# The Cybersecurity education in smart grids Body of Knowledge development and implementation roadmap

Authors:

Rūta Pirta-Dreimane, Andrejs Romānovs, Jana Bikovska, Jānis Pekša, Maria Valliou, Panos Kotsampopoulos, Bahaa Eltahawy, Tero Vartiainen, Mike Mekkanen, Jirapa Kamsamrong

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 4

Riga Technical University, University of Vaasa, National Technical University of Athens, University of Oldenburg

This project has received funding from the European Union’s Erasmus+ Programme under Grant Agreement № 2020-1-FI01-KA203-066624.

# Contents

# Abbreviations

| | |
|---|---|
| ACM | Association for Computing Machinery |
| NICE | National Initiative for Cybersecurity Education |
| CC-RSG | Cybersecurity Curricula Recommendations for Smart Grids |
| CPES | Center for Power Electronics Systems |
| ENISA | European Network and Information Security Agency |
| EU | European Union |
| JTF | Joint Task Force |
| IT | Information Technology |
| IO | Intellectual output |
| MOOC | Massive online open courses |
| NIST | National Institute of Standards and Technology |
| PMU | Phasor Measurement Unit |
| OT | Operational Technology |
| SCADA | Supervisory control and data acquisition |
| SMEs | Small and medium-sized enterprises |
| VET | Vocational education and training |
| WP | Work Package |

# Executive summary

This document represents part of the project “Cybersecurity Curricula Recommendations for Smart Grids” (CC-RSG) Work Package 4 (WP4) outcomes. The document aims to conceptualise knowledge and provide recommendations for the development of cybersecurity curricula for smart grids.

Within WP4 a model for specific educational curricula is proposed. It consists of three core elements: education curricula content, education programme design methodology, tools and methods bank.

Ten work roles have been defined for the curriculum content model, which are the most relevant in the field of cybersecurity in smart grids. For each work role, key tasks are defined, and smart grid-specific competences are described.

The knowledge areas and units are adopted based on the “ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020” Association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC). In addition, a specific Smart Grid Security Knowledge Unit is developed to focus on protecting the assets and the data of the grid from unauthorized access or any sorts of malicious activities that might result in malfunction or degradation of the grid performance.

Next, the method and tools bank suggest methods and toolbox that study programme designers and educators can use in all education development process phases (analysis, design, development, implementation and evaluation). The following tools and methods recommended as the most effective: simulation tools, CPES labs and testbeds; gamification; experiential/active learning; problem-based/project-based learning; flipped classroom; cooperative learning.

The benchmarking of the proposed approach is done to gain insights regarding the aspects that can be further improved. First, through a literature review, the characteristics that benefit the modern educational approaches identified, and secondly, a questionnaire was formulated to have the perspective of the project training event participants.

Finally, an implementation roadmap is developed to support the successful implementation of the developed curricula model. t outlines the actions required and proposes a timetable for implementation.

# 1. Introduction

Cybersecurity is defined as one of European strategic capabilities and it has been acknowledged that the EU must significantly improve its digital capacities in the cybersecurity field [1]. This includes the deployment of digital technologies, as well as the necessary digital skills for all EU workforces. Cybersecurity is interdisciplinary subject [2]- [3], to ensure all critical competences, several dimensions and disciplines must be integrated in education programs, such as computer science, engineering, psychology, sociology, and law. Cybersecurity specialists must have deep technical knowledge, meantime, also general skills are essential, especially in crisis situations.

Environment of smart grids involves additional complexity in terms of the cybersecurity. Smart grid integrates variety of sensors, control systems and communication networks what increases the cyberattack surface. Cybersecurity specialists working in the smart grid environment must have wide range of competences to protect the infrastructure, balancing cybersecurity and electrical engineering competences, along with the soft skills.

## 1.1 Background and Objectives

This document represents the project “Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)” WP4 outcome. This work activity aims to conceptualize knowledge gained in the project and provide recommendations for cybersecurity curricula development for smart grids.

This document considers the results of previous project intellectual outputs (IOs):

- **IO.1. State of the Art, Trends and Skill gaps in Cybersecurity in Smart Grids** presents the state of the art of education offering in smart grids cybersecurity, highlights the skill gaps and defines requirements towards educational programs.
- **IO.2. Strategy for Cybersecurity Education in Smart Grids** defines challenges that the industry faces in the field of cybersecurity in smart grids, proposes their mitigation plan and provides recommendations to education providers, policy makers and the industry.
- **IO.3. Massive Open Online Course for Cybersecurity in Smart Grids** summarize the cybersecurity in smart grids knowledges in the form of open online course.

The main objectives of the document is to provide recommendations for educators and other relevant parties for educational programs development, considering, industry needs, workforce requirements, student-centric educational methods and emerging support tools.

## 1.2 Audience

The main audience of the document are:

- **Designers of educational programs** of cybersecurity in smart grids, that can consider recommendations in the educational programs development.
- **Energy industry representatives** that can take into consideration work roles profiles in enterprise operating model designing.
- **Energy citizens** that can identify required competences to use energy systems and connected devices in a secure manner.

# 2. Model for Education Curricula

The aim of the model is to provide guidance for competence-driven cybersecurity education programs for smart grids design, execution and evaluation. The model explains how body of knowledge (e.g., this document) should be used to enable workforce and education dimensions integration.

The model is based on the methodology proposed in [4] and it consists of three key building blocks (Figure 1):

1. **Education curricula content** defines roles and tasks-specific competences and associated knowledge areas, knowledge units, learning topics and learning outcomes.
2. **Education program design methodology** suggests study programs and courses design, execution and evaluation principles and process.
3. **Tools and methods bank** includes methods and tools list and their usage guidance (patterns), that can be used in cybersecurity education programs for smart grids design, execution and evaluation.

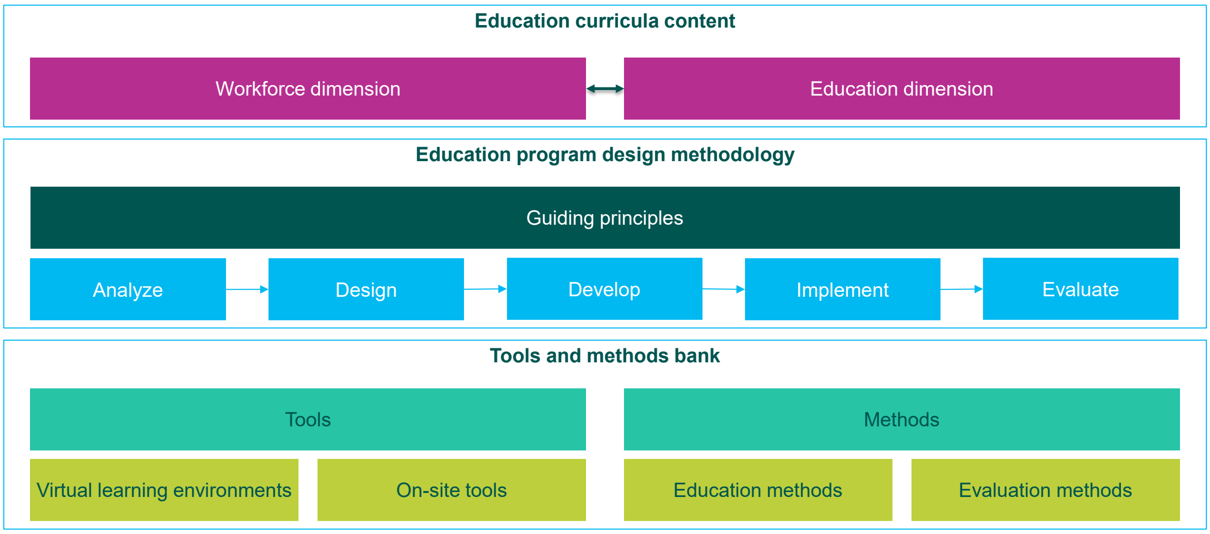


Figure 1 Model for Education Curricula Overview

## 2.1 Education Curricula Content Model

Education curricula must be designed based on workforce requirements to ensure that cybersecurity specialists competences meet industry demand, including skills that need to be taught and areas of expertise that need to be covered [2].

The proposed model for education curricula incorporates two dimensions – workforce dimension and education dimension (Figure 2).

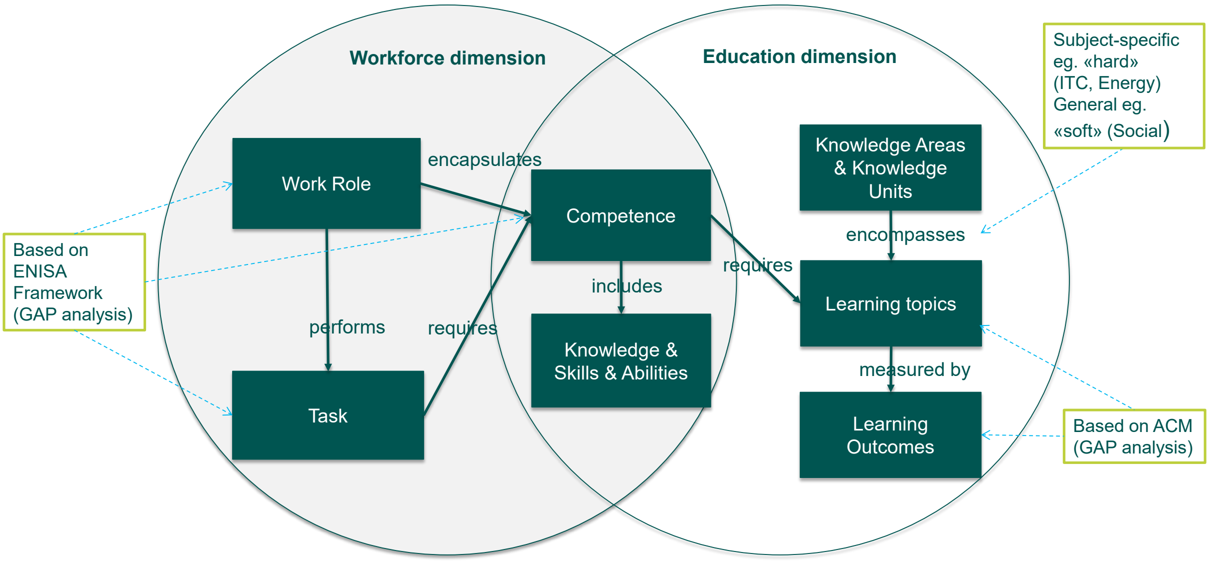

Workforce dimension
Education dimension
Subject-specific eg. «hard» (ITC, Energy) General eg. «soft» (Social)
Work Role
encapsulates
Competence
Knowledge Areas & Knowledge Units
encompasses
Based on ENISA Framework (GAP analysis)
requires
Learning topics
includes
performs
requires
Knowledge & Skills & Abilities
measured by
Task
Learning Outcomes
Based on ACM (GAP analysis)

Figure 2 Model for Education Curricula Content

The workforce dimension includes the following key concepts [5]:

- **Work roles** are the most detailed groupings of cybersecurity-related work, including a list of attributes, i.e. knowledge, skills, and abilities required to perform tasks associated with the role.
- **Tasks** represent specific defined pieces of work that, combined with other identified tasks, compose the work scope in a specialty area or work role.
- **Competencies** describe capabilities of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position. It is important to distinguish the capabilities between subject-specific (eg., “hard skills”) and general (eg., “soft-skills”). Hard skills include technical or administrative competence. Soft skills are a cluster of productive personality traits that characterize one's relationships in a social environment. These skills can include social graces, communication abilities, language skills, personal habits, cognitive or emotional empathy, time management, teamwork and leadership traits.

Several frameworks define cybersecurity related roles, associated tasks and required competences, for example, National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST NICE framework) [5] and the European Union Agency for Cybersecurity (ENISA) skill framework (ENISA framework) [6].

NIST NICE framework defines cybersecurity roles, describes tasks statements and the knowledge, skills and abilities statements required to perform the tasks. According to the NIST NICE framework, these statements are the foundation for cybersecurity education.

ENISA has released draft version of cybersecurity skills framework (final version to be released in Q4 2022). The model aims [6]: “to create a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage". Additionally, it is planned that the model will support the design of cybersecurity-related training programs for skills and career development.

For cybersecurity education in smart grids, it is suggested to use ENISA competence model as basis for education programs design, as it has simpler work roles structure comparing to NIST. NIST roles are mainly designed for large enterprises, therefore they represent siloed cybersecurity capabilities split across organization. Empirical observations shows that enterprises typically combine similar roles and enable "T-shaped" competences and multi-functional teams.

Existing cybersecurity competence models focuses on cybersecurity governance and IT-specific cybersecurity aspects, but they don't address smart-grids cybersecurity roles, tasks and competences. Therefore smart-grids cybersecurity specific tasks are incorporated into ENISA model (Section 3.2.). Tasks and competences are suggested by project expert team (Section 3). Therefore, this document defines reference model for smart-grid cybersecurity roles and tasks that is basis for relevant education programs design.

The workforce dimension interferes with education dimension via competences, that includes skills, abilities and knowledges. The education dimension includes following key concepts [7]:

- **Knowledge areas** and **knowledge units** are thematic grouping that encompasses multiple, related **learning topics**.
- **Learning outcomes** represent more detailed outcomes than the competencies and may be seen as course or lesson learning outcomes. Learning outcomes emphasize what students can do over merely what students know.

Several cybersecurity curriculum recommendations suggest main knowledge areas, knowledge units, learning topics and learning outcomes. For example, Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) prepared by Association for Computing Machinery Committee for Computing Education in Community Colleges [7] and CSEC2017 Joint Task Force on Cybersecurity Education (JTF) global cybersecurity curricular recommendations [3].

The JTF recommendations are based on a comprehensive view of the cybersecurity field, the base discipline's specific demands, and the relationship between the curriculum and cybersecurity workforce frameworks. The JTF emphasizes that cyber- security is an interdisciplinary course of study, including law, policy, human factors, ethics, risk management, and computing. The model consists of 8 knowledge areas - data, software, component, connection, system, human, organization, societal and eight cross-cutting concepts - confidentiality, integrity, availability, risk, negative thinking, and systems thinking.

Cyber2yr2020 is based on CSEC2017 and inspired by CAE-CD 2Y knowledge units [8] and NIST NICE [5]. The guidance focuses on competencies and learning outcomes. The Cyber2yr2020 competencies include the ability to describe various human factors that could affect privacy and security and the ability to compare different mental models and their impact on the user's response to cybersecurity risks. The model consists of 8 knowledge areas - data security, software security, components security, connection security, system security, human security, organizational security, social security.

For cybersecurity education in smart grids it is suggested apply Cyber2yr2020 guidelines for IT specific cybersecurity knowledge units, knowledge areas, topics and learning outcomes definition. Smart grids specific cybersecurity education are addressed limited in existing frameworks, therefore smart-grids cybersecurity specific competences, learning topics and learning outcomes are incorporated into Cyber2yr2020 model. Smart-grid specific cybersecurity competences, learning topics and learning outcomes are suggested by project experts team (Section 3.3.).

In this document, the competences are divided in four groups:

- IT-specific competences define knowledge, abilities and skills required to perform IT-specific cybersecurity tasks. These competences are based on Cyber2yr2020 guidelines (only essential competences). These competences defines ‘‘what is to be done’’ aspects [7].
- Smart-Grids -specific competences define knowledge, abilities and skills required to perform smart grids-specific cybersecurity tasks. These competences are prepared by project experts team and validated with industry experts. These competences defines ‘‘what is to be done’’ aspects [7].
- Operational competences compile managerial and operational competences what defines ‘‘how activities should be done’’ in both – IT specific and smart-grids specific areas.
- General competences define expected “soft skills”.

## 2.2 Education Program Design Methodology

Education program design methodology defines general principles what need to be followed and main steps how education program should be defined (Figure 2). In program definition, execution and evaluation educators can use smart grid cybersecurity competence model and curricular content recommendations described in this document. However, precise content must be aligned to program learner profiles and their needs (target roles etc.).

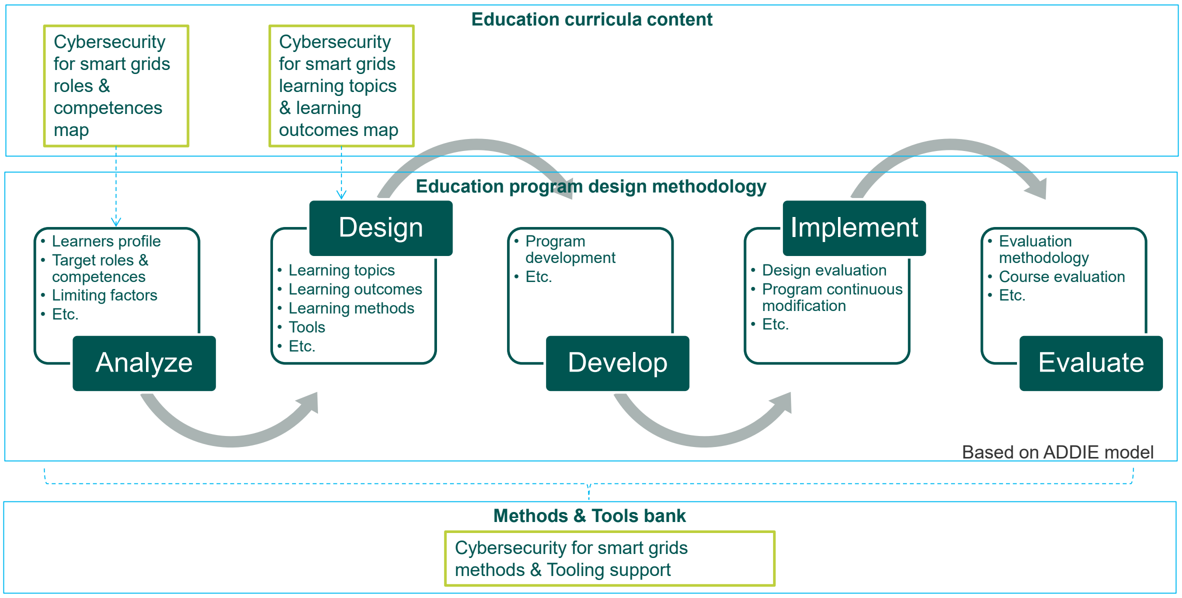

Education curricula content
Cybersecurity for smart grids roles & competences map
Cybersecurity for smart grids learning topics & learning outcomes map
Education program design methodology
• Learners profile
• Target roles & competences
• Limiting factors
• Etc.
Analyze
Design
• Learning topics
• Learning outcomes
• Learning methods
• Tools
• Etc.
• Program development
• Etc.
Develop
Implement
• Design evaluation
• Program continuous modification
• Etc.
• Evaluation methodology
• Course evaluation
• Etc.
Evaluate
Based on ADDIE model
Methods & Tools bank
Cybersecurity for smart grids methods & Tooling support

Figure 3 Education Program Design Methodology

Education programs should be prepared following several guiding principles. According to design thinking approach regarding the usage in educational design [9], [10] design principles are frequently used to state main direction that must be followed in programs design and execution [11]. The design principles are defined as [10]: "'...an intermediate step between scientific findings, which must be generalized and replicable, and local experiences or examples that come up in practice. Because of the need to interpret design-principles, they are not as readily falsifiable as scientific laws. The principles are generated inductively from prior examples of success and are subject to refinement over time as others try to adapt them to their own experiences". Design principles elicit design knowledge from successful learning environments [11] and summarize reusable best practices.

For cybersecurity education in smart grids, it is suggested to follow such key principles (Figure 4):

1) **Target roles and tasks driven competence design** - competences must be defined based on learners' target roles to enable workforce and education dimensions integration.
2) **Learner centricity and personalization** – study programs must focus on students needs and provide profile specific competence development.
3) **Subject-specific and general competences synergy** – general competences must be integrated in every learning topic along with subject-specific competences.
4) **Real-world experiences integration** – study programs and courses content must reflect real-world challenges and must adapt over times.
5) **Vertical integration** – cybersecurity is multi-disciplinary subject, programs must integrate social sciences (as psychology) to enable general competences development.
6) **Feedback based continuous improvement** – continuous improvement must be planned based on learners and workforce feedbacks.

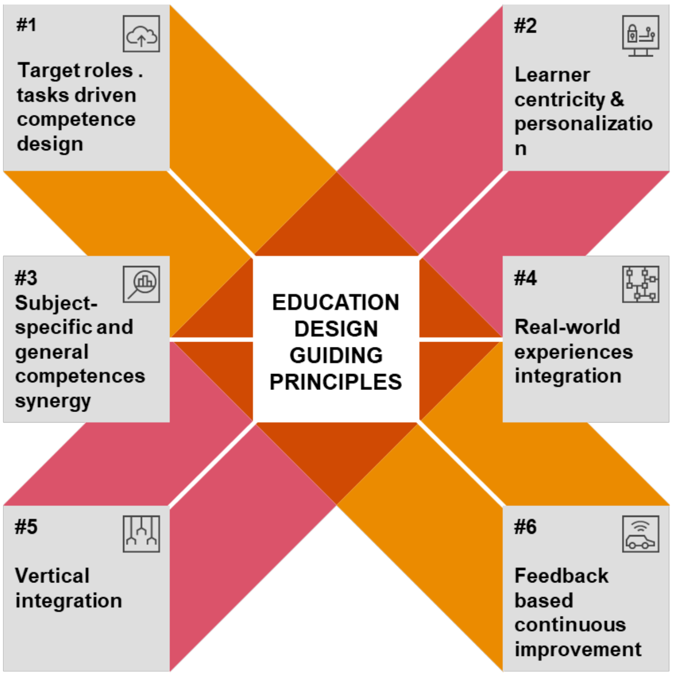

#1
Target roles . tasks driven competence design
#2
Learner centricity & personalizatio n
#3
Subject-specific and general competences synergy
EDUCATION DESIGN GUIDING PRINCIPLES
#4
Real-world experiences integration
#5
Vertical integration
#6
Feedback based continuous improvement

Figure 3 Education Program Design Principles

The suggested education program design process is based on ADDIE model [12]. The ADDIE model is the generic process traditionally used by instructional designers and training developers. The model includes five phases:

1. **Analysis** - learners profiles analysis (including their characteristics, existing competence, expected target roles and training needs), instructional goals and objectives definition. The program must be designed to incorporate competences that are required for learners' target roles. This document includes typical cybersecurity roles that are enriched with smart-grid specific cybersecurity tasks and competences (Section 3.2.). This document can be used as reference model for learner's target roles mapping. The roles are designed based on identified typical smart grid cybersecurity learners profiles (Section 3.1.) that are defined based on project experts experience.
2. **Design –** study program objectives, learning topics, learning outcomes and teaching methods definition. This document defines set of learning topics and learning outcomes that defined roles must have (Section 3.3.). The topics are encapsulated in knowledge areas and units. The topics must be selected based on identified learners target roles. Learners can have individual plans, based on their existing competences (eg., if learner has previous education in IT specific cybersecurity and he aims to became Security architect in energy sector institution, he/she must obtain smart grid specific cybersecurity competences). The document includes methods bank (Section 4) and tools bank (Section 5) that can be used for education program design support.
3. **Development** – study program materials development and loading in e-learning systems (if applicable).
4. **Implementation – actual program and courses delivery.**
5. **Evaluation –** feedback and data collection for improvement areas identification. The document includes methods bank (Section 4) and tools bank (Section 5) that can be used for education program evaluation support.

This document mainly focuses on "Design" phase and it provides recommendations for roles and tasks required competences in smart grid cybersecurity.

The education program design process can be supported by tools and methods, defined in methods and tools bank (Section 4).

## 2.3 Methods and Tools Bank

The methods bank and the tools bank (Section 4) suggest methods and toolbox that study program designers and educators can use in all education development process phases (analysis, design, development, implementation and evaluation). Methods and tools are defined in form of reusable patterns forming knowledge base for courses design and execution support. Methods and tools linkage to education design and execution process phases are described on each method /tool card.

# 3. Education Curricula Recommendations

Education curricula recommendations forms reference model for workforce and education integration. It includes such main concepts:

- **Learners profiles** – typical smart grid cybersecurity learners profiles provides grounds for target work roles definition;
- **Work roles and tasks** represent learners target roles, tasks and required competences (including, IT-specific cybersecurity competences, smart grid specific cybersecurity competences, operational and general competences);
- **Knowledge units and knowledge areas** define **learning topics and learning outcomes** required to obtain competences.

The recommendations are prepared based on methodology described in the Section 2.

## 3.1 Learners Profiles

The purpose of the student profile is to highlight student groups to which the curriculum model can be applied.

Here two groups of graduates who can be interested in continuing their education in the area of cybersecurity for smart grids can be highlighted: graduates in computing area and graduates in power systems.

The other two groups are professionals either IT&OT or management of smart grids. They have work experience in power systems and smart grids however they need more advanced knowledge in cybersecurity for smart grids.

Learners' profiles are summarised in the Table below

| Profile name<br>Attributes | Graduated student (Computing) | Graduated student<br>(Power Systems) | Professional<br>(IT&OT) | Professional<br>(Smart Grids)<br>*policy makers* |
|---|---|---|---|---|
| Background | STEM, Computing | STEM, Power Systems | Power Systems | Management |
| Educational needs | Basic knowledge in power systems and smart grids,<br>advanced knowledge in cybersecurity | Basic knowledge in computer systems and cybersecurity, advanced knowledge in power systems | Advanced knowledge in smart grids and cybersecurity | Advanced knowledge in smart grids and cybersecurity |
| Expectations | Ability to address cybersecurity | Ability to address cybersecurity | Knowledge of modern cybersecurity tools and standards and | Knowledge of cybersecurity processes and standards, ability to |

| | | | | |
|---|---|---|---|---|
| | problems in smart grids | problems in smart grids | their application in smart grids, ability to develop cybersecurity scenarios to protect smart grid infrastructure | develop cybersecurity strategy for smart grids |

The following attributes are considered for the profile:

- background refers to educational attainment or professional skills of a learner;
- educational needs is the gap between the learner's current level of knowledge, skills, and attitudes and the desired one, in order to adapt to a new situation which can be acquired through education,
- Expectations describe the knowledge and skills that students are expected to demonstrate by the end the studies.

The energy industry needs a cybersecurity-literate workforce, and higher education could play a valuable role in filling the gap.

## 3.2. Work Roles and Tasks

The practical-oriented selection from European Cybersecurity Skills Framework Work Roles, does not include out of scope not primary learners target roles, therefore Cyber Threat Intelligence Specialist, Cybersecurity Researcher, Cybersecurity Educator, Digital Forensics Investigator, and Penetration Tester are not selected. For selection has been taken Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Implementer, and Cybersecurity Risk Manager. Existing tasks have been taken and supplemented according to the specifics of the smart grid.

The ENISA roles were supplemented by new roles considering the specifics of the smart-grids – Energy Citizen, Grid Assets Manager and Grid Communication Engineer. The common business objectives for smart-grid specific roles are [13]: maintain safety, maintain power system reliability, maintain power system resilience and support grid modernization.

### 3.2.1. Chief Information Security Officer

| Name | **Chief Information Security Officer** |
|---|---|
| Description [6] | Manages an organization's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected. |
| Tasks (general tasks [6], supplemented | • TCISO01. Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organizational objectives. |

| | |
|---|---|
| by smart-grid specific tasks) | • TCISO02. Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organization and ensure their execution.<br>• TCISO03. Supervise the application and improvement of the Information Security Management System (ISMS).<br>• TCISO04. Educate senior management about cybersecurity risks, threats and their impact on the organization.<br>• TCISO05. Ensure the senior management approves the cybersecurity risks of the organization.<br>• TCISO06. Develop cybersecurity plans.<br>• TCISO07. Develop relationships with cybersecurity-related authorities and communities.<br>• TCISO08. Report cybersecurity incidents, risks, findings to the senior management.<br>• TCISO09. Monitor advancement in cybersecurity.<br>• TCISO10. Secure resources to implement the cybersecurity strategy.<br>• TCISO11. Negotiate the cybersecurity budget with the senior management.<br>• TCISO12. Ensure the organization's resiliency to cyber incidents.<br>• TCISO13. Manage continuous capacity building within the organization.<br>• TCISO14. Review, plan and allocate appropriate cybersecurity resources. |
| IT-specific Competence | N/A |
| Smart-Grid - specific Competences | • SGC001. Identity and understand the organization's role in the supply chain [13].<br>• SGC002. Identify and understand the placement of their organization in the grid infrastructure to help manage and avoid cascading effects [13].<br>• SGC003. Understand smart grid impact to cybersecurity (for example, the dependence on bi-directional, real-time data flows) [13].<br>• SGC004.Determine organizational risk tolerance while considering the potential cascading effects on the immediate geographic area, larger region, and the energy sector overall [13].<br>• SGC005. Understand the stakeholder landscape in the modernized grid [13]. |
| Operational Competences [6] | • OC001. Assess and enhance an organization's cybersecurity posture<br>• OC002. Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks.<br>• OC003. Analyse and comply with cybersecurity-related laws, regulations and legislations.<br>• OC004. Implement cybersecurity recommendations and best practices.<br>• OC005. Manage cybersecurity resources.<br>• OC006. Develop, champion and lead the execution of a cybersecurity strategy.<br>• OC007. Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing. |

| | |
|---|---|
| | • OC008. Review and enhance security documents, reports, SLAs and ensure the security objectives.<br>• OC009. Identify and solve cybersecurity-related issues.<br>• OC010. Establish a cybersecurity plan.<br>• OC011. Anticipate required changes to the organisation’s information security strategy and formulate new plans.<br>• OC012. Define and apply maturity models for cybersecurity management.<br>• OC013. Anticipate cybersecurity threats, needs and upcoming challenges. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>• GC002. Influence an organization's cybersecurity culture.<br>• GC003. Motivate and encourage people.<br>• GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16].<br>• GC005. Manage relationships [15].<br>• GC006. Manage conflicts and solve problems [2], [15], [14].<br>• GC007. Manage changes [15].<br>• GC008. Present effectively [2].<br>• GC009. Teach others [2].<br>• GC010. Manage time, people, assets and projects [15].<br>• GC014. Work under pressure [17]. |

### 3.2.2. Cyber Incident Responder

| | |
|---|---|
| Name | **Cyber Incident Responder** |
| Description [6] | Monitor the organization's cybersecurity state, manage incidents during cyber-attacks and ensure the continued operations of ICT systems. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks) | • TCIRO01. Contribute to the development, maintenance and assessment of the Incident Response Plan<br>• TCIRO02. Develop, implement and assess procedures related to incident handling<br>• TCIRO03. Identify, analyse, mitigate and communicate cybersecurity incidents<br>• TCIRO04. Assess and manage technical vulnerabilities, including vulnerabilities of modernized distributed energy resources<br>• TCIRO05. Measure cybersecurity incidents detection and response effectiveness<br>• TCIRO06. Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident<br>• TCIRO07. Adopt and develop incident handling testing techniques<br>• TCIRO08. Establish procedures for incident results analysis and incident handling reporting<br>• TCIRO09. Document incident results analysis and incident handling actions<br>• TCIRO10. Cooperate with Secure Operation Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs)<br>• TCIRO11. Cooperate with key personnel for reporting of security incidents according to applicable legal framework. |

| | |
|---|---|
| | • TSG01.  Decide on the use of Historian and/or Intrusion Detection Systems to make sure the system will always operate in a safe state<br>• TSG02. Design physical failsafe's to counteract potential cyber sabotage<br>• TSG03 Determine how the distributed resources of a smart grid are part of the energy restoration plans [13].<br>• TCRM09. Determine how the proposed Incident Response Plan will affect the other stakeholders (external to the company but interconnected because of the system) [13]. |
| IT-specific Competences | • TC001. Work on operating systems, servers, clouds and relevant infrastructures.<br>• TC002. Manage and analyze log files.<br>• TC003. Collect, analyse and correlate cyber threat information originating from multiple sources. |
| Smart-Grid - specific Competences | • SGC006. Create an Incident Response Plan that considers the requirements of the grid's components (procedures to shut down, procedures to start up, requirements coming from the batteries, requirements coming from the generators).<br>• SGC007. Train and educate the personnel for the power restoration processes [13].<br>• SGC008. Understand intelligent and distributed technologies such as advanced metering infrastructure (AMI) and automated distribution management systems [13].<br>• SGC003. Understand smart grid impact to cybersecurity (for example, the dependence on bi-directional, real-time data flows) [13].<br>• SGC009. Understand and monitor vulnerabilities of modernized distributed energy resources [13]. |
| Operational Competences | • OC014. Practice all technical, functional and operational aspects of cybersecurity incident handling and response. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>• GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16].<br>• GC006. Manage conflicts and solve problems [2], [15], [14].<br>• GC014. Work under pressure [17].<br>• GC015. Collaborate effectively in a team [18]. |

### 3.2.3. Cyber Legal, Policy & Compliance Officer

| | |
|---|---|
| Name | **Cyber Legal, Policy & Compliance Officer** |
| Description [6] | Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organization's strategy and legal requirements. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks) | • TCLPCO01. Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations.<br>• TCLPCO02. Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies and procedures. |

| | |
|---|---|
| | • TCLPCO03. Enforce and advocate organization's data privacy and protection program.<br>• TCLPCO04. Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities.<br>• TCLPCO05. Act as a key contact point to handle queries and complaints regarding data processing.<br>• TCLPCO06. Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance.<br>• TCLPCO07. Monitor audits and data protection related training activities.<br>• TCLPCO08. Cooperate and share information with authorities and professional groups.<br>• TCLPCO09. Contribute to the development of the organization's cybersecurity strategy, policy and procedures.<br>• TCLPCO10. Manage legal aspects of information security responsibilities and third-party relations.<br>• TSG02. Analyse the impact of the existence of power usage data in the context of GDPR and personal data handling |
| IT-specific Competence | N/A |
| Smart-Grid - specific Competences | • SGC010. Legislation regarding cybersecurity that applies to critical infrastructure.<br>• SGC011. Design agreements with external stakeholders of the power system and third-party suppliers of components to assign the various security requirements of the system. |
| Operational Competences | • OC015. Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements.<br>• OC016. Carry out working-life practices of data protection and privacy issues involved in the implementation of the organizational processes, finance and business strategy.<br>• OC017. Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties.<br>• OC018. Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools.<br>• OC019. Explain and communicate data protection and privacy topics to stakeholders and users.<br>• OC020. Understand legal framework modifications implications to the organization's cybersecurity and data protection strategy and policies. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14]<br>• GC012. Understand, practice and adhere to ethical requirements and standards.<br>• GC006. Manage conflicts and solve problems [2], [15], [14].<br>• GC006. Present effectively [2].<br>• GC007. Teach others [2].<br>• GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16]. |

| | |
|---|---|
| | • GC014. Work under pressure [17].<br>• GC015. Collaborate effectively in a team [18]. |

### 3.2.4. Cybersecurity Architect

| Name | **Cybersecurity Architect** |
|---|---|
| Description [6] | Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks) | • TCAR01. Design and propose a secure architecture to implement the organization's strategy.<br>• TCAR02. Develop organization's cybersecurity architecture to address security and privacy requirements.<br>• TCAR03. Produce architectural documentation and specifications.<br>• TCAR04. Present high-level security architecture design to stakeholders.<br>• TCAR05. Establish a secure environment during the development lifecycle of systems, services and products.<br>• TCAR06. Coordinate the development, integration and maintenance of cybersecurity components ensuring the cybersecurity specifications.<br>• TCAR07. Analyse and evaluate the cybersecurity of the organization's architecture.<br>• TCAR08. Assure the security of the solution architectures through security reviews and certification.<br>• TCAR09. Collaborate with other teams and colleagues.<br>• TCAR10. Evaluate the impact of cybersecurity solutions on the design and performance of the organization's architecture.<br>• TCAR11. Adapt the organization's architecture to emerging threats.<br>• TCAR12. Assess the implemented architecture to maintain an appropriate level of security.<br>• TCAR13. Decide on a balance between the need to serve the load reliably and effectively and implement cybersecurity procedures such as identity authentication [13]. |
| IT-specific Competences | • TC004. Conduct user and business requirements analysis.<br>• TC005. Draw architectural and functional specifications.<br>• TC006. Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles.<br>• TC007. Propose cybersecurity architectures based on stakeholder's needs and budget.<br>• TC008. Build resilience against points of failure across the architecture. |
| Smart-Grid - specific Competences | • SGC012. Identify and understand resilience requirements to support delivery of critical services that are established for all operating states (e.g., under duress/attack, during recovery, normal operations) [13].<br>• SGC013. Prepare security design of power systems and data flows [13].<br>• SGC014. Design networks segmentation (e.g., DER devices could be segmented to limit exposure to the rest of the power system infrastructure) [13].<br>• SGC015. Understand and design modernized devices authentication principles and methods to the grid network [13].<br>• SGC003. Understand smart grid impact to cybersecurity (for example, the dependence on bi-directional, real-time data flows) [13]. |

| | |
|---|---|
| | - SG015. Understand and design power system hardware [13].<br>- SGC001. Identity and understand the organization’s role in the supply chain [13]. |
| Operational Competences | - OC020. Guide and communicate with implementers and IT/OT personnel.<br>- OC021. Select appropriate specifications, procedures and controls.<br>- OC022. Provide technological design leadership.<br>- OC023. Coordinate the integration of security solutions. |
| General Competences (soft skills) | - GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14]<br>- GC006. Manage conflicts and solve problems [2], [15], [14].<br>- GC008. Present effectively [2].<br>- GC009. Teach others [2].<br>- GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16].<br>- GC005. Manage relationships [15].<br>- GC007. Manage changes [15].<br>- GC014. Work under pressure [17].<br>- GC015. Collaborate effectively in a team [18]. |

### 3.2.5. Cybersecurity Auditor

| Name | **Cybersecurity Auditor** |
|---|---|
| Description [6] | Perform cybersecurity audits on the organization's ecosystem. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks) | - TCAU01. Develop the organization's auditing policy, procedures, standards and guidelines.<br>- TCAU02. Establish the methodologies and practices used for systems auditing.<br>- TCAU03. Establish the target environment and manage auditing activities.<br>- TCAU04. Define audit scope, objectives and criteria to audit against.<br>- TCAU05. Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests.<br>- TCAU06. Review target of evaluation, security objectives and requirements based on the risk profile.<br>- TCAU07. Audit compliance with cybersecurity-related applicable laws and regulations.<br>- TCAU08. Audit conformity with cybersecurity-related applicable standards.<br>- TCAU09. Execute the audit plan and collect evidence and measurements.<br>- TCAU10. Maintain and protect the integrity of audit records.<br>- TCAU11. Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports. |
| IT-specific Competence | - TC009. Follow and practice auditing frameworks, standards and methodologies.<br>- TC010. Apply auditing tools and techniques.<br>- TC011. Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls. |

| | |
|---|---|
| Smart-Grid - specific Competences | • SGC003. Understand smart grid impact to cybersecurity (for example, the dependence on bi-directional, real-time data flows) [13].<br>• SGC001. Identity and understand the organization’s role in the supply chain [13]. |
| Operational Competences | • OC024. Communicate, explain and adapt legal and regulatory requirements and business needs.<br>• OC025. Collect, evaluate, maintain and protect auditing information.<br>• OC026. Audit with integrity, being impartial and independent. |
| General Competences (soft skills) | • GC012. Organise and work in a systematic and deterministic way based on evidence.<br>• GC013. Plan and conduct interviews in a systematic and deterministic manner.<br>• CC007. Written and oral communication [2].<br>• GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16].<br>• GC005. Manage relationships [15].<br>• GC006. Manage conflicts and solve problems [2], [15], [14].<br>• GC008. Present effectively [2].<br>• GC009. Teach others [2].<br>• GC014. Work under pressure [17]. |

### 3.2.6. Cybersecurity Implementer

| | |
|---|---|
| Name | **Cybersecurity Implementer** |
| Description [6] | Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks) | • TCI01. Develop, implement, maintain, upgrade, test cybersecurity products.<br>• TCI02. Provide cybersecurity-related support to users and customers.<br>• TCI03. Integrate cybersecurity solutions and ensure their sound operation.<br>• TCI04. Securely configure systems, services, products and devices, including power system devices<br>• TCI05. Maintain and upgrade the security of systems, services and products.<br>• TCI07. Monitor and assure the performance of the implemented cybersecurity controls.<br>• TCI09. Work close with the IT/OT personnel on cybersecurity-related actions.<br>• TCI10. Implement, apply and manage patches to products to address technical vulnerabilities. |
| IT-specific Competences | • TC012. Integrate cybersecurity solutions to the organization's infrastructure.<br>• TC013. Configure solutions according to the organization's security policy.<br>• TC014. Assess the security and performance of solutions.<br>• TC015. Develop and test secure code and scripts. |

| | |
|---|---|
| | - TC016. Identify and troubleshoot cybersecurity-related issues. |
| Smart-Grid -specific Competences | - SGC016. Develop, implement and maintain power systems and their hardware [13].<br>- SGC017. Develop or integrate modernized devices authentication to the grid network [13].<br>- SGC018. Apply resource -intensive cryptographic mechanisms to interfere with the functional performance of control systems [13].<br>- SGC019. Create and maintain baseline configurations for power system devices [13]. |
| Operational Competences | - OC027. Implement cybersecurity procedures and controls.<br>- OC028. Document and report on the security of systems, services and products. |
| General Competences (soft skills) | - GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>- GC004. Think critically, strategically and systematically [2], [15], [14], [16].<br>- GC014. Work under pressure [17].<br>- GC015. Collaborate effectively in a team [18]. |

### 3.2.7. Cybersecurity Risk Manager

| Name | **Cybersecurity Risk Manager** |
|---|---|
| Description [6] | Manage the organization's cybersecurity-related risks aligned to the organization's strategy. Develop, maintain and communicate the risk management processes and reports. |
| Tasks (general tasks [6], supplemented by smart-grid specific tasks [13]) | - TCRM01. Develop an organization's cybersecurity risk management strategy.<br>- TCRM02. Manage an inventory of organization's assets, including IT components embedded in OT devices within the grid modernization infrastructure.<br>- TCRM03. Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems.<br>- TCRM04. Identify of threat landscape including attackers' profiles and estimation of attacks' potential.<br>- TCRM05. Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organization's strategy.<br>- TCRM06. Monitor effectiveness of cybersecurity controls and risk levels.<br>- TCRM07. Ensure that all cybersecurity risks remain at an acceptable level for the organization's assets.<br>- TCRM08. Develop, maintain, report and communicate complete risk management cycle.<br>- TCRM.09. Develop, establish, assess, manage and align cyber supply chain risk management processes [13].<br>- TSGM10. Identify and assess supply chain and third-party risks of energy delivery systems [13].<br>- TSGM10. Manage cybersecurity risks to power system, including integrity and timeliness of data and control commands [13]. |

| | |
|---|---|
| IT-specific Competence | • TC017. Build a cybersecurity risk-aware environment [6]. |
| Smart-Grid - specific Competences | • SGC020. Implement supply chain risk management processes [13].<br>• SGC021. Identify all distributed, modernized assets owned by the enterprise, including IT components embedded in OT devices within the grid modernization infrastructure [13].<br>• SGC022. Analyse supply chain and third-party risks of energy delivery systems [13].<br>• SGC023. Identify unique threats and risks of the grid modernization environment and the distributed and multi-owner nature of the environment [13].<br>• SGC008. Understand and monitor vulnerabilities of modernized distributed energy resources [13]. |
| Operational Competences | • OC029. Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards.<br>• OC030. Analyse and consolidate organization's quality and risk management practices.<br>• OC031. Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks.<br>• OC032. Enable employees to understand, embrace and follow the controls.<br>• OC033. Propose and manage risk-sharing options. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>• CC006. Present effectively [2].<br>• GC004. Think critically, strategically and systematically [2], [15]8], [7].], [16].<br>• GC005. Manage relationships [15].<br>• GC006. Manage conflicts and solve problems [2], [15], [14].<br>• GC008. Present effectively [2].<br>• GC009. Teach others [2].<br>• GC010. Manage time, people, assets and projects [15].<br>• GC014. Work under pressure [17].<br>• GC015. Collaborate effectively in a team [18]. |

### 3.2.8. Energy Citizen

| | |
|---|---|
| Name | **Energy Citizen** [19] |
| Description | Engage with energy as a meaningful part of his practices, use energy systems and connected devices. |
| Tasks | ● TEC01. Use information and information systems in a secure manner<br>● TSEC.01. Use energy systems and connected devices in a secure manner. |
| IT-specific Competence | • TC018. Understand and manage information system use through intuitive and undemanding means. |

| | |
|---|---|
| Smart-Grid -specific Competences | • SGC024. Understand and manage energy use through intuitive and undemanding means. |
| Operational Competences | • CO021. Understand cybersecurity threats and their potential impact.<br>• CO022. Understand personal data protection legalization and data subject rights.<br>• CO023. Identify and assess information security risks. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>• GC012. Understand, practice and adhere to ethical requirements and standards.<br>• GC014. Work under pressure [17].<br>• GC004. Think critically, strategically and systematically [2], [15], [14], [16]. |

### 3.2.9. Grid Assets Manager

| Name | **Grid Assets Manager** |
|---|---|
| Description | Decides on third-party components that will be used based on their technical characteristics. Acts as a point of knowledge/communication for the components that are part of the system, their characteristics, communication protocols used, ownership status. |
| Tasks | ● TACM001. Being updated on the subject of the communication protocols that are used by the various components.<br>● TACM002. Identify cybersecurity risks in the form of proprietary software, legacy devices, devices that were not designed to operate while connected to the internet (designed when security by obscurity was used).<br>● TACM003. Being updated on the subject of the limitations that the legislation poses for a smart grid to operate (requested ancillary services, reserve capacity, limitations in reconnecting after loss of power).<br>● TACM004. Being updated on the ownership of the various devices. Inform Cyber Incident Responder for changes. |
| IT-specific Competence | N/A |
| Smart-Grid -specific Competences | ● SGC021. Identify all distributed, modernized assets owned by the enterprise, including IT components embedded in OT devices within the grid modernization infrastructure [13]. |
| Operational Competences | ● OC031. Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks.<br>● OC033. Propose and manage risk-sharing options. |
| General Competences (soft skills) | • GC001. Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [2], [14].<br>• GC010. Manage time, people, assets and projects [15]. |

| | |
|---|---|
| | • GC015. Collaborate effectively in a team [18]. |

### 3.2.10. Grid Communications Engineer

| Name | **Grid Communications Engineer** |
|---|---|
| Description | Monitor the communications network including the remote access to components, the Advanced Metering Infrastructure if present and is responsible for the addition of new devices to the communication network. |
| Tasks | • TGCE001. Monitor alerts from the Communications network<br>• TGCE002. Communicate with Cybersecurity Incident Responder if necessary<br>• TGCE003. Identify access points to the system (routers, remote control, physical access to network)<br>• TGCE004. Identify and troubleshoot poor or non-communicating network<br>• TGCE005. Monitor authorized and unauthorized access to assets<br>• TGCE006. Prepare network analyses with a focus on cyber security.<br>• TGCE007. Connect new devices to the communication network and perform the necessary modifications in the exchanged messages (use of IEC61850, MQTT and others)<br>• TGCE008. Decide on the communication protocols to be used |
| IT-specific Competence | • TC012. Integrate cybersecurity solutions to the organization's infrastructure.<br>• TC013. Configure solutions according to the organization's security policy.<br>• TC016. Identify and troubleshoot cybersecurity-related issues. |
| Smart-Grid -specific Competences | • SG017. Develop or integrate modernized devices authentication to the grid network [13].<br>• SG018. Apply resource-intensive cryptographic mechanisms to interfere with the functional performance of control systems [13].<br>• SG019. Create and maintain baseline configurations for power system devices [13]. |
| Operational Competences | • OC027. Implement cybersecurity procedures and controls.<br>• OC028. Document and report on the security of systems, services and products. |
| General Competences (soft skills) | • GC015. Collaborate effectively in a team [18]. |

## 3.2 Knowledge Areas and Knowledge Units

Knowledge areas and units are based on "ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020"[1] Association for Computing

[1] ttps://dl.acm.org/doi/book/10.1145/3381686

Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC).

Essential competencies with flavor for Smart Grid and supplement competencies are not considered. New knowledge area "Smart-Grid Security" supplements the ACM framework.

### 3.3.1. Data Security

**Definition [4]:** Focuses on the protection of data at rest, during processing, and in transit. This knowledge area requires the application of mathematical and analytical algorithms to fully implement.

**Knowledge Units and Learning Topics [4]:** Access Control, Cryptanalysis, Cryptography, Data Integrity and Authentication, Data Privacy, Digital Forensics, Information Storage Security, Secure Communication, Protocols

**Learning Outcomes:**

1. Cryptography
   - Analyze which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation [4].
   - Apply symmetric and asymmetric algorithms as appropriate for a given scenario [4].
   - Investigate hash functions for checking integrity and protecting authentication data [4].
   - Apply resource -intensive cryptographic mechanisms to interfere with the functional performance of control systems [13].
   - Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenère cipher, ROT-13, Hill cipher, and Enigma machine simulator, to encrypt and decrypt data [4].

2. Digital Forensics [4]
   - Discuss the concept, need, and value of digital forensics.
   - Describe components of a digital investigation, sources of digital evidence, limitations of forensics, and ethical considerations.
   - Discuss key rules, laws, policies, and procedures that impact digital forensics.
   - Explain how to preserve the chain of custody for digital evidence.
   - Perform fundamental incident response functions including detecting, responding, and recovering from security incidents.

3. Data Integrity and Authentication [4]
   - Contrast the concepts and techniques to achieve data integrity, authentication, authorization, and access control.
   - Summarize the benefits and challenges of multifactor authentication.
   - Execute one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools.
   - Apply basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers.

4. Access Control

- Describe access control best practices, such as separation of duties, job rotation, and clean desk policy [4].
- Discuss physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction [4].
- Identify physical access controls to the power system components as needed, including modernized and distributed grid components [13]
- Implement data access control to manage identities, credentials, privileges, and related access [4].
- Differentiate among the different types of identities, such as federated identities [4].
- Differentiate access control models, including role-based, rule-based, and attribute-based [4].

5. Secure Communication Protocols [4]
   - Explain end-to-end data security.
   - Illustrate important application and transport layer protocols, such as HTTP, HTTPS, SSH, SSL/TLS, IPsec and VPN technologies.

6. Cryptanalysis [4]
   - Classify various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force.

7. Data Privacy [4]
   - Examine various ways that privacy can be jeopardized by using contemporary technology, including social media.

8. Information Storage Security [4]
   - Discuss storage device encryption implemented at the hardware and software levels.
   - Contrast techniques for data erasure and their limitations in implementation.

### 3.3.2. Software Security

**Definition [4]**: Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited. The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. Documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

**Knowledge Units and Learning Topics [4]:** Analysis and Testing, Deployment and Maintenance, Design, Documentation, Ethics, Fundamental Principles, Implementation

**Learning Outcomes:**

1. Fundamental Principles [4]
   - Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software.
   - Execute access decisions and permissions based on explicit need.
   - Diagram simple secure application design.
   - Explain software security controls in an open design.
   - Modify the levels of abstraction in a given piece of software to provide single layer abstraction whenever possible.

- Implement software as a system of secure co-operating components.
- Explain session management and its role in securing web-based applications and services.

2. Design [4]
   - Explain security requirements in software design for a given scenario.
   - Examine the waterfall and agile development models' relationship to software security.
   - Describe what makes a programming language type safe. Understanding

3. Implementation [4]
   - Discuss significant implementation issues in a secure software life cycle.
   - Write secure code which implements input validation and prevents buffer overflow, integer range violations, and input type violations.
   - Apply appropriate restrictions to process privileges.
   - Implement appropriate error and exception handling and user notification.
   - Develop a secure application or script using defensive programming techniques.

4. Analysis and Testing [4]
   - Carry out security-related testing procedures for a given piece of software.
   - Explain the difference between static and dynamic software analysis and testing.

5. Deployment and Maintenance [4]
   - Perform software installation, configuration, maintenance, and patching tasks in a secure manner.
   - Explain potential security implications for software decommissioning and retiring.

6. Documentation [4]
   - Write appropriate security notations within software documentation.
   - Use available documentation to resolve security-related issues throughout
   - the software life cycle.

7. Ethics [4]
   - Explain various ethical aspects related to software development, including vulnerability disclosure.

### 3.3.3. Component Security

**Definition [4]:** Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems. The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

**Knowledge Units and Learning Topics [4]:** Component Design, Component Procurement, Component Reverse Engineering, Component Testing

**Learning Outcomes:**

1. Component Design

- Discuss how a component’s design may create vulnerabilities in information systems [4].
- Prepare security design of power systems and data flows [13].

2. Component Procurement
    - Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain [4].
    - Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation [4].
    - Explain how externally - owned devices and third -party owners/operators can be included in a vulnerability management plan [13].

3. Component Testing [4]
    - Perform component security testing.
    - Describe unit testing tools and techniques, as distinguished from those used in system-level testing.

4. Component Reverse Engineering [4]
    - Describe common reverse engineering scenarios for components of a system.

### 3.3.4. Connection Security

**Definition [4]:** Focuses on the security of the connections between components including both physical and logical connections. It is critical that every cybersecurity professional have a basic knowledge of digital communications and networking. Connections are how components interact. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.

**Knowledge Units and Learning Topics [4]:** Distributed Systems Architecture, Hardware and Physical Component, Interfaces and Connectors, Network Architecture, Network Defense, Network Implementations, Network Services, Physical Media

**Learning Outcomes:**

1. Physical Media
    - Diagram transmission flow in a medium, including, VSAT, RF, cell, microwave [20].
    - Contrast the communications characteristics of shared and point-to-point media [4].
    - Explain various schemes for sharing media between multiple clients, including PPP and CSMA/CD [4].
    - Examine characteristics of common networking standards including frame structure, including IEEE 802.3 and 802.11 [4].

2. Hardware and Physical Component Interfaces and Connectors
    - Manipulate physical components of an organizational network and their interfaces, such as network cables, motherboards, memory, current CPU chips, and buses [4].
    - Explain various standards for network connector hardware, such as RJ-11, RJ-45, ST, and SC [4]/
    - Perform installation and configuration of device drivers for network components in an organization [4].

- Create and perform baseline configuration for power system devices [13].
- Explain third parties owned devices integration in organizational configuration change control processes [13].

3. Distributed Systems Architecture
    - Describe architectures for running processes in a distributed system and enabling communication between them [4].
    - Summarize the evolution of the Internet as a distributed platform, including the role of the world-wide-web [4].
    - Compare the OSI model and the TCP/IP model [4].
    - Categorize commonly used network protocols based on the layers of the OSI model [4].
    - Explain common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. [4].
    - Classify various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) [4].
    - Perform the setup and configuration of a virtual machine in a hypervisor environment [4].

4. Network Architecture
    - Diagram common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards [4].
    - Diagram external network communications (e.g., access points into ICS/SCADA systems, VPNs, vendor/third party access points, mobile devices) [20].
    - Design and describe bi-directional power flows [12].
    - Distinguish various network topologies and their transmission characteristics [4].
    - Distinguish industrial protocols (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC) [20].
    - Describe various types of virtualization, including native virtualization (Type 1) and hosted virtualization (Type 2) [4].

5. Network Implementations [4]
    - Differentiate between various connection attacks, such as SYN-scanning, and associated vulnerabilities, and how they can affect an organization’s network.
    - Differentiate between various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization’s network.

6. Network Services [4]
    - Describe the concept of an operating system service or daemon, and how it could be vulnerable to exploitation.

7. Network Defense [4]
    - Explain how network defenses should be structured using layering, segmentation, and other controls to achieve maximum confidentiality, integrity, and availability (CIA).

### 3.3.5. System Security

**Definition [4]:** Focuses on the security aspects of systems that are composed of components and connections and use software. Understanding the security of a system requires viewing it not only as a set of components and connections, but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems.

**Knowledge Units and Learning Topics**: Common System Architectures, System Access and Control, System Management, System Testing, System Thinking

**Learning Outcomes**:

1. System Thinking [4]
   - Describe how components work together to secure a system.
   - Apply a security threat model to a given scenario.
   - Explain fundamental principles of secure systems.

2. System Management
   - Describe the components of a security policy for a system [4].
   - Discuss methods and tools for system monitoring and recovery, including power systems monitoring [4], [13].
   - Explain monitoring approach of vendors and external service providers access to organization IT and IO environment [13].
   - Describe the use of vulnerability reports and patching in maintaining the security of a system [4].

3. System Access and Control
   - Contrast various system-related methods for authentication, authorization, and access control [4].
   - Explain authentication mechanisms of IT and OT systems and networks [13].
   - Write documentation for a system with security considerations in mind.
   - Differentiate among types of malware [4].
   - Describe how malicious activity can be detected, including the use of intrusion detection systems [4].
   - Describe potential system attacks and the actors that might perform them [4].

4. System Testing [4]
   - Execute system security test protocols.
   - Discuss the differences between unit testing and system testing.

5. Common System Architectures [4]
   - Discuss system security issues related to common system architectures such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems.

6. Creating [4]
   - Describe the components of a SCADA industrial control system.
   - Diagram an Internet of Things system.

### 3.3.6. Human Security

**Definition [4]:** Focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity. Humans have a responsibility to ensure the confidentiality, integrity, and availability (CIA) of their organizational and personal computer systems.

**Knowledge Units:** Awareness and Understanding, Identity Management, Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms, Personal Data Privacy and Security, Social Engineering, Usable Security and Privacy

**Learning Outcomes:**

1. Identity Management [4]
   - Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and multifactor systems.
   - Discuss attacks and mitigations associated with identity management, such as brute force attacks, spoofing attacks, strong password policies, and restricted access systems.

2. Social Engineering [4]
   - Compare various social engineering attacks, such as phishing, vishing, email compromise, and baiting, along with suitable mitigations.
   - Describe psychological and behavioral factors which contribute to social engineering attacks, such as adversarial thinking, cognitive biases, and trust building.
   - Analyze one's personal social media use with respect to organizational policies, rules, and ethical norms.

3. Awareness and Understanding
   - Carry out formal or informal security education, training, and awareness program tasks [4], [2].
   - Communicate grid impact to cybersecurity, integrate relevant topics in awareness tasks (for example, the dependence on bi-directional, real-time data flows) [13].
   - Explain unique threats and risks of the grid modernization environment and the distributed and multi-owner nature of the environment [13].
   - Define and carry out motivational measures to influence and build an organization's cybersecurity culture and motivate and encourage people.

4. Personal Data Privacy and Security [4]
   - Evaluate potential risks to personal data privacy and security for a given scenario.

5. Usable Security and Privacy
   - Describe the impact usability and user experience have on security and privacy, including compliance with laws such as HIPAA and FERPA [4].
   - Describe human factors which impact privacy and security, such as the psychology of adversarial thinking, resistance to biometric authentication, and the economics of security [4].
   - Describe behavioral aspects that enable metacognition and work under pressure [17].

### 3.3.7. Organizational Security

**Definition [4]:** Focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. Organizations have a responsibility to meet the needs of many constituencies and those needs must inform risk management, security governance, business continuity, and security program management.

**Knowledge Units and Learning Topics [4]**: Analytical Tools, Business Continuity, Disaster Recovery, and Incident Management, Cybersecurity Planning, Personnel Security, Risk Management, Security Governance & Policy, Security Program Management, Systems Administration, Stakeholder and Leadership Engagement

**Learning Outcomes:**

1. Risk Management
   - Identify and list physical devices, systems, software platforms and applications within the organization and external systems [13].
   - Classify organizational risk factors due to security failure, such as financial loss, operational disruption, and reputational damage [4];
   - Describe the components that contribute to an organization's security posture [4];
   - Identify and assess supply chain and third-party risks of energy delivery systems [13].

2. Security Governance & Policy [4]
   - Perform tasks in compliance with information security governance and policy.
   - Summarize relevant independent and government-sponsored cybersecurity frameworks.
   - Discuss the importance of ethical codes of conduct for cybersecurity professionals and their organizations.

3. Analytical Tools [4]
   - Use tools to collect and analyze data to generate security intelligence including threats and adversary capabilities.

4. Systems Administration
   - Describe components that secure the operating system and system database from vulnerabilities [4].
   - Explain vulnerabilities of modernized distributed energy resources [13].
   - Demonstrate administrative functions, such as using group membership to assign permissions [4].
   - Discuss security features that are embedded within a cloud environment [4].

5. Cybersecurity Planning
   - Apply Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis in an organization [4].
   - Explain the organization's role in the supply chain and placement in the grid infrastructure [12].

6. Business Continuity, Disaster Recovery, and Incident Management
   - Identify and prioritize enterprise resources (e.g., hardware, devices, data, time, personnel, and software) based on their classification, criticality, and business value [13].

- Identify and assess dependencies and critical functions for delivery of critical services [13].
- Understand and explain resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) [13].
- Explain the components of a business continuity plan, such as contingency planning, incident response, emergency response, backup, and recovery efforts [4].
- Explain consideration to be taken to address backups of devices owned by third parties [13].
- Describe a disaster recovery plan that ensures minimal down time and quick recovery [4].
- Explain collaboration between IT and OT personnel in recovery activities [13].

7. Security Program Management
    - Perform project, time, people and assets management tasks that provide for security of data [4], [15].
    - Perform change management tasks required to improve security of data [15].
    - Analyze the meaning and use of various security metrics used in protecting the network [4].
    - Describe the use of quality assurance and quality control to prevent mistakes and increase the quality of a system [4].
    - Discuss factors to be applied for critical, strategic and systematic security program management [2], [15]8], [7], [16].

8. Personnel Security [4]
    - Describe the proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool in various contexts, such as physical security, password security, and social engineering.
    - Classify components of third-party security services.
    - Discuss components that ensure the protection of personally identifiable information.

9. Stakeholder and Leadership Engagement:
    - Understand the stakeholder landscape in the modernized grid and list roles and responsibilities of all relevant stakeholders, including third parties [13].
    - Communicate, coordinate and collaborate efficiently in cybersecurity tasks execution with internal and external stakeholders in a written and oral form [2], [14].
    - Perform relationship management tasks to manage and solve problems [2], [15], [14].
    - Effectively present information required for stakeholder and leadership engagement in cybersecurity improvement [2].

### 3.3.8. Societal Security

**Definition [4]:** Focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse. Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across global society is serious and growing. Laws, ethics and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

**Knowledge Units [4]:** Cyber Ethics, Cyber Law, Cyber Policy, Cybercrime, Privacy

**Learning Outcomes:**

1. Cybercrime [4]
   - Categorize different types of cybercrime.
   - Investigate the economic impact of cybersecurity and cybercrime for a given city, state, or nation.

2. Cyber Law
   - Describe various categories of global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property [4].
   - Understand ownership/contractual agreements of power control and delivery with the manufacturers [13].

3. Cyber Ethics [4]
   - Analyze given cyber ethics scenarios, including topics on codes of conduct and professional ethics.
   - Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war.

4. Cyber Policy [4]
   - Discuss cyber policies and related liability issues.

5. Privacy [4]
   - Contrast privacy and transparency from a societal perspective, including goals and tradeoffs.
   - Investigate cultural differences in the existence of privacy norms and boundaries.

### 3.3.9. Smart-Grid Security

Focuses on protecting the modern power grid's assets and data from unauthorized access and any sorts of malicious activities that might result in malfunction or degradation of the grid's performance. Information technology, operational technology, advanced metering infrastructure, SCADA supervisory and control system, as well as communication protocols, are the key elements for smart grid security

**Knowledge Units:** Smart Grid Supply Chain, Smart Grid Infrastructure, Electrical and Cyber-physical Systems, Smart Grid Threats, Risks and Vulnerabilities, IT and OT Security

Learning Outcomes:

1. Smart Grid Supply Chain
   - Describe the systems, facilities and processes involved in the production and delivery of energy as well as information exchange within the grid.
   - Highlights associated complexity of the smart grid since many systems are involved in generation and distribution of energy.
   - Introduces communication protocols used for data exchange

- Gives emphasis on renewable resources integration, and their economic and environmental benefits.
- Gives consideration to consumers and other stakeholders' demands

2. Smart Grid Infrastructure
    - Introduces the architecture of the smart grid, the components involved, the relationship between the different layers, the flow of information within the grid, and the control system.

3. Electrical and Cyber-physical Systems
    - Presents the structure and gives an example of conventional electrical systems.
    - Defines physical and cyber systems
    - Introduces the concept of cyber-physical systems and gives an example of the smart gird as a typical cyber-physical system and what benefits such a concept brings.
    - Highlights other technologies related to the CPS concept, such as Internet of Things IoT, Cloud computing, and so.

4. Smart Grid Threats, Risks and Vulnerabilities

    - Gives introduction to risk analysis and risk assessment
    - Defines threats, risks and vulnerabilities
    - Describe risks associated with the modern grid
    - Provides a framework and methodology for conducing risk and vulnerability analysis
    - Introduces technologies used for risk mitigation
    - Consider legalization, authority, and sector standards and/or practices. Smart Grid Benefits

5. IT and OT Security

    - Differentiates between security practices for IT and OT systems
    - Emphasis on the integration of different security solutions when dealing with Critical Infrastructure CI
    - Reviews the CIA Triad model, and introduces other measures such as non-repudiation, utility, Authentication, Authorization, and Access Control AAA concepts.
    - Presents the different drives and methods for hacking the grid
    - Presents the different attack tools
    - Introduces the models used for securing the grid, e.g., NISTIR 7628, EU M/490 and SGCG reference architecture, ISA-62443 zones and conduits, and the McAfee security model for CI
    - Introduces the concepts of Layered security architecture, endpoints, field zone protection, control zone protection, zone separation, advanced network monitoring, and situational awareness.

# 4. Methods & Tools Bank

In WP2, the following eight educational methods were reviewed regarding their effectiveness when applied on teaching cybersecurity. The goal was to find papers where teachers were reporting their experience when they used some of the below mentioned methods to teach about cybersecurity preferably also involving smart grids or power systems in general.

1. Experiential learning
2. Active learning
3. Cooperative learning
4. Flipped classroom
5. Inquiry based learning
6. Problem based learning
7. Project based learning
8. Gamification

In this chapter, some of these methods were selected (based on the frequency of use that resulted from the review) to be further presented in the form of “Method cards”. A quick way for the teachers/trainers that want to formulate a curriculum, to see the basic elements of the method and its usual use cases on the topic of cybersecurity and/or smart grids. Along with the educational methods the tool of simulation testbeds is also described with some use-cases provided.

## 4.1. Simulation tools, CPES laboratories and testbeds

| **Tool name** | Simulation testbeds |
|---|---|
| **Description** | Testbeds are used to simulate in varying degrees real-life systems. Some testbeds use software simulation for parts of the system and others use only hardware components. Additionally, there are testbeds that only simulate a component of the system and others that simulate the whole system. Using a real-time simulator combined with real hardware (like inverters and PMUs) to simulate an entire microgrid is the most realistic and complete way to study the behavior of an electrical grid under a cyber-attack. |
| **Prerequisites** | This educational tool relies on the use of equipment. It can be a mixture of commercia and non-commercial equipment, simulation tools, Real Time Simulation (specific computers), a remote connection system and/or virtual machines. The remote and/or 24h access of the students to the equipment requires the need for additional staff to support the lab access. |
| **Use cases** | 1. Using the [21] testbed that comprises from commercial equipment and software, hardware and simulation/emulation the students can be taught about the communications and perform a security analysis in depth. |

| | |
|---|---|
| | 2. A testbed using Real Time Digital Simulator to simulate the power system is developed in [22]. The communications subsystem is simulated through DeterLab which allows the creation, planning, monitoring and analysis of cyber-security aspects of the system.<br>3. A larger testbed is used in [23]. With a Control System at heart, a Distribution Management System, along with Smart Meters, RTUs and PVs are simulated. Based on this testbed, a subject is developed regarding “Critical infrastructure security: Smart Grid” where students learn about SCADA systems and the communication protocols that are used for the control of power systems in general. |

## 4.2. Gamification

Gamification is a teaching method in which elements and mechanisms from game designing are used to increase the student engagement [24]. Those elements and mechanisms can be for example a narrative story, limited time to accomplish a task, points, badges and level-beating.

| | |
|---|---|
| **Method ID** | M001 |
| **Method name** | Gamification |
| **Description** | Gamification consists of three elements: Mechanics, Dynamics and Emotions. The Mechanics refer to the decisions of the teachers (rules and context of the game). The Dynamics are the result of the implemented Mechanics in the form of strategies employed by the students. The Emotions aimed are fun, excitement, curiosity. Although the use of a real game is not mandatory there are some types of games that can be easily adapted to the requirements of a technical subject. Strategy games can train the learners into how to use efficiently limited resources (e.g., generator allocation) and how to plan and recover from an incident [24]. In analysis of the different types of drivers for the players and kinds of games is given in [25]. |
| **Prerequisites** | There are no prerequisites from the side of students specifically for gamification. Prior knowledge might be needed based on the level of knowledge of the target audience. From the side of teachers/trainers they should design the “Mechanics” of the game [24] aiming to create engagement to the students/trainees. In case a real digital game is implemented, hardware may be needed. |
| **Use cases** | 1. Students design and then present “Capture the Flag” games in an open day event [26].<br>2. Company employees use a tabletop game to be trained about cyber security at the office [27].<br>3. Students learn the dynamics of a power control system via “Grid Game” [28].<br>4. Using the aforementioned testbed of TCIPG a summer school was created where through a virtual company (TCIPGco) the students understand the impact of information disclosure and lack of fundamental security as a culture that can result in systemic security failures. |

## 4.3. Problem/Project based learning

In Problem-based learning (PBL) a group of students investigates an open-ended real-world problem and tries to come up with the most suitable solution which then the group presents to other peers. Project Based Learning is based on the same idea but in general it has a longer duration and a concrete outcome rather that a theoretical solution provided.

| | |
|---|---|
| **Method ID** | M002 |
| **Method name** | Problem/Project based learning |
| **Description** | Problem and Project based learning require a small group of students to work on an open-ended problem. In general, the process that is followed is that the students are presented with the problem, identify the facts, generate some hypotheses, identify the knowledge deficiencies and through self-directed learning they apply the new knowledge to generate better hypotheses or correct the facts identified. Due to a solid outcome, Project BL also includes the stages of design, building, testing and evaluation of the solution that the group proposes. |
| **Prerequisites** | Problem/Project based learning is more easily applied when the student groups are homogenous regarding the level of previous knowledge and when they already have some level of autonomy on the subject at hand. |
| **Use cases** | 1. In [29] two problems are presented, one is a phishing email attack, one is an attack related to unauthorized access to data.<br>2. In [30] students use the campus' network as a case study to identify cyber threats and provide possible solutions.<br>3. In [31] scenarios and practices are proposed that can be used for teaching cybersecurity for industrial control systems using Problem-Based Learning. |

## 4.4. Flipped learning

The main characteristic of Flipped learning is that the students study the material that is usually studied during class hours at their home. In that way when they are at class they have the opportunity to reflect on the studied material and have time for experimentation.

| | |
|---|---|
| **Method ID** | M003 |
| **Method name** | Flipped learning |
| **Description** | Flipped classroom is the methodology in which the students study the material that they would be normally taught during the lectures in their homes and during the lecture time they can deepen their understanding with the facilitation of the teacher. The study material could be as simple as the book(s) that are used for the course throughout the semester but it can also be videos already on the web or slides and videos specifically prepared by the teacher(s) for the subject. The teacher/professor can allocate the time in class using other techniques like active learning techniques (e.g., concept maps), experiential learning techniques (e.g., simulations) and problem-based learning (see M002) to help the students attain higher levels of thinking skills. |
| **Prerequisites** | The prerequisites of the method include the fact that students need to have access to appropriate equipment to study at home and teacher(s) need to find or prepare the study material in addition to organizing the work that is done during the class hour. |

| | |
|---|---|
| **Use cases** | 1. In [Do project-based learning, hands-on activities, and flipped teaching enhance student’s learning of introductory theoretical computing classes?] the authors test the hypotheses of whether PBL and flipped learning benefit the students perception by teaching a computer systems course in the span of 6 years. The use of video of hands-on activities that students can review later was found to be beneficial. The interest level and motivation of the students significantly increased.<br>2. In [KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems], cybersecurity of industrial control systems is taught in a flipped classroom format with the emphasis being given on creating games that replicate real cyber attacks. The work at home include various tasks like creating presentations, reading papers, creating a game draft and build upon the draft until completion and also creating the survey for the game evaluation.<br>3. In [Hybrid Implementation of Flipped Classroom Approach to Cybersecurity Education Aparicio Carranza \| Casimer DeCusatis] a version of the flipped classroom was proved to be an effective way of engaging students in studying computer security. Their approach includes weekly reading assignments and nine lab reports completed in a span of 15 weeks. There are weekly class meetings but also each student is encouraged to communicate with the teachers as needed. |

# References

[1] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade," 2020. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3093952.

[3] Joint Task Force on Cybersecurity Education, *Curricula 2017 Cybersecurity Curriculum - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, vol. Version 1., no. December. 2017.

[4] R. Pirta-Dreimane, A. Brilingaite, E. Roponena, and K. Parish, "Multi-dimensional Cybersecurity Education Design: A Case Study," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Sep. 2022, pp. 1–8. doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[5] D. S. M. C. S. K. A. W. and G. W. R. Petersen, "Workforce Framework for Cybersecurity (NICE Framework)," 2020.

[6] E. European Union Agency for Cybersecurity, "European cybersecurity skills framework," *https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles*, 2022.

[7] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. 2020. doi: 10.1145/3381686.

[8] NSA and DHS, "2020 CAE Cyber Defense (CAE-CD) Knowledge Units," *https://dl.dod.cyber.mil/ wp-content/uploads/cae/pdf/unclass-cae-cd{ }ku.pdf*, 2020.

[9] I. Wrogemann, L. Sarp, N. Susser, and J. Falk, "D-Learning – Design Thinking as a means to innovative product development in adult learning," *https://cesie.org/media/ d-learning-manual-en.pdf* , 2021.

[10] S. Panke, "Design Thinking in Education: Perspectives, Opportunities and Challenges," *Open Education Studies*, vol. 1, no. 1. 2019. doi: 10.1515/edu-2019-0022.

[11] Y. Kali, R. Levin-Peled, and Y. Dori, "The role of design-principles in designing courses that promote collaborative learning in higher-education. Computers in Human Behavior," *Comput Human Behav*, vol. 25, 2009.

[12] G. Morrison and S. Ross, *Designing Effective Instruction, 7th Edition*. 2013.

[13] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, "Cybersecurity framework smart grid profile," Gaithersburg, MD, Jul. 2019. doi: 10.6028/NIST.TN.2051.

[14] Bret Fund, "16 Soft Skills You Need to Succeed in Cyber Security," *https://flatironschool.com/blog/soft-skills-cyber-security/*, 2021.

[15] Frederick Scholl, “Developing your portfolio of soft skills for cybersecurity,” *https://www.qu.edu/quinnipiac-today/developing-your-portfolio-of-soft-skills-for-cybersecurity-2020-01-29/*, 2020.

[16] Katherine Hibbs Pherson, “Key critical thinking skills for security professionals,” *https://www.sourcesecurity.com/insights/key-critical-thinking-skills-security-professionals-co-14642-ga.22310.html?utm_source=SIc&utm_medium=Redirect&utm_campaign=Int%20Redirect%20Popup*.

[17] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab, “An organizational psychology perspective to examining computer security incident response teams,” *IEEE Secur Priv*, vol. 12, no. 5, 2014, doi: 10.1109/MSP.2014.85.

[18] J. Steinke *et al.*, “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” *IEEE Security and Privacy*, vol. 13, no. 4. 2015. doi: 10.1109/MSP.2015.71.

[19] M. Goulden, B. Bedwell, S. Rennick-Egglestone, T. Rodden, and A. Spence, “Smart grids, smart users? the role of the user in demand side management,” *Energy Res Soc Sci*, vol. 2, 2014, doi: 10.1016/j.erss.2014.04.008.

[20] B. Cope *et al.*, “Curriculum Guidance Document Industrial Control Systems Deliverable 6.B Contract: HSHQDC-16-A-B0010/70RCSA20FR0000103,” 2021.

[21] P. W. Sauer and W. H. Sanders, “A project to develop a trustworthy cyber infrastructure for the power grid (TCIPG),” in *IEEE Power and Energy Society General Meeting*, 2012. doi: 10.1109/PESGM.2012.6345765.

[22] R. Liu and A. Srivastava, “Integrated simulation to analyze the impact of cyber-attacks on the power grid,” in *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2015 - Held as Part of CPS Week, Proceedings*, 2015. doi: 10.1109/MSCPES.2015.7115395.

[23] J. Xie, J. C. Bedoya, C. C. Liu, A. Hahn, K. J. Kaur, and R. Singh, “New educational modules using a Cyber-Distribution system testbed,” *IEEE Transactions on Power Systems*, vol. 33, no. 5, 2018, doi: 10.1109/TPWRS.2018.2821178.

[24] S. Deterding, K. O’Hara, M. Sicart, D. Dixon, and L. Nacke, “Gamification: Using game design elements in non-gaming contexts,” in *Conference on Human Factors in Computing Systems - Proceedings*, 2011. doi: 10.1145/1979742.1979575.

[25] A. P. Markopoulos, A. Fragkou, P. D. Kasidiaris, and J. P. Davim, “Gamification in engineering education and professional training,” *International Journal of Mechanical Engineering Education*, vol. 43, no. 2, 2015, doi: 10.1177/0306419015591324.

[26] V. Švábenský, M. Cermak, J. Vykopal, and M. Laštovička, “Enhancing cybersecurity skills by creating serious games,” in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, 2018. doi: 10.1145/3197091.3197123.

[27] S. Hart, A. Margheri, F. Paci, and V. Sassone, “Riskio: A Serious Game for Cyber Security Awareness and Education,” *Comput Secur*, vol. 95, 2020, doi: 10.1016/j.cose.2020.101827.

[28] T. R. McJunkin *et al.*, “Multidisciplinary game-based approach for generating student enthusiasm for addressing critical infrastructure challenges,” in *ASEE Annual Conference and Exposition, Conference Proceedings*, 2016, vol. 2016-June. doi: 10.18260/p.25763.

[29] M. Shivapurkar, S. Bhatia, and I. Ahmed, “Problem-based Learning for Cybersecurity Education.” [Online]. Available: https://medicine.missouri.edu/news/students-take-active-role-education-pbl

[30] A. T. Sherman *et al.*, “Project-Based Learning Inspires Cybersecurity Students: A Scholarship-for-Service Research Study,” *IEEE Secur Priv*, vol. 17, no. 3, 2019, doi: 10.1109/MSEC.2019.2900595.

[31] B. S. Junqueira, M. V. S. de Souza, V. B. Lima, W. S. F. de J. Gonçalves, and H. A. Lepikson, “LEARNING PROPOSAL FOR CYBERSECURITY FOR INDUSTRIAL CONTROL SYSTEMS BASED ON PROBLEMS AND ESTABLISHED BY A 4.0 DIDACTIC ADVANCED-MANUFACTURING-PLANT,” 2022. doi: 10.5151/siintec2021-208706.

## Appendix 1: Benchmarking

This Work package also includes the benchmarking of the proposed approach in order to gain insights regarding the aspects that can be further improved in the future. The benchmarking was implemented in two axes. First, through a literature review, the characteristics that benefit the modern educational approaches were identified and secondly a questionnaire was formulated in order to have the perspective of the students that participated in person at the workshop at the Final event of CC-RSG in Vaasa, Finland (March 2023).

The questionnaire had eight answers which are not enough to draw quantitative conclusions from but can still be helpful as a qualitative indicator. Half of the students -who all have background that is relevant to the project's subjects- were not familiar with the educational methods used (such as gamification, virtual labs etc) and the other half were familiar with them (Figure 6). Probably this indicates that familiarity with the methods is heavily influenced by the institute the students are enrolled in.

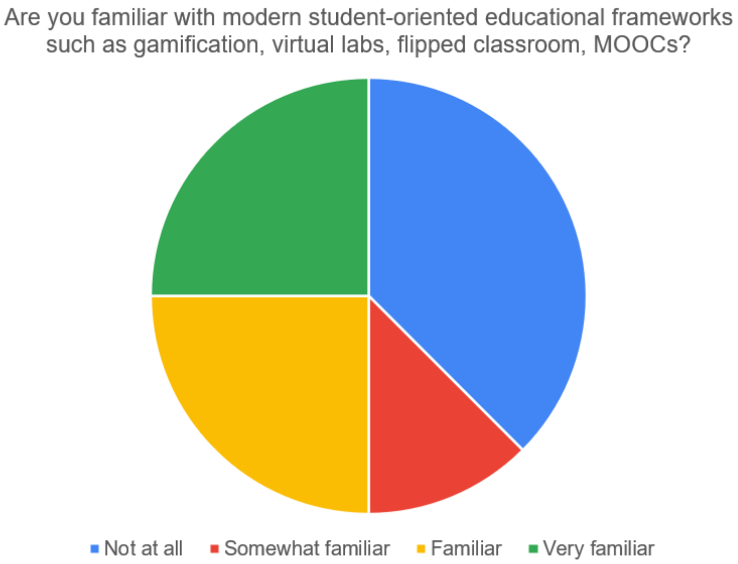
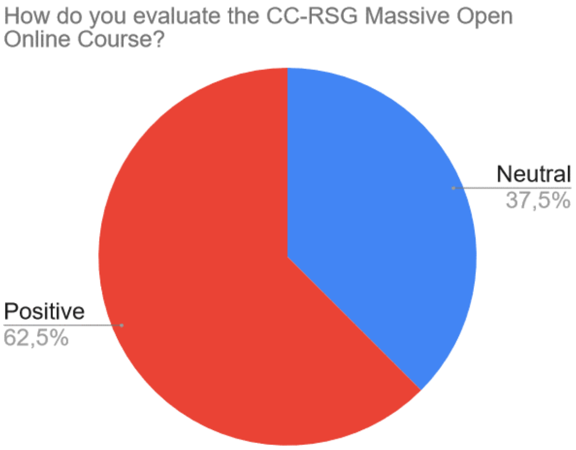
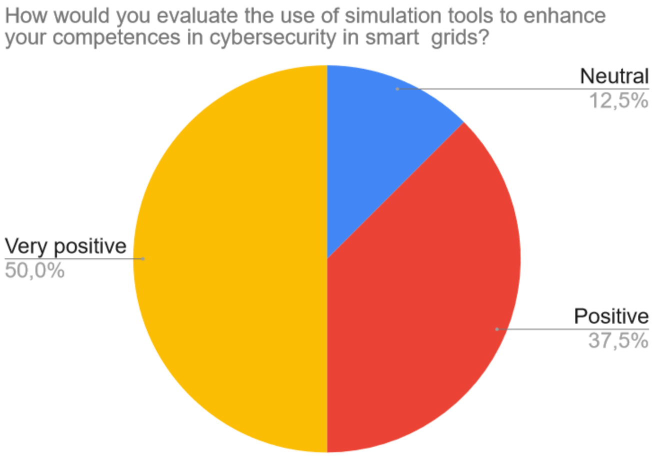


Figure 6 Familiarity with modern student-oriented educational frameworks

Regarding the cybersecurity frameworks, half of the students were aware of NIST NICE, but they were mostly not familiar with the popular cybersecurity frameworks. Overall, they evaluated positively the project's MOOC  and the use of simulation tools and gamification as educational methods on this subject.





Regarding the comparison of the CC-RSG project's approach with the traditional method, the students emphatically agreed that it enhances the importance and reliability of curriculum contents and the learner's interest on the subject. Also they leaned positively regarding the increase of efficiency and flexibility of the curriculum.

It is optimistic that the students reported that it was generally easy to implement the simulation case studies that were presented to them (Figure 7), and they would choose a subject with a similar approach in the future.

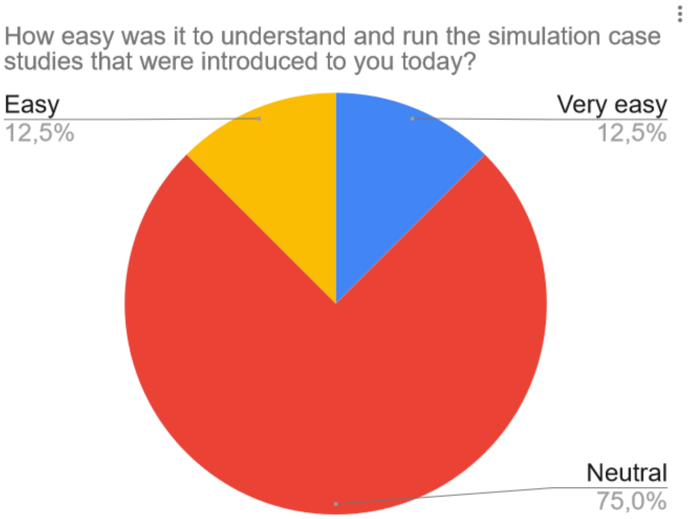


Figure 7 Level of difficulty to understand and run the simulation case studies

The suggestions provided include the addition of the subject of automation/control in the presented case studies and the possibility to work individually instead of in the form of small teams.

# Appendix 2: Implementation Roadmap

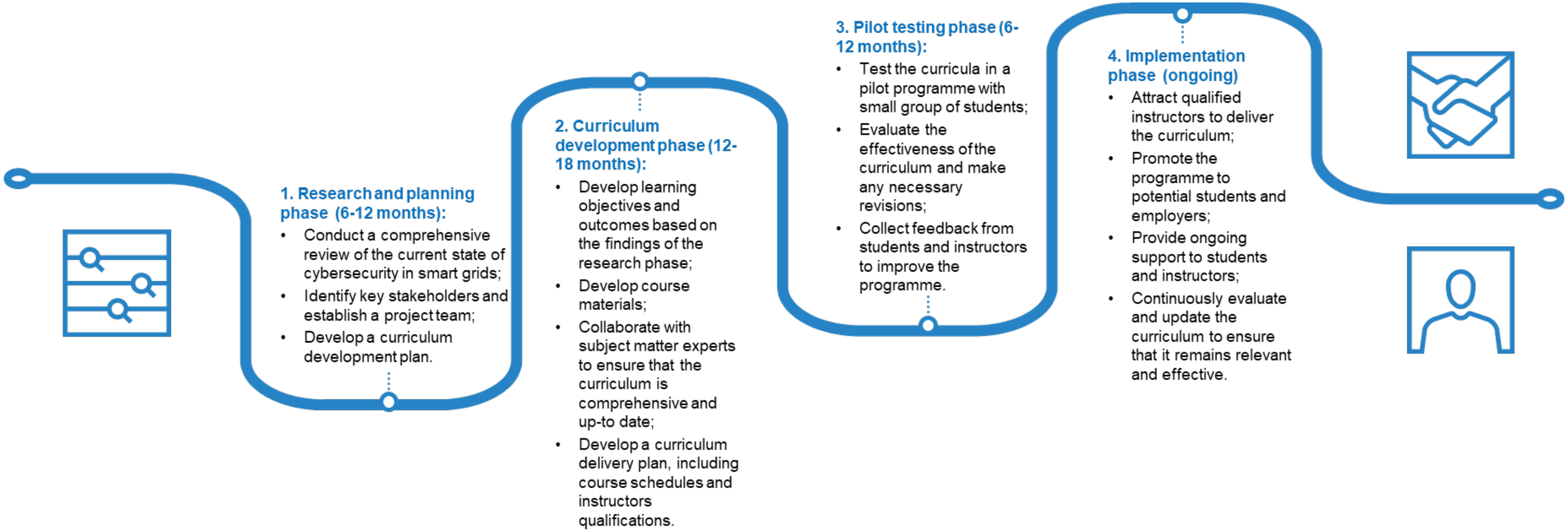
The objective of implementation roadmap is to provide a structured plan for implementation of developed curricula model, and it outlines the steps that need to be taken and implementation timeline.

The roadmap for implementing the education curricula model includes the following steps:

1. Identify the key stakeholders in the smart grid industry who will be involved in the implementation of education curricula model, e.g., education institutions, representatives from energy companies, and cybersecurity experts.
2. Define the learning objectives with a focus on cybersecurity in smart grids in collaboration with the stakeholders to ensure that objectives are aligned with their needs.
3. Develop the curriculum content in collaboration with smart grid and cybersecurity experts from academia and industry. Consider the unique needs of the smart grid industry.
4. Identify the delivery mechanism. This may include on-site classes, online courses, or a combination of both.
5. Develop assessment methods and tools, e.g., quizzes, exams, hands-on projects that simulate real-world cybersecurity scenarios in smart grids.
6. Train instructors on how to effectively deliver the education curricula. Provide them with training materials and conduct workshops that covers the unique challenges of securing smart grid infrastructure.
7. Implement the education curricula. This may involve marketing the programme to individuals and organisations in the smart grid industry who need cybersecurity training, enrolling students, and establish partnership with industry stakeholders.
8. Evaluate and improve the education curricula model by gathering feedback from students and instructors, analysing assessment results, and updating the curriculum content to ensure that it remains relevant to the rapidly evolving smart grid cybersecurity landscape.

By following this roadmap, the education curricula that provides individuals and organisations with the knowledge and skills needed to address the unique cybersecurity challenges of smart grids.

The following the education curricula development and implementation timeline could be proposed:



**1. Research and planning phase (6-12 months):**

- Conduct a comprehensive review of the current state of cybersecurity in smart grids;
- Identify key stakeholders and establish a project team;
- Develop a curriculum development plan.

**2. Curriculum development phase (12-18 months):**

- Develop learning objectives and outcomes based on the findings of the research phase;
- Develop course materials;
- Collaborate with subject matter experts to ensure that the curriculum is comprehensive and up-to date;
- Develop a curriculum delivery plan, including course schedules and instructors qualifications.

**3. Pilot testing phase (6-12 months):**

- Test the curricula in a pilot programme with small group of students;
- Evaluate the effectiveness of the curriculum and make any necessary revisions;
- Collect feedback from students and instructors to improve the programme.

**4. Implementation phase (ongoing)**

- Attract qualified instructors to deliver the curriculum;
- Promote the programme to potential students and employers;
- Provide ongoing support to students and instructors;
- Continuously evaluate and update the curriculum to ensure that it remains relevant and effective.

Figure 8 The education curricula development and implementation timeline

It is important to note that the timeline for each phase may vary, and adjustment may need to be made as the project progress. Additionally, the success of the programme will depend on the engagement and commitment of key stakeholders, including industry partners, educators, and students.

There are several challenges that can arise during the implementation of an education curricula model for cybersecurity in smart grids:

- Keeping up with rapid technological advancements. The field of cybersecurity is constantly evolving, and new threats and technologies are emerging at rapid pace. It can be a challenge to develop and update the education curricula model quickly enough to keep up with these advancements.
- Access to subject matter experts. The development of the education curricula requires input from subject matter experts in the smart grid industry. However, it can be challenging to find and access these experts, particularly in niche areas of expertise.
- Limited resources. Developing and implementation an education curriculum requires significant resources, including funding, time, and staff.
- Lack of industry standards. There are currently no standardised guidelines or best practices for cybersecurity in smart grids, which can make it difficult to develop, which can make it difficult to develop an education curricula model that is universally applicable and relevant.
- Balancing theory and practice. Cybersecurity education requires both theoretical knowledge and skills. It can be a challenge to strike the right balance between these two aspects in the curricula, particularly when it comes to simulation real-world scenarios.
- Integration of different perspectives. The interdisciplinary nature of the education curricula requires the integration of expertise from various fields, including cybersecurity, electrical engineering, power systems, computer science, and others.