

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

# Cybersecurity Essentials and Management for Energy Sector

## CSP001\_C\_E

PRESENTATION BY:

**CRISTINA ALCARAZ**

UNIVERSITY OF MALAGA, SPAIN

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

# Acknowledgement

- *Co-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*

# Topic-2: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge

## Overview

- Define energy cybersecurity and its significance in the energy domain
- Understand the various components of an energy cybersecurity ecosystem
- Classify cybersecurity threats and vulnerabilities specific to energy systems
- Overview of the Cybersecurity Body of Knowledge

# Topic-2: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge

## Overview

- **Define energy cybersecurity and its significance in the energy domain**
- Understand the various components of an energy cybersecurity ecosystem
- Classify cybersecurity threats and vulnerabilities specific to energy systems
- Overview of the Cybersecurity Body of Knowledge

## Definition of “energy cybersecurity”

- **Energy cybersecurity** is the field responsible for providing all those preventive and protective measures necessary to safeguard “energy” and all related equipment for its correct performance, also guaranteeing reliable power production and distribution services

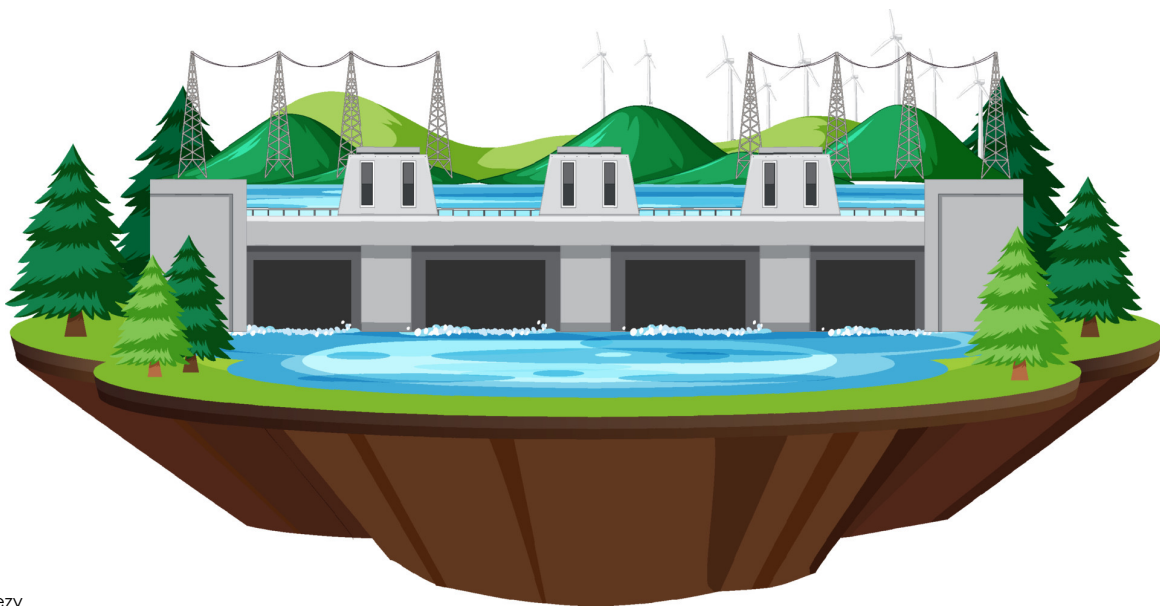


Figure source: Vecteezy  
URL: <https://www.vecteezy.com/vector-art/4496530-isolated-hydro-power-plants-generate-electricity>

## Why is energy relevant?

- Within energy sector, we can find several energy sources:

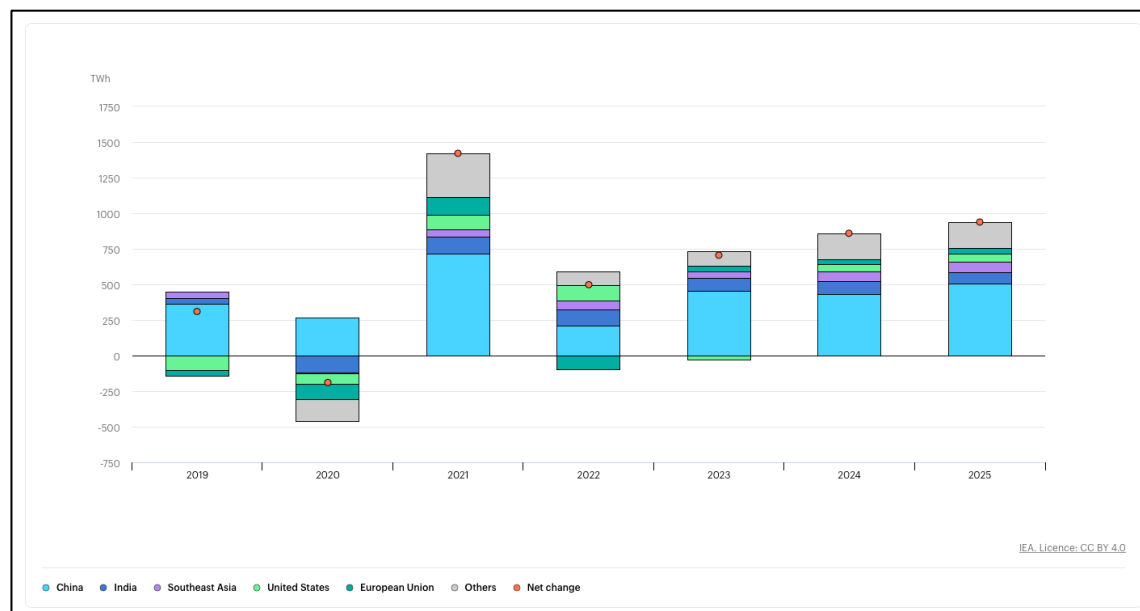
- Coal
- Oil and gas
- Nuclear
- **Electricity**

Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields.

- All of them are considered "**essential resources**", mainly because they guarantee:
  - Social and economic well-being
  - Continuity of other fundamental activities belonging to other dependent infrastructures

## Why is energy relevant?

- According to the International Energy Agency (IEA), there is a **high demand** for the power production and for the different countries, including Europe
  - Except in 2020 (after COVID-19) and 2022 (post-COVID-19)



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

CSP001\_C\_E – TOPIC 2: Cristina Alcaraz, University of Malaga, Spain

## Why is energy relevant?

- Unfortunately, this demand is typically subject to other essential sources such as water or wind,
  - Which creates a strong dependency among the essential sources themselves, and among systems
  - Without water → No energy production at hydroelectric power plants
  - But without energy → There is no way to manage water in other systems

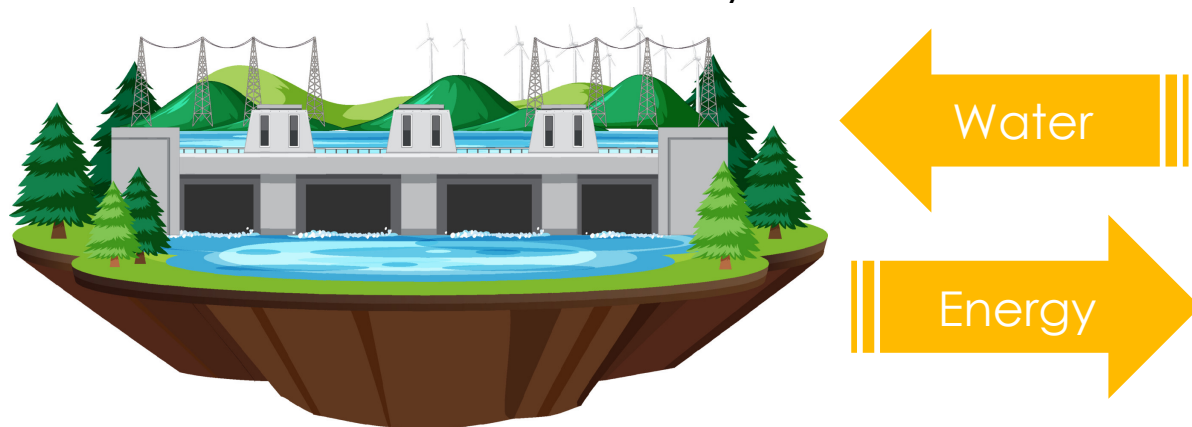


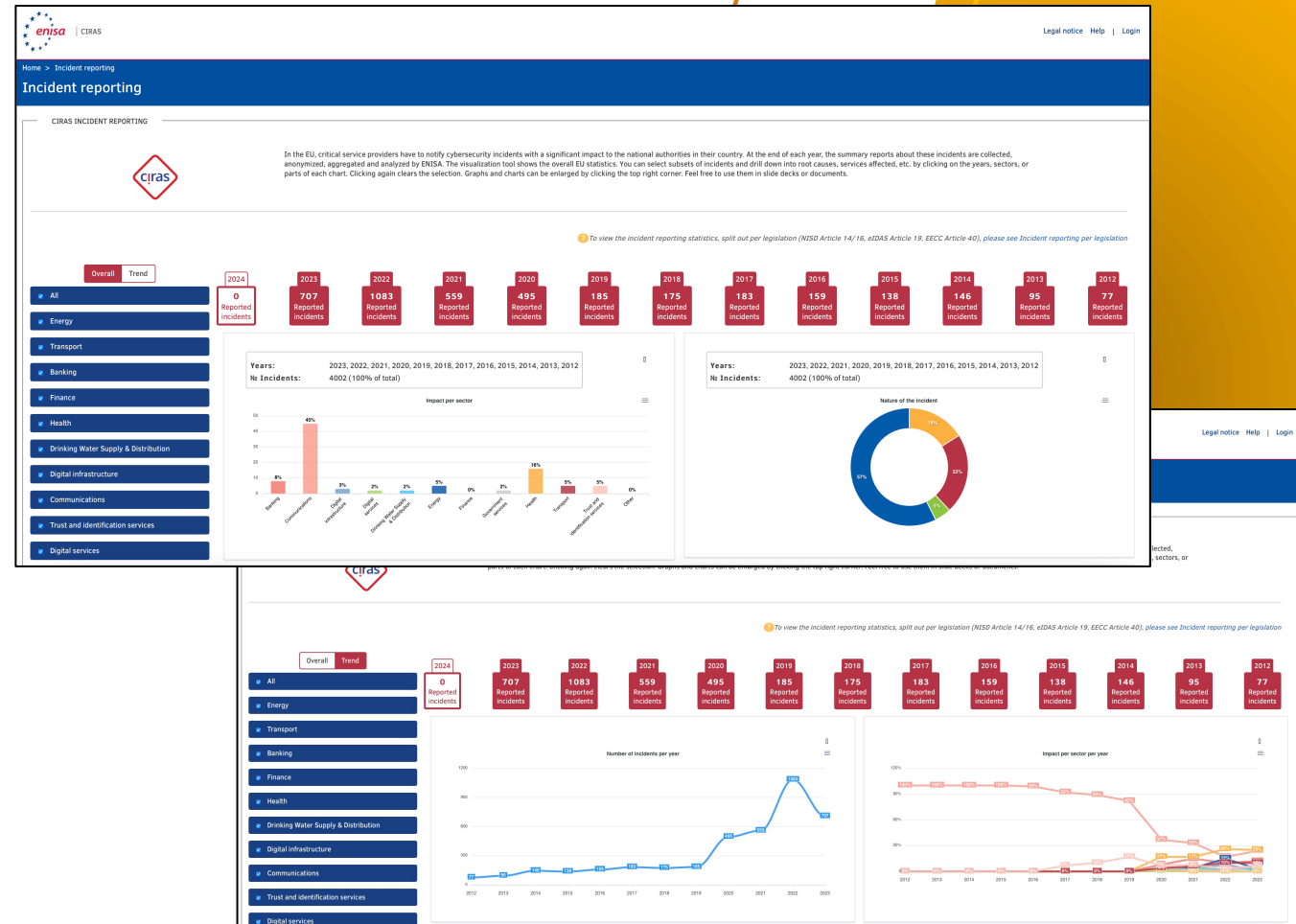
Figure source: Vecteezy  
URL:<https://www.vecteezy.com/vector-art/4496530-isolated-hydro-power-plants-generate-electricity>

# Why is energy relevant?

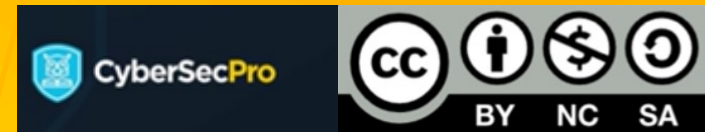
- In fact, many Critical Infrastructures (CIs) **depend on energy** for their proper operations such as:
  - Transportation systems
  - Water treatment systems
  - Manufacturing systems
  - Hospitals
  - Chemical facilities
  - Financial services
  - Food and agriculture
  - Communication systems
  - And other related CIs
- As a result, a network of systems (systems of systems) is created where different infrastructures depend on each other for **business continuity**
  - And indirectly for social and economic welfare

## Why is energy relevant?

- Unfortunately, **adversaries** know the essence of these dependencies between CIs, and the impact when essential resources are not properly provided, and in different terms
  - Social welfare
  - Economic wellbeing
  - Organizational reputation, ...
- European Union Cybersecurity Agency (ENISA), though CIRAS incident system, annually updates and reports the cybersecurity incidents caused in European critical service providers, such as power systems



Source: ENISA, CIRAS, 2024  
 URL: <https://ciras.enisa.europa.eu>



## Why is energy relevant?

- Considering the reports provided by ENISA, and for some critical infrastructures including communication systems:

	2024	2023	2022	2021	2020
Power	?	27	169	26	13
Transport	?	72	109	34	22
Health	?	183	284	98	88
Water	?	22	34	16	21
<b>Communications</b>	?	175	187	188	188

- We determine that the number of security incidents is increasing every year, especially in communication systems
- This is an added risk because many communication systems are part of the operations of other critical infrastructures for its correct digitization and proper management

## Why is energy cybersecurity relevant?

- On the other hand, when the CIs do not provide essential services or fundamental resources to other CIs
  - This may lead to the famous ...

## CASCADE EFFECT

- This type of effect also occurs internally within the same system when individual cyber-physical components do not provide their services to others
  - Mainly because they are based on:

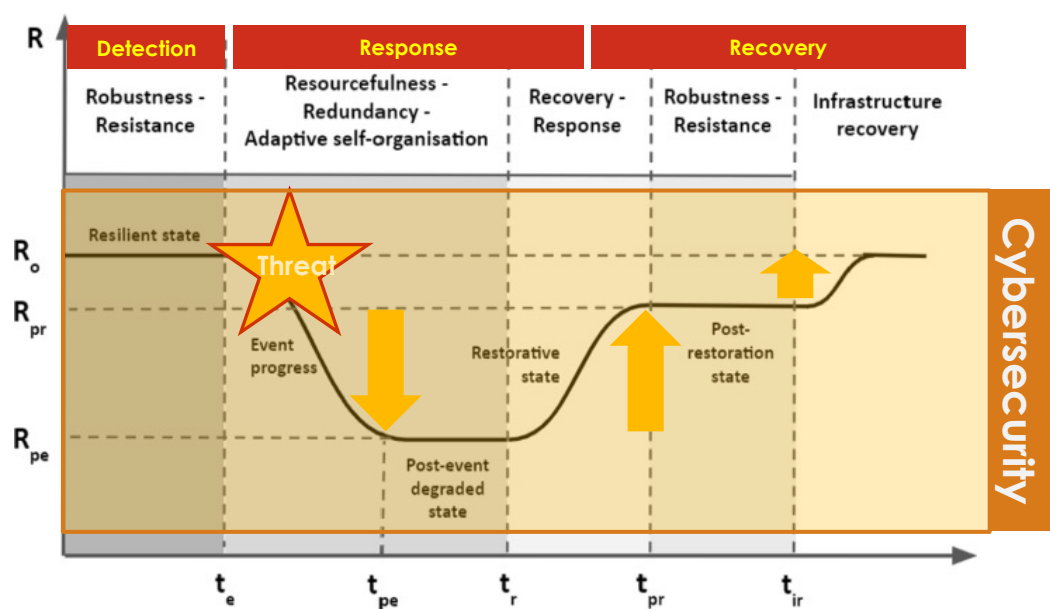
## SYSTEMS OF SYSTEMS

# Why is energy cybersecurity relevant?

- Maximum protection is therefore required, as also referenced by international organizations such as:
  1. *European Cyber Security Organization (ECSSO), "Energy Networks and Smart Grids", 2018*
  2. *ENISA, "Smart Grid Threat Landscape and Good Practice Guide", 2013*
- In turn, this protection requires:
  - **Safety-critical**: functional protection, including people, against malfunctions, failures or errors
  - **Security**: cyber protection against potential and deliberate threats, including physical and cyber attacks
- Moreover, this protection can require measures related to detection, response and recovery
  - Any system must be able to recover its normal states and ensure their stability at all times, guaranteeing **resilience**

## Why is energy cybersecurity relevant?

- Indeed, **resilience** is “the ability of a system to withstand, absorb and rapidly recover from an external, high-impact, low-probability devastating event, like an extreme weather event or a cyber-attack”
  - In power systems, this resilience normally passes through different types of states, and follows the following life-cycle:



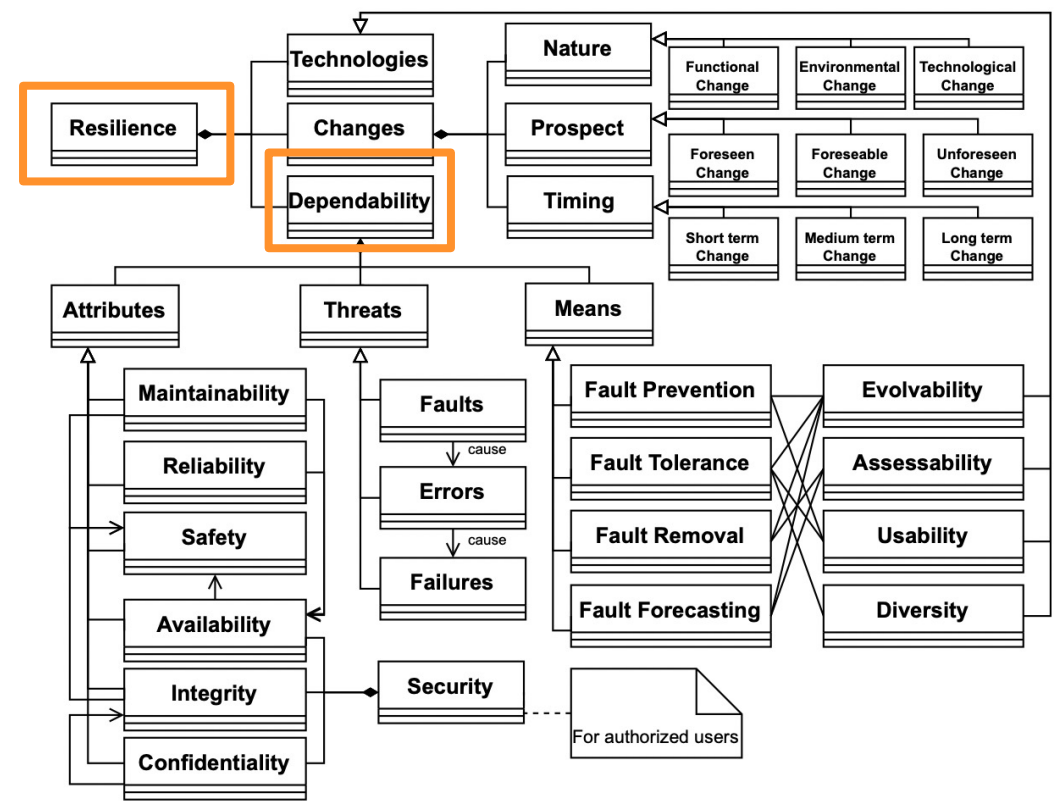
Source: A. D. Symakesis, C. Alcaraz, and N. D. Hatzigiorgiou, "Classifying resilience approaches for protecting smart grids against cyber threats", International Journal of Information Security, vol. 21, pp. 11891210, 2022.

CyberSecPro

CC BY NC SA

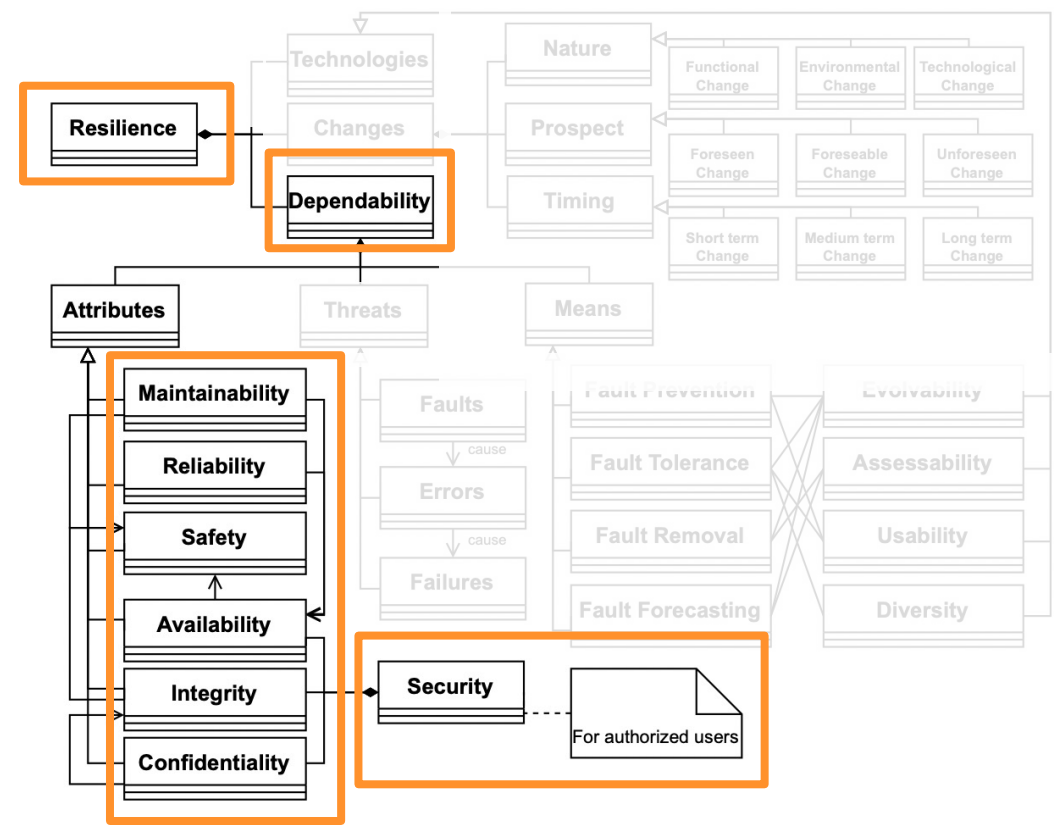
# Why is energy cybersecurity relevant?

- In other words, resilience entails:



# Why is energy cybersecurity relevant?

- In other words, resilience entails:



## Final remarks

- Energy infrastructures are fundamental systems for social and economic wellbeing
  - Everyone depends on energy to live
  - All organizations, companies and institutions depends on energy to work
  - All critical infrastructures depend on energy to operate
- Unfortunately, these systems trend to be susceptible to multiple types of attacks
  - The number of incidents is increasing every year, with the added risk of impacting other infrastructures, systems or components
- In this regard, it is essential to ensure the minimum principles of resilience
  - Which are subject to detection, response and recovery

# References and sources

1. Some figures are attributed from Vecteezy, URL: <https://www.vecteezy.com/> - thanks !
2. DeepL Translator for Proofreading: URL: <https://www.deepl.com/translator>
3. IEA, Year-on-year change in electricity demand by region, 2019-2025, IEA, Paris, IEA. Licence: 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, "Energy Networks and Smart Grids", Cyber Security for the Energy Sector, WG3, Sectoral Demand, November 2018  
URL: <https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf>
5. ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>
6. M. Panteli, P. Mancarella, "The grid: stronger, bigger, smarter? Presenting a conceptual framework of power system resilience", IEEE Power Energy Mag, 13(3), pp. 58–66, 2015
7. A. D. Syrmakesis, C. Alcaraz, and N. D. Hatzigargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats", 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., "Towards Trustworthy Autonomous Systems: Taxonomies and Future Perspectives", IEEE Transactions on Emerging Topics in Computing, 2022  
URL: <http://doi.org/https://doi.org/10.1109/TETC.2022.3227113>



# Connect with CyberSecPro: How to register and other practical information

1. Website:  
[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

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany <a href="#">Visit Website</a>	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria <a href="#">Visit Website</a>	APIROPLUS SOLUTIONS LTD Cyprus <a href="#">Visit Website</a>	SINTEF AS Norway <a href="#">Visit Website</a>	Social Engineering Academy GmbH Germany <a href="#">Visit Website</a>	Tallin University of Technology Estonia <a href="#">Visit Website</a>
Logo missing	 COFAC COOPERATIVA DE FORMAÇÃO E ANIMACÃO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Portugal <a href="#">Visit Website</a>	COFAC Portugal <a href="#">Visit Website</a>	Consiglio Nazionale delle Ricerche Italy <a href="#">Visit Website</a>	Technical University of Braunschweig Germany <a href="#">Visit Website</a>	Technical University of Crete Greece <a href="#">Visit Website</a>	trustilio B.V. The Netherlands <a href="#">Visit Website</a>
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 UNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FOCAL POINT Belgium <a href="#">Visit Website</a>	Goethe University Frankfurt Germany <a href="#">Visit Website</a>	Information Technology for Market Leadership Greece <a href="#">Visit Website</a>	Uninova Portugal <a href="#">Visit Website</a>	Universidad de Malaga Spain <a href="#">Visit Website</a>	Universidade Nova De Lisboa Portugal <a href="#">Visit Website</a>
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD 1969 SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télecom France <a href="#">Visit Website</a>	Laurea University of Applied Sciences Finland <a href="#">Visit Website</a>	Maggioli S.p.A. Italy <a href="#">Visit Website</a>	University of Cyprus Cyprus <a href="#">Visit Website</a>	University of Novi Sad Faculty of Sciences Serbia <a href="#">Visit Website</a>	University of Piraeus Research Center Greece <a href="#">Visit Website</a>
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal <a href="#">Visit Website</a>	Security Labs Consulting Ltd Ireland (Republic) <a href="#">Visit Website</a>	Serious Games Interactive Denmark <a href="#">Visit Website</a>	ZELUS P.C. Greece <a href="#">Visit Website</a>		

# Thank you

If you have any questions, please do not hesitate to contact:

- Cristina Alcaraz  
Associate Professor  
University of Malaga  
[alcaraz@uma.es](mailto:alcaraz@uma.es)