

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

# Network Protection for Energy Control Systems

## CSP004\_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: Common Security Weaknesses and Attacks in Energy Control Networks

## Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- Final remarks
- References and sources

# Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

## Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- **Final remarks**
- References and sources

# Final remarks

- Throughout this module, we have seen that **industrial communication protocols do not guarantee sufficient security measures** in terms of:
  - Availability, integrity, confidentiality and authentication/authorization
- This also means that industrial protocols depend on the **security protocols of the TCP/IP stack**
  - This stack is fundamental in energy control networks as it enables greater connectivity of elements and resources (e.g. CPS, IoT or IIoT devices)
- However, we have also seen that **the TCP/IP stack itself has a significant number of security breaches** and there are multiple offensive tools that may corrupt their performance
  - Therefore, the use of stack-specific security protocols becomes a primary requirement
  - These security protocols will be presented under the following topic
- Among the first protective actions, it is recommended to be aware of the existing **standards, recommendations and guidelines**, which can help to identify and deploy security measures in energy control networks
  - There are interactive tools that allow us to navigate between the different regulatory frameworks, facilitating their correct use

# Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

## Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- Final remarks
- **References and sources**

# 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. CloudShark.org – modbus-bug0.pcapng  
URL: <https://www.cloudshark.org/captures/4b8f9f3579b3>
4. K. Yasar, M. E. Shacklett, A. Novotny, "TCP/IP", 2024  
URL: <https://www.techtarget.com/searchnetworking/definition/TCP-IP>
5. CloudShark, "http-get-request.pcapng", 2024  
<https://www.cloudshark.org/captures/83390916ab62>
6. CloudShark, "ftp.pcap", 2024  
URL: <https://www.cloudshark.org/captures/abdc8742488f>
7. CloudShark "telnet-client-server.pcapng", accessed in 2024  
URL: <https://www.cloudshark.org/captures/818ceaef07b8?filter=telnet>
8. NIST, "Defence-in-depth", Computer Security Resource Center, Glossary, 2024  
URL: [https://csrc.nist.gov/glossary/term/defense\\_in\\_depth](https://csrc.nist.gov/glossary/term/defense_in_depth)
9. NIST, "Cybersecurity Framework (CSF) 2.0 Reference Tool", 2024  
URL: <https://csrc.nist.gov/Projects/Cybersecurity-Framework/Tools#/csf/filters>
10. ENISA, "Minimum Security Measures for Operators of Essentials Services", 2024  
URL: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services>

# 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**

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

 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 ANIMACAO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Italy <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)