Project No. 101083594 Project start: 2022-12-01
Call: DIGITAL-2021-SKILLS-01 Project duration: 36 months

CyberSecPro

D3.4
CyberSecPro Bundle of Cybersecurity Curricula for Energy Sector

Document Identification	
Due date	2024-05-31
Submission date	2024 -05-30
Re-submission date	2024 -06-24
Version	1.1

Related WP	WP3	Dissemination Level	PU
Lead Participant	UMA	Lead Author	Cristina Alcaraz, Javier Lopez (UMA)
Contributing Participants	UMA, TUBS, TUC, UCY, AIT, CNR, UNI, C2B, ITML, SEA, SGI, FCT, LAU, PDMFC, TALTECH, UPRC, APIRO, SLC, Trustilio	Related Deliverables	D2.1, D2.2, D2.3, D3.1, and D4.1

Abstract: The CyberSecPro (CSP) Deliverable D3.4 corresponds to the outcomes of T3.5 regarding the "*Energy Specific Curricula*" with deadline for Month 18. The proposal of this deliverable is to provide a comprehensive cybersecurity programme portfolio targeted to the energy sector and focused on intensifying knowledge and practical skills in line with the current security challenges facing the sector. Likewise, this deliverable also exposes the methodological process carried out in T3.5. It deals with aligning the syllabi of the 12 CPS generic training modules defined in D3.1 to the particularities of the energy scenarios, adapting and parametrising relevant inputs contemplated in the D3.1 templates to specific use cases and applications. The resulting parametrisation is widely outlined throughout this document, where the Cyber Security Body of Knowledge (CyBoK) framework has continued to be a reference for the process of integration and adaptation of topics, facilitating the completeness of content. Additionally, this process is also attributed to the intensive collaboration of the CSP partners who have demonstrated expertise and competencies in the fields of cybersecurity, energy and education. All of this experience, combined with a methodology for aligning with previous works, have certainly helped to establish the 12 CPS sector-specific training modules in the form of courses, seminars, practical exercises, workshops, summer schools, etc. with the final proposal to showcase its value proposition for the operational phase.

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 the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594.

Executive Summary

The energy-specific CyberSecPro (CSP) bundle/portfolio includes a set of cybersecurity curricula meticulously designed to provide knowledge and skills to professionals of the sector. The result is a compendium of 12 CPS sector-specific training modules adapted according to the insights gained from the market analysis, the training offers provided by the CSP partners, and the mapping established with the 12 CPS generic training modules identified in D4.1. This alignment between generic and sector-specific modules is subject to a process of adaptation and parameterisation under a collaborative, iterative methodology, which connects the work made in D3.1 and its templates to the particular features of the sector. As a result, several specific syllabi have been tailored specifically for the energy sector, addressing various topics of interest and in terms of security, privacy, resilience, etc., including various scenarios for application that may be subject to different threats and risks. This can range from traditional energy systems based on electrical substations and control networks to the conceptualisation of defensive measures for new smart grid systems comprising microgrid-based systems, distributed energy resources, renewable energy systems, charging infrastructures, electric vehicles, smart metering, etc. The holistic articulation of these scenarios together with cybersecurity topics is what provides relevance and significance to this contribution, as it allows the community and experts to deepen their knowledge of current interest and need for the protection of these and other dependent systems. Through the CSP portfolio, stakeholders can learn to make decisions on their own and implement proactive solutions to increase resilience of power systems against cyber threats.

Document information

Contributors

Name	Beneficiary
Cristina Alcaraz, Javier Lopez, Antonio Muñoz-Gallego, Ruben Rios del Pozo, Davide Ferraris, Manuel Nicolas Enciso Garcia-Oliveros, Carmen Fernandez-Gago	UMA
Antonios Ntib	TUBS
Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis	TUC
Paulo Figueiras, Ruben Costa, Vasco Delgado-Gomes	UNINOVA
José Manuel Fonseca, Ricardo Gonçalves	FCT
Dimitra Siaili	ITML
Paresh Rathod	LAU
Ricardo Gregorio Lugo	Taltech
Kitty Kioskli	Trustilio
Martin Bärman, Louise Præstin	SGI
Nuno Pedrosa, Stylianos Karagiannis, Luis Miguel Campos	PDMFC
Chatzopoulou Argyro	APIRO
Artsiom Yautsiukhin, Fabio Martinelli	CNR
Abdelkader Shaaban, Stefan Schauer	AIT
Elias Athanasopoulos	UCY
Nineta Polemi, Dimitris Koutras	UPRC
Bruno Bender	C2B
Shareeful Islam, Athina Labropoulou	SLC
Sebastian Pape	SEA

Reviewers

Name	Beneficiary
Christos Grigoriadis, Paris Laras	Focal Point
Nektaria Kaloudi	SINTEF

History

Version	Date	Contributor(s)	Comment(s)
0.1	2023-09-02	Cristina Alcaraz and Javier Lopez	1st Draft of ToC
0.2	2023-09-06	Nineta Polemi	Review of ToC, and feedback
0.3	2023-09-08	Cristina Alcaraz, Javier Lopez, and Nineta Polemi	Technical inputs and consolidated ToC with WP leaders

0.4	2023-12-11	Dimitris Koutras and Cristina Alcaraz	Review of the ToC, including the training providers
0.5	2024-02-02	Cristina Alcaraz	Updating of the ToC with changes about allocation of modules
0.6	2024-02-08	Antonios Ntib	Modules 1, 4, and 5 added
0.6	2024-02-12	Cristina Alcaraz, Javier Lopez, and Fabio Martinelli	Review of the contents and new contributions about the syllabi. Modules 3.
0.6	2024-02-12	Cristina Alcaraz, Javier Lopez, Stefan Schauer, and Abdelkader Shaaban	Module 4 updated
0.6	2024-02-12	Cristina Alcaraz, Javier Lopez, Stefan Schauer, Abdelkader Shaaban, Elias Athanasopoulous	Module 8 updated
0.6	2024-02-12	Cristina Alcaraz, Javier Lopez, Antonio Muñoz, Davide Ferraris, Ruben Rios, Paresh Rathod, Ricardo Gregorio Lugo, Kitty Kioskli, Martin Bärman, Nuno Pedrosa, and Stylianos Karagiannis	Module 1 updated
0.6	2024-02-14	Sebastian Pape	Module 1 updated
0.6	2024-02-15	Vasco Delgado-Gomes	Modules 7 and 12 updated
0.6	2024-02-16	Dimitra Siaili	Module 11 updated
		Bruno Bender and Fabio Martinelli	Module 11 updated
0.7	2024-03-01	Cristina Alcaraz and Javier Lopez	Review of the deliverable and edition and update of some sections
0.8	2024-03-08	Fabio Martinelli	Module 5 updated
0.9	2024-03-11	Cristina Alcaraz and Paresh Rathod	Module 1 review, and add new content
0.10	2024-03-15	Cristina Alcaraz and Javier Lopez	First edition and review
0.11	2024-05-07	Cristina Alcaraz and Javier Lopez	Integration, review of the entire document and corrections
0.12	2024-05-08	Cristina Alcaraz, Javier Lopez, Carmen Fernandez-Gago	Corrections corresponding to the first review round, and integrations
0.13	2024-05-19	Cristina Alcaraz, Javier Lopez, Manuel Nicolas Enciso Garcia-Oliveros	Corrections corresponding to the second review round, and integrations
0.14	2024-05-26	Cristina Alcaraz	Last corrections and final review
1.0	2024-05-30	Frederic Tronnier, Atiyeh Sadeghi	Final check, layout refinement and submission process
1.1	2024-06-12	Atiyeh Sadeghi	Final check, layout refinement for re-submission process

Table of Contents

Document information ..... **v**
1 Introduction **1**
1.1 Background **2**
1.2 Purpose and Scope **3**
1.3 Relation to Other Work Packages and Deliverables **3**
1.4 Structure of the Deliverable **4**
2 Mapping From Generic to Specific Training Modules **5**
2.1 Value Proposition for Energy **5**
2.2 Development Methodology for CSP Energy Modules **6**
2.3 Training Material and Video Teaser for CSP Training Modules for Energy **6**
3 CyberSecPro Customised Modules Syllabus for Energy **9**
3.1 Module 1 - Cybersecurity Essentials and Management for Energy **9**
3.1.1 CSP001_C_E: Cybersecurity Essentials and Management for Energy Sector 9
3.1.2 CSP001_S_E: Cybersecurity Essentials and Management for Energy Sector 18
3.1.3 CSP001_CS-E_E: RxB - Cyber Security Management Game 24
3.2 Module 2 - Human Factors and Cybersecurity for Energy **29**
3.2.1 CSP002_S_E: Human Factors and Energy Cybersecurity 29
3.2.2 CSP002_SS_E: Human Factors and Cybersecurity 35
3.2.3 CSP002_CS-E_E: HATCH 42
3.2.4 CSP002_CS-E_E: PROTECT 47
3.3 Module 3 - Cybersecurity Risk Management and Governance for Energy **51**
3.3.1 CSP003_S_E: Cybersecurity Risk Management and Governance in the Energy sector 51
3.3.2 CSP003_S_E: Cybersecurity Risk Assessment and Management for Energy Sector 56
3.4 Module 4 - Network Security for Energy **62**
3.4.1 CSP004_C_E: Network Security for Energy 62
3.4.2 CSP004_C_E: Network Protection for Energy Control Systems 67
3.5 Module 5 - Data Protection and Privacy Technologies for Energy **73**
3.5.1 CSP005_C_E: Data Protection and Privacy Technologies for energy 73
3.5.2 CSP005_S_E: Data Protection and Privacy Technologies for Energy 78
3.6 Module 6 - Cyber Threat Intelligence for Energy **82**
3.6.1 CSP006_C_E: Cyber Threat Intelligence in the Energy Network 82
3.6.2 CSP006_S_E: Cyber Threat Intelligence and Threat Hunting in the Energy Domain 89
3.7 Module 7 - Cybersecurity in Emerging Technologies for Energy **96**
3.7.1 CSP007_C_E: Cybersecurity in Emerging Technologies for Energy 96
3.7.2 CSP007_S_E: Cybersecurity in Emerging Technologies for the Energy Network 103
3.8 Module 8 - Critical Infrastructure Security for Energy **110**
3.8.1 CSP008_C_E: Critical Energy Infrastructure Security 110
3.8.2 CSP008_S_E: Protecting Charging Stations Against Specific Threats 116
3.9 Module 9 - Software Security for Energy **124**
3.9.1 CSP009_S_E: Mechanics for Memory Corruption 124
3.10 Module 10 - Penetration Testing for Energy **129**

3.10.1 CSP010_S_E: Cybersecurity in Energy 129

3.11 Module 11 - Cyber Ranges and Operations for Energy 134

3.11.1 CSP011_S_E: Cyber range and operations on SCADA 134

3.11.2 CSP011_S_E: Alerting, Reporting, and Monitoring Strategies for Cybersecurity in the Energy Sector 141

3.12 Module 12 - Digital Forensics for Energy 148

3.12.1.1 CSP012_S_E: Digital Forensics for Energy 148

4 Conclusions 157

5 References 157

List of Acronyms

A	**A**	Advanced
	AI	Artificial Intelligence
	AIT	AIT Austrian Institute of Technology GmbH
	APIRO	ApiroPlus Solutions Ltd
	APT	Advanced Persistent Threat
B	**B**	Basic
C	**C**	Course
	C2B	C2B Consulting
	CI	Critical Infrastructure
	CIA	Confidentiality, Integrity and Availability
	CIS	Critical Security Controls
	CISO	Chief Information Security Officer
	CNR	Consiglio Nazionale Delle Ricerche (National Research Council)
	CoA	Certificate of Attendance
	CPS	Cyber-Physical System
	CS-E	CyberSecurity Exercise
	CSO	Chief Security Officer
	CSV	Comma-Separated Value
	CTI	Cyber Threat Intelligence
	CVE	Common Vulnerabilities and Exposures
	CyBoK	Cyber Security Body of Knowledge
D	**DCM**	Dynamic Curriculum Management
	DCMS	Dynamic Curriculum Management System
	DCS	Distributed Control System
	DER	Distributed Energy Resource
	DMZ	Demilitarised Zone
	DNS	Domain Name System
E	**EC**	European Commission
	ECSF	European Cybersecurity Skills Framework
	ECSO	European Cyber Security Organisation
	ECTS	European Credit Transfer and Accumulation System
	ENISA	European Union Agency for Cybersecurity
	ETSI	European Telecommunications Standards Institute
	EU	European Union
	EV	Electrical Vehicle
F	**FCT**	Universidade NOVA de Lisboa (NOVA University of Lisbon)
	FERC	Federal Energy Regulatory Commission
	FTP	File Transfer Protocol
G	**GDPR**	General Data Protection Regulation
	GNSS	Global Navigation Satellite System
H	**H**	Hackathon
	HEI	Higher Education Institution

	HMI	Human-Machine Interfaces
	HSM	Hardware Security Modules
	HTTP	Hypertext Transfer Protocol
	HTTPS	Hypertext Transfer Protocol Secure
I	**IACS**	Industrial Automation & Control System
	ICS	Industrial Control System
	ICT	Information and Communication Technology
	IDS	Intrusion Detection System
	IEC	International Electrotechnical Commission
	IEEE	Institute of Electrical and Electronics Engineers
	IND-CPA	INDistinguishability under Chosen Plaintext Attack
	IoE	Internet of Energy
	IoT	Internet of Things
	IPS	Intrusion Prevention System
	ISO	International Organisation for Standardisation
	IT	Information Technology
	ITML	Information Technology for Market Leadership
K	**KA**	Knowledge Area
L	**LAN**	Local Area Network
	LAU	Laurea-Ammattikorkeakoulu Oy (Laurea University of Applied Sciences)
M	**MAN**	Metropolitan Area Network
	MFA	Multi-Factor Authentication
	MOOC	Massive Open Online Courses
	MQTT	Message Queuing Telemetry Transport
N	**N/A**	Not Applicable
	NAT	Network Address Translation
	NIS	Security of Network and Information System
	NIST	National Institute of Standards and Technology
O	**O**	Other
	OCPP	Open Charge Point Protocol
	OS	Operating System
	OSI	Open System Interconnection
	OSINT	Open-Source Intelligence
	OT	Operational Technology
P	**PC**	Project Coordinator
	PDMFC	Pdm e fc Projecto Desenvolvimento Manutencao Formacao e Consultadorialda
	PET	Privacy Enhancing Technique
	PKI	Public Key Infrastructure
	PLC	Programmable Logic Controller
	PPT	Power Point Presentation
	PoC	Proof of Concept
Q	**OR**	Quick-Response
R	**RAID**	Redundant Array of Inexpensive Disk

	RBAC	Role-Based Access Control
	RFC	Request for Comments
	RTU	Remote Terminal Unit
S	**S**	Seminar
	SCADA	Supervisory Control And Data Acquisition
	SDPbd	Security Data and Privacy by design
	SEA	Social Engineering Academy
	SIS	Safety-Instrumented System
	SGI	Serious Games Interactive ApS
	SLC	Security Labs Consulting Limited
	SOC	Security Operations Center
	SS	Summer School
	SSH	Secure Shell
	SSL	Secure Sockets Layer
T	**TalTech**	Tallinna Tehnikaülikool (Tallinn University of Technology)
	TBD	To Be Determined
	TCP	Transmission Control Protocol
	TCP/IP	Transmission Control Protocol / Internet Protocol
	TCSEC	Trusted Computer System Evaluation Criteria
	TLS	Transport Layer Security
	ToC	Table of Contents
	TRUSTILIO	
	TTP	Tactic, Technique and Procedure
	TUBS	Technische Universitaet Braunschweig (Technical University of Braunschweig)
	TUC	Polytechneio Kritis (Technical University of Crete)
U	**UCY**	University of Cyprus
	UDP	User Datagram Protocol
	UMA	Universidad de Malaga (University of Malaga)
	UNINOVA	Uninova-Instituto de Desenvolvimento de Novas Tecnologiasassociacao (UNINOVA - Institute for the Development of New Technologies)
	UPRC	University of Piraeus Research Center
V	**VLAN**	Virtual LAN
	VM	Virtual Machine
	VPN	Virtual Private Network
	VR	Virtual Reality
W	**W**	Workshop
	WP	Work Package

Glossary of Terms

C **CSP competence**

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across European Union (EU) nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, "*The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it."*

CSP Dynamic Curriculum Management System (DCMS)

Includes all the procedures and processes that CyberSecPro will use to manage the curriculum portfolio. The open-source learning platforms Moodle and/or e-class will be used (since the academic partners already use it in the academic programmes) for the CyberSecPro Dynamic Curriculum Management (DCM) integration. It will entail the entire curriculum creation, evaluation, review, approval, promotion processes, and regulation compliance (e.g. General Data Protection Regulation (GDPR)).
The main requirements of the CyberSecPro online DCM will be flexibility and responsiveness to the continuously changing needs of the cybersecurity market. The online DCM tool will be integrated by parametrising the Moodle or e-class open-source learning platform where the cybersecurity market needs will be monitored, and curricula will be managed.

CSP Knowledge Areas (KAs)

The Knowledge Areas (KAs) derived from D2.3 listed were based on the CyBoK Skills Framework, JRC recommendation and mainly from the European Cybersecurity Organisation report based on industry-academia cooperation and development work. However, the project will be further aligned with the European Cybersecurity Skills Framework (ECSF) and the market analyses' outcomes.

CSP practical skill

The initial studies confirmed the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, "*The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results*".

CSP sector-specific training modules

CSP training modules will concentrate on the health, maritime, and energy sectors. The modules will be shaped around real-life challenges in collaboration with the Higher Education Institutions (HEIs), companies and industries, adapting their content and approach to the specific knowledge areas and parametrising the training tools and practical exercises accordingly.

CSP syllabus

All training modules are accompanied by a syllabus that include information like learning outcomes, who should attend, relative conventions and standards, prerequisite competencies (skills & knowledge), training module outline, list tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training, training tools that will be used, assessment methods, exams, study time (physical and online learning) and so on.
A standard template for a CSP syllabus is available in this deliverable and it will be used in all CSP training modules.

CSP Trainees

CSP Trainees refer to prospective Information Technology (IT) professionals or individuals who enrol in CyberSecPro training programme.

CSP Trainers

CSP Trainers refer to CyberSecPro partners who provide training in each cybersecurity domain.

CSP training format

CSP training format describes the way how modules will be provided, i.e., "OnDemand," "Web-based," "Live Online," "Live in Person," "Hybrid/mix" etc.

CSP training material

Corresponds to all material that will be used by the educator/trainer to provide the CSP training module.

CSP training modules

Comprises courses, mini-courses, lectures, cyber hands-on exercises, cyber hackathons, cyber mornings & events, cybersecurity games, red/blue team exercises, summer schools, workshops, ad-hoc sector-specific seminars, on-demand mini-technological courses, and crisis management training.

CSP training programme

The programme consists of training modules that can be offered individually or as a package of modules; it will not lead to any certification, degree, or career paths; it will be used to enhance existing training offers to close the gaps between academic training supply and marketing professional demands.

CSP training tools

Training tools that will be used in the training of the CSP modules (the assessment of the various tools, selection and portfolio occurs in T2.3).

1 Introduction

The Energy sector is one of the Critical Infrastructures (CIs) that is on continuous demand by our society, but it is also one of the most susceptible ones to potential threats. Current needs revolve around modernising the control infrastructures and including new industrial paradigms (Industry 4.0/5.0 [1]) in the operational processes, and to guarantee the digital transformation and the dynamic automatisation of processes lead to increased risk for unforeseen impacts. The attack surface continuously expands, intensifying the number of physical and cyber threats, which may provoke major interruptions in the provision of essential services to other essential infrastructures such as health and maritime.

This also means that security risks in the energy sector are not only subject to physical or casual threats, but they also extend to the cyber world, consequently affecting the correct performance of well-known Cyber-Physical Systems (CPSs) that normally integrate the traditional Supervisory Control and Data Acquisition (SCADA) systems. Proof of this weakness is found in [2,3], where international organisations such as the European Union Agency for Cybersecurity (ENISA), the European Cyber Security Organisation (ECSO) or the MITRE Corporation are frequently reporting potential risks and threats. Particularly, ENISA annually details the threat landscape [4], not only in general terms but also specific ones to each sector [5], where attacks tend to be well-planned and attackers prove to be well-equipped to carry out their exploits. Clear examples of real-world incidents can be found in the literature, such as Stuxnet, Triton, BlackEnergy, Petya or notPetya, among many others, and all of them illustrate the current threat landscape.

Under this situation knowledge and skills to prevent and mitigate such effects are nowadays a primary requirement. Any expert in the field of energy must understand the existing security risks and potential threats, and must identify the appropriate measures to guarantee business continuity under established resilience and trust principles. This feature is part of the main objectives of the CyberSecPro (CSP) project. From the Work Package (WP) 2, a comprehensive research and market analysis has been addressed to identify and show the shortcomings in the current cybersecurity training offers for experts in the energy domain. This shortcoming underlines the need for a specialised education and training programme that addresses the challenges specific to the energy sector and its corresponding networks, paradigms, and infrastructures such as SCADA systems, Smart Grids, microgrid-based systems, Distributed Energy Resources (DERs), Electrical Vehicle (EV) charging infrastructures, etc.

Considering this need, the CSP project has raised a number of coordinated actions from WP2 and are reflected throughout the deliverables D2.1, D2.2, D2.3, D3.1 and D4.1. All of them were used as input to this work providing the foundations for a methodological approach for cybersecurity training within the energy sector, which are consolidated in the deliverable D3.4. This deliverable compiles the 12 CSP core training modules associated to Cybersecurity Essentials and Management, Human Factors and Cybersecurity, Cybersecurity Risk Management and Governance, Network Security, Data Protection and Privacy Technologies, Cyber Threat Intelligence, Cybersecurity in Emerging Technologies, Critical Infrastructure Security, Software Security, Penetration Testing, Cyber Ranges and Operations, and Digital Forensics. All of them are equivalent to those modules defined in D3.3 and D3.5, but each one leading different actions, and under the criteria of specialisation according to each sector of application.

As commented, and particularly for the energy domain, these 12 core modules are mainly designed to prepare experts of the field, or even those interested in the sector, and provide them with the necessary skills and knowledge to deal with cybersecurity risks. Thus, this deliverable aims to delineate the structure, requirements, and specifications of these training modules, providing ***a comprehensive framework for the CyberSecPro education and training programme*** adapted to the energy sector

1.1 Background

As mentioned, CyberSecPro provides a clear picture of the current needs in cybersecurity training, with specialisation in particular domains like the energy sector. This study was widely developed in CSP D2.1 through a comprehensive market analysis, where the field of energy was one of the target sectors during the study, culminating in D2.3 with 10 essential CSP Knowledge Areas (KAs) identified on the basis of actual demand (D2.1) and according to training offerings supplied by the CPS consortium members. Evidently, these two deliverables were subsequently keys to establish the set of CSP Training Modules, all of them classified and specified in D4.1 as part of the catalogue of CyberSecPro training operational plan.

On the basis of these 12 CSP training modules and the 10 KAs, this deliverable compiles the training programme, which includes among other things the specification of syllabi and the way to prepare the learning process. The aim is to promote knowledge and skills within the field of cybersecurity but specifically oriented to professionals within the energy sector who must know about current security risks and the corresponding measures to prevent or mitigate their effects. This also means that experts must comprehend the complexity of new energy application contexts, where multiple Information Technologies (ITs) converge toward operational networks to modernise their operations and allow a better automatisation of processes from anywhere, at any time and in any way.

To homogenise the contents and the approach and establish the learning process among diffenet modules, this deliverable also considers all those templates established in D3.1. These templates specify the CyberSecPro 12 generic training modules syllabus, allowing future trainers to maintain coherence and consistence with the current frameworks (e.g. European Cybersecurity Skills Framework (ECSF) [6]) but tailored to the needs of the particular application context. Evidently, this adaptation process also involves respecting the requirements of the operational environment, comprehend the main stakeholders and operational components, comply with the current regulatory frameworks and standards, and, of course, to reflect the main security problems and risks that the new energy ecosystems bring to the society and its economy. This also means that all CSP partners involved in the development of the modules show sufficient expertise in the field of energy and extensive knowledge in the field of cybersecurity.

The modules tailored to the energy sector will have to be part of the of the Dynamic Curriculum Management (DCM) platform where all the learning process will be subject to a dynamic training programme. The DCM platform is a digital content platform documented in D3.1 whose system architecture is designed to allow the full parametrisation of modules, and which provides an interface which is extensively detailed to facilitate the access and the management of the training materials. These materials must be based on the syllabi and conditions established in the current deliverable, which adapts the D3.1 generic templates to specific topics of the sector, in which a set of practical exercises and examples can also be customised.

Therefore, the background of this deliverable is mainly based on all those previous studies carried out throughout the project, comprising:

- The market analysis about the demand and its current needs in the field of the cybersecurity, and particularly looking at the three main CSP sectors like the energy.
- The 10 CPS KAs identified as part of D2.3, which are related to: Cybersecurity Management (KA1), Human Aspects of Cybersecurity (KA2), Cybersecurity Risk Management (KA3), Cybersecurity Policy, Process, and Compliance (KA4), Network and Communication Security (KA5), Privacy and Data Protection (KA6), Cybersecurity Threat Management (KA7), Cybersecurity Tools and Technologies (KA8), Penetration Testing (KA9), and Cyber Incident Response (KA10).
- The aforementioned 12 CPS training modules classified in D4.1.

- The generic templates and syllabi of these 12 CPS training modules, which have been outlined in D3.1 to lay the sector-specific syllabus foundations and training materials.

Beyond this, there are also other factors that also add value to this adaptation process, such as:

- The knowledge provided by the CSP partners, who have demonstrated a great expertise in the field of cybersecurity and skills to adapt the cybersecurity to the energy sector.
- We continue considering the main cybersecurity professional profiles of the ECSF provided by ENISA in [6], which are: Chief Information Security Officer (CISO - ECSF Profile 1), Cyber Incident Responder (ECSF Profile 2), Cyber Legal, Policy & Compliance Officer (ECSF Profile 3), Cyber Threat Intelligence Specialist (ECSF Profile 4), Cybersecurity Architect (ECSF Profile 5), Cybersecurity Auditor (ECSF Profile 6), Cybersecurity Educator (ECSF Profile 7), Cybersecurity Implementer (ECSF Profile 8), Cybersecurity Researcher (ECSF Profile 9), Cybersecurity Risk Manager (ECSF Profile 10), Digital Forensics Investigator (ECSF Profile 11), Penetration Tester (ECSF Profile 12).

All these input points work in unison to enable the orchestration of the objectives this deliverable has set out to fulfil, and were selected to offer a solid and adequate contribution to the CyberSecPro project and the sectors it sets out to assist and improve.

1.2 Purpose and Scope

This section underlines the main objective of this deliverable, which is to ***customise the syllabi of the 12 CPS generic training modules defined in D3.1 to the specific characteristics of the energy sector***. This includes tailoring particular security-specific topics to the cybersecurity needs of each application context, taking into account the environment's components, protocols, operations, regulations and stakeholders. With this adaptation, we additionally provide an extensive portfolio of curricula developed throughout of T3.5 about "*Energy-Specific Curricula*", which contemplates established energy cybersecurity professional competencies considering the specification of topics, exercises and particular examples to the sector; all of them aligned to the needs identified in D2.1.

This also means that the scope of this deliverable focuses primarily on providing the learning inputs that will activate the training programme in its operating phase, and will facilitate the comprehension of current problems and risks in the energy sector, and paves a way to the use of measures to moderate them. As is self-evident, the stakeholders who could be interested in the objectives of this work could be all those related to the energy world and its operations. This includes authorities, policy makers and standardisation bodies, energy providers, human operators / engineers / administrators, engineering students, educators, researchers, and associations, but also to all those interested in receiving cybersecurity knowledge and skills applied to the respective application domains.

1.3 Relation to Other Work Packages and Deliverables

As previously commented, this deliverable is aligned with other related project actions, which have been progressively evolving since the beginning of the CyberSecPro project. Particularly, this deliverable is related to the activities performed in WP2 about "*CyberSecPro Professional Programme Analysis*" and WP4 "*Operating CyberSecPro Professional Training Program*", but also with other tasks deployed in the same WP3 "*CyberSecPro Curricula Portfolio*" where T3.5 (together with its D3.4) belongs to.

Indeed, T3.5 is included WP3 and interacts with other CSP WPs in the following way: it receives information from WP2 about current cybersecurity needs in the relevant sectors and KAs detailed in D2.1 and D2.3, respectively. With this information in hand and the templates developed in D3.1 according to the 12 CSP modules identified in D4.1, T3.5 expands the work by adapting the templates

to the specific security features of the sector. In turn, T3.5 and D3.4 aim to provide the professional training programme together with the syllabi for the energy sector, exercises, and examples necessary to activate the operation in the field.

1.4 Structure of the Deliverable

Taking as a basis the templates established in D3.1, this deliverable details the deployment characteristics of the CSP modules, adapted to the energy sector and its particular features. These modules, represented in different modes, either through courses, seminars, workshops, exercises, summer school, hackathons, etc., are widely described throughout the subsequent sections and subsections. More specifically, Chapter 2 provides a mapping from the generic to the sector-specific modules in order to connect the work performed in D3.1 to D3.4. Chapter 3 outlines the different sector-specific module offerings, detailing the description of the modules, the preparedness plan, the materials and exercises, and the verification process of learning outcomes and skills. Finally, Chapter 4 highlights some final remarks, concluding the deliverable.

2 Mapping From Generic to Specific Training Modules

This chapter focuses on mapping the syllabi established for the generic training modules to the specific ones associated with the energy sector.

2.1 Value Proposition for Energy

As commented in the Introduction section, the energy sector is generally composed as clusters of infrastructures, networks and components susceptible to multiple types of threats that may cause serious problems to the well-being of other CIs and society at large. In fact, the energy sector is one of the more relevant infrastructures within the field of CI, since other multiple CIs depend on this sector to operate properly, or at all. For example, hospitals depend on electricity generators and storage mechanisms to provide minimum services to society, but also ships need electricity to navigate and operate when transporting essential services for society, such as medication, food, etc. Any cascade effect may trigger an immediate effect against the social and economic welfare of most communities.

The value proposition of this type of infrastructure lies in the need to guarantee an acceptable level of security to ensure resilience and business continuity. Historically, the number of threats and cyber-attacks has increased considerably [4,5,7], especially in recent years -- demonstrating the need to promote awareness and knowledge, and to guarantee a minimum of security requirements for the protection of energy systems and their adjacent systems, including control networks. Professionals or future experts in the power field must comprehend the problems currently facing the sector, discover the severity of exploitation of current vulnerabilities and common bad practices, comprehend recent or existing regulations, and learn about existing security mechanisms and their appropriate use.

Thus, the rationale for this type of modularity and to create the groundwork for a value proposition which will empower professionals with specific, long-term cybersecurity skills is illustrated by the following points:

- **Real cyberattacks and vulnerabilities**: the number of cyber-incidents, exploitations of zero-day vulnerabilities, and the execution of advanced and persistent attacks has increased significantly, and attackers do not abstain from attacking the energy sector. Historical examples have clearly shown their capacity to provoke drastic social impact such as attacks on BlackEnergy, Triton, Industroyer, Industroyer 2, and many others. The vast majority of attacks are performed by well-equipped attackers who are able to carry out multiple types of attacks, from social engineering and lateral movements, to compromise through malware, and to performing data exfiltration or destruction of critical assets such as controllers. A list of attacks against European energy companies and utilities can be found in [7], where EnergiCERT showcased the main target types and modus operandi of attackers, as well as the consequences of these attacks.
- **Needs from D2.1**: the study carried out in D2.1 also justifies the need of activating long-term learning mechanisms through the training. It is necessary to situate experts to actual situations and to connect them to complex scenarios in which they can discover tactics to protect the energy sector, its resources, and the impact it has on social welfare. What is more, this type of training should be enabled by a dynamic training programme capable of adapting to recent events and evolving needs. Guaranteeing full resilience for an increased period of time using traditional security measures and without exploring new techniques or threats, it is impossible. It is expected that threats against these types systems vary depending on many factors, such as: the kind of target, the new technologies and their integrations, the type of attacker and interests, skills and forms of attacks, etc.

Both points justify why a tailored training programme is required within the CSP project. It is imperative to equip experts with the necessary knowledge and skills to enable them to make decisions by themselves, learn how to protect a system from risks, and avoid major consequences in the long term.

2.2 Development Methodology for CSP Energy Modules

The development methodology, considered in this deliverable for CSP energy modules, follows the strategy established also for D3.3 and D3.5. This methodology enables the adaptation of each training module defined in D3.1 to a specific one applied to the energy domain. Particularly, the methodology entails three main execution stages for the design of modules:

1. **Identify and extract the generic syllabi from D3.1 and its templates**: this phase comprises the identification of the syllabi according to existing expertise. These syllabi are designed and integrated in D3.1 together with their generic templates which help to align the generic definitions - subject to the Cyber Security Body of Knowledge (CyBoK) Framework [8] - to the specific contents of each sector.
2. **Adapt and construct the syllabus for each sector-specific training module**: each tailored syllabus is developed with reference to the general description and templates given in D3.1, guaranteeing coherence in the training programme, and across all CSP modules. In this process, the CyBoK framework continues serving as a guideline to framing all security knowledge areas, but this time adapted to the features of the energy sector (in terms of functional views, networks, technologies, protocols, threats, risks, vulnerabilities, etc.).
    a. Therefore, the mapping process from generic to sector-specific training modules also involves the parameterisation of **the contents to the application context**. This means that each syllabus must be tailored to the particular features of the application context, incorporating insights from D3.1.
    b. As part of the parameterisation and to complete the adaptation process, it is essential to **extract a dedicated preparedness plan, the verification of learning outcomes, and the types of exercises**. This last step additionally ensures that the training phase is not only based on theoretical knowledge but is also highly relevant to the practical challenges faced by energy professionals.
3. **Provide materials, exercises and examples adapted to the applied context**: once the parametrisation of the module is stable and agreed by the different trainers implied in its development, it is necessary to customise examples, case studies, and exercises to reflect real-world energy scenarios, enriching the applicability and effectiveness of the training.

As noticed, this development methodology is designed to be iterative and collaborative, in a manner that integrates the input of cybersecurity experts, energy professionals, and educators. This approach ensures that the modules are not only pedagogically sound but also technically accurate, and directly aligned with the needs of the energy sector.

2.3 Training Material and Video Teaser for CSP Training Modules for Energy

All the CSP training modules are identified under a unique code based on “CSP00X_Y_E”, where X is the number that identifies the module, Y corresponds to the type of module (e.g. course, seminar, laboratory exercise, summer school, etc.) and E represents the power field. All these modules with their respective codes are documented throughout this deliverable together their corresponding syllabus. To provide usefulness in the operational phase of CyberSecPro, all the training materials produced

according to the tailored syllabus of each module must be available together with their respective video teaser on the DCM platform. The details concerning this platform are described in D3.1.

3 CyberSecPro Customised Modules Syllabus for Energy

This section contemplates all those modules defined in D3.1 but customised for energy sector and its corresponding control domains, detailing the specific contents related to the syllabus, titles of the modules and their corresponding codes, alternative titles, description of the modules, assessment methods, etc. As a result of the developed methodology in Section 2.2, the CyberSecPro project provides a total of 24 training modules for energy sector, covering the 12 CSP generic training modules established in D3.1 and D4.1.

More specifically:

- 24 training modules for energy sector are detailed below.
- From these 24 modules, 7 are courses, 13 seminars, 3 cybersecurity exercises, and 1 summer school.
    - From the 7 courses, 2 courses are at basic level and the rest at advanced level. This corresponds to 57% of the courses at advanced level, and 43% at basic level.
    - From the 13 seminars, 8 seminars are at basic level and the rest at advanced level. This corresponds to 38% of the seminar at advanced level, and 62% at basic level.
    - The 3 cybersecurity exercises are at basic level, and the summer school is focused to be provided at advanced level.
- Therefore, there are 14 modules planned to be executed at basic level, and 10 at advanced level. This means that 58% of the modules in the CyberSecPro portfolio (for the energy sector) are of a basic level, and the remaining 42% are of an advanced nature.

3.1 Module 1 - Cybersecurity Essentials and Management for Energy

3.1.1 CSP001_C_E: Cybersecurity Essentials and Management for Energy Sector

3.1.1.1 Description of Training Module

The module provides a comprehensive overview of cybersecurity's essential concepts and principles for managers and energy sector cybersecurity aspiring professionals. This also means that this training module is mainly designed for individuals involved in the energy sector, such as human operators, engineers, administrators, providers, authorities, and energy organisations, who seek to enhance their understanding of cybersecurity essentials and management principles.

To equip professionals or future experts with the knowledge and skills needed to defend against evolving cyber threats in the critical energy industry, the design of this module goes beyond generic cybersecurity training. It addresses the unique challenges and vulnerabilities faced by energy providers, covering a wide range of topics to gain deep understanding of the cyber landscape targeting energy infrastructures, and includes aspects such as: (i) industry-specific threats and vulnerabilities, including targeted attacks on SCADA systems, smart grids, and other critical energy assets; (ii) generic and energy specific regulatory compliance; (iii) development of strategies to identify, assess, and mitigate cyber risks; and (iv) the implementation of effective technical and organisational measures, including cybersecurity controls, among other issues.

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_C_E**
Module Title *The title of the training module*	**Cybersecurity Essentials and Management for Energy Sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cybersecurity Essentials for Energy. • Cybersecurity Management. • Cybersecurity for the Modern Workplace-Cyber Security Essentials and Principles. • A Comprehensive Overview of Cybersecurity Core Concepts for Energy. • From Essentials to Management: Cybersecurity for Managers and Leaders. • Essential Cybersecurity Skills for Managers and Leaders. • Introduction to Information and Cyber Security for Energy. • Management of Information Security.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	This training module provides a foundational understanding of cybersecurity essentials and management principles, equipping participants with the knowledge and skills to manage information and cybersecurity in the energy sector.
Module description *Indicates the main purpose and description of the module.*	This CSP training module is designed to equip trainees and professionals with the knowledge and skills needed to defend against evolving cyber threats in the critical energy industry. Specifically tailored for the energy sector, this module goes beyond generic cybersecurity training to address the unique challenges and vulnerabilities faced by energy providers. The participants will gain a deep understanding of the cyber

	landscape targeting energy infrastructure, including industry-specific threats and vulnerabilities, as well as targeted attacks on SCADA systems, smart grids, and other critical energy assets. Also, they will gain knowledge about generic and energy specific regulatory compliance, ways to develop strategies that enable them to identify, assess, and mitigate cyber risks, and ways to implement effective technical and organisational measures including cybersecurity controls.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:** • Define cybersecurity and its significance in the energy sector. • Identify and assess energy cybersecurity threats. • Understand the principles of cybersecurity risk management. • Understand the principles of network segmentation, firewall configuration, and access control. • Understand the importance of password security, Multi-Factor Authentication (MFA), data encryption, and patch management. • Understand the importance of incident response planning and procedures. • Understand energy cybersecurity regulations and guidelines. • Analyse real-world energy cybersecurity cases. **Skills:** • Develop and execute cybersecurity risk management plans. • Design and implement secure network architectures. • Deploy and manage security controls for energy systems. • Develop and execute incident response plans. • Comply with energy cybersecurity regulations and guidelines. • Apply cybersecurity concepts and techniques through practical exercises. • Communicate cybersecurity risks, policies, and procedures effectively. • Develop and maintain cybersecurity documentation. • Demonstrate a willingness to stay up-to-date with the latest cybersecurity threats and trends. **Competencies:** • Apply ethical decision-making in cybersecurity situations. • Analyse the impact of cybersecurity threats and vulnerabilities.

	• Design and implement secure solutions. • Manage and mitigate cybersecurity risks.
Main topics and content list *A list of main topics and key content*	• Ethical conduct and professionalism in the cybersecurity field. • Foundational knowledge of cybersecurity and body of knowledge. • Threats and vulnerabilities (including those specific to the energy sector). • Human factor considerations in cybersecurity (including energy sector specific). • Secure architecture design and implementation. • Security controls selection and implementation. • Security Data and Privacy by design (SDPbd) for the energy sector. • Cybersecurity governance for energy organisations. • Energy cybersecurity compliance and regulations. • Transferable skills and continuous learning in the cybersecurity profession.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment:** ongoing process of evaluating participants' learning during a training programme comprising pre-assessment, during and post-assessment in each training topic. It provides valuable feedback to instructors and participants, helping to ensure that learning goals are being met and that participants are making progress. • **Summative assessment:** learner needs to produce targeted outcomes and deliverables at the end of the training by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to tackle the threats based on a real-world scenario.
Training Provider *Name(s) of training providers.*	LAU, UMA, TALTECH, SGI, PDMFC, Trustilio.
Contact *Name(s) of the main contact person and their email address.*	• Paresh Rathod: Paresh.Rathod@laurea.fi • Cristina Alcaraz: alcaraz@uma.es • Ruben Rios: ruben.rdp@uma.es • Antonio Muñoz: anto@uma.es • Davide Ferraris: ferraris@uma.es • Ricardo Gregorio Lugo: ricardo.lugo@taltech.ee • Kitty Kioskli: kitty.kioskli@trustilio.com • Martin Bärman: mba@seriousgames.net • Nuno Pedrosa: nuno.pedrosa@pdmfc.com • Stylianos Karagiannis: stylianos.karagiannis@pdmfc.com
Dates offered *Indicates the semester / specific dates for the schedule of the*	Refer and check online CyberSecPro DCM System for current information

trainings, as well as periodicity (e.g. even after the end of the CSP programme).	
Duration *Duration of the training.*	11-12 weeks. This will depend on the calendar each year.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual, physical or both, depending on the situation (please, check the DCM platform).
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA1 - Cybersecurity Management. Minor content matches with other including: • KA2 – Human Aspects of Cybersecurity. • KA3 – Cybersecurity Risk Management. • KA4 – Cybersecurity Policy, Process, and Compliance. • KA5 – Network and Communication Security. • KA6 – Privacy and Data Protection. • KA10 – Cyber Incident Response.
Pre-requisites	Basic IT and security knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO).
Tools to be used *A list of tools that will be used for the operation of this training module.*	Several tools may be applied, such as: Nmap, Nessus, Wireshark, Suricata, Wazuh, Metasploit, Hydra, Jupyter Notebooks, VirtualBox, NFStream, ELK Stack, pfSense, Tshark, Metadon (PDM tool), Chimera (PDM Tool), Metago (PDM Tool), Caldera, eRamba, OpenCTI, MS Threat Modelling Tool, GPG, OpenSSL, Snort, YARA rules, Sigma Rules, Nessus, OpenVAS, MISP,

	STIX, TAXII, WPScan, Hping, LOIC, Splunk, ufw, Windows firewall, Vsftpd, Bitlocker, Cryptool2, OpenSSH, PuTTY, Kleopatra (for PGP), Veracrypt/Truecrypt, Thunderbird (for PGP and S/MIME), and XCA. Also, there are other online tools that will widely be considered such as ENISA CIRAS (https://ciras.enisa.europa.eu), CloudShark (https://www.cloudshark.org/), cryptii (https://cryptii.com) or those belonging to asecuritysite (https://asecuritysite.com). Any other tool used will be dynamically posted in the DCM platform
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Spoken: English or Greek. • Language for the material and the assessment/evaluation: English or Greek.
ECTS *If applicable, the number of ECTS.*	Recommended equivalent to 5 ECTS.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.1.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Understanding the Importance of Ethical Conduct and Professionalism in Energy Cybersecurity	• Recognise the ethical principles that underpin cybersecurity practices. • Understand the importance of responsible professional disclosure and ethical practices.

	• Implement appropriate ethical guidelines and policies for energy cybersecurity.
Topic-2: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge	• Define energy cybersecurity and its significance in the energy domain. • Understand the various components of an energy cybersecurity ecosystem. • Classify cybersecurity threats and vulnerabilities specific to energy systems. • Overview of the cybersecurity body of knowledge.
Topic-3: Energy Threats and Vulnerabilities	• Identify and categorise common energy cybersecurity threats, such as malware, ransomware, phishing, and social engineering. • Recognise the specific vulnerabilities that energy systems face, including outdated software, weak passwords, and unpatched vulnerabilities. • Energy sector specific threats and vulnerabilities include targeted attacks on SCADA systems, smart grids, and other critical energy assets. • Understand the role of human error and insider threats in energy cybersecurity incidents.
Topic-4: Human Factor Considerations in Energy Cybersecurity	• Recognise the role of human error as a significant contributor to cybersecurity incidents. • Understand the psychology of cybersecurity threats and how they exploit human behaviour. • Implement effective cybersecurity awareness training and education programmes. • Encourage a culture of cybersecurity vigilance and responsibility among energy personnel.
Topic-5: Secure Architecture Design and Implementation for Energy Systems	• Design and implement secure network architectures for energy systems. • Secure network architecture in the energy sector including SCADA systems, smart grids, and other critical energy assets. • Utilise network segmentation to isolate critical systems and reduce the impact of cyberattacks. • Configure firewalls and access control systems to protect energy networks and restrict unauthorised access. • Implement Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and protect networks. • Employ Virtual Private Networks (VPNs) for secure remote access to energy systems and sensitive data.

Topic-6: Security Controls Selection and Implementation for Energy Environments	• Select and implement appropriate security controls based on the specific needs of energy systems. • Implement strong password policies and MFA to protect user accounts. • Encrypt sensitive data at rest and in transit to prevent unauthorised access and data breaches. • Regularly apply security updates and patches to software systems to address vulnerabilities.
Topic-7: Data security and Privacy by design (SDPbd) for the Energy Sector	• Implement data security measures to protect sensitive energy data, including personal information and operational data. • Employ privacy by design principles to integrate data protection into the development and operation of energy systems. • Comply with relevant data privacy regulations and energy cybersecurity guidelines.
Topic-8: Cybersecurity Governance for Energy Organisations	• Establish a comprehensive cybersecurity governance framework for energy organisations. • Designate a cybersecurity champion or team to oversee and manage cybersecurity initiatives. • Develop and implement cybersecurity policies and procedures that align with organisational goals. • Conduct regular cybersecurity risk assessments and audits to maintain an effective cybersecurity posture.
Topic-9: Energy Cybersecurity Compliance and Regulations	• Understand and comply with relevant energy cybersecurity regulations. • Implement a process for monitoring and staying up-to-date with evolving cybersecurity regulations. • Conduct periodic cybersecurity compliance audits to ensure adherence to regulatory requirements.
Topic-10: Transferable Skills and Continuous Learning in Cybersecurity Profession	• Continuously self-assess cybersecurity knowledge and skills. • Stay up-to-date with the latest cybersecurity trends and technologies. • Participate in professional development training and certifications. • Embrace a growth mindset and actively seek opportunities to learn.

3.1.1.3 Planning for Preparedness

All the preparedness activities are planned and coordinated among the trainers. To do this, an internal action table has been created to facilitate the allocation of tasks and the estimation of time to carry out the training actions, also indicating the work methodology and the schedule for training. This collaborative approach, with clear roles and responsibilities, will ensure efficient training delivery. Each training topic has a designated lead trainer who holds primary responsibility for tasks such as developing and managing topic presentations, overseeing practical activities, creating specific materials and responsible trainers for respective training topics. In order to have a correct and suitable

training phase, all these materials will have to be available on the DCM platform and/or relevant course management systems for the delivery of training in advance. This includes, but not mandatory, videos, presentations, slides, questionnaires, assignments, serious games, and others encapsulated with selected pedagogical and learning approach. This is because each topic presents a different nature, and its handling may be different for its correct delivery, so each trainer can apply his or her didactic resources according to the needs or complexities to address in the corresponding topic, allowing flexibility in the process and encouraging the adaptability of materials according to needs.

The preparation phase will also imply that all trainers have access to the DCM platform and all of them will have to be synchronised and communicated each other using different medium for that, in addition to following an initial plan strategy that benefits the coordination between trainers, and the natural execution of the actions during the entire training period.

3.1.1.4 Materials and Exercises

As discussed previously, trainers follow a detailed internal action plan to ensure all materials and exercises are prepared well before each module launch. This plan guarantees a rich learning experience tailored to each topic's specific features and thematic. This means that each topic comprises a set of materials and exercises according to its own features, nature and thematic, providing participants with a comprehensive learning experience. For example, if the topic facilitates to carry out a set of practical actions based on the game-based learning methodology, a serious game will therefore be established with a particular time-frame, conditions and format

Thus, each topic will lead to different actions and different ways to address the training, using, for example, case studies, research analysis, discussions, development of lab exercises and other. Evidently, the focus of these activities will be subject to the level of the module, that in this case is basic, and the trainers will have to always maintain this level to facilitate the progressive learning, and the connection with other modules in the future.

As expected by CyberSecPro objective, the exercises shall be of a practical nature, even if some cases are of reflexive nature to allow participants to immerse themselves in situations that are relevant and keys for their own learning. They must understand the specific situations within the energy sector and its respective ecosystems, including the control, but also to comprehend the problem in each situation, and if required, provide solutions to avoid or mitigate them. Moreover, this module is planned to enable connecting experts in the energy sector to the cybersecurity field, but also participants without knowledge of the energy sector to the cybersecurity field as well, introducing, for example, in Topic 2, all the elements that comprises the ecosystem of energy, including control components and the transition to Smart Grid environments and its microgrid-based systems. Of course, we also aim to create an atmosphere based on discussion and reflection, in which participants can be open to critical thinking, either through the classes with direct connection with the trainer/s and the remaining learners or by means of the resources offered by the DCM platform such as forums.

Therefore, this module aims to provide the basis required to introduce participants to the security world, and particularly focused on a critical application context, with specific stakeholders, components, networks, protocols, risks and needs.

3.1.1.5 Verification of Learning Outcomes, and Skills

Various assessment elements and high-level process to determine participants have achieved the learning outcomes including and not limited to

- Formative assessment: ongoing process of evaluating participants' learning during a training programme including pre-assessment, during and post-assessment in each training topic. It provides valuable feedback to instructors and participants, helping to ensure that learning goals are being met and that participants are making progress.

- Summative assessment: learner needs to produce targeted outcomes and deliverables at the end of the training by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to tackle the threats based on a real-world scenario.

As part of the CyberSecPro goals, this module also incorporates all those assessment forms required to facilitate the evaluation of the training actions, allowing the continuous improvement and optimisation of resources, materials, exercises, and ways to train. This also means that in the final term of the CPS001_C_E, participants will be encouraged to complete these forms to evaluate for themselves the level received, and the optimal extent of the resources provided.

Trainers will also assess the degree of success of the learning outcomes by evaluating the different exercises, the interaction and development of critical thinking through the discussions or reflections in the activities, progress made by each participant and others. The overall evaluation elements can be summarised as below:

- Participant evaluation through self-assessment: towards the end of the CPS001_C_E module, participants will be encouraged to complete self-assessment forms. This will allow them to reflect on their learning experience and the value of the provided resources.
- Trainer evaluation: trainers will assess learning outcomes by evaluating various aspects, including:
    - exercise performance.
    - Participant interaction and critical thinking during discussions and activities.
    - Individual participant progress.
    - This evaluation process helps trainers gauge the comprehensiveness of the topics covered and identify areas for improvement, such as optimising content, intensifying instruction, or refining methods for knowledge and skill development in future sessions.
- Certificate of attendance: upon successful completion of the seminar, participants will be eligible to receive a certificate of attendance. This certificate acknowledges their commitment to expanding their knowledge of the cybersecurity concepts covered in CPS001_C_E, specifically within the energy sector context. It serves as a tangible recognition of their participation and dedication to professional development in cybersecurity with real-world application in the energy domain.

3.1.2 CSP001_S_E: Cybersecurity Essentials and Management for Energy Sector

3.1.2.1 Description of Training Module

The Cybersecurity Essentials and Management for Energy Sector training module, CSP001_S_ E, is a comprehensive guide designed to equip professionals within the energy industry with the necessary knowledge and tools to effectively safeguard critical assets and sensitive data from evolving cyber threats. Tailored specifically for the unique challenges faced by the energy sector, the module covers essential policies, strategies, and best practices to mitigate risks such as unauthorised access, data breaches, and insider threats. Intended for a diverse audience ranging from cybersecurity students/professionals to energy producers or utility providers, the module aims to bolster the resilience of the energy sector against present and future cybersecurity challenges, ensuring a secure foundation for sustainable growth.

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_S_ E**
Module Title *The title of the training module*	**Cybersecurity Essentials and Management for Energy Sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cybersecurity Essentials in the Energy Sector - Management and Policies. • Energy Cybersecurity Essentials. • Energy Cybersecurity Management. • Cybersecurity for the Modern Workplace - Cybersecurity Essentials and Principles in Energy Sector. • A Comprehensive Overview of Energy Cybersecurity Core Concepts. • Mastering the Fundamentals of Energy Cybersecurity • Introduction to Information and Cyber Security in Energy Sector. • Introduction to Information Security Management for Energy Sector.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	This training module dives deep into the essential concepts and principles of cybersecurity in the energy sector. It provides all the necessary policies to administer and monitor users and employees for the energy sector infrastructure in order to avoid leaks, breaches and whistle-blowers.

Module description *Indicates the main purpose and description of the module.*	All sectors are gradually transitioning to the digital era. The energy sector could not be left outside of this evolution. Big part of this digitalisation process is the challenge the organisation and businesses face in order to protect employees, infrastructure and users from unauthorised access of data, disruption of energy production or whistle-blowers which are keen to steal and leak data. This seminar provides all the essential knowledge that needs to be applied to protect all parties of the Energy Industry while being ready for future challenges.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge (understanding and awareness of following):** • Understanding of cybersecurity threats specific to the energy sector. • Familiarity with relevant cybersecurity standards governing energy cybersecurity. • Knowledge of cyber risks prevalent in energy operations. • Awareness of case studies and real-world examples of cybersecurity incidents in the energy industry. • Understanding of risk assessment and management methods and tools tailored to the energy sector. • Understanding of best practices for securing energy Information Technology (IT) and Operational Technology (OT) systems. • Cybersecurity policies and principles as they should be applied and provisioned. • IT administration and the challenges that this specific personnel faces in this particular sector. • Familiarity with business continuity and best practices in the energy sector. • Restoration and backup policies to recover from disastrous events. • Staff education on cybersecurity best practices. **Skill and Competence (applications and practice):** • Ability to identify and assess cybersecurity threats in energy operations. • Capacity in applying risk assessment and management methodologies as well as tools specific to the energy sector. • Competence in applying cybersecurity standards and best practices to safeguard energy systems and infrastructure. • Skill in interpreting and adhering to relevant cybersecurity standards and regulations in an energy context.

	• Ability to analyse case studies and real-world examples of cybersecurity incidents in the energy industry. • Competence in contributing to the overall cybersecurity posture and resilience of energy organisations. • Capacity in using methods for backup and recovery.
Main topics and content list *A list of main topics and key content*	• Overview of cybersecurity threats in the energy sector. • Importance of energy cybersecurity. • Relevant cybersecurity standards. • Identification of cyber risks in energy operations. • Case studies and real-world examples of cybersecurity incidents in the energy industry. • IT & OT infrastructure and devices. • Risk assessment and management methods.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** these assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery by the instructor.
Training Provider *Name(s) of training providers.*	TUC and TUBS.
Contact *Name(s) of the main contact person and their email address.*	• Pinelopi Kyranoudi: pkyranoudi@tuc.gr • Antonios Ntib: antonios.ntib@tu-braunschweig.de
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	2 hours.

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response.*	Mainly: • KA1 – Cybersecurity Management. • KA3 – Cybersecurity Risk Management. • KA4 – Cybersecurity Policy, Process, and Compliance.
Pre-requisites	Basic IT knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO). • ECSF Profile 3: Cyber Legal, Policy & Compliance Officer. • ECSF Profile 4: Cyber Threat Intelligence Specialist. • ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 8: Cybersecurity Implementer. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	ENISA Minimum Security Measures for Operators of Essentials Services, ENISA Good practices for Internet of Things (IoTs) and Smart Infrastructures Tool, mdadm.
Language	English, Greek.

Indicates the spoken language and the language for the material and the assessment/evaluation.	
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.1.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to Energy Cybersecurity	• Overview of cybersecurity threats in the energy sector. • Importance of energy cybersecurity. • Introduction to relevant cybersecurity standards (e.g. Organización Internacional de Normalización (ISO)/ International Electrotechnical Commissio (IEC) 2700x, ISO 27019, National Institute of Standards and Technology (NIST) SP-800-82).
Topic-2: Understanding Energy Cyber Risks	• Identification of cyber risks in energy operations. • Case studies and real-world examples of cybersecurity incidents in the energy industry. • IT & OT infrastructure and devices.

Topic-3: Risk Assessment and Management	• Risk assessment VS risk management. • Risk assessment and management methods. • Risk assessment and management in cyber-physical systems and OT.
Topic-4: Business Continuity and Best Practices	• Incident response. • Data backup and recovery planning. • Staff education on cybersecurity best practices (e.g. Redundant Array of Inexpensive Disk (RAID), cold storages, access methods to server rooms).

3.1.2.3 Planning for Preparedness

As long as the trainees cover the required knowledge for the level of this seminar, its structure is designed in such a way that no special preparation is required on their part. Everything needed will be provided in advance on the DCM platform and will be covered throughout the seminar.

3.1.2.4 Materials and Exercises

The CSP001_S_ E training material is to be shared on the DCM platform in the form of comprehensive slides. Any exercises and tests related to this will be shared with trainees during the seminar.

3.1.2.5 Verification of Learning Outcomes, and Skills

Completion of attendance.

3.1.3 CSP001_CS-E_E: RxB - Cyber Security Management Game

3.1.3.1 Description of Training Module

RxB is an asymmetrical strategy game about cyber attacks and defences. You play as the blue team trying to protect your system against various attacks from the red team. Your goal is to find vulnerabilities in your system and learn how to respond to threats. The module introduces the well-known red vs. blue approach to understanding cybersecurity through gamification. The game covers essential concepts and management strategies in the context of cybersecurity within the energy sector. The learning material is targeted toward beginners/intermediates in the cybersecurity field, and therefore requires the user to have a basic knowledge of cybersecurity frameworks and terms. It may appeal to security managers or IT-support employees working in the energy sector, who want to expand their knowledge. Additionally, it may also appeal to university students who study IT and cybersecurity on a basic level. The RxB game aims to equip users with knowledge of different cyber security protocols as well as a variety of cyberattacks that occur in the energy sector on a regular basis.

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_CS-E_E**
Module Title *The title of the training module*	**RxB - Cyber security management game**

Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cyber security management game. • RxB - cyber security game. • Educational game for teaching cyber security management.
Training offering type *Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O).*	Cybersecurity Exercise (CS-E).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The training module will consist of a playthrough of the "RxB - Cyber security management" game. The users will play through a energy specific training scenario, where they will play as a cyber security manager of a hospital.
Module description *Indicates the main purpose and description of the module.*	The player's goal is to identify vulnerabilities in their network, detect threats and protect your assets, so their company avoids any major damage from outside cyber attacks. In the game the players will have to assign their team members (non-playable characters), to various tasks and improve their skill sets as the game progresses. Throughout the game, the red team (hackers) will continuously try and breach your security and exploit various vulnerabilities. The energy section of the game will feature a number of different events and assets that are specific to the given sector. No practical technical skill is required to play. However, it helps to know about cybersecurity terminology and concepts - if not, the user will learn by failing.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners should have gained an understanding of various concepts in the following areas: **Knowledge:** • Cybersecurity Essentials and Management. **Skill and Competence:** • Risk assessment, prioritisation, and resource management. • Recognise different types of vulnerabilities. • Learn about various attack vectors and strategies. • Learn about various defensive mitigations and strategies. • Learn about protocols from the NIST framework.
Main topics and content list *A list of main topics and key content*	RxB aims to deliver more awareness within the following topics: • Cyber security defences require regular adjustment. • Promote situation awareness by navigating through an active attack. • Familiarisation with hacker and cyber defence terminology. • How and when specific protocols are used in the NIST framework.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Performance based assessment:** During gameplay learners will be evaluated on how well their decision making is, through the use of in-game feedback. • **Attitudinal assessments:** Learners need to answer an online questionnaire, where they are graded on their understanding of cybersecurity practices.
Training Provider *Name(s) of training providers.*	Serious Games Interactive (SGI)
Contact *Name(s) of the main contact person and their email address.*	• Louise Præstin: lp@seriousgames.dk • Martin Bärmann: mba@seriousgames.net

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	45 minutes exercise.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual, as it is an individual exercise it will be distributed through the DCM and played using the following link (be aware that the link may be updated later, so check the DCM to see the updated version of the game): https://beta.seriousgames.net/games/spider/1.0.0/ Training sessions will occasionally be held physically, though the locations will vary from time to time. Currently two sessions are planned, one in Porto, during the IPCS summer school and another at the Copenhagen Business School, sometime in September.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly • KA1 – Cybersecurity Management. Secondary areas would include: • KA2 – Human Aspects of Cybersecurity • KA3 – Cybersecurity Risk Management
Pre-requisites	Basic IT and Security Knowledge.

Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF.*	• ECSF Profile 1: Chief Information Security Officer (CISO).
Tools to be used *A list of tools that will be used for the operation of this training module.*	Learners will need a computer and Internet access. No additional tools are required.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates	From the launch of the DCM to the end of the CyberSecPro project.

3.1.3.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Threats and Vulnerabilities for Energy Sector	• Signs of threats or cyber security breaches. • Introduction to network assets and asset specific vulnerabilities. • Introduction to the NIST protocols.
Topic-2: Introduction to Human Aspects of Energy Cybersecurity	• Examples based on case studies from real-world energy incidents.

	• Consequences of neglecting the human factor in the energy sector.

3.1.3.3 Planning for Preparedness

The training can be carried out both virtually or physically. When carried out virtually, the game would either be sent out as a link, or hosted on an online platform that distributes learning materials. The game will primarily work as a self-facilitated exercise, and it is therefore not a requirement that facilitators are present during the exercise. The exercise can be carried out at any physical location, as long as the user has a computer and internet connection.

3.1.3.4 Materials and Exercises

The cybersecurity exercise only requires the user to have a computer, internet connection and a method of distribution for the game. Examples of distribution channels could be the form of email, online platforms, Quick-Response (QR) codes or similar methods.

3.1.3.5 Verification of Learning Outcomes, and Skills

The RxB exercise will primarily be evaluated through performance-based assessment. This will primarily be through feedback within the game, which gives the user an idea of how their choices impacted the outcome. Furthermore, the user will be given a questionnaire that will have the user reflect upon cybersecurity practices and priorities that were presented in the game, which would fall under Attitudinal assessments.

3.2 Module 2 - Human Factors and Cybersecurity for Energy

3.2.1 CSP002_S_E: Human Factors and Energy Cybersecurity

3.2.1.1 Description of Training Module

The training module, "Human Aspects of Cybersecurity in the Energy Sector," is designed to empower managers, engineers, administrators, and other key personnel within the energy domain. This initiative is critical not only for aspiring cybersecurity professionals but also for seasoned operators and providers engaged with energy infrastructures. The distinctive nature of this module extends beyond the typical boundaries of generic cybersecurity training. It delves into the specific human challenges and vulnerabilities of inherent to the energy sector, equipping participants with a profound understanding of the cyber landscape. This comprehensive curriculum addresses human factors that can influence the nuanced threats that target critical components such as SCADA systems, smart grids, and other essential energy assets.

The module also integrates discussions on industry-specific regulatory compliance and the development of robust strategies aimed at human and organisational behaviours to assess and mitigate cyber risks, ensuring a comprehensive understanding for preparedness. The modules emphasise the implementation of both human and organisational cybersecurity behaviours, tailored to the unique needs of the energy sector. This approach ensures that participants are not only aware of the potential threats posed to humans, but are also proficient in developing behavioural mitigation strategies against potential cyber-attacks and increase cyber resilience.

With a focus on fostering a cybersecurity-aware culture, this training is essential for all stakeholders within the energy sector aiming to enhance their defensive capabilities against the ever-growing cyber threats in this critical industry.

Thus, CSP002_S_E is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing.

Code *Code format: CSP002_x where x is the training of offering type (see below)*	**CSP002_S_E**
Module Title *The title of the training module*	**Human Aspects of Energy Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• The Human Dimension in Energy Cybersecurity. • Navigating Energy Cyber Threats: The Human Element. • Elements of Cyberpsychology in Energy. • Humans in Energy Cybersecurity. • Human centric cyber defence in energy domains.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The module aims to provide energy stakeholders with the knowledge necessary about human aspects of cybersecurity pertinent for the energy domain, both at the individual and organisational levels, as well as at the strategic, operational, and tactical levels.

Module description *Indicates the main purpose and description of the module.*	This seminar navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees will uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations. It further highlights the vital importance of communication and collaboration at strategic, operational, and tactical levels specific to the energy sector. Participants will investigate how proficient communication between energy domains and effective decision-making can strengthen cybersecurity measures in energy operations.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:** • Gain an understanding of the psychological, social, and organisational elements that shape cybersecurity actions within the energy domain. • Understand the critical role of communication and teamwork in bolstering energy cybersecurity across different sectors. • How decision-making frameworks are used at strategic, operational, and tactical levels within energy cybersecurity. • Recognise the profiles and strategies of adversaries targeting energy operations. • Evaluate human-related threats and vulnerabilities in energy contexts. **Competencies:** • Understand the discussions pertinent to energy cybersecurity at various levels of decision-making. • Cultivate an environment of transparent communication and teamwork focused on energy cybersecurity. • Reflect on cybersecurity decision-making with the understanding of how human factors are related in the energy arena. • Identify human-centric threats and vulnerabilities in energy operations.
Main topics and content list	• Ethical and professional practices. • Introduction to human aspects of energy cybersecurity. • Psychological and social factors in energy cybersecurity. • Human vulnerabilities in energy cybersecurity

A list of main topics and key content	• Organisational culture, communication, and cybersecurity. • Communication and collaboration across domains. • Decision making at strategic, operational, and tactical levels. • Training, awareness, and communication programmes for energy personnel. • Future trends, challenges, and the role of communication.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment:** learner needs to answer short questions to show an understanding of different human aspects. • **Summative assessment:** learner needs to produce a 1500-word report based on an energy cybersecurity case study that reflects over different human aspects of an energy cybersecurity breach.
Training Provider *Name(s) of training providers.*	TalTech, Trustilio, Laurea.
Contact *Name(s) of the main contact person and their email address.*	• Ricardo Lugo: Ricardo.Lugo@taltech.ee • Kitty Kioskli: kitty.kioskli@trustilio.com • Paresh Rathod: Paresh.Rathod@laurea.fi
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	4 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-2: Human Aspects of Cybersecurity. • KA-7: Cybersecurity Threat Management.
Pre-requisites	None.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO). • ECSF Profile 7: Cybersecurity Educator. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Personal computer with world wide web access necessary.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek.
ECTS	N/A.

If applicable, the number of ECTS.	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.2.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to Human Aspects of Energy Cybersecurity	• Energy cybersecurity landscape. • Cost of neglecting the human element. • Examining real-world energy incidents.
Topic-2: Psychological and Social Factors in Energy Cybersecurity	• Understanding cognitive biases. • Social engineering techniques. • Group dynamics.
Topic-3: Human Vulnerabilities in Energy Cybersecurity	• Insider threats. • Impact of stress and fatigue. • Case studies. • Mitigation strategies.
Topic-4: Organisational Culture, Communication, and Energy Cybersecurity	• Organisational values. • Leadership's role. • Proactive security culture for energy.
Topic-5: Communication and Collaboration Across Domains	• Effective communication. • Role of mediators.

Topic-6: Decision Making at Strategic, Operational, and Tactical Levels	• Layers of decision-making. • Role of data-driven decision-making.
Topic-7: Training, Awareness, and Communication Programmes	• Designing impactful training. • Role of continuous education. • Leveraging technology to enhance training.
Topic-8: Future Trends, Challenges, and the Role of Communication	• Anticipating threats. • Role of emerging technologies in energy. • Artificial Intelligence (AI) and automation.

3.2.1.3 Planning for Preparedness

As long as the trainees cover the required knowledge for the level of this seminar, its structure is designed in such a way that no special preparation is required on their part. Everything needed will be provided in advance on the DCM platform and will be covered throughout the seminar. Participants will be encouraged to lead discussions of various subjects.

3.2.1.4 Materials and Exercises

The training material is to be shared on the DCM platform in the form of comprehensive slides. Any exercises and tests related to this will be shared with trainees during the seminar.

3.2.1.5 Verification of Learning Outcomes, and Skills

Successful completion of attendance and at least borderline pass of the mean of the grades of the quizzes done during the seminar.

3.2.2 CSP002_SS_E: Human Factors and Cybersecurity

3.2.2.1 Description of Training Module

The training module, "Human Aspects of Cybersecurity in the Energy Sector," is designed to empower managers, engineers, administrators, and other key personnel within the energy domain. This initiative is critical not only for aspiring cybersecurity professionals but also for seasoned operators and providers engaged with energy infrastructures. The distinctive nature of this module extends beyond the typical boundaries of generic cybersecurity training. It delves into the specific human challenges and vulnerabilities of inherent to the energy sector, equipping participants with a profound understanding of the cyber landscape. This comprehensive curriculum addresses human factors that can influence the nuanced threats that target critical components such as SCADA systems, smart grids, and other essential energy assets.

CSP002_SS_E also integrates discussions on industry-specific regulatory compliance and the development of robust strategies aimed at human and organisational behaviours to assess and mitigate cyber risks, ensuring a comprehensive understanding for preparedness. The module emphasises the implementation of both human and organisational cybersecurity behaviours, tailored to the unique needs of the energy sector. This approach ensures that participants are not only aware of the potential threats posed to humans but are also proficient in developing behavioural mitigation strategies against potential

cyber-attacks and increase cyber resilience. Participants will also be required to research and present findings and develop mitigation strategies pertinent for increasing awareness and mitigating cyber threats.

With a focus on fostering a cybersecurity-aware culture, this training is essential for all stakeholders within the energy sector aiming to enhance their defensive capabilities against the ever-growing cyber threats in this critical industry. Thus, CSP002_SS_E is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing.

Code *Code format: CSP002_x where x is the training of offering type (see below)*	**CSP002_SS_E**
Module Title *The title of the training module*	**Human Aspects of Energy Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• The Human Dimension in Energy Cybersecurity. • Navigating Energy Cyber Threats: The Human Element. • Elements of Cyberpsychology in Energy. • Humans in Energy Cybersecurity. • Human centric cyber defence in energy domains.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	SS (Summer School).
Level *Training level: B (Basic), A (Advanced)*	A (Advanced).

Module overview *High-level module overview*	The module aims to provide energy stakeholders with the knowledge necessary about human aspects of cybersecurity pertinent for the energy domain, both at the individual and organisational levels, as well as at the strategic, operational, and tactical levels.
Module description *Indicates the main purpose and description of the module.*	This module navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees will uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations. It further highlights the vital importance of communication and collaboration at strategic, operational, and tactical levels specific to the energy sector. Participants will investigate how proficient communication between energy domains and effective decision-making can strengthen cybersecurity measures in energy operations.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:** • Gain an understanding of the psychological, social, and organisational elements that shape cybersecurity actions within the energy domain. • Understand the critical role of communication and teamwork in bolstering energy cybersecurity across different sectors. • How decision-making frameworks are used at strategic, operational, and tactical levels within energy cybersecurity. • Recognise the profiles and strategies of adversaries targeting energy operations. • Evaluate human-related threats and vulnerabilities in energy contexts. • How to implement cybersecurity trainings in energy operations. **Skills:** • Use effective communication plans tailored to energy cybersecurity needs. • Detect and counteract human-centric threats and vulnerabilities in energy operations.

	• Engage with interdisciplinary teams to tackle the human dimensions of cybersecurity in energy settings. • Examine real-world energy cybersecurity breaches to pinpoint human errors and lapses in communication. • Classify adversaries targeting energy interests and scrutinise their tactics. • Design and evaluate cybersecurity trainings tailored for energy domains. **Competencies:** • Lead the discussions pertinent to energy cybersecurity at various levels of decision-making. • Cultivate an environment of transparent communication and teamwork focused on energy cybersecurity. • Understand the needs of training within cybersecurity.
Main topics and content list *A list of main topics and key content*	• Ethical and professional practices. • Introduction to human aspects of energy cybersecurity. • Psychological and social factors in energy cybersecurity. • Human vulnerabilities in energy cybersecurity. • Organisational culture, communication, and cybersecurity. • Communication and collaboration across domains. • Decision making at strategic, operational, and tactical levels. • Training, awareness, and communication programmes for energy personnel. • Future trends, challenges, and the role of communication.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment:** learner needs to answer short questions to show an understanding of different human aspects. • **Summative assessment:** learner needs to produce a 3000-word report based on an energy cybersecurity case study that reflects over different human aspects of an energy cybersecurity breach and possible mitigation strategies at the individual and organisational level, develop a training plan for promoting cybersecurity behaviours in energy personnel.
Training Provider *Name(s) of training providers.*	TalTech, Trustilio, Laurea.

Contact *Name(s) of the main contact person and their email address.*	• Ricardo Lugo: Ricardo.Lugo@taltech.ee • Kitty Kioskli: kitty.kioskli@trustilio.com • Paresh Rathod: Paresh.rathod@laure.fi
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	2 days.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-2: Human Aspects of Cybersecurity • KA-7: Cybersecurity Threat Management
Pre-requisites	None.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO). • ECSF Profile 7: Cybersecurity Educator. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Personal computer with world wide web access necessary.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek.
ECTS *If applicable, the number of ECTS.*	N/A.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.2.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to Human Aspects of Energy Cybersecurity	• Energy cybersecurity landscape. • Cost of neglecting the human element. • Examining real-world energy incidents.
Topic-2: Psychological and Social Factors in Energy Cybersecurity	• Understanding cognitive biases. • Social engineering techniques. • Group dynamics.
Topic-3: Human Vulnerabilities in Energy Cybersecurity	• Insider threats. • Impact of stress and fatigue. • Case studies. • Mitigation strategies.
Topic-4: Organisational Culture, Communication, and Energy Cybersecurity	• Organisational values. • Leadership's role. • Proactive security culture for energy.
Topic-5: Communication and Collaboration Across Domains	• Effective communication. • Role of mediators.

Topic-6: Decision Making at Strategic, Operational, and Tactical Levels	• Layers of decision-making. • Role of data-driven decision-making.
Topic-7: Training, Awareness, and Communication Programmes	• Designing impactful training. • Role of continuous education. • Leveraging technology to enhance training.
Topic-8: Future Trends, Challenges, and the Role of Communication	• Anticipating threats. • Role of emerging technologies in energy. • AI and automation.

3.2.2.3 Planning for Preparedness

As long as the trainees cover the required knowledge for the level of this seminar, its structure is designed in such a way that no special preparation is required on their part. Everything needed will be provided in advance on the DCM platform and will be covered throughout the module. CSP002_SS_E will also use flipped classroom approaches for group led discussion and presentations.

3.2.2.4 Materials and Exercises

The CSP002_SS_E training material is to be shared on the DCM platform in the form of comprehensive slides. Any exercises and tests related to this will be shared with trainees during the seminar.

3.2.2.5 Verification of Learning Outcomes, and Skills

Successful completion of attendance, group work and presentation of case study, and at least borderline pass of the mean of the grades of the quizzes done during the workshop.

3.2.3 CSP002_CS-E_E: HATCH

3.2.3.1 Description of Training Module

HATCH is a serious game to elicitate social engineering threats and to provide an interactive group training that teaches participants to identify and successfully defend against social engineering attacks. HATCG is a scenario-based training and complies with ISO/IEC 27001 control A.7.2.2. A company-specific adaption is possible but not planned in the course of CyberSecPro.

When playing HATCH, players attack personas in a virtual scenario based on cards with psychological principals and social engineering attacks. While personas are by definition imaginary, they provide a realistic description of stakeholders or in this case employees, who have names, jobs, feelings, goals, and certain needs. This way players can learn about the attackers' perspective, their vulnerabilities and get a better understanding of potential attack vectors.

However, HATCH can not only be used for training purposes but also to elicit security requirements to prevent social engineering. Instead of the virtual personas, players describe social engineering attacks on their colleagues. Since players know their colleagues, no persona descriptions are necessary and players can exploit their knowledge about processes in their work environment, i. e. about how to cut through the red tape and informal ways of handling tasks. As a result, at the end of the game a list of potential attacks can be investigated by the IT department.

Code *Code format: CSP002_x where x is the training of offering type (see below)*	**CSP002_CS-E_E**
Module Title *The title of the training module*	**HATCH**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	N/A
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	• Seminar (S). • Cybersecurity exercise (CS-E).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	Social Engineering.
Module description *Indicates the main purpose and description of the module.*	A serious game where players will be in the role of an attacker and apply social engineering attacks in a virtual scenario. The game offers the most common social engineering attacks, psychological principles, and a game plan with virtual personas. Based on the social engineering attack cards and the social principle cards the player drew, players need to come of with attacks on the personas in the game. If needed (depending on the knowledge of the players), an introduction to social engineering can be given before. According to our work plan, the scenario will be from the energy sector. Other scenarios (e.g.

	maritime) would be available as well or are under development (health) if needed.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	N/A
Main topics and content list *A list of main topics and key content*	N/A
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Participation.
Training Provider *Name(s) of training providers.*	SEA.
Contact *Name(s) of the main contact person and their email address.*	• Sebastian Pape: sebastian.pape@social-engineering.academy
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g.*	Refer and check online CyberSecPro DCM System for current information.

even after the end of the CSP programme).	
Duration *Duration of the training.*	• A minimum of 2 hours is needed; 3 to 4 hours would be optimal.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-10: Human Aspects of Cybersecurity
Pre-requisites	None.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	N/A

Tools to be used *A list of tools that will be used for the operation of this training module.*	HATCH, the serious card/board game developed by us.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Spoken: English or German. • Material and assessment: English or German. • Portuguese is in development.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.2.3.2 Adapted Syllabus

Refer and check online CyberSecPro DCM System for current information.

3.2.3.3 Planning for Preparedness

Playing the game requires a game master who will explain the rules and guide through the game. The game is a physical board game, thus players need to meet in person. Material will be provided by SEA. The room should have tables for 4 to 5 persons. Each game master can supervise roughly 4 groups. An online version is planned but not ready as of now. The duration of the game is minimum 120 minutes.

3.2.3.4 Materials and Exercises

• Card game

- 12 attacker type cards
- 17 Psychological principle cards
- 26 Social engineering attack cards

• Scenarios
- Game plan
- Persona cards

• Attack forms

All material is intellectual property of SEA and will be provided by SEA when executing a game.

3.2.3.5 Verification of Learning Outcomes, and Skills

The outcome of the game will be social engineering attacks in the played scenario. Those can be evaluated. It is also possible to run pre- and post-game surveys.

3.2.4 CSP002_CS-E_E: PROTECT

3.2.4.1 Description of Training Module

Since security policies are documents often unread by the users, the serious game PROTECT was developed to train users in behaving according to the organisation's security policies. PROTECT is a digital card game where players have to defend against attacks with the correct defences in a solitaire like game type. Special cards allow users to peak on the card pile and skip attack cards when they do not hold the corresponding defences.

Code *Code format: CSP002_x where x is the training of offering type (see below)*	**CSP002_CS-E_E**
Module Title *The title of the training module*	**PROTECT**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	N/A

Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	• Cybersecurity exercise (CS-E).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	Social Engineering.
Module description *Indicates the main purpose and description of the module.*	A serious game where players will be needed to defend against social engineering attacks in a virtual card game. A demo with only limited cards can be found here: https://demo.protect.social-engineering.academy/en/ The cards can be customised and adapted to a certain training as long as they follow the pattern that they come in attack/defence pairs. According to our work plan, the scenario will be from the energy sector. Other scenarios (e.g. maritime) would be available as well or are under development (health) if needed.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	N/A
Main topics and content list *A list of main topics and key content*	N/A

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Participation in the virtual game.
Training Provider *Name(s) of training providers.*	SEA.
Contact *Name(s) of the main contact person and their email address.*	• Sebastian Pape: sebastian.pape@social-engineering.academy
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	• Depends on player, for the first game around 20 minutes should be planned. Follow-up games can be done in a shorter time since the player will be familiar with the rules
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual.

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-10: Human Aspects of Cybersecurity.
Pre-requisites	None.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	N/A
Tools to be used *A list of tools that will be used for the operation of this training module.*	PROTECT, a virtual serious card game developed by us.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Material, assessment: English or German.
ECTS *If applicable, the number of ECTS.*	N/A.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.2.4.2 Adapted Syllabus

Refer and check online CyberSecPro DCM System for current information.

3.2.4.3 Planning for Preparedness

Game duration should be planned with roughly 15 minutes for the first time. The game is online and contains a tutorial. Thus, no supervision or coordination with other players is needed.

3.2.4.4 Materials and Exercises

Players need a browser to open the game. Apps are planned but as of now not ready for production.

3.2.4.5 Verification of Learning Outcomes, and Skills

The game has a dashboard which reports the outcome of the games in a privacy-aware manner.

3.3 Module 3 - Cybersecurity Risk Management and Governance for Energy

3.3.1 CSP003_S_E: Cybersecurity Risk Management and Governance in the Energy sector

3.3.1.1 Description of Training Module

This module is designed for energy sector practitioners and potential employees including IT, security, and business leaders who need to understand the basic concepts regarding Cybersecurity Risk Management and Governance. The targeted learners should be beginners/intermediates the IT and cybersecurity field, who have only basic knowledge of IT and cybersecurity. The recent university

graduate and final year students from computing and cybersecurity disciple can also attend this module to expand their knowledge relating to risk management and governance.

Code *Code format: CSP003_x where x is the training of offering type (see below)*	**CSP003_S_E**
Module Title *The title of the training module*	**Cybersecurity Risk Management and Governance in the Energy sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cybersecurity Governance in Energy. • Energy Sector Cybersecurity Risk management and Governance.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S (Seminar).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The module aims to provide an overview of cybersecurity risk management and governance for the energy sector. It allows the learners to understand the threats, vulnerabilities, and mitigation actions to ensure security and governance of energy sector.
Module description *Indicates the main purpose and description of the module.*	The module provides an understanding of the underlying properties and principles associated with cybersecurity risk management with particular focus on the energy sector. It offers the learners the opportunity to understand and adopt the relevant standard for risk management and governance to the energy domain.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:**

participants as a result of taking a CSP module	• Demonstrate an in-depth understanding of cyber. security risk management framework in the energy sector. • Recognise the significant cybersecurity governance. structures and processes in the energy sector. **Skill and Competence:** • Critically assess and report security risk and suggest suitable mitigation strategies in professional manner. • Critically develop and evaluate security policy and select controls by following ISO 27019 for security governance.
Main topics and content list *A list of main topics and key content*	• Overview of cyber security in energy sector. • Risk management framework. • Threats landscape in energy sector. • Industry standard. • Security controls for energy utility domain.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Coursework portfolio (80%) Summative assessment:** learner needs to produce a 3000-word portfolio at the end of the module by performing a list of tasks to demonstrate the learning outcomes are achieved. • **Presentation (20%) Summative assessment:** learners need to present the outcomes of the portfolio to demonstrate their understanding.
Training Provider *Name(s) of training providers.*	SLC, APIRO
Contact *Name(s) of the main contact person and their email address.*	• Prof. Dr. Shareeful Islam, shareeful@gmail.com • Athina Labropoulou athinalabrop@gmail.com • Chatzopoulou Argyro, ac@apiroplus.solutions
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	4 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA1: Cybersecurity Management. • KA3: Cybersecurity Risk Management.
Pre-requisites	Basic IT and security Knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO). • ECSF Profile 3: Cyber Legal, Policy & Compliance Officer. • ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	• Risk register template. • Audit checklist.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.

Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.3.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Overview of cyber security in energy sector	• Cyber security fundamentals. • Cyber security context in energy sector.
Topic-2: Risk management framework	• Risk management basic. • Principles of risk management and process.
Topic 3: Threats landscape in energy sector	• Threats and vulnerability management for energy sector.
Topic 4: Industry standard	• Introduction to ISO/IEC 27001, status, versions, structure (Clauses 1-4 and Annex A). • ISO 27001:2022 / ISO/IEC 27002:2022 control themes
Topic 5: Security controls for energy utility domain	• Terms and definitions of ISO 27000 adapted to the energy utility domain • Guidance on the controls of ISO/IEC 27002:2022 adapted to the energy utility domain • Energy specific controls by following ISO/IEC 27019 (DIS).

3.3.1.3 Planning for Preparedness

The training for CSP003_S_E is planned to delivery through dual delivery modes mainly both virtually and physically depending on the learners. This seminar will be well structured and systematically covered the topics. The trainees from APIRO and SLC ensure the required knowledge necessary for this seminar and no special preparation is required. All teaching and learning content will be provided in advanced on the DCM platform, preparation phase focuses on ensuring the materials are uploaded prior the training delivery.

3.3.1.4 Materials and Exercises

This training module follows topic-based teaching and learning material preparation. In particular, there are five distinct topics covered within the module and materials are prepared accordingly. The training material will be shared on the DCM platform in the form slides. Practical scenarios relating to threats

and vulnerabilities in energy sectors and security controls by following the standards will be added within the training content. Task based exercise related to the topic will be shared with the trainees as a part of assessment during the seminar.

3.3.1.5 Verification of Learning Outcomes, and Skills

Upon completion of the CSP003_S_E training, learners need to participate into the summative assessment components which consists of a one thousand words coursework portfolio and a presentation. The coursework will cover tasks relating to the key topics of the training content and presentation will demonstrate the learning understanding about the knowledge relating to the domain. This ensures the achievement of the learning outcomes by the trainee and supports progress to the next level upon completion of the training. Trainee will also complete the end of training evaluation form to provide feedback about the training. Finally, a certificate of attendance will be given to the trainees as a recognition for the training completion.

3.3.2 CSP003_S_E: Cybersecurity Risk Assessment and Management for Energy Sector

3.3.2.1 Description of Training Module

CPS003_S_E provides an overview of the security risks in the energy sector, as the main aim of this seminar is to understand how to identify, prevent and manage risks depending on the situation. Therefore, the seminar is designed for energy professionals, managers, and directives in charge of managing critical energy application domains, but also for those industrial engineers and IT/OT administrators, higher education students and cybersecurity aspirants without sufficient knowledge of security risks in the sector and who want to understand the associated threats and existing techniques to prevent or mitigate them.

Code *Code format: CSP003_x where x is the training of offering type (see below)*	**CSP003_S_E**
Module Title *The title of the training module*	**Cybersecurity Risk Assessment and Management for Energy Sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Survey-based Risk Assessment for Energy Sector.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If*	Seminar (S).

other, please specify the specific type.	
Level *Training level: B (Basic), A (Advanced)*	Basic (B).
Module overview *High-level module overview*	The rate of cyber incidents is increasing in certain strategic sectors to the point of causing greater damage and consequences to society, as is the case of the energy sector, whose services are considered "essential" for social and economic welfare. Therefore, this seminar aims to show how to prevent these situations by learning about how to identify risks, assess them and manage them properly.
Module description *Indicates the main purpose and description of the module.*	This seminar provides a set of terms and concepts associated with cybersecurity risk management and its associated assessment, specifically applied to the energy sector. Within risk assessment, various topics are covered such as: (1) risk identification in the energy sector considering assets, threats, and vulnerabilities (including security controls); (2) risk analysis and its associated methods; and (3) risk evaluation. The seminar ends with the treatment of risk to avoid major consequences when the affected sector is the energy sector or their main operational elements.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Basic definitions related to information security management systems and information security governance, and especially applied to the energy sector and its operational systems. • Risk management and its assessment for specific critical sectors such as energy and its operational systems. • Basic phases and principles for an effective risk management methodology. **Skills:** • Identify and know to apply an appropriate methodology for information security risk management and risk

	assessment according to the specific characteristics of the energy scenarios. **Competencies:** • Lead and participate in strategic, operational, and tactical cybersecurity discussions, with a particular focus on the energy sector. • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories; all of them specific to the energy sector and its operational systems. • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks in the energy sector and its operational systems.
Main topics and content list *A list of main topics and key content*	• Threats and vulnerabilities for energy sector. • Risk assessment and management processes and methodologies for energy sector.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessment**: through two evaluation tests; one launched at the beginning of the seminar (pre-assessment), and another (with the same evaluation content as the first test) at the end of the seminar (post-assessment) to verify that the new knowledge has been correctly acquired. Likewise, learners will have report analysis about specific case studies focused on the energy sector.
Training Provider *Name(s) of training providers.*	CNR and UMA.
Contact *Name(s) of the main contact person and their email address.*	• Artsiom Yautsiukhin, CNR, artsiom.yautsiukhin@iit.cnr.it • Javier Lopez, Full Professor, Unviersity of Malaga, Spain, javierlopez@uma.es • Cristina Alcaraz, University of Malaga, Spain, alcaraz@uma.es
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.

Duration *Duration of the training.*	Approximately 2 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual or both. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA3 – Cybersecurity Risk Management. Nonetheless, minor content matches with other including: • KA1 – Cybersecurity Management. • KA4 – Cybersecurity Policy, Process, and Compliance.
Pre-requisites	Basic knowledge of cybersecurity essentials (related to CSP Module 1) and IT.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief information Security Officer (CISO). • ECSF Profile 3: Cyber Legal, Policy & Compliance Officer. • ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 10: Cybersecurity Risk Manager.

Tools to be used *A list of tools that will be used for the operation of this training module.*	PPT for presentations, SATRA tool/service.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Spoken: English, Italian or Spanish. • Language for the material and the assessment/evaluation: English.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.3.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Threats and Vulnerabilities for Energy Sector	• Vulnerabilities for the energy sector. List and description of various cyber security threats which can be caused by internal or external attackers, as well as incidental and environmental attacks. • Vulnerabilities and security controls for the energy sector. List and discussion about ISO 27002 controls and their effect on threats in the energy sector.

Topic-2: Risk Assessment and Management Processes and Methodologies for Energy Sector	• Risk assessment and related terms. Define risk assessment and the related terms, with application and impact in the energy sector and its operational systems. • Risk assessment process. Describe the main steps of the risk assessment process. • Risk analysis. Describe different forms of risk analysis and ways to perform it. • Tools for risk assessment. Present various tools and approaches which could be helpful in conducting risk assessment. • Risk treatment. Introduce the four risk treatment options with a particular focus on risk reduction in the energy sector and its operational systems.

3.3.2.3 Planning for Preparedness

All preparedness activities are planned and coordinated among the trainers before the start of the seminar. To do so, the trainers will coordinate a predefined action plan to be carried out during the 2 hours of the module, assigning responsibilities per activity and time (e.g. Topic 1/2 - responsible and estimated time). Among the actions to be pre-established, two assessment tests with the same contents will be pre-configured, one at the beginning of the seminar and one at the end, as well as some reflection activities or use cases, which will be evaluated and reported later to the trainers.

The action plan will be established at least one week in advance to allow the trainers to have sufficient time to implement or prepare their respective actions. In addition, all materials will be available in advance, and the trainers will provide - whenever possible - multiple types of additional resources and materials to assist in the learning process (e.g. additional videos, URLs, references to books or scientific papers, etc.).

3.3.2.4 Materials and Exercises

As discussed previously, the CSP003_S_E trainers will follow a detailed action plan to ensure that all materials, tests, and exercises are ready before the launch of the module. This involves (i) reviewing the platform, (ii) identifying possible improvements or optimisations of the contents (slides, assigments, tests, etc.) as well as possible updates or new material. This way of operating will also allow the trainers to have the seminar completely updated within the DCM plataform, and at all times, according to the characteristics and preferences of the learners; e.g. according to the assessment forms and comments collected from learners in previous editions.

3.3.2.5 Verification of Learning Outcomes, and Skills

Considering that this module has a duration of 2 hours, the CSP003_S_E seminar mainly evaluates the formative knowledge by comparing mainly the results obtained from two tests carried out during the two training hours: (i) the pre-assessment test and (ii) the post assessment test. Both tests will contain the same questions and the same answers in order to understand the level of new knowledge acquired by the learners. Likewise, the reflections provided through the reports will also be key to verify that this knowledge maintains a more practical vision, and learners are able to identify problems and tentative risks (skills and competencies) within the energy sector and their respective control infrastructures.

Last but not least, the evaluations made to the trainers and to the module in general will also be key to maintain an updated and dynamic system for the following editions of the seminar.

3.4 Module 4 - Network Security for Energy

3.4.1 CSP004_C_E: Network Security for Energy

3.4.1.1 Description of Training Module

This module provides a comprehensive overview of network security essentials for the energy sector. The target audience for this module is IT administrators, engineers, and developers. The module offers a thorough introduction to Linux administration, network security, basic structure of attacks, theory about cryptography, hashes, cryptographic algorithms, basics web attacks. It also offers hands-on experience with laboratory exercises which involve several types of attacks and analysing network capture files for better understanding of network traffic protocols and attacks.

Code *Code format: CSP004_x where x is the training of offering type (see below)*	**CSP004_C_E**
Module Title *The title of the training module*	**Network Security for Energy**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers.*	• Computer Networks Protocols, Vulnerabilities, and Linux Prerequisites for efficient Administration and setup.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	• C (Course). • O (Lab).
Level *Training level:* *B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The module aims to provide network administrators with an overview of basic knowledge of network protocols, network, and web attacks, Linux commands to administer networks and basic cryptography theory.

Module description *Indicates the main purpose and description of the module.*	The module provides an understanding of what are the network protocols, how the work (according to the Request For Comment (RFC) standards), known vulnerabilities and policies that should be applied to protect data and networks. Also, there are labs for some hands-on experience in order to display real time how networks operate on real time scenarios, demonstrate security breaches, prevention methods and live policies that could be applied for prevention and remedy in case of an exploit.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:** • Demonstrate knowledge and understanding of networks, security, and Linux admin policies. • Gain knowledge about vulnerabilities, applying patches or settings to prevent them. • Usage of industry tools to do all the above. • Learn about basic security vulnerabilities, reverse engineer attacks, and learn defence mechanisms. **Skill and Competence:** • Computer Science focused on network protocols and security. • Knowledge of Linux Operating System (OS) and use of terminal focusing to administer networks and servers. • Audit networks. • Theoretical knowledge and reproduction security breaches. • Methods to prevent the above security issues. • Conditional data access and security methods to secure data. • Cryptography and cryptographic algorithms.
Main topics and content list *A list of main topics and key content*	• Network basics. • Linux OS introduction. • Usage of Linux OS for network administration. • Vulnerabilities. • Security breaches. • Operating system security basics • Introduction to Domain Name System (DNS), web threats and vulnerabilities, man-in-the-middle attacks. • Introduction to cryptography, terminology used, ciphers, cryptographic engineering, basic cryptographic protocols (public key encryption).

Evaluation and verification of learning outcomes. *Assessment elements and high-level process to determine participants have achieved the learning outcomes.*	• Mandatory attendance of all theoretical lessons. • Lab exercises. • Oral examination.
Training Provider *Name(s) of training providers.*	TUBS.
Contact *Name(s) of the main contact person and their email address.*	• Antonios Ntib: antonios.ntib@tu-braunschweig.de
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity* *(e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration. *Duration of the training.*	• 12 academic hours (1 semester). • 10-12 Labs.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing*	Mainly: • KA-5: Network and Communication Security. • KA-7: Cybersecurity Threat Management. • KA-8: Cybersecurity Tools and Technologies. • KA-9: Penetration Testing. • KA-10: Cyber Incident Response.

KA10 – Cyber Incident Response	
Pre-requisites	None and/or Basic IT and security knowledge, programming knowledge, usage of Linux distributions.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 2: Cyber Incident Responder. • ECSF Profile 4: Cyber Threat Intelligence Specialist. • ECSF Profile 5: Cybersecurity Architect. • ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 12: Penetration Tester.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Nmap, Lynis, Aircrack-ng, Hydra, Wireshark, Metasploit, Skipfish, Nessus, Burp Suite Scanner, BeEF, sqlmap, Apktool, John the Ripper, King Phisher, Yersinia, Social Engineering Toolkit, Linux terminal commands.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English.
ECTS *If applicable, the number of ECTS.*	3.2 ECTS.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.4.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Basic network fundamentals, architectures and protocols	• Basic Linux prerequisites, basic Linux network commands. • Networking principles and basics.

Topic-3: Web and Software Security	• Introduction to DNS, threat and vulnerabilities, web threats, man-in-the-middle attacks. • Software vulnerabilities.
Topic-4: Threat modelling and hunting	• Malware analysis. • Man-in-the-middle attacks. • Symbolic execution.
Topic-4: Cryptography	• Introduction to cryptography, terminology used, ciphers, cryptographic engineering, basic cryptographic protocols (public key encryption)
Topic-5: Operating System Security Basics – Access Control	• OS policies, user policies on Unix/Linux OSs, etc.

3.4.1.3 Planning for Preparedness

Preparedness of the course CSP004_C_E involves trainers to gather the student online or with physical appearance or combination of both for the theoretical part. Theory can be taught using the slides that are uploaded to the DCM platform.

As for the laboratory exercises, what is needed is either a physical laboratory with PC running some Linux distribution such as Ubuntu and/or Kali Linux either directly installed on bare metal or using a Virtual Machine (VM). Also, according to the audience that will enrol to this course servers running VMs, that will play the role of the "victim" and the role of the router using software such as pfsense. The servers in combination with the terminals of the laboratory will be setup in isolated VPN network that also could be accessed remotely via PtP Wireguard VPN, that students will access using specific certificates issued by the trainers and temporary credentials. The terminals that could be used for the lab exercises could either be PC already existing in a lab setup or even laptops of the students. Wireguard VPN will also offer the capability for students to attend the labs from distance. Wireless access points should also be deployed in the lab in order for students to execute Wi-Fi specific attacks.

3.4.1.4 Materials and Exercises

The training module is supported by the following material:

- Presentation material that will be used during the course and be provided digitally to the learners.
- Labs.
- This module requires from students to have a laptop, an Internet connection, if possible a fast one with low latency. This way the students will be able to download the material and do the laboratory exercises in case they want to attend remotely.

3.4.1.5 Verification of Learning Outcomes, and Skills

The verification of learning outcomes and skills will be mostly determined during the laboratory exercises. Students will be assessed in terms of their capability to successfully follow the laboratory exercises and if they have attended all theoretical lessons and all lab exercises. During the labs, learners will be observed if they can follow the instructions given by the trainers without having difficulty to do so. In successful attendance of the course, learners will get the certificate of attendance.

3.4.2 CSP004_C_E: Network Protection for Energy Control Systems

3.4.2.1 Description of Training Module

CPS004_C_E consists of an intensive course, the objective of which is to reinforce security knowledge but from a practical and advanced point of view. Therefore, the module is designed for engineers and IT/OT administrators in charge of managing control networks, and energy professionals with some knowledge of cybersecurity, including among others human operators, managers and directives, energy suppliers, and employees in general of the corporate network. Also, the course can also be taken by students of industrial engineering or computer sciences, researchers, and educators in the field of energy with some knowledge of cybersecurity.

Code *Code format: CSP004_x where x is the training of offering type (see below)*	**CSP004_C_E**
Module Title *The title of the training module*	**Network Protection for Energy Control Systems**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Network Security Management for Energy Control Systems. • Secure Management of Energy Control Networks and Substations. • Energy Control Network Threat Prevention.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).
Level	Advanced (A).

Training level: B (Basic), A (Advanced)	
Module overview *High-level module overview*	This course aims to provide a clear vision and understanding of current needs, especially those related to the secure deployment of energy control networks and access to their data. The idea is then to show and provide the minimum tools to not only protect communication channels and hosts, but also to give guarantees of "*defence in depth*" (only at communication level).
Module description *Indicates the main purpose and description of the module.*	The proposal of this course is to provide a clear understanding of the threats in power control networks to subsequently understand the main security weaknesses of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols and their impact on critical communication networks. To this end, we will also study the security issues of industrial communication protocols and the implications they have on the implementation of TCP/IP protocols such as telnet or File Transfer Protocol (FTP). From this study, we will proceed to analyse the security protocols of the TCP/IP stack and their guarantees for providing secure industrial communication channels, as well as all those perimeter defences, considering intrusion detection systems, monitoring systems and firewalls (at host level).
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, learners will have gained the following: **Knowledge:** • Knowledge of the most common vulnerabilities and threats in specific network systems and their associated protocols – not only in terms of TCP/IP protocols but also those applied in industrial communication networks. • Knowledge of the most relevant security protocols such as Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) or IPSec, and their importance for the protection of systems and communication networks. • Knowledge of the most relevant security mechanisms such as IDS/IPS to protect network perimeters and access to private domains, such as corporate networks • Knowledge of the most relevant security mechanisms to protect the end points of a communication, considering, for example, firewalls. **Skills:** • Analyse communication scenarios deployed in energy substations or control networks, and identify possible misconfigurations or vulnerabilities that could lead to security risks or threats.

	• Configure systems following the basic security principles (e.g. user control, port control, etc.). • Identify and apply those security elements or mechanisms that contribute to improving the security of a communication system. **Competencies:** • Know how to identify possible misconfigurations or errors that may lead to significant security risks with a serious impact the energy sector. • Lead the configuration and deployments of secure communication systems for specific energy communication scenarios. • Take own criteria under critical thinking to identify and apply existing security technologies, mechanisms, and protocols to protect the communications of the charging stations and related infrastructures.
Main topics and content list *A list of main topics and key content*	• 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.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Knowledge-based assessment**: through an evaluation test at the end of the course, in addition to performing some practical actions and tasks addressing case studies and practical activities, which should be reported. The idea is that learners will have the opportunity to reflect, analyse and implement specific activities (e.g. analysis of network traffic traces, configurations with errors, etc.), taking into account the application scenario and its level of criticality.
Training Provider *Name(s) of training providers.*	UMA and AIT.
Contact *Name(s) of the main contact person and their email address.*	• Dr. Cristina Alcaraz, University of Malaga, Spain, alcaraz@uma.es • Dr. Abdelkader Shaaban, AIT, Austrian Institute of Technology, abdelkader.shaaban@ait.ac.at
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.

Duration *Duration of the training.*	About 2 weeks, 20h for teaching. But the course probably is extended depending on the practical activities.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual or both. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA5 – Network and Communication Security Nonetheless, minor content matches with other including: • KA7 – Cybersecurity Threat Management. • KA9 – Penetration Testing.
Pre-requisites	Basic knowledge of IT, cybersecurity essentials (related to CSP Module 1), and experience with operating systems, network configurations and communication protocols.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 5: Cybersecurity Architect. • ECSF Profile 12: Penetration Tester.
Tools to be used	GNS3 Client and VM, Kali Linux, Virtualbox, Arpspoof, Bettercap, Wireshark, CloudShark, Hping3, xarp, Arpwatch, Suricata, Snort, Snort Analyzer, Raspberrypi Linux Image,

A list of tools that will be used for the operation of this training module.	pyModbusTCP, ufw, OpenVAS, Nmap, Nmap-vulners, IPtables, nftables, iPerf3, Scapy, Hydra, Zenmap, Etherape, legion, Ettercap, Vsftpd (ftp client-server), telnet (client-server), fping, ping, ss, OpenVPN/Wireguard, Metasploitable2 VM, Snorpy, the online CVSS 3.0/3.1 calculator, other open-source VPN tools for testing, among others.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Spoken: English. • Language for the material and the assessment/evaluation: English.
ECTS *If applicable, the number of ECTS.*	1.8 - 2.2 ECTS (according to the online ECTS Calculator).
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.4.2.2 Adapted Syllabus

Main topics	Suggested Content

Topic-1: Introduction to Energy Control Network Protection	• Introduce the application scenario (networks, components, protocols) and its scope. • Motive the problem by exposing the main security challenges of power control systems when the new information technologies (mainly with access to the Internet and wireless communication) arise within the operational ecosystems (e.g. cloud/edge computing, IIoT, remote control, blockchain). • Classify threats in energy control networks and real cases (e.g. due to supply chain). To do so, specific repositories such as MITRE ATT&CK (for Industrial Control Systems – specifically looking at those related to energy) and taxonomies will be considered and explored by students. • Case studies and analysis.
Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks	• Highlight the main security weaknesses of the control networks, and particularly of their communication protocols such as ModbusTCP and its lack of security for confidentiality. • Highlight the main security weaknesses of some TCP/IP communication protocols such as Hypertext Transfer Protocol (HTTP), FTP, Telnet, TCP, User Datagram Protocol (UDP). The idea is to show the main weaknesses if industrial communication protocols are applied together with unsecure TCP/IP communication protocols. • List a few typical offensive tools against confidentiality, integrity, and availability, and practical exercises to understand the weaknesses mentioned in the previous point.
Topic-3: Essential Protection for Energy Control Networks	• Provide an overview of the main TCP/IP security protocols such as TLS, IPSec and Secure Shell (SSH), and how they can be adapted in operational networks. • Explore security measures for endpoints like Human-Machine Interfaces (HMIs), analysing specific vulnerabilities (e.g. unsecured open ports and Common Vulnerabilities and Exposures (CVEs)), as well as configuring firewall rules at the operating system level (Linux) to prevent possible intrusions. • Practical exercises.
Topic-4: Advanced Protection for Energy Control Networks	• Introduce intrusion detection mechanisms and techniques to later specify detection rules at the network level where communication is based on industrial communication protocols such as ModbusTCP. • Provide 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.

3.4.2.3 Planning for Preparedness

All preparedness activities have already been planned according to an action plan and from the design of the syllabus, considering in this case a two-week intensive course (with approximately 20 hours in total) with practical contents. This also means that the action plan not only addresses the topic to be covered each day, but also assigns trainers to the corresponding topics and for certain execution times (e.g. Topic *x* - responsible person *y* and estimated time z).

As the course is of intensive character and has a mainly practical focus, materials, resources, and any additional support must be updated in the DCM platform in advance – either the course as a whole or the topic to be taught in the following section. This will allow learners to continue with their respective individual activities proposed for each day and for each session.

3.4.2.4 Materials and Exercises

As indicated in the previous section, trainers will have to take into account the plan of action established from the design of the syllabus in order to ensure that all materials, tests, and exercises are available before the launch of the module or for the following session. As part of the preparedness plan and in order to ensure a dynamic DCM platform, this platform will have to be sufficiently up to date, and trainers will have to:

- Review the platform and its contents on a daily basis;
- Be attentive to learners' doubts by making available interactive resources (such as forums, chats, text messaging, etc.) that facilitate learners' interaction with each other or with the trainer; and
- Verify that the access and interaction of learners is adequate to the respective resources, in order to ensure the availability of materials and exercises at all times.

All materials have a practical focus, allowing learners to investigate and apply security tools between OT/IT components, such as a master and a slave (or a SCADA server and a controller) operating, for example, in ModbusTCP.

3.4.2.5 Verification of Learning Outcomes, and Skills

This module primarily assesses problem-solving skills, identifying solutions and addressing actions to avoid drastic situations. This also means that learners will have to deploy and work in a virtualised OT/IT environment in which they will have to deal with a set of specific activities as well as reflexive tasks exposing specific situations or use cases. Verification of learning outcomes will therefore depend on the ability to solve problems, the level of resolution, and the ability to adapt existing techniques and tools to prevent, detect and mitigate situations.

Similarly, evaluation of the module and trainers will help to improve the quality of the module in subsequent sessions, ensuring continuous improvement and optimisation of the materials (slides, pdf, videos, links, etc.), exercises and teaching techniques.

3.5 Module 5 - Data Protection and Privacy Technologies for Energy

3.5.1 CSP005_C_E: Data Protection and Privacy Technologies for energy

3.5.1.1 Description of Training Module

CPS005_C_E focuses mainly on the development of specific skills on data privacy, providing knowledge about existing data protection and privacy techniques. Therefore, this course is primarily intended for implementers, but any aspiring cybersecurity practitioner or anyone interested in this field could also consider it.

Code *Code format: CSP005_x where x is the training of offering type (see below)*	**CSP005_C_E**
Module Title *The title of the training module*	**Data Protection and Privacy Technologies for energy**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Privacy Technologies. • Privacy by Design. • Data Security and Protection. • Data Privacy. • Privacy and Online Rights.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).
Level *Training level: B (Basic), A (Advanced)*	Basic (B).
Module overview *High-level module overview*	This module will provide a course for data protection and privacy for energy.
Module description *Indicates the main purpose and description of the module.*	The module provides techniques for data security policies and tools in energy.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Data protection best practices: gain knowledge of effective data security measures, data retention and deletion practices, and data breach response plans.

	• Emerging trends: recognise the impact of new technologies (e.g. AI, Big Data) on data privacy and ethical considerations. **Skills:** • Security policy and procedure development: define and implement data security policies and procedures, including access control and MFA. • Data anonymisation and sharing techniques: apply Privacy-Enhancing Technologies (PETs) to anonymise data and enable secure data sharing. **Competencies:** • Critical thinking: analyse complex data privacy scenarios and recommend appropriate solutions.
Main topics and content list *A list of main topics and key content*	• Data Protection Lifecycle Management. • Privacy-Enhancing Technologies (PETs).
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Questionnaire at the end of the seminar.
Training Provider *Name(s) of training providers.*	CNR.
Contact *Name(s) of the main contact person and their email address.*	• Fabio Martinelli: Fabio.Martinelli@iit.cnr.it.
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	2 hours.

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA6 – Privacy and Data Protection
Pre-requisites	Basic IT training + suggested minimum know-how in above section.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 8: Cybersecurity Implementer.
Tools to be used *A list of tools that will be used for the operation of this training module.*	PPT for presentations.
Language	English or Italian.

Indicates the spoken language and the language for the material and the assessment/evaluation.	
ECTS *If applicable, the number of ECTS.*	N/A
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.5.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Data Protection Lifecycle Management	• Data security and technical safeguards: encryption, access controls, incident response.
Topic-2: Privacy-Enhancing Technologies (PETs)	• Introduction to PETs and their role in data protection.

3.5.1.3 Planning for Preparedness

No initial knowledge is required to follow this course.

3.5.1.4 Materials and Exercises

The training course is supported by the following material:

- Presentations that will be used during the course and be provided digitally to the learners from the DCM platform

3.5.1.5 Verification of Learning Outcomes, and Skills

An optional questionnaire on-line will be provided for checking the outcome for attendees willing to test it.

3.5.2 CSP005_S_E: Data Protection and Privacy Technologies for Energy

3.5.2.1 Description of Training Module

In this training module the students are going to learn several policies and rules on how to administer users in an energy infrastructure in order to keep the representative business/organisation secure. Also, encryption methods will be presented in order to be applied to a corresponding infrastructure. Access control methods, mandatory GDPR policies and integrity protections will be presented that are necessary for the energy sector.

Code *Code format: CSP005_x where x is the training of offering type (see below)*	**CSP005_S_E**
Module Title *The title of the training module*	**Data Protection and Privacy Technologies for Energy**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Computer Infrastructure: Privacy Policies & Data Protection.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	• Seminar (S). • Other (O): Lab.
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The module aims to provide policies to administer in a secure way computer networks, data and users in order to prevent any data leaks and unauthorised access.

Module description *Indicates the main purpose and description of the module.*	The module provides a presentation of good practises on higher level in order to help personnel of the energy sector to protect the data and the privacy of the users of an energy grid, additionally to the organisations and business of the energy providers.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module, learners will be expected to be able to: **Knowledge:** • Methos, rules and policies applied in the computer network and network connected SCADA networks between energy sector business and organisations. **Skill and Competence:** • Learning to administer and setup security devices. • Knowledge of Linux OS and use of terminal focusing to administer networks and servers. • Setup servers and networks to avoid leaks and breaches. • Encryption algorithms and methods.
Main topics and content list *A list of main topics and key content*	• Security Protocols. • Encryption. • Methods of authorisation. • Policies of data handling. • Security models: integrity, confidentiality, and protection of the data. • GDPR necessary policies. • Introduction to access control types.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• Mandatory attendance. • Oral examination.
Training Provider *Name(s) of training providers.*	TUBS.
Contact *Name(s) of the main contact person and their email address.*	• Antonios Ntib: antonios.ntib@tu-braunschweig.de

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	10-12 academic hours (1 semester).
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both (please check the DCM platform).
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-1: Cybersecurity Management. • KA-2: Human Aspects of Cybersecurity. • KA-4: Cybersecurity Policy, Process, and Compliance. • KA-6: Privacy and Data Protection. • KA-8: Cybersecurity Policy, Process, and Compliance.
Pre-requisites	Basic IT and security Knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles*	• ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 7: Cybersecurity Educator. • ECSF Profile 8: Cybersecurity Implementer. • ECSF Profile 3: Cyber Legal, Policy & Compliance Officer. • ECSF Profile 5: Cybersecurity Architect.

needs this module.	
Tools to be used *A list of tools that will be used for the operation of this training module.*	mdadm, sssd, and Nikto.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English.
ECTS *If applicable, the number of ECTS.*	2.0 ETCS.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.5.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Data Privacy Methods and Architectural Policies and Rules to secure data	• Principles for user authentication. • Linux/Unix access control principles (Bell – LaPadula model). • Public key encryption, digital signatures, Public Key Infrastructure (PKI) technology & interoperability, cryptography, ciphers, perfect secrecy, IND-CPA security, hash functions. • HSM (Hardware Security Modules). • Integrity protection models. • Trusted Computer System Evaluation Criteria (TCSEC) and common criteria. • Data Privacy.

	• GDPR policies. • Operating system Security basics – access control.

3.5.2.3 Planning for Preparedness

CSP005_S_E is mainly theoretical. Students need to download the corresponding material from the DCM platform, have a laptop and an internet connection to either attend remotely or physically. The seminar can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar). Trainers should just define a time schedule for teaching the course.

3.5.2.4 Materials and Exercises

The training seminar is supported by the following material:

- Presentations that will be used during the course and be provided digitally to the learners from the DCM platform.

3.5.2.5 Verification of Learning Outcomes, and Skills

Learners should attend all lessons to get a certificate of attendance.

3.6 Module 6 - Cyber Threat Intelligence for Energy

3.6.1 CSP006_C_E: Cyber Threat Intelligence in the Energy Network

3.6.1.1 Description of Training Module

The CSP006_C_E course is a comprehensive training programme designed to equip participants with the necessary skills to address cybersecurity challenges specific to the energy sector, particularly in the context of emerging technologies like IoT, blockchain, and AI. The course curriculum covers a wide range of topics, from the foundations of cyber threat intelligence and threat modelling to advanced topics like anomaly detection and the practical application of threat modelling and security investigation. Each module of the course includes both theoretical knowledge and practical exercises, utilising advanced cybersecurity toolkits and software platforms to simulate real-world scenarios.

The course prepares participants through a blend of formative assessments, which provide ongoing feedback, and summative assessments, which test their ability to apply what they've learned in practical settings. Materials for the course are carefully prepared in advance and are accessible on the DCM platform, ensuring that all participants, regardless of their previous knowledge level, can follow along and benefit from the training.

CSP006_C_E is intended for professionals in the energy sector who are involved in or responsible for cybersecurity, including technology managers, engineers, policy makers, and security practitioners. It is also suitable for participants who are new to the energy sector but have a background in cybersecurity, providing them with an understanding of the specific cybersecurity challenges and solutions in the energy context. This makes the course highly relevant for anyone looking to enhance their capabilities in securing emerging technologies within the energy network.

Code *Code format: CSP006_x where x is the training of offering type (see below)*	**CSP006_C_E**
Module Title *The title of the training module*	**Cyber Threat Intelligence in the Energy Network**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cybersecurity Intelligence Collaboration. • Security Threat Information Sharing. • Cyber Threat Analysis and Collaboration in the Energy Domain. • Intelligence-driven Cyber Defence in the Energy Domain. • Threat Information Collaboration. • Collaborative Threat Mitigation in the Energy Domain. • Intelligence-led Cybersecurity. • Cybersecurity and Threat Hunting in the Energy Domain.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).
Level *Training level: B (Basic), A (Advanced)*	Advanced (A).
Module overview *High-level module overview*	This training module aims to provide learners with an overview of threat intelligence and management in the energy domain. It allows the learners to analyse the known and unknown threats and determine a course of action to tackle them.
Module description *Indicates the main purpose and description of the module.*	This training module explains the underlying properties and principles associated with cyber threats within an energy organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this course, learners will be able to demonstrate: **Knowledge:** • Demonstrate knowledge and understanding of threats to an energy information and network system. • Taxonomy of cyber threats, actors, and motivations. • Threat intelligence lifecycle and its components. • Variety of threat intelligence sources and their strengths/weaknesses. • Security controls and standards relevant to specific threats. • Vulnerability assessment techniques and tools. • Effective communication and dissemination of threat intelligence. • Ethical and legal considerations surrounding Cyber Threat Intelligence (CTI) acquisition and use. • Knowledge on available data sources and collections, how to validate them and how to use the data. • Understand how to identify potential threat actors and analyse their tactics. • Knowledge of different threat modelling approaches and an understanding of potential cyber threats and vulnerabilities that could lead to cyber-attacks. **Skills:** • Analyse and interpret various sources of threat intelligence. • Conduct threat modelling and identify vulnerabilities in systems. • Apply advanced analytical techniques to identify and prioritise threats. • Disseminate actionable threat intelligence to different audiences. • Evaluate and select CTI tools and platforms based on specific needs. • Align security controls and standards with identified threat profiles. • Communicate threat intelligence effectively in written and verbal formats. • Conduct ethical threat research and responsibly disclose vulnerabilities. **Competencies:** • Critical thinking and problem-solving in the context of cyber threats. • Ability to analyse complex data and identify patterns and trends. • Effectively collaborate and share information with diverse stakeholders. • Adapt to evolving threat landscapes and technologies.

	• Make informed decisions based on threat intelligence. • Maintain ethical and responsible practices in CTI activities.
Main topics and content list *A list of main topics and key content*	• Foundations of cyber threat intelligence (CTI)-taxonomy, lifecycle, security controls and standards. • Threat modelling and analysis in the energy network. • Energy data sources and collection. • Energy data analysis and data processing. • Threat actors and tactics in the energy network. • Vulnerabilities assessment techniques. • cyber threat intelligence information sharing, Dissemination, communication, and implementation. • Anomaly detection in the energy network. • Practical threat modelling and security investigation.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment**: learner needs to develop a logbook based on the individual energy exercise covered at the end of each session to demonstrate their understanding of the knowledge covered by the module. • **Summative assessment**: learner needs to produce a 2000-word report at the end of the module by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to tackle the threats based on a energy real-world scenario.
Training Provider *Name(s) of training providers.*	FCT.
Contact *Name(s) of the main contact person and their email address.*	• José Manuel Fonseca: jmrf@fct.unl.pt
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	9 weeks.

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical or virtual. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA7 – Cybersecurity Threat Management and some minor topics from: • KA1 – Cybersecurity Management. • KA8 – Cybersecurity Tools and Technologies.
Pre-requisites	Basic IT and Security Knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 2: Cyber Incident Responder. • ECSF Profile 4: Cyber Threat Intelligence Specialist. • ECSF Profile 8: Cybersecurity Implementer. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Servers, presentation files, VPN to access the lab server and execute the exercises.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Portuguese.

ECTS *If applicable, the number of ECTS.*	TBD.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.6.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Foundations of Cyber Threat Intelligence (CTI)	• Cyber threats taxonomy: classification of threats, threat actors, and motivations. • Threat intelligence lifecycle: collection, analysis, dissemination, and feedback loop. • Sources of threat intelligence: Open-Source Intelligence (OSINT), commercial feeds, malware analysis, vulnerability databases. • Security controls and standards: aligned with identified threats. • Goals of security control, security control types, security control functions, access control properties, patch management, CIS (Critical Security Controls).
Topic 2: Threat Modelling and Analysis in the Energy Network	• Identifying and prioritising assets: understanding energy critical infrastructure and data. • Attack vectors and threat actors: exploiting vulnerabilities and analysing adversary capabilities. • Threat hunting: proactively searching for malicious activity within networks.
Topic 3: Data sources and collection	• Overview on different types of energy data sources. • Validation and verification of energy data as well as processes for preparing and processing the collected information.

	• Automation techniques and tools to optimise energy data source collection and scalability.
Topic 4: Energy Data analysis and processing	• Energy data processing techniques and advanced analytics techniques (data mining and machine learning). • visualisation and big data tools.
Topic 5: Threat actors and tactics in the Energy Network	• Known threat actors, their motives, Tactics, Techniques and Procedures (TTPs). • Identify and classify threat actors. • Analyse the different tactics, techniques and procedures.
Topic 6: Vulnerabilities Assessment Techniques	• Basic of vulnerability, vulnerability groups, vulnerability exploitation, zero-day exploit. • Vulnerability types. • Identifying and prioritising energy system vulnerabilities. • Vulnerability exploitation.
Topic 7: Cyber Threat Intelligence Information Sharing, Dissemination, Communication, and Implementation	• Tailoring intelligence to different audiences: delivering actionable insights to decision-makers. • Threat reports and briefings: communicating threat intelligence effectively. • Collaboration and information sharing: sharing intelligence within and across organisations. • Developing and implementing a CTI programme: defining goals, roles, processes, and metrics. • Security controls and standards implementation: mitigating risks based on identified threats.
Topic 8: Anomaly detection in the Energy Network	• Basic concepts of anomaly detection. • Understanding how to identify and deal with anomalies in different data sources. • Real-time anomaly detection in large data streams. • Introduction to tools and techniques to detect, classify, and respond to anomalies in real time.
Topic 9: Practical Threat Modelling and Security Investigation	• Overview of threat modelling approaches to identify security vulnerabilities in a system design. • Automated estimation of risk, assessment of risk level.

3.6.1.3 Planning for Preparedness

In anticipation of the "Cyber Threat Intelligence in the Energy Network" course (CSP006_C_E), all preparedness activities are intricately planned and coordinated among the trainers. An internal action table is utilised to delineate tasks, estimate time requirements, and outline the methodology and schedule for training actions. This includes detailing the roles and responsibilities clearly, ensuring efficient training delivery. Each training topic, such as "Foundations of Cyber Threat Intelligence" or "Threat Modelling and Analysis in the Energy Network," has a designated lead trainer responsible for developing topic-specific presentations, overseeing practical activities, and creating tailored materials. These materials, which include videos and presentations, are aligned with the pedagogical approaches

suitable for each topic's nature and complexities. They are made available in advance on the DCM platform and other relevant course management systems to ensure a smooth training phase. Additionally, trainers are provided access to the DCM platform, fostering synchronisation and communication through various mediums, supporting an effective coordination strategy throughout the training period.

3.6.1.4 Materials and Exercises

Materials and exercises for CSP006_C_E are meticulously prepared in accordance with a detailed internal action plan, ensuring readiness before each module begins. The plan is crafted to offer a rich learning experience, tailored to the specific features and themes of each topic. For instance, the topic on "Vulnerability Assessment Techniques" includes practical actions based on game-based learning methodologies, setting specific time-frames, conditions, and formats for serious games. Similarly, other topics involve a diverse array of training approaches, including case studies, research analysis, and development of lab exercises, aimed at maintaining a basic level of instruction while facilitating progressive learning and inter-module connectivity. The practical nature of these exercises is designed to immerse participants in relevant situations within the energy sector, helping them understand specific issues and develop solutions. This module, in particular, aims to bridge experts in the energy sector with the field of cybersecurity and introduces essential elements of the energy ecosystem, promoting an atmosphere conducive to critical thinking and discussion.

3.6.1.5 Verification of Learning Outcomes, and Skills

The verification of learning outcomes and skills involves a combination of formative and summative assessments to ensure participants achieve the course objectives. Formative assessments occur throughout the training, offering timely feedback to both instructors and participants, facilitating ongoing learning adjustments. Summative assessments require participants to demonstrate their learning through practical tasks, such as threat and vulnerability assessments within real-world scenarios, reflecting the module's focus on practical application. To enhance training effectiveness, the course incorporates various forms of assessments that promote continuous improvement and optimisation of resources, exercises, and training methodologies. Additionally, towards the module's end, participants are encouraged to complete self-assessment forms to reflect on their learning experiences, while trainers evaluate various aspects of participant performance, including exercise execution and critical thinking during discussions. This comprehensive evaluation process helps in optimising content delivery and refining instructional methods for future sessions.

3.6.2 CSP006_S_E: Cyber Threat Intelligence and Threat Hunting in the Energy Domain

3.6.2.1 Description of Training Module

This seminar, which aims to cover some aspects of cyber intelligence and threat hunting, is designed for executives, managers, or employees in charge of critical energy domains. However, CPS006_S_E can also be taken by anyone else interested in the subject, such as aspiring cybersecurity professionals, researchers, or educators.

Code *Code format: CSP006_x where x is the training of offering type (see below)*	**CSP006_S_E**

Module Title *The title of the training module*	**Cyber Threat Intelligence and Threat Hunting in the Energy Domain**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cyber Threat Intelligence Approaches in the Energy Domain. • Threat Actors and Tactics for Energy Systems. • Cybersecurity and Threat Hunting for Energy Systems. • Threat Modelling Approaches for the Energy Domain.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S (Seminar).
Level *Training level: B (Basic), A (Advanced)*	A (Advanced).
Module overview *High-level module overview*	The seminar aims to provide critical infrastructure operators from the energy sector (power providers, transmission network operators, power plant operators, etc.) with an overview of threat intelligence and management. It allows the participants to analyse the known and unknown threats in the energy domain and determine a course of action to tackle them. Overall, this seminar provides participants with a solid foundation to effectively conduct threat analysis and defend against threats in energy network. They will be able to identify current attack techniques, proactively look for potential threats and take appropriate countermeasures to ensure the security of systems and data.

Module description *Indicates the main purpose and description of the module.*	Initially, the participants will obtain an overview on cyber threat intelligence and cyber threat hunting together, its main concepts and benefits with some special examples from the energy domain. Then, the seminar will focus on the main sources of information for threat intelligence, presenting some of the standard tools in that area and also discuss the specificities of data gathering within energy systems. Afterwards, the participants will get an overview on threat actors and tactics, covering classical approaches like the Cyber Kill Chain, the Cyber Attack Lifecycle and the MITRE ATT&CK framework. In the end, the seminar will give an overview on the threat modelling tool ThreatGet and its application possibilities in for energy systems and networks.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	A comprehensive understanding of the challenges, strategies, and best practices for identifying cyber threat intelligence data and threat actors in the energy domain, the ability to use common threat intelligence tools and to perform threat modelling for energy networks.
Main topics and content list *A list of main topics and key content*	• Introduction to threat intelligence and threat hunting. • Data sources and collection. • Threat actors and tactics. • Practical threat modelling and security investigation.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Knowledge-based assessments:** these assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery orally by the instructor.
Training Provider *Name(s) of training providers.*	AIT.
Contact *Name(s) of the main contact person and their email address.*	• Stefan Schauer: stefan.schauer@ait.ac.at • Abdelkader Shabaan: abdelkader.shabaan@ait.ac.at

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	4 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual or both.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-1: Cybersecurity Management. • KA-7: Cybersecurity Threat Management. • KA-8: Cybersecurity Tools and Technology.
Pre-requisites	Basic IT training + suggested minimum know-how in above section.

Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO).
Tools to be used *A list of tools that will be used for the operation of this training module.*	ThreatGet. Any other tool will be listed in the CyberSecPro DCM System.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English and German.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.6.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Data sources and collection	Different types of data sources such as public feeds, dark web, malware analysis, security blogs and social media are explained. Methods for identifying and selecting suitable data sources based on the specific requirements in the energy sector are taught. Automation techniques and tools to optimise data source collection and scalability will be covered. Current developments, trends and best practices in data source collection will be emphasised.
Topic-2: Threat actors and tactics	This topic focuses on the study of known threat actors, their motives, tactics, techniques, and procedures (TTPs) and their impact on different systems in the energy sector. The aim is to develop an in-depth understanding of potential threat actors facing energy systems. Participants will be able to identify and classify threat actors, analyse the different tactics, techniques and procedures, and examine their impact on industries and organisations. In addition, they should discuss preventive and defensive measures and be able to develop and implement effective security strategies
Topic-3: Practical Threat Modelling and Security Investigation	This part covers various threats and provides an overview of threat modelling approaches to identify security vulnerabilities in a system design. Therefore, ThreatGet, as the well-known threat modelling approach, will be utilised to investigate potential cyber threats that attackers can seize to exploit existing security vulnerabilities and reach a particular malicious goal. This comprehensive approach helps build a secure system design, verify its security, and prioritise the security measures to maintain cyber risk at an acceptable level.

3.6.2.3 Planning for Preparedness

As part of the early steps in the preparedness process, we circulated an initial table internally to consolidate all relevant module information. Subsequently, we collected inputs to define the module content and outline key topics. These inputs provide a high-level view of the module and offer insights and vision for all the topics presented for CSP006_S_E. Additionally, the table outlines the work methodology to be followed regarding tasks and the training schedule. Each module has a lead responsible for developing course tasks, which include creating presentations, organising practical activities, and defining materials. Hence, discussions with the module lead were held to negotiate and brainstorm topic details that align with the module's requirements. These discussions are essential to ensure the delivery of high-quality module content and to confirm that all proposed topics are consistent throughout the entire module, preventing repetition of content. As agreed, upon within the CyberSecPro consortium, the DCM platform for the course management system has been developed to manage all

agreed-upon topics for CyberSecPro materials efficiently. Therefore, all module presentations are stored on the DCM platform, which also facilitates the uploading of related materials, such as video teasers and final assessments. Additionally, the platform allows all module trainers to access and synchronise with others, aiding in the completion of planned training materials.

3.6.2.4 Materials and Exercises

To ensure the high quality of materials and meet the expectations of the previously discussed key topics and course objectives, we developed and integrated advanced materials covering different topics related to threat intelligence and threat hunting in the energy sector. This module includes the presentation of different categories of potential threats that threaten computer systems in the energy sector. Additionally, various types of intelligence can be utilised to characterise threats. Multiple open-source tools that facilitate sharing intelligence, automating responses, and leveraging the wide range of publicly available sources of Cyber Threat Intelligence have been included to provide more details on the module's topics and how to address such malicious activities in a critical domain like the energy sector. All related materials are gathered from various sources to provide a comprehensive learning experience for all participants, enabling them to engage with the defined course content that matches the module objectives. Additionally, the module includes various activities such as describing more specific case studies, conducting research analysis, holding open discussions, and identifying approaches/tools that can be used for actions related to each topic. This approach offers different interactive methods for the course activities, ensuring engagement and avoiding boredom among all participants.

Practical actions are also considered an essential activity of this module, which supports participants in becoming more engaged with activities related to cyber threats and in using approaches to determine potential cyber threats. For instance, as part of the activities of this module, a detailed discussion on the different threat modelling approaches to be conducted in the energy sector is included. Then, practical work with a threat modelling will be accompanied, allowing all participants to be actively involved in using threat modelling in some examples from the energy sector. Additionally, understanding how this approach helps in identifying unforeseen cyber threats and estimating cyber risks is crucial. These practical exercises will support the participants in applying all the lessons learned regarding their gained theoretical knowledge to apply the threat modelling approach to real-world scenarios, thereby enhancing cybersecurity critical issues in the energy domain. The partial interaction with the threat modelling will promote their understanding of analysing cyber threats and assessing risks in a more real-world scenario related to the energy sector.

3.6.2.5 Verification of Learning Outcomes, and Skills

Multiple assessments will be conducted throughout the course to ensure the full integration of all participants with the course content and to support the overall evaluation of the course. There are two main evaluations for each participant that must be conducted individually, as follows:

- Practical works: each participant will have to carry out a partial activity through a threat modelling tool to develop different examples in the energy sector. The participant will work deeply in investigating different potential threats and how to assess them to provide a clear way to mitigate cyber risk. This assessment will enhance the skills of the participant to give them a chance to provide a decision making on such cyber security issues that need attention for support in defining the mitigation strategies in examples which mimic real world scenario. This will also support the assessment of the participant's progress to ensure that all the theoretical knowledge discussed and presented in the course is reflected in the practical demonstration of the participant's skills.
- Final Assessment: at the end of the course, each student will have the opportunity to evaluate the skills they have acquired through the final assessment. This assessment will be available on our DCM platform, providing us as trainers with an effective way of tracking all activities

completed by students and ensuring that all learning progress is achieved in line with the key objectives of our module.

In addition, an open discussion among participants will be essential for focusing on the critical aspects of cybersecurity in the energy domain. This will support the improvement of critical thinking in participants, involving them in the problem and any possible solutions for mitigating cyber threats in the energy domain. On the other hand, it will also improve the environment of collaboration and knowledge sharing among all participants, ensuring the enhancement of their skills and the overall course outcomes. This will also significantly improve the evaluation of the course progress, providing an indication of the students' satisfaction with the course content. It will also give an impression of how any space for improvement in communication and interaction among participants can change the dynamics or activities of the discussion, such as the creation of small groups of participants to enhance communication activities. These groups will improve the integration of the participants into the discussion topics and give them more space for the improvement of their critical thinking skills in such a complex system as the energy sector.

The trainers are keen to ensure the continued success of the learning outcomes. Therefore, we will provide a comprehensive assessment after collecting all student exercises and final assessments. The trainer will then analyse this information to provide further evidence for improvement. This evaluation is essential for assessing the learning outcomes through the course content and the methods followed in teaching the course content. In addition to providing feedback from students regarding the course, their satisfaction, and their expectations of the course contents and trainers, this also provides a complete image for improvement and paves the way for giving more space to enhance the overall contents of the course and the methods followed for presenting the topics.

The whole evaluation process can be summarised as follows:

1. Self-assessment: each student in the CSP006_S_E will undergo a final assessment, allowing them to evaluate themselves and reflect on their learning experience.
2. Trainer evaluation: trainers will assess the outcomes of the course by evaluating various aspects, including:
   - Participant communication and interaction, focusing on critical thinking about possible solutions to mitigate cyber threats in the energy sector through open discussion or small group creation.
   - This evaluation process helps trainers gauge the comprehensiveness of the topics covered and identify areas for improvement, such as optimising content, intensifying instruction, or refining methods for developing knowledge and skills in future sessions.
   - Participant feedback: collect all feedback on course content and trainers to provide a space for improvement.
3. Certificate of attendance: upon successful completion of the seminar, participants will be eligible to receive a certificate of attendance. This certificate acknowledges their commitment to expanding their knowledge of the cybersecurity concepts covered in CSP, specifically within the energy sector context.

3.7 Module 7 - Cybersecurity in Emerging Technologies for Energy

3.7.1 CSP007_C_E: Cybersecurity in Emerging Technologies for Energy

3.7.1.1 Description of Training Module

The "Cybersecurity in Emerging Technologies for Energy" course is an advanced training module designed for professionals in the energy sector, including engineers, administrators, technology managers, and cybersecurity specialists. It equips participants with essential knowledge and skills to address the unique cybersecurity challenges that arise with the integration of cutting-edge technologies

such as the IoT, cloud computing, blockchain, and AI in energy systems. The course delves into a comprehensive examination of the cybersecurity landscape specific to these technologies, exploring detailed vulnerabilities, threat vectors, and the necessary security measures to safeguard energy infrastructures.

Targeting both seasoned professionals and those new to the field, the course is particularly beneficial for those involved directly or indirectly with the cybersecurity aspects of energy technologies. This includes individuals responsible for managing and securing infrastructure as well as policymakers and consultants who influence and implement security strategies within the energy sector. Through interactive lectures, hands-on labs, and discussions, participants gain profound insights into securing various emerging technologies, building upon foundational cybersecurity knowledge to develop advanced competencies in protecting interconnected energy systems.

Code *Code format: CSP007_x where x is the training of offering type (see below)*	**CSP007_C_E**
Module Title *The title of the training module*	**Cybersecurity in Emerging Technologies for Energy**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Security Challenges in Emerging Energy Technologies. • Protecting Emerging Tech: Energy Cybersecurity Considerations. • Securing Future Technologies: Energy Cyber Threats and Solutions. • Cyber Risks in Energy Emerging Tech Landscapes. • Safeguarding Innovation: Cybersecurity in New Energy Technologies. • Emerging Tech Security: Addressing Energy Cyber Threats. • Cyber Defence for Energy Emerging Technological Landscapes. • Ensuring Security in Cutting-Edge Energy Technologies. • The Intersection of Cybersecurity and Energy Emerging Tech. • Future Tech Security: Navigating Energy Cyber Challenges.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).

Level *Training level: B (Basic), A (Advanced)*	Advanced (A).
Module overview *High-level module overview*	The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge energy technologies. As the energy business embrace innovations such as the Internet of Energy (IoE), AI, blockchain, and 5G, robust cybersecurity measures become paramount. This module aims to provide a comprehensive understanding of the cybersecurity landscape within the energy context.
Module description *Indicates the main purpose and description of the module.*	This training module explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, equipping participants with the knowledge and skills needed to protect their environments. Through interactive lectures, hands-on labs, and discussions, participants will gain insights into energy securing various technologies like the IoT, cloud computing, blockchain, AI, and more. This advanced training delves deep into the intricacies of cybersecurity within the context of energy emerging technologies, building upon foundational cybersecurity knowledge.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon completing CSP007_C_E, trainees should be well-equipped to address the cybersecurity challenges posed by integrating AI, Cloud, and IoE technologies. They should possess a strong foundation of knowledge, practical skills, and ethical considerations necessary for securing energy interconnected systems in energy systems. Trainees are able to demonstrate following specific learning target including: **Knowledge:** • In-depth understanding of various emerging technologies (IoE, cloud, blockchain, AI, etc.) and their inherent security risks. • Comprehensive knowledge of energy specific vulnerabilities and attack vectors associated with each technology. • Solid grasp of established security principles and best practices applicable to emerging technology environments. • Knowledge of specialised security tools and methodologies for different emerging technology platforms.

	• Understanding of evolving threats and trends in the emerging technology security landscape. **Skills and competences:** • Critical thinking and problem-solving in complex energy emerging technology security scenarios. • Ability to analyse and interpret technical information and develop data-driven security solutions. • Effectively collaborate and communicate technical security concepts to diverse audiences. • Adaptability and agility in responding to the ever-changing emerging technology security landscape. • Strong decision-making skills based on comprehensive understanding of risks and best practices.
Main topics and content list *A list of main topics and key content*	• Introduction to cybersecurity in energy emerging technologies including IoE, cloud, blockchain, AI. • Anomaly detection techniques • Securing the energy emerging technologies (e.g. IoE, cloud, blockchain, AI) • Data analysis for cybersecurity in the energy network • Security tools and techniques for energy emerging technologies • The future of emerging technology security and its application in the energy network
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment**: ongoing process of evaluating participants' learning during a training programme including pre-assessment, during and post-assessment in each training topic. It provides valuable feedback to instructors and participants, helping to ensure that learning goals are being met and that participants are making progress. • **Summative assessment**: learner needs to produce a targeted outcomes and deliverables at the end of the training by performing a list of tasks to demonstrate the knowledge of the cybersecurity in emerging technologies applied to the energy network.
Training Provider *Name(s) of training providers.*	UNINOVA and LAU.
Contact *Name(s) of the main contact person and their email address.*	• Ruben Costa: rddc@uninova.pt • Paresh Rathod: Paresh.Rathod@laurea.fi

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	12 weeks.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical or virtual. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly • KA-8: Cybersecurity Tools and Technologies.
Pre-requisites	Basic programming skills, particularly in languages commonly used in cybersecurity, such as Python.

Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 4: Cyber Threat Intelligence Specialist. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 11: Digital Forensics Investigator.
Tools to be used *A list of tools that will be used for the operation of this training module.*	GDPR, HIPAA, Zero Trust, VPNs, RBAC, SSL/TLS, IPsec, SSH, MQTT.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Portuguese.
ECTS *If applicable, the number of ECTS.*	TBD.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.7.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Introduction to Cybersecurity in Energy Emerging Technologies	• Overview of emerging technologies and their impact on cybersecurity landscape. • Unique security challenges associated with different technology categories (IoE, cloud, blockchain, AI).

	• Regulatory and compliance considerations for energy emerging technologies.
Topic 2: Anomaly Detection Techniques	• Introduction to anomaly detection. • Machine Learning-based method. • Time series anomaly detection. • Anomaly detection in real-world energy-related applications.
Topic 3: Securing the Energy Emerging Technologies	• IoE architecture and its vulnerabilities. • Securing devices, networks, and data in IoE environments. • Best practices for managing IoE security risks. • Cloud security models and shared responsibility model. • Cloud-specific threats and mitigation strategies. • Understanding blockchain technology and its security properties. • Vulnerabilities and attack vectors specific to blockchain platforms. • Security risks associated with AI, including bias, data privacy, and adversarial attacks. • Methods for securing AI models and training data.
Topic 4: Data Analysis for Cybersecurity in the Energy Network	• Data-driven insights to effectively detect and respond to cyber threats. • Data analysis techniques and tools, and its application to energy cybersecurity scenarios.
Topic 5: Security Tools and Techniques for Energy Emerging Technologies	• Specialised security tools and frameworks for different energy emerging technologies. • Hands-on practice with tools for vulnerability scanning, threat detection, and security configuration in a energy network.
Topic 6: The Future of Emerging Technology Security and its application in the Energy Network	• Anticipating emerging threats and trends in the energy security landscape. • Developing a proactive approach to securing emerging technologies in the energy network.

3.7.1.3 Planning for Preparedness

Planning for preparedness is meticulously executed to ensure all trainers and materials are perfectly synchronised and tailored to meet the specialised demands of energy sector cybersecurity. An internal action table helps in coordinating the tasks, time management, and training methodology, facilitating a smooth and efficient training delivery. Each topic within the course has a designated lead trainer responsible for developing presentations, overseeing practical exercises, and creating customised materials which are made available well in advance through the DCM platform or relevant course management systems.

3.7.1.4 Materials and Exercises

Materials and exercises are designed to ensure a rich, interactive learning experience tailored to the specific features and challenges of each topic covered in the course. These include practical activities that use game-based learning methodologies and serious games with specific timeframes and conditions, as well as case studies, research analysis, and lab exercises. These materials are crafted to immerse participants in scenarios that reflect real-world challenges within the energy sector, allowing them to develop practical solutions to these problems.

3.7.1.5 Verification of Learning Outcomes, and Skills

Verification of learning outcomes and skills is conducted through a combination of formative and summative assessments. Formative assessments provide ongoing feedback throughout the training, helping to ensure that the learning goals are met and that participants are making consistent progress. Summative assessments require participants to demonstrate their knowledge and skills through practical tasks, such as threat and vulnerability assessments in simulated scenarios, reflecting the course's focus on real-world application. This robust assessment framework is designed to not only test the participants' understanding and skills but also to foster continuous improvement in training methodologies and resource optimisation.

3.7.2 CSP007_S_E: Cybersecurity in Emerging Technologies for the Energy Network

3.7.2.1 Description of Training Module

The "Cybersecurity in Emerging Technologies for the Energy Network" seminar is designed to address the unique cybersecurity challenges posed by emerging technologies such as the IoT, blockchain, and AI within the energy sector. The seminar includes a well-structured curriculum that covers various aspects of cybersecurity in emerging energy technologies, from foundational concepts to specialised security tools and proactive security strategies. The topics discussed include the impact of emerging technologies on the cybersecurity landscape, the architecture of IoE and its vulnerabilities, securing blockchain platforms, and mitigating risks associated with AI.

Preparation for CSP007_S_E involves meticulous planning to synchronise trainers and materials, emphasising a dynamic and adaptive training approach suitable for the evolving nature of cybersecurity in the energy sector. The seminar offers a blend of theoretical knowledge and practical exercises, including interactive simulations and real-world scenario testing, designed to enhance the problem-solving and critical thinking skills of participants.

The audience for CSP007_S_E typically comprises professionals in the energy sector who are either directly involved in cybersecurity roles or are stakeholders in the security process, such as technology managers, policy makers, and engineers. It is also suitable for participants from various professional backgrounds looking to gain a comprehensive understanding of cybersecurity challenges and solutions specific to emerging technologies in the energy industry. The seminar's focus is on equipping these professionals with the skills and knowledge necessary to effectively secure and manage cybersecurity risks in their respective domains, making it an essential training for those at the intersection of cybersecurity and energy technology.

Code *Code format: CSP007_x where x is the training of offering type (see below)*	**CSP007_S_E**
Module Title *The title of the training module*	**Cybersecurity in Emerging Technologies for the Energy Network**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Security Challenges in Emerging Energy Technologies. • Protecting Emerging Tech: Energy Cybersecurity Considerations. • Securing Future Technologies: Energy Cyber Threats and Solutions. • Cyber Risks in Energy Emerging Tech Landscapes. • Safeguarding Innovation: Cybersecurity in New Energy Technologies. • Emerging Tech Security: Addressing Energy Cyber Threats. • Cyber Defence for Energy Emerging Technological Landscapes. • Ensuring Security in Cutting-Edge Energy Technologies. • The Intersection of Cybersecurity and Energy Emerging Tech. • Future Tech Security: Navigating Energy Cyber Challenges.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	Basic (B).
Module overview *High-level module overview*	The training module is designed to provide participants with an overview of the unique challenges posed by integrating cutting-edge energy technologies. As the energy business embrace innovations such as the IoE, AI, blockchain, and 5G, robust cybersecurity measures become paramount. This module aims

	to provide an understanding of the cybersecurity landscape within the energy context.
Module description *Indicates the main purpose and description of the module.*	This seminar explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, providing the participants with an overview of how to protect their energy environments. It introduces the learner into energy securing various technologies like the IoT, cloud computing, blockchain, and AI.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon completing this seminar, trainees should be well-knowledge of the cybersecurity challenges posed by integrating AI, Cloud, and IoE technologies. Trainees are able to demonstrate following specific learning target including: **Knowledge:** • Understanding of various emerging technologies (IoE, cloud, blockchain, AI, etc.) and their inherent security risks. • Knowledge of energy specific vulnerabilities and attack vectors associated with each technology. • Knowledge of security tools and methodologies for different emerging technology platforms. • Understanding of evolving threats and trends in the emerging technology security landscape. **Skills and competences:** • Critical thinking and problem-solving in complex energy emerging technology security scenarios. • Effectively collaborate and communicate technical security concepts to diverse audiences. • Adaptability and agility in responding to the ever-changing emerging technology security landscape.
Main topics and content list *A list of main topics and key content*	• Introduction to cybersecurity in energy emerging technologies including ioe, cloud, blockchain, AI. • Securing the energy emerging technologies (e.g. IoE, cloud, blockchain, AI). • Security tools and techniques for energy emerging technologies. • The future of emerging technology security and its application in the energy network.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine*	• **Knowledge-based assessment**: through two evaluation tests; one launched at the beginning of the seminar (pre-assessment), and another (with the same evaluation content as the first test) at the end of the seminar (post-assessment) to verify that the new knowledge has been

participants have achieved the learning outcomes	correctly acquired. Likewise, learners will have report analysis about specific case studies focused on the energy sector.
Training Provider *Name(s) of training providers.*	UNINOVA and FCT.
Contact *Name(s) of the main contact person and their email address.*	• Ruben Costa: rddc@uninova.pt • José Manuel Fonseca: jmrf@fct.unl.pt
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	20 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical or virtual. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-8: Cybersecurity Tools and Technologies.
Pre-requisites	Basic programming skills, particularly in languages commonly used in cybersecurity, such as Python.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 4: Cyber Threat Intelligence Specialist. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 11: Digital Forensics Investigator.
Tools to be used *A list of tools that will be used for the operation of this training module.*	GDPR, VPNs, RBAC, SSL/TLS, IPsec, SSH, MQTT.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Portuguese.
ECTS *If applicable, the number of ECTS.*	TBD.
Certificate of Attendance (CoA)	Yes.

Indicates Yes or No (even in case of partial attendance)	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.7.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Introduction to Cybersecurity in Energy Emerging Technologies	• Overview of emerging technologies and their impact on cybersecurity landscape. • Unique security challenges associated with different technology categories (IoE, cloud, blockchain, AI).
Topic 2: Securing the Energy Emerging Technologies	• IoE architecture and its vulnerabilities. • Securing devices, networks, and data in IoE environments. • Best practices for managing IoE security risks. • Cloud security models and shared responsibility model. • Cloud-specific threats and mitigation strategies. • Understanding blockchain technology and its security properties. • Vulnerabilities and attack vectors specific to blockchain platforms. • Security risks associated with AI, including bias, data privacy, and adversarial attacks. • Methods for securing AI models and training data.
Topic 3: Security Tools and Techniques for Energy Emerging Technologies	• Specialised security tools and frameworks for different energy emerging technologies.
Topic 4: The Future of Emerging Technology Security and its application in the Energy Network	• Anticipating emerging threats and trends in the energy security landscape. • Developing a proactive approach to securing emerging technologies in the energy network.

3.7.2.3 Planning for Preparedness

In preparing for the "Cybersecurity in Emerging Technologies for Energy Network" seminar, a meticulous internal action plan is executed, ensuring all trainers and materials are synchronised and catered to the unique demands of energy sector cybersecurity. The Seminar targets emerging threats and innovative technologies such as the Internet of Things (IoT), blockchain, and Artificial Intelligence (AI) within the energy context, necessitating a dynamic and adaptive training approach. The planning process emphasises a comprehensive understanding of each topic's unique aspects, with a structured timeline and clear responsibilities assigned to lead trainers. These trainers are responsible for developing customised presentations, overseeing practical exercises, and curating seminar materials that align with the dynamic landscape of energy cybersecurity. This tailored approach ensures that all materials—ranging from interactive simulations to detailed case studies—are prepared and available on the DCM platform well before the commencement of the course. The training environment fosters critical thinking and problem-solving skills, crucial for tackling real-world cybersecurity challenges in the energy sector. Trainers will facilitate discussions and practical exercises that mirror the complex scenarios participants might face, enhancing their ability to respond effectively to emerging cybersecurity threats. By ensuring a robust preparatory phase, involving both theoretical and hands-on components, the course aims to equip participants with the necessary skills and knowledge to navigate and secure emerging technology environments within the energy network.

3.7.2.4 Materials and Exercises

For the "Cybersecurity in Emerging Technologies for the Energy Network" seminar, the educational materials and exercises are meticulously curated to match the advanced technical requirements of energy sector cybersecurity. This includes detailed guides on securing IoT devices, protecting energy data transactions via blockchain, and employing AI for threat detection. Each module features up-to-date, real-world scenarios that provide participants with the opportunity to apply theoretical knowledge practically. Interactive labs are set up to simulate network environments typical to the energy sector, allowing trainees to experiment with and respond to cyber threats in a controlled setting. This hands-on experience is supported by advanced cybersecurity toolkits and software platforms, which are integral to the course materials. The exercises are designed to challenge participants, requiring them to employ strategic thinking and technical skills to navigate and resolve complex security issues.

3.7.2.5 Verification of Learning Outcomes, and Skills

To ensure the efficacy of the "Cybersecurity in Emerging Technologies for the Energy Network" seminar, verification of learning outcomes and skills is conducted through a rigorous assessment framework. This includes both formative assessments during the course and a summative evaluation at its conclusion. Participants undergo scenario-based testing that mirrors real-life cybersecurity challenges in the energy sector, evaluating their ability to apply learned concepts in practical settings. Skills verification also includes peer assessments and group discussions, which encourage collaboration and the sharing of diverse problem-solving approaches among participants. The assessment involves a comprehensive examination and a practical project that requires participants to implement a cybersecurity solution for a hypothetical, but plausible, scenario in the energy sector. This not only tests their acquired knowledge and skills but also reinforces their ability to innovate and adapt to new cybersecurity challenges. These revised sections ensure that the course materials and assessments are directly aligned with the specialised needs of cybersecurity in the energy network, providing a robust framework for learning and application.

3.8 Module 8 - Critical Infrastructure Security for Energy

3.8.1 CSP008_C_E: Critical Energy Infrastructure Security

3.8.1.1 Description of Training Module

The "Critical Energy Infrastructure Security" course is an advanced-level training designed to equip professionals with the knowledge and skills necessary to protect critical energy infrastructures from a range of cybersecurity threats. This module covers the essential strategies and practices needed to secure critical energy systems against cyber threats, addressing technology, policy, and legal perspectives. Participants will learn about common vulnerabilities in critical infrastructure technologies, including IT and OT, and assess these vulnerabilities using established standards and methodologies.

CSP008_C_E is targeted at professionals involved in safeguarding critical energy infrastructures, such as utility managers, policy makers, and cybersecurity specialists.

Code *Code format: CSP008_x where x is the training of offering type (see below)*	**CSP008_C_E**
Module Title *The title of the training module*	**Critical Energy Infrastructure Security**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Protecting Vital Energy Infrastructure: Security Measures. • Critical Systems Security: Safeguarding Energy Infrastructure. • Securing Energy Essential Services and Infrastructure. • Critical Energy Infrastructure Protection: Security Strategies. • Infrastructure Resilience and Security. • Safeguarding Critical Energy Assets: Infrastructure Security. • Security of Key Infrastructure Energy Systems. • Defending Critical Energy Infrastructure from Threats. • Energy Infrastructure Security and Resilience Measures. • Ensuring Resilient Critical Energy Infrastructure Security. • Hardening Critical Energy Systems Against Threats.

Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C).
Level *Training level: B (Basic), A (Advanced)*	Advanced (A).
Module overview *High-level module overview*	The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge energy technologies. As the energy business embrace innovations such as the IoE, AI, blockchain, and 5G, robust cybersecurity measures become paramount. This module aims to provide a comprehensive understanding of the cybersecurity landscape within the energy context. This training module will address the different aspects of critical energy infrastructure security that includes different perspectives: technology, policy, and legal.
Module description *Indicates the main purpose and description of the module.*	This training module explores the energy definitions and characteristics of CIs together with their information systems will be identified, and common threats and vulnerabilities of the CI technologies (Information and Communication Technology (ICT)/IT and OT) will be assessed and estimated based on existing standards and methodologies.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Acquire a comprehensive understanding of the strategies, and best practices involved in securing critical energy infrastructure systems against various threats and vulnerabilities. • Acquire a comprehensive understanding of the main security and resilience challenges for the protection 24/7 of critical energy infrastructures, considering the diverse involved perspectives (technological, policy and legal).

	• Knowledge of the most common vulnerabilities and particular threats to Critical energy Infrastructures, considering the drawbacks of maintaining legacy devices (and their protocols) and the real-time performance condition. • Knowledge of the most current regulations and normative associated with the CIs and their specific application sectors, as well as conduct and ethical criteria. **Competencies and skills:** • Identify essential services, threats and possible risks in a CI or between CIs. • Know how to identify possible misconfigurations or errors in IT and OT devices and (industrial) communication protocols that may lead to significant security risks. • Lead the design, configuration, and deployments of secure and resilient CIs. • Know how to support organisations in implementing measures to harden their systems, ensuring the robustness and resilience of their critical infrastructures against potential and specific threats. • Know how to apply standards, recommendations, and best practices, but also legal, social and privacy criteria.
Main topics and content list *A list of main topics and key content*	• Introduction to critical energy infrastructure security and challenges. • Risk assessment and mitigation strategies. • Security controls, resilience, and best practices. • Regulations and standards including privacy, ethical, legal, and social implications.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Formative assessment**: ongoing process of evaluating participants' learning during a training programme including pre-assessment, during and post-assessment in each training topic. It provides valuable feedback to instructors and participants, helping to ensure that learning goals are being met and that participants are making progress. • **Summative assessment**: learner needs to produce a targeted outcomes and deliverables at the end of the training by performing a list of tasks to demonstrate the knowledge of the critical energy infrastructures.
Training Provider *Name(s) of training providers.*	UNINOVA, FCT, and PDMFC.
Contact	• Ruben Costa: rddc@uninova.pt • José Manuel Fonseca: jmrf@fct.unl.pt

Name(s) of the main contact person and their email address.	• Luis Miguel Campos: luis.campos@pdmfc.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	12 weeks.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical or Virtual. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-1: Cybersecurity Management. • KA-4: Cybersecurity Policy, Process and Compliance • KA-5: Network and Communication Security Nonetheless, minor content matches with other including: • KA-2: Human Aspects of Cybersecurity. • KA-3: Cybersecurity Risk Management. • KA-6: Privacy and Data Protection. • KA-7: Cybersecurity Threat Management.
Pre-requisites	Basic knowledge of cybersecurity essentials (related to CSP Module 1) and basic IT training.
Relevance to European Cybersecurity Skills Framework (ECSF)	• ECSF Profile 5: Cybersecurity Architect. • ECSF Profile 6: Cybersecurity Auditor. • ECSF Profile 10: Cybersecurity Risk Manager. • ECSF Profile 9: Cybersecurity Researcher. • ECSF Profile 7: Cybersecurity Educator.

An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.	
Tools to be used *A list of tools that will be used for the operation of this training module.*	Wireshark, OpenVPN, Python, XCA, IBM QRadar, SCADA/ICS.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Portuguese.
ECTS *If applicable, the number of ECTS.*	TBD.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.8.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Introduction to Critical Infrastructure Security and Challenges	• Definition, scope, and importance of critical infrastructure. • Critical infrastructure sectors and examples (energy, transportation, water, etc.) • Interdependencies between various critical system. • Overview of national and international security frameworks.

	• Global threat landscape and its impact on critical infrastructure.
Topic-2: Common Security Weaknesses and Threat Landscape	• Most common security Weaknesses in CI: the deployment of new technologies and the adoption of new IT paradigms, such as Industry 4.0/5.0 and simulation, bring with them numerous security issues, especially those related to "legacy" devices and protocols. This means that the number of vulnerabilities may increase significantly, as well as the risks of their exploitation. Learners must therefore understand the major drawbacks that new IT brings to operational ecosystems, and the consequences that this in turn entails. • Threat landscape: classify and model attacker types and specific interests; categorise potential threats to critical infrastructure, such as Advanced Persistent Threats (APTs) or supply chain attacks, and associate those that are more targeted to specific types of critical infrastructure.
Topic-3: Cascading Effects and Risk Assessment	• Relations and Interdependencies: identify dependencies and interdependencies between critical infrastructures and establish levels of priority and criticality, in order to subsequently compute consequences between affected assets, services and users, as well as other critical infrastructures and their essential services. • Visualisation of the cascading effect: model the relationships between infrastructures and their services to subsequently visualise and analyse the exploits of cascading effects between or among CIs, including the effects they might have on their own IT-OT layers. This will allow learners to have a clearer understanding of the problem and prepare contingency and recovery plans for resilience. • Risk management and assessment: identify threats and possible risks; understanding cyber, physical, and natural threats; risk management and risk assessment through well-known methodologies, applied to critical systems.
Topic-4: Regulations and Standards	• Regulations and standards: overview of regulatory frameworks and standards (e.g. NIST, ISO, ENISA, European Telecommunications Standards Institute (ETSI) guidelines); and compliance requirements for critical infrastructure security.

Topic-5: Security and Resilience	• Cybersecurity for critical infrastructures: cyber threats to critical systems; network security, including encryption, perimeter defence (equivalent to CSP Module 4), advanced intrusion detection; coordinated and advanced incident response; (dynamic) recovery against potential cyber-attacks; and situational awareness and sharing data through cyber threat intelligence. • Security and resilience (including safety): risk treatment plan and security policy; disaster recovery plan; and business continuity plan.
Topic-6: Privacy, Ethical, Legal, and Social Implications	• Ethical, legal, and social implications: ethical considerations in critical infrastructure security; legal aspects and privacy concerns; and social impacts and community resilience.

3.8.1.3 Planning for Preparedness

For the preparation of CSP008_C_E, all activities are meticulously planned and coordinated among the trainers through an internal action table that details the allocation of tasks, timelines, methodologies, and training schedules. This ensures that each trainer is well-prepared with custom materials and presentations for their respective training topics. The planning process is designed to be flexible, allowing trainers to adapt their instructional strategies to the specific needs and complexities of their topics. All training materials, including videos, presentations, and reading resources, are made available on the DCM platform well in advance of the course start to ensure smooth delivery.

3.8.1.4 Materials and Exercises

The CSP008_C_E materials and exercises are carefully prepared to ensure they align with the specific security needs of critical energy infrastructures. This includes a mix of theoretical content and practical exercises that reflect real-world scenarios. Participants engage in game-based learning, case studies, hands-on lab exercises, and discussions that foster a deep understanding of how to secure critical infrastructures. The exercises are designed to be interactive and practical, allowing participants to apply what they have learned in simulated environments that mimic actual energy sector challenges.

3.8.1.5 Verification of Learning Outcomes, and Skills

Learning outcomes are verified through a combination of formative and summative assessments. Formative assessments occur throughout the course, providing ongoing feedback and ensuring that learning objectives are being met. Summative assessments include practical tasks where participants demonstrate their ability to conduct threat and vulnerability assessments on simulated critical energy infrastructure scenarios. These assessments help confirm that participants have mastered the necessary skills and knowledge to effectively respond to and mitigate cybersecurity threats within the energy sector.

3.8.2 CSP008_S_E: Protecting Charging Stations Against Specific Threats

3.8.2.1 Description of Training Module

CPS008_S_E is a specific seminar presenting a particular case study of Smart Grids, the well-known electric vehicle charging infrastructures. The module is aimed at IT/OT engineers and administrators in

charge of managing the control networks of charging stations, and professionals in the energy sector, including human operators, managers and directives, energy suppliers and employees. In addition, the seminar can also be taken by students of industrial engineering or computer sciences, cybersecurity aspirants, researchers and educators interested in the protection of charging stations.

Code *Code format: CSP008_x where x is the training of offering type (see below)*	**CSP008_S_E**
Module Title *The title of the training module*	**Protecting Charging Stations Against Specific Threats**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Hardening Charging Stations Against Potential Threats. • Defending Energy Charging Networks from Modern Threats. • Charing Station Protection: Security and Best Practices.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	Advanced (A).
Module overview *High-level module overview*	This seminar provides an overview of some security issues currently presented by charging stations and their main challenges, as well as possible implications and recommendations to guide the configuration and protection of charging stations, both at the communications and software level.
Module description *Indicates the main purpose and description of the module.*	This seminar aims to (1) provide an overview of the main security and privacy issues, showing the possible cascading effects and impact on the power grid itself and other critical infrastructures, and (2) list a set of possible security measures to

	provide guidelines and best practices for (future) experts in this application area.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Understand the definition, scope, and importance of stations charging across the energy sector, and their impact to other critical infrastructures. • Grasp the unique security challenges and vulnerabilities specific to the charging stations. • Develop knowledge of cyber and physical threats, attack vectors, and potential consequences of security breaches in charging stations. • Understand the principles and methodologies to analyse cascading effects and evaluate security risks. • Gain knowledge of effective security measures, controls, and best practices for protecting charging stations (at communication and cyber level). • Stay informed about new threats and trends in the field of charging station security. **Skills:** • Apply best practices for implementing physical and cyber security controls in charging infrastructures. • Identify and utilise specialised security tools and mechanisms. **Competencies:** • Critical thinking and problem-solving in charging station security scenarios. • Ability to analyse and interpret technical information and develop data-driven security solutions. • Strong decision-making skills based on comprehensive understanding of risks and best practices.
Main topics and content list *A list of main topics and key content*	• Introduction to the energy charging infrastructures. • Security challenges in energy charging stations. • Cascading effects and impact to other critical infrastructures. • Security measures and best practices for charging stations.

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Knowledge-based assessment**: through an evaluation test at the end of the seminar where some of the contents will have a practical approach dealing with case studies on which learners will have to reflect and analyse, taking into account the application scenario and its level of criticality.
Training Provider *Name(s) of training providers.*	UMA, UCY and AIT.
Contact *Name(s) of the main contact person and their email address.*	• Dr. Cristina Alcaraz, Associate Professor, University of Malaga (UMA), Spain, alcaraz@uma.es • Dr. Elias Athanasopoulos, Associate Professor, University of Cyprus (UCY), athanasopoulos.elias@ucy.ac.cy • Dr. Stefan Schauer, Senior Scientist, Austrian Institute of Technology (AIT), stefan.schauer@ait.ac.at • Dr. Abdelkader Shaaban, Scientist, Austrian Institute of Technology (AIT), abdelkader.shaaban@ait.ac.at
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	4 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual, physical, or both. Any information about the physical location or the URL link, it will be posted on the DCM platform.

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-1: Cybersecurity Management. • KA-3: Cybersecurity Risk Management. • KA-4: Cybersecurity Policy, Process and Compliance. • KA-5: Network and Communication.
Pre-requisites	Basic knowledge of cybersecurity fundamentals (related to CSP module 1), and experience with operating systems, network configurations and communication protocols from a generic point of view.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 5: Cybersecurity architect
Tools to be used *A list of tools that will be used for the operation of this training module.*	OCPP and probably its corresponding simulator or libraries.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	• Spoken: English. • Language for the material and the assessment/evaluation: English.

ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.8.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to the Energy Charging Infrastructures	• Motive the problem explaining the concept of "charging stations", its benefits for society, environment, and economy, as well as their main components (e.g. smart meters, control systems, etc.), protocols, and security technologies. Basically, the topic focuses on providing the scope of the infrastructure, and importance to the society. • Introduce the relations and interdependencies with other systems, including energy control systems, legal entities, utilities, providers, and end users.
Topic-2: Security Challenges in Energy Charing Stations	• Highlight the main security challenges of the deployment of stations charging stations, and their communication protocols such as Open Charge Point Protocol (OCPP) or ModbusTCP. • List and classify the main vulnerabilities and threats to security and privacy in energy charging stations, allowing learners to understand the current situation, and the need to protect this type of systems, their main infrastructures, and stakeholders, such as the power grid, control systems and end users.

Topic-3: Cascading of Energy and impact to other Critical Infrastructures	• Introduce the dependences and interdependencies of the stations charging with respect to other critical infrastructures, such as healthcare or maritime. For structural analysis and visualisation, a graph representation (the interdependency graph) will be discussed during the seminar. • Provide practical studies based on simulations and analysis of cascading effects. Based on the discussions on interdependencies, this part will cover the implications on threats and their consequences. The concept of cascading effects will be introduced and highlighted by various examples from the literature and from practice. An abstract model for describing the effects of a threat on an individual system with a critical energy infrastructure will be presented. Taking the interdependency graph into account, a stochastic model for the simulation of the cascading effects across the internal network of critical systems as well as the external network with other critical infrastructures will be presented and discussed.
Topic-4: Security Measures and Best Practices for Charging Stations	• Show the most typical best practices, considering existing recommendations given for international organisations. • Provide a set of security measures and controls at the communications and software level to help future experts to execute best practices, avoiding threats that may cause significant damage and effects against the power grid itself or other critical infrastructures.

3.8.2.3 Planning for Preparedness

As part of the early steps in the preparedness process, we circulated an initial table internally to consolidate all relevant module information. Subsequently, we collected inputs to define the module content and outline key topics. These inputs provide a high-level view of the module and offer insights and vision for all the topics presented for CSP008_S_E. Additionally, the table outlines the work methodology to be followed regarding tasks and the training schedule. Each module has a lead responsible for developing course tasks, which include creating presentations, organising practical activities, and defining materials. Hence, discussions with the module lead were held to negotiate and brainstorm topic details that align with the module's requirements. These discussions are essential to ensure the delivery of high-quality module content and to confirm that all proposed topics are consistent throughout the entire module, preventing repetition of content. As agreed, upon within the CyberSecPro consortium, the DCM platform for the seminar management system has been developed to manage all agreed-upon topics for CyberSecPro materials efficiently. Therefore, all module presentations are stored on the DCM platform, which also facilitates the uploading of related materials and final assessments. Additionally, the platform allows all module trainers to access and synchronise with others, aiding in the completion of planned training materials.

3.8.2.4 Materials and Exercises

To ensure the high quality of materials and meet the expectations of the previously discussed key topics and seminar objectives, we developed and integrated advanced materials covering various aspects of

cybersecurity challenges and related mitigation actions for protecting charging stations. This module (CPS008_S_E) introduces the energy charging infrastructure, which includes power, control, and payment systems. Additionally, it discusses the challenges and mitigation actions for protecting the charging station infrastructure from different types of cyber-attacks. Also, the cascading effects and their impact on this critical infrastructure, along with best practices for security measures at charging stations, are considered as part of this module. All related materials are gathered from various sources to provide a comprehensive learning experience for all participants, enabling them to engage with the defined seminar content that matches the module objectives.

Additionally, the module includes various activities such as case studies, research analysis, and open discussions. These activities provide diverse interactive approaches for activities, ensuring engagement and preventing boredom among participants. Practical examples of the cascading effects of cyberattacks will be included in this module to provide deeper insights into how to simulate cyberattacks and demonstrate their impact on infrastructure and the surrounding environment. These practical activities will help participants fully engage with the concept of cascading effects, visually mimicking the propagation of attacks and their impacts. This will assist participants in understanding and further investigating the lessons learned from their theoretical knowledge of cascading effects in real-world scenarios.

3.8.2.5 Verification of Learning Outcomes, and Skills

In order to ensure full integration of all participants with the seminar content and support the overall evaluation of CPS008_S_E, an open discussion among participants will be essential. This discussion will focus on cybersecurity-related aspects of charging stations. It will support the enhancement of critical thinking of the participants by involving them in identifying problems and potential solutions for mitigating cyber threats to this critical infrastructure. On the other hand, it will also improve the environment of collaboration and knowledge sharing among all participants, thereby enhancing their skills and the overall course outcomes. This approach will significantly improve the evaluation of seminar progress, providing an indication of the learners' satisfaction with the seminar content. It will also highlight how improvements in communication and interaction among participants can change the dynamics or activities of the discussion, such as creating small groups to enhance communication activities. These groups will improve participants' integration into the discussion topics and give them more opportunities to enhance their critical thinking skills.

At the end of the seminar, each learner will have the opportunity to evaluate the skills they have acquired through the final assessment. This assessment will be available on our DMC platform, providing us as trainers with an effective way of tracking all activities completed by learners and ensuring that all learning progress is achieved in line with the key objectives of our module.

The trainers are keen to ensure the continued success of the learning outcomes. Therefore, we will provide a comprehensive assessment after collecting all trainee activities and final assessments. The trainer will then analyse this information to provide further evidence for improvement. This evaluation is essential for assessing the learning outcomes through the course content and the methods followed in teaching the seminar content. In addition to providing feedback from learners regarding the seminar, their satisfaction, and their expectations of the seminar contents and trainers, this also provides a complete image for improvement and paves the way for giving more space to enhance the overall contents of the seminar and the methods followed for presenting the topics.

The whole evaluation process can be summarised as follows:

4. Self-assessment: each student in the CSP008_S_E will undergo a final assessment, allowing them to evaluate themselves and reflect on their learning experience.
5. Trainer evaluation: trainers will assess the outcomes of the course by evaluating various aspects, including:

- Participant communication and interaction, focusing on critical thinking about possible solutions to mitigate cyber threats in charging infrastructures through open discussions or the creation of small groups.
- This evaluation process helps trainers gauge the comprehensiveness of the topics covered and identify areas for improvement, such as optimising content, intensifying instruction, or refining methods for developing knowledge and skills in future sessions.
- Participant feedback: collect all feedback on seminar content and trainers to provide a space for improvement.

3.9 Module 9 - Software Security for Energy

3.9.1 CSP009_S_E: Mechanics for Memory Corruption

3.9.1.1 Description of Training Module

This is an introductory seminar to memory corruption and the security implications of it. Students of all levels are welcome. A basic background of computer programming is useful but not essential.

Code *Code format: CSP009_x where x is the training of offering type (see below)*	**CSP009_S_E**
Module Title *The title of the training module*	**Mechanics for Memory Corruption**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Introduction to software vulnerabilities. • Exploiting vulnerabilities in native software. • Managing vulnerabilities for C/C++ software.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	Advanced (A).

Module overview *High-level module overview*	This seminar provides an overview of how memory-corruption vulnerabilities work and are managed. Special focus is given in energy-based systems.
Module description *Indicates the main purpose and description of the module.*	This seminar aims to (1) provide an overview of how native software works, (2) how simple bugs can be used to execute an attacker's code, and (3) how such bugs are managed.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Understand some basic foundations about the execution of software produced by a C/C++ compiler. • Understand the difference between memory-safe and memory-unsafe systems. • Understand what a memory-corruption vulnerability is and how it differs from other bug classes. • Understand the mechanics for exploiting memory-corruption vulnerabilities. • Understand the operation of some basic defences. **Skills:** • Produce a simple PoC exploit. • Use compiler options to defend the PoC exploit. **Competencies:** • Good understanding of how software works. • Ability to assess how careless code can lead to undesired security consequences. • Strong decision-making skills based on comprehensive understanding of risks and best practices.
Main topics and content list *A list of main topics and key content*	• Differences between C/C++ and Java in memory management. • Use of the stack in C/C++ software. • Buffer overflows and overreads. • Prevalence of native code in the energy sector. • Handling of known vulnerabilities (Comma-Separated Value, CSV).
Evaluation and verification of learning outcomes	• **Knowledge-based assessment**: through an evaluation test at the end of the seminar.

Assessment elements and high-level process to determine participants have achieved the learning outcomes	
Training Provider *Name(s) of training providers.*	University of Cyprus (UCY) and FCT.
Contact *Name(s) of the main contact person and their email address.*	• Elias Athanasopoulos, University of Cyprus (UCY), athanasopoulos.elias@ucy.ac.cy • José Manuel Fonseca: jmrf@fct.unl.pt
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	4 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual, physical or both. Any information about the physical location or the URL link, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection*	Mainly: • KA-1: Cybersecurity Management. • KA-3: Cybersecurity Risk Management. • KA-8: Cybersecurity Tools and Technologies. • KA-9: Penetration Testing.

KA7 – Cybersecurity Threat Management *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	
Pre-requisites	Basic knowledge of cybersecurity fundamentals (related to CSP module 1), and experience with operating systems.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 1: Chief Information Security Officer (CISO). • ECSF Profile 5: Cybersecurity architect. • ECSF Profile 9: Cybersecurity researcher. • ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	gcc (GNU C compiler), GNU binutils, and GNU gdb.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More*	Refer and check online CyberSecPro DCM System for current information.

information will be provided in the module description.	

3.9.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to memory-unsafe programming systems	• Introduction to programming systems (C/C++, Java, etc.). • Memory safety in C/C++ vs Java.
Topic-2: Foundations of executing software	• The role of the stack in x86 architectures. • The life of a C function. • How control data is used to direct control flow.
Topic-3: Memory-corruption vulnerabilities	• Spatial safety (buffer overflows). • Temporal safety (use-after-free). • Turning a vulnerability to an exploit. • Demonstrations.
Topic-4: Defences and vulnerability management	• How compilers and OSs defend software against memory corruption. • Managing CVEs.

3.9.1.3 Planning for Preparedness

The module is delivered through multiple trainers. To ensure that everything is ready, all material has been uploaded beforehand on the DCM platform. The material includes slides, and other supplementary content, such as assignments and code examples. The DCM platform acts as a central point that can orchestrate all activities of the trainers. Collecting all material on a central portal allows all trainers to have a global view of the module and, therefore, adjust their content accordingly. Additionally, having all content on the DCM allows trainers to review the material of other trainers and therefore have a consistent view and presentation of the entire module.

3.9.1.4 Materials and Exercises

material is primarily delivered through slides. This makes both physical and remote participation of trainees possible. Slides are in English but can be delivered orally in dfferent languages. Slides contain the basic elements for conveying the core ideas of the module, behind memory corruption and the mechanics of it. However, since this is a very practical topic, a lot of code accompanies the slides. Through code examples, and live demonstration, the trainees have the opprorunity to sense all ideas and see how memory corruption can be used to compromise small example programmes.

As far as code is concerned, it will be mainly consisted of very small intentionally vulnerable programmes. The goal of the module is to showcasee the mechanics of exploiting memory-corruption vulnerabilities and not to analyse real-world exploits or replicate authentic CVEs in actual software; a

process, which is much more involved and complicated. Although the demos are on simple code and not on actual software, the experience gained from the entire process is valuable. This is because simple programmes do not exhibit the complexity of actual software and, thus, allow the focus to be entirely on how exploitation works.

For the demostrations on code, gdb is used. This is the GNU debugger and it is a programme that allows to pause a process and inspect its memory contents. Typically, gdb is not used for launching real attacks, but building the attack using gdb allows for many educational benfits. By using gdb, the trainee can see how an attack is carried out in a step-by-step fashion. Moreover, by using gdb the attack can be delivered incrementally with the assistance of the trainee (e.g. by asking questions and trying ideas or proposals formed by the audience).

3.9.1.5 Verification of Learning Outcomes, and Skills

The module first begins with outlining the theoreetical foundation, then continues with demonstration on code examples, and finally there is a phase where trainees attempt to carry out similar tasks with the ones that were demonstrated, but on binaries. This series of phases (theoretic lecture, demonstration, replication of learned concepts) is carried out several times for outlining different concepts. It is therefore natural that the participants will be verified in multiple ways.

First, there will be heavy interaction between the trainers and the trainees during the demonstation phase. Participants will be asked for specific decisions during the demonstration of exploitation. Second, after the demonstration session, the participants will be given the opportunity to apply learned concepts on other software. Furthermore, the partipants will be requested to fill in a short multiple-choise based test and evaluate the trainers. Finally, the participants will be able to receive a certificate of attendance.

3.10 Module 10 - Penetration Testing for Energy

3.10.1 CSP010_S_E: Cybersecurity in Energy

3.10.1.1 Description of Training Module

The " Cybersecurity in Energy Sector" seminar is a tailored educational initiative designed specifically for cybersecurity professionals aiming to enter or enhance their skills in the specialised field of binary penetration testing within the energy sector. Over three hours, this module provides a concentrated experience that combines lectures, demonstrations, and interactive discussions to impart essential knowledge and skills. Participants will learn about the cybersecurity landscape of the energy sector, understand the basics of binary penetration testing, and gain practical insights into applying these skills effectively. The seminar targets cybersecurity professionals at the beginning of their career in binary analysis or those from other cybersecurity areas seeking to specialise in this critical aspect of energy sector security.

Code *Code format: CSP010_x where x is the training of offering type (see below)*	**CSP010_S_E**
Module Title *The title of the training module*	**Cybersecurity in Energy**

Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Energy and binary security
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S (Seminar).
Level *Training level: B (Basic), A (Advanced)*	A (Advance).
Module overview *High-level module overview*	The binary penetration testing in the energy sector seminar is a concise, intensive introduction aimed at equipping participants with the foundational skills and knowledge needed to begin addressing binary vulnerabilities within the energy sector. Over the course of 3 hours, through a combination of lectures, demonstrations, and interactive discussions, participants will explore the cybersecurity landscape of the energy sector, delve into the basics of binary pen testing, and learn how to apply these skills practically. This seminar is an essential starting point for cybersecurity professionals in the energy sector looking to enhance their technical capabilities in binary analysis and exploitation.
Module description *Indicates the main purpose and description of the module.*	This module introduces participants to the specialised field of binary penetration testing with a focus on the energy sector. It covers the cybersecurity landscape of the energy sector, introduces the fundamentals of binary pen testing, including the tools and techniques used to find and exploit vulnerabilities in binary applications, and offers a practical approach to applying these skills in the energy sector. The module is designed for those new to binary pen testing or those seeking to apply their existing cybersecurity knowledge within the energy sector context.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	• Understand the critical importance of cybersecurity and binary pen testing within the energy sector. • Be familiar with the common cybersecurity challenges and vulnerabilities in the energy sector's operational technology. • Have a foundational knowledge of binary pen testing, including key concepts, tools, and techniques. • Be able to identify basic binary vulnerabilities and understand the steps for their exploitation. • Know how to set up a simple testing lab for practicing binary pen testing skills.
Main topics and content list *A list of main topics and key content*	• The cybersecurity landscape of the energy sector. • Fundamentals of binary penetration testing. • Practical approaches to binary penetration testing. • Setting up a binary pen testing lab for the energy sector. • Demonstration of exploiting a binary vulnerability. • Best practices for vulnerability reporting and mitigation.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• A practical demonstration or walkthrough of a basic binary vulnerability identification and exploitation (if time and resources allow). • A short QnA covering the cybersecurity landscape of the energy sector, fundamental principles of binary pen testing, and basic tools and techniques for binary analysis and exploitation.
Training Provider *Name(s) of training providers.*	UPRC
Contact *Name(s) of the main contact person and their email address.*	• Prof. Nineta Polemi: polemid@unipi.gr
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	3 hours.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the*	Physical.

location. If virtual, provide the URL link of the website.	
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-4: Cybersecurity Policy, Process, and Compliance. • KA-7: Cybersecurity Threat Management. • KA-8: Cybersecurity Tools and Technology. • KA-9: Penetration Testing.
Pre-requisites	Kali Linux -> Nmap, GDB compiler
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 10: Cybersecurity Risk Manager. • ECSF Profile 8: Cybersecurity Implementer. • ECSF Profile 12: Penetration Tester.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Customised VMs.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English.
ECTS *If applicable, the number of ECTS.*	N/A.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.10.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction (15 Minutes)	• Quick overview of the seminar's goals. • Importance of cybersecurity and binary pen testing in the energy sector.
Topic-2: Session 1: The Cybersecurity Landscape of the Energy Sector (30 Minutes)	• Overview of critical infrastructure and its cybersecurity significance. • Specific challenges and common vulnerabilities in the energy sector's OT.
Topic-3: Session 2: Fundamentals of Binary Penetration Testing (1 Hour)	• Introduction to binary pen testing: key concepts, goals, and scope. • Overview of essential tools for binary analysis and exploitation • Basic binary vulnerabilities: understanding and identifying buffer overflows and format string vulnerabilities.
Topic-4: Session 3: Practical Approaches to Binary Penetration Testing in the Energy Sector (1 Hour)	• Setting up a basic binary pen testing lab: tools and environments tailored for energy sector applications. • Demonstrating a simple binary exploit: a step-by-step walkthrough of exploiting a common vulnerability in a binary application relevant to the energy sector. • Best practices for reporting and mitigating vulnerabilities.

Topic-5: Conclusion and Q&A (15 Minutes)	• Recap of key points. • Open floor for questions and discussion on applying binary pen testing skills in the energy sector.

3.10.1.3 Planning for Preparedness

Participants in the seminar will receive a variety of materials to enhance their learning experience. Detailed lecture slides and notes will cover the fundamental concepts of binary penetration testing and cybersecurity within the energy sector, providing a strong theoretical base to guide the learning process. Instead of pre-recorded videos, CSP010_S_E will feature live demonstration presentations where instructors showcase the process of identifying and exploiting vulnerabilities in binary applications. These live sessions allow for real-time interaction and clarification, significantly enhancing the learning experience. Additionally, reading assignments will be provided, offering further insights and context related to binary penetration testing and the unique challenges faced by the energy sector.

3.10.1.4 Materials and Exercises

To complement the theoretical materials, participants will engage in several practical activities. They will receive instructions and support to set up personal binary penetration testing labs using simulated environments that closely mimic real-world energy sector scenarios, essential for practicing the skills discussed during the seminar. While formal exercises are not included, optional tasks will be provided for participants eager to further apply what they have learned. These tasks are designed to encourage exploration and application of skills in identifying and mitigating vulnerabilities. Furthermore, through discussions of real-world case studies, participants will examine specific problems within the energy sector's cybersecurity landscape, which is crucial for understanding how to apply theoretical knowledge in practical, impactful ways within the industry.

3.10.1.5 Verification of Learning Outcomes, and Skills

The verification of learning outcomes and skills in the seminar involves assessing participants' understanding and application of the concepts through a combination of formative and summative methods. This process ensures that participants have effectively grasped the key concepts and practical skills necessary for binary penetration testing in the energy sector. Feedback from these assessments helps guide ongoing learning and development, allowing for continuous improvement of both the participant's skills and the seminar's instructional methods.

3.11 Module 11 - Cyber Ranges and Operations for Energy

3.11.1 CSP011_S_E: Cyber range and operations on SCADA

3.11.1.1 Description of Training Module

The cyber range and operations on SCADA focuses on the general use of SCADA elements influencing several sectors as it is broadly used, in particular in the energy sector. During the seminar a group of trainees will have the opportunity to familiarise with the use and leaks of these equipment, used to manage power supply installations and networks.

Most often observed attacks of SCADA (including fatal ones in other sectors) are detailed and presented during the seminar and specific analysis are conducted on equipment.

Code *Code format: CSP011_x where x is the training of offering type (see below)*	**CSP011_S_E**
Module Title *The title of the training module*	**Cyber range and operations on SCADA**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Threats and attacks on PLC / SCADA. • Cyberdefence of PLC / SCADA. • Preventing Attacks of PLC / SCADA. • Securing Industrial Automation & Control Systems (IACS).
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	• W (Workshop). • S (Seminar).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The cyber-range and operations module focuses on Programmable Logic Controllers (PLC) and on the general use of SCADA present in Industrial Automation & Control Systems (IACS). These devices are broadly used in several sectors as the energy, transportation, production and logistics. There use is in particuar intensive in the energy sector, present in oil & gaz, electrical / nuclear plants. During the seminar a group of trainees will have the opportunity to be introduced to the use of PLCs / SCADA, the leaks of these equipments, used in several ways by industrial stakeholders to manage production units, power supply installations and distribution networks as partially included in the IoTs.
Module description *Indicates the main purpose and description of the module.*	The purpose of this module its to familiarise trainees with the use of PLC / SCADA, their architectures, and the cybersecurity weaknesses of PLC / SCADA. Most often observed and future attacks impacting SCADA (including fatal ones in other sectors)

	are detailed and presented during the seminar and specific analysis are conducted on equipment. After having seen how PLC/SCADA are working and how they are introduced in network levels, most used architectures will be presented. The concept of information security on OT and its importance to industrial organisation will be presented. Types of information assets that need to be protected, as well as the different threats and vulnerabilities that these assets face will be introduced via several use cases and scenarios. A section dedicated to evidence of attacks incidents on SCADA/ PLC will allow to establish the specific threats and vulnerabilities that exist in the industrial domain. It will also present the different types of attacks and the attackers that launch them, as well as the different solutions to mitigate them. The module relying partly on recognised information sources as: • ISA: International Society of Automation • NIST Cybersecurity Framework (CSF) • ISO/IEC 27001: Information security management systems • OWASP Top 10 security risk for ICS Security • SANS: Institute Top 20 Critical Security Controls for Effective Cyber Defence • ENISA: Good Practices for Industrial Control Systems Security CIS Controls for OT Security • FERC: (Federal Energy Regulatory Commission) Cyber Security and Physical Security Standards. • NATO ENSEC COE: Guide for protecting industrial automation and control systems against cyber incidents (NATO energy Security centre of excellence) At least the module will present several scenarios within the framework of CIA (the three pillars of information security: Confidentiality, Integrity, and Availability). It will explain what each scenario represents as a risk to each pillar and why it could impact the industrial activities. Other security models that can be used to protect information assets will be used during the workshop. These models include the NIST Cybersecurity Framework, the ISO/IEC 27001 standard, and the COBIT framework.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Trainees should be capable to apprehend cyberattacks and incidents on PLC / SCADA used in energy systems supported by such devices (hardware and software). Trainees will be able to demonstrate following specific capacities including: **Knowledge:** • In-depth understanding of SCADA and their inherent leaks. • Ability to identify and characterise threats. • Knowledge of energy infrastructure specific vulnerabilities and attack vectors using SCADA. • Acquisition of cybersecurity principles and best practices applicable to the energy sector. • Knowledge of tools and tactics for defending and / or intruding SCADA. **Skills and competences:** • Critical thinking and problem-solving in scenarios using SCADA as vector of attack. • Adaptability and agility in responses to threats and incidents. • Strong decision-making based on comprehensive understanding of risks and best practices.
Main topics and content list *A list of main topics and key content*	• Introduction to cybersecurity in iot used to support the energy sector. • Anomaly/incident detection techniques and forensics. • Security incident event management and coordination. • Cyber defence tools and techniques for iot systems. The systems include, but are not limited to: • Industrial control systems, including Distributed Control Systems (DCSs), PLCs, Remote Terminal Units (RTUs), intelligent electronic devices, SCADA, networked electronic sensing and control, and monitoring and diagnostic systems. In this context, process control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether physically separated or integrated. • Advanced or multivariable control, online optimisers, dedicated monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems. • Internal, human, network, or HMIs used to provide control, safety, and manufacturing operations

	functionality to continuous, batch, discrete, and other processes.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Evaluation to understanding the way PLC/SCADA are working, the different type of architectures, and incidents to answer following questions: • What are the functions and assets that have to be protected? • What are the likely threats to those chosen assets and functions? • How will identified assets and functions be protected from identified threats in the most cost efficient way ?
Training Provider *Name(s) of training providers.*	C2B
Contact *Name(s) of the main contact person and their email address.*	• Bruno Bender: Bruno.bender@ventura-associate.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	• 1 / year in 2024. • 2 / year in 2025.
Duration *Duration of the training.*	2 days.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physically - Toulon (France). - Potentially in Mons (Belgium) In cooperation with the NATO energy security centre of excellence (Vilnius Lithuania).

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-9: Penetration Testing. Partly: • KA-10: Cyber Incident Response. • KA-7: Cybersecurity Threat Management
Pre-requisites	Cyberdefence advanced skill.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 11: Digital Forensics Investigator. • ECSF Profile 12: Penetration tester.
Tools to be used *A list of tools that will be used for the operation of this training module.*	• Control network infrastructure design (network architecture concepts, including topology, protocols, and components) and relation to IEC 62443. • Windows command line tools to analyse the system and investigating high-risk items as well as Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programmes to perform continuous monitoring of various tools • Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems) • Better understand the systems' security lifecycle • Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation) • Use your skills in computer network defence (detecting host and network-based intrusions via intrusion detection technologies)

	• Implement incident response and handling methodologies • Map different ICS technologies, attacks, and defences to various cybersecurity standards including NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, centre for Internet Security Critical Security Controls, and COBIT 5 • GDPR, HIPAA, Zero Trust, VPNs, RBAC, SSL/TLS, IPsec, SSH, MQTT.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	French, English (2025).
ECTS *If applicable, the number of ECTS.*	TBD.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.11.1.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: SCADA engineering	• What is a SCADA. • How does it work. • Use of SCADA in the energy / transportation sector.
Topic-2: Risks and Threats	• What are the threats that SCADA can bring to the energy sector. • Risks of SCADA used in Energy networks.

Topic-3: Cyberdefence Tools and Techniques	• Introduction to Anomaly Detection. • SCADA monitoring and updates. • Security Operations Center (SOC) and anomaly Detection on electric networks.
Topic-4: Penetration	• Specialised security tools and frameworks for different energy emerging technologies. • Hands-on practice with tools for vulnerability scanning, threat detection, and security configuration in a energy network.

3.11.1.3 Planning for Preparedness

The planning of a training session within the seminar CSP011_S_E can be scheduled in advance of the proposed courses. The deployment of a realistic simulating environment will be organised without connection to a network (for security reasons and ability to work on electrical networks). But a simulation platform could be arranged in advance (1 month delay) to organise a hands-on training session.

3.11.1.4 Materials and Exercises

Training material includes documentary support and power point presentation as well as the possibility of a simulating environment in a dedicated platform deployed in the facilities of the company's location (Toulon, – France or Mons – Belgium, Vilnius – Lithuania tob e confirmed).

3.11.1.5 Verification of Learning Outcomes, and Skills

A practical evaluation can be organised and the trainer will assess the learning outcomes and achievements for trainees. A questionnaire could be addressed to the trainees to assess the general knowledge on the provided courses during the seminar.

3.11.2 CSP011_S_E: Alerting, Reporting, and Monitoring Strategies for Cybersecurity in the Energy Sector

3.11.2.1 Description of Training Module

This module can reinforce fundamental concepts and provide hands-on experience with specific tools. Throughout CSP011_S_E, participants will delve into practical demonstrations and exercises focusing on the implementation of cybersecurity alerting, reporting, and monitoring strategies tailored specifically for the energy sector. Attendees will gain insights into configuring real-time threat notification systems, generating actionable reports, and setting up continuous infrastructure monitoring using cloud-based platforms. Moreover, participants will explore industry-specific challenges and learn how to proactively address security gaps to enhance organisational resilience against cyber threats.

This seminar is tailored for a diverse audience within the energy sector, including IT security professionals (especially entry level ones), system administrators, network engineers, managers, executives, and compliance officers. But, irrespective of their affiliation with the energy sector, IT security professionals, system administrators, network engineers, and individuals with a keen interest in

cybersecurity, including students and enthusiasts, stand to benefit significantly from attending this seminar.

CSP011_S_E offers a valuable opportunity for participants to acquire practical insights into cybersecurity strategies and to develop an understanding of industry challenges. Moreover, the hands-on demonstrations and exercises featured in the seminar serve to complement theoretical knowledge typically acquired in academic settings, thereby enriching participants' comprehension of cybersecurity concepts and tools through practical application.

Code *Code format: CSP011_x where x is the training of offering type (see below)*	**CSP011_S_E**
Module Title *The title of the training module*	**Alerting, Reporting, and Monitoring Strategies for Cybersecurity in the Energy Sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Energy Cyber: Securing Operations in the Energy Sector. • Cybersecurity Solutions for the Energy Industry. • Cyber Power: Navigating Cyber Ranges in Energy Operations. • Energy Shield: Protecting Critical Infrastructure from Cyber Threats. • Secure Energy: Enhancing Cyber Resilience in the Energy Industry. • Energy Defend: Fortifying Cyber Operations in the Energy Sector.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S (Seminar).
Level *Training level: B (Basic), A (Advanced)*	B (Basic).
Module overview *High-level module overview*	The seminar provides a comprehensive exploration of cybersecurity strategies specifically tailored for the energy sector. Attendees will gain practical insights through detailed demonstrations using the Security Infusion tool. The seminar covers topics such as real-time notifications for malicious

	activities, generating actionable reports on system status, and continuous monitoring of critical infrastructure via a cloud-based security information management system.
Module description *Indicates the main purpose and description of the module.*	This seminar offers a comprehensive exploration of cybersecurity strategies tailored specifically for the energy sector. Through detailed demonstrations featuring the Security Infusion tool, participants will gain practical insights into fortifying their cyber defences effectively. Attendees will discover how to configure a cloud-based security information management system to receive real-time notifications via email or Slack alerts, empowering IT service providers to swiftly respond to malicious activities. Hands-on exercises will guide participants in configuring notifications for security alerts to ensure rapid threat mitigation. Furthermore, the seminar will delve into generating insightful reports on system status, identifying new vulnerabilities, and providing actionable feedback. Participants will learn to utilise the Security Infusion tool to proactively address security gaps, enhancing the resilience of energy related systems against cyber threats. In addition, attendees will gain valuable expertise in using a security information management system to continuously monitor a critical infrastructure. They will master the navigation of a centralised dashboard, enabling 24x7 surveillance and analysis of historical events at a granular level. By the end of the seminar, participants will be equipped with the knowledge and skills necessary to enhance cybersecurity resilience in the energy industry and navigate the evolving threat landscape confidently.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	**Knowledge:** • Understanding of cyber ranges and their application in the energy sector. • Knowledge of common cyber threats and vulnerabilities specific to the energy sector. • Familiarity with real-time threat notification systems and their implementation. • Understanding of vulnerability management principles and practices in energy sector. • Knowledge of cloud-based security management platforms for continuous infrastructure monitoring. **Skills:** • Ability to set up and configure real-time threat notifications via email and Slack alerts. • Proficiency in using the Security Infusion tool for identifying and remediating vulnerabilities.

	• Skill in generating actionable reports on system status and vulnerabilities for stakeholders. • Competence in setting up and maintaining continuous infrastructure monitoring using cloud-based tools. • Skill in analysing historical events and trends to ensure 24x7 surveillance. **Competences:** • Competence in implementing effective cybersecurity strategies tailored to the energy sector. • Ability to respond swiftly and effectively to cybersecurity incidents in energy sector. • Competence in proactively identifying and addressing security gaps to enhance energy operations resilience.
Main topics and content list *A list of main topics and key content*	• Introduction to cyber ranges in the energy sector. • Real-time threat notifications and response. • Vulnerability management and reporting. • Continuous infrastructure monitoring with cloud-based tools. • Future trends and considerations in the energy domain.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	N/A.
Training Provider *Name(s) of training providers.*	ITML.
Contact *Name(s) of the main contact person and their email address.*	• Dimitra Siaili: disiaili@itml.gr
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	2 times x 2 hours or 4 hours.
Training method and provision	Physical or virtual.

Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.	
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-10: Cyber Incident Response. • KA-5: Network and Communication Security. • KA-8: Cybersecurity Tools and Technologies.
Pre-requisites	Basic IT and security Knowledge.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 2: Cyber Incident Responder.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Security Infusion.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English/Greek.
ECTS *If applicable, the number of ECTS.*	N/A.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.11.2.2 Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to Cyber Ranges in the Energy Sector	• Overview of cyber ranges and their significance in energy operations. • Discussion on cybersecurity challenges specific to the energy industry. • Case studies illustrating the importance of cyber ranges in energy infrastructure protection.
Topic-2: Real-time Threat Notifications and Response	• Demonstrations on setting up real-time threat notifications via email and Slack alerts using a cloud-based manager. • Examples of common cyber threats targeting energy infrastructure. • Best practices for swift and effective response to cyber incidents in the energy sector.
Topic-3: Vulnerability Management and Reporting	• Overview of vulnerability management principles in energy operations. • Hands-on exercises on using the Security Infusion tool to identify and remediate vulnerabilities. • Creating actionable reports on system status and vulnerabilities for stakeholders.
Topic-4: Continuous Infrastructure Monitoring with Cloud-Based Tools	• Introduction to cloud-based management platforms for infrastructure monitoring. • Live demonstration of setting up continuous monitoring of critical energy systems.

	• Demonstration of how to use a centralised dashboard to analyse historical events and ensure 24x7 surveillance and examining any low-level historical event, if needed.
Topic-5: Future Trends and Considerations in energy domain	• Discussion on the importance of ongoing education and training for cybersecurity professionals in the energy domain. • Reflection on key takeaways from the seminar and recommendations for continued improvement in energy cybersecurity strategies.

3.11.2.3 Planning for Preparedness

A meticulous preparatory phase is essential to facilitate the smooth transition into the training phase, during which participants will engage with the alerting, reporting, and monitoring Strategies for cybersecurity in the energy sector seminar.

Fundamental to this preparatory stage is the timely availability of all essential training materials on the DCM platform and/or relevant course management systems, ensuring accessibility and readiness prior to the commencement of training activities. Furthermore, the appointment of a central trainer, entrusted with primary responsibilities encompassing the development and management of topic presentations, oversight of practical activities, and the creation of tailored materials, underscores the structured approach to training delivery. While the central trainer assumes a pivotal role, provisions are made for the potential assignment of additional trainers during the training phase to address evolving needs and ensure comprehensive coverage. Flexibility is inherent in our approach, with training materials subject to modification to align with specific training requirements, including variations in lecture duration, audience demographics, situational dynamics, and technical considerations. This adaptive strategy necessitates additional time for material refinement and preparatory support for the deployment of live tools. Furthermore, feedback garnered from preceding training sessions informs iterative improvements, particularly concerning hardware enhancements, with responsibility for such enhancements resting with the central trainer.

3.11.2.4 Materials and Exercises

As part of the CSP011_S_E, comprehensive materials and exercises will be provided to participants via the DCM platform well in advance of the seminar launch. These materials are meticulously curated to offer a structured and engaging learning experience, ensuring participants grasp the essential concepts and strategies discussed during the seminar.

The seminar materials will include detailed presentations, instructional guides ,demos, videos, case studies, research analysis, discussions, development of lab exercises and supplementary resources covering a wide range of cybersecurity topics tailored specifically for the energy sector. Participants will have access to in-depth explanations of cybersecurity principles, industry best practices, and practical implementation strategies, all aimed at fortifying cyber defences within energy companies. In addition to the instructional materials, participants will engage in hands-on exercises designed to reinforce their understanding and application of cybersecurity strategies. These exercises will simulate real-world scenarios commonly encountered in the energy sector, allowing participants to practise configuring threat notification systems, generating reports, and implementing continuous monitoring solutions using cloud-based platforms.

Moreover, interactive elements within the materials and exercises will encourage active participation and foster collaboration among participants. The material subjects to the level of the module, that in this

case is basic. Trainers will always be mindful of the basic level of understanding among participants, while fostering an atmosphere conducive to open discussion and critical thinking. Material is based on these principles.

Overall, the seminar materials and exercises are thoughtfully designed to empower participants with the knowledge, skills, and confidence needed to enhance cybersecurity resilience within the energy sector.

3.11.2.5 Verification of Learning Outcomes, and Skills

Evaluation and verification of learning outcomes play a crucial role in ensuring the effectiveness of the seminar. Self-assessment forms a fundamental component, providing each participant with an opportunity to reflect on their learning journey and gauge their understanding of the cybersecurity strategies discussed. Additionally, evaluation from the trainer encompasses participant communication and interaction, with a focus on fostering critical thinking through open discussions. This collaborative environment not only enhances participants' comprehension of cybersecurity concepts but also encourages exploration of critical aspects specific to the energy domain. Upon successful completion of the seminar, participants will receive a certificate of attendance, acknowledging their dedication to expanding their knowledge of cybersecurity within the context of the energy sector. This certification serves as a testament to their commitment and signifies their readiness to apply their newfound knowledge in practical scenarios.

3.12 Module 12 - Digital Forensics for Energy

3.12.1.1 CSP012_S_E: Digital Forensics for Energy

3.12.1.2 Description of Training Module

The "Digital Forensics for Energy" seminar is an advanced training module that provides comprehensive insights into digital forensic practices tailored specifically for the energy sector. This seminar explores the nuances of conducting forensic examinations within energy infrastructures like SCADA systems and smart grids, aiming to equip participants with the skills necessary to undertake digital forensic investigations that address cybercriminal activities and generate legally sound digital evidence in the energy context. The module is designed for professionals such as forensic analysts, incident responders, and cybersecurity specialists in the energy sector, focusing on practical applications of digital forensics to protect critical energy infrastructure.

Code *Code format: CSP012_x where x is the training of offering type (see below)*	**CSP012_S_E**
Module Title *The title of the training module*	**Digital Forensics for Energy**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	• Cyber Forensics in the Energy Sector. • Digital Investigation and Analysis in Energy Infrastructure. • Energy Forensics. • Cybercrime Forensics in the Energy Grid. • Incident Response and Forensics in the Energy Grid. • Energy Data Forensics.

	• Energy Forensic Cybersecurity. • Energy Information Forensics.
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S).
Level *Training level: B (Basic), A (Advanced)*	Advanced (A).
Module overview *High-level module overview*	The module introduces learners to digital forensics to equip them with the knowledge and skills to undertake cybercriminal investigations that produce digital evidence that may prove a malicious activity in the energy sector.
Module description *Indicates the main purpose and description of the module.*	This seminar provides a set of terms and concepts associated with digital forensics, specifically applied to the energy sector. It introduces the learner to digital forensics and techniques for conducting forensic examinations in energy infrastructures (e.g. SCADA systems and smart grids).
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** • Knowledge of digital forensics methods, best practices and tools. • Knowledge of energy digital forensics analysis and testing techniques. • Knowledge of cyber threats and vulnerabilities. • Advanced knowledge of energy cybersecurity attack tactics and techniques. **Competences and skills:** • Critical thinking and problem-solving in complex digital forensic scenarios. • Ability to analyse and visualise digital evidence, identify relevant indicators, and draw sound conclusions.

	• Effective communication and presentation skills to articulate technical findings to technical and non-technical audiences. • Independent ability to conduct and manage digital forensic investigations in the energy sector from start to finish.
Main topics and content list *A list of main topics and key content*	• Introduction to digital forensics. • Tools for energy digital forensics. • Data/evidence acquisition. • Legal aspects of digital forensics. • Digital forensics analyses (including energy sector specific). • Computing investigation and crime processing (including energy sector specific). • Metwork forensics and incident response (including energy sector specific). • Digital forensics reporting and presentation. • Advanced topics in digital forensics.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Knowledge-based assessment**: through two evaluation tests; one launched at the beginning of the seminar (pre-assessment), and another (with the same evaluation content as the first test) at the end of the seminar (post-assessment) to verify that the new knowledge has been correctly acquired. Likewise, learners will have report analysis about specific case studies focused on the energy sector.
Training Provider *Name(s) of training providers.*	UNINOVA, FCT, and PDMFC.
Contact *Name(s) of the main contact person and their email address.*	• Ruben Costa: rddc@uninova.pt • José Manuel Fonseca: jmrf@fct.unl.pt • Luis Miguel Campos: luis.campos@pdmfc.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g. even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	20 hours.

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical or Virtual. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: • KA-1: Cybersecurity Management. • KA-10: Cyber Incident Response. Nonetheless, minor content matches with other including: • KA-2: Human Aspects of Cybersecurity.
Pre-requisites	Basic knowledge of cybersecurity essentials (related to CSP Module 1) and basic IT training.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	• ECSF Profile 2: Cyber Incident Responder. • ECSF Profile 11: Digital Forensics Investigator.
Tools to be used *A list of tools that will be used for the operation of this training module.*	FTK Imager, Autopsy.

Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Portuguese.
ECTS *If applicable, the number of ECTS.*	N/A.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes.
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

3.12.1.3 Adapted Syllabus

Main topics	Suggested Content
Topic 1: Introduction to Digital Forensics	• Understand the fundamentals of general forensic science and digital forensics. • Benefits and process of digital forensics. • Digital forensics process.
Topic 2: Tools for Energy Digital Forensics	• Hardware and software selection and validation. • Energy digital forensics quality assurance.
Topic 3: Data/evidence acquisition	• Understanding data storage formats and digital evidence. • Acquisition tools and determination of best acquisition methods. • Validation of data acquisitions.

Topic 4: Legal aspects of digital forensics	• Understanding the legal aspects of digital forensics and their impact on digital forensics.
Topic 5: Digital forensics analyses	• Malware analysis. • Volatile memory analysis. • Timeline analysis. • Intrusion analysis.
Topic 6: Computing investigation and crime processing	• Digital forensics process model: introduction to energy cybercrime scene. • Scene and evidence documentation. • Chain of custody. • Forensic evidence cloning. • Integrity of evidence; reporting.
Topic 7: Network Forensics and Incident Response	• Investigating energy network intrusions and cyberattacks through digital evidence analysis. • Incident response procedures and evidence collection in energy cybercrime scenarios.
Topic 8: Digital Forensics Reporting and Presentation	• Writing comprehensive digital forensic reports, documenting findings and analysis. • Presenting digital evidence effectively in court, legal proceedings, and technical settings. • Visualising complex digital forensic data for clear communication.
Topic 9: Advanced Topics in Digital Forensics	• Cloud forensics and investigating evidence stored in cloud platforms. • Emerging trends and challenges in energy digital forensics (cybercrime evolution, IoT forensics, smarty grids).

3.12.1.4 Planning for Preparedness

Preparation for the "Digital Forensics for Energy" seminar (CSP012_S_E) involves coordinated efforts among trainers to align the seminar's content with the unique demands of forensic practices in the energy sector. A structured action plan delineates the responsibilities of each trainer, who will develop tailored content, manage logistical arrangements, and ensure all resources such as case studies, forensic tools, and reading materials are accessible on the seminar's learning management system before the seminar begins. This preparation ensures that trainers are ready to deliver a seamless educational experience, emphasizing the application of digital forensics in energy scenarios.

3.12.1.5 Materials and Exercises

The materials for the seminar CSP012_S_E include detailed lecture notes, slides, real-life case studies, and a suite of digital forensic tools relevant to the energy sector. Exercises are designed to be hands-on and scenario-based, allowing participants to practise skills such as data acquisition, analysis, and reporting within the context of energy cyber infrastructures. Participants will engage in simulations that mimic real-world forensic challenges in energy systems, enhancing their ability to apply theoretical

knowledge in practical settings. These exercises aim to develop proficiency in using forensic tools and techniques to investigate and respond to incidents in energy networks.

3.12.1.6 Verification of Learning Outcomes, and Skills

To assess and verify the learning outcomes, the seminar employs a combination of formative and summative assessments. Formative assessments occur throughout the seminar to monitor progress and adjust teaching strategies as needed. Summative assessments include practical exercises and final evaluations that test participants' abilities to conduct comprehensive digital forensic investigations in the energy sector. These assessments measure participants' competence in handling complex forensic scenarios, ensuring they can effectively apply their skills to protect critical energy infrastructures from cyber threats.

4 Conclusions

This deliverable details 12 CSP energy-specific training modules, which have been methodically designed to promote cybersecurity knowledge and skills to the particular features and needs of the energy sector. More specifically, the 12 modules comprise the syllabus and the conditions necessary to cover a set of CSP knowledge areas, which were also extracted from the study performed in D2.1. Through these syllabi, CSP consortium pursues to enable existing or future experts of the energy sector to be equipped and prepared against unforeseen situations. To do this, a working methodology has been established to reach the expected synergy between tasks (T3.1 and T3.5), and the adaptation and parametrisation of the D3.1 syllabi. The transition between tasks (T3.1 and T3.5) has taken a natural process, equivalent to those carried out in T3.4 and T3.6 (about training programme for the health and maritime sectors, respectively), allowing the leaders to perform coordinated actions.

By applying this methodology, each module has been adapted considering the templates outlined in D3.1 and the CyBok framework to ensure its effectiveness in the learning process and practicality to the particular security issues that arise today the energy sector. For the operational plan of the modules, the CSP partners have established different ways and opportunities to provide the learning modules, either through courses, seminars, workshops, summer schools, hackathon, laboratory exercises, among others, where they may, for example, be incorporated as supplementary or additional resource to existing or new programmes of Higher Education Institutions (HEIs).

Through these resources, CSP partners seek to distribute knowledge related to the particularities of the sector. For example, HEIs could propose specific studies using the CSP resources as supplementary material in order to prepare the future experts to the individual challenges of the sector. Professionals in the sector could also benefit from these resources by intensifying or refreshing knowledge. As stated throughout this deliverable, these resources do not only contain purely theoretical topics but also practical exercises, placing furture experts or professionals in complex situations where they must demonstrate the capabilities and skills necessary to understand the risk and mitigate it

5 References

[1] M. Breque, L. De Nul, A. Petridis, , “Indsutry 5.0, Towards a sustainable, human-centric and resilient European industry”, European Comision 2021.
[Available] URL: https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/ (last access in April 2024).

[2] H. Bahsi, H. Ochieng‘Dola, S. M. Khalil, T. Korõtko, “A cyber attack taxonomy for microgrid systems”. In 2022 17th Annual System of Systems Engineering Conference (SOSE), pp. 324-331, IEEE, 2022.

[3] I. Zografopoulos, N. D. Hatziargyriou, C. Konstantinou, “Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations”, IEEE Systems Journal, 2023.

[4] ENISA, “ENISA Threat Landscape 2023”, 2023. [Available] URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (last access in April 2024).

[5] ENISA, “Smart Grid Threat Landscape and Good Practice Guide”, December 2013, [Available] URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide (last access in April 2024).

[6] ENISA, “European Cybersecurity Skills Framework Role Profiles”, September 2022. [Available] URL: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (last access in April 2024).

[7] EnergiCERT, “Cyber Attacks Against European Energy & Utility Companies”, September 2022.
[Available] URL: https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf (last access in April 2024).

[8] University of Bristol, Cyber Security Body of Knowledge, 2002-2020. [Available] URL: https://www.CyBoK.org (last access in April 2024).