UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA
DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA
DELLE TELECOMUNICAZIONI

TESI DI LAUREA

Smart Grid: Sistemi di Controllo, Sistemi di Sicurezza e Mercato dell'Energia

Relatore: Tomaso Erseghe
Laureando: Marco Migliorini 436408/TC

19 aprile 2012

Indice

1 La Rete Attuale **5**

2 Smart Grid: Definizione **9**
2.1 Smart Grid 9
2.2 Caratteristiche Smart Grid 10
2.3 Definizione di Smart Grid 12
2.4 Architettura Smart Grid e Smart Metering 14
2.5 Attività di Normalizzazione e Standard Europei 18
2.6 Standardizzazione Europea 19
2.7 Comitati di Standardizzazione Tecnica 20

3 Sistemi di Controllo e Sicurezza **22**
3.1 Introduzione al concetto di Sicurezza nelle Smart Grid 22
3.2 Cyber Sicurezza Fisica 24
3.3 Privacy 26
3.4 Integrazione Sicura 29

4 SCADA **31**
4.1 Introduzione ai Sistemi SCADA 31
4.2 Definizione del Sistema SCADA 32
4.3 Funzioni del sistema SCADA 33
4.4 Il Processo Controllato 34

5 Sistemi di Sicurezza **38**
5.1 Minacce ai Sistemi SCADA 39
5.2 Precedenti Attacchi 41

5.3 Sistemi di Sicurezza 42
5.3.1 Firewall Principali Proprietà 42
5.3.2 Definizione di Firewall 43
5.3.3 Perchè usare un Firewall 44
5.4 Architetture di Rete 46
5.4.1 Firewall a due porte 46
5.4.2 Architettura Router e Firewall 47
5.4.3 Firewall con Zona Demilitarizzata 48
5.4.4 Coppia di Firewall di cui uno collegato alla Rete Aziendale e uno collegato alla Rete di Controllo 50
5.4.5 Combinazione di Firewall, Reti di Controllo PCN basate su V-LAN 51
5.5 Confronto tra le configurazioni e le loro Prestazioni 53
5.6 Politiche di Gestione del Firewall su Rete di Controllo PCN e Reti SCADA 54

6 Mercato dell' Energia **56**
6.1 Introdizione sul Mercato dell'Energia 56
6.2 La Formazione del Prezzo 57
6.3 Panoramica su alcuni Modelli per la Formazione del Prezzo . . 59
6.3.1 ARMA 60
6.3.2 SARIMA 61
6.3.3 ARMAX 62
6.3.4 GARCH 63
6.4 Investimenti Governativi 64

7 Politiche Energetiche **67**
7.1 La Politica Energetica americana di Barack Obama 67
7.2 Contesto Socio Economico e gli obbiettivi di Orizzonte 2020 69
7.2.1 PMI: Piccole e Medie Imprese 72
7.2.2 Il Ruolo della Cooperazione Internazionela 72
7.3 Europa 2020 73

Bibliografia **76**

... Ai miei Familiari

Ringraziamenti

Con questa giornata si chiude un'avventura durata molti anni e finalmente conclusa. Se oggi sono qui devo ringraziare molte persone, in particolare familiari e amici. Non mi metterò a fare l'elenco delle persone anche perchè non voglio dimenticare nessuno. Sicuramente ho fatto pochi inviti, e solamente alle poche persone che ritengo più care e vicine.

Un grazie particolare comunque lo devo a Mauro ed Alessandro per il sostegno che mi hanno dato nei 4 anni del dimagrimento, a Michela per avermi supportato e sopportato per 4 anni ed in fine il grazie più grande ai miei genitori che mi hanno sempre appoggiato in questi 33 anni.

Miglio

Capitolo 1

La Rete Attuale

I tumultuosi e veloci cambiamenti a livello mondiale degli ultimi anni hanno reso necessario un importante cambiamento anche in un mercato strategico sia per le società occidentali sia per le società in via di sviluppo: il mercato dell'energia. Questo fatto ha reso indispensabile ripensare molti aspetti delle strategie energetiche dei vari paesi tra cui la generazione e il trasporto dell'energia elettrica. Un ruolo fondamentale in questo tipo di cambiamento è giocato dalle SMART GRID. Le smart grid, letteralmente tradotto 'reti intelligenti', sono reti che dovrebbero realizzare e consentire un notevole cambiamento delle attuali reti energetiche sia dal lato della generazione che da quello dell'utente. Dal punto di vista della generazione dovranno cambiare le fonti e il modo di distribuire l'energia. Mentre dal punto di vista dell'utente dovrà cambiare il modo di consumare l'energia ricevuta, i tempi di consumo e contemporaneamente il consumatore può diventare un piccolo produttore che non solo assorbe ma anche immette energia in rete. Però prima di sviluppare il concetto di smart grid iniziamo dalla vecchia rete elettrica per capire da dove partiamo e di conseguenza dove andare a intervenire per realizzare il cambiamento che vogliamo ottenere.

Agli albori della distribuzione su larga scala dell'elettricità le centrali effettuavano una produzione di corrente elettrica in corrente continua e la consegna era fatta su brevi distanze e sempre alla tensione di produzione. Le centrali così concepite erano estremamente dispendiose e poco efficienti.

Per questa ragione si sono via via modificate le infrastrutture fino ad arrivare alle attuali centrali e linee di distriubuzione. Per quello che riguarda la generazione le sorgenti sono catalogate a seconda della fonte di energia che utilizzano, i principali tipi di centrale sono i seguenti:

- Centrale Idroelettrica: impianto che trasforma l'energia dell'acqua di fiume o di uno sbarramento in energia elettrica;

- Centrale Termoelettrica: impianto che trasforma l'energia termica termica dei combustibili fossili in energia elettrica;
- Centrale Eolica: impianto che trasforma l'energia del vento in energia elettrica;
- Impianti da Fonti Rinnovabili: sono impianti che ricavano elergia elettrica da fonti rinnovabili quali impianti fotovoltaici, impianti geotermici o a biomasse. Questi ultimi tipi di sorgenti sono le meno diffuse, ma la loro diffusione è un elemento determinante in quello che saranno sia le smart grid sia in quella che sarà la sfida di una produzione energetica sostenibile.

Per quello che riguarda le reti di distribuzione dell'energia la struttura tipica è di questo tipo:

- Linee elettriche di trasmissione ad Altissima Tensione (AAT) e ad Alta Tensione (AT): portano tensione dai 380 kV ai 220 kV e servono per il trasporto dell'energia elettrica su grandi distanze. I vantaggi portati da linee di questo tipo sono tre: il primo è la maggior efficienza nella trasmissione dell'energia dato che l'energia dissipata per effetto Joule è direttamente proporzionale al quadrato dell'intensità di corrente. Di conseguenza raddoppiando la tensione le perdite per effetto Joule si riducono ad un quarto. La seconda ragione per cui si usano linee di questo tipo è che occorre un minor numero di istallazioni per coprire un ampio territorio e quindi si ha una minore compromissione del territorio. Infine questo tipo di reti realizzano un'economia di scala, cioè all'aumentare della dimensione del sito di produzione si riduce il costo dell' unità di energia.
- Stazioni di Trasformazione AAT/AT o Stazioni Primarie (380/132 kV).
- Linee elettriche di distribuzione ad Alta Tensione (AT: 132-50 kV).
- Stazione di trasformazione AT/MT (132-50/15 kV) o Cabine Primarie (CP).
- Linee elettriche di distribuzione a Media Tensione (MT: 15 kV).
- Cabine di trasformazione MT/BT (15 kV/380-220 V) o Cabine Secondarie (CS).
- Linee elettriche di distribuzione a Bassa Tensione (BT: 380-220 V).

Quindi l'energia viene prodotta e poi distribuita dalla sorgente al consumatore passando dalle grandi dorsali ad alta tensione fino all'utenza casalinga a bassa tensione. Malgrado questo tipo di architettura di rete abbia ben servito nel secolo scorso, il cambiamento del mercato dell'energia negli ultimi anni ha messo in luce le seguenti criticità e inefficienze di questo tipo di modello:

1. Modello Unidirezionale e Passivo: in questa struttura di rete l'utente finale partecipa solo ed esclusivamente sotto forma di carico passivo ma non partecipa in alcun modo né alla gestione dei flussi di energia né alla generazione. Dunque il flusso di energia è unidirezionale dalla sorgente all' utente.

2. Elevate perdite per effetto Joule: l'infrastruttura appena descritta è costosa per le enormi perdite di energia dissipata nella trasmissione dalla sorgente all'utente finale. Tutto questo pesa sui costi di produzione dell'energia e quindi incide sul costo finale pagato dall'utente.

3. Impossibilità di gestire efficacemente i flussi di energia in modo da convogliarla dove è più necessaria. Questo è dovuto alla mancanza di protocolli per la gestione dinamica dei flussi.

4. Difficoltà ad integrare del sistema fonti di energia rinnovabili come eolico o fotovoltaico.

5. Tempi di risposta molto lunghi nel caso di black-out su grandi dimensioni e quindi l'impossibilità di limitare le cadute di tensione e le interruzioni di servizio conseguente con i relativi disagi per l'utenza.

Questa è una panoramica su quella che è la generazione e la trasmissione dell'energia ad oggi; seguita da un'analisi di quelli che sono i principali limiti e vulnerabilità di questo tipo di rete elettrica, e proprio per superare questi limiti stanno iniziando a prendere piede le smart grid che ora vado a introdurre.

Qui di seguito riporto in Figura 1.1 l'attuale rete elettrica.

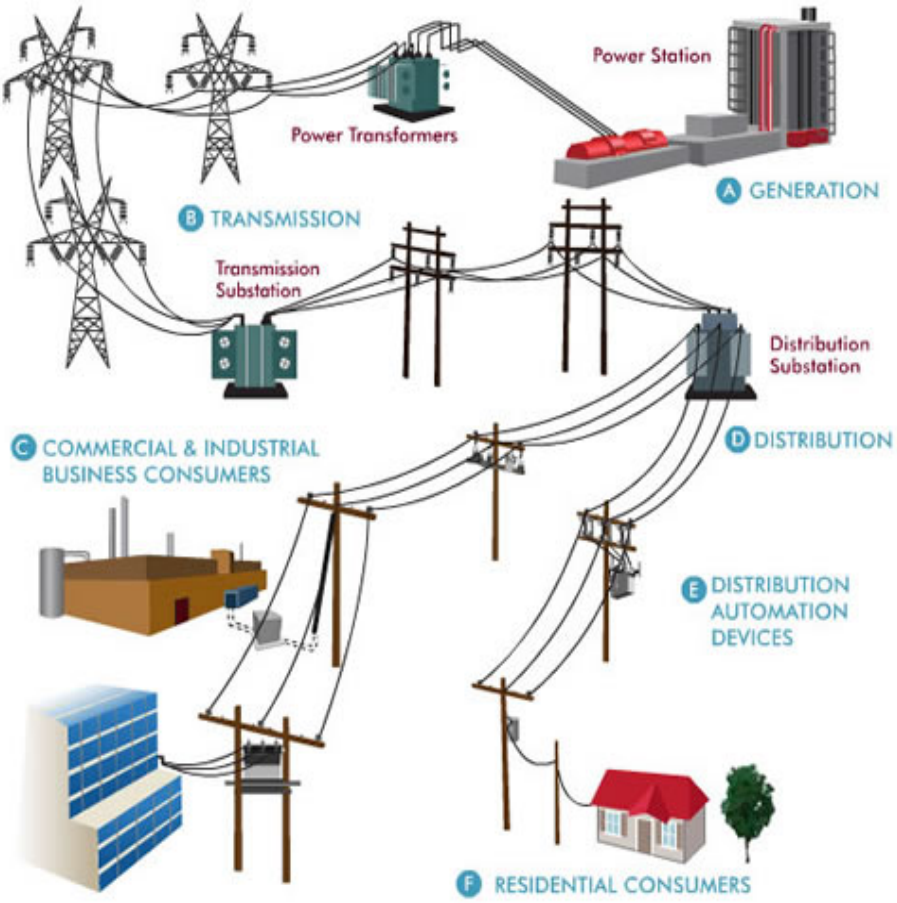

Figura 1.1: L'attuale rete elettrica.

Capitolo 2

Smart Grid: Definizione

2.1 Smart Grid

I limiti e le vulnerabilità dell'attuale rete elettrica impongono un cambiamento sia nella generazione sia nella distribuzione dell'energia.

Uno dei motivi per cui Smart Grid stanno prendendo piede è la motivazione ambientale. L'attuale sistema di generazione dell'energia è basato su energia derivante da fonti fossili prodotta in grandi impianti attorno ai quali si sviluppano le reti di distribuzione. Questo tipo di centrali sono altamente inquinanti per cui diventa necessario cercare di non utilizzare questo tipo di fonte e sostituirla con energie rinnovabili anche per aderire al cosiddetto 'Piano 20-20-20'. Il PIANO 20-20-20 è un pacchetto di norme clima-energia approvato dal Parlamento Europeo e sottoscritto anche dal Parlamento Italiano nel quale si prevede di raggiungere entro il 2020 i seguenti obiettivi:

- Ridurre del 20% le emissioni dei gas serra.
- Aumentare fino al 20% la quota di energia consumata prodotta da fonti rinnovabili.
- Portare al 20% il risparmio energetico.

La disattivazione totale o parziale delle centrali a combustibile fossile richiede la sostituzione di questa fonte con altre fonti di energia: le energie rinnovabili. La grande sfida che si sta cercando di vincere attraverso le Smart Grid è quella di arrivare a soddisfare la richiesta media giornaliera di energia con fonti rinnovabili non inquinanti e utilizzare le vecchie centrali termoelettriche solo per far fronte a picchi di energia come quello mostrato in Figura 2.1 e Figura 2.2.

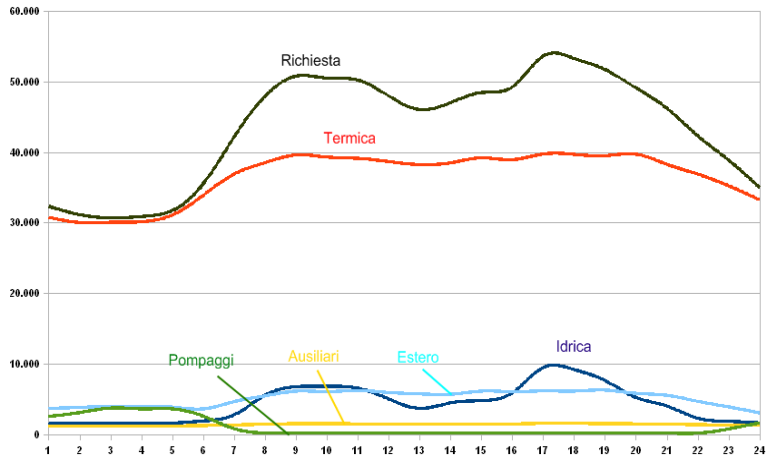

Figura 2.1: Andamento della richiesta giornaliera di energia scomposta nelle varie fonti.

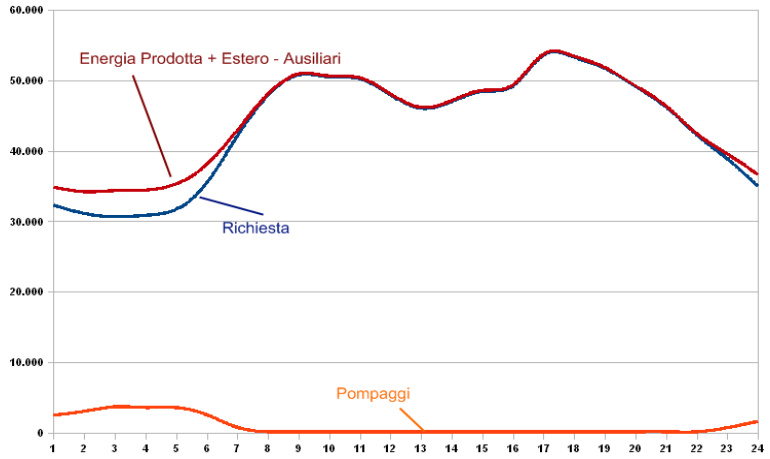

Figura 2.2: Andamento della richiesta giornaliera di energia con tutte le fonti aggregate meno i pompaggi.

2.2 Caratteristiche Smart Grid

Le principali caratteristiche che le reti Smart Grid devono avere sono le seguenti:

- Reti Intelligenti: per rete intelligente si intende il fatto che nelle Smart Grid la comunicazione ed il trasferimento dell'enrgia non sono più soltanto unidirezionali, ma al contrario saranno bidirezionali realizzando un vero e proprio scambio di informazioni real-time tra l'utility che fornisce l'energia e il consumatore finale. Per realizzare un'architettu-

ra di rete di questo tipo diventano indispensabili dispositivi come gli Smart Metering Communications. Questi sono dispositivi di controllo automatizzati per la gestione in tempo reale della domanda di energia e dell'eventuale produzione domestica.

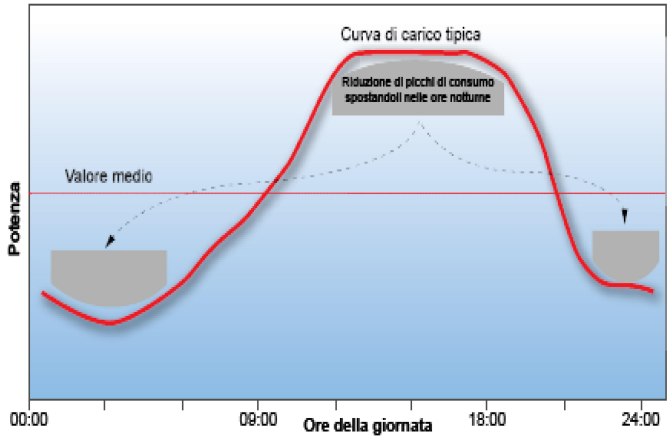

Figura 2.3: Profilo di carico giornaliero tipico per i consumi di energia elettrica.

Quindi l'utente non è più solamente un carico remoto che riceve energia. Grazie a questo tipo di dispositivi l'azienda fornitrice di energia può inviare informazione relative ai consumi agli utenti. Un esempio di questo concetto può essere fatto riferendoci alla Figura 2.3; se l'utility fornisce all'utente i dati relativi al suo consumo e ai costi dell'energia nelle varie fasce orarie durante il giorno, questo consente all'utente di spostare il proprio consumo energetico in altri momenti della giornata più economici. Questo porta ad un triplice risultato positivo:

1. l'utente ha la possibilità di organizzare i propri consumi scegliendo di consumare in fasce fuori picco quando l'energia costa molto meno, quindi un notevole risparmio per l'utente.
2. per l'utility che fornisce l'energia perchè più la domanda si sposta fuori dal picco di consumo e meno l'azienda deve ricorrere all' attivazioni di centrali termoelettriche per soddisfare la domanda, quindi un risparmio per l'azienda produttrice di energia.
3. per l'ambiente perchè meno si ricorre a a centrali termotecniche, minore sarà l'emissione di gas serra e maggiore sarà la percentuale di energia rinnovabile prodotta, quindi maggiore sarà la penetrazione delle energie rinnovabili sul mercato, e più vicino il raggiungimento degli obbiettivi del PIANO 20-20-20.

- Reti Aperte: per rete aperta si intende che la rete accetta energia da qualsiasi sorgente integrando perfettamente tutti i tipi di generazione. Quindi la rete deve essere in grado di gestire flussi energetici importanti che arrivano da centrali termoelettriche o nucleare e allo stesso tempo flussi molto più modesti che arrivano da piccoli impianti solari residenziali.

- Reti Capaci di Autodiagnosi: all' interno delle Smart Grid è possibile, attraverso dispositivi con capacità di calcolo, fare diagnosi in tempo reali per determinare eventuali malfunzionamenti della rete e prevenire buchi o sovraccarichi di tensione (picchi). Una volta riscontrati questi problemi si avvieranno procedure per la soluzione del problema che si è rilevato.

- Reti Robuste: la rete, quando è possibile, deve essere in grado sempre più di saper fronteggiare eventuali attacchi da parte di hacker, disastri naturali o eventi accidentali. Eventi che possano interrompere il flusso di energia e quindi creare un notevole disagio ad un vasto numero di utenti oltre che per un forte danno per l'utility.

- Reti che Utilizzano Tecnologie Internet: spesso nelle Smart Grid i dispositivi usano protocolli internet per lo scambio di dati e per la sicurezza.

- Protocolli Comuni: la Comunità Europea attraverso il lavoro di diverse commissioni sta cercando di produrre standard e protocolli che consentono l'interoperabilità e la compatibilità di reti, dispositivi e i dati prodotti da tali dispositivi anche in paesi diversi della UE.

Ora, dopo aver visto le caratteristiche di funzionalità che sono richieste alle Smart Grid per migliorare la vecchia rete, cerchiami di dare una definizione di cosa è una Smart Grid.

2.3 Definizione di Smart Grid

Le svariate funzionalità richieste alle Smart Grid, molte delle quali sono ancora istanze da realizzare, hanno fatto si che in letteratura esistano molte definizioni di Smart Grid tra loro diverse. Riporto di seguito le definizioni di Smart Grid date dai più importanti organismi che si sono occupati di questa nuova tecnoligia:

- Una smart grid trasferisce energia elettrica da fornitori ai consumatori utilizzando una tecnologia digitale a due vie per controllare gli apparecchi al domicilio dei consumatori per risparmiare energia, ridurre i costi e aumentare l'affidabilità e la trasparenza. Tale rete elettrica moderna è promossa da molti governi come un modo di affrontare l'indipendenza energetica, il riscaldamento globale e le questioni di robustezza in emergenza. (Wikipedia)

- Reti elettriche che possono integrare in modo intelligente il comportamento e le azioni di tutti gli utenti ad esse collegati (i generatori, i consumatori e quelli che fanno entrambe le cose) al fine di fornire in modo efficiente, sostenibile, economico e sicuro le forniture di elettricità. (European Technology Platform SmartGrids).

- Una smart grid è essenzialmente una modernizzazione degli aspetti di trasmissione e distribuzione della rete elettrica. In termini di trasmissione, una rete intelligente rende più facile la fornitura di energia da fonti alternative come eolico e solare da impianti rurali verso i centri città. La distribuzione è importante tanto quanto le capacità di trasmissione nell'aggiornamento della nostra rete elettrica. Una smart grid fornisce energia elettrica utilizzando la tecnologia digitale che registra il consumo di energia con contatori intelligenti, speciali contatori elettrici che trasmettono immediatamente le informazioni di utilizzo di energia alle società elettriche tramite reti wireless. I contatori intelligenti consentono anche di tracciare il nostro uso di energia ora per ora su Internet e con programmi di terze parti per computer. (http://www.inhabitat.com/2009/04/30/energy-101-what-is-a-smart-grid/).

- La Smart Grid non è un oggetto, ma piuttosto una visione e per essere completa, tale visione deve essere espressa da varie prospettive i suoi valori, le sue caratteristiche, e le tappe per la sua realizzazione.

- Una rete elettrica completamente automatizzata che monitora e controlla ogni cliente e nodo, garantendo un flusso bidirezionale di energia elettrica e di informazioni tra la centrale elettrica e l'apparecchio, e tutti i punti in mezzo. La sua intelligenza distribuita, insieme con le comunicazioni a banda larga e i sistemi di controllo automatizzato, permette transazioni in tempo reale e interfacce senza soluzione di continuità tra le persone, edifici, impianti industriali, impianti di generazione e la rete elettrica. (Department of Energy Grid 2030).

- I molti significati di 'Smart Grid': una Smart Grid non è né un unico concetto chiaramente definito, né una singola tecnologia. Piuttosto è come un cestino contenente varie combinazioni di palle. Il contesto e l'interpretazione dipendono dall'utente. Carnegie Mellon University ha recentemente pubblicato un articolo che descrive tutte le varie palle tipiche di questo cestino metaforico. Alcune di esse rappresentano innovazioni che sono ancora in fase di sviluppo, mentre altre rappresentano tecnologie che sono già state applicate da anni. (Carnegie Mellon University).

- Che cosa significa intelligenza? La smart grid non fornisce solo energia ma anche informazioni e di intelligenza. L'intelligenza si manifesta in un migliore utilizzo di tecnologie e soluzioni per meglio pianificare e gestire le reti elettriche esistenti, per controllare in modo intelligente la produzione e per permettere nuovi servizi energetici e miglioramenti di efficienza energetica. (http://www.smartgrids.eu/?q=node/163).

Alla luce di tutte queste definizioni, date da alcune delle più importanti commissioni che si occupano di questa materia, si può dire che la definizione finale che raggruppa tutti i concetti fino ad ora illustrati sulle Smart Grid è la seguente:

'Una rete intelligente che consegna l'elettricità prodotta dalle sorgenti ai consumatori utilizzando tecnologie informatiche in modo tale da risparmiare energia, ridurre i costi di produzione, accrescere l'affidabilità e la trasparenza dei sistemi elettrici. Indirettamente questo contribuisce all'indipendenza energetica, alla riduzione del riscaldamento globale e ad aumentare la sicurezza'. Dunque, con il concetto di Smart Grid si aggiunge capacità di analisi, monitoraggio, controllo e comunicazione al sistema di distribuzione (e trasmissione) elettrico, affinché possa ottimizzare l'efficienza del sistema e contribuire al risparmio energetico.

2.4 Architettura Smart Grid e Smart Metering

Viste le principali funzionalità che sono richieste alle Smart Grid vediamo ora l'architettura che dovrebbe avere la rete per riuscire a soddisfare tutte le sfide cui è chiamata. Lo sviluppo di questo tipo di tecnologia richiede sforzi notevoli a vari livelli:

- Tecnologico: dovranno essere sviluppate tecnologie, dispositivi e brevetti sia da parte dei privati che investono in aziende produttrici di energia sia da parte dello stato con investimenti in ricerca.
- Legislativo: gli stati dovranno produrre normative che regolamento questo nuovo tipo di tecnologia andando a modificare un mercato molto importante in ogni paese: il mercato dell'energia.
- Direttive Tecniche: dovranno essere messi a punto standard attraverso Direttive UE che vanno a definire alcuni aspetti delle Smart Grid in modo che le infrastrutture e i formati relativi ai dati che viaggiano in rete siano compatibili tra tutti gli stati dell'Unione Europea.

Tutto questo sempre allo scopo di ottenere significativi risparmi di energia abbassando quanto più possibile la domanda di energia nelle ore di picco e quindi ridurre al minimo il ricorso a centrali termotecniche altamente inquinanti. Si stima che il risparmio annuo Europeo potrebbe variare tra i 65 e i 70 miliardi di euro. Tutto ciò dimostra che questa nuova tecnologia non porta vantaggi solo ambientali, o non deve essere rispettata solo per conformità alle nuove direttive, ma porta anche notevoli vantaggi economici per stati, imprese e consumatori.

Passo ora all'analisi della rete. Un sitema di misurazione e comunicazione intelligente è costituito dai seguenti componenti:

- Smart Metering o contatore intelligente
- HAN: Home Area Network
- Metering Gateway
- NAN: Neighborhood Area Network
- Data Concentrator (DC): concentratore di dati
- WAN: Wide Area Network
- Distribution Controller: centri di controllo centrali
- Utility

Lo Smart Metering (o Contatore Intelligente) è lo strumento principale nella realizzazione delle Smart Grid perchè questo dispositivo realizza la comunicazione dibirezionale. Come mostrato in Figura 2.4 i contatori intelligenti sono posizionati all'interno delle abitazioni e misurano i consumi:

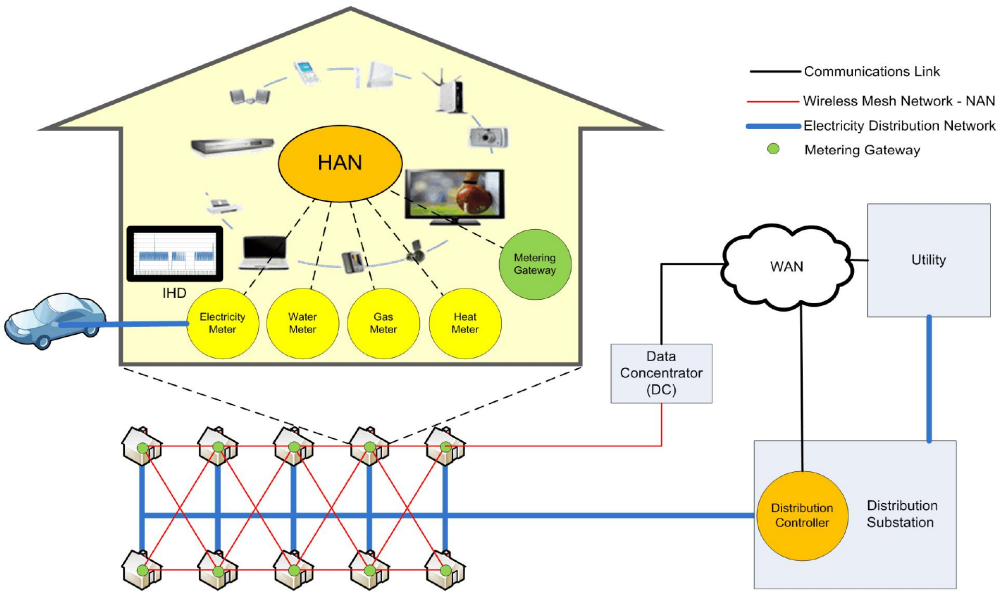

Figura 2.4: Architettura di una Rete Smart Grid.

elettricità, gas, acqua, calore. Tutti gli Smart Metering all'interno delle abitazioni sono collegati tra loro in una HAN (Home Area Network) e trasmettono i dati che raccolgono al Metering Gateway. Quest'ultimo dispositivo ha il compito di inoltrare i pacchetti di dati ricevuti dai vari contatori intelligenti alla NAN (Neighborhood Area Network). Le NAN raccolgono i dati provenienti da molteplici HANs per fornirli ad un Concentratore di Dati il quale organizzarà tutti i dati ricevuti in data base secondo standard di formattazione molto precisi. A questo punto le WAN (Wide Area Network) dovranno raccogliere i dati formattati dai concentratori di dati e redistribuirli o ai centri di controllo e analisi dei dati o alle Utility.

Durante il processo di normazione europea, è diventato evidente che un unico modello di formattazione dei dati è obbligatorio per migliorare l'interoperabilità e la compatibilità dei diversi metering e database. Uno di questi modelli che ha ricevuto molta attenzione è il dispositivo (DLMS / COSEM).

Da tutto questo risulta evidente che una caratteristica fondamentale delle Smart Grid è l'interconnessione di un numero potenzialmente elevato di reti, di utility, di smart metering e di consumatori che allo stesso tempo sono anche generatori di energia. Più tecnologie di comunicazione possono coesistere all'interno dello stesso sistema per cui diventano irrinunciabili degli stantard di comunicazione in modo che tutti i dispositivi possano comunicare tra loro indipendentemente dal mezzo fisico di comunicazione. Questa necessità è stata recentemente ribadita e sottolineata dal recente vertice UE M/441 su

Smart Meter.

La Tabella 2.1 mostra alcune delle tecnologia di trasmissione che sono utilizzati a seconda del tipo di rete e della vastità territoriale della rete.

Type of Network	*Range*	*Data Rate Requirements*	*Potential Technologies*
HAN	Tens of meters	Application dependant but generally low bit rate control information	ZigBee, Wi-Fi, Ethernet, PLC
NAN	Hundreds of meters	Depends on node density in the network (e.g. 2Kbps in the case of 500 meters sending 60 byte metering data every 2 minutes per NAN)	ZigBee, Wi-Fi, PLC, cellular
WAN	Tens of kilometers	High capability device such as a high speed router/switch (a few hundred Mbps to a few Gbps)	Ethernet, microwave, WiMax, 3G/LTE, fibre optic links

Tabella 2.1: Tabella delle tecnologie utilizzate a seconda del tipo e dell'estensione della rete.

Si può prevedere che in sistemi complessi come le Smart Grid le tecnologie di comunicazione utilizzate per soddisfare le diverse esigenze del sistema sono eterogenee. Di conseguenza, il principale obiettivo della standardizzazione dei dispositivi hardware e dei formati dei messaggi per le reti intelligenti è garantire l'interoperabilità e la compatibilità tra le diverse componenti del sistema (meterig, dispositivi o protocolli).

Il successo della distribuzione energetica attraverso contatori intelligenti e reti smart grid dipenderà in modo significativo dalla disponibilità di meccanismi aperti e standard che consentono a consumatori e fornitori di interoperare

e di interfacciarsi in un modo efficace al fine di risolvere i problemi per cui questa tecnologia è nata.

2.5 Attività di Normalizzazione e Standard Europei

Per realizzare una rete intelligente che sia in grado di soddisfare tutte le funzionalità e gli obiettivi prima elencati è necessario realizzare degli standard che assicurino interoperabililità, compatibilità, e affidabilità tra i diversi dispositivi comunicanti. Come detto il dispositivo fondamentale per realizzare le Smart Grid sono i contatori intelligenti che attaverso misure dettagliate da inviare alle utility riescono a reallizzare il collegamento bidirezionale efficace ad efficiente. Una rete Smart Grid avendo accesso in tempo reale alle informazioni sul flusso di energia consente una gestione più intelligente sia da parte del fornitore dell'energia sia da parte del consumatore. Inoltre la possibilità di un rilevamento in tempo reale del consumo consente il rilevamento di danni, guasti o addirittura furti di energia. Gli Smart Metering e le Smart Grid si stanno diffondendo in molte parti del mondo, ma le tecnologie adottate per la comunicazione dei dati saranno molto diverse a seconda dei fattori geografici, economici, politici e sociali. Sono molti gli stati, le aziende e i soggetti interessati a vario titolo a questa tecnologia, quindi diventa indispensabile l'intervento di un organo regolatore e legislatore che definisca con standard, direttive e norme per garantire l'integrazione di tutti i dispositivi in un unico sistema ben funzionante.

Nella direttiva 2009/72/CE del 13 luglio 2009, la Commissione europea ha deciso di istituire una task force sulle reti intelligenti che mirano a sviluppare una comune visione Europea delle smart grid e definire le questioni chiave che devono essere risolte. La task force è costituita da un comitato direttivo e da tre gruppi di esperti. Il comitato direttivo di alto livello comprende organismi di regolamentazione, sistemi di trasmissione (GST), gestori del sistema di distribuzione (GRD), Distribution Network Operators (DNOs) che lavorano congiuntamente per facilitare lo sviluppo delle smart grid e smart metering, e sostenere la realizzazione degli obiettivi del PIANO 20-20-20.

I tre gruppi di esperti sono i seguenti:

- Gruppo di Esperti 1: questo gruppo di esperti ha il compito di definire le funzionalità delle reti intelligenti, dei contatori intelligenti e a fronte dello stato attuale delle tecnologia quali servizi devono fornire queste componenti.

- Gruppo di Esperti 2: questo gruppo di esperti si occupa della sicurezza delle reti, della sicurezza dei dati e della loro gestione e protezione. Anche in questo campo è necessaria una standardizzazione per definire format e favorire la sicurezza informatica.

- Gruppo di Esperti 3: questo gruppo di esperti deve normare ruoli e responsabilità degli attori coinvolti nelle reti intelligenti

Lo sforzo della Comunità Europea è atto a creare un unico insieme di norme che dovrà essere attuato su tutti gli stati membri della UE recependo le direttive che il parlamento propurrà nei singoli sistemi legislativi nazionali.

2.6 Standardizzazione Europea

La lettura automatica e remota degli Smart Metering è una pratica consolidata a livello internazionale, tuttavia le funzionalità previste per i contatori intelligenti richiedono l'interfacciamento tra vari dispositivi e l'adozione di nuovi format per i dati. Per realizzare tutto questo è stato necessario razionalizzare e coordinare le attività di tutti i comitati tecnici che si occupano di standardizzazione. Per rispondere alla necessità di individuare standard per tutti gli aspetti delle Smart Grid la Commissione Europea ha dato mandato al comitato M/441 EN nel marzo del 2009.

Questo mandato è stato poi rivolto ai seguenti tre enti di normativi:

1. CEN (European Committee for Standardization).

2. CENELEC (Comitato Europeo di Normazione Elettrotecnica).

3. ETSI (European Telecommunications Standards Institute).

Nelle Figure 2.6 e 2.7 è possibile vedere i principali standard utilizzati nelle diverse tipologie di rete, attualmente le reti HAN sono basate sulla tecnologia di comunicazione 802.15.4 e ZigBee e in uscita prossimamente lo ZigBee 2.0.

	Connection between smart meters, devices, and displays	SM to SM-GW	HBES (home automation network device, control, server, external server)	HBES to SM or SM-GW interface
Application	ZigBee Smart Energy 1.0/2.0, proprietary data model	**CEN TC 294**: EN 13757-3 M-Bus, **CLC TC 13**: IEC 62056 COSEM	**CLC TC 205**: EN 50090-3	**CLC TC 205**: EN 50090-3, **CLC TC 13**: IEC 62056 COSEM
Network and transport	ZigBee 2.0, 6LoWPAN	ZigBee 2.0, 6LoWPAN	**CLC TC 205**: EN 50090-4	**CLC TC 205**: EN 50090-4
Link and physical media	ZigBee, PLC, 802.15.4, Bluetooth, Proprietary protocols	**CEN TC 294**: EN 13757-2 M-Bus wired, **CEN TC 294**: EN 13757-4 M-Bus wireless, **CLC TC 13**: IEC 62056-31, Euridis 2	**CLC TC 205**: EN 50090-4	**CLC TC 205**: EN 50090-4

Figura 2.5: Tabella standard di comunicazione per reti HAN.

	SM-GW to Data Concentrator	Concentrator to DCS	SM-GW to DCS
Application	**CLC TC 13**: IEC 62056 COSEM	SMTP, SFTP, Web Service, COSEM	**CLC TC 13**: IEC 62056 COSEM
Network and transport	TCP/IP	TCP/IP	TCP/IP
Link and physical media	**CLC TC 13 / IEC TC 57**: IEC 62056 COSEM, DLMS/COSEM over IEC 61334/S-FSK, PLC, GPRS and/or Ethernet/ADSL	GPRS/GSM, PLC G3, Fibre VLAN, Point to multi-point radio	**CLC TC 13 / IEC TC 57**: IEC 62056 COSEM, DLMS/COSEM over GPRS

Figura 2.6: Tabella standard di comunicazione per reti WAN.

2.7 Comitati di Standardizzazione Tecnica

La Comunità Europea ha previsto cinque diversi Comitati di Standardizzazione Tecnica che ora andrò ad elencare:

1. Smart Meters gruppo di coordinamento (SM-CG).
2. CENELEC TC 13 (Strumenti per la misurazione dell'energia elettrica e controllo del carico).
3. CEN TC 294 (Sistemi di comunicazione per Smart Metering e lettura remota dei contatori).
4. CENELEC TC 205 (Sistemi Home e Building Electronic).
5. ETSI M2M.

Capitolo 3

Sistemi di Controllo e Sicurezza

3.1 Introduzione al concetto di Sicurezza nelle Smart Grid

L'analisi e l'implementazione di sistemi di sicurezza nelle Smart Grid rappresenta una sfida, ma anche un importante compito e impegno per chi deve sviluppare questa tecnologia; soprattutto considerando l'entità dei potenziali danni che potrebbero essere causati da attacchi informatici. La protezione contro gli accessi indesiderati è un requisito indispensabile per poter controllare e utilizzare i dati che fluiscono all'interno del sistema. Questo perchè i dati per poter essere validi e utilizzabili devono prima di tutto essere attendibili e sicuri sia quando sono inviati dall'utente sia quando vengono inviati dal fornitore di energia. Rendere un sistema di questo tipo sicuro è un'operazione non banale per vari motivi: come prima causa l'enorme numero di reti e dispositivi diversi che un framework deve attraversare, ogni uno dei quali può usare standard e protocolli diversi. Un secondo motivo non meno importante è la regolamentazione degli accessi; infatti in ogni rete si può accedere secondo standard di sicurezza diversi, alcuni più rigidi e altri meno che potrebbero permettere l'intrusione di hacker.

Le Smart Grid hanno introdotto, rispetto alle reti precedenti, la comunicazione bidirezionale da cui deriva l'inevitabile necessità di proteggere i dati che consumatori e fornitori si scambiano; cosa che non accadeva nelle vecchie reti perchè la comunicazione era al massimo unidirezionale. Questa nuova funzionalità, la bidirezionalità nelle comunicazioni, può contribuire in modo decisivo a consentire:

- Riduzione del carico;

- Gestione dei Consumi;
- Accumulo di Energia per esempio nel ricarico di auto elettriche;
- Produzione Distribuita di Energia ad esempio attraverso le fonti rinnovabili.

Quindi la necessità di un più raffinato monitoraggio dei dati e di misurazioni intelligenti richiede inevitabilmente una avanzata struttura di controllo e di sicurezza sui dati misurati e trasmessi. Il successo della sfida della sicurezza nelle Smart Grid dipende molto dall' architettura del sistema.

Ad esempio consideriamo la struttura del sistema di misurazione nelle Figure 3.1 e 3.2:

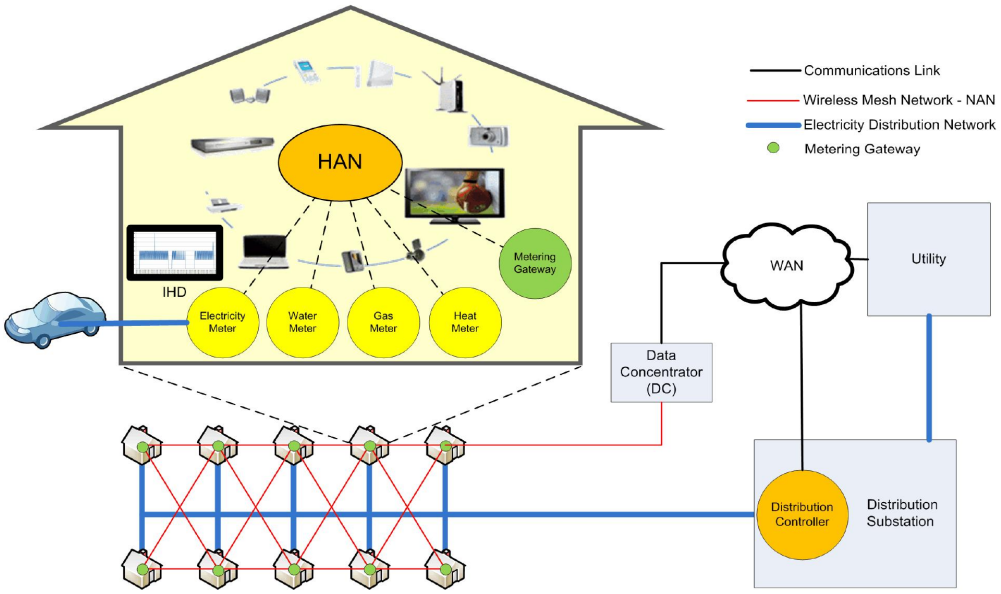

Figura 3.1: Architettura di una Rete Smart Grid.

L'attacco o la disfunzione della rete potrebbe avvenire per diverse cause:

- Avaria o guasti di qualche componente;
- Hackeraggio da un singolo punto;
- Hackeraggio da più punti di attacco.

La buona riuscita di un attacco potrebbe causare notevoli disagi ai clienti dell'area colpita dovuti all'interruzione del servizio elettrico. Per evitare la

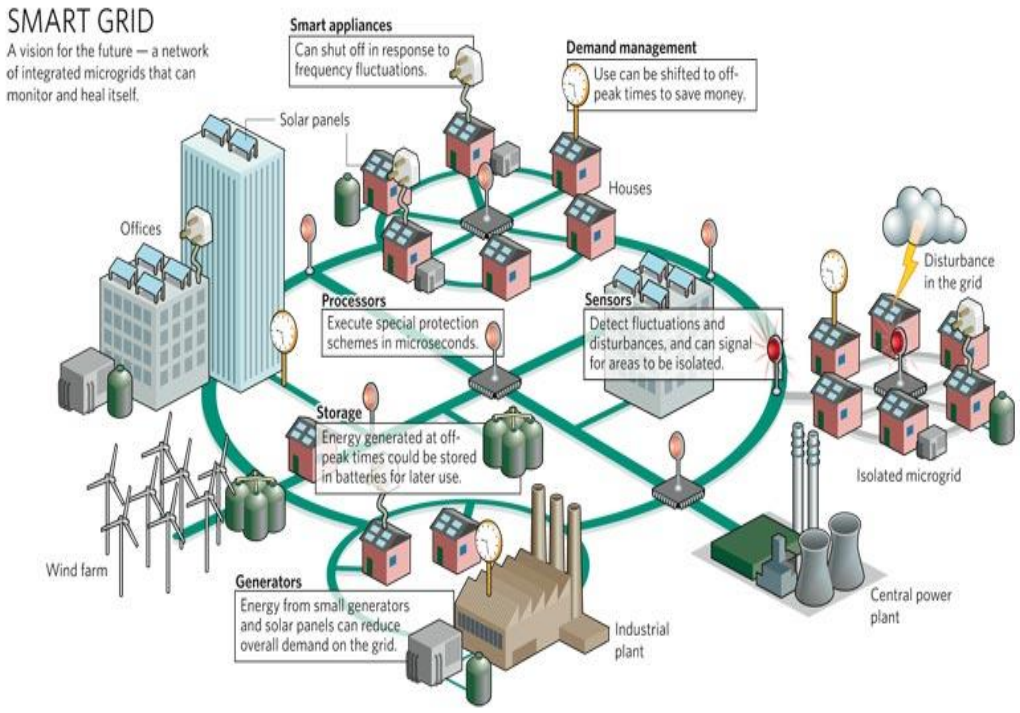

Figura 3.2: Architettura di una Rete Smart Grid.

buona riuscita di questi attacchi la strategia di sicurezza deve essere organizzata su più livelli in modo che anche nel caso peggiore in cui l'attacco vada a buon fine i danni che riesce a produrre siano minimi. Più in generale, nelle Smart Grid si possono individuare due diverse strategie per la sicurezza della rete:

1. Top-Down: si occupa di analizzare la sicurezza relativa agli scenari dell'utente e quindi la lettura automatizzata dei contatori e la fatturazione

2. Bottom-Up: questo aspetto si concentra su aspetti della sicurezza come l'integrità dei dispositivi, l' autenticazione e quindi l'autorizzazione ad un dispositivo ad entrare in rete, la gestione delle chiavi, e il rilevamento delle intrusioni.

3.2 Cyber Sicurezza Fisica

Le minacce informatiche sulle Smart Grid possono rappresentare potenzialmente un pericolo per la sicurezza nazionale, la stabilità economica del siste-

ma e anche alla sicurezza fisica. Le centrali elettriche e il sistema SCADA (Sistema di Controllo di Supervisione e Acquisizione Dati) sono i sistemi più presi di mira dagli hacker. Inoltre l'apertura delle reti energetiche a reti e protocolli IP per lo scambio dati introduce nuovi elementi di vulnerabilità del sistema. Ad esempio l'integrità dei dati e l'autenticazione sugli accessi può essere compromessa attraverso attacchi come Manin-Middle Spoofing o Denial of Service (DoS).

Se riuscissimo a proteggere la rete attacchi esterni, dobbiamo proteggerla anche da attacchi interni come sabotaggi o cavalli di Troia. Questo tipo di minaccia diventa significativamente pericoloso se si considera l'utilizzo di reti Internet per la trasmissione di dati relativi a reti energetiche.

Una volta che un attaccante (hacker) riesce a trovare un punto di accesso alla rete e quindi ad entrare, poi diventa molto più facile produrre un attacco a cascata lungo le reti intelligenti. Per esempio un attacco hacker sul canale per la trasmissione dei prezzi e consumi in tempo reale può permettere furti di energia o il controllo in remoto degli elettrodomestici. Quindi rigorosi sistemi di sicurezza sia hardware che software è necessaria per garantire la sicurezza delle Smart Grid.

Per esempio: se un utente riesce ad assumere una Head-End e quindi potrebbe essere in grado di inviare risposte come contatore intelligente, può chiedere con un comando l'interruzione dell'alimentazione. L'interruzione può essere fatta in modo temporaneo o permanente oppure attraverso opportuni comandi le chiavi crittografiche il cui nuovo valore è conosciuto solo dall'hacker che compie l'attacco. L'impatto di un simile attacco può essere potenzialmente enorme: milioni di case possono rimanere senza elettricità fino a quando non vengono ripristinate le chiavi crittografiche autentiche, i disagi delle persone possono essere enormi, potenzialmente anche la salute e la sicurezza potrebbe essere compromessa (pensiamo per esempio ai problemi che potrebbe causare un blackout in un'ospedale).

Oltre a questi aspetti già di per se molto importanti; ai potenziali danni dell'attacco vanno sommati anche i danni economici che questo può determinare: le imprese che forniscono il servizio possono subire danni di milioni di euro. Le Smart Grid devono quindi occuparsi della Cyber Sicurezza e garantire:

1. Prevenire gli attacchi;

2. Prevedere procedure di recupero: meccnismi di sopravvivenza o di gestione dell'emergenza in caso l'attacco vada a buon fine per riuscire comunque a limitarne i danni e garantire dei servizi minimi considerati irrinunciabili.

Tra le soluzione che sono state proposte sono un tasto di ripristino della chiave crittografica autentica nello Smart Metering; quindi una soluzione hardware che ha bisogno dell'intervento umano. Questa è una soluzione hardware, altre due soluzioni più complesse possono essere:

1. PKI (Public Key Infrastructure);
2. IBE (Identity Based Encryption).

In particolare IBE può essere molto interessante per le Smart Grid perchè é un sistema di accesso distribuito senza una configurazione precedente.

Questo permette una facile diffusione di dispositivi a bassa potenza come sensori, perchè possono inviare messaggi senza la necessità di contattare un server che gestisce chiavi d'accesso e autenticazione degli utenti.

Un perfetto sistema di sicurezza è costituito da livelli di controllo gerarchici; quindi un sistema centrale e sistemi di controllo periferici.

3.3 Privacy

La frequente raccolta di misurazioni e analisi dei dati può contribuire a migliorare l'efficienza energetica, come precedentemente discusso. I contatori intelligenti sono tenuti ad eseguire misurazioni precise e trasmettere i dati rilevati periodicamente o su richiesta precisa da parte della società che fornisce il servizio. Tuttavia, questo scambio di informazioni può andare a scapito della privacy dell'utente. Infatti le informazioni trasmesse dagli Smart Meter e raccolte nei data base delle utility possono essere utilizzati anche per scopi che esulano la sola efficienza energetica, crendo un problema di privacy nella gestione di questo tipo di infrastruttura. In particolare, i dati raccolti dai contatori intelligenti possono fornire molte informazioni su come l'utente utilizza gli apparecchi nella propria residenza; e quindi analizzando i dati sui consumi residenziali è possibile ricostruire per deduzione molte altre informazioni sulla vita, o sugli stili di vita dell'individuo utente. Per questo motivo l'uso di meccanismi di controllo degli accessi e di autenticazione degli utenti di fatto non è sufficiente a risolvere il problema privacy sulle Smart Grid.

Il problema della tutela della privacy degli utenti nelle Smart Grid è importante e la soluzione è difficile da trovare per tre ordini di motivi:

1. Il primo è che all'interno della rete i dati devono essere divulgati tra più dispositivi interessati a riceverli, e quindi gli stessi dati sono trasmessi, ricevuti, condivisi ed elaborati da molti utenti.

2. Il secondo è che la gamma e il dettaglio delle informazioni sullo stile di vita dell'utente che si possono dedurre dai sui consumi non è ancora chiaro.

3. Il terzo è che il concetto di privacy in una tecnologia in via di sviluppo come le Smart Grid non è ancora definito.

Attualmente il problema della privacy sulle Smart Grid è affrontato da NALM (Non Invasive Appliance Monitoring). Questo tipo di tecnologia di sorveglianza del carico consente di estrarre informazioni dettagliate sull'utilizzo degli elettrodomestici e quindi sullo stile di vita di chi li usa. Recenti risultati suggeriscono che anche quando i consumi all'interno di una casa risulano essere la sommatoria dei consumi di diversi utenti (diversi familiari o inquilini della casa) è comunque possibile scomporre i consumi dei potenziali utenti con elevata precisione. Questo è possibile anche perchè diversi elettrodomestici lasciano scie di consumo energetico diverso dalle quali è possibile risalire all'elettrodomestico usato. Esperti del settore sostengono di poter dimostrare che sia possibile attraverso sistemi di calcolo e algoritmi che analizzano i dati sui consumi individuare il consumo di un singolo elettrodomestico con un margine di errore inferiore al 10%. Un esempio di rilevamento degli singoli apparecchi partendo dalla curva di consumo di una casa è rappresentata nella Figura 3.3.

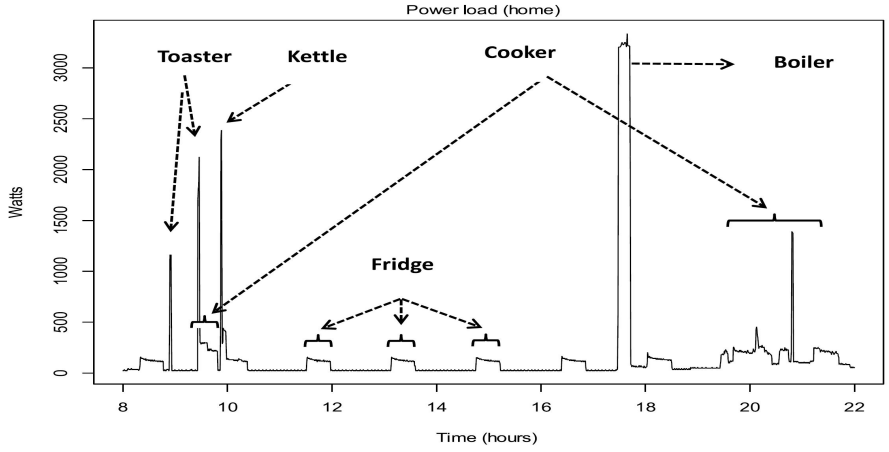

Figura 3.3: Analisi di Consumi Domestici.

L'accuratezza con la quale possono essere individuati gli elettrodomestici dipende molto dalla frequenza con la quale il contatore campiona la potenza consumata e generalmente si va da una lettura ogni minuto a una ogni 5 minuti. Come si vede dalla figura precedente; tali informazioni così dettagliate

sul consumo di energia possono mettere a nudo le abitudini quotidiane del consumo di energia di una famiglia e consentire di individuare i tipi di elettrodomestici usati. Da questo tipo di analisi è possibile ricavare tendenze di comportamento personali dei componenti della famiglia anche con frequenze di campionamento relativamente basse (ad esempio ogni 30 minuti). Da quanto esposto risulta chiaro che la privacy nelle Smart Grid è un problema di primaria importanza che deve essere risolto. Attualmente esistono due modi per proteggere della privacy:

1. Regolamentare per via normativa.

2. Per via tecnologica.

Le attuali attività di standardizzazione nel campo delle Smart Grid si stanno concentrando sullo sviluppo di norme per aiutare a proteggere la privacy dei clienti nelle reti intelligenti. A tale proposito negli USA la NIST ha riconosciuto che il vantaggio principale di ottenere abbondanti informazioni sui clienti in modo bidirezionale è anche un tallone d'Achille di questa tecnologia. Inoltre la NARUC (National Association of Utility Commissioners) ha elaborato una risoluzione la quale afferma che: 'le informazioni sui clienti fornite alle utility possono essere utilizzati per differenziare in servizi utili da quelli meno utili in modo che il tutto crei un valore aggiunto per il cliente'

In Europa, parallelamente all'America, la commissione Europea ha istituito una Task Force che si occupa di Smart Grid al fine di sviluppare una visione comune sulle questioni chieve che riguardano le reti intelligenti. Come risposta a questa esigenza sono stati istituiti tre Gruppi di Esperti (EG) uno di questi è il Gruppo di Esperti 2 (EG2) che punta ad identificare procedure di regolamentazione appropriate, scenari di sviluppo e raccomandazioni per la gestione dei dati e la sicurezza e la tutela dei consumatori. Una delle raccomandazioni di EG2 è quello di utilizzare servizi in anonimato per proteggere la privacy del cliente. Per esempio, i dati delle misurazioni effettuate dagli Smart Metering possono essere trasmessi su frequenze diverse per esempio sulla frequenza più bassa mentre i dati sulle fatturazioni in alta frequenza. In questo caso la sfida è riuscire a mantenere l'anonimato sui dati a frequenza più alta.

Comunque lo sviluppo di questo tipo di tecnologia è ancora all'inizio e anche il concetto di privacy su reti Smart Grid dovrà assere sviluppato ancora molto prima di avere una chiara definizione.

3.4 Integrazione Sicura

La sfida della sicurezza, oltre alla protezione dei dati personali, in senso più ampio riguarda le modalità di accesso alla rete intelligente; in particolare alla protezione da accessi non autorizzati e quindi il rifiuto della richiesta di accesso da dispositivi e Smart Meter non abilitati. Questo è un requisito importante in mancanza del quale i dati AMR non sono considerati attendibili sia dai fornitori del servizio sia dai consumatori.

I dati AMR sono i dati che viaggiano su strutture omonime. L'AMR (Advanced Multicenter Research) costituisce una infrastruttura tecnologica unica composta da diversi moduli applicativi perfettamente integrabili tra loro ma con gestione indipendente per consentire la massima flessibilità del sistema alle esigenze dello studio.

Per risolvere questo problema sono richieste soluzioni su più livelli come protocolli End-To-End di comunicazione sicura e per farlo devono essere utilizzate le seguenti cose:

- Componenti Hardware in grado di resistere ad attacchi fisici (ad esempio i contatori intelligenti).
- Una rete in grado di rilevare componenti mal funzionanti o potenziali hacker.
- Il Software del contatore intelligente deve essere privo di bug.

Si può ritenere che il problema della comunicazione AMI (Advanced Metering Infrastructure) possa essere risolto combinando protocolli già esistenti di crittografia a prova di manomissione, soluzioni Hardware e Software affidabili e solide contro gli attacchi, e con un'architettura di rete aperta sia all'ingresso di nuovi utenti ma anche aperta a nuovi test di sicurezza. Allo stesso tempo come descritto precedentemente è importante anche sviluppare i meccanismi di protezione contro attacchi provvenienti dall'interno della rete intelligente. L'uso di una rete intelligente con una struttura aperta richiede l'esistenza di un' interfaccia (gateway) che gestisce l'accesso di nuovi soggetti e dati di processo AMR.

Purtroppo, storicamente si è visto che le politiche sulla sicurezza dei dati e la legislazione sulla privacy, come è prevedibile non sono molto efficienti nel contrasto ad attacchi hacker, ma le tecniche e gli algoritmi per l'estrazione e lo sfruttamento di dati personali si evolvono molto rapidamente quando c'è un forte incentivo finanziario.

Quindi la sfida è quella di saper realizzare un giusto compromesso tra sicurezza e prestazioni, cioè gli algoritmi di sicurezza non devono essere pesanti

tanto da pregiudicare le prestazioni del sistema e, viceversa, non bisogna abbassare troppo il livello di sicurezza del sistema a favore delle prestazioni perchè altrimenti il sistema è esposto agli attacchi e a tutti i rischi potenziali precedentemente esposti. In futuro le reti Smart Grid dovranno integrare tra loro reti diverse, sistemi eterogenei e applicazioni Internet.

In definitiva dagli scenari sopra descritti risulta chiaro che l'integrazione di servizi da luogo a tutta una nuova gamma di vulnerabilità rispetto alla sicurezza. L'analisi dei rischi deve essere in grado di individuare anomalie nel sistema e adottare adeguate misure di risposta. Inoltre la condivisione tra più soggetti dei dati sui consumi energetici, posizione, le informazioni sullo stile di vita, e altre informazioni personali aumentano le potenziali minacce e danni. Infatti, la futura integrazione di sistemi e servizi in modo trasparente richiede meccanismi di protezione sicuri più che mai.

Capitolo 4

SCADA

4.1 Introduzione ai Sistemi SCADA

SCADA è un acronimo che sta per Supervisory Control And Data Acquisition, cioè Sistimi di Acquisizione di Dati per la Supervisione e il Controllo. Di fatto nel nome sono sintetizzate le funzioni principali che devono essere svolte dal sistema. Chiaramente delle tre attività svolte da questo tipo di sistemi l'acquisizione dati è predominante rispetto alle altre due, cioè alla funzione si supervisione e controllo. Senza una buona acquisizione di dati non sarebbe possibile realizzare una osservazione del processo controllato , e nemmeno una buona supervione, così come non sarebbe possibile realizzare un buon controllo. Quindi la possibilità di mettere in atto una serie di azioni tese a gestire o modificare l'evoluzione del processo controllato è possibile se e solo se si realizza una buona acquisizione dati.

Quanto detto fino ad ora non definisce i sistemi SCADA, sistemi che svolgono attività di questo tipo possono essere molti, quindi è necessario specificare quali sono le caratteristiche che differenziano questo sistema da altri sistemi con funzioni analoghe. Alcune di queste caratteristiche sono:

- Distribuzione Geografica.
- Distribuzione o Concentrazione dell' Intelligenza di Controllo.
- Grado di Interazione Uomo-Macchina: cioè il grado di interazione tra l' operatore che segue il sistema di controllo e il sistema stesso.
- Tempo di reazione ad un evento prodotto dal processo sotto controllo.

Sistemi di questo tipo sono largamente utilizzati nel controllo del traffico, nei sistemi di trasporto dei fluidi, di distribuzione dell'energia, nella

gestione delle linee di produzione che realizzano i sistemi industriali e del telerilevamento.

4.2 Definizione del Sistema SCADA

La definizione più comunemente usata per i sistemi SCADA corrisponde al significato esteso dell'acronimo perchè rappresenta molto chiaramente quali sono gli scopi e le funzioni di questo tipo si sitema. L'acronimo SCADA sta per Supervisory Control And Data Acquisition e altro non è che l'elencazioni delle tre funzioni principali di questo sistema: supervisione, controllo e acquisizione. In realtà la scrittura per esteso dell'acronimo non definisce i sistemi SCADA perchè esistono moltissimi altri sistemi e dispositivi che svolgono le stesse funzioni o solo alcune di esse. All'acronimo per essere completo manca il modo in cui queste funzioni vengono realizzate e a quale campo vengono applicate.

Per esempio: un sitema che svolge funzioni analoghe al sistema SCADA è il DCS acronimo di Distributed Control System. La differenza tra SCADA e DCS sta nella diversa distribuzione del sitema di controllo e di calcolo rispetto al sistema di acquisizione. Nello SCADA il sitema di acquisizione è composto da una rete di sensori sparsi nel territorio su vasta scala, mentre il sistema di elaborazione dei dati, quindi la parte che svolge le restanti due funzioni di supervisione e controllo, è concentrata in un unico sistema che elabora i dati raccolti dal sistema di acquisizione. Al contrario nei sitemi DCS le ditanze tra i dispositivi di acquisizione dei dati e la struttura di supervisione e controllo sono molto inferiori o addirittura nulle. Questo fa si che i dispositivi di acquisizione e le strutture di supervisione e controllo sono un tuttuno nella stessa macchina, quindi una struttura di acquisizione con elevata capacità di elaborazione; cioè acquisizione, supervisione e controllo sono fisicamente e tecnologicamente contigue. Per questa ragione nei sistemi DCS non si può parlare di un vero e proprio sistema di acquisizione, come nei sistemi SCADA, poichè consistono in veri e propri sistemi di elaborazione più o meno complessi ed in grado interpretare i dati osservati, eleborarli e prendere decisioni su come intervenire sui processi sotto controllo direttamente in loco. Quindi si può dire che i sistemi DCS sono sistemi centralizzati, mentre i sistemi SCADA sono sistemi a controllo distribuito, e in quanto tali offrono la possibilità di avere sistemi sempre più scalabili in termini di estensione. Con lo sviluppo delle tecnologie e dei sistemi di comunicazione dei dati è diventato possibile realizzare sistemi come lo SCADA che acquisiscono dati nei punti desiderati e li trasmettono ad un centro di calcolo centrale che li elabora. La scelta

di una soluzione o dell'altra dipende dal tipo si processo da monitorare, dai vantaggi e svantaggi che le due diverse architetture offrino caso per caso.

4.3 Funzioni del sistema SCADA

Vista la definizione del sistema SCADA e la distinzione col sistema DCS vediamo ora quali sono le tre funzioni che deve svolgere uno SCADA per essere tale:

1. Acquisizione Dati: delle tre funzioni l'acquisizione dati è la principale e un prerequisito per il funzionamento corretto delle altre due funzioni. L'acquisizone dei dati deve essere precisa, cioè i dati devono essere corretti e attendibili in modo che possano rappresentare fedelmente il processo che devono descrivere. In questo modo si pongono le basi per mettere in comunicazione lo SCADA col processo controllato, comunicazione che come precedentemente detto è necessariamente bidirezionale. Sulla base dei dati raccolti l'analisi del processo viene svolta a posteriori. Come visto l'acquisizione dati è talmente importante che rientra anche nella definizione di sistema SCADA per il semplice fatto che non è possibile realizzare la supervisione e il controllo senza l'acquisizione dello stato preciso in cui si trova il processo osservato. La funzione di acquisizione dati è considerata una funzione di scambio puro e semplice di informazioni tra la parte del sistema che realizza supervisione e controllo e il processo da osservare, quindi è completamente assente qualsiasi processo decisionale nel luogo di acquisizione. Come precedentemente detto quando questa condizione non è verificata allora il sistema non è più uno SCADA ma qualcosa di diverso, cioè una struttura ad intelligenza distribuita.

2. Supervisione: la supervisione è la funzione attraverso la quale il sitema SCADA rende possibile realizzare l'osservazione dello stato nel quale si trova un processo in un determinato istante. Campionamenti ripetuti e successivi del valore dello stato penmettono di valutare l'evoluzione del processo controllato. Rientrano in questa funzione anche compiti quali:

   (a) La visualizzazione dei dati acquisiti.

   (b) La gestione della successione dei campioni acquisiti, quindi della memoria del sistema.

   (c) Mettere in evidenza i campioni e gli stati che non rientrano in una normale gestione o evoluzione del sistema.

Questa funzione è una delle due finalità del modello SCADA ed è determinante nella sua implementazione; in quanto un sistema che non permette l'accesso, la visualizzazione delle informazioni acquisite; sia dei dati correnti sia della memoria (la storicità) del processo controllato non può essere definito sistema SCADA.

3. Controllo: questa funzione prevede che sia possibile orientare il comportamento del processo controllato; cioè influenzarne gli stati futuri cambiando i valori di alcuni parametri chiave. La funzione di controllo rappresenta quindi la capacità di un sistema di prendere decisioni relative all'evoluzione dello stato del processo, potendolo controllare con meccanismi di feed-back l'evoluzione del processo controllato stesso. L'architettura sia hardware che software del sistema di controllo devono essere stabilite caso per caso a seconda del processo da controllare. Le due funzioni precedenti sono tali per cui una acquisisce i dati e l'altra li gestisce, li immagazzina o ne gestisce la visualizzazione, quindi la funzine di controllo riceve dati grezzi, non elaborati. La funzione di controllo dovrà quindi eleborare i dati e prendere delle decisioni sugli interventi da fare o non fare sul processo monitorato. Una volta fatta la decisione dovrà sfruttare il sistema di acquisizione in senso inverso per andare a cambiare l'evoluzione del processo, andando a modificare i parametri chiave che determinano gli stati futuri.

4.4 Il Processo Controllato

Una volta definiti i sistemi SCADA bisogna dire che esistono molte tipologie di SCADA, tutte diverse a seconda del processo controllato. Il processo da controllare a seconda delle sue caratteristiche, della sua estensione, del luogo in cui si trova richiede sistemi SCADA molto diversi tra loro che dovranno essere progettati su misura per quel tipo di impianto e che probabilmente non saranno utilizzabili per monitorare nessun'altro tipo di processo che non sia analogo. Bisogna quindi andare a studiare le specifiche del processo da controllare perchè tali specifiche si tradurranno in vincoli precisi nella progettaione di un sistema di controllo SCADA specifico per quel processo.

Qui di seguito sono riportati alcuni parametri rispetto ai quali valutare il processo da monitorare. Catalogare i processi rispetto a questi elementi permette di dedurre i vincoli e le specifiche tecniche dei sistemi SCADA che poi li dovranno monitorare. Tali carateristiche conferiscono al sistema di controllo per quel processo elementi distintivi che lo rendono diverso rispetto ai

sistemi di controllo di tutti gli altri processi. I principali elementi qualificanti di un processo cono i seguenti:

1. Realtime: il termine realtime si riferisce alla capacità del sistema di reagire alle sollecitazioni del processo con ritardi trasgurabili rispetto alla dinamica evolutiva del processo medesimo. Contemporaneamente la realizzazione del sistema deve essere tale per cui i tempi di elaborazione siano compatibili con i tempi imposti dagli obbiettivi di controllo. La capacità di reazione del sistema di controllo è un requisito irrinunciabile, in mancanza del quale diventerebbe impossibile controllare il sistema influenzandone l'evoluzione entro tempi accettabili. La rapidità richiesta al sistema di controllo può essere frenata da diversi fattori:

   - Limiti imposti dalla tecnologia: questi dipendono dalla capacità e dalla potenza computazionale dei sistemi di calcolo, fattore che determina il tempo di risposta a fronte di una massa di dati da eleborare.
   - Dimensioni geografiche: chiaramente più i sistemi sono estesi e più i tempi di trasmissione dei dati, eleborazione e trasmissione della risposta si allungano.
   - Tecnologie di Trasmissione: a seconda della rete o del mezzo di trasmissione che utilizzo il tempo di trasmissione, eleborazione e restituzione del dato sarà diverso. I tempi di trasferimento dati per quanto migliorabili non sono mai annullabili per cui sono variabili di cui tenere sempre conto nella progettaione del sistema SCADA di controllo.

   Tutti questi fattori e i relativi tempi di ritardo sommati assieme danno quello che è il TEMPO DI REAZIONE di un processo ad un determinato evento.

2. Alta Affidabilità: oltre ai limiti imposti dalla tecnologia ci sono altri elementi in grado di limitare e condizionare l'efficace funzionamento di un sistema di controllo, tra cui l'affidabilità a la disponibilità. Per affidabilità si intende la RELIABILITY. Ogni sistema di controllo ed ogni sua parte può essere valutato rispetto al suo grado di affidabilità, cioè: il valore della probabilità di malfunzionamento espresso come percentuale del tempo di esercizio del componente medesimo. Essendo un sistema per definizione composto da vari elementi ciascuno dei cuali ha una sua affidabilità, l'affidabilità globale del sistema dipenderà quindi in modo determinante dall'affidabilità delle singole componenti, in particolare da quella dell'elemento meno affidabile. L'obbiettivo ultimo è

la realizzazione di un sistema con una percentuale di affidabilità del 100 per 100. La non completa affidabilità comunque non è detto che pregiudichi l'affidabilità del sistema.

Per esempio: se in un sistema il numero di campionamenti è molto alto tale che il rapporto tra l'intervallo di tempo tra un campione e l'altro e il tempo totale di osservazione è trascurabile. In questo caso la perdita di qualche dato o di qualche campione non mi pregiudica il funzionameto del sistema di controllo.

3. Alta Disponibilità: la disponibilità è l'altro parametro non tecnologico che influenza l'affidabilità del sistema di controllo. La definizione di disponibilità è la seguente: la percentuale di tempo per la quale deve essere garantito lo stato di esercizio del sistema, cioè il tempo complementare della percentuale di tempo in cui il sistema è rimasto fermo a causa di malfunzionamenti, manutenzioni o altro. La disponibilità può avere un peso diverso a seconda del processo produttivo che si sta monitorando.

   Per esempio in caso di processi produttivi dell'industria chimica, o di tutti i processi produttivi che trattano materiali pericolosi, possono degenerare e arrivare a stati molto pericolosi se il sistema non è sufficientemente monitorato con un sistema con un' adeguata disponibilità. Ci sono poi sistemi in qui questo parametro è meno incisivo.

4. Grado di Interazione Uomo-Macchina: in questo tipo di sistemi è sempre immancabile la presenza di un operatore da cui il rapporto di interazione uomo-macchina. In inglese sistemi di questo tipo sono detto HMI (Human-Machine Interface). Chiaramente l'iterazione può essere molto diversa da sistema a sistema. In alcuni casi l'uomo si può limitare al semplice monitoraggio in altri avere capacità di controllo e decisione molto maggiori; come sempre dipende dal processo da monitorare e dalle esigenze che da questo processo derivano.

5. Sistemi di Dimensioni Geografiche: le dimensioni geografiche di un sistema SCADA sono determinate dalla dislocazione sul territorio dei sensori e dispositivi di acquisizione dati. La parte di supervisione e controllo che caratterizza l'intelligenza centrale non determinano la dimensione del sistema dovendo essere queste centralizzate in un centro di calcolo. Le dimensioni possono andare da quelle di un edificio a sistemi intercontinentali. Chiaramente più il sistema è grande più è complesso perchè oltre ai dispositivi di acquisizione e ai sistemi di ela-

borazione e controllo devono essere aggiunte e integrate infrastrutture di cominucazione dei dati.

Al sistema di comunicazione allo stesso modo sono richieste qualità come: elevata affidabilità, continuità di servizio e qualità del servizio. L'affidabilità del sistema di trasmissione dei dati va a inficiere o a migliorare l'affidabilità dell'intero sistema perchè dati corrotti o trasferiti non con la necessaria velocità vanno ad annullare la possibilità di supervisione e controllo efficace.

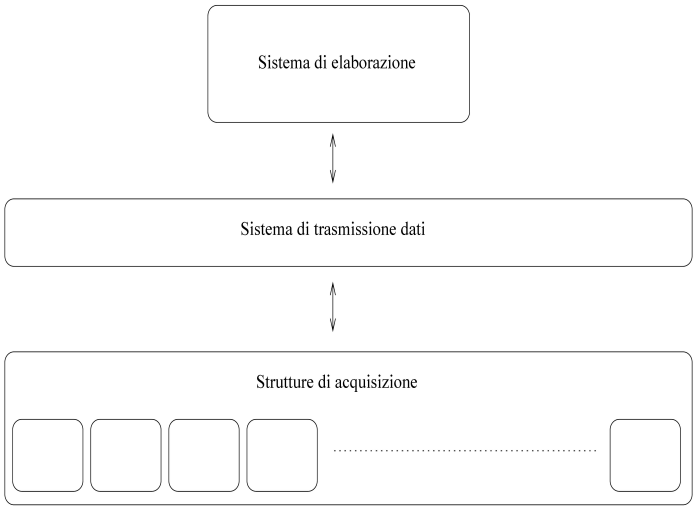

Figura 4.1: Architettura di un sistema SCADA.

Capitolo 5

Sistemi di Sicurezza

Negli ultimi anni la maggior parte dei sistemi di controllo come SCADA (Supervisory Control and Data Acquisition) e DCS (Distributed Control System) cioè sistemi di automazione e controllo utilizzano sempre più spesso tecnologie e prodotti tipici dell'IT (Information Technology) come Ethernet, il protocollo TCP, il protocollo IP, Windows, ecc... Fino a pochi anni fa questo tipo di tecnologie non era integrato con le altre reti e soprattutto con la rete globale (Internet), avevano reti e sistemi di trasmissione dedicati che creavano un isolamento che era la prima e più efficace arma di difesa di questi sistemi.

Un tempo le RTU (Remote Terminal Unit) distribuite sul territorio trasmettevano i loro dati su reti e sistemi di comunicazione dedicati e questo isolamento le metteva al riparo da hacker e da tutti i tipi di attacchi informatici che possono essere portati attraverso Internet. Il rapido cambiamento socio-economico e le diverse richieste da parte degli utenti hanno portato ad un cambiamento radicale di questo stato di cose; la situazione attuale è che questo tipo di sistemi sono stati integrati all'interno di reti informatiche aziendali e basati su software e canali commerciali. Questo nuovo stato di cose ha portato molti aspetti positivi tra cui un maggiore integrabilità dei sistemi. L'utilizzo di software, hardware e tecnologie di tipo commerciale che utilizzano protocolli da anni collaudati e perfettamente integrabili tra di loro, facilita notevolmente la diffusione e l'utilizzo di sistemi SCADA e DCS. Allo stasso tempo però, l'utilizzo di tecnologie protocolli e software commerciali e di Internet per la trasmissione dei dati ha reso questi sistemi vulnerabili a minacce alla sisurezza e alla privacy.

I sistemi SCADA sono applicati a reti energetiche, idriche, gasdotti, oleodotti e a molti altri sistemi di rilevanza nazionale. L'interdipendenza generata tra queste diverse infrastrutture può rendere i danni di un attacco hacker o di malfunzionamento molto più pesanti propagandosi da un'infrastruttura

all'altra o addirittura arrivando a colpire singoli utenti. Come precedentemente ricordato un blackout dei servizi può generare danni ingenti sia agli utenti che alle utility.

Importanti analisti ritengono che nel futuro la maggior parte delle azioni dolose e attentati terroristici potranno essere portati attraverso il cyberspace o via Internet. Vediamo di seguito alcune possibili minacce che possono essere portate a sistemi SCADA.

5.1 Minacce ai Sistemi SCADA

Le minacce che possono essere portate a sistemi SCADA o DCS dal cyberspace possono essere divise in tre categorie diverse, le stesse rappresentate nella Figura 5.1:

1. Azioni Mirate (Insider): hanno come obbiettivo quello di acquisire il controllo del sistema SCADA per ottenere che l'impianto si comporti secondo prefissate e improprie politiche secondo modalità anomale e non corrette. Questo può essere ottenuto rubando le password di accesso al sistema, sfruttando black-doors o altri buchi nel sistema di sicurezza.

   Altro sistema per boicottare il sitema SCADA è quello di inserirsi nelle comunicazioni tra il CORE-SCADA e le RTU inviando informazioni errate all'una o all'altra parte, questa tecnica prende il nome di SPOOFING. La granzezza e complessità di alcuni sistemi SCADA fa si che azioni di questo genere possano essere portati solo da un INSIDER, cioè da una persona che conoscono bene il sistema e l'impatto.

   I rimedi possibili contro questo tipo di attacchi possono essere una maggiore attenzione alle politiche di definizione aggiornamento e conservazione delle password ipotizzando anche possibili strumenti di indentificazione degl operatori con dati biometrici o smart card. Un'altra importante strategia che le utility possono mettere in atto è un controllo dei dipendenti, selezinarli e controllare i loro comportamenti e le loro intenzioni, soprattutto di coloro i quali possono accedere alle password o dati sensibili.

2. Azioni Broadcast (Virus): questo tipo di attacchi sfruttano i punti deboli comuni a molti utenti in modo da poter colpire una quantita numericamente molto grande di persone anche dal punto di vista dell'estensione territoriale.In questo tipo di attacco rientrano virus, hacker e worm. Lo worm slammer in particolare può essere utilizzato per scopi

subdoli come ad esempio utilizzare parte delle risorse del dispositivo nel quale entra (esempio potenza di calcolo o banda) per scopi diversi da quelli per cui è stato programmato, una vera e proprio distrazione di risorse. La sempre maggione interconnessione dei sistemi rende sempre più probabile la diffusione di queste azioni, che non sono potenzialmente dannose tanto quanto le precedenti, ma comunque pericolose e portatrici di forti disagi. Questo tipo di rischi oltre che potenzialmente meno pericolosi sono anche più facilmente arginabili attraverso firewall e anti-virus, non sempre sono sufficienti ma sono un livello minimo di protezione.

3. Azioni Indotte (CIIP): il nome deriva dal fatto che un malfunzionamento di un dispositivo a catena può provocare il malfunzionamento di altri dispositivi. Il livello di pericolosità anche in questo caso è inferiore del primo caso però i danni o i malfunzionamenti che a cascata un dispositivo che funziona in modo anomalo può provocare sono potenzialmente incalcolabili, soprattutto per gli utenti. L'interdipendenza tra i sistemi può essere la causa della diffusione della disfunzione tra i vari sistemi causando disfunzioni a catena. Chiaramente la natura imprevedibile di un evento di questo tipo non può consentire di predisporre sistemi automatizzati per bloccarne la diffusione. L'unica precauzine utile contro queste azioni e la riduzione dell'interdipendenza tra i sistemi, ma questa è di fatto irrealizzabile in quanto tutto porta ad una integrazione sempre maggiore.

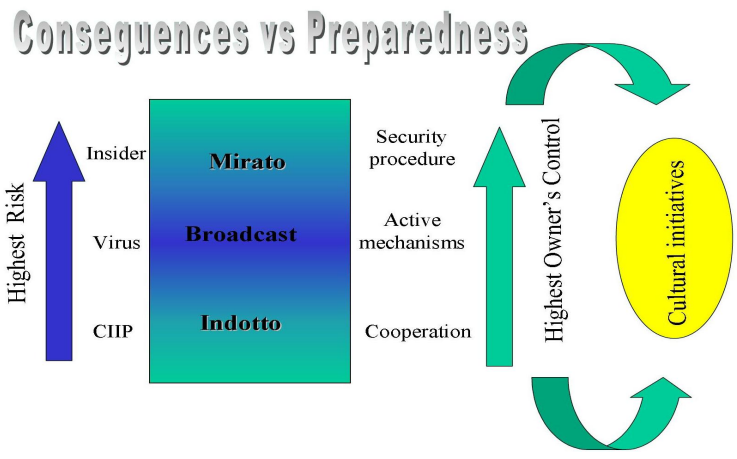

Figura 5.1: I tre principali tipi di minacce a SCADA dal cyberspace.

5.2 Precedenti Attacchi

Alla luce si quanto detto vediamo i principali attacchi hacker, disfunzioni o sabotaggi:

1. Nel 2000 a Maroochy Shire (Australia) un ex-dipendente riuscì ad introdursi nel sistema di tele-controllo di un impianto di depurazione provocando, da remoto, il riversamento di circa 1.200.000 litri di liquami non trattati direttamente nell'ambiente.

2. Nel 2001 un attacco hacker alla Cal-ISO, la principale società per il trasporto dell'energia elettrica in California, fu scoperto solo dopo 17 giorni. Non è stato possibile stabilire che tipo di informazioni siano state carpite durante questo periodo né quali erano i reali obiettivi dell'azione.

3. Nel 2003 il worm informatico Slammer, con la sua rapida diffusione, ha causato problemi a diversi sistemi di controllo. Negli USA il worm è riuscito a penetrare anche all'intero del sistema di controllo di una centrale nucleare in dismissione (senza creare seri problemi grazie alla presenza di circuiti di back-up in analogico). Esso è riuscito, inoltre ad interrompere il traffico dei sistemi di monitoraggio e controllo di due società di distribuzione dell'energia elettrica (in un caso penetrando all'interno del sistema informatico e nell'altro saturando la banda del canale ATM utilizzata, tramite una connessione Frame Relay, per colloquiare con le unità periferiche).

4. Sempre nel 2003 un rapporto intermedio della commissione congiunta US-Canada, istituita per far luce sulle cause del black-out del 14 agosto 2003, ha evidenziato che la causa scatenante va ricercata nel contatto fra un albero ed una linea a 345 kV. Tale evento, per altro relativamente usuale, è stato in una certa misura indotto e, soprattutto, non gestito correttamente a causa di una pluralità di problemi registrati dal sistema SCADA utilizzato per il monitoraggio e il controllo della rete elettrica da parte dell'operatore FirstEnergy. In particolare, si è riscontrato che lo 'stimatore' utilizzato per prevedere l'evoluzione della rete rimase non operativo per circa 4 ore riprendendo a funzionare solo pochi minuti prima del black-out (a causa sia di errori umani che di problemi tecnici). Un differente guasto ai server del sistema SCADA ha reso non operativa la gestione degli allarmi (cioè le segnalazioni agli operatori che determinate grandezze assumevano valori anomali) rallentando, inoltre, la funzionalità complessiva dello SCADA (ed in particolare le

operazioni di aggiornamento dei valori misurati sul campo) rendendo di fatto 'ciechi' gli operatori nella sala di controllo rispetto a quanto stava accadendo alle linee.

5. Nel 2004 il 3 maggio il worm Sasser, sfruttando una vulnerabilità del sistema Micorsoft Windows, riesce a penetrare diverse installazioni in tutto il mondo. In particolare, il sistema di gestione dell'aeroporto di Dubai risulta compromesso mandando in tilt il traffico aereo.

5.3 Sistemi di Sicurezza

Visti i danni che attacchi o malfunzionamenti possono causare a un numero grandissimo di utenti e utility con la potenzialità di mettere a rischio addirittura la sicurezza nazionale di qualche stato, cerchiamo di studiare uno degli strumenti di protezione più diffusi: il FIREWALL.

5.3.1 Firewall Principali Proprietà

Come precedentemente detto col passare del tempo, spinti da esigenze sia socio-economiche e da esigenze di integrabilità tra protocolli che altrimenti avrebbero isolato i sistemi, si sono via via utilizzati protocolli e standard software e hardware sempre più commerciali e diffusi. Se questo da un lato ha reso i sistemi più integrati dall'altro a favorito la diffusione di minacce come malware, hacker o veri e proprio cybercriminali con finalità terroristiche.

Una delle soluzioni ad oggi più utilizzate è quella di dividere i sistemi SCADA e PCN (Process Controll Network) per evitarne la connessione diretta a Internet e alla rete aziendale EN (Enterprise Network) con l'utilizzo di barriere come i FIREWALL. Attorno al firewall si possono strutturare architetture di rete diverse, ogniuna delle quali ha vantaggi, svantaggi e livelli di protezione diversi. In generale le architetture che danno i migliori risultati sono quelle che prevedono le DMZ (Demilitarized Zone - Zona Demilitarizzata) tra la rete aziendale EN e la rete di controllo PCN. La soluzione suggerita dagli esperti di Information Technology (IT) è quella di isolare la rete di controllo PCN dal resto della rete aziendale EN e da Internet attraverso un Firewall. Anche i Firewall però non sono la soluzione perfetta perchè a loro volta introduconoalcuni svantaggi:

- In primo luogo i Firewall sono prodotti consolidati per le normali reti, però non sono ancora del tutto collaudati per reti all'interno delle quali siano integrati sistemi SCADA; quindi la loro reale efficacia è ancora sotto valutazione.

- In secondo luogo posti all'interno della rete introducono inevitabilmente tempi di ritardo.
- I firewall potrebbero non essere in grado di gestire tutti i protocolli presenti all'interno delle varie reti connesse tra loro.
- Possono introdurre tempi di latenza che sono inaccettabili per applicazioni real-time.

Quindi una regola pratica da seguire sempre è quella di non collegare mai direttamente la rete degli uffici con la rete di controllo, è sempre meglio tenerle divise con un firewall.

5.3.2 Definizione di Firewall

La definizione di Firewall si basa sull'assunto che la rete è suddivisa in due schieramenti:

- gli appartenenti all'ente che amministra la rete i quali possono avere accesso alle risorse della rete di appartenenza senza particolari restrizioni e controlli;
- tutti i dispositivi che non fanno parte dell'ente che amministra la rete. Chi fa parte di questo secondo gruppo per accedere alle risorse della rete ha bisogno di autorizzazione all'accesso.

Questi controlli sono fatti al fine di impedire o quanto meno ridurre la possibilità di accedere alle risorse della rete da parte di persone non autorizzare o addirittura malintenzionate. In una rete di calcolatori, il firewall è un dispositivo che si occupa di:

- registrare il traffico entrante o uscente;
- scartare o instradare il traffico entrante e uscente.

Quindi il Firewall è una struttura hardware e software che separa una rete privata dal resto di Internet e consente all'amministratore di rete di controllare e gestire il flusso di traffico tra il mondo esterno e le risorse interne, stabilendo quali pacchetti lasciare transitare e quali bloccare. Di conseguenza un Firewall ha i seguenti tre obbiettivi:

1. Tutto il traffico che transita dall'esterno verso l'interno della rete e viceversa deve passare attraverso il Firewall. Volendo sarebbe possibile anche realizzare Firewall distribuiti o livelli multipli di Firewall. Rimane comunque preferibile collocare un solo Firewall in un solo punto d'accesso per rendere più semplice la politica di accesso alla rete.

2. Una volta definiti i criteri di accesso alla rete, solo il traffico autorizzato potrà avere accesso alla rete e alle sue risorse. Questo è possibile perchè tutto il traffico in entrata e in uscita alla rete deve passare per il Firewall che quindi può effettuare la selezione.

3. Occorre installare il Firewall correttamente altrimenti diventa inefficace ed è come non averlo a protezione della rete. Mentre se ben installato garantisce una immunità alla penetrazione di traffico non autorizzato.

I Firewall possono essere classificati in tre grandi categorie:

1. Filtri di pacchetti (Packet Filter).

2. Filtri con memoria dello stato (Stateful Filter).

3. Gateway a livello di applicazione (Application Level Gateway).

5.3.3 Perchè usare un Firewall

Come detto i sistemi SCADA, DCS e le Reti di Controllo (PCN) non sono più sistemi chiusi ed isolati accessibili solo a persone 'fidate' i cosiddetti trusted; cioè utenti o dispositivi autorizzati a vario titolo. La possibilità di accesso al sistema si è estesa ad accessi dall'esterno da parte di manutentori che si collegano in remoto al sistema, dipendenti che devono accedere ai dati. Questo come precedentemente detto espone il sistema ad ulteriori rischi di attacchi informatici che possono pregiudicare il corretto funzionamento della rete di controllo.

Lo scopo del Firewall è quindi quello di cercare di ridurre per quanto possibile i rischi connessi ad accessi non autorizzati alla rete di controllo PCN e a tutto il sistema SCADA in generale.

Qui di seguito sono elencati alcuni modi possibili con cui ridurre rischi in intrusioni non autorizzate:

1. Eliminare accessi diretti dalla rete aziendale o da internet alla rete di controllo e al centro decisionale del sistema SCADA.

2. Ridurre l'accesso alla rete di controllo solo a pochi ed autorizzati dipendenti dell'azienda.

3. Facilitare agli utenti autorizzati l'accesso alla rete di controllo e ai dati da essa prodotti, server Historian compresi.

4. Consentire accessi da parte di utenti esterni solo se muniti di autorizzazione (esempio: manutentori del sistema).

5. Stabilire connessioni sicure stando attenti ad esempio a dispositivi Wireless che potrebbero essere punti di accesso per non autorizzati.

6. Definire il traffico consentito sulla rete di controllo ed una volta definito monitorarlo per escludere pacchetti non autorizzati.

Tutte queste considerazioni possono essere condensate nella Figura 5.2 dove viene riportato uno studio dell'Università Carnegie Mellon a Pittsburgh in Pennsylvania. Tale ricerca evidenzia un sempre crescente numero di attacchi e intrusioni fino ad arrivare a 26000 nei primi tre mesi 2002, numero che supera gli attacchi totali di tutto l'anno 2000. Inoltre lo studio condotto da questa università dimostra che non solo il numero di attacchi sta aumentando in modo vertiginoso, ma nel contempo le conoscenze informatiche degli intruder decresce nel tempo. Questo aspetto che sembra paradossale in realtà può essere spiegato considerando che i tool e i programmi attraverso i quali vengono portati gli attacchi sono diventati sempre più potenti nel tempo. Questo fa si che azioni di sabotaggio che una volta avrebbero richiesto notevoli capacità da parte dell'hacker, oggi possono essere condotte da persone meno competenti perchè ci sono strumenti informatici che fanno questo al posto dell'hacker. Inoltre questi tool sono facilmente reperibili in Internet.

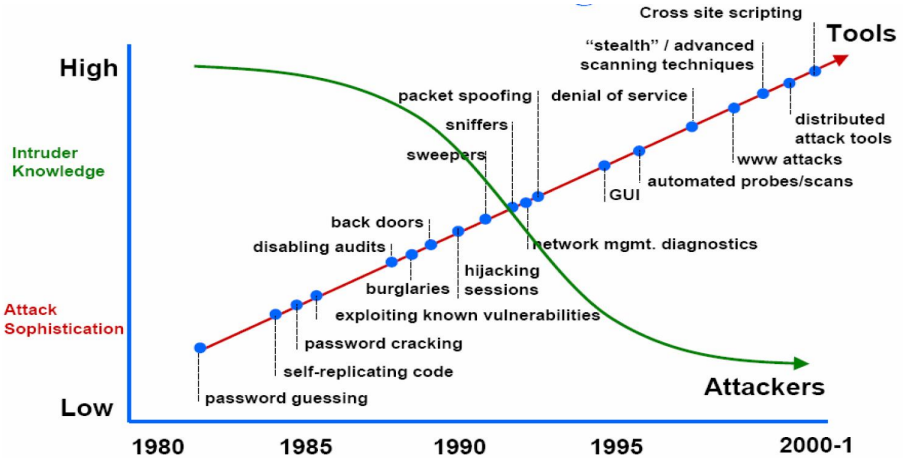

Figura 5.2: Evoluzione del grado di sofisticazione degli attacchi tramite il cyberspace (in rosso) e del livello di conoscenza richiesto agli assalitori (in verde).

5.4 Architetture di Rete

Andiamo ora a vedere alcune delle principali architetture di rete che consentono attraverso i Firewall l'isolamento delle reti di controllo dalle reti aziendali e da internet.

5.4.1 Firewall a due porte

Questo primo caso rappresenta l'architettura di rete più semplice ed è composta da una rete di controllo e una rete aziendale separate da un Firewall a due porte. Il Firewall può controllare tutti i pacchetti che lo attraversano con vari livelli di severtà, dal semplice livello TCP fino a messaggi applicativi di protocolli come FTP, HTTP, SMTP. Una volta che il Firewall è stato installato è possibile scegliere la profondità del controllo da esso effettuato, chiaramente più il controllo sarà rigido e minore sarà il successo di eventuali intrusi nel sistema. Con un Firewall configurato in modo da portare il controllo al massimo della severtità è possibile limitare di molto le probabilità di successo di un attacco.

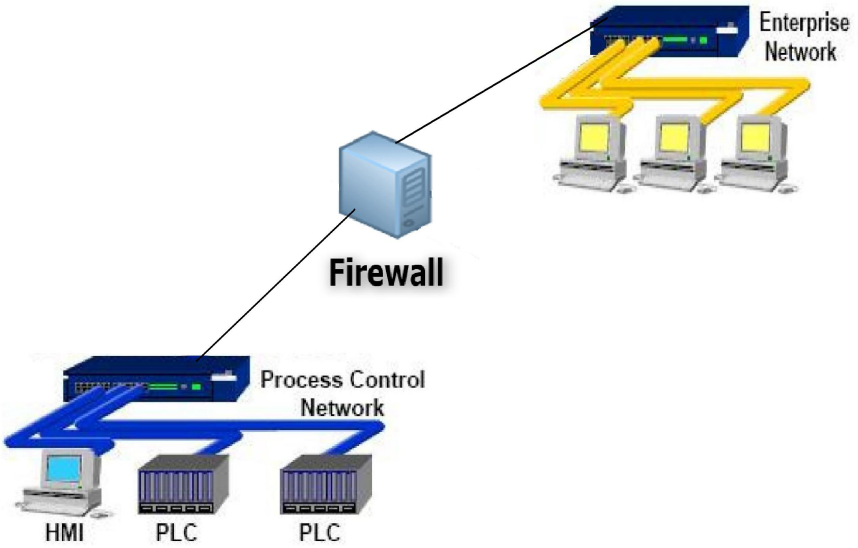

Figura 5.3: Separazione delle reti con architettura a Singolo Firewall.

Questa architettura di rete, mostrata in Figura 5.3, prevede che venga deciso a priori, cioè prima dell'istallazione, dove debbano essere posizionati i server come gli Historin, database server web o altri. Vediamone alcuni vantaggi e svantaggi:

- Se i server sono posizionati sul lato del firewall collegato con la rete aziendale ogni qualvolta che in server deve comunicare con un dispositivo della rete di controllo PCN protetta dal firewall dovrà passare attraverso quest'ultimo. Questo significa che il firewall dovrà essere configurato in modo da regolare il traffico di richieste che arrivano dalla rete aziendale e dai server verso i dispositivi di controllo (PLC e HMI). Regolamenterebbe l'accesso alla rete di controllo e filtrerebbe i pacchetti fermando quelli in arrivo da un host malevolo.

- Quel'ora i server, contrariamente alla configurazione precedente, fossero inclusi nella rete di controllo protetta dal firewall e non nella rete aziendale si dovranno fissare regole di accesso da parte della rete aziendale ai server e ai dispositivi di controllo. La differenza rispetto alla configurazione precedente sta nel fatto che nel primo caso un eventuale messaggio malware che superasse il firewall andrebbe ad intaccare un solo dispositivo di controllo. Nel secondo caso una volta superata la barriera del firewall il virus potrebbe estendersi a cascata anche ai server rendento l'attacco molto più pericoloso.

- Un altro modo per sabotare la rete di controllo potrebbe essere quello di entrare all'interno della rete di controllo con pacchetti progettati in modo tale da superare i filtri del firewall per poi dirottare i dati fuori dalla PCN utilizzando porte o protocolli di comunicazione, spesso HTTP, ritenuti sicuri e quindi non controllati dal firewall. A questo punto i pacchetti inviati dai dispositivi di controllo al di fuori della PCN potrebbero essere dirottati a destinazioni scorrette.

Questa architettura di rete con un firewall a due porte riduce la possibilità di attacco dall'esterno al sistema, realizza la divisione tra rete di controllo PCN e rete aziendale EN, però deve inevitabilmente lasciare dei canali di comunicazione aperti perchè le due reti che compongono lo stesso sitema possano scambiarsi dei dati per poter funzionale. Sfruttanto questi canali malware e hacker possono portare il loro attacco. Per cercare di limitare anche quest'ultimo tipo di intrusioni bisogna quindi controllare il corretto funzionamento dei dispositivi e del sistema una volta che questo è stato installato, proprio perchè malfunzionamenti potrebbero essere il segnale di intrusioni indesiderate.

5.4.2 Architettura Router e Firewall

L'architettura precedentemente vista è la più semplice, vediamo ora una seconda architettura che realizza la separazioni tra la rete di controllo PCN e

la rete aziendale EN utilizzando il firewall ma combinandolo con le funzionalità di un router. I router viene posizionato tra la rete internet esterna e il firewall in modo da effettuare un primo filtraggio dei pacchetti in ingresso al sistema SCADA da controllare. I pacchetti che superano questo primo filtraggio dovranno poi andare in ingresso al firewall e non direttamente nel sistema di controllo per un secondo filtraggio più complesso e accurato. Questa configurazione è spesso realizzata in sistemi che utilizzano molto internet per comunicare con l'esterno. Il router è in grado per sua natura di gestire grandi quantità di pacchetti in ingresso, eseguendo un primo filtraggio su possibili pacchetti con virus o malware ed alleggerendo il lavoro del firewall.

Questo tipo di configurazione, ha le seguenti peculiarità:

- Consente di prevenire attacchi dall'esterno in particolar modo attacchi di tipo DoS (Denial of Service).
- Come evidente dalla figura stessa le barriere da superare perchè l'attacco vada a buon fine sono due e non più una al contrario della configurazione precedente.
- Una prima scrematura dei pacchetti in ingresso permette un allegerimento del lavoro del firewall.
- Lo scopo principale di questo tipo di architettura è quello di separare il sistema SCADA dalla rete esterna internet più che separare la rete di controllo PCN e la rete aziendale EN. Se il ruoter venisse istallato dopo il firewall con lo scopo di separare la rete di controllo della rete aziendale verrebbe visto come un filtro aggiuntivo ma poco utile.

5.4.3 Firewall con Zona Demilitarizzata

Viste le prime due architetture, questa introduce un nuovo elemento le DMZ (Zone Demilitarizzate). Aggiungendo una o più zone demilitarizzate (DMZ) tra la rete di contrllo (PCN) e la rete aziendale (EN) è possibile ottenere un notevole miglioramento nelle prestazioni del sistema. Le Zone Demilitarizzate sono delle sottoreti in cui vengono collocate componenti 'critiche' per il buon funzionamento dello SCADA. All'interno di questa sottorete vengono collocati server Historian, i punti di accesso Wireless, database e server web. Strutturare la rete secondo questa architettura è possibile solo utilizzando firewall con a più porte. Il firewall divide la rete in sottoreti, isola alcuni settori in zone demilitarizzate (DMZ) che vengono anche chiamate Process Information Network (PIN). Come detto per realizzare una rete con questa struttura serve un firewall a più porte, dove le porte sono così distribuite:

- Su una porta c'è il collegamento verso l'esterno, quindi verso la rete internet.
- Su una porta per il collegamento verso la rete aziendale interna (EN).
- Una porta per collegare la rete di controllo (PCN) realizzando la separazione dalla rete aziendale.
- Sulle rimanenti porte si possono collegare tutte le sottoreti demilitarizzate (DMZ) con tutti i server, database e dispositivi critici per il buon funzionamento dello SCADA.

Nella Figura 5.4 è riportata l'architettura di rete descritta ora.

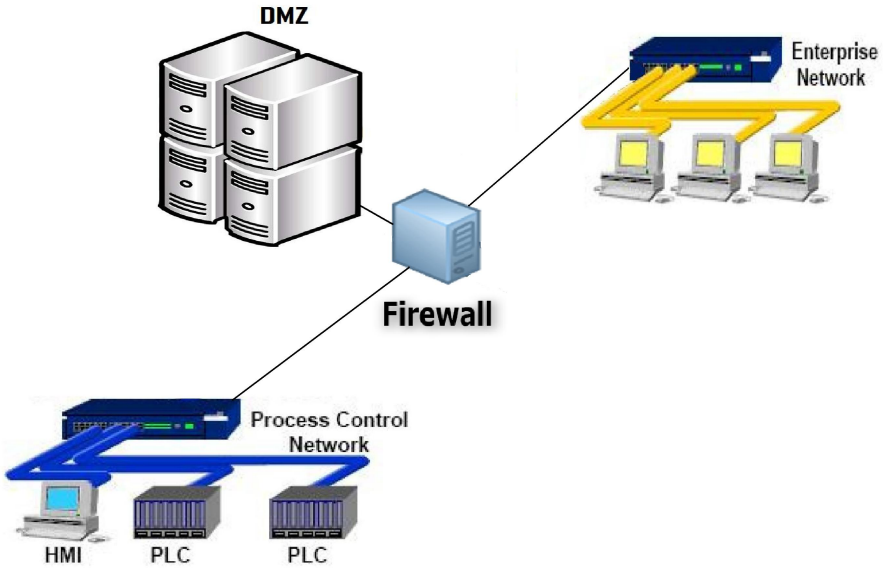

Figura 5.4: Architettura con separazione tra le reti affidata ad un Firewall e DMZ.

Lo scopo del firewall è quello di regolare il traffico tra le varie porte e quindi tra le varie sottoreti che a queste sono collegate, inoltre ponendo i principali dispositivi richiesti dalle reti aziendali nella zona demilitarizzata non è più necessario richiere l'accesso alla rete di controllo per accedere a questi dispositivi.

Le peculiarità di questa configurazione sono le seguenti:

- In una rete di questo tipo c'è un accesso facilitato, cioè un controllo meno rigido, tra la rete demilitarizzata e la rete di controllo. Per questo

motivo il rischio più grave in questa architettura è che se un un host della DMZ viene compromesso poi a cascata può portare l'attacco agli altri dispositivi della rete demilitarizzata e attraverso il collegamento del firewall attaccare anche la rete di controllo e i suoi dispositivi. Rendendo più stretti in controlli tra la zona demilitarizzata e la rete di controllo si possono ridurre i rischi anche se il rischio rimane.

- Una struttura come quella descritta è molto più complessa delle precedenti, e questo potrebbe rallentare le comunicazioni dei dati ed essere fonti di errori nella configurazione e nella gestione delle ACL (Access Control List), cioè l'elenco degli utenti registrati ed autorizzati ad accedere al sistema o solo ad alcune zone di questo. Quindi queste liste vanno compilate e aggiornate e sono fonte di errori.

- I firewall usati in questa configurazione sono più costosi, allo stesso tempo la sicurezza garantita da questa configurazione è buona, per cui la sua diffusione è ampia.

5.4.4 Coppia di Firewall di cui uno collegato alla Rete Aziendale e uno collegato alla Rete di Controllo

Un ulteriore passo avanti rispetto alla configurazione precedente (Firewall multiporta con zona DMZ tra rete di controllo PCN e rete aziendale EN) è l'utilizzo di una coppia di Firewall posizionati tra la rete aziendale EN e la rete di controllo PCN. I due Firewall creando di fatto una DMZ tra le due reti, dove vengono posizionati i server che saranno utilizzati in comune dagli utenti delle due reti. I computer in questa DMZ sono di solito i server che vengono chiamati PIN (Production o Process Information Network) o anche MES (Manufacturing Execution Systems).

Il firewall connesso con la rete aziendale ha lo scopo di filtrare i pacchetti che arrivano dalla rete aziendale e sono destinati o alla DMZ o alla PCN. Il firewall collegato con la rete di controllo evita che messaggi indesiderati o malware provvenienti dalla DMZ entrino nella rete di controllo.

Questa configurazione, mostrata in Figura 5.5, potrebbe anche permettere di assegnare a gestori diversi le diverse parti della rete che compongono il sistema SCADA. In questo modo ciascun gestore amministra il suo firewall e la sua sottorete. Questo permette anche di isolare meglio i compiti e le eventuali responsabilità in caso di malfunzionamento.

Le peculiarità di questo sistema sono le seguenti:

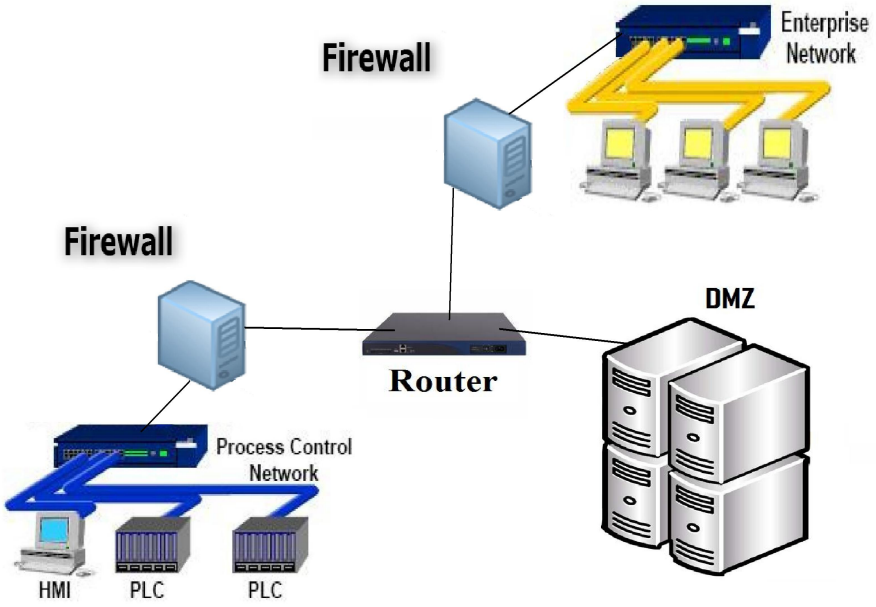

Figura 5.5: Coppia di Firewall di cui uno collegato alla Rete Aziendale e uno collegato alla Rete di Controllo.

- un'architettura così complessa è molto costosa, sia da gestire sia di installazione;
- la complessità di questo sistema però è anche uno dei suoi punti di forza permettendo livelli di sicurezza molto più elevati avendo più firewall che fanno da filtro ai messaggi;
- permettere di dividere la rete SCADA in sottoreti, affidare le varie sottoreti a gestori diversi e quindi rendere evidenti le responsabilità di gestione nel caso di malfunzionamenti.

5.4.5 Combinazione di Firewall, Reti di Controllo PCN basate su V-LAN

Fino a questo momento abbiamo sempre parlato di PCN, cioè di rete di controllo come se fossero un corpo unico, ma non è sempre così. In molte realtà aziendali la rete di controllo è a sua volta suddivisa in sottoreti ciascuna delle quali identifica diverse aree funzionali, impianti o sistemi all'interno dell'azienda. Ciascuna di queste sottoreti identifica un sistema di control-

lo che rappresenta un ramo, una parte, della rete di controllo complessiva. I dispositivi che fanno parte di questa sottorete mantengono comunque la possibilità di comunicare con i server di memorizzazione ed elaborazione dei dati, però non è più possibile avere una comunicazione tra dispositivi appartenenti a segmenti diversi della rete PCN a meno che la comunicazione non sia autorizzata.

Quindi la rete di controllo è stata suddivisa in sottoreti VLAN. Le sottoreti VLAN sono tutte connesse ad uno Switch, di conseguenza eventuali comunicazioni tra VLAN diverse devono essere autorizzate dallo Switch che farà da filtro e deciderà quali pacchetti possono entrare in una sottorete VLAN e quali no. Potendo controllare l'accesso a una sottorete lo switch può anche fermare eventuali messaggi non autorizzati, virus o malware. Chiaramente i dati e le comunicazioni non sono solo tra diverse VLAN della rete di controllo ma attraverso il firewall si può sempre comunicare anche con la rete aziendale e la zona demilitarizzata.

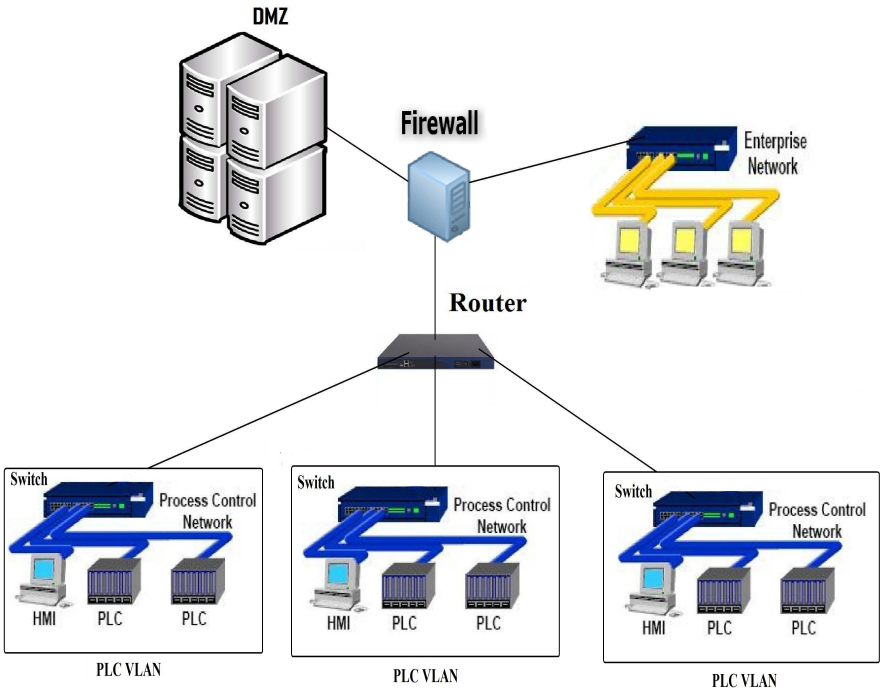

Figura 5.6: Combinazione di Firewall, Reti di Controllo PCN basate su V-LAN.

Le peculiarità di questa architettura, mostrata in Figura 5.6, sono le

seguenti:

- tra gli svantaggi di questa architettura ci sono sicuramente la sua complessità e il suo costo legato alla sua grande complessità. Il costo non dipende solo dal costo di acquisto e installazione delle componenti ma anche dai costi di manutenzione di un sistema che può diventare molto vasto e complesso in funzione anche di quanto esteso è il territorio o il processo da controllare.
- Questa configurazione viene ampiamente usata a livello industriale soprattutto in aziende dove è richiesto il monitoraggio di macchinari.
- Questo tipo di architettura è molto sicura potendo prevedere vari dispositivi che fanno da filtro tra la rete aziendale e la rete di controllo o una sua sottorete VLAN.

5.5 Confronto tra le configurazioni e le loro Prestazioni

Le configurazioni di queste reti sono tutte fatte allo scopo di dividere la rete di controllo (PCN) e la rete aziendale (EN). Esistono tre tipi possibili di architetture con cui ottenere il suddetto obbiettivo:

1. Separazione della rete di controllo (PCN) dalla rete aziendale (EN) senza utilizzare firewall. Questa architettura di rete è la più semplice e qui non è stata trattata.
2. Separazione della rete di controllo (PCN) dalla rete aziendale (EN) utilizzando firewall, senza la zona demilitarizzata (DMZ).
3. Separazione della rete di controllo (PCN) dalla rete aziendale (EN) utilizzando firewall e la costituzione di zone demilitarizzate (DMZ).

.

Nella Figura 5.7 vengono riassunte le architetture fino ad ora viste valutandole secondo i seguenti tre parametri:

1. Sicurezza.
2. Facilità di gestione.
3. Scalabilità.

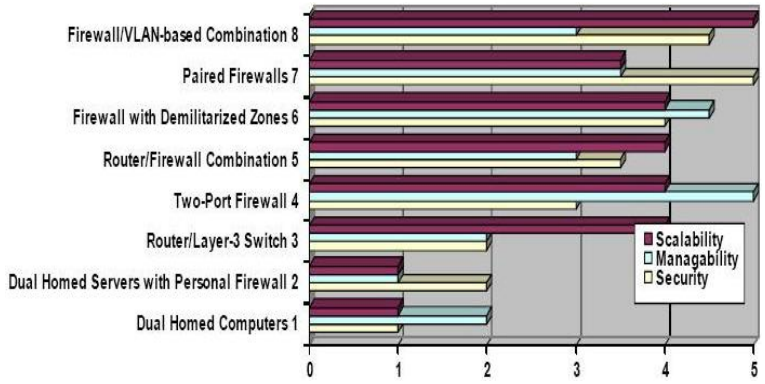

Figura 5.7: Confronto tra le configurazioni e le loro Prestazioni.

Ciascun parametro avrà una valutazione da 1 (il minimo) a 5 (il massimo).

In conclusione è possibile notare che le architetture che forniscono un sistema più sicuro sono quelle più complesse in cui la rete di controllo (PCN) e la rete aziendale (EN) sono separate da uno o più firewall e dove sono state installate una o più zone demilitarizzate (DMZ).

5.6 Politiche di Gestione del Firewall su Rete di Controllo PCN e Reti SCADA

Come visto nelle architetture precedentemente esposte il Firewall è una componente fondamentale per l'isolamento e la protezione della rete di controllo PCN. Il Firewall è una componente importante dal punto di vista della sicurezza ma anche dal punto di vista del costo; infatti una rete SCADA con rete di controllo PCN ha costi notevoli dal punto di vista della progettazione, dell'acquisto, dell'installazione e configurazione ed infine la manutenzione durante tutto il suo ciclo di vita. In molti casi vengono fatti investimenti importanti inizialmente che poi non vengono aggiornati nel corso del tempo col risultato di ritrovarsi con un sistema poco sicuro malgrado l'importante investimento. Vediamo alcune accortezze di cui preoccuparsi per garantire la sicurezza del sistema nel tempo:

1. Fare attenzione alla gestione della configurazione e della documentazione: come detto precedentemente una cattiva configurazione del firewall può condizione il funzionamento della rete,e di conseguenza anche il consumo energetico e la sicurezza del sistema e del processo da esso controllato. Diventa necessario nel corso del tempo aggiornare il si-

stema, gestire gli accessi alla rete, raccogliere e documentare tutte le varizioni fatte in modo di avere una storiografia dei cambiamenti, eseguire spesso il back-up del sistema in modo da avere gli ultimi parametri funzionanti in caso di problemi. Inoltre tenere aggiornati gli elenchi del virus e aggiornato l'antivirus in modo che il sistema sia sempre pronto a rilevare e isolare virus e malware.

2. Verificare periodicamente chi è autorizzato ad accedere al sistema ed eventuali tentativi di intrusione nel sistema.

3. Predisporre un Piano di Emergenza: pensare ad un piano di intervento in caso di incidenti o malfunzionamenti, così da avere una procedura precisa da seguire, con ruoli e responsabilità preassegnatee per ogni attore del sistema. Questo allo scopo di evitare azioni affrettate e spesso dannose in caso di situazioni inattese.

4. Il sistema una volta installato può garantire per molto tempo un ottimo livello di sicurezza senza la necessità di spendere altri soldi in dispositivi e software; solo aggiornandolo al meglio. Per fare questo è necessario avere un amministratore del sistema competende, preparato riguardo ai nuovi rischi e a come prevenirli. Quindi un altro grande contributo al funzionamento sicuro del sistema è dato da personale competente e da corsi di continuo aggiornamento del personale perchè sia sempre ben preparato.

Capitolo 6

Mercato dell' Energia

6.1 Introdizione sul Mercato dell'Energia

In questo ultimo capitolo cerco di analizzare quello che è il mercato dell'energia. Chiaramente la salvaguardia dell'ambiente, il rispetto dei trattati internazioneli, la riduzione dei gas serra sono tutti obbiettivi nobili; ma il lato economico ha il sopravvento in un settore strategico come quello energetico. Per questo motivo in questo capitolo andrò a descrivere quali sono i principali modelli attualmente utilizzati per il calcolo del prezzo dell'energia elettrica e quali sono le cifre in termini di investimenti che riguardano questo settore nei prossimi anni.

Fin dall'inizio degli anni '90 i prezzi non erano liberalizzati ed erano sottoposti a stretti controlli da parte delle commissioni governative dei vari paesi. In queste situazioni non c'era mercato e l'unica variabile era la domanda; il prezzo era fisso e non modificabile se non per via governativa in funzione dei costi di generazione e distribuzione. In una simile situazione l'incertezza era veramente piccola, proprio perchè i prezzi erano imposti. Dall'inizio degli anni '90 tutta questa situazione è cambiata e l'enegia iniziò a diventare un bene liberalizzato e quindi soggetto alle leggi di mercato. La liberalizzazione ha i seguanti obbiettivi primari:

1. promuovere l'efficienza in temini di guadagni,
2. stimolere innovazioni tecnologiche,
3. motivare investimenti efficienti.

Inevitabilmente ci fù una notevole variazione dei prezzi e del numero degli operatori. Come era prevedibile i vari fornitori iniziarono a competere nella produzione e distribuzione per acquisire sempre più clienti a discapito delle

ditte concorrenti. Questo ha portato una notevole scelta per il consumetore. Nel contempo ha fatto si che le variabili dalle quali dipendeva il prezzo finale dell'energia fossero molte di più rispetto al modello statalista; causando una volatilità notevole dei prezzi, superiore anche alla normale volatilità di altri mercati finanziari. Questa situazione ha reso indispensabile avere dei modelli per stimare la serie dei prezzi dell'energia al fine di proteggere sia in consumatori sia i produttori da questa volatilità dei prezzi. Il principale obbiettivo di questi modelli, che fanno previsioni, è quello di permettere un'analisi degli investimenti e la pianificazione dei guadagni o perdite che gli investimenti portano a lungo tempo. Mentre gli stessi modelli di previsione dei prezzi se applicati sul breve termine servono per determinare i prezzi nel breve periodo. In questa tesi vado ad analizzare i modelli di statistici di previsione dei prezzi perchè sono più precisi e accurati di altri e perchè sono modelli più adatti a descrivere fenomeni con caratteristiche di stagionalità come il mercato energetico.

6.2 La Formazione del Prezzo

Prima di partire ad analizzare il mercato dell'energia e i modelli di previsione dei prezzi vediamo quali sono le fasi della fornitura del servizio elettrico:

1. Generazione: consiste nella produzione di energia elettrica mediante la trasformazione di fonti primarie;

2. Dispacciamento: questa funzione serve a determinare quali centrali attivare e quali no per far fronte al fabbisogno energetico. Dato che l' energia non può essere immagazzinata bisogna fare uno studio per capire quali centrali attivare a seconda della domanda di energia elettrica;

3. Trasmissione: consiste nel trasporto dell'energia su grandi distanze;

4. Distribuzione: consiste nella distribuzione di energia fino all'utente finale, generalmente il bassa tensione;

5. Vendita: consiste nel fornire il prodotto energia all'utente finale in cambio del pagamento di un prezzo.

I prezzi dell'energia elettrica dipendono da moltissimi fattori ambientali, metereologici, oppure dalla stagione dell'anno. Qui di seguito vado a fare un elenco dei principali fattori che influenzano il valore di mercato del prezzo dell'energia:

- la temperatura dell'ambiente: la posizione geografica del luogo implica una temperatura media giornaliera che va ad incidere sul consumo di energia per raffreddamento i riscaldamento;
- la temperatura massima registrata quel giorno: esempio tipico, d'estate con in condizionatori accesi la domanda di energia da parte dell'utenza sale moltissimo;
- la temperatura minima registrata durante il giorno;
- l'ora del giorno;
- il giorno della settimana;
- la domanda del giorno prima;
- la stagione.

Prima di iniziare ad analizzare i modelli di determinazione dei prezzi vediamo le quattro caratteristiche tipiche dei prezzi dell'elettricità:

1. Stagionalità: la domanda di elettricità può essere influenzata dalle attività economiche, dalle condizioni climatiche e atmosferiche. Per esempio: nei paesi caldi c'è una maggiore domanda di energia per climatizzare gli edifici, questo causa una maggiore domanda e quindi un rincaro del prezzo. Esempi analoghi possono essere fatti per quanto riguarda intervalli di tempo giornalieri, settimanali, mensili o annuali.

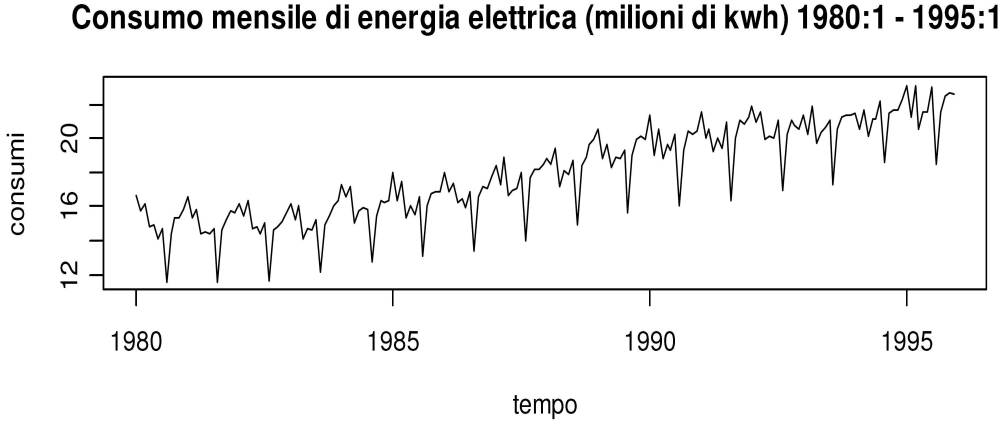

Figura 6.1: Consumo mensile di energia elettrica dal 1980 al 1995 e medie mensili.

Com'è possibile notare dalla Figura 6.1 il trend della richiesta di energia è crescente e questo può dipendere dallo sviluppo economico del paese, sviluppo che fa aumentare l'uso di energia elettrica e quindi del prezzo. La serie mostra la presenza di una connotazione stagionale nella domanda di energia.

2. Mean-Reversion: nei mercati la curva di domanda e di offerta si incrociano determinando il prezzo. Nel mercato dell'energia la domanda influisce sull'offerta. Maggiore è la domanda e maggiore sarà l'utilizzo di centrali che devono soddisfare alla domanda e quindi maggiore sarà il prezzo. Per questo il meccanismo dei prezzi è autoregressivo.

3. Volatilità: per volatilità si intende la dispersione rispetto al prezzo medio nel periodo di tempo assegnato. La volatilità dipende dai seguenti fattori:

   - la prima causa è la variazione della domanda collegata con l'impossibilità di immagazzinare energia;
   - carenza di produzione legata per esempio ad avarie nelle centrali di generazione;
   - condizioni climatiche impreviste che determinano una variazione della domanda di energia;
   - variabilità del prezzo dei combustibili;
   - leggi sui limiti delle emissioni;
   - congestione della rete;
   - le regole finanziarie e legislative che regolamentano il mercato.

4. Presenza di Jumps: sono movimenti repentini dei prezzi verso l'alto o verso il basso e sono facilmente visibili in un grafico. La caratteristica tipica dei jumps è l'istantaneità, cioè i prezzi ritornano molto rapidamente al livello precedente. Queste fluttuazioni di solito sono dovute a rapide variazioni del carico (dovute per esmpio a variazioni atmosferiche o problemi tecnici) e inducono improvvise vaziazioni del prezzo.

6.3 Panoramica su alcuni Modelli per la Formazione del Prezzo

Iniziamo la panoramica di alcuni dei più diffusi modelli stocastici attraverso i quali è possibile realizzare la previsione dei prezzi partendo da serie stori-

che. Prima di tutto vediamo la definizione del sistema ARMA generale, cioè non applicata e sistemi economici. ARMA è l'acronimo di Auto Regressive-Moving Average cioè modello autoregressivo a media mobile; è un modello lineare che fornisce istante per istante un valore di uscita basandosi sui precedenti valori di entrata e uscita. Un sistema di questo tipo può essere descritto dalla seguente equazione:

$$y(t)+\alpha_1 y(t-1)+...+\alpha_n y(t-n) = \beta_0 u(t)+\beta_1 u(t-1)+...+\beta_n u(t-n) \quad (6.1)$$

Questa equazione prefigura due tipi di sistemi diversi a seconda del valore di β_0:

- Se $\beta_0 \neq 0$ l'ingresso attuale u(t) influenza direttamente l'uscita y(t) e il sistema è detto *IMPROPRIO*.
- Se $\beta_0 = 0$ allora l'ingresso attuale non influenza l'uscita attuale y(t) e in sistema è detto *PROPRIO*.

L' equazione precedente può essere riscritta anche nella forma seguente:

$$y(t) = \sum_{i=1}^{n}(-\alpha_i)y(t-i) + \sum_{i=0}^{n}\beta_i u(t-i) \quad (6.2)$$

dove le due sommatorie hanno il seguente significato:

- $\sum_{i=1}^{n}(-\alpha_i)y(t-i) \Rightarrow$ *AUTOREGRESSIONE (AR = Auto Regressive)* ;
- $\sum_{i=0}^{n}\beta_i u(t-i) \Rightarrow$ *MEDIA MOBILE (MA = Moving Average)* .

6.3.1 ARMA

Nell'ingegneria il modello ARMA è quello più frequentemente utilizzato per descrivere modelli di natura casuale tenendo conto delle correlazioni temporali tra gli eventi passati del fenomeno osservato. ARMA sta per modello autoregressivo a media mobile, e si indica anche con la notazione ARMA(p,q) dove:

- P_t rappresenta il prezzo dell'energia all'istante t;
- p indica l'*Ordine della Componete Autoregressiva* cioè il numero di campioni passati del prezzo che contribuiscono alla determinazione del prezzo attuale P_t;

- q indica l'*Ordine della Componete a Media Mobile* cioè il numero di precedenti valori del rumore bianco.

L'equazione che descrive questo modello è la seguente:

$$\Phi(B)P_t = \Theta(B)\epsilon_t \tag{6.3}$$

in cui:

- B rappresenta l'operatore ritardo, cioè $BP_t = P_{t-1}$, $B^2P_t = P_{t-2}$ e in generale $B^kP_t = P_{t-k}$;
- Il polinomio $\Phi(B) = 1 - \Phi_1 B - ... - \Phi_p B^p$;
- Il polinomio $\Theta(B) = 1 + \Theta_1 B + ... + \Theta_q B^q$;
- $\Phi_1, ..., \Phi_p$ rappresentano i coefficienti del polinomio autoregressivo;
- $\Theta_1, ..., \Theta_q$ rappresentano i coefficienti del polinomio media mobile;
- ϵ_t è indipendente ed identicamente distribuito (iid) come un rumore bianco a media nulla e varianza finita, di solito nelle simulazioni si utilizza un rumore bianco gaussiano.

Nel caso q fosse nullo (q=0) otterremmo un *modello completamente autoregressivo* AR(p).

Il modello ARMA parte dall'assunto che la serie storica dei prezzi sia debolmente stazionaria. Se non lo fosse prima di applicare alla serie storica dei prezzi questo modello è necessario operare la trasformazione in serie stazionaria differenziando attraverso l'algoritmo di Box e Jenkins ottenendo un modello denominato ARIMA. Qualora la differenziazione fosse ottenuta con un ritardo maggiore di 1 allora il modello è noto come ARIMA STAGIONALE o SARIMA.

6.3.2 SARIMA

Il modello SARIMA ed è utile per descrivere andamenti periodici di tipo stagionale; e queste sono caratteristiche tipiche dell'andamento del prezzo dell'energia.

In questo modello matematico le equazioni contengono delle componenti stagionali che contribuiscono a descrivere il mercato. Una componente stagionale può essere indipendente dalle altre componenti non stagionali, oppure la componente stagionale può essere correlata con le componenti non

stagionali. Questo tipo di modello utilizzabile anche su sistemi non stazionari periodici ed è molto utile per stimare i prezzi orari giornalieri dell'energia elettrica. Un processo SARIMA può essere descritto attraverso la seguente equazione:

$$\phi(B)\Phi(B^S)(1-B)^d(1-B^S)^D P_t = \theta(B)\Theta(B^S)\epsilon_t \tag{6.4}$$

in cui i precedenti simboli hanno il seguente significato:

- S esprime il periodo di tempo della stagione che andiamo a descrivere con questo modello, cioè il numero di osservazioni che vengono fatte mediamente in un periodo;
- il polinomio $\phi(B) = (1 - \phi_1 B - \phi_2 B^2 - ... - \phi_p B^p)$ è *l'operatore autoregressivo non stagionale di ordine p stazionario*;
- il polinomio $\Phi(B^S) = (1 - \Phi_1 B^S - \Phi_2 B^{2S} - ... - \Phi_p B^{PS})$ è *l'operatore autoregressivo stagionale di ordine P stazionario*;
- il polinomio $\theta(B) = (1 + \theta_1 B + \theta_2 B^2 + ... + \theta_q B^q)$ è *l'operatore a media mobile non stagionale di ordine q invertibile*;
- il polinomio $\Theta(B^S) = (1 + \Theta_1 B^S + \Theta_2 B^{2S} + ... + \Theta_Q B^{QS})$ è *l'operatore a media mobile stagionale di ordine Q invertibile*;
- $\Delta^d = (1 - B)^d$ rappresenta *l'operatore differenza di ordine d non stagionale*;
- $\Delta_S^D = (1 - B^S)^D$ rappresenta *l'operatore differenza di ordine D stagionale*;
- $\epsilon_t \approx WN(0, \sigma^2)$ e rappresenta un rumore bianco gaussiano a media nulla e varianda finita.

Di conseguenza $P_t, P_{t-S}, P_{t-2S}, ...$ in teoria dovrebbero essere tutti valori simili e fortemente correlati tra loro rappresentando valori campionati con periodo pari a S intervalli di tempo su un processo periodico.

6.3.3 ARMAX

I modelli ARMA permettono di stimare il prezzo dell'energia partendo dalla serie storica che ne rappresenta il passato ma senza utilizzare altre informazioni. Nella realtà però il valore del prezzo non è determinato solo dalla propria serie storica dei prezzi, ma possono incidere anche altri parametri e

le loro serie storiche nella determinazione del prezzo. Un esempio di fattore esterno ai valori stagionali possono essere le condizioni atmosferiche ambientali. Le variabili che influenzano il prezzo ma che sono esterne alla serie storica dei prezzi sono dette *variabili esogene*. Il modello ARMAX è un modello autoregressivo a media mobile con variabili esogene e quindi è utilizzato perchè permette di mettere il relazione le serie storiche del prezzo con variabili al di fuori delle serie storiche stesse, esogene per l'appunto. Il modello ARMAX(p,q,$r_1, r_2, ..., r_k$) può essere ben descritto dalla seguente equazione:

$$\phi(B)P_t = \vartheta(B)\epsilon_t + \sum_{i=1}^{k} \Psi^i(B)\nu_t^i \tag{6.5}$$

in cui:

- i rappresenta l'ordine dei fattori esogeni $\nu^1, ..., \nu^k$ tra i quali temperatura o la disponibilità della centrale a fornire energia elettrica;
- $\Psi^i(B)$ può essere espresso attravarso la seguente espressione: $\Psi^i(B) = \Psi_0^i + \Psi_1^i B + ... + \Psi_{ri}^i B^{ri}$ in cui Ψ_j^i sono i coefficienti polinomiali.

Talvolta il modello ARMAX viene rappresentato attraverso la sua *funzione di trasferimento* nella quale è possibile esprimere il prezzo dell'energia al tempo t (P_t) in funzione di tutti i parametri appena elencati:

$$P_t = \frac{\vartheta(B)}{\phi(B)}\epsilon_t + \sum_{i=1}^{k} \Psi^i(B)\nu_t^i \tag{6.6}$$

I modelli di serie storiche con l'inclusione di variabili esogene vengono ampiamente utilizzati nelle previsioni del prezzo dell'energia a breve termine.

6.3.4 GARCH

I modelli ARMA sono detti *omoschedastici*, cioè con la medesima varianza. Ciò significa che in una rappresentazione grafica i dati sono dispersi omogeneamente al di sopra o al di sotto di una linea che ne rappresenta la media. I prezzi dell'energia elettrica seguono una dinamica non lineare perchè fortemente influenzati dalle serie passate.

L'inclusione della omoschedasticità in un modello matematico può essere realizzato utilizzando il modello di Bollerslev il quale è un modello generallizzato autoregressivo con eteroschedasticità condizionale e si indica con GARCH(p,q). In questo modello la varianza condizionale dipende dai valori

passati delle serie storiche e da una media mobile di varianze condizionali passate:

$$h_t = \epsilon_t \sigma_t \tag{6.7}$$

di cui

$$\sigma_t^2 = \alpha_0 + \sum_{i=1}^{q} \alpha_i h_{t-i}^2 + \sum_{j=1}^{p} \beta_j \sigma_{t-j}^2 \tag{6.8}$$

dove

- $\epsilon_t \approx WN(0, \sigma^2)$ e rappresenta un rumore bianco gaussiano a media nulla e varianda finita;
- i coefficienti devono soddisfare le seguenti due condizioni $\alpha_i \geq 0$ e $\beta_j \geq 0$;
- $\alpha_0 \succ 0$,

Queste ultime condizioni assicurano che la varianza condizionale sia sempre strettamente positiva. Questi modelli sono molto utili nelle previsioni puntuali.

6.4 Investimenti Governativi

Nella Figura 6.2 è riportato il grafico del carico giornaliero tipico dei consumi energetici dove è indicato anche il consumo medio oltre a quello orario.

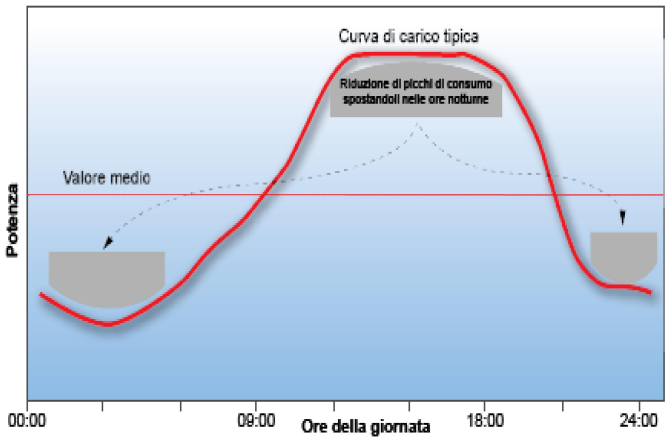

Figura 6.2: Profilo di carico giornaliero tipico per i consumi di energia elettrica.

Come si vede dal grafico la potenza richiesta nell'arco della giornata ha sia un picco di richiesta sopra la media, sia dei minimi abbondantemente sotto la media. Se si riducessero i consumi di picco, appiattendo la curva di carico ottenendo un profilo costante, questo genererebbe dei vantaggi economici altissimi. Questo concetto è alla base di tutte le iniziative internazionali tese a sviluppare la diffusione delle Smart Grid. Si punta infatti a ridurre i picchi di consumo attraverso tariffazioni dinamiche multiorarie che inducano i clienti a spostare i loro consumi dalla fascia oraria corrispondente al picco in fascie orarie corrispondenti alle zone di valle. Questo perchè anche nel mercato dell'energia quando la domanda è alta il prezzo dell'energia aumenta.

Vediamo ora alcune stime di risparmio:

1. Uno studio svolto da centri di ricerca e relativo al consumo elettrico nel 2007 negli Stati Uniti afferma che una riduzione del picco del 5% genera; a parità di consumi totali, un risparmio di 3 miliardi di dollari permettendo di spegnere circa 625 centrali e relative infrastrutture.

2. A dimostrazione del fatto che una tariffazione dinamica multioraria porta ad una riduzione dei consumi vediamo l'esempio della Finlandia. In Finlandia è bastato fornire agli utenti i dati relativi al loro consumo in tempo reale per ottenere un risparmio energetico del 7% sempre a parità di potenza richiesta e consumata.

In conclusione fornisco alcune cifre relative ai finanziamenti governativi a questo settore per dare l'idea di quanto vale questo settore e di quanto ci si aspetta dallo sviluppo della tecnologia Smart Grid:

- Lo sviluppo di reti intelligenti di distribuzione dell'energia elettrica sta diventando una priorità centrale per la politica energetica di molti governi. In questo primo esempio esamino il caso degli Stati Uniti in cui le Smart Grid sono un punto centrale e qualificante della politica energetica del Presidente Barack Obama. Infatti nel febbraio 2009 il governo americano ha varato un piano per 787 miliardi di dollari per risanare l' economia in crisi, di questi ben 49,7 miliardi (circa il 6.3%) per lo sviluppo di reti energetiche intelligenti.

- Questa rivoluzione tecnologica è arrivata anche in Europa dove ci sono prospettive di business importanti. Nel merito la Commissione Europea analizzando il progetto 'European Smart Grids Technology Platform' stima in 750 miliardi di euro gli investimenti che saranno messi in campo nei prossimi 30 anni tra investimenti di aziende private, incentivi

governativi ed incentivi europei. Quindi investimenti che permetteranno non solo di adempiere al 'PIANO 20-20-20' ma anche si superarlo. Di questi 750 miliardi di euro circa 100 miliardi riguarderanno la trasmissione, 300 miliardi la distribuzione e i restanti 350 miliardi la generazione. Agli investimenti parteciperanno le principali aziende europee nei settori dell'energia e delle telecomunicazioni, in particolare per l'Italia: Enel e Telecom Italia.

Capitolo 7

Politiche Energetiche

7.1 La Politica Energetica americana di Barack Obama

In U.S.A. come nel resto del pianeta la crisi economica ha imposto cambiamenti negli stili di vita e nel modo di consumare le risorse ambientali. Barack Obama sin dal 2008 durante la campagna elettorale si è distinto promuovendo politiche energetiche diverse rispetto al passato, più inclini a una politica ambientale basata su energie rinnovabili e tecnologie a bassa emissione di gas serra. Il piano energetico del presidente Obama ideato col suo vice Presidente Biden venne approvato dal Congresso degli Stati Uniti nel 13 febbraio del 2009 con il nome 'New Energy for America'.

Questa nuova proposta energetica si fonda sulle seguenti tre linee guida:

1. Delineare un Nouvo Futuro Energetico (Chart a new Energy Future): questo obbiettivo mira ad ottenere uno sviluppo delle anergie rinnovabili e pulite al fine di limitare la dipendenza degli Stati Uniti dal petrolio.

2. Investimenti in Energie Pulite e Rinnovabili (Invest in clear, renewable Energy): in questo punto l'amministrazione U.S.A. si impegna a mettere in atto politiche energetiche che porteranno gli Stati Uniti a produrre il 25% del loro fabbisogno energetico con fonti rinnovabili interne.

3. Combattere il Cambiamento Climatico (Fight climate Change): diminuire l'inquinamento atmosferico ed ambientale facendo uso di energie rinnovabili dove possibile, oppure in alternativa promuovere tecnologie a più basso impatto ambientale quando non fosse possibile azzerare le emissioni inquinanti.

Queste tre linee guida teoriche descrivono un piano generale per il futuro. La loro realizzazione pratica sarà attraverso i seguenti provvedimenti:

- Minore dipendenza dalle importazioni di fonti fossili: questo obbiettivo è uno degli obbiettivi primari del Presidente Obama. Una riduzione del consumo di petrolio comporterebbe un triplice vantaggio:

  1. Un risparmio economico legato alla quantità di petrolio non più consumato. Per dare un'idea del vantaggio economico che se ne trarrebbe basti pensare che dal 1992 al 2005 il consumo di petrolio negli U.S.A. è aumentato del 20% arrivando a costare 500 miliardi di dollari solo nel 2006.
  2. Un notevole calo dell'inquinamento dato che il consumo di petrolio è una delle fonti primarie dell'inquinamento atmosferico.
  3. Un vantaggio dal punto di vista strategico per il pease che sarebbe meno esposto ad una dipendenza dai paesi fornitori di greggio.

- Piani di incentivo per incoraggiare l'uso di biocombustibili, l'acquisto di automobili di ultima generazione e la creazione delle adeguate strutture sia di rifornimento che di distribuzione di questo carburante.

- Riduzione delle emissioni di GAS SERRA attraverso il meccanismo detto 'CAP-AND-TRADE'. Questo accordo a cui il Presidente Obama ha aderito prevede la riduzione dell'80% delle emissioni di gas serra rispetto al livello di riferimento dell'anno 1990, ed inoltre deve essere fissato un limite massimo alle emissioni annue. Questo piano prevede che le aziende che superano i limiti imposti debbano pagare delle penali, oppure acquistare un permesso governativo che le rende esenti dal rispetto dei limiti sull'inquinamento. Una sorta di tassa sull'inquinamento che poi il governero americano utilizzerà per finanziare imprese e centri di ricerca che sviluppano tecnologie rinnovabili e a minor impatto ambientale.

- Promozione dell'EFFICIENZA ENERGETICA nel campo dell'edilizia. Nel piano del Presidente Obama è presente l'obbiettivo di riuscire a costruire edifici 'Carbon Neutral' entro il 2030 puntando sull'efficienza energetica.

- Incentivi per le fonti rinnovabili in modo da arrivare a produrre il 25% del fabbisogno di energia elettrica nazionale con fonti rinnovabili. Il governo americano conta di investire in incentivi 150 miliardi di dollari nei prossimi 10 anni.

- Riduzione del 20% delle emissioni di gas serra derivanti dalle centrali a carbone ancora attive e blocco delle futura costruzione di questo tipo di centrali.

- Infine l'amministrazione americana ha varato un piano di risparmio energetico mirato per il settore dell'automobile promuovendo la diffusione di auto che funzionano con biocarburanti o con motore elettrico. Le stime diffuse dal governo U.S.A. parlano di un risparmio di circa 1.8 miliardi di barili di petrolio pari a 900 milioni di tonnellate in meno di gas serra prodotti.

In conclusione è bene dire che non tutti i punti previsti nel piano 'New Energy for America' approvato nel 2009 sono stati attuati dal Presidente Obama a causa della forte recessione economica che anche in America ha impedito al governo di fare investimenti gravando sul debito pubblico.

7.2 Contesto Socio Economico e gli obbiettivi di Orizzonte 2020

Lo scenario economico dal 2008 in poi a cuasa della recessione economica è drasticamente cambiato, non solo negli Stati Uniti, ma anche nel resto del mondo e in Europa daterminando una crisi profonda sia nei consumi che negli investimenti. Purtroppo questo quadro è andato a toccare tutti i settori delle attività produttive, dalle attività manifatturiere alla attività di ricerca scientifica. Lo scopo della Commissione Europea è quello di mettere in atto una serie di provvedimenti e incentivi atti a far ripartire l'economia del continente cercando di affrontare la crisi del debito con la stabilizzazione della finanza e la creazione di canali di credito specifici per centri di ricerca e PMI (Piccole e Media Imprese). In particolare lo sviluppo delle piccole e medie imprese rappresenterebbe qual'ora questo piano di incentivi andasse in porto una risorsa decisiva per l'economia italiana essendo questa fondata su una rete di aziende di cui più del 90% piccole o medie.

I governi stanno cercando di darsi regole comuni per il risanamento dei bilanci pubblici tentando di porre un freno a quella che viene detta crisi del debito. Malgrado questi sforzi, tutti i ministri economici sostengono che il rilancio dell'Europa non andrà a buon fine se non supportato da una politica di incentivi alla crescita e allo sviluppo. Gli obbiettivi che la Comunità Europea punta a centrare sono in ordine alle seguenti materie:

- Cambiamenti Climatici.

- Invecchiamento della Popolazione: se da un lato l'allungamento della vita delle persone è un parametro che indica quanto la nostra società si sia sviluppata; il lato negativo è che persone in avanzata età rappresentano un costo maggiore dal punto di vista previdenziale e sanitario. Purtroppo queste due voci sono due parti importanti della spesa statale e del debito che l'Europa impone di ridurre.

- Cercare di trasformare la società dal punto di vista dell'efficienza dello sfruttamento delle risorse a sua disposizione.

L'investimento in innovazione e ricerca è considerato uno degli strumneti princiapali in grado di far ripartire l'economia per una serie di ragioni:

- Crea nuovi posti di lavoro sia intellettuale che manuale.

- Migliora la qualità della vita.

- Crea nuove opportunità commerciali e nuovi brevetti.

Nonostante l'Europa sia un'area del mondo che eccelle dal punto di vista della ricerca e dello sviluppo deve comunque reggere un continuo confronto con i centri di ricerca che si stanno sviluppando nei paesi emergenti oltre a quelli delle altre aree del mondo già sviluppate. In concreto la proposta dell'Unione Europea è quella di investire in ricerca e sviluppo una quantità di risorse pari a circa il 3% del PIL complessivo Europeo.

Le proposte uscite dalle commissioni Economia e Sviluppo il 30 novembre 2011 per Orizzonte 2020 sono atte a stabilire:

1. La quantità dei finaziamenti erogati dalla Comunità Europea.

2. I criteri di scelta dei destinatari delle sovvenzioni.

3. I criteri di valutazione della produttività del finanziamento, cioè di quanto è stato prodotto scientificamente, o di quanti brevetti sono stati registrati a fronte dell'investimento fatto.

Per realizzare queste proposte diventano indispensabili degli interventi sul sistema attuale che mirino a:

- Sburocratizzare le procedure di assegnazione dei finanziamenti in modo che questi arrivino in tempi più celeri.

- Privilegiare tutti quei tipi di ricerca che possano dare prodotti commercializzabili in poco tempo. In pratica dare la precedenza a progetti di ricerca che possono arrivare alla commercializzazione in tempi brevi, questo allo scopo far ripartire la produzione industriale e le assunzioni.

- Incentivi a giovani scienziati che presentano progetti di ricerca brillanti o facilmente commercializzabili in poco tempo per i medesimi motivi del punto precedente.

Un piano di rilancio europeo così massiccio deve inevitabilmente coinvolgere tutte le principali sfere della società Europea: sfera Sociale, sfera Industriale e sfera Scientifica. Vado ora ad analizzare singolarmente i tre aspetti:

- Sfera Sociale e Umanistica: tra le priorità dell'ambito sociale ci sono il finanziamento di tutte le attività che riguardano il welfare state, gli stili di vita e gli aspetti climatici. Le componenti che vanno ad incidere sull'aspetto sociale e umanistico dello sviluppo europeo sono:

    1. Energia da fonti rinnovabili, quindi più sicure e meno inquinanti, con evidenti implicazioni sul clima, sull'inquinamento e sulla salute.
    2. Trasporti migliori, più efficienti, meno inquinanti.
    3. Efficientamento delle spese della sanità e del welfare state.

- Sfera Scientifica: lo scopo della Comunità Europea in questo ambito è quello di mantenere il livello di eccellenza per la ricerca europea. Il fine è quello di andare a sostenere i migliori scienziati a livello europeo, i giovani ricercatori finanziandoli nelle loro attività.

- Sfera Industriale: lo scopo della comunità europea in questo ambito è quello di incentivare gli investimenti in nuove imprese attraverso opere di sburocratizzazione e incentivi alle aziende, in particolari a due tipi di aziende:

    1. Grandi Aziende: cioè quelle aziende che possono investire capitali in innovazione e mettere in piedi collaborazioni con centri di ricerca allo scopo di creare brevetti e sviluppare tecnologie sempre migliori.
    2. Piccole e Medie Imprese: fornire fondi a queste imprese perchè possano crescere e aumentare l'occupazione al fine di rilanciare l'economia europea.

Le tre sfere sociali appena viste sono tra loro complementari e un miglioramento in uno di questi ambiti causa a cascata benefici anche negli altri due. Lo sviluppo delle energie rinnovabili, Smart Grid sono la parte principale dei finanziamenti destinati per le aziende e lo sviluppo in questo settore

di ricerca. Le Commissioni congiunte Economia e Sviluppo puntano ad arrivare ad impiegare in questo settore strategico anche per l'ambiente il 60% dei fondi a loro disposizione e il 35% in ricerche connesse al clima e alla tutela dell'ambiente.

Orizzonte 2020 è un piano della durata preventivata di 7 anni, dal 2014 quando entrerà in vigore al 2020 come dice il nome stesso. La struttura di questo insieme di norme sarà composta in una parte di finanziamenti e interventi che una volta decisi rimarranno costanti nei sette anni; mentre la restante parte sarà flessibile in modo da consentire al legislatore un intervento mirato a fronte di eventuali variazioni delle condizioni socio-economiche in corso d'opera. Per concludere la trattazione di Orizzonte 2020 dopo aver visto come si struttura e quali scopi ha questo piano di incentivi vado ad analizzare alcuni punti qualificanti.

7.2.1 PMI: Piccole e Medie Imprese

Come precedentemente ricordato le Piccole e Medie Imprese sono una parte importantissima del tessuto imprenditoriale Italiano comprendendo circa il 90% delle aziende nazionali. Contemporanemente le PMI sono un attore importante, anche se in percentuali inferiori, dell'economia di molti altri paesi. Le PMI per loro natura sono aziende dinamiche e flessibili che sanno adattarsi meglio di grandi colossi industriali alle variazioni dell'economia. Purtroppo però la loro piccola dimensione fa si che i bilanci di queste aziende non siano sufficientemente ricchi da permettere loro investimenti in settori quali ricerca e sviluppo. Ne consegue che i prodotti di queste aziende non possano essere sviluppati anche se innovativi. Il piano Orizzonte 2020 destina a queste imprese il 15% del finanziamento complessivo. Per accedere ai fondi le PMI interessate dovranno depositare richiesta di finanziamento presso uno sportello unico. Una commissione valuterà le richieste di finanziamento premiando le aziende con i prodotti più innovativi o quelle innovazioni facilmente brevettabili e commercializzabili in breve tempo. Da tutto questo la commissione punta ad ottenere un rilancio dell'economia e dell'occupazione. Infine il Consiglio Europeo oltre ai fondi europei di Orizzonte 2020 intende anche promuovere l'attivazione di canali di credito privilegiato per le PMI in accordo con istituti di credito nazionali e regionali all'interno degli stati membri.

7.2.2 Il Ruolo della Cooperazione Internazionela

La Cooperazione Internazionale è uno strumento molto importante per raggiungere gli obbiettivi di Orizzonte 2020. La Cooperazione Internazionele

si realizza essenzialmente favorendo la mobilità dei ricercatori e di tutti gli addetti all'innovazione. Lo scopo di questa attività è la diffusione e il commercio di nuove tecnologie al fine di ottenere standard comuni. Lo scopo ultimo è quello di ottenere standard condivisi a livello mondiale. Se così fosse molti prodotti sarebbero compatibili tra di loro e questo faciliterebbe il commercio internazionale di beni. Sempre a livello Europeo si è cercato di arrivare a questo obbiettivo anche attraverso le Direttive Europee. Le Direttive vengono emanate dal Parlamento Europeo e devono essere recepite entro scadenze prestabilite dei parlamenti nazionali. Il loro scopo è quello di superare le divergenze tra le diverse normative tecniche nei vari stati membri al fine di facilitare la circolazione di beni e servizi all'interno dell'Unione Europea.

7.3 Europa 2020

Orizzonte 2020 rappresenta in piano di interventi e incentivi promossi dalla Comunità Europea al fine di uscire dalla crisi e mantenere l'eccellenza nella ricerca scientifica in Europa. Questa strategia di crescità però entrerà in vigore nel 2014 e sarà attiva per 7 anni fino al 2020. La strategia di crescita attualmente in vigore prende il nome di Europa 2020. Europa 2020 è stata presentata il 3 Marzo del 2010, in piena crisi economica, per cui gli obbietivi sono i medesimi di Orizzonte 2020. Analogamente anche le strategie di crescita economica proposte da Europa 2020 sono simili a quelle di Orizzonte 2020, cioè fondate sugli stessi tre punti chiave. In particolare per Europa 2020 la Commissione Europea e il presidente della Commissione Europea fissano cinque traguardi da raggiungere per il decennio che va dal 2010 al 2020:

1. Il 75% delle persone di età compresa tra i 20 e i 64 anni deve avere un lavoro.
2. Il 3% del PIL della Zona Euro deve essere ivestito in ricerca e sviluppo.
3. I traguardi del 'PIANO 20-20-20' devono essere raggiunti.
4. Cercare di limitare l'abbandono scolastico al di sotto del 10% e contemporaneamente far si che almeno il 40% dei giovani raggiungano il diploma o la laurea.
5. 20 milioni di persone in meno sotto la soglia della povertà.

Per raggiungere questi obbiettivi la Commissione Europea indica una serie di linee guida che riporto di seguito:

- Riorientare la maggior parte di investimenti possibili in investimenti per la ricerca e lo sviluppo.
- Investire in idee innovative al fine di tradurle in brevetti prima e in prodotti poi.
- Realizzare il 'Brevetto Comunitario'. La Commissione Europea stima in 289 milioni di euro l'anno i risparmi che ne deriverebbero per le aziende.
- Promuovere la mobilità dei ricercatori tra i vari centri di ricerca a livello europeo in modo da favorire una ricerca migliore.
- Abbattimento del digital divide cioè rendere accessibile a quante più persone possibili un collegamento internet ad alta velocità. Ad oggi sono ancora molte le persone ed aziende che non dispongono di un collegamento internet o di un collegamento veloce. Per questo importante traguardo sono previsti finanziamenti per 80 miliardi di euro.
- Realizzazione del Mercato Unico Digitale e dell'Agenda Europea del Digitale. Purtroppo questo punto non sarà raggiunto in tempo nè in Italia nè in Europa.
- Raggiungimento dei traguardi del 'PIANO 20-20-20'. Il piano prevede di:
  - Ridurre del 20% le emissioni dei gas serra.
  - Aumentare fino al 20% la quota di energia consumata prodotta da fonti rinnovabili.
  - Portare al 20% il risparmio energetico.

  Si stima che il raggiungimento di questo obbiettivo porti la riduzione di 60 miliardi le spese per le importazioni di greggio e gas entro il 2020.
- Politiche industriali di incentivi alle aziende che investono in ricerca e sviluppo di tecnologie verdi.
- Piattaforma europea contro la povertà, cioè l'attivazione di politiche di sostegno alla spesa per le fascie sociali più deboli al fine di far ripartire l'economia e l'occupazione.

Chiaramente alcuni obbiettivi di Orizzonte 2020 sono i medesimi di Europa 2020 perchè Orizzonte 2020 è una prosecuzione delle iniziative promosse

in Europa 2020. Al contrario molti obbiettivi di Europa 2020 non sono citati in Orizzonte 2020 perchè si considera che nel 2014 dovrebbero essere già stati raggiunti. Per concludere bisogna dire che ad oggi,purtroppo, obbiettivi come l'abbattimento del digital divide sono lontani e quindi diventano qualificanti per Orizzonte 2020.

Bibliografia

[1] SMART GRID: La Rete Intelligente. Breve Guida alla Rivoluzionaria Tecnologia Sostenibile 2.0. Dalla Spinta di Obama alle Prime Start Up della Nuova Rete Elettrica del Futuro; *http://www.genitronsviluppo.com/2009/04/07/smart-grid-rete-elettrica-intelligente/*.

[2] SMART GRID: 10 Cose che La Rete Elettrica Intelligente può Imparare da Internet. Vantaggi, Standard Aperti, Facilità di Connessione e Comunicazione; *http://www.genitronsviluppo.com/2009/05/11/smart-grid-internet/*.

[3] Campi elettromagnetici a bassa frequenza; *http://www.arpa.emr.it/pubblicazioni/cem/generale-49.asp*.

[4] Elena Ragazzi, Ettore Bompard, Enrico Pons, Alberto Stefanini, Ning Xie; *STATO DELL' ARTE SULLE SMART GRID: Orientamenti,Attori, Prospettive*; Cnr-Ceris.

[5] Distribuzione di energia elettrica; *http://it.wikipedia.org/wiki/Distribuzione-di-energia-elettrica*; Da Wikipedia, l'enciclopedia libera.

[6] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin; *Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities*; IEEE Communications Society, 11 gennaio 2012.

[7] Stefano Bimbo, Enrico Colaiacovo; *Sistemi SCADA Supervisory control and data acquisition*; APOGEO srl.

[8] Stefano Panzieri, Roberto Setola; *Vulnerabilità indotte dal Cyberspace sui Sistemi di Monitoraggio e Controllo*; Convegno Nazionale ANIPLA ENERSIS 2004.

[9] Stefano Panzieri, Ilaria Scarano, Roberto Setola; *Vulnerabilità Informatica dei Sistemi SCADA Connessi alle Reti Pubbliche.*

[10] Fabio L. Bellifemine, Claudio Borean, Roberto De Bonis; *Smart Grids: Energia e ICT*; Notiziario Tecnico Telecom Italia, Anno 18, No. 3, 2009.

[11] James F. Kurose, Keith W. Ross; *Reti di Calcolatori e Internet, un approccio top-down*; Pearson Addison Wesley 4 edizione.

[12] Tommaso Proietti; *Econometria Applicata*; Dipartimento di Scienze Statistiche Universit'a di Udine.

[13] Riccardo Lucchetti; *Appunti di analisi delle serie storiche.*

[14] Matteo Pelagatti; *Un algoritmo IML per la stima robusta dei modelli ARIMA e per l'individuazione dei valori anomali nelle serie storiche*; Facoltà di Scienze Statistiche Università degli Studi di Milano Bicocca.

[15] COMMISSIONE EUROPEA; *COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI*; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0808:FIN:it:PDF

[16] Agi Energia; *La Politica Energetica di Barack Obama*; http://www.museoenergia.it/museo.php?stanza=78&ppost=622.

[17] Agi Energia; *La politica energetica di Barack Obama e la nuova riforma nel settore automotive*; http://www.agienergia.it/Notizia.aspx?idd=352 id=19&ante=0.

[18] sublimina.it; *Smart Grid:verso le reti energetiche di nuova generazione*; http://www.sublimina.it/linee-di-ricerca-smart-grid/77-smart-gridverso-le-reti-energetiche-di-nuova-generazione.html.

[19] Wikipedia; *Wikipedia definizione Smart Grid*;

[20] European Technology Platform SmartGrids; *Definizione Smart Grid*;

[21] http://www.inhabitat.com/2009/04/30/energy-101-what-is-a-smart-grid/; *Definizione Smart Grid*;

[22] Department of Energy Grid 2030; *Definizione Smart Grid*;

[23] Carnegie Mellon University; *Definizione Smart Grid*;

[24] http://www.smartgrids.eu/?q=node/163; *Definizione Smart Grid*;

[25] Alessia Barban; *Previsione di Prezzi nel Mercato Elettrico: Modelli e Applicazioni*; UNIVERSITA' DEGLI STUDI DI PADOVA.

[26] Bozzolan Nicola; *Previsione di Prezzi nel Mercato Elettrico: Modelli e Applicazioni*; UNIVERSITA' DEGLI STUDI DI PADOVA.

[27] Marina Marzovilli; *MODELLAZIONE E PREVISIONE DEI PREZZI DEL MERCATO DELL'ENERGIA ELETTRICA: UN CONFRONTO FRA DIVERSE STRATEGIE*; UNIVERSITA' DEGLI STUDI DI PADOVA.

[28] Enzo M. Tieghi; *Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.)*; Quaderni CLUSIT-Associazione Italiana per la Sicurezza Informatica.