Strategy for Cybersecurity Education in Smart Grids

Authors:

Maria Valliou, Alexandros Chronis, Panos Kotsampopoulos,

Bahaa Eltahawy, Tero Vartiainen, Mike Mekkanen,

Andrejs Romānovs, Jana Bikovska, Jānis Pekša,

Rūta Pirta-Dreimane, Jirapa Kamsamrong, Bjoern Siemers

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 2

April 2022

Reviewers: Foivos Palaiogiannis and Lars Fischer
Coordinator: University of Vaasa
Partners: OFFIS, Riga Technical University, National Technical University of Athens

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

Vaasan yliopisto
UNIVERSITY OF VAASA

National Technical University of Athens

1862
RIGA TECHNICAL UNIVERSITY

CARL VON OSSIETZKY universität OLDENBURG

Contents

Definitions, Acronyms and Abbreviations

Abbreviation	Meaning
ACM	Association for Computing Machinery
AN	Analyze
CEN	European Committee for Standardization
CIM	Common Information Model
CO	Collect and Operate
CPES	Cyber Physical Energy System
CSEC	Cyber Security Education Consortium
CSIRT	Computer Security Incident Response Team
CTF	Capture the flag
DMS	Distribution Management System
DSO	Distribution System Operator
ENISA	European Network and Information Security Agency
EQF	European Qualifications Framework
ESCO	European Skills, Competences, Qualifications and Occupations
EU	European Union
GDPR	General Data Protection Regulation
HEI	Higher Educational Institute
HEMRM	Harmonized Electricity Market Role Model
HIL	Hardware in the loop
ICS	Industrial Control System
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IN	Investigate
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
MDE	Mechanics Dynamics Emotions
MOOC	Massive pen Online Courses
MQTT	MQ Telemetry Transport
NICE	National Initiative for Cybersecurity Education
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OM	Operate and maintain
OSI	Open Systems Interconnection
OT	Operational Technology
OV	Oversee and govern
PBL	Problem based learning
PMU	Phasor Measurement Unit
PR	Protect and Defend
PV	Photovoltaics

RC	Risk Cause
REST API	Representational State Transfer Application Programming Interface
RTU	Remote Terminal Unit
SAREF	Smart Applications Reference Ontology
SCADA	Supervisory Control and Data Acquisition
SETA	Security Education, Training, and Awareness
SG	Skill Gap
SIEM	Security Information and Event Management
SME	Small medium enterprises
SOC	Security Operations Centre
SP	Securely provision
STEM	Science Technology Engineering and Mathematics
TCP SYN	Transmission Control Protocol with SYNchronization
TSO	Transmission System Operator
UK	United Kingdom
UNISET	Universities in the SET plan
UP-RES	Urban planners with Renewable Energy Skills
US	United States
VET	Vocational education and training
WP	Work Package

List of figures

List of Tables

Executive summary

This report is the outcome of WP2 "Development of the cybersecurity education strategy for smart grids" of the project "Cybersecurity Curricula Recommendations for Smart Grids".

Chapter 2 addresses the challenges faced by the industry in the field of cybersecurity. The challenges were identified through a literature review and interviews with industry experts. The interviews were conducted as part of the WP1. Below are the main challenges identified through the literature review:

1. It needs high investment cost to create a Cyber Physical Energy System (CPES) with all the components to train the workforce adequately
2. Existing standards and guidance documents don't cover adequately the critical assets to be protected or the recommended countermeasures
3. Existing modeling tools are incapable of mimicking both the power and communication systems in entire fullness scenario
4. Certification schemes for cybersecurity skills are not widely adopted nor integrated in the curricula
5. It is difficult to create a cybersecurity culture in a workforce that does not have relevant responsibilities in their job description explicitly
6. Lack of strong interconnection between Higher Educational Institutes (HEIs) and industry
7. Regulators are often seen as law enforcement figures rather than a central entity for information sharing and connection between different players

Below are the key challenges that were identified through the interviews:

1. Interviewees agree with the findings of WP1 that show that Human Organizational and Societal security are not covered in the relevant literature
2. There is lack of educators that can teach both the technical and non-technical aspects of cybersecurity
3. Graduates lack practical experience
4. Graduates lack management and communication skills.

The challenges are then used to identify needs in policy change and educational changes which are listed below:

1. Providing hands-on experience and training programs
2. Enhancing cross-functional collaboration (internship programs etc)
3. Building cybersecurity culture

In Chapter 3 a skill gaps mitigation plan is produced describing the mitigation actions that need to be followed by the various actors. The Association for Computing Machinery (ACM) framework is used as a reference. The ACM framework categorizes the various aspects of cybersecurity on a first level in eight big groups named "Knowledge areas (KAs)" and on a second level each KA includes several "Knowledge Units (KUs)". For each knowledge unit for each of the main knowledge areas an assessment is made on whether the change in the field should mostly be initiated by the educational institutes or the industry. In each case some key actions are recommended. Chapter 3 also includes the main difficulties of the integration of the proposed roadmap to existing curricula. They are organized in four groups namely

teachers' difficulties, subject/curriculum difficulties, learners' difficulties, and organization difficulties.

Chapter 4 aims to suggest the appropriate educational methods for use by universities, Vocational education and training institutes (VETs) and Industries. The following eight educational methods are analysed:

1. Lecture based learning (the traditional method where the teacher explains the subject using a narrative and visual aids like a board and the students passively watch)
2. Experiential learning (learning from experience or learning by doing)
3. Active learning (students participate actively in the learning process by being asked to answer, discuss, propose, write etc)
4. Cooperative learning (students work in small groups with common interests)
5. Flipped classroom (students study the subject at home prior to the class and during the class they reflect on what they studied with the facilitation of the teacher)
6. Inquiry based learning (students use methods similar with those scientists do when they conduct research investigating their own questions)
7. Problem and Project based learning (in Problem-Based-Learning students work in small groups on an open-ended problem. They first study the trigger material and work individually to come up with an idea to solve the problem and then the team discusses on choosing the solution. Project based-learning is an extension of problem-based learning where the duration is longer, and the outcome might be more concrete than an idea like a product or software)
8. Gamification (elements from games like badges, leaderboards and others are used in teaching in order to improve student's engagement)

After the analysis, various examples from the literature, where those methodologies were applied in courses relevant to cybersecurity, are presented and useful conclusions are drawn from this review. The main outcomes are the following:

- For the use of active learning to be successful, the students need to already have some level of autonomy in the subject and the groups of students (if present) need to be small and homogenous
- When using gamification, the students should adopt both the roles of the attacker and the defender because the two perspectives are useful in different ways
- Capture the flag contests inherently help the students stay engaged and can be combined with Open Day events that act as career days with the involvement of industry
- When students are also involved in the organization of those events, they gain very important managing and soft skills that can help them in their future career
- Gamification was successfully used for teaching non-technical employees to prevent phishing attacks, but care must be taken to balance the challenge in order to maximize the engagement of the learners
- Using hands-on techniques like project-based learning can enhance the retention rate of the students some weeks after the end of the course
- The use of remote accessibility to labs can help greatly the students do their research or learning in the hours they want if the additional staff hours that are needed for technical support are available

- Real Time Simulators offer a very realistic setting for the students to study the effects and mitigation of cyberattacks on power systems.

Lastly, in Chapter 5 after reviewing many documents (mainly academic papers, documents produced from European projects, taskforces and others) that were relevant to the fields of cybersecurity and/or smart grids, we provide some high-level recommendations grouped together for the various stakeholders. The recommendations that resulted from the CC-RSG workshop that was conducted in May 2021 are also included here. The main recommendations per group are listed below:

1. Universities
   - 1.1. Create an observatory and continuously monitor the new and ongoing research results
   - 1.2. Create a database with experts and researchers along with their areas of work and skills developed in the two fields
   - 1.3. Create Joint Master's degrees
   - 1.4. Harmonize the European accreditation systems through the use of the European Credit Transfer System in accordance with the Bologna Process
   - 1.5. Create an inventory where the Universities and research centres can connect their infrastructures
   - 1.6. Create a course module repository where the Universities share the design of their courses, the learning outcomes, best practices and educational content
   - 1.7. Cover less-technical aspects like the legal frameworks (General Data Protection Regulation - GDPR, Network and Information Systems - NIS directive)
   - 1.8. Give emphasis on creating professionals that both specialize in a subject but they also possess enough general knowledge to be able to cooperate with the other professionals of their field
   - 1.9. Lastly a table with the relevant recommendations that resulted from the Workshop that was conducted in the context of WP1 of our CC-RSG project is provided
2. VETs
   - 2.1. Create a project like UP-RES (Urban planners with Renewable Energy Skills) that showcases the creation of educational content and training in a field that results from the crossing of two fields
   - 2.2. Create courses and online training modules focusing on important and specific subjects like the production of an Intrusion Detection Algorithm. They can also formulate a Micro Master's degree
   - 2.3. Help the students acquire relevant certificates
3. Industry
   - 3.1. Technical recommendations
     - 3.1.1. Recommendations on technical areas to be taught:
       - 3.1.1.1. Choose a message-based model when choosing between this and a shared database model
       - 3.1.1.2. Smart Applications REFerence ontology (SAREF) model
       - 3.1.1.3. Continuous updatability and upgradability of the components
       - 3.1.1.4. Security by design and by default
     - 3.1.2. Recommendations targeting Legacy equipment
       - 3.1.2.1. Systematic patch management when available
       - 3.1.2.2. Physical security can be beneficial for legacy equipment protection

4.4. General recommendations

4.4.1. Elaborate and give enough details about new data roles. Harmonized Electricity Market Role Model (HEMRM) can be used as reference.

4.4.2. Apply Common Information Model (CIM) standards in Transmission System Operators (TSOs) and Distribution System Operators (DSOs)

4.4.3. Include a risk/cost estimation for the implementation of the various recommendations to overcome the fear of adoption that some stakeholders might have

4.4.4. Adopt a clear communication scheme

1. Introduction

The past few years have been decisive about the paradigm shift that happens in the field of the energy sector. Power systems are expanding, getting ready to accommodate the wide use of electric vehicles and energy production becomes more distributed with the use of renewable energy sources like photovoltaics and wind turbines [1]. These changes can only happen in a grid that remains reliable if they are accompanied by the almost-real-time exchange of information with which the grid is regulated. The high rate of information exchanged, the rise of the potential attack points (which form the attack surface) and the increased value of the data that is being exchanged create the need to have a workforce that is trained in the combined field of Power Systems and Information and Communication Technologies (ICT). The need for development of cybersecurity in the energy sector as a result of the increase of digitalization has also been pointed out in [2]

In the project "Cybersecurity curricula recommendations for Smart Grids" our goal is to ease the adaptation of the post-secondary European curricula as they must include learning objectives relative to cybersecurity among the others. In the previous report of the project titled "IO1: Report on state of the art, trends and skill gaps in the field of cybersecurity in smart grids in the EU" one of the objectives was to identify the skill gaps in the field of cybersecurity in smart grids. In this report (in the framework of WP2) we aim to provide directions for the relevant stakeholders on how to train the current and future workforce in the subject of cybersecurity in smart grids.

1.1 Objectives

More specifically the objectives of the current report are the following:

- Analyse the challenges that the industry faces in the field of cybersecurity in smart grids
- Create a mitigation plan based on the identified challenges and skill gaps from WP1
- Analyse and suggest appropriate innovative educational methodologies to the education providers
- Provide recommendations to education providers, policy makers and the industry

1.2 Structure of the document

The document is structured as follows:

Chapter 2 identifies the challenges faced by the industry

Chapter 3 describes the proposed mitigation plan

Chapter 4 presents an analysis on traditional and innovative educational methods considering examples of application in the field of power sector and their impact

Chapter 5 provides high level recommendations to the relevant stakeholders

This document is completed with the conclusions and annexes containing more detailed information where it was deemed required.

2. Challenges faced by the industries that work in smart grids regarding cybersecurity

The energy system is considered the most critical infrastructure around the world to provide services to other sectors. Emerging Industry 4.0 (Fourth Industrial Revolution) which integrates operational technology (OT) with information technology (IT) uses and expands the concepts of digitalization, connectivity and automation but makes the concern about cybersecurity more intense for the business and system operators. According to Global Information Security Workforce Study, there will be a shortage of 1.8 million cybersecurity jobs by 2022 [3]. It obviously indicates that there is a cybersecurity labour shortage in the market and the system is not able to keep up with the number and severity of cybercrime. Several cyberattack events have been reported which cause severe damage to businesses. For example, NotPetya malware attack in December 2017 targeted Ukrainian energy which cost around $10 billion in damages [4]. Small and medium enterprises (SMEs) are also the victims of cyberattacks even though they have not reported such incidents [5].

Cybercrime has risen dramatically, there is a high demand for cybersecurity workforce but the hiring depends on the cybersecurity skills possessed by the workforce [6], [7] [8] [9]. Lack of appropriate policy attention and cybersecurity information sharing between government and SMEs may result in more cyberattack targets. Some SMEs are alert for cybercrime and willing to transform their businesses toward industry 4.0. However, they are not well prepared to identify the cybersecurity workforce with adequate skills for hiring in their companies.

This section provides the analysis on challenges faced by the industry defined through a literature review and the qualitative interviews that were conducted in the context of WP1 of this project in the context of cybersecurity in smart grids. The challenges will serve us as the input to identify the needs in policy and educational changes to enable the development of a concrete strategy for cyber security education to meet the industry expectation on becoming a competent cybersecurity professional.

2.1 Challenges that emerged through literature review

Industry 4.0 aims to integrate information and communications technology (ICT) to automate the whole supply chain industrial operations [6] [10]. Cyber-Physical Energy Systems (CPES) enable digitalized automation services but also pose a cybersecurity concern to system operators. This is because the existing infrastructure was not designed for the cyber vulnerabilities which can harm the business performance during the industry 4.0 transformation. Emerging industry 4.0 has imposed several challenges to both technical and non-technical sectors related to cybersecurity which the business owners must take into account and prepare for active and passive measures. While technical challenges need technological solutions, non-technical challenges are related to a cybersecurity culture.

In the past, cybersecurity was seen as a technical challenge rather than a subject related to employee behaviour that can cause business risks. It is a challenge for the industry how to raise the cybersecurity culture awareness related to the business services [11] [12, 6]. Most employees do not have security risk management responsibilities in their job descriptions, so leadership involvement and cross-functional collaboration are essential to prevent and minimize the risk and additional costs [12, 13, 14, 5]. Fundamental cybersecurity education and knowledge are provided by high education institutions (HEIs) and online open courses

mainly on the areas of data, network and computer systems. However, the cybersecurity ethics and cybersecurity culture, as well as the personal prejudice related to cybersecurity, are still inadequate in the curricula of HEIs. While there is much discussion around technical solutions to cybersecurity issues in literature, there is far less focus on a skills mismatch between what industries would like to see in a candidate for employment and the skills that the candidates possess after graduating. Cybersecurity encompasses a very broad range of specialty areas and work roles, and no single educational program can be expected to cover all of the specialized skills and sector-specific knowledge desired by each employer.

2.1.1 Technical Challenges

Students need to be offered both a theoretical and practical background in the field of smart grids and have the opportunity to gain hands on experience. Offering the real-world simulation environment is highly required for students to gain competencies that can be acquired through exercise and cybersecurity context. Universities and industries have set up CPES laboratories and testbeds to provide education and training to students but still lack real-life scenarios and multidisciplinary knowledge. It is nearly impossible to have all critical components in a single laboratory due to high investment costs. One solution with lower investment cost is to use virtual components and/or virtual access through the collaborations between institutes and industrial partners. The industry and university can exchange the experience i.e. industry shares the real-life scenario, the university provides the experimental training. Some CPES laboratories can only provide one domain either a power system or a communication system, however, laboratories must provide both domains in a complete scenario to demonstrate their integration and interaction. Students should be able to understand the cybersecurity development platform where vulnerabilities would occur and how to prevent them.

In the CPES ecosystem, no one solution can solve and address all cyber threats. High-skilled professionals or highly interconnected multi-professional teams with multidisciplinary knowledge and hands-on experiences are highly required in the smart grid domain. Cybersecurity training should be better prepared at the curricula especially the more practical and hands-on scenarios to prepare students to become competent cyber security professionals for the future labour market [15, 16, 5]. High education institutions (HEI) have adapted their curricula for students to meet the industry expectations but still cannot meet all requirements. Students should be well prepared for both technical and non-technical challenges to be able to tackle the vulnerabilities that might arise from the cyberattack or human error and/or negligence. This section will elaborate on the challenges that have been addressed in literature in technical aspects.

Existing security standards and guidance documents such as ISO/IEC 27001 on information security management systems issued by the International Organization for Standardization (ISO) and the NIST cybersecurity framework promoted by the US National Institute of Standards and Technology (NIST) provide high-level cybersecurity guidelines but they don’t cover adequately the critical assets to be protected or the recommended up to date measures [12]. European Union Agency for Cyber-Security (ENISA) has developed a cybersecurity EU education map with specific cybersecurity tasks and cybersecurity skill gaps as the guidelines for developing the effective cybersecurity education [17]. In addition, the report from ENISA in 2020 has clearly pointed out the major challenge for a strong collaboration between HEIs and industry [17].

In the EU, CEN (European Committee for Standardization) has provided certification schemes for cybersecurity skills and competencies based on the Role Profiles in the workplace [5, 18, 19]. Role and Role profile are derived from an organizational assignment to an employee and its profile is related to specific activities or tasks. Two standards in the EU are providing the reference and competencies for the role profile in the ICT areas which are EN16234-1 and EN16458. While EN16234-1 provides the European Qualification Framework (EQF) by defining 41 competencies, skills and knowledge required for performing the job in the ICT sector, EN16458 identifies the EU ICT Professional Role Profiles which consists of four Role Profiles related to cybersecurity: cybersecurity manager, system administrator, network specialist and cyber security specialist. In the USA, the competence and role profiles are identified by National Initiative for Cybersecurity Education (NICE) initiative which consists of Securely provision (SP), Operate and maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyse (AN), Collect and Operate (CO), Investigate (IN) [5, 20].

In addition to providing hands-on experience and a real-world simulation environment, relevant certification should be further harmonized and developed to enhance the essential skills by covering the hands-on experiences required by the industry. This will help encourage the educator within the industry and HEI to develop and revise the course outlines and training program to meet the employer's expectations.

2.1.2 Non-Technical Challenges

Several non-technical challenges have been addressed in the literature related to the cybersecurity culture. The cybersecurity culture implies attitudes, mindset, perception, and ethics. Several studies have revealed consistently that building a cybersecurity culture is essential for improving employees' security behaviour. Cybersecurity culture is "contextualized to the behaviour of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements cautiously and attentively as embedded through regular communication, awareness, training and education initiatives" [21]. The organization can implement the guideline of SETA (Security Education, Training, and Awareness) to improve the cybersecurity culture. SETA programs have been used since the 1990s in many big companies to ensure that their employees are aware of the current cyber threats in their working environment. [22] The five key initiatives are 1) Identifying key cybersecurity behaviours, 2) establishing a cybersecurity champion network, 3) developing a brand for the cybersecurity team, 4) build a cybersecurity hub, and 5) align security awareness with external campaigns. The cybersecurity culture can be introduced at the HEIs to raise awareness about cybersecurity behaviour. This is the fundamental knowledge for building the mindset and attitude towards cybersecurity. In the UK, every course provided by the British Computer Society must give students an awareness of external factors which may affect the work of the computer professional [23]. This guideline can also apply to every curriculum at the HEIs rather than focusing only on the students in the computer science area.

During employment, leadership in cybersecurity and organization policy are driving factors to enhance the cybersecurity culture in the company. Employee negligence such as malicious behaviour, password storage, and phishing emails, is still a major cause of cyberattacks. Executives and top managers have more responsibilities in cybersecurity than other employees because the severity of a cyberattack might result in high costs i.e. paying

the ransom or hiring an external cybersecurity specialist to solve the attack. Non-ICT employees are not very active and interested in cybersecurity skills and awareness to be able to understand the vulnerabilities and to react properly and promptly in the case of a cyber incident [24, 11, 6, 13, 14, 25]. It is the employer's responsibility to express the leadership involvement in cybersecurity to provide and enforce a set of practices to the employee such as cybersecurity updates or roadshows, internal and external communication initiatives serving as cybersecurity advocates. Big companies with high-tech products and services are already characterized by a stronger cybersecurity culture. In other words, the cybersecurity culture should be a strategic and operational priority for the company.

According to the ENISA report in 2020 [17], the lack of strong interconnection between HEIs and industry is a major challenge of providing adequate education and training in cybersecurity which includes funding and technical support. Poor collaboration between HEIs and industry may lead to misunderstanding about the real situation of the cybersecurity labour market which would result in a lack of specialization of cybersecurity of HEI educators for the current situation. Collaboration and information sharing by building trust within and between organizations are highly needed to coordinate action. Trust in this context implies competence to perform functions or actions reliably, benevolence (in that harm will not occur to participants in the relationship), and integrity in keeping commitments. A study of cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry, has indicated the information-sharing network into three levels: interpersonal (micro), organization-to-organization dyadic (meso), and organization-to-multiorganization triadic (macro) levels [15]. Trust between individuals and trust between organizations develops sequentially through three different modes or phases: 1) calculus-based trust, which is short-term and transactional; 2) knowledge-based trust, which is based on a history of interactions between the two parties; and 3) identification-based trust, where the two parties each believe that the other can faithfully represent their interests in dealings with others. Building trust and sharing information depends on the business context and their relationship intensity.

A regulatory authority is often not seen as a central entity for information sharing but rather as a law enforcement entity. As a result, a weak voluntary collaboration between stakeholders and the regulator can be seen. Regulators should play a key role in improving threat and solution awareness and reducing uncertainty. On the other hand, the company and industry leaders may establish collaboration at the micro, meso, and macro level to enhance trust within and across the network to share the proof of practice that can be implemented in the event of cybersecurity attacks.

In addition, international collaboration is also needed to raise awareness and knowledge solution sharing from technical, managerial and social standpoints. The study has indicated that some schemes in the USA are still missing in the EU for example the topics of Organizational security, Anonymising data, Social Security, Physical interface, and connectors.

2.2 Challenges that emerged through interviews (qualitative analysis)

The literature review provides nearly up-to-date information but cyber technology trends change very quickly. A qualitative interview is needed to fill the gaps and ensure that all cybersecurity education aspects are addressed. Hence, the qualitative interview was conducted in the framework of CC-RSG with interviewees from industry and academia. Due to the time and resource limitation, there were only five interviewees, therefore the small

sample size prevents us from doing a quantitative analysis of the results, rather a qualitative analysis is made of their opinions which are very relevant because of the close collaboration with both students and clients in the field of cybersecurity in smart grids. The interviews took place virtually without recording due to the General Data Protection Regulation (GDPR). Each interview took approximately 30-40 mins with a structured interview protocol as shown in Annex 1. To align with the literature review in section 2.1, the analysis of qualitative interview is elaborated to the education extent into two aspects: hard-cybersecurity skill (technical aspect) and soft-cybersecurity skill (non-technical aspect).

2.2.1 Hard-cybersecurity skill education

According to the literature review of WP1, there is extensive research on system security, connection security, and component security whereas the focus on organization, human and societal security is very low as shown in Figure 1 Categorization of skill gaps based on the literature review [26]. The interviewees were asked if they agreed to these findings. All interviewees agreed with the findings shown in Figure 1. This figure shows the results of a literature review [26] , about whether the different knowledge areas of the ACM framework are being researched. The results show that hard security skills related to technological cybersecurity solutions such as system, connection and component have been areas of significant focus whereas soft-cybersecurity skills are the least covered in the curricula. In other words, soft-cybersecurity skills are mostly undervalued compared to hard cybersecurity skills.

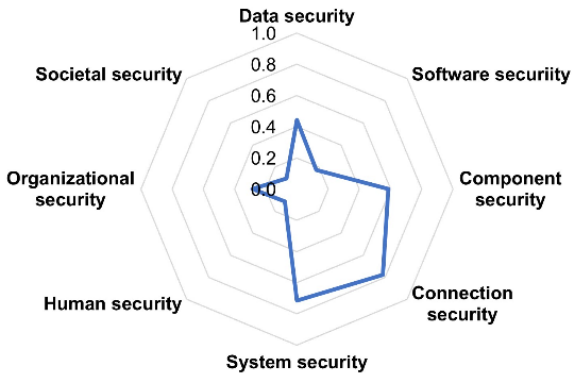


Figure 1 Categorization of skill gaps based on the literature review [26]

Societal security is rarely included in the curricula but human security and organization security are somewhat considered. As a result, practices and training programs in soft-cybersecurity skills are very low. One interviewee has expressed that it is nearly impossible to provide a detailed program covering all cybersecurity domains in one single curriculum due to lack of educator workforce who are specialized both in hard and soft cybersecurity skills. Soft cybersecurity skills should be given greater attention in the curricula because an employee in practice does not only deal with the technology but also non-technical cybersecurity challenges.

Interviewees have expressed that recent graduates have general knowledge about cybersecurity but it is considered as the junior level. It is aligned with the literature that students lack hands-on experiences that they need to learn on the job. In addition, if the recent graduates acquired high-level knowledge on an informational standard such as ISO

27001 information security management system (ISMS), it would enhance the training period on the job more effectively. Information Security Management Systems (ISMS) provide a set of policies and procedures managing cybersecurity in an organization as shown in Figure 2. Organizations and companies should provide cybersecurity know-how to the employees both IT and non-IT employees. Students should be able to understand to a certain extent how information security is managed in the organization. This can help to bridge the gaps of ineffective communication between non-IT and IT employees.

Lifecycle of the security concept	
P	**Planning and conception** • Choosing a method for risk analysis • Classification of risks or damages • Risk analysis • Development of a strategy for handling risks • Selection of safeguards
D	**Implementation** • Implementation plan for the security concept • Implementation of the safeguards • Supervising and control of the implementation • Implementation of a Business Continuity Management • Training and Awareness
C	**Performance review and monitoring** • Detection of security incidents during operations • Monitoring compliance of regulations • Monitoring suitability and effectiveness of safeguards • Management reports
A	**Optimization and improvement** • Correction of defects • Improvement of safeguards

Figure 2 Overview of the lifecycle of a policy for information security [27]-redrawn

In addition, strong engagement with practical knowledge is the main reason for recent graduates to be ready for the job. Some students lack in-depth knowledge on the topics which can be mitigated by the mentoring program through internship programs and student assistant jobs during their study. However, internship programs from the companies depend on the interests of the company and the projects at hand. The main driving factor for students to engage in practical knowledge is their interest and motivation on the topics. This gap should be the main focus of cybersecurity education curricula. Interviewees highlighted that if new employees lack such technical skills, they will be trained from scratch during their probation period through training on the job (i.e. external commissioning project), mentoring programs, external training programs provided by private educators and/or university, self-study, workshops and seminars.

2.2.2 Soft-cybersecurity skill education

Cybersecurity culture is highly required besides the technical basic knowledge. The cybersecurity culture includes elements such as mindset, awareness, openness, critical thinking and willingness to learn. One interviewee has specified the need for secure administration domain which is important for ensuring the security of an organization's computer systems. The cybersecurity culture would help the new employee to absorb the

required skills of the job during the training period and further develop new solutions related to problems. Some interviewees have indicated that new employees lack soft-cybersecurity skills because it is always seen as a minor topic compared to hard cybersecurity skills during their studies. This is also in line with the literature review.

Interviewees also indicate that new employees lack soft skills besides cybersecurity knowledge such as management and communication skills. Junior cybersecurity experts need to practice on the job for effective communication between IT and non-IT employees and clients. Lack of effective communication is one of the identified gaps. This is because students are taught in the class using technical terms and rarely practice how to communicate. As a result, recent graduates face communication challenges to non-cyber security employees including executives. Communication skills can be trained during the study with hands-on experiences and training on the job with customers.

Risk management is one of the soft-skill topics that young cybersecurity professionals should obtain during the job which will help them to minimize the costs related to uncertainty and ensure business operations continuity. Interviewees have confirmed that executive and top managers have a direct impact on enhancing cybersecurity awareness and knowledge. The cybersecurity issues must be seen as the policy rather than the KPI (Key Performance Indicator) to meet and/or additional cost of the company. The mindset of the executive is very essential to establish the roadmap and action plan to prevent the vulnerabilities that might occur.

2.3 Identified needs in policy and educational changes

The previous sections provide the challenges faced by industry from the literature and qualitative interview. Technical skills or hard-cybersecurity education with hands-on experiment is indeed needed to perform the tasks in real-world whereas soft skills must be enhanced in the curricula to perform the tasks more effectively. The policies enforced and the educational roadmap should both develop the skills of the graduates in alignment with the industry needs and help further the career for the recent graduates. This section provides the policy recommendations for the education changes to enhance cybersecurity skills as well as the collaborations between industry and academia.

Proposition 1: Providing hands-on experience and training program

The field of cybersecurity changes very quickly and it is nearly impossible for the recent graduate to be ready for the job from day one without hands-on experience. Basic technical educations and skills are provided in the curricula such as computer architectures, networking, coding principles, common exploitation methods and mitigation techniques [25] but students still lack hands-on experiences and use cases. Cybersecurity challenges are dynamic, hence higher education institutes (HEIs) need to provide the cybersecurity science for future professionals to be capable of updating their skills in the technological dynamic environment. There are several studies suggested for the cybersecurity education curricula such as ENISA database and the CyberSec4Europe project [28, 29, 30]. These studies can be used to further develop and update the missing skills for the students in the future.

A study has suggested two models for the future of cybersecurity with hands-on experience to balance the employability of the students [31]. The first one is an information-technology specialist program that provided experienced employees or students the chance to enhance their skills for governance, risk management, constraints and control. The second one is similar to the first one but aims to the students or new employees with high-level expertise to enhance risk management and asset evaluation and vulnerabilities removal. There are several techniques for teaching students towards cybersecurity. Capture the flag (CTF) games and competition approach is a promising technique which has been taught successfully in school and university classes [15]. An example is shown in Figure 3. The students are able to practice a wide variety of cybersecurity skills online in a hands-on environment. Curricula relevant to cybersecurity should reach a broader audience to IT and non-IT students and the contents must be adapted to their background knowledge, ability and intended skills for the career.

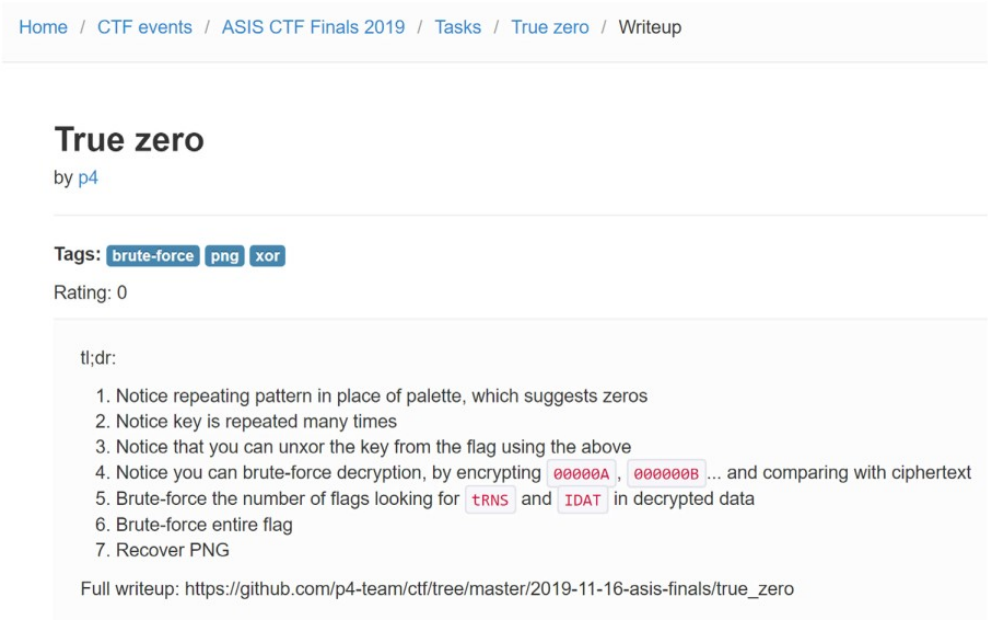


Figure 3 Example of a writeup. Source: https:// ctftime.org/ writeup/ 17308 [15]

In addition to the hands-on experience, there is a high need for cybersecurity curricula on organizational, human, and social domains which results in missing managing and operating skills on the job. One study has indicated that the documentation area is not well covered in the current curricula which found that only 15% of the programs cover this aspect [5]. This area should be included in future curricula to teach recent graduates how to develop good documentation in the cybersecurity field. Cybersecurity in the EU should pay attention more to multidisciplinary knowledge, and practice-oriented rather than theory-based education.

Proposition 2: Enhancing cross-functional collaboration

To provide hands-on experience to the students, industry can play a key role in providing the use cases that students can learn and practice. An internship program can be found in some companies but the topics depend on the company's expertise, services and budget. Collaborations between universities and industries should be strongly enhanced and supported by the government especially the research budget. Building trust between industries and the university is one of the essential policies of the government to enhance

effective collaboration. Research budget and its framework should be developed in the long term. Some industrial sectors may have information-sharing networks to exchange the knowledge and lessons learned between them but between university and industry it is not well formulated. The university can have real-world use cases with support from the industry whereas the industry can develop innovative cybersecurity measures to protect their businesses. Government is a key driving force for building trust and collaboration platforms between industry associations, governmental agencies, research and academic institutions at national and international levels.

Proposition 3: Building cybersecurity culture

Cybersecurity culture is highly needed for education and real-world employment. However, the cybersecurity culture is not well covered in the current curricula. Cybersecurity culture is essential to develop a cybersecurity mindset and awareness towards student's behaviour improvement. The current Cybersecurity Curricular Guidelines (CSEC) 2017 defines cybersecurity as "a computing-based discipline involving technology, people, information, and processes to enable assured operations" [15]. Higher educational institutions can create new education and training courses on cybersecurity culture for IT and non-IT students as well as interested people. A manager of the ICT department should understand the practical techniques to prevent and mitigate vulnerabilities while a manager that leads a non-IT department should at least understand the risks and methods to protect the company's assets.

Cybersecurity culture can make an impact on daily activities and beyond the business level if the executives understand cybersecurity and how it affects the businesses. Several companies and organizations use Security Education, Training, and Awareness (SETA) courses to improve their employee's awareness and mitigate cybersecurity threats. However, some employees may not be well informed about the available cybersecurity course due to several factors such as individual mindset, conflicts with their roles, complicated content. Educational institutions must enhance cybersecurity culture to students in the school by establishing content that is easy to understand. This would help the student to mitigate the vulnerabilities not only related to their future jobs but also their daily activity. Building a cybersecurity culture requires effort and time, hence it should be provided in the school for young students (i.e. primary and secondary school) with the adjustment of the content that is suitable for the audience.

To summarize the above chapter, through conducting both a literature review and a small number of interviews with representatives from the industry some key observations were made. Cybercrime in the energy field has risen dramatically, and cybersecurity workforce cannot cope with the number and severity of cybercrime due to the shortage and inadequate required skills. Basic technical skills (i.e. hard-cybersecurity skills) are provided in the current curricula but it is not well equipped with hands-on experiences as well as soft-cybersecurity skills and cybersecurity culture. While there are extensive studies about the component, connection and system security domains, soft-security skills such as human, societal and organizational domains are not yet well represented. Graduate students also often lack effective communication skills with non-IT employees, executives, and clients. There are three policy recommendations for future education changes in the cybersecurity context which are 1) Providing hands-on experience and training programs, 2) Enhancing cross-functional collaboration, and 3) Building cybersecurity culture. Experiences from the industry are highly required to provide hands-on practices to the students. Available testbeds and laboratories

are set up for providing scenario experiments to the students but not all can support multi-domain experiments and real-world use cases. Higher educational institutions can encourage students to attend webinars, open-online courses, mentorship programs, internships, and student assistant tasks. Most importantly, cybersecurity technology is dynamic and changes very quickly, therefore the curricula should also support the students to update their skills in the dynamic technological field. Multidisciplinary knowledge with hands-on experience is the priority to enhance the cybersecurity labour shortage in the EU.

Obtaining hands-on experience can be greatly facilitated by industry involvement. The existing collaborations between industry and education institutions are not yet well formulated. Existing collaboration can be seen as knowledge-based trust and calculus-based trust where two parties have historical interactions and activities in the short term. Government should establish a sustainable collaboration platform at the macro level with research funding to build long term trust between them. Building trust between industry and academic institutions is a key factor for successful collaboration. Information sharing between industry and education institutions will increase the hands-on experience of the students whereas industry can gain innovative ideas. An inadequate workforce with real-world experience can be enhanced by promoting collaborations between industry and high education institutes. This is not only limited to information sharing within the EU but it includes international collaborations. Although there are many curricula addressing cybersecurity (from the IT perspective), cybersecurity should be included to an extent in many more fields of study as it is a horizontal issue. Building a cybersecurity culture requires effort and time so it should be also introduced in the school for younger students. The content must be designed to be suitable to their background, interests, and skills. Cybersecurity culture should reach a broader audience of IT and non-IT students as well as interested persons and non-IT employees. A training program on cybersecurity culture would enhance students' awareness behaviour, improve vulnerability detection and protection on the job and their daily activity.

3. Skill gaps mitigation plan

In this chapter actions are summarized in a skill gaps mitigation plan that consists of several initiatives that can be performed by industry and/or academia.

3.1 Mitigation actions

In EU, the subject of Cybersecurity is represented in different education forms such as Higher education (both universities and VETs), Continuing education and MOOC (Massive Open Online Courses). However, there are significant skill gaps, especially, in smart grids specific cybersecurity knowledge areas. The various cybersecurity subjects are divided in knowledge areas and knowledge units according to the Association of Computing Machinery (ACM) Cybersecurity Curricular Guidelines classification [32] . Skill gaps are identified based on performed literature review (Project's WP1), Cybersecurity MSc Education survey results [33] as well as smart grid cybersecurity industry and academia experts' workshops (Project's WP1).

Scientific and industry literature analysis results (Project's WP1) highlight skill gaps in cybersecurity management tools, secure smart grid systems design and organizational security. MSc Education survey results [33] conclude that skill gaps are identified in almost all ACM and NIST defined knowledge areas: Data Security, Software Security, Connection Security, System Security, Human Security, Organizational Security, Societal Security. Industry experts additionally emphasize skill gaps in cybersecurity architecture, cybersecurity tools and energy supply chain cybersecurity.

Literature and experts [33] [34]] identify the following skill gaps frequent Root Causes (RC):

- **RC1**. Insufficient academic and professional cybersecurity education offering and coverage, including:
  - limited smart grids security specific education offering;
  - limited practical cybersecurity exercises and real-life scenarios simulation integration in education programs;
  - lack of role-specific cybersecurity trainings (for example, specific cybersecurity trainings for Cyber Defence Forensics Analyst, Database Administrator, Enterprise Architect or Lawyer roles);
- **RC2.** Limited cybersecurity education accessibility, including:
  - time management issues caused by heavy experts' workload;
  - unavailable trainings budget for individuals and enterprises;
  - courses time and form limitation – limited availability of distance, online and blended academic education programs.
- **RC3.** Missing knowledge and best practices in smart grid specific cybersecurity management;
- **RC4.** Insufficient usage of automated cybersecurity management tools with built-in best practices.

The mitigation plan of CC-RSG outlines recommended initiatives to eliminate or reduce cybersecurity skill gaps in smart grids that can be performed by academia and/or industry. Both areas' (industry and academia) collaboration is essential to reduce skill gaps and improve overall cybersecurity capabilities level.

For academia it is suggested to focus on the following actions as treatment for skill gaps root causes:

- **RC1**. Enhance cybersecurity education offering and coverage from academic education perspective;
- **RC2**. Increase academic education availability and
- **RC3**. Generate new knowledge from scientific research.

The main recommended initiatives for academia are:

1) Enhance smart grids cybersecurity education programmes accessibility & coverage, including:
   - smart grid cybersecurity courses integration in energy study programmes;
   - distance, online & blended cybersecurity education offering increase;
   - interdisciplinary cybersecurity programmes offering increase (for example, law, ICT and psychology studies integration);
2) Conduct research projects in cybersecurity field to get new knowledge about skill gaps related aspects that can be communicated via publications and conferences, as well as integrated in education programmes;
3) Design and implement technical infrastructure to increase practical trainings possibilities such as virtual laboratories and digital twins (that can be used for real-life scenarios simulation, for example, SCADA (Supervisory Control and Data Acquisition) or domain controllers cyberattacks).

For industry it is suggested to focus on the following actions as treatment for skill gaps root causes:

- **RC1**. Enhance cybersecurity education offering and coverage from professional education perspective;
- **RC2**. Enable cybersecurity trainings accessibility,
- **RC3**. Gain new professional knowledge; and
- **RC4**. Implement cybersecurity management tools.

Main recommended initiatives for industry are:

1) Establish industry specific competences & excellence centers that focus on smart grid security topics and include both industry enterprises and relevant academia bodies;
2) Increase access to roles-specific professional education and relevant certifications;
3) Promote trainings and education as mandatory for personnel (part of working time can be allocated to trainings, training budget must be available);
4) Establish innovation laboratories inside organizations to enable new cybersecurity technology explorations and implementation;
5) Increase cybersecurity tools usage in organizations (as SIEM- Security Information and Event Management, SOC- Security Operations Centre etc.);
6) Perform regular security awareness trainings in organizations (including, gamification elements), as well as relevant soft skills trainings (as stress management etc.)

Main recommended industry and academia collaboration initiatives are:

1) Collaboration in education and training programs development (education programs must be designed taking in consideration industry needs);
2) Collaboration in cybersecurity related R&D projects (as cybersecurity tools or cyber-range platforms development) to rise both sides personnel competence level and gain new knowledge that can be used to increase overall cybersecurity capabilities level.

In the following table (
Table 1), for each of the knowledge units of the ACM classification and for each knowledge unit, we have included a set of mitigation actions based on our estimation of whether the skill gaps in this knowledge unit are mainly caused by the industry or the education.

Mitigation Actions												
Knowledge area	**Knowledge unit**	**Knowledge of the component in the power system**	**Conduct international research in cyber security**	**Knowledge of network security**	**Professional training**	**Certificates**	**Self-teaching**	**Knowledge**	**Workable Soft-Skills**	**Learn new technologies**	**Practical use cases**	**Basic tools for threat analysis**
Data Security	Cryptography	X	X	X	X	X						
	Digital Forensics						X	X	X	X	X	X
	Data Integrity and Authentication	X	X	X	X	X						
	Access Control	X	X	X	X	X						
	Secure Communication Protocols	X	X	X	X	X						
	Cryptanalysis						X	X	X	X	X	X
	Information Storage Security						X	X	X	X	X	X
Software Security	Fundamental Principles	X	X	X	X	X						
Connection Security	Physical Media						X	X	X	X	X	X
	Hardware and Physical Component Interfaces and Connectors						X	X	X	X	X	X
	Distributed Systems Architecture	X	X	X	X	X						
	Network Architecture	X	X	X	X	X						
	Network Implementations	X	X	X	X	X						
	Network Services						X	X	X	X	X	X
	Network Defence						X	X	X	X	X	X
System Security	System Management						X	X	X	X	X	X
	System Access and Control						X	X	X	X	X	X
	System Testing	X	X	X	X	X						
	Common System Architectures	X	X	X	X	X						

Human Security	Identity Management	X	X	X	X	X						
	Social Engineering	X	X	X	X	X						
	Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms						X	X	X	X	X	X
	Awareness and Understanding						X	X	X	X	X	X
	Personal Data Privacy and Security	X	X	X	X	X						
Organizational Security	Risk Management						X	X	X	X	X	X
	Security Governance & Policy						X	X	X	X	X	X
	Systems Administration						X	X	X	X	X	X
	Security Capabilities						X	X	X	X	X	X
	Cybersecurity Planning						X	X	X	X	X	X
	Cybersecurity Performance Indicators						X	X	X	X	X	X
	Business Continuity, Disaster Recovery, and Incident Management						X	X	X	X	X	X
	Security Program Management						X	X	X	X	X	X
Societal Security	Cyber Law	X	X	X	X	X						
	Cyber Policy	X	X	X	X	X						
	Cyber Ethics	X	X	X	X	X						
Cybersecurity tools	Cybersecurity tools overview						X	X	X	X	X	X
	SIEM						X	X	X	X	X	X
	Digital Twins usage in cybersecurity						X	X	X	X	X	X
Energy supply chain cybersecurity	Energy supply chain cybersecurity fundamentals						X	X	X	X	X	X
	Energy supply chain cybersecurity management tools (incl. energy domain controllers monitoring tools)						X	X	X	X	X	X
	Energy supply chain cybersecurity monitoring						X	X	X	X	X	X
	Energy supply chain cybersecurity events management						X	X	X	X	X	X

Table 1 Smart grid cybersecurity skills gaps mitigation plan of CC-RSG

3.2 Difficulty of the integration of the proposed actions to existing curricula

To complete the mitigation scheme, the mitigation actions should be considered as the baseline for developing educational curricula that are able to fill the identified skill gaps. For future implementations, the task of adopting a new roadmap in new curricula is rather simple and straightforward since the skills and their requirements are considered while still being in the design phase. Such an early adoption and integration comes with many benefits as it helps

to achieve effectiveness as well as efficiency of implementation. In contrast, the task of integrating a roadmap and developing existing curricula is seen challenging as it comes associated with some difficulties that need to be addressed.

At this point, one can classify curricula integration difficulties into four categories, namely, teachers' difficulties, subject/curriculum difficulties, learners' difficulties, and organization difficulties. First, regarding the human factor, teachers and instructors – generally – face issues with introducing new skills and concepts to current curricula since this task requires coordination, upgrades of technical and pedagogical skills, in addition to the time being consumed [35]. In [35] and [36], the main difficulties faced by teachers are extracted and highlighted as follows:

1. Alternation of the teaching methodology: changes being made to the style and methods of teaching. These typically are perceived positively while being in the development phase, but the results following implementation might drastically differ.
2. Inadequacy to teaching some matters to different curricula: the focus would shift towards some topics or concepts, leaving other topics not properly covered
3. Changes in objectives and syllabus
4. Adjusting teaching means: This is related to point 1, and also relates to the organization changes in next section
5. Evaluation: evaluation criteria would need to be adjusted to reflect on the new changes
6. Structuring, availability, and applicability of content

Second, regarding subject, integration of new curricula or frameworks face the following challenges [37] [38]:

1. Lack of learning resources: resources are not always available to cover the development and required changes
2. Underdeveloped staff: related to the previous section, staff skills directly affect the quality of curricula delivery. Accordingly, new objectives cannot be met until staff are highly qualified and ready to implement the developed curricula
3. Management support
4. Workload: new implementations might be time consuming
5. Readiness to accept new approaches
6. Implication: In minor situations, curriculum integration might lead to unexpected negative impacts.

Third, regarding learners, the changes in long established curricula might be considered as deviations and not as a change in direction, which creates the need to adequately communicate to the students the need for the change in the curriculum. However, mostly changes will be associated with resistance, and might lead to low trust in the organization and its credibility. Finally, since upgrading curricula might require special services and educational/training tools, not all organizations are able to afford such upgrades, which accordingly would affect the delivery and quality of the upgraded curricula.

Previous issues are typical of difficulties that need to be considered while developing new curricula. Still, as indicated in [39], it would help to give special emphasis to creating cross-national curricula that has much flexibility and thus serve more regions and sectors.

4. Proposal of Educational methodology

An educational methodology is not only a set of rules by which the act of teaching is implemented but also a description of the goals the teaching has and the means that are going to be used to achieve those goals. The primary traditional methodology is the lecture-based learning which can be easily and cheaply implemented for large audiences of students and is often complemented with a limited use of more practical methodologies (e.g., in labs) that are examples of experiential learning.

In the next paragraphs the results of a review of the traditional and innovative educational methods will be presented along with examples of their use in the domain of power systems and smart grids and the impact they had on the learning process. Depending on the results of the review, proposals are given to increase the effectiveness of the teaching in different settings.

4.1 Characteristics of educational methods

4.1.1 The traditional learning model - Lecture based learning

Lecture based learning is a passive form of learning where the students are exposed to a large amount of information within a limited amount of time mostly about abstract symbols and ideas and subjective experience does not take place [40]. Johnson (1998) and Hall (2002) recognized two stages in traditional learning: encoding and decoding. They are followed by examination to assess the students' performance [40]

This format is chosen because it has three main advantages. First it can be scaled up to large audiences while requiring one teacher for the lecturing, second the teacher (and consequently the institution) has the control of the contents of the lecture and third it has a large ratio of volume of information relative to time required [40] The main disadvantages of the method mentioned in [40] are that the knowledge delivered by the teacher appears unchallengeable and that the students invest their effort in memorizing the material rather than understanding it in order to be able to apply it.

4.1.2 Experiential learning

Experiential learning is a model published by David Kolb in 1984 and it is based on the idea that "Learning is the process whereby knowledge is created through the transformation of experience" [41]. The model (Figure 4) contains four stages that are meant to be repeated cyclically and expand one's knowledge. Through active experimentation the student gains some concrete experience on the subject studied. With reflective observation upon the results of the experience from various perspectives, the student engages in abstract conceptualization through which they create theories. Those theories are used in order for the design of the new experiments likely in a more sophisticated level and the cycle begins again.

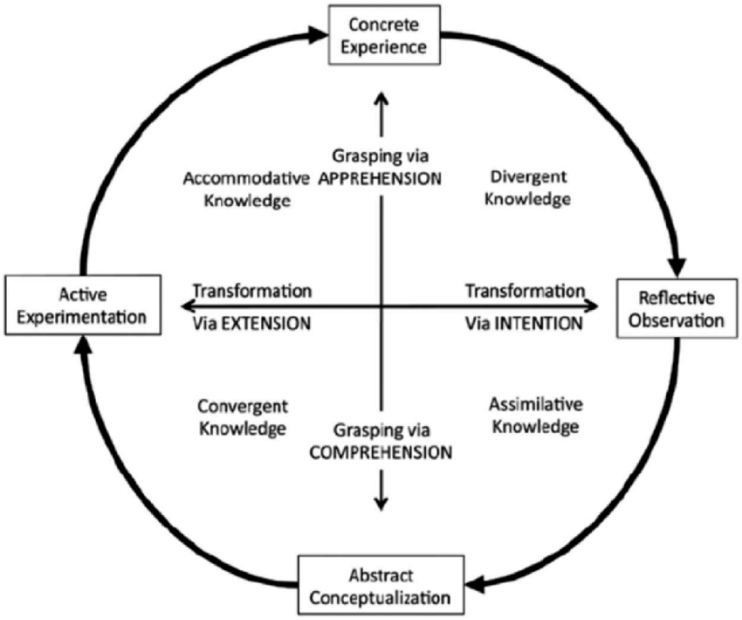


Figure 4: Experiential learning cycle [109]– reproduced under license

The basic characteristics of experiential learning are the following: [41]

- Learning is not finalized at a point based on outcomes but it is a process that is always ongoing. Ideas are constantly reformed so it is important not only to create new ideas but to examine the old ones and modify or dispose them. Sometimes one cannot absorb a new idea because it conflicts with one that they already have. So, it is very important for the process to analyse and test the students' existing ideas in order to accommodate the integration of the new ones.
- The four stages of the process require four different abilities that lie on the ends of two different axes. Concrete experience and abstract conceptualization are the two ends of the "Grasping" axis and Active experimentation and Reflective observation are on the ends of the "Transformation" axis.
- Learning is a holistic adaptive process that integrates all the functions of a human like feeling, perceiving and behaving and it involves transaction between the student and the environment. Through the process of learning, one acquires knowledge which is the result of the transaction between the personal and the social knowledge.

In [42], three distinct applications of experiential learning are mentioned for use in higher education: 1) Field based experiences (like internships and community service), 2) Prior learning assessment and 3) Experiential applications for personal development and classroom-based learning. Prior learning assessment means that an institute like a VET (Vocational education and training) can recognise that a student has achieved the learning outcomes of a subject by assessing the knowledge and skills he/she has developed through non-formal or informal learning [43]. Experiential applications in classroom take the form of role-plays, debates, simulations and others.

4.1.3 Active learning

Active learning intends to increase the engagement of the students by asking them to participate in the learning process. The main elements or activities used are talking and listening, writing, doing, reading and reflecting and they can be done individually, in pairs, in smaller or larger groups [44]. According to [45] Active learning techniques include both experiential (like simulations) and non-experiential techniques. They are all characterized by student involvement, development of student skills and higher order thinking on behalf of the students. Some examples of active learning techniques mentioned in [44] are the following:

- Concept maps:
  The students can be asked to create a concept map about the material of the course where the ideas discussed are organized and the relationships between them are identified.
- Collaborative writing:
  A group of students can be given a writing assignment and be asked to divide it to sections in order for each student to write a different part of the final document and then they have to discuss on the integration of the parts.
- One Minute Paper/Free Write:
  Students are asked to write for a few minutes on a topic or question from the teacher. When used between sections it can be very useful to give a glimpse to the teacher about the level of understanding of the students.
- Teaching to learn/Peer teaching:
  Students have to deepen their own understanding of a subject in order to be able to teach about it in a small group of their peers. It can also take the form of Panel discussions where students form groups and after working on a subject, they present it to the rest of the class and receive questions.

4.1.4 Cooperative learning

Cooperative learning "is based upon the work of small groups with common interests according to the motivations and needs in a specific area" [46]. It is based in the social interdependence theory which also states the five conditions that have to be met in order for cooperative learning to succeed and they are shown in the next image (Figure 5):

Figure 5: Conditions to be met for Cooperative learning to succeed [46]-redrawn

Cooperative learning provides foundation for other methodologies like Problem-Based-Learning. There are three scales on which cooperative learning is used in the university classroom:

- Informal cooperative learning in which students create ad-hoc temporary groups for a few minutes up to one class period.
- Formal cooperative learning that last from one class period to several weeks.
- Cooperative base groups which are long-term learning groups with stable membership [47]

A very important aspect of cooperative learning is that the students do not just work together in different parts of the group work but they also have the responsibility to monitor the group work, be aware of the skills and knowledge of their fellow students in order to allocate the appropriate workforce of the team to the tasks and are held responsible not only for their own part of the teamwork but for the whole teams' performance.

4.1.5 Flipped classroom

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. There may be more than one options through which the student can reach the expected learning outcome. It is important to notice that studying at home means that the student can follow his/her own pace, rewind or rewatch the parts that he/she cannot understand.

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 (which will be analysed later) to help the students attain higher levels of thinking skills.

The advantages of the method are that it is appropriate for many different kinds of learners, there is more flexibility mainly on what and when the student studies in order to be ready for the class and overall, there is better student engagement. The disadvantages on the other hand are mainly the fact that students that do not have the appropriate equipment to study at home could be left behind and more work is needed from the teacher(s) to find or prepare the study material and/or organize the work that is done during the class hour. [48]

4.1.6 Inquiry-based learning

Inquiry-based learning is the methodology that is more related to the scientific method. It includes testing hypotheses by conducting experiments and arriving to new conclusions [49]. The whole process is called an inquiry cycle as it can be cyclically repeated. It is divided in phases in order to help the students navigate through the complex scientific process. Those phases are: Orientation, Conceptualization, Investigation, Conclusion, and Discussion.

During "Orientation" the problem statement is made and the main variables are defined either by the teacher or the student. "Conceptualization" is further broken down into two sub-phases: "Questioning" and "Hypothesis generation". "Questioning" begins from the problem

statement of the previous phase and through understanding the various concepts of the problem research question(s) are formulated. In “Hypothesis generation” those research questions are transformed into a testable hypothesis. The third phase is “Investigation” during which, different experiment settings and variables are explored and data are collected. The data collected in “Investigation” are then used in the phase of “Conclusion” in order to answer the original research question and arrive on a final “Conclusion”.

After the “Conclusion”, the final phase is the “Discussion”. It also contains two sub-phases. In “Communication”, the students present their work to their peers and receive feedback whereas in “Reflection” the students reflect on their own questions, suggest changes for improvement of the experiment and formulate new hypotheses to test. These phases are illustrated in the next figure (Figure 6):

Depending on the level of the students and how close they are to graduation, the designer of the course can choose how much guidance and input information will be provided by the teacher. When the students are more mature, they can choose more freely the parameters of their experiment and set the expected learning outcomes of each phase with the facilitation of the teacher.

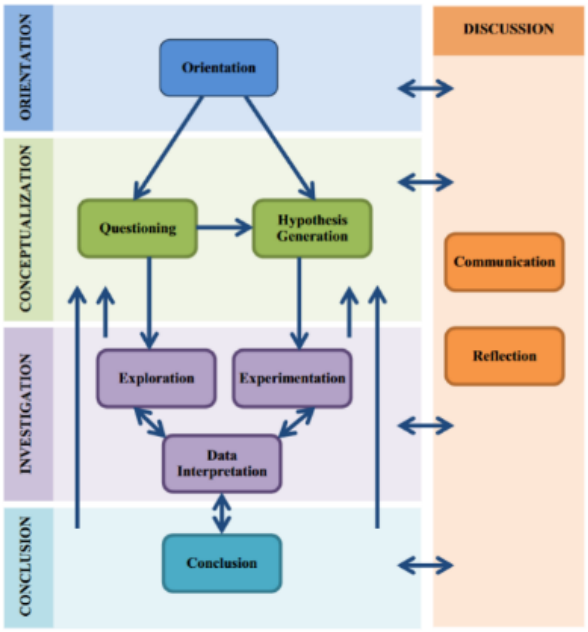


Figure 6 The phases and sub-phases of Inquiry-based learning [49]– reproduced under license

4.1.7 Problem-based learning and 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. After the group is presented with the problem, the students have to identify the facts that are available and the knowledge deficiencies that are present which will guide them towards the possible solutions [50]. The stages of PBL are shown in Figure 7.

PBL uses the Cooperative learning that we introduced previously and it is very important for the members of the group to understand that by cooperation they are able to come up with a possible solution for a problem that would be too difficult for each one to solve alone.

Another very important aspect of PBL is for the students to be mindful about the learning strategies that they develop, how they can be reapplied and how they can be more efficient. [51]

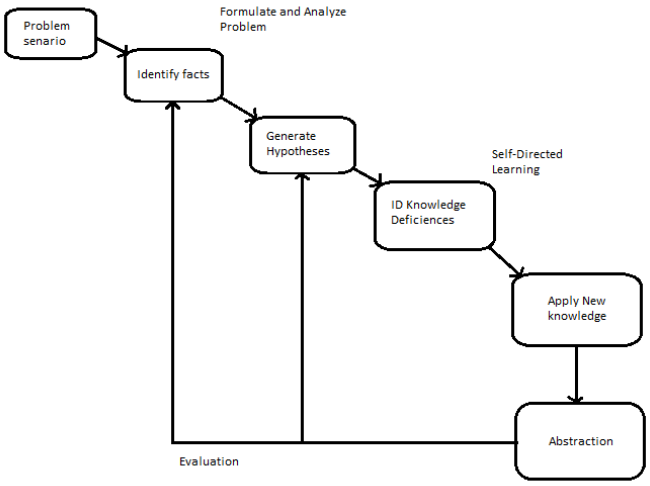


Figure 7: The stages of Problem-based learning [51]-redrawn

Project-based learning has many similarities with problem-based learning and they are both frequently referred with the acronym PBL. Their similarities include the formation of groups, the driving question (the open-ended real-world problem) and the presentation of the solution. The difference is that Project-based learning usually lasts longer and the solution is not only theoretical but it has a concrete and explicit outcome [52] like a computer program or a model. Thus, in the phases of Project-based learning as presented in [53] (Figure 8) the phase of building, testing and evaluating is shown.

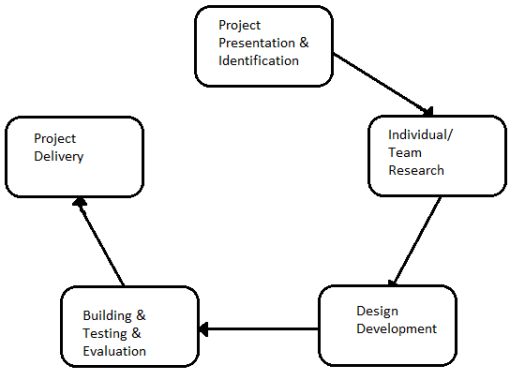


Figure 8: The five steps of Project-based learning [54]-redrawn

4.1.8 Gamification

Gamification is a teaching method in which elements and mechanisms from game designing are used to increase the student engagement [55]. Those elements and mechanisms can be for example a narrative story, limited time to accomplish a task, points, badges and level-beating. The use of Gamification does not imply that the students will develop or use a specially purposed or commercial game but that their learning experience

has some of the previously mentioned elements. Since this methodology is relatively new its definitions are still under modification. In [56] the MDE (Mechanics Dynamics Emotions) framework is introduced (Mechanics, Dynamics, and Emotions) which is graphically illustrated in the following picture (Figure 9):

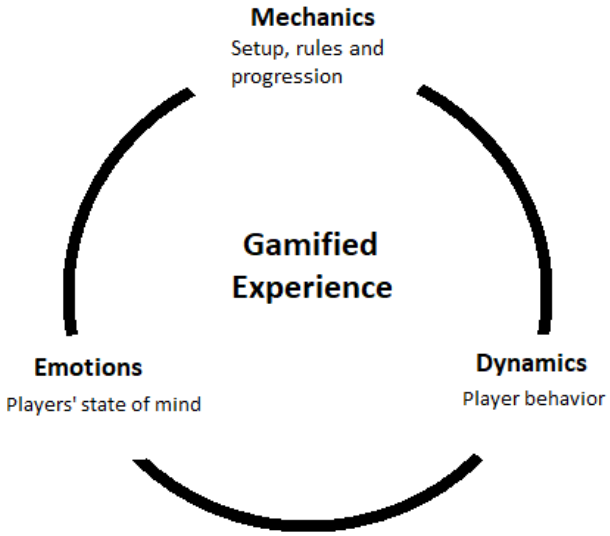


Figure 9: The MDE framework of Gamification [56]-redrawn

Mechanics refer to the rules, the interactions and the context in which the students participate and they remain constant. They are the outcome of the decisions of the game designers. Dynamics are the type of behaviours that emerge from the students (players) when they partake in the game. Strategies may emerge and they may include competition, cooperation, cheating and others. Emotions are the result of the Mechanics and the Dynamics that emerge and the designers should aim to create emotions of excitement, fun, curiosity but negative emotions are unavoidable.

Although as we mentioned 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. Puzzle games pose a problem and the learner has to solve enigmas or learn how to use tools to solve it. Adventure games add the element of the plot so they can give a near real-life experience of the work situation to the learners. Simulation games can also prepare the students for real work situations, but they can be costly to develop. Lastly 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. [57]

4.2 Examples of use and impact in the fields of cybersecurity and Power Systems - Proposals

4.2.1 Methodology

For the identification of the impact of the various educational methods (e.g., project-based learning) and the various practices (e.g., demonstration of simulation of a system) we collected information in two ways. First, a review was made in a pool of papers that were gathered from Google Scholar searching the terms: “Educational method”, “smart grid”, “cybersecurity” for each of the methods mentioned in this document. For each search only the most relevant papers were chosen. We also added into the pool papers that were part of the literature review of WP1 that were deemed relevant. The resulting papers were further categorized based on whether the authors described their experience from teaching a relative subject or not. Overall, 21 papers are written from authors that taught a relative course and 22 are more general papers that were written not using firsthand experience but other sources (e.g., literature review).

For the identification of the methods used we either collected the information directly from the authors stating the method they used or we inferred it where it seemed appropriate (e.g., use of the expression “learning by doing” instead of experiential learning). The more general methods like experiential learning and active learning were mentioned in 10 and 9 papers respectively and if we consider the fact that project-based learning is a form of experiential learning [58] then 16 out of 21 papers use experiential learning. Interestingly Inquiry-based learning, the method which resembles the scientific method the most, is not mentioned by name in any of the papers.

An important remark is that active learning techniques are not only challenging because of their increased demands in staff, time and resources in general but they also pose challenges relevant to the characteristics of the students [59]. For the use of active learning to be successful the students need to already have a minimum level of “strength” in the subject, which means that they can function with some autonomy, otherwise the presence of the teacher needs to be stronger with individual instructions for each student and the groups (if present) need to be small enough to be homogenous.

4.2.2 Use of gamification in Universities

A very promising active learning method is gamification which was used in almost one third of the papers and was mentioned in a lot of the review material. Gamification is reported as having potential in facilitating the understanding of “complex and unfamiliar concepts associated with cybersecurity” [60]. In [61] a board game named Riskio is presented which was designed for use primarily by employees and secondary by undergraduate students that major in cybersecurity. It is highly recommended for use in industry and especially for teaching to non-technical employees because the presented attack scenarios (e.g., a USB stick containing malware) concern all the types of employees. Another advantage is that the players adopt both the roles of an attacker and a defender. One point that needs improvement is that the students reported that it was difficult to understand the game, something not reported from the employees.

4.2.2.1 Capture the flag and Hacking Day events

In [62] Capture the Flag (CTF from now on) contests are presented. They are a form of experiential and collaborative learning in general and by definition they belong to the gamification method. In CTF contests the players aim to discover the vulnerabilities of the system (either in hardware or software) and discover a key that is hidden inside the system by the organizers (the flag). It can take the form of "Attack-Defense" (two or more teams opposing each other), "Jeopardy" (every contestant team tries to hack the organizers' system and win points for each level) and "Hack-Quest" (most probably a synonym of "Jeopardy"). One of the challenges of CTF contests is to ease the way in for a novice player when the team already has experienced players which could be discouraging. Another recommendation is to rotate the players between red (attack) and blue (defend) teams as they benefit the players in different ways.

In [63] the CTF contest is combined with three other characteristics making it a very holistic approach. Firstly, the students themselves form small groups and design the games during the semester with the facilitation of the teachers. Through this process they must understand very well the cybersecurity issues and they also must develop other soft skills through the collaboration with their peers in the team, the evaluation team and the teachers. Secondly, six of the students that successfully passed the introductory course can opt to be part of the follow-up course in which they do not attend the theoretical lectures, but they immediately start to work on their chosen project about securing a network. They also adopt the role of advisor for the students of the introductory course further enhancing the quality of their learning for both. The third element is the Open Day event at the end of the semester in which the designed games are presented and can be played by the other students of the university and get more feedback. The participation of other students in the event can increase their chance of choosing cybersecurity as their career choice as it is stated in [64]. The importance of organizing such events is stretched even more in [65] where it was reported from past students who were involved in the event that the skills they gained were very useful in their job afterwards. Those events have also the potential to function as career days with industry invited or the industry could also be part from the beginning by sponsoring the necessary equipment as in [65] or [66].

Similar to [63], in [67] the students are developing their own CTF games that are tested in a hacking event at the end of the semester from the other students. The ICS testbed that is used throughout the course is described in both the hardware and software perspectives. A more relevant to our field of interest setup is described in [68] where the infrastructure used is a SCADA system using real control systems in University of South Australia. The authors point out that since in industry the students will be asked to be the "Blue" (defend) team, then maybe they should only train on defense. Contrary to that, in [69] it is argued that teaching cybersecurity from the offensive perspective is always beneficial because it better builds the cybersecurity mindset and being more exciting it can lead to better engagement from the students.

4.2.3 Use of gamification in industry

The use of gamification to train employees on organizational security was studied in extent in [70]. The impact of the proposed method was measured by hiring a third-party firm that tried to phish the employees. The data shows that the proposed training using gamification had significant improvement in preventing a phishing attack and it also shows that the training by email that was used before in the company did not offer any improvement

relative to the control group that had no training at all. When designing the gamified environment, the goal is to achieve engagement, which requires to have good balance between "too challenging" and "not challenging enough" otherwise the learners become less interested.

4.2.4 Use of demonstration

An interesting example of cybersecurity course is presented in [71] where Shodan is used. Shodan is a search engine that searches for devices connected to the internet and can filter the results using several parameters (e.g., show only webcams). For the first three weeks, the students are given the theoretical background of IoT devices, architecture, and connection and of common cybersecurity attacks in lecture format and the next three weeks are taught using the flipped classroom methodology. The students are given material to study at home and during class they apply queries to Shodan search engine. With the guidance of the teacher, they witness actual devices like public webcams and home automation systems connected to the internet that are either not protected at all or they are protected only using the default credentials which are easy to break. In the following table (Table 2) a summary of these devices can be seen:

IoT Device	Mootool-Based Webcams	Insteon Smart Home Controller	Somfy Alarm System	IoT Proliphix Thermostats	Cannon VB-M600 Network Cameras	Twonky Media Server
#Shodan Results	141	19	17,294	192	51	3846
#Analyzed Devices	20	19	20	20	20	20
#Devices without Authentication	20	15	-	-	9	20
#Devices with Default Credentials	-	-	2	3	4	-
#Devices Affected by CVEs	4	-	-	-	1	-
#Detected CVEs	66	-	-	-	359	-

Table 2: Categories of devices analysed in the paper [71] reproduced under license

The guidance of the teacher is particularly important because of the legality issues that could arise if Shodan is not used with care and if someone wishes to adapt said course to their own country, they should first be sure what is permitted from their national/university/company legislation. A similar course, which could be simply a demonstration from the trainer of exposed or vulnerable devices could be used in industrial training to show to (especially non-technical) employees the importance of having good cybersecurity habits.

4.2.5 Use of Project-based learning

Apart from gamification, the second method that was more frequently used, is project-based learning [72], [73], [74], [75]. In [74] it is argued through survey results (Table 3) that when the students are taught a course using hands-on techniques, there is significant improvement in their retention rate a few weeks after the end of the course. The results are shown in the next table for the experimental (Exp.) and the control (Cnt.) group.

	Exp.	Cnt.
Pre-test (Min:0-Max:5)	1.84	1.63
Post-test (Min:0-Max:5)	4.32	3.39
Delayed-test (Min:0-Max:5)	18.17	10.75

Table 3: Average test scores for the two groups, before the test, after the test and a few weeks later [74]-redrawn

In [72] a full virtual company named TCIPGco is run from portable equipment and the students have access through the use of their laptop. The virtual company has both Windows and Linux systems, a SCADA system and is in the middle of upgrading some security protocols. In these settings the students are taught about various cybersecurity tools and acquire skills.

4.2.6 Virtual labs and remote access

One aspect to be considered that is not directly coupled with an educational methodology but rather with an educational tool is the use of virtual labs either with physical presence or with remote access. It was recognized as a trend as early as 2010 [76] and the COVID-19 pandemic, which is ongoing, creates an even stronger motivation for the set-up of remotely accessible labs than before.

In [77] three examples of virtual labs that are used for teaching cybersecurity are presented. Statistical results show that the peak times when students use the equipment is late evening when usually the labs are closed and that they use the remote lab to interact with each other. A drawback of using remote labs is the additional staff hours needed, not only because digital communication is slower but also because additional problems arise from the use of remote connectivity. The use of a Frequently Asked Questions can smooth greatly the student experience. Informal assessments show that the use of virtual lab helps the students to connect the theory with practice and also that the employers that hired new graduates reported being more satisfied with the learning outcomes.

4.2.7 Using testbeds to teach about cybersecurity

Testbeds vary greatly in the detail with which they simulate the 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.

An example of this setting is given in [78] using a Real-Time Digital Simulator, synchrophasor devices, DeterLab and a wide area monitoring application with closed loop control. DeterLab is used for the simulation of the communication network which is a shared testbed used for the study of cyber defense and is funded by the Department of Homeland Security, the National Science Foundation, and the Department of Defense. Two cyber-attacks

are used as test cases which are Man In The Middle attack and TCP SYN (Transmission Control Protocol with SYNchronization) flood attack.

Another example is [79] where an OPAL-RT real-time simulator is used in combination with communications simulation software with cyber-attack functions developed by Scalable Networks. This testbed provides a closed-loop testing environment where the after-fault analysis of cascaded events can be studied or strategies to predict such events can be developed. As a test case, a packet delay and modification attack are studied in an islanded grid, where the wrong information causes not only wrong trip commands but also frequency and voltage fluctuations.

In [73] a testbed with emphasis in distribution management (DMS) and the integration of smart meters and PVs is created. The testbed is then used in teaching three courses with one of them being about cybersecurity. Students are taught the DNP3 protocol and establish SCADA connection. The learning outcomes of this course include the analysis of various logs to detect an attack and how they can predict similar future attacks. A survey was conducted among the students to analyze which areas need improvement.

The above examples clearly show the advantages of developing a real time testbed that incorporated both the power system and the communications network. This way their complex interaction can be studied in circumstances that are possible real-life scenarios. The most important parameter is of course the continuation of operation under attack.

5. Recommendations

The last part of this report is about high-level recommendations to all stakeholders that will help ease the way into creating professionals adequately equipped to handle cybersecurity issues relevant to power systems. These recommendations are the result of reviewing several European documents produced in the context of projects or by task forces and agencies that have objectives partly covering at least one of the topics that we analyse together namely: cybersecurity, power systems, education and behaviour of the employees.

Some examples are the "Roadmap for European Universities in Energy" [80] by UNISET (Universities in the SET plan), the "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity" [81] by the European Union Agency for Cybersecurity (ENISA), the "Cybersecurity and Resilience" [82] report of the Data Management Working Group in the BRIDGE process [83] which also produced a report named "Main findings and recommendations" [84]. Bellow the recommendations are presented and grouped based on the relevant stakeholder.

5.1 Recommendations for cybersecurity education

5.1.1 Universities

The recommendations towards universities are outlined in the following table (Table 4) and selected subjects are further explained below:

Recommendation	Effect	Existing example
Create an observatory and continuously monitor the new and ongoing research results [43].	• Help the universities focus their efforts on innovative directions • A place for professionals to be informed on the current trends	
Create a database with experts and researchers along with their areas of work and skills developed in the two fields [43].	• Enable the students to select Erasmus+ or Master's programs based on the skills they want to develop • Universities can build collaborations and create Joint Masters programs by offering different but complementary knowledge and skills	Erasmus Mundus (no results relevant to our field were found as of May 2021) [44]
Create Joint Master's degrees **[85]**		"European Master in Renewable Energy" [45].
Harmonize the European accreditation systems through the use of the European Credit Transfer System in accordance with the Bologna Process **[85]**	• Enable the mobilization of the students and young graduates • Help the companies create a more accurate description of the skills and knowledge required for a position and employ workforce from different countries	
Create an inventory where the Universities and research centres can connect their infrastructures **[85]**	• Help smaller institutes be part of the innovation and train their trainers	ERIGRID and ERIGRID 2.0 project [43]
Create a course module repository where the Universities share the design of their courses, the learning outcomes, best practices and educational content	• Speed up the modernization of the European curricula on the field of cybersecurity in smart grids	

Cover less-technical aspects like the legal frameworks (GDOR, NIS directive) **[86]**		

Table 4 Recommendations towards universities

The usefulness of Joint Master's degrees results from the fact that our field of interest is a combination of two other fields namely ICT and smart grids. Therefore, a unified curriculum could be created from two universities with different expertise and possibly from different countries giving the students the opportunity to work, study and make contact with different cultures and companies. A similar example is the "European Master in Renewable Energy" [87]. For a Joint curriculum to exist, the harmonization between European accreditation systems through the use of the European Credit Transfer System is very important and it should continue in accordance with the Bologna Process. This harmonization will not only enable the mobilization of the students and young graduates but it will also help the companies to create a more accurate description of the skills and knowledge required for a position and employ workforce from different countries.

Apart from Erasmus Mundus, EIT InnoEnergy [88] (funded by the European Union) offers to students in cooperation with European Universities, Masters' programs like the "Master's in Smart Electrical Networks and Systems" which covers relevant modules like the "Data science and ICT as enablers for smart grids" at KTH Royal Institute of Technology, Sweden, and also it operates a career centre to bring the young professionals closer to employment. For industry partners it offers programmes for professional training. We recommend adding a programme relevant to ICT and cybersecurity as the current programmes do not cover this field.

Another possible obstacle especially for smaller Universities is the cost of relevant infrastructure which can be overcome by creating an inventory where the Universities and research centres can connect their infrastructures similar to the work done in the ERIGRID and ERIGRID 2.0 project [85] . An example of how the ICCS-NTUA infrastructure is presented in the ERIGRID 2.0 site can be seen in the next figure (Figure 10). This can help not only the education process for the students but also the research and training of the teachers.

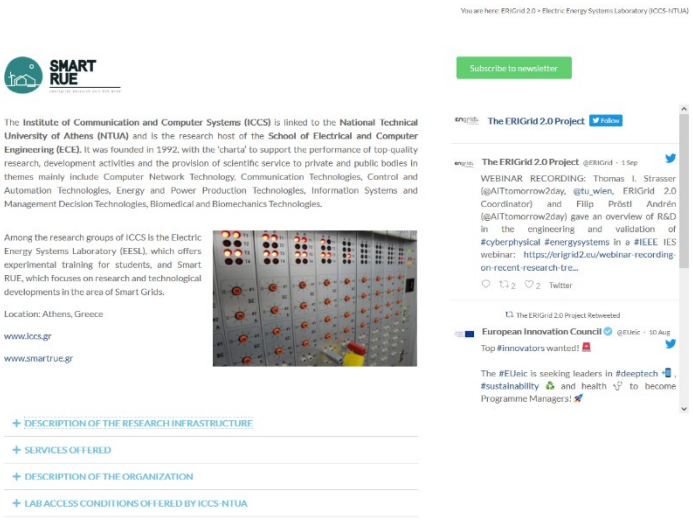


Figure 10: An example of how the ICCS-NTUA infrastructure is presented in the ERIGRID 2.0 site

There are currently two opposing trends affecting the professionals of the future. The evolution of technology creates a need for professionals with high specialization on their field, but because the development of a product (e.g., a smart meter) requires multiple specializations, the professionals should also possess a wide range of general knowledge in order for them to cooperate efficiently. This concept is called a T-shaped engineer [89], [86] where the horizontal bar represents the general knowledge and the vertical bar represents the specialization field.

In [86] the importance of multi/inter – disciplinary approach is mentioned where people from different disciplines work together synthesizing and integrating their knowledge [90]. Because of the fact that the real-life situations often need to be viewed from many perspectives to find the best solution there should be an institutional commitment about the use of interdisciplanary work especially when creating master's and PhD programs. It should also be noted that one of the perspectives to be taken into account is the societal and ethical one which can be overlooked in STEM (Science Technology Engineering and Mathematics) programmes. A graphical representation of the above can be seen in the next figure (Figure 11).

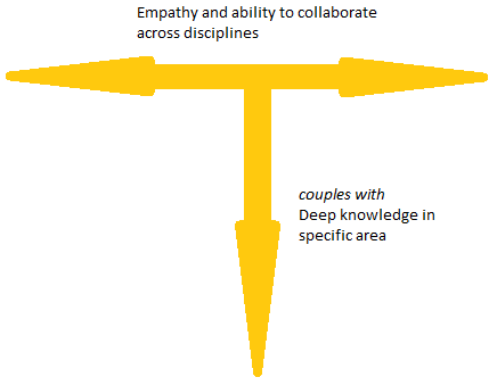


Figure 11: A visualization of the concept of T-shaped engineer [112]-redrawn

5.1.1.1 Recommendations that resulted from the CC-RSG Workshop for Universities

In the CC-RSG Workshop that was conducted in the context of WP1 in May 2021 it was also stressed in the discussion-brainstorming about the skills that the academia provides, that there is a need for more coverage in non-technical areas like organizational security, societal security and human security (ACM categorization). Other recommendations that resulted from the workshop are presented below in Table 5. The four groups are formed as follows:

Keep continuing: Actions that are already implemented and should continue with the same weight
More of: Actions that are already implemented and their use should be expanded
Start doing: Actions that are not already implemented
Less of: Actions that are already implemented and their use should be reduced

Keep continuing	More of
Cybersecurity of critical infrastructure	Organizational security
System security	Societal security
HIL (Hardware in the loop) testbed in Lab	Human security
Knowledge about connection security	General security

Required tools developing and testing	Certificates like CISM/CISSP/CISA/CEH
Industrial security	Specific cases
Basic knowledge of cyber security	Knowledge on network security
Practical experience	Practical experience
Industrial security	International hires
Start doing	Less of
Design, implement, monitor and proactively develop cybersecurity measures;	Theory
Using and conducting international research in cybersecurity	
There is no "bridging" between power system and communication infrastructure knowledge	
Knowledge of device/component in the the power system (RTU-Remote Terminal Unit, IED- Intelligent electronic device, PMU-Phasor Measurement Unit)	
Lack of money for research	

Table 5 Recommendations for universities that resulted from the CC-RSG workshop

5.1.2 VETs

Vocational Education and Training institutes in Europe can be divided in two categories. According to [91] Initial VET or I-VET takes place before students begin their working life in secondary or post-secondary level and Continuing VET or C-VET takes place after the higher education and continues throughout the working life of the individual.

Our relevant recommendation for VET institutes is a creation of a project like UP-RES [92], [93] which also had the goal to bring together two distinct disciplines, namely urban planners and renewable energy. During the project 1.200 planners received training and ten training modules were created while 30 best practice cases were investigated for future use. In addition, five partner countries cooperated, further fostering the so important collaboration that we mentioned earlier.

More generally, C-VET providers should formulate courses and online training modules that focus on a specific subject such as, how to implement a modern communication protocol in a way that is secure for a specific family of legacy equipment, or how to build Intrusion Detections algorithms based on historical data and how dangerous a command can be. These kinds of courses can formulate a Micro Master's programme which is the equivalent of a semester of a master's degree [86].

In the field of cybersecurity, the possession of a certificate relevant to the job position can increase the chance to be successful when applying for a job even though certificates as viewed by the employers are not enough on their own [94]. We recommend though to the educational providers to create subjects that can act as preparation for the students to pursue relevant certificates. The choice of the certifications can be quite difficult. There should be consideration to prepare the students for certificates that have a good potential to be relevant in the next years and avoid certificates on subjects that are new and could be short lived. On

the other hand, there is the risk that very well-established certificates can be about tools and methods that are not so relevant today.

5.1.3 Industry

The cybersecurity competence of the employees of a company could be analysed in two broad categories:

- 1) Firstly, the skills and knowledge that are technical and relevant to the product or service of the company, for example the attack points of a legacy device or the compliance of the product with the GDPR.
- 2) Secondly, the importance of the human factor in cybersecurity breaches which in turn can be broken down into two subcategories:
    - a) The employee must be aware of how their habits affect the security of the company, for example when creating a very weak password.
    - b) When designing a product, the employee-designer must take into account the habits of the end-user and create a product that enables or even helps the end-user to follow good security practices, for example by making necessary the change of the default password.

The results from the review that was made will be presented below for the cases 1 and 2a.

1. Technical aspects to be included in industry training:

The relevant recommendations from the reviewed literature about the content of the teaching are presented in the following table (Table 6):

Recommended topics	Effect
Choose a message-based model when choosing between this and shared database model **[84]**	• Better security mechanisms and better scalability potential
Smart Applications REFerence ontology (SAREF) model which aims to analyse all the home IoT devices and create a code of their building blocks and the relationships between them **[95]**	• Mitigate the obstacle of the growing heterogeneity of devices which is pointed out in [55] • Enable the interoperability of devices of different vendors
Continuous updatability and upgradability of the components because of the rapid pace in which new kinds of attacks and points of entry are discovered **[96]**	
Security by design and by default **[96]**	• Its predecessor, security by obscurity cannot longer be implemented because it was based in physical isolation and use of proprietary software and hardware

Table 6 Recommended topics regarding the technical aspects of cybersecurity to be included in industry training

The use of **legacy equipment** which was built without the ***Security-by-design*** strategy and are still in use today are especially mentioned in [82]and [97] as one of three main points which differentiate the cybersecurity field of the energy sector from cybersecurity in general. The second is the **cascading effects** which could affect the availability of the system in large areas and the third is the **real-time requirements**. Real-time requirements refer to the fact that the response time in parts of the power network is smaller than the minimum time that

a security protocol needs in order to decide if an action is safe. Thus, the training of the employees should include as good practices the following examples of [82]:

Legacy equipment:

- Systematic patch management when available
- Physical security can be beneficial for legacy equipment protection
- Regular risk analysis targeting legacy devices and their interfaces with more modern devices

Cascading effects:

- Classification of the assets considering their interdependencies and criticality
- Identification of critical nodes to avoid single point of failure
- Cooperation between the different actors of the grid to prevent a cascading event from happening

Real-time requirements:

- Segregation of networks: By dividing the equipment in logical zones the flexibility to use different cybersecurity approaches can be beneficial
- Classification of the assets considering the different real-time requirements
- Physical security should be considered when the other options (like upgrading) are not available.

2a. Employee's behaviour effects on company cybersecurity to be included in industry training

Companies should organise training sessions for their employees where their current competence on the sector 2a is measured. The goal is to find out what kind of decisions the employees make, relevant to security. What kind of passwords do they use? Do they change the default credentials? Do they update their systems regularly? Do they know how to recognise a phishing attack? Do they keep regular back up files? After the initial measurement of competences, they should be taught about the best practices as we mention in the previous chapter.

The different staff categories from the ones the ESCO (European Skills, Competences, Qualifications and Occupations) provides, [98] that are relevant to the energy sector are "Managers", "Professionals", "Technicians and associate professionals" and "Plant and machine operators". They were also used for a similar analysis in [99] . From those categories only the managers should undergo some additional training on how their behaviour impacts the employees they manage. In [81] several relevant remarks are made. For example, it has to be clear for all employees that they should not prioritise their productivity over security. Managers should be aware of the fact that the security testing and the compliance to the standards requires some dedicated time which has to be given to the security analysts. It is also mentioned that because attention is a limited resource, the security measures of a company should be designed to not disrupt the main tasks of the employee. Lastly, an important remark is that it is more effective to enable the good security behaviour than to stretch the possible dangers.

It is also useful for the employees to familiarize with the tool "Good practices for IoT and Smart Infrastructures Tool" [100] which ENISA provides and it can be very useful especially to smaller companies. There are five main categories, namely, Smart Cars, Smart Cities, Industry 4.0, Smart Hospitals and Smart Airports from which the first three are relevant to our domain. For each category there are several Proposals and Good practices listed along with relevant threats and references. One can filter out only the proposals that they seek guidance for.

A particularly important part of the employee training should be about the current legislative documents. A good overview can be found in [101] which can help navigate the field up until mid-2017. Also, more general pieces of legislation can be relevant like the GDPR about the use of personal data and the NIS directive which was the first European document about cybersecurity and was superseded by NIS 2.0 in late 2020.

Lastly, a recommendation not relevant to the training content is about the part that different players play in the training of the employees as mentioned in [17]. All relevant players (educational institutes, graduates and industry) should keep in mind that higher education institutes only equip graduates with broad knowledge and some of the real-life skills and that they should be given the opportunity and time in their working life to further develop their skills and knowledge in more specialized areas. The adoption of certification for the cybersecurity degrees could clarify the point at which the employees and employers take over the lifelong learning from the institutes.

5.1.3.1 Recommendations that resulted from the CC-RSG Workshop for the industry

In correspondence with the recommendations for educational providers in the next table (Table 7) you can find the Workshop results in the discussion about what the industry wants/needs:

Keep continuing	More of
Zero trust	Basic toolset for threat analysis
Workable soft skills	Able to understand multiple tools
Network fundamentals TCP/IP OSI model	Training on new and arising technologies
Software defines networking	Know the difference between OT and IT
Self teaching	Nature of energy system
Ability to acquire needed skills	Basic cyber hygiene
Multi-domain understanding between computer and power system	Mindset for security
Internship and mentoring	Serverless concepts
	Knowledge of the vulnerabilities of a power system
	Knowledge of most popular SCADA platforms
	More practical use cases
	Hands on and know how skills
	More and deeper cooperation between academia and industry
	Understanding of basic operational requirements of electrical power systems
	The requirements for critical infrastructure system
	Need for soft skills for designing

	Specialized knowledge and hard skills for implementation

Table 7 Recommendations for industry that resulted from the CC-RSG workshop

5.1.4 Policy makers

Finally, and from a higher perspective, laws and policies are of great importance to the governance and protection scheme of power systems, since they define and declare actions to be taken in the event of accidents, as well as maintaining accountability and liability on actions being taken. Accordingly, policy makers and regulators must enact policies and rules that address cyber risks that may affect or disrupt the functionality of these systems adequately. Moreover, means of enforcement [102] should be employed and monitored constantly to ensure that policies and rules are being followed and adopted without any sort of violation. Here, recommended practices for policy makers can be categorized into four groups; namely, recommendations for member states, recommendations for industries, recommendations for national cooperation, and general recommendations.

Regarding the member states: first, the European NIS Directive 2 should be considered as a reference model for network and information systems security, and thus states should be examined against the way they implement and follow its recommendations regarding the structure of the Computer Security Incident Response Team (CSIRT) and the existence of NIS authority [95]. Such deployment would help ensure harmony and homogeneity between the different states, demonstrate a readiness to provide and adjust policies according to needs, and help unify and standardize protocols and means of communication. Second, it is advised to create a common repository/platform, where operators and other parties in the industry can share detailed information on incidents and early warnings about attacks and violations [103], to help spread knowledge about existing threats and avoid potential attacks as quickly as possible.

Regarding the industry: industries come in different sectors, sizes, and processes; accordingly, requirements may differ from an industry to another, and policies therefore should be adjusted to reflect on their specific needs. First, industries should list their assets, operations, and critical infrastructure components [103], in addition to identifying the operators of essential services according to the NIS Directive recommendations. This will help create and implement a backup plan and maintain the level of resilience required for such systems. Second, a minimum-security scheme should be defined and strictly met [103]. Third, platforms being utilized should be listed, and the criteria for platforms interoperability should be defined [104]. This latter is a part of the recommended enterprise architecture practices [105] and can save resources being wasted on duplicates and unnecessary operations that are done across different platforms. Fourth, it is essential to maintain up to date skills, thus the need for a repository where the industry can continuously monitor and upgrade the skills needed [85]. Fifth, the issue of communication and dissemination of information between different levels and parties, was noticeable, and thus means of clarifying communication should be considered, by adopting a unified protocol for communication to avoid these risks [84]. Finally, it was stated in the workshop that the ISO/IEC 27001 family of standards which is used by some companies today gives limited support to the managers. As it was written to be a general protocol, perhaps it needs to be superseded by a new protocol especially made for the power systems domain.

On a higher level, regarding national cooperation: states are encouraged to develop and use regulations and policies that can be widely adopted [106], e.g. GDPR. This will mitigate

any sorts of conflict between the member states, ensure seamless protection, and help in developing better solutions. Models already exist, thanks to the GDPR; however, due to the long term adopted proprietary solutions, special attention must be paid to compliance [104] and developing conceptual data exchange models that can operate across all states. Moreover, existing available communication means [84], e.g. MQTT and REST API, are highly recommended since these are widely adopted and can save time and resources given to develop own solutions, which are not recommended.

Finally, some general recommendations to policy makers are: first, elaborate and give enough details about new data roles [104], to avoid misunderstandings and future conflicts. It is better in this case to harmonize the approach of role definitions by using the ones included in models as Harmonized Electricity Market Role Model (HEMRM) for example. Second, applying Common Information Model (CIM) standards in Transmission System Operator (TSO) and Distribution System Operator (DSO), and developing the standard accordingly [104] if needed. Third, to consider including a risk/cost estimation for the adoption of future recommendations [82]. Fourth and lastly, adopt a clear communication scheme in order to increase awareness of users and all stakeholders being considered [105].

5.2 Recommendations on how to foster collaboration among stakeholders

As it has been stated before, cybersecurity education in power systems needs the coordinated action of many stakeholders and it is a field that changes in high pace. We recommend for the creation of a high-level dialogue forum that will convene annually or bi-annually with the participation of the relevant policy makers, DSOs, TSOs, Universities, VETs to exchange information of on-going and planned activities in the domain.

Another chance for keeping the communication ongoing is the organization of large events in educational institutions with the support of the industry that could provide the equipment. In parallel those events can act as career days and increase the chance that students choose cybersecurity as their career path.

6. Conclusions

In the above report we aimed to understand in what areas the education in cybersecurity in smart grids is lacking and propose effective educational methods and other high-level recommendations to help improve the education in this field. The analysis was made through extensive literature review, interviews with representatives from the industry and a dedicated workshop that was conducted in the context of CC-RSG in May 2021.

The challenges faced by the industry are mainly relevant to young graduates not having enough training in practical situations similar with the ones that will come up during employment nor in management and communication issues.

Regarding the educational methods, gamification appears to be the most promising one for the field of cybersecurity. It can be used both for the training of non-technical employees that work in the power systems industry to acquire cybersecurity literacy, and it can also be used for the training of technical staff especially helping them acquire practical experience.

Project-based learning has been found to improve the retention-rate after a few weeks but as all the active-learning methods it is subjected to some limitations with the most important ones being that it can be applied to students that already have a level of autonomy in the subject concerned and the teams of the students must be homogenous.

The subject at hand is very closely connected to hardware, so it is very important to develop ways for as many stakeholders as possible to gain access to the relevant equipment. This can be done in many ways like expanding the use of remote accessibility for testbeds in research centers or educational institutes, organizing a way for sharing the infrastructure (ERIGRID 2.0 EU project as an example) or inviting the industry to be part in relevant university courses. The equipment can mean both general hardware equipment like computers and also specialized equipment like PMUs, RTUs, Real Time Simulators etc.

The recommendations to the stakeholders are to a large extent relevant to ways of communication and mapping of the available resources (professionals, best practices, infrastructure). The mapping is the basis to develop effective ways to pool the available resources like creating Joint degrees, an early warning system for cybersecurity incidents and others.

Apart from the previous recommendations, we have included a brief analysis of knowledge that industries should seek to teach to their technical stuff and how the cybersecurity of power systems is different than the cybersecurity field in general.

For policy makers the most important task is to create the paths for communication like a common language for managers and technicians, the European Cybersecurity Skills Framework that is anticipated by ENISA (although it is not specific to power systems) and the directives and regulations to minimize the use of proprietary solutions.

The analysis above demonstrates the advantages of developing real time testbeds that model both the power system and the communications network. This model can then be used in order to analyze possible attacks (perhaps in combination with human error) under the unique conditions and requirements that smart grids (and power systems in general) operate.

7. Bibliography

[1] European Union, “DIRECTIVE 2009/28/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 23 April 2009,” in *Official Journal of the European Union*, 2009.

[2] EDDIE "Education for Digitalisation of Energy", “eliverable 2.1 Current challenges in the energy sector and state of the art in education/training,” 2020.

[3] A. H. Booz, “2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk,” 2017. [Online]. Available: https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx. [Accessed October 2021].

[4] S. A. Rick Randall, “Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry,” *International Journal of Critical Infrastructure Protection,* p. 100454, June 2021.

[5] B. Jerman Blažič, “The cybersecurity labour shortage in Europe: Moving to a new concept for education and training,” *Technology in Society,* p. 101769, November 2021.

[6] C. A. R. J. L. Juan Enrique Rubio, “Current cyber-defense trends in industrial control systems,” *Computers & Security,* p. 101561, November 2019.

[7] ICS-CERT, “Overview of Cyber Vulnerabilities,” [Online]. Available: https://us-cert.cisa.gov/ics/content/overview-cyber-vulnerabilities. [Accessed October 2021].

[8] IBM, “A survey of the cyber,” 2016. [Online]. Available: https://www.ciosummits.com/2016_Cyber_Security_Intelligence_Index_for_Fnl_Svcs.pdf. [Accessed May 2018].

[9] Sikich, “Manufacturing report, Taking your business to the next level and ensuring a successful future,” 2016.

[10] M. L. M. L. Angelo Corallo, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts,” *Computers in Industry,* p. 103165, January 2020.

[11] M. W. D. R. Paul Formosa, “A principlist framework for cybersecurity ethics,” *Computers & Security,* p. 102382, October 2021.

[12] F. F. M. P. a. M. S. G. Culot, “Addressing Industry 4.0 Cybersecurity Challenges,” *IEEE Engineering Management Review,* pp. 79-86, September 2019.

[13] M. J. E. Johannes M. Bauer, “Cybersecurity: Stakeholder incentives, externalities, and policy options,” *Telecommunications Policy,* pp. 706-719, November–December 2009.

[14] D. J. M. C. Obi Ogbanufe, “Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures,” *Information & Management,* p. 103507, November 2021.

[15] P. Č. J. V. S. B. Valdemar Švábenský, “Cybersecurity knowledge and skills taught in capture the flag challenges,” *Computers & Security,* p. 102154, Month 2021.

[16] J. M. F. Lorena González-Manzano, “Design recommendations for online cybersecurity courses,” *Computers & Security,* pp. 238-256, January 2019.

[17] ENISA, “CYBERSECURITY SKILLS DEVELOPMENT IN THE EU,” 2020.

[18] “Role profiles,” [Online]. Available: https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework/. [Accessed October 2021].

[19] “e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 2: User Guide,” [Online]. Available: https://standards.iteh.ai/catalog/standards/cen/843eb75f-d024-4a43-b274-073423eb0d8c/cen-tr-16234-2-2021. [Accessed October 2021].

[20] NIST GOV, “NICE Framework Resource Center,” [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center. [Accessed October 2021].

[21] L. V. A. B. M. H. Adéleda Veiga, “Defining organisational information security culture—Perspectives from academia and industry,” *Computers & Security,* p. 101713, May 2020.

[22] C. H. Z. Z. Siqi Hu, “Security Education, Training, and Awareness Programs: Literature Review,” *Journal of Computer Information Systems,* 2021.

[23] M. Alshaikh, “Developing cybersecurity culture to influence employee behavior: A practice perspective,” *Computers & Security,* p. 102003, November 2020.

[24] D. C. P. D. A Reevesa, ““Get a red-hot poker and open up my eyes, it's so boring”1: Employee perceptions of cybersecurity training,” *Computers & Security,* p. 102281, July 2021.

[25] C. A. A. F. F.-G. J. L. E. M. L. I. M. A. Simone Fischer-Hübner, “Stakeholder perspectives and requirements on cybersecurity in Europe,” *Journal of Information Security and Applications,* p. 102916, September 2021.

[26] S. A. J. K. M. B. M. V. R. P.-D. J. G. N. K. M. M. T. V. S. L. Bjorn Siemers, “Modern Trends and Skill Gaps of Cyber Security in Smart Grid : Invited Paper,”

IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, 2021.

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1. [Accessed October 2021].

[28] P. C. S. f. Europe, "Research and Development Roadmap 1," [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf. [Accessed October 2021].

[29] C. S. f. Europe, "Common Framework Handbook 1," [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf. [Accessed October 2021].

[30] C. S. f. Europe, "Education and Training Review," [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf. [Accessed October 2021].

[31] J. I. R. K. R. H. S. M. R. A. A. J. T. P. E. S. Allen Parrish, "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline," in *ITiCSE 2018 Companion: Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 2018.

[32] Joint Task Force on Cybersecurity Education, "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," ACM, 2017.

[33] N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs," *IEEE Security and Privacy,* vol. 19, no. 1, pp. 81-88, 2021.

[34] University of Oldenburg, "Report on State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids," 2021.

[35] L. &. G. K. Fenton, "Integrated Experiential Education: Definitions and a Conceptual Model.," *Canadian Journal for the Scholarship of Teaching and Learning,* vol. 7, no. 2, p. 7, 2016.

[36] L. Tudor, "Perception of Teachers on Curriculum Integration. Integration Patterns Practice," *Procedia - Social and Behavioral Sciences,* vol. 127, pp. 728-732, 2014.

[37] R. R. &. S. S. Hipkins, "Curriculum changes, priorities and issues: Findings from the NZCER secondary 2006 and primary 2007 national surveys.," NZCER, 2008.

[38] B. (. B. Rachel Lowe, “Pre-Service Teachers’ Experiences With Curriculum Integration: A Qualitative Study,” 2017.

[39] J. M. T. Nyamkhuu, “Challenges in integrating 21st century skills into education systems,” 2019. [Online]. Available: https://www.brookings.edu/blog/education-plus-development/2019/02/05/challenges-in-integrating-21st-century-skills-into-education-system/.

[40] Z. B. M. Z. Bilal Khalid Khalaf, “Traditional and Inquiry-BasedLearning Pedagogy: A Systematic Critical Review,” *International Journal of Instruction,* vol. 11, no. 4, pp. 545-564, 2018.

[41] D. A. Kolb, Experiential Learning: Experience As The Source Of Learning And Development, Prentice-Hall, 1984.

[42] C. J. W. Linda H. Lewis, “Experiential Learning: Past and Present,” *New Directions for Adult and Continuing Education,* pp. 5-16, 1994.

[43] European Commission, “Education and training: Supporting education and training in Europe and beyond,” 10 02 2020. [Online]. Available: https://ec.europa.eu/assets/eac/education/ects/users-guide/recognising-prior-learning_en.htm. [Accessed 14 05 2021].

[44] D. S. K. Mr. Z. Zayapragassarazan, “Active Learning Methods,” *NTTC BULLETIN,* vol. 19, no. 1, pp. 3-5, 2012.

[45] L. O. Hamer, “The Additive Effects of Semistructured Classroom Activities on Student Learning: An Application of Classroom-Based Experiential Learning Techniques,” *Journal of Marketing Education ,* vol. 22, no. 1, pp. 25-34, 2000.

[46] J. Á. Ariza, “Design of open source platform for automatic control systems education based on cooperative learning,” in *IEEE Frontiers in Education Conference (FIE)*, Erie, PA, USA , 2016.

[47] R. T. J. a. K. A. S. David W. Johnson, “Cooperative Learning: Improving University Instruction By BasingPractice On Validated Theory,” *Journal on Excellence in UniversityTeaching,* vol. 25, no. 3&4, pp. 85-118, 2013.

[48] A. Taylor, “Flipping Great or Flipping Useless? A review of the flipped classroom experiment at Coventry University London Campus,” *Journal of Pedagogic Development,* vol. 5, no. 3, pp. 57-65, 2015.

[49] M. M. L. A. T. d. J. S. A. v. R. E. T. C. C. Z. C. Z. E. T. Margus Pedaste, “Phases of inquiry-based learning: Definitions and the inquiry cycle,” *Educational Research Review,* vol. 14, pp. 47-61, 2015.

[50] K. Elaine H.J.Yew, “Problem-Based Learning: An Overview of its Process and Impact on Learning,” *Health Professions Education,* vol. 2, no. 2, pp. 75-79, 2016.

[51] C. E. Hmelo-Silver, “Problem-Based Learning: What and How DoStudents Learn?,” *Educational Psychology Review,,* vol. 16, no. 3, pp. 235-266, 2004.

[52] O. H. Maija Aksela, “PROJECT-BASED LEARNING (PBL)IN PRACTISE: ACTIVE TEACHERS’ VIEWS OF ITS’ ADVANTAGES AND CHALLENGES,” in *5th International STEM in Education Conference Proceedings: Integrated Education for the Real World*, Brisbane, Australia, 2019.

[53] E. A. T. P. A. S. Anna Lyza Felipe, “Vietnamese Students Awareness towards a Project Based Learning Environment,” in *Anna Lyza Felipe1, Edouard Amouroux1, Thanh Pham1, Alex Stojcevski1*, Guimaraes, Portugal, 2016.

[54] A. Kolmos, “Reflections on Project Work and Problem-based Learning,” *European Journal of Engineering Education ,* vol. 21, no. 2, pp. 141-148, 1996.

[55] K. O. M. S. D. D. L. N. Sebastian Deterding, “Gamification: Using game design elements in non-gaming contexts,” in *Proceedings of the International Conference on Human Factors in Computing Systems, CHI 2011, Extended Abstracts Volume*, Vancouver, BC, Canada, 2011.

[56] K. P. J. H. K. I. M. L. P. Karen Robson, “Is it all a game? Understanding the principles of gamification,” *Business Horizons,* vol. 58, no. 4, pp. 411-420, 2015.

[57] A. F. P. D. K. a. J. P. D. Angelos P Markopoulos, “Gamification inengineering educationand professional training,” *International Journal of MechanicalEngineering Education,* vol. 43, no. 2, pp. 118-131, 2015.

[58] V. McLain, “Cybersecurity in Action,” in *Innovations in Cybersecurity Education*, Springer, 2020, p. 325.

[59] Z. R. E. P. Valery Vodovozov, “Challenges of Active Learning in a View of Integrated,” *Educ. Sci.,* vol. 11, no. 43, 2021.

[60] R. M. B. R. Joshua C. Nwokeji, “THE USE OF GAMIFICATION TO TEACH CYBERSECURITY,” in *Proceedings of the 2020 AIS SIGED International Conference on Information Systems Education and Research*, Online, 2020.

[61] A. M. F. P. V. S. Stephen Hart, “Riskio: A Serious Game for Cyber Security Awareness and Education,” *Computers & Security,* vol. 95, 2020.

[62] A. Rege, “Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation,” in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2015.

[63] J. V. M. C. M. L. Valdemar Švábenský, “Enhancing Cybersecurity Skills by Creating Serious Games,” in *Conference on Innovation and Technology in Computer Science Education*, Larnaca, Cyprus, 2018.

[64] K. W. A. M. Aunshul Rege, “An experiential learning cybersecurity project for multiple STEM undergraduates,” in *IEEE Integrated STEM Education Conference (ISEC)*, Princeton, New Jersey, 2019.

[65] M. L. Julia Armstrong, “An Informal Learning Program as a Replicable Model for Student-Led, Industry-Supported Experiential Learning,” in *2020 ASEE Virtual Annual Conference Content Access*, Virtual, 2020.

[66] A. N. Özdemir Göl, “Collaborative Learning in Engineering Education,” *Global J. of Engng. Educ.,* vol. 11, no. 2, pp. 173-180, 2007.

[67] J. V. V. S. K. S. Pavel Celeda, “KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems,” in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*, Portland, OR, USA, 2020.

[68] E. F. R. B. V. Elena Sitnikova, “The Power of Hands-On Exercises in SCADA Cyber Security Education,” in *IFIP World Conference on Information Security Education*, Auckland, New Zealand, 2013.

[69] M. Kranch, “Why You Should Start with the Offense: How to Best Teach Cybersecurity’s Core Concepts,” in *Colloquium for Information Systems Security Education (CISSE)*, Las Vegas, USA, 2019.

[70] P. B. L. Mario Silic, “Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance,” *Journal of Management Information Systems,* vol. 37, no. 1, pp. 129-161, 2020.

[71] P. F.-L. Tiago M. Fernández-Caramés, “Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases,” *Sensors,* vol. 20, no. 11, p. 3048, 2020.

[72] S. U. K. N. P. S. Tim Yardley, “Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application,” in *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*, Madrid, Spain, 2014.

[73] J. C. B. ,. C.-C. L. A. H. K. J. K. a. R. S. Jing Xie, “New Educational Modules Using a Cyber-Distribution System Testbed,” *IEEE TRANSACTIONS ON POWER SYSTEMS,* pp. 5759-5769, 9 2018.

[74] K. O. K. K. Yoshitatsu Ban, “Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education,” in *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, Hamamatsu, Japan , 2017.

[75] A. Eltom, W. Elballa, N. Sisworahardjo, R. Hay and G. Kobet, “Smart Distribution Course for 21st Century Power Sector Workforce,” *IEEE Transactions on Power Systems,* vol. 33, no. 5, pp. 5639-5647, 2018.

[76] P. T. Kirsi Aaltola, “Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training,” *Information & Security,* vol. 43, no. 2, pp. 123-133, 2019.

[77] B. H. R. D. A. S. a. S. B. Kara Nancea, “Virtual Laboratory Environments: Methodologies for Educating Cybersecurity Researchers,” *Methodological Innovations Online,* vol. 4, no. 3, pp. 3-14, 2009.

[78] A. S. R. Liu, “Integrated Simulation to Analyze the Impact ofCyber-Attacks on the Power Grid,” in *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Seattle, WA, USA, 2015.

[79] S. L. L. W. M. K. S. Q. A. J.-N. P. S. L. Lixi Zhang, “Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools,” in *PAC World Americas Conference*, Raleigh, North Carolina, USA, 2019.

[80] UNISET, EUA-EPUE, innoEnergy, “Roadmap for European Universities in Energy,” 2016.

[81] ENISA, “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity,” 2018.

[82] BRIDGE project: Data management working group, “Cybersecurity and Resilience,” 2019.

[83] [Online]. Available: https://www.h2020-bridge.eu/.

[84] BRIDGE project: Data management working group, “Main findings and recommendations,” 2019.

[85] A.Georgakaki, U.von Estorff, “Strategic Energy Technology Plan: Study on Energy Education and Training in Europe,” JRC, 2014.

[86] UNISET, EUA-EPUE, InnoEnergy, “Energy Transition and the Future of Energy,” 2017.

[87] KEYSTONE MASTER STUDIES, “European Master in Renewable Energy,” 2021. [Online]. Available: https://www.masterstudies.com/European-Master-in-Renewable-Energy/Belgium/EUREC/.

[88] EIT Inno Energy, “Accelerating sustainable energy innovations,” [Online]. Available: https://www.innoenergy.com/. [Accessed 05 2021].

[89] Z. R. E. P. Valery Vodovozov, “Challenges of Active Learning in a View of IntegratedEngineering Education,” *Education and Sciences, Engineering Education in Knowledge Based Society,* 1 2021.

[90] A. R. Jensenius, “Disciplinarities: intra, cross, multi, inter, trans,” [Online]. Available: https://www.arj.no/2012/03/12/disciplinarities-2/. [Accessed 27 05 2021].

[91] European Commission, “EU policy in the field of vocational education and training,” [Online]. Available: https://ec.europa.eu/education/policies/eu-policy-in-the-field-of-vocational-education-and-training-vet_en. [Accessed 5 2021].

[92] Aalto university professional development, “UP-RES,” [Online]. Available: http://aaltopro2.aalto.fi/projects/up-res/index.html. [Accessed 05 2021].

[93] Euroheat & Power, “UP-RES: Urban Planners with Renewable Energy Skills,” [Online]. Available: https://www.euroheat.org/our-projects/res-urban-planners-renewable-energy-skills/.

[94] C. M. a. M. P. Kenneth J. Knapp, “Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance,” *Journal of Information Systems Education,* vol. 28, no. 2, pp. 101-114, 2017.

[95] BRIDGE project, “Minutes BRIDGE Topics meeting,” 2019.

[96] THE EU AGENCY FOR CYBERSECURITY, “INDUSTRY 4.0 CYBERSECURITY: CHALLENGES & RECOMMENDATIONS,” ENISA, 2019.

[97] European Commission, “COMMISSION RECOMMENDATION on cybersecurity in the energy sector,” 2019.

[98] European Commision ESCO, “Occupations,” [Online]. Available: https://ec.europa.eu/esco/portal/occupation?resetLanguage=true&newLanguage=en. [Accessed 05 2021].

[99] EDDIE "Education for Digitalisation of Energy", “Deliverable 2.2 Current and future skill needs in the Energy Sector,” 2020.

[100] ENISA, “ENISA Good practices for IoT and Smart Infrastructures Tool,” [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/#IoT.

[101] R. Leszczyna, “Cybersecurity and Privacy in Standards for Smart Grids – a Comprehensive Survey,” *Computer Standards & Interfaces 56,* 09 2017.

[102] G. D. Solis, “Cyber warfare,” *Military Law Review,* pp. 1-52, 2019.

[103] SMART GRIDS TASK FORCE - EXPERT GROUP 2 - CYBERSECURITY, “Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity,” 2018.

[104] BRIDGE project: Data management and Regulation working groups, “TSO-DSO Coordination,” 2019.

[105] M. Rohloff, “Enterprise Architecture - Framework andMethodology for the Design of Architectures in theLarge,” in *European Conference on Information Systems (ECIS)*, Regensburg, Germany, 2005.

[106] ENERGY EXPERT CYBER SECURITY PLATFORM, “Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,” 2017.

[107] European Commission, “Erasmus Mundus Joint Masters scholarships,” [Online]. Available: https://ec.europa.eu/programmes/erasmus-plus/opportunities/individuals/students/erasmus-mundus-joint-masters-scholarships_en. [Accessed 25 5 2021].

[108] R. W. M.J. Turner, “An Evaluation of Flipped Courses in Electrical Engineering Technology Using Course Learning Outcomes and Student Course Assessments,” *Journal of Engineering Technology,* vol. 34, no. 2, pp. 34-43, 2017.

[109] D. Y. K. &. S. N. Martin, “Improving learning opportunities for specialeducation needs (SEN) students by engagingpre-service science teachers in an informalexperiential learning course,” *Asia Pacific Journal of Education,* vol. 38, pp. 319-347, 2018.

[110] U. E. S. A.Georgakaki, “Strategic Energy Technology Plan: Roadmap on Education and Training,” 2014.

[111] A. T. a. J. W. Filipo Sharevski, “Novel Approach for Cybersecurity Workforce,” in *IEEE Integrated STEM Conference (ISEC)*, Princeton, NJ, USA, 2018.

[112] D. K. Fleischmann, “Volume 11 Re / materialising Design Education Futures,” *STUDIES IN MATERIAL THINKING,* vol. 11, no. 3, 2015.

[113] N. U.-B. Luis Emilio Alvarez-Dionisi, “Implementing a Cybersecurity Culture,” *ISACA,* vol. 2, 2019.

[114] A. N. H. &. C. M. Heylighen, “ICT revisited-from information & communication to integrating curricula?,” *Journal of Information Technology in Construction,* vol. 9, no. 7, pp. 101-120, 2004.

Annex 1

This Annex contains the protocol of the interviews that were conducted in order to identify the challenges the industry faces.

[DRAFT] ERASMUS INTERVIEW PROTOCOL

Interviewee Name: _____

Date and time: _____

Researchers conducting session: _____

Note Taker: _____

My name is _____ and I will be facilitating this interview along with my colleague(s) _____ . The goal of this project is to To identify the gaps in the skills that are being offered from the education and the skills that are required by the industry in the combined field of cybersecurity in smart grids.. This qualitative interview also aims to gather opinions from industry about the challenges they face regarding cybersecurity.

We value your opinions and insights. We want to know what works and what does not. Ultimately this study will provide recommendations for future cybersecurity education for the students to be prepared for the real-world experience and meet industry's expectations for such essential and needed skills.

The information from this effort will be handled as anonymous. Prior to the interview, we sent an introductory letter and two consent forms (one to sign and return and one to keep) prior to the session today. The interview will take approximately 30-40 minutes and will follow a designed interview protocol.

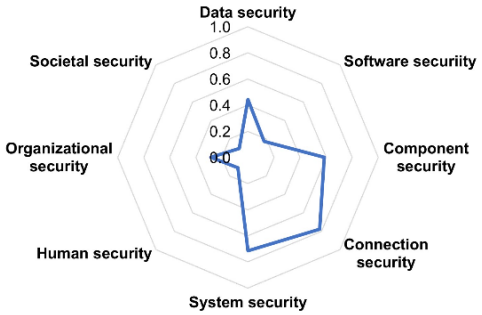
Do you have any questions? If there are no further questions, let's get started with the first question.

[Note: the researcher will use phrases such as "Tell me more", "Could you give me an example?", "Could you explain that?" as prompts to solicit more detailed information when needed.]

1. To get started, let's introduce ourselves. In the introduction please tell us who you are, and where you currently work as well as your responsibility related to cybersecurity?

2. We have reviewed academic papers and reports from European bodies about cybersecurity in smart grid. This figure shows to what extent each knowledge area is covered in the state-of-the-art research (based on the Association for Computing Machinery (ACM) framework).

   What do you think about whether this figure aligns with your thought that most of the studies overlook societal, organizational, and human security aspects?



3. Could you please tell us about the positive experiences that you have seen with recent graduates with cybersecurity education working with you?
   3.1 What are the main impressions about the skill to perform the job in your opinion?
   3.2 Could you tell me more about your opinion/thought why the new hired staffs you mentioned have such good skills?

4. Could you please tell us about the negative experiences that you have seen with recent graduates working with you?
   4.1 Could you tell us what kind of skills they do not normally have but are needed for the job?
   4.2 How did you train the new staff on the job related to cybersecurity?

5. Does your company/organization extensively on leadership involvement in cybersecurity? For example, the policy from the executive board, communication initiative about cybersecurity updates, and roadshow.

6. Does your company provide such an internship program? Could you please tell us more about how did you select the thesis topic? And why this topic?

7. Can you identify the main challenges that are being faced by the industry in the field of cybersecurity?

Please only mention these proposed challenges to start the example if necessary to avoid the bias thought from the interviewee

- Specialists do not have enough depth in their knowledge or skills
- Management seniors are not involved enough in cybersecurity matters because of the technical complexity of the field
- The multiplication of entry points (move operations on cloud, more equipment connected to the internet etc)
- Blending of home and work equipment especially during the COVID-19 epidemic
- Human factor: negligence on behalf of the employees
- Cybersecurity is seen as pure cost and not as potential value creation
- Lack of appropriate language for the efficient communication between cybersecurity experts and managers
- Implementation of standards (like ISO27001) is not substantial and it is difficult to assess the level of actual protection they offer

8. What advice would you like to share in order to improve the education and better match the skills required in the field of cybersecurity in smart grids in the future?

Thank you very much for your collaboration in this interview. We will provide you a copy of the protocol by next week.

In the meantime, if you have any questions or further comments, please kindly reach us by email directly.