# ENERGY CYBERSECURITY REPORT 2018

## I rischi derivanti dalla digitalizzazione della filiera elettrica e gli strumenti a disposizione delle imprese

Luglio 2018

POLITECNICO
MILANO 1863

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

energystrategy.it

# Indice

# Introduzione

La digitalizzazione è un fenomeno pervasivo e inarrestabile che sta modificando in modo "epocale" interi settori economici, generando processi di innovazione più o meno radicale di processi e prodotti, abilitando nuove funzionalità e servizi, dando luogo a nuovi business model e nuovi scenari competitivi.

Ma, come sempre accade nel caso di cambiamenti del contesto, la digitalizzazione crea opportunità, ma anche rischi. Tra quest'ultimi vi sono quelli derivanti dalle minacce che arrivano dal cyberspazio, ovvero dal dominio virtuale delle tecnologie ICT.

Tutto questo vale anche per il settore energetico: la filiera elettrica, in particolare, è caratterizzata da trasformazioni importanti, derivanti da fenomeni quali la diffusione delle fonti rinnovabili, la generazione distribuita, le smart grid e, più in generale, le innovazioni legate all'introduzione di tecnologie digitali per la gestione delle attività "core" ai vari stadi della filiera (dalla produzione al consumo). Tutto questo ha però comportato però una crescente interconnessione digitale che, unitamente al vertiginoso aumento del numero di attori operanti in alcuni stadi della filiera, ha esponenzialmente aumentato il rischio di attacchi di natura informatica che hanno come obiettivo le attività operative. Ne deriva quindi la necessità per le imprese di adottare opportune contromisure di natura tecnologica e organizzativa, e, più in generale, di dotarsi di un adeguato sistema di governance della cybersecurity anche in ambito industriale. Considerata l'importanza strategica del comparto

(non a caso la rete elettrica è annoverata tra le "infrastrutture critiche" del Paese), in questo processo un ruolo importante è ricoperto dalle istituzioni, che possono imporre l'adozione di determinate misure o standard di sicurezza, ma anche prevedere opportuni meccanismi di coordinamento e cooperazione tra i vari operatori del comparto (a livello nazionale e internazionale).

Il primo Report sull'Energy Cybersecurity si propone di approfondire questo tema, evidenziando i nuovi rischi e i potenziali impatti per le imprese della filiera, facendo il quadro sul contesto di riferimento (in termini di quadro regolatorio e di iniziative in corso a livello nazionale), e analizzando le soluzioni adottabili dalle imprese, con un focus particolare sull'evoluzione degli standard di riferimento. L'ultima parte dell'indagine si focalizza sugli end-user di natura industriale, con l'obiettivo di valutare il livello di consapevolezza delle imprese sui rischi legati alla digitalizzazione.

Ne emerge un quadro in evoluzione, caratterizzato al momento ancora da grandi differenze. I grandi operatori che operano ai vari stadi della filiera sembrano essere molto più strutturati (nonché spesso direttamente coinvolti nei vari gruppi di lavoro nazionali e internazionali), mentre la sensibilità dei piccoli operatori (soprattutto nell'ambito della generazione distribuita) appare ancora piuttosto limitata, così come vi è ancora una scarsa consapevolezza dei rischi da parte degli end-user industriali (sia consumatori che prosumer). Un panorama che è fonte di qualche preoccupazione, soprattutto alla luce degli sviluppi previsti dalla SEN, che prevede un ulteriore incremento del peso

delle fonti rinnovabili e una transizione sempre più marcata verso le generazione distribuita, nonché della crescente diffusione delle tecnologie digitali a tutti gli stadi della filiera.

L'Energy Cybersecurity è il terzo dei Rapporti di ricerca del 2018. Dopo la pausa estiva sarà il turno della mobilità elettrica, e, a seguire, della digital energy e della gestione dell'acqua. Ulteriori importanti occasioni di incontro e di dibattito sui temi cari alla community di Energy & Strategy.

**Umberto Bertelè**
*School of Management - Politecnico di Milano*

**Vittorio Chiesa**
*Direttore Energy & Strategy Group*

# Executive Summary

La sicurezza dei dati immagazzinati e comunicati tramite le infrastrutture informatiche è da tempo un tema di grande attualità, sia dal punto di vista della privacy, sia da quella della protezione dei dati «mission critical».

In un mondo sempre più interconnesso, le minacce provengono dalle fonti più disparate (e più remote), e gli autori degli attacchi sono sempre più difficili da individuare. Si parla in questo senso di **cyberspazio** e di **cybersecurity.**

La cybersecurity può quindi essere intesa come:

L'insieme di **strumenti, procedure e sistemi** che consente a una entità (ad esempio, una nazione, una organizzazione, un cittadino)...

**...la protezione dei propri asset fisici** e della **confidenzialità, integrità e disponibilità delle proprie informazioni** attraverso un'attività di **prevenzione, rilevazione e risposta** agli attacchi provenienti **dal «cyberspazio»**

Il concetto di cybersecurity, pertanto, tende a includere gli ambiti tipici dell'**ICT security** (ovvero la protezione dei dati – sia all'interno dei database che nell'ambito dei flussi di comunicazione sulle reti informatiche), ma include anche la protezione degli **asset fisici**.

Gli attacchi provenienti dal cyberspazio che un'impresa si trova a dover fronteggiare sono tipicamente perpetrati da **soggetti** molto diversi:

- Hacker «isolati»

- Organizzazioni terroristiche
- Nazioni
- Concorrenti
- Business partners (fornitori di prodotti/servizi)
- Dipendenti

Va precisato che in taluni casi questi soggetti rappresentano i **«mandanti»** dell'operazione, mentre in altri si tratta di **esecutori**. Va inoltre sottolineato che alcuni di tali soggetti possono essere dei «veicoli» involontari (una sorta di «portatori sani di infezione»). E' il caso tipicamente dei dipendenti e di alcuni business partners (consulenti IT, revisori contabili, ecc), i quali hanno maggiore probabilità di accedere ai sistemi informativi aziendali (e di connettersi alle reti LAN) e possono contribuire ad «aggirare» le difese perimetrali e contribuire al successo di un attacco, qualora non rispettino le policy e le precauzioni dovute nell'espletamento delle loro attività (es: credenziali condivise, PC/USB pen infette, ecc).

Anche le finalità di un attacco possono essere molteplici. Tipicamente sono riconducibili a tre macro-obiettivi, illustrati nella figura a pagina seguente.

**Perché uno studio sul settore energetico?**

Il settore dell'energia (e in particolare la filiera elettrica) è caratterizzato da trend innovativi che ne stanno aumentando la possibile esposizione ad attacchi cibernetici. Si fa riferimento in particolare:

- al crescente peso del peso delle **fonti rinnovabili**
- alla diffusione del modello **«prosumer»**
- all'impatto della **digitalizzazione** (cioè del crescente uso di tecnologie ICT per gestire tutte le attività della

| AMBITO | DESCRIZIONE | FINALITA'/ DETERMINANTI |
|---|---|---|
| **CYBER CRIME** | **Atti criminali** commessi **usando sistemi informativi o reti di comunicazione elettroniche** al fine di perseguire vantaggi di tipo economico | Economiche |
| **CYBER TERRORISM** | **Attacchi** che, attraverso l'utilizzo e lo sfruttamento di computer o reti di comunicazione, sono **volti** a generare incidenti tali da **generare paura o danni** nei soggetti «target» | Ideologiche |
| **CYBER WARFARE** | **Attacchi**, che sfruttando computer o le reti di comunicazione, sono **volti a danneggiare gli asset fisici o digitali di una nazione al fine di comprometterne l'operatività** | Politiche/ Militari |

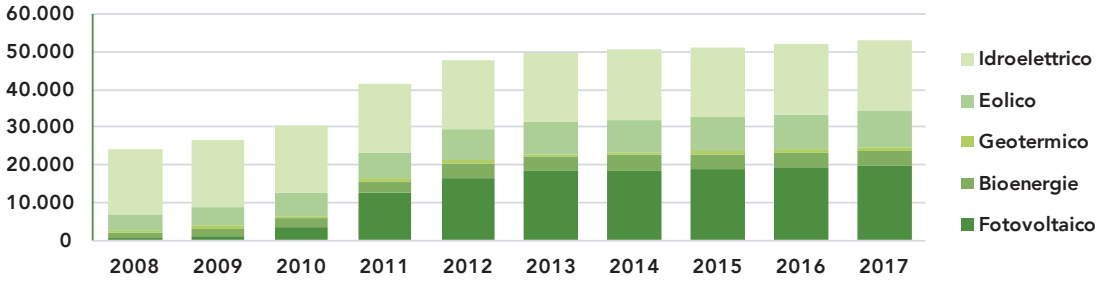
catena del valore dei vari operatori della filiera - la cosiddetta «digital energy»).

Come si può notare, i primi due trend sono peculiari della fase di produzione dell'energia elettrica, mentre la digitalizzazione ha un impatto sicuramente più pervasivo all'interno della filiera, anche se vi sono ovviamente dei legami tra i vari trend (es: la generazione distribuita è resa possibile dalle tecnologie di gestione «intelligente» della rete).

In particolare, la potenza installata da **fonti rinnovabili** ha raggiunto nel 2017 i **53 GW**, contribuendo a coprire il **36,2%** della produzione annua (pari 103,4 TWh). In base alle previsioni contenute nel documento che illustra la **Strategia Elettrica Nazionale**, tale percentuale dovrebbe salire al **60%** entro il 2030 (per un valore pari a 184 TWh).

La diffusione degli impianti di produzione da fonti rinnovabili comporta un vertiginoso **incremento del numero di impianti** di generazione (parchi fotovoltatici, eolici, ecc), cui corrisponde anche un significativo numero di **nuovi entranti** nel settore (tipicamente con scarsa esperienza e ridotta conoscenza dei rischi di natura «cyber»).

Similmente, la nascita dei **«prosumer»** (ovvero di imprese industriali, attività commerciali, famiglie che ricoprono il duplice ruolo di generatori e consumatori di energia) aumenta in modo esponenziale **il nu-**



**mero di attori connessi alla rete** in qualità di produttori (sebbene di piccola/piccolissima taglia). Aumenta di conseguenza la cosiddetta **«superficie d'attacco»**, cioè la probabilità che attacchi (soprattutto se di tipo «phishing») vadano a buon fine.

La **digitalizzazione** della filiera (la cosiddetta «digital energy») coinvolge invece tutti gli attori della filiera, e costituisce tipicamente un abilitatore di nuove funzionalità e di nuovi servizi per i vari attori operanti all'interno della filiera elettrica. Tra gli effetti più significativi è possibile annoverare:

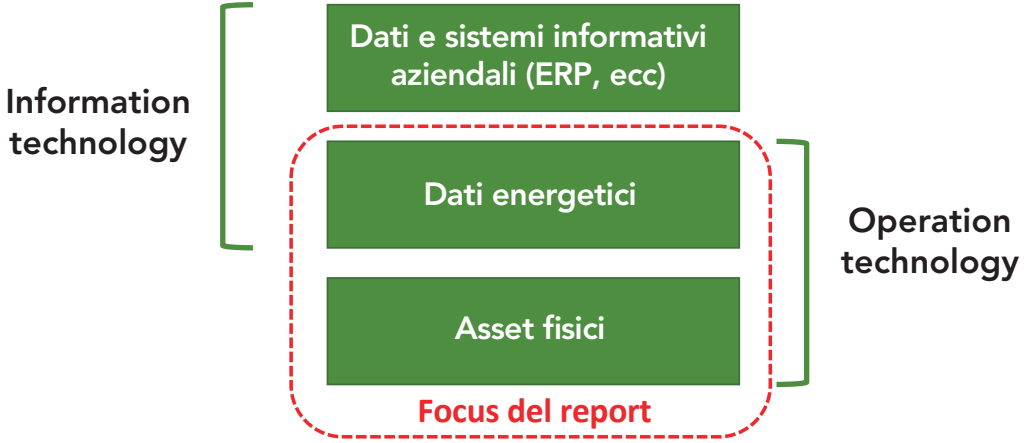
- lo sviluppo delle **«smart grid»**, ovvero delle reti «intelligenti» (fondamentali peraltro nel passaggio al modello di generazione distribuita tipico delle rinnovabili)
- nella fase di **generazione**, la possibilità di introdurre strumenti di **stima della produzione** di energia (particolarmente importanti nel caso degli impianti a fonte rinnovabile), di ottimizzazione delle attività di produzione (grazie a funzionalità di telemonitoraggio e telecontrollo) e di **predictive maintenance**
- per gli end-user, la possibilità di contenere i consumi di energia (sugli impianti già installati), di ottimizzare gli investimenti in efficienza energetica, nonché di utilizzare i dati energetici per fare manutenzione preventiva

Tutte queste nuove potenzialità comportano una **crescente interconnessione** degli impianti (di produzione, trasmissione, distribuzione dell'energia, nonché degli utilizzatori finali), il che ovviamente espone tali asset alle stesse minacce cui sono soggetti i sistemi informativi e le reti aziendali.

Ne è una riprova il crescente numero

di attacchi perpetrati ai danni delle infrastrutture energetiche: tra questi, i più famosi sono sicuramente quello ad opera del **trojan Havex**, che ha infettato finora più di 2.000 apparati dotati di ICS tra Europa e USA, e quello che ha bloccato l'intera rete di distribuzione della compagnia ucraina **Kyivoblenergo** nel dicembre 2015.

Da qui la decisione di focalizzare questo report sul tema della **sicurezza industriale**, e quindi sui dati energetici e sugli asset fisici utilizzati nell'ambito delle operations, tralasciando le problematiche «classiche» dell'ICT security.



**I rischi di natura «cyber» per la filiera elettrica**

Il rischio legato alla crescente digitalizzazione delle operations è particolarmente elevato perché, dal momento che storicamente gli asset industriali lavoravano in modalità **«stand-alone»**, essi non erano soggetti ad attacchi di natura informatica. Di conseguenza, i sistemi operativi e i software installati per gestire tali asset **non venivano quasi mai aggiornati** (e quindi le vulnerabilità mai eliminate). Da qui la necessità di prevedere opportune soluzioni di tipo tecnologico e organizzativo, volte a minimizzare il rischio di incidenti di sicurezza nel momento in cui tali dispositivi vengono interconnessi in rete, o comunque, iniziano a scambiare dati con altri dispositivi hardware (come una banale chiavetta USB).

A questo problema, che riguarda tutto il «parco installato», si aggiunge quello relativo agli investimenti in nuovi asset, che devono adeguarsi al nuovo contesto e garantire quindi adeguati **standard minimi di sicurezza.**

Nel corso dello studio sono stati in primo luogo analizzati i rischi per i diversi stadi della filiera elettrica, e precisamente:

- **Player della generazione**, i quali possiedono e gestiscono gli impianti di produzione
- **Trasmission System Operator** e **Distribution System Operator**, chiamati a gestire rispettivamente la rete di trasmissione e quella di distribuzione
- **Prosumer**: una figura intermedia che è contemporaneamente consumatore e produttore di energia, ed è quindi esposta ai rischi che caratterizzano entrambe le categorie.

- **Consumatori di energia** (di natura industriale o residenziale)

Considerato il focus dell'analisi, in questo studio non sono stati considerati i puri retailer di energia.

Per ciascuno stadio si è proceduto ad analizzare:
- I possibili **impatti sulle attività (e sugli asset)** degli attacchi di natura cyber
- I conseguenti **danni economici**

In generale, gli attacchi di natura cyber in ambito OT sono mirati a:
- Catturare **informazioni** sui parametri di funzionamento di apparati e sistemi
- **Alterare** il funzionamento di apparati e sistemi, interrompendo flussi di dati o alterando i dati di input (per esempio attraverso i sistemi di telecontrollo), fino a giungere al danneggiamento degli asset .

A titolo d'esempio, nella figura seguente sono riportati i possibili rischi operativi e i conseguenti impatti economici nel caso dei player della generazione (e dei prosumer, nella veste di produttori di energia elettrica).

Dopo aver analizzato le possibili conseguenze per i singoli attori della filiera, l'attenzione si è spostata sul rischio «di sistema», ovvero sulla possibilità che attacchi di natura cibernetica possano mettere in crisi la stabilità della rete elettrica nazionale, o comunque comportino degli extra-costi significativi per il ribilanciamento tra domanda e offerta (è noto, infatti, che la rete elettrica deve essere caratterizzata sempre un bilanciamento - quasi in tempo reale - tra domanda e offerta di energia).

In particolare, gli approfondimenti

| | RISCHI | IMPATTI ECONOMICI |
|---|---|---|
| PLAYER GENERAZIONE «PURA» | • **Mancata produzione di energia elettrica**<br>• **Inaccessibilità ai sistemi di monitoraggio e telecontrollo** (perdita di visione e controllo sugli impianti)<br>• **Danni fisici agli impianti di produzione** | • **Riduzione del margine di contribuzione** (legato alla mancata vendita d'energia)<br>• **Penali da mancata vendita energia elettrica**<br>• **Mancato margine da fornitura di servizi ancillari**<br>• **Costi legati ai danni a impianti o persone** |
| PROSUMER (NELLA VESTE DI PRODUTTORI) | • **Mancata produzione di energia elettrica**<br>• **Danni agli impianti di produzione** | • **Riduzione dell'autoconsumo,** con conseguente **aumento della bolletta energetica**<br>• **Marginalità legata alla mancata vendita d'energia**<br>• **Costi legati a danni a impianti o persone** |

hanno riguardato:

- L'analisi degli extra-costi per il sistema derivanti dalla diminuzione dell'energia prodotta nel corso di un anno da impianti a fonte rinnovabile (parchi fotovoltaici e eolici) a causa

di attacchi ripetuti e «distribuiti», tali da compromettere temporaneamente il funzionamento di tali impianti (in termini di ore di funzionamento e/o quantità di energia prodotta), con conseguente necessità da parte di Terna di ribilanciare la rete facendo ricorso al Mercato dei Servizi di Dispacciamento;
- L'analisi del potenziale rischio di black-out derivante dall'improvviso mancato apporto di energia da parte di un certo numero di impianti a fonte rinnovabile (a seguito di un incidente di natura «cyber» che porta al blocco temporaneo dell'operatività di tali impianti) in un momento di picco di domanda (quindi tipicamente in un giorno feriale estivo, caratterizzato da alte temperature, nelle ore di punta.

In particolare, i risultati delle simulazioni evidenziano che:
- Gli extra-costi generati dal ricorso più frequente al MSD appaiono tutto sommato abbastanza contenuti nei vari scenari ipotizzati (per esempio: nel caso di attacchi che portano a una riduzione del 50% della potenza erogata per il 10% delle ore medie annue di funzionamento, tali costi variano da circa 10 a oltre 80 mil€ a seconda dell'area geografica di riferimento, per un totale a livello italiano di circa 264 mil€)
- Assumendo come giorno di riferimento le ore 12 del 21 Luglio 2017 (uno dei giorni di picco massimo di domanda di energia nel corso del 2017), una riduzione improvvisa della potenza pari a 3 GW (soglia oltre la quale si ritiene più probabile il rischio di instabilità e di conseguente black-out temporaneo della rete) si sarebbe

raggiunta con un'indisponibilità contemporanea del 12,7% della potenza generata dagli impianti eolici e fotovoltaici. Una percentuale piuttosto significativa, quindi, anche se va tenuto presente che la percentuale di energia fornita da fonti rinnovabili è destinata ad aumentare nel futuro, per cui l'incremento della «superficie d'attacco» potrebbe incrementare i rischi di instabilità del sistema, qualora non si investa sufficientemente nella sicurezza di tali impianti, nonché in soluzioni finalizzate a garantire comunque la stabilità della rete.

## Il quadro normativo di riferimento

Data il ruolo strategico ricoperto dalla rete elettrica all'interno di qualsiasi nazione, è naturale che la sicurezza di tali infrastrutture rappresenta da sempre una priorità per chi è chiamato a governarle.
La crescente esposizione ai rischi di natura informatica cui vanno incontro le infrastrutture critiche ha portato all'emanazione di direttive (a livello internazionale e nazionale) e a iniziative finalizzate a garantire un'adeguata protezione e una risposta adeguata in caso di crisi cibernetiche a livello nazionale.

Tra queste risultano particolarmente rilevanti nel contesto italiano:

- **la direttiva UE «NIS»** (Network and Information Security – EU 2016/1148)
- **il Quadro Strategico Nazionale Per La Sicurezza Dello Spazio Cibernetico**
- **il DPCM 13 aprile 2017** (noto come DPCM «**Gentiloni**»)
- **il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica**

In particolare, la **direttiva NIS** (recentemente recepita in Italia con DPCM del 16 maggio 2017 e in vigore dal 26 giugno scorso) prevede che all'interno di ciascun Stato membro vengano individuati i cosiddetti «operatori di servizi essenziali» all'interno di alcuni settori fondamentali (tra cui quello energetico).

Tali operatori saranno quindi obbligati a:

- **adottare misure adeguate** atte a prevenire e minimizzare l'impatto di **incidenti a carico della sicurezza della rete** e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali
- **fornire** all'autorità competente NIS:
  - le **informazioni necessarie a valutare la sicurezza della loro rete** e dei sistemi informativi, compresi i documenti relativi alle politiche di sicurezza
  - la **prova dell'effettiva attuazione delle politiche di sicurezza**, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato
- **notificare** al Computer Security Incident Response Team **(CSIRT)** nazionale (e per conoscenza alle autorità competenti NIS) **ogni incidente** avente un **impatto rilevante** sulla continuità del servizio fornito.

In ossequio a quanto richiesto dall'Articolo 7 della Direttiva, il decreto di recepimento prevede inoltre l'adozione di una **strategia nazionale di sicurezza cibernetica** da parte del Presidente del Consiglio dei Ministri

Tale strategia dovrà prevedere in particolare le misure di **preparazione, risposta e recupero** dei servizi a seguito di incidenti informatici, la definizione di un **piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione** in materia di sicurezza informatica.

Gran parte degli elementi costituenti tale strategia sono peraltro già contenuti (a grande linee) nei documenti programmatici già emanati a livello nazionale, ovvero nel **Quadro strategico nazionale per la sicurezza dello spazio cibernetico** del 2013 e nel successivo **Piano nazionale per la protezione cibernetica e la sicurezza informatica** del 2017.

In questo ambito va infine segnalato che la **Strategia Energetica Nazionale** prescrive due differenti linee di azione con riferimento alla cybersecurity, riguardanti rispettivamente:

- Lo sviluppo di **un piano di ricerca nel settore elettrico** (che include attività di modellazione, simulazione e di natura sperimentale, nonché la partecipazione a tavoli di lavoro per la definizione di standard e la certificazione)
- Lo sviluppo delle **collaborazioni a livello internazionale** (per esempio con NATO ed ENISA) e il rafforzamento delle attività di **cooperazione pubblico-privato a livello nazionale.**

Dall'esame del framework regolatorio si nota come, fatta eccezione per le iniziative previste nell'ambito della SEN, le direttive non facciano riferimento specifico al settore elettrico. Questo comporta una certa «generi-

cità» delle misure prescritte, che lascia ampi margini di interpretazione e potrebbe rendere piuttosto «complicato» l'adeguamento alle norme (e quindi le attività di compliance).

Sorprende, inoltre, che tra gli operatori di servizi essenziali del settore energetico non figurino i produttori di energia.

**Le soluzioni per una corretta gestione della security e il ruolo degli standard**

Per rispondere alle minacce di natura «cyber», gli operatori della filiera elettrica sono chiamati a rispondere mettendo a punto un **cybersecurity management system** in ambito industriale (in modo del tutto analogo a quanto avviene per l'IT «tradizionale»), tenendo conto delle peculiarità dell'ambiente OT (per esempio, la priorità del requisito di disponibilità rispetto all'integrità e alla riservatezza).

Si tratta di un insieme di processi, risorse e adeguati meccanismi di governance che consentano a un'impresa di garantire un adeguato livello di sicurezza (quindi un'esposizione al rischio in linea con le normative di riferimento e/o i valori target fissati). Le attività previste comprendono:

- Le risk analysis
- L'identificazione delle contromisure adeguate
- Monitoraggio e miglioramento continuo
- Sensibilizzazione e formazione
- La definizione di policy e guidelines.

Nella progettazione di tale sistema di gestione della cybersecurity (e in particolare nella definizione del

«cosa» proteggere e del «come» garantire un adeguato livello di sicurezza) un ruolo importante è ricoperto dagli standard.

In questo report abbiamo focalizzato l'attenzione sugli standard più rilevanti nell'ambito della sicurezza OT delle reti elettriche, e precisamente:

- ISA 62443
- IEC 62351
- NERC 1300 CIP
- NIST Cybersecurity Framework (e NIST 800-82)
- ISO 27019

Alcuni di tali standard sono caratterizzati da uno «scope» più ampio, e cercano di fornire delle guidelines per la progettazione dei sistemi di gestione della cybersecurity. Tra questi rientra sicuramente il **Cybersecurity Framework** sviluppato dal **National Institute of Standards and Technology (NIST)**. L'approccio sviluppato dal NIST consente di confrontare l'assetto di governance della cybersecurity con i modelli proposti e di identificare gli eventuali gap.

Anche l'ISO 27019 (che deriva dalla ISO27001 e ISO27002) è caratterizzato da un ambito di impatto piuttosto ampio. Esso infatti definisce **un insieme di regole/practice finalizzato a garantire la sicurezza dei sistemi di controllo e delle tecnologie di automazione** utilizzati nell'ambito della produzione, trasmissione/distribuzione dell'elettricità, del gas, del petrolio e del calore.

Lo **standard NERC CIP 1300**, messo a punto dalla North American Electric Reliability Corporation (NERC), identifica i requisiti minimi da implementare e mantenere al fine di garantire la sicurezza cibernetica degli asset presenti all'interno

dei sistemi generazione, trasmissione e distribuzione del sistema elettrico.

Lo **standard IEC-62443**, precedentemente noto con il nome di ISA 99, è stato sviluppato dall'International Society for Automation (ISA) e dall'International Electrotechnical Commission (IEC) nel 2010. Lo standard definisce **le linee guida** da utilizzare per incrementare la sicurezza informatica degli **Industrial Control System**. Lo standard definisce dei livelli «target» di sicurezza degli ICS. Questo ha delle ripercussioni importanti sui **produttori** degli apparati ICS, **in quanto**:

- Gli utilizzatori possono utilizzare questo standard per definire i requisiti di sicurezza nell'ambito delle gare o delle procedure di acquisto
- I vendor, di contro, possono «garantire» i livelli di sicurezza offerti dai propri prodotti ricorrendo a opportuna **certificazione**.

Anche lo standard **NIST 800-82** si focalizza sulla sicurezza dei sistemi ICS, attraverso una «defense-in-depth» strategy che prevede l'adozione di una serie di contromisure di varia natura (restrizione degli accessi, procedure di business continuity e disaster ricovery), nonché soluzioni organizzative ad hoc.

Infine, lo standard **IEC-62351** (*Power systems management and associated information exchange – Data and communications security*) è stato sviluppato dalla commissione tecnica 57 (TC 57) dell'International Electrotechnical Commission (IEC), e si focalizza sugli standard di sicurezza dei **protocolli di comunicazione** dei sistemi di generazione.

L'analisi condotta porta a conclude-

re che il livello di «copertura» degli standard sia oramai abbastanza avanzato, sia con riferimento al «*cosa proteggere*», che con riferimento al «*come*», anche se su quest'ultimo fronte ci sono ancora diversi sviluppi in corso (anche per via della continua evoluzione delle tecnologie – e delle vulnerabilità –).

La sfida adesso sembra consistere nel livello di adozione di tali standard, sia da parte delle imprese energetiche, sia da parte dei costruttori. In particolare, appare abbastanza cruciale il ruolo delle (grandi) imprese clienti nell' «imporre» l'adozione degli standard da parte dei loro fornitori, dal momento che quest'ultimi appaiono talvolta un po' riluttanti per via del timore di perdere il potere contrattuale derivante dal fatto di proporre soluzioni proprietarie.

**L'indagine empirica: il punto di vista degli end-user**

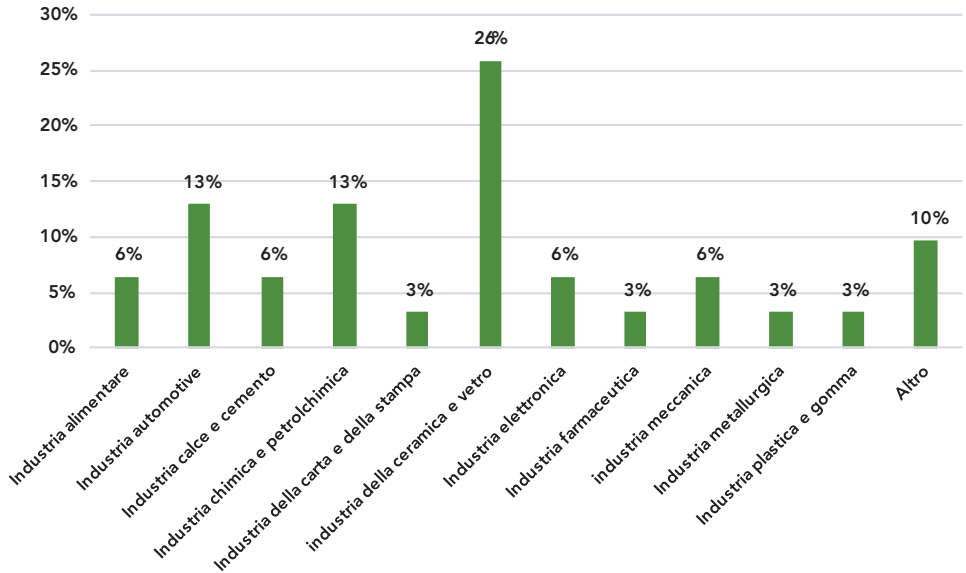
L'ultima parte del report si è focalizzata sugli end-user di natura industriale, con il duplice obiettivo di:

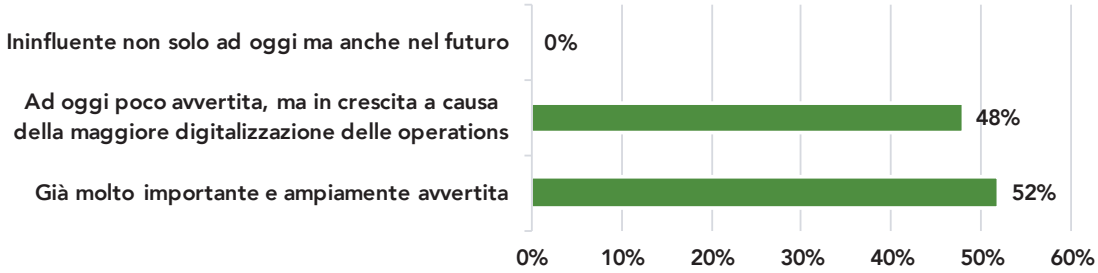
- verificare il grado di diffusione della **cultura della cybersecurity** in ambito **OT** all'interno del sistema industriale del nostro Paese, con particolare riferimento alle nuove minacce derivanti dalla digitalizzazione dei processi industriali
- Verificare (nel caso dei «prosumer») il livello di **consapevolezza dei rischi** legati alle attività di **generazione di energia.**

A tal fine è stata somministrata una survey a un campione di circa 700 imprese di varia dimensione e operanti in diversi settori, ottenendo 93 risposte. La distribuzione dei ri-

spondenti per settore di attività è riportato nel grafico sottostante. Come si può notare, i settori maggiormente rappresentati sono quelli della **ceramica e del vetro** (il 26% delle imprese rispondenti), **l'automotive e la chimica e petrolchimica** (entrambe al 13%).

Le risposte delle imprese evidenziano come l'importanza del tema della sicurezza OT sia in crescita. Circa metà dei rispondenti ha infatti affermato che il tema è già molto sentito,

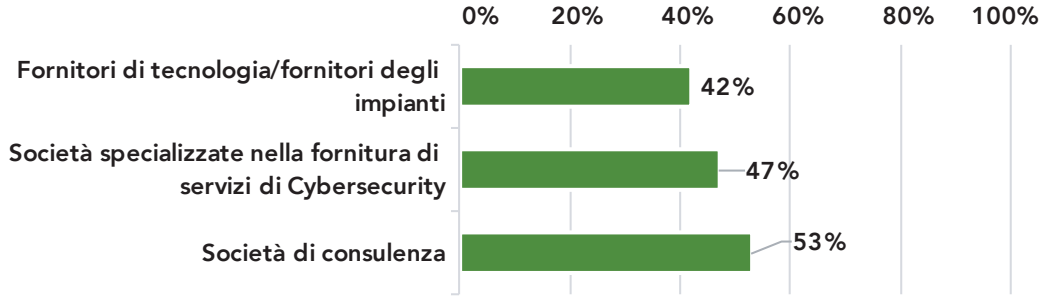





mentre la restante metà ritiene che l'attenzione crescerà notevolmente in futuro per via della crescente digitalizzazione.

Con riferimento agli aspetti organizzativi, la configurazione organizzativa più diffusa sembra essere quella «mista», che prevede l'utilizzo di risorse interne, supportate da terze parti (configurazione adottata dal **58%** delle imprese). Va altresì segnalato che il 10% dei rispondenti ha dichiarato di non aver ancora adottato nessuna soluzione organizzativa «stabile».

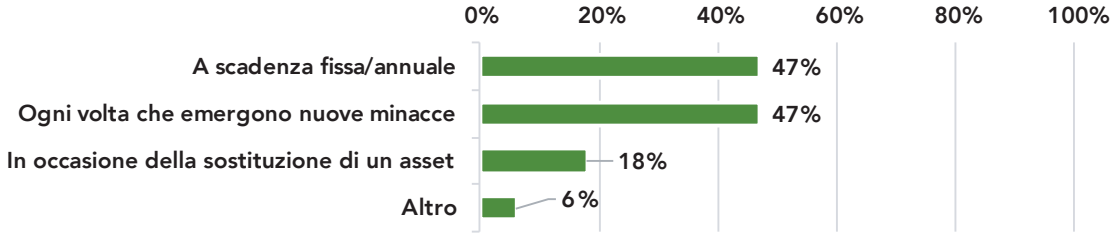
Analizzando più in profondità la natura dei business partner coinvolti nella gestione della cybersecurity OT, si scopre che le imprese si rivolgono sia a società di consulenza IT che a società specializzate nei servizi e soluzioni di cybersecurity. Da notarsi come solo il 42% dei rispondenti ha affermato di coinvolgere




i costruttori di apparati e impianti (nonostante la loro importanza strategica).

Questo risultato va visto in combinazione con le risposte ottenute in merito all'importanza attribuita dalle imprese alle **prestazioni di sicurezza degli apparati e dei componenti** nell'ambito del processo di aquisto. Solo il 10% dei rispondenti dichiara che tali performance sono rilevanti (e sono quindi inserite tra i requisiti), mentre poco più della metà delle imprese dichiara che tali prestazioni, per quanto prese in considerazione, non rappresentano un driver di scelta.

L'analisi del livello di strutturazione delle attività necessarie per una corretta gestione della cybersecurity fornisce dei risultati piuttosto preoccupanti: solo poco più di metà delle imprese, infatti, afferma di svolgere attività di **risk analysis** in ambito OT.




Ancora più preoccupante l'analisi delle **modalità** con cui viene volta tale attività. Come si può notare dal grafico sottostante, quasi la metà dei rispondenti afferma di condurla a cadenza fissa (tipicamente annuale), mentre un altro 47% dichiara di condurla quando emergono nuove minacce.

Ancor più significativo appare il dato sugli **investimenti**: solo il 23% delle imprese rispondenti ha infatti dichiarato di aver effettuato investimenti dedicati alla cybersecurity OT.

Nella parte finale della survey si è cercato di valutare la sensibilità delle imprese «**prosumer**» nei confronti dei rischi di natura cyber legati alla produzione di energia.

Più di metà dei rispondenti ha infatti dichiarato di essere anche produttore di energia: in particolare, il 45% ha installato **cogeneratori/trigene-**

**ratori**, mentre il 33% afferma di possedere un **impianto fotovoltaico**.

Risulta interessante osservare come le imprese prosumer ritengano questi impianti immuni a possibili attacchi di natura cyber. Infatti, solamente il **6% dei rispondenti** ritiene che l'operatività di questi impianti possa essere compromessa da attacchi cibernetici.

I risultati di questa indagine evidenziano come la cybersecurity OT sia considerata di fatto dalle imprese un tema strategicamente ancora poco rilevante (al di là delle dichiarazioni iniziali). La ridotta sensibilità sul tema e l'assenza di una casistica significativa di attacchi cibernetici volti a bloccare o a compromettere l'attività produttiva fa sì che le imprese preferiscano indirizzare gli investimenti verso altre aree.

Ancor più significative le risposte dei prosumer in merito ai rischi cui sono esposti gli impianti di produzione di energia da loro gestiti: il livello di consapevolezza risulta estremamente basso, tant'è che il problema non viene praticamente nemmeno preso in considerazione.

**Paolo Maccarrone**
*Responsabile della Ricerca*

**Davide Perego**
*Project Manager*

POLITECNICO
MILANO 1863

MIP
POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

es

# L'ambito di analisi 1

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

# La Cybersecurity: differenti visioni

- Come si può notare dalle definizioni qui sotto riportate, non vi è piena convergenza sul concetto di «cybersecurity»

L'abilità di **proteggere l'uso del cyberspazio** da possibili **minacce di tipo cyber**
***(Fonte NIST)***

**La raccolta di strumenti**, policy, concetti e misure di sicurezza, linee guida, approcci di risk management, azioni, strumenti di formazione, best practice, strumenti assicurativi e tecnologie che possono essere **utilizzati per proteggere l'ambiente cibernetico, l'organizzazione e le risorse degli utenti**
***(Fonte ITU – International Telecommunication Union)***

**La tutela della riservatezza, della integrità e della disponibilità delle informazioni** all'interno del cyberspazio
***(Fonte ISO/IEC JTC 1)***

# La Cybersecurity: la nostra definizione

- Analizzando e rielaborando le varie fonti abbiamo elaborato la seguente definizione:

> L'insieme di **strumenti, procedure e sistemi** che consente a una entità (ad esempio, una nazione, una organizzazione, un cittadino) **la protezione dei propri asset fisici** e della **confidenzialità, integrità e disponibilità delle proprie informazioni** attraverso un'attività di **prevenzione, rilevazione e risposta** agli attacchi provenienti **dal «cyberspazio»**

- Alcune considerazioni:
  - Gli attacchi provengono dal «***cyberspazio***»: con questo termine si intende il dominio virtuale costituito dall'insieme di PC, sistemi informativi e reti di telecomunicazione interconnessi a livello globale Due tipologie di asset sotto attacco: dati e infrastrutture fisiche
  - Una corretta gestione della cybersecurity implica:
    - Lo svolgimento sistematico di attività di **risk assessment**, finalizzate a identificare gli asset aziendali a rischio e a monitorare le possibili minacce cui tali asset sono esposti
    - La definizione di **piani di azione** (e delle relative risorse necessarie) finalizzati a garantire il massimo livello di sicurezza possibile
    - La corretta definizione di tutti gli aspetti **organizzativi** (unità coinvolte, ruoli e responsabilità, flussi di comunicazione, ecc)
    - La creazione di una **cultura organizzativa** orientata alla sicurezza

# La Cybersecurity: una tematica «complessa»

La complessità concettuale della cybersecurity da molteplici fattori, tra cui:

- **I differenti ambiti di applicazione**
- **Le differenti finalità degli attacchi**
- **L'esistenza di numerose tipologie di attacker**

- Questo implica che la stessa vulnerabilità possa essere sfruttata per portare attacchi molto diversi fra loro, a seconda della natura dell'attaccante e della finalità
- Le tre dimensioni sopra riportate verranno illustrate più dettagliatamente nel seguito

# La Cybersecurity: i differenti ambiti di applicazione

- La cybersecurity può riguardare **differenti ambiti**:

| AMBITO | DESCRIZIONE |
|---|---|
| **TELECOMMUNICATIONS (o NETWORK) SECURITY** | Protezione nei confronti delle **minacce all'infrastruttura di telecomunicazione** |
| **INFORMATION (o DATA) SECURITY** | Protezione contro la minaccia di **furto, cancellazione o alterazione di dati** memorizzati o trasmessi all'interno di un sistema informativo (o su altro supporto) |
| **(CRITICAL) INFRASTRUCTURE SECURITY** | **Protezione contro attacchi (di natura sia digitale che fisica)** che possono provocare danni ad asset fisici strategici, come nel caso delle infrastrutture critiche di un Paese |

- Due considerazioni:
  - attenzione alle possibili conseguenze di un attacco «cyber» sull'operatività di sistemi/apparati/infrastrutture ( $\longrightarrow$ ottica «di processo»)
  - Gli attacchi provenienti dal cyberspazio possono provocare danni anche agli **asset fisici** (ex: le infrastrutture critiche), anche in combinazione con attacchi di natura fisica

# La Cybersecurity: le differenti finalità

- Gli attacchi cibernetici sono perpetrati con finalità differenti. Si distingue generalmente tra **Cyber Crime, Cyber Terrorism e Cyber Warfare:**

| AMBITO | DESCRIZIONE | FINALITA'/ DETERMINANTI |
|---|---|---|
| **CYBER CRIME** | **Atti criminali** commessi **usando sistemi informativi o reti di comunicazione** elettroniche **al fine di perseguire vantaggi di tipo economico** | Economiche |
| **CYBER TERRORISM** | **Attacchi** che, attraverso l'utilizzo e lo sfruttamento di computer o reti di comunicazione, sono **volti** a generare incidenti tali da **generare paura o danni** nei soggetti «target» | Ideologiche |
| **CYBER WARFARE** | **Attacchi**, che fruttando computer o le reti di comunicazione, sono **volti a danneggiare gli asset fisici o digitali di una nazione al fine di comprometterne l'operatività** | Politiche/ Militari |

# La Cybersecurity: le tipologie di attacker

- Le minacce di tipo cyber possono essere apportate da soggetti diversi, generalmente raggruppati in due macro-categorie:
  - **Attaccanti esterni all'impresa**, a loro volta suddivisibili in sotto-categorie: hackers, terroristi/cyber-terroristi, competitor industriali, fornitori, Nazioni
  - **Attaccanti interni all'impresa**: dipendenti e manager

| | FONTE MINACCIA | DESCRIZIONE |
|---|---|---|
| ESTERNI | **Nazioni** | In un contesto di evoluzione del concetto di «warfare» gli stati si stanno dotando di capacità offensive volte a **generare attacchi nei confronti di «nazioni nemiche»** finalizzati a impossessarsi di dati sensibili, proprietà intellettuali o a bloccarne l'operatività |
| | **(Black) hackers** | Sogetti che mirano a **individuare e sfruttare vulnerabilità** presenti all'interno delle reti e dei **sistemi aziendali,** al fine **di ottenere il controllo delle stesse o dei dati** in essi presenti |
| | **(Cyber) terroristi** | Individui o organizzazioni interessate a effettuare **attacchi volti a generare paura all'interno della comunità** |
| | **Competitor industriali** | I competitor industriali possono essere **interessati a ottenere informazioni** (quali ad esempio dati o proprietà intellettuali) o a **compromettere le attività operative dei rivali** |
| | **Fornitori** | **I fornitori** possono costituire per le imprese una minaccia non solo come veri e propri **attaccanti**, ma soprattutto **come veicoli privilegiati per avere accesso alle reti e alle infrastrutture aziendali**, sfruttando ad esempio i canali/strumenti che le imprese lasciano a disposizione dei propri fornitori al fine di fare telecontrollo e manutenzione da remoto degli impianti |
| INTERNI | **Dipendenti/ manager** | I dipendenti possono essere **autori di azioni volontarie volte ad arrecare danni alla propria azienda, ma nella maggior parte** sono sfruttati da altre tipologie di attaccanti, quali **veicoli per ottenere l'accesso alle reti aziendali** attraverso tecniche quali il phishing e social engineering. |

# La Cybersecurity: le tipologie di attacker

- Osservando il ruolo che ciascuna di queste tipologie di attacker ricopre all'interno degli attacchi possiamo identificare come:
  - Le **nazioni** ricoprano non solo il ruolo di **mandante degli attacchi,** ma attraverso la creazione di «gruppi militari» volti al cyber-warfare possono essere esse stesse degli **attaccanti**
  - I **competitor industriali tipicamente** non hanno le competenze tecniche per realizzare un attacco, quindi nella maggior parte dei casi ricoprono il ruolo di **mandante dell'attacco**
  - **Black hackers**, i quali svolgono principalmente la funzione di realizzatori dell'attacco
  - **Cyberterroristi**, i quali possono assumere il ruolo di mandanti degli attacchi affidandosi a gruppi di black hackers per realizzare fisicamente l'attacco oppure possono realizzarli in prima persona
  - I **fornitori** e **i dipendenti** possono essere realizzatori fisici degli attacchi compiendo essi stessi gli attacchi o introducendo volontariamente le minacce all'interno dei confini aziendali, ma nella maggior parte dei casi sono invece **veicoli involontari degli attacchi**

| ATTACKER | MANDANTE | REALIZZATORE | VEICOLI PASSIVI |
|---|---|---|---|
| Nazionl | ■ | ■ | |
| (Black) hackers | | ■ | |
| (Cyber) terroristi | ■ | ■ | |
| Competitor industriali | ■ | | |
| Fornitori | | ■ | ■ |
| Dipendenti/Manager | | ■ | ■ |

# Physical security vs. Cybersecurity

- **Le minacce di tipo cibernetico** presentano caratteristiche completamente **differenti rispetto a quelle fisiche**

| PHYSICAL SECURITY | CYBERSECURITY |
|---|---|
| **Asset fisici**, concentrati in determinate aree geografiche e **facilmente difendibili** | Gli **asset** sono **intangibili nel caso di dati** oppure **distribuiti nel caso di oggetti fisici** |
| Gli **attacchi**, per essere implementati, **necessitano della prossimità fisica** | Gli **attacchi** possono essere **condotti a distanza**, in quanto gli attaccanti possono superare le possibili barriere fisiche **attraverso l'utilizzo delle reti informatiche** |
| Gli **attacchi** e i **possibili attaccanti** risultano **facilmente identificabili** | **Maggiore difficoltà nell'identificazione degli attacchi e dei possibili attaccanti** |
| **DIFENSORE in posizione di vantaggio** | **ATTACCANTE in posizione di vantaggio** |
| **«PERIMETER DEFENCE»**<br>**gli investimenti** in sicurezza sono volti a **fortificare il perimetro esterno dell'impresa/infrastruttura** | **«MODULAR DEFENCE»**<br>**gli investimenti** in sicurezza sono volti a garantire una separazione tra gli asset, al fine di limitare la possibilità di **compromettere asset differenti attraverso un solo attacco** |

# Energy Cybersecurity Report

- Perché sviluppare un report sulla tematica dell'Energy Cybersecurity?

  - **Il settore Energy** è caratterizzato da trend e dinamiche che stanno aumentando **la possibile esposizione ad attacchi cibernetici**

  - Le **minacce** relative a possibili attacchi si stanno **concretizzando**. Alcuni esempi:
    - **Il caso Saudi–Aramco**
    - **Il trojan Havex**
    - **L'attacco alla power grid ucraina**

  - In risposta a questi crescenti rischi, negli ultimi anni si è assistito:
    - A un crescente peso delle **normative** volte in particolare a definire gli obblighi a cui gli operatori di servizi essenziali (che comprendono anche gli operatori del settore energetico) devono sottostare
    - Allo sviluppo di **standard** per una corretta gestione di tutte le attività connesse alla sicurezza da parte degli operatori della filiera
    - A una presa di coscienza da parte delle **imprese**, che hanno iniziato (sebbene con notevoli differenze da caso a caso) ad affrontare il tema in modo sistematico e strutturato

# BOX 1: Gli attacchi cyber – il caso Saudi Aramco

- Il **15 Agosto del 2012** un self-replicating virus denominato Shamoon infettò più di 30.000 computer all'interno dell'infrastruttura dell'impresa, **determinando la distruzione dell'85% dell'hardware dell'impresa** e forzando i dipendenti a **scollegare dalla rete i sistemi rimanenti per più di 10 giorni** per evitare un'ulteriore propagazione del virus

- Sebbene la compagnia abbia riportato che **le attività di perforazione e di estrazione non siano state intaccate dall'attacco** - mantenendo una produzione di 9,5 milioni di barili di greggio al giorno - l'indisponibilità dei sistemi informativi ha compromesso la **gestione dell'attività a valle dell'estrazione, generando rallentamenti all'interno delle attività operative**

- **Questa tipologia di attacco** non è solo uno dei primi attacchi a una impresa del settore energetico ma, a causa del peso dell'impresa nel contesto saudita, **rappresenta di fatto il tentativo di compromettere l'economia di un nazione**

# BOX 2: Gli attacchi cyber – Il trojan Havex

- **Havex è un trojan ad accesso remoto scoperto nel 2013** come parte di una campagna di spionaggio e attacco nei confronti degli Industrial Control Systems (ICS)

- Si stima che **Havex abbia già colpito più di 2000 siti legati alle infrastrutture europee e degli Stati Uniti, colpendo soprattutto il settore energetico**, in particolare operatori del settore della generazione e trasmissione/distribuzione elettrica, gestori degli oleodotti e fornitori di infrastrutture industriali. Havex ha però avuto impatti anche sui settori della aviazione, della farmaceutica e della petrolchimica.

- La **campagna di attacco Havex è iniziata nel 2010, utilizzando tecniche di spear phishing**, al fine di ottenere accesso e infettare le infrastrutture industriali delle vittime di attacco. In particolare **Havex**, dopo essere stato installato, procede a effettuare una scansione del sistema infetto al fine di individuare i sistemi ICS e SCADA presenti all'interno dell'infrastruttura, **raccogliendo informazioni utili a sviluppare attacchi specifici volti a interrompere il funzionamento o provocare danni materiali** a quelle specifiche infrastrutture critiche.

# BOX 3: Gli attacchi cyber – l'attacco alla Power Grid ucraina

- Il primo attacco di natura cibernetica finalizzato a compromettere una infrastruttura critica nazionale si verificò, il **23 dicembre 2015, ai danni della compagnia ucraina di distribuzione elettrica Kyivoblenergo**

- L'attacco fu realizzato attraverso un'**intrusione** da parte di un soggetto terzo **all'interno del network aziendale e all'interno dei sistemi SCADA destinati al monitoraggio delle cabine elettriche**, determinando la disconnessione dalla rete di 30 cabine elettriche (7 cabine a 110 kV e 23 a 35 kV) e la mancata fornitura di energia elettrica per tre ore a più di di 225.000 utenti sul territorio ucraino

- A causa del **ridotto numero di utenti convolti e del basso tempo di downtime** (3 ore) l'attacco creò un **impatto limitato** sulla rete di trasmissione e distribuzione elettrica ucraina

# Energy Cybersecurity: gli ambiti di analisi del report

- In questa prima edizione dell'Osservatorio ci siamo focalizzati in particolare sulla filiera elettrica, analizzando le nuove minacce «cyber» legate ad alcuni trend in atto, qui di seguito riportati:

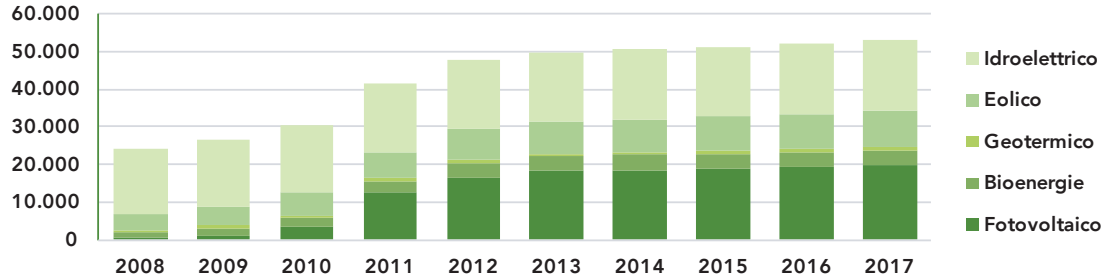
**SISTEMA ELETTRICO**

- **Crescente peso del peso delle fonti rinnovabili**
- **La diffusione del modello «prosumer»**
- **L'impatto della «digitalizzazione» sui vari stadi della filiera (produzione, trasmissione, distribuzione, ecc)**

- Si è poi proceduto ad analizzare il punto di vista degli **end user** industriali in merito:
  - all'impatto della digitalizzazione sui processi industriali
  - ai nuovi rischi di natura informatica conseguenti alla digitalizzazione (ivi compresi quelli legati alla fornitura di energia elettrica)

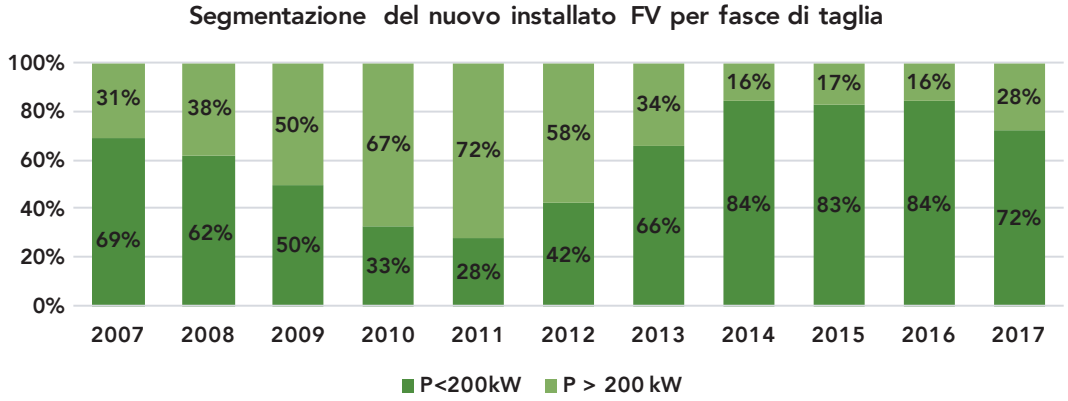
# I trend in atto nel sistema elettrico: la diffusione delle fonti rinnovabili

- La **potenza installata da rinnovabili nel 2017 è aumentata di 900 MW**, raggiungendo un **installato di 53 GW** (36 GW se si esclude l'idroelettrico «storico» già installato prima degli anni 2000), contribuendo a coprire **il 36,2% della produzione** (103,4 TWh/anno)
- L'impatto delle FER sul sistema elettrico nazionale è destinato ad aumentare nel futuro. La **SEN**, infatti, prevede che **per il 2030** le **FER** coprano il **60% della produzione elettrica** (pari a 184 TWh/anno)
- La diffusione degli impianti di produzione da fonti rinnovabili comporta comunque un vertiginoso **aumento del numero di attori** (e di impianti di generazione: parchi fotovoltatici, eolici, ecc). A questo si associa mediamente un **minore livello di maturità** dei sistemi di gestione dei rischi di natura «cyber» (soprattutto laddove tali impianti non siano gestiti da operatori «storici» del settore)



# I trend in atto nel sistema elettrico: l'affermazione del modello «prosumer»

- Lo sviluppo delle fonti rinnovabili, in particolare del fotovoltaico, ha portato anche alla nascita del cosiddetto **«utente prosumer»**, ovvero di un utente elettrico che è **contemporaneamente produttore e consumatore** di energia elettrica
- La **diffusione del paradigma prosumer** – tra gli utenti residenziali, commerciali e industriali – pone un **possibile problema di cybersecurity** nei confronti della rete elettrica, **a causa dell'aumento della superficie di attacco** a disposizione di eventuali soggetti malintenzionati. Anche in questo caso a questo si aggiunge una minor livello di consapevolezza e di competenze di questi attori sui rischi di natura «cyber»



# I trend in atto nel sistema elettrico: le «smart grid»

- **L'avvento della generazione distribuita e del modello prosumer** implica per la rete elettrica il passaggio da un funzionamento unidirezionale, caratterizzato da una produzione centralizzata, a un **modello «smart grid», caratterizzato da flussi di energia bidirezionali**

- L'implementazione di un modello di rete di tipo **«smart grid»** permette di conseguire i seguenti **obiettivi:**
  - Una **migliore gestione** della rete elettrica, ottenuta anche attraverso l'implementazione di sensori e di sistemi SCADA, abilitando il monitoraggio dei dati di funzionamento e il telecontrollo degli impianti da remoto.
  - Una **maggiore efficienza nella trasmissione dell'elettricità**, ottenuta attraverso un **migliore bilanciamento della rete** e un livellamento dei picchi di domanda
  - Una **riduzione dei costi operativi relativi alla manutenzione e alla gestione della rete**
  - Una migliore **integrazione della produzione** relativa ai grandi impianti di produzione **rinnovabili** e degli impianti posseduti dai **prosumer**

# I trend in atto nel sistema elettrico: l'impatto della digitalizzazione nella produzione di energia

- **L'introduzione delle tecnologie IT all'interno della generazione** ha permesso di effettuare una **migliore attività di monitoraggio degli impianti**, abilitando vantaggi che sono riconducibili alle tre macrocategorie seguenti:

**Predizione della produzione**

L'introduzione delle tecnologie IT ha permesso di sviluppare **modelli predittivi sulla produzione negli impianti a fonte rinnovabile**, attraverso l'integrazione dei dati storici sulla produzione con le informazioni relative alle condizioni metereologiche in tempo reale, consentendo **l'ottimizzazione della produzione**

**Miglioramento dell'efficienza e della flessibilità di produzione**

La raccolta dei dati istantanei di produzione, effettuato attraverso **sistemi di monitoraggio/telecontrollo**, permette di rendere più efficiente la produzione, consentendo un migliore controllo e una **regolazione avanzata dei parametri operativi degli impianti**

**Ottimizzazione delle attività di O&M**

**Il monitoraggio dei dati relativi alla produzione** degli impianti permette ai detentori di asset e agli O&M di monitorare in dettaglio le performance di ciascun impianto, **abilitando la possibilità d'implementare programmi di manutenzione preventiva, riducendo il downtime degli impianti e i costi** relativi alla manutenzione

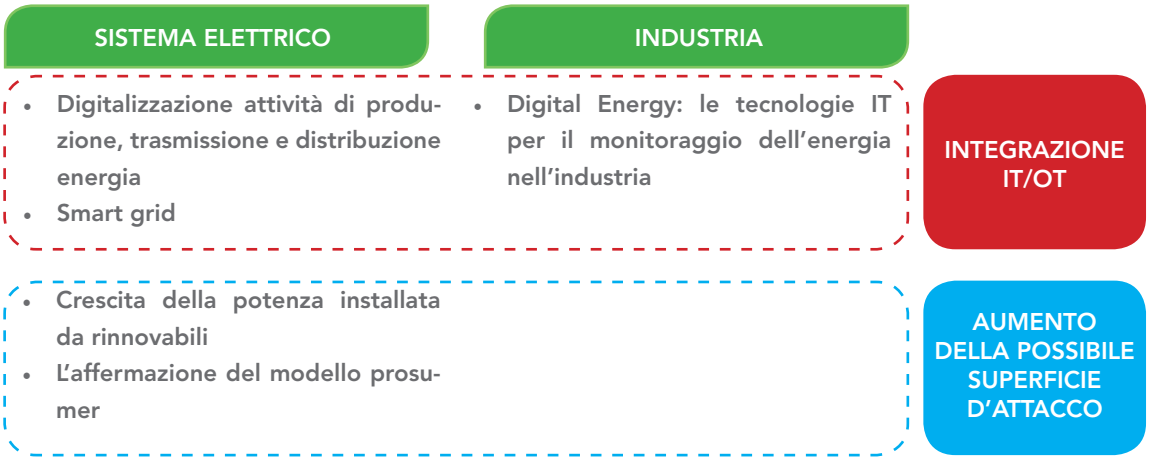
# I trend in atto nel settore elettrico: la «digital energy» e gli utenti industriali

- **Il piano industria 4.0**, avviato a livello italiano nel Settembre 2016 e con una dotazione di **13 Miliardi di € tra il 2017 e il 2020**, ha contribuito a stimolare la trasformazione digitale delle imprese manifatturiere italiane

- In ambito energy l'implementazione di tecnologie digitali ha permesso di ottenere una **maggiore visibilità sull'effettivo funzionamento del processo produttivo**, abilitando, da parte delle imprese, la possibilità di **aumentare la propria efficienza energetica**

- La **maggiore disponibilità di dati**, derivante dall'installazione di sistemi/sensori volti a monitorare i consumi elettrici e termici, **permette**:
  - **Il miglioramento dei sistemi di gestione dell'energia**, riducendo la bolletta energetica dell'impresa
  - **L'individuazione di problematiche presenti all'interno della catena produttiva**, **abilitando** possibili **investimenti** finalizzati all'adozione di **tecnologie produttive più efficienti dal punto di vista energetico.**
  - Miglioramento della **disponibilità** e **operatività** degli impianti di produzione attraverso l'implementazione di concetti di **predictive manteinance**

# Energy Cybersecurity: il quadro riassuntivo dei trend



# L'integrazione IT-OT: due mondi «storicamente» differenti

- Per decenni il mondo dell'**Information Technology** e dell'**Operation Technology**, hanno avuto **differenti caratteristiche e finalità** e sono state gestite da strutture organizzative differenti

| | Operation technology | Information technology |
|---|---|---|
| **Hardware/ software** | **Hardware e software sviluppati ad hoc** per lo specifico utilizzo | Utilizzo di **soluzioni off-the-shelf** sia per quanto riguarda la componente hardware sia per la componente software |
| **Protocolli di comunicazione** | **Dispositivi stand–alone**, la cui comunicazione con altri apparati avviene con **protocolli proprietari** | **Dispositivi interconnessi** la cui comunicazione avviene attraverso **protocolli standard** |
| **Sicurezza** | Garantita dal **presidio fisico dei dispositivi** | Garantita da una **continua implementazione di patch software** e dall'applicazione degli ultimi **standard/policy di sicurezza** |
| **Ciclo di vita** | Quantificabile in **decenni** | Quantificabile in **anni** |
| **Responsabilità gestione** | La responsabilità della gestione di queste infrastrutture OT è tipicamente a carico delle **business unit operative** | La responsabilità della gestione delle infrastrutture IT è a carico del **reparto ICT** |

## L'integrazione IT-OT: differenti priorità


- Nel **mondo IT l'obiettivo principale** è garantire la **confidenzialità del dato**, ovvero l'impossibilità da parte di chi non ne possiede i privilegi di avere accesso ai dati

- Nel **contesto della rete elettrica italiana**, e più in generale all'interno del mondo dell'**Operation Technology**, risulta invece **fondamentale garantire la disponibilità degli impianti**, in quanto possibili indisponibilità degli impianti di regolazione e sicurezza all'interno delle cabine elettriche potrebbero creare dei blackout

- Le **differenti priorità dei due mondi determinano l'impossibilità di applicare fedelmente le logiche di sicurezza del mondo IT** (quali ad esempio l'aggiornamento/patching del software) **all'interno del contesto OT**

# L'integrazione IT-OT: a chi è demandata la sicurezza?

- **L'avvento della convergenza tra IT e OT**, determina l'introduzione **delle minacce tipiche del contesto IT** all'interno del **mondo OT**, tendenzialmente non pronto a difendersi dalle minacce cyber

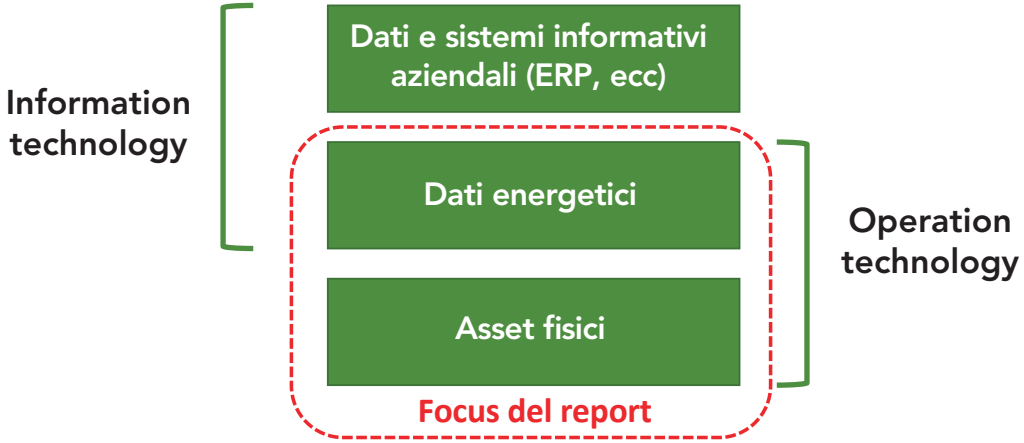
- All'interno di questo contesto i **fornitori tecnologici** sono chiamati a garantire la sicurezza dei propri prodotti, **gestendo lungo tutto il ciclo di vita del prodotto** non solo la **componente HW del loro prodotti, ma anche quella software**

- I fornitori tecnologici dovranno dotarsi di una «**divisione software**» finalizzata a:
  - identificare le minacce inerenti ai propri prodotti,
  - sviluppare e testare le opportune contromisure software per garantire la sicurezza operativa dei prodotti

- I **fornitori tecnologici** sono inoltre chiamati a aiutare **i propri clienti** (soprattutto quelli più piccoli, caratterizzati da limitate competenze e risorse) a **sviluppare una cultura legata alla cybersecurity**, al fine di modificare i loro processi in ottica di **Security by Design**

# Il focus del report: i dati energetici e macchine fisiche

- Nel contesto del primo report sull'Energy Cybersecurity si focalizzerà l'analisi sulle **tematiche della sicurezza delle macchine fisiche e dei dati energetici derivanti da esse**, tralasciando tutta la tematica relativa alla difesa dei dati aziendali e della gestione della privacy relativa ai dati finali dei clienti



POLITECNICO
MILANO 1863

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

es

# I rischi per la filiera elettrica 2

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

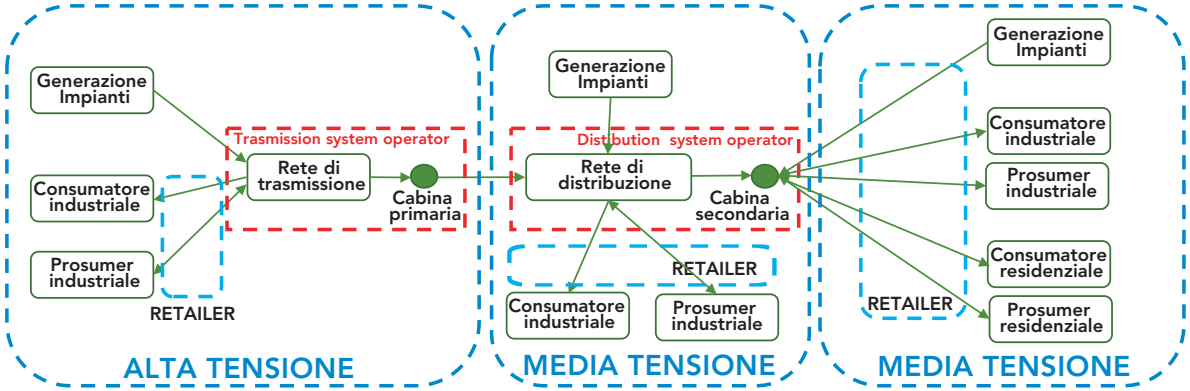
# Obiettivi della sezione

- L'obiettivo della sezione consiste nell'identificare i possibili **impatti** derivanti da **attacchi** di natura «cyber», sia in termini operativi/fisici (interruzione dei processi, perdita di dati, danni ai sistemi/alle infrastrutture), sia in termini economici

- **A livello metodologico**, le informazioni presenti all'interno di questo capitolo sono state reperite attraverso:
  - **Analisi della letteratura**
  - **Interviste con key informant** (e.g. player operanti nel settore, imprese «O&M», consulenti, fornitori di tecnologie, ricercatori, ecc)

# La rete elettrica italiana: gli attori

- Il grafico seguente illustra l'articolazione della filiera elettrica:




- E' possibile quindi individuare la seguente tipologia di operatori:
  - **Player della generazione**, i quali possiedono e gestiscono gli impianti di produzione
  - **Trasmission System Operator** e **Distribution System Operator**, chiamati a gestire rispettivamente la rete di trasmissione e quella di distribuzione
  - **Retailer**: player a cui è demandata la vendita di energia ai clienti finali
  - **Prosumer**: una figura intermedia che è contemporaneamente consumatore e produttore di energia, ed è quindi esposta ai rischi che caratterizzano entrambe le categorie
  - **Consumatori di energia** (di natura industriale o residenziale)

# La rete elettrica italiana: il ruolo degli attori all'interno della filiera

- Incrociando la tipologia di attori con il ruolo ricoperto all'interno della filiera è possibile quindi ottenere questa matrice:

| | PRODUTTORI ENERGIA | TSO | DSO | RETAILER | PROSUMER | CONSUMATORI FINALI |
|---|---|---|---|---|---|---|
| GENERAZIONE | ■ | | | | ■ | |
| TRASMISSIONE | | ■ | | | | |
| DISTRIBUZIONE | | | ■ | | | |
| VENDITA | | | | ■ | | |
| CONSUMO | | | | | ■ | ■ |

# La generazione: il cambio di paradigma

- L'avvento della **generazione distribuita** ha determinato il passaggio da un modello «concentrato», in cui la produzione di energia elettrica era affidata ad **un numero ridotto di player**, ovvero i possessori delle grandi centrali termoelettriche o idroelettriche, a un modello caratterizzato da un notevole incremento del numero di attori, tra cui spiccano in particolare i gestori di **impianti a fonte rinnovabile** (nonché i **prosumer**)
- La **dimensione** dei player operanti all'interno della generazione sembra essere positivamente correlata con il **livello di sviluppo** dei sistemi di gestione della cybersecurity. In particolare:
  - I **grandi player** sono mediamente caratterizzati da un **approccio proattivo** alla gestione della cybersecurity, in quanto: sono **attivi all'interno dei programmi internazionali**, si sono dotati di **strutture organizzazione interne** volte alla gestione delle minacce e stanno utilizzando il loro potere contrattuale per **spingere i fornitori a prestare maggiore attenzione alla sicurezza dei loro prodotti**
  - I **piccoli player**, al contrario, spesso **non percepiscono o non dispongono di risorse e competenze sufficienti** per fronteggiare le minacce cyber. Fondamentale in questo caso risulta il ruolo delle terze parti, e in particolare:
    - Dei **fornitori di tecnologie**, che potrebbero in qualche modo «sopperire» (almeno in parte) alle carenze gestionali di tali operatori
    - Di altri attori quali ad esempio **«O&M» e asset manager**, che spesso di fatto gestiscono gli impianti (e che a loro volta non sembrano essere spesso così sensibili al tema)

# I rischi: Player generazione «pura» e Prosumer

- Incrociando la tipologia di attori con il ruolo ricoperto all'interno della filiera è possibile quindi ottenere questa matrice:

| | RISCHI | IMPATTI ECONOMICI |
|---|---|---|
| PLAYER GENERAZIONE «PURA» | • **Mancata produzione di energia elettrica**<br>• **Inaccessibilità ai sistemi di monitoraggio e telecontrollo** (perdita di visione e controllo sugli impianti)<br>• **Danni fisici agli impianti di produzione** | • **Riduzione del margine di contribuzione** (legato alla mancata vendita d'energia)<br>• **Penali da mancata vendita energia elettrica**<br>• **Mancato margine da fornitura di servizi ancillari**<br>• **Costi legati ai danni a impianti o persone** |
| PROSUMER (NELLA VESTE DI PRODUTTORI) | • **Mancata produzione di energia elettrica**<br>• **Danni agli impianti di produzione** | • **Riduzione dell'autoconsumo,** con conseguente **aumento della bolletta energetica**<br>• **Marginalità legata alla mancata vendita d'energia**<br>• **Costi legati a danni a impianti o persone** |

# BOX 1: I possibili attacchi agli impianti eolici

- A livello accademico uno degli ultimi filoni di ricerca in ambito accademico ha riguardato lo studio della sicurezza dei sistemi OT e in particolare il ricercatore Jason Staggs, dell'università di Tusla Oklahoma, ha focalizzato la propria attenzione nell'ambito degli impianti eolici.

- La sua ricerca si è focalizzato sull'hacking delle wind farm presenti all'interno del territorio americano, arrivando a compiere, con successo, cinque «penetration test» su altrettante wind farm ognuna caratterizzata dall'utilizzo di componenti forniti da un differente fornitore.

- In particolare Staggs ha evidenziato come i Programmable Automation Controllers (PAC) presenti all'interno di questi impianti fossero caratterizzati da:
  - Utilizzo di default password o semplici da scoprire
  - Mancanza della firma del codice
  - Utilizzo di un profilo di root permettendo di fatto di accedere agli impianti in modalità amministratore
  - Utilizzo di sistemi insicuri volti a effettuare remote management
  - Assenza di autenticazione e cifratura dei messaggi di controllo
  - Mancanza di segmentazione della rete che interconnette le differenti turbine
  - Mancanza di presidio o di misure di sicurezza adeguate volte a proteggere e limitare l'accesso fisico agli impianti

- Al fine di attaccare i parci eolici Staggs ha sfruttato la ridotta sicurezza fisica degli impianti per penetrare fisicamente all'interno delle stesse e attaccare allo switch relativo alla rete del sistema ICS presente nella turbina un dispositivo di controllo da remoto (ovvero un Raspberry PI dotato di connettività cellulare o Wi–fi).

- Ottenuto l'accesso da remoto a una turbina l'attaccante a causa della mancata segmentazione della rete può estendere il proprio attacco a tutte le altre turbine presenti all'interno del campo eolico provocando le seguenti conseguenze:
  - Blocco della produzione volto a ottenere un riscatto monetario in cambio dello sblocco della produzione
  - Danneggiamento fisico degli impianti bloccando la turbina tramite i freni di emergenza (Attacco Windshark)

- L'attaccante al fine di coprire l'attacco in corso potrebbe mandare attraverso il sistema di telecontrollo segnali errati ai proprietari degli impianti al fine di confermare il corretto funzionamento degli impianti ritardando di fatto la rilevazione di eventuali danni.

# La trasmissione e la distribuzione dell'energia elettrica

- Riferendosi all'**infrastruttura elettrica italiana** è possibile individuare **due differenti tipologie di reti** (e di attori demandate a gestirle):

**Rete di trasmissione ad alta tensione (380kV – 220 kV – 150 kV)**

consente il trasporto dell'energia elettrica su lunghe distanze su tutto il territorio nazionale, dalle centrali di produzione alle stazioni di collegamento con la linea di distribuzione (cabine primarie)

**Trasmission System Operator (TSO),** hanno in carico **la gestione della rete di trasmissione e dei flussi che transitano sulla stessa**. In Italia sono presenti 10 player all'interno di questa categoria, ma il maggiore operatore è rappresentato da Terna – Rete Elettrica Nazionale

**Rete di distribuzione:**

conclude la filiera del sistema elettrico, con la consegna dell'elettricità in media e bassa tensione agli utenti finalil

**Distribution System Operator (DSO)**, hanno in carico la **gestione della rete di distribuzione e la consegna dell'energia elettrica ai clienti finali**. In Italia sono presenti 135 operatori, ma il maggior player è rappresentato da Enel Distribuzione che detiene una quota pari all'85% della capacità installata

# I rischi: TSO, DSO

- Nonostante le peculiarità che caratterizzano le due tipologie di operatori, non sono emerse particolari differenze con riferimento ai rischi di natura «cyber»:


(*)NOTA: i clienti in bassa tensione che subiscono un'interruzione di durata superiore a 8 ore per i centri urbani e a 12 ore per le altre zone ricevono un indennizzo automatico, differenziato tra clienti domestici e clienti non domestici; dal 2020 gli indennizzi automatici saranno erogati al superamento delle 8 ore per tutti i clienti BT e delle 4 ore per tutti i clienti in media tensione.

# I rischi: Consumatori residenziali e industriali

| | RISCHI | IMPATTI ECONOMICI |
|---|---|---|
| CONSUMATORE RESIDENZIALE | • **Black-out causa mancata fornitura di energia elettrica,** in caso di attacchi alla rete elettrica<br>• **Aumento dei consumi energetici** in caso di attacchi a dispositivi IOT installati su elettrodomestici e altri dispositivi domestici | • **Aumento dei costi energetici**<br>• **Costi legati a danni a oggetti o persone** |
| CONSUMATORE INDUSTRIALE | • **Black-out a causa della mancata fornitura di energia elettrica**, in caso di attacchi alla rete elettrica<br>• **Blocco della produzione o aumento dei consumi energetici** in caso di attacchi agli asset produttivi (e.g. sistemi SCADA) | • **Costi legati all'eventuale mancata produzione**<br>• **Aumento dei costi energetici**<br>• **Costi legati a danni a impianti o persone** |

# CASE STUDY

## Gli impatti di un attacco agli impianti di produzione eolica e FV

# Obiettivi

- **La rete elettrica italiana** potrebbe teoricamente essere attaccata **in due modi distinti**:
  - Un **attacco diretto all'infrastruttura elettrica**, attraverso per esempio un intrusione nei sistemi SCADA presenti all'interno delle cabine primarie e secondarie (sulla falsariga dell'attacco alla *power grid* ucraina)
  - Un **attacco agli impianti di produzione**, volto a rendere indisponibili questi impianti e generare una carenza di energia elettrica. Tale temporanea indisponibilità, se non adeguatamente bilanciata, si potrebbe tradurre in possibili blackout

- Per scongiurare queste tipologie di attacchi è necessario quindi:
  - **incrementare la sicurezza** relativa alle **reti di trasmissione/distribuzione e agli impianti di produzione**
  - garantire la **capacità della rete di far fronte a un'indisponibilità degli impianti di produzione**

- All'interno di questa sottosezione andremo **a simulare un possibile attacco agli impianti di produzione fotovoltaici ed eolici,** al fine di **verificare l'impatto** che una loro indisponibilità potrebbe avere a livello di **mancata produzione elettrica** e di **aumento dei costi per ribilanciare la rete**

# Metodologia di analisi

- Per **stimare gli impatti di un attacco agli impianti di produzione eolica e FV** si è seguita la seguente metodologia, volta a:
  - **Individuare la potenza eolica e fotovoltaica** presente all'interno di ciascuna area geografica italiana
  - **Individuare le ore di funzionamento medie relative a ciascun impianto**
  - Creare **differenti «scenari di attacco»**, individuando **differenti livelli di potenza** colpita (5%, 10%, 25%, 50%) e **differenti livelli di mancato funzionamento** (1%, 5%, 10% delle ore medie di funzionamento), **determinando i possibili extra costi annuali legati al bilanciamento della rete.**
  - **Confrontare questi extra costi con i volumi standard del mercato dell'MSD a salire** (in particolare si è preso in considerazione il periodo ottobre 2017-gennaio 2018)

# BOX 2: Il mercato dell'MSD

- **Il Mercato per il Servizio di Dispacciamento (MSD)** è lo strumento attraverso il quale **Terna S.P.A.** si approvvigiona delle risorse necessarie alla **gestione e al controllo del sistema elettrico**
- Sul **MSD** Terna agisce come controparte centrale: **le offerte** da parte di chi è in grado di fornire energia (o di ridurne la produzione), una volta accettate, **vengono remunerate al prezzo proposto (Pay-as-Bid)**
- Al fine della gestione del mercato del MSD l'Italia è divisa nelle seguenti **aree geografiche virtuali,** di seguito riportate:

| ACRONIMO | NOME ZONA | DETTAGLIO | TIPO |
|---|---|---|---|
| **BRNN** | **Brindisi** | Localizzata in Puglia | **Polo di produzione limitato** |
| **CNOR** | **Centro Nord** | Toscana, Umbria, Marche | **Geografica** |
| **CSUD** | **Centro Sud** | Lazio, Abruzzo, Campania | **Geografica** |
| **FOGN** | **Foggia** | Localizzata in Puglia | **Polo di produzione limitato** |
| **NORD** | **Nord** | Val D'Aosta, Piemonte, Liguria, Lombardia, Trentino, Veneto, Friuli Venezia-giulia, Emilia Romagna | **Geografica** |
| **PRGP** | **Priolo Gargallo** | Localizzata in Sicilia | **Polo di produzione limitato** |
| **ROSN** | **Rossano** | Localizzata in Calabria | **Polo di produzione limitato** |
| **SARD** | **Sardegna** | | **Geografica** |
| **SICI** | **Sicilia** | | **Geografica** |
| **SUD** | **Sud** | Puglia, Basilicata, Calabria | **Geografica** |

# Nota metodologica

- Al fine di determinare gli extra costi legati al bilanciamento della rete derivante dall'indisponibilità degli impianti di produzione FV e eolica sono state formulate **due ipotesi semplificative**

- La **prima** di queste ipotesi semplificative consiste nell'aggregazione **dei volumi di energia** transati nei **poli di produzione** limitata **all'interno delle aree geografiche di appartenenza**, il che ha portato alla seguente configurazione:

| ACRONIMO | DETTAGLIO | VOLUMI SCAMBIATI MSD-UP MAGGIO 2017-APRILE 18 (MWh) | CORRISPETTIVO ECONOMICO VOLUMI SCAMBIATI MSD-UP MAGGIO 2017- APRILE 2018 (€) |
|---|---|---|---|
| NORD | Val D'Aosta, Piemonte, Liguria, Lombardia, Trentino, Veneto, Friuli Venezia-giulia, Emilia Romagna | 4.544.209,2 | 483.483.524 |
| CNOR | Toscana, Umbria, Marche | 260.135,1 | 28.259.577 |
| CSUD | Lazio, Abruzzo, Campania | 826.675,1 | 222.919.851 |
| SUD* | Puglia (include Brindisi e Foggia) , Basilicata, Calabria (include Rossano) | 2.872.248,5 | 285.968.386,3 |
| SARD | | 1.019.008,6 | 83.815.741 |
| SICI* | Include Priolo G. | 2.540.731,4 | 279.117.793,6 |

# Nota metodologica

- La **seconda** ipotesi semplificativa ha riguardato la **stima delle ore di funzionamento** degli impianti:
  - In particolare per la stima delle ore di funzionamento degli **impianti FV** sono stati utilizzati **valori medi di riferimento relativi all'area considerata**
  - **Per gli impianti eolici**, invece, le ore di utilizzo sono state identificate effettuando la **media pesata delle ore di funzionamento** degli impianti presenti in ciascuna regione dell'area considerata moltiplicate per la **potenza presente all'interno della regione** stessa

| ACRONIMO | POTENZA FV PRESENTE NELL'AREA (MW) | POTENZA FV PRESENTE NELL'AREA (MW) | POTENZA EOLICA PRESENTE NELL'AREA (MW) | ORE DI FUNZIONAMENTO MEDIE EOLICO |
|---|---|---|---|---|
| **NORD** | 8.710,3 | 1100 | 106,8 | 1851 |
| **CNOR** | 2.336 | 1200 | 165,8 | 1668 |
| **CSUD** | 2.832 | 1250 | 1.537 | 1754 |
| **SUD*** | 3.695,8 | 1300 | 5.303 | 1915 |
| **SARD** | 750,9 | 1350 | 963,8 | 1699 |
| **SICI*** | 1.369,9 | 1400 | 1.734 | 1606 |

# Analisi area geografica NORD

- L'area geografica **NORD** è caratterizzata da una notevole presenza di **impianti fotovoltaici**, per una **potenza complessiva** installata pari a **8710,3 MW** (pari al 44,2% di quella distribuita lungo il territorio nazionale). La potenza eolica risulta invece particolarmente limitata, è pari a **106,8 MW** (**1% della potenza** eolica nazionale)
- Utilizzando come dati medi di funzionamento rispettivamente **1.100 ore per gli impianti FV e 1.851 ore per quelli eolici**, otteniamo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 509.705 | 2.548.527 | 5.097.053 |
| | 10% | 1.019.411 | 5.097.053 | 10.194.106 |
| | 25% | 2.548.527 | 12.742.633 | 25.485.266 |
| | 50% | 5.097.053 | 25.485.266 | 50.970.532 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 10.519 | 52.597 | 105.193 |
| | 10% | 21.039 | 105.193 | 210.386 |
| | 25% | 52.597 | 262.983 | 525.965 |
| | 50% | 105.193 | 525.965 | 1.051.931 |

# Analisi area geografica NORD

- Il mercato a salire dell'MSD per area geografica NORD all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **4.544.209 MWh**, con una valorizzazione economica complessiva pari a **483.483.524 €** (prezzo medio: **106,40 €/MWh**).

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **si determina una mancata produzione pari a 488.953 MWh** e un conseguente **aumento dei costi per il ribilanciamento del sistema elettrico pari al 10,7%** (52.022.462 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 488.953 | 52.022.462 |

# Analisi area geografica CNOR

- L'area geografica **CNOR** è caratterizzata da una notevole presenza di potenza **fotovoltaica** (**2,4 GW**, pari al **11,9%** di quella **nazionale**). La potenza eolica, come nell'area geografica NORD, si rivela invece **limitata** (**165,8 MW**, pari al **1,7%** della **potenza eolica nazionale**)
- Utilizzando come dati di funzionamento **1.200 ore per gli impianti FV e 1.668 per quelli eolici**, otteniamo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 152.262 | 761.309 | 1.522.617 |
| | 10% | 304.523 | 1.522.617 | 3.045.235 |
| | 25% | 761.309 | 3.806.544 | 7.613.087 |
| | 50% | 1.522.617 | 7.613.087 | 15.226.174 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 15.026 | 75.129 | 150.258 |
| | 10% | 30.052 | 150.258 | 300.516 |
| | 25% | 75.129 | 375.645 | 751.289 |
| | 50% | 150.258 | 751.289 | 1.502.579 |

# Analisi area geografica CNOR

- Il mercato a salire dell'MSD per area geografica CNOR all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **260.135,1 MWh**, con una valorizzazione economica pari a **28.259.577 €** (prezzo medio: **108,60 €/MWh**)

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **determina una mancata produzione pari a 153.992 MWh** e un conseguente **un aumento dei costi per il ribilanciamento del sistema elettrico pari al 59,2 %** (16.728.753 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 153.992 | 16.728.753 |

# Analisi area geografica CSUD

- All'interno dell'area geografica **CSUD** si può identificare la presenza di **2,8 GW di potenza FV** (pari a al 14,4% della potenza totale FV nazionale). **Rilevante** appare il **peso delle installazioni eoliche** presenti che costituiscono il 15,7% della potenza nazionale eolica
- Utilizzando come dati di funzionamento **1250 ore per gli impianti FV e 1754 per quelli eolici**, ottenia-mo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 477.348 | 2.386.739 | 4.773.478 |
| | 10% | 954.696 | 4.773.478 | 9.546.956 |
| | 25% | 2.386.739 | 11.933.695 | 23.867.391 |
| | 50% | 4.773.478 | 23.867.391 | 47.734.782 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 363.573 | 1.817.865 | 3.635.730 |
| | 10% | 727.146 | 3.635.730 | 7.271.461 |
| | 25% | 1.817.865 | 9.089.326 | 18.178.652 |
| | 50% | 3.635.730 | 18.178.652 | 36.357.303 |

# Analisi area geografica CSUD

- Il mercato a salire dell'MSD per l'area geografica CSUD all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **826.675,1 MWh**, con una valorizzazione economica pari a **222.919.851 €** (prezzo medio: **269,70 €/MWh**)

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **determina una mancata produzione pari a 311.847 MWh** e un conseguente **un aumento dei costi per il ribilanciamento del sistema elettrico pari al 37,7%** (84.092.085 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 311.847 | 84.092.085 |

# Analisi area geografica SUD*

- L'**area geografica SUD** è l'area caratterizzata dalla maggiore presenza di **potenza eolica (5,3 GW** – 54% di quella distribuita lungo il territorio nazionale). La potenza fotovoltaica, seppur importante, si rivela inferiore a quella eolica (**3,7 GW** pari al 18,8% della potenza FV nazionale)
- Utilizzando come dati di funzionamento **1300 ore per gli impianti FV e 1915 per quelli eolici**, ottenia-mo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 239.176 | 1.195.881 | 2.391.761 |
| | 10% | 487.352 | 2.391.761 | 4.783.523 |
| | 25% | 1.195.881 | 5.979.403 | 11.958.807 |
| | 50% | 2.391.761 | 11.958.807 | 23.917.613 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 505.557 | 2.527.783 | 5.055.567 |
| | 10% | 1.011.113 | 5.055.567 | 10.111.134 |
| | 25% | 2.527.783 | 12.638.917 | 25.277.834 |
| | 50% | 5.055.567 | 25.277.834 | 50.555.668 |

# Analisi area geografica SUD*

- Il mercato a salire dell'MSD per area geografica SUD* all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **2.872.248,5 MWh** con una valorizzazione economica pari a 285.968.386,3 € (prezzo medio **99,6 €/MWh**)

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **determina una mancata produzione pari a 748.005 MWh** e un conseguente **un aumento dei costi per il ribilanciamento del sistema elettrico pari al 26%** (74.473.281 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 748.005 | 74.473.281 |

# Analisi area geografica SARDEGNA

- L'area geografica **SARDEGNA**, a causa della sua ventosità, è caratterizzata da un notevole **installazione di impianti eolici** i quali costituiscono con **964 MW** circa il 10% del totale della potenza eolica nazionale. **La potenza istallata FV** nell'isola è pari a **750,9 MW**
- Utilizzando come dati di funzionamento **1350 ore per gli impianti FV e 1699 per quelli eolici**, ottenia-mo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 41.690 | 208.451 | 416.902 |
| | 10% | 83.380 | 416.902 | 833.803 |
| | 25% | 208.451 | 1.042.254 | 2.084.508 |
| | 50% | 416.902 | 2.084.508 | 4.169.016 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 67.347 | 336.737 | 673.475 |
| | 10% | 134.695 | 673.475 | 1.346.950 |
| | 25% | 336.737 | 1.683.687 | 3.367.374 |
| | 50% | 673.475 | 3.367.374 | 6.734.749 |

# Analisi area geografica SARDEGNA

- Il mercato a salire dell'MSD per area geografica SARDEGNA all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **1.019.008,6 MWh** con una valorizzazione economica pari a 83.815.741 € (prezzo medio **82,3 €/MWh**)

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **determina una mancata produzione pari a 132.565 MWh** e un conseguente **un aumento dei costi per il ribilanciamento del sistema elettrico pari al 13%** (10.903.765 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 132.565 | 10.903.765 |

# Analisi area geografica SICILIA*

- L'area geografica **SICILIA**, al pari della Sardegna, è caratterizzata dalla presenza di un maggiore **potenza eolica (1734 MW** pari 17,7% della **potenza eolica** nazionale), rispetto a quella relativa agli impianti FV (**1370 MW** – 14% del totale delle **potenza FV** nazionale)
- Utilizzando come dati di funzionamento **1400 ore per gli impianti FV** e **1606 per quelli eolici**, otteniamo le seguenti simulazioni:

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 105.345 | 526.727 | 1.053.454 |
| | 10% | 210.691 | 1.053.454 | 2.106.908 |
| | 25% | 526.727 | 2.633.636 | 5.267.271 |
| | 50% | 1.053.454 | 5.267.271 | 10.534.542 |

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 152.960 | 764.801 | 1.529.602 |
| | 10% | 305.920 | 1.529.602 | 3.059.205 |
| | 25% | 764.801 | 3.824.006 | 7.648.012 |
| | 50% | 1.529.602 | 7.648.012 | 15.296.025 |

# Analisi area geografica SICILIA*

- Il mercato a salire dell'MSD per area geografica SICILIA* all'interno del periodo Maggio 2017- Aprile 2018 è stato caratterizzato da un totale di transazioni pari a **2.540.731,4 MWh** con una valorizzazione economica pari a 279.117.793,6 € (prezzo medio **109,9 €/MWh**)

- Prendendo in considerazione il **caso di un attacco** le cui conseguenze determinano una riduzione del 10% delle ore di funzionamento sul 50% della capacità eolica e fotovoltaica presente all'interno dell'area, **determina una mancata produzione pari a 235.128 MWh** e un conseguente **un aumento dei costi per il ribilanciamento del sistema elettrico pari al 9,2%** (25.830.567 €) di quelli sostenuti lungo il periodo Maggio 2017 – Aprile 2018

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) | AUMENTO COSTI MSD (€) |
|---|---|---|
| | 235.128 | 25.830.567 |

# Analisi riassuntiva ITALIA

- A livello italiano prendendo in considerazione lo scenario peggiore, ovvero un **mancata disponibilità del 50% della potenza FV e eolica per il 10% delle ore di funzionamento annuali,** si osserva una mancata produzione elettrica annuale di circa **2 TWh**, pari a:
  - **4,9% della produzione elettrica annuale da impianti FV ed eolici**
  - **2% della produzione elettrica annuale da rinnovabili**
  - **Meno dell'1% della produzione elettrica nazionale**

| POTENZA (MW) | 19.670 |
|---|---|

| MANCATA PRODUZIONE SOLARE (MWh) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 11.831 | 59.153 | 118.305 |
| | 10% | 23.661 | 118.305 | 236.610 |
| | 25% | 59.153 | 295.763 | 591.526 |
| | 50% | 118.305 | 591.526 | 1.183.052 |

# Analisi riassuntiva ITALIA

| POTENZA (MW) | 9.811 |
|---|---|

| MANCATA PRODUZIONE EOLICO (MWh) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 8.874 | 44.372 | 88.744 |
| | 10% | 17.749 | 88.744 | 177.488 |
| | 25% | 44.372 | 221.860 | 443.719 |
| | 50% | 88.744 | 443.719 | 887.438 |

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | MANCATA PRODUZIONE (MWh) |
|---|---|
| | 2.070.490 |

# Analisi riassuntiva ITALIA

- A livello italiano si osserva che per ribilanciare la mancata produzione, di circa 2 TWh, Terna sarebbe chiamata ad **aumentare i volumi transati sul mercato dell'MSD a salire** della medesima quantità, determinando un **aumento della spesa**, per la collettività, **pari a oltre 264 milioni***

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI FV (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 1.525.527 | 7.627.633 | 15.255.266 |
| | 10% | 3.051.053 | 15.255.266 | 30.510.532 |
| | 25% | 7.627.633 | 38.138.165 | 76.276.330 |
| | 50% | 15.255.266 | 76.276.330 | 152.552.660 |

(*)Nota: stima effettuata utilizzando i prezzi medi relativi ai volumi transati all'interno del mercato dell'MSD a salire nel periodo Maggio 2017- Aprile 2018

# Analisi riassuntiva ITALIA

| AUMENTO COSTO MSD PER INDISPONIBILITÀ IMPIANTI EOLICI (€) | | ORE MANCATO FUNZIONAMENTO | | |
|---|---|---|---|---|
| | | 1% | 5% | 10% |
| Potenza non disponibile | 5% | 1.114.983 | 5.574.913 | 11.149.825 |
| | 10% | 2.229.965 | 11.149.825 | 22.299.651 |
| | 25% | 5.574.913 | 27.874.563 | 55.749.127 |
| | 50% | 11.149.825 | 55.749.127 | 111.498.253 |

| CASO: 50% POTENZA FV E EOLICA INTERESSATA DALL'ATTACCO PER IL 10% DELLE ORE DI FUNZIONAMENTO | AUMENTO COSTI MSD (€) |
|---|---|
| | 264.050.913 |

# Simulazione di attacco: 21 luglio 2017

- L'analisi di un attacco, distribuito lungo il corso di un anno, agli impianti eolici e fotovoltaici ha permesso di evidenziare come il sistema elettrico italiano sembrerebbe pronto a far fronte a questa tipologia di evenienza.

- Nel corso delle nostre simulazioni si è provato a identificare cosa potrebbe accadere al sistema elettrico in caso di attacco nei confronti degli impianti eolici e fotovoltaici in una giornata estiva in cui risultano ai massimi i consumi. Al fine di effettuare la nostra analisi abbiamo scelto come giorno **il 21 luglio 2017**, utilizzando come **orario per la nostra simulazione di attacco le 12**.

- Utilizzando i dati disponibili (Fonte Terna) è possibile osservare come a quell'orario la capacità di **produzione elettrica impegnata** era stata di **51,426 GW.**

- Data la natura della giornata caratterizzata sostanzialmente da un cielo sereno possiamo ipotizzare che la **quasi totalità degli impianti fotovoltaici stesse producendo in quel determinato istante** (in particolare all'interno della simulazione ipotizzeremo che il 95% degli impianti stesse effettivamente producendo a piena potenza).

- Per quanto riguarda invece gli impianti eolici in mancanza di dati puntuali sulla ventosità della giornata in quel determinato orario abbiamo **ipotizzato** per prudenza che solo il **50% della capacità eolica installata** stesse effettivamente producendo alla massima potenza in quel determinato orario.

# Simulazione di attacco: 21 luglio 2017

- Coerentemente con i dati disponibili alle 12 del 21/7/2017 era **impegnata** la seguente **capacità**:

| TIPOLOGIA DI FONTE | CAPACITÀ UTILIZZATA (GW) |
|---|---|
| FOTOVOLTAICA | 18,7 |
| EOLICA | 4,9 |
| ALTRA FONTE (idroelettrico, termico, altro) | 27,8 |

- Identificando con **3 GW la soglia di capacità attaccata e resa indisponibile** oltre al quale si potrebbero generare dei problemi al sistema elettrico nazionale, è possibile osservare che per raggiungere questa soglia **l'attacco dovrebbe interessare il 12,7% della capacità eolica e fotovoltaica** che risultava impegnata.

- Considerando come **alle 12 del 21/7/2017**, secondo i dati Terna, ci fosse **a disposizione per il dispacciamento un potenza disponibile effettiva pari a 45,6 GW a livello italiano**, anche in caso di attacco effettuato in una singola giornata estiva il sistema elettrico italiano sembrerebbe in grado in breve tempo di coprire il calo di capacità disponibile legato al possibile attacco in corso.

# Simulazione di attacco: 21 luglio 2017

- Si deve sottolineare però come **la dismissione degli impianti di produzione elettrica** alimentati a carbone e la sostituzione con impianti a fonte rinnovabile (eolico, FV e idroelettrico), potrebbe nel futuro ampliare la possibile base di attacco a disposizione di eventuali attaccanti al sistema elettrico.

- Questo scenario potrebbe aumentare la possibilità di eventuali blackout e disservizi, nel caso in cui non vengano effettuati **adeguati investimenti** volti a garantire sia la sicurezza di questi impianti che il mantenimento di capacità disponibile adeguata in caso di malfunzionamenti agli impianti eolici e FV ( es. dotandosi di sistemi di storage e/o attraverso l'utilizzo di meccanismi quali ad esempio il capacity market)

POLITECNICO
MILANO 1863

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

# Il contesto normativo 3

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

# Obiettivi della sezione

- Il presente capitolo ha l'obiettivo di fornire un'**evoluzione del quadro normativo** relativo alla tematica della **cybersecurity**, con un particolare focus sull'aspetto energetico, focalizzando l'attenzione sia sulle **direttive nazionali** che su quelle **internazionali**

- In particolare saranno analizzate:
  - A livello **europeo**: la **direttiva NIS** (Network and Information Security – EU 2016/1148)
  - A livello **italiano**:
    - il **Quadro Strategico Nazionale Per La Sicurezza Dello Spazio Cibernetico**
    - il **DPCM 13 aprile 2017** (DPCM «Gentiloni»)
    - il **Piano Nazionale Per La Protezione Cibernetica e La Sicurezza Informatica**

- **Inoltre, verranno illustrate** le linee guida della **Strategia Energetica Nazionale (SEN)**, con particolare riferimento ai piani d'azione sul fronte della cybersecurity

# **Europa:** la direttiva NIS - gli obiettivi

- La **direttiva NIS** – Network and Information Security – (EU 2016/1148) rappresenta, in ambito europeo, **il primo insieme di regole** relative alla **sicurezza delle reti e dei sistemi**

- La **direttiva prescrive** agli stati membri dell'UE l'implementazione di **piani strutturati volti a impedire** che le reti e i sistemi informativi, a causa della loro importanza per il corretto funzionamento delle attività economiche e sociali, possano diventare facile bersaglio di **azioni tese a danneggiare o interromperne la loro operatività**

- In particolare la direttiva NIS si prefigge i seguenti obiettivi:
  - L'istituzione per ciascuno stato membro di un'**autorità nazionale competente per la sicurezza informatica** e di un **Computer Security Incident Response Team (CSIRT)**
  - L'istituzione di un **gruppo di cooperazione**, al fine d'agevolare la cooperazione strategica e lo scambio di informazioni inerenti ai rischi e alla gestione degli incidenti di sicurezza informatica
  - L'applicazione di **obblighi di cybersecurity** in capo agli **operatori di servizi essenziali (OES)**

# **Europa:** la direttiva NIS - gli operatori di servizi essenziali (OES)

- Ogni stato europeo deve:
  - trasporre la normativa **all'interno degli ordinamenti nazionali entro maggio 2018***
  - **identificare**, entro novembre 2018, gli **operatori di servizi essenziali** che saranno chiamati a implementare la normativa NIS

- Le nazioni dovranno identificare gli operatori come **fornitori di servizi essenziali** nel caso in cui:
  - Il **servizio** fornito è **essenziale** per il **mantenimento di attività sociali e/o economiche fondamentali**
  - La **fornitura** di tale servizio **dipende dalla rete e dai sistemi informativi**, per cui un incidente inerente a queste infrastrutture comporterebbe effetti negativi rilevanti sulla fornitura del servizio
  - L'**impatto** di tali **eventi negativi** - valutati attraverso il numero di utenti, la quota di mercato dell'operatore e l'area interessata dal malfunzionamento - risulta **rilevante all'interno del contesto nazionale**

(*)Nota: in Italia la direttiva è stata recepita tramite il Decreto Attuativo del Consiglio dei Ministri del 26/05/2018, ed è entrata in vigore il 26/06/2018.

# **Europa:** la direttiva NIS - i settori relativi ai servizi essenziali

- Gli operatori di servizi essenziali saranno identificati all'interno dei seguenti settori:
  - Trasporti
  - Settore bancario
  - Infrastrutture dei mercati finanziari
  - Settore sanitario
  - Fornitura e distribuzione di acqua potabile
  - Infrastrutture digitali
  - **Energia**:
    - **Energia elettrica**, ovvero i gestori del sistema del sistema di **trasmissione**, del sistema di **distribuzione** e le imprese elettriche che esercitano l'attività di **fornitura**;
    - **Petrolio**, ovvero i gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto del petrolio e i gestori degli oleodotti
    - **Gas**, ovvero i gestori del sistema di trasmissione e di distribuzione, i gestori degli impianti di raffinazione e trattamento del gas naturale, i gestori del sistema di stoccaggio e del sistema GNL e le imprese fornitrici

# **Europa:** la direttiva NIS - gli obblighi per gli OES

- Gli operatori di servizi essenziali dovranno:
  - adottare **misure adeguate atte a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete** e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali

  - **fornire all'autorità competente NIS:**
    - Le **informazioni necessarie a valutare la sicurezza della loro rete** e dei sistemi informativi, compresi i documenti relativi alle politiche di sicurezza
    - La **prova dell'effettiva attuazione delle politiche di sicurezza**, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato

  - **notificare** al Computer Security Incident Response Team (CSIRT) nazionale e per conoscenza alle autorità competenti NIS, **ogni incidente** avente un impatto **rilevante sulla continuità del servizio fornito**

# **Italia:** il Quadro strategico nazionale per la sicurezza dello spazio cibernetico

- Approvato nel **dicembre 2013, il quadro strategico nazionale (QSN)** mirava ad accrescere la capacità del paese di contrastare le minacce provenienti dal cyberspazio indirizzando gli sforzi nazionali verso obiettivi comuni

- A tal fine il documento individuava **6 indirizzi strategici** (declinati in 11 indirizzi operativi), volti a:
  - Migliorare le **capacità tecnologiche**, **operative e di analisi** degli attori istituzionali
  - Potenziare le capacità di **difesa delle infrastrutture critiche nazionali**
  - Incentivare la **cooperazione tra istituzioni e imprese nazionali**
  - Promuovere e diffondere una **cultura della sicurezza cibernetica**
  - Rafforzare le capacità di **contrasto alla diffusione di attività e contenuti illegali online**
  - Rafforzare la **cooperazione internazionale**

- All'interno del quadro strategico si **individuano** inoltre **i ruoli e i compiti dei soggetti pubblici** e si afferma la **centralità della partnership pubblico-privato**, al fine di garantire la protezione cibernetica

# **Italia:** il DPCM «Gentiloni» - (DPCM 13 aprile 2017)

- Il **DPCM Gentiloni** sostituisce il precedente DPCM Monti (DPCM 24 gennaio 2013), e attraverso la razionalizzazione **dell'architettura nazionale per la cybersecurity** garantisce una migliore capacità di **coordinamento, preparazione e gestione di eventuali crisi di natura cibernetica**

- In particolare il DPCM Gentiloni prevede:
  - Il rafforzamento del ruolo del ***Dipartimento delle informazioni per la Sicurezza*** (DIS) – al cui interno è **costituito il *Nucleo Sicurezza Cibernetica*** (NSC) – chiamato a definire linee di azione volte e innalzare e migliorare i livelli di sicurezza che caratterizzano le reti e le infrastrutture nazionali.
  - **l'istituzione del *Centro di Valutazione e Certificazione Nazionale***, con lo scopo di verificare la sicurezza dei prodotti e dispositivi destinati alle infrastrutture critiche nazionali
  - Il **sempre maggiore coinvolgimento degli operatori privati**, quali ad esempio gli operatori di servizi essenziali, per garantire una corretta diffusione delle informazioni relative agli attacchi in atto e delle best practice da adottare al fine di minimizzarne gli impatti

# **Italia:** il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica

- Aggiornato nel marzo 2017, il **Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica** recepisce il DPCM Gentiloni attraverso:
  - L'**aggiornamento** degli indirizzi emersi dal **QSN**
  - La **razionalizzazione del processo decisionale** in caso di crisi cibernetiche, attraverso una **semplificazione dell'architettura nazionale per la cybersecurity**
  - La **progressiva fusione** dei due **Computer Emergency Response Team** (CERT), ovvero del CERT Nazionale e del CERT relativo alla Pubblica Amministrazione, al fine di assicurare una migliore capacità di rilevazione e analisi degli incidenti cibernetici

- Il Piano Nazionale mira inoltre a sviluppare strumenti operativi di tipo tecnico e tecnologico attraverso:
  - L'istituzione di un **centro di valutazione e certificazione nazionale ICT**, volto a valutare la componentistica destinata ad infrastrutture critiche e strategiche
  - Lo sviluppo di un **partenariato pubblico-privato**, attraverso forme di venture capital
  - L'istituzione di un **Centro nazionale di ricerca e sviluppo in cybersecurity**
  - La costituzione di un **Centro Nazionale di crittografia**

# **Italia:** la Strategia Energetica Nazionale - le linee d'azione sulla cybersecurity

- La Strategia Energetica Nazionale in ambito cybersecurity energetica prescrive **due differenti linee di azione**, riguardanti rispettivamente:
  - Lo sviluppo di un **piano di ricerca in ambito cybersecurity nel settore elettrico**
  - Lo sviluppo della **coordinazione e la cooperazione** (a livello nazionale e internazionale)

- Il **piano della ricerca cyber nel settore elettrico** affronterà il tema dell'innovazione delle infrastrutture attraverso:
  - Attività di **modellistica e simulazione** relativamente **alle minacce cyber nei sistemi di controllo**
  - Attività sperimentali volte a **verificare le misure di sicurezza preventive e reattive** usate nei sistemi di comunicazione del settore elettrico
  - **Dimostrazione di scenari cyber** al fine di rafforzare la resilienza dei sistemi
  - **Partecipazione attive ai comitati di standardizzazione** e ai **gruppi di lavoro** dei regolamenti UE in tema cybersecurity
  - Lo **sviluppo di metodologie**, strumenti, piattaforme, buone pratiche e documenti di guidance **per la valutazione del rischio cyber delle infrastrutture energetiche**

# **Italia:** Strategia Energetica Nazionale - le linee d'azione sulla cybersecurity

- La SEN prescrive non solo una **collaborazione tra** le diverse **nazioni e enti europei/internazionali**, ma anche un **cooperazione pubblico-privato** a livello nazionale

- Sul fronte delle **collaborazioni internazionali**, diverse istituzioni (quali ad esempio la NATO e l'ENISA) hanno avviato **esercizi e simulazioni**, volte a migliorare la capacità da parte delle nazioni di **sviluppare piani d'azione** coordinati e favorire lo scambio di informazioni tra gli attori

- Per quanto concerne invece la **cooperazione pubblico-privato**, le università, gli istituti di ricerca e il settore privato sono chiamate a:
  - **Collaborare** all'interno dei **piani di ricerca** relativamente alle tematiche di cybersecurity
  - **Partecipare** all'interno delle **esercitazioni congiunte nazionali**, al fine di testare scenari ipotetici di attacchi informatici e favorire lo scambio di informazioni
  - Partecipare allo **sviluppo di sistemi di prevenzione e risposta**
  - **Garantire il controllo delle filiere tecnologiche**, per le quali risulta fondamentale la **standardizzazione e certificazione dei prodotti, apparati e sistemi** destinati alle infrastrutture critiche

# Messaggi chiave

- L'analisi del quadro normative e delle iniziative «istituzionali» permette di osservare come, in **mancanza di direttive specifiche focalizzate sul settore energetico**, il tema della cybersecurity venga analizzato all'interno di **normative di carattere più generale**, che si focalizzano in particolare sulla protezione delle **infrastrutture critiche**

- Le normative analizzate sono piuttosto di **alto livello**, e non identificano **un piano di azioni operative specifiche** (in termini di soluzioni organizzative e tecnologiche) che le imprese dovrebbero implementare al fine di raggiungere livelli di sicurezza minimi

- Inoltre, desta qualche perplessità il fatto che tra gli operatori di servizi essenziali del settore energetico non figurino (almeno in modo «esplicito») i produttori di energia elettrica

- Le iniziative previste nell'ambito della SEN pongono molta enfasi sulle attività di ricerca e sulla necessità di rafforzare le **collaborazioni tra** le diverse **nazioni ed enti europei/internazionali**, nonché le **cooperazioni pubblico-privato** a livello nazionale

- Inoltre, si ravvisa la necessità di creare **gruppi di standardizzazione** a livello internazionale e nazionale finalizzati a **certificare i prodotti** che saranno utilizzati a livello di infrastrutture critiche, nonché a definire **standard** (di processo e prodotto)per il conseguimento di livelli di sicurezza «minimi» condivisi (che saranno oggetto di approfondimento nel prossimo capitolo)

POLITECNICO
MILANO 1863

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

es

# Le soluzioni tecnologico - organizzative: il ruolo degli standard 4

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

# La gestione della cybersecurity industriale in ambito energetico

- Per rispondere alle minacce di natura «cyber», gli operatori della filiera elettrica sono chiamati ad adottare opportune **contromisure**

- Tali contromisure prevedono un mix di soluzioni di natura organizzativa e tecnologica finalizzate a:
  - ridurre le vulnerabilità (e quindi la probabilità che un eventuale attacco vada buon fine)
  - ridurre gli eventuali danni conseguenti a un incidente di sicurezza

- Si tratta quindi di mettere a punto un sistema di gestione della cybersecurity in ambito industriale (in modo del tutto analogo a quanto avviene per l'IT «tradizionale»), tenendo conto delle peculiarità dell'ambiente OT (per esempio, la priorità del requisito di disponibilità rispetto all'integrità e alla riservatezza)

- Tale **cybersecurity management system**, se ben progettato e messo in pratica, dovrebbe garantire un livello di esposizione al rischio che sia sempre inferiore a quello massimo consentito (in base alle normative e/o al risk appetite complessivo della specifica impresa)

- Va da sé che, vista l'estrema dinamicità del contesto, e la continua nascita di nuove minacce, particolare attenzione va data al monitoraggio continuo e al conseguente aggiornamento delle contromisure

# Gli standard di riferimento

- Come sempre accade in questi casi, dopo una fase «embrionale» (in cui le imprese «pioniere» hanno iniziato a sperimentare modelli e soluzioni organizzative e tecnologiche) stanno emergendo degli **standard** di riferimento anche nell'ambito della sicurezza industriale in ambito energetico

- In particolare, gli **standard di riferimento** più rilevanti (nell'ambito della sicurezza OT delle imprese energetiche) sono **cinque**, ovvero:
  - ISA 62443
  - IEC 62351
  - NERC 1300 CIP
  - NIST Cybersecurity Framework (e NIST 800-82)
  - ISO 27019

- Alcuni di tali standard fanno riferimento alle procedure e alle soluzioni che devono essere adottate dagli operatori energetici, mentre altri si focalizzano sui requisiti degli asset industriali da proteggere (e quindi dei loro componenti). Il ruolo dei fornitori di tecnologia risulta infatti molto rilevante, in quanto il livello di sicurezza «intrinseco» dei prodotti (componenti, sotto-sistemi, ecc) che compongono un impianto di generazione/trasmissione/distribuzione dell'energia elettrica è fondamentale rilevanza nel determinare il livello di esposizione complessiva al rischio dell'impianto stesso

# IEC-62443/ ISA 99

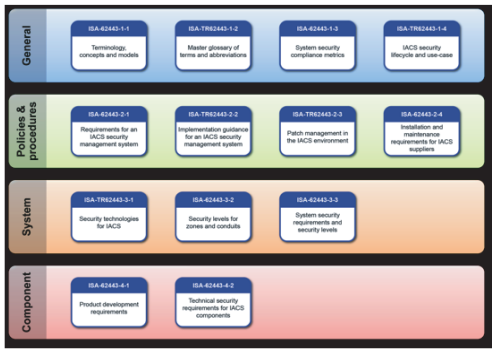
- **Lo standard IEC-62443**, precedentemente noto con il nome di ISA 99, è stato realizzato dalla International Society for Automation (ISA) e dalla International Electrotechnical Commission (IEC) nel 2010.

- Lo standard **definisce le linee guida da utilizzare per incrementare la sicurezza informatica degli Industrial Control System**, volto a creare un sistema di controllo che permetta di:
  - Garantire un adeguato livello di security contro le minacce esterne
  - Aumentare il livello di protezione dei dati
  - Aumentare l'affidabilità dei sistemi ICS

- Lo standard **si applica non solo agli utenti finali** (ovvero i possessori degli impianti), ma **soprattutto anche ai produttori degli apparati ICS**, infatti:
  - **Gli utilizzatori finali possono utilizzare questo standard per valutare meglio i prodotti offerti dai fornitori tecnologici**, in quanto la IEC-62443 semplifica la definizioni dei requisiti di sicurezza richiesti nei confronti dei fornitori, identificando un «livello di sicurezza richiesto» e non più a una lista di feature di sicurezza individuali
  - **I vendor possono dimostrare i livelli di sicurezza offerti dai propri prodotti certificandoli** secondo i livelli di sicurezza target indentificati all'interno della IEC-62443

# IEC-62443/ ISA 99: il framework

- Il framework dello standard IEC 62443 è organizzato all'interno di quattro categorie:
  - **GENERAL (IEC-62443-1)**: contiene i concetti, i modelli e la terminologia relativa agli Industrial Automation and Control Systems (IACS)
  - **POLICIES & PROCEDURES (IEC-62443-2)**: analizza i requisiti legati alla creazione e al mantenimento di un programma di sicurezza relativa agli IACS
  - **SYSTEM (IEC-62443-3)**: contiene i requisiti e le tecnologie volte a garantire la sicurezza degli IACS e introduce i concetti di «Zone» e «Conduit»
  - **COMPONENT (IEC-62443-4)**: contiene i requisiti di sicurezza per lo sviluppo di componenti IACS



# IEC-62443/ ISA 99: i livelli di sicurezza target e attuali

- Lo standard IEC-62443 prescrive alle imprese di effettuare una risk analysis volta a identificare le vulnerabilità carico dei propri asset.
- In seguito alla risk analysis, in funzione delle vulnerabilità identificate, dei possibili impatti rilevati e della probabilità di accadimento, a ciascun asset sarà assegnato uno dei seguenti 5 livelli di sicurezza **target da raggiungere**

| Security Level | Definizione |
|---|---|
| SECURITY LEVEL 0 (SL 0) | Nessuna protezione richiesta |
| SECURITY LEVEL 1 (SL 1) | Protezione contro violazioni occasionali o casuali (i.e. configurazione di parametri non consentiti, intercettazione di una password in chiaro sulla rete) |
| SECURITY LEVEL 1 (SL 1) | Protezione contro violazioni intenzionali effettuate con mezzi scarsi, con risorse scarse, competenza generiche del sistema e motivazione scarsa (i.e. virus, sfruttamento delle vulnerabilità più comuni) |
| SECURITY LEVEL 1 (SL 1) | Protezione contro violazioni intenzionali complesse (i.e. exploit di sistemi operativi, conoscenza avanzata dei sistemi target) |
| SECURITY LEVEL 1 (SL 1) | Protezione contro violazioni intenzionali alla rete di processo, effettuate con mezzi sofisticati con risorse ingenti, competenza specifiche del sistema e forte motivazione(i.e. StuxNet attack) |

Focus sulla componente IT

- Dopo aver identificato i livelli di sicurezza target, questi sono **confrontati con i livelli di sicurezza attuali** che caratterizzano i medesimi asset, **andando a colmare gli eventuali gap** tramite l'implementazione di soluzioni tecnologiche e di nuove policy organizzative.

# BOX 1: IEC-62443 / ISA 99 – Le contromisure di sicurezza

- La IEC-62443 identifica al suo interno delle contromisure generali sia di tipo tecnico sia di tipo gestionale volte a migliorare la sicurezza dei sistemi ICS.

| Misure Tecniche | Misure organizzative/gestionali |
|---|---|
| • **Antivirus, antispyware**<br>• **Firewalls, traffic analyzers**<br>• **Encryption, Virtual Private Networks** (VPN)<br>• **Passwords, sistemi di autentificazione**<br>• **Controllo degli accessi, Intrusion Detection Systems** (IDS), **Intrusion Prevention Systems** (IPS)<br>• **Network Segmentation** | • **Rights management e Access control**, ovvero la definizione delle azioni che un utente può compiere all'interno del sistema e delle reti<br>• **Patch management** (relativa ai sistemi operativi e alle applicazione)<br>• **Security incidents managements**<br>• **Training del personale** |

- All'interno delle pagine seguenti si effettuerà un approfondimento relativo all'applicazione all'interno dei sistemi OT di alcune alle tecnologie, quali:
  - FIREWALL
  - INTRUSION DETECTION SYSTEM /INTRUSION PREVENTION SYSTEMS
  - ANTIVIRUS / ANTI-MALAWARE
  - VPN

# BOX 2: le soluzioni tecnologiche per la cybersecurity - FIREWALL

- I firewall tipicamente costituiscono la **prima linea di difesa perimetrale tra due differenti reti**, una interna detta **Local Area Network (LAN)** e una esterna detta Wide Area Network, costituita, nella maggior parte dei casi, dalla rete internet e permettono anche di limitare l'accesso a sezioni della rete interna aziendale.
- Il compito del firewall è infatti quello di monitorare e **filtrare, sulla base di apposite regole, il traffico dati che intercorre tra due reti**, al fine di prevenire possibili accessi indesiderati all'interno delle reti aziendali o a segmenti di esse.
- A livello di classificazione dei firewall si identificano le seguenti tre categorie:
  - **PACKET FILTERING FIREWALL**: il firewall più basico, in quanto effettua solamente un controllo a livello di pacchetti (livello 3 dell'Open Systems Interconnection model) valutando informazioni quali ad esempio gli indirizzi IP. I vantaggi di questo sistema di firewall sono costi ridotti e un basso impatto sulle performance.
  - **STATEFUL INSPECTION FIREWALL**: questo firewall agisce sul livello 4 dell'Open Systems Interconnection model effettuando un controllo del contenuto dei pacchetti al fine di indentificare o permettere il transito del pacchetto stesso
  - **APPLICATION PROXY GATEWAY FIREWALL**: Questa classe di firewall esamina i pacchetti a livello dell'application layer filtrando il traffico in base alle regole specifiche dell'applicazione o dei protocolli. I firewall di questo tipo offrono un elevato livello di sicurezza, ma possono generare problemi a livello delle prestazioni di rete

- All'interno dei sistemi ICS, i **firewall** sono principalmente **utilizzati al fine dei separare la rete dei sistemi ICS da quella aziendale**, permettendo di migliorare la sicurezza di sistemi OT attraverso una **riduzione degli accessi indesiderati da e verso la rete dei sistemi ICS**, permettendo anche di migliorare le tempistiche di risposta di questi sistemi attraverso la rimozione delle comunicazioni non necessarie effettuate sulla rete ICS.
- All'interno dei **sistemi ICS** i firewall dovrebbero essere configurati il fine di **bloccare di default tutte le comunicazioni in entrata e in uscita**, abilitando solo le connessioni che si ritengono affidabili inserendole come regole all'interno della whitelist del firewall.

# BOX 3: le soluzioni tecnologiche per la cybersecurity – IDS/IPS

- **Gli Intrusion Detection System – Intrusion Prevention Systems** sono software volti **ad analizzare il traffico di dati che si origina all'interno di una rete al fine di identificare (IDS) e bloccare (IPS) possibili «intrusioni»** all'interno della stessa.

- Al fine di identificare eventuali intrusioni, questi sistemi monitorano non solo il flusso di traffico sulla rete, ma analizzano anche attività sospette quali l'utilizzo di porte solitamente non utilizzate o cambi all'interno dei file del sistema operativo.

- L'analisi del traffico, specialmente in contesti caratterizzati da elevato traffico o da limitate capacità di calcolo, impone un **trade off tra efficacia nell'individuare possibili minacce e efficienza nell'utilizzo della potenza di calcolo.**

- Per questo gli IPS-IDS presenti ad esempio nelle cabine elettriche operano secondo una **duplice modalità operativa**. La prima modalità, detta **«lightweight mode»**, risulta **sempre attiva** ed è **volta ad analizzare solo parte dei pacchetti** che transitano all'interno della rete, mentre la **«comprehensive mode», è attivata solamente in caso di individuazione di una minaccia** da parte della «lightweight mode», determinando la **scansione completa del traffico all'interno della rete**, e l'aumento dell'utilizzo della capacità computazionale

## BOX 4: le soluzioni tecnologiche per la cybersecurity – ANTIVIRUS/ANTI - MALWARE

- **I sistemi antivirus/antimalware valutano i file che sono presenti all'interno dei database aziendali e che transitano all'interno confrontandoli con una lista di possibili minacce conosciute**, e nel caso in cui un file sia riconosciuto come un possibile virus/malaware sarà il software stesso a eliminarlo o a porlo in quarantena al fine di limitarne la propagazione all'interno dei sistemi informativi aziendali.

- I software antivirus possono essere installati all'interno delle workstations, dei server o dei firewall e al fine di garantire la massima protezione **devono funzionare full-time.**

- Il loro uso rappresenta **all'interno del mondo IT una pratica di sicurezza standard,** mentre il loro utilizzo **all'interno del mondo OT deve essere preceduto da una analisi volta a verificarne la compatibilità con i sistemi e gli impatti sull'operatività degli impianti**. Queste verifiche devono essere ripetute ogni qual volta che vengono rilasciati degli aggiornamenti alla versione del software antivirus/anti-malaware.

# BOX 5: le soluzioni tecnologiche per la cybersecurity – VPN

- Le VPN sono un metodo di criptazione delle comunicazioni volto a creare **una rete di comunicazione sicura attraverso internet, utilizzando il meccanismo del tunneling.**

- La sicurezza all'interno della VPN è garantita attraverso un **controllo degli accessi**, in quanto solamente gli utenti registrati possono accedere alla rete e **algoritmi di cifratura**, volti a proteggere la riservatezza della comunicazione che avviene all'interno della VPN.

- All'interno dei sistemi OT, le VPN sono utilizzate soprattutto per garantire un accesso sicuro alla rete di controllo dei sistemi ICS, partendo da reti non sicure come potrebbero essere Internet o la rete corporate aziendale. Le **VPN** se propriamente configurate possono **migliorare la sicurezza e i tempi di risposta dei sistemi ICS** attraverso uno stretto controllo degli accessi e la rimozione di tutto il traffico non essenziale rivolto nei confronti della rete di controllo dei sistemi ICS.

# IEC-62443/ ISA 99 : Security zone e Conduit

- La IEC-62443 introduce i concetti di «**Security zone**» e «**Conduit**» come strumenti volti a segmentare e isolare i vari sotto-sistemi di un sistema di sistema di controllo.

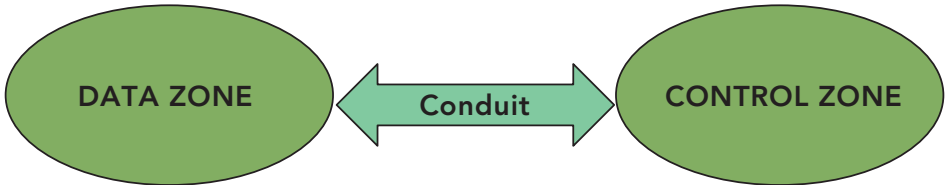
- Una **«Security zone»** è definita come un raggruppamento di asset logici o fisici che condividono gli stessi requisiti di sicurezza definiti in base a fattori quali la criticità delle minacce e i possibili impatti. Una zona deve avere dei confini definiti (che possono essere fisici o logici) volti a definire gli asset che sono inclusi all'interno della stessa.

- Da questa definizione è possibile identificare come al fine di conoscere le criticità di sicurezza e i possibili impatti relativi a ciascun asset sia necessario svolgere una accurata fase risk assessment volta a identificare gli asset presenti all'interno dell'impresa e i relativi rischi/minacce ad essi associati.

- Gli asset presenti all'interno di una «security zone» devono presentare un security level pari o superiore a quello definito dal livello di sicurezza target. Nel caso questa condizione non sia verificata l'impresa è chiamata a implementare azioni correttive – attraverso nuove tecnologie o policy – volte a raggiungere i livelli di sicurezza target

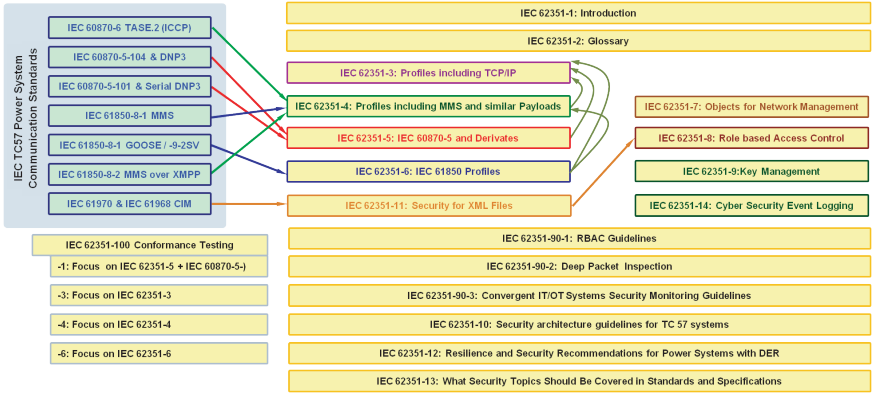
# IEC-62443 / ISA 99 : Security zone e Conduit

- Lo standard prevede che le **comunicazioni tra le diverse zone avvengano attraverso un «conduit».**
- Il **«conduit»** è definito come un percorso per garantire il passaggio di informazioni tra due zone ed è dotato di tutte le funzioni di sicurezza volte a **controllare l'accesso alle zone, a proteggere da malaware e a garantire l'integrità e la riservatezza del traffico sulla rete.**
- Tipicamente i «conduit» sono utilizzati al fine di mitigare le differenza relative ai livelli di sicurezza che possono sussistere tra differenti zone e per garantire un flusso sicuro di informazioni possono essere implementate tecnologie quali:
  - **INDUSTRIAL FIREWALL**
  - **VPN**



# IEC 62351

- Lo standard **IEC-62351** (*Power systems management and associated information exchange – Data and communications security*) è stato sviluppato del Working Group 15, che fa parte della commissione tecnica 57 (TC 57) dell'International Electrotechnical Commission (IEC), un'organizzazione no-profit internazionale quasi-governativa che si occupa di standardizzazione e di conformity assessment per tutti i prodotti, le reti e i servizi elettrici ed elettronici
- La TC 57, in particolare, si occupa di sviluppare standard e soluzioni end-to-end per la sicurezza dei protocolli di comunicazione nell'ambito dei sistemi di produzione dell'energia
- L'utilizzo di adeguate **policies, procedure e tecnologie** volte a implementare una sicurezza di tipo end-to-end permette infatti di ritenere che lo scambio di informazioni tra un mittente e un destinatario sia al sicuro da possibili accessi non autorizzati o da modifiche.



# IEC 62351

- La IEC 62351 prevede di coprire, nell'ordine, la 4 requisiti di sicurezza:
  - **AVAILABILITY**: la possibilità di accedere ai dati (che potrebbe invece essere compromessa da attacchi di tipo «Denial of Service»)
  - **INTEGRITY**: ovvero la prevenzione relativa al furto o alla modifica non autorizzata dei dati
  - **CONFIDENTIALITY**: ovvero la prevenzione dell'accesso non autorizzato alle informazioni
  - **NON-REPUDIATION/ACCOUNTABILITY:** attraverso strumenti che prevedano la registrazione di tutte le attività (e i soggetti) che hanno avuto accesso/hanno modificato i dati

- E' una famiglia di standard che definisce in modo completo le tecniche di protezione dei protocolli IEC destinati all'impiego per il telecontrollo dei sistemi elettrici e specifica pertanto i meccanismi di protezione dei canali di comunicazione e dei messaggi. Questo standard definisce inoltre le tecniche per il Role Base Access Control, il Key Management ed il monitoraggio dei sistemi della grid. La famiglia di standard IEC 62351 include anche le norme di conformance relative.

# NERC CIP 1300

- Lo **standard NERC CIP 1300**, messo a punto dalla North American Electric Reliability Corporation (NERC), identifica i **requisiti minimi da implementare** e mantenere al fine di garantire la sicurezza cibernetica degli asset presenti all'interno dei **sistemi generazione, trasmissione e distribuzione del sistema elettrico**

- Lo standard NERC CIP 1300 può essere suddiviso nei seguenti **8 differenti ambiti**:
  - **CIP-002 CYBER SECURITY – Critical Cyber Asset Identification**
    Le imprese sono chiamate a identificare quelli che sono gli asset critici per il funzionamento dell'infrastruttura elettrica, e dovrebbero svolgere una analisi di tipo qualitativa volta a identificare e descrivere le minacce a carico degli asset, le probabilità di accadimento e le conseguenze di questi possibili rischi

  - **CIP-003 CYBER SECURITY – Security Management Controls**
    Le imprese sono chiamate a creare un framework volto a gestire la sicurezza dei sistemi OT, all'interno del quale dovrebbero essere elencate le normative a cui è soggetta e i principali principi di sicurezza e gli standard utilizzati dall'impresa per realizzare il proprio piano di cybersecurity

# NERC CIP 1300

- **CIP-004 CYBER SECURITY – Personnel & Training**
  Tutto il personale che ha un ruolo nella gestione della sicurezza del sistema elettrico, inclusi coloro che hanno accesso agli asset devono collaborare al fine di garantire la sicurezza dell'infrastruttura elettrica. Le imprese sono chiamate inoltre ad effettuare un controllo dei precedenti penali di tutto il personale ed a limitare l'accesso agli asset solamente al personale strettamente necessario, che dovrà essere rivisto su base trimestrale o in seguito a un ambio di ruolo/posizione all'interno dell'organigramma aziendale

- **CIP-005 CYBER SECURITY – Electronic Security Perimeter**
  Il perimetro «elettronico» delle reti aziendali dell'impresa dovrebbe essere adeguatamente delineato e implementato. Ogni accesso alle reti aziendali che non avvenga all'interno di porte controllate dovrebbe essere bloccato di default mentre il traffico che avviene all'interno della rete dovrebbe essere criptato usando almeno una cifratura a 128 bit

- **CIP-006 CYBER SECURITY – Physical Security Of Cyber Systems**
  Le imprese dovrebbero controllare i perimetri fisici di accesso agli impianti, implementando un sistema di autentificazione a due fattori centralizzato di cui dovrebbero essere controllati mensilmente per verificare accessi non autorizzati e mantenuti i log per 90 giorni. Le imprese dovrebbero inoltre richiedere ai dipendenti e ai visitatori di indossare un badge di riconoscimento con foto. Tutti questi controlli volti ad assicurare il perimetro fisico dell'infrastruttura devono essere rivisti su base trimestrale

# NERC CIP 1300

- **CIP-007 CYBER SECURITY – System Security Management**
  L'impresa oltre alla mappatura degli asset critici, dovrebbe fare anche effettuare una mappatura di tutti gli asset non critici, bloccare tutte le porte e i servizi informativi che non sono necessari all'operatività dell'infrastruttura, dotarsi di sistemi antivirus e anti-malaware con update delle minacce da effettuare almeno ogni 24 ore, e dovrebbe mantenere di log centralizzato volto generare dati, da tenere almeno per 90 giorni, sulle operazioni che avvengono all'interno dell'infrastruttura elettrica

- **CIP-008 CYBER SECURITY – Incident Reporting And Responce Planning**
  Le imprese in caso di incidente sono chiamate a avvertire le autorità competenti e devono conservare i registri di tutti gli incidenti, compresi i system e host logs, i video delle telecamere e i registri relativi agli accessi fisici agli impianti

- **CIP-009 CYBER SECURITY – Recovery Plans For Cyber Systems**
  Le imprese devono prevedere piani di ripristino dell'operatività dell'infrastruttura volti a minimizzare i tempi di fermo, coinvolgendo all'interno degli stessi anche i fornitori. Al fine di garantire la minimizzazione del downtime l'impresa dovrebbe creare un backup della configurazione dell'infrastruttura comprendente le applicazioni e le configurazioni dei sistemi operativi e delle rete. All'interno dei backup dovrebbero essere è presenti anche i file relativi ai meccanismi di autentificazione

# NIST Cybersecurity Framework

- **Il National Institute of Standards and Technology (NIST)** ha sviluppato un **Cybersecurity Framework** volto a supportare le imprese nella creazione di un sistema volto alla gestione della cybersecurity.

- Il **Cybersecurity Framework** è stato sviluppato come **strumento** a disposizione delle imprese per confrontare i propri processi e la propria organizzazione, con i quattro modelli/Implementation Tiers (Partial, Risk Informed, Repetable, Adaptive) descritti all'interno del framework, al fine di **evidenziare eventuali carenze e gap nell'approccio alla gestione dei rischi di cybersecurity e sviluppare piani di miglioramento**, volti a identificare le attività e i processi che sono più importanti per i «critical service» dell'impresa, massimizzando di fatto l'impatto degli investimenti in sicurezza.

# NIST Cybersecurity Framework

- Il NIST Cybersecurity Framework prevede l'identificazione di **5 «core funtions»** che dovrebbero essere monitorate costantemente e contemporaneamente dalle imprese per creare una cultura aziendale volta alla gestione dei rischi relativi alla cybersecurity:
  - **IDENTIFY**: le imprese sono chiamate a sviluppare una cultura aziendale volta a identificare e gestire i rischi di cybersecurity relativi ai sistemi/asset, alle persone e ai dati
  - **PROTECT**: dopo aver identificato i rischi di cybersecurity a carico degli asset aziendali, le imprese sono chiamate a sviluppare e implementare misure appropriate di sicurezza al fine di assicurare l'erogazione di quelli che sono i servizi critici
  - **DETECT**: le imprese inoltre devono anche dotarsi di strumenti adeguati volti a monitorare costantemente quello che avviene all'interno dei propri perimetri, identificando tempestivamente possibili attacchi di cybersecurity in atto
  - **RESPOND** and **RECOVER**: le imprese sono chiamate a creare piani strutturati e appropriati volti a rispondere adeguatamente a un possibile attacco cyber, che provvedano non solo a contrastare l'attacco in corso, ma anche a ripristinare il coretto funzionamento di tutti gli asset/servizi aziendali

# NIST 800-82

- Lo standard **NIST 800-82** rappresenta una **guida volta a migliorare la sicurezza all'interno dei sistemi ICS** (nei quali ricadono ad esempio i sistemi di SCADA, i Distributed control system DSC e i Programmabe Logic Controlles PLC).

- L'attenzione posta dal NIST verso questi sistemi è causato da due principali motivazioni:
  - **l'incremento delle possibili vulnerabilità e minacce** derivanti dal passaggio da sistemi ICS caratterizzati da hardware e software proprietario a device standard che comunicano tramite Internet Protocol (IP)
  - **le possibili conseguenze derivanti da un attacco a questi sistemi ovvero:**
    - Danni agli asset e al personale
    - Danni all'ambiente
    - Perdite finanziarie derivanti dal fermo della produzione
    - Impatti all'economia di una nazione (in caso di attacchi alle infrastrutture critiche)
    - Compromissione di informazioni proprietarie

# NIST 800-82: le minacce

- Lo standard NIST 800-82 prevede che i possibili attacchi a un sistema ICS possono includere:
  - **Il blocco o il rallentamento del flusso di informazioni** lungo la rete del sistema ICS, i quali possono determinare un rallentamento o l'interruzione delle attività produttive
  - **Il cambio non autorizzato di comandi o soglie di allarme**, le quali possono portare al fermo o al danneggiamento degli impianti o a danni all'ambiente e alla salute degli operatori
  - **Invio di informazioni inaccurate agli operatori**, che possono portare gli stessi a prendere decisioni errate comportando conseguenze negative per l'impresa
  - **La modifica della configurazione e dei software dei sistemi ICS**, attraverso ad esempio l'utilizzo di un malware
  - **La disattivazione dei sistemi di sicurezza**, operazione che costituisce non solo un rischio di possibili danni agli impianti, ma anche un pericolo per gli operatori presenti nelle vicinanze degli stessi

# NIST 800-82: gli obiettivi di sicurezza da perseguire

- Al fine di ridurre le probabilità di attacco ai sistemi ICS le imprese dovrebbero gestire la sicurezza di questi sistemi tramite una **«defense-in-depth» strategy** che include le seguenti attività:
  - **SVILUPPARE POLICIY E PROCEDURE DA APPLICARE SPECIFICATAMENTE AI SISTEMI ICS**
  - **GESTIONE DELLA SICUREZZA LUNGO TUTTO IL CICLO DI VITA DEGLI ICS**, dalla scelta dell'architettura da implementare, all'acquisto e scelta dei componenti fino all'installazione e alla successiva manutenzione
  - **RESTRIZIONE DELL'ACCESSO «LOGICO» ALLA RETE DEI SISTEMI ICS**, questa azione può essere conseguita attraverso una architettura di rete all'interno della quale sono presenti demilitarized zone (DMZ) e firewall a fine di prevenire un «passaggio diretto» dalla rete corporate aziendale a quella relativa ai sistemi ICS (network segregation). Al fine di aumentare il controllo relativo all'accesso alla rete ICS è necessario che le imprese utilizzino sistemi di autentificazione separati per le due tipologie di reti.
  - **RESTRIZIONE DELL'ACCESSO «FISICO» ALLA RETE ICS E AI DISPOSITIVI IN ESSA PRESENTI**, in quanto l'accesso non autorizzato ai componenti dei sistemi ICS potrebbe compromettere la funzionalità di questi sistemi. Per questo le imprese dovrebbero utilizzare una combinazione di controlli fisici quali ad esempio lucchetti, card reader e guardie.

## NIST 800-82: gli obiettivi di sicurezza da perseguire

- **PROTEZIONE DEI COMPONENTI DEL SISTEMA ICS DA POSSIBILI ATTACCHI**. Al fine di minimizzare i possibili accessi non autorizzati al sistema ICS le imprese sono chiamate a: applicare le patch di sicurezza il più velocemente possibile dopo averle adeguatamente testate in condizioni operative; disabilitare tutte le porte e i servizi non utilizzati; restringere l'accesso ai sistemi ICS solamente agli utenti che ne hanno effettiva necessità sulla base del loro ruolo (role based access) all'interno dell'impresa; utilizzare controlli quali software antivirus e programmi volti a verificare l'integrità dei file al fine di indentificare possibili malware
- **MANTENERE IL FUNZIONAMENTO DEL SISTEMA ICS ANCHE IN CASO DI CONDIZIONI AVVERSE**, ovvero è necessario nella progettazione di un sistema ICS che tutte le componenti critiche siano ridondante e operino su reti ridondanti. Inoltre in caso di malfunzionamento di un componente è necessario che questo sia progettato per non generare traffico non necessario all'interno delle rete e per evitare ulteriori malfunzionamenti che si potrebbero generare in cascata
- **RIPRISTINO DEI SISTEMI IN SEGUITO A UN MALFUNZIONAMENTO/INCIDENTE**, infatti a causa dell'impossibilità di prevenire completamente eventuali attacchi/malfunzionamenti al sistema, è necessario da parte dell'impresa creare un piano di «incident response» volto a garantire il ripristino delle funzionalità del sistema ICS nel più breve tempo possibile.

## NIST 800-82: l'organizzazione

- Al fine di gestire al meglio queste minacce e lo sviluppo di un piano di sicurezza nei confronti dei sistemi ICS, la NIST prescrive la formazione di un team di Cyber Security che dovrebbe includere le seguenti tipologie di figure:
  - membri dello staff IT,
  - ingeneri e operatori competenti sui sistemi di controllo,
  - esperti di sicurezza IT e delle reti,
  - membri esperti nel garantire la sicurezza fisica degli impianti
  - personale proveniente dal management.

- Il team di Cyber security è inoltre chiamato a collaborare attivamente con i vendor del sistema ICS al fine di avere una ottimale conoscenza delle possibili nuove minacce e per avere la garanzia che l'applicazione delle patch di sicurezza non vada a bloccare l'operatività dei sistemi OT.

# ISO 27019

- Lo **standard ISO 27019**, partendo dallo standard ISO 27002, identifica per il settore energy un **insieme di regole/practice volto a garantire la sicurezza dei sistemi di controllo e delle tecnologie di automazione** utilizzati per controllare e monitorare la produzione, trasmissione/distribuzione dell'elettricità, del gas, del petrolio e del calore.

- Lo standard ISO 27019 **permette la creazione di un sistema di Information Security Management standardizzato volto non solo a garantire la sicurezza dei dati ma anche quella dei processi**, monitorando componenti quali ad esempio:
  - Controller digitali e componenti relative all'automazione (i.e. PLC, attuatori)
  - Advanced Metering Infrastructure (i.e. smart metering) e strumenti di misura
  - Protezioni digitali e sistemi di sicurezza (i.e. relay di protezione, safety PLC)
  - I sistemi informativi e le tecnologie di comunicazione utilizzate per garantire la piena funzionalità dei sistemi di controllo (i.e. reti, sistemi di archiviazione e consultazione dei dati, sistemi di reporting, sistemi di monitoraggio e telecontrollo)
  - I sistemi di remote manteinance

# ISO 27019

- Lo standard ISO 27019, al fine di garantire il mantenimento dell'operatività, prescrive alle imprese appartenenti al settore energy di focalizzare la propria attenzione sulle seguenti aree:

  - **L'ORGANIZZAZIONE DELL'INFORMATION SECURITY**: in particolare le imprese sono chiamate a creare un processo di information security risk assessment, con ruoli designati all'interno dell'organizzazione e il cui compito è quello di identificare:
    - I rischi, le probabilità di accadimento e le possibili conseguenze a livello di ciascun asset
    - I livelli accettabili di rischio per ciascun asset
    - I rischi da risolvere con maggiore priorità, in seguito allo svolgimento di una gap analysis volta a confrontare i livelli di rischio attuali e quelli ritenuti accettabili

  - **LA SICUREZZA FISICA E AMBIENTALE**: le imprese sono chiamate a garantire anche al sicurezza fisica dei centri di controllo, che specialmente del settore della trasmissione e della distribuzione dell'energia, potrebbero trovarsi in aree non presidiate fisicamente da personale dell'organizzazione. Al fine di garantirne la sicurezza fisica le imprese non solo devono collocare gli impianti in strutture caratterizzate da basso rischio di terremoti e inondazioni e dalla presenza di adeguati sistemi antincendio, ma devono anche prevenire accessi non autorizzati all'interno degli stesse.

# ISO 27019

- **LA GESTIONE DEGLI ASSET E DEL PERSONALE**: le imprese sono chiamate a identificare quelli che sono gli asset presenti all'interno dell'azienda, limitando l'accesso e la possibilità di utilizzarli sono al personale qualificato, attraverso l'implementazione di sistemi quali password o altri sistemi di controllo degli accessi che permettano di identificare eventuali responsabilità di caso di problemi.

- **LA SICUREZZA DELLE OPERATIONS**, al fine di garantire la sicurezza delle operations le imprese sono chiamate a creare procedure relative all'installazione e configurazione dei vari sistemi, alla risoluzione di eventuali errori e alle procedure di ripristino e recovery dei sistemi. Le imprese devono inoltre implementare sistemi di event logging e controlli contro i malaware che, laddove non possano essere implementate a livello software, dovrebbero prevedere la messa in sicurezza di tutte le interfacce fisiche e logiche e la segmentazione e l'isolamento di parti della rete

- **LA SICUREZZA DEI SISTEMI DI COMUNICAZIONE E DELLE RETI**: le imprese dovrebbero implementare policy volte a aumentare la sicurezza delle reti di controllo e a limitare gli accessi non autorizzati. All'interno di questo contesto le imprese sono chiamate a effettuare una segmentazione della rete in zone caratterizzate da differenti funzioni e livelli di protezione richiesti, attraverso l'utilizzo di firewall o filtering router/gateway, volti a filtrare tutte le comunicazioni ritenute come non rilevanti

- **GLI ASPETTI DI INFORMATION SECURITY LEGATI ALLA BUSINESS CONTINUITY**: al fine di garantire la disponibilità e la continuità del servizio offerto le imprese sono chiamate a utilizzare sistemi e architetture ridondanti.

# BOX 6: CERTIFICAZIONE

- All'interno della SEN e del DPCM Gentiloni si afferma la necessità di instituire un sistema di certificazione in ambito cybersecurity relativo ai dispositivi OT e soprattutto ai prodotti che sono destinati ad essere utilizzati all'interno delle infrastrutture critiche nazionali

- L'opportunità di introdurre un sistema di certificazione è un tema attualmente ampiamente dibattuto, e su cui non vi è piena convergenza

- La certificazione di prodotto è un tema complesso:
  - si deve tener presente che non è possibile definire a priori il livello di sicurezza richiesto ad un determinato prodotto, in quanto esso dipende dal livello di rischio derivante dal contesto e dall'utilizzo previsto.
  - Inoltre, il livello di sicurezza di una infrastruttura è pari al livello di sicurezza del suo **«anello più debole»**: pertanto, tutti i prodotti che vengono utilizzati in un medesimo sistema dovrebbero essere certificati secondo la medesima procedura al fine di assicurare coerenza e omogeneità tra tutti i dispositivi

- Un recente position paper di Confindustria Digitale sottolinea che l'approccio relativo allo schema certificativo in ambito cybersecurity non può essere rigido e non può rimanere immutato per un lungo periodo, ma, a causa della continua evoluzione delle vulnerabilità, deve prevedere le seguenti tre caratteristiche:
  - essere **modulare**
  - consentire l'identificazione del **percorso più efficace** in considerazione del tipo di prodotti, della natura dei rischi e dei costi della certificazione
  - prevedere un **continuo aggiornamento** degli standard relativi ai test, che devono essere continuamente rivisti sulla base delle nuove minacce emergenti e dei nuovi requisiti di sicurezza necessari a proteggersi dalle stesse

- A tal fine, nel documento si ipotizza la possibilità di introdurre una **duplice modalità di certificazione**, in base all'ambito di utilizzo del dispositivo, ovvero:
  - certificazione **obbligatoria** presso terze parti per tutte le categorie di prodotti/servizi utilizzati nell'ambito di infrastrutture critiche o utilizzati in ambito Business-to-Business (B2B). Questa situazione permetterebbe di minimizzare la possibilità di introdurre «anelli deboli» all'interno delle infrastrutture critiche
  - **auto-certificazione** di prodotti e servizi dedicati al mercato Business-to-Consumer (B2C), purché essi siano ritenuti privi di interazioni a rischio con infrastrutture critiche. In quest'ultimo caso, anche per la categoria di prodotti B2C è auspicabile una certificazione completa presso una terza parte

- **Gli enti certificatori** di prodotti da utilizzare all'interno delle infrastrutture critiche o nell'ambito B2B dovrebbero essere chiamate a partecipare a **riunioni con i CSIRT europei**, al fine di favorire lo scambio di informazioni e rimanere costantemente aggiornati sulle nuove possibili minacce e sule nuove best practice da adottare, garantendo un rapido adattamento delle norme e degli standard di certificazione ad un contesto ampiamente mutevole come quello della sicurezza informatica

- La creazione di uno standard europeo di certificazione condiviso permetterebbe di creare un **database**, a disposizione di soggetti quali ad esempio le **Autorità nazionali e gli Operatori di Servizi Essenziali,** contenente tutte le informazioni di dettaglio sui prodotti che sono stati certificati in qualsiasi laboratorio accreditato, utilizzabile in caso di eventi di sicurezza che rendano necessario entrare in maggiori dettagli in relazione a caratteristiche e comportamenti dei prodotti stessi

- Infine, gli enti certificatori, a causa del lungo ciclo di vita che caratterizza i dispositivi utilizzati in ambito OT, sarebbero chiamati a certificare solo dispositivi che hanno delle caratteristiche di tipo **«future-proof»**, ovvero con potenze di calcolo e di memoria tali da supportare le feature di sicurezza che saranno aggiunte lungo tutto il ciclo di vita del prodotto, al fine di garantire il medesimo livello di sicurezza riscontrato in sede di certificazione iniziale

- La proposta di Confindustria Digitale appare sicuramente interessante e condivisibile su molti aspetti

- Non vanno però sottovalutati anche i rischi derivanti da un sistema di certificazione, soprattutto se non ben progettato.

- A nostro avviso è infatti fondamentale che un eventuale processo di certificazione sia essere il più possibile «snello» (dal punto di vista amministrativo-burocratico), flessibile e poco oneroso. In caso contrario, si corrono due rischi principali:
  - i fornitori di minore dimensione verrebbero inevitabilmente danneggiati
  - il tasso di innovazione (e quindi l'aggiornamento tecnologico dei prodotti stessi) potrebbe subire un rallentamento, al fine di evitare di dover replicare il processo di certificazione «da zero» ad ogni nuova release di prodotto

## Messaggi chiave

- L'analisi degli standard ha permesso di osservare come questi, a differenza delle normative permettano di supportare le imprese al fine di individuare i gap presenti all'interno della gestione della tematica relativa alla cybersecurity, sviluppando piani di miglioramento relativi al sistema di risk management aziendale.

- Gli standard relativi alla tematica della cybersecurity, sebbene in continua evoluzione, sembrano essere già maturi e adeguati nel supportare le imprese nella definizione sia di quali elementi proteggere (NIST 800-82, ISO 27019, IEC 62443, NERC CIP 1300) che delle modalità con cui proteggerli (IEC 62351).

- Appare auspicabile una maggiore diffusione di questi standard all'interno del settore elettrico, con le grandi utility che sembrano avere un ruolo chiave nell'incentivare i fornitori di apparati industriali per il settore elettrico a sviluppare prodotti coerenti con questi standard condivisi e con una logica di prodotto legata al «security-by-design», garantendo di fatto una interoperabilità tra tutti i sistemi e un livello di sicurezza adeguato soprattutto per quelli che sono i sistemi utilizzati all'interno delle infrastrutture critiche nazionali.

POLITECNICO
MILANO 1863

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

# I rischi Cyber e la sicurezza industriale: 5

## Il punto di vista degli end - user

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

# Obiettivi della sezione

- In questa sezione del report l'attenzione si sposta sull'ultimo anello della filiera **(gli end user)**, con particolare riferimento al comparto industriale

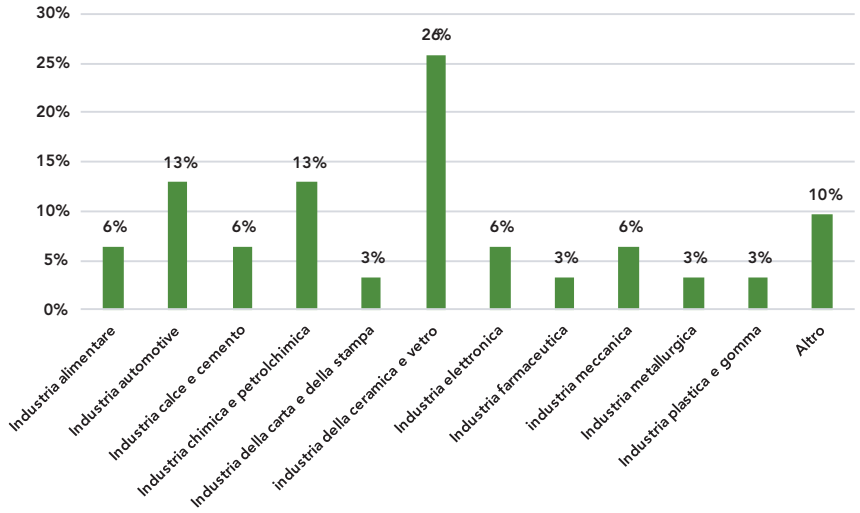
- L'obiettivo di quest'ultima fase dello studio era duplice:
  - verificare il grado di diffusione della **cultura della cybersecurity** in ambito **OT** all'interno del sistema industriale del nostro Paese, con particolare riferimento alle nuove minacce derivanti dalla digitalizzazione dei processi industriali
  - Verificare (nel caso dei «prosumer») il livello di **consapevolezza dei rischi** legati alle attività di **generazione di energia**

- L'indagine è stata svolta grazie alla somministrazione di un **questionario anonimo** indirizzato a manager ricoprenti il ruolo di responsabili operations/direttori di stabilimento/energy manager (laddove possibile)

- Tra il gennaio e il maggio 2018, il questionario è stato somministrato a un campione di oltre **700 imprese**, ottenendo **93 risposte** che vanno a costituire il campione di analisi utilizzato per la survey di cui si dà conto in questo capitolo

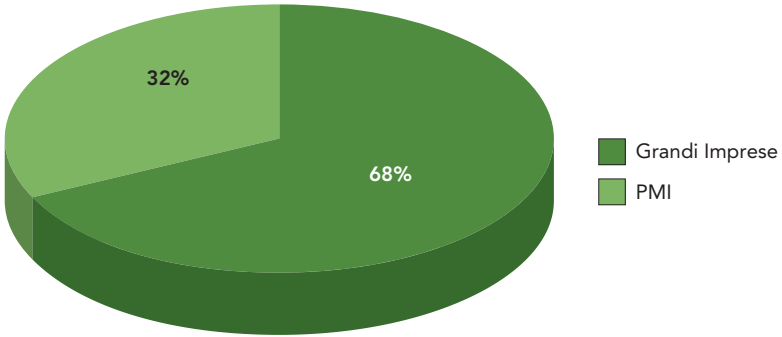
# Il campione di analisi

- Nel campione di analisi sono presenti **12 differenti comparti industriali**: i settori maggiormente rappresentati sono quelli della **ceramica e del vetro** (il 26% delle imprese che hanno risposto al questionario sono attive in tale settore), quello dell'**automotive** e della **chimica e petrolchimica** (il 13% delle imprese intervistate appartiene a questo settore)



# Il campione di analisi

- Il campione di analisi si presenta inoltre piuttosto variegato anche dal punto di vista della **taglia delle imprese** coinvolte all'interno della survey
- All'interno di questa analisi si definisce di **grandi dimensioni** una impresa che presenta un **fatturato annuo superiore ai 50 mln €** (tale definizione discende da quella relativa alla Piccola e Media Impresa data dalla raccomandazione della Commissione 2003/361/CE e recepita in Italia con il D.M. del 18/4/2005)
- Il campione di analisi in particolare risulta essere costituito per il **68% da grandi imprese**



# Il questionario

- Il questionario della survey è composto da 2 macro-sezioni, con obiettivi distinti:
  1. **Sezione I: La digitalizzazione nelle imprese**. Tale sezione si prefigge di valutare **l'importanza strategica** che le imprese italiane attribuiscono alla **digitalizzazione dei processi produttivi**, al fine di assicurare la competitività all'interno delle proprie aree di business. Si indagherà inoltre sulle motivazioni che spingono le imprese a fare investimenti in quest'area.
  2. **Sezione II: La cybersecurity in ambito Operation Technology**. L'obiettivo di questa sezione consiste nell'indagare il **livello di «maturità» della cybersecurity in ambito OT**, tramite l'analisi dei sistemi e delle procedure che le imprese hanno sviluppato per gestirla, nonché del volume di investimenti (già realizzati o previsti nel prossimo futuro). All'interno di tale sezione sono previste alcune domande riservate alle sole imprese catalogabili come **«prosumer»** (che quindi ricoprono il duplice ruolo di produttori e consumatori di energia elettrica), finalizzate a valutare **il livello di consapevolezza sui rischi di natura «cyber»** legati alle attività di generazione di energia elettrica, dal momento che tali imprese normalmente non vantano grande esperienza in questo campo.

- Nel resto del capitolo verranno presentati e discussi i risultati, suddivisi secondo le sezioni sopra identificate

# Sezione I: La digitalizzazione nelle imprese

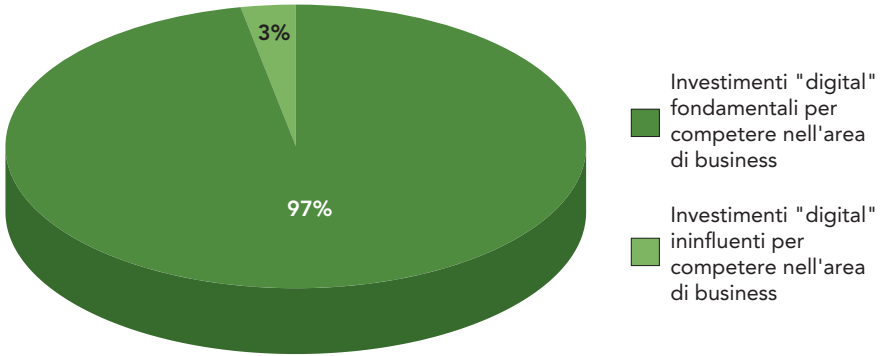
- In questa sezione sono stati approfonditi i seguenti temi:
  - **Le tecnologie «Digital» come differenziale competitivo**: si è indagato se e in che misura gli investimenti in tecnologie «digital» vengano percepiti come un un differenziale competitivo per le imprese del campione
  - **Gli investimenti in ambito «Digital»**: si è indagato sul volume attuale e sulla propensione futura delle imprese a effettuare investimenti in ambito «Digital»
  - **Le motivazioni sottostanti gli investimenti «Digital»**: sono stati identificati i driver che hanno spinto le imprese a realizzare investimenti in tecnologie «Digital»

# Sezione I: L'importanza delle tecnologie «digital» per l'impresa

**Ritenete che effettuare investimenti di natura «digital» sia fondamentale per mantenere un elevato livello di competitività all'interno del vostro settore?**

- Con questo primo quesito si intendeva valutare la percezione da parte delle imprese del campione circa la rilevanza strategica della digitalizzazione (con particolare riferimento alle operations)

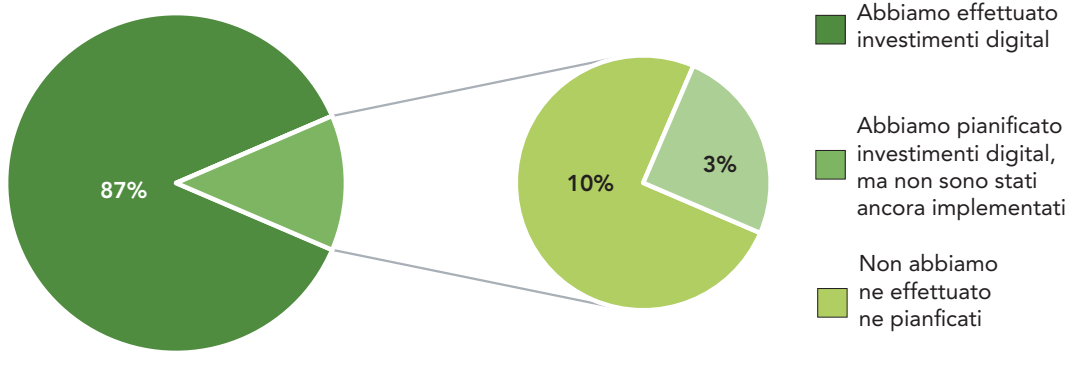
- L'analisi delle risposte ottenute mostra come la **quasi totalità del campione** (**97%** delle imprese) ritenga l'investimento in tecnologie «digital» come **driver fondamentale per generare differenziali competitivi** all'interno delle proprie aree di business



# Sezione I: Gli investimenti in ambito «Digital»

**Avete implementato degli strumenti "digital" (sistemi di automazione, sistemi di tele-monitoraggio, SCADA ecc...) all'interno dei vostri processi produttivi?**

- L'obiettivo di questo quesito consisteva nel verificare l'**effettiva adozione** di tecnologie «digital» all'interno dei processi produttivi
- L'analisi delle risposte ottenute permette di osservare come il **97% delle imprese abbia già effettuato o comunque pianificato investimenti su queste tecnologie**
- Risulta interessante inoltre osservare come **il 77%** delle imprese che ha **già implementato** soluzioni in ambito digital afferma di aver già **programmato di effettuare ulteriori investimenti** in questo campo **nei prossimi 3 anni**

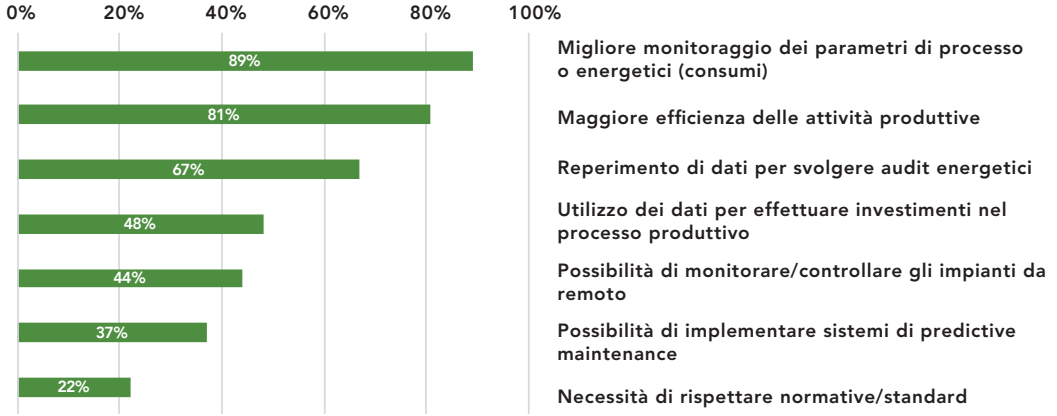


# Sezione I: Motivazioni per l'implementazione di investimenti «Digital»

## Quali motivazioni vi hanno spinto ad effettuare investimenti in tecnologie digital?

- L'obiettivo di questo quesito consisteva nel verificare le motivazioni che hanno portato le imprese del campione a effettuare investimenti in tecnologie digital

- In particolare, le imprese del campione hanno identificato **7 driver principali**, come identificato nel grafico sottostante:



# **Sezione I:** Motivazioni per l'implementazione di investimenti «Digital»

- L'**89%** delle imprese identifica come driver fondamentale la possibilità di ottenere grazie alle tecnologie digital **un migliore monitoraggio dei parametri di processo e dei consumi energetici**
- Questi dati sono utilizzati principalmente al fine di **migliorare l'efficienza delle attività produttive**, driver che è stato infatti indicato **dall'81%** delle imprese
- Il reperimento di dati per svolgere **audit energetici** o **per pianificare investimenti futuri** nel processo produttivo rappresentano driver di scelta rispettivamente per il **67%** e il **48%** delle imprese
- La **possibilità di telecontrollare gli impianti produttivi da remoto e di implementare sistemi di predictive mainteinance** costituiscono driver abilitanti **rispettivamente** per il **44%** e il **37%** delle imprese, mentre **solo il 22%** delle imprese ha scelto di effettuare investimenti in ambito digital a seguito della **necessità di implementare degli standard** o per rendersi **compliant a normative**

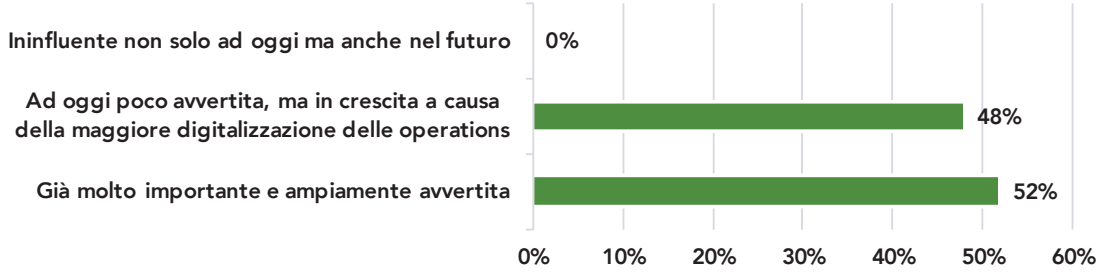
# Sezione II: La cybersecurity nelle imprese

- In questa sezione sono stati approfonditi i seguenti punti:
  - **L'importanza della cybersecurity OT**: si è inteso verificare l'importanza che le imprese assegnano alla tematica della cybersecurity in ambito Operation Technology
  - **Le tipologie di attaccanti**: è stato domandato alle imprese del campione quali fossero secondo loro le fonti più probabili di attacchi ai processi produttivi
  - **Le modalità organizzative per gestire la cybersecurity OT**: si è indagato sulle soluzioni scelte dalle imprese per la gestione della cybersecurity
  - **Gli investimenti in cybersecurity OT**: è stato chiesto alle imprese se avessero già effettuato degli investimenti per la sicurezza industriale (o se fossero previsti a breve). Inoltre, si è cercato di capire se il livello di sicurezza stia diventando uno dei driver fondamentali che guidano la scelta di un nuovo asset produttivo
  - **La cybersecurity relativa agli impianti di produzione elettrica**: quest'ultima parte della survey era riservata ai soli «prosumer». In particolare, si è cercato di capire quanto queste imprese siano consapevoli dei rischi cui vanno incontro, domandando loro se e quanto ritenessero i propri impianti di produzione elettrica potessero essere oggetto di possibili attacchi «cyber»

# Sezione II: l'importanza della cybersecurity OT

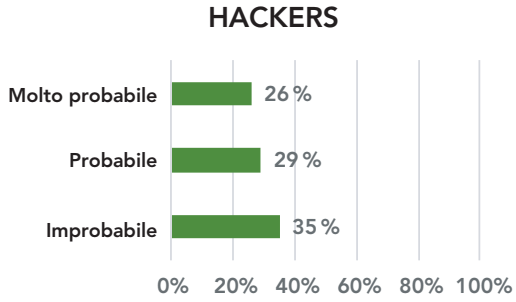
**Qual è l'importanza della tematica della cybersecurity all'interno della vostra industry?**

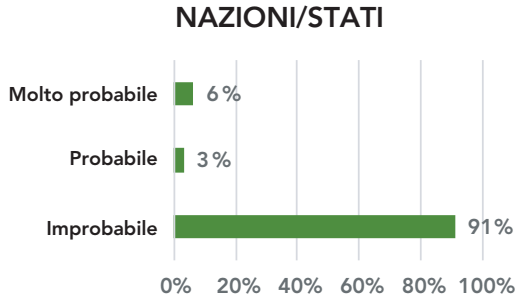
- Il primo degli aspetti analizzati riguarda l'attenzione che le imprese italiane dedicano alla tematica della Cybersecurity in ambito Operation Technology.
- È possibile osservare dal grafico seguente come il **52% delle imprese** ritenga che **la tematica della Cybersecurity** in ambito OT sia **già molto importante** all'interno della propria industry.
- Il **48% delle imprese** ritiene invece che la rilevanza della tematica della cybersecurity sia attualmente poco avvertita, ma sia comunque destinata a crescere nel futuro, a causa della sempre maggiore digitalizzazione delle operations.

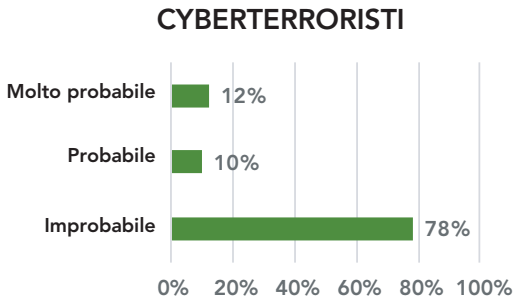


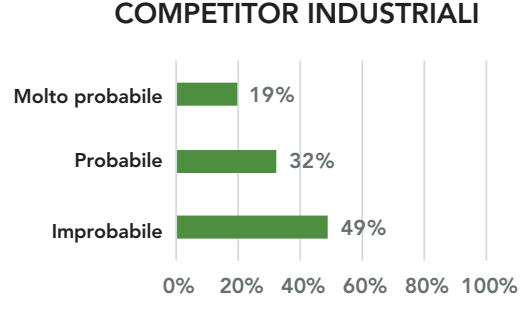
# Sezione II: le tipologie di attaccanti

**Quali sono le tipologie di attaccanti che ritenete abbiano maggiore probabilità di portare attacchi alle operations della vostra impresa?**



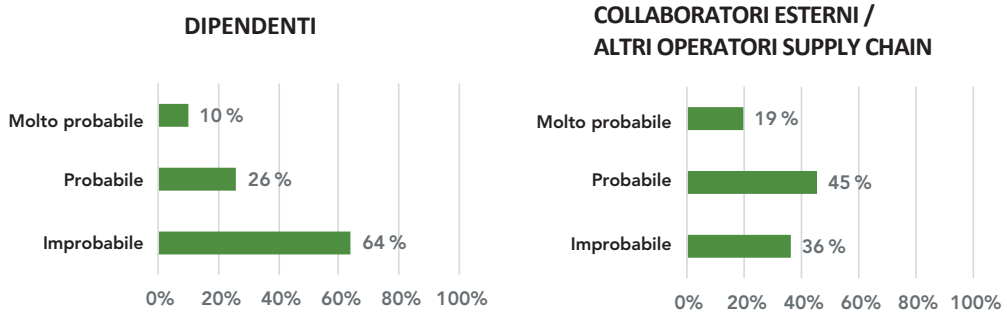



# Sezione II: le tipologie di attaccanti

**Quali sono le tipologie di attaccanti che ritenete abbiano maggiore probabilità di portare attacchi alle operations della vostra impresa?**




- All'interno del questionario un quesito è stato dedicato ai possibili attaccanti che le imprese ritengono possano costituire una minaccia reale ai propri impianti produttivi
- Dai risultati illustrati dai grafici precedenti è possibile osservare come le imprese coinvolte nella survey, non rientrando all'interno degli operatori di servizi essenziali, ritengano **poco probabile un attacco da parte di nazioni/stati o gruppi di cyberterrorismo**

# Sezione II: le tipologie di attaccanti

- **La minaccia posta dagli hacker è ritenuta quella più concreta**, infatti il **26% delle imprese** coinvolte dalla survey considera molto probabile la possibilità di subire un attacco alle operations da parte di questa tipologia di attori.

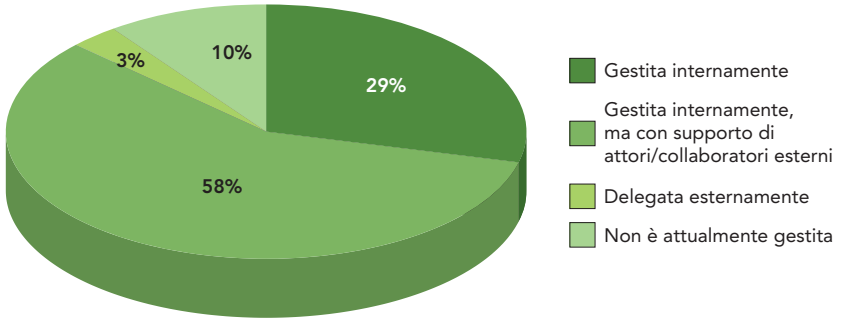
- Le imprese inoltre identificano come possibili attaccanti non solo i propri collaboratori esterni o gli altri player presenti all'interno della propria supply chain, ma anche gli altri competitor industriali presenti all'interno della propria area di business. In particolare il **54%** dei rispondenti identifica come **probabili o molto probabili** attacchi da parte di **fornitori** o comunque altri **player presenti all'interno della propria supply chain**, mentre il **51%** identifica come **almeno probabili** gli attacchi da parte dei **competitor industriali**

- È possibile osservare come solamente il **36%** dei rispondenti identifica come **almeno probabile** un attacco derivante da azioni dirette o indirette effettuate **dai dipendenti.** Questo risultato è in contrasto con quanto sottolineato all'interno **degli standard**, i **quali identificano** i dipendenti come fonte molto probabile di attacco in quanto non solo possono essere **autori di azioni volontarie volte ad arrecare danni alla propria azienda**, ma soprattutto sono utilizzati da altre tipologie di attaccanti come **veicoli per ottenere l'accesso alle reti aziendali**

# Sezione II: Le modalità organizzative per la cybersecurity OT

**Come è gestita all'interno della vostra impresa la tematica della cybersecurity OT?**

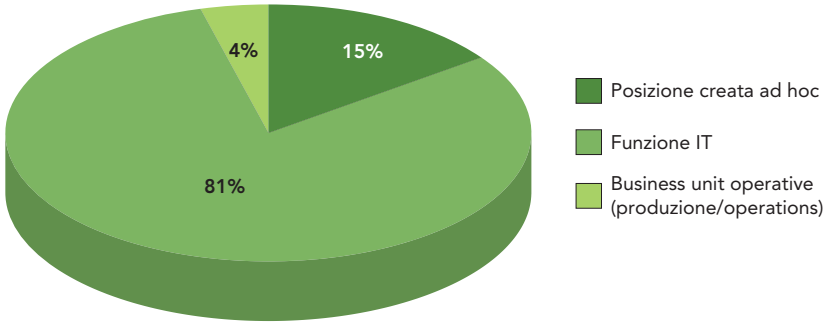
- L'attività di gestione della cybersecurity può essere svolta internamente, magari con l'appoggio di attori esterni, oppure delegata esternamente nel caso in cui l'impresa ritenga di non avere adeguate conoscenze o una scala tale da rendere economicamente conveniente prevedere delle risorse dedicate
- Il modello di gestione della cybersecurity più diffuso sembra essere quello di una **gestione interna con un supporto esterno**, il quale è adottato dal **58%** delle imprese del campione. Al secondo posto (con il **29%**) troviamo il modello di gestione della cybersecurity **totalmente «in house»**, mentre solo il **3%** decide di **delegarne totalmente la gestione a soggetti terzi**
- È importante infine osservare come il **10%** delle imprese affermi di **non aver ancora previsto nessun meccanismo «stabile» di gestione di queste attività**



# Sezione II: Le modalità organizzative per la cybersecurity OT

## A quale funzione interna è demandata la gestione interna della cybersecurity in ambito OT?

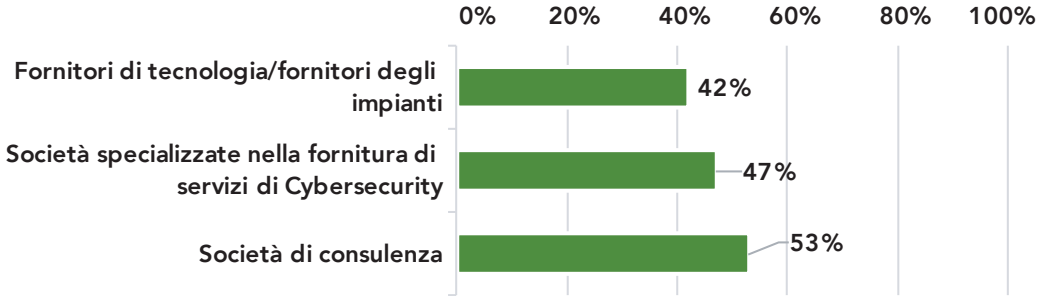
- Il seguente quesito è volto ad identificare a quale funzione/posizione organizzativa è assegnata la gestione della cybersecurity in ambito OT, laddove vi sia anche un presidio interno (cioè nella stragrande maggioranza dei casi, come si è visto dalle risposte date alla precedente domanda)
- Dai risultati illustrati nel grafico sottostante è possibile osservare come il **15% delle imprese** del campione abbia **creato una posizione organizzativa ad hoc** a cui è demandata la gestione di questa tematica, mentre solamente il **4% delle imprese** ha deciso, anche a causa delle peculiarità dei processi OT rispetti a quelli IT, di affidarne la gestione alle **business unit operative**
- Nella maggior parte dei casi **(81% delle imprese)** la gestione della tematica è invece affidata alla funzione IT, che ha quindi in carico tutta la gestione della cybersecurity aziendale sia a livello IT e OT



# Sezione II: Le modalità organizzative per la cybersecurity OT

**A quali tipologie di attori/collaboratori esterni la vostra impresa utilizza per ottenere supporto nella gestione della cybsercurity in ambito OT?**

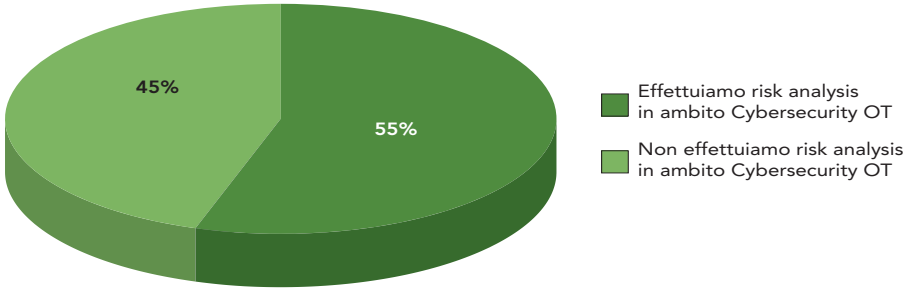
- Il seguente quesito è volto ad identificare quali attori esterni le imprese coinvolgono al fine di ricevere supporto nella gestione della cybersecurity in ambito OT.
- Osservando i risultati illustrati dal grafico sottostante è possibile osservare come le imprese non abbiano un interlocutore preferenziale quando si tratta di coinvolgere attori esterni nella gestione della cybersecurity in ambito OT.
- Sorprende comunque osservare come soltanto il **42% delle imprese intervistate affermi di coinvolgere i fornitori** dei propri impianti industriali nella gestione della tematica della cybersecurity, nonostante il ruolo fondamentale ricoperto da questi attori (soprattutto nella definizione delle specifiche dei vari prodotti in sede progettuale e nelle fasi successive di aggiornamento lungo il ciclo di vita dei prodotti stessi)



# Sezione II: Le modalità organizzative per la cybersecurity OT

**Effettuate una risk analysis volta a identificare le possibili minacce a cui sono esposti gli impianti produttivi? Con che frequenza?**

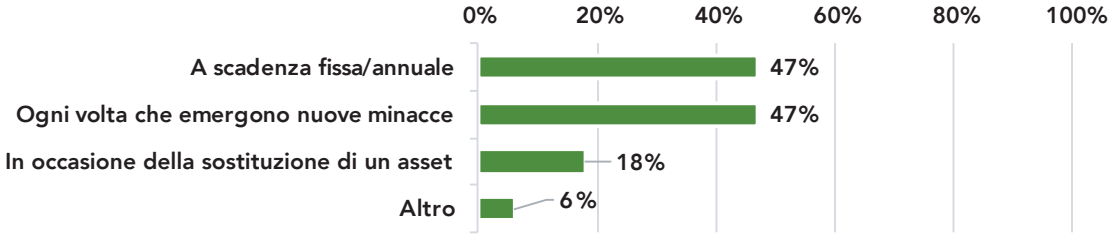
- Il seguente quesito è volto ad identificare la propensione delle imprese a effettuare una risk analysis in ambito cybersecurity.
- Come emerge dal grafico sottostante, **solamente il 55% del campione afferma di effettuare risk analysis** volte a identificare gli asset presenti all'intero dell'impresa, le minacce a cui potrebbero andare incontro e le contromisure da adottare sia a livello tecnologico che di policy organizzative, assegnando a ciascun asset un livello di sicurezza target da raggiungere.



# Sezione II: Le modalità organizzative per la cybersecurity OT

**Effettuate una risk analysis volta a identificare le possibili minacce a cui sono esposti gli impianti produttivi? Con che frequenza?**

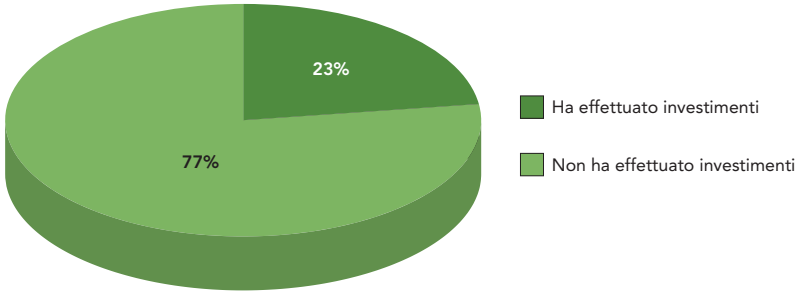
- Relativamente alla frequenza con cui sono svolte le risk analysis, il seguente grafico riporta la visione d'insieme delle risposte fornite dalle imprese (era possibile indicare più di una risposta)
- È curioso osservare come non sembra emergere una frequenza predominante con la quale svolgere le risk analysis. Il **47% del campione** afferma infatti di effettuarle secondo **una scadenza fissa** (tipicamente annuale). Un altro **47%** trova invece necessario ripeterla **ogni qual volta emergano nuove minacce a carico degli asset aziendali.**
- Minoritaria (ma non trascurabile) è la percentuale di imprese **(18% del campione)** che afferma di svolgere questa attività solo **al momento della sostituzione di un asset produttivo**



# Sezione II: La «cultura» degli investimenti in Cybersecurity OT

## Avete effettuato investimenti relativi alla Cybersecurity in ambito OT?

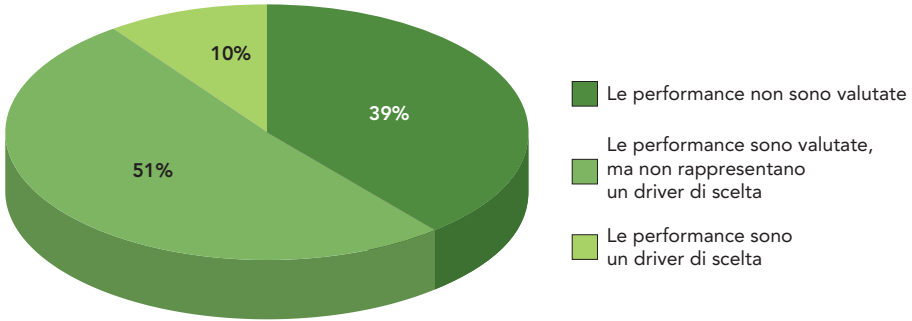
- La survey ha permesso di identificare se vi fosse una reale correlazione tra l'importanza che le imprese assegnano alla tematica della cybersecurity in ambito OT e gli investimenti realizzati dalle stesse
- Come evidenziato dal grafico sottostante è possibile osservare come, nonostante le imprese si rendano conto che la digitalizzazione dei processi produttivi le stia esponendo a nuove minacce, ad oggi la **maggior parte** delle stesse **(77%) non ha ancora deciso di cautelarsi effettuando investimenti mirati**



# Sezione II: La «cultura» degli investimenti in Cybersecurity OT

**In seguito alla necessità di sostituire un impianto produttivo o nella fase di scelta del fornitore e della nuova soluzione sono valutate le prestazioni in ambito cybersecurity?**

- Attraverso questo quesito si è identificata la propensione delle imprese a considerare la **cybersecurity** come un **driver fondamentale nella scelta dei propri fornitori all'atto del cambio degli impianti produttivi**
- Come evidenziato dal grafico sottostante è possibile notare come nel **39% dei casi** le prestazioni in termini di sicurezza OT **non sono prese in considerazione** nel processo decisionale che porta alla scelta del prodotto, mentre nel **51% dei casi**, pur essendo in qualche modo valutate, **non risultano di fatto un driver di scelta**
- Solo il **10%** dei rispondenti afferma di aver **inserito dei parametri legati alle performance di sicurezza nel processo di valutazione delle soluzioni** proposte dai vari fornitori. Questo risultato conferma che il livello di maturità nella gestione della cybersecurity industriale è ancora piuttosto basso



# **Sezione II:** La Cybersecurity relativa agli impianti di produzione elettrica

**Oltre a approvigionarvi dalla rete elettrica avete altri impianti (i.e. Impianti FV o cogeneratori/ trigeneratori) volti a soddisfare i vostri fabbisogni elettrici?**
**Ritenere che questi impianti possano essere soggetti a attacchi volti a comprometterne l'operatività?**

- Questo quesito è volto ad identificare non solo la diffusione del paradigma «prosumer» all'interno delle imprese del campione d'analisi, ma soprattutto la sensibilità di tali imprese ai rischi di natura cyber legati al loro ruolo di produttori di energia elettrica

- Più di metà del campione **(58% delle imprese)** afferma di appartenere dei **prosumer** industriali, e in particolare il **45% delle imprese** ha adottato **cogeneratori/trigeneratori**, mentre il **33%** afferma di possedere un **impianto fotovoltaico**

- Risulta interessante osservare come le imprese prosumer ritengano questi impianti immuni a possibili attacchi di natura cyber. Infatti, solamente il **6% del campione ritiene che l'operatività di questi impianti possa essere compromessa da attacchi cibernetici**

# Sezione II: La Cybersecurity relativa agli impianti di produzione elettrica

**Quali sono le motivazioni che vi spingono a ritenere questi impianti al sicuro da possibili cyber-attacchi?**

- Le principali motivazioni che conducono le imprese a presupporre l'immunità agli attacchi cyber sono due:
  - la **mancanza di possibilità di telecontrollo** di questi impianti induce il **65% delle imprese prosumer** del campione a credere che le uniche fonti di «reale» minaccia siano costituite da guasti e da possibili manomissioni interne
  - Le restanti imprese prosumer del campione **(35%)** ritengono che **gli strumenti di sicurezza** inseriti all'interno di questi impianti da parte dei fornitori e una corretta installazione e configurazione degli stessi siano **sufficienti a garantire la copertura da attacchi di tipo cyber**
- Questa percezione, unitamente alla **mancanza di dati** relativi ad attacchi volti a compromettere l'operatività degli impianti degli impianti di generazione distribuita*, spinge le imprese a non **effettuare investimenti** finalizzati a incrementare la sicurezza di questi impianti.

(*) NOTA: sebbene molti ricercatori abbiano indentificato – soprattutto per quanto riguarda i campi eolici – una possibilità non solo di bloccare la produzione di energia elettrica, ma anche di creare dei danni fisici agli impianti, ad oggi si è a conoscenza di attacchi che sono riusciti solamente a rendere indisponibile la possibilità effettuare al monitoraggio della produzione di questi impianti

# La survey: Messaggi chiave

- L'analisi delle risposte relative alla parte della survey sulla cybersecurity OT ha permesso di identificare come le **imprese considerino questa tematica come importante e da presidiare a causa della sempre maggiore digitalizzazione introdotta all'interno dei processi produttivi.**

- Ad oggi le imprese identificano come **tipologie di attaccanti più probabili gli hackers**, ma non sembrano trascurabili le minacce provenienti da fornitori o altri attori della propria supply chain, nonché dai competitor industriali

- Il **modello organizzativo** più utilizzato dalle imprese per gestire la cybersecurity in ambito OT risulta essere di tipo «**misto**», che prevede sia un presidio **interno** (tipicamente affidata alla funzione IT), supportato da una serie di attori **esterni** (quali le società di consulenza, le società specializzate in servizi di sicurezza cyber e i fornitori tecnologici).

- I **processi** con cui le imprese gestiscono le cybersecurity OT **non** sembrano però essere ancora **adeguatamente strutturati**. Infatti solo poco più della metà del campione analizzato ha affermato di effettuare una risk analysis volta a identificare vulnerabilità, potenziali danni conseguenti e contromisure necessarie in modo sistematico.

## La survey: Messaggi chiave

- La mancata implementazione di un processo strutturato volto a identificare le minacce a carico degli impianti produttivi, e le loro tuttora bassa probabilità di accadimento, induce le **imprese a non effettuare investimenti specifici in ambito cybersecurity OT**

- Le imprese non solo non effettuano investimenti specifici volti a migliorare la sicurezza cyber degli impianti produttivi, ma nella maggior parte dei casi (90% del campione) **non considerano le prestazioni** in ambito cybersecurity come un **driver fondamentale** nella scelta di un nuovo impianto produttivo e del relativo fornitore.

- La tendenza a non effettuare investimenti in ambito cybersecurity OT si riscontra anche nella gestione degli impianti di produzione elettrica (quali impianti fotovoltaici, cogeneratori e trigeneratori) che sono ritenuti quasi sempre **esenti da possibili minacce**

- Queste analisi confermano come all'interno delle imprese la cybersecurity OT sia ritenuta ancora un tema strategicamente ancora poco rilevante. La ridotta sensibilità sul tema e l'assenza di una casistica significativa di attacchi cibernetici volti a bloccare o a compromettere l'attività produttiva fa sì che le imprese preferiscano dare priorità ad altre aree. Ne consegue un volume di investimenti e un livello di maturità complessivo dei sistemi di cybersecurity governance mediamente molto basso.

# Gruppo di lavoro

Vittorio Chiesa - *Direttore Energy & Strategy Group*

Davide Chiaroni - *Vice direttore*
Federico Frattini - *Vice direttore*

Paolo Maccarrone - *Responsabile della Ricerca*
Davide Perego - *Project Manager*

Cristian Pulitano
Giulia Besozzi
Martino Bonalumi
Francesca Capella
Damiano Cavallaro
Andrea Di Lieto
Simone Franzò
Marco Guiducci
Luca Manelli
Vito Manfredi Latilla
Anna Temporin
Andrea Urbinati

Con la collaborazione di: Stefano Vasquez

# La School of Management

La School of Management del Politecnico di Milano è stata costituita nel 2003.
Essa accoglie le molteplici attività di ricerca, formazione e alta consulenza, nel campo del management, dell'economia e dell'industrial engineering, che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili.
Fanno parte della Scuola: il Dipartimento di Ingegneria Gestionale, i Corsi Undergraduate e il PhD Program di Ingegneria Gestionale e il MIP, la Business School del Politecnico di Milano che, in particolare, si focalizza sulla formazione executive e sui programmi Master.
La Scuola può contare su un corpo docente di più di duecento tra professori, lettori, ricercatori, tutor e staff e ogni anno vede oltre seicento matricole entrare nel programma undergraduate.
La School of Management ha ricevuto, nel 2007, il prestigioso accreditamento EQUIS, creato nel 1997 come primo standard globale per l'auditing e l'accreditamento di istituti al di fuori dei confini nazionali, tenendo conto e valorizzando le differenze culturali e normative dei vari Paesi.

POLITECNICO
MILANO 1863

MIP
POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

# L'Energy & Strategy Group

L'Energy & Strategy Group della School of Management del Politecnico di Milano è composto da docenti e ricercatori del Dipartimento di Ingegneria Gestionale e si avvale delle competenze tecnico-scientifiche di altri Dipartimenti, tra cui in particolare il Dipartimento di Energia.
L'Energy & Strategy Group si pone l'obiettivo di istituire un Osservatorio permanente sui mercati e sulle filiere industriali delle energie rinnovabili, dell'efficienza energetica e della sostenibilità ambientale d'impresa in Italia, con l'intento di censirne gli operatori, analizzarne strategie di business, scelte tecnologiche e dinamiche competitive, e di studiare il ruolo del sistema normativo e di incentivazione.
L'Energy & Strategy Group presenta i risultati dei propri studi attraverso:

- rapporti di ricerca "verticali", che si occupano di una specifica fonte di energia rinnovabile (solare, biomasse, eolico, geotermia, ecc.);
- rapporti di ricerca "trasversali", che affrontano il tema da una prospettiva integrata (efficienza energetica dell'edificio, sostenibilità dei processi industriali, ecc.).

# Le Imprese Partner

CESI

ENEL

GDATA

TERNA

CESI - Centro Elettrotecnico Sperimentale Italiano - è stato fondato nel 1956 dal professor Ercole Bottani, docente di Elettrotecnica generale presso il Politecnico di Milano, per facilitare lo sviluppo e la sicurezza del Sistema Elettrico Italiano, oltre che per offrire laboratori di testing e servizi di certificazione per l'industria elettromeccanica.
Oggi CESI sviluppa un giro d'affari di oltre 120 milioni di euro ed opera in più di 40 paesi al mondo, grazie ad un network di 1.000 professionisti e attraverso i propri stabilimenti ed uffici in Italia (Milano, Seriate e Piacenza), Germania (Berlino e Mannheim), Emirati Arabi Uniti (Dubai) e in Brasile (Rio de Janeiro). CESI opera da oltre 50 anni come leader globale nella fornitura di servizi integrati di testing e certificazione, consulenza ed ingegneria per gli operatori del settore elettro-energetico come imprese di generazione e distribuzione, gestori delle reti di trasmissione, enti regolatori, pubblica amministrazione, sviluppatori, nonché per aziende internazionali di componentistica elettromeccanica ed automazione industriale. CESI inoltre collabora con importanti enti finanziatori di progetti volti a realizzare grandi infrastrutture elettriche come EuropeAid, World Bank, European Bank of Reconstruction and Development, Asian Development Bank, African Development Bank e Inter-American Bank.
Il marchio CESI è riconosciuto sul mercato globale ed è associato ad esperienza, qualità ed indipendenza nonché a competenze tecniche e attrezzature di laboratorio distintive a livello internazionale. CESI possiede un vasto network commerciale internazionale ed importanti referenze globali. Avanzato know-how tecnologico, esperienza, indipendenza, sviluppo di soluzioni ad hoc, fanno di CESI un leader dei servizi tecnico-specialistici e della consulenza agli operatori del settore elettrico.
CESI è una società indipendente che vanta importanti aziende nazionali ed internazionali come shareholders, tra i quali Enel, Terna e ABB.

Enel è una multinazionale dell'energia e uno dei principali operatori integrati globali nei settori dell'elettricità, del gas e dell'energie rinnovabili. Enel è la più grande utility europea in termini di capitalizzazione di mercato e si situa fra le principali aziende elettriche d'Europa in termini di capacità installata e reported EBITDA. Il Gruppo opera in oltre 30 Paesi nei 5 continenti, produce energia attraverso una capacità gestita di 86 GW, di cui 40 GW da rinnovabili. Enel distribuisce energia elettrica e gas attraverso una rete di oltre 2 milioni di chilometri e con oltre 65 milioni di utenze residenziali e industriali nel mondo, il gruppo presenta la più grande customer base tra i competitors europei.


Fondata nel 1985 a Bochum, G DATA vanta una storia di oltre trent'anni nella lotta e prevenzione contro le minacce informatiche ed è uno dei principali fornitori al mondo di soluzioni per la sicurezza IT, insignite di numerosi riconoscimenti per la qualità della protezione fornita e l'intuitività d'uso.
G DATA produce e commercializza soluzioni di sicurezza totalmente aderenti alle normative europee sulla protezione dei dati. Il portafoglio prodotti G DATA comprende soluzioni di sicurezza per le imprese, dalle micro alle grandi aziende, e applicazioni rivolte all'utenza consumer.

Partner tecnico di Ducati Corse per la MotoGP, G DATA ha il compito di proteggere i sistemi IT di pista del team Ducati. L'azienda patrocina altresì il Teatro Comunale di Bologna e diversi eventi volti all'accrescimento culturale e all'aggregazione sociale tra cui mostre e corsi presso istituti scolastici per favorire un uso consapevole del web e dei social media.

Ulteriori informazioni su G DATA e sulle soluzioni di sicurezza del vendor teutonico sono consultabili sul sito www.gdata.it

Terna S.p.A. è uno dei principali operatori europei di reti per la trasmissione dell'energia elettrica con oltre 72.000 km di linee gestite in Italia. Quotata in borsa dal 2004, Terna ricopre un ruolo centrale nel sistema elettrico italiano in quanto, in attuazione del Decreto Legislativo 79/99 e del DM 15/12/2010, è proprietaria della Rete elettrica di Trasmissione Nazionale in alta ed altissima tensione (RTN) e svolge il servizio pubblico per la trasmissione e il dispacciamento, ovvero la gestione in sicurezza dei flussi di energia sulla rete.
Forte delle competenze e dell'esperienza acquisite nella gestione della rete italiana, il Gruppo è pronto a cogliere nuove opportunità di business, offrendo servizi di ingegneria, approvvigionamento e costruzione (EPC), esercizio e manutenzione (O&M) e telecomunicazioni (TLC), sia in ambito nazionale che internazionale. Inoltre, a partire dal 2018, con l'acquisizione di Avvenia, società leader nel settore dell'efficienza energetica Terna arricchisce l'offerta di soluzioni energetiche integrate e si propone come Energy Solution Provider.
La posizione unica di Terna nel panorama italiano permette una visione di lungo periodo dei sistemi energetici, consentendo al Gruppo di ricoprire un ruolo strategico e di guidare la transizione energetica verso modalità di produzione più efficienti ed eco-compatibili.
Terna gestisce le proprie attività tenendo sempre in considerazione le loro possibili ricadute economiche, sociali ed ambientali e lavora costantemente per creare, mantenere e consolidare un rapporto di dialogo e di reciproca fiducia con tutti i suoi stakeholder, nell'intento di allineare gli interessi strategici di sviluppo con le esigenze della collettività e coniugando eccellenza nel business e sostenibilità.
Il Piano Strategico 2018-2022 prevede un'accelerazione degli investimenti per lo sviluppo della rete elettrica in Italia, il backbone energetico del Paese. Il Piano prevede, inoltre, il consolidamento delle attività a mercato, in Italia e all'estero, per lanciare nuovi servizi a supporto della transizione energetica cogliendo opportunità ad alto valore aggiunto coerenti con le competenze distintive del Gruppo.
Sul fronte delle attività internazionali l'impegno di Terna è finalizzato a rendere ancora più centrale il proprio ruolo a livello europeo, per rafforzare il posizionamento dell'Italia come hub energetico per tutta l'area del Mediterraneo e uno dei Paesi europei elettricamente più connessi.

## Note

## Note

## Note

## Note

## Note

## Note

Collana Quaderni AIP
Registrazione n. 433 del 29 giugno 1996 - Tribunale di Milano

Direttore Responsabile: Umberto Bertelè

Progetto grafico e impaginazione: Ntounas Stefano
Stampa: Tipografia Galli & C. s.r.l.
ISBN: 978-88-98399-26-0

Partner

CESI
Shaping a Better Energy Future

enel

G DATA
TRUST IN
GERMAN
SICHERHEIT

Terna

STAMPATO SU
CARTA RICICLATA

ISBN: 978-88-98399-26-0