

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

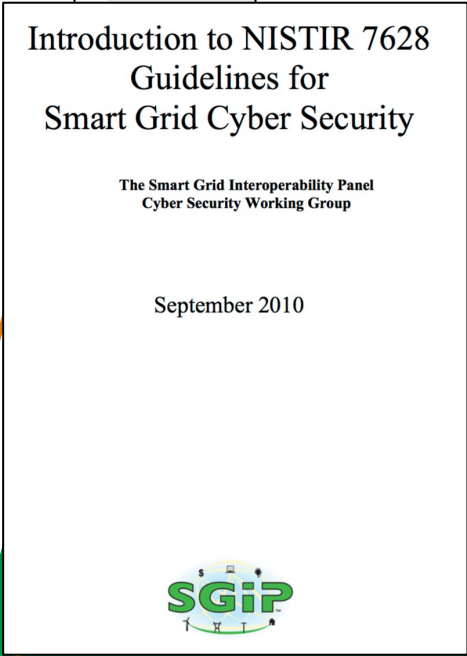
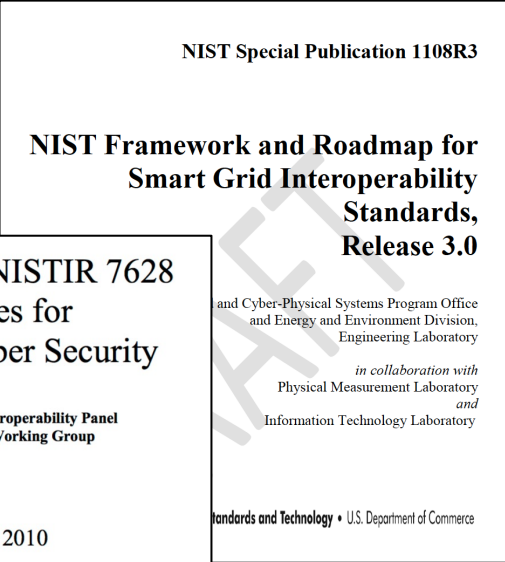
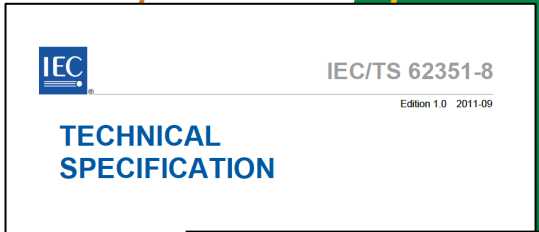
- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- **Best practices, recommendations and guidelines**
- Final remarks
- References and sources

# Defence in-depth

- From the previous sections, we deduce that it is required to establish a **defence in depth**
  - Not only providing direct security measures to the data within a system, but also protecting the whole system as a whole
- The National Institute of Standards and Technology (NIST) defines defence-in-depth as:
  - *“Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization”*
  - This also means that preventive measures at the level of the network and its perimeter must also be considered, and any access to resources must be controlled and regulated through regulatory frameworks
- A **regulatory framework** ranges from the application of standards and recommendations to the implementation of security policies under regulations

# Multiple resources for comprehensive regulatory frameworks

- **COBIT:** Control Objectives for Information and Related Technology
- **CSS:** Council on Cybersecurity
- **ANSI/ISA-62443-2-1 (99.02.01)-2009:** Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- **ANSI/ISA-62443-3-3 (99.03.03)-2013:** Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- **ISO/IEC 27001:** Information technology -- Security techniques – Information security management systems – Requirements
- **NIST SP 800-53 Rev. 4:** NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 7628:**
  - Vol1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
  - Vol2 - Privacy and the Smart Grid
  - Vol 3 - Supportive Analyses and References
- **NIST - NIST SP 800 82r2:** Guide to Industrial Control Systems (ICS) Security
- **NIST - Draft NISTIR 8228:** Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
- **IEC 62351:** Security Standards for the Power System Information Infrastructure
- **NISTIR 8183:** Cybersecurity Framework Manufacturing Profile
- NIST, **Framework for Improving Critical Infrastructure Cybersecurity**, v1.1
- NIST, **NIST Cybersecurity Framework, CSF 2.0**, NIST CSWP 29, 2024
- ...



# Multiple resources for comprehensive regulatory frameworks

**NIST Cybersecurity Framework (CSF) 2.0 Reference Tool**

Search:

**Function GOVERN (GV):** Establish an organizational context surrounding the organization and its information systems.

**Function PROTECT (PR):** Use safeguards to protect organizational information systems.

**Function DETECT (DE):** Find and analyze possible events that may indicate a cybersecurity incident.

**Function RECOVER (RC):** Restore assets and operations that were impacted by a cybersecurity incident.

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

CSP004\_C\_E – TOPIC 2: Cristina Alcaraz, University of Malaga, Spain



# Multiple resources for comprehensive regulatory frameworks

- The European Union Agency for Cybersecurity (ENISA) also provides attractive tools to identify and implement the best actions in critical domains such as the energy sector
- Among the tools, we highlight:
  - **“Minimum Security Measures for Operators of Essentials Services”**

SECURITY MEASURES	STANDARDS
<b>Incident Report</b>	<ul style="list-style-type: none"> <li>ISO 27019                             <ul style="list-style-type: none"> <li>13.1 Reporting information security events and weaknesses</li> </ul> </li> <li>NERC CIP                             <ul style="list-style-type: none"> <li>CIP-008 Cyber Security - Incident Reporting and Response Planning</li> <li>CIP-001 Sabotage Reporting</li> </ul> </li> <li>NIST SP-800-82                             <ul style="list-style-type: none"> <li>6.2.8 Incident Response</li> </ul> </li> </ul>
<b>Logging</b>	<ul style="list-style-type: none"> <li>ISO 27019                             <ul style="list-style-type: none"> <li>11.5.1 Secure log-on procedures</li> </ul> </li> <li>NERC CIP                             <ul style="list-style-type: none"> <li>CIP-007-6 Table R4 - Security Event Monitoring</li> </ul> </li> <li>NIST SP-800-82                             <ul style="list-style-type: none"> <li>5.16 Monitoring, Logging, and Auditing</li> </ul> </li> </ul>
<b>Logs correlation and analysis</b>	<ul style="list-style-type: none"> <li>ISO 27019                             <ul style="list-style-type: none"> <li>10.2.2 Monitoring and review of third party services</li> <li>10.10.2 Monitoring system use</li> </ul> </li> <li>NERC CIP                             <ul style="list-style-type: none"> <li>CIP-007-6 Table R4 - Security Event Monitoring</li> <li>CIP-007-6 Table R3 - Malicious Code Prevention</li> </ul> </li> <li>NIST SP-800-82                             <ul style="list-style-type: none"> <li>5.16 Monitoring, Logging, and Auditing</li> </ul> </li> </ul>
<b>Detection</b>	<ul style="list-style-type: none"> <li>NERC CIP                             <ul style="list-style-type: none"> <li>CIP-007-6 Table R4 - Security Event Monitoring</li> <li>CIP-007-6 Table R3 - Malicious Code Prevention</li> </ul> </li> <li>NIST SP-800-82                             <ul style="list-style-type: none"> <li>3.3 Potential ICS Vulnerabilities</li> </ul> </li> </ul>
<b>Information system security incident response</b>	<ul style="list-style-type: none"> <li>ISO 27019                             <ul style="list-style-type: none"> <li>13 Information security incident management</li> </ul> </li> <li>NERC CIP                             <ul style="list-style-type: none"> <li>CIP-008-5 Table R1 - Cyber Security Incident Response Plan Specifications</li> <li>CIP-008-5 Table R2 - Cyber Security Incident Response Plan Implementation and Testing</li> </ul> </li> <li>NIST SP-800-82                             <ul style="list-style-type: none"> <li>5.17 Incident Detection, Response, and System Recovery</li> </ul> </li> </ul>

Taking into account the characteristics of this module, this **network-level protection** should contemplate:

- Incident Report
- Logging
- Logs correlation and analysis
- Detection
- Information system security incident response
- Human resource security
- Information system security indicators
- Information system security risk analysis
- Information system security audit
- Information system security accreditation
- Information system security policy
- Authentication and identification
- IT security maintenance procedure
- System segregation
- Cryptography
- Industrial control systems
- Administration accounts
- Physical and environmental security
- Access rights
- Traffic filtering
- Administration information systems
- Systems configuration
- Disaster recovery management
- Business continuity management

Source: 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 ANIMACÃO 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)