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*

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

CSP004_C_E – TOPIC 2:
Cristina Alcaraz, University of Malaga, Spain

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

CSP004_C_E – TOPIC 2:
Cristina Alcaraz, University of Malaga, Spain

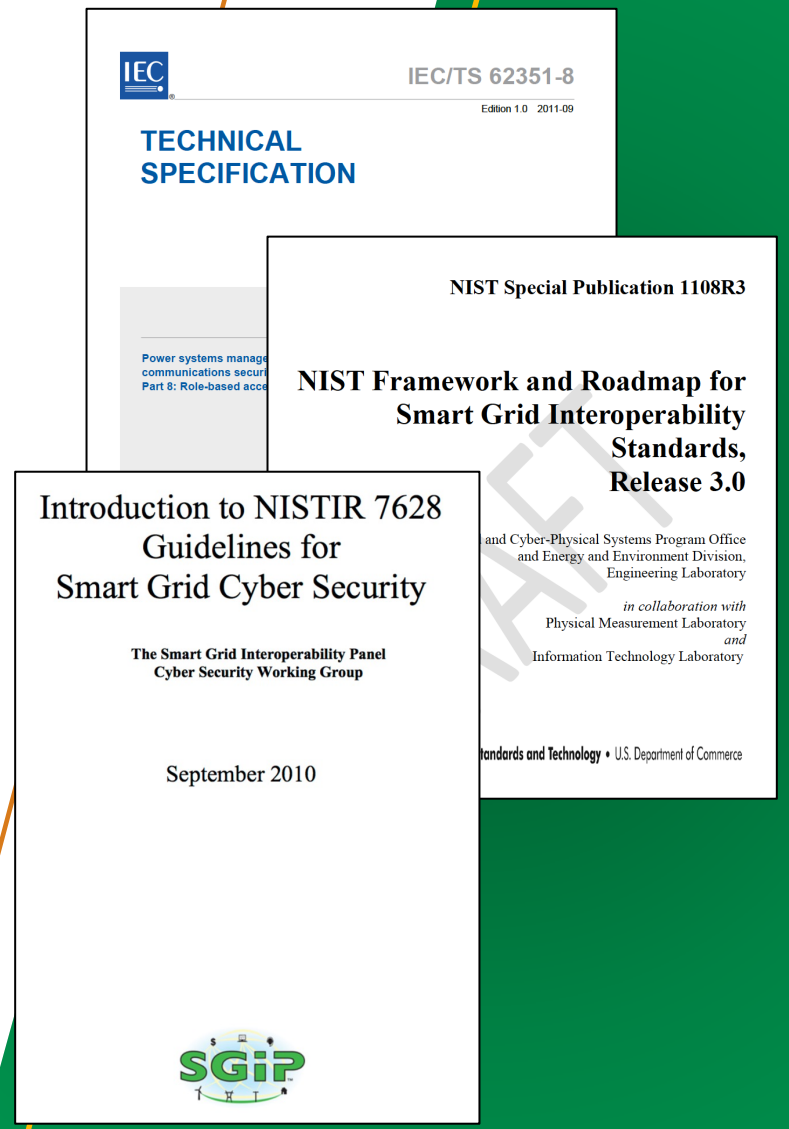
Defence in-depth

- 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

Source: NIST, "Defence-in-depth", Computer Security Resource Center, Glossary, 2024
URL: https://csrc.nist.gov/glossary/term/defense_in_depth

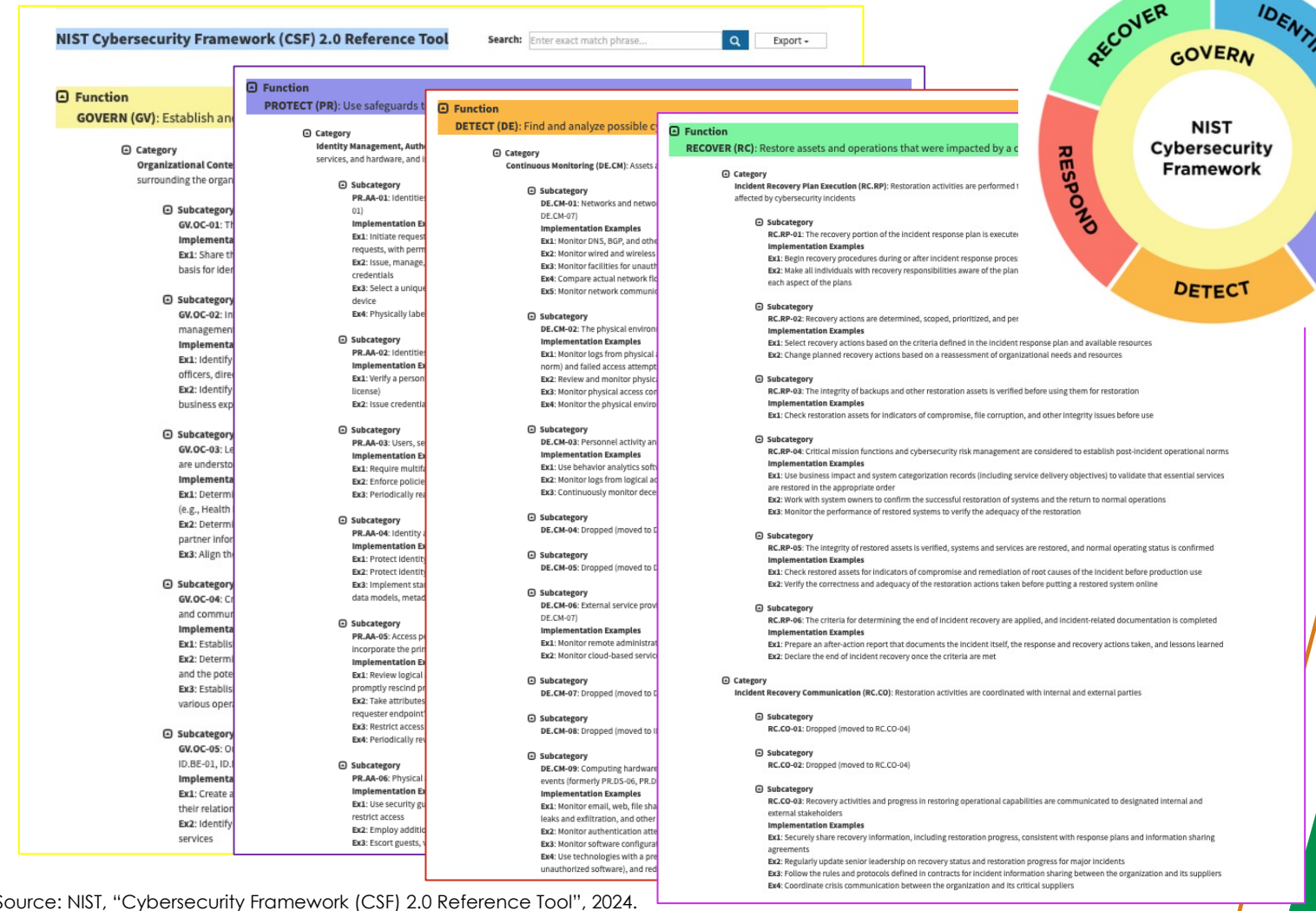
Multiple resources for comprehensive regulatory frameworks

- **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
- …



REGULATORY FRAMEWORKS

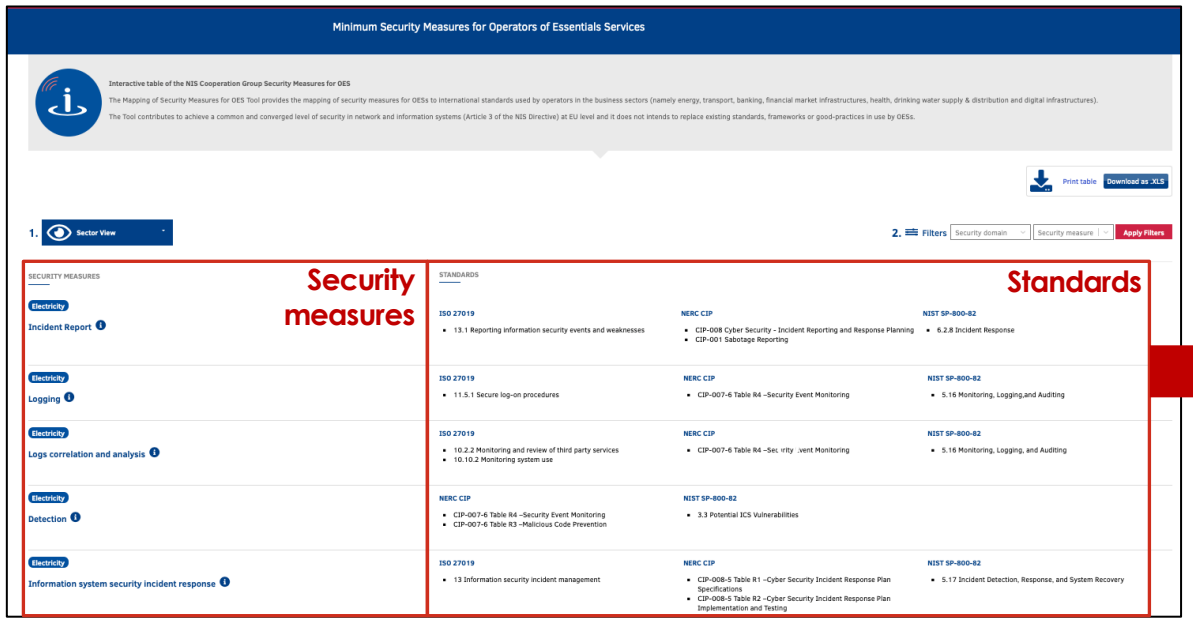
Multiple resources for comprehensive regulatory frameworks



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

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***"



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
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:

- Cristina Alcaraz
  Associate Professor
  University of Malaga
  alcaraz@uma.es