Bridging Theory and Practice for Enhanced Cybersecurity Awareness in Critical Infrastructures

Abdelkader Magdy Shaaban*
AIT Austrian Institute of Technology
abdelkader.shaaban@ait.ac.at

Stefan Schauer
AIT Austrian Institute of Technology
stefan.schauer@ait.ac.at

ABSTRACT

Developing advanced cybersecurity training programs is crucial for increasing cybersecurity awareness, especially when dealing with Critical Infrastructures (CIs). There is a significant gap in addressing both theoretical and practical activities to build a comprehensive and effective program that matches real-life cyberattacks on critical systems. This paper presents the efforts undertaken within the EU project CyberSecPro to bridge this gap by providing advanced training materials that align theoretical insights with practical activities to handle real scenarios.

Keywords

Cybersecurity, critical infrastructure, energy sector, awareness training.

INTRODUCTION

Background

Critical infrastructures (CIs) consist of multiple components, classified as physical and cyber. Both work together to exchange data and perform critical operations (König et al., 2023). The CI sectors encompass diverse industries essential to economic stability, public safety, and national security. These sectors include Energy, Transportation, Food and Agriculture, Healthcare, Nuclear Reactors, and many others that play a critical role in the functioning of modern society (CISA, 2025).

There are many cybersecurity challenges when considering protection measures for CIs (König et al., 2023). These reflect the importance of ensuring the continuous operation of essential services, as both public and private sectors heavily rely on CI facilities such as water supply, electricity, and healthcare (Klimburg et al., 2022).

Additionally, human vulnerabilities are another key factor that increases the likelihood of cyber attacks (Taylor, 2023). European Union Agency for Cybersecurity (ENISA), 2021 emphasizes this issue to raise the need for cybersecurity awareness and the importance of understanding cyber risks, their associated threats, and effective mitigation strategies. Sprinto, 2025 provides an overview of building a robust cybersecurity program aimed at protecting CIs and increasing stakeholder awareness. Furthermore, recent cybersecurity incidents have heightened the need for increased awareness among CI operators.

Problem Statement

Bridging the gap between theoretical insights and practical activities in cybersecurity education and training programs is considered one of the challenges in increasing cybersecurity awareness more efficiently. Traditional educational systems primarily focus on building a solid theoretical foundation and a comprehensive understanding of cybersecurity challenges from a theoretical perspective is necessary. However, it remains insufficient where real-world scenarios require practical solutions that effectively mitigate cyber risks (SecuritySenses, 2023). Furthermore, providing a comprehensive theoretical foundation in cybersecurity and integrating related practical activities into training programs is crucial for developing a comprehensive understanding of cyber risks and the solutions needed. Such an approach provides individuals with the skills necessary to address current and future cybersecurity challenges and has been conducted as an essential goal of the EU project CyberSecPro.

*Abdelkader Magdy Shaaban

Research Contributions

The CyberSecPro project aims to bridge the gap between theoretical and practical activities in cybersecurity training programs. Therefore, CyberSecPro encompasses collaboration between 27 active European partners, all collaborating to develop cutting-edge education, courses, and training materials in cybersecurity in critical sectors like healthcare, maritime, and energy (CyberSecPro Consortium, 2023). This paper presents CyberSecPro's efforts and role in enhancing cybersecurity awareness for CIs. While the CyberSecPro project addresses three sectors: energy, maritime, and health, this paper focuses primarily on the energy sector. It highlights key cybersecurity topics within this domain by examining three representative modules (see the following section for more details on the CyberSecPro modules):

- **CSP004_C_E**: Essential Protection for Energy Control Networks.
- **CSP006_S_E**: Cyber Threat Intelligence and Threat Hunting in the Energy.
- **CSP008_S_E**: Protecting Charging Stations Against Specific Threats.

This paper presents the developed modules as case studies to illustrate how CyberSecPro has effectively created relevant, sector-specific training materials that integrate thorough theoretical knowledge with practical activities, thereby enhancing cybersecurity awareness within the energy sector.

CYBERSECPRO OVERVIEW

The EU DEP Project "Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries" (CyberSecPro) aims to develop advanced educational and training materials to support teams working across multiple critical domains. This educational materials should integrate both theoretical knowledge and practical activities to ensure skill development in cybersecurity. The project has a clear focus on the energy sector, health sector and maritime sector but designs a curriculum for cybersecurity trainings that can be adopted to any critical industry sector. The goal is to enhance the awareness among CI employees for cyber risks, their potential effects within an organization and the multi-level consequences on the entire interconnected system of CI (CyberSecPro Consortium, 2023).

Skill Gaps and Approach

The CyberSecPro consortium investigated the main practical skills gaps in cybersecurity in Europe and analyzed the market demand for these skills. Since a complete list of these skills can be complex and interpreted differently by EU member states and organizations, a list of practical knowledge areas and highly essential practical skills has been compiled (CyberSecPro Project Consortium, 2023). This was achieved by implementing a systematic, in-depth literature review on cybersecurity frameworks, knowledge areas and skills, followed by a tailored market demand survey with cybersecurity professionals from the respective industries and the analysis of data collected during workshops with practitioners and experts. The resulting skill set (cf. Figure 1) represents not only the skills needed by the markets but also the practical skills offered in the EU academic programs and the gaps between demand and supply of practical skills. As not all critical industry sectors could be covered, a main focus was laid on the energy, health and maritime sectors.

As a result, more than 25 essential practical knowledge areas were identified that are relevant for the health, energy and maritime as well as the ICT and other sectors. Based on these knowledge ares, the practical skills gaps in Europe were extracted and clustered into "high-demand" and "in-demand" areas. This list was then used as the basis for the conceptualization of twelve CyberSecPro Training Modules that comprise the CyberSecPro Syllabus (cf. Figure 2). These modules are directly aligned with the identified skill gaps, whereas one module can address two or more gaps or one gap can be addressed by two or more modules. For example, the high demand "Network and Communications Security" (Figure 1) is addressed in the module "Network Security" and partially covered in the modules "Cybersecruity Essentials and Management" as well as "Human Factors and Cybersecurity" and "Digital Forensics", depicted in Figure 2. Each module has a clear definition of the target audience and the topics that should be covered therein. Further, CyberSecPro partners have developed a set of courses, seminars, workshops and hands-on trainings for each of the modules, implementing the respective topics. Additionally, the material for each module is instantiated for the project's main sectors energy, health and maritime. Accordingly, each instantiated module is labeled with the module number (e.g., "CSP004" for "Network Security"), the type of the module (e.g., "C" for course, "S" for seminar, etc.) and the respective domaine (e.g., "E" for energy, "H" for health and "M" for maritime). Overall, CyberSecPro produced a collection of 70+ courses, seminars, workshops and trainings.

Figure 1. Collection of the cybersecurity skill gaps identified in CyberSecPro. (CyberSecPro Project Consortium, 2023)

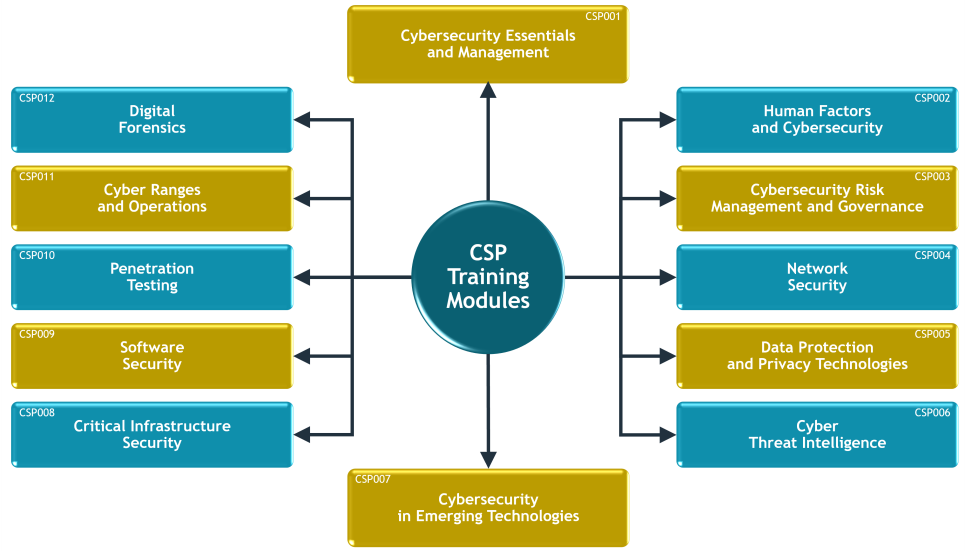

Figure 2. Illustration of the CyberSecPro Training Modules. (CyberSecPro Project Consortium, 2024a)

Target Audience Overview for Sector-Specific Cybersecurity Training Modules

In order to ensure the theoretical and practical relevance and effectiveness of cybersecurity training programs, the CyberSecPro project has carefully tailored its training modules to meet the needs of diverse stakeholders across critical sectors. Each module addresses multiple cybersecurity challenges with varying levels of expertise, starting from entry-level students to experienced practitioners. That aims to ensure that theoretical foundations and practical activities are accessible and meaningful for the intended audience. The table below provides a high-level overview of the targeted audiences for the developed modules in the energy, maritime, and health sectors.

Energy Sector

The training modules for the energy sector are designed for a diverse audience with various roles and expertise levels. They target human operators, engineers, IT/OT administrators, developers, and other technical staff responsible for managing and securing energy systems. The modules also help cybersecurity professionals, forensic analysts, incident responders, and those involved in digital threat intelligence or CI protection. Managers, executives, policymakers, and directives manage critical energy application domains. Additionally, the training also includes materials designed for university undergraduate and postgraduate students, early-career professionals, and individuals with a basic understanding of IT or cybersecurity. Since these modules target participants with varying levels of

expertise, while some modules require no prior knowledge, others require some basic understanding of IT and cybersecurity fundamentals, including network configurations, communication protocols, and operating systems. Certain modules also recommend programming skills, especially in languages commonly used in cybersecurity, such as Python, as well as familiarity with Linux distributions, such as Kali Linux. Advanced modules may require a prior understanding of cyber defence techniques to fully engage with more complex scenarios. CyberSecPro Deliverable D3.4 (CyberSecPro Project Consortium, 2024c) provides more detailed information about each module developed in the energy sector.

Maritime Sector

The training modules for the maritime sector target a diverse audience, including seafarers, ship owners, port authorities, and maritime organizations seeking to strengthen their understanding of cybersecurity fundamentals. They also address the needs of IT and security professionals responsible for managing cyber threats and information systems in maritime contexts, as well as business leaders who require strategic awareness of the evolving threat landscape. Additionally, the training supports specialists involved in safeguarding maritime CI, such as ports, offshore energy facilities, and underwater networks, by equipping them with knowledge of digital risks and sector-specific protection measures. These modules may require specific knowledge to ensure participants are well integrated with the module content. While some modules do not require any prior knowledge, others require a basic understanding of IT and cybersecurity concepts. Depending on the module's focus, familiarity with maritime operations, networking principles, or common security tools may be necessary. Again, certain modules recommend experience with Kali Linux, Active Directory, or programming skills, particularly in Python when machine learning applications are involved. CyberSecPro Deliverable D5.3 (CyberSecPro Project Consortium, 2024d) provides more detailed information about all developed modules for the maritime domain.

Health Sector

The training modules for the health sector are designed for a wide range of professionals working in hospitals, clinics, medical device environments, and related healthcare organizations. The target audience includes healthcare managers, IT professionals, cybersecurity specialists, and anyone handling sensitive patient data. The modules offer foundational and advanced knowledge in areas such as cybersecurity management, risk governance, threat intelligence, and anomaly detection. They also provide practical skills for protecting health information systems, focusing on both strategic frameworks and technical implementations like machine learning-based threat detection and data analysis across healthcare networks. Pre-requisite knowledge for practical aspects may be required for participants to be more familiar with the advanced topics covered in these modules. Therefore, some modules may require a foundational understanding of IT and cybersecurity. Additionally, depending on the module, participants may need familiarity with basic hardware and software used in network security, as well as proficiency in networking concepts such as IP addressing, routing, and subnetting. Some modules recommend basic skills in operating systems, software installation, and troubleshooting, as well as experience with Kali Linux, Active Directory, and initial knowledge of Active Directory attacks. Furthermore, modules that explore machine learning applications may require good programming skills, particularly in Python. CyberSecPro Deliverable D3.3 (CyberSecPro Project Consortium, 2024b) provides more detailed information on each developed module for the health sector.

THEORETICAL CYBERSECURITY AWARENESS

Cybersecurity Threat Landscape and Risk Factors in CIs

CyberSecPro includes advanced topics as part of its theoretical contribution to increasing cybersecurity awareness in the energy sector including essential topics for addressing key security challenges in power control systems. The energy sector modules in CyberSecPro provide an overview of major cyberattack incidents in the energy sector and their societal impact, as discussed in Fursov et al., 2022. Figure 3 illustrates the distribution of these attacks over specific years, highlighting the locations and the exact facilities affected by these incidents.

The graph shows specific cyberattack incidents and their impacts on targeted particular energy facilities. For example, in 2015, a Distributed Denial of Service (DDoS) attack targeted electricity operators in Ukraine, resulting in the disconnection of approximately 30 substations from the smart grid and causing electricity outages in multiple locations. Similarly, in Austria in 2022, a cyberattack affected around 5,800 wind turbines across Europe, requiring several hours to restore their functionality to normal (Fursov et al., 2022).

These incidents demonstrate how cyberattacks on energy infrastructures can target various critical components, including physical resources such as the grid or micro-grid, Distributed Energy Resources (DERs), charging infrastructures, generators, transformers, and other essential assets. The module CSP004_C_E "Network Protection

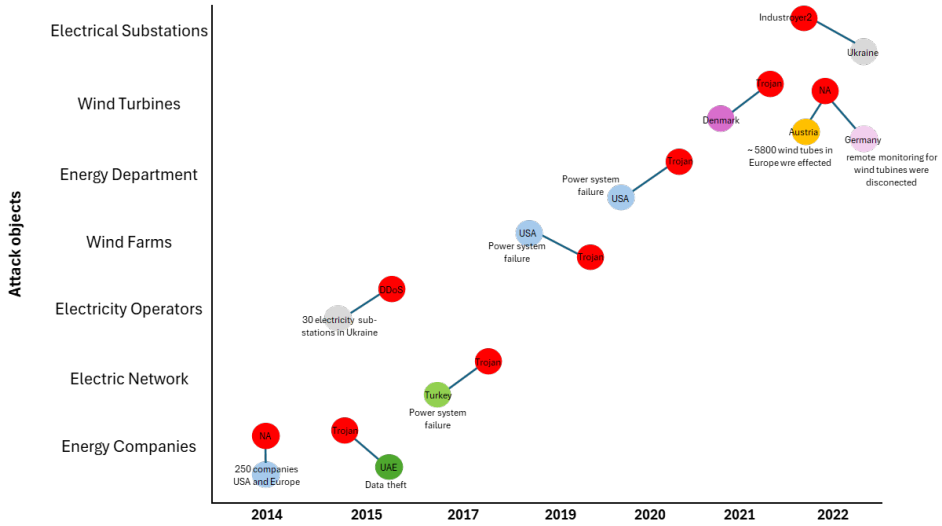

Figure 3. An Overview of Cyberattacks and their Impacts on CIs

for Energy Control Systems" describes the structure of the energy sector, covering multiple stages, including electricity generation, transformers, transmission, and distribution, until it reaches the consumers. This provides an understanding of the energy sector's structure, from generation to consumer. Then, the module classifies threats and taxonomy in control networks based on the AIC+A/A model, as follows:

- **Availability (A)**: Ensuring system service continuity is a fundamental cybersecurity objective (A. M. Shaaban et al., 2022). Jamming attacks pose significant risks by disrupting wireless communications, including ZigBee PRO, WirelessHART, and ISA100.11a. Denial of Service (DoS) attacks are another major threat to availability that aims to flood the network with many packets, leading to an overload of targeted network nodes (Alcaraz and Lopez, 2010).
- **Integrity (I)**: Attacks targeting integrity aim to manipulate packet contents without legal authorization, including information manipulation, routing falsification, and Sybil attacks (Alcaraz and Lopez, 2010). The CyberSecPro modules address these threats and demonstrate how integrity violations can lead to severe consequences in the energy sector. For instance, attackers could take over the control of critical units responsible for monitoring or controlling operations in the smart grid by injecting malicious code into the control network.
- **Confidentiality (C)**: Ensuring that information is accessed or manipulated only by authorized parties (A. M. Shaaban et al., 2022). Data eavesdropping could be one of the threats that could violate confidentiality, leading to a man-in-the-middle (MITM) attack and compromising the control network in the energy sector.
- **Authentication and Authorization (A/A)**: Every individual or entity accessing sensitive data related to critical information must be properly authenticated and authorized. The project's modules discuss spoofing attacks or entity impersonation, where attackers steal and misuse the identity of a legitimate node. Such attacks can lead to further threats, including MITM attacks, unauthorized access to critical devices, eavesdropping on communications, and more.

Cybersecurity attacks can directly target energy facilities; however, they may also exploit subsystems of the smart grid to cause significant disturbances to electricity services. For example, with the increasing development of electric vehicles (EVs), which are considered part of smart transportation and smart infrastructure as well (Garofalaki et al., 2022), the number of Electric Vehicles Charging Stations (EVCS) is also growing to accommodate the growing demand for EVs (IEA, 2024). The integration of EVs with EVCS forms a smart grid system, connecting various nodes like mobile devices and Cyber-Physical Systems (CPS), introducing new cybersecurity challenges (Garofalaki et al., 2022). Module CSP008_S_E "Protecting Charging Stations Against Specific Threats" discusses the cybersecurity challenges within EVCS. The module outlines key Charging Station (CS) infrastructure components, including process devices, controllers such as Programmable Logic Controller (PLC) and Remote Terminal Units (RTU), and field devices such as sensors, actuators, and smart meters. Additionally, it covers devices with limited capabilities that integrate with CSs, such as embedded devices (e.g., Arduino) and small computing devices (e.g., Raspberry Pi).

Additionally, the module highlights the common cybersecurity risks in CS applications, such as malware, lack of encryption, API abuse, supply chain risks, and insufficient authentication (Dorot, 2023). The module covers real-world cyberattacks on EVCS, highlighting vulnerabilities in 16 Internet-enabled EVCS software products, including firmware-based, web-based, and mobile-based systems. 13 severe Common Weakness Enumeration (CWE) vulnerabilities and their potential risks have also been discussed. As the smart grid is the primary concern, cyberattacks directly targeting the power grid through EVCS, such as manipulating charging and discharging demand, could be exploited by attackers to disrupt its overall performance (Nasr et al., 2022).

Security challenges raised in the module CSP008_S_E also include security weaknesses in traditional communications (e.g., Ethernet, WiFi) and industrial protocols (e.g., Open Charge Point Protocol (OCPP), Modbus/TCP, Open Platform Communications Unified Architecture (OPC UA)). It details OCPP security challenges, highlighting improvements in v2.0.1 over v1.6, which lacks built-in security. Some of these challenges are discussed in (Alcaraz et al., 2023), as follows:

- Denial of Service (DoS) attacks against charging stations
- Manipulation of OCPP configuration variables (CVs)
- Charging station (CS) spoofing
- Manipulation of Distributed Energy Resources (DERs) and storage systems
- User and Energy Management System spoofing
- Information disclosure
- User authorization and administrative security risks in EVCS.

In order to provide knowledge about the threat-related actors, module CSP006_S_E "Cyber Threat Intelligence and Threat Hunting in the Energy Domain" outlines threat actors, the attack lifecycle, and types of intelligence used to characterize threats. It demonstrates open-source tools for intelligence sharing and response automation, including examples like the MITRE ATT&CK framework (MITRE, 2025), including the tactics and techniques attackers use to target a system. CyberSecPro incorporates practical security exercises, guiding participants through a fictitious attack scenario based on the MITRE ATT&CK lifecycle for hands-on experience securing target data.

Threat modelling is a key part of system engineering that helps identify potential threats and necessary security measures to reduce risk (A. Shaaban, 2021). It has been integrated into module CSP006_S_E to provide detailed methodologies for cybersecurity professionals to address existing system weaknesses effectively. The Cascading Effects and their impact on other CIs are critical topics in CSP008_S_E. The module demonstrates how cascading effects provide estimates of the impact on each component (König et al., 2023) within the energy domain. Additionally, it explores how the impact of a threat can disrupt the operation of other CIs, with potential damage influencing interconnected infrastructures.

Mitigation Strategies and Theoretical Insights to Enhancing Security Awareness in CIs

Effective security mitigation strategies and solutions are crucial for addressing cyberattacks. Cybersecurity trainings should focus on providing comprehensive knowledge that relates closely to real-world scenarios.

CyberSecPro's models also provide insights into advanced cybersecurity solutions in the energy sector that can increase the stakeholders' knowledge of protecting critical assets. Module CSP004_C_E outlines regulatory frameworks that guide the protection of CIs, such as:

- IEC 62443-2-1: Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners (IEC, 2024).
- IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels (IEC, 2013).
- ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO, 2022).
- NIST SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations, (NIST, 2013).

- NISTIR 7628 Rev. 1: Guidelines for Smart Grid Cybersecurity, (NIST, 2014).
- NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security, (NIST, 2015).
- IEC 62351: Cyber Security Series for the Smart Grid, (IEC, 2023).
- NIST IR 8183: Cybersecurity Framework Manufacturing Profile, (NIST, 2017).
- Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, (NIST, 2010).
- NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0, (NIST, 2021).
- The NIST Cybersecurity Framework (CSF) 2.0, (NIST, 2024).

Module CSP008_S_E discusses security measures to mitigate cyber risks in EVCS and the smart grid, highlighting the importance of robust countermeasures and endpoint authentication to protect CS applications from information disclosure.

Module CSP004_C_E defines key security protocols to ensure secure communication among interconnected systems in the energy sector (Katar, 2025). Internet Protocol Security (IPsec) is also discussed, and its advantages in real-world applications are presented. The Secure Sockets Layer (SSL) is also covered, describing its architecture and role in securing communications (Stallings, 2010). Additionally, the module addresses Transport Layer Security (TLS), explaining the differences between TLS and SSL, the importance of SSL/TLS for data protection, and how SSL helps mitigate cyberattacks by authenticating web servers and preventing data tampering during transit (Cloudflare, 2025).

The module also explores security countermeasures for specific threats. It presents cryptographic checksums to mitigate data modification, Trojan horse browsers, and memory tampering. Robust encryption techniques address confidentiality and authentication violations (Stallings, 2010). Additionally, the module discusses the role of SSL/TLS in securing Internet of Things (IoT) components in the energy sector, including the use of trusted SSL/TLS certificates to authenticate and encrypt IoT devices. It also emphasizes the importance of TLS in establishing secure connections to IoT hubs and verifying identities between servers and clients (Microsoft, 2025).

Further, it covers advanced protection methods for energy control networks, focusing on intrusion detection techniques and monitoring solutions like Security Information and Event Management (SIEM) systems. It describes the types of security information and events and the tools that generate them, such as Intrusion Detection Systems (IDSs) and firewalls. The module also addresses the challenges of managing and analyzing large volumes of security data (e.g., logs). It introduces SIEM solutions as an efficient way to tackle these challenges by offering an efficient approach (Wazuh, 2025):

- Asset discovery
- Vulnerability assessment
- Network analysis
- Host-Based Intrusion Detection Systems (HIDS)
- Network-Based Intrusion Detection Systems (NIDS)
- File integrity monitoring
- Log management

SIEM solutions enhance threat detection, response, and security operations, enabling a robust approach to protecting energy control networks.

PRACTICAL CYBERSECURITY AWARENESS

Cybersecurity Practical Activities: Demonstrations and Effective Security Solutions

CyberSecPro offers deeper knowledge by combining the previously discussed theoretical solutions with real-world applications, which provides a sharper vision of the previously discussed theoretical cybersecurity challenges and related best practices for addressing them and bridging the gap between theory and practice. This supports trainees in better understanding how cyberattacks in real-world scenarios can be accomplished and how to determine suitable security mitigations for protecting systems and their data from unexpected attacks. Furthermore, module CSP004_C_E delivers intensive practical activities that offer a better understanding of various cybersecurity tools that attackers could use to exploit existing system vulnerabilities. It also provides deep knowledge of technical cybersecurity solutions for addressing and mitigating these cyber risks.

Simulation Environment and Cyberattack Demonstrations

To provide an effective virtual lab with a closed, cybersecurity-isolated environment, participants can engage with multiple cybersecurity tools to demonstrate how these tools can be employed for various cyberattack activities and address existing security weaknesses, helping to avoid or mitigate related cyber risks. Furthermore, we used the GNS3 Network Simulator (GNS3 Development Team, 2024), which facilitates the integration of Virtual Machines (VMs) that act as a set of victim machines and an attacker machine. Figure 4 illustrates the developed lab environment used in the practical activities within the module CSP004_C_E.

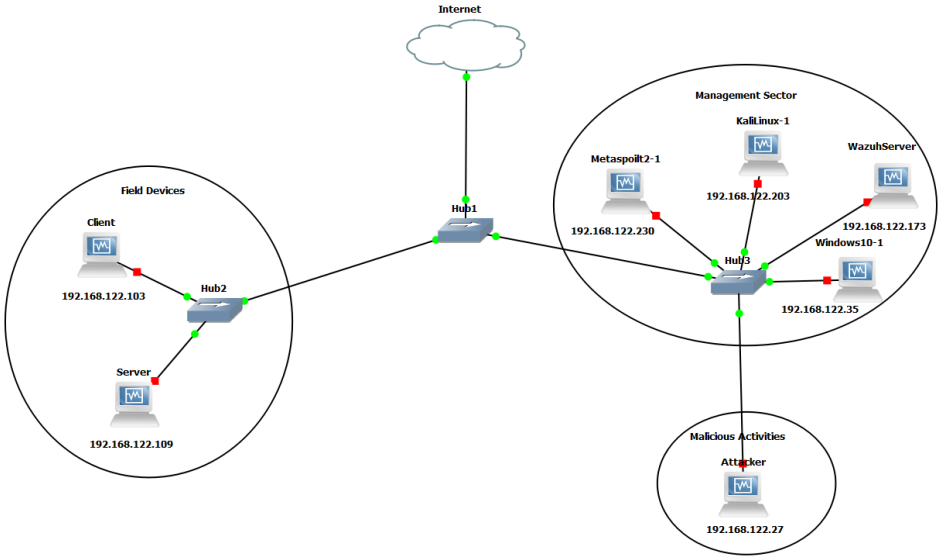

Figure 4. An Isolated Cybersecurity Environment

The figure illustrates the distribution of multiple interconnected VMs, classified into three main sections:

- **Field Devices Section**: This section contains two victim machines (e.g., client and server) using the Linux Raspberry Pi. Both machines utilize the ModbusTCP protocol, implemented using a Python library (Lefebvre, 2024), where the protocol is used to simulate the transmission of packets from the client to the server, as in a real-world example.
- **Management Section**: This section includes a set of VMs responsible for network management and monitoring:
  - **Kali Linux**: It is utilized as a management and monitoring device to continuously observe and detect suspicious activity within the virtual network.
  - **Windows Machine**: A Windows machine is used to show some compatible tools for cybersecurity activities.
  - **Metasploit Server**: It acts as a vulnerable system containing multiple security weaknesses. It provides participants with an opportunity to understand common vulnerabilities that can exist in a network and how attackers could exploit them.

  - **Wazuh Server**: Integrated into the practical activities as a SIEM system, monitoring and protecting critical network assets.

- **Attacker Section**: A Kali Linux machine demonstrates various cybersecurity attack scenarios employed against victims' machines within the virtual environment.

The primary objective of creating this isolated environment using the GNS3 simulator is to ensure that all cybersecurity activities are conducted within a controlled virtual setting. That aims to prevent direct or indirect threats to real networks, devices, or assets while maintaining ethical considerations.

Cyberattack Demonstrations in the Simulation Environment

Multiple cyberattack demonstrations were conducted within this simulation environment. Here are some examples of the practical cybersecurity exercises that have been conducted during the practical activities:

- **Denial of Service (DoS) Attack:** Demonstrated how victim machines, mainly the Raspberry Pi devices, can be affected by overwhelming their network traffic with many packets, leading to degraded service performance or making the whole system downtime.

- **Metasploit Exploitation:** The Metasploit server assists participants in identifying and exploiting common cybersecurity weaknesses, discovering vulnerabilities, and understanding how to address these issues.

- **Brute Force Attack:** A brute force attack is performed against the Metasploit server to demonstrate how attackers can exploit weak credentials by attempting to guess usernames, passwords, or both.

- **Unauthorized Sniffing & Packet Analysis:** An attacker can intercept packets for unauthorized analysis. The practical activities demonstrate data exchange between two victim devices (as shown in the field devices sector in Figure 4), both using the ModbusTCP protocol, with the client sending data to the server. Then, it is demonstrated that an attacker can use Wireshark to intercept and analyze transmitted packets. This exercise allows trainees to see how weak confidentiality measures can expose critical data exchanged between the client and server to potential threats.

- **Exploiting Open Ports:** It demonstrated how attackers can use simple tools to exploit security weaknesses, such as missing open points in the network.

- **Man-in-the-Middle (MITM) Attack:** Demonstrated how an attacker could intercept and manipulate communication between two devices within the network.

- **ARP Spoofing / ARP Poisoning Attack:** Address Resolution Protocol (ARP) spoofing, or ARP poisoning (DevX, 2023), is a spoofing attack that attackers use to intercept data. In this attack, the attacker tricks a device into sending its data to the hacker instead of the intended recipient (Lenaerts-Bergmans, 2022). The practical activities include demonstrating this attack and how an attacker performs an MITM attack to intercept the data flow between the victim and the gateway. This allows the attacker to sniff packets, such as victim credentials, when the victim does not use encryption solutions, such as accessing a website with an HTTP service instead of a secure HTTPS connection. Additionally, code injection is also demonstrated, where an attacker injects malicious code into the victim's system.

- **DNS Spoofing:** The Domain Name System (DNS) spoofing attack is another cyber attack in which the attacker manipulates DNS requests so that the attacker's device intercepts them. The attacker can then redirect the victim's request to an incorrect IP address, leading the victim to a fake website instead of the intended legitimate one. This attack is demonstrated by having the victim device visit a specific website while the attacker performs DNS spoofing using a Kali Linux VM. A fake website hosted and run locally on the Kali VM is then sent to the victim instead of the requested page. This is a critical threat if the victim attempts to provide personal information or credentials, which could lead to serious consequences.

Cybersecurity Practical Solutions for Detecting and Mitigating Cyber Risks

The practical activities also focus on detecting and mitigating critical cyberattacks within the simulated virtual network. Here are some examples of the practical solutions that have been conducted during the practical activities:

- **Network Scanning:** Different techniques for network scanning have been employed in practical activities to identify unauthorized devices connected to the network. So, these techniques are used to collect more information about all connected devices within the network, such as the type of active operating system (OS) or IP addresses. That gives the way for raising an alert that a potential attacker may be active.
- **Firewalls:** Firewalls are essential for securing computer networks. Furthermore, the iptables tool is conducted in practical activities as it is considered the Linux internal firewall. This tool enables system administrators to define rules for handling incoming and outgoing network traffic and determining whether to accept, drop, or reject packets. That provides a better understanding of how firewall protections can be executed on particular devices to mitigate cyber threats. For example, defining rules that allow communication only between authorized parties can mitigate attacks such as packet injection and DoS attacks.
- **ARP Spoofing Detection:** As discussed previously, ARP spoofing is a type of cyberattack that can impact target devices. Practical activities have demonstrated solutions that can be integrated into different OS to automatically or manually detect and prevent ARP spoofing attacks.
- **Maintaining Confidentiality:** Ensure data secrecy can be achieved by implementing robust encryption techniques in data exchanges between interconnected nodes. These techniques help maintain data confidentiality even in the event of successful attacks, such as ARP spoofing or accessing unsecured websites (e.g., HTTP). The practical exercises demonstrate how Virtual Private Networks (VPNs) enhance data confidentiality and highlight the importance of integrating TLS/SSL to secure HTTP communications and protect transmitted data from cyber threats.
- **Intrusion Detection Systems (IDS):** IDS is one of the most efficient approaches for automatically detecting suspicious activities within a network. Therefore, SURICATA (OISF, 2025) has been utilized in practical activities to demonstrate a real IDS system within a network, identifying and altering potential intrusion attempts. To test the effectiveness of network intrusion detection, the testmyNIDS is utilized for evaluating NIDS detection (3CORESec, 2025). The results demonstrated how SURICATA can effectively detect and respond to such threats.
- **SIEM Solutions:** SIEM solutions play a crucial role in security monitoring and IT system protection. They offer multiple functionalities, including configuration assessment, malware detection, file integrity monitoring, threat hunting, log data analysis, vulnerability detection, incident response, and more (Wazuh, 2025). In the practical activities, all victim machines were configured with Wazuh as active agents, while the Wazuh Server managed security services. The Wazuh dashboard provided a professional and graphical overview of all active agents, highlighting security vulnerabilities on each endpoint. An example of file integrity monitoring was demonstrated to show how, in the event of a cyberattack attempting to manipulate a file's content on a target device, Wazuh detects and reports unauthorized changes. It provides precise alerts, identifying the type of modification and determining which file was altered. The threat-hunting feature has also been demonstrated by simulating a backend tool manipulating a particular port's status, such as unauthorized opening or closing, to show how Wazuh effectively detects such activities.

Threat Modeling with ThreatGet

Threat modelling is an essential approach for supporting cybersecurity training, as it helps investigate and identify security weaknesses in system models. Widely used tools, which primarily run on local machines, provide valuable capabilities for structured threat analysis. However, integrating such tools into cybersecurity training programmes can present challenges. As desktop applications, they offer limited collaborative functionality, which may restrict teamwork in dynamic training environments. In contrast, the latest version of ThreatGet (AIT Austrian Institute of Technology, 2024) offers a web-based approach. It supports flexibility in modelling, making the process easier, as it is not restricted to a particular operating system (OS). The tool has also had a significant impact across multiple EU projects where ThreatGet has been integrated. Through its application in real-world case studies, it supports a deeper understanding of cybersecurity risk analysis approaches, demonstrating its effectiveness as a valuable component of cybersecurity training programs.

Therefore, ThreatGet has been presented to show how such an effective cybersecurity analysis framework can be utilized in more realistic use cases related to the energy sector. ThreatGet was developed by AIT - Austrian Institute of Technology [1], which aims to provide a straightforward understanding of which security mechanisms need to be implemented to mitigate any potential cyber risks. The tool automates risk analysis and evaluates identified

[1] https://www.ait.ac.at/en/

risks to detect cybersecurity vulnerabilities that require further attention (A. M. Shaaban et al., 2023). Additionally, this approach builds multiple paths by mapping all identified threats detected by the tool. That highlights all the possible ways that attackers could follow to reach malicious goals (A. Shaaban et al., 2024). This feature enables users to explore all potential routes an attacker might take to compromise a system, supporting deeper analysis and proactive risk mitigation, functionality not available in most similar solutions.

The tool has been developed to be applied across multiple domains, including automotive, industrial, IoT, CPS, Unmanned Aerial Vehicles (UAV), agriculture, etc. ThreatGet offers a wide range of components that users can utilize to model various system designs that closely reflect real-world structures. Figure 5 illustrates an example of the energy sector modelled using a set of interconnected components to represent the data flow between them.

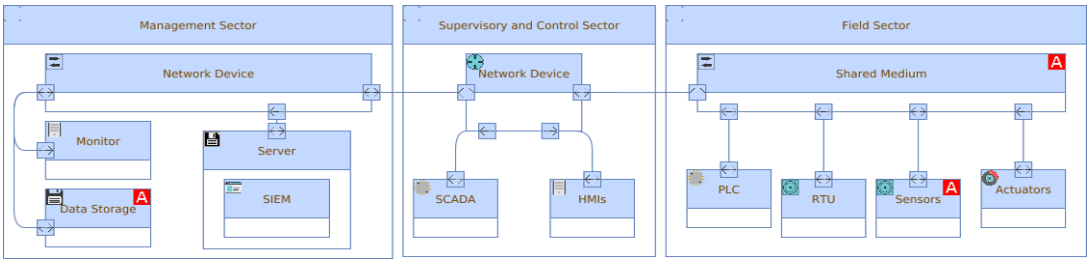

Figure 5. General Components of the Energy Sector

The figure illustrates the structure of interconnected components in the energy sector. A set of sensors collects specific data, which PLCs then process, while SCADA systems facilitate monitoring and control. The data is subsequently stored remotely on a data server, with security solutions such as a SIEM system operating within the management sector to detect suspicious activities within this network.

Once the model is complete, the user can launch a risk analysis through ThreatGet, checking all interconnected components and identifying potential threats from existing security vulnerabilities in the system model. This analysis process is mainly based on ThreatGet's predefined rules to detect cyber threats, classifying each one according to the STRIDE model for a better understanding of attack behaviours and assisting in selecting appropriate mitigation measures. Figure 6 shows the outcomes of ThreatGet based on the model defined in Figure 5.

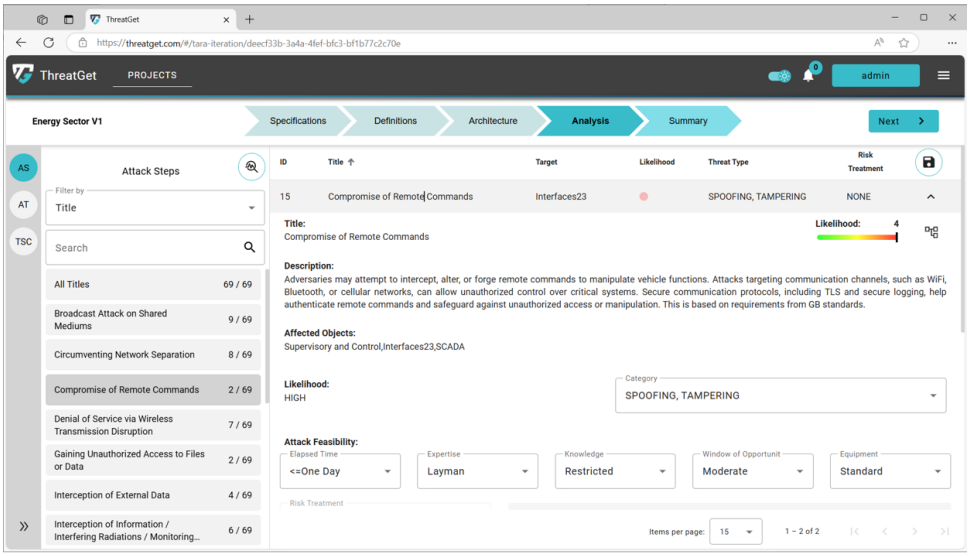

Figure 6. ThreatGet Outcomes for Cybersecurity Risk Analysis

The figure illustrates ThreatGet's outcomes with all threats detected. The tool provides information for each threat, such as a title, a brief description, and a likelihood estimation. The likelihood value is calculated in ThreatGet based on multiple factors, including attack feasibility, required expertise, knowledge level, window of opportunity, and necessary equipment. The STRIDE model is also presented to categorize each threat accordingly. Based on the results, the user or participant can determine the appropriate mitigation strategies to address security issues that may threaten the entire system or specific components within it.

Integrating ThreatGet with the practical activities within the developed modules provides a robust, effective solution that aligns with the theoretical insights of threat modelling and demonstrates how the cybersecurity analysis process is conducted in real-world scenarios.

Cascading Effects with CASSANDRA

Successful cyberattacks against CIs can trigger cascading effects due to interdependencies with other infrastructures. A disruption that occurs in one CI could be propagated to other infrastructures and lead to destabilising and impacting the operations of others. For example, Figure 7 illustrates how a power plant influences other critical sectors such as healthcare, transportation, etc.

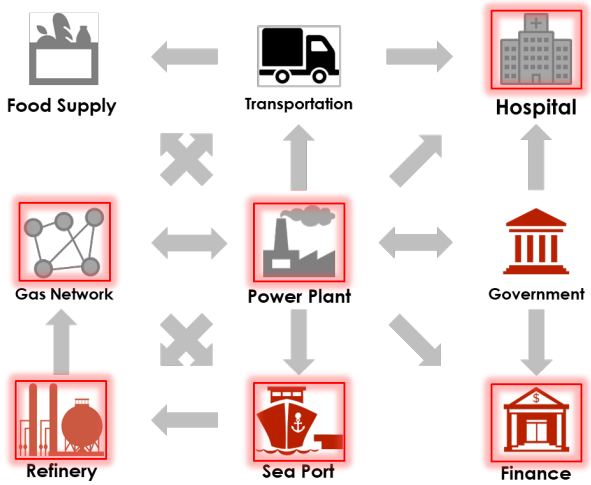

Figure 7. A High-Level Model of the Energy Sector with its Interdependencies with Other CIs

As shown in Figure 7, CIs should not be considered in isolation, as they provide multiple essential resources and services to other infrastructures.

Modelling cascading effects is essential for precise estimation. Binary systems can be used to model these effects, but they are ineffective in real scenarios. Furthermore, automata or state machines are considered better approaches. These allow the description of multiple state transitions and probabilistic values for uncertainties and complexities that match real-life operations.While several tools offer valuable features for simulating the propagation of attacks, many are tailored to specific domains that could not effectively provide assessments of the cascading effects in CIs and their subsequent systems. They may also lack high-level visualizations of cascading effects across interconnected systems, an essential feature for understanding the initially affected targets and their dependent or related systems impacted by particular attacks.

In CyberSecPro, we integrated the cascading effects simulation tool CASSANDRA, which is developed by AIT and provides a comprehensive estimation of the total impact by analyzing state changes across all connected CIs until the final state is determined. The tool also allows for multiple scenario simulations, where physical incidents can affect the cyber domain and vice versa. CASSANDRA records all state changes and the final states of each simulation run. The simulation outputs an overview of the system's evolution, including:

- Which asset has been "affected" in which step
- What is the new state of the asset
- Which asset caused the state change

Figure 8 shows how cascading affects the CASSANDRA simulation approach, which illustrates the nodes where cyber components are represented as dots and physical components as squares (König and Shaaban, 2022). Additionally, various visualizations and reports can be generated, such as:

- Average final state of an asset
- Average case scenario

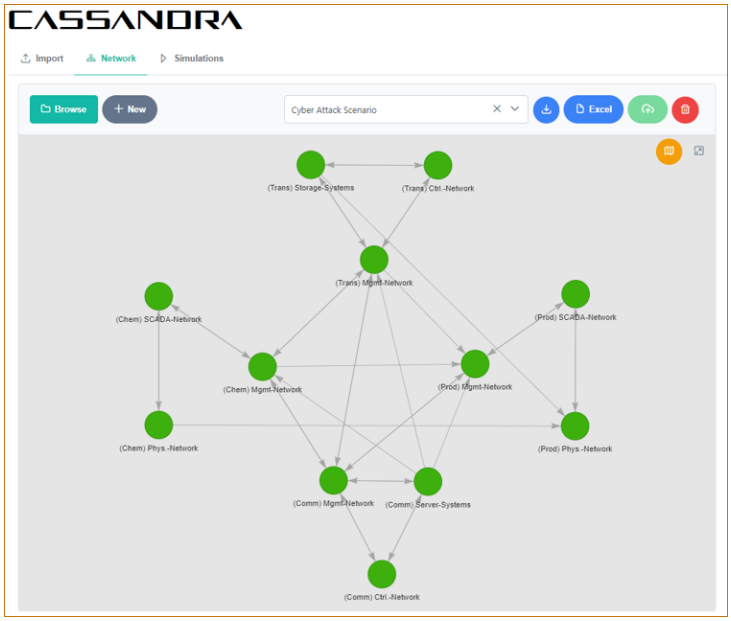

Figure 8. Example of Modeling Cascading Effects in CI Using the CASSANDRA Simulation Approach

- Worst case scenario

Figure 9 illustrates the change in each node's state according to the cascading effects during the CASSANDRA simulation, showing how this is visualized through different colors such as yellow, orange, and red.

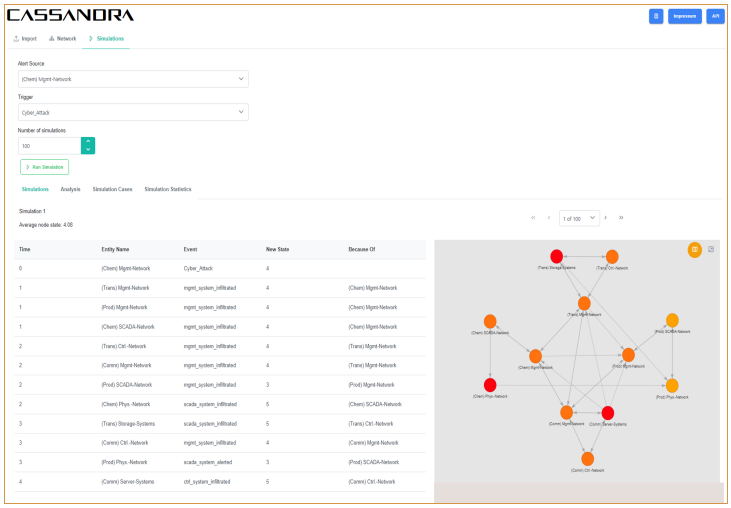

Figure 9. Visualization of Node State Transitions

Introducing CASSANDRA within the cascading effects topics in CyberSecPro modules opens up opportunities for trainees to gain a comprehensive understanding of this advanced approach for simulating the cascading effects of attacks. The tool has already been adopted in multiple EU-funded projects and has paved the way for enhancing cybersecurity training programs, enabling a better understanding of cascading effects through real case studies. That also enhances the knowledge needed to recognize the importance of implementing suitable security measures to mitigate risks that could impact a particular IC and other interconnected ones.

DISCUSSION

It is essential to ensure operators working with CIs stay informed about the latest cybersecurity issues. That will help them understand new attack methods and vulnerabilities that could threaten these critical systems. Additionally, it is crucial to provide them with up-to-date and effective cybersecurity solutions capable of mitigating current and

future threats. This can be achieved by involving people in advanced cybersecurity training programmes, combining theoretical insights and practical activities. Integrating theory and practice is necessary, as they will provide deeper insights into a better understanding of how real security solutions can be effectively implemented in real scenarios. That will also ensure enhancing the protection of the CIs and their interdependencies.

CONCLUSION

This paper gives an overview of the efforts undertaken as part of the EU project CyberSecPro, which offers advanced training materials to boost cybersecurity awareness in the healthcare, energy, and maritime sectors. It highlights the role of selected modules, i.e., CSP004_C_E, CSP006_S_E, and CSP008_S_E, as case studies in this paper, providing theoretical insights into vulnerabilities in real-world cyberattacks and effective mitigation strategies for addressing these risks. The paper also shows how the practical activities developed within the project provide a better understanding of cybersecurity measures, particularly in the energy sector. This effort aims to bridge theoretical insights and practical activities in traditional cybersecurity training programs, enhancing cybersecurity awareness in CIs.

RESEARCH OUTLOOK

ThreatGet and CASSANDRA effectively provide robust cybersecurity approaches and support cybersecurity efforts. As these two tools are conducted separately, it is planned to integrate them; where ThreatGet detects a cyber threat, CASSANDRA analyzes the propagation of the attack within the system and its surrounding environment. Integrating this advanced approach into future training materials and courses will help enhance cybersecurity awareness and provide a more effective method for detecting and mitigating cyber risks in CIs.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided by the ”CyberSecPro: Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries” project, which has received funding from the European Union’s Digital Europe Programme (DEP) under grant agreement No. 101083594. Special thanks to the project partners and their collaboration in preparing advanced training materials. The views expressed in this paper represent only the views of the authors and not of the European Commission. Finally, the authors declare that no conflicts of interest, including any financial or personal relationships, could be perceived as potential conflicts.

REFERENCES

3CORESec. (2025). Testmynids.org: A website and framework for testing nids detection. https://github.com/3CORESec/testmynids.org

AIT Austrian Institute of Technology. (2024). ThreatGet - Threat Analysis and Risk Management. https://www.threatget.com/

Alcaraz, C., Cumplido, J., & Triviño, A. (2023). Ocpp in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*, *22*(5), 1395–1421. https://doi.org/10.1007/s10207-023-00698-8

Alcaraz, C., & Lopez, J. (2010). A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *40*(4), 419–428.

CISA. (2025). Critical infrastructure systems. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems

Cloudflare. (2025). What is ssl (secure sockets layer)? https://www.cloudflare.com/learning/ssl/what-is-ssl/

CyberSecPro Consortium. (2023). Cybersecpro eu project. https://www.cybersecpro-project.eu/

CyberSecPro Project Consortium. (2023). *D2.1 cybersecurity practical skills gaps in europe: Market demand and analyse* (tech. rep.). CyberSecPro Consortium. https://www.cybersecpro-project.eu/wp-content/uploads/2023/10/D2.1-Cybersecurity-Practical-Skills-Gaps-in-Europe-v.1.0.pdf

CyberSecPro Project Consortium. (2024a). *D3.1 cybersecpro programme main components and procedures* (tech. rep.). CyberSecPro Consortium. https://www.cybersecpro-project.eu/wp-content/uploads/2024/05/D3.1-v1.3-Re-submitted.pdf

CyberSecPro Project Consortium. (2024b). *D3.3 cybersecurity curriculum for the health sector* (tech. rep.). CyberSecPro Project. https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.3-CyberSecPro_Health_v1.0_FINAL_submitted.pdf

CyberSecPro Project Consortium. (2024c). *D3.4 training activities and learning paths for cybersecurity in critical infrastructures* (tech. rep.). CyberSecPro Project. https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.4-V1.1-Re-submitted-.pdf

CyberSecPro Project Consortium. (2024d). *D3.5 evaluation report on the training activities and feedback collection* (tech. rep.). CyberSecPro Project. https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.5.-Submitted-2024-06-04.pdf

DevX. (2023). Address resolution protocol spoofing. https://www.devx.com/terms/address-resolution-protocol-spoofing/

Dorot, U. (2023). Ev charging station applications – a growing cyber security risk. https://www.radware.com/blog/application-protection/ev_charging_station_cyber_threats/

European Union Agency for Cybersecurity (ENISA). (2021). *ENISA Threat Landscape 2021* (tech. rep.). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Fursov, I., Yamkovyi, K., & Shmatko, O. (2022). Smart grid and wind generators: An overview of cyber threats and vulnerabilities of power supply networks. *Radioelectronic and Computer Systems*. https://api.semanticscholar.org/CorpusID:255920671

Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp). *IEEE Communications Surveys & Tutorials*, *24*(3), 1504–1533. https://doi.org/10.1109/COMST.2022.3184448

GNS3 Development Team. (2024). *Gns3 documentation*. https://docs.gns3.com/

IEA. (2024). Electric vehicles. https://www.iea.org/energy-system/transport/electric-vehicles

IEC. (2013). *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*. International Electrotechnical Commission. https://webstore.iec.ch/publication/7033

IEC. (2023). *IEC 62351: Power systems management and associated information exchange – Data and communications security*. International Electrotechnical Commission. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/

IEC. (2024). *Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners*. International Electrotechnical Commission. https://webstore.iec.ch/en/publication/62883

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization. https://www.iso.org/standard/27001

Katar, P. (2025). 3 main types of protocols — networking — computers. https://www.engineeringenotes.com/networking/3-main-types-of-protocols-networking-computers/14862

Klimburg, A., Joshi, A., & Beato, F. (2022). Why defining and securing systemically important critical infrastructure is so vital. *World Economic Forum*. https://www.weforum.org/stories/2022/05/securing-systemically-important-critical-infrastructure/

König, S., & Shaaban, A. M. (2022). Parametrization of probabilistic risk models. *Proceedings of the 17th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3538969.3544454

König, S., Shaaban, A. M., Hadjina, T., Gregorc, K., & Kutej, A. (2023). Identification and evaluation of cyber-physical threats on interdependent critical infrastructures. *Proceedings of the 18th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3600160.3605026

Lefebvre, L. (2024). Pymodbustcp: A simple modbus/tcp library for python. https://pypi.org/project/pyModbusTCP/

Lenaerts-Bergmans, B. (2022). Address resolution protocol (arp) spoofing: What it is and how to prevent an arp attack. https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/arp-spoofing/

Microsoft. (2025). Transport Layer Security (TLS) support in IoT Hub. https://learn.microsoft.com/en-us/azure/iot-hub/iot-hub-tls-support

MITRE. (2025). Mitre att&ck framework. https://attack.mitre.org/

Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security*, *112*, 102511. https://doi.org/https://doi.org/10.1016/j.cose.2021.102511

NIST. (2010). *Guidelines for Smart Grid Cyber Security* (tech. rep. No. NISTIR 7628). National Institute of Standards and Technology. https://www.nist.gov/system/files/documents/smartgrid/nistir-7628_total-2.pdf

NIST. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (Special Publication No. 800-53 Revision 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

NIST. (2014). *Guidelines for Smart Grid Cybersecurity* (NIST Interagency/Internal Report (NISTIR) No. 7628 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7628r1

NIST. (2015). *Guide to Industrial Control Systems (ICS) Security* (Special Publication No. 800-82 Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

NIST. (2017). *Cybersecurity Framework Manufacturing Profile* (tech. rep. No. NISTIR 8183). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8183

NIST. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0. https://doi.org/10.6028/NIST.SP.1108r4

NIST. (2024). *The nist cybersecurity framework (csf) 2.0* (Cybersecurity White Paper No. CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

OISF. (2025). *Suricata: Observe. protect. adapt*. https://docs.nethserver.org/en/v7/suricata.html

SecuritySenses. (2023). Bridging theory and practice through cybersecurity education. https://securitysenses.com/posts/bridging-theory-and-practice-through-cybersecurity-education

Shaaban, A. (2021). *An ontology-based cybersecurity framework for the automotive domain - design, implementation, and evaluation* [Doctoral dissertation, University of Vienna].

Shaaban, A., Christl, K., & Schmittner, C. (2024). Rule-based approach using threatget for automatically generating attack paths in industrial automation and control systems. In P. Doucek, M. Sonntag, & L. Nedomova (Eds.), *Idimt-2024 changes to ict, management, and business processes through ai* (pp. 195–202, Vol. 53). https://doi.org/10.35011/IDIMT-2024-195

Shaaban, A. M., Jung, O., & Fas Millan, M. A. (2022). Toward applying the iec 62443 in the uas for secure civil applications. In P. Haber, T. J. Lampoltshammer, H. Leopold, & M. Mayr (Eds.), *Data science – analytics and applications* (pp. 45–52). Springer Fachmedien Wiesbaden.

Shaaban, A. M., Jung, O., & Schmittner, C. (2023). The need for threat modelling in unmanned aerial systems. In J. Guiochet, S. Tonetta, E. Schoitsch, M. Roy, & F. Bitsch (Eds.), *Computer safety, reliability, and security. safecomp 2023 workshops* (pp. 73–84). Springer Nature Switzerland.

Sprinto. (2025). Protecting what matters: Cybersecurity for critical infrastructure. https://sprinto.com/blog/cybersecurity-for-critical-infrastructure/

Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th). Prentice Hall.

Taylor, L. P. (2023). *Raising cybersecurity awareness and improving organizational resilience in the critical infrastructure sector* [Master's thesis, Laurea University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/817634/Taylor_Leila_Pina.pdf?sequence=2&isAllowed=y

Wazuh. (2025). Wazuh platform overview. https://wazuh.com/platform/overview/