

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training



Co-funded by  
the European Union

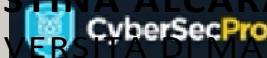
Elementi  
essenziali e  
gestione della  
sicurezza  
informatica per  
il settore  
energetico

# CSP001\_C\_E

PRESENTAZIONE DI:

CRISTINA ALCARAZ

UNIVERSITÀ DI MALAGA SPAGNA



EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training



Co-funded by  
the European Union

# Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

# Argomento 2: Conoscenze fondamentali e tassonomia della sicurezza informatica energetica e corpus di conoscenze

## Panoramica

- Definire la sicurezza informatica energetica e la sua importanza nel settore energetico
- Comprendere i vari componenti di un ecosistema di sicurezza informatica energetica
- Classificare le minacce e le vulnerabilità alla sicurezza informatica specifiche dei sistemi energetici
- Panoramica del corpus di conoscenze sulla sicurezza informatica

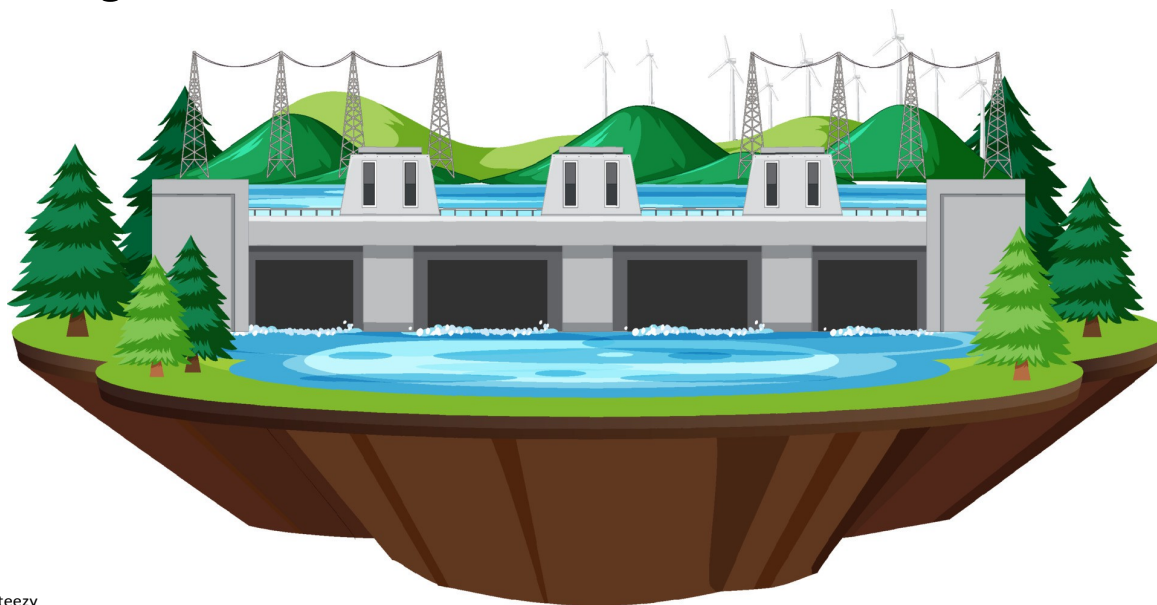
# Argomento 2: Conoscenze di base e tassonomia della sicurezza informatica energetica e corpus di conoscenze

## Panoramica

- **Definire la sicurezza informatica nel settore energetico e la sua importanza in questo ambito**
- Comprendere i vari componenti di un ecosistema di sicurezza informatica energetica
- Classificare le minacce e le vulnerabilità alla sicurezza informatica specifiche dei sistemi energetici
- Panoramica del corpus di conoscenze sulla sicurezza informatica

## Definizione di "sicurezza informatica energetica"

- **La sicurezza informatica energetica** è il settore responsabile di fornire tutte le misure preventive e protettive necessarie per salvaguardare l'"energia" e tutte le apparecchiature correlate per il suo corretto funzionamento, garantendo anche servizi affidabili di produzione e distribuzione di energia elettrica.



Fonte dell'immagine: Vecteezy  
URL: <https://www.vecteezy.com/vector-art/4496530-isolated-hydro-power-plants-generate-electricity>

## Perché l'energia è importante?

- Nel settore energetico esistono diverse fonti di energia:

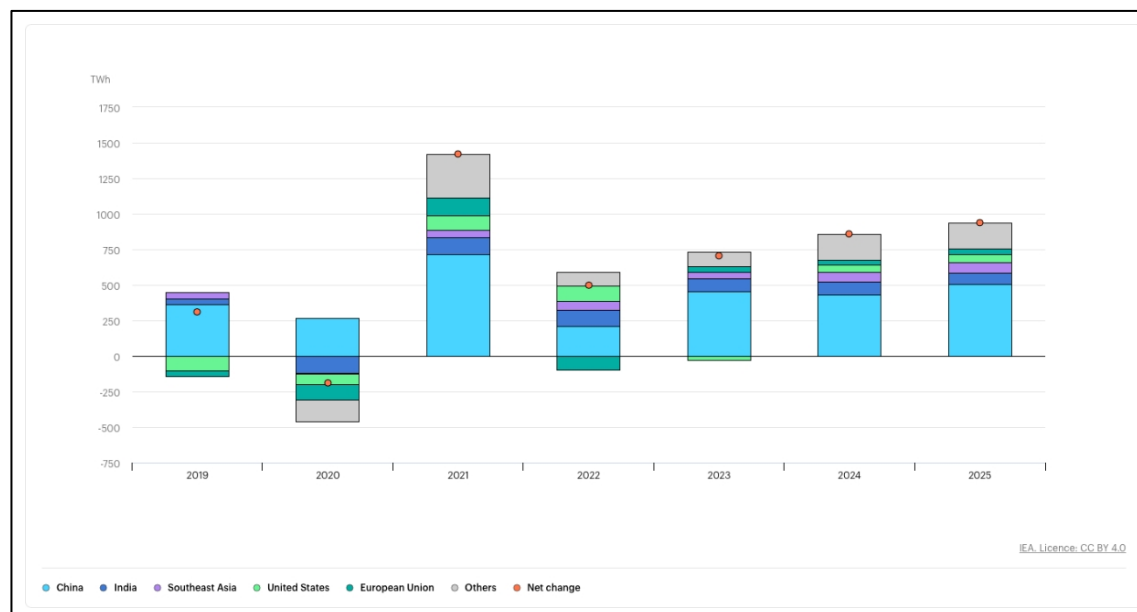
- Carbone
- Petrolio e gas
- Nucleare
- **Elettricità**

Si noti che questo modulo si concentrerà sulle questioni relative all'energia elettrica, ma i concetti appresi si estendono a tutti gli altri campi correlati.

- Tutte queste risorse sono considerate "**essenziali**", principalmente perché garantiscono:
  - Benessere sociale ed economico
  - La continuità di altre attività fondamentali appartenenti ad altre infrastrutture dipendenti

## Perché l'energia è importante?

- Secondo l'Agenzia internazionale per l'energia (AIE), esiste una **forte domanda** di produzione di energia elettrica in diversi paesi, compresa l'Europa
  - Ad eccezione del 2020 (dopo il COVID-19) e del 2022 (post-COVID-19)



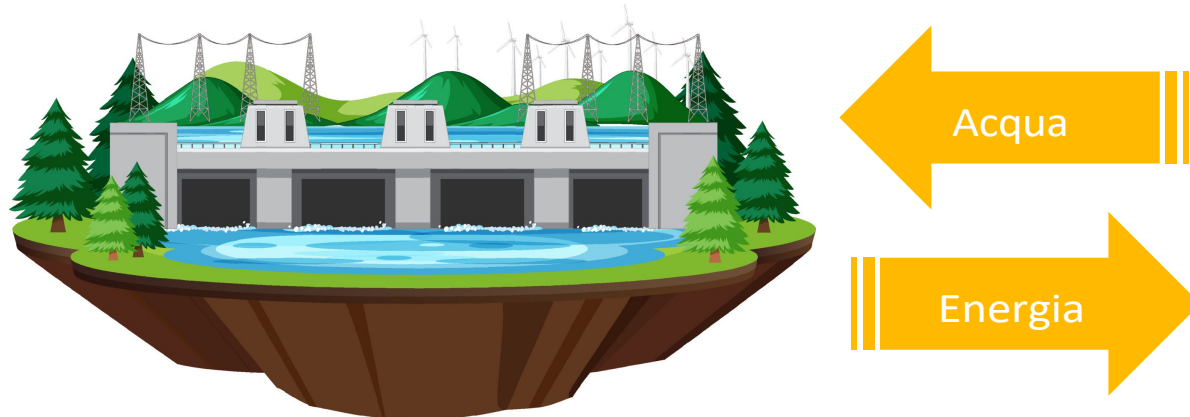
IEA. Licenza: CC BY 4.0

Fonte: IEA, Variazione anno su anno della domanda di elettricità per regione, 2019-2025, IEA, Parigi

URL: <https://www.iea.org/data-and-statistics/charts/year-on-year-change-in-electricity-demand-by-region-2019-2025>, IEA. Licenza: CC BY 4.0

## Perché l'energia è importante?

- Purtroppo, questa domanda è tipicamente soggetta ad altre fonti essenziali come l'acqua o il vento,
  - il che crea una forte dipendenza tra le fonti essenziali stesse e tra i sistemi
  - → Senza acqua □ non è possibile produrre energia nelle centrali idroelettriche
  - Ma senza energia → Non c'è modo di gestire l'acqua in altri sistemi



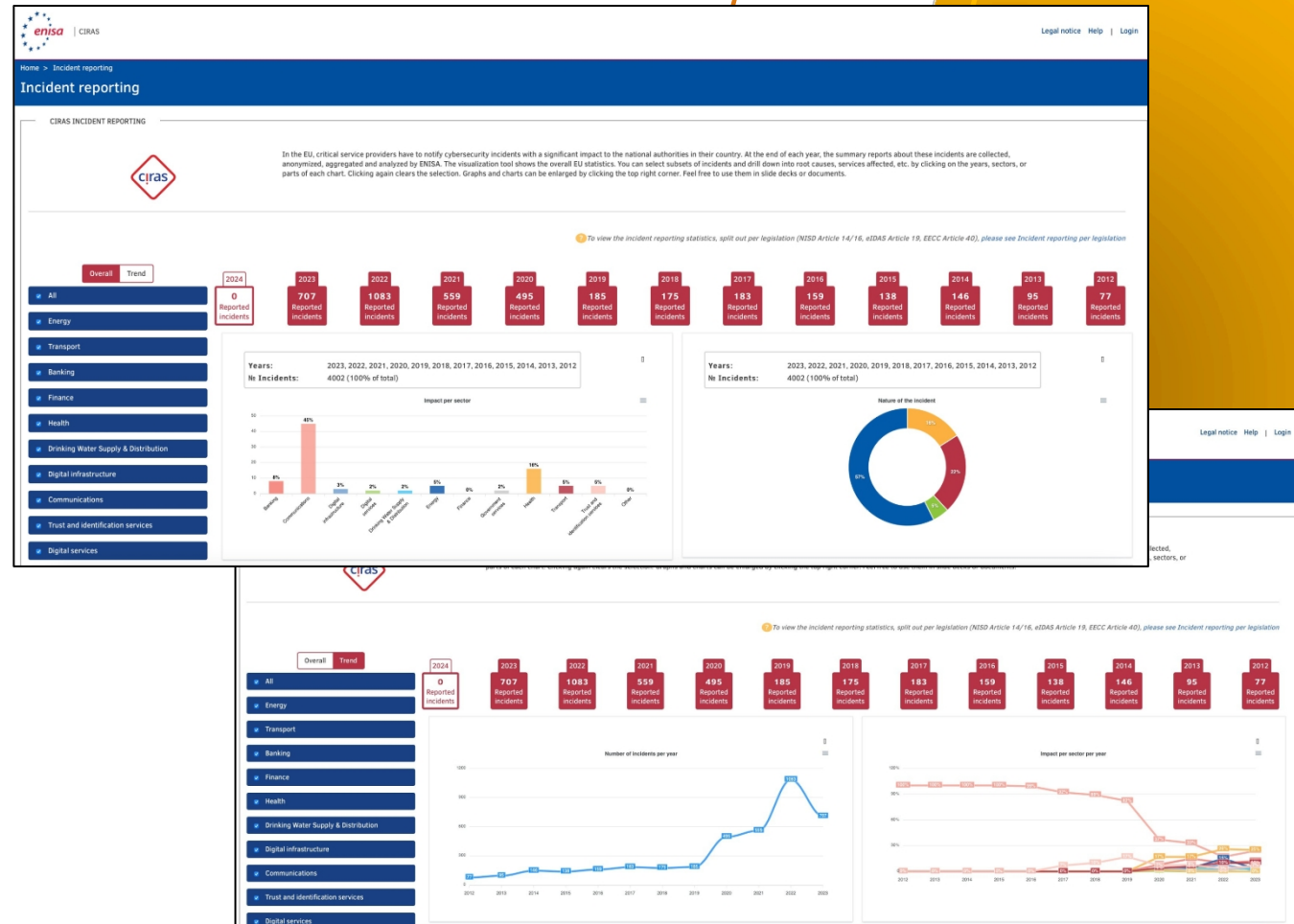
Fonte dell'immagine: Vecteezy  
URL: <https://www.vecteezy.com/vector-art/4496530-isolated-hydro-power-plants-generate-electricity>

## Perché l'energia è importante?

- Infatti, molte infrastrutture critiche (CI) **dipendono dall'energia** per il loro corretto funzionamento, come ad esempio:
  - Sistemi di trasporto
  - Sistemi di trattamento delle acque
  - Sistemi di produzione
  - Ospedali
  - Impianti chimici
  - Servizi finanziari
  - Alimentare e agricoltura
  - Sistemi di comunicazione
  - E altre infrastrutture critiche correlate
- Di conseguenza, viene creata una rete di sistemi (sistemi di sistemi) in cui diverse infrastrutture dipendono l'una dall'altra per **la continuità operativa**
  - E indirettamente per il benessere sociale ed economico

## Perché l'energia è importante?

- Purtroppo, **gli avversari** conoscono l'essenza di queste dipendenze tra le infrastrutture critiche e l'impatto che si verifica quando le risorse essenziali non vengono fornite in modo adeguato, e in termini diversi
  - Benessere sociale
  - Benessere economico
  - Reputazione organizzativa, ...
- L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), attraverso il sistema di segnalazione degli incidenti CIRAS, aggiorna e segnala annualmente gli incidenti di sicurezza informatica causati ai fornitori di servizi critici europei, come i sistemi di alimentazione elettrica



## Perché l'energia è importante?

- Considerando le relazioni fornite dall'ENISA e per alcune infrastrutture critiche, compresi i sistemi di comunicazione:

	2024	2023	2022	2021	2020
Potenza	?	27	169	26	13
Trasporti	?	72	109	34	22
Salute	?	183	284	98	88
Acqua	?	22	34	16	21
<b>Comunicazioni</b>	?	175	187	188	188

- Abbiamo constatato che il numero di incidenti di sicurezza aumenta ogni anno, soprattutto nei sistemi di comunicazione.
- Questo rappresenta un rischio aggiuntivo, poiché molti sistemi di comunicazione fanno parte delle operazioni di altre infrastrutture critiche per la loro corretta digitalizzazione e gestione adeguata

## Perché la sicurezza informatica nel settore energetico è importante?

- D'altra parte, quando le infrastrutture critiche non forniscono servizi essenziali o risorse fondamentali per l' e ad altre infrastrutture critiche
  - Ciò può portare al famoso...

CASCADE EFFECT  
**EFFETTO A CASCATA**

- Questo tipo di effetto si verifica anche internamente allo stesso sistema quando i singoli componenti cyber-fisici non forniscono i propri servizi agli altri
  - Principalmente perché si basano su:

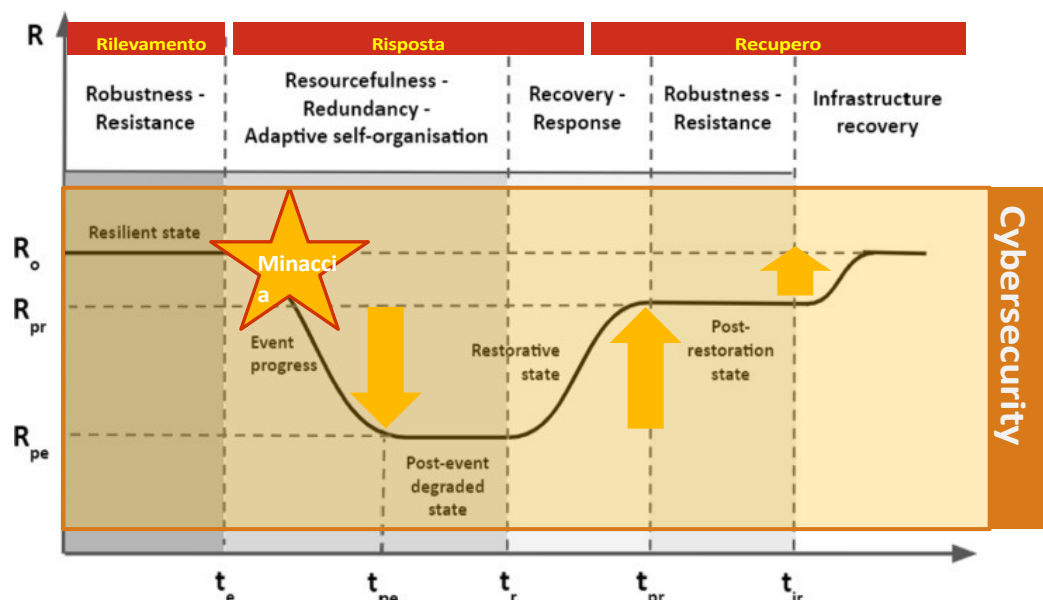
SYSTEMS OF SYSTEMS  
**SISTEMI DI SISTEMI**

## Perché la sicurezza informatica energetica è importante?

- È quindi necessaria la massima protezione, come indicato anche da organizzazioni internazionali quali:
  1. *Organizzazione europea per la sicurezza informatica (ECISO), "Reti energetiche e reti intelligenti", 2018*
  2. *ENISA, "Panorama delle minacce alle reti intelligenti e guida alle buone pratiche", 2013*
- A sua volta, questa protezione richiede:
  - Sicurezza critica: protezione funzionale, comprese le persone, da malfunzionamenti, guasti o errori
  - **Sicurezza**: protezione informatica contro minacce potenziali e deliberate, compresi attacchi fisici e informatici
- Inoltre, questa protezione può richiedere misure relative al rilevamento, alla risposta e al ripristino
  - Qualsiasi sistema deve essere in grado di ripristinare il proprio stato normale e garantirne la stabilità in ogni momento, assicurando **la resilienza**

## Perché la sicurezza informatica nel settore energetico è importante?

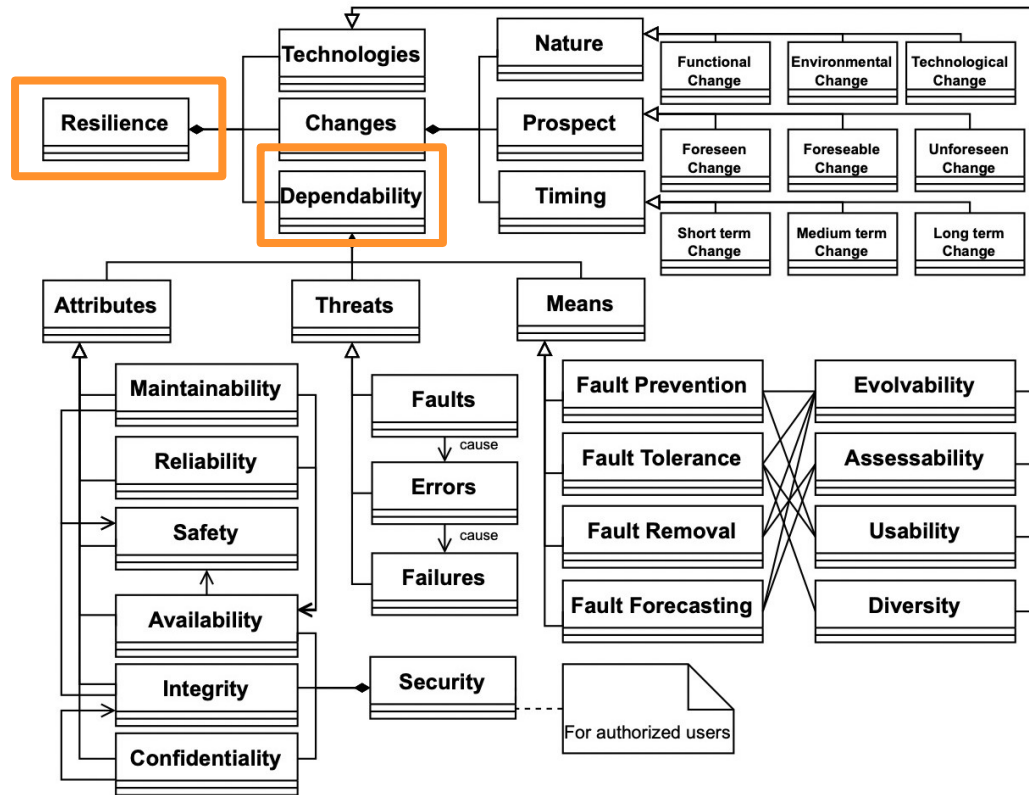
- Infatti, **la resilienza** è "*la capacità di un sistema di resistere, assorbire e riprendersi rapidamente da un evento esterno devastante, ad alto impatto e a bassa probabilità, come un evento meteorologico estremo o un attacco informatico*".
- Nei sistemi di alimentazione, questa resilienza attraversa normalmente diversi tipi di stati e segue il seguente ciclo di vita:



Fonte: A. D. Syrmakesis, C. Alcaraz e N. D. Hatzigargyriou, "Classificazione degli approcci di resilienza per la protezione delle reti intelligenti dalle minacce informatiche", International Journal of Information Security, vol. 21, pagg. 1189-1210, 2022.

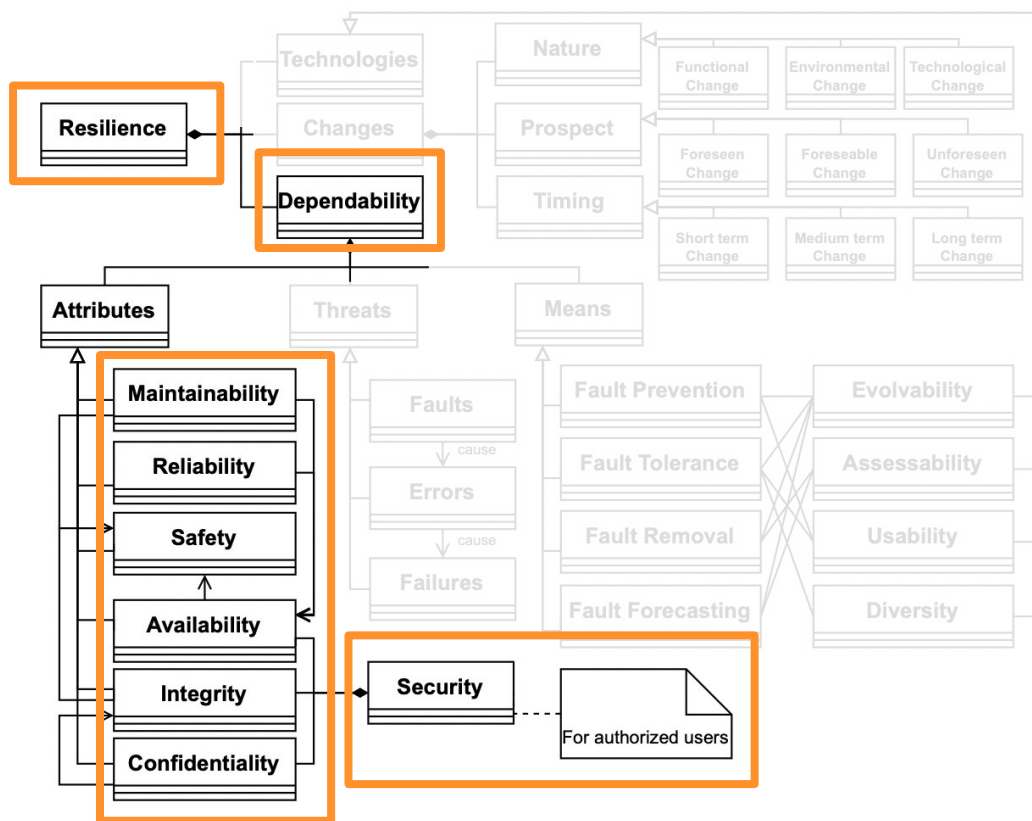
# Perché la sicurezza informatica nel settore energetico è importante?

- In altre parole, la resilienza comporta:



## Perché la sicurezza informatica nel settore energetico è importante?

- In altre parole, la resilienza comporta:



## Considerazioni finali

- Le infrastrutture energetiche sono sistemi fondamentali per il benessere sociale ed economico
  - Tutti dipendono dall'energia per vivere
  - Tutte le organizzazioni, le aziende e le istituzioni dipendono dall'energia per lavorare
  - Tutte le infrastrutture critiche dipendono dall'energia per funzionare
- Purtroppo, questi sistemi tendono ad essere vulnerabili a diversi tipi di attacchi
  - Il numero di incidenti aumenta ogni anno, con il rischio aggiuntivo di influire su altre infrastrutture, sistemi o componenti
- A questo proposito, è essenziale garantire i principi minimi di resilienza
  - Che sono soggetti a rilevamento, risposta e ripristino

# Riferimenti e fonti

1. Alcuni dati sono stati forniti da Vecteezy, URL: <https://www.vecteezy.com/> - grazie!
2. DeepL Translator per la revisione:  
URL: <https://www.deepl.com/translator>
3. IEA, Variazione anno su anno della domanda di energia elettrica per regione, 2019-2025, IEA, Parigi, IEA. Licenza: CC BY 4.0, URL: <https://www.iea.org/data-and-statistics/charts/year-on-year-change-in-electricity-demand-by-region-2019-2025>
4. ECSO, "Reti energetiche e reti intelligenti", Sicurezza informatica per il settore energetico, WG3, Domanda settoriale, novembre 2018  
URL: <https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf>
5. ENISA, "Panorama delle minacce alle reti intelligenti e guida alle buone pratiche", dicembre 2013  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>
6. M. Panteli, P. Mancarella, "La rete: più forte, più grande, più intelligente? Presentazione di un quadro concettuale della resilienza dei sistemi energetici", IEEE Power Energy Mag, 13(3), pagg. 58-66, 2015
7. A. D. Syrmakesis, C. Alcaraz e N. D. Hatzigryriou, "Classificazione degli approcci di resilienza per la protezione delle reti intelligenti dalle minacce informatiche", International Journal of Information Security, vol. 21, pp. 11891210, 2022.  
URL: <http://doi.org/https://doi.org/10.1007/s10207-022-00594-7>
8. F. Flammini, et al., "Verso sistemi autonomi affidabili: tassonomie e prospettive future", IEEE Transactions on Emerging Topics in Computing, 2022  
URL: <http://doi.org/https://doi.org/10.1109/TETC.2022.3227113>



# Connettiti con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web:  
[www.cybersecpro-project.eu](http://www.cybersecpro-project.eu)
2. X (Twitter):  
[https://twitter.com/CyberSecPro\\_eu](https://twitter.com/CyberSecPro_eu)
3. LinkedIn:  
<https://www.linkedin.com/company/cybersecpro-euproject/>



Co-funded by  
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

# Grazie

Per qualsiasi domanda, non esitate a contattare:

- Cristina Alcaraz  
Professore associato  
Università di Malaga  
[alcaraz@uma.es](mailto:alcaraz@uma.es)