;
- Permette di ottenere alte prestazioni di multicast;
- È estensibile e flessibile in modo da adattarsi rapidamente alla configurazione del sistema.

La struttura dello standard ISO/IEC 61850[25] è mostrata in Figura 5.16.



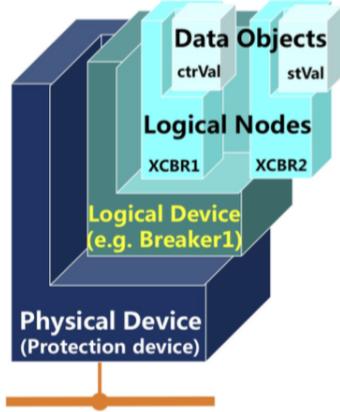
**Figura 5.16:** Struttura dello standard ISO/IEC 61850

ISO/IEC 61850 suddivide ogni sottostazione in tre livelli[25] chiamati *Station Level*, *Bay Level* e *Process Level*. La suddivisione dei livelli è mostrata in Figura 5.17.



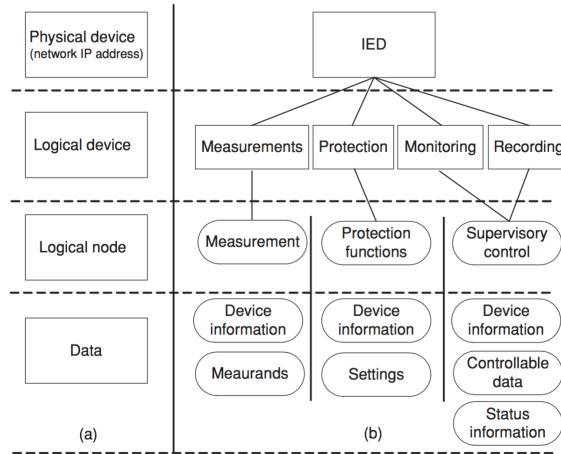
**Figura 5.17:** Livelli di una sottostazione

Il protocollo identifica le funzioni e le caratteristiche dei dispositivi fisici che si modellano in uno o più dispositivi logici. I dispositivi logici sono a loro volta suddivisi in nodi logici che sono in relazione tra loro in base a *data* e *data attribute* (vedi Figura 5.18).



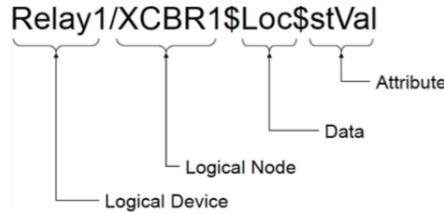
**Figura 5.18:** *Device Model ISO/IEC 61850*

Come mostrato in Figura 5.19a, un device model considera inizialmente un physical device. Tale modello consente ad un singolo dispositivo fisico di agire da gateway di informazioni per più dispositivi. Successivamente vengono specificati i logical device all'interno di tale dispositivo. Ogni logical device contiene uno o più logical node, logicamente correlati ad una funzione della stazione. I logical node sono definiti da gruppi di data object e relativi servizi, ognuno modellato secondo gli schemi definiti dalle **Common Data Classes** (CDC).



**Figura 5.19:** *ISO/IEC 61850 data structure*

La Figura 5.20 mostra un esempio di nome per un oggetto in un formato standard. Utilizzando tale formato si è in grado di indicare le informazioni relative allo status o alla posizione di un dispositivo. I logical node sono identificati con nomi definiti dallo standard in cui la prima lettera indica l'attinenza (e.g. A controllo automatico, M misura, X switchgear, etc).



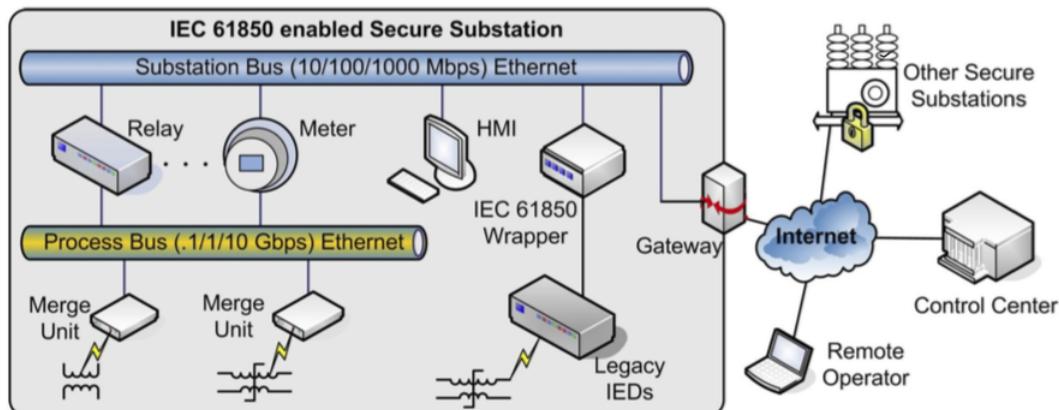
**Figura 5.20:** Struttura del nome di un oggetto

L'ISO/IEC 61850 si basa sulla specifica degli *oggetti* e dei *servizi astratti* di comunicazione che permettono di scrivere un'applicazione indipendentemente dai protocolli tradizionali. Si definisce quindi un modello che prende il nome di Abstract Communication Service Interface (ACSI) che definisce l'insieme dei servizi e le risposte a quei servizi che rendono gli IED uguali dal punto di vista della rete. Inoltre, tale modello interpreta i dati e gli attributi dei vari elementi garantendone l'interoperabilità. Gli oggetti e i servizi definiti dall'ACSI vengono implementati attraverso il protocollo ISO-9560 Manufacturing Message Specification (MMS). Si tratta di un protocollo flessibile in grado di supportare funzioni complesse e la logica a oggetti ACSI. Tale protocollo definisce i messaggi di comunicazione tra i vari centri di controllo oppure tra le stazioni e i centri di controllo.

Il concetto di astrazione e standardizzazione presuppone l'utilizzo di un linguaggio comune di configurazione. L'ISO/IEC 61850 si serve di un linguaggio basato su *XML* chiamato *Substation Configuration Language* (SCL). Grazie all'utilizzo di un linguaggio standard è possibile garantire l'interoperabilità tra gli IED che usano diversi protocolli, permettere una configurazione automatica dei dispositivi, ridurre la presenza di errori dovuti all'intervento umano nella gestione degli IED e consentire maggiore trasportabilità facendo in modo che ogni IED, che supporta ISO/IEC 61850, presenti un file SCL che ne definisce la configurazione. Nella Figura 5.19b è mostrato un esempio di IED.

Gli elementi fondamentali del modello di una sottostazione sono elencati di seguito (vedi Figura 5.21):

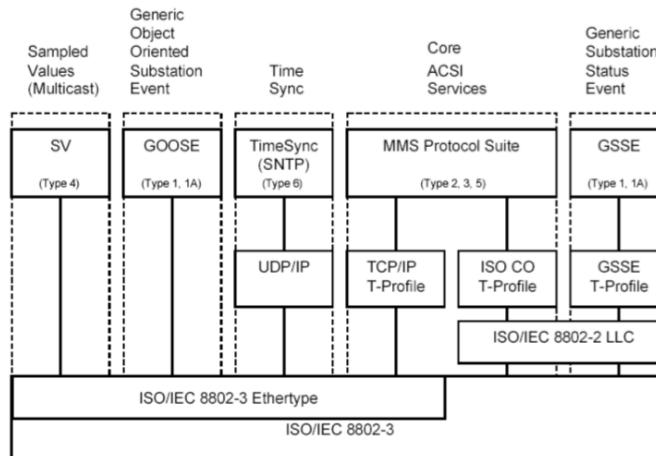
- **Merge Unit:** a livello di processo, i dati raccolti da sensori ottici, elettronici, da TV e TA, sui valori di tensione e corrente o sullo status dei componenti, sono recuperati dalle Merge Unit (MU). In genere, sono situate in corrispondenza del centro di controllo;
- **Intelligent Electronic Device:** gli IED che supportano ISO/IEC 61850 comunicano attraverso le MU e un process bus Ethernet a 10 Gbps;
- **Wrapper ISO/IEC 61850:** gli IED che non supportano il protocollo ISO/IEC 61850 utilizzano un Wrapper;
- **Process Bus e Station Bus:** le MU comunicano con il Bay Level attraverso un process bus mentre tutti i nodi logici (IED) comunicano attraverso un bus Ethernet a 100 Mbps;
- **Gateway e Internet:** diverse sottostazioni comunicano tra loro attraverso la rete Internet. Un Gateway permette di collegarsi alla rete e accedere alle informazioni da un centro di controllo o da remoto seguendo una procedura che garantisce la robustezza e sicurezza del sistema.



**Figura 5.21:** Architettura del sistema con lo standard ISO/IEC 61850

Lo standard ISO/IEC 61850 si serve dei seguenti strumenti per la gestione delle informazioni (vedi Figura 5.22):

- Generic Substation Event (GSE);
  - Generic Object Oriented Substation Event (GOOSE);
  - Generic Substation State Event (GSSE).
- Sampled Measured Values (SMV);
- Time Synchronization;
- Report e Logging.



**Figura 5.22:** Tools di ISO/IEC 618504

**GSE** è un protocollo che fornisce uno strumento veloce ed affidabile per la segnalazione di *eventi* all'interno della sottostazione. Le caratteristiche principali sono il servizio multicast/broadcast con modello di comunicazione publish/subscribe. I messaggi sono trasmessi in formato binario. GSE prevede due modelli di servizio che prendono il nome di GOOSE e GSSE.

**GOOSE** è stato progettato per essere *brand independent*. Utilizza Virtual LAN, stabilendo più network virtuali sulla stessa rete fisica e determinando livelli di priorità per i messaggi, consentendone anche la ritrasmissione (un identificativo indica se il messaggio è nuovo o ritrasmesso).

**GSSE** è utilizzato per lo scambio di informazioni sui soli cambiamenti di stato. In questo caso i messaggi sono costituiti da una serie di bit che rappresentano liste di stati. GSSE necessita un tempo di trasmissione maggiore se confrontato con GOOSE.

**SMV** è un protocollo per lo scambio di dati e la trasmissione di misure prodotte dai trasduttori delle sottostazioni: permette lo scambio di segnali tra gli IED. Prevede due metodi di comunicazione:

- *SV over Serial Unidirectional Multidrop Point-to-Point fixed link*: Sistema di comunicazione unidirezionale che specifica una serie di dataset (tensioni trifase, correnti trifase, etc). I valori analogici vengono codificati a 16 bit;
- *SV over Ethernet*: Versione più generica e flessibile di SV che fornisce la possibilità di definire dataset con valori di diversa dimensione e tipo, configurabili dall'utente grazie all'utilizzo di SCL. Utilizza un modello di comunicazione publish/subscribe con possibilità di multi-casting.

**Time Synchronization** è un servizio di sincronizzazione dei clock fondamentale per applicazioni real-time. Utilizza un subset di Network Time Protocol (NTP) con riferimento allo Universal Coordinated Time (UTC). NTP è il protocollo tipicamente utilizzato per sincronizzare i clock di computer collegati ad Internet e in LAN.

**Report** è lo strumento che permette di memorizzare i cambiamenti dei dati e degli attributi relativi ai nodi logici. Genera dataset contenenti attributi di interesse e richiede ai nodi logici l'invio delle informazioni riguardanti le variazioni nel sistema.

**Log** è la registrazione degli eventi relativi ad un dispositivo. I log sono registrati in un server e, a differenza dei Report, i dispositivi logici creano al loro interno un database di eventi senza inviarne notifica.

Tra i limiti di ISO/IEC 61850 si evidenziano i costi elevati per l'installazione dei server e dei dispositivi atti alla gestione dei dati ma anche complessità dal punto di vista dell'architettura. ISO/IEC 61850 è affiancato da ISO/IEC 62351 che garantisce la sicurezza e specifica i requisiti tecnici che devono essere rispettati dai fornitori.

## 5.3 Standard per la sicurezza

Gli standard per la sicurezza informatica sono di recente invenzione e fondamentali data la grande mole di informazioni sensibili memorizzate sui computer che sono collegati ad Internet. Inoltre, molte attività che prima erano condotte manualmente, oggi sono svolte dalle macchine in maniera automatica introducendo quindi un maggiore bisogno di affidabilità e di sicurezza in tali sistemi informatici. Come ampiamente discusso nel Capitolo 4, la sicurezza è un fattore importante per gli individui che devono proteggersi dal cosiddetto furto di identità ma anche per le aziende perché devono proteggere i loro segreti industriali e le informazioni sui dati personali dei clienti.

I problemi relativi alla sicurezza vanno quindi dagli accessi non autorizzati a informazioni recuperate dagli smart meter, lo spegnimento dei dispositivi da parte di un attaccante così come un attacco alla Smart Grid per causare un'interruzione al passaggio di corrente. I problemi relativi alla privacy riguardano invece l'alta frequenza con cui vengono effettuate le letture per misurare il consumo energetico in quanto esse mostrano totalmente il comportamento dell'utente. In generale si cerca di aggregare le informazioni dei meter per rilevare sia frode che perdite (per esempio nel caso del gas, dove un'eventuale perdita pone un problema di sicurezza) utilizzando schemi di aggregazione *privacy-friendly* in modo da mascherare i singoli consumi dei meter.

Nell'ambito dei power system, esistono diversi standard che si applicano alla sicurezza delle apparecchiature all'interno delle sottostazioni e molti sono in fase di sviluppo. Per la valutazione complessiva della sicurezza, è ampiamente utilizzata la norma ISO 27001 e specifica la valutazione dei rischi e la strategia da utilizzare per lo sviluppo di un sistema di sicurezza in modo da limitarli.

### 5.3.1 ISO/IEC 62351

ISO/IEC 62351 è uno standard sviluppato dal WG15 facente parte della TC57 dell'organo internazionale IEC. Questo standard è stato sviluppato per gestire la sicurezza nella serie di protocolli della commissione tecnica 57, tra i quali le serie ISO/IEC 60870-5, ISO/IEC 60870-6 series, ISO/IEC 61850, ISO/IEC 61970 e ISO/IEC 61968.

Tra i diversi obiettivi di sicurezza che lo standard persegue ci sono:

- Autenticazione nel processo di trasferimento di dati tramite firma digitale;
- Garanzia di accessi esclusivamente dopo autenticazione;
- Prevenzione dell'*eavesdropping* (ossia intercettazioni della comunicazione non autorizzate);
- Prevenzione da attacchi di *playback* e attacchi di *spoofing* (ovvero sostituirsi ad una controparte della comunicazione);
- Rilevamento delle intrusioni.

E' suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues: fornisce un'introduzione agli aspetti relativi alla sicurezza delle informazioni;
2. Glossary of terms: comprende i principali termini utilizzati nella serie IEC 62351. La maggior parte dei termini utilizzati nell'ambito della sicurezza informatica sono formalmente definiti da altri organismi e inclusi anche all'interno di questo glossario;
3. Communication network and system security - Profiles including TCP/IP: specifica come fornire riservatezza, rilevare manomissioni e l'autenticazione per i protocolli SCADA e di telecontrollo che fanno uso di TCP/IP come message transport layer;
4. Profiles including MMS: definisce procedure, i miglioramenti del protocollo, e gli algoritmi atti a promuovere l'aumento dei messaggi di sicurezza trasmessi su MMS;
5. Security for IEC 60870-5 and derivatives: specifica messaggi, procedure e algoritmi per la sicurezza delle operazioni nei protocolli basati su IEC 60870-5 e derivati;
6. Security for IEC 61850: specifica messaggi, procedure e algoritmi per garantire il funzionamento di tutti i protocolli basati su 61850 e derivati;
7. Network and system management (NSM) data object models: definisce i data object model (NSM) specifici per il funzionamento del sistema di

alimentazione. Questi data object NSM sono utilizzati per monitorare lo stato delle reti e dei sistemi, per rilevare eventuali intrusioni, e per gestire le prestazioni e l'affidabilità dell'infrastruttura relativa alle informazioni;

8. Role-Based Access Control: approccio a sistemi ad accesso ristretto per utenti autorizzati. Tre regole fondamentali sono definite per il modello RBAC (Assegnazione dei ruoli, Autorizzazione dei ruoli, Autorizzazione alla transazione).

## **Capitolo 6**

# **Principali vulnerabilità delle Smart Grid: attacchi e contromisure**

Negli ultimi anni, un numero sempre crescente di infrastrutture critiche è stato digitalizzato, aggiungendo capacità di comunicazione e di computazione a numerosi dispositivi nelle reti di distribuzione dell'energia e dell'acqua, sistemi di trasporto, e manifatturieri. Ciò avviene in parte con lo scopo di aumentare l'efficienza, ma spesso è anche un requisito necessario a gestire l'ambiente che muta, come ad esempio la generazione locale dell'energia o il passaggio ai veicoli elettrici nel caso della distribuzione energetica.

Un progetto di digitalizzazione molto visibile è il passaggio dai *meter* analogici ai digitali (*smart*), che è attualmente in corso in vari paesi del mondo. Oltre ad una fatturazione complessivamente più precisa, uno smart meter può anche dare input agli algoritmi di controllo della grid, essere usato nei mercati energetici, comunicare con la *smart home* (ad esempio, per regolare l'aria condizionata ed i sistemi di riscaldamento quando la richiesta energetica è alta), oppure per disconnettere da remoto un consumatore. In questo modo, un dispositivo precedentemente disconnesso e non critico si trasforma in un dispositivo connesso che può generare dati *process-critical*.

La robustezza dei dati e dei comandi di switch è vitale - se una grande quantità di famiglie viene disconnessa simultaneamente, l'energia in eccesso non ha dove andare, potrebbe danneggiare la grid. In maniera simile, se gli algoritmi di manutenzione si basano su dati provenienti da misure effettuate dagli smart meter, input errati possono produrre effetti di gran lunga peggiori delle frodi di fatturazione. Ciò pone una nuova sfida per i produttori di

meter: progettare dispositivi economici, largamente distribuiti e che lavorino su canali con banda molto ristretta.

## 6.1 Open Smart Grid Protocol

L'Open Smart Grid Protocol (OSGP) [29] è un protocollo di comunicazione per smart grid costruito sullo stack protocollare ISO/IEC 14908-1 [27], sviluppato dalla Energy Service Network Association (ESNA), ed è uno standard dell'European Telecommunications Standards Institute (ETSI) fin dal 2012. È stato uno dei primi protocolli di comunicazione su powerline per smart meters disponibile sul mercato, ed è largamente utilizzato per comunicare tra smart meter e l'aggregatore di dati, il quale è un dispositivo che colleziona dati provenienti da diverse centinaia di meter in un segmento di PLC (Power Line Communication) e li inoltra ad un controllore centralizzato.

Nonostante l'OSGP sia principalmente utilizzato per applicazioni di smart-metering, esso è stato progettato per un utilizzo più ampio all'interno di dispositivi della Smart Grid. Lo stack protocollare è molto leggero. Tale leggerezza è ottenuta pagando in sicurezza, infatti le primitive crittografiche consigliate dal NIST (ad esempio: Advanced Encryption Standard - AES, in *authenticated mode*) sono evitate, optando per altre meno intense computazionalmente: lo stream cipher RC4 per la cifratura ed una funzione digest non standard per l'autenticazione dei messaggi.

In OSGP si introducono misure per proteggere la *privacy* dei clienti, restringendo l'accesso ai dati e cifrando questi ultimi per evitare che persone non autorizzate possano modificarli. Si introducono, inoltre, misure per rintracciare potenziali tentativi di eludere le funzioni di metering, che potrebbero risultare in accessi non registrati ai servizi.

Come detto in precedenza, OSGP è costruito sullo stack protocollare ISO/IEC 14908-1, che fornisce servizi di autenticazione, ma non include meccanismi per garantire la confidenzialità dei dati. Per questo motivo, OSGP completa la sicurezza di questo standard, aggiungendo un proprio *security layer* che fornisce autenticazione e confidenzialità [67].

Il protocollo OSGP si suddivide in:

- *Setup*, in cui si effettua la configurazione iniziale degli smart meter e del data concentrator;
- *Communication with authenticated encryption*, in cui gli smart meter comunicano con i data concentrator utilizzando meccanismi di autenticazione e di cifratura dei dati.

### **6.1.1 Setup**

Durante il processo di produzione industriale, i dispositivi OSGP vengono configurati con una *Open Media Access Key* (OMAK) univoca a 96 bit. Tali chiavi sono poi consegnate in maniera sicura alle società di servizi, che provvedono poi a dotare il proprio data concentrator della chiave OMAK del dispositivo afferente alla zona di competenza.

Il data concentrator è in grado di rilevare ogni dispositivo a lui afferente grazie ad un processo di discovery; successivamente, genera ed invia la Shared Key relativa alla sua zona di competenza ad ogni nuovo dispositivo scoperto. Tale comunicazione avviene in maniera cifrata, utilizzando come chiave di cifratura la OMAK del dispositivo. Ogni dispositivo, poi, rimpiazza la sua OMAK originaria con la Shared Key ricevuta.

La Shared Key è utilizzata per i seguenti scopi:

- Per l'autenticazione di messaggi;
- Come chiave in input per l'OSGP OMA Digest Algorithm;
- Per la cifratura: dall'OMAK, si deriva inizialmente una Base Encryption Key (BEK) a 128 bit che, successivamente, si combina in XOR con un OSGP digest, per produrre la chiave di cifratura di RC4.

### **6.1.2 Communication with authenticated encryption**

OSGP è un protocollo master - slave, in cui il master è rappresentato dal data concentrator e lo slave dallo smart meter, che si basa sulla Shared Key per cifrare i messaggi scambiati durante la comunicazione. In particolare, la comunicazione è iniziata dal data concentrator il quale invia un messaggio di richiesta cifrato allo smart meter; successivamente, lo smart meter decifra il messaggio, ne verifica l'autenticità (vedi paragrafo Authentication) e invia la risposta, anch'essa opportunamente cifrata. Smart meter e data concentrator sono identificati dai campi Subnet e Node ID del pacchetto di richiesta/risposta.

#### **6.1.2.1 Authentication**

Il data concentrator OSGP utilizza autenticazione basata su digest a livello applicativo per autenticare messaggi del livello applicazione tra i dispositivi. Questa forma di autenticazione richiede la metà dei pacchetti richiesti dall'autenticazione EN 14908. Per evitare replay attack, viene effettuato l'*append* di un sequence number al *payload* e successivamente se ne effettua

il digest complessivo.

Quando il device è in fase di inizializzazione sceglie un proprio sequence number iniziale casuale. Assumendo che il dispositivo si aspetti un sequence number  $N$ , esso rifiuta qualsiasi messaggio che non abbia sequence number compreso tra  $N - 1$  ed  $N + M$ , dove  $M$  è pari ad 8. Quando è ricevuta una richiesta con sequence number  $N - 1$ , la response per tale richiesta inviata originariamente, se presente, viene nuovamente inviata. Se il sequence number ricevuto in una richiesta è fuori dal range specificato ( $[N - 1, N + M]$ ), il dispositivo risponderà a tale richiesta con una NACK response contenente il messaggio di “*invalid sequence number*”, seguita dal sequence number desiderato. A quel punto sta al data concentrator iniziare ad usare il nuovo sequence number.

Le richieste rispettano il seguente formato:

Request	Sequence (4 byte)	Digest (8 byte)
---------	-------------------	-----------------

Il digest nella fase di request è computato sui dati seguenti, utilizzando l’Algoritmo 1 che fa uso della OMA key a 96 bit.

Subnet (1 byte)	Node (1 byte)	Request	Sequence
-----------------	---------------	---------	----------

Le response seguono il seguente formato:

Response	Digest (8 byte)
----------	-----------------

Il digest nella fase di response è computato sui seguenti dati, utilizzando come prima l’Algoritmo 1:

Subnet (1 byte)	Node (1 byte)	Request	Sequence	Response	Response Length (1 byte)
-----------------	---------------	---------	----------	----------	--------------------------

Da notare che anche le response NACK sono rese sicure nel modo che abbiamo appena visto.

I dispositivi OSGP possono inviare i seguenti tipi di NACK:

“Subnet” e “Node” nei diagrammi visti sopra si riferiscono sempre a subnet/node del target della richiesta. Ovvero, è lo stesso indirizzo in entrambe le direzioni. “Request” e “Sequence” fanno riferimento sempre ai valori nel messaggio di richiesta originale.

Si assume che il dispositivo possa mantenere il suo sequence number per più riavii (*power cycle*). Quindi, il primo messaggio autenticato in seguito

all'accensione richiederà uno scambio extra.

Tutti i dati dei device critici sono protetti dall'autenticazione basata su digest al livello applicativo sia per operazioni di lettura che di scrittura. Questo include:

- Configurazione di un dispositivo OSGP
- Fatturazioni e profili di carico OSGP
- Richieste di cancellazione del carico
- Time setting

Le seguenti operazioni sono protette attraverso la *challenge authentication* di EN 14908. Questa verifica dell'autenticazione è responsabilità dell'interfaccia EN 14908, e non del dispositivo OSGP:

- Indirizzamento logico di EN 14908
- Modifica della authentication key
- Misura di fase
- Impostazioni di compatibilità
- Cambio della modalità del nodo
- Letture/Scritture in memoria

Le seguenti operazioni non sono protette da autenticazione:

- Query di stato EN 14908
- Misure della potenza del segnale

### 6.1.2.2 Encryption

Si analizza quindi lo schema di *authenticated encryption* utilizzato nell'Open Smart Grid Protocol.

Tale schema si suddivide in una parte di autenticazione ed una di cifratura e si basa su tre algoritmi: l'algoritmo EN 14908 [27], lo stream cipher RC4 ed il digest OMA, quest'ultimo è un *message authentication code* (MAC). Questi tre algoritmi sono combinati secondo gli approcci *MAC-and-encrypt* e *MAC-then-encrypt*, a formare uno schema di cifratura autenticata. Da notare

che, mentre il digest OMA è descritto nella specifica OSGP [29], informazioni pubbliche riguardo l'algoritmo EN 14908, specificato in ISO-IEC 14908-1 [27], sono difficili da recuperare. Tutte le informazioni su quest'ultimo sono state ottenute dalla specifica OSGP.

#### 6.1.2.2.1 Notazione

Una stringa  $x$  di  $n$  bit è un elemento di  $\{0,1\}^n$ . La taglia di  $x$  in bit è denotata da  $|x|$ . La concatenazione di stringhe di bit è identificata da  $\parallel$ . Dato un vettore di stringhe di bit  $(x_0, \dots, x_{n-1})$ , si denota con  $x_{i,j}$  il  $j$ -esimo bit della  $i$ -esima stringa dove  $0 \leq i \leq n - 1$ . Quando si le stringhe di bit sono interpretate come interi si utilizza il formato little-endian denotato in esadecimale.

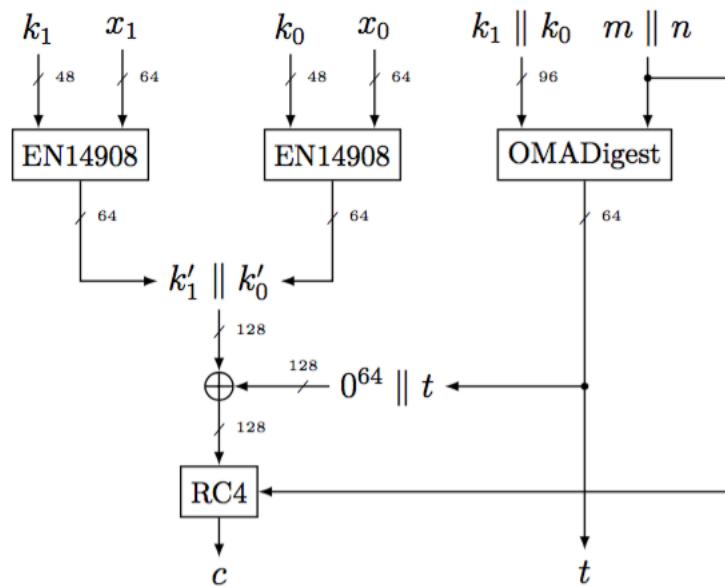
Una stringa di bit composta da  $n$  zero è denotata da  $0^n$ .

Una rotazione ciclica di una stringa di bit  $x$  di  $m$  bit verso sinistra e destra sono denotate con  $x \ll m$  ed  $x \gg m$ , rispettivamente. La differenza di due stringhe di bit  $x$  ed  $x'$  rispetto allo XOR è denotata da  $\Delta x$ , mentre la differenza rispetto all'addizione modulo  $2^n$  è denotata da  $\delta^\square x$ .

#### 6.1.2.2.2 Infrastruttura Crittografica di OSGP

La struttura ad alto livello dello schema di cifratura autenticata (AE) di OSGP è mostrata in Figura 6.1. La sicurezza dello schema AE di OSGP dipende dalla *Open Media Access Key* (OMAK) a 96 bit  $k = k_1 \parallel k_0$ , da cui deriva tutto ciò legato alla chiave. La OMAK è solitamente univoca per ogni device ma non *hardcoded* e può essere cambiata.

Dalla OMAK derivano due cose: inizialmente, è computata una *Base Encryption Key* (BEK)  $k' = k'_1 \parallel k'_0$ , che è una chiave a 128 bit che compone la base della chiave di cifratura di RC4. La BEK è costruita (la specifica OSGP non è chiara su come la BEK sia rilevata, la descrizione presentata è basata sulle investigazioni svolte in [31]. L'osservazione chiave qui è che la BEK è derivata dall'OMAK. Non è importante il modo, ed è solamente descritto per completezza) utilizzando l'algoritmo EN 14908, che sembra essere la base dell'OMA digest ma usa chiavi più piccole a 48 bit e processa i byte dei messaggi in ordine inverso. L'algoritmo EN 14908 è applicato ad ognuna delle metà  $k_0$  e  $k_1$  dell'OMAK e delle due costanti  $x_0 = \{ 81, 3F, 52, 9A, 7B, E3, 89, BA \}$ , ed  $x_1 = \{ 72, B0, 91, 8D, 44, 05, AA, 57 \}$ . I due risultati a 64 bit sono concatenati per formare  $k'$ , come mostrato in Figura 6.1. La BEK dipende solo dall'OMAK ed è quindi fissata fin quando  $k$  resta invariato.



**Figura 6.1:** Lo schema AE di OSGP. Notazione:  $x_0 = \{81, 3F, 52, 9A, 7B, E3, 89, BA\}$ ,  $x_1 = \{72, B0, 91, 8D, 44, 05, AA, 57\}$ ,  $k = k_1 \parallel k_0$ : Open Media Access Key (OMAK),  $m$ : messaggio,  $n$ : numero di sequenza,  $t$ : tag di autenticazione,  $k' = k'_1 \parallel k'_0$ : Base Encryption Key (BEK),  $c$ : ciphertext.

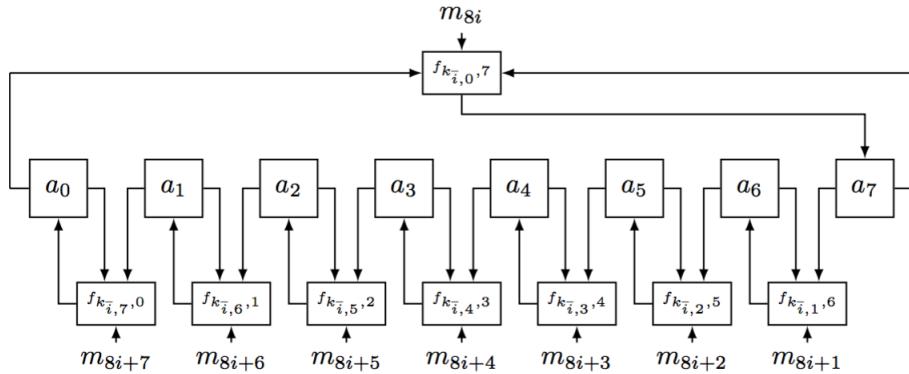
In secondo luogo, un tag di autenticazione  $t$  è prodotto utilizzando il digest OMA sul messaggio  $m$  concatenato ad una *sequence number*  $n$  e la OMAK  $k$ . Si denoti con  $l$  la taglia di  $m\|n$  in byte. Il digest OMA inizia con gli 8 byte  $a = (a_0, \dots, a_7)$  del suo stato interno impostati a 0. Per prima cosa,  $m\|n$  è zero-padded ad un multiplo di 144 byte, cioè

$$m' = m\|n\|0^{-l \bmod 144}.$$

Il primo, e potrebbe anche ultimo, blocco da 144 byte del messaggio è denotato da  $m' = m'_0 \| \dots \| m'_{143}$ . Lo stato interno è continuamente aggiornato utilizzando una funzione nonlineare  $f_{b,c}$  dove  $b = k_{i \bmod 12,7-j}$  è un bit chiave e  $c = j$  è la posizione corrente nello stato. La sua specifica è riportata di seguito:

$$f_{b,c}(x, y, z) = \begin{cases} y + z + (\neg(x + c)) \lll 1 & \text{if } b = 1 \\ y + z - (\neg(x + c)) \ggg 1 & \text{altrimenti.} \end{cases}$$

Per aggiornare l'elemento di stato  $a_j$ , la funzione  $f$  prende, per  $0 \leq i \leq 17$  e  $7 \geq j \geq 0$ , due elementi di stato adiacenti  $a_j$  ed  $a_{j+1 \bmod 8}$  ed un byte del messaggio  $m'_{8i+7-j}$  in input, ad esempio,  $a_j = f_{k_{i \bmod 12,7-j},j}$ , ed in funzione del valore del bit chiave  $k_{i \bmod 12,7-j}$  uno dei due rami mostrati sopra viene valutato. Il prossimo blocco da 144 byte del messaggio è processato in maniera simile, con lo stato interno proveniente dal blocco precedente. Lo pseudocodice del digest OMA è mostrato nell'Algoritmo 1 ed una visualizzazione del ciclo più interno, dove i byte del messaggio sono processati, è mostrata in Figura 6.2. Dopo la generazione del tag  $t$ , ne viene effettua-



**Figura 6.2:** Processing dei dati (da destra verso sinistra) nel digest OMA, con  $\bar{i} = i \bmod 12$ .

to lo XOR con la metà bassa della BEK  $k'$  che poi produce la chiave di cifratura di RC4 a 128 bit  $k' = k'_1 \| (k'_0 \oplus t)$ , come mostrato in Figura 6.1.

```

Function OMADigest ( $m, k$ )
   $a \leftarrow (0, 0, 0, 0, 0, 0, 0, 0)$ 
   $m \leftarrow m \parallel 0^{-|m| \bmod 144}$ 
  foreach 144-byte block  $b$  of  $m$  do
    for  $i \leftarrow 0$  to 17 do
      for  $j \leftarrow 7$  to 0 do
        if  $k_{i \bmod 12, 7-j} = 1$  then
          |  $a_j \leftarrow a_{(j+1) \bmod 8} + b_{8i+(7-j)} + (\neg(a_j + j)) \lll 1$ 
        else
          |  $a_j \leftarrow a_{(j+1) \bmod 8} + b_{8i+(7-j)} - (\neg(a_j + j)) \ggg 1$ 
        end
      end
    end
  end
  return  $a$ 

```

**Algorithm 1:** Il digest OMA di OSGP.  $a$  8 byte (output tag della funzione),  $a_j$  e  $j$  ognuno da 8 bit,  $\neg(a_j + j)$  negazione bit a bit della rappresentazione binaria della somma dei due interi da 8 bit.

Questa scelta è intesa per fornire ad RC4 materiale chiave in continuo cambiamento, così producendo un *keystream* nuovo ad ogni messaggio, per cui, in accordo alla specifica OSGP, il numero di sequenza  $n$ , concatenato ad  $m$ , è continuamente incrementato.

I sequence number sono condivisi tra mittente e destinatario in OSGP. Il destinatario di un messaggio verifica che il corretto sequence number sia stato concatenato a quest'ultimo. I messaggi con sequence number nel range  $\{n, \dots, n + 8\}$  sono accettati come richieste valide. Se un messaggio con sequence number  $n - 1$  è ricevuto, il destinatario non esegue la richiesta, ma reinvia la risposta della richiesta (eseguita precedentemente) numero  $n - 1$ . I numeri di sequenza fuori di tale range fanno scattare un errore ed i dispositivi OSGP rispondono con un codice di fallimento ed il corretto sequence number.

Dopo che la fase di setup è terminata,  $k''$  è utilizzato per cifrare  $m \parallel n$  tramite RC4 per ottenere il ciphertext  $c$ . Infine,  $c \parallel t$  è trasmesso. La taglia massima consentita dei messaggi  $m \parallel n$  processati in OSGP è di 114 byte.

### 6.1.3 Analisi

OSGP utilizza RC4 per la cifratura. RC4 è soggetto ad attacchi di *statistical key recovery* e *plaintext key recovery*, ed è dimostrato come tali siano fattibili [34], [35], [37], [36]. Comunque, in questa analisi non ci si concentra su RC4, ma sul digest OMA (vedi Algoritmo 1). L'algoritmo del digest OMA presenta più falle. Per iniziare, utilizza un semplice padding a zero byte, che risulta in messaggi con un qualsiasi numero di zeri finali che condividono lo stesso tag. Inoltre, data una tupla  $(a, m, k)$  dove  $a$  è lo stato del digest OMA o il tag di autenticazione,  $m$  un messaggio e  $k$  la OMAK, la funzione non impedisce agli attaccanti di ottenere il messaggio originale (si veda l'Algoritmo 2) il che è una proprietà molto comoda per loro. Allo stesso modo, è anche possibile prendere uno stato interno arbitrario e continuare a processarlo come per riprendere un messaggio di cui si è fatto un digest parziale. Ciò è mostrato nell'Algoritmo 3.

```

Function OMABackward  $(a, m, k, n)$ 
  /* Assumes  $|m| \leq 144$  */  

   $m \leftarrow m \parallel 0^{-|m| \bmod 144}$   

  for  $l \leftarrow 0$  to  $n - 1$  do  

     $i, j \leftarrow \lfloor l/8 \rfloor, l \bmod 8$   

    if  $k_{(17-i) \bmod 12, 7-j} = 1$  then  

      |  $x \leftarrow (a_j - a_{(j+1) \bmod 8} - m_{143-8i-j}) \ggg 1$   

    else  

      |  $x \leftarrow (a_{(j+1) \bmod 8} + m_{143-8i-j} - a_j) \lll 1$   

    end  

     $a_j \leftarrow \neg x - j$   

  end  

  return  $a$ 
```

**Algorithm 2:** Il “backward” digest OMA di OSGP, ripristina lo stato interno di  $n$  byte dei messaggi.

```

Function OMAForward ( $a, m, k, n$ )
  /* Essentially Algorithm 1, but start at byte  $m_n$  with
   a known state  $a$ , and assume  $|m| \leq 144$ . */
   $m \leftarrow m \| 0^{-|m| \bmod 144}$ 
  for  $l \leftarrow n$  to 143 do
     $i, j \leftarrow \lfloor l/8 \rfloor, 7 - l \bmod 8$ 
    if  $k_{i \bmod 12, 7-j} = 1$  then
      |  $a_j \leftarrow a_{(j+1) \bmod 8} + m_{8i+7-j} + (\neg(a_j + j)) \lll 1$ 
    else
      |  $a_j \leftarrow a_{(j+1) \bmod 8} + m_{8i+7-j} - (\neg(a_j + j)) \ggg 1$ 
    end
  end
  return  $a$ 

```

**Algorithm 3:** Il “forward” digest OMA di OSGP, inizia con uno stato iniziale noto e processa byte di messaggi a partire dalla posizione  $n$ .

Di seguito è riportato un attacco mirato a recuperare la OMAK, mediante cifratura di un testo in chiaro scelto dall’attaccante.

### Chosen-Plaintext Key Recovery Attack

Sia  $a = (a_0, \dots, a_7)$  lo stato interno a 8 byte del digest OMA. L’attacco discusso in seguito, utilizza messaggi scelti a 144 byte della forma  $m = m_0 \| \dots \| m_{143}$  e sfrutta le debolezze differenziali nel digest OMA.

**Bitwise Key Recovery.** Tale attacco recupera l’intera chiave un bit alla volta, attraverso la crittoanalisi differenziale [30]. Nello specifico, sfrutta lo XOR-differential  $(\Delta_{m_i}, \Delta_{a_j}) = (80, 80)$ , in cui  $\Delta_{m_i}$  e  $\Delta_{a_j}$  sono, rispettivamente, le differenze in input e output per  $j = 7-i \bmod 8$ . La differenza in output è ottenuta subito dopo il *processing* del byte  $m_i$  del messaggio (vedi Algoritmo 1), e può essere scritto come

$$\begin{aligned}
 & f_{k,j}(a_j, a_{j+1 \bmod 8}, m_i \oplus 80) \\
 &= a_{j+1 \bmod 8} + (m_i \oplus 80) \pm (\text{FF} \oplus (a_j + j) \lll r) \\
 &= (a_{j+1 \bmod 8} + m_i \pm (\text{FF} \oplus (a_j + j) \lll r)) \oplus 80 \\
 &= f_{k,j}(a_j, a_{j+1 \bmod 8}, m_i) \oplus 80
 \end{aligned}$$

in cui la rotazione ciclica  $r \in \{1, 7\}$  e l’operazione  $\pm$ , dipendono dal valore del bit chiave  $k \in \{0, 1\}$ . Questo XOR-differential ha probabilità 1, in accordo a proprietà differenziali ben note dell’addizione modulo  $2^n$  [66], e

si propaga nettamente attraverso lo stato  $a$  per le successive 8 iterazioni, restituendo come risultato la seguente differenza

$$\Delta_a = (80, 80, 80, 80, 80, 80, 80, 80).$$

L'iterazione successiva dell'algoritmo rivela un bit chiave della OMAK. Linearizzando attraverso lo XOR la funzione  $f$  di aggiornamento dello stato, la nuova differenza in output  $\Delta_{a'_j}$  è della forma

$$\begin{aligned} \Delta_{a'_j} = & ((a_{j+1 \text{ mod } 8} \oplus 80) \oplus m_i \oplus (\text{FF} \oplus ((a_j \oplus 80) \oplus j) \ll r)) \oplus \\ & (a_{j+1 \text{ mod } 8} \oplus m_i \oplus (\text{FF} \oplus (a_j \oplus j) \ll r)) \end{aligned}$$

dove  $r \in \{1, 7\}$ . Di conseguenza, si ha che  $\Delta_{a'_j} = 81$  se il bit  $7-i \text{ mod } 8$  di  $k_{\lfloor i/8 \rfloor \text{ mod } 12}$  è pari a 1, e  $\Delta_{a'_j} = C0$ , se lo stesso bit chiave è 0. Sebbene l'addizione e lo XOR tra interi si comportino diversamente rispetto alla propagazione delle differenze XOR, il bit meno significativo dell'addizione tra interi e dello XOR si comportano allo stesso modo in questo caso e possono essere utilizzati per recuperare il bit chiave con probabilità 1.

Tale *leak*, combinato con l'Algoritmo 2, può trasformarsi in un *chosen-plaintext key-recovery attack* che restituisce la OMAK  $k$  bit a bit in al più 96+1 query. L'algoritmo 4 descrive questo attacco in dettaglio. Guardando in Figura 6.1, si può immediatamente vedere che la ricostruzione di  $k$  rompe lo schema completo OSGP AE.

```

Function RecoverKey( $\mathcal{O}$ )
  /*  $\mathcal{O}$  is an oracle returning a message's OMADigest
     under key  $k$  */
   $k \leftarrow \{0\}^{12}$ 
   $m \stackrel{\$}{\leftarrow} \{0..255\}^{144}$ 
   $a \leftarrow \mathcal{O}(m)$ 
  for  $i \leftarrow 0$  to  $11$  do
    for  $j \leftarrow 0$  to  $7$  do
       $m' \leftarrow m$ 
       $m'_{136-8i-1-j} \leftarrow m'_{136-8i-1-j} \oplus 80$ 
       $a' \leftarrow \mathcal{O}(m')$ 
       $b \leftarrow \text{OMABackward}(a, m, k, 8i)$ 
       $b' \leftarrow \text{OMABackward}(a', m', k, 8i)$ 
       $k_{(17-i) \bmod 12, 7-j} \leftarrow (b_{j,0} \oplus b'_{j,0})$ 
    end
  end
  return  $k$ 

```

**Algorithm 4:** Bitwise Key Recovery attack

## 6.2 Attacking Smart Meters and Smart Devices

Uno dei maggiori problemi legati alla sicurezza degli smart meter è che i consumatori hanno accesso fisico, e potenzialmente anche logico, a tali dispositivi. Sebbene in passato i consumatori avessero accesso ai vecchi meter, questi ultimi non operavano utilizzando tecnologie familiari ai consumatori o a cui potessero avere accesso, in quanto venivano utilizzate tecnologie proprietarie. A causa della prevalenza di tecnologie ben note, utilizzate dagli smart meter, tali dispositivi risultano essere i principali obiettivi di attacchi, per cui è necessario applicare metodologie di *security testing* su di essi.

Di seguito viene analizzato il più comune manuale di security testing, che fornisce le metodologie standard utilizzate per il testing degli smart meter.

### 6.2.1 Open Source Security Testing Methodology Manual

Nel Gennaio 2001, in USA e Spagna, fu fondato l’Institute for Security and Open Methodologies (ISECOM): organizzazione no-profit il cui scopo è quello di fornire soluzioni pratiche per security awareness, ricerca, certificazione e business integrity. Il loro *Open Source Security Testing Methodology Manual* (OSSTMM) [38] fornisce agli utenti le metodologie per effettuare security

testing. L'OSSTMM contiene sei sezioni che recensiscono un numero enorme di aspetti di sicurezza, incluse reti, dispositivi wireless, e sicurezza fisica. Per tali aspetti, è possibile applicare l'OSSTMM al security testing degli smart meter.

Sezioni dell'ISECOM *Open Source Security Testing Methodology Manual*:

1. Information Security
2. Process Security
3. Internet Technology Security
4. Communications Security
5. Wireless Security
6. Physical Security

Eseguire security testing in accordo all'OSSTMM richiede che ogni modulo contenuto in ogni sezione sia testato secondo sei approcci comuni al testing: dal Double Blind, in cui sia target che attaccante non abbiano informazioni prima di condurre il testing, al Tandem, dove il target e l'attaccante condividono informazioni riguardo il testing apertamente. L'approccio mostrato di seguito è quello Double Blind in quanto è quello che più si avvicina ad una situazione reale. Le prime tre sezioni dell'ISECOM OSSTMM saranno analizzate in dettaglio nei paragrafi successivi.

#### **6.2.1.1 Information Security**

In questa sezione risiedono sette moduli:

1. Posture assessment
2. Information integrity review
3. Intelligence survey
4. Internet document grinding
5. Human resources review
6. Competitive intelligence review
7. Privacy controls review Information controls review

La sezione di Information Security dell'OSSTMM si concentra su *information gathering* e *validation*. Dalla prospettiva di un attaccante, include l'ottenimento e la revisione di informazioni riguardo la marca e modello dello smart meter target per studiarne il funzionamento, gli standard utilizzati e determinare quali attacchi possano essere più adatti rispetto ad altri.

#### **6.2.1.2 Process Security Testing**

La seconda sezione dell'ISECOM *Open Source Security Testing Methodology Manual* si concentra sull'analisi di sicurezza dei processi del target e contiene i seguenti cinque moduli:

1. Posture review
2. Request testing
3. Reverse Request testing
4. Guided Suggestion testing
5. Trusted Persons testing

La seconda sezione, quindi, si occupa di ciò che solitamente è chiamata “social engineering”. Ogni modulo punta ad ottenere informazioni da persone attraverso la coercizione e l'inganno. In relazione all'attacco di smart meter, ciò include impersonare il tecnico di una compagnia o un consumatore. Con questi metodi, sarebbe possibile ottenere informazioni di valore come specifiche tecniche o amministrative, o credenziali degli utenti.

#### **6.2.1.3 Internet Technology Security Testing**

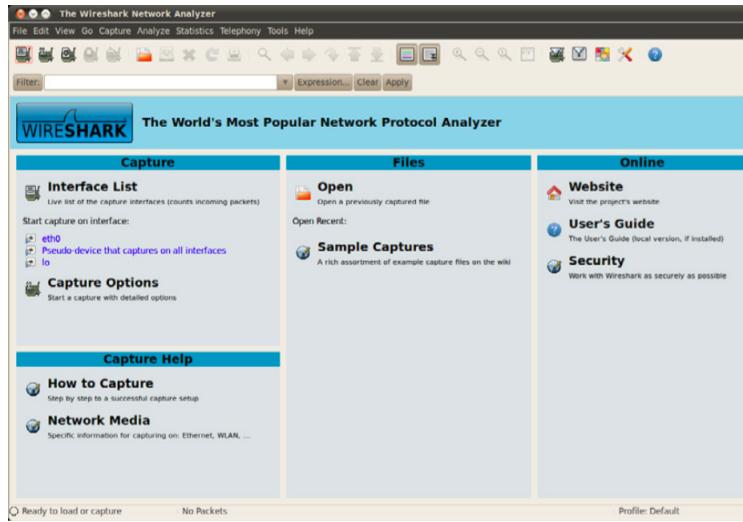
La maggior parte dei moduli applicabili al testing della sicurezza degli smart meter è contenuta nei quattordici moduli di questa sezione:

1. Network Surveying
2. Port Scanning
3. Services Identification
4. System Identification
5. Vulnerability Research and Verification
6. Internet Application Testing

7. Router Testing
8. Trusted Systems Testing
9. Firewall Testing
10. Intrusion Detection System Testing
11. Containment Measures Testing
12. Password Cracking
13. Denial of Service Testing
14. Security Policy Review

### Network Surveying

Punta all'identificazione dei sistemi target accessibili in rete. Nel caso di smart meter, questi sono accessibili agli attaccanti attraverso sia reti wireless che le home area network. In entrambi i casi, il Network Surveying consiste nell'ottenere informazioni sui target (*information gathering*). Ciò può essere realizzato in uno dei seguenti modi: passivamente, ascoltando il traffico di passaggio sulla rete, o attivamente, facendo *IP probing* in attesa di una response.



**Figura 6.3:** Wireshark sniffing tool

Per l'identificazione passiva, può essere utilizzato Wireshark, Figura 6.3.[41] Wireshark cattura il traffico che attraversa qualsiasi rete in tempo reale e fornisce l'ispezione di centinaia di protocolli. È possibile inoltre specificare gli indirizzi IP di cui effettuare lo sniffing, così da limitare la raccolta di informazione ai possibili target.

Internet Control Message Protocol (ICMP) è utilizzato per individuare i target attivi in rete analizzando le loro response. Nel caso in cui il traffico ICMP sia bloccato, è spesso utilizzato il ping di TCP. Per entrambi i casi è utilizzato il tool di sicurezza Nmap[42].

### **Port Scanning**

Consiste nel fare *probing* sul target in attesa di risposte sulle 65,536 porte TCP e/o UDP. Ottenere una response significa che dei servizi sono in esecuzione sulle porte associate e che potrebbero contenere debolezze che esporrebbero il target. Il tool di port-scanning più utilizzato è Nmap, che permette di effettuare scan TCP completando l'*handshake*, o attraverso scan TCP SYN che utilizza solamente i messaggi iniziali di SYN e SYN ACK dell'*handshake* TCP.

L'OSSTMM suggerisce che la scelta di quali delle 65,536 porte da analizzare è a discrezione dell'attaccante e dipende dal contesto.

### **Services Identification and System Identification**

Lo scopo di questi due moduli è di enumerare i servizi in esecuzione sulle porte TCP o UDP che hanno prodotto una response nella fase di port scanning, così come identificare il sistema operativo del target.

Entrambi i compiti sono svolti dal tool Nmap, attivando lo switch **-sV** che fornisce informazioni addizionali ad esempio il numero di versione, come è possibile verificare nella Figura 6.4.

In questo caso il target utilizzato, *webserver.domain.com*, fornisce informazioni quali il sistema operativo in quanto esposte dal server web Apache. Un attaccante userebbe le informazioni ottenute per verificare la presenza di fallo nelle specifiche versioni dei servizi, per poi preparare un attacco.

### **Vulnerability Research and Verification**

Una volta noti sistema operativo e servizi in esecuzione con relative versioni si passa alla ricerca e verifica di vulnerabilità tramite testing manuale ed automatizzato.

Un tool comunemente utilizzato per effettuare tale scan è Nessus [43], sviluppato dalla Tenable Network Security, mostrato in Figura 6.5. Sebbene Nessus

A terminal window titled "Terminal — bash — 82x13" showing the command "sudo nmap -sT -sV -p 443 webserver.domain.com". The output shows the host is up and port 443 is open, revealing Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Subversion-Patch mod\_ssl/2.2.8 OpenSSL/0.9.8g). The Python tab is also visible.

```

Old-Trafford:~ jmorehouse$ sudo nmap -sT -sV -p 443 webserver.domain.com
Starting Nmap 5.21 ( http://nmap.org ) at 2010-05-08 13:34 EDT
Nmap scan report for webserver.domain.com (192.168.1.1)
Host is up (0.0015s latency).
PORT      STATE SERVICE VERSION
443/tcp    open  ssl/http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Sub
osin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)

Old-Trafford:~ jmorehouse$
```

**Figura 6.4:** *Nmap version detection ouput*

sia ottimo per eseguire scanning automatizzato per determinare debolezze come una versione non aggiornata di Apache, il testing manuale dovrebbe coadiuvare quello automatizzato per individuare debolezze che potenzialmente potrebbero essere trascurate.

L'OSSTMM consiglia che il testing automatizzato venga effettuato da

A screenshot of the Nessus web interface. The title bar says "Nessus" and the address bar shows "https://localhost:8834/". The main menu includes "Reports", "Scans", "Policies", and "Users". The "Reports" tab is selected, showing a table of results. The table has columns: Port, Protocol, SVC Name, Total, High, Medium, and Low. There are 4 results listed:

Port	Protocol	SVC Name	Total	High	Medium	Low
0	tcp	general	4	0	0	4
0	udp	general	1	0	0	1
80	tcp	www	3	0	0	3
443	tcp	https?	0	0	0	0

**Figura 6.5:** *Interfaccia web di Nessus*

almeno due scanner, seguito poi da una verifica manuale. Le tecniche utilizzate per la verifica manuale di vulnerabilità variano molto in funzione della vulnerabilità che si sta cercando, come ad esempio l'uso di Telnet per osservare la versione di uno specifico servizio connettendoci, o l'utilizzo di un client FTP per connettersi ad un server FTP anonimo.

Nel processo di attacco a smart meter, la fase in esame è un passo critico in quanto fornisce i potenziali punti d'ingresso nello smart meter che potrebbero essere sfruttati nel modulo che segue.

### **Internet Application Testing**

Spesso, gli scanner di vulnerabilità non includono la possibilità di eseguire identificazione di vulnerabilità e verifica per Web application.

Con l'aumentare delle misure di sicurezza adottate dai produttori di sistemi all'interno del proprio ciclo di sviluppo, il numero di servizi in esecuzione a disposizione di attaccanti si è man mano ridotto. Ciò ha portato questi ultimi a concentrarsi sulle web application in esecuzione sui dispositivi target. Nel caso degli smart meter, tali applicazioni consentono al consumatore di visualizzare o configurare le informazioni di utilizzo, o permettono ai tecnici di configurare il dispositivo. Lo scopo di questo modulo è lo stesso del precedente, ma in un ambiente differente.

Effettuare identificazione e verifica di vulnerabilità su web application è significativamente più complesso che eseguire lo stesso test su servizi in esecuzione. Questo è il risultato del livello di personalizzazione trovato in ogni web application: è raro il caso che una web application sia esattamente come un'altra, ed anche nel caso di due *webapp* identiche trovate in esecuzione, la loro infrastruttura di backend potrebbe differire. Per questo il testing manuale gioca un ruolo significativo e i tool a supporto di tale operazione sono molteplici. L'Open Web Application Security Project (OWASP) ha sviluppato una guida al testing per le web application, disponibile a questo indirizzo [https://www.owasp.org/index.php/Category:OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/Category:OWASP_Testing_Project).

### **Password Cracking**

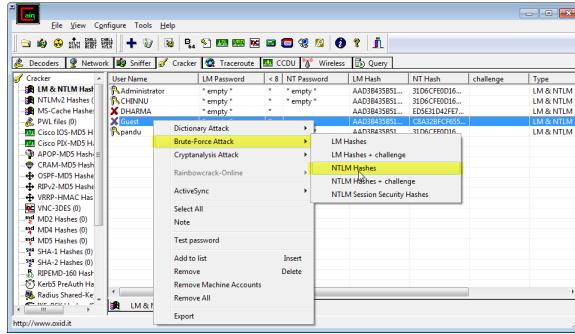
Questo modulo consiste nell'individuazione delle credenziali valide di un servizio in esecuzione o di una web application. Il testing può essere effettuato sia a partire da una lista precompilata di password, noto come attacco basato su dizionario, che provando ogni possibile combinazione di un certo alfabeto di caratteri, noto come attacco brute force.

Quando si esegue password cracking, è bene tenere a mente che molti servizi e web application implementano un servizio di blocco temporaneo o permanente, che disabilita un account se si verificano troppi tentativi di accesso con password invalide durante un determinato periodo di tempo.

Un tool comunemente utilizzato nell'ambito del password cracking, che supporti sia attacchi con dizionario che brute force, è Cain & Abel [44],

mostrato in Figura 6.6.

Il password cracking ha un ruolo fondamentale nell'attacco ad uno smart



**Figura 6.6:** Il tool di password cracking Cain & Abel

meter quando ci si trova davanti ad un prompt di autenticazione. Se un attaccante riesce ad ottenere le credenziali di uno smart meter, egli può istantaneamente avere accesso al dispositivo.

### Denial of Service Testing

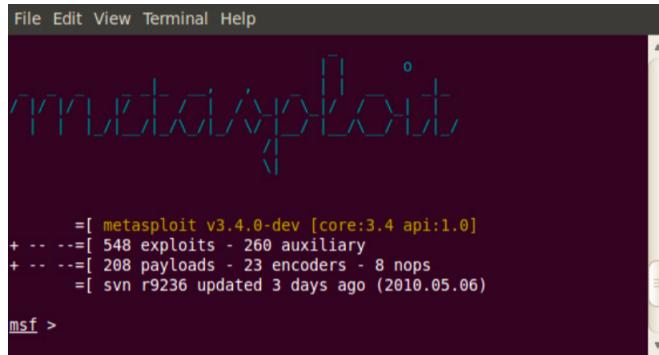
Il modulo di Denial of Service si occupa di identificare i punti deboli che potrebbero essere del device stesso o all'interno dell'infrastruttura sottostante. Tale operazione potrebbe coinvolgere l'utilizzo degli strumenti precedentemente descritti, Wireshark e Nmap. Ad esempio, Wireshark potrebbe essere utilizzato per determinare i regolari pattern di traffico da e verso lo smart meter. Nmap invece potrebbe essere utilizzato per incrementare gradualmente il traffico verso lo smart meter nell'intento di sovraccaricare il dispositivo o la sua infrastruttura.

Se l'obiettivo dell'attaccante è semplicemente di negare il servizio ad uno smart meter, sarebbe molto semplice condurre un attacco del genere se comparato con attacchi che mirano alla compromissione della confidenzialità e/o integrità dello smart meter.

### Exploit Testing

Tutti i moduli descritti finora gettano le basi per l'esecuzione dell'exploit testing. L'exploit testing punta ad utilizzare le vulnerabilità identificate per compromettere lo smart meter. Esempio di exploit testing includono l'utilizzo di codice per sfruttare un buffer overflow in un servizio in esecuzione o utilizzando SQL injection per accedere ad una shell di comando attraverso una falla nella validazione di un input all'interno di una web application.

Metasploit è un exploit tool disponibile gratuitamente che offre ai tester di sicurezza e agli attaccanti un considerevole numero di *vulnerability exploit* e *payload* [45]. Per un security tester, lo scopo finale è spesso quello di



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with "File", "Edit", "View", "Terminal", and "Help". Below the menu, the Metasploit logo is displayed in a stylized font. Underneath the logo, the text reads: "[ metasploit v3.4.0-dev [core:3.4 api:1.0] + ... =[ 548 exploits - 260 auxiliary + ... =[ 208 payloads - 23 encoders - 8 nops = [ svn r9236 updated 3 days ago (2010.05.06) msf >". The bottom part of the window shows a command-line interface with the prompt "msf >".

**Figura 6.7:** Il tool di vulnerability exploit Metasploit

compromettere il target, laddove per un attaccante, la sola compromissione dello smart meter possa essere un altro passo nella propria metodologia personale di raggiungere l'obiettivo preposto.

### 6.3 False Data Injection

Nelle Smart Grid, la rete elettrica è potenziata dai più recenti progressi nei campi del sensing, della misurazione e dei dispositivi di controllo con una comunicazione bidirezionale tra produttore e consumatore. Le componenti della produzione, della trasmissione, della distribuzione ed il consumo di elettricità scambiano informazioni sullo stato della griglia che vengono recapitate agli utenti del sistema, agli operatori ed ai dispositivi.

La stima dello stato ha una funzione chiave nella costruzione di modelli *real-time* della rete elettrica nei centri di gestione dell'energia (EMC) [46]. Un modello *real-time* è una rappresentazione matematica quasi statica delle attuali condizioni all'interno di una rete elettrica interconnessa. Questa rappresentazione matematica è solitamente ottenuta dai dati provenienti dalle misurazioni e dalla telemetria che avvengono a distanza di pochi secondi nel centro di controllo dell'energia (ECC). Modelli *real-time* della rete possono essere utilizzati per fare scelte ottimali, rispettando vincoli tecnici come congestione delle linee di trasmissione, voltaggio e stabilità transiente. In pratica, sia economicamente che in termini di fattibilità, non è possibile misurare tutti i possibili stati nella rete; quindi, la stima dello stato è uno

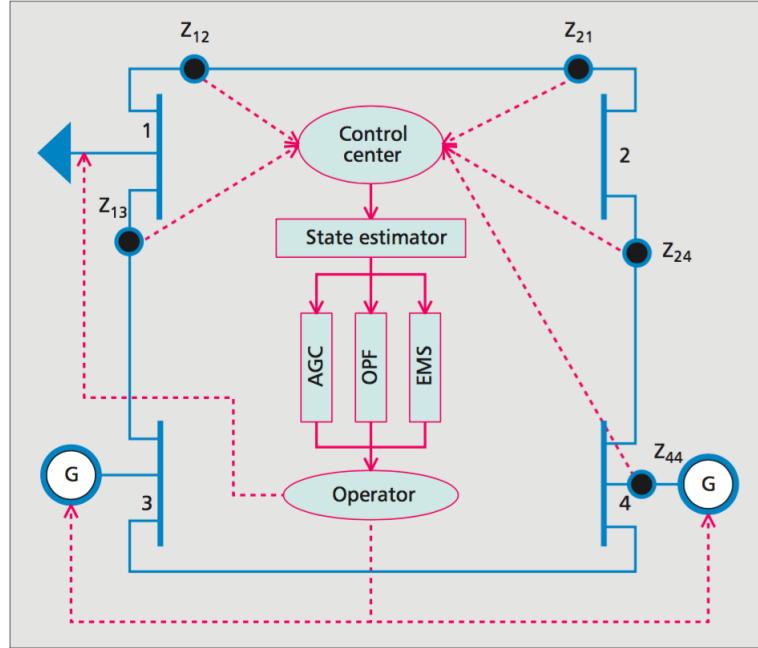
strumento utile per stimare tali quantità, a partire da un insieme limitato di misurazioni. Solitamente sono usati due tipi di informazione per la stima dello stato:

- Dati analogici di sistemi come grandi flussi di corrente alternata sulle linee principali, il carico  $P$  e  $Q$  sui generatori e trasformatori, e i voltaggi dei bus di sistema;
- Lo stato on/off dei dispositivi di switch come interruttori di circuito, switch di disconnessione, e tap dei trasformatori che determinano la topologia di rete.

Data l'importanza della stima dello stato, è fondamentale preservarlo e proteggerlo da attacchi, che si basano sull'*iniezione* di misurazioni scorrette nel sistema. Gli effetti negativi di questi tipi di attacchi sono noti in letteratura [47]. Le misurazioni scorrette possono verificarsi a causa di anomalie impreviste, o iniezioni dovute ad attacchi malevoli. Ad esempio, [48] è il lavoro pionieristico nello studio degli attacchi di *bad data injection* che non possono essere rilevati (chiamati *stealth attacks*), e mostra come un attaccante possa portare a compimento tali attacchi “*stealth*” falsificando le misure del flusso elettrico alle unità terminali remote (RTUs), manomettendo l'eterogenea rete di comunicazione o infiltrandosi all'interno del sistema della supervisione di controllo e dell'acquisizione dati (SCADA) attraverso la LAN dell'ufficio del centro di controllo. Si consideri che un sistema SCADA o un sistema di misurazione su larga area (WAMS) ottiene informazioni sulla rete elettrica (valori delle misure, stato degli interruttori, ecc.) a specifici tempi e luoghi. I centri di controllo usano le informazioni collezionate per scopi diversi, ad esempio la risoluzione di un problema di stima dello stato. In [49], viene mostrata la fattibilità degli attacchi di bad data injection non rilevabili, con l'obiettivo di manipolare i prezzi del mercato elettrico.

### 6.3.1 Stima dello stato e Bad Data Injection

I sistemi elettrici in generale consistono di tre sottosistemi: generazione, trasmissione e distribuzione. Le linee di trasmissione sono utilizzate per trasmettere la corrente elettrica generata ai consumatori. In teoria, la corrente complessiva trasmessa tra il bus  $i$  ed il bus  $j$  dipende dalla differenza di voltaggio tra i due bus, ed è funzione dell'impedenza tra questi bus. In genere, le linee di trasmissione hanno un alto rapporto reattanza/resistenza ( $X/R$ ), e quindi l'impedenza di una trasmissione può essere approssimata con la sua reattanza. La corrente attiva trasmessa dal bus  $i$  al bus  $j$  può



**Figura 6.8:** Illustrazione di una rete elettrica a quattro bus, centro di controllo, varie funzioni principali (AGC, OPF, EMS), e l'operatore. G rappresenta un generatore, il punto nero rappresenta misurazioni attive sul flusso di corrente ed il triangolo sul bus rappresenta il carico della regione o città.

essere scritta come

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j),$$

dove  $V_i$  è la tensione,  $\theta_i$  è l'angolo di fase del voltaggio nel bus  $i$ , ed  $X_{ij}$  è la reattanza della linea trasmissiva tra il bus  $i$  ed il bus  $j$ .

Negli studi del flusso di corrente DC (che in questo caso sta per linearità delle equazioni piuttosto che corrente diretta), solitamente si assume che le differenze di fase tra due bus siano piccole, e che le ampiezze dei voltaggi nei bus siano vicine all'unità (dopo essere state normalizzate). Per cui, un'ulteriore semplificazione porta ad una relazione lineare tra gli angoli di fase e la reattanza delle linee,

$$P_{ij} = \frac{\theta_i \theta_j}{X_{ij}}.$$

Negli studi sui flussi di potenza, l'angolo di fase del voltaggio ( $q_i$ ) del bus di riferimento è fissato e noto; quindi, solamente  $n - 1$  angoli devono essere stimati. I vettori di stato sono definiti come  $\mathbf{x} = [\theta_1, \dots, \theta_n]^T$ , cioè il vettore degli  $n$  angoli di fase dei bus  $\theta_i, i = 1, \dots, n$ .

Il problema della stima dello stato consiste nello stimare gli  $n$  angoli di fase  $\theta_i$ , osservando  $m$  misure in tempo reale, denotate dal vettore  $\mathbf{z}$  al centro di controllo. Queste misure potrebbero essere sia di corrente attiva trasmessa dal bus  $i$  al bus  $j$ ,  $P_{ij}$ , sia di corrente attiva al bus  $i$ ,  $P_i$ . La corrente attiva iniettata nel bus  $i$  è la super composizione della corrente trasmessa tramite le linee connesse al bus  $i$  come  $P_i = \sum_j P_{ij}$ . Il vettore delle osservazioni  $\mathbf{z}$  può essere descritto come  $\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$ , dove  $\mathbf{h}(\mathbf{x})$  è la relazione non lineare tra le misure  $\mathbf{z}$  e lo stato del sistema  $\mathbf{x}$ , ed  $\mathbf{e} = [e_1, \dots, e_m]^T$  è il vettore del rumore Gaussiano delle misure con matrice di covarianza  $\Sigma_e$ .

La matrice del Jacobiano  $\mathbf{H} \in \mathbb{R}$  è definita come

$$\mathbf{H} = \frac{\partial \mathbf{h}(\mathbf{x})}{\partial \mathbf{x}}|_{x=0}.$$

Se la differenza di fase è piccola, il modello di approssimazione lineare della misura di corrente può essere descritto come

Misura sotto Operazioni Normali:  $\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}$ .

Da notare che  $\mathbf{H}$  è generalmente sconosciuta agli attaccanti ma nota all'ISO. Date le misure sul flusso di corrente, il vettore di stato stimato  $\hat{\mathbf{x}}$  può essere computato come  $\hat{\mathbf{x}} = (\mathbf{H}^T \Sigma_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \Sigma_e^{-1} \mathbf{z}$ .

La Figura 6.8 mostra il sistema di test a quattro bus della IEEE: ogni bus ha il corrispondente voltaggio ( $V_q$ ) e l'angolo di fase ( $\theta_q$ ); il centro di controllo invia i dati delle misurazioni ( $z_{qr}$ ) ed in seguito lo stimatore di stato inferisce gli stati del sistema che possono essere utilizzati in differenti funzioni, come ad esempio il controllo della generazione automatico (AGC), il flusso di controllo ottimale (OPF), ed il sistema di gestione dell'energia (EMS). L'operatore effettua la decisione finale per il controllo dei generatori e la gestione del carico (per bilanciare la fornitura e la domanda).

### 6.3.2 Bad Data Detection

Nella stima dello stato di un sistema elettrico, i “bad data” come ad esempio bias di misurazione, derive di misura o connessioni errate devono essere identificate. Con il *bad data injection*, gli attaccanti possono iniettare dati all'interno del vettore di misure  $r$  ed il sistema può essere descritto come

Misura sotto Attacco non-Stealth:  $\mathbf{z}' = \mathbf{H}(\mathbf{x}) + \mathbf{b} + \mathbf{e}, \mathbf{a} = I\mathbf{b}$ .

Si definisce il vettore residuo  $\mathbf{r}$  come la differenza tra le qualità misurate ed i valori calcolati dagli stati stimati, precisamente,  $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ . La media e la covarianza del residuale sono rispettivamente  $E(\mathbf{r}) = 0$ , e  $cov(\mathbf{r}) = I\Sigma_e$ ,

dove  $I = \mathbf{I} - \mathbf{M}$ , ed  $\mathbf{M} = \mathbf{H}(\mathbf{H}^T \sum_e^{-1} \mathbf{H}) - \mathbf{1}\mathbf{H}^T \sum_e^{-1}$ .

I minimi quadrati pesati dell'errore di misura  $r^T \sum_e^{-1} r$  seguono la distribuzione del chi-quadro con  $n - m$  gradi di libertà [46]. L'ipotesi a riguardo del rilevamento dei dati fasulli può essere espressa come,  $\mathbf{r}^T \sum_e^{-1} \mathbf{r} \leq \chi_{n-m}^2, \zeta$ , dove  $\zeta$  è la probabilità della confidenza del rilevamento.

I residuali normalizzati, di tutte le misure, sono utilizzati per identificare i “bad data”. Se la misura corrispondente al maggior residuale normalizzato è maggiore di una soglia di identificazione fissata  $\gamma$ ,

$$\max_i(|\mathbf{r}_i|/\sqrt{\text{cov}(\mathbf{r})}) \geq \gamma,$$

allora quella misura è considerata come un dato fasullo ed è eliminato dalla stima dello stato.

### 6.3.3 Stealth Bad Data Injection

Utilizzando lo schema di rilevamento discusso precedentemente, il centro di controllo può difendersi da attacchi *naive* di data injection ed identificare la sorgente di dati corrotti. Questo tipo di attacchi sono chiamati *non stealth*. Però, se un attaccante ha conoscenza della topologia  $\mathbf{H}$ , può iniettare dati fasulli della forma  $\mathbf{H}\delta\mathbf{x}$  nella misura  $\mathbf{r}$ , più precisamente,

Misura sotto Attacco Stealth:  $\mathbf{z}' = \mathbf{H}(\mathbf{x} + \delta\mathbf{x}) + e$ .

In questo caso, il test dell'ipotesi fallirebbe il rilevamento dell'attaccante, ed il centro di controllo crederebbe che il vero stato sia  $\mathbf{x} + \delta\mathbf{x}$ . Questa è chiamata *stealth bad data injection*. Un'assunzione critica per la fattibilità di questo tipo di attacchi è la disponibilità di informazione completa sulla topologia. Tale assunzione può essere rilassata dal punto di vista dell'attaccante.

### 6.3.4 Meccanismo Difensivo

La strategia difensiva presentata in [50] si basa sull'analisi statistica online della sequenza di dati simultanea al controllo del ritardo di rilevamento e la probabilità di errore entro i livelli desiderati. I metodi di stima dello stato convenzionali [51], [52] per la *bad data detection* utilizzano le misure per bilanciare il tasso di falsi allarme o il rapporto dei rilevamenti persi. Invece, l'approccio presentato in [50] punta a minimizzare il delay di rilevamento soggetto al vincolo sulla probabilità di errore.

Si rappresenti con  $z_t$  il vettore di osservazioni  $m$ -dimensionale al tempo  $t$ . In assenza di un avversario,  $z_t$  può essere modellato, per trattabilità, come una distribuzione Gaussiana multivariata a media zero  $\mathcal{N}(0, \sum_z)$ . Si assume che l'avversario sia inattivo inizialmente; ad un tempo casuale sconosciuto  $t$ , diventa attivo ed inietta dati malevoli. L'ipotesi binaria può

essere formulata come  $\mathcal{H}_0 : \mathbf{Z}_t \sim \mathcal{N}(0, \Sigma_t)$  ed  $\mathcal{H}_1 : \mathbf{Z}_t \sim \mathcal{N}(\mathbf{a}_t, \Sigma_z)$ , dove  $\mathbf{a}_t = [a_{t,1}, a_{t,2}, \dots, a_{t,m}]^T \in R^m$  è il vettore dei dati malevoli sconosciuti iniettati dall'attaccante al tempo  $t$ , ed  $\Sigma_z$  è  $\mathbf{H} \sum_x \mathbf{H}^T + \Sigma_e$ . In altre parole, si vuole rilevare un cambiamento nella distribuzione da  $(\bar{N})(0, \Sigma_z)$  a  $(\bar{N})(\mathbf{a}_t, \Sigma_z)$  ad un tempo non noto  $t$  con  $\mathbf{a}_t$  sconosciuto.

Sia  $T_h$  lo *stopping time*, il tempo in cui viene rilevato il cambiamento. Se  $T_h < \tau$ , è un falso allarme. La lunghezza di esecuzione media (ARL) è  $T_d = E[T_h - \tau]$ . Basandosi sulla formulazione di Lorden [53], è possibile minimizzare il delay nel caso peggiore, che può essere descritto come  $T_d = \sup_{\tau \geq 1} E_\tau[T_h - \tau | T_d \geq \tau]$ . Per computare il minimo  $T_d$ , l'algoritmo CUSUM di Page è la miglior tecnica per affrontare questo tipo di problemi [53]. La maggior parte dei modelli basati su CUSUM assume la conoscenza perfetta delle funzioni di likelihood. Nella detection della bad data injection, i parametri della distribuzione  $\mathcal{H}_1$  non possono essere completamente definiti a causa dei parametri degli attaccanti e del modello statistico che non sono noti. Per cui, bisogna progettare meccanismi per il più rapido rilevamento in presenza di parametri non noti.

Il CUSUM test adattivo è ricorsivo per sua natura. Ogni ricorsione comprende due step interfogliati:

- test CUSUM multi-thread
- risolutore lineare di parametri non noti

Il CUSUM test multi-thread estende l'algoritmo di Page. Esso considera il tasso di likelihood di  $m$  misure a tempo  $t$  così da determinare il tempo di stop  $T_h$ , che può essere descritto come  $T_h = \inf\{t \geq 1 | S_t > h\}$ , in cui la soglia di rilevamento  $h$  è una funzione del tasso di falso allarme (FAR), del tasso di rilevamenti persi (MDR), e la varianza del processo, con statistiche cumulative al tempo  $t$ :  $S_t = \max_{1 \geq k \geq T_h} \sum_{t=k}^{T_h} L_t$ , con  $L_t$  pari alla somma della funzione del tasso di likelihood per tutte le misure ( $z_{t,j}, j \in \{1, 2, \dots, m\}$ ) al tempo  $t$ . È possibile esprimere  $L_t(\mathbf{Z}_t)$  come

$$\sum_{j=1}^m \log \frac{f_1(z_{t,j})}{f_0(z_{t,j})},$$

dove  $f_1(z_{t,j})$  e  $f_0(z_{t,j})$  corrispondono alla distribuzione della  $j$ -esima osservazione al tempo  $t$  sotto attacco. Al tempo  $t$ , la statistica cumulativa  $S_t$  può essere risolta ricorsivamente come  $\max[0, S_{t-1} + L_t(\mathbf{Z}_t)]$ , dove  $S_0 = 0$  quando  $t = 0$ . Il centro di controllo fa scattare un allarme quando l'accumulazione supera una determinata soglia  $h$ .

A causa di un modello statistico avversario sconosciuto, il test del tasso di likelihood generalizzato (GLRT) può essere utilizzato nell'algoritmo CUSUM di Page [53]. L'idea è quella di applicare GLRT sostituendo il parametro

sconosciuto secondo la stima a maximum likelihood. Quindi, l'espressione ricorsiva del CUSUM test non è più valida in quanto GLRT ha bisogno di computare ogni elemento non noto di ogni misurazione al tempo  $t$  stimandolo dalle osservazioni fino al tempo corrente  $t$ . In altre parole, GLRT richiede la memorizzazione delle osservazioni e l'esecuzione della stima ML dei parametri sconosciuti ad ogni punto temporale. Per cui, GLRT è troppo costoso computazionalmente da implementare in pratica per effettuare rilevamento veloce.

Per ridurre la complessità computazionale, è possibile applicare il test Rao [53], che è un modello di test asintoticamente equivalente a GLRT. Il Rao test computa le derivate rispetto al parametro non noto valutato in zero, e può essere implementato efficientemente. Inoltre, il Rao test non coinvolge la complessa computazione della stima a maximum likelihood.

### 6.3.5 Strategia di attacco

Gli attacchi stealth sono attuabili quando gli attaccanti hanno piena conoscenza della topologia. Una domanda importante che sorge spontanea è: *se la topologia non è disponibile, può un attaccante effettuare comunque stealth bad data injection?* Sorprendentemente, *si*. L'idea principale presentata in [54], si basa su parametri del sistema variabili in un piccolo range dinamico, infatti, l'informazione sulla topologia è incorporata nelle correlazioni tra le misure di flusso di potenza. Siano  $\mathbf{z}(t)$  e  $\mathbf{x}(t)$  le misure ed i vettori di stato al tempo  $t$ , dove  $\mathbf{x}(t)$  è sconosciuto. Ad un certo tempo  $t$ , è impossibile inferire  $\mathbf{H}$  solamente a partire da  $\mathbf{z}(t)$ . Comunque, con il passare del tempo, e la conoscenza delle proprietà stocastiche del processo casuale  $\mathbf{x}(t)$ , si potrebbe essere in grado di inferire  $\mathbf{H}$ .

Nei sistemi elettrici, le variabili di stato sono generalmente una funzione non lineare dei carichi  $\mathbf{y}$  e della topologia  $\mathbf{H}$ :  $\mathbf{x} = f(\mathbf{y}, \mathbf{H})$ . Mentre la topologia è nota per essere statica in un determinato periodo temporale, i carichi possono essere modellati come *indipendentemente* variabili. Se tali variazioni sono sufficientemente piccole,  $f$  può essere approssimata utilizzando  $\mathbf{x} = \mathbf{Ay}$ , dove  $\mathbf{A}$  è la matrice dei coefficienti di primo ordine dell'espansione di Taylor in  $\mathbf{y}$  ( $\mathbf{z} = \mathbf{HAy} + \mathbf{e}$ ).

Con  $\mathbf{HA}$  ed  $\mathbf{y}$ , è possibile portare a compimento l'attacco modificando i dati misurati come  $\mathbf{z}' + \mathbf{HA}\delta\mathbf{y}$ , dove  $\delta\mathbf{y}$  è scelto arbitrariamente. Il vettore di stato è stimato come  $\hat{\mathbf{x}} = (\mathbf{H}^T \sum_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \sum_e^{-1} \mathbf{z}'$ . Sia  $\delta\mathbf{x} = A\delta\mathbf{y}$ . Siccome  $r = \mathbf{z}' - \mathbf{H} \wedge \mathbf{x} = \mathbf{z} + \mathbf{H}(\hat{\mathbf{x}} + \delta\mathbf{x})$ ,  $E(\mathbf{r}) = 0$ ,  $cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M}) \sum_e$ . In altre parole, la media e la varianza di  $\mathbf{r}$  sono le stesse del caso senza

attaccanti. Quindi, utilizzando il metodo del residuale massimo, l'attacco non può essere rilevato.

Per inferire  $\mathbf{HA}$  ed  $\mathbf{y}$ , è possibile adottare la tecnica della *linear independent component analysis* (ICA). La Linear ICA [55] è un metodo sviluppato di recente che ha lo scopo di trovare una rappresentazione lineare dei dati cosicché le componenti siano quanto più statisticamente indipendenti possibile. È un caso speciale della *blind source separation*, formulata come segue.

$$\mathbf{u} = \mathbf{G}\mathbf{v},$$

con  $\mathbf{u} = [u_i, i = 1, 2, \dots, m]$  che è il vettore delle osservazioni degli  $m$  segnali di monitoraggio,  $\mathbf{G} = [g_{ij}, i = 1, 2, \dots, m, j = 1, 2, \dots, n]$  è la matrice di mixing non nota, e  $\mathbf{v} = [v_i, i = 1, 2, \dots, n]$  è il vettore delle  $n$  variabili indipendenti latenti.

Dato il modello e la realizzazione di  $\mathbf{u}$ , ICA può inferire sia la matrice di mixing  $\mathbf{G}$  che il vettore  $\mathbf{v}$  calcolando in maniera adattiva il vettore dei pesi  $\mathbf{w}$  che massimizza una misura di *non Gaussianità* del  $\mathbf{w}^T\mathbf{u}$  calcolato.

L'algoritmo è mostrato in Figura 6.9: FastICA [55], alla riga 1, è un algorit-

Input: $\mathbf{z}$ = data matrix 1. $[\mathbf{G}$ and $\mathbf{y}] = \text{FastICA}(\mathbf{z})$ 2. If $\max(\mathbf{z} - \mathbf{G}\mathbf{y}) > \epsilon$ then exit 3. Generate $\delta\mathbf{y} \sim N(0, \sigma^2)$ 4. $\mathbf{z}' = \mathbf{z} + \mathbf{G}(\mathbf{y} + \delta\mathbf{y})$ Output: false data $\mathbf{z}'$
---

**Figura 6.9:** Stealth false data injection.

mo popolare ed efficiente per la ICA che iterativamente trova la direzione in cui il vettore dei pesi  $\mathbf{w}$  massimizza la non Gaussianità della proiezione  $\mathbf{w}^T\mathbf{z}$  per i dati  $\mathbf{z}$ .  $\mathbf{G}$  deve soddisfare  $\mathbf{w}^T\mathbf{G} = \mathbf{I}$ , con  $\mathbf{I}$  matrice identità. Le entrate di  $\mathbf{G}$  minori di una certa soglia  $\epsilon$  sono rimosse. Infine, il vettore di stato  $\mathbf{y}$  può essere stimato da  $\mathbf{w}^T\mathbf{z}$ .

La riga 2 verifica che  $\mathbf{z}$  segua un modello lineare. Se le assunzioni di linearità sono valide,  $\max(\mathbf{z} - \mathbf{G}\mathbf{y})$  dovrebbe essere piccolo.

La riga 3 genera un attacco random tramite una variabile casuale Gaussiana, ed è aggiunto alla variabile inferita  $\mathbf{y}$  alla riga 4, risultando così in un attacco stealth che non può essere rilevato.

## 6.4 Disconnect Attack

Gli smart meter sono la parte più visibile della transizione verso la moderna Smart Grid. Questi sono tipicamente controllati ed interrogati attraverso comunicazioni wireless o su power-line: tali comunicazioni e possibilità di controllo remoto introducono potenziali fonti di attacco con conseguenze gravi per i consumatori ed i proprietari delle infrastrutture.

In particolare, lo switch di servizio e la possibilità di connessione/disconnessione remota (RCD) associata degli smart meter, ha colpito l'attenzione della comunità della sicurezza negli ultimi anni [56], [57], [58]. Un attacco RCD potrebbe causare un blackout diffuso su larga scala o addirittura la minaccia di compiere il suddetto attacco in cambio di soldi [56]. Questo tipo di attacco potrebbe potenzialmente danneggiare la rete elettrica o altri carichi elettrici causando deviazioni nel voltaggio o nella frequenza [57]. In tutti i casi, un attacco portato a termine avrebbe serie conseguenze politiche ed economiche.

Mentre le misure di sicurezza come la cifratura dei dati ed i sistemi di rilevamento delle intrusioni (IDS) offrono un certo livello di protezione per i sistemi AMI, essi non sono d'aiuto nel caso in cui un attaccante sia capace di compromettere il sistema e far eseguire comandi malevoli a centinaia di migliaia (o milioni) di dispositivi.

Le contromisure adottate, presenti in letteratura, fanno uso di ritardi casuali per l'esecuzione dei comandi RCD rendendo così la Smart Grid più resistente:

1. Prevenendo rapidi cambiamenti nel carico che potrebbero destabilizzare il sistema elettrico;
2. Dando il tempo di rilevare e fermare un attacco in corso.

Tali meccanismi di ritardo sono tecnicamente fattibili: alcuni meter supportano un ritardo configurabile prima di rispristinare il servizio dopo un guasto [59].

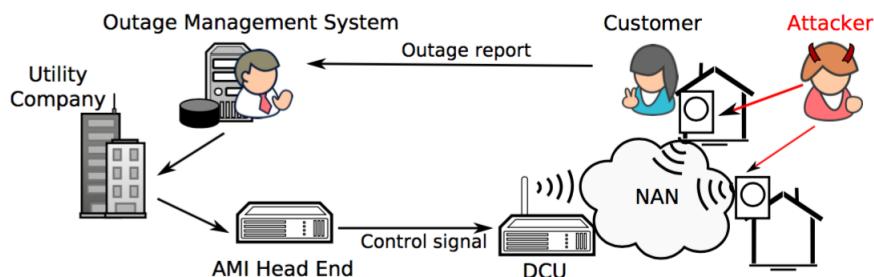
### 6.4.1 Modellare attacchi di Remote Disconnect su AMI

Si descrivono di seguito i modelli del sistema e degli attaccanti utilizzati per studiare le contromisure di *time delay* per attacchi RCD.

## Modello del sistema

Si consideri il sistema semplificato di una Smart Grid, in Figura 6.10, in cui una compagnia utilizza un'unità AMI per controllare un insieme di smart meter a casa dei propri clienti. La comunicazione tra l'unità ed il meter è instradata da più *data concentrator unit* (DCU) intermedi, posizionati in *neighborhood area networks* (NANs). L'unità può effettuare richieste di disconnessione, tramite un DCU, di qualunque meter. Il modello permette di astrarre da protocolli, tecnologie di comunicazione e funzionalità di sicurezza disponibili.

Il modello del sistema include un *outage management system* (OMS), presso



**Figura 6.10:** Ambiente semplificato. Smart Grid con AMI, sistema di gestione guasti ed un attaccante che sta inviando comandi di disconnessione da remoto ai meter.

la compagnia, raggiungibile dai clienti tramite telefono o internet. Tale OMS consente alla compagnia di aggregare ed analizzare i report degli utenti.

## Modello dell'attaccante

Si consideri un attaccante con due scopi possibili:

1. Denial-of-electrical-service per i clienti di un'azienda durante un determinato periodo di tempo;
2. Disturbo fisico della frequenza della rete elettrica attraverso l'eliminazione del carico.

L'impatto del primo attacco, un attacco di disconnessione su vasta scala in una importante città, può essere devastante ed è discusso in dettaglio in [56]. Oltre questo scenario da caso pessimo, gli attacchi RCD su scala minore (ad esempio a livello del vicinato) possono comunque avere serie ripercussioni, ed essere meno impegnativi per gli attaccanti [58]. Il secondo attacco, la

connessione/disconnessione mirata di meter per modificare i parametri del sistema elettrico, discusso in [57]. Tale attacco richiederebbe un alto livello di conoscenza del sistema così come un alto numero di dispositivi compromessi. Si modella un attaccante forte per entrambi gli scenari come segue: si assume che l'attaccante abbia la conoscenza esatta dell'infrastruttura della compagnia (inclusa la topologia di rete, le specifiche degli smart meter e le strategie di controllo) e delle contromisure impiegate dal sistema. L'attaccante può trasmettere messaggi di disconnessione ad ogni meter e tali comandi sono accettati come autentici. Questa astrazione tiene conto di un vasto numero di vettori d'attacco possibili; ad esempio, la compromissione della master key dell'unità AMI, lo sfruttamento di una falla di un protocollo debole e attacchi dall'interno da parte di un operatore AMI. L'attaccante può prevenire la trasmissione di messaggi sul canale di comunicazione primario, se necessario (ad esempio, facendo uso di jammer). L'attaccante è limitato all'interazione con l'unità, DCU e smart meter, inoltre, non può attaccare direttamente l'OMS, la compagnia o canali di comunicazione secondari.

#### 6.4.2 Contromisura Delayed Disconnect

Molte sono le contromisure a disposizione delle compagnie preoccupate per attacchi RCD. Autenticazione e schemi di gestione delle chiavi ben progettati sono componenti essenziali della soluzione, ma in assenza di potenti meccanismi di rilevamento, c'è poco da poter fare nel caso in cui un attaccante ottenga accesso al sistema. I sistemi di *intrusion detection* (IDS) sono un'area di ricerca molto attiva, ma un attaccante potrebbe essere capace di eludere o disabilitare il sistema.

Per tale ragione, [60] concentra la sua attenzione su un altro tipo di contromisura - un delay a tempo casuale per tutte le operazioni RCD. Questo delay dovrebbe essere implementato in ogni smart meter, e la configurazione dei parametri di delay dovrebbe richiedere la presenza fisica per prevenire che un attaccante li modifichi da remoto. Anche se l'IDS o le misure di autenticazione fallissero, questo meccanismo di delay renderebbe la Smart Grid più resistente preventendo rapidi cambiamenti nel carico e fornendo il tempo necessario al rilevamento di un attacco in corso così da poterlo fermare.

Le specifiche dei meccanismi di rilevamento e ripristino dipendono da molti fattori e dal sistema della compagnia. In [60] è analizzato un meccanismo di rilevamento che comprende il processo di gestione dei guasti della società, come mostrato in Figura 6.10.

Se un attaccante disconnette con successo lo smart meter di un cliente, questo

sarà in grado di contattare la compagnia e riferire la perdita di corrente entro un intervallo di tempo ragionevole. Se l'attaccante colpisce un gran numero di clienti, l'OMS della compagnia inizia a ricevere un alto numero di comunicazioni, che innescano un'investigazione. Una volta che l'investigazione stabilisce che i guasti erano di origine malevola, la compagnia può reagire. Si assume che la compagnia sia in grado di far scattare da remoto una modalità *fail-safe*, che cancella tutte le richieste di disconnessione dei meter in sospeso. Questo *trigger* può essere inviato attraverso il canale di comunicazione primario, o nel caso questo sia in controllo dell'attaccante, su un canale secondario. Una possibilità potrebbe essere quella di utilizzare radio secondarie o riconfigurabili [61]. Un'altra è l'attivazione manuale da parte dell'utente.

Ed è proprio la presenza di umani nella rete che rende questa contromisura impegnativa per un attaccante - a patto che il periodo di delay sia lungo abbastanza da far terminare il processo di rilevamento/intervento. Questo fa nascere spontanea la domanda su quanto il delay colpisca le operazioni giornaliere della compagnia, che fa uso di RCD per varie applicazioni.

#### **6.4.3 Impatto del delay sui tempi di operazioni RCD**

Si discutono quattro casi d'uso per compagnie RCD (raggruppati in tabella 6.1) e stimata la loro sensibilità ai time delay. Usando queste stime, sono sviluppate contromisure che migliorano la resistenza del sistema con basso impatto sulle operazioni giornaliere.

#### **Routing Service Switching**

Quando un cliente si trasferisce, la compagnia necessita di fare un *routine service toggling*. Le aziende possono ridurre significativamente i costi operazionali effettuando tali compiti da remoto, piuttosto che inviare tecnici sul luogo. Mentre lo switch del servizio da remoto è portato a termine in minuti [62], [63], non è un'operazione particolarmente *time-critical*. Se un'abitazione è stata sgomberata, avrà una richiesta energetica residuale molto bassa. Inoltre, mentre alla compagnia è noto un periodo di trasferimento giorni prima, non lo è l'ora esatta del giorno. Per cui, è ragionevole aspettarsi una finestra RCD di alcune ore.

## Clienti non paganti

Senza la possibilità di disconnessione da remoto, l'azienda deve disporre di personale addetto alla disconnessione dei clienti non paganti. A volte, questi tecnici sono minacciati quando provano ad accedere al meter. Quindi la disconnessione remota fornisce un guadagno assicurato, così come un beneficio di sicurezza importante. Se un cliente che dispone di uno smart meter *RCD-enabled* non paga le sue bollette, l'azienda può disporre di un “hard” switch-off, o di un “soft” switch. Così come per il routine service switching, anche questo caso d'uso non è particolarmente time-critical. Senza RCD, potrebbe tranquillamente richiedere ore o addirittura giorni identificare un cliente non pagante, schedulare la disconnessione manuale, e spedire un tecnico in quella particolare area. Per cui questo caso d'uso dovrebbe consentire una finestra RCD di qualche ora.

Num.	Caso d'uso	Beneficio Aziendale	Requisito Temporale	Alternative
1	Routine service switching	Risparmi di costi	Ore	Switch Manuale
2	Clienti non paganti	Sicurezza del dipendente, garanzia di guadagno	Ore	Switch Manuale
3	Limitazione della domanda	Gestione demand-side	Minuti - Ore	Prezzo Dinamico
4	Cancellazione del carico	Controllo del carico a basso livello	Minuti - Ore	Interruttori delle sottostazioni

**Tabella 6.1:** Casi d'uso per Smart Meter Remote Connect/Disconnect

## Limitazione della domanda

Molti meter supportano una modalità *demand limiting*, che penalizza clienti (sia attraverso la disconnessione o forzando un prezzo più alto dell'elettricità) che eccedono un livello massimo predefinito. È importante tenere presente che la domanda è definita come il carico del cliente in media su un determinato periodo di tempo [64]. In pratica, questo intervallo temporale sarebbe tra i 5 ed i 30 minuti. Se uno smart meter rileva una violazione del limite della domanda, dovrebbe essere capace di eseguire la conseguenza appropriata nel prossimo intervallo. Comunque, delay più lunghi prima dello *shutoff* potrebbero verificarsi in alcuni casi, come ad esempio un governo che imponga un limite obbligatorio per abitazione. In uno scenario del genere, la disconnessione del meter agisce da deterrente più che da meccanismo di response real-time.

## Cancellazione del carico

Sebbene le compagnie siano sempre state capaci di eliminare il carico aprendo gli interruttori di circuito, la presenza di smart meter RCD-enabled consente di avere una response più precisa. Il tempo d'esecuzione richiesto per la

cancellazione del carico differisce in funzione dell'applicazione. Ad esempio, in situazioni di emergenza la compagnia deve essere in grado di eliminare il carico in real-time. In un sistema con carenze di forniture che necessita di andare in blackout, gli smart meter RCD-enabled consentono un preciso controllo del carico con vincoli temporali meno stringenti.

#### 6.4.4 Progettazione delle contromisure di delay

Introdurre delay prima dell'esecuzione di comandi RCD dovrebbe avere un basso impatto sui casi d'uso visti nella sezione precedente, finché il delay è tenuto al di sotto di una certa soglia. Questo delay massimo è indicato da  $d_{max}$ , che è variabile dalle decine di minuti alle 2 ore circa, in base agli scenari. Si vede ora come usare questo periodo di delay per migliorare la capacità di recupero della Smart Grid.

##### Contromisura Delay: il modello

Si consideri una compagnia con  $n$  RCD-enabled smart meter. Lo scopo dell'azienda è di minimizzare il numero totale di meter disconnessi progettando una distribuzione appropriata dei delay temporali su  $[0, d_{max}]$ . Come anticipato nel Modello del sistema, si considera un processo di rilevamento che coinvolge un sistema di gestione delle interruzioni, che riceve comunicazioni sui guasti da parte degli utenti. [60] sviluppa due modelli per il processo di rilevamento da parte dell'OMS, con differenti livelli di astrazione: un modello semplificato per la valutazione analitica, ed un altro più dettagliato da utilizzare all'interno di simulazioni.

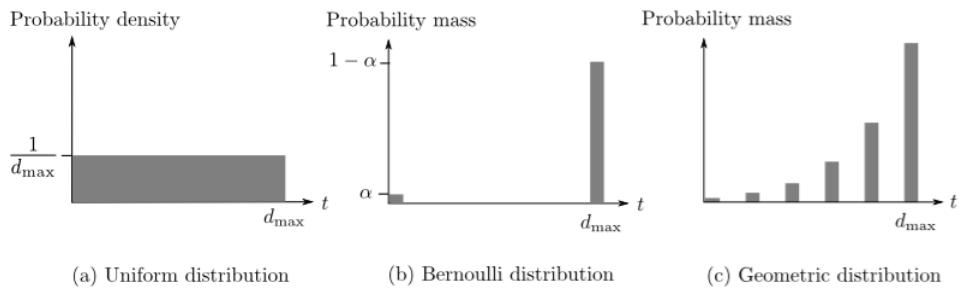
Nel modello semplificato si assume che l'azienda sia capace di rilevare e fermare un attacco in corso entro  $d$  minuti ( $d < d_{max}$ ) una volta che  $\tau$  meter siano stati disconnessi in una determinata finestra temporale. In questo modello,  $d$  include il tempo necessario affinché i clienti interessati (disconnessi) possano segnalare il guasto, ed il tempo necessario alla compagnia per investigare e concludere che sta avvenendo un attacco, ed inviare comandi che fermino tutte le connessioni in maniera *fail-safe*.

Nel modello più dettagliato, si assume che l'attacco sia rilevato una volta che siano state ricevute  $\tau'$  segnalazioni di guasto da parte dei clienti tramite l'OMS durante un periodo temporale (i tempi di segnalazione individuali sono campionati da una specifica distribuzione). Quando questa condizione è verificata, l'azienda ha tempo aggiuntivo,  $d'$ , per investigare prima di inviare comandi *fail-safe*. In ogni caso, il valore di  $\tau$  (o  $\tau'$ ) dovrebbe corrispondere

ad una piccola frazione del numero totale di meter, ma deve essere grande abbastanza da escludere la maggior parte dei guasti non relativi alla sicurezza. Il tempo di risposta  $d$  (o  $d'$ ) dovrebbe essere circa dello stesso ordine di  $d_{max}$ . L'intervallo temporale impostato per il rilevamento in accordo alla finestra temporale dell'obiettivo dell'attaccante, che si assume essere nell'ordine delle ore.

### **Meccanismi di delay**

Le performance della contromisura RCD time delay dipende dalla distribuzione del delay, che deve essere progettata contro un attaccante che può selezionare il numero di meter da colpire e pianificare quando inviare i comandi di disconnessione. Si considerino ora, tre distribuzioni di delay: uniforme, Bernoulli e geometrica. Si sviluppano i limiti analitici per il numero di meter che un attaccante può disconnettere con successo seguendo una sua strategia ottimale. La Figura 6.11 mostra le funzioni di probabilità densità/massa dei tre meccanismi.



**Figura 6.11:** Meccanismi di delay RCD.

**Delay Uniforme.** Secondo questo meccanismo di delay molto basico, una volta che un meter riceve un comando di disconnessione autenticato, esso seleziona un back-off di delay casuale uniformemente da  $[0, d_{max}]$ . Ogni meter seleziona il suo delay di back-off indipendentemente e si disconnette dopo tale tempo.

Si esamini il momento in cui  $\tau$  meter si sono appena disconnessi. Secondo il modello di rilevamento e notifica, l'azienda sarebbe in grado di fermare l'attacco entro altri  $d$  minuti, annullando tutti i comandi di disconnessione che sono ancora in corso. Durante questi  $d$  minuti, l'attaccante può continuare a disconnettere  $nd/d_{max}$  meter aggiuntivi in media, assumendo che un attaccante abbia già inviato i comandi di disconnessione a tutti i

meter. Siccome non c'è miglior strategia di attacco, questo fornisce un limite superiore al numero totale di meter disconnessi pari a  $\tau + dn/d_{max}$ , che cresce linearmente con  $n$  dato  $d/d_{max}$  costante.

**Delay Bernoulli.** Una distribuzione alternativa per ridurre il numero di meter disconnessi è la distribuzione di Bernoulli. In pratica, ogni meter lancia una moneta truccata per scegliere tra due possibili intervalli, ognuno di almeno 10 secondi per evitare problemi di stabilità. In particolare, con probabilità  $\alpha$  (parametro di sistema), il meter si disconnette quasi immediatamente. Altrimenti, esso pospone la sua disconnessione verso la fine del periodo consentito ( $delay \approx d_{max}$ ). L'intuizione alla base è semplice: se sono attaccati un gran numero di meter, quelli che si disconnettono quasi immediatamente innescherebbero il rilevamento da parte dell'OMS, che a sua volta ferma l'attacco in corso per la maggior parte dei meter che pospongono la disconnessione.

In questo caso la miglior strategia per un attaccante è di non inviare comandi di disconnessione a tutti gli  $n$  meter in un solo colpo: continuando ad utilizzare questa strategia consentirebbe alla compagnia di impostare  $\alpha$  ad un valore molto basso così da ridurre il numero di meter disconnessi. Invece, un attaccante può massimizzare il numero di meter disconnessi lanciando un attacco *two-batch*: l'attaccante sceglie il numero totale di meter in un primo gruppo così che il sottoinsieme di meter disconnessi immediatamente non faccia scattare la notifica. Nel momento in cui il sottoinsieme di meter del primo gruppo che sceglie di posporre inizia a disconnettersi (e notificherà presto all'azienda), l'attaccante invia i comandi a tutti gli altri meter. Sotto un attacco del genere, tutti i meter nel primo gruppo e, ci si aspetta, un sottoinsieme di una frazione  $\alpha$  dei meter nel secondo gruppo si sarebbero disconnessi prima che i comandi di disconnessione in attesa siano annullati. Sommando questi due termini otteniamo un limite superiore al numero totale di meter disconnessi pari a  $\tau/\alpha + (n - \tau/\alpha)\alpha$ . L'azienda potrebbe scegliere strategicamente  $\alpha = \sqrt{\tau/n}$  per minimizzare il limite a  $2\sqrt{\tau n} - \tau$ , che cresce in maniera sublineare in  $n$ .

**Delay Geometrico.** Se il delay RCD massimo  $d_{max}$  è poche volte maggiore di  $d$ , la compagnia può ridurre ulteriormente il numero di meter disconnessi applicando una distribuzione geometrica sui periodi di delay consentiti. Sia  $k = [d_{max}/d]$ . Con questo meccanismo di delay, un meter sceglierà tra  $k$  possibili intervalli, con l' $i$ -esimo ( $i = 1, \dots, k$ ) intervallo di delay di durata circa  $(i-1)d/d_{max}$  e scelto con probabilità  $(\beta^i - \beta^{i-1})/(\beta^k - 1)$ . In questo

caso,  $\beta$  è un parametro di sistema che può essere ottimizzato in accordo a  $k$  ed altri parametri (ad esempio  $n$  e  $\tau$ ). Si noti che quando  $k = 2$ , l'ottimizzazione di  $\beta$  degenererebbe il meccanismo di delay geometrico nel meccanismo di delay Bernoulliano.

Utilizzando questa distribuzione geometrica ed il modello definito in precedenza, a prescindere dalla strategia adottata dall'attaccante, in media meno di  $\tau(1 + \beta) + (n - \tau)(\beta - 1)/(\beta^k - 1)$  meter sarebbero disconnessi. Il primo termine limita il numero di meter a cui è stato inviato il comando di disconnessione prima che  $\tau$  meter siano disconnessi, ed il secondo termine limita il numero di meter a cui è stato inviato il comando di disconnessione dopo di ciò. Con la costante  $\beta$ , il primo termine cresce linearmente con  $\tau$ , che è una piccola frazione di  $n$ , ed il secondo termine decade geometricamente con  $k$ , che sarà anch'esso una piccola frazione di  $n$ , anche per piccoli valori di  $k$ .

Delay mechanism	Number of disconnected meters	
	Analytical bound	Example
Uniform	$\tau + dn/d_{\max}$	$\approx 100,000$
Bernoulli	$2\sqrt{\tau n} - \tau$	$\approx 48,000$
Geometric (with $\beta = 3$ )	$4\tau + \frac{2(n-\tau)}{3^{d_{\max}/d}-1}$	$\approx 5,600$

**Figura 6.12:** Riepilogo dell'analisi con un setting d'esempio di  $d = 10$  min,  $d_{\max} = 60$  min,  $\tau = 1000$  ed  $n = 600.000$ .

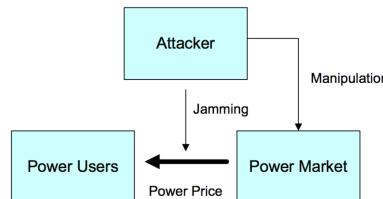
**Riepilogo.** La Figura 6.12 riassume i risultati analitici per i tre meccanismi di delay. Per ognuno di essi, il numero di meter disconnessi cresce ad un tasso asintotico differente rispetto ad  $n$ . Come illustrato nel setting d'esempio, secondo il meccanismo di delay geometrico, fin quando  $d_{\max}$  è poche volte (ad esempio,  $6\times$ ) maggiore di  $d$ , il numero di meter disconnessi sarà piccolo ( $< 1\%$  di  $n$ ). In confronto, secondo il meccanismo di delay uniforme, un numero significativamente maggiore di meter ( $> 10\%$  di  $n$ ) sarebbe disconnesso. Per il meccanismo di delay di Bernoulli, il numero di meter disconnessi è nell'ordine di  $\sqrt{\tau n}$ , quindi dipende altamente dalla soglia di rilevamento  $\tau$ . Quando  $\tau$  è circa lo 0.2% di  $n$  (come nei setting d'esempio), il numero di meter disconnessi può comunque raggiungere circa l'8% di  $n$ . Un confronto di questi tre meccanismi di delay suggerisce:

1. Se possibile, un'azienda dovrebbe rendere  $d_{max}$  svariate volte maggiore di  $d$ , ed utilizzare il meccanismo di delay geometrico;
2. Altrimenti, se  $\lceil d_{max}/d \rceil = 2$  ed il meccanismo di distribuzione geometrico degenera al Bernoulliano, la compagnia deve portare la sua soglia di rilevamento  $\tau$  al valore minore possibile per favorire la propria capacità di recupero sotto attacchi RCD.

## 6.5 Jamming

L'infrastruttura di comunicazione svolge un ruolo predominante nelle Smart Grid. Si occupa principalmente di broadcast real-time del prezzo della corrente, di riportare i consumi energetici e di monitorare lo stato del sistema. Grazie allo scambio di informazioni in tempo reale un utente è in grado di determinare il proprio consumo energetico ottimale.

Così come i vantaggi, l'infrastruttura di comunicazione presenta alcune vulnerabilità. In questa sezione, si analizza in dettaglio una strategia di attacco che manipola il mercato elettrico utilizzando la tecnica del *Jamming*. Questo attacco causa cambiamenti nei consumi energetici e tende quindi a destabilizzare le power grid (vedi Figura 6.13).



**Figura 6.13:** Un'illustrazione della manipolazione del mercato attraverso il Jamming

Si assume che è utilizzato un sistema di comunicazione wireless, come Wi-MAX, per effettuare il broadcast delle informazioni relative ai prezzi. Un attaccante, utilizzando un jammer molto potente in un'area abbastanza vasta, disturba l'invio real-time dei prezzi[68]. Si assume che ogni consumer continua a far riferimento al vecchio prezzo in quanto le informazioni aggiornate sul prezzo non arrivano a destinazione. L'attaccante continua a fare jamming fin quando non c'è una variazione reale sul prezzo. Una volta ricevuto il nuovo prezzo, gli utenti coinvolti modificheranno e/o si adegueranno, causandone una diminuzione o un incremento, facile da predire.

In questo modo un attaccante può cambiare il prezzo della corrente quando e nella direzione in cui vuole.

### **6.5.1 Strategia di attacco**

Descrizione relativa alla procedura d'attacco:

1. L'attaccante fa jamming in un'area molto popolata;
2. L'utente coinvolto è a conoscenza del vecchio prezzo della corrente dal momento in cui il nuovo prezzo non gli è noto;
3. L'attaccante monitora il mercato elettrico e continua a fare jamming;
4. Nel momento in cui il prezzo cambia significativamente, si smette di fare jamming;
5. Ogni utente adatta il suo consumo energetico in base al nuovo prezzo. Se il nuovo prezzo è superiore al vecchio, l'utente diminuisce i suoi consumi, facendo calare il prezzo della corrente con alta probabilità. Viceversa, se il nuovo prezzo è più piccolo, un utente incrementa i suoi consumi, aumentando con alta probabilità il prezzo dell'energia;
6. L'attaccante può avere dei profitti dalla manipolazione del mercato.

### **6.5.2 Contromisure**

A causa dei potenziali gravi danni che questo attacco può infliggere al mercato elettrico, il meccanismo price-response deve essere in grado di impedire un tale attacco. L'essenza della contromisura sta nell'evitare di modificare il consumo di energia in maniera simultanea. L'idea è basata sui protocolli come l'Aloha e CSMA, in cui i diversi trasmettitori utilizzano backoff casuali per evitare le collisioni dovute a trasmissioni simultanee. Ogni consumer sceglie un tempo casuale per cambiare la propria power response evitando che l'attaccante possa predire il comportamento dell'utente e quindi capire in che modo varia il prezzo della corrente.

# Bibliografia

- [1] Tony Flick and Justin Morehouse. *Securing the Smart Grid. Next Generation Power Grid Security*. Elsevier Inc, 2011.
- [2] Stuart Borlase. *Smart Grids: Infrastructure, Technology, and Solutions*. CRC Press, 2013.
- [3] Janaka Ekanayake, Kithsiri Liyanage, Jianzhong Wu, Akihiko Yokoyama and Nick Jenkins. *Smart Grid: Technology and Applications*. Wiley, 2012.
- [4] Hassan Farhangi. The Path of the Smart Grid. In *IEEE power & energy magazine*, pages 18-28, january/february 2010.
- [5] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. In *IEEE Communications Surveys & Tutorials*, vol.15, no.1, 2013.
- [6] Nico Saputro, Kemal Akkaya and Suleyman Uludag. *A survey of routing protocols for smart grid communications*. In Computer Networks 56, pages 2742–2771, 2012.
- [7] Xi Fang, Satyajayant Misra, Guoliang Xue and Dejun Yang. *Smart Grid – The New and Improved Power Grid: A Survey*. In IEEE Communications Surveys & Tutorials, vol.14, no.4, 2012.
- [8] Fundamental of Electricity: Radial, Loop, & Network Systems. <http://epb.apogee.net/foe/ftdstr.asp>
- [9] NIST Website about Smart Grids. <http://www.nist.gov/smartgrid/>
- [10] Gungor VC, et al. *A survey on smart grid potential applications and communication requirements*. IEEE Trans. Ind. Inform. 2013;9(1):28–42.

- [11] M. Lee, O. Aslam, B. Foster, D. Kathan, J. Kwok, L. Medearis, R. Palmer, P. Sporborg, and M. Tita. *Assessment of demand response and advanced metering*. Federal Energy Regulatory Commission, Tech. Rep., 2013 <https://www.ferc.gov/legal/staff-reports/12-20-12-demand-response.pdf>
- [12] C. McKerracher, J. Torriti. *Energy consumption feedback in perspective: integrating australian data to meta-analyses on in home displays*. Energy Effic. 2012;6(2), 387–405.
- [13] Morgan Trevor. *Smart Grids and Electric Vehicles Made for Each Other*. Germany: International Transport Forum on Seamless Transport, Discussion Paper; 2012.
- [14] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang. *Smart transmission grid: Vision and framework*. IEEE Trans. on Smart Grid, 1(2):168–177, 2010.
- [15] K. Vu, M. M. Begovic, D. Novosel, and M. M. Saha. *Use of local measurements to estimate voltage-stability margin*, IEEE Trans. Power Syst., vol. 14, no. 3, pp. 1029–1035, Aug. 1999.
- [16] B. Milosevic and M. Begovic. *Voltage-stability protection and control using a wide-area network of phasor measurements*, IEEE Trans. Power Syst., vol. 18, no. 1, pp. 121–127, Feb. 2003.
- [17] D. Povh, D. Retzmann, J. Kreusel. *Integrated AC/DC transmission systems — Benefits of power electronics for security and sustainability of power supply*. PSCC 2008, Glasgow, U.K., July 14–17, 2008.
- [18] European Technology Platform. *Vision and Strategy for Europe's Electricity Networks of the Future*. European Commission. [https://ec.europa.eu/research/energy/pdf/smartgrids\\_en.pdf](https://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf)
- [19] W. Breuer, D. Povh, D. Retzmann, and E. Teltsch. *Trends for future HVDC Applications*. 16th CEPSI, Mumbai November 6–10, 2006.
- [20] Yvonne-Anne Pignolet, Holger Elias, Timo Kyntäjä, Ignacio Martín Díaz de Cerio, Jürgen Heiles, Didier Boëda, Raphael Caire. *Future Internet for Smart Distribution Systems*. IEEE PES Innovative Smart Grid Technologies (ISGT) Europe Conference, 2012.
- [21] Low, D. (2011) IEEE 802.3 Ethernet, IEEE, March 2011, <http://www.ieee802.org/minutes/2011-March/802%20workshop/index.shtml>.

- [22] ZigBee. <http://www.zigbee.org>
- [23] Cudak, M. (ed.) (2010) IEEE 802.16m System Requirements, IEEE 802.16 Task Group M, January 2010, [http://ieee802.org/16/tgm/docs/80216m-07\\_002r10.pdf](http://ieee802.org/16/tgm/docs/80216m-07_002r10.pdf).
- [24] IEEE Power & Energy Society (2010) IEEE Std 1815TM-2010. *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, June.
- [25] Jianqing Zhangand Carl A. Gunter. *IEC 61850 - Communication networks and systems in substation: An overview of computer science*. University of Illinois at Urbana Champaign, Jan. 2010.
- [26] T. Dierks, E. Rescorla. *RFC 5246: The Transport Layer Security (TLS) Protocol*. Version 1.2, August 2008.
- [27] International Organization for Standardization. *ISO/IEC 14908-1:2012: Information technology – Control network protocol – Part 1: Protocol stack*, 2012.
- [28] Vaudenay, S.: *Security Flaws Induced by CBC Padding — Applications to SSL, IPSEC, WTLS ...* In: Knudsen, L.R. (ed.) Advances in Cryptology — EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 – May 2, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2332, pp. 534–546. Springer (2002)
- [29] ETSI: Open Smart Grid Protocol (OSGP). Reference DGS/OSG-001, European Telecommunications Standards Institute, Sophia Antipolis Cedex – France (January 2012). <http://www.osgp.org/>
- [30] Differential cryptanalysis. [https://en.wikipedia.org/wiki/Differential\\_cryptanalysis](https://en.wikipedia.org/wiki/Differential_cryptanalysis)
- [31] Jovanovic, Philipp, and Samuel Neves. *Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol*, Cryptology ePrint Archive, Report 2015/428, 2015.
- [32] Andreas Klein. *Attacks on the RC4 stream cipher*. Des. Codes Cryptography, 48(3):269–286, 2008.

- [33] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. *Breaking 104 bit WEP in less than 60 seconds*. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, Information Security Applications, 8th International Workshop, WISA 2007, Jeju Island, Korea, August 27-29, 2007, Revised Selected Papers, volume 4867 of Lecture Notes in Computer Science, pages 188–202. Springer, 2007.
- [34] AlFardan, N.J., Bernstein, D.J., Paterson, K.G., Poettering, B., Schuldt, J.C.N.: *On the Security of RC4 in TLS*. In: King, S.T. (ed.) Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14–16, 2013. pp. 305–320. USENIX Association (2013).
- [35] Fluhrer S.R., Mantin I., Shamir A.: *Weaknesses in the Key Scheduling Algorithm of RC4*. In: Vaudenay, S., Youssef, A.M. (eds.) Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers. Lecture Notes in Computer Science, vol. 2259, pp. 1–24. Springer (2001)
- [36] Fluhrer S.R., McGrew D.A.: *Statistical Analysis of the Alleged RC4 Keystream Generator*. In: Schneier, B. (ed.) Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10–12, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1978, pp. 19–30. Springer (2000)
- [37] Gupta S.S., Maitra S., Paul G., Sarkar S.: *(Non-)Random Sequences from (Non-)Random Permutations – Analysis of RC4 Stream Cipher*. J. Cryptology 27(1), 67–108 (2014).
- [38] Hertzog P., OSSTMM - Open Source Security Testing Methodology Manual. Institute for Security and Open Methodologies. <http://www.isecom.org/osstmm>
- [39] Aircrack-ng. <http://www.aircrack-ng.org/>
- [40] Kali Linux. <https://www.kali.org/>
- [41] Wireshark. <https://www.wireshark.org/>
- [42] Nmap. <https://www.nmap.org/>
- [43] Nessus. <https://www.nessus.org/>
- [44] Cain & Abel. <http://www.oxid.it/>

- [45] Metasploit. <http://www.metasploit.com/>
- [46] A. Monticelli. *Electric Power System State Estimation*. Proc. IEEE, vol. 88, Feb. 2000, pp. 262–82.
- [47] M. Esmalifalak, Z. Han, and L. Song, *Effect of Stealthy Bad Data Injection On Network Congestion In Market Based Power System*. IEEE WCNC 2012, Paris, France, Apr. 2010.
- [48] Y. Liu, M. K. Reiter, and P. Ning. *False Data Injection Attacks Against State Estimation in Electric Power Grids*. 16th ACM Conf. Computer and Commun. Security, Gaithersburg, MD, Nov. 2009, pp. 21–30.
- [49] L. Xie, Y. Mo, and B. Sinopoli. *False Data Injection Attacks in Electricity Markets*. 1st IEEE Int'l. Conf. Smart Grid Commun., Gaithersburg, MD, Oct. 2010, pp. 226–31.
- [50] Huang, Yi, et al. *Bad data injection in smart grid: attack and defense mechanisms*. Communications Magazine, IEEE 51.1 (2013): 27-33.
- [51] A. Abur and A. G. Exposito. *Power System State Estimation: Theory and Implementation*. Marcel Dekker, 2004.
- [52] A. J. Wood and B. F. Wollenberg. *Power Generation, Operation, and Control*. Wiley, 1996.
- [53] H. V. Poor and Q. Hadjiliadis. *Quickest Detection*. Cambridge Univ. Press, 2008.
- [54] Esmalifalak M., Huy Nguyen, Rong Zheng, Zhu Han. *Stealth false data injection using independent component analysis in smart grid* Smart Grid Communications (SmartGridComm) 2011 IEEE International Conference, vol., no., pp.244-248, 17-20 Oct. 2011.
- [55] J. Himberg and A. Hyvarinen, *Independent Component Analysis for Binary Data: An Experimental Study*. 3rd Int'l. Conf. Independent Component Analysis and Blind Signal Separation, Malm, Sweden, June 2001.
- [56] R. Anderson and S. Fuloria, *Who controls the off switch?*. Proc. of the Conference on Smart Grid Communications (SmartGridComm), 2010.
- [57] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou and C. Saunders. *Remote control of smart meters: friend or foe?*. Proc. of the European Conference on Computer Network Defense (EC2ND), 2011.

- [58] D. Grochocki, J. H. Huh, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, *AMI threats, intrusion detection requirements and deployment recommendations*. Proc. of the Conference on Smart Grid Communications (SmartGridComm), 2012.
- [59] *GE I-210+ remote disconnect FAQs* [http://www.tantalus.com/pdf/products/TUNet\\_TC\\_1110-1210RD\\_plus-R3-2.pdf](http://www.tantalus.com/pdf/products/TUNet_TC_1110-1210RD_plus-R3-2.pdf).
- [60] Temple, William G., Binbin Chen and Nils Ole Tippenhauer. *Delay makes a difference: Smart grid resilience under remote meter disconnect attack*. Smart Grid Communications (SmartGridComm). IEEE International Conference on. IEEE, 2013.
- [61] A. Ghassemi, S. Bavarian, and L. Lampe, *Cognitive radio for smart grid communications*. Proc. of the Conference on Smart Grid Communications (SmartGridComm), 2010.
- [62] *Avista utilities update to idaho public utility commission staff on remote reconnect/disconnect pilot* <http://www.puc.idaho.gov/fileroom/cases/elec/AVU/AVUE0709/company/20130211UPDATE%20ON%20REMOTE%20RECONNECT%20DISCONNECT.PDF>.
- [63] *Texas-new mexico power company's request for approval of an advanced metering system (ams) deployment and ams surcharge* [https://www.smartgrid.gov/files/TexasNew\\_Mexico\\_Power\\_Company\\_Request\\_For\\_Approval\\_Advance\\_201005.pdf](https://www.smartgrid.gov/files/TexasNew_Mexico_Power_Company_Request_For_Approval_Advance_201005.pdf).
- [64] W. H. Kersting. *Distribution system modeling and analysis*. CRC Press, LLC, 2012.
- [65] F. Li and R. Bo. *Congestion and price prediction under load variation*. IEEE Control System Magazine, vol.19, pp.59–70, Oct. 2009.
- [66] Lipmaa H., Moriai S.: Efficient Algorithms for Computing Differential Properties of Addition. In: Matsui, M. (ed.) Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2–4, 2001 Revised Papers. Lecture Notes in Computer Science, vol. 2355, pp. 336–350. Springer (2001).
- [67] *Open Smart Grid Protocol (OSGP)*. ETSI. [http://www.etsi.org/deliver/etsi\\_gs/osg/001\\_099/001/01.01.01\\_60/gs osg001v010101p.pdf](http://www.etsi.org/deliver/etsi_gs/osg/001_099/001/01.01.01_60/gs osg001v010101p.pdf)

- [68] Li, Husheng, Zhu Han. *Manipulating the electricity power market via jamming the price signaling in smart grid*. GLOBECOM Workshops, IEEE 2011.