Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
- **CRISTINA ALCARAZ**, UNIVERSITY OF MALAGA, SPAIN

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*

Protecting Charging Stations Against Specific Threats

01. Goals: Who-What-Why you need to take this training

02. Training logistics: When-Where-How

03. Learning outcomes

04. Training outlines

05. Exercises details

06. Practical information and requirements

07. Registration information and contacts

Goals: Who-What-Why you need to take this training

WHO

Anyone interested in learning about the protection of energy control networks, such as IT/OT engineers and administrators, energy professionals, students, researchers and educators with some knowledge of IT systems and basic cybersecurity

WHAT

Establishes the basis (though in an advanced level) for understanding the relevance of cybersecurity in a specific field of the energy sector

WHY

Equipping participants with the knowledge and skills necessary to develop a strategy for the protection of critical systems, their network infrastructures, data and essential resources such as control and power

CSP Training Logistic: When-Where-How

WHEN

As the module is held several times, it is advisable to check the CyberSecPro DCM platform for updated information

20 hours in total
(2 intensive weeks for teaching, 1+ week for practical activities = 3 weeks)

WHERE

Online, physical or both

All information on the connection mode will be published the DCM system

HOW

A module based on **synchronous classes** where each trainer will explain specific topics, and the end of the module various activities will be proposed, and an evaluation test will be carried out

Value Propositions

Benefits to Participants

- Exploration of a specific, but very common, field of application within the **Energy Sector**
- Level of training module: **Advance**
- **Cybersecurity professional training** in the field of energy control networks
- **Hands-on skills development**
- Rooted with **European cybersecurity skills frameworks**
- Cutting-edge insights from industry-academic experts
- Providing **adequate support for skills development and career advancement**

WHO

Profile of Training Participants

- Network engineers
- IT/OT administrators
- Energy professionals, including operators, managers and directives, energy suppliers, and employees in general of the corporate network
- Researchers, educators and students
- Cybersecurity practitioners
- Cybersecurity enthusiasts

WHO

Profile of Trainer

- **Cristina Alcaraz**
  Associate Professor at University of Malaga, PhD. in computer Science with extended experience on cybersecurity and critical infrastructure protection in power grids and Smart Grids
- **Abdelkader Shaaban**
  Scientist Security & Communication Technologies Centre for Digital Safety & Security PhD in Computer Science, Austrian Institute of Technology (AIT)

WHAT

Training Topics

- Introduction to energy control network protection
- Common security weaknesses and attacks in energy control networks
- Essential protection for energy control networks
- Advanced protection for energy control networks

WHY (Knowledge)

Learning Outcomes

- **Knowledge of vulnerabilities and threats** in specific network systems and protocols
- **Knowledge of** the most relevant **security protocols and mechanisms to protect critical networks**
- **Knowledge of** the most **relevant security mechanisms to protect the critical endpoints** of a communication, considering, for example, firewalls

WHY-2 (Practical Skills)

Learning Outcomes

- **Analyse** energy scenarios and **identify** configuration errors, vulnerabilities and risks
- **Configure** systems following basic security principles
- **Identify and implement** security mechanisms that improve the security of networks and critical endpoints

Training Outline

Trainers, sessions and estimated hours

Topic-1: Introduction to Energy Control Network Protection

- Cristina Alcaraz
- 1 session, 2 hours

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

- Cristina Alcaraz, Shaaban Abdelkader
- 2 sessions, 4 hours

Training Outline-2

Trainers, sessions and estimated hours

Topic-3: Essential Protection for Energy Control Networks

- Shaaban Abdelkader, Cristina Alcaraz
- 3 sessions, 6 hours

Topic-4: Advanced Protection for Energy Control Networks

- Shaaban Abdelkader, Cristina Alcaraz
- 3 sessions, 6 hours

Topic-1: Introduction to Energy Control Network Protection

We will cover these skills

- Introduction to the application context
- Main security challenges in power control networks, especially when the new ITs converge with OTs
- Classification of threats in energy control networks
- Case studies and analysis

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

We will cover these skills

- Main security weaknesses of the control networks, and their communication protocols
- Security weaknesses of the TCP/IP communication protocols and understand the security risks due to inheritance issues
- Offensive tools against the well performance of control networks and their resources
- Practical exercises to understand the weaknesses mentioned in the previous point

Topic-3: Essential Protection for Energy Control Networks

We will cover these skills

- The main TCP/IP security protocols to intensify the protection in operational communication channels
- Security measures for endpoints in order to prevent possible intrusions
- Practical exercises

Topic-4: Advanced Protection for Energy Control Networks

We will cover these skills

- Intrusion detection mechanisms and techniques to later specify detection rules at the network level where communication is based on industrial protocols
- Advanced monitoring mechanisms that controls the security management in energy control networks, as well as the logs that management endpoints such as IT and OT devices
- Practical exercises

Training Practical Exercises

Various types of practical exercises will be offered throughout the entire module:

- **Optional practical tasks**, which are not evaluated by the trainers
- **Final practical assignment**, which will be evaluated according to the number of activities, quality of the development or the technical applied by the leaners, and the quality of the reports

Evaluation method

Outline the evaluation elements and assessment process

Evaluation Element	How	Notes
Case studies (part of the optional tasks and test)	(Optional) individual tasks to reflect in the corresponding topic	Simple actions based on predominant readings to scientific articles, news, etc.
Final project / assignments – under 'quality' reports (REQUIRED)	Individual/team project to be submitted later	Practical actions using multiple types of tools and specialized simulators
Final test (REQUIRED)	Assessment test, which may integrate case studies where learners must show practical knowledge	In presence of the trainers (approx. 40-60 minutes)

Assignments (Score: 0.0-7.0)	Test (Score: 0.0 – 3.0)
70% of 10.0	30% of 10.0

Minimal score to successful pass the module: >= 5.0

Background Knowledge and Prerequisites

Background knowledge:

- Knowledge of cybersecurity fundamentals
- Knowledge of basic computer concepts
- Familiar with the traditional Operating Systems Linux and Windows

Prerequisites:

- Basic knowledge of IT and cybersecurity essentials
- Experience with operating systems, network configurations and communication protocols

Technical Tools and Other Requirement

Technical Tools

- Computer with Internet access for connection
- Access to the DCM platform
- Office software for reports
- Technical Tools: at least the GNS3 simulator, a hypervisor (Virtualbox/Vmware), and two Linux Virtual Machines (preferently Kali Linux or Parrot) – the rest of tools will be installed during the module

Other Requirements

- **Willingness to learn and experiment**
- **Awareness of Internet security practices, and its caution**
- **Active Participation**

Resources: Books and Reference Materials

1. QACafe, CloudShark, 2024
   URL: https://www.qacafe.com/analysis-tools/cloudshark/

2. ENISA, CIRAS, 2024
   URL: https://ciras.enisa.europa.eu

3. C. Alcaraz, J. Lopez, A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, no. 4, pp. 419-428, 2010, ISSN: 1094-6977

4. Netresec, "Captures files from 4SICS Geek Lounge", 2024
   URL: https://www.netresec.com/?page=PCAP4SICS

5. CS3Sthtlm, 2014-2020, 2024
   URL: https://cs3sthlm.se

6. 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

7. K. Yasar, M. E. Shacklett, A. Novotny, "TCP/IP", 2024
   URL: https://www.techtarget.com/searchnetworking/definition/TCP-IP

8. NIST, "Cybersecurity Framework (CSF) 2.0 Reference Tool", 2024
   URL: https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

9. NIST, NIST SP 800-113, 2008
   URL: https://csrc.nist.gov/pubs/sp/800/113/final

Resources: Books and Reference Materials

10. IETF, IP Security Protocol (IPSec), 2003-2004
    URL: https://datatracker.ietf.org/wg/ipsec/about/

11. IETF, IP Security (IPSec) and Internet Key Exchange (IKE) Document Roadmap,2011
    URL: https://datatracker.ietf.org/doc/html/rfc6071

12. Wireshark, 2024
    URL: https://www.wireshark.org

13. IETF, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408
    URL: https://datatracker.ietf.org/doc/html/rfc2408

14. Source: William Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition

15. What is IPsec? | How IPsec VPNs work | Cloudflare
    URL: https://www.cloudflare.com/en-gb/learning/network-layer/what-is-ipsec/

16. K. Brown, How to install and use telnet on Kali Linux, Linuxconfig.cong, 2021.
    URL: https://linuxconfig.org/how-to-install-and-use-telnet-on-kali-linux

17. PhoenixNAP, How to Install FTP Server on Ubuntu with vsftpd, 2024.
    URL: https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd

18. K. Scarfone and P. Hoffman, "Guidelines on Firewalls and Firewall Policy", NIST SP 800-41-rev1, NIST, Sept. 2009

Resources: Books and Reference Materials

19. Archlinux, nftables, 2024
URL: https://wiki.archlinux.org/title/nftables

20. NIST, "Guidelines for Smart Grid Cybersecurity", NIST IR 7628 Rev. 1, 2024.
URL: https://csrc.nist.gov/pubs/ir/7628/r1/final

21. NIST, "Intrusion detection", Computer Security Resource Centre, 2024
URL: https://csrc.nist.gov/glossary/term/intrusion_detection

22. NIST, "Guide Industrial Control Systems (ICS) Security", 2023
URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

23. IETF, Internet Security Glossary, 2007
URL: https://datatracker.ietf.org/doc/html/rfc4949

24. ENISA, "Appropriate security measures for smart grids.
Guidelines to assess the sophistication of security measures implementation", 2012
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

25. C. Davis, "Snorpy", 2024.
URL: http://snorpy.cyb3rs3c.net

26. Buchanan, William J (2024). Snort Analyser. Asecuritysite.com.
URL: https://asecuritysite.com/forensics/snort

Resources: Books and Reference Materials

27. Buchanan, William J (2024). Snort Analyser. Asecuritysite.com. https://asecuritysite.com/forensics/snort URL:https://asecuritysite.com/forensics/snort?fname=bit.pcap&rulesname=bit.rules

28. Seguridad en Sistemas Informáticos Detección de intrusión URL: https://www.tlm.unavarra.es/pluginfile.php/11611/mod_resource/content/0/clases/08_SSI-monitorizacion1.pdf

29. NIST, NIST 800-61r2, Computer Security Incident Handling Guide, 2012, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

30. Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee, Network Intrusion Detection and Prevention, Springer, ISBN 978-0-387-88770-8, 2010

Registration: How to register and other practical information

The specific registration process may vary depending on the training provider, institution, or access conditions established for each module

Nonetheless, the general steps are explicitly detailed in the **DCM platform**

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): 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

Thank you

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

- Cristina Alcaraz
  alcaraz@uma.es
- Abdelkader Shaaban
  abdelkader.shaaban@ait.ac.at