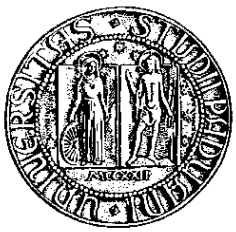


Università degli Studi di Padova

FACOLTÀ DI INGEGNERIA
Corso di Laurea Triennale in Ingegneria Elettronica

Tesi di laurea triennale

Infrastrutture di misura e problematiche di sicurezza nelle reti intelligenti (Smart Grid)

Candidato:
Federico Rodighiero
Matricola 571295

Relatore:
Simone Buso

Anno Accademico 2010–2011

Indice

Introduzione

La caratteristica che più distingue il XX secolo dai precedenti è la rapida crescita tecnologica. La diffusione della scienza e della ricerca ha portato a progressi sorprendenti nei campi più importanti dell'ingegneria, come le telecomunicazioni e i trasporti, e nel settore della medicina. Tanto per ricordarne alcuni: la diffusione dell'automobile e l'aereo, l'uomo sulla luna, l'elettrificazione dei paesi, con conseguente arrivo nelle case di frigorifero, radio televisione e computer. La lista è lunghissima, ma quello che è importante notare è come tutto questo abbia portato ad un generale miglioramento delle condizioni di vita.

Con questi miglioramenti la popolazione mondiale è passata da 1.65 miliardi di persone nel 1900 ai quasi 7 miliardi dei giorni nostri [1] e tutto questo incremento ha contribuito ad accrescere anche i consumi di energia.

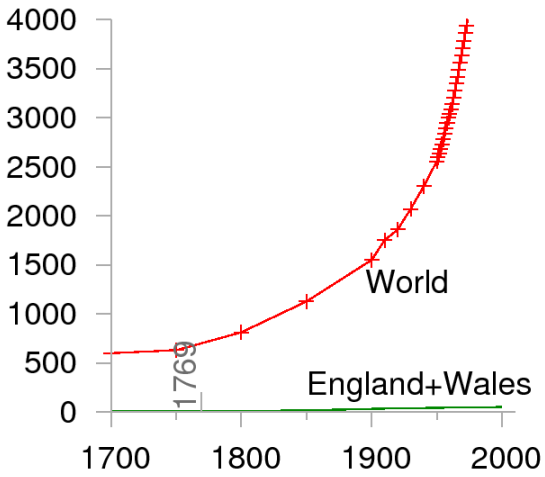


Figura 1: Aumento della popolazione mondiale dal 1700 al 2000 [28].

Energia in senso generico, non limitato all'elettricità ma esteso anche all'utilizzo di petrolio,gas e carbone (figura 2). L'elettricità stessa è in gran parte prodotta dalla combustione di fonti fossili (figura 3) con conseguente inquinamento ambientale. Di particolare gravità è l'emissione di gas nocivi (figura 4) che hanno contribuito a creare il cosiddetto effetto serra. Ed è proprio a causa dell'odierna situazione del sistema climatico che negli ultimi decenni si è assistito ad un progressivo interesse per la tutela ambientale. Questo interesse ha portato in tempi recenti alla fondazione di enti sovranazionali con lo scopo di monitorare, regola-

[1] la figura 1 riporta i dati fino al 2000 ma ad oggi si stima che la popolazione abbia quasi raggiunto i 7 miliardi [1]

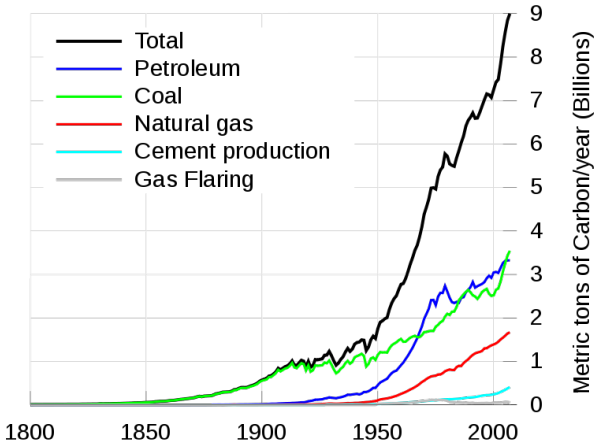


Figura 2: Consumo di fonti fossili dal 1800 ad oggi [50].

mentare le emissioni inquinanti e trovare una soluzione che ci consenta di trovare un equilibrio sostenibile tra consumi e inquinamento. Dai vari summit è emerso che essendo impossibile fermare la crescita demografica e altrettanto difficile rinunciare alle attuali comodità, cui siamo abituati, l'unica strada perseguibile è quella di trovare un modo alternativo e meno inquinante per la generazione dell'energia. Tale esigenza, con le attuali tecnologie disponibili, si traduce nella necessità di aumentare e usare al meglio l'energia prodotta dalle fonti energetiche rinnovabili. Questo tipo di fonti energetiche soffre però di due grosse limitazioni, l'irregolarità della fornitura e il basso rendimento in termini di rapporto costo/produzione e dimensioni/produzione. Per poter quindi sfruttare questo tipo di risorse è necessario rendere più flessibile il sistema di trasmissione, che nella maggior parte dei paesi è rimasto quello della grande elettrificazione avvenuta intorno gli anni '40. Il sistema di trasmissione di quel tempo era stato studiato bene per le esigenze di allora, ha consentito l'ultimo sviluppo economico ed è tuttora in grado di fornirci elettricità con un discreto grado di affidabilità (99.7%). Tuttavia, con un massiccio ingresso di fonti rinnovabili e auto elettriche la rete è destinata al collasso; si presenta infatti estesa e robusta nella struttura, ma, al tempo stesso, lenta e rigida rispetto a qualunque cambiamento di assetto. Tanto lenta che negli ultimi 60 anni i cambiamenti sono stati veramente rari e, per sottolineare quanto poco sia cambiato il sistema di trasmissione, si è soliti paragonarlo ai settori dell'Information and Communications Technology (ICT). Si ipotizza infatti che se Alexander Graham Bell si trovasse ai giorni nostri avrebbe grosse difficoltà a trovare qualcosa di simile al suo telefono negli attuali cellulari o nel Voice over Internet Protocol (voIP) mentre Thomas Edison sarebbe totalmente a suo agio nelle attuali reti elettriche [15]. Si nota quindi che le reti elettriche, allo stato attuale, non sono adeguate alle tecnologie attualmente disponibili né per i cambiamenti che ci investiranno nei prossimi anni. Da qui l'urgenza di un rinnovamento della rete, sia nella struttura che nella concezione. É proprio questo lo scopo delle Smart Grid, reinventare il sistema dell'energia elettrica.

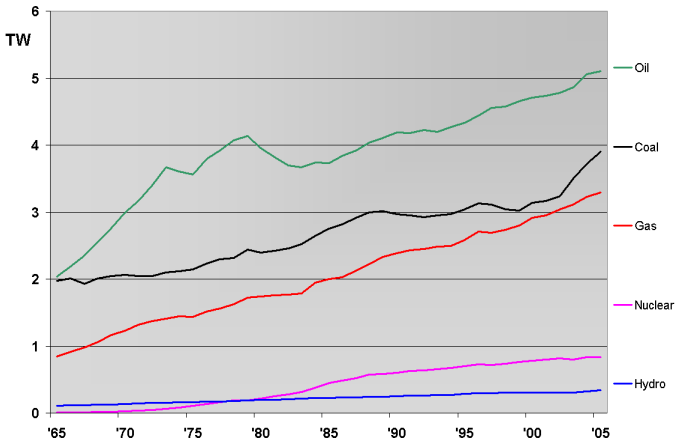


Figura 3: Consumo di energia elettrica mondiale e fonti di provenienza [54].

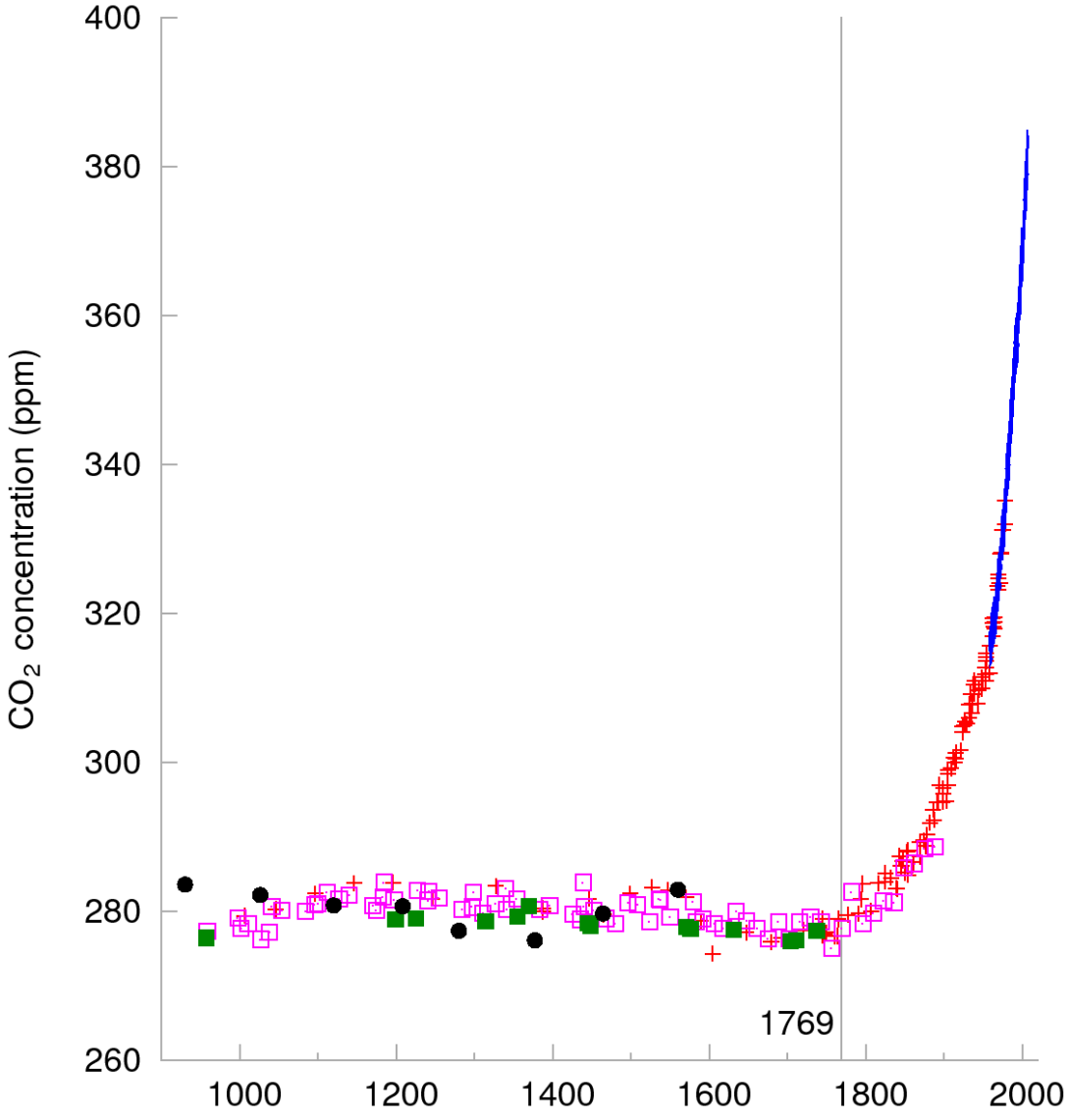


Figura 4: Concentrazione di CO_2 dell' ultimo millennio misurata in parti per milione [28].

Capitolo 1

Smart-Grid: Cosa sono e perché saranno essenziali

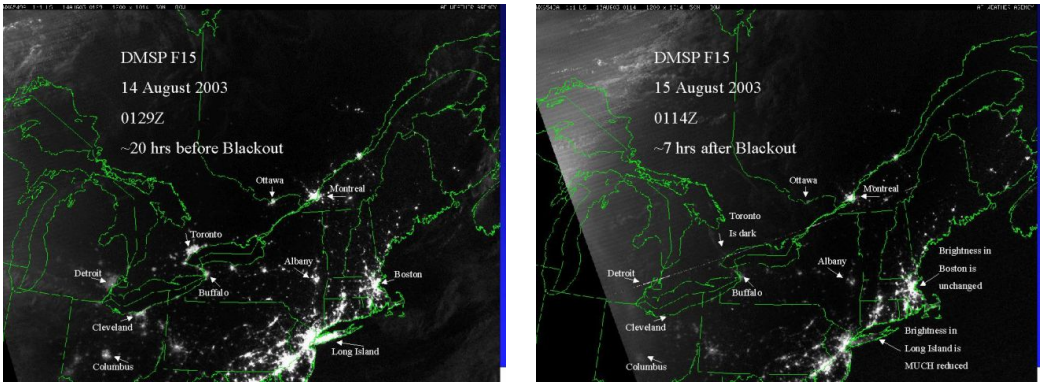
Smart Grid è un termine derivante dall'inglese; usualmente non si traduce in italiano ma il significato di *smart* in questo caso sarebbe: intelligente, sveglio, furbo. La parola vuole rendere l'idea di un sistema attivo, in grado di prendere decisioni in modo autonomo, efficace, intelligente. In ambito tecnico, quando si parla di Smart Grid, si fa riferimento a tutto quell'insieme di innovazioni atte a rinnovare la rete elettrica odierna. Prima di andare a vedere da cosa sono composte queste nuove reti, è utile analizzare in dettaglio quali sono i problemi delle attuali reti così facendo, risulterà più immediato capire il perché di certe scelte progettuali.

1.1 I limiti delle reti di oggi

1.1.1 Affidabilità

Al giorno d'oggi le reti sono concepite con una struttura centralizzata, una grande centrale con una vasta rete di trasmissione che alimenta molte utenze. In Italia ci sono circa 40 grosse centrali [1] con 62000 chilometri di linee [47] che alimentano quasi 9 milioni di utenze [2] inoltre, importiamo moltissima energia dall'estero(il 13% del nostro fabbisogno [48, p. 11]). Questo fa del caso italiano un esempio non in linea con gli altri paesi, ma i numeri danno comunque un'idea della situazione. Il sistema è dunque formato da pochi punti nevralgici di estrema importanza per il funzionamento della rete nazionale. Nel momento in cui venisse a mancare, per un qualche motivo, l'apporto energetico di una centrale importante, una vasta area del paese potrebbe restare al buio, a causa della reazione a catena prodotta da tale incidente. É quanto avvenne il 28 settembre 2003 quando l'Italia intera (tranne Sardegna e Capri) restò senza corrente per oltre 12 ore; in quel caso la causa fu un guasto su una linea ad Alta Tensione (AT) che portava energia dalla Svizzera [21]. Tale imprevisto provocò un sovraccarico sulle altre linee che portano corrente all'Italia; essendo notte, le nostre centrali erano al minimo della loro capacità di produzione e, data la rapidità con cui avvengono queste cose, non furono in grado

[1] dato ottenuto considerando le centrali con una produzione superiore ai 500 MW dalla lista [51]



(a) 20 ore prima del blackout (b) 7 ore dopo il blackout

Figura 1.1: Immagini dei satelliti del DMSP prima e durante il blackout del 2003 nel nord-ovest dell'america [34].

di andare a regime. Al fine di mostrare come questo tipo di problemi non affligga solo il nostro paese è bene ricordare che sempre nel 2003, il Nord America, nella notte del 14, agosto (figura 1.1) subì uno dei più grandi blackout della sua storia, con 55 milioni di persone al buio per oltre 12 ore.

Questi fatti, per quanto rari, sono comunque molto dannosi sia per i disagi arrecati alle persone che per le perdite economiche a cui portano; ciò nonostante fungono anche da campanello d'allarme. In questo caso mettono in luce la contraddizione della società in cui viviamo, dove la tecnologia regna sovrana in molti ambiti, ma continua a dipendere da un sistema elettrico centralizzato e costruito molto prima dell'avvento dei microprocessori [15]. Volendo riassumere, la situazione descritta e gli esempi presentati ci indicano chiaramente che l'aumento di affidabilità sarà una delle sfide che le Smart Grid dovranno affrontare.

1.1.2 Mancanza di infrastrutture di comunicazione adeguate

Nella sezione precedente abbiamo illustrato come l'attuale rete elettrica sia basata su una struttura gerarchica, dove ai piani più alti troviamo le centrali che, oltre a svolgere la funzione di generazione, sono spesso adibite a sede di controllo e monitoraggio della rete. Questa tipologia di organizzazione, oltre la scarsa affidabilità, presenta un'ulteriore limitazione; è molto poco automatizzata e c'è bisogno di una consistente supervisione umana. Tale problematica è legata ai limiti dell'infrastruttura comunicativa degli attuali sistemi di controllo (figura 1.2). Tali sistemi, detti Supervisory Control and Data Acquisition (SCADA), sono formati dai vari sensori e attuatori delle cabine elettriche, che comunicano con la centrale di controllo tramite delle apposite linee telefoniche, tipicamente usando dei modem da 1200 baud [18]. Il problema di questa tipologia di sistema è la lentezza di comunicazione; i sensori rilevano moltissimi dati, ma, a causa dei limiti della banda, non è possibile ricevere i risultati in real-time nella centrale e, tantomeno, attivare le protezioni in caso di bisogno, dato che il più delle volte, i dati ricevuti in centrale sono in ritardo di 2-5 secondi[40]. Pertanto, qualora una cabina si trovi in difficoltà, deve essere in

Figura 1.2: Una sala controllo della rete elettrica.

grado di attivare autonomamente le protezioni, senza sapere cosa sta succedendo alla rete. Questa "ignoranza" è una possibile causa di guasti a catena; infatti, la cabina si occupa soltanto di proteggere se stessa e le utenze, ma non è in grado di trovare una soluzione "intelligente" al problema.

Un'altra limitazione che sta cominciando a presentarsi è l'impossibilità di interagire con gli impianti di generazione distribuita (DG). In questi ultimi 2-3 anni, si è visto un boom della cosiddetta microgenerazione; sono molti i cittadini che hanno deciso di dotarsi di impianti fotovoltaici o eolici di piccola taglia. La prospettiva che sembra attenderci nel futuro sarà quindi quella di una rete con molti punti attivi in grado di produrre piccole quantità energetiche. Tale aspetto mette seriamente in discussione l'attuale organizzazione della rete; si passerebbe infatti da una struttura gerarchica con flusso energetico unidirezionale ad una rete dove le direzioni delle correnti saranno molto più complicate delle attuali. Al giorno d'oggi, il sistema continua a funzionare perché l'energia fornita da questi impianti è irrisoria rispetto a quella prodotta dalle centrali, ma, quando le quantità immesse in rete dalla generazione diffusa cominceranno a diventare consistenti, ci sarà la necessità di convogliare l'energia fornita dalle rinnovabili secondo degli schemi precisi, in modo da ottimizzarne e massimizzarne l'utilizzo. Continuando ad utilizzare la struttura gerarchica a cui siamo abituati, l'operazione è molto ardua; il vasto numero e la diversità degli impianti, sommati alla variabilità dell'energia prodotta, rende necessario dotare la rete di un sistema di controllo più autonomo e decentrato.

L'ultima problematica dovuta alla limitata comunicazione tra i vari dispositivi riguarda il monitoraggio delle linee di distribuzione. Per capire l'arretratezza della analisi dei guasti sulle linee è interessante vedere come vengono tipicamente rilevati i guasti. Le modalità sono due; se c'è un guasto che lascia senza corrente un utenza sarà l'interessato ad avvertire del problema; nel caso in cui il guasto non sia così grave da compromettere il funzionamento della linea, l'unica speranza è che sia

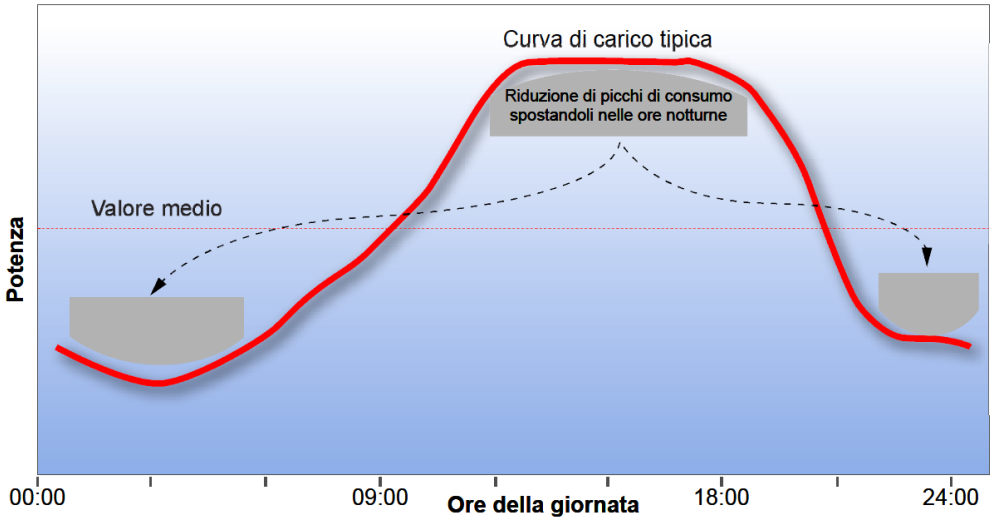


Figura 1.3: Profilo di carico giornaliero tipico per i consumi di elettricità [16].

notato dalle persone adibite all'ispezione delle linee. In Italia l'ispezione della rete elettrica AT e MT viene effettuata visivamente con l'ausilio di un elicottero e una telecamera dotata di teleobiettivo; il limite più stringente di questo sistema è la lentezza. La disponibilità di un solo elicottero adibito a questo scopo fa sì che, per analizzare l'intero sistema di trasmissione italiana, siano necessari 2 anni e questo solo per la registrazione. Successivamente i dati vengono passati al centro di controllo che li analizza, analisi che procede alla velocità di 20Km al giorno. Ciò nonostante, questa metodologia di analisi è da ritenersi molto evoluta se si pensa che fino al 2001 l'ispezione a piedi era il metodo più diffuso nel nostro paese. [41]

1.1.3 Irregolarità della domanda durante le 24h

L'ultima parte di questa sezione tratta un argomento che non si può definire esattamente un problema delle reti in se; è un problema prettamente legato alle nostre abitudini. Come si vede in figura 1.3, l'andamento dei consumi è molto altalenante durante le ore del giorno; ci sono dei picchi, ed è proprio su questi valori massimi che vengono dimensionate le centrali. I gestori dell'energia, basandosi sulle statistiche dei periodi precedenti, devono essere in grado di prevedere i picchi di richiesta e garantire una sufficiente offerta alle utenze; in caso contrario, alla presenza di un picco inaspettato può succedere che i parametri di rete (tensione e frequenza) vadano fuori limite a causa dell'eccessiva domanda, con conseguente apertura delle protezioni. Ci sono varie soluzioni per supplire a questi picchi di richiesta e una soluzione spesso adottata nelle regioni montuose, dove ci sono a disposizione bacini con centrali idroelettriche, consiste nel fare andare al massimo i generatori nei momenti di maggior richiesta (generalmente di giorno) e pompare l'acqua nel bacino (dal basso all'alto) durante la notte, per essere in grado di supplire alle esigenze del giorno seguente.

Un altro elemento molto importante da considerare sono le centrali nucleari che, all'opposto delle idroelettriche, sono estremamente statiche nella produzione,

generano l'energia per cui sono state progettate e le possibilità di regolazione sono minime. Chiaramente, il caso italiano è esente dal problema (opportunità) del nucleare, ma i nostri vicini d'oltralpe francesi hanno ben 59 reattori e di notte, nei momenti di abbondanza, sono ben contenti di fornirci un po' di energia. Per approfondire ulteriormente il problema, è interessante citare uno studio del 2007, riguardante un'analisi svolta negli Stati Uniti. La ricerca riporta che se si riuscisse a diminuire il picco del 5%, lasciando inalterati i consumi totali, si potrebbero eliminare 625 centrali e relative infrastrutture; inoltre, in termini economici, ci sarebbe un risparmio di 3 miliardi di dollari [17]. Si evince che il problema del picco, se affrontato in maniera adeguata, può significativamente ridurre l'inquinamento e consentire di eliminare diverse centrali. A rafforzare questa tesi viene in aiuto un altro studio, effettuato questa volta nel nostro continente. La sperimentazione riguarda le abitudini dei cittadini finlandesi, i quali, provvisti di uno speciale contatore in grado di visualizzare all'interno della casa i consumi in tempo reale, sono riusciti a diminuire i loro consumi di ben il 7%. La cosa più sorprendente degli ultimi dati è quanto la popolazione sia pronta e disponibile a cambiare i propri modelli di consumo se fornita di strumenti adeguati. Si vede dunque come il problema del picco giornaliero sia un elemento determinante per raggiungere gli obiettivi ecologici prefissati. Compito delle reti del futuro sarà dunque creare un infrastruttura che metta a disposizione i mezzi tecnologici di analisi e controllo dei consumi, tali da consentire ai cittadini e alle altre utenze di scegliere meglio quando consumare.

1.2 Le reti del futuro

Come detto nell'introduzione, le attuali reti elettriche sono state costruite intorno al '40, negli anni della grande elettrificazione. In quegli anni furono posate la maggior parte delle linee elettriche che vediamo ogni giorno; erano anni di grande sviluppo sia in Italia che negli altri paesi, la popolazione era molto fiduciosa nel progresso e le grandi opere come questa erano viste con orgoglio. Il contrario di quanto accade oggi, dove la costruzione di nuove infrastrutture viene spesso additata come qualcosa di pericoloso, da qui, la valutazione negativa di linee elettriche tralicci e quant'altro. Si tratta del *Not In My Back Yard*, un fenomeno esploso da qualche anno che interessa tutti i paesi cosiddetti avanzati, limitando la possibilità di innovazione nel campo delle infrastrutture.

Nota la situazione delle attuali reti, appena presentata, e, avendo brevemente illustrato le motivazioni, legate all'opinione popolare, che limitano la possibilità di nuove costruzioni, si può procedere ad analizzare come saranno strutturate le nuove reti. Sostanzialmente si tratterà di trovare un modo poco invasivo per rinnovare le infrastrutture esistenti aggiungendo ad esse un adeguato apparato di comunicazione.

1.2.1 Modello delle nuove reti

La figura 1.4 riporta lo schema di una probabile organizzazione delle future reti elettriche; sono riportati i vari soggetti che concorrono nel nuovo modello e i tipi di

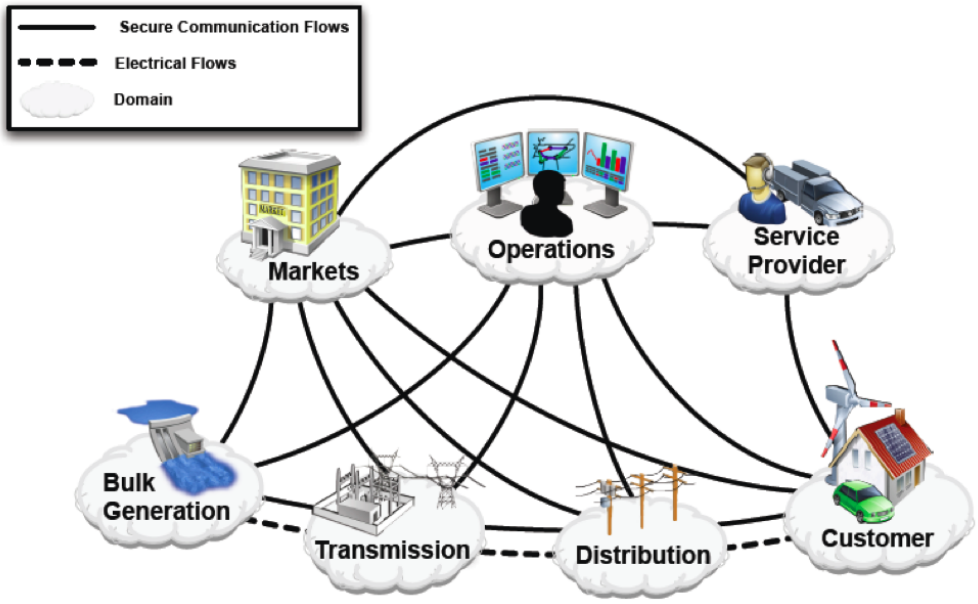


Figura 1.4: Soggetti e domini di competenza delle Smart Grid [42].

collegamento tra di essi. [2] La prima cosa che si nota sono i due diversi tipi di collegamento, elettrici e di comunicazione. Mentre i primi sono già fisicamente presenti, i secondi non sono ancora disponibili e la loro implementazione verrà trattata nella sezione 2.2. Nel frattempo, si procederà mediante un esame astratto, tralasciando le modalità di interazione, e concentrandosi sulle potenzialità del nuovo sistema. Vediamo ora brevemente cosa rappresentano i 7 domini presenti nell'immagine 1.4:

Markets (Mercato, Borsa)(figura 1.5a): gestisce e coordina i partecipanti al mercato energetico. Fornisce gli strumenti di gestione del mercato. Interfaccia gli altri domini e si occupa di assicurare la coordinazione e la competitività del mercato. Esercita inoltre il compito di distribuire le informazioni sulle operazioni tra i vari fornitori, per esempio un veicolo PHEV collegato sull'impianto X le cui spese devono essere addebitate in bolletta ad Y.

Operations (Operazioni)(figura 1.5b): rappresenta la "centrale operativa", chi gestisce i movimenti dell'elettricità tra gli altri domini, si occupa di controllare consumi, manutenzione, guasti, sicurezza, gestione dei picchi di richiesta ecc. . Per adempiere a questi compiti è collegato in maniera bidirezionale alla rete di comunicazione, così da potere interagire con sottostazioni, utenze e qualsiasi altro dispositivo necessario per ottemperare ai compiti sopraelencati.

Service provider (Fornitore)(figura 1.5c): è l'azienda che si interpone tra utente finale e gli enti necessari per la fornitura energetica. Consente all'utenza di interagire con gli altri soggetti e di accedere ai servizi di monitoraggio dei consumi nonché di AD. Risulta inoltre essere la figura di riferimento per il consumatore finale in caso di guasti e prima installazione.

[2] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [42, vedi appendice] e [49]

Bulk generation (grossista dell'energia)(figura 1.5d): chi si occupa di generare l'elettricità in grande quantità, tramite fonti rinnovabili e non. In alcuni casi può effettuare anche lo stoccaggio dell'energia per la fornitura nei momenti di maggior bisogno.

Trasmission (reti AT e MT)(figura 1.5e): rappresenta la rete elettrica di trasmissione sulle lunghe distanze, il cui scopo è portare l'energia dalle grandi centrali alla distribuzione. In alcuni casi possono essere collegati impianti di produzione derivanti da fonti rinnovabili di grossa taglia (grossi impianti fotovoltaici di grosse aziende collegate alla MT).

Distribution (reti BT)(figura 1.5f): è la parte di rete elettrica a corto raggio che generalmente va da cabine MT a utilizzatori finali. Connette la maggior parte di fonti energetiche rinnovabili installate presso le abitazioni o le aziende.

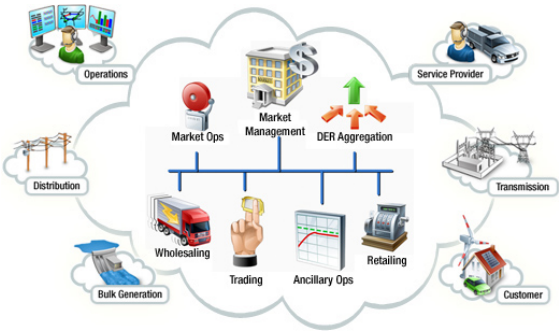
Customer (utente finale)(figura 1.5g): rappresenta il dominio dell'utente finale che sia abitazione o azienda. Il contatore, oltre a rappresentare il gateway attraverso il quale l'utenza comunica con gli altri enti, si occupa di raccogliere le richieste dei carichi interni e inviarle al soggetto di competenza.

Come si vede dalle immagini 1.5 e 1.4 la componente caratterizzante delle reti di nuova generazione è la fitta comunicazione tra i vari soggetti che dovrà essere in grado di soddisfare le esigenze necessarie per supplire ai problemi elencati nella sezione precedente e sostenere le innovazioni previste, che vedremo in dettaglio nella sezione seguente:

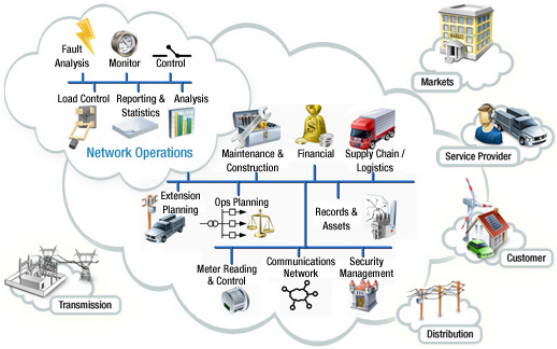
- DR, DP
- Supporto PHEV & PEV
- Supporto interattivo della generazione distribuita
- Monitoraggio real-time

1.2.2 AD, DR & DP

Il tre termini sono gli acronimi di Active Demand (AD), Demand Response (DR), Dynamic Pricing (DP), tecnologie diverse, ma con uno scopo comune, cambiare gli attuali modelli di consumo. Il fine di queste iniziative è quello di ridurre il classico picco di consumi giornaliero e tentare di livellare il più possibile l'assorbimento. Per riuscire in questo scopo, si punta ad una visione più intelligente e autonoma dei carichi, unita ad un prezzo variabile in tempo reale dell'energia. A grandi linee, si pensa di dotare le abitazioni di un dispositivo centrale con lo scopo di far interagire dispositivi interni (termostati, elettrodomestici ecc.) e rete esterna. L'oggetto in questione si può pensare come un particolare tipo di contatore che, note le richieste dell'abitazione e la situazione dei consumi nella rete esterna, sia in grado di trovare un punto d'incontro tra entrambe le esigenze. Con un'organizzazione di questo tipo, sarà possibile comandare i carichi in modo da:

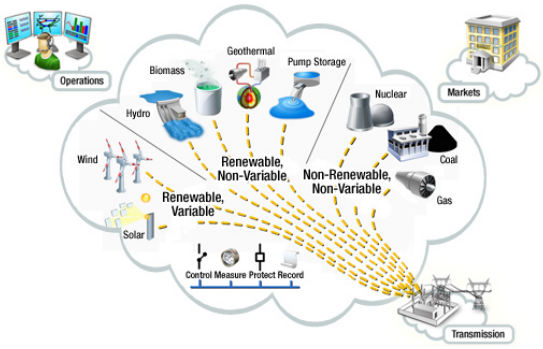


(a) Markets

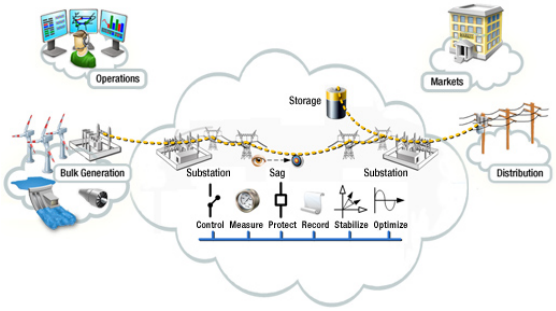


(b) Operations

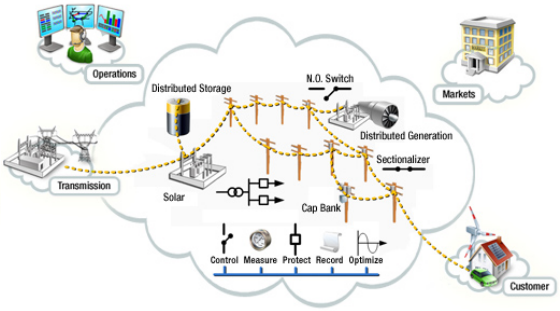
(c) Service provider



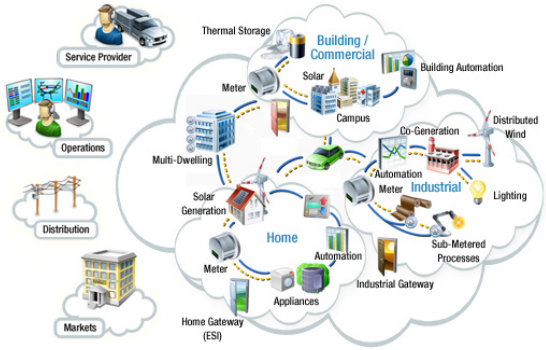
(d) Bulk generation



(e) Trasmission



(f) Distribution



(g) Customer

Figura 1.5: Rappresentazione dettagliata dei dominii

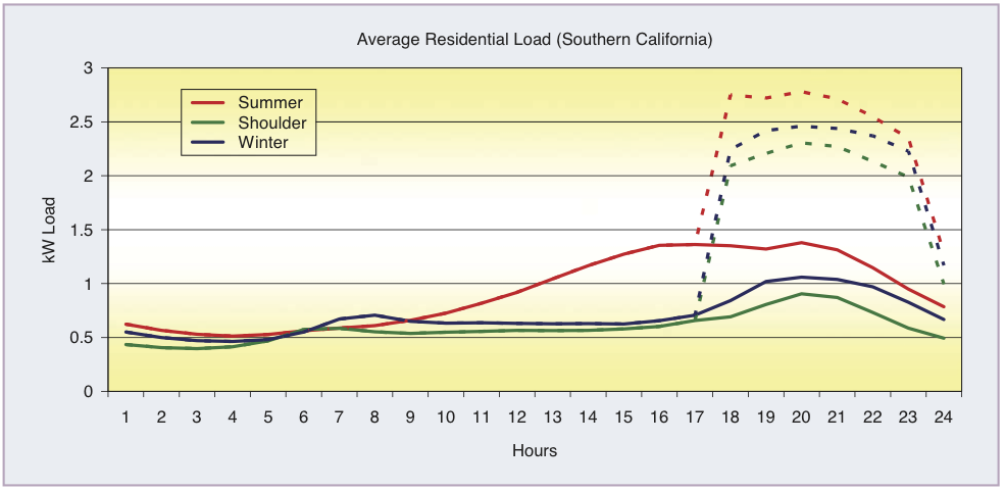


Figura 1.6: Profilo di carico giornaliero di un'abitazione con sovrapposto l'ipotetico carico derivante da veicoli elettrici [25].

Evitare sovraccarichi all'interno dell'utenza soprattutto a carico della rete, ma anche a livello di potenza contrattuale installata. Si può, ad esempio evitare l'accensione contemporanea di 2 motori. Nel caso delle abitazioni, è un caso tipico quello di due condizionatori, oppure lavatrice e lavastoviglie che funzionano contemporaneamente.

Evitare sovraccarichi sulla rete in caso di una situazione d'emergenza. Anziché aspettare l'intervento delle protezioni, la cabina di distribuzione in sovraccarico potrebbe comunicare alle proprie utenze di staccare i carichi non prioritari, in modo da evitare un blackout.

Risparmiare sul costo dell'energia questa è una prerogativa del DR ossia la variazione del prezzo dell'energia in tempo reale. Tutto ciò rappresenta un'ottima opportunità che consente all'utenza di risparmiare e ai fornitori di avere un consumo meno variabile durante le 24h.

1.2.3 Supporto PEV & PHEV

PEV & PHEV ossia Plug-in Electric and Hybrid Electric Vehicles, in italiano veicoli elettrici ibridi o puramente elettrici con la possibilità di caricarsi tramite connettore alla rete elettrica. Si pensa che nei prossimi anni, grazie ai loro vantaggi ambientali e ai progressi nelle tecnologie di stoccaggio dell'energia elettrica, questi tipi di veicoli avranno un'ampia diffusione. Tuttavia, l'introduzione a larga scala di tali mezzi di trasporto è uno degli aspetti più critici per le attuali reti elettriche e il motivo è ben rappresentato dalla figura 1.6, che rappresenta il consumo elettrico giornaliero di un'abitazione con sovrapposta l'aggiunta di consumi derivanti dai veicoli Plug-in.

L'immagine mostra come, durante le ore in cui si caricano i veicoli, il consumo medio dell'utenza è più che raddoppiato, questo prendendo come presupposto di poter lasciare l'auto in carica tutta la notte. Se invece ci fosse la necessità di tempi di carica più ridotti, meno di 3-4 ore, sarebbe necessario dotare l'utenza di potenze

contrattuali molto più alte dei tipici 3.5 kWh attuali, soluzione che comporterebbe picchi di assorbimento di oltre 6kW per abitazione [25]. Un'aumento di consumi di queste proporzioni sarebbe veramente troppo per le reti elettriche odierne, che già attualmente lavorano spesso in condizioni limite. La situazione che si prospetta non è quindi del tutto rosea; è vero che l' introduzione di veicoli elettrici e in grado di ridurre l'immissione nell'atmosfera dei gas serra, ma bisogna tenere presente che tale introduzione richiede la presenza di una rete elettrica adeguata.

Con l'avvento delle Smart Grid, si punta a risolvere questo tipo di problema come nel caso della sezione precedente usando l' "intelligenza" e la flessibilità nella gestione dei carichi, che se sfruttata con furbizia, può costituire addirittura un'opportunità. Secondo vari studi, sarebbe infatti possibile utilizzare gli accumulatori delle auto parcheggiate come un sistema di stoccaggio distribuito, da caricare nei momenti di minore domanda e scaricare nelle fasi di bisogno. Chiaramente, tutto il sistema deve essere automatizzato e gestito in modo da soddisfare sia le esigenze degli utenti che "prestano" le loro batterie, che la rete [25].

1.2.4 Supporto interattivo della DG

Abbiamo spiegato all'inizio del capitolo che l'attuale sistema elettrico si basa su una distribuzione dell'energia top-down; l'energia viaggia dalla centrale alle utenze a senso unico. Con la diffusione della DG avremo invece un decentramento della produzione elettrica.[3] Per sfruttare al meglio le possibilità offerte dalle rinnovabili, l'idea più diffusa è quella di concentrasi su un uso "interattivo" dell'energia rinnovabile, facendola dirigere dove ce n'è più bisogno in quel momento. Con un modello di questo tipo, la gestione dei flussi energetici si prospetta molto più complessa dell'attuale. Tuttavia, senza entrare nei dettagli, l'idea principale sarà quella di far percorrere meno strada possibile all'energia. Si punta sulla riduzione della distanza generatore-utilizzatore, in modo da minimizzare le perdite sui collegamenti. Soluzione che con un opportuna quantità di DG ha come effetto secondario quello di evitare la costruzione di nuove centrali e linee. La vicinanza produttore-consumatore farà si che l'energia venga spostata il meno possibile, con conseguente diminuzione dell'energia in transito sulle grosse linee MT/AT. L'idea del futuro è dunque quella di automatizzare la gestione del Power Flow Control in modo da rendere minimi i percorsi compiuti dall'energia sulle reti. L'implementazione di tale automatismo ha però 2 requisiti essenziali, di cui le attuali reti sono scarsamente dotate: infrastrutture di comunicazione e sensori in grado di fornire ai sistemi di controllo un adeguata mole di dati per rendere il sistema efficiente.

1.2.5 Monitoraggio Real-Time

L'avvento delle infrastrutture necessarie per soddisfare le esigenze di automazione della rete aprirà la strada a nuovi strumenti di misura e analisi. Il punto cruciale di questo cambiamento sarà l'ampia diffusione dei PMU che, sincronizzati tra di loro, consentiranno di ottenere informazioni in tempo reale sullo stato della

[3] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [32]

rete. I Phasor Measurement Unit (PMU), oltre all'ampiezza di tensione e corrente, sono in grado di misurare il loro sfasamento fornendo così informazioni anche sulla "qualità" dell'energia. Di per sé, il loro utilizzo non costituisce niente di nuovo; sono usati da molti anni. La novità sta nella loro dislocazione su tutta la rete e nella loro sincronizzazione tramite GPS. Grazie alla precisione temporale fornita dal GPS, è quindi possibile ottenere una correlazione causa effetto degli eventi registrati andando così a creare una sistema di monitoraggio su larga scala di nuova generazione. Sistemi di questo tipo sono detti Geographic Information System (GIS) e l'applicazione in ambito elettrico costituirà un innovazione importante per le Smart Grid, in quanto offrirà la possibilità di fornire informazioni in tempo reale sulla salute della rete. Sarà così possibile capire dove sono collocati geograficamente i punti critici e cercare una soluzione ad eventuali problemi.

Capitolo 2

Prospettive per l'implementazione e sistemi esistenti

In questo capitolo andremo a vedere come il panorama mondiale si sta mettendo in azione per l'implementazione dei servizi presentati nel capitolo 1. Essendo le Smart Grid un elemento recente, la situazione normativa e di standardizzazione è ancora in via di definizione. Quindi verranno descritti principalmente i progetti più importanti o più influenti per il nostro paese. Proprio per questo motivo, nella seguente sezione analizzeremo un progetto della comunità europea destinato a definire le modalità di gestione dell'AD.

2.1 L'approccio di ADDRESS

ADDRESS è un progetto cofinanziato dalla Comunità Europea nell'ambito del Settimo Programma Quadro (FP7) il cui obiettivo principale è elaborare un quadro tecnico e commerciale per lo sviluppo dell'AD. L'attività di ADDRESS, coordinata da ENEL Distribuzione SpA, è partita nel 2004 e ha in programma di produrre 8 Work Package (WP), documenti tecnici, con lo scopo di analizzare e trovare una soluzione ai problemi legati allo sviluppo della nuova infrastruttura dedicata all'AD. Il WP1 si occupa di definire l'architettura tecnica e commerciale di ADDRESS e sviluppare un'idea astratta (indipendente dall'infrastruttura di comunicazione) dei metodi di interazione tra utente finale e fornitore. Il WP2, la cui pubblicazione dovrebbe avvenire tra febbraio e giugno 2011, si dovrebbe invece concentrare sull'infrastruttura di metering e la gestione dei carichi.

2.1.1 L'architettura di ADDRESS

La figura 2.1 riporta l'architettura di ADDRESS con i rispettivi soggetti. Come si vede, ci sono alcune differenze, ma l'organizzazione è simile a quella riportata nel capitolo 1. Ciononostante, vale la pena introdurre brevemente il ruolo degli elementi di nostro interesse, ma prima di fare questo è fondamentale definire tre termini:

- Il **prodotto AD**; è ciò che l'aggregator vende ai fornitori di servizio, i quali a loro volta lo usano per creare i servizi offerti. Si tratta di potenza che un

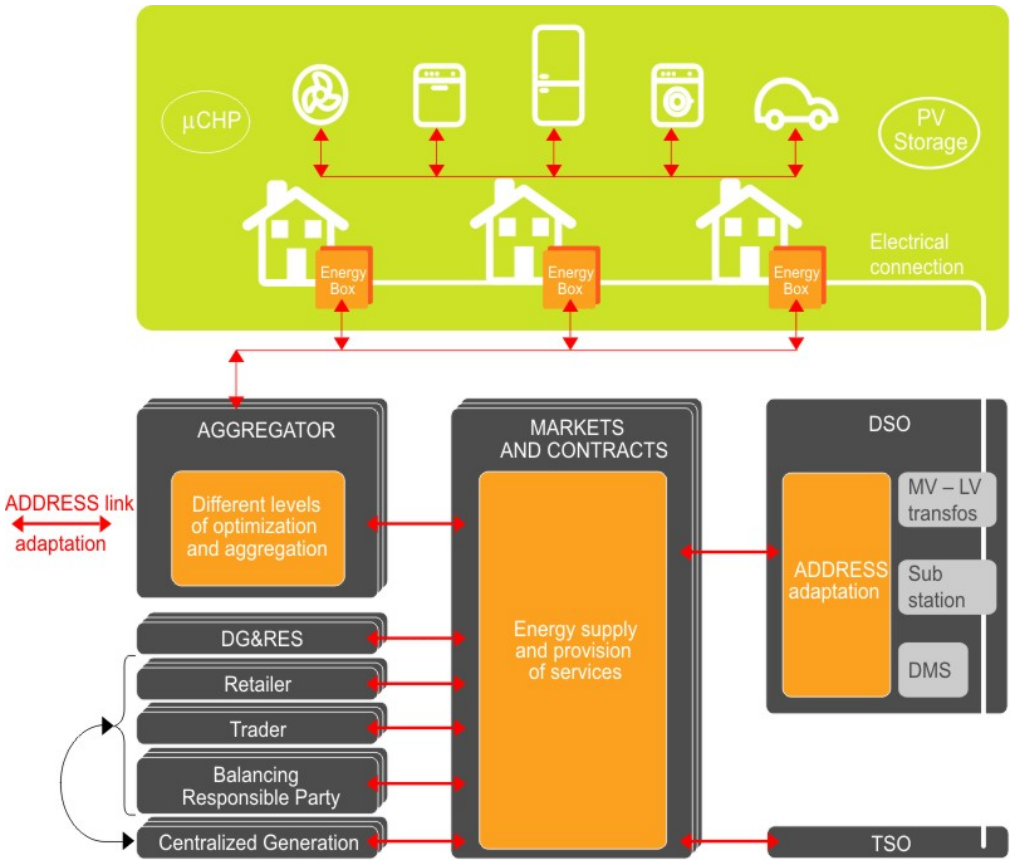


Figura 2.1: Architettura di ADDRESS

certo aggregator assorbe in un determinato momento. In termini più semplici è quanto l'aggregator riesce a cambiare i consumi di un gruppo di utenze e, dal lato delle utenze, lo si può vedere come una riduzione dei consumi, "quanto riesco a non consumare in un certo istante". [12, p. 25]

- Il prodotto AD diventa **servizio AD** quando è acquistato dai fornitori di servizi e rivenduto agli utenti finali. [12, p. 25]

A prima vista, le ultime due definizioni possono sembrare strane perché siamo abituati a pensare ad un mercato dove all'aumentare dei consumi aumenta la spesa. Con l'AD il risparmio non è più solo una riduzione della spesa, ma diventa un vero e proprio prodotto con un suo valore.

Fatta questa premessa possiamo procedere esaminando i due elementi di nostro interesse:

Aggregator: Il ruolo dell'aggregator è quello di mediatore tra gli utenti finali che forniscono prodotti AD e il mercato formato dai vari enti del sistema energetico, dove l'aggregator vende i prodotti AD creati dell'utente finale. Per svolgere la sua attività l'aggregator[12, p. 60]:

- Deve essere il soggetto che mette in contatto il consumer con gli altri soggetti del mercato

- Necessita di una conoscenza approfondita dell'utente a tutti i livelli
- Deve gestire i rischi e le problematica associate all' AD e più precisamente i rischi legati alla qualità e al prezzo
- Ha bisogno di raccogliere un'offerta di consumatori. Tale attività si traduce in:
  - Trovare dei clienti interessati a vendere la propria flessibilità.
  - Identificare e selezionare l'area geografica dei propri clienti.
  - Costruire un offerta commerciale valida
- Studiando i consumi delle utenze, con l'ausilio dei dati forniti dalle energy box, sarà possibile raccogliere informazioni sullo stile di consumo dell'utenza. Così facendo, verrà effettuata una classificazione dei diversi tipi di utenza in base al proprio profilo di carico e sarà possibile definire il ruolo delle varie utenze durante le varie ore della giornata.
- Gestire la comunicazione necessaria all'AD, ossia misurare i consumi o l'energia immessa in rete e tenere aggiornato il prezzo dell'energia elettrica secondo le modalità che verranno concordate.

Energy box: É il gateway della casa, si occupa di mettere in comunicazione tutti i dispositivi (contatore, carichi, impianto DG) della casa con l'aggregator e fa da portavoce delle esigenze interne. In base alla disponibilità elettrica della rete, al tipo di contratto sottoscritto e alle preferenze impostate, deciderà come e quando adempiere alle richieste pervenute dai carichi in base a quanto suggerito dall'aggregator. Per le utenze dotate di microgenerazione, come con i carichi passivi, l'energy box si occuperà di accordarsi con l'aggregator sulla quantità di energia da produrre.

2.1.2 Timeframe

Un ulteriore elemento per gestire meglio le future Smart Grid e l'AD sono i timeframe.[1] Non si tratta di un qualcosa di fisico, ma dell'insieme di intervalli temporali di monitoraggio che sono stati definiti per gestire al meglio la DR. Vediamoli più in dettaglio:

Demand response - ore. Si tratta dell'intervallo più lungo, operando sulla scala delle ore non necessita di comunicazioni ad alta velocità. La sua funzione è quella che abbiamo visto fino ora, ossia comandare i dispositivi delle utenze secondo le indicazioni dell'energy box. Una versione più evoluta del controllo potrebbe anche offrire la possibilità di regolare dinamicamente i termostati o altri dispositivi che possono funzionare a vari livelli di potenza.

Protezione automatica dai sovraccarichi - secondi. Questo secondo timeframe non viene molto tenuto in considerazione nonostante la sua importanza sia maggiore del precedente per quanto riguarda la stabilità delle reti. Ogni

[1] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [39]

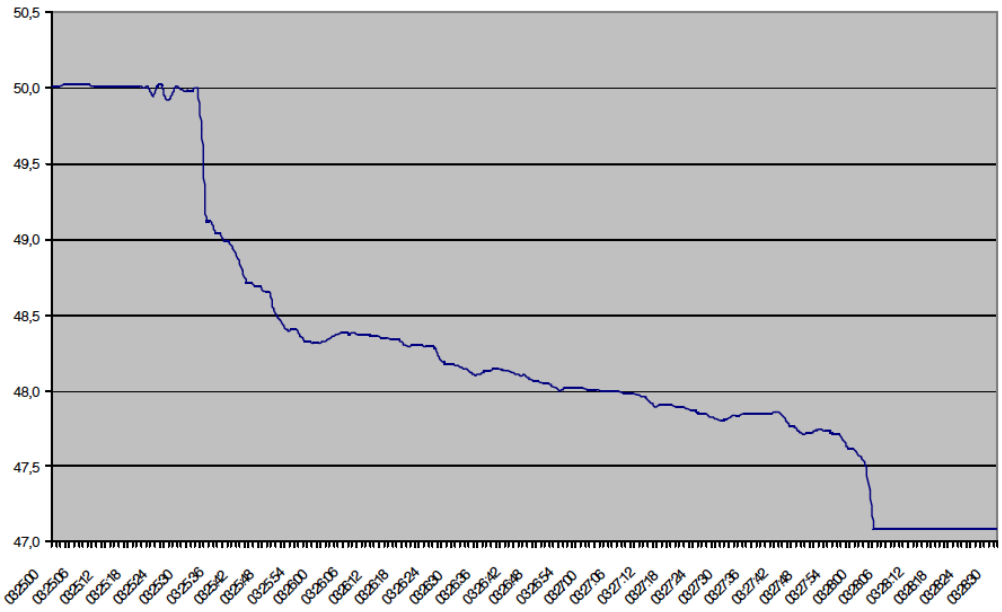


Figura 2.2: Andamento della frequenza sulla rete durante il blackout del 2003 [5].

rete ha una capacità di carico massima; se questa viene superata tensione e frequenza crollano. Quando succede, come conseguenza i motori elettrici (non controllati) assorbono più corrente. Data la loro consistente presenza sulla rete (circa 40% del carico) questo provoca una reazione a catena che abbassa ancora di più tensione e frequenza. Effetti di questo tipo sono in genere la causa della maggior parte dei black-out, come quelli riportati nella sezione 1.1.1. In figura 2.2 vediamo cosa successe alla frequenza di rete in quell'episodio.

L'idea per superare questo problema è quella di sfruttare l'energia accumulata in degli UPS o, più semplicemente, usando le batterie dei veicoli PHEV. Il processo di sovraccarico in genere è abbastanza lento, può durare da diversi secondi al minuto prima di causare il crollo della rete, quindi gli accumulatori sopracitati non avrebbero problemi ad intervenire. Allo stesso tempo, data la breve durata della fornitura rispetto alla capacità di accumulo, l'effetto di scarica è irrilevante e senza effetti negativi per la salute della batteria. Un altro punto a favore di questa tecnica è rappresentato dalla località di azione, presumendo che ogni utenza abbia almeno un veicolo PHEV collegato, le informazioni necessarie per tenere in piedi il sistema resteranno in ambito LAN senza necessità di comunicazioni ad alta velocità con l'esterno.

Un sistema di questo tipo sarebbe molto utile per la stabilità della rete, i sovraccarichi causati da fenomeni di questo tipo sono molto critici per i fornitori. L'unica soluzione è quella di trovare delle forniture extra o aumentare il regime delle centrali in funzione, tuttavia l'inerzia dei grossi alternatori e la velocità con cui avvengono questi fenomeni rende molto difficile trovare una soluzione. L'unica possibilità per i fornitori è quella di fare un attenta analisi dei consumi in modo da tenersi lontani da fenomeni di questo tipo.

Compensazione automatica del $cos\phi$ - millisecondi. É l'intervallo più cor-

to. Scopo di questo timeframe è migliorare la qualità dell'energia. Come sappiamo, i carichi moderni hanno dei fattori di potenza molto bassi:

- Lampade CFL - 0.5
- LED - 0.5
- Personal Computer - 0.7 - 0.8

Vista la quantità sempre maggior di questo tipo di dispositivi la loro influenza sulla rete è piuttosto consistente e quindi con un Power Factor (PF) basso ci si trova con molta corrente reattiva che carica le linee senza motivo. Quello che si pensa di fare è aumentare il fattore di potenza con l'ausilio di dispositivi di microgenerazione e UPS distribuiti localmente su tutta la rete. Attualmente la compensazione del PF avviene solo a livello delle centrali o delle sottostazioni di grosse dimensioni. Ciò a cui si punta con la correzione automatica del $cos\phi$ è una compensazione distribuita e gestita localmente in modo che quanto esce dalle utenze sia perfettamente compensato, diminuendo l'inutile corrente reattiva presente in rete. Un approccio di questo tipo, oltre a tradursi in una riduzione dei costi di infrastrutture per i fornitori, porterebbe ad un miglioramento della qualità dell'energia disponibile sulla rete.

2.1.3 I carichi

L'irregolarità del carico durante le 24 ore fa dell'analisi dei carichi l'elemento più importante tra quelli elencati.[2] Come detto nel capitolo 1 l'idea alla base dell'AD è quella di spostare l'avvio dei carichi nei momenti più favorevoli per la rete elettrica. La prima classificazione che si può fare è la seguente:

Dispositivi con capacità di stoccaggio elettrica o termica possono consumare energia in qualsiasi momento e utilizzarla nei momenti di bisogno. Degli esempi di questi dispositivi sono gli scaldabagno elettrici, frigoriferi, ventilconvettori elettrici e notebook. Con questi dispositivi l'energia può essere acquistata in anticipo, nei momenti in cui costa meno, oppure la loro accensione può essere posticipata. La flessibilità di questi carichi fa sì che la spese da loro prodotta possa essere minimizzata se sono gestiti in modo intelligente. Ai fini di monitoraggio e controllo di questi dispositivi possono essere utili i seguenti parametri:

Capacità totale (kWh): indica la quantità di energia accumulabile

Stato di carica: indica la percentuale di accumulo presente nel dispositivo

Potenza nominale assorbita (kW): energia assorbita dalla rete

Potenza nominale scambiata (kW): è l'energia effettivamente fornita all'utente. Questo indice è fondamentale per capire qual'è l'effettivo consumo dell'utente.

[2] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [11]

Il controllo che si utilizza con questi carichi è una funzione che dipende dallo stato di carica e dal costo dell'energia. In condizioni normali, il carico assorbe energia quando costa poco e, nel caso in cui lo stato di carica sia molto basso, a qualsiasi prezzo.

Carichi shiftabili: possono spostare il loro avvio in qualsiasi momento. Esempi tipici sono lavastoviglie, lavatrice e asciugatrice. Attualmente, l'avvio di questi carichi avviene alla pressione del pulsante; l'idea del futuro è quella di dare un orario entro il quale il processo deve essere terminato. La pressione del bottone si tradurrà in "la lavastoviglie deve aver finito il lavaggio entro le 7" al posto di "avvia il lavaggio adesso". Gli indici utili ai fini del controllo di questi dispositivi sono:

- durata del processo
- potenza usata durante il processo (assumendola costante)
- orario in cui deve essere concluso il processo

L'algoritmo di controllo di questi tipi di carichi è basato sul prezzo istantaneo dell'energia e l'ora per cui deve essere finito il processo: inizialmente, il processo parte solo se il prezzo dell'energia è molto basso, se questo non avviene, col passare del tempo la soglia di prezzo necessaria per l'avviamento si alza linearmente finchè raggiunge il punto massimo, quando non è più possibile ritardare l'avvio del processo. Questo sistema da la possibilità di risparmiare, ma allo stesso tempo rispetta le richieste dell'utente.

Carichi non controllabili: è l'insieme di quei dispositivi sui quali non è possibile effettuare un controllo senza causare grossi svantaggi per il cliente. Fanno parte di questi carichi tutti i dispositivi di illuminazione, PC desktop, televisori, piani cottura elettrici, ecc.. Di conseguenza i sopracitati carichi non subiscono alcun tipo di controllo e la loro attivazione è a discrezione dell'utilizzatore.

2.1.4 Un esempio di comunicazione tra i vari soggetti

Il progetto ADDRESS divide e cataloga prodotti e servizi AD sulla base di diversi parametri, tra i quali la priorità e la destinazione (scopo del pacchetto).[3] Tra tutti quelli elencati nel documento [12] vale la pena analizzarne uno per capire a grandi linee quali siano le contrattazioni che si vanno ad instaurare durante il funzionamento della rete. Come esempio in figura 2.3 viene riportato il caso di un pacchetto CRP-VRPF-FT (Conditional Re-Profiling for Voltage Regulation and Power Flow control (fast)).

Un pacchetto CRP-VRPF-FT è un richiesta lanciata da DSO (gestore della distribuzione) o TSO (gestore della trasmissione) a causa di una situazione di imminente criticità nella rete, può trattarsi di sovraccarico di una linea o abbassamento della tensione. L'invio della richiesta al mercato e quindi agli aggregator

[3] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [12]

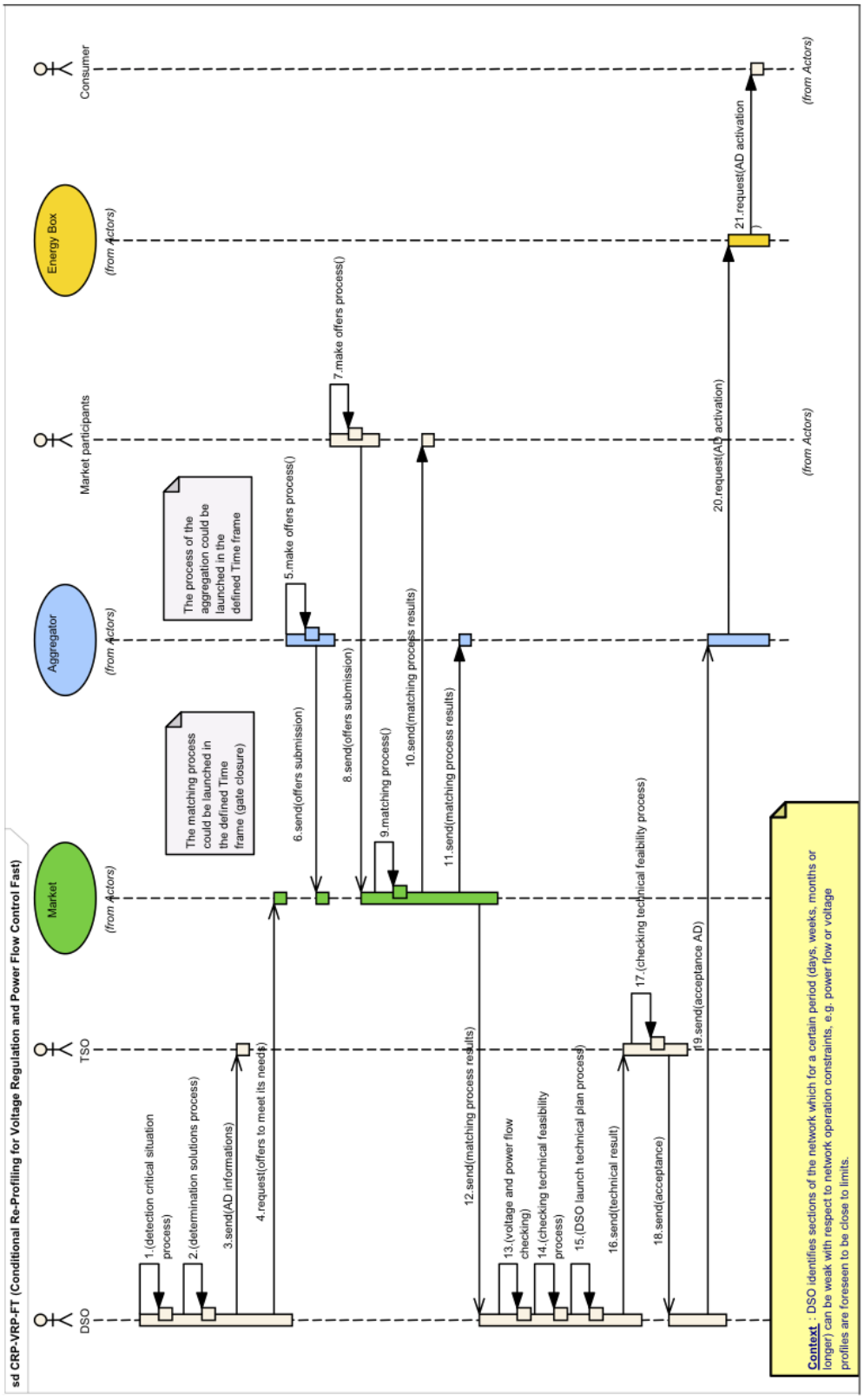


Figura 2.3: Richiesta di un CRP-VRPF-FT da parte di un DSO o TSO [12, p. 57]

ha lo scopo di cercare una possibile soluzione al problema riducendo i consumi dei clienti, in modo da evitare la richiesta di un surplus di energia ai grossi produttori energetici.

Vediamo le fasi di questo processo:

1. DSO o TSO identificano una potenziale criticità in qualche punto della rete (sovraccarico linea o limite di tensione)
2. le possibili soluzioni sono:
   - modificazione della topologia della rete
   - ricorrere al mercato dell'AD
   - altre soluzioni fornite dal mercato elettrico
3. se c'è una soluzione AD accettabile (requisiti di costo e gestione della rete) il DSO e TSO si accordano su chi si deve occupare del problema in modo da evitare doppie richieste agli aggregators.
4. Il DSO lancia sul mercato la richiesta di un prodotto CRP (prezzo e quantità di energia)
5. gli aggregators preparano la loro offerta e la lanciano sul mercato
6. gli altri soggetti del mercato preparano la loro offerta e la lanciano sul mercato
7. Al termine delle offerte il DSO riceve le proposte disponibili sul mercato e in base alle condizioni e alle posizione geografica, decide da chi acquistare il CRP-VRPF-FT.
8. DSO e TSO si consultano per verificare la fattibilità della soluzione
9. se la verifica è positiva il DSO da conferma all'aggregator offerente
10. l'aggregator ha ora il compito di adempiere all'offerta presentata secondo i tempi e le modalità previste
11. l'aggregator lancia le richieste alle energy box ad esso collegate
12. le energy box delle utenze controllano i dispositivi dell'utenza secondo le richieste dell'aggregator

2.2 Reti di comunicazione

Fino ad ora, in tutto il documento, abbiamo trascurato la parte dell'infrastruttura di comunicazione, dando per scontato che i vari dispositivi della rete comunicassero tra di loro senza problemi. La situazione che si trova nel panorama mondiale è invece diametralmente opposta. Diverse enti nazionali e internazionali stanno provvedendo alla creazione di standard o linee guida per i dispositivi e le comunicazioni delle Smart Grid. Al tempo stesso, le grandi industrie già attive nei campi

di telecontrollo, comunicazioni e sistemi elettronici di misura, stanno mettendo sul mercato i loro prodotti, con scelte tecnologiche piuttosto eterogenee. Ci troviamo dunque in una fase in cui il mercato offre già diversi dispositivi all'avanguardia, tuttavia l'interoperabilità non è garantita, a causa della mancanza di uno standard. Situazioni di questo tipo non sono certo nuove al mondo dell'elettronica, basta pensare alla guerra delle correnti della fine '800, ciò nonostante anche lo sviluppo delle Smart Grid è affetto da queste problematiche. Diversi enti nazionali e sovranazionali sono al lavoro per definire standard e linee guida per le comunicazioni e i dispositivi necessari a collegare i soggetti delle reti intelligenti, tuttavia la situazione non è ancora molto ben definita. Dato lo scenario, ciò che possiamo fare in questa sezione è dare una visione d'insieme delle tecnologie di più probabile utilizzo per l'infrastruttura di rete.

2.2.1 Requisiti delle reti di comunicazione

L'infrastruttura di comunicazione è sicuramente l'elemento più importante per lo sviluppo delle Smart Grid; senza di essa non può avere inizio lo sviluppo di cui c'è bisogno dato che costituisce la base per dar modo ai vari soggetti di scambiarsi informazioni. Fino ad oggi, i canali di comunicazione usati per il controllo remoto di sottostazioni e cabine sono stati basati su infrastrutture private, di proprietà delle rispettive utilities. Tali canali, costituiti da un mix di tecnologie (fibre ottiche, Power line communication (PLC), cavi di rame e comunicazioni wireless di vario genere) avevano ed hanno un costo elevato per i loro proprietari, ma la necessità di affidabilità ed efficienza era tale da giustificare la spesa. Con l'arrivo delle Smart Grid, il tipo di infrastruttura richiesta è piuttosto diversa, si passa dalla necessità di avere poche linee a lunga distanza ad aver bisogno di una diffusione capillare dei punti con cui comunicare. Chiaramente, la spesa per implementare tale infrastruttura è troppo alta anche per le utilities e qui entra in campo la possibilità di usare un infrastruttura di comunicazione condivisa.[3, 26]

Lo sviluppo delle reti di comunicazione dell'ultimo decennio ha visto il protocollo IP diffondersi a macchia d'olio in diversi settori (voIP,Internet Protocol Television (IPTV)) e ci si aspetta che esso sia alla base anche della rete per l'energia. Il principale vantaggio fornito dal protocollo IP è la possibilità di effettuare i collegamenti con mezzi eterogenei (fibra ottica, ponti radio, Wireless Fidelity (WiFi), Worldwide Interoperability for Microwave Access (WiMAX),PLC, ecc.) con un unica tecnologia di rete in grado di supportare diversi tipi di applicazioni senza dover modificare i protocolli di comunicazione a basso livello. Un'ulteriore vantaggio del protocollo IP nell'uso di infrastrutture condivise deriva dall'ormai consolidata capacità di gestire con priorità diverse i flussi di dati in transito [3, p. 30]. Parallelamente allo sviluppo del protocollo IP c'è stata una diffusione esponenziale delle connessioni a banda larga in abitazioni e aziende che ha contribuito a creare l'infrastruttura che usiamo abitualmente per connetterci ad internet. Guardando al caso italiano, Telecom Italia, data la vasta infrastruttura fisica distribuita sul territorio nazionale (150000 armadi e migliaia di edifici adibiti a centrali), è un naturale candidato per la gestione dell'infrastruttura di comunicazione per le Smart Grid del futuro [16].

Il problema principale che deriva dall'uso di un infrastruttura di rete condivisa è legato all'efficienza e alla qualità del sevizio. Vediamo quali possono essere i requisiti da soddisfare per garantire il corretto funzionamento delle applicazioni per le Smart Grid [3]:

Banda: indica la quantità di dati che possono essere trasferiti nell'unità di tempo, è misurata in **bit/s**. Al contrario delle applicazioni multimediali o di scambio dati, nell'ambito di nostro interesse le moli di dati da trasferire sono modeste; ciononostante, è necessario che il fornitore garantisca una capacità di trasferimento minima anche in caso di traffico intenso. Particolarmente limitante è il dispositivo lungo il percorso con la banda minore che costituisce il cosiddetto collo di bottiglia.

Latenza: indica il tempo richiesto dai dati per andare dalla sorgente alla destinazione, l'unità di misura tipica è il millisecondo (**ms**). La latenza ha componenti fisse dovute al tempo dell'elaborazione dei nodi e alla propagazione del segnale; è inoltre presente una componente variabile dipendente dall'altro traffico che condivide i collegamenti e può congestionare la rete.

Affidabilità: indica in termini di tempo quanto una connessione è in grado di offrire il servizio richiesto. L'affidabilità della rete dipende direttamente dai dispositivi e i collegamenti utilizzati. Solitamente, si misura in percentuale il cui valore è dato dal rapporto del tempo di funzionamento sul tempo totale.

Un ulteriore divisione si può ricavare dai campi di utilizzo delle varie porzioni di rete. Abbiamo finora considerato l'esigenza di comunicazione come un elemento unico, con caratteristiche uguali. Tuttavia, lo scenario è piuttosto diversificato ed è possibile catalogare i vari tipi di sistemi con caratteristiche ed esigenze simili in 3 categorie [3]:

Monitoraggio: di questa categoria fanno parte i sistemi di raccolta dati provenienti da sensori di vario genere. Il traffico dati prodotto da questi sistemi è piuttosto considerevole, non tanto per la banda occupata da un singolo sensore, ma per la moltitudine di sensori distribuiti. La valutazione della banda necessaria per queste reti sarà caratterizzante per dimensionare la capacità di trasferimento dati complessiva. Per quanto riguarda la latenza sono invece i dispositivi con esigenze meno stringenti.

Controllo: fanno parte di questa categoria i sistemi di controllo delle cabine e della DG. Le necessità di questa categoria sono leggermente più stringenti a causa della bidirezionalità delle comunicazioni; tuttavia, le esigenze sono piuttosto blande. Il termine critico potrebbe essere la latenza che, comunque, richiede tempi dell'ordine dei secondi per la rete di distribuzione.

Protezione/Sicurezza: in questa categoria risiedono le comunicazioni che controllano i dispositivi (interruttori e sezionatori) di protezione in caso di emergenza. In queste connessioni è necesario un tempo di latenza breve per garantire che i "sistemi intelligenti" intervengano prima delle protezioni passive in

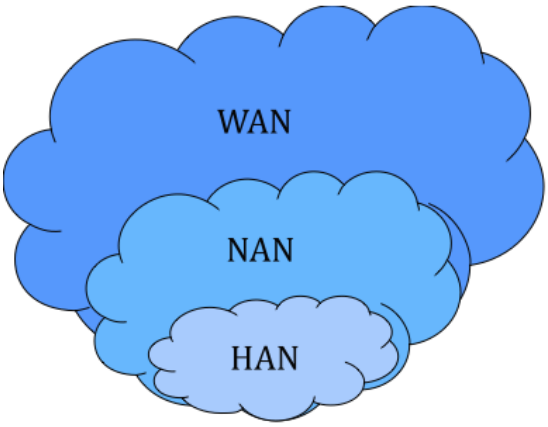


Figura 2.4: Suddivisione in aree della rete di comunicazione per Smart Grid

modo da evitare blackout a catena. Un esempio di questi sistemi è rappresentato dal controllo remoto dei dispositivi preposti a scollegare dalla rete la DG in caso di guasto. Tali interfacce richiedono tempi di intervento dell'ordine dei 100-200 ms.

2.2.2 Struttura della rete

Avvicinandosi sempre di più al processo di realizzazione fisica della rete ci si rende conto che gli scenari da affrontare sono molto diversi, in relazione alla collocazione geografica e alla disponibilità di infrastrutture preesistenti. É facile capire che la tipologia di rete usata per raccogliere i dati dei meter in una zona residenziale, con molte utenze ravvicinate e raggiunta da fibra ottica, è diversa da quella di una zona di campagna o montagna dove spesso regna il digital divide. Di conseguenza, la scelta di un'architettura gerarchica con tecnologie eterogenee è la migliore soluzione. Tale architettura, ispirata alla reti di computer, è un buono spunto per dividere le comunicazioni delle Smart Grid in base all'area di utilizzo. Per capire come è stata fatta la suddivisione in aree, analizziamo la figura 2.4 [3]:

Home Area Network (HAN): rappresenta la rete interna all'abitazione, o azienda, dell'utente adibita a collegare sensori, dispositivi di misura e controllo. Il punto di connessione tra HAN e il resto della rete è rappresentato dall' Home Gateway (HG).

Neighborhood Area Network (NAN): è il cosiddetto ultimo miglio, raggruppa i collegamenti tra più meter geograficamente vicini e l'accentratore. Per fare un paragone con la rete elettrica è quella parte di linee che va dalla cabina all'utilizzatore. Questa parte della rete è caratterizzata da una moltitudine di punti da connettere. Bisogna sottolineare che questa definizione di area non è recepita in modo coerente dai vari addetti ai lavori; c'è chi con NAN fa riferimento al solo raggruppamento dei dati dei contatori (zona con un raggio delle centinaia di metri) e chi la intende in termini più vasti, come una rete locale (zona con un raggio di qualche km). [3, 16]

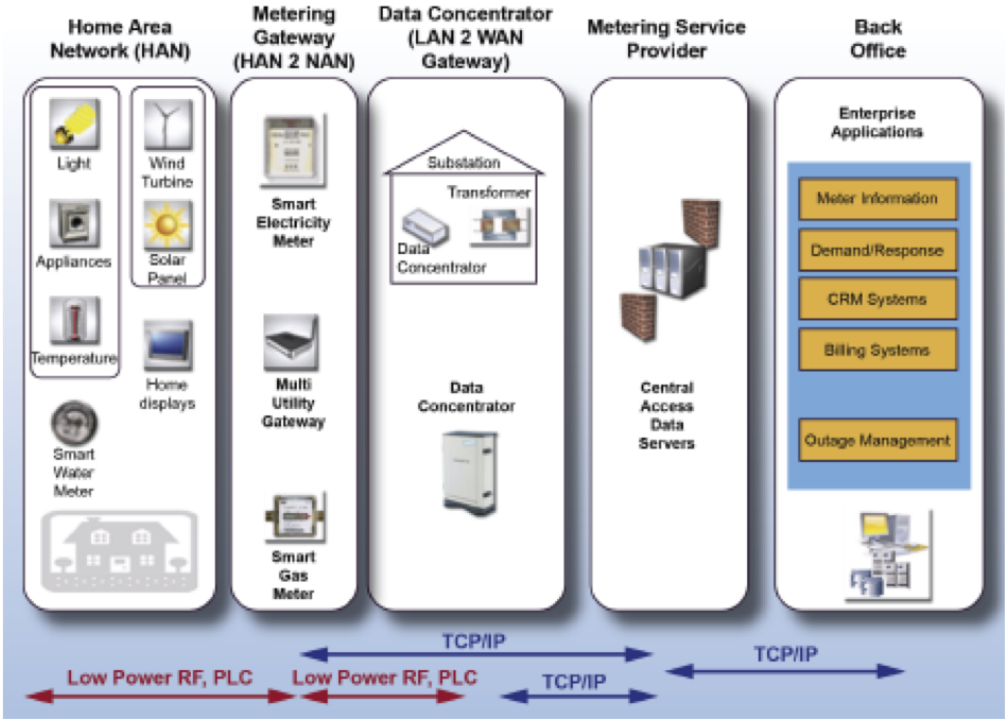


Figura 2.5: Schema di un ipotetica architettura di Smart Metering [16].

Wide Area Network (WAN): sono i collegamenti a lunga distanza, possono essere dei riammodernamenti di vecchie linee proprietarie delle utilities o linee condivise fornite da operatori di telefonia. Di quest'area fanno parte le connessioni atte a far comunicare i centri di controllo e gestione regionali o nazionali. I punti collegati da questa porzione di rete sono pochi rispetto alle aree NAN.

Con questa suddivisione abbiamo ora un'idea delle dimensioni e il numero di punti da connettere nelle varie aree, risulta quindi più chiaro analizzare quali tecnologie siano più adatte ad ogni area. Tuttavia, prima di passare all'analisi delle possibili implementazioni, vale la pena osservare la figura 2.5 per avere un'idea generale del funzionamento dei collegamenti nelle Smart Grid.

Partendo da sinistra, abbiamo l'HAN (primo rettangolo) con tutti i dispositivi tipici delle abitazioni (elettrodomestici, termostati, ecc.) e, naturalmente, le varie tecnologie di microgenerazione (eolico, solare, ecc.). Questi soggetti comunicano con l'HG (secondo rettangolo) che si occupa di gestire i rapporti tra esigenze dei dispositivi interni e della rete esterna. Procedendo con il percorso, i dati raggiungono il concentratore di zona (qui termina l'NAN) per poi passare nell'ambito WAN dove i dati vengono inviati alle utilities [16].

2.2.3 Tecnologie per le comunicazioni

In questa sezione analizzeremo quali soluzioni tecnologiche possono essere usate nelle varie aree viste nella sezione 2.2.2. Chiaramente, le soluzioni sono molte e sarebbe inutile elencare cosa offrono i vari produttori; faremo quindi una panora-

mica sulle tecnologie che hanno più probabilità di prendere piede nei prossimi anni. In particolare, ci concentreremo sulle aree NAN e HAN che, come abbiamo visto, sono la vera sfida per l'implementazione dell'infrastruttura di comunicazione per Smart Grid. Di conseguenza, le WAN saranno tralasciate in quanto la loro implementazione può essere molto simile a quella delle dorsali usate per l'infrastruttura di internet.

Ambito NAN

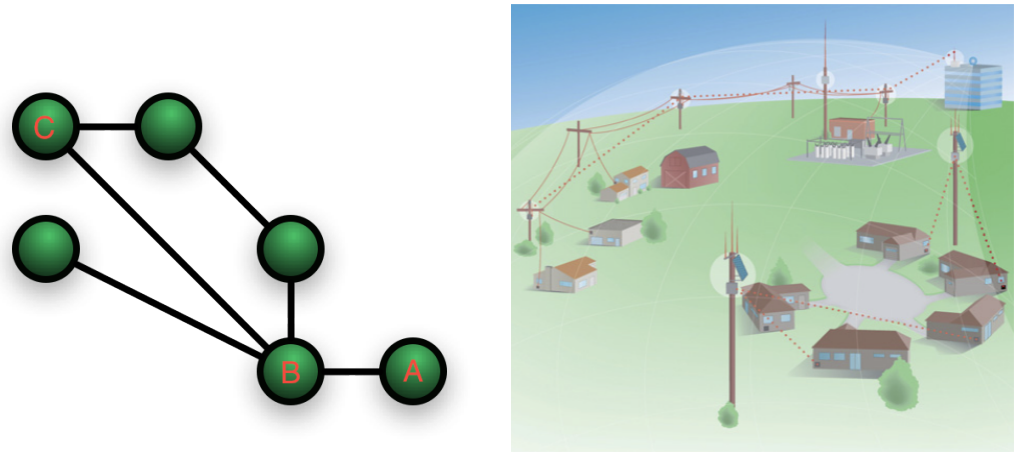
In sezione 2.2.2 abbiamo detto che l'ambito NAN è caratterizzato da un grosso numero di utenti in un raggio relativamente contenuto (al massimo qualche chilometro). Per implementare tale infrastruttura è dunque necessaria la presenza di una rete capillare e, per soddisfare tali esigenze, le soluzioni non invasive sono di due tipi:

PLC: è una tecnologia che usa come mezzo fisico la stessa rete elettrica e, modulando il segnale di informazione ad una frequenza più alta di quella di rete, è in grado di trametterе dati [53]. I vantaggi di questa tecnologia sono dati dalla semplicità di installazione, dato che non è necessario collocare nessun ulteriore conduttore nell'area di interesse. D'altro canto il punto debole è dato dalla limitata capacità di banda.

soluzioni wireless: le tecnologie wireless sono basate sulle comunicazioni via radio ed, in particolare, la maggior parte delle soluzione disponibili sono basate sullo standard 802.11 e lavorano ad un frequenza di 2.4 GHz. Tuttavia, di questa categoria fanno parte anche il WiMAX e le reti cellulari.[3, 36]

Le soluzioni WiFi sono molto interessanti sotto vari aspetti. Le reti WiFi sono versatili e scalabili, consentendo di connettere senza problemi 2, o migliaia di utenti. Questa prima caratteristica rende le reti WiFi adatte a diverse circostanze che possono presentarsi in ambito NAN. Il secondo punto a loro favore è dato dal supporto del protocollo TCP/IP (IPv4 e IPv6) e dalla banda che parte da 1Mbps con lo standard 802.11b e arriva ai 600Mbps del 802.11n. Un ulteriore elemento a loro favore è la sicurezza e l'interoperabilità con altri dispositivi. Queste ultime caratteristiche si devono al fatto che la realizzazione dello standard è iniziata nel 1999 e, ad oggi, la tecnologia si può ritenere sufficientemente matura. Come conseguenza, sono stati sviluppati sistemi di sicurezza efficienti e l'interoperabilità con altri dispositivi Radio Frequency (RF) in genere non presenta problemi. Altro elemento da considerare è il costo; il fatto che la banda utilizzata sia libera consente ai produttori di mantenere prezzi più bassi rispetto a WiMAX e reti cellulari, che lavorano su banda licenziata. Allontanandosi dalle caratteristiche tecnologiche e passando a quelle topologiche, il WiFi offre un ulteriore opportunità che lo rende perfetto per l'ambito NAN. L'utilizzo combinato di una topologia mesh (figura 2.6a) con ponti Hiperlan tra i vari Access Point (AP) (figura 2.6b) da la possibilità di creare delle reti di ampio raggio (figura 2.6b) in grado di raggiungere luoghi in digital divide. [20]

Come vediamo la topologia mesh è caratterizzata da una struttura decentralizzata dove ogni punto fa da ripetitore per il segnale, portandolo ai punti più



(a) (b)

Figura 2.6: Topologia di una rete mesh e Illustrazione di una possibile implementazione di una rete mesh in ambito NAN [52, 20].

lontani. Prendiamo per esempio la topologia in figura 2.6a e supponiamo che **A** voglia comunicare con **C** ma non lo possa fare a causa della distanza. Con l'ausilio del nodo intermedio **B**, che fa da ripetitore, **A** e **C** possono comunicare. A livello pratico in una NAN si può pensare ad una serie di AP che comunicano tra di loro con ponti Hiperlan; se a questi aggiungiamo un accentratore collegato alla WAN il sistema è completo.

Ambito HAN

Per quanto riguarda la comunicazione in area HAN esistono vari protocolli con una certa maturità e affidabilità.[4] In particolare, ZigBee si sta affermando come leader per la gestione dell'abitazione. Si tratta di una tecnologia radio in banda libera (Industrial, Scientific and Medical (ISM) a 2.4 GHz e 868 MHz) ma, al contrario del WiFi, viaggia a velocità basse (da 20 a 250 kb/s). Lo ZigBee è basato sullo standard 802.15.4 il quale ne definisce il livello fisico e Data Link, mentre la ZigBee Alliance specifica i livelli di rete e gli applicativi. Il maggior vantaggio del ZigBee è rappresentato dai consumi ridotti, associati ad un eccezionale range di trasmissione. Caratteristiche di questo tipo lo rendono un ottimo candidato per fornire connessione a dispositivi non collegati alla rete elettrica, dove è necessario fornire energia tramite batteria.

In ambito HAN come per il NAN come alternativa alle comunicazioni via radio, c'è la possibilità di usare la già citata tecnologia PLC e in particolare l'Home plug alliance tiene testa a ZigBee spingendo sull'uso di questa tecnologia.

Un ulteriore elemento da considerare in ambito HAN oltre all'infrastruttura di rete è il gateway. L'HG ha lo scopo di connettere tutte le utenze all'interno della HAN e consentire alle loro richieste di essere instradate verso l'esterno. Ci sono molte questioni da chiarire sull'HG; le opinioni e le soluzioni proposte sono molto

[4] I dati e le informazioni presenti in questa parte del documento derivano principalmente da [16, 3, 6]

varie. Questa varietà, oltre a una divergenza di opinioni, nasce anche dalle diversità storiche della gestione del metering nei vari paesi. Con questa affermazione si fa riferimento, in particolare, al luogo di installazione dei contatori. Volendo monitorare anche acqua e gas, non è detto che i requisiti di un HG italiano siano gli stessi di un HG che andrà installato nel nord europa o negli Stati Uniti. La principale divergenza di opinioni sull'HG riguarda la presenza di 2 possibili alternative per l'installazione del suddetto dispositivo. La prima prevede che HG e meter siano all'interno dello stesso dispositivo, l'altra li vede come 2 oggetti separati. Essendo il meter sempre connesso alla rete elettrica, l'idea di unificare HG e meter è piuttosto naturale; infatti, tale soluzione è già stata adottata da alcuni paesi, come ad esempio l'Olanda. Tuttavia, dato che, come già detto, l'HG si occuperà anche di fornire dati su acqua e gas, laddove le aziende di distribuzione di elettricità e gas non coincidono o ancora peggio, come succede in Italia, siano concorrenti. In questo caso, il distributore del gas si trova a dipendere da un dispositivo di proprietà del gestore elettrico. Per ovviare a questo inconveniente in alcuni paesi (ad esempio in Germania) si è pensato di lasciare divisi i 2 dispositivi e installare nelle case un HG che si occupi di gestire e coordinare tutti i dispositivi della casa (meters compresi) affiancato da un meter per l'elettricità in grado di fornire i dati necessari. Questa soluzione elimina il ruolo gerarchico del gestore elettrico, ma pone il problema organizzativo di definire a chi appartiene questo oggetto, chi ha il dovere di alimentarlo e come gestire i rapporti tra le utilities che devono sfruttarlo per la telelettura.

Su questo campo c'è dunque parecchia confusione, tuttavia, tra le diverse opinioni e problemi presenti spiccano due progetti che vale la pena tenere d'occhio:

OpenMeter: progetto europeo facente parte dell'FP7.

Home Gateway Initiative (HGI): un'organizzazione no-profit appoggiata da una lunga serie di brand molto importanti [24, 23].

2.3 Situazione italiana

2.3.1 Oggi

Nel 2001, in anticipo rispetto a molti altri paesi, l'Italia ha iniziato la sostituzione dei vecchi contatori elettromeccanici. Il progetto Telegestore, sviluppato e messo in atto da ENEL, ha fatto del nostro paese un punto di riferimento internazionale per il tema Smart Grid. Per avere un idea del risultato ottenuto, basta pensare che, a 4 anni dalla fine del progetto, siamo tuttora la nazione con più contatori elettronici installati, 32 milioni di utenze. I lavori necessari per mettere insieme il sistema sono stati molti, ma le tempistiche previste sono state rispettate e nel 2006 il sistema era completo. Oltre ai contatori (visibile in figura 2.7) è stato necessario installare 320000 concentratori per la raccolta dei dati dei meter e scegliere un mezzo di comunicazione in grado di sostenere l'infrastruttura [30].

Vediamo quali novità ha introdotto il sistema:

Telelettura Grazie ai nuovi contatori è finalmente possibile la lettura remota dei consumi dell'utenza. Prima del progetto Telegestore, le misure dei consumi

Figura 2.7: Contatore elettronico ENEL

erano effettuate manualmente; un operatore passava per le case e leggeva i consumi direttamente sul contatore. Il problema fondamentale di questa metodologia, oltre al costo del personale, era dovuto alla posizione del contatore. Nel nostro paese la collocazione dei meter è piuttosto varia, nei casi fortunati si trova lungo la strada e facilmente accessibile dall'esterno, ma spesso non è così. Per esempio, in molti condomini di vecchia data, i contatori si trovano nel vano scale che collega al garage. Si presentava quindi la necessità di entrare fisicamente nell'edificio con le conseguenze del caso. Situazioni di questo tipo non sono limitate ai condomini; in molte case è presente lo stesso tipo di problematica. Di conseguenza, l'introduzione della lettura remota dei consumi consente, prima di tutto, di ottenere una riduzione delle spese e, in secondo luogo, costituisce anche una comodità per gli utenti.

Tariffa multioraria Questa nuova funzionalità è di estrema importanza per il futuro. La tariffa multioraria ha costituito il primo vero e proprio passo verso l'AD, con il costo dell'energia diviso nelle fasce:

F1 (ore di punta): dalle ore 8:00 alle ore 19:00 dal lunedì al venerdì

F2 (ore intermedie): dalle ore 07:00 alle ore 08:00 e dalle ore 19:00 alle ore 23:00 dal lunedì al venerdì e dalle ore 07:00 alle ore 23:00 del sabato

F3 (ore non di punta): dalle ore 00:00 alle ore 07:00 e dalle ore 23:00 alle ore 24:00 dal lunedì al sabato e tutte le ore della domenica e dei giorni 1 e 6 Gennaio; lunedì dell' Angelo; 25 Aprile; 1Maggio; 2 Giugno; 15 Agosto; 1 Novembre , 8, 25 e 26 Dicembre

ENEL punta a spingere i propri utenti verso un consumo più controllato. In particolare mira a far calare i consumi in fascia F1 applicando a questa fascia la tariffa più alta e diminuendo progressivamente il prezzo nelle fasce F2 e F3.

Amministrazione remota Oltre al controllo dei consumi, il nuovo sistema di metering consente all'ente erogante la gestione remota di quelle attività di ordinaria amministrazione che, fino a poco tempo fa, dovevano essere svolte

fisicamente dagli operatori sul luogo. I casi più frequenti sono l'attivazione o la disattivazione di nuove utenze e il cambio di potenza contrattuale, operazioni che, finalmente, sono fatte direttamente dalla centrale senza interruzioni e senza la necessità di far uscire gli operatori. Tali vantaggi sono dovuti sopratutto all'automatizzazione delle cabine elettriche, le quali adesso possono essere controllate da remoto. La loro automazione non è totale, manca ancora la rete di self-control di cui abbiamo parlato nel capitolo 1, ma è stata comunque raggiunta un'automazione a livello gestionale. Oltre alla gestione rmota delle utenze, l'automazione di cabine e il monitoraggio dei clienti ha consentito ad ENEL di creare un database dei punti critici della rete. Avendo a disposizione un quadro preciso delle linee che presentano spesso problemi, è di conseguenza possibile intervenire con priorità più alta in tali punti con interventi di riparazione e ammodernamento.

Work Force Management (WFM) Il sistema WFM anche se non strettamente legato all'infrastruttura della rete vale la pena di essere analizzato. Si tratta di un kit hardware-software destinato ai tecnici che operano sulla rete elettrica che consente di avere informazioni in tempo reale sullo stato della rete. Ogni operatore o squadra è dotata di un tablet PC completo di una suite di applicazioni che supportano tutti i processi e ambiti di competenza dei tecnici. La soluzione WFM è particolarmente utile per la gestione logistica delle squadre per evitare i doppi accessi e le uscite a vuoto e risulta inoltre essenziale in caso di calamità naturale o guasto diffuso. In tali situazioni, le squadre o i singoli operatori si trovano spesso ad operare fuori zona e la possibilità di disporre della cartografia tecnica della rete è fondamentale per poter operare. L'adozione di questi strumenti si traduce direttamente in un risparmio per la gestione e un miglioramento del servizio offerto agli utenti.

2.3.2 LonWorks

LonWorks è la piattaforma di rete utilizzata dal sistema di metering di ENEL, si tratta di un sistema completo per lo sviluppo di reti di controllo e monitoraggio su larga scala. La piattaforma è costruita su un protocollo ideato dalla Echelon Corporation che consente al sistema di funzionare con layer fisici eterogenei. Tra i principali citiamo il classico doppino telefonico, il PLC, la fibra ottica e la trasmissione in radiofrequenza. Il nome deriva da un idea del 1999 della sopracitata compagnia che progettò un protocollo di comunicazione specifico per il controllo di automazioni industriali, abitazioni, trasporti ecc.. Tale protocollo, chiamato LonTalk è stato sottoposto a standardizzazione da parte di vari enti nazionali e, come ultimo passo, nel 2009 è stato riconosciuto a livello globale ed è ora noto come ISO/IEC 14908-1.

Tornando a LonWorks, andiamo a vedere quali sono i punti forti che hanno spinto ENEL ad adottare tale tecnologia:

Protocollo open: il già citato protocollo LonTalk è nato in casa Echelon, ma, essendo attualmente standardizzato da vari enti, la sua modifica è totalmente nella mani di ISO/IEC, ANSI e EN che dispongono del brevetto che Echelon

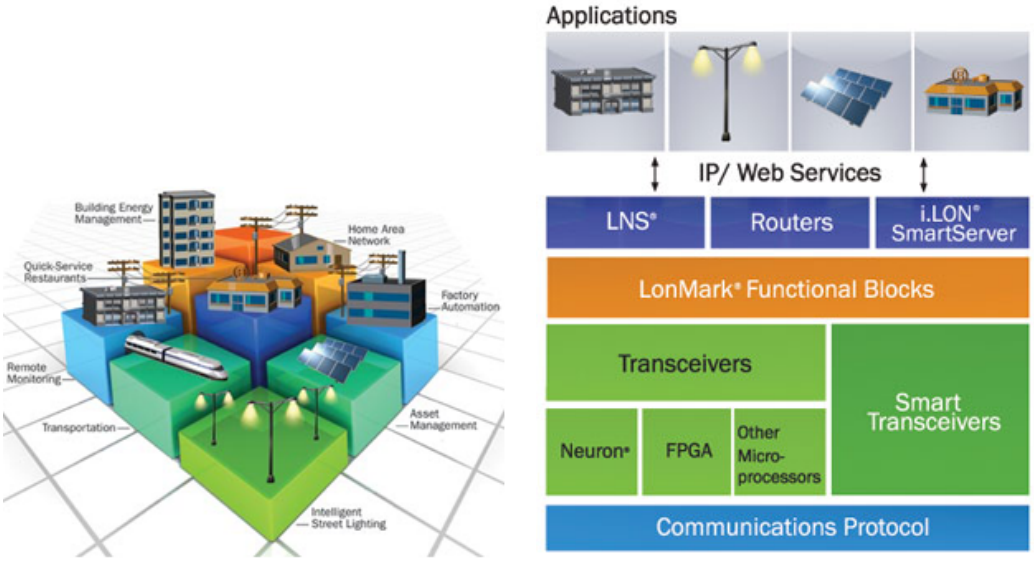


Figura 2.8: Ambiti di utilizzo e architettura della piattaforma LonWorks [35].

ha dovuto fornire nel momento della standardizzazione. Il protocollo è aperto, qualsiasi produttore interessato a produrre dispositivi basati su protocollo LanWorks può farlo. Tuttavia, Echelon ha adottato un piccolo stratagemma per avere degli introiti; ogni chip che sfrutta il protocollo LonWorks per funzionare correttamente deve avare un ID e la fornitura di tale ID costa 0.15$ al produttore di chip. La situazione è simile a quanto accade per i dispositivi di rete, i quali per essere provvisti di un MAC address univoco, devono pagare una tassa alla 3COM. La scelta di un protocollo di questo tipo è stata fatta perché dà la sicurezza di supporto per il futuro. L'uso di un protocollo proprietario vincola al produttore, e lo sviluppo e nelle mani del produttore. Al contrario, la presenza di uno standard fa pensare che nei prossimi anni ci possano essere dei miglioramenti, e di conseguenza, anche la rete attuale potrà beneficiarne.

Esperienza in campo PLC [4] l'idea di ENEL per la realizzazione dell'infrastruttura di comunicazione era quella di non dovere creare una nuova rete, ma sfruttare le potenzialità del PLC. I vantaggi sono notevoli, ma tale tecnologia non è vista di buon occhio da molti a causa della ristrettezza della banda e l'insicurezza. Ciò nonostante, ENEL aveva intravisto le potenzialità del mezzo e per implementare la rete si è rivolta a Echelon, azienda con esperienza quindicennale nel campo della comunicazione PLC. Echelon, con uno studio approfondito a basso livello delle comunicazioni su PLC, è riuscita ad ottenere delle buone prestazioni sia in termini di banda che affidabilità. Un'ulteriore vantaggio molto importante di questo tipo di connessione è la possibilità di sapere quali meter sono collegati ad un determinato trasformatore e, di conseguenza, la possibilità di creare una sorta di mappa della rete, sfruttando i dati relativi all'attenuazione del segnale inviato dai meter. Inoltre, sfruttando un'infrastruttura fisica già esistente, si evitano spese per il mantenimento di nuovi apparati.

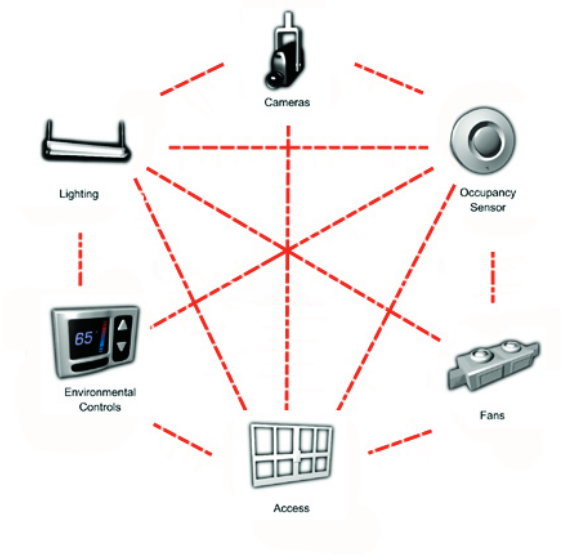


Figura 2.9: Architettura p2p [35].

Rete p2p l'ultimo dei vantaggi importanti dell'utilizzo del protocollo LonWorks è legato alla tipologia della rete. Si tratta di una struttura decentrata di tipo p2p (figura 2.9).Nelle architetture p2p ogni punto è connesso con tutti gli altri e non è presente alcun dispositivo master; questa struttura si traduce in:

- maggiore sicurezza e affidabilità in caso di guasti o attentati.
- tutti i dispositivi sono in grado di comunicare uno con l'altro e, di conseguenza, non è necessario passare per un dispositivo centrale prima di arrivare all'altro utente. Questo significa tempi di risposta più veloci e meno problemi con i colli di bottiglia tipici delle strutture centralizzate.

Tuttavia, allo stato attuale, nella rete ENEL le potenzialità di questa architettura sono utilizzate al minimo; abbiamo visto che i meter comunicano con i concentrator per la raccolta dati e il monitoraggio da centrale, ma non sono ancora in grado di comunicare tra di loro per dar vita all'automazione descritta nella sezione 1.2.4.

2.3.3 Prossimi progetti

Data la sua posizione in prima linea nello sviluppo delle Smart Grid, ENEL è impegnata in diversi progetti finalizzati a rinnovare la rete elettrica.[5] Tra gli scopi principali di questi progetti troviamo:

- L'elettrificazione del settore dei trasporti con lo sviluppo di un estesa infrastruttura di ricarica per veicoli Plug-in Hybrid Electric Vehicle (PHEV).

[5]I dati e le informazioni presenti in questa parte del documento derivano principalmente da [45]

(a) Primo piano di una presa per la ricarica delle auto elettriche della sperimentazione

(b) Colonnine per la ricarica installate a pisa da ENEL

Figura 2.10: Alcuni particolari del progretto E-Mobility [13].

- La realizzazione di un sistema di AD completo, come quello descritto nel capitolo 1, abilitando i piccoli produttori al mercato dell'energia.
- L'integrazione in modo intelligente dei dispositivi di DG nella rete nazionale.

L'elettrificazione dei trasporti, tramite l'ausilio di auto elettriche e infrastrutture di ricarica distribuite sul territorio, è una delle innovazioni di cui si parla da molti anni, ma che, in pratica, non hanno avuto molte sperimentazioni. Nel 2008, ENEL e Smart hanno stipulato un accordo che prevedeva la sperimentazione di un infrastruttura completa per il trasporto elettrico. Il progetto chiamato E-mobility Italy della durata di 3 anni a partire dal 2010, coinvolge 3 città italiane (Roma, Milano e Pisa) nelle quali verranno installate 400 colonnine (figura 2.10b) adibite alla ricarica delle auto PHEV. Le auto, fornite dalla Smart, sono dotate di motore elettrico da 41 CV e batteria agli ioni di litio con capacità di 17kWh in grado di garantire un autonomia di 135 km. La ricarica (figura 2.10a) può avvenire collegando l'auto alla rete di casa o tramite le colonnine installate nelle varie città. Il ruolo di questa sperimentazione è di notevole importanza per lo sviluppo delle tecnologie dei trasporti elettrici e la loro standardizzazione; ENEL partecipa ad entrambi questi compiti in ambito europeo e questa sperimentazione sarà utile per verificare la validità del lavoro svolto finora.[13]

Il secondo punto della lista fa riferimento al ruolo di ENEL nel progetto ADDRESS, di cui abbiamo parlato nella sezione 2.1. Per quanto riguarda le sperimentazioni in tale ambito, sembra che con l'anno prossimo ci saranno i primi test in laboratorio ai quali seguiranno delle dimostrazioni reali, con coinvolgimento dei consumatori in Spagna, Italia e Francia.

L'ultimo punto che ci resta da analizzare è il più coerente con gli argomenti trattati in questo documento. ENEL ha in programma una sperimentazione di Smart Grid in alcune zone del paese; il progetto punta principalmente ad acquisire competenze per non trovarsi impreparati alla massiccia diffusione della DG.

Network	LV	MV	LV+MV
Connected capacity(MW)	28	141	169
Connection request (MW)	73	4494	4567

Figura 2.11: Risorse di generazione distribuita già installate e richieste pendenti di connessione. I dati sono suddivisi tra bassa tensione (LV) e media tensione (MV). [45]

Saranno coinvolte zone del sud Italia dove le scarse infrastrutture di rete rendono più forte l'impatto della generazione distribuita. Le zone geografiche scelte rappresentano un ambiente ideale per fonti rinnovabili come fotovoltaico ed eolico e ci si aspetta una forte crescita degli impianti di microgenerazione per il futuro. Il progetto prevede l'installazione di grandi impianti a energie rinnovabili con dimensioni minime di 20MW per la bassa tensione e 50MW per la media tensione; coinvolgerà inoltre 100000 utenze. Nelle reti delle zone selezionate già buona parte di energia è proveniente dalla generazione distribuita. Ciò nonostante, ENEL ha ricevuto molte richieste per ulteriori impianti. Nella tabella in figura 2.11 sono riportate le quantità in questione. ENEL quindi punta a sfruttare queste zona per vedere se la generazione distribuita può realmente sostituirsi alla costruzione di nuove centrali, garantendo la qualità dell'energia. Il problema più consistente da affrontare è la variabilità della produzione elettrica delle fonti rinnovabili e il punto centrale del progetto è proprio quello di verificare se un efficiente apparato di controllo e gestione della DG è in grado di funzionare in zone così vaste. Per raggiungere lo scopo principale appena discusso bisogna però passare attraverso altri step che adesso elencheremo:

- Controllare l'ampiezza e la frequenza della tensione
- Garantire una qualità dell'energia adeguata (controllo delle oscillazioni di tensione, della frequenza e la presenza di armoniche)
- Aumentare la capacità della rete
- Facilitare il funzionamento ad isola di alcune zone in caso di guasti
- Garantire il funzionamento tenendo conto della variabilità del carico e della generazione
- Ridurre le perdite di rete regolando opportunamente i flussi energetici
- Attivare l'AD

Questi ambiziosi risultati si possono ottenere con un mix di nuove tecnologie; in particolare sono molto importanti gli apparati di comunicazione (figura 2.12) e i dispositivi di stoccaggio energetico. Mentre i primi danno la possibilità ai vari dispositivi di comunicare, i secondi sono utili soprattutto per supplire ai picchi di richiesta inaspettati e gestire l'andamento della richiesta. Sempre restando in ambito tecnologico, il progetto prevede:

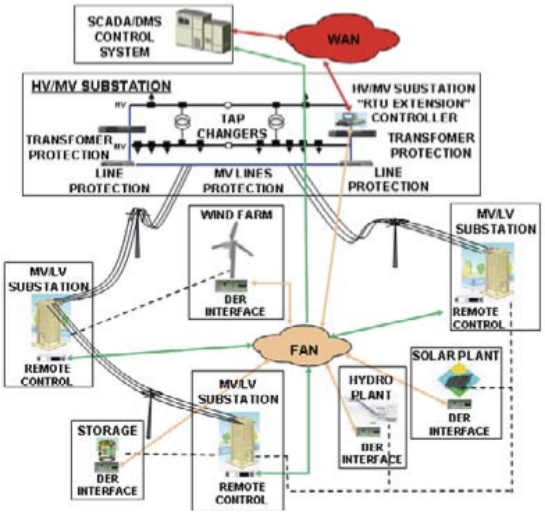


Figura 2.12: Schema dell'infrastruttura per l'integrazione della DG nella rete MT [45].

- L'installazione di router e modem a banda larga per costituire un infrastruttura di comunicazione IP-based
- L'uso di inverter controllabili da remoto per consentire il comando degli impianti di media e grossa taglia
- Un nuovo apparato di supervisione SCADA in grado di controllare autonomamente il sistema dotato di algoritmi di self-healing (autoripristino)
- L'uso di nuovi sensori per la misura dei parametri di interesse e di nuovi attuatori in grado di essere controllati da remoto
- Vari strumenti per la partecipazione al mercato dell'energia delle utenze dotate di microgenerazione

Attualmente il progetto è in fase di sviluppo teorica; tuttavia ENEL sembra intenzionata a iniziare i lavori di implementazione già dall'inizio del 2011, non appena sarà conclusa la fase progettuale.

Capitolo 3

Sicurezza

Con il passaggio dalle reti elettriche statiche di oggi alle reti con una fitta comunicazione del domani si pone un problema finora trascurato, la sicurezza. Iniziamo

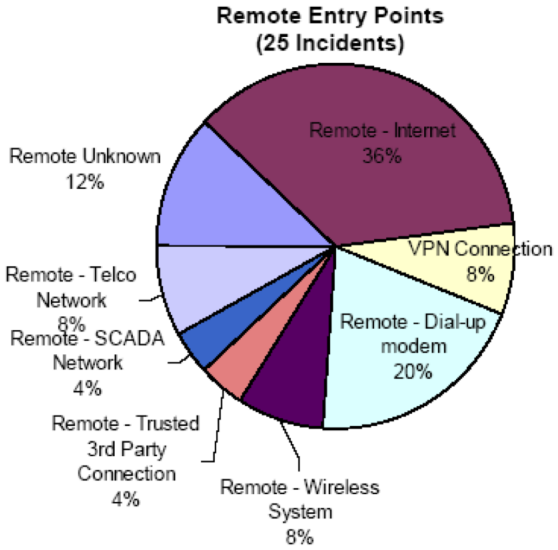


Figura 3.1: Percentuale degli attacchi effettuati sui vari punti di accesso. Dati basati solo sugli attacchi provenienti dall'esterno [22].

l'analisi del problema sicurezza osservando la figura 3.1 dove sono riportate le percentuali degli attacchi effettuati nei vari punti della rete ENEL. Si vede che di particolare criticità sono le connessioni alle cabine di distribuzione dislocate nel territorio, che, come abbiamo visto nella sezione 1.1.2, spesso sono dotate di semplici modem con connessione dial-up con sistemi di protezione minimi. L'esempio fornito da queste strutture è emblematico e dà conferma di quanto detto da Ken Van Meter, presidente della Lockheed Martin, una prestigiosa società specializzata nella sicurezza degli apparati tecnologici. "If you can communicate with it, you can hack it" affermazione banale, ma che mette in risalto l'impossibilità di un'assoluta sicurezza dei sistemi tecnologici dotati di comunicazione. É una situazione analoga al classico "guardia e ladri" del mondo reale; viene inventata una serratura più sicura della precedente e, dopo un po' qualcuno riesce a forzarla; viene inventato un nuovo missile e l'esercito opposto crea un adeguato apparato anti-

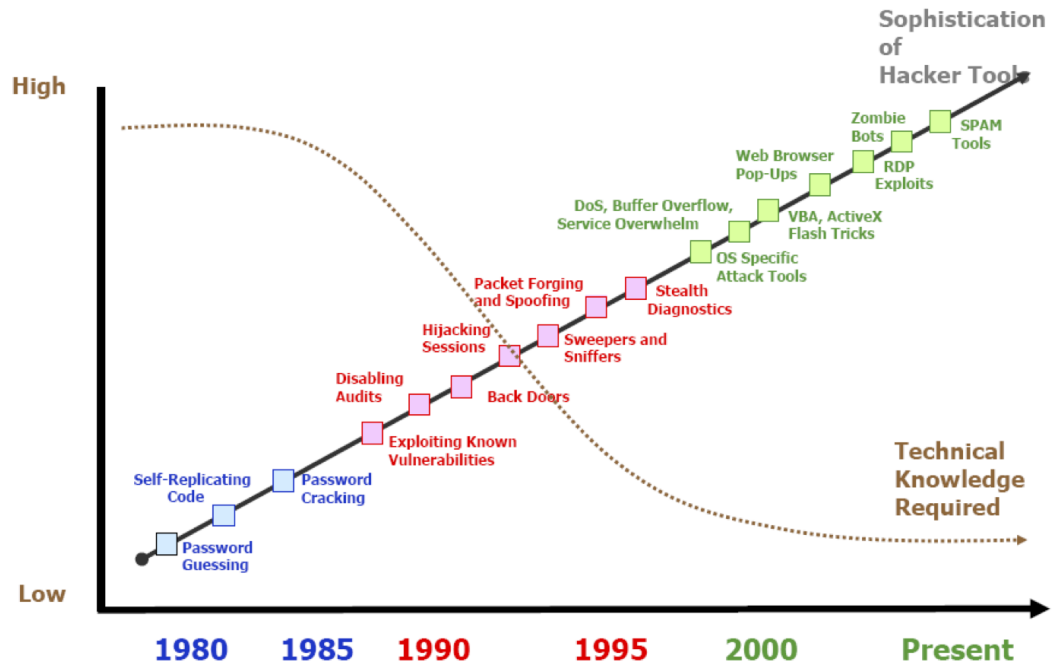


Figura 3.2: Evoluzione degli strumenti utilizzati dagli hacker dagli anni '80 ad oggi [10, p. 19]

missilistico. Nonostante l'apparente pessimismo, queste affermazioni non devono portare a pensare che qualsiasi sistema sia insicuro, bensì dare consapevolezza che, pur non essendoci una soluzione assoluta e definitiva, molto si può fare per ridurre i rischi di intrusioni.

L'esigenza di sicurezza nelle reti intelligenti deriva principalmente dal cambiamento di concetto di rete elettrica; nelle reti di vecchia concezione la maggior parte dei dispositivi erano passivi e privi di comunicazione, con le Smart Grid avremo uno scenario completamente opposto. La rapida diffusione di queste nuove reti aprirà la strada ad una vasta e variegata tipologia di dispositivi connessi da un lato alla rete elettrica e dall'altro ad un'infrastruttura di comunicazione. La maggior parte di queste apparecchiature, dovendo essere dotate di "intelligenza", saranno di conseguenza basate sull'utilizzo di microprocessori; ci si troverà quindi ad avere una rete di dispositivi con una consistente presenza di software. Come noto, la complessità e i vari bug fanno del software uno degli elementi più critici per la sicurezza. Un'ulteriore aggravante di questo problema è l'aumento della complessità degli attacchi e la diminuzione del know-how necessario per metterli in atto. In figura 3.2 è riportato un grafico molto eloquente sull'evoluzione degli strumenti utilizzati dagli hacker negli ultimi anni. Un altro elemento da considerare è l'inesperienza delle utilities nel campo sicurezza elettronica. Fino ad ora, le varie aziende che si occupavano di generare e distribuire energia elettrica facevano solo quello e dati i mezzi arcaici usati per il controllo remoto dei dispositivi non davano molto peso al problema sicurezza. Andy Bochman, che gestisce il settore sicurezza del reparto Energy dell' IBM, ha raccolto una serie di motivazioni del perché le utilities non si sono fino ad ora occupate di sicurezza [8]:

1. Non se ne preoccupavano
2. Si concentravano su altri campi, ritenendo che non fosse un problema di grande importanza
3. Non avevano soldi da investire e mancava uno staff dedicato a questo ambito
4. Si sentivano al sicuro con le semplici attenzioni che adottavano

Nei prossimi anni, per quanto elencato precedentemente, le utilities si troveranno davanti ad una rete con milioni di dispositivi intercomunicanti e dovranno imparare a gestirla in fretta, perché i progressi sono veloci, le vulnerabilità sono molte e la loro esperienza in questo campo è quasi nulla.

3.1 Episodi e ipotetici esempi di attacchi o altri problemi legati alla sicurezza

Nell'aprile del 2009, il Wall Street Journal ha pubblicato un allarmante articolo riguardante la sicurezza della rete elettrica degli USA. Secondo le informazioni fornite dall'agenzia di sicurezza nazionale americana, c'era stata una violazione del sistema di gestione della rete elettrica da parte di alcune organizzazioni Russe. Non sono stati fatti danni, ma il livello di accesso ottenuto dagli hacker era tale da poter compromettere la rete; si sono invece limitati a lasciare ben nascosti dei software in grado di consentire loro di riprendere il controllo il caso di bisogno. Tuttavia, oltre il rischio corso, il fatto più eclatante di questa notizia è che non sono state le varie utilities ad accorgersi dell'intrusione, bensì l'agenzia di sicurezza nazionale. [19]

Questo fatto è solo uno dei tanti episodi avvenuti negli ultimi anni; l'arrivo delle Smart Grid apre le porte ad un'infinità di vulnerabilità e sarebbe impossibile analizzarle tutte. Risulta però utile capire a grandi linee quali danni possono causare i tipi di attacco più comuni.

False data injection attacks in electricity markets. Durante l' IEEE SmartGridComm2010, Li Xie ha dimostrato come la modifica dei dati proveniente dai sensori possa essere usata per scopi fraudolenti. Come abbiamo già detto nella sezione 1.1.3, le utilities si organizzano sull'energia da acquistare dai grossisti in base a modelli statistici, c'è quindi una contrattazione preventiva e, nel caso di una richiesta non programmata, le utilities pagano caro quanto non avevano previsto. Un malintenzionato, in grado di modificare in maniera adeguata i dati rilevati dai sensori lungo la rete, potrebbe far visualizzare alla centrale un carico fittizio e, così facendo, costringere le utilities ad acquistare energia in eccesso. Inoltre, se il malintenzionato fosse abbastanza ferrato potrebbe puntare dei soldi nel mercato dell'energia e ricavarne un profitto prevedendo in anticipo una domanda inaspettata. [9]

False data injection attacks in electrical grid. Allo stesso modo dell'attacco precedente un malintenzionato che riuscisse ad introdursi nel sistema di monitoraggio della rete potrebbe inserire dati falsi che portino la centrale a vedere

su una determinata linea un carico inferiore a quello reale. Così facendo, si avrebbe un sovraccarico sui generatori, con la conseguente attivazione dei sistemi di protezione passiva che staccano la corrente. A questo punto, per le cause viste nella sezione 1.1.1 potrebbe seguire un blackout a catena. [9]

Attacchi al sistema SCADA. Il sistema di supervisione e controllo è da molti anni soggetto ad attacchi da parte di hacker; di particolare rilevanza è un episodio avvenuto quest'anno. In luglio c'è stata per la prima volta la diffusione su larga scala di un malware in grado compromettere la sicurezza dei sistemi SCADA usati dai vari enti. La diffusione, iniziata in Iran e continuata in molti altri paesi del mondo, è di particolare criticità in quanto ha consentito ai malintenzionati di mappare il sistema di supervisione e avrebbe addirittura consentito di azionare dispositivi da remoto. Tale capacità è particolarmente pericolosa, dato che moltissimi sistemi industriali sono sullo SCADA. Senza esagerare, gli autori del gesto avrebbero potuto mettere le mani sulla sala controllo di una centrale nucleare, di una diga o della rete elettrica. Fino ad ora, attacchi simili erano stati molto rari perché l'apparato tecnologico che supporta i sistemi SCADA è, nella maggior parte dei casi, basato su (PLC) Programmable Logic Controller della Siemens. Tali apparecchiature sono dotate di un linguaggio di programmazione proprietario che richiede una certa competenza per essere forzato. In questo caso, l'attacco è partito da una memoria USB fornita direttamente ad un operatore di sala controllo con qualche scusa o più semplicemente lasciata appositamente in un luogo dove potesse essere raccolta dalla persona giusta. La chiavetta, una volta inserita in un computer interno alla rete, sfruttando una vulnerabilità di Windows ha eseguito un codice che ha contaminato il PC. Sfruttando una seconda vulnerabilità, il malware è riuscito a espandersi nella rete e una volta trovato uno di quei PC adibiti al monitoraggio dei PLC era in grado di riportare le informazioni tramite internet all'intrusore. A questo punto, altre 2 vulnerabilità di Windows avrebbero consentito al malintenzionato di iniettare codice maligno all'interno del PLC e comandare i dispositivi ad esso connessi. [29]

Come spesso accade l'attacco, è stato possibile per la presenza di più di una vulnerabilità; se ce ne fosse stata solo una o due il malware non sarebbe partito o comunque non sarebbe arrivato ad avere i privilegi tali da consentirgli di iniettare codice sul PLC. Si evince quindi che nessuna vulnerabilità può essere tralasciata e per arginarle è fondamentale tenere aggiornati i software. A questo scopo, risulta utile citare uno studio. Jonathan Pollet della Red Tiger Security ha voluto effettuare una ricerca sulle vulnerabilità che affliggono i sistemi SCADA; i dati emersi sono piuttosto drammatici. Il tempo medio da quando viene scoperta a quando viene tappata una falla è di 331 giorni con un picco di 1100 giorni per il caso peggiore. Questo si traduce nel fatto che, in media, un malintenzionato può sfruttare per 1 anno una vulnerabilità, ma se gli va bene, può usufruirne per più di 3 anni [37, p. 13].

Falsificazione dei dati provenienti dai meters. Questa situazione è di impatto minore rispetto alle precedenti, ma costituisce comunque un elemento da

non trascurare. Come sappiamo, il meter è il dispositivo che tra gli altri compiti si occupa anche di misurare i consumi dell'utenza ed è di facile accesso per l'utenza, dato che viene installato all'interno della proprietà. Queste caratteristiche preannunciano una situazione abbastanza pericolosa, in quanto un utente con cattive intenzioni, avendo a disposizione accesso al contatore potrebbe in qualche modo manometterlo. L'idea è semplice, ma il processo è piuttosto complicato. Tuttavia, una persona dotata di sufficienti competenze potrebbe riuscire a falsificare i propri consumi senza dare nell'occhio. Lo stesso contatore installato da ENEL sembra essere soggetto da qualche tempo a manomissioni che consentirebbero all'utente di aumentare la potenza contrattuale disponibile senza pagare un supplemento sulla bolletta. Le notizie riguardanti questa pratica sono piuttosto inaffidabili; ciononostante, una cosa è certa, il dispositivo installato da ENEL è dotato di porta infrarossi. Quest'ultima viene usata durante l'installazione con l'ausilio del tablet facente parte del sistema WFM di cui abbiamo parlato nella sezione 2.3.1. Sicuri che ENEL abbia pensato a qualche sistema di autenticazione, la possibilità di comunicare con il meter tramite questa porta è comunque un buon punto di partenza per eventuali malintenzionati.[33]

Uso fraudolento dei dati. Uno dei grossi problemi derivanti dalla vasta diffusione di sensori e strumenti di misura sulla rete elettrica è la privacy degli utenti. Con l'arrivo delle Smart Grid e l'attivazione dell'AD è necessario un intenso scambio di dati tra i vari soggetti partecipanti alla gestione dell'energia. Come spiegato nella sezione 2.1, per attivare l'AD è necessario monitorare i consumi delle singole utenze e passare i dati ad un ente terzo che gestisce la rete; da qui nasce l'esigenza di tutelare tali dati dai non addetti ai lavori. L'idea potrebbe sembrare un po' paranoica e qualcuno potrebbe obiettare:"si tratta soltanto dei dati sul consumo di energia di un'utenza, a chi mai potrebbero interessare". Nulla di più sbagliato. Il National Institute of Standards & Technology (NIST), nella sua guida alla sicurezza, ha pubblicato un elenco di usi non consueti dei dati di consumo dei cittadini; vediamoli brevemente [44] :

- Le **compagnie assicurative**, tramite lo studio dei consumi, potrebbero ricavare le abitudini dei clienti e da queste ottenere dati interessanti per le loro analisi dei rischi. Per esempio, consumi anomali durante la notte potrebbero indicare che l'inquilino non dorme bene, il che potrebbe significare che tale persona non è in buono stato di salute e questo garantirebbe un aumento sulla polizza a vita. La stessa cosa potrebbe avvenire per le polizze sui furti; un'abitazione dove c'è spesso qualcuno a casa è meno a rischio di una dove gli abitanti lavorano 12 ore al giorno. Dai consumi è facile ottenere questo tipo di informazioni.
- Dai dati sui consumi le **aziende pubblicitarie** potrebbero ottenere molte informazioni importanti sui nostri stili di vita.
- Le **forze dell'ordine** potrebbero usare i dati per rilevare attività illegali o sorvegliare l'abitazione per vedere in tempo reale se c'è qualcuno in casa e cosa sta facendo. Applicazioni di questo tipo sono già state usate

negli Stati Uniti per determinare le coltivazioni casalinghe di marijuana; in tali abitazioni i consumi risultavano eccessivi, ma, sopratutto, continui.

- Il **proprietario** di un appartamento potrebbe usare i dati dell' **affittuario** per verificare il rispetto dei termini concordati nel contratto di locazione. Dai consumi non è difficile rilevare il numero di occupanti dell'abitazione.
- I **mass-media** potrebbero pubblicare articoli in cui analizzano i consumi dell'abitazione di un personaggio famoso. Un esempio di questo tipo di utilizzo fraudolento è rappresentato dai vari articoli che commentavano i consumi eccessivi della casa in Tennessee di Al Gore.
- Le **banche**, come le assicurazioni, dal cambiamento nello stile di vita di un loro cliente potrebbero ottenere informazioni sul rischio del credito offerto; anche qui, consumi inaspettati durante la notte possono indicare problemi al lavoro con conseguente aumento del rischio di disoccupazione.
- Dei **criminali** potrebbero usare le informazioni sui consumi per rilevare la presenza in casa di persone e il tipo di dispositivi in essa presenti. Allo stesso modo, nelle aziende, i dati sui consumi potrebbero fornire dalle buone informazioni sulle tecnologie utilizzate dai concorrenti, una sorta di **spionaggio industriale**.

3.2 Come migliorare la sicurezza

Come detto all'inizio della sezione precedente, il concetto di sicurezza assoluta è un'idea non raggiungibile in pratica. Il lavoro da svolgere è quello di ridurre le possibilità di intrusione e, per ottenere questo risultato, il principio più efficiente è quello di usare un sistema a livelli. Con sicurezza stratificata a livelli, si intende l'uso contemporaneo di più sistemi di difesa (principalmente firewall, Intrusion Detection System (IDS), antivirus e crittografia) ognuno destinato a proteggere determinati segmenti della rete. [43, p. 25]

3.2.1 Sicurezza di alto livello

Nell'agosto scorso, il NIST ha pubblicato 3 volumi riguardanti le linee guida per la sicurezza delle Smart Grid. Scopo del documento è fornire indicazioni a produttori ed enti su come muoversi per sviluppare i propri progetti, mantenendo uno standard di sicurezza accettabile. All'interno del testo vengono analizzate in dettaglio le problematiche che potrebbero affliggere i vari rami della rete. In figura 3.3 è riportato lo schema dei collegamenti tra i vari soggetti che da l'idea di quanto complesso sia il sistema. Per dare delle indicazione sul livello di sicurezza da adottare nei vari collegamenti, il NIST ha diviso gli ipotetici collegamenti in 22 categorie che raggruppano i tipi di collegamenti con requisiti simili [43, p. 27]. Successivamente basandosi sui concetti di [43, p. 73], ovvero:

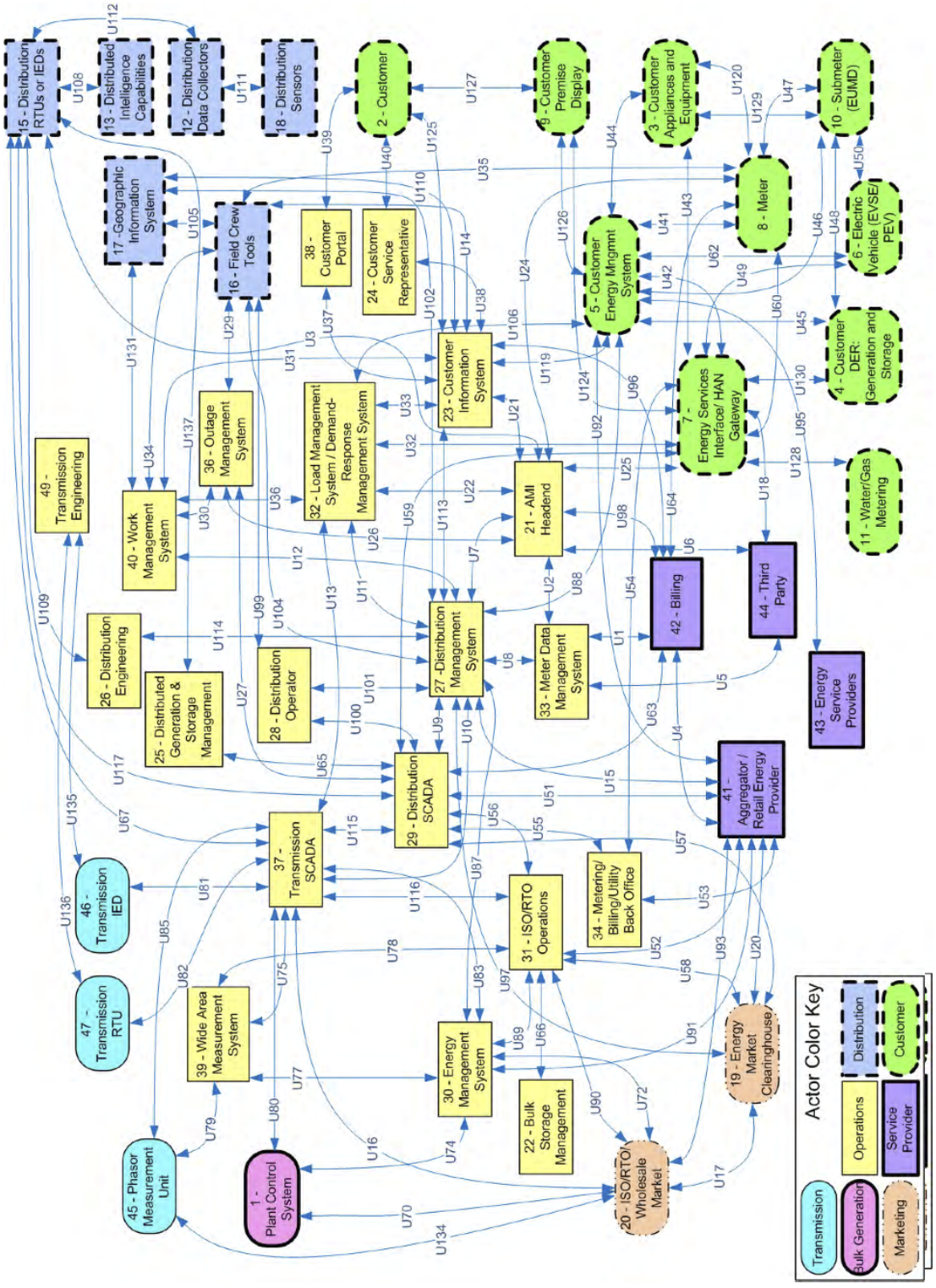


Figura 3.3: Schema dei soggetti partecipanti alla Smart Grid e collegamenti tra di essi [44].

Logical Interface Category	Confidentiality	Integrity	Availability
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	M	L
8	H	M	L
9	L	M	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	L	H	L
19	L	H	M
20	L	H	M
21	L	H	L
22	H	H	H

Figura 3.4: Livello di priorità ([L] basso,[M] medio, [H] alto) per definizioni e categorie [43, p. 75].

Confidenzialità: preservare l'accesso a informazioni e limitarne la diffusione non autorizzata. La mancanza di confidenzialità è intesa come la diffusione non autorizzata di dati protetti.

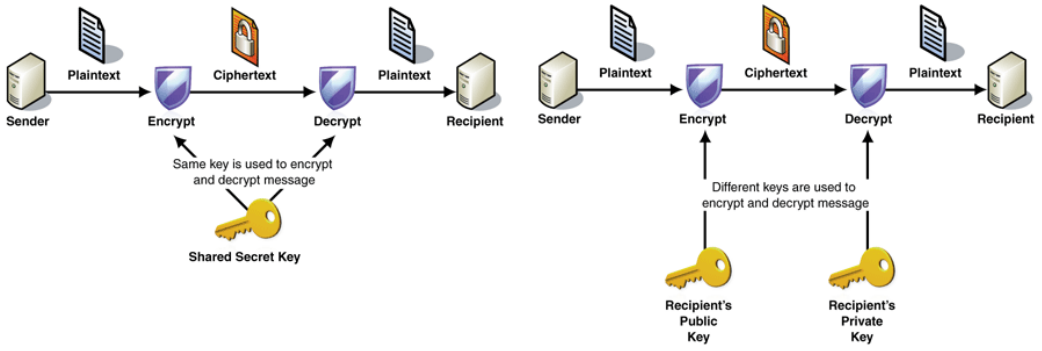
Integrità: proteggere le informazioni da modifiche o eliminazioni non autorizzate in modo da garantirne l'autenticità. Con perdita di integrità si fa riferimento alla modifica o l'eliminazione non autorizzata di dati.

Disponibilità: assicurare il pronto e affidabile accesso alle informazioni. Una perdita di disponibilità significa non poter accedere alle informazioni.

ha redatto una tabella (figura 3.4) dove ad ognuna categoria è associato un livello di priorità per le tre definizioni appena elencate. Come ultimo passo, per dare informazioni dettagliate su come organizzare la sicurezza, il NIST fornisce una tabella ([vedi 43, p. 79, tabella 3.3]) che elenca dettagliatamente quali requisiti deve soddisfare ogni categoria.

3.2.2 Crittografia e gestione chiavi

Oltre a fornire indicazioni ad alto livello sulla sicurezza, il NIST menziona l'uso di una infrastruttura di crittografia a chiave pubblica per le connessioni tra i vari dispositivi della rete [43, p. 211]. Lo scopo di questo sistema è di cifrare i dati in transito sui canali di comunicazione, in modo che le informazioni siano incomprensibili ad eventuali malintenzionati. In particolare la Public Key Infrastructure (PKI) sembra piuttosto adatta al compito da svolgere [31, p. 101]. La figura 3.5a rappresenta il processo di crittografia a chiave simmetrica. Per criptare il messaggio, il mittente passa la chiave e il testo in chiaro all'algoritmo di codifica



(a) (b)

Figura 3.5: Crittografia a chiave simmetrica e asimmetrica

che dà in uscita il testo cifrato. Questo a sua volta viene inviato sul canale di comunicazione e il ricevente può leggerlo usando l'algoritmo di decodifica e la chiave. La sicurezza di questo sistema di codifica è basta sulla robustezza dell'algoritmo e la sicurezza della chiave, ed è proprio quest'ultimo il punto debole. Dal nome crittografia a chiave simmetrica si capisce che la chiave è una sola e viene usata sia per la codifica che la decodifica; di conseguenza entrambi i soggetti devono avere la stessa chiave. Per far sì che questo avvenga, i 2 soggetti devono in qualche modo scambiarsi la chiave e se il canale di comunicazione usato non è sicuro la chiave potrebbe essere intercettata. Lo stesso problema affligge lo stoccaggio delle chiavi; se i 2 soggetti non le custodiscono adeguatamente la sicurezza diminuisce.

Passando alla figura 3.5b vediamo lo schema del principio di funzionamento della crittografia a chiave asimmetrica: come si vede, ogni soggetto deve avere 2 chiavi, una pubblica e una privata. Supponiamo che il mittente (Alice) voglia inviare un messaggio al destinatario (Bob); Alice deve cifrare il messaggio usando la chiave pubblica di Bob. Una volta ricevuto, tramite la sua chiave privata e l'algoritmo di decodifica Bob lo può decifrare. La sicurezza di tale sistema è garantita dalla robustezza dell'algoritmo di cifratura e la sicurezza con cui è conservata la chiave privata. Rispetto al caso precedente traspare un notevole vantaggio, in quanto ogni soggetto si deve occupare solo di tenere al sicuro la propria chiave privata. Quella pubblica, in quanto tale, può essere liberamente distribuita in modo che gli altri soggetti possano inviare messaggi cifrati leggibili solo dal legittimo destinatario. Come svantaggio, rispetto al sistema precedente, si hanno degli algoritmi più complessi, che richiedono una capacità di calcolo maggiore. Per ovviare a questo problema si pensa di utilizzare una PKI come sistema base per consentire ai soggetti di poter scambiare delle chiavi simmetriche in modo sicuro. Vediamo, analizzando la figura 3.6, come funziona il processo:

1. Il soggetto interessato a comunicare in modo sicuro con gli altri componenti della rete invia alla Registration Authority (RA) una Certificate Signing Request (CSR). Il CSR è un documento contente informazioni che identificano il soggetto richiedente e la sua chiave pubblica.

2. L' RA verifica l'identità del richiedente, e in caso affermativo, firma il certificato e lo passa alla Certificate Authority (CA).

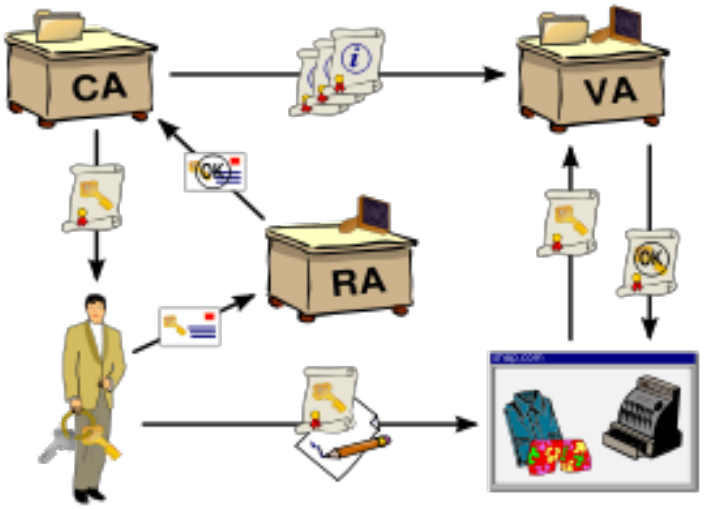


Figura 3.6: Componenti del sistema PKI e principali soggetti

3. La CA distribuisce il certificato.

Una volta che tutti i soggetti della rete hanno effettuato questo processo, la CA possiede tutti i certificati dei soggetti ed è in grado di garantire la loro autenticità. A questo punto i vari soggetti che partecipano alla rete possono autenticarsi tra di loro e scambiarsi le chiavi per costituire dei collegamenti a crittografia simmetrica. In questo modo le chiavi condivise vengono scambiate in maniera sicura e non c'è un eccessivo carico computazionale dato che gli unici dati passati tramite una sessione a crittografia asimmetrica sono quelli relativi alla chiave condivisa [31].

3.2.3 Sistemi per la tutela della privacy

Nella sezione 3.1 abbiamo visto quali danni possano causare i dati sui consumi se finiscono nelle mani sbagliate. D'altro canto, tutti i concetti che abbiamo visto nella sezione 2.1 e nelle precedenti richiedono l'identificazione del meter per consentire alla DG di funzionare. All'IEEE SmartGridComm2010 due ricercatori della Toshiba hanno presentato una soluzione a questo problema. L'idea su cui si basa il sistema è quello di imitare il lavoro svolto da un server proxy, che nasconde l'indirizzo IP di un computer prima di metterlo in contatto con la rete esterna [7].

Il punto di partenza è fornire il meter di due ID, indirizzi univoci che lo identificano nella rete, come il MAC address per le schede di rete. I due ID avranno i seguenti scopi:

LFID: servirà per le comunicazioni poco frequenti, cioè si occuperà di gestire i dati settimanali o mensili per la gestione del contratto e delle bollette.

HFID: servirà per le comunicazioni più frequenti, che possono fornire dati sulla vita privata e che consentono il funzionamento della DG.

In questo modo, come si vede dalla figura 3.7, alle utilities vengono inviati direttamente soltanto i dati provenienti da LFID mentre i dati provenienti da

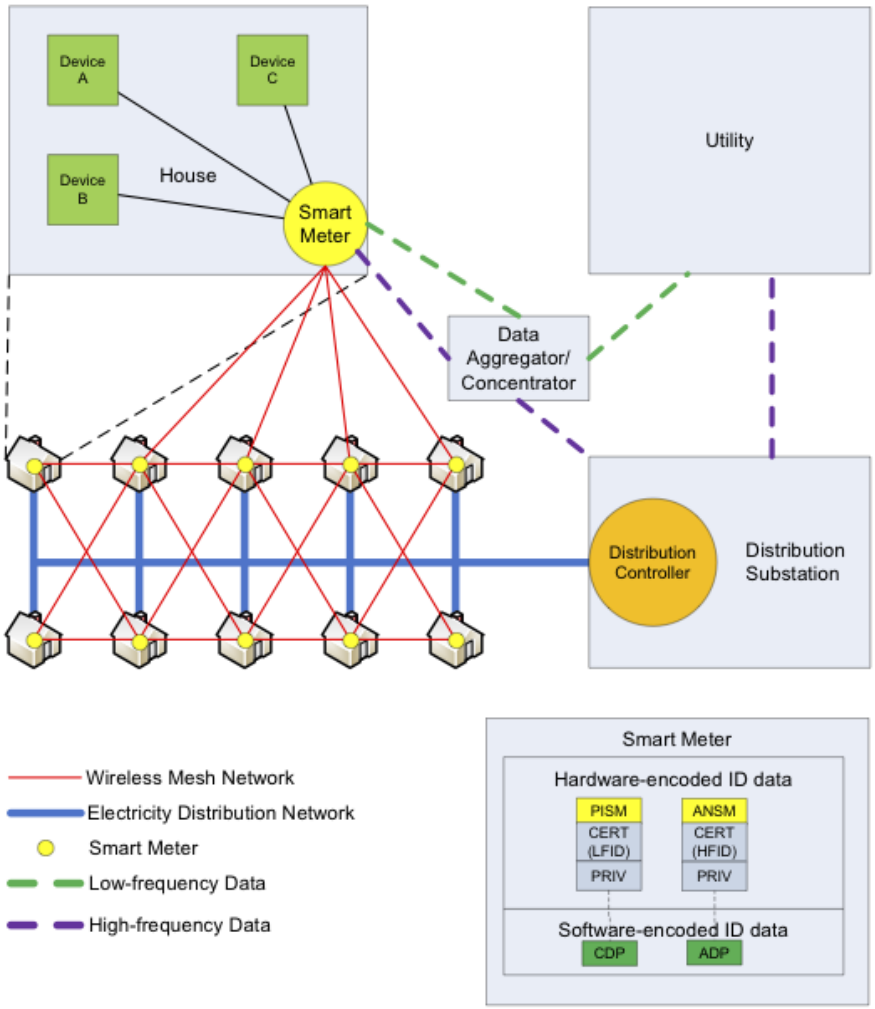


Figura 3.7: Componenti del sistema per la tutela della privacy presentato da Toshiba [14].

HFID vanno nelle sottostazioni, dove servono per gestire la DG. I dati che arrivano nelle sottostazioni hanno come unico identificativo l'HFID. Dato che questo non è visibile o ricavabile dal meter, non è associato ad un'utenza fisica, garantendo così l'anonimato.[14]

Conclusioni

In questo documento abbiamo potuto osservare come le Smart Grid possano essere un elemento utile e innovativo per cambiare l'attuale sistema di distribuzione energetica. I cambiamenti che ci aspettano nei prossimi anni non riguardano solo la struttura della rete e le tecnologie. Con l'avvento della AD, gli elettrodomestici saranno dotati di una certa autonomia e dovremo quindi abituarci a convivere con questo nuovo modello di consumo.

Il processo di cambiamento non è semplice, nè veloce; prima di vedere attive tutte le funzionalità di cui abbiamo parlato passeranno diversi anni. Come abbiamo visto nel capitolo 2, ci sono molti cambiamenti da effettuare sia per l'implementazione delle infrastrutture che per la gestione del nuovo sistema.

Ad oggi, già molti paesi si sono attivati per lo sviluppo della nuova rete elettrica, ma quello che manca è una standardizzazione a livello sovranazionale. Nonostante l'intenso lavoro di molti enti autorevoli, come IEEE e IEC, la strada è ancora lunga. Ci sono già molte tecnologie interessanti pronte all'uso, ma la difficoltà è mettere d'accordo i vari paesi. Ogni paese ha finora gestito il proprio sistema elettrico in maniera autonoma e ci troviamo davanti ad un eterogeneità di sistemi che non rende il compito facile.

Collegato alla mancanza di standardizzazione, si allaccia il problema dell'interoperabilità dei dispositivi già presenti sul mercato. Molti marchi prestigiosi (IBM, CISCO, ecc.) offrono soluzioni per l'infrastruttura di rete, sia in ambito HAN che nelle aree più vaste. Da questo deriva che un utente potrebbe presto trovarsi a comprare dispositivi pronti per l'AD che, al momento del bisogno, non saranno in grado di funzionare, perché usano uno standard diverso da quello dell'HG.

L'ultimo aspetto, che è emerso dall'analisi effettuata nel documento, riguarda la sicurezza. L'avvento delle Smart Grid e la conseguente mole di dati disponibili sui consumi non deve diventare l'ennesima sorgente di informazioni per pubblicitari, malintenzionati ecc.. Emerge la necessità di sviluppare un sistema sufficientemente sicuro per garantire la privacy agli utenti ed evitare che malintenzionati riescano a comprometterne l'efficienza.

Acronimi

ICT	Information and Communications Technology
voIP	Voice over Internet Protocol
AT	Alta Tensione
MT	Media Tensione
BT	Bassa Tensione
SCADA	Supervisory Control and Data Acquisition
DG	Distributed Generation
PHEV	Plug-in Hybrid Electric Vehicle
PEV	Plug-in Electric Vehicle
AD	Active Demand
ADDRESS	Active Distribution networks with full integration of Demand and distributed energy RESourceS
FP7	Settimo Programma Quadro
AMI	Advanced Metering Infrastructure
HAN	Home Area Network
WP	Work Package
WFM	Work Force Management
PLC	Power line communication
NIST	National Institute of Standards & Technology
IDS	Intrusion Detection System
PKI	Public Key Infrastructure
RA	Registration Authority
CSR	Certificate Signing Request

CA	Certificate Authority
NAN	Neighborhood Area Network
HAN	Home Area Network
WAN	Wide Area Network
HG	Home Gateway
WiMAX	Worldwide Interoperability for Microwave Access
IPTV	Internet Protocol Television
RF	Radio Frequency
AP	Access Point
ISM	Industrial, Scientific and Medical
HGI	Home Gateway Initiative
DR	Demand Response
DP	Dynamic Pricing
WiFi	Wireless Fidelity
PMU	Phasor Measurement Unit
GPS	Global Positioning System
GIS	Geographic Information System
PF	Power Factor

Bibliografia

[1] URL: http://www.worldometers.info/.

[2] Il sole 24 ore. *Enel: 9 mln utenze domestiche elettriche target al 2011*. URL: http://archivio-radiocor.ilsole24ore.com/articolo-554711/enel-9-mln-utenze-domestiche/.

[3] Maurizio Delfanti Antonio Capone. "Infrastrutture e tecnologie di comunicazione per le Smart Grid". In: *AEIT* 5/6 (2010).

[4] *As LonWorks 2.0 ships, Echelon reflects on smart grid milestones*. 2010. URL: http://www.echelon.com/company/news/articles/2010/2010.04.13_SmartGridToday-2mmMeters.pdf.

[5] Commissione di Indagine del Ministro delle Attività Produttive. *Black-out del sistema elettrico italiano del 28 settembre 2003*. URL: http://dgerm.sviluppoeconomico.gov.it/dgerm/downloads/RapportoBlackout-28092003.pdf.

[6] C. Bennett e D. Highfill. "Networking AMI Smart Meters". In: *Energy 2030 Conference, 2008. ENERGY 2008. IEEE*. Nov. 2008, pp. 1 –8. DOI: 10.1109/ENERGY.2008.4781067.

[7] Ariel Bleicher. "Privacy on the Smart Grid". In: *IEEE spectrum* (ott. 2010). URL: http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

[8] Andy Bochman. *SGSB Webcast 5: Smart Grid Software Security*. URL: http://www.slideshare.net/abochman/sgsb-5-sg-software-security.

[9] Kevin Bullis. *How to Hack the Power Grid for Fun and Profit*. Technology Review Published by MIT, ott. 2010. URL: http://www.technologyreview.com/printer_friendly_article.aspx?id=26472&channel=energy&section=.

[10] Benjamin M. Butchko. *Cyber and process control security*. PlantData Technologies, ott. 2005. URL: http://www.ifssevent.com/pdf/paper_archives/57032.pdf.

[11] F. De Ridder, M. Hommelberg e E. Peeters. "Four potential business cases for demand side integration". In: mag. 2009, pp. 1 –6. DOI: 10.1109/EEM.2009.5207197.

[12] *Deliverble D1.1 ADDRESS Technical and commercial conceptual architectures*. 2009.

[13] *E-mobility italy official website*. URL: http://www.e-mobilityitaly.it/.

[14] Costas Efthymiou e Georgios Kalogridis. "Smart Grid Privacy via Anonymization of Smart Metering Data". In: *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. Ott. 2010, pp. 238 –243. DOI: 10.1109/SMARTGRID.2010.5622050.

[15] U.S. Deparment of Energy. *The Smart Grid: An introduction*. URL: http://www.oe.energy.gov/SmartGridIntroduction.htm.

[16] Roberto De Bonis Fabio L. Bellifemine Claudio Borean. "Smart Grids: Energia e ICT". In: *Notiziario tecnico Telecom Italia* 3 (2009).

[17] Ahmad Faruqui. *The Power of Five Percent: How Dynamic Pricing Can Save $35 Billion in Electricity Costs*. Mag. 2007. URL: http://www.brattle.com/_documents/UploadLibrary/Upload574.pdf.

[18] Katie Fehrenbacher. *The Power Grid Is So Dumb That...* URL: http://gigaom.com/cleantech/the-power-grid-is-so-dumb-that/.

[19] Siobhan Gorman. "Electricity Grid in U.S. Penetrated By Spies". In: *The wall street journal* (2009). URL: http://online.wsj.com/article/SB123914805204099085.html.

[20] Mark Thompson Greg Ennis. "Wireless networks will enable the smart grid worldwide". In: *Metering International magazine* (2010).

[21] GRTN. *Blackout: gli eventi accaduti il 28 settembre 2003*. URL: http://www.aei.it/grtn01-10-03.pdf.

[22] Luca Guidi. *Sicurezza informatica degli impianti di generazione elettrica:l'esperienza ENEL e il Laboratorio Cybersecurity SCADA*. URL: www.progettoreti.enea.it/presentazioni/ENEL-Cybersecurity.ppt.

[23] *Home Gateway Initiative*. URL: http://www.homegatewayinitiative.org/.

[24] Home Gateway Initiative. *Home Gateway Technical Requirements: Release 1*. 2006. URL: http://www.homegatewayinitiative.org/publis/HGI_V1.0.pdf.

[25] A. Ipakchi e F. Albuyeh. "Grid of the future". In: *Power and Energy Magazine, IEEE* 7.2 (mar. 2009), pp. 52 –62. ISSN: 1540-7977. DOI: 10.1109/MPE.2008.931384.

[26] Mike E. Beehler James G. Cupp. "Implementing Smart Grid Communications". In: *TECHbriefs* (2008).

[27] Fangxing Li et al. "Smart Transmission Grid: Vision and Framework". In: *Smart Grid, IEEE Transactions on* 1.2 (set. 2010), pp. 168 –177. ISSN: 1949-3053. DOI: 10.1109/TSG.2010.2053726.

[28] David JC MacKay. *Sustainable Energy — without the hot air*. UIT, 2008.

[29] Paul Marks. *Why the Stuxnet worm is like nothing seen before*. Ott. 2010. URL: http://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before.html.

[30] Meters e More Association. *Comunicato stampa, 18/02/2010*. URL: http://www.metersandmore.eu/doc/press_release_it.pdf.

[31] A.R. Metke e R.L. Ekl. "Security Technology for Smart Grid Networks". In: *Smart Grid, IEEE Transactions on* 1.1 (giu. 2010), pp. 99 –107. ISSN: 1949-3053. DOI: 10.1109/TSG.2010.2046347.

[32] Cristina Morere e Jean Trzcinski. "Distributed generation in Belgium: What are the challenges and solutions for the actors of the energy value chain?" In: *Metering International magazine* Issue 3 (2010).

[33] Erica Naone. *Hacking the Smart Grid*. Technology Review Published by MIT, ago. 2010. URL: http://www.technologyreview.com/printer_friendly_article.aspx?id=25920.

[34] NOAA. *NOAA POSTS IMAGES ONLINE OF NORTHEAST BLACKOUT*. URL: http://www.noaanews.noaa.gov/stories/s2015.htm.

[35] *Official LonWorks website by Echelon*. URL: http://www.echelon.com/products/lonworks_control_networking.htm.

[36] Michael Longrie Philippe Guillemette. "Build a smart grid with a multi-technology communications approach". In: *Metering International magazine* (2010).

[37] Jonathan Pollet. *Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters*. Red Tiger Security, lug. 2010. URL: http://media.blackhat.com/bh-us-10/whitepapers/Pollet_Cummins/BlackHat-USA-2010-Pollet-Cummings-RTS-Electricity-for-Free-wp.pdf.

[38] K. Schneider et al. "Impact assessment of plug-in hybrid vehicles on pacific northwest distribution systems". In: *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE* (lug. 2008), pp. 1 –6.

[39] Timothy Schoechle. *Energy management home gateway and interoperability standards*. GWAC. URL: http://www.smartgridnews.com/artman/uploads/1/Schoechle.pdf.

[40] Samuel Sciacca. *SCADA Innovation Begins Now*. URL: http://www.pennenergy.com/index/power/customer-service/display/6442709778/articles/utility-automation-engineering-td/volume-15/issue-9/features/scada-innovation-begins-now.html.

[41] Rai.tv Scienza. *Il controllo della rete elettrica italiana*. Apr. 2010. URL: http://www.youtube.com/watch?v=HDJb-RzTxR8.

[42] NIST National Institute of Standards & Technology. *Framework and Roadmap for Smart Grid Interoperability Standards,Release 1.0*. URL: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[43] NIST National Institute of Standards & Technology. *Guidelines for Smart Grid Cyber Security Vol.1*. Ago. 2010.

[44] NIST National Institute of Standards & Technology. *Guidelines for Smart Grid Cyber Security Vol.2*. Ago. 2010.

[45] Jon Stromsather. "Enel's experience on smart grids and solutions for large scale integration of renewables renewables". In: *Metering International magazine* (2010).

[46] Symantec. *W32.Stuxnet Dossier*. Nov. 2010. URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[47] Terna. *Chi siamo*. URL: http://www.terna.it/default/Home/AZIENDA/chi_siamo.aspx.

[48] Terna. *Dati Statistici sull'energia elettrica in Italia, Dati generali*. 2009. URL: http://www.terna.it/LinkClick.aspx?fileticket=VwAE%2bmEq1B4%3d&tabid=418&mid=2501.

[49] IEEE Smart Grid website. *Smart Grid Conceptual Framework*. URL: http://smartgrid.ieee.org/nist-smartgrid-framework.

[50] Wikipedia. *Global Carbon Emission*. URL: http://commons.wikimedia.org/wiki/File:Global_Carbon_Emissions.svg.

[51] Wikipedia. *Lista delle centrali elettriche presenti in Italia*. URL: http://it.wikipedia.org/wiki/Lista_delle_centrali_elettriche_presenti_in_Italia.

[52] Wikipedia. *Mesh networking*. URL: http://en.wikipedia.org/wiki/Mesh_networking.

[53] Wikipedia. *Power line communication*. URL: http://en.wikipedia.org/wiki/Power_line_communication.

[54] Wikipedia. *World Energy consumption*. URL: http://commons.wikimedia.org/wiki/File:World_Energy_consumption.png.