



# smart grid survey

---

Marco Amoruso, Daniele Anello, Francesco Farina, Iolanda Rinaldi

4 dicembre 2015

Università degli Studi di Salerno

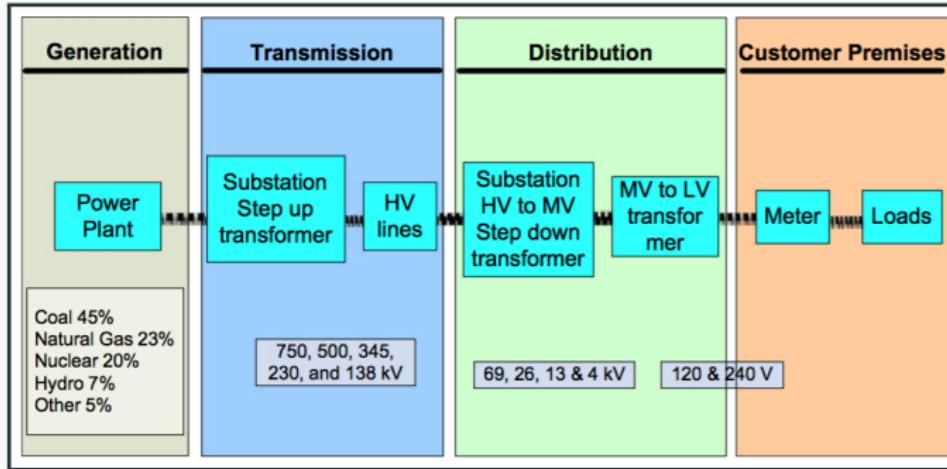
# sommario

1. Smart Grid:  
panorama attuale e definizione
2. Architettura
3. Smart Grid Cybersecurity
4. Standard e tecnologie
5. Principali vulnerabilità delle Smart Grid:  
attacchi e contromisure

## smart grid: panorama attuale e definizione

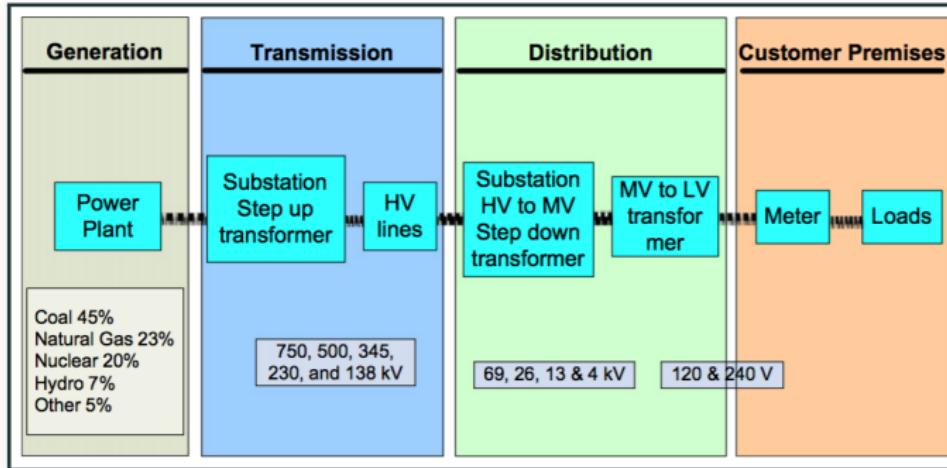
---

# rete elettrica attuale



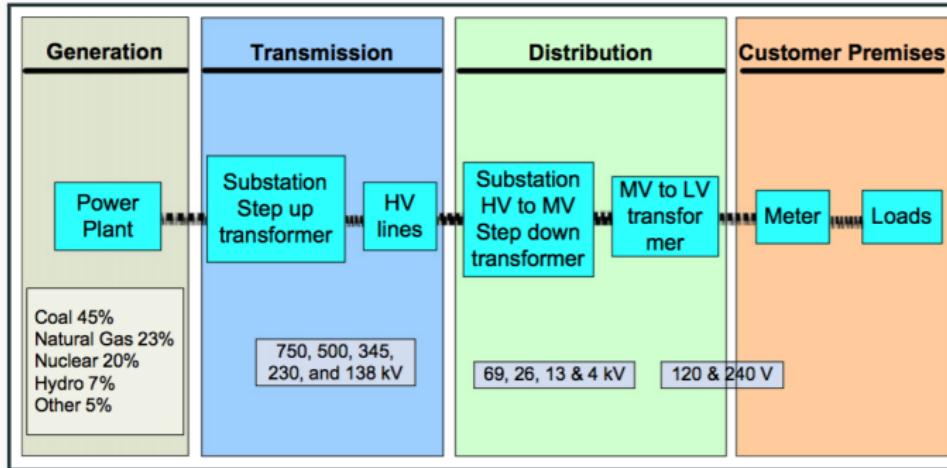
- Tre sottosistemi distinti

# rete elettrica attuale



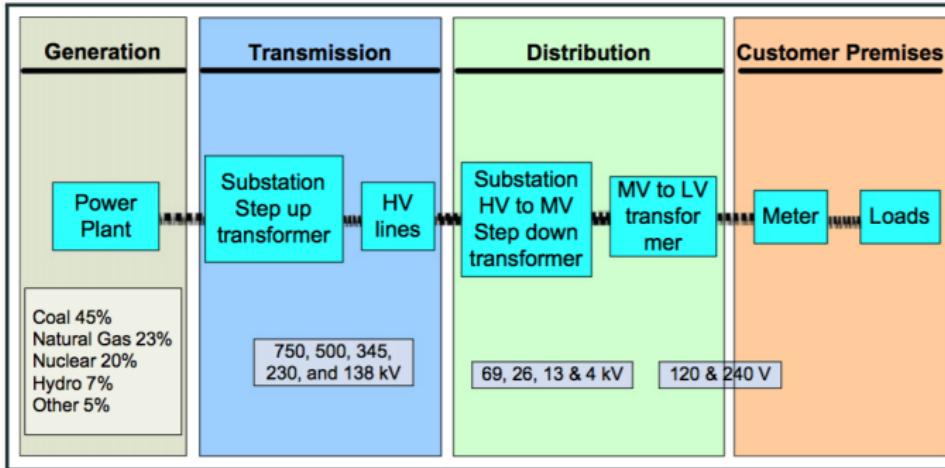
- Tre sottosistemi distinti
  - Generazione

# rete elettrica attuale



- Tre sottosistemi distinti
  - Generazione
  - Trasmissione

# rete elettrica attuale



- Tre sottosistemi distinti
  - Generazione
  - Trasmissione
  - Distribuzione

## rete elettrica attuale

---

- Comunicazione unidirezionale

## rete elettrica attuale

- Comunicazione unidirezionale
- Interconnessione e ridondanza per risolvere i problemi

## rete elettrica attuale

- Comunicazione unidirezionale
- Interconnessione e ridondanza per risolvere i problemi
- Distribuzione dell'energia gestita da un controllore centralizzato

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente
  - Conservazione dell'energia

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente
  - Conservazione dell'energia
  - Riduzione globale dellemissione di anidride carbonica

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente
  - Conservazione dell'energia
  - Riduzione globale dellemissione di anidride carbonica
- Non ci si pu affidare all'infrastruttura attuale

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente
  - Conservazione dell'energia
  - Riduzione globale dellemissione di anidride carbonica
- Non ci si può affidare all'infrastruttura attuale
  - Inadeguatezza della struttura gerarchica

# problemi della rete elettrica attuale

---

- Numerosi problemi da risolvere
  - Diversificazione della generazione di energia
  - Gestione delle richieste utente
  - Conservazione dell'energia
  - Riduzione globale dellemissione di anidride carbonica
- Non ci si può affidare all'infrastruttura attuale
  - Inadeguatezza della struttura gerarchica
    - Effetto domino in caso di guasti

# problemi della rete elettrica attuale

---

- Necessit di digitalizzare le infrastrutture critiche

# problemi della rete elettrica attuale

---

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione

# problemi della rete elettrica attuale

---

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione
  - Requisito necessario per gestire l'ambiente che muta

# problemi della rete elettrica attuale

---

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione
  - Requisito necessario per gestire l'ambiente che muta
- Esempio di digitalizzazione: meter analogico → Smart meter

# problemi della rete elettrica attuale

---

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione
  - Requisito necessario per gestire l'ambiente che muta
- Esempio di digitalizzazione: meter analogico → Smart meter
  - Dispositivo disconnesso e non critico → Dispositivo connesso ad Internet che pu generare dati critici

# problemi della rete elettrica attuale

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione
  - Requisito necessario per gestire l'ambiente che muta
- Esempio di digitalizzazione: meter analogico → Smart meter
  - Dispositivo disconnesso e non critico → Dispositivo connesso ad Internet che pu generare dati critici
- Fondamentale la sicurezza dei dati e dei comandi degli smart meter

# problemi della rete elettrica attuale

- Necessit di digitalizzare le infrastrutture critiche
  - Aggiunta di capacit di computazione e comunicazione
  - Requisito necessario per gestire l'ambiente che muta
- Esempio di digitalizzazione: meter analogico → Smart meter
  - Dispositivo disconnesso e non critico → Dispositivo connesso ad Internet che pu generare dati critici
- Fondamentale la sicurezza dei dati e dei comandi degli smart meter
- Obiettivo della survey: capire la sicurezza della nuova infrastruttura

# perch la smart grid?

---

- Vari fattori influenzano lo sviluppo della rete elettrica

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi
  - Sicurezza delle forniture

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi
  - Sicurezza delle forniture
  - Iniziative nazionali

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi
  - Sicurezza delle forniture
  - Iniziative nazionali
- Significative opportunit offerte da

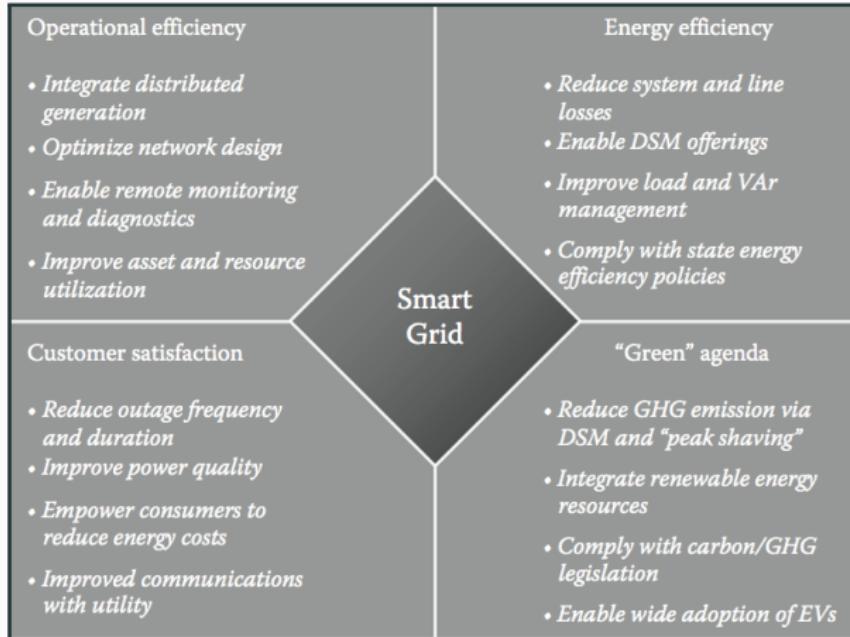
# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi
  - Sicurezza delle forniture
  - Iniziative nazionali
- Significative opportunit offerte da
  - ICT

# perch la smart grid?

- Vari fattori influenzano lo sviluppo della rete elettrica
  - Strutture non pi adeguate
  - Vincoli termici e operativi
  - Sicurezza delle forniture
  - Iniziative nazionali
- Significative opportunit offerte da
  - ICT
  - Monitoraggio costante delle componenti della rete

# perch la smart grid?



# smart grid: definizione

---

- Smart Grid = tecnologie + soluzioni per utenti finali

# smart grid: definizione

---

- Smart Grid = tecnologie + soluzioni per utenti finali
- Non esiste una singola definizione precisa

# smart grid: definizione

---

- Smart Grid = tecnologie + soluzioni per utenti finali
- Non esiste una singola definizione precisa
- possibile trovare una serie di caratterizzazioni

# smart grid: definizione

## Secondo l'European Technology Platform

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

# smart grid: definizione

In accordo all'US Department of Energy

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

# smart grid: definizione

## Per *Smarter Grids: The Opportunity*

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

# requisiti di una smart grid

---

- Quality of Service

# requisiti di una smart grid

---

- Quality of Service
  - Bassa latenza: la maggior parte delle interazioni deve avvenire in tempo reale

# requisiti di una smart grid

---

- Quality of Service
  - Bassa latenza: la maggior parte delle interazioni deve avvenire in tempo reale
  - Larghezza di banda sufficiente per permettere la trasmissione simultanea di messaggi senza impatto sulla latenza

# requisiti di una smart grid

---

- Quality of Service
  - Bassa latenza: la maggior parte delle interazioni deve avvenire in tempo reale
  - Larghezza di banda sufficiente per permettere la trasmissione simultanea di messaggi senza impatto sulla latenza
- Interoperabilit

# requisiti di una smart grid

---

- Quality of Service
  - Bassa latenza: la maggior parte delle interazioni deve avvenire in tempo reale
  - Larghezza di banda sufficiente per permettere la trasmissione simultanea di messaggi senza impatto sulla latenza
- Interoperabilità
  - Abilità delle diverse parti della Smart Grid di lavorare insieme

# requisiti di una smart grid

---

- Scalabilit

# requisiti di una smart grid

---

- Scalabilit
  - Facilitare linserimento di nuovi dispositivi, nuovi servizi, e meccanismi di monitoraggio real-time

# requisiti di una smart grid

---

- Scalabilit
  - Facilitare linserimento di nuovi dispositivi, nuovi servizi, e meccanismi di monitoraggio real-time
- Standardizzazione

# requisiti di una smart grid

---

- Scalabilit
  - Facilitare l'inserimento di nuovi dispositivi, nuovi servizi, e meccanismi di monitoraggio real-time
- Standardizzazione
  - IEEE P2030 group si occupa di definire standard e linee guida

# requisiti di una smart grid

---

- Sicurezza

# requisiti di una smart grid

---

- Sicurezza
  - Gestire attacchi volontari (terroismo, spionaggio, utenti non contenti)

# requisiti di una smart grid

---

- Sicurezza
  - Gestire attacchi volontari (terrorismo, spionaggio, utenti non contenti)
  - Gestire manomissioni involontarie (fallimenti delle attrezzature, disastri naturali)

# requisiti di una smart grid

---

- Sicurezza
  - Gestire attacchi volontari (terroismo, spionaggio, utenti non contenti)
  - Gestire manomissioni involontarie (fallimenti delle attrezzature, disastri naturali)
  - North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), IEEE, National Infrastructure Protection Plan (NIPP), e NIST stabiliscono i requisiti di sicurezza della Smart Grid

# requisiti di una smart grid

- Sicurezza

- Gestire attacchi volontari (terroismo, spionaggio, utenti non contenti)
- Gestire manomissioni involontarie (fallimenti delle attrezzature, disastri naturali)
- North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), IEEE, National Infrastructure Protection Plan (NIPP), e NIST stabiliscono i requisiti di sicurezza della Smart Grid
- Denominatore comune: autenticazione, autorizzazione e tecnologie per la privacy

## building blocks: requisiti

---

- Building blocks rete elettrica → Smart Grid

## building blocks: requisiti

---

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing

# building blocks: requisiti

---

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione

# building blocks: requisiti

---

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione
  - Controllo

# building blocks: requisiti

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione
  - Controllo
- Requisiti

# building blocks: requisiti

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione
  - Controllo
- Requisiti
  - Rilevare malfunzionamenti/deviazioni dal normale range operativo

# building blocks: requisiti

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione
  - Controllo
- Requisiti
  - Rilevare malfunzionamenti/deviazioni dal normale range operativo
  - Permettere che l'input dei sensori raggiunga gli elementi di controllo

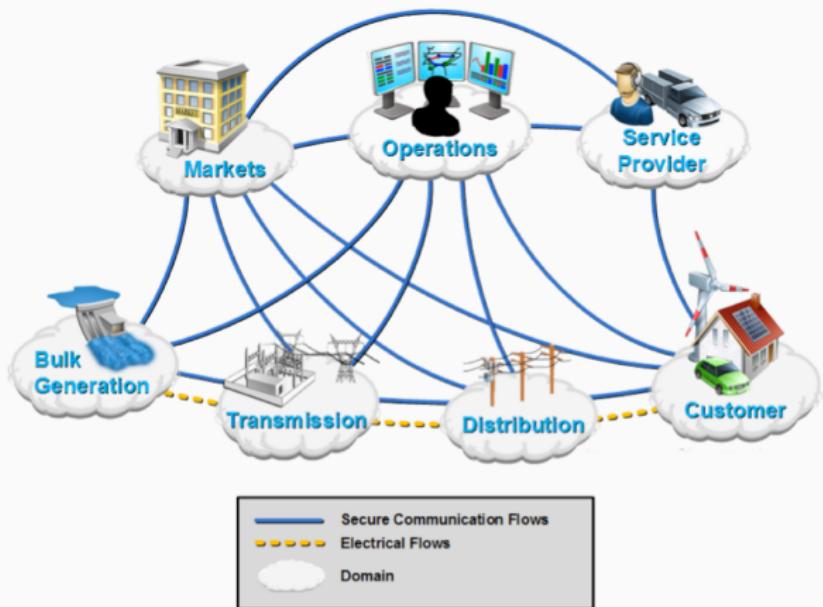
# building blocks: requisiti

- Building blocks rete elettrica → Smart Grid
  - Monitoraggio/sensing
  - Comunicazione
  - Controllo
- Requisiti
  - Rilevare malfunzionamenti/deviazioni dal normale range operativo
  - Permettere che l'input dei sensori raggiunga gli elementi di controllo
  - Generare messaggi per assicurarsi che la trasmissione sia conforme alle aspettative

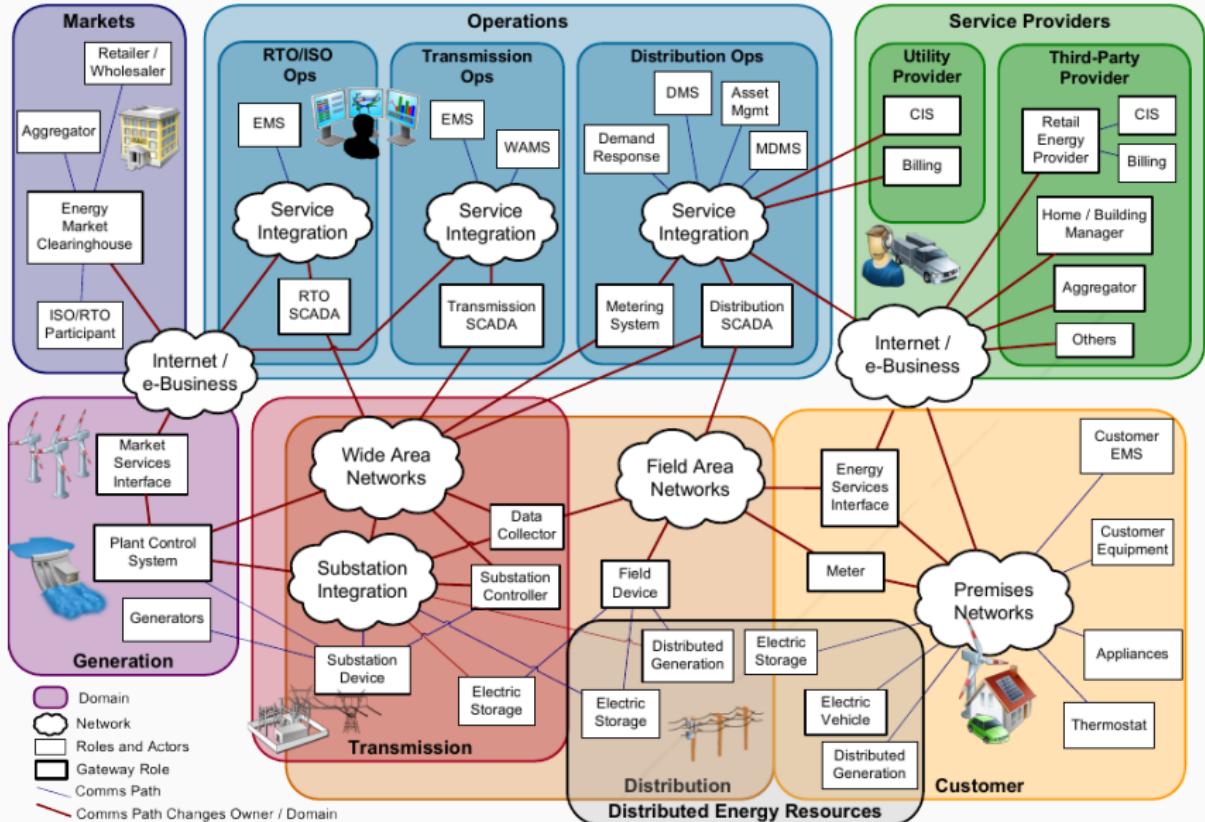
architettura

---

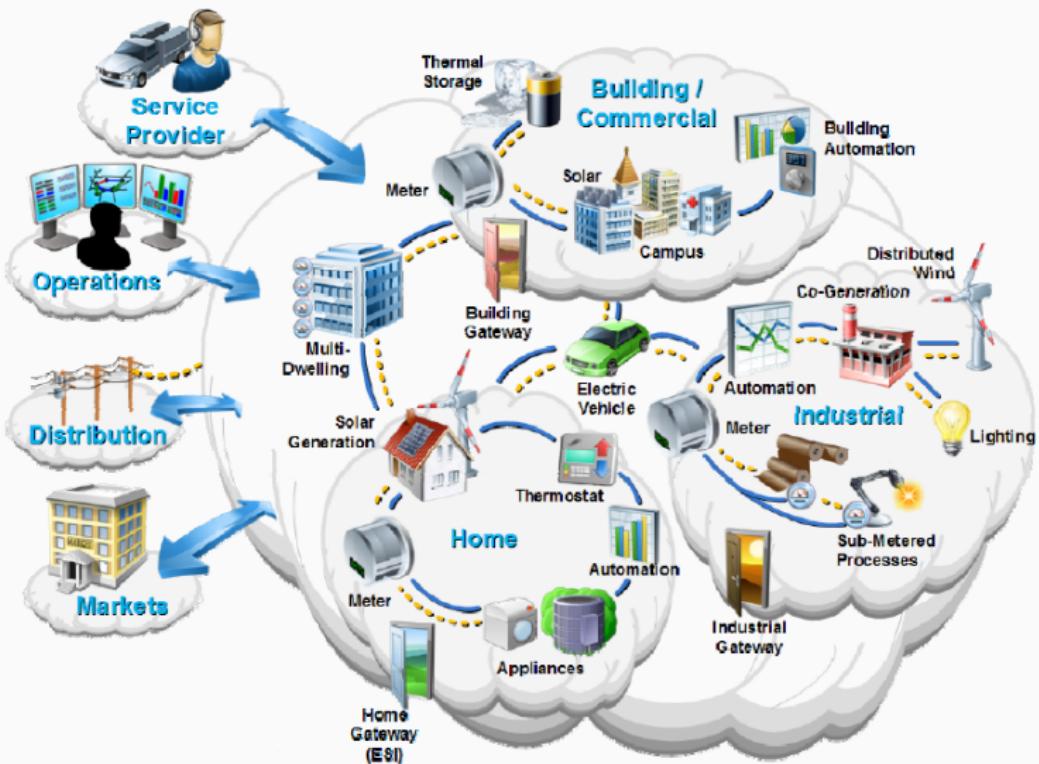
# architettura



# architettura



# customer



- Smart meter un dispositivo elettronico che registra consumi di energia elettrica

- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione

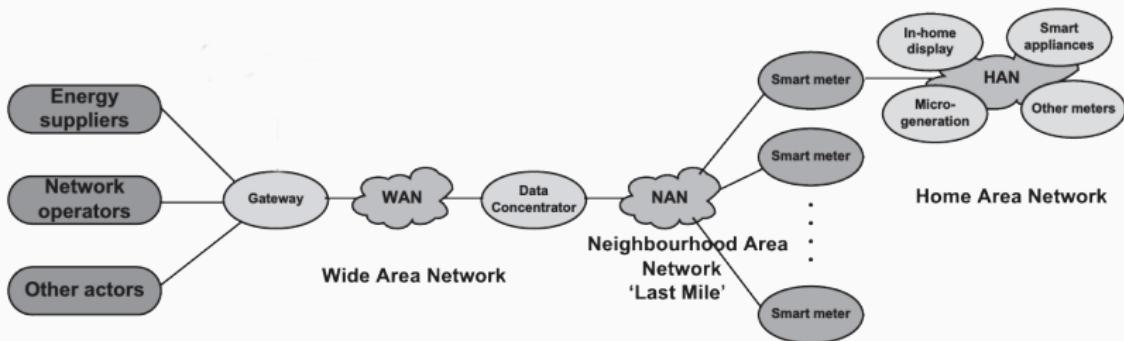
- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione
  - Blocca la fornitura di energia

- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione
  - Blocca la fornitura di energia
  - Notifica informazioni per monitoraggio e in caso di manomissione

- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione
  - Blocca la fornitura di energia
  - Notifica informazioni per monitoraggio e in caso di manomissione
- Advanced Metering Infrastructure (AMI)

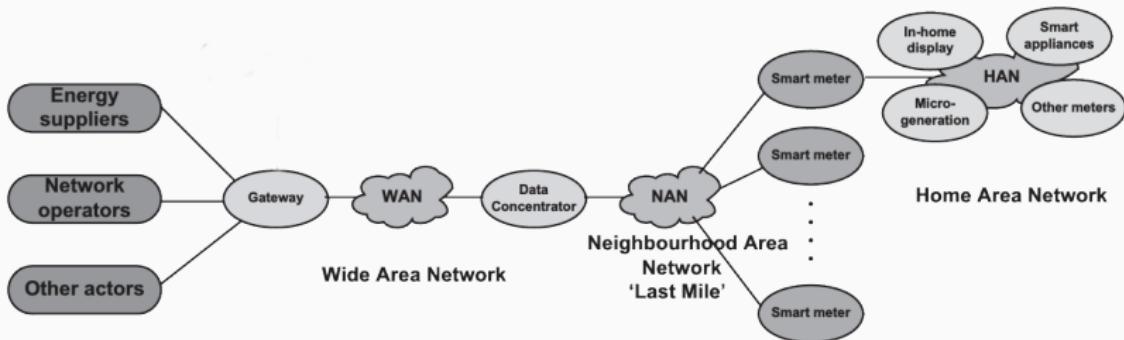
- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione
  - Blocca la fornitura di energia
  - Notifica informazioni per monitoraggio e in caso di manomissione
- Advanced Metering Infrastructure (AMI)
  - Consente una comunicazione bidirezionale fra utility e consumer

- Smart meter un dispositivo elettronico che registra consumi di energia elettrica
  - Comunica informazioni per scopi di fatturazione
  - Blocca la fornitura di energia
  - Notifica informazioni per monitoraggio e in caso di manomissione
- Advanced Metering Infrastructure (AMI)
  - Consente una comunicazione bidirezionale fra utility e consumer
  - Misura, colleziona, analizza il consumo energetico e comunica con gli smart device



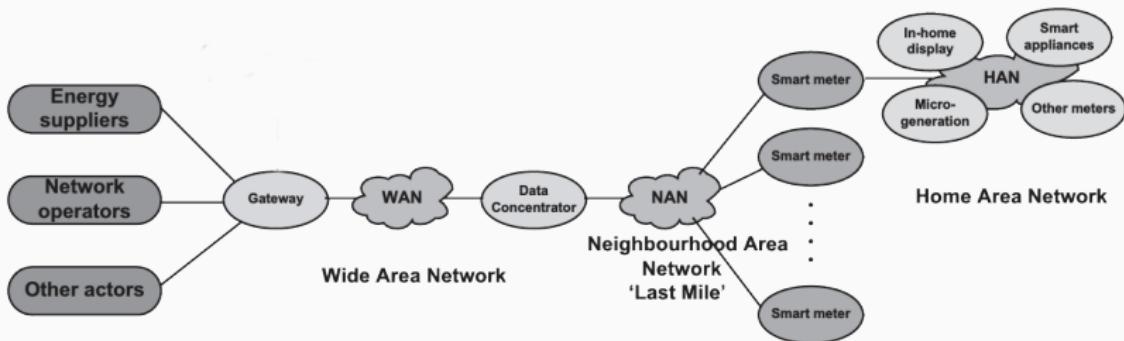
## Data Concentrator

- Dispositivo elettronico che si pone fra gli smart meter e gateway



## Data Concentrator

- Dispositivo elettronico che si pone fra gli smart meter e gateway
- Gestisce e controlla gli smart meter collegati ad esso



## Data Concentrator

- Dispositivo elettronico che si pone fra gli smart meter e gateway
- Gestisce e controlla gli smart meter collegati ad esso
- Punto di aggregazione delle misurazioni effettuate dagli smart meter

# markets



# service provider



## service provider

---

- Sviluppano interfacce e standard per un sistema basato su un modello di mercato dinamico, proteggendo le infrastrutture di energia critiche

## service provider

---

- Sviluppano interfacce e standard per un sistema basato su un modello di mercato dinamico, proteggendo le infrastrutture di energia critiche
- Non devono compromettere la sicurezza informatica, l'affidabilit, la stabilit, l'integrit o la sicurezza della rete

## service provider

---

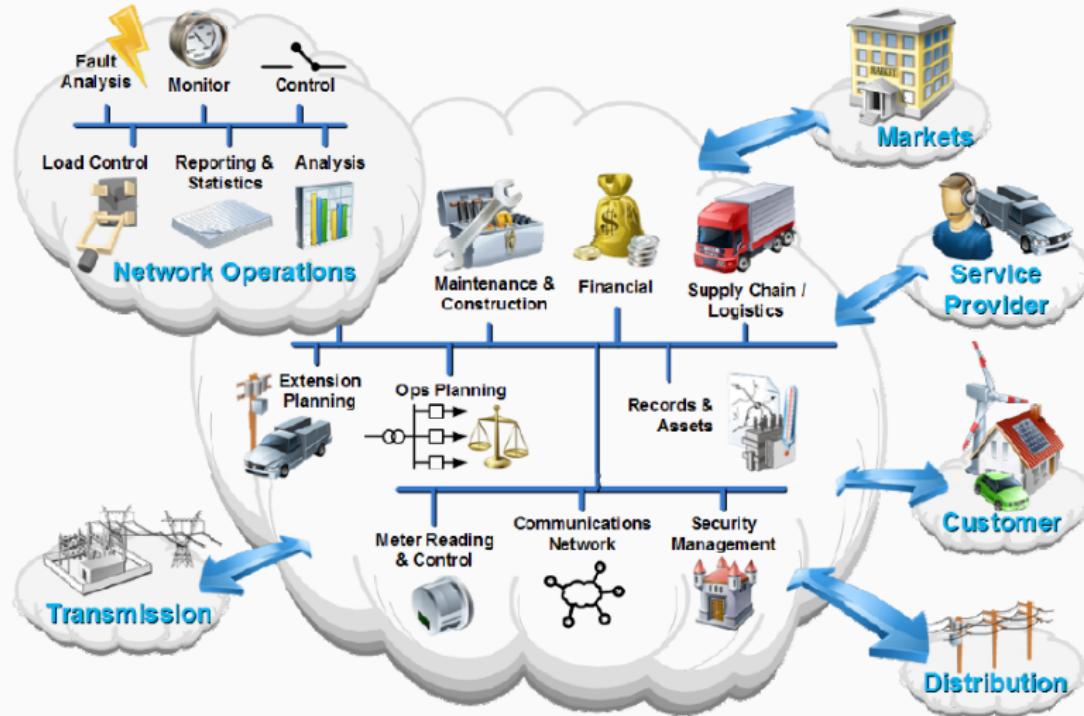
- Sviluppano interfacce e standard per un sistema basato su un modello di mercato dinamico, proteggendo le infrastrutture di energia critiche
- Non devono compromettere la sicurezza informatica, l'affidabilit, la stabilit, l'integrit o la sicurezza della rete
- Creano servizi e prodotti per rispondere alle nuove esigenze e le opportunit offerte dall'evoluzione delle Smart Grid

## service provider

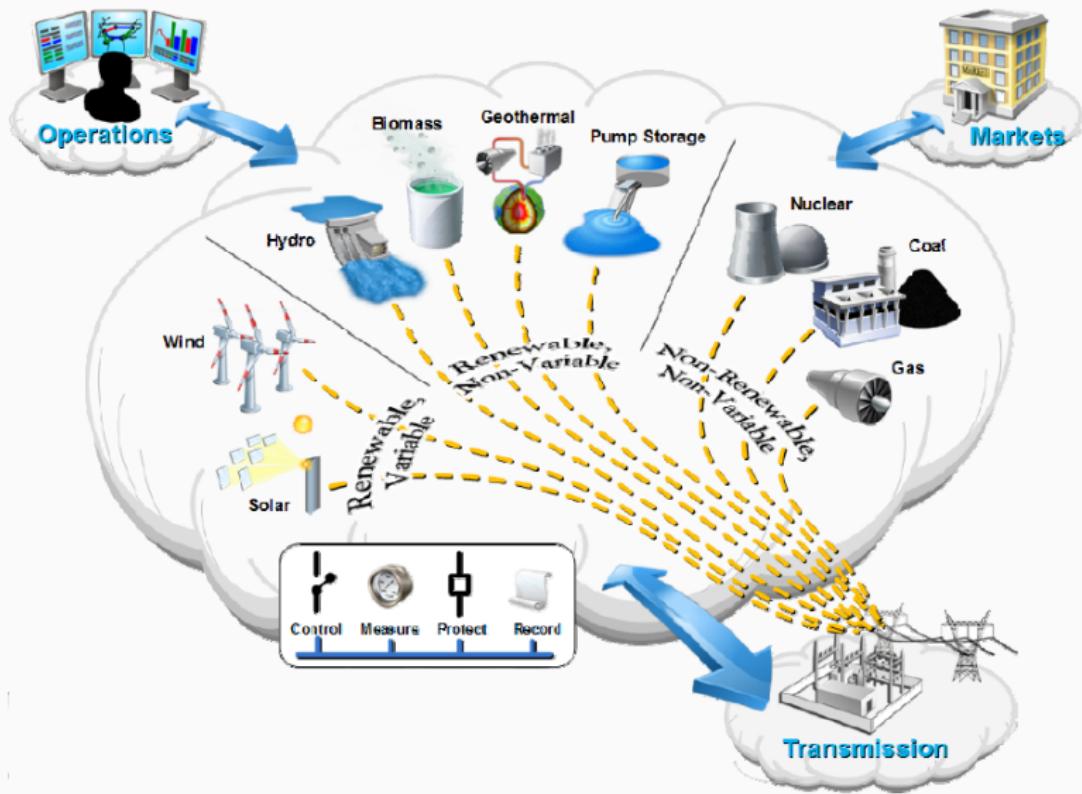
---

- Sviluppano interfacce e standard per un sistema basato su un modello di mercato dinamico, proteggendo le infrastrutture di energia critiche
- Non devono compromettere la sicurezza informatica, l'affidabilit, la stabilit, l'integrit o la sicurezza della rete
- Creano servizi e prodotti per rispondere alle nuove esigenze e le opportunit offerte dall'evoluzione delle Smart Grid
- Rappresentano una zona di notevole crescita economica

# operations



# generation



# generation

---

- Gestire il flusso energetico e l'affidabilità del sistema

# generation

---

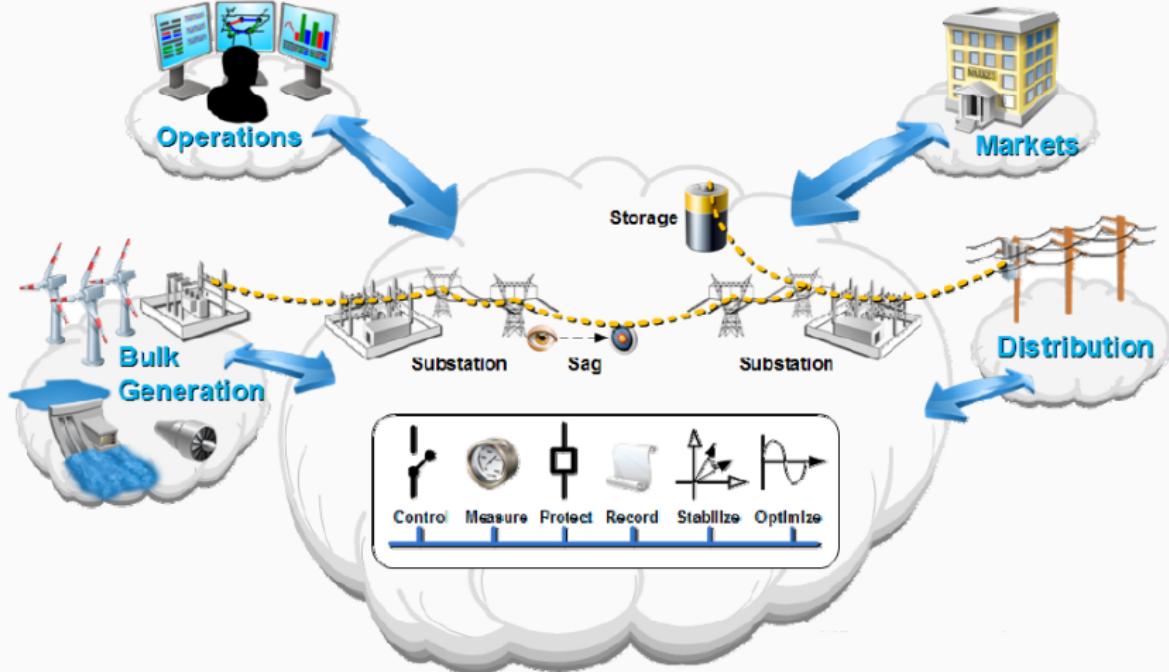
- Gestire il flusso energetico e l'affidabilità del sistema
- Reagire rapidamente ai guasti, interruzioni di corrente o abbassamenti di tensioni

# generation

---

- Gestire il flusso energetico e l'affidabilità del sistema
- Reagire rapidamente ai guasti, interruzioni di corrente o abbassamenti di tensioni
- Monitoraggio delle strutture per valutarne le condizioni

# transmission



- Gestita da un Regional Transmission Operator o Independent System Operator (RTO/ISO)

- Gestita da un Regional Transmission Operator o Independent System Operator (RTO/ISO)
  - Mantiene la stabilità della rete bilanciando la generazione con la domanda energetica

- Gestita da un Regional Transmission Operator o Independent System Operator (RTO/ISO)
  - Mantiene la stabilità della rete bilanciando la generazione con la domanda energetica
- Monitorata da sistemi di supervisione e controllo di acquisizione dati

- Gestita da un Regional Transmission Operator o Independent System Operator (RTO/ISO)
  - Mantiene la stabilità della rete bilanciando la generazione con la domanda energetica
- Monitorata da sistemi di supervisione e controllo di acquisizione dati
- Composta da substation, torri di trasmissione, linee elettriche e dispositivi di telemetria

Le substation sono una componente chiave del sistema di trasmissione

- Punto di connessione del sistema di trasmissione e distribuzione

Le substation sono una componente chiave del sistema di trasmissione

- Punto di connessione del sistema di trasmissione e distribuzione
- Costituite da componenti automatizzate

Le substation sono una componente chiave del sistema di trasmissione

- Punto di connessione del sistema di trasmissione e distribuzione
- Costituite da componenti automatizzate
- Gestiscono, supervisionano e monitorano le apparecchiature di trasmissione

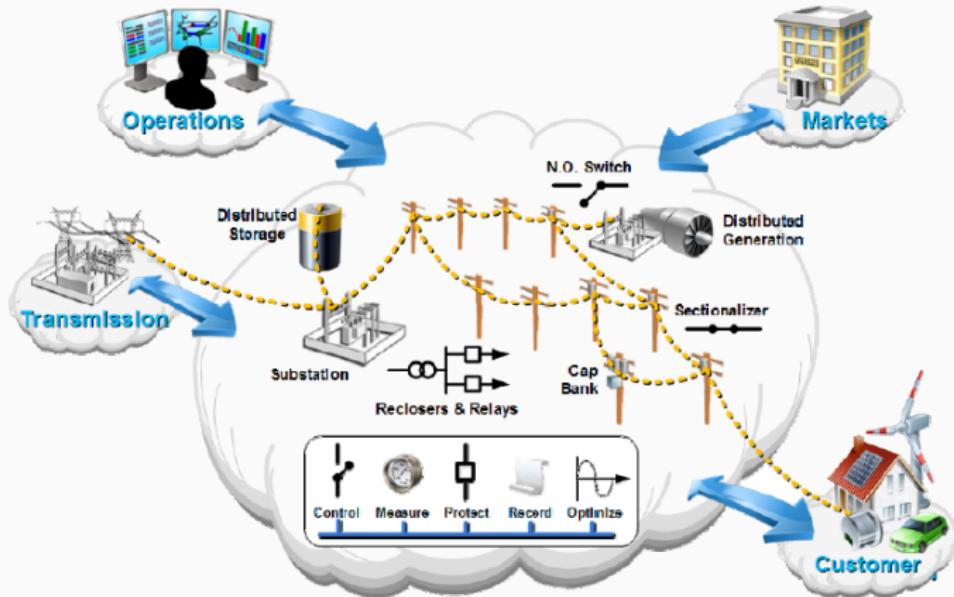
Le substation sono una componente chiave del sistema di trasmissione

- Punto di connessione del sistema di trasmissione e distribuzione
- Costituite da componenti automatizzate
- Gestiscono, supervisionano e monitorano le apparecchiature di trasmissione
- Gestiscono dinamicamente il **voltaggio**

Le substation sono una componente chiave del sistema di trasmissione

- Punto di connessione del sistema di trasmissione e distribuzione
- Costituite da componenti automatizzate
- Gestiscono, supervisionano e monitorano le apparecchiature di trasmissione
- Gestiscono dinamicamente il voltaggio
- Adottano politiche di ripristino, previsione e correzione

# distribution



smart grid cybersecurity

---

# smart grid cybersecurity: sommario

---

- Stuxnet
- Definire la sicurezza
  - Confidentiality
  - Integrity
  - Availability
  - Control
  - Authenticity
  - Usability
- Building blocks
  - Layered security model
  - Authentication
  - Authorization
  - Auditing
  - Key management
  - Message, Network and System integrity
- Threats and impacts
  - Consumer threats
  - Utility companies threats

# smart grid cybersecurity: sommario

---

- Stuxnet
- Definire la sicurezza
  - Confidentiality
  - Integrity
  - Availability
  - Control
  - Authenticity
  - Usability
- Building blocks
  - Layered security model
  - Authentication
  - Authorization
  - Auditing
  - Key management
  - Message, Network and System integrity
- Threats and impacts
  - Consumer threats
  - Utility companies threats

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente
  2. Ricercava software Siemens Step7

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente
  2. Ricercava software Siemens Step7
  3. Comprometteva i programmable logic controller

## un caso esemplare di attacco: stuxnet

---

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente
  2. Ricercava software Siemens Step7
  3. Comprometteva i programmable logic controller

## un caso esemplare di attacco: stuxnet

- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente
  2. Ricercava software Siemens Step7
  3. Comprometteva i programmable logic controller

Stuxnet stato creato dal governo USA in collaborazione col governo  
Israeliano e diffuso nella centrale iraniana di Natanz

## un caso esemplare di attacco: stuxnet

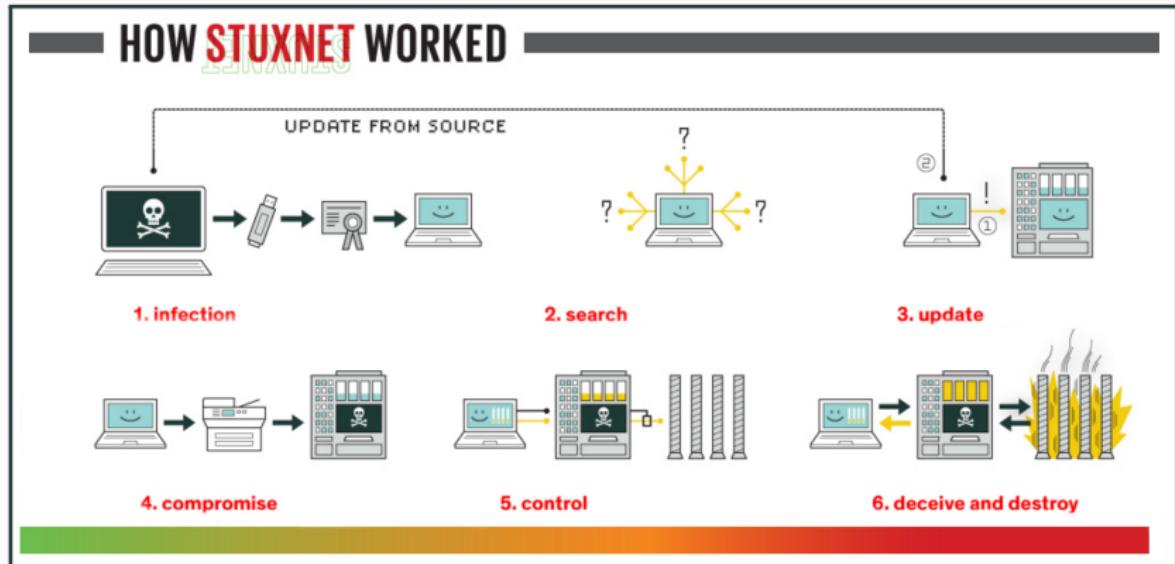
- Noto **worm** di 500 Kbyte scoperto nel 2010
- Attaccava in 3 fasi:
  1. Attaccava macchine Windows e reti, replicandosi ripetutamente
  2. Ricercava software Siemens Step7
  3. Comprometteva i programmable logic controller

Stuxnet stato creato dal governo USA in collaborazione col governo  
Israeliano e diffuso nella centrale iraniana di Natanz

### Scopo

Sabotare la centrifuga della centrale tramite comandi inviati all'hardware  
di controllo industriale responsabile della velocità di rotazione delle turbine  
con l'intento di danneggiarle

# un caso esemplare di attacco: stuxnet

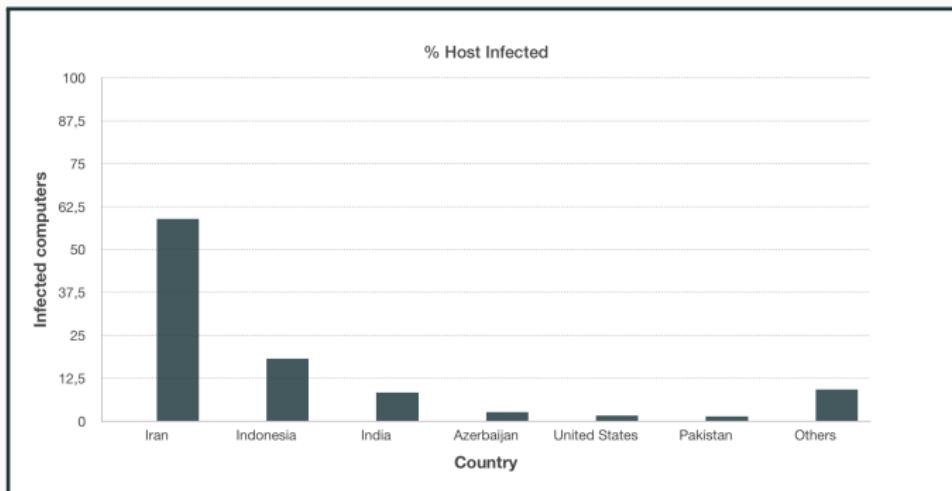


# un caso esemplare di attacco: stuxnet

## Danni Causati

L'azione di Stuxnet ha distrutto tra le 900 e le 1000 centrifughe (circa il 10% di quelle totali), nonostante l'intento di distruggerle tutte

Uno studio da parte di **Symantec** relativo alla diffusione di Stuxnet mostra la percentuale di host infetti nei giorni successivi all'attacco



# smart grid cybersecurity: sommario

---

- Stuxnet
- Definire la sicurezza
  - Confidentiality
  - Integrity
  - Availability
  - Control
  - Authenticity
  - Usability
- Building blocks
  - Layered security model
  - Authentication
  - Authorization
  - Auditing
  - Key management
  - Message, Network and System integrity
- Threats and impacts
  - Consumer threats
  - Utility companies threats

# definire la sicurezza: parkerian hexad



## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema

## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema
- Informazioni ricavate dal lavoro delle componenti della Smart Grid

## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema
- Informazioni ricavate dal lavoro delle componenti della Smart Grid
- Dati personali dei clienti → garantire la *privacy*

## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema
- Informazioni ricavate dal lavoro delle componenti della Smart Grid
- Dati personali dei clienti → garantire la *privacy*
- **Informazioni aziendali**

## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema
- Informazioni ricavate dal lavoro delle componenti della Smart Grid
- Dati personali dei clienti → garantire la *privacy*
- Informazioni aziendali
- Punti che introducono rischio: locazioni di memoria e meccanismi di trasmissione dati

## Confidentiality

- Dati confidenziali → se noti, potrebbero causare danni alla sicurezza delle operazioni di tutto il sistema
- Informazioni ricavate dal lavoro delle componenti della Smart Grid
- Dati personali dei clienti → garantire la *privacy*
- Informazioni aziendali
- Punti che introducono rischio: locazioni di memoria e meccanismi di trasmissione dati
- Soluzioni: **cifratura dei dati e controllo degli accessi**

## Integrity

- Abilit del sistema di evitare che le informazioni siano modificate da persone o da sistemi non autorizzati

## Integrity

- Abilit del sistema di evitare che le informazioni siano modificate da persone o da sistemi non autorizzati
- Mancanza di integrity → il sistema riceve dati non accurati → instabilit della Smart Grid

## Integrity

- Abilit del sistema di evitare che le informazioni siano modificate da persone o da sistemi non autorizzati
- Mancanza di integrity → il sistema riceve dati non accurati → instabilit della Smart Grid
- Punti che introducono rischio: componenti in cui si consente il passaggio dati da un sistema ad un altro

## Integrity

- Abilit del sistema di evitare che le informazioni siano modificate da persone o da sistemi non autorizzati
- Mancanza di integrity → il sistema riceve dati non accurati → instabilit della Smart Grid
- Punti che introducono rischio: componenti in cui si consente il passaggio dati da un sistema ad un altro
- Soluzioni: *auditing, authorization, nonrepudiation, message-signing*

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno
- Punti che introducono rischio: sistema che gestisce le comunicazioni e l'inoltro di comandi

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno
- Punti che introducono rischio: sistema che gestisce le comunicazioni e l'inoltro di comandi
- Soluzioni: tecniche di ridondanza

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno
- Punti che introducono rischio: sistema che gestisce le comunicazioni e l'inoltro di comandi
- Soluzioni: tecniche di ridondanza

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno
- Punti che introducono rischio: sistema che gestisce le comunicazioni e l'inoltro di comandi
- Soluzioni: tecniche di ridondanza

## Control (o Possession)

- Capacità di controllare le informazioni che necessitano protezione

## Availability

- Capacità del sistema di compiere il lavoro che gli è stato assegnato, nel momento in cui se ne ha bisogno
- Punti che introducono rischio: sistema che gestisce le comunicazioni e l'inoltro di comandi
- Soluzioni: tecniche di ridondanza

## Control (o Possession)

- Capacità di controllare le informazioni che necessitano protezione
- Mancanza di controllo dati → compromissione del sistema che li trasmette → provenienza delle informazioni non garantita → diminuzione dell'affidabilità

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza
- Assicurarsi che la fonte dei dati e i dati stessi siano autentici

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza
- Assicurarsi che la fonte dei dati e i dati stessi siano autentici

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza
- Assicurarsi che la fonte dei dati e i dati stessi siano autentici

## Usability (o Utility)

- Assicurare che i dati siano utilizzabili

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza
- Assicurarsi che la fonte dei dati e i dati stessi siano autentici

## Usability (o Utility)

- Assicurare che i dati siano utilizzabili
- Flusso di dati cifrato → garantisce la sicurezza ma rende difficile far s che le informazioni siano utili

# definire la sicurezza

## Authenticity

- Processo utilizzato per descrivere la certezza della provenienza
- Assicurarsi che la fonte dei dati e i dati stessi siano autentici

## Usability (o Utility)

- Assicurare che i dati siano utilizzabili
- Flusso di dati cifrato → garantisce la sicurezza ma rende difficile far s che le informazioni siano utili
- Usabilità fornisce valore a livello aziendale → trattato come il requisito a più alta priorità

# smart grid cybersecurity: sommario

---

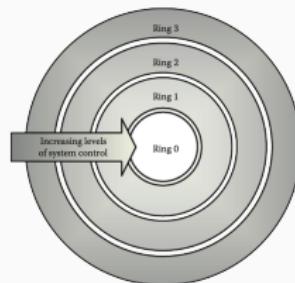
- Stuxnet
- Definire la sicurezza
  - Confidentiality
  - Integrity
  - Availability
  - Control
  - Authenticity
  - Usability
- Building blocks
  - Layered security model
  - Authentication
  - Authorization
  - Auditing
  - Key management
  - Message, Network and System integrity
- Threats and impacts
  - Consumer threats
  - Utility companies threats

# building blocks

---

## Layered security model

- Struttura ad anello
- Comunicazione tra gli strati del sistema sicura
- Assicurare che un fallimento in uno strato non abbia impatto n in uno strato pi basso n in qualsiasi sistema dello stesso strato



# building blocks

---

- Authentication

# building blocks

---

- Authentication
  - Verifica dell'identità di una persona o di un servizio che richiede l'accesso ad una risorsa

# building blocks

---

- Authentication
  - Verifica dell'identità di una persona o di un servizio che richiede l'accesso ad una risorsa
  - Autenticazione non solo per l'utente ma anche tra sistemi, processi o componenti hardware

# building blocks

---

- Authentication
  - Verifica dell'identità di una persona o di un servizio che richiede l'accesso ad una risorsa
  - Autenticazione non solo per l'utente ma anche tra sistemi, processi o componenti hardware
- Authorization

# building blocks

---

- Authentication
  - Verifica dell'identità di una persona o di un servizio che richiede l'accesso ad una risorsa
  - Autenticazione non solo per l'utente ma anche tra sistemi, processi o componenti hardware
- Authorization
  - Verifica di ciò che la persona o il servizio autenticato può fare all'interno del contesto del sistema

# building blocks

---

- Auditing

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid
  - Testing delle componenti essenziali per mettere in sicurezza le operazioni

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid
  - Testing delle componenti essenziali per mettere in sicurezza le operazioni
- Key management

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid
  - Testing delle componenti essenziali per mettere in sicurezza le operazioni
- Key management
  - Gestione dell'emissione delle chiavi per utenti, applicazioni e dispositivi

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid
  - Testing delle componenti essenziali per mettere in sicurezza le operazioni
- Key management
  - Gestione dell'emissione delle chiavi per utenti, applicazioni e dispositivi
  - Stabilire l'identità dell'utente e garantire l'integrità dei messaggi

# building blocks

---

- Auditing
  - Revisione periodica dell'efficacia dei meccanismi di sicurezza della Smart Grid
  - Testing delle componenti essenziali per mettere in sicurezza le operazioni
- Key management
  - Gestione dell'emissione delle chiavi per utenti, applicazioni e dispositivi
  - Stabilire l'identità dell'utente e garantire l'integrità dei messaggi
  - Impiego di Public Key Infrastructure

# building blocks

---

- Message integrity

# building blocks

---

- Message integrity
  - Signing

# building blocks

---

- Message integrity
  - Signing
    - Messaggio inviato da un sistema ad un altro → autenticazione → autorizzazione → scambio di messaggi

# building blocks

---

- Message integrity
  - Signing
    - Messaggio inviato da un sistema ad un altro → autenticazione → autorizzazione → scambio di messaggi
  - Nonrepudiation

# building blocks

---

- Message integrity
  - Signing
    - Messaggio inviato da un sistema ad un altro → autenticazione → autorizzazione → scambio di messaggi
  - Nonrepudiation
    - Mittente riconosciuto tramite una prova inconfutabile della sua identità

# building blocks

---

- Message integrity
  - Signing
    - Messaggio inviato da un sistema ad un altro → autenticazione → autorizzazione → scambio di messaggi
  - Nonrepudiation
    - Mittente riconosciuto tramite una prova inconfutabile della sua identità
  - Encryption

# building blocks

---

- Message integrity
  - Signing
    - Messaggio inviato da un sistema ad un altro → autenticazione → autorizzazione → scambio di messaggi
  - Nonrepudiation
    - Mittente riconosciuto tramite una prova inconfutabile della sua identità
  - Encryption
    - Messaggio non può essere letto da una persona/sistema non diretto destinatario

# building blocks

---

- Network integrity

# building blocks

---

- Network integrity
  - Firewall

# building blocks

---

- Network integrity
  - Firewall
  - Rilevamento e prevenzione delle intrusioni

# building blocks

---

- Network integrity
  - Firewall
  - Rilevamento e prevenzione delle intrusioni
- System integrity

# building blocks

---

- Network integrity
  - Firewall
  - Rilevamento e prevenzione delle intrusioni
- System integrity
  - Protezione da malware

# building blocks

---

- Network integrity
  - Firewall
  - Rilevamento e prevenzione delle intrusioni
- System integrity
  - Protezione da malware
  - Gestione della configurazione del sistema

# building blocks

---

- Network integrity
  - Firewall
  - Rilevamento e prevenzione delle intrusioni
- System integrity
  - Protezione da malware
  - Gestione della configurazione del sistema
  - **Validazione e testing**

# smart grid cybersecurity: sommario

---

- Stuxnet
- Definire la sicurezza
  - Confidentiality
  - Integrity
  - Availability
  - Control
  - Authenticity
  - Usability
- Building blocks
  - Layered security model
  - Authentication
  - Authorization
  - Auditing
  - Key management
  - Message, Network and System integrity
- Threats and impacts
  - Consumer threats
  - Utility companies threats

## threats and impacts: consumer threats

---

- Minacce naturali

## threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti

## threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni

## threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni
  - **Ladri e stalker**

## threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni
  - Ladri e stalker
  - Hacker

# threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni
  - Ladri e stalker
  - Hacker
  - **Terrorismo**

# threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni
  - Ladri e stalker
  - Hacker
  - Terrorismo
  - Governo

# threats and impacts: consumer threats

---

- Minacce naturali
  - Venti, tempeste, tornadi e terremoti
- Minacce da singoli o da organizzazioni
  - Ladri e stalker
  - Hacker
  - Terrorismo
  - Governo
  - Società di servizi, in particolare i lavoratori

## Privacy del consumatore

- Raccolta di informazioni personali
- Attaccante pu utilizzarli per scopi malevoli

## Privacy del consumatore

- Raccolta di informazioni personali
- Attaccante pu utilizzarli per scopi malevoli

## Impatto sull'availability

- Obiettivo Smart Grid: disponibilit perenne di corrente
- Attacchi possono causare: alterazione di termostati, limitazione di servizi d'emergenza

## Privacy del consumatore

- Raccolta di informazioni personali
- Attaccante pu utilizzarli per scopi malevoli

## Impatto sull'availability

- Obiettivo Smart Grid: disponibilità perenne di corrente
- Attacchi possono causare: alterazione di termostati, limitazione di servizi d'emergenza

## Impatto finanziario

- Corruzione di dati → emissione di bollette inaccurate

# threats and impacts: utility companies threats

---

## **Confidentiality**

- Privacy del consumatore

# threats and impacts: utility companies threats

---

## Confidentiality

- Privacy del consumatore
  - Attacco alla Web application della società

# threats and impacts: utility companies threats

---

## Confidentiality

- Privacy del consumatore
  - Attacco alla Web application della società
  - Analisi dello storico dei consumi → identificare comportamenti utente

## Confidentiality

- Privacy del consumatore
  - Attacco alla Web application della società
  - Analisi dello storico dei consumi → identificare comportamenti utente
- Informazioni proprietarie

# threats and impacts: utility companies threats

---

## Confidentiality

- Privacy del consumatore
  - Attacco alla Web application della società
  - Analisi dello storico dei consumi → identificare comportamenti utente
- Informazioni proprietarie
  - Segreto aziendale → target appetibile per hacker

# threats and impacts: utility companies threats

---

## Integrity

- Frode

## Integrity

- Frode
  - Manomissione dello smart meter per sottostimare i consumi → bollette meno costose

## Integrity

- Frode
  - Manomissione dello smart meter per sottostimare i consumi → bollette meno costose
  - Modifica dati relativi alla produzione di energia → compensi maggiori

## Integrity

- Frode
  - Manomissione dello smart meter per sottostimare i consumi → bollette meno costose
  - Modifica dati relativi alla produzione di energia → compensi maggiori
- Manipolazione dei dati dei sensori

## Integrity

- Frode
  - Manomissione dello smart meter per sottostimare i consumi → bollette meno costose
  - Modifica dati relativi alla produzione di energia → compensi maggiori
- Manipolazione dei dati dei sensori
  - Simulare un guasto → la società spende tempo e denaro per le riparazioni

# threats and impacts: utility companies threats

---

## Availability

- Clienti

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente
- Organizzazioni

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente
- Organizzazioni
  - Hacker che vuole danneggiare la società → *Denial of Service attack*

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente
- Organizzazioni
  - Hacker che vuole danneggiare la società → *Denial of Service attack*
  - Ex dipendente di un'azienda

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente
- Organizzazioni
  - Hacker che vuole danneggiare la società → *Denial of Service attack*
  - Ex dipendente di un'azienda
- Manipolazione del mercato

# threats and impacts: utility companies threats

---

## Availability

- Clienti
  - Connessione allo smart meter di un utente → cambio password + spegnimento corrente
- Organizzazioni
  - Hacker che vuole danneggiare la società → *Denial of Service attack*
  - Ex dipendente di un'azienda
- Manipolazione del mercato
  - Team di hacker + esperti di mercati finanziari → Ottenere significative quantità di denaro in poco tempo

standard e tecnologie

---

# standard e tecnologie: sommario

---

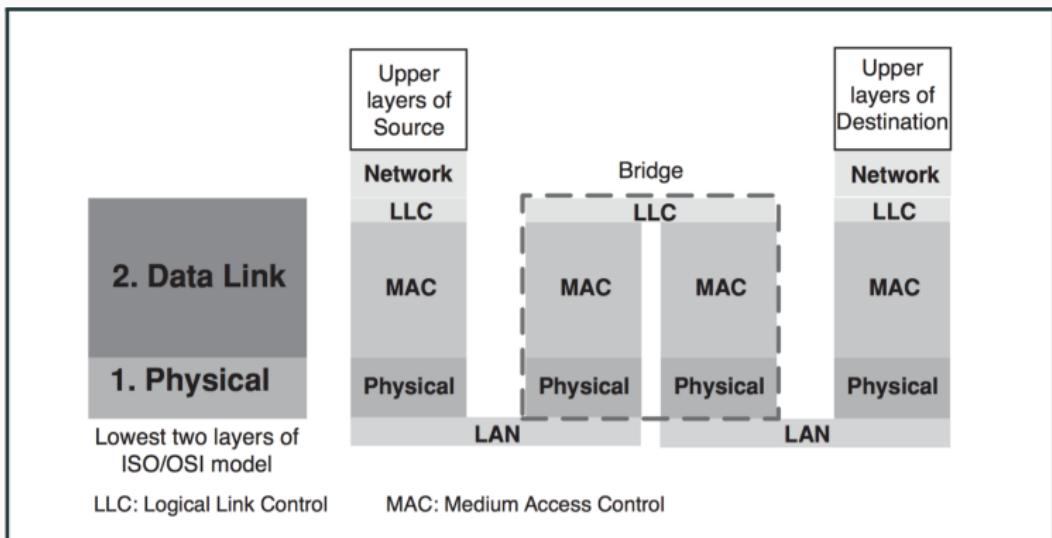
- Tecnologie di comunicazione
  - IEEE 802
    - Ethernet
    - Wireless
    - Bluetooth
    - ZigBee & 6LoWPAN
    - WiMAX
  - Power Line Communication
- Standard per lo scambio di informazioni
  - Modbus
  - ISO/IEC 61850
- Standard per la sicurezza
  - ISO/IEC 62351

# standard e tecnologie: sommario

---

- Tecnologie di comunicazione
  - IEEE 802
    - Ethernet
    - Wireless
    - Bluetooth
    - ZigBee & 6LoWPAN
    - WiMAX
  - Power Line Communication
- Standard per lo scambio di informazioni
  - Modbus
  - ISO/IEC 61850
- Standard per la sicurezza
  - ISO/IEC 62351

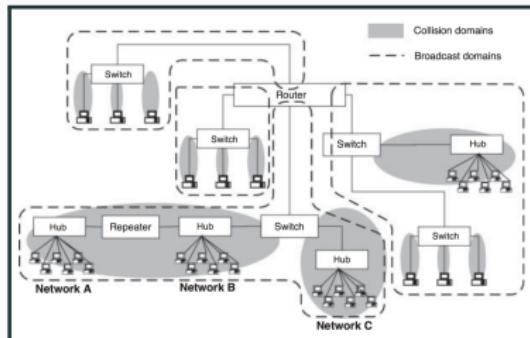
- Famiglia di standard sviluppati per il supporto alle reti locali
- L'architettura incentrata sui due livelli inferiori del modello ISO/OSI



## Ethernet

Xerox Corporation, Intel Corporation e la Digital Equipment Corporation nel 1978 portarono alla standardizzazione di 802.3 e nel 1980 ci fu la pubblicazione della versione 1.0 dello standard Ethernet

- Una tra le tecnologie di rete più utilizzate per le LAN cablate
- Frame-based
- Utilizza un mezzo condiviso (collisioni gestite da CSMA/CD)



## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

# ieee 802[.11]

## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

- Definisce un insieme di standard per le Wireless LAN

## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

- Definisce un insieme di standard per le Wireless LAN
- Utilizza un mezzo condiviso (collisioni gestite da *CSMA/CA*)

## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

- Definisce un insieme di standard per le Wireless LAN
- Utilizza un mezzo condiviso (collisioni gestite da *CSMA/CA*)
- Componenti:

# ieee 802[.11]

## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

- Definisce un insieme di standard per le Wireless LAN
- Utilizza un mezzo condiviso (collisioni gestite da *CSMA/CA*)
- Componenti:
  - Station

## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

- Definisce un insieme di standard per le Wireless LAN
- Utilizza un mezzo condiviso (collisioni gestite da *CSMA/CA*)
- Componenti:
  - Station
  - Access Point (**BSS**)

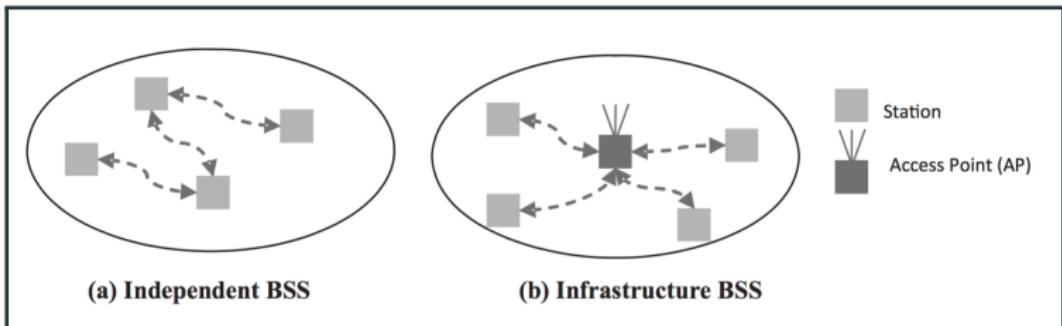
## Wireless

Vic Hayes stato coinvolto nella progettazione degli standard 802.11a e 802.11b all'interno di IEEE nel settembre del 1999

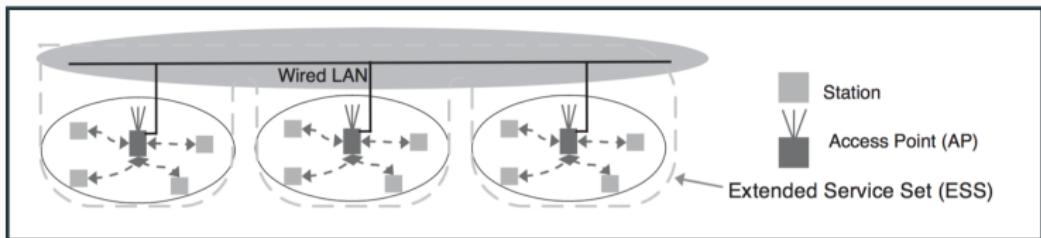
- Definisce un insieme di standard per le Wireless LAN
- Utilizza un mezzo condiviso (collisioni gestite da *CSMA/CA*)
- Componenti:
  - Station
  - Access Point (**BSS**)
  - Distribution System (**ESS**)

## Wireless

### Basic Service Set (BSS)



## Wireless Distribution System



## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - **Corto raggio d'azione**

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete
  - Piconet

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete
  - Piconet
    - Un dispositivo *Master*

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete
  - Piconet
    - Un dispositivo *Master*
    - Fino a sette dispositivi *Slave*

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

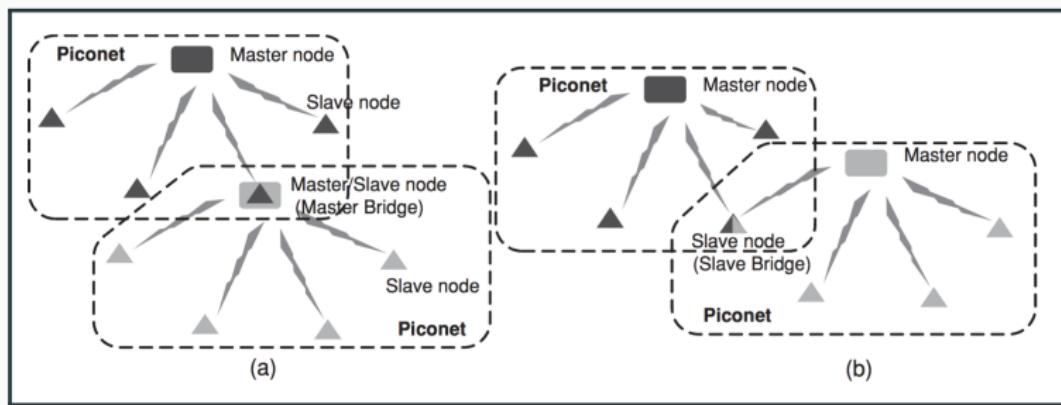
- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete
  - Piconet
    - Un dispositivo *Master*
    - Fino a sette dispositivi *Slave*
  - **Scatternet**

## Bluetooth

Inventato da Ericsson nel 1994, originariamente concepito come una alternativa senza fili ai cavi RS-232

- Tecnologia wireless progettata per collegare dispositivi mobili o fissi
  - Bassi consumi
  - Corto raggio d'azione
  - Basso costo di produzione per dispositivi compatibili
- Presenta due architetture di Rete
  - Piconet
    - Un dispositivo *Master*
    - Fino a sette dispositivi *Slave*
  - Scatternet
    - Un insieme di Piconet

## Bluetooth



## ZigBee & 6LoWPAN

Sono due tecnologie per Wireless Private Area Network (WPAN)

- Basso consumo

## ZigBee & 6LoWPAN

Sono due tecnologie per Wireless Private Area Network (WPAN)

- Basso consumo
- Alta flessibilit

## ZigBee & 6LoWPAN

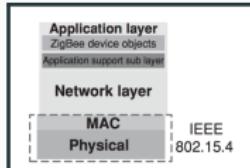
Sono due tecnologie per Wireless Private Area Network (WPAN)

- Basso consumo
- Alta flessibilit
- Bassi costi

## ZigBee

La prima specifica fu ratificata il 14 dicembre 2004. La ZigBee Alliance annuncia la disponibilità della specifica 1.0 il 13 giugno 2005

- *Application Support* e *Network Layer* sono definiti dalla ZigBee Alliance
- Un device può essere di due tipi
  - Full Function Device (FFD)
    - Coordinatore, Router, Device
    - Pu interagire sia con un FFD che con un RFD
  - Reduced Function Device (RFD)
    - Device
    - Pu interagire solo con un FFD

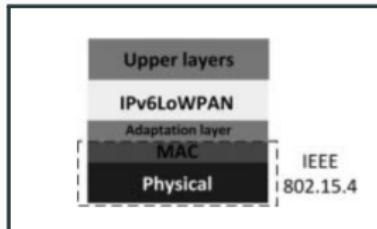


## 6LoWPAN

Il gruppo di lavoro IETF 6LoWPAN stato approvato nel marzo del 2005.

Nel 2009 la ZigBee Alliance ha annunciato l'integrazione di ZigBee con 6LoWPAN

- Consente l'invio e la ricezione di pacchetti *IPv6*
- E' stato inserito un Adaptation Layer per il collegamento tra lo strato *MAC* e il *Network Layer IPv6*



## WiMAX

Prima pubblicazione effettuata dal WiMAX Forum l'8 aprile del 2002 con lo standard IEEE 802.16-2001

## WiMAX

Prima pubblicazione effettuata dal WiMAX Forum l'8 aprile del 2002 con lo standard IEEE 802.16-2001

- Tecnologia wireless adatta a trasmissione sia di tipo urbano che rurale

## WiMAX

Prima pubblicazione effettuata dal WiMAX Forum l'8 aprile del 2002 con lo standard IEEE 802.16-2001

- Tecnologia wireless adatta a trasmissione sia di tipo urbano che rurale
- Implementa diverse tecniche di crittografia, sicurezza ed autenticazione

## WiMAX

Prima pubblicazione effettuata dal WiMAX Forum l'8 aprile del 2002 con lo standard IEEE 802.16-2001

- Tecnologia wireless adatta a trasmissione sia di tipo urbano che rurale
- Implementa diverse tecniche di crittografia, sicurezza ed autenticazione
- **Tecnica di Orthogonal Frequency Division Multiple Access (OFDMA)**

## WiMAX

Prima pubblicazione effettuata dal WiMAX Forum l'8 aprile del 2002 con lo standard IEEE 802.16-2001

- Tecnologia wireless adatta a trasmissione sia di tipo urbano che rurale
- Implementa diverse tecniche di crittografia, sicurezza ed autenticazione
- Tecnica di Orthogonal Frequency Division Multiple Access (OFDMA)
- Soddisfa varie specifiche imposte da una tipica Smart Grid

## WiMAX

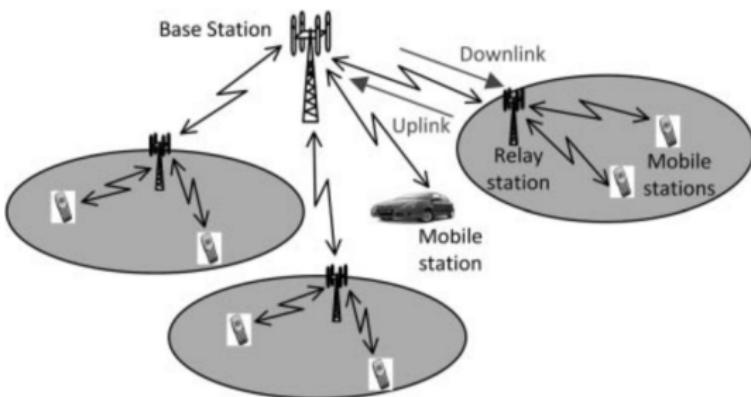


Figure 3.19 WiMax network

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid
- Trasporto informazioni su conduttori e linee elettriche

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid
- Trasporto informazioni su conduttori e linee elettriche
- Servizi di comunicazione per AMI e HAN

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid
- Trasporto informazioni su conduttori e linee elettriche
- Servizi di comunicazione per AMI e HAN

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid
- Trasporto informazioni su conduttori e linee elettriche
- Servizi di comunicazione per AMI e HAN

*In una tipica rete PLC, gli smart meter sono collegati al data concentrator attraverso power line e i dati vengono trasferiti al data center tramite tecnologie di rete cellulare*

## Power Line Communication

I primi standard sono stati progettati nel 2001 dalla Homeplug Powerline Alliance

- Tecnologia di rete proposta per la trasmissione in ambiente Smart Grid
- Trasporto informazioni su conduttori e linee elettriche
- Servizi di comunicazione per AMI e HAN

*In una tipica rete PLC, gli smart meter sono collegati al data concentrator attraverso power line e i dati vengono trasferiti al data center tramite tecnologie di rete cellulare*

## Problema

Presenza di disturbi che possono corrompere le informazioni, non garantendo più la continuità del servizio

# standard e tecnologie: sommario

---

- Tecnologie di comunicazione
  - IEEE 802
    - Ethernet
    - Wireless
    - Bluetooth
    - ZigBee & 6LoWPAN
    - WiMAX
  - Power Line Communication
- Standard per lo scambio di informazioni
  - Modbus
  - ISO/IEC 61850
- Standard per la sicurezza
  - ISO/IEC 62351

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona
- Automazione delle substation

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona
- Automazione delle substation
- Comunicazione

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona
- Automazione delle substation
- Comunicazione
  - Master  $\xrightarrow{\text{query}}$  Slave/broadcast

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona
- Automazione delle substation
- Comunicazione
  - Master  $\xrightarrow{\text{query}}$  Slave/broadcast
  - Slave (monitoring delle *query*)

# standard per lo scambio di informazioni

## Modbus

Protocollo creato nel 1979 da Modicon (azienda ora parte del gruppo Schneider Electric)

- Protocollo di messaggistica (*Application Layer*)
- Dispositivi collegati su diversi bus e reti
- Ethernet su fibra ottica con trasmissione seriale asincrona
- Automazione delle substation
- Comunicazione
  - Master  $\xrightarrow{\text{query}}$  Slave/broadcast
  - Slave (monitoring delle *query*)
  - Slave  $\xrightarrow{\text{trigger}}$  azione

standard per lo scambio di informazioni

## ISO/IEC 61850

Un gruppo IEC di 60 membri si è diviso in 3 gruppi di lavoro per la creazione di ISO/IEC 61850 nel 1995

# standard per lo scambio di informazioni

## ISO/IEC 61850

Un gruppo IEC di 60 membri si è diviso in 3 gruppi di lavoro per la creazione di ISO/IEC 61850 nel 1995

- Progettazione dei sistemi di automazione per le substation

# standard per lo scambio di informazioni

## ISO/IEC 61850

Un gruppo IEC di 60 membri si è diviso in 3 gruppi di lavoro per la creazione di ISO/IEC 61850 nel 1995

- Progettazione dei sistemi di automazione per le substation
- Sovrastruttura che coordina e gestisce protocolli e tecnologie esistenti

# standard per lo scambio di informazioni

## ISO/IEC 61850

Un gruppo IEC di 60 membri si è diviso in 3 gruppi di lavoro per la creazione di ISO/IEC 61850 nel 1995

- Progettazione dei sistemi di automazione per le substation
- Sovrastruttura che coordina e gestisce protocolli e tecnologie esistenti
- Garantisce interoperabilità

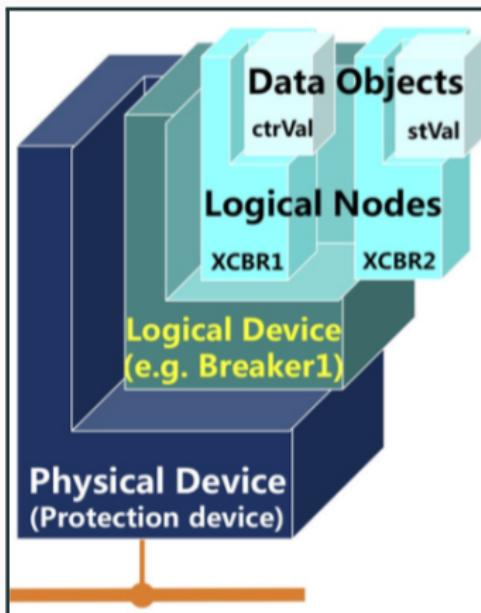
## ISO/IEC 61850

### Vantaggi

- Coordina la complessità di unità indipendenti
- Si integra con sistemi preinstallati in rete
- Scalabile e facilita integrazione
- Si basa su standard esistenti
- Supporta i *self descriptive device*
- Si basa su *data object*
- Estensibile e flessibile
- Si adatta rapidamente alla configurazione del sistema

standard per lo scambio di informazioni

## ISO/IEC 61850 Device Model



standard per lo scambio di informazioni

---

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione
  - Substation Configuration Language (SCL)

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione
  - Substation Configuration Language (SCL)
    - + Interoperabilità tra IED

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione
  - Substation Configuration Language (SCL)
    - + Interoperabilità tra IED
    - + Configurazione automatica

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione
  - Substation Configuration Language (SCL)
    - + Interoperabilità tra IED
    - + Configurazione automatica
    - + Riduzione della presenza di errori

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

- Oggetti e servizi astratti di comunicazione
- Abstract Communication Service Interface (ACSI)
  - Oggetti e servizi implementati attraverso il protocollo Manufacturing Message Specification (MMS)
- Linguaggio comune di configurazione per astrazione e standardizzazione
  - Substation Configuration Language (SCL)
    - + Interoperabilità tra IED
    - + Configurazione automatica
    - + Riduzione della presenza di errori
  - Ogni IED presenta un file SCL che ne definisce la configurazione

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

- Generic Substation Event (GSE)

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

- Generic Substation Event (GSE)
  - Generic Object Oriented Substation Event (GOOSE)

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

- Generic Substation Event (GSE)
  - Generic Object Oriented Substation Event (GOOSE)
  - Generic Substation State Event (GSSE)

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

- Generic Substation Event (GSE)
  - Generic Object Oriented Substation Event (GOOSE)
  - Generic Substation State Event (GSSE)
- Sampled Measured Values (SMV)

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

- Generic Substation Event (GSE)
  - Generic Object Oriented Substation Event (GOOSE)
  - Generic Substation State Event (GSSE)
- Sampled Measured Values (SMV)
- Time Synchronization

# standard per lo scambio di informazioni

---

## ISO/IEC 61850

Lo standard si serve dei seguenti strumenti per la gestione delle informazioni

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

# standard e tecnologie: sommario

---

- Tecnologie di comunicazione
  - IEEE 802
    - Ethernet
    - Wireless
    - Bluetooth
    - ZigBee & 6LoWPAN
    - WiMAX
  - Power Line Communication
- Standard per lo scambio di informazioni
  - Modbus
  - ISO/IEC 61850
- Standard per la sicurezza
  - ISO/IEC 62351

## I problemi relativi alla sicurezza

- Accessi non autorizzati a informazioni recuperate dagli smart meter
- Spegnimento di dispositivi
- Attacco alla Smart Grid per causare un'interruzione al regolare passaggio di corrente

# standard per la sicurezza

## I problemi relativi alla sicurezza

- Accessi non autorizzati a informazioni recuperate dagli smart meter
- Spegnimento di dispositivi
- Attacco alla Smart Grid per causare un'interruzione al regolare passaggio di corrente

## I problemi relativi alla privacy

- Alta frequenza di letture per misurare il consumo energetico
- + Si cerca di aggregare le informazioni per mascherare i singoli consumi dei meter

standard per la sicurezza

## ISO/IEC 62351

Standard sviluppato nel 1999 dal WG15 facente parte della TC57  
dell'organo internazionale IEC

# standard per la sicurezza

## ISO/IEC 62351

Standard sviluppato nel 1999 dal WG15 facente parte della TC57 dell'organo internazionale IEC

### Obiettivi di sicurezza

- Autenticazione nel processo di trasferimento di dati tramite firma digitale
- Garanzia di accessi esclusivamente dopo autenticazione
- Prevenzione dell'**eavesdropping**
- Prevenzione da attacchi di **playback** e attacchi di **spoofing**
- Rilevamento delle intrusioni

standard per la sicurezza

## ISO/IEC 62351

E'suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues

standard per la sicurezza

## ISO/IEC 62351

E'suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms

# standard per la sicurezza

## ISO/IEC 62351

E'suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP

standard per la sicurezza

## ISO/IEC 62351

E' suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP
4. **Profiles including MMS**

standard per la sicurezza

## ISO/IEC 62351

E'suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP
4. Profiles including MMS
5. Security for IEC 60870-5 and derivatives

standard per la sicurezza

## ISO/IEC 62351

E' suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP
4. Profiles including MMS
5. Security for IEC 60870-5 and derivatives
6. **Security for IEC 61850**

standard per la sicurezza

## ISO/IEC 62351

E' suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP
4. Profiles including MMS
5. Security for IEC 60870-5 and derivatives
6. Security for IEC 61850
7. Network and system management (NSM) data object models

# standard per la sicurezza

## ISO/IEC 62351

E' suddiviso in 8 parti:

1. Communication network and system security - Introduction to security issues
2. Glossary of terms
3. Communication network and system security - Profiles including TCP/IP
4. Profiles including MMS
5. Security for IEC 60870-5 and derivatives
6. Security for IEC 61850
7. Network and system management (NSM) data object models
8. Role-Based access control

principali vulnerabilità delle smart grid:  
attacchi e contromisure

---

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità computazione e comunicazione

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità computazione e comunicazione
- Dispositivi non critici e disconnessi

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità computazione e comunicazione
- Dispositivi non critici e disconnessi
  - Connessi → Dati PROCESS-CRITICAL

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità computazione e comunicazione
- Dispositivi non critici e disconnessi
  - Connessi → Dati PROCESS-CRITICAL
- Anello debole della catena

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità di computazione e comunicazione
- Dispositivi non critici e disconnessi
  - Connessi → Dati PROCESS-CRITICAL
- Anello debole della catena
  - Smart Meter

# principali vulnerabilità delle smart grid: attacchi e contromisure

---

- Digitalizzazione delle infrastrutture critiche
  - Aggiunta capacità computazione e comunicazione
- Dispositivi non critici e disconnessi
  - Connessi → Dati PROCESS-CRITICAL
- Anello debole della catena
  - Smart Meter
- Nuova sfida per i produttori

# principali vulnerabilità delle smart grid: sommario

---

- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- Disconnect Attack
- Jamming

# principali vulnerabilità delle smart grid: sommario

---

- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- Disconnect Attack
- Jamming

## Smart Devices

- Dispositivi capaci di computare e comunicare
- Godono di tutte le feature di un tipico dispositivo connesso alla rete
- Possono essere soggetti ad attacchi

## Institute for Security and Open Methodologies (ISECOM)

### Open Source Security Testing Methodology Manual (OSSTMM)

- Information Security
- Process Security
- **Internet Technology Security**
- Communications Security
- Wireless Security
- Physical Security

## Internet Technology Security

- Penetration Testing

## Internet Technology Security

- Penetration Testing
  - Kali Linux

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing
  - Nmap

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing
  - Nmap
- Internet Application Testing

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing
  - Nmap
- Internet Application Testing
  - Nessus

## Internet Technology Security

- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing
  - Nmap
- Internet Application Testing
  - Nessus
- Exploit Testing

## Internet Technology Security

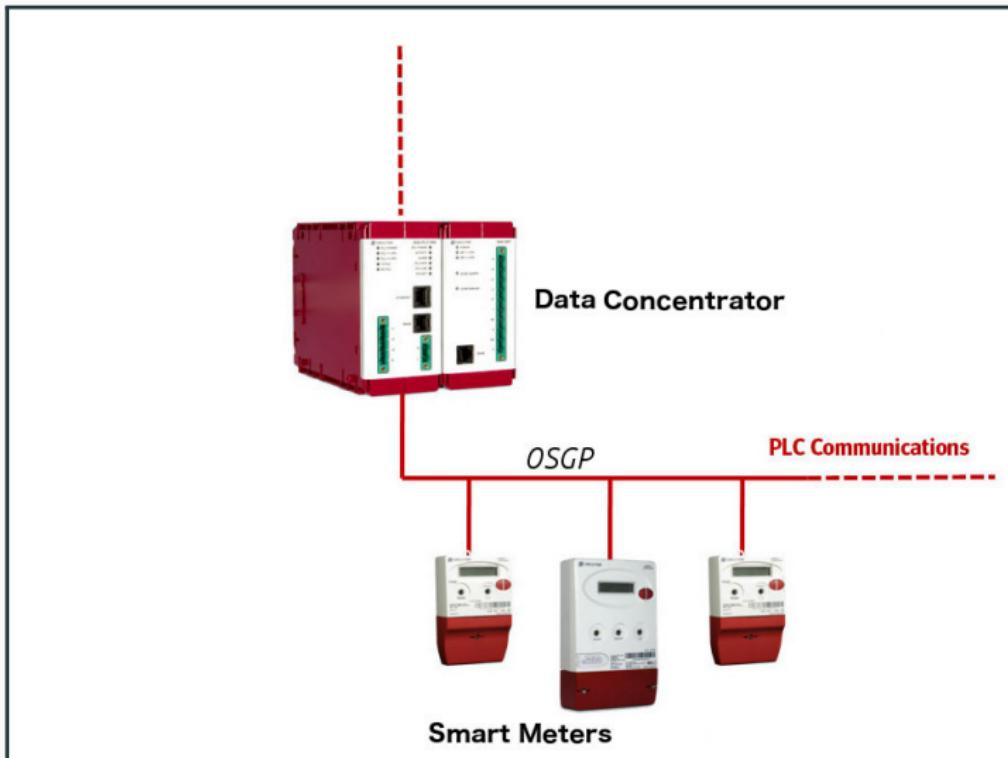
- Penetration Testing
  - Kali Linux
- Network Surveying
  - Wireshark
- Port Scanning, Services/System Identification, DoS Testing
  - Nmap
- Internet Application Testing
  - Nessus
- Exploit Testing
  - Metasploit

# principali vulnerabilità delle smart grid: sommario

---

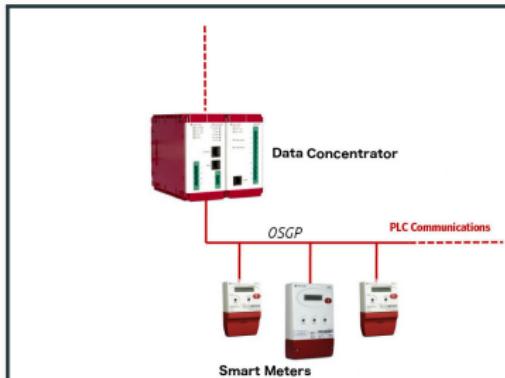
- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- Disconnect Attack
- Jamming

# principali vulnerabilità delle smart grid: comunicazione tra data aggregator e smart meter



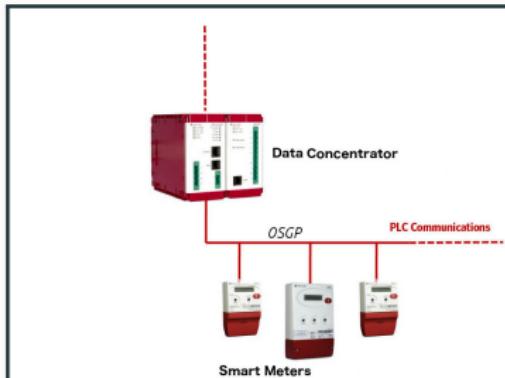
# principali vulnerabilità delle smart grid: open smart grid protocol

- Sviluppato da European Telecommunications Standards Institute (ETSI), 2011



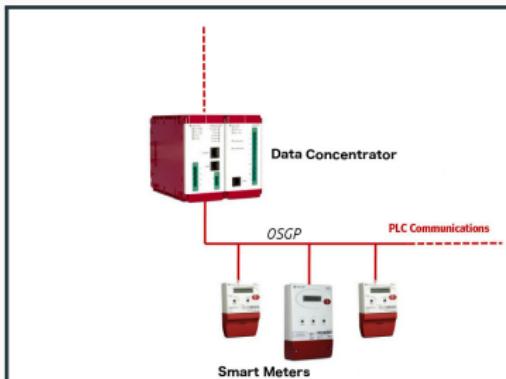
# principali vulnerabilità delle smart grid: open smart grid protocol

- Sviluppato da European Telecommunications Standards Institute (ETSI), 2011
- Comunicazione su Powerline tra Data Concentrator (Aggregatore) e Smart meter



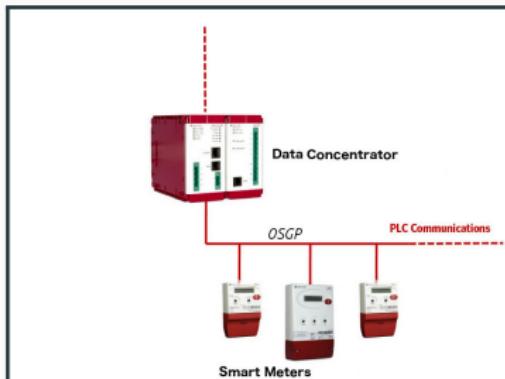
# principali vulnerabilità delle smart grid: open smart grid protocol

- Sviluppato da European Telecommunications Standards Institute (ETSI), 2011
- Comunicazione su Powerline tra Data Concentrator (Aggregatore) e Smart meter
  - Protocollo Master-Slave: Master (Aggregatore) - Slave (Smart Meter)



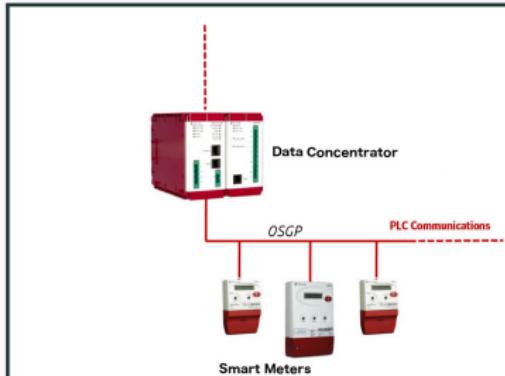
# principali vulnerabilità delle smart grid: open smart grid protocol

- Sviluppato da European Telecommunications Standards Institute (ETSI), 2011
- Comunicazione su Powerline tra Data Concentrator (Aggregatore) e Smart meter
  - Protocollo Master-Slave: Master (Aggregatore) - Slave (Smart Meter)
  - Ogni Aggregatore ha una zona di competenza a cui afferisce un certo numero di Smart Meter



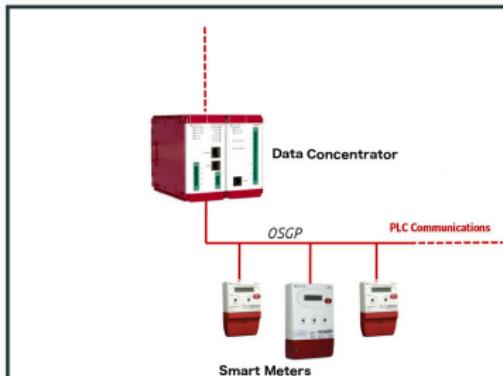
# principali vulnerabilità delle smart grid: open smart grid protocol

- Fornisce meccanismi per proteggere la *privacy* dei clienti



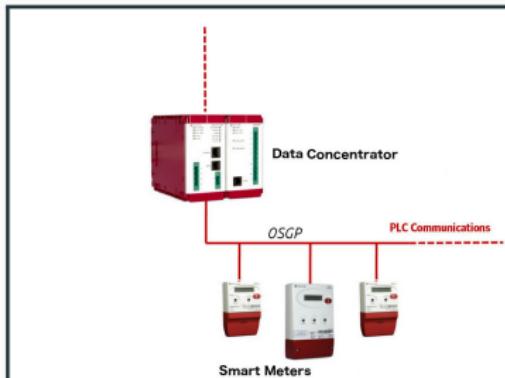
# principali vulnerabilità delle smart grid: open smart grid protocol

- Fornisce meccanismi per proteggere la *privacy* dei clienti
  - Restringendo l'accesso ai dati e cifrandoli evitando accessi non autorizzati



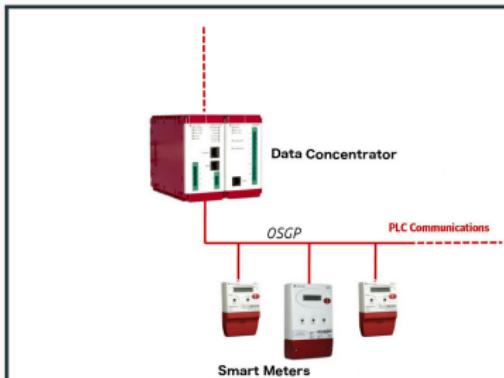
# principali vulnerabilità delle smart grid: open smart grid protocol

- Fornisce meccanismi per proteggere la *privacy* dei clienti
  - Restringendo l'accesso ai dati e cifrandoli evitando accessi non autorizzati
- Costruito sullo stack protocollare ISO/IEC 14908-1



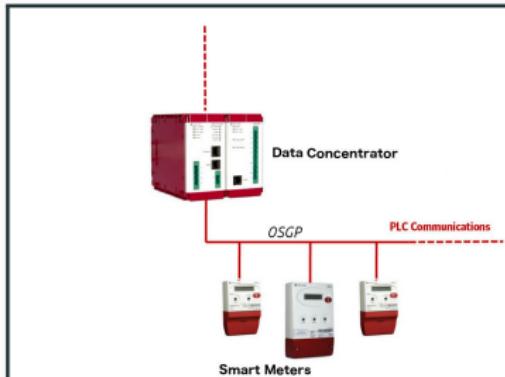
# principali vulnerabilità delle smart grid: open smart grid protocol

- Fornisce meccanismi per proteggere la *privacy* dei clienti
  - Restringendo l'accesso ai dati e cifrandoli evitando accessi non autorizzati
- Costruito sullo stack protocollare ISO/IEC 14908-1
  - Fornisce servizi di autenticazione ma non garantisce *confidentiality* dei dati



# principali vulnerabilità delle smart grid: open smart grid protocol

- Fornisce meccanismi per proteggere la *privacy* dei clienti
  - Restringendo l'accesso ai dati e cifrandoli evitando accessi non autorizzati
- Costruito sullo stack protocollare ISO/IEC 14908-1
  - Fornisce servizi di autenticazione ma non garantisce *confidentiality* dei dati
- Migliora la sicurezza aggiungendo un proprio *security layer*



# principali vulnerabilità delle smart grid: open smart grid protocol

---

## Fasi del protocollo OSGP

- Setup
- Communication with Authenticated Encryption

# principali vulnerabilità delle smart grid: open smart grid protocol

---

## Fasi del protocollo OSGP

- Setup
- Communication with Authenticated Encryption

## principali vulnerabilità delle smart grid: osgp - setup

---

- Processo di produzione del device OSGP

## principali vulnerabilità delle smart grid: osgp - setup

---

- Processo di produzione del device OSGP
  - Il dispositivo configurato con una Open Media Access Key (OMAK) univoca a 96 bit

## principali vulnerabilità delle smart grid: osgp - setup

---

- Processo di produzione del device OSGP
  - Il dispositivo configurato con una Open Media Access Key (OMAK) univoca a 96 bit
- La chiave OMAK del device consegnata alla società di servizi

## principali vulnerabilità delle smart grid: osgp - setup

---

- Processo di produzione del device OSGP
  - Il dispositivo configurato con una Open Media Access Key (OMAK) univoca a 96 bit
- La chiave OMAK del device consegnata alla società di servizi
- La società di servizi provvede a dotare il proprio Data Concentrator della chiave OMAK del dispositivo afferente alla zona di competenza

## principali vulnerabilità delle smart grid: osgp - setup

---

- Il Data Concentrator in grado di rilevare ogni dispositivo a lui afferente grazie ad un processo di discovery

## principali vulnerabilità delle smart grid: osgp - setup

---

- Il Data Concentrator è in grado di rilevare ogni dispositivo a lui afferente grazie ad un processo di discovery
- Il Data Concentrator genera ed invia la Shared Key relativa alla sua zona di competenza ad ogni nuovo dispositivo scoperto

## principali vulnerabilità delle smart grid: osgp - setup

---

- Il Data Concentrator è in grado di rilevare ogni dispositivo a lui afferente grazie ad un processo di discovery
- Il Data Concentrator genera ed invia la Shared Key relativa alla sua zona di competenza ad ogni nuovo dispositivo scoperto
  - Comunicazione cifrata utilizzando la OMAK del dispositivo

## principali vulnerabilità delle smart grid: osgp - setup

---

- Il Data Concentrator è in grado di rilevare ogni dispositivo a lui afferente grazie ad un processo di discovery
- Il Data Concentrator genera ed invia la Shared Key relativa alla sua zona di competenza ad ogni nuovo dispositivo scoperto
  - Comunicazione cifrata utilizzando la OMAK del dispositivo
- Ogni dispositivo rimpiazza la sua OMAK originaria con la Shared Key ricevuta

# principali vulnerabilità delle smart grid: open smart grid protocol

---

## Fasi del protocollo OSGP

- Setup
- Communication with Authenticated Encryption

# principali vulnerabilità delle smart grid: osgp - communication with authenticated encryption

---

- Comunicazione iniziata dal Data Concentrator (Master)

# principali vulnerabilità delle smart grid: osgp - communication with authenticated encryption

---

- Comunicazione iniziata dal Data Concentrator (Master)
- Data Concentrator invia messaggio di richiesta allo Smart Meter (Slave)

# principali vulnerabilità delle smart grid: osgp - communication with authenticated encryption

---

- Comunicazione iniziata dal Data Concentrator (Master)
- Data Concentrator invia messaggio di richiesta allo Smart Meter (Slave)
- Smart Meter decifra il messaggio, ne verifica l'autenticità e invia la risposta

# principali vulnerabilità delle smart grid: osgp - communication with authenticated encryption

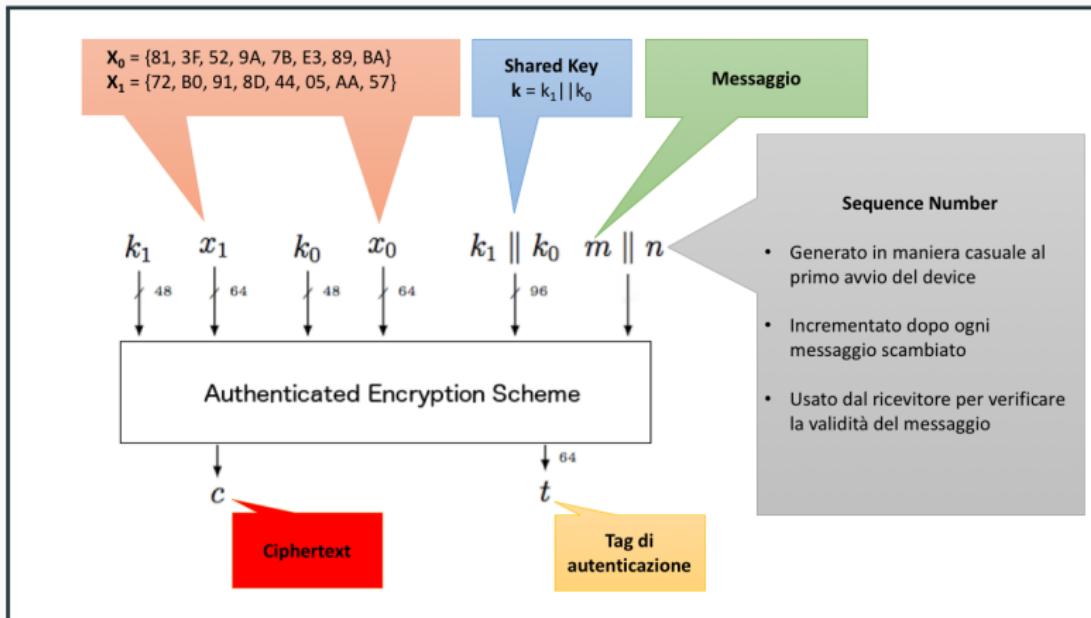
- Comunicazione iniziata dal Data Concentrator (Master)
- Data Concentrator invia messaggio di richiesta allo Smart Meter (Slave)
- Smart Meter decifra il messaggio, ne verifica l'autenticità e invia la risposta
- Richiesta e risposta cifrate con Shared Key

# principali vulnerabilità delle smart grid: osgp - communication with authenticated encryption

- Comunicazione iniziata dal Data Concentrator (Master)
- Data Concentrator invia messaggio di richiesta allo Smart Meter (Slave)
- Smart Meter decifra il messaggio, ne verifica l'autenticità e invia la risposta
- Richiesta e risposta cifrate con Shared Key
  - Smart Meter e Data Concentrator sono identificati dai campi Subnet e Node ID del pacchetto di richiesta/risposta

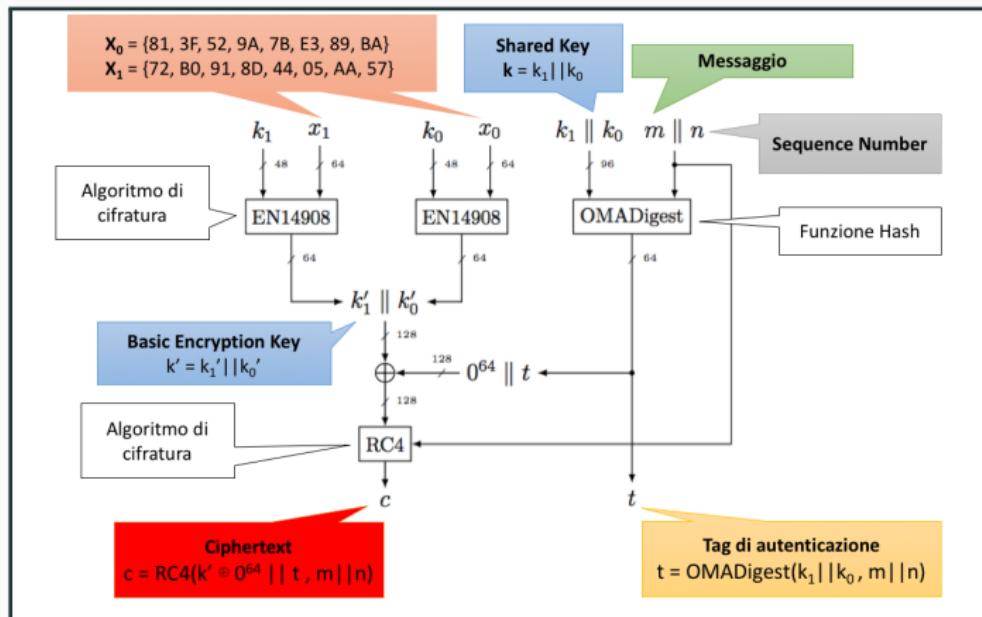
# principali vulnerabilità delle smart grid: osgp - authenticated encryption scheme

## Schema di cifratura



# principali vulnerabilità delle smart grid: osgp - authenticated encryption scheme

## Schema di cifratura



# principali vulnerabilità delle smart grid: sommario

- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- Disconnect Attack
- Jamming

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- **Manomettere le misure**

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - **Frode**

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile
- *Stealth Bad Data Injection*

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile
- *Stealth Bad Data Injection*
  - Non rilevabile

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile
- *Stealth Bad Data Injection*
  - Non rilevabile
  - Necessaria conoscenza della topologia

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile
- *Stealth Bad Data Injection*
  - Non rilevabile
  - Necessaria conoscenza della topologia
  - Possibile inferire i parametri legati alla topologia

# principali vulnerabilità delle smart grid: false data injection

- Scambio informazioni stato
- Stima dello stato → Modello *real-time*
- Manomettere le misure
  - Frode
  - Sovraccaricare l'infrastruttura
  - Manipolare prezzi di mercato
- *Bad Data Injection*
  - Rilevabile
- *Stealth Bad Data Injection*
  - Non rilevabile
  - Necessaria conoscenza della topologia
  - Possibile inferire i parametri legati alla topologia
    - *Linear Independent Component Analysis*

# principali vulnerabilità delle smart grid: attacchi e contromisure

## Modello Matematico

### Vettore delle misurazioni

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$$

- $\mathbf{h}(\mathbf{x})$ : relazione non lineare tra le misure  $\mathbf{z}$  e lo stato del sistema  $\mathbf{x}$
- $\mathbf{e} = [e_1, \dots, e_m]^T$ , rumore Gaussiano delle misure

# principali vulnerabilità delle smart grid: attacchi e contromisure

## Modello Matematico

### Vettore delle misurazioni

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$$

- $\mathbf{h}(\mathbf{x})$ : relazione non lineare tra le misure  $\mathbf{z}$  e lo stato del sistema  $\mathbf{x}$
- $\mathbf{e} = [e_1, \dots, e_m]^T$ , rumore Gaussiano delle misure

### Modello di approssimazione lineare della misura di corrente

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

- Vettore di stato stimato:  $\hat{\mathbf{x}} = (\mathbf{H}^T \sum_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \sum_e^{-1} \mathbf{z}$
- $\mathbf{H} \in \mathbb{R}$ , definito come
  - $\mathbf{H} = \frac{\partial \mathbf{h}(\mathbf{x})}{\partial \mathbf{x}}|_{\mathbf{x}=0}$
  - Matrice di covarianza  $\Sigma_e$

# principali vulnerabilità delle smart grid: attacchi e contromisure

## Modello Matematico

- Bad Data Injection
  - Misura sotto attacco non stealth:  $\mathbf{z}' = \mathbf{H}(\mathbf{x}) + \mathbf{b} + \mathbf{e}$
  - Vettore residuo:  $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$
  - Rilevamento bad data:  $\max_i(|\mathbf{r}_i|/\sqrt{\text{cov}(\mathbf{r})}) \geq \gamma$
- Stealth Bad Data Injection
  - Misura sotto attacco stealth:  $\mathbf{z}' = \mathbf{H}(\mathbf{x} + \delta\mathbf{x}) + \mathbf{e}$
  - Non rilevabile usando meccanismi a soglia

---

$\mathbf{H}(\mathbf{x})$  e  $\mathbf{H}(\mathbf{x} + \delta\mathbf{x})$  sono prodotti *matrice*  $\times$  *vettore*

# principali vulnerabilità delle smart grid: sommario

- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- **Disconnect Attack**
- Jamming

## principali vulnerabilità delle smart grid: disconnect attack

- Remote Connect Disconnect (RCD)

## principali vulnerabilità delle smart grid: disconnect attack

- Remote Connect Disconnect (RCD)
- Attacco RCD → Blackout/Danni alla rete

## principali vulnerabilità delle smart grid: disconnect attack

- Remote Connect Disconnect (RCD)
- Attacco RCD → Blackout/Danni alla rete
- Difesa: ritardi casuali nell'esecuzione dei comandi RCD

## principali vulnerabilità delle smart grid: disconnect attack

- Remote Connect Disconnect (RCD)
- Attacco RCD → Blackout/Danni alla rete
- Difesa: ritardi casuali nell'esecuzione dei comandi RCD
  - Prevenire rapidi cambiamenti del carico elettrico

## principali vulnerabilità delle smart grid: disconnect attack

- Remote Connect Disconnect (RCD)
- Attacco RCD → Blackout/Danni alla rete
- Difesa: ritardi casuali nell'esecuzione dei comandi RCD
  - Prevenire rapidi cambiamenti del carico elettrico
  - Tempo per rilevare e fermare un attacco in corso

# principali vulnerabilità delle smart grid: sommario

- Security Testing
- Open Smart Grid Protocol
- False Data Injection
- Disconnect Attack
- Jamming

## principali vulnerabilità delle smart grid: jamming

Strategia d'attacco utilizzata per la manipolazione del mercato elettrico

# principali vulnerabilità delle smart grid: jamming

Strategia d'attacco utilizzata per la manipolazione del mercato elettrico

## Assunzione

Si utilizza un sistema di comunicazione wireless, come **WiMAX**, per effettuare il broadcast delle informazioni relative ai prezzi

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata
2. L'utente rimane a conoscenza del vecchio prezzo della corrente

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata
2. L'utente rimane a conoscenza del vecchio prezzo della corrente
3. L'attaccante monitora il mercato elettrico

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata
2. L'utente rimane a conoscenza del vecchio prezzo della corrente
3. L'attaccante monitora il mercato elettrico
4. Quando il prezzo cambia significativamente, si smette di fare Jamming

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata
2. L'utente rimane a conoscenza del vecchio prezzo della corrente
3. L'attaccante monitora il mercato elettrico
4. Quando il prezzo cambia significativamente, si smette di fare Jamming
5. Ogni utente adatta il proprio consumo energetico in base al nuovo prezzo

# principali vulnerabilità delle smart grid: jamming

## Attacco

[Li, Husheng, and Zhu Han. "Manipulating the electricity power market via jamming the price signaling in smart grid." *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.]

1. L'attaccante fa Jamming in un'area molto popolata
2. L'utente rimane a conoscenza del vecchio prezzo della corrente
3. L'attaccante monitora il mercato elettrico
4. Quando il prezzo cambia significativamente, si smette di fare Jamming
5. Ogni utente adatta il proprio consumo energetico in base al nuovo prezzo
6. L'attaccante può avere profitti da questa manipolazione del mercato

# principali vulnerabilità delle smart grid: jamming

## Contromisure

Evitare di modificare il consumo di energia in maniera simultanea.

**IDEA:** si utilizza uno schema di backoff

# principali vulnerabilità delle smart grid: jamming

## Contromisure

Evitare di modificare il consumo di energia in maniera simultanea.

**IDEA: si utilizza uno schema di backoff**

Ogni consumer sceglie un tempo casuale per cambiare la propria power response evitando che l'attaccante possa predire il comportamento dell'utente e quindi capire in che modo varia il prezzo della corrente

grazie per l'attenzione!

---