Strategy for Cybersecurity Education in Smart Grids (Executive Report)

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.

Contents

Definitions, Acronyms and Abbreviations

Abbreviation	Meaning
ACM	Association for Computing Machinery
CPES	Cyber Physical Energy System
CSIRT	Computer Security Incident Response Team
CTF	Capture the flag
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
IT	Information Technology
KA	Knowledge Area
KU	Knowledge Unit
MQTT	MQ Telemetry Transport
NIS	Network and Information Systems
OT	Operational Technology
PBL	Problem based learning
REST API	Representational State Transfer Application Programming Interface
SAREF	Smart Applications Reference Ontology
SIEM	Security Information and Event Management
UPRES	Urban planners with Renewable Energy Skills

List of Tables

1. Introduction

The integration of the power grids all around the world with Information and Communication Technology capabilities have created a need for professionals that have an interdisciplanary knowledge of both the field of smart grids and the field of cybersecurity. Our project "Cybersecurity curricula recommendations for Smart Grids" aims to ease the adaptation of the post-secondary European curricula as they must include learning objectives relative to cybersecurity among the others. In this report the skill gaps identified in the IO1 of the project are used in order to provide directions for the relevant stakeholders on how to train the current and future workforce in a way that mitigates those skill gaps.

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 the bibliography.

2. Challenges faced by the industry

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.

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 Analysis of the industry interviews and literature review

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. Certification schemes for cybersecurity skills are not widely adopted nor integrated in the curricula
4. It is difficult to create a cybersecurity culture in a workforce that does not have relevant responsibilities in their job description explicitly
5. Lack of strong interconnection between Higher Educational Institutes (HEIs) and industry
6. 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.

2.2 Identified needs in policy and educational changes

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

3. Skill gaps mitigation plan

3.1 Mitigation actions

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. In the following table (Table 1), the key actions are presented

Mitigation Actions												
Knowledge area	**Knowledge unit**	**Knowledge of the component in the power system**	**Conduct international research in cyber**	**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						
	Risk Management						X	X	X	X	X	X

Organizational Security	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 roadmap to existing curricula

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.

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 [1] [2]:

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 meanwhile developing existing curricula. Still, as indicated in [3], 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

In this chapter our goal is to find the educational methodologies or techniques that will be helpful when teaching about cybersecurity in smart grids. For this purpose, initially we analyse eight educational methods and then we conduct a review of their use in the fields of interest either separately or in combination. From the results of the review, we make proposals for the various teaching settings.

4.1 A brief presentation of the methods that were taken into account

The traditional learning model-Lecture based learning

Lecture based learning is the most widely used teaching method due to its scalability potential and the fact that the teacher has the control of what will be taught and in what way. Its main disadvantage is that the students can resort to memorization instead of understanding in

order to pass the exams. It is frequently combined with some forms of experiential learning like simulations and lab exercises.

Experiential learning

Experiential learning is a term that includes all the forms of learning where knowledge is acquired through experience. It was described by David Colb in 1984 as a cycle that can be repeated continuously where the experience leads to the formation of theories which then can be used to formulate new experiments and gain more experience.

Active learning

Active learning is also a rather broad term and it is based on increasing the engagement of the students through their participation in various ways. During the lecture it can take the form of creating a concept map, asking a question to the audience, writing a one-minute paper, or peer teaching.

Cooperative learning

Cooperative learning describes the work of a group where each student not only allocates his/her time in doing part of the group work but also each student is responsible for the performance of the group and the effectiveness of the skill allocation between the group members.

Flipped classroom

In flipped classroom technique, the students are expected to have studied the material for the class beforehand. The material can be already existing like a book or a series of videos but it can also be specially made for the course. During the class time the teacher can use active learning techniques to test and deepen the students' understanding of the course material. One possible disadvantage is the non-homogenous access to electronic means in the students' homes.

Inquiry based learning

Inquiry based learning resembles the scientific method the most. Its phases include Orientation, Conceptualization, Investigation, Conclusion and Discussion. Depending on the maturity of the students the teacher can provide more or less guidance and input.

Problem-based learning and project-based learning

The basis of those two methods is cooperative learning. In Problem-based learning (PBL) a group of students investigates an open-ended real-world problem and tries to come up with the most suitable solution which then the group presents to other peers. Project-based learning is very similar at its core with problem-based learning but it usually lasts longer and the solution is not only theoretical but it has a concrete and explicit outcome like a computer program or a model.

Gamification

In gamification, elements and mechanisms that are commonly incorporated during the design of a game (level beating, limited time to complete a task and others) are used in order increase the engagement of the students.

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

In order to identify the impact of the use of the various methods in teaching cybersecurity for smart grids we conducted a literature review in a pool of 43 documents. 21 of them are written from authors that used some of the above methods to teach a relative course and the rest are more general. The remarks from the literature review are presented below:

Restrictions posed for the use of active learning techniques:

The use of active learning techniques requires not only more staff, time and resources but also the groups of students have to be homogenous and already have a minimum level of strength on the subject.

Use of gamification in Universities:

Gamification in universities can take the form of actual games like Riskio which is a board game and can be used for undergraduate students or non-technical employees in industry.

Capture the flag and Hacking Day events:

Capture The Flag contests are a form of gamification and they have elements from experiential learning and collaborative learning. 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 two teams opposing each other or every contestant team tries to hack the organizers' system. CTFs are appropriate for training on attacks that happen in a short time window. Special care should be given to ease the way in for a novice player. CTFs can take the form of a career day with the participation of the industry. Some of the students can be the organizing team of the event which gives them very important skills for the industry.

Use of gamification in industry

Gamification in industry has been successfully used in non-technical employees to improve the prevention of a phishing attack. It is important to notice that in the company where the data were collected, the group that had previously been trained to prevent phishing attacks via email, had the same results as the control group with no training at all.

Use of demonstration

Demonstration can be used for both undergraduate students and employees. In one example Shodan is used, which can find various devices that are connected to the internet without credentials or with the use of default credentials. Students and employees can realize the potential impact of their behavior about keeping good cybersecurity habits.

Use of Project-based learning:

Project-based learning is the most frequently used method along with gamification. It has been argued through survey results 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. [4]

Virtual labs and remote access:

The trend for use of virtual labs that began in 2010 has been strengthened because of the COVID-19 pandemic. Statistical results in [5] show that there is a need from the students for use of the labs during the hours that they are usually closed to the public but to set up the lab additional staff hours are needed for the technical support.

Using testbeds to teach about cybersecurity:

The most complete and realistic way to study the effects and recovery process of a cyber-attack is to use a testbed. In a testbed the system is simulated in very high detail. The level of detail increases as more components of the simulated system are represented by hardware rather that software and as more components of the same system are added. Examples of using Real Time Simulators to study cyberattacks can be found in [6], [7].

5. Recommendations

The last part of the report consists of high-level recommendations organized by the stakeholder they are addressed to, namely universities, VETs, Industry and policy makers. The recommendations were the result of a synthesis on many (mainly European) documents like report of a taskforce, deliverable of a project and others. In the next paragraphs we briefly present the recommendations to the various stakeholders.

5.1.1 Universities:

- Create an observatory to continuously monitor the new and ongoing research results on the combined field
- Create a database of experts and researchers along with their areas of work to help create Joint Masters programs that are currently absent from Erasmus Mundus for the particular field.
- Continue and expand the use of European Credit Transfer in accordance with the Bologna Process. The harmonization of the European accreditation systems is a prerequisite for the existence of Joint curricula.
- Overcome the obstacle of lack of equipment by creating an inventory of infrastructure according to the example of the ERIGRID 2.0 project.
- Create a course module repository to share the design of the courses and best practices to speed up the adoption of the relevant learning outcomes.
- Universities should orient more in creating T-shaped engineers that possess both a wide range of general knowledge (horizontal bar of T) and a high specialty domain (vertical bar of the T)
- The general knowledge should include the ethical, social and legal aspects which can be overlooked in STEM (Science Technology Engineering and Mathematics) programmes

5.1.2 VETs:

- Create a project like UP-RES [8] which was also an example of a project with two fields to be combined namely renewable energy resources and urban planning. The output will be trained professionals, best practices for education, educational material and possible collaboration between universities.
- C-VET providers should formulate courses and online training modules with very specific focus like how to implement a communication protocol on a legacy device. These can formulate a micro master which is the equivalent of a master semester.
- Some courses can act as preparation for acquiring a certificate which generally can help increase the employability of the graduate student with special care on the selection of certificates.

5.1.3 Industry:

The cybersecurity competency of the employees can be analysed in two broad categories which are firstly the skills and knowledge that are technical and relevant to the

product or service of the company and secondly the awareness of how the human factor (both the employee's and the customer's) can affect the security of the system.

- Topics and principles that should be taught to the employees include:
  - Between a shared database model and a message-based model, the message-based one is beneficial [9]
  - Smart Applications REFerence ontology (SAREF) model which analyses the home IoT devices in their building blocks and the relationships between them.
  - Orientation on how to enable the continuous updatability and upgradability of the components.
  - Application of the principles of **security-by-design** and **security-by-default**.
  - Relevant legislation. A good overview until mid-2017 can be found in [10] and more recently GDPR and NIS 2.0 directive were added.

The three points which differentiate the cybersecurity field of the energy sector from the field of cybersecurity in general are [11] the use of legacy equipment, the existence of cascading effects because of the high interconnection between the european grids and the real-time requirements which means that some actions in a power grid must happen very quickly and the security protocols must be selected accordingly. For each of these three sectors the teaching of the following principles and best practices is recommended:

Legacy equipment: Systematic patch management and regular risk analysis targeting legacy devices

Cascading effects: Classification of assets and identification of critical nodes to avoid single point of failure

Real-time requirements: Segregation of networks

- Recommendations relevant to the effect of the human factor in cybersecurity
  - Companies should organize sessions where the competence of the employees is measured and the quality of the decisions they make that are relevant to the cybersecurity
  - Managers should receive additional training on how their behavior affects the persons they manage [12], for example to make clear that security should not be neglected in favour of productivity.
  - Use of the ENISA tool "Good practices for IoT and Smart Infrastructures Tool" which can be helpful especially for small businesses.

5.1.4 Policy makers:

- Member states should be examined on how they implement the NIS 2.0 directive which can act as a reference model. The existence of NIS authority and Computer Security Incident Response Team (CSIRT) are important. Industries should list their assets, operations, and critical infrastructure components in addition to identifying the operators of essential services according to the NIS directive.
- Create a repository where operators and other parties can share detailed information on incidents and early warnings about attacks and violations.
- A minimum-security scheme should be defined and strictly met.
- The platforms that are utilized should be listed and the criteria for platforms interoperability should be defined as the recommended enterprise architecture practices suggest [13].

- Create a repository where the industry can monitor continuously the skills needed.
- Create a common language that will help remove the communication obstacle especially between managers and technical employees.
- Existing available communication means like MQQT and REST API are highly recommended to replace proprietary solutions.
- Elaborate on the new data roles, perhaps by using the Harmonized Electricity Market Role Model
- Apply the Common Information Model standards in Transmission System Operator and Distribution System Operator

5.1.5 Recommendations on how to foster collaboration among stakeholders:

As it has been stated before, the cybersecurity education in the 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 the 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 is the education in cybersecurity in smart grids 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] R. R. &. S. S. Hipkins, "Curriculum changes, priorities and issues: Findings from the NZCER secondary 2006 and primary 2007 national surveys.," NZCER, 2008.

[2] B. (. B. Rachel Lowe, "Pre-Service Teachers' Experiences With Curriculum Integration: A Qualitative Study," 2017.

[3] 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/.

[4] 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)*, 2017.

[5] 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.

[6] 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.

[7] 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.

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

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

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

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

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

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

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