Real-Time Physical Cybersecurity Massive Open Online Course MOOC – Teacher's Handbook

(Executive Report)

Authors:

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

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 3

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

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

Contents

Contents 2

Definitions, Acronyms and Abbreviations 3

1. Introduction 4

1.1 Objectives 5

1.2 Structure of the document 5

2. Course Design Methodology 5

3. A Review of Educational Methodologies 6

4. Instructional Design Models 7

5. Course Design Outline 7

6. Course Content 8

6.1 Part 1: Smart Grids, Cyber Security and Grids 8

6.1.1 Chapter 1: Fundamentals of Smart Grid Systems 8

6.1.2 Chapter 2: Cybersecurity and Operational Security in Smart Grid Systems 8

6.1.3 Chapter 3: IEC 61850 and IEC 62351 9

6.2 Part 2: Real-Time Simulation, The Theory 9

6.2.1 Chapter 4: Simulation Fundamentals 9

6.2.2 Chapter 5: Real-Time Simulation for System Design 9

6.2.3 Chapter 6: Parallel and Distributed Real-Time Simulation 9

6.2.4 Chapter 7: Tools and Applications 9

6.3 Part 3: Exercises and Case Scenarios 9

6.3.1 Exercise 1 9

6.3.2 Exercise 2 10

6.3.3 Exercise 3 10

6.3.4 Exercise 4 10

7. Tools 10

8. Bibliography 11

Definitions, Acronyms and Abbreviations

ADDIE	Analyze, Design, Develop, Implement, and Evaluate
CC-RSG	Cybersecurity Curricula Recommendations for Smart Grid
CI	Critical Infrastructure
CPS	Cyber-physical Systems
DEVS	Discrete Event System Specification
HIL	Hardware in the Loop
ICS	Industrial Control Systems
ID	Instructional Design
IO	Intellectual Output
MOOC	Massive Open Online Course
RCP	Rapid Control Prototyping
RT	Real-time
SCADA	Supervisory Control and Data Acquisition
SIL	Software in the Loop
SPSP	Smart Power Security Professional
UML	Unified Modeling Language
WP	Work Package

1. Introduction

Recently, the energy sector has undergone significant changes, leading to the emergence of the concept of smart grids. A smart grid refers to an electricity network that integrates the actions and behavior of all users, including generators, consumers, and those that function as both, with the aim of delivering sustainable, economical, and secure electricity supplies efficiently. Cybersecurity of the smart grids has become a critical issue that needs to be addressed due to the increasing attack surface and the criticality of connected assets. Cybersecurity is one of the essential digital capabilities that the European Union aims to achieve. It encompasses several aspects such as tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be employed to protect an organization and user's assets and the cyber environment. Despite the availability of numerous tools and software packages from different vendors that cover security needs and ensure grid robustness, cybersecurity remains a prominent issue.

Cybersecurity Curricula Recommendations for Smart Grid (CC-RSG) project has delved deeper into the issue of cybersecurity in smart grids using surveys, reviews, and workshops. The investigation revealed the following findings:

1. The current approach to addressing cybersecurity topics in smart grids is inadequate.
2. There is a shortage of cybersecurity professionals in the smart grid field due to the scarcity of educational programs that cover this specific field practically.
3. The existing educational offerings do not meet the Smart Power Security Professional (SPSP) requirements.
4. Real-life scenarios and connections with industry are lacking.

Providing educational opportunities that can enhance skills and address the gaps mentioned above is an important need, especially given previous reports highlighting that at least 50% of cybersecurity incidents stem from human error. To address this issue, CC-RSG project seeks to assist post-secondary institutions in integrating learning outcomes related to cybersecurity in smart grids into their curricula. This report provides the outline of the course that was designed to cover this issue.

This report presents the outcome of Work Package (WP) 3, “Designing, Developing, and Piloting” – Intellectual Output (IO) 3 – of CC-RSG project in brief. Hence, the report builds on the results of previous reports and IO’s, to provide a Massive Open Online Course (MOOC) for real-time physical cybersecurity systems. The course aims at filling the found gaps in Cyber-physical Systems (CPS), as well as building skills around real-time simulation systems that are used for high-speed simulations, testing of Critical Infrastructure (CI), and evaluating security operations and functions. To design the course, different approaches have been investigated and tested, thus to find the most suitable methods that serve the purpose of creating the course and filling the skill gaps that were highlighted. The course therefore is to make use of the following approaches: Flipped learning, Simulations, and Virtual and remote labs. These approaches were carefully chosen based on their capabilities for providing means for interaction, building analytical and problem-solving skills, as well as promoting hands-on skills.

The main contributions of IO3 course report are:

1. Providing the theoretical background regarding real time simulation systems
2. Building hands-on skills on using real time simulation

3. Introducing and applying use cases, scenarios, and exercises for practice and training purposes.

In IO3 course report, “Real-Time Physical Cybersecurity Massive Open Online Course MOOC – Teacher’s Handbook”, theoretical and foundational knowledge have been taken care of, by furnishing strong grounds and providing the base for knowledge about smart grids, smart grids communication protocols, and cybersecurity in smart grids. In addition, real-time simulation systems, since being identified as one of the niche and most effective tools for experimenting, testing and learning about critical infrastructure and smart grids, has been given special consideration. Accordingly, many concepts around real-time simulation have been presented. Moreover, the course not only focuses on the theoretical knowledge, but it surpasses to cover the hands-on skills required by the industry. Thus, four exercises were built around selected industrial scenarios, and were implemented through a physical Real-Time Simulator system.

Finally, IO3 course design report acts as the teacher’s handbook. Thus, while designing the course, we tried to gather all information needed to cover the topic of cybersecurity in smart grids comprehensively. To use this report, teachers/instructors are advised to use the material here to design presentations and handouts, also since the emphasis is on flipped-learning and MOOC, the design of pre-recorded videos and automated tasks is highly recommended.

1.1 Objectives

The main objective of IO3 is to design a course that provides participants with the knowledge required to embark on the field of CPS, especially cybersecurity in smart grids.

1.2 Structure of the document

- Section 2 presents the course design methodology
- Section 3 reviews educational methodologies and learning approaches utilized
- Section 4 presents the general Instructional Design (ID) models
- Section 5 presents the course design outline
- Section 6 presents the content of the course and topics covered briefly.
- Finally, Section 7 presents the tools used

2. Course Design Methodology

To design the course effectively, the following processes were adopted:

1. Give emphasis on the need for the course design
2. Define the case and context of the course
3. Specify the aims and desired outcome
4. Specify learning methodologies and activities
5. Specify course content
6. Choose evaluation criteria
7. Development and implementation

3. A Review of Educational Methodologies

The significance of educational methodology cannot be understated as it defines the ways in which learning goals are achieved and assessed. First, various educational methodologies and techniques are available depending on the desired level of knowledge retention. These include lecture-based instruction, experiential learning, active learning, cooperative learning, flipped learning, inquiry-based learning, problem-based and project-based learning, and gamification, as follows:

1. The conventional method of learning, lecture-based learning, entails an instructor delivering the course material, conducting assessments, and assuming full responsibility for the educational experience. However, this method is primarily passive and relies heavily on memorization. By incorporating activities like cold calling, discussions, learning cards, and other interactive elements, lecture-based learning can be transformed into an active and more effective approach.
2. Experiential learning is an active approach to learning that requires students to engage in the learning process and develop experience as they learn. Active learning, on the other hand, is not just about incorporating activities and encouraging participation, but also entails the processing of all learners' responses before presenting new information.
3. Cooperative learning is a team-based approach in which participants collaborate to achieve specific goals and take full responsibility for completing a task. Flipped learning is a modern approach that empowers learners to take ownership of their learning by providing educational material beforehand, allowing for a more dynamic and interactive classroom experience.
4. Inquiry-based learning is an approach that involves students following the same practices as professional scientists to gain knowledge and experience. Problem and project-based learning actively engage participants in the learning process by exploring a specific problem or question with the aim of finding answers or developing a solution.
5. Lastly, gamification employs game-like features such as storytelling, level-beating, and badges to encourage participation and make the learning process more engaging. By utilizing these different approaches, educators can create a more effective and engaging learning environment for their students.

Second, the above-mentioned educational methodologies are typically used to reflect on the learning retention rate that is defined by the course objectives and available resources. It is noted that the more the engagement in the learning process, the higher the retention rate; however, the more resources also needed. Following is the retention rate of different learning activities:

1. Conventional method and lectures: 5%
2. Reading and self-study: 10%
3. Audio-Visual illustrations: 20%
4. Demonstration and semi-active participation: 30%
5. Planning, discussions, and active participation: 50%
6. Learning by doing: 75%
7. Teaching others: 90%

When designing a course, it is critical to firstly define which retention level is targeted, and thus adjust the workload and resources to match this criterion

4. Instructional Design Models

Since IO3 is about course design, general ID models mentioned below were used to help in the process of defining goals, selecting activities, and choosing course material.

1. Bloom's Taxonomy is a hierarchical model used to assess learning progress. It includes various levels of learning, with remembering at the bottom and creating at the top. Depending on the desired outcome, activities can be tailored accordingly to ensure that students are achieving their learning goals.
2. Gagne's Nine Events Model is a comprehensive framework of instructional events that must be considered to ensure effective learning. These events include gaining attention, informing objectives, recalling prior knowledge, presenting content, providing guidance, facilitating practice, providing feedback, assessing performance, and enhancing retention and transfer.
3. The ADDIE Model is a structured framework for designing and developing courses, consisting of five stages: Analyze, Design, Develop, Implement, and Evaluate. The model emphasizes the importance of continuous revision and improvement throughout the course development process.
4. Merrill's Principles identify several principles common to effective instructional design models. These include task/problem-centered design, activation of prior knowledge, demonstration of new knowledge, application of new knowledge, and encouraging integration of new knowledge.
5. The Dick and Carey Model, also known as the Systems Approach Model, is a planning model for lesson development. It includes defining instructional goals, conducting instructional analysis, defining entry requirements, specifying performance objectives and test items, developing instructional strategy and materials, and conducting formative and summative evaluations. This model ensures that the lesson plan is comprehensive and covers all aspects of the instructional process.

It is important to note that while these methodologies provide a comprehensive framework for designing and developing courses, they may not always align perfectly with the specific goals and resources of a given course offering. In practice, it may be necessary to make adjustments to the defined attributes to ensure that the course meets its intended objectives. These methodologies are meant to serve as a guide and should be adapted to fit the unique needs and circumstances of the course. Ultimately, the goal is to use these methodologies to create effective and engaging learning experiences for students. While they provide a solid foundation for course development, they should be tailored to suit the specific needs of each course, taking into account factors such as the audience, subject matter, and available resources.

5. Course Design Outline

Based on the specified objectives and resources for the course design, the following outline is adopted:

1. Learning Objectives: To cover the gap of cybersecurity knowledge in smart grids
2. Prerequisites: The course shall only be open to students and professionals with pre-knowledge in the fields of cybersecurity and smart grids
3. Retention level projected by this course: 60% to 75%, aiming at active discussions and simple practice by doing tasks

4. Instructional Design methodologies adopted: ADDIE and Dick and Carey models for design, and targeting the third level – applying – of Bloom's Taxonomy for retention.
5. Approaches used: Flipped learning and gamification mainly, with tasks that promote cooperative learning
6. Method of delivery: Supervised recorded sessions
7. Criteria to increase attention and engagement: Bonus points, the use of games, and discussion forums
8. Assessment and Measurement: Regular quizzes and a final exam, preferably automated self-evaluated ones.
9. Course load:125-140 hours of lectures, exercises, and self-study material

6. Course Content

The designed course is divided into three parts. Part one covers Smart Grids, Cyber Security and Grids. Part two covers Real-Time Simulation, the Theory. Finally, part three concerns building practical skills by providing Exercises and Case Scenarios. The said three parts include seven chapters and four hands on training exercise. In the next subsections, the main points of each chapter are briefly presented.

6.1 Part 1: Smart Grids, Cyber Security and Grids

6.1.1 Chapter 1: Fundamentals of Smart Grid Systems

This chapter covers the main concepts of smart grid systems, including: components of the smart grid, drivers of the smart grids, main benefits and challenges facing implementation and realization of the smart grid, and the smart grid architecture model. The chapter proceeds with introducing smart grid technologies in terms of framework, functionalities and capabilities, resources and energy storage systems, microgrids, smart substations, and the communication protocol IEC 61850. Next is the challenges and success factors of the grid, in which 6 challenges that include business transformation, convergence of operations, integrated system approach, the complexity of having a heterogenous system, cybersecurity and finally privacy, are introduced, followed by the main success factors of the grid. Lastly, final sections of the chapter include the global initiatives on smart grids, specifically in the European market, and the future of smart grid.

6.1.2 Chapter 2: Cybersecurity and Operational Security in Smart Grid Systems

This chapter covers the security aspects of the grid including hacking the grid and the main attack methods, security models for the Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) and smart grid, and finally concludes with methods for security the smart grid, including implementation of security controls, field zone protection, control zone protection, service zone protection, establishing strong boundaries and zone separation, advanced network mentoring, protecting data and applications, and situational awareness.

6.1.3 Chapter 3: IEC 61850 and IEC 62351

IEC 61850 has been used for long as the standardized protocol for smart grid communication. This chapter covers the main aspects and architecture of this standard, and also gives introduction to the complementary security protocol IEC 62351 that is used to establish a security layer on top of IEC 61850.

6.2 Part 2: Real-Time Simulation, The Theory

6.2.1 Chapter 4: Simulation Fundamentals

This chapter covers the main concepts regarding simulation technologies. This includes discreate, continuous and hybrid models, high speed real-time hybrid simulation, formalized approach for the design of distributed systems, modeling using Discrete Event System Specification (DEVS) and Unified Modeling Language (UML) languages, and tools for integration with MATLAB and Simulink.

6.2.2 Chapter 5: Real-Time Simulation for System Design

This chapter covers the concepts of system design, including progressive simulation, Hardware in the Loop (HIL) and Software in the Loop (SIL) concepts, validation and validator tools, and finally the concept of use Rapid Control Prototyping (RCP) to facilitate system design and testing.

6.2.3 Chapter 6: Parallel and Distributed Real-Time Simulation

This chapter introduces a testbed using DNP3 protocol, then gives emphasis on the use of system approach to simulation for training.

6.2.4 Chapter 7: Tools and Applications

This chapter presents the time dilation concept, thus accurate simulation in large-scale systems could be achieved. Related concepts to this as virtualized systems, CPU scheduling, network emulation and memory emulation, are also introduced.

6.3 Part 3: Exercises and Case Scenarios

6.3.1 Exercise 1

A Guide for Getting Started with Real-Time Simulator EXATA CPS and HYPERSIM OPAL-RT

6.3.2 Exercise 2

Real-Time Co-Simulations of a Microgrid Active Power Management Against Delay Attack

6.3.3 Exercise 3

Real-Time Co-Simulations of a Microgrid Active Power Management Against Modify Data Packet Attack

6.3.4 Exercise 4

Real-Time Co-Simulations of a Microgrid Based on Controller Hardware in the Loop HIL

7. Tools

Tools used throughout this course include tools for learning assistance, and tools for exercises and hands on skills, as follows:

1. Learning assistance tools: Those are the tools used to assist in the learning process. Here, since the course being offered is in the form of a MOOC, a dedicated repository (MOODLE) is used to host the learning material, discussion forums, quizzes and online exams. Other tools that might be used include available communication and video streaming tools, as well as tools for designing presentations and video editing.
2. Hands on skills tools: In this course, OPAL-RT system, which is a real-time simulator, is used to conduct training sessions and to deliver participants with the skills that were identified in the course objectives.

8. Bibliography

[1] European Technology Platform, European Commission, “Strategic deployment document for Europe electricity networks of the future”, April 2010.

[2] Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." UNECE. www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Grids. Overview. pdf, (2015).

[3] European Commission (2020). Europe investing in digital: the Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[4] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan, and Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. Auerbach publications, 2003.

[6] Vacca, John R., ed. Managing information security. Elsevier, 2013.

[7] Romanovs, Andrejs, et al. "State of the Art in Cybersecurity and Smart Grid Education." IEEE EUROCON 2021-19th International Conference on Smart Technologies. IEEE, 2021.

[8] Valliou, Maria, et al. "Strategy for Cybersecurity Education in Smart Grids." (2022).

[9] González-Manzano, Lorena, and Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.

[10] Scott, Bernard, and Chunyu Cong. "Knowledge and task analysis methods for course design." Readings in Technology in Education: Proceedings of the International Conference on Information Communications Technologies in Education. 2007.

[11] Arora, Bela. "Teaching cyber security to non-tech students." Politics 39.2 (2019): 252-265.

[12] A comprehensive guide. John Wiley & Sons, 2020.

[13] Becker, S. Adams, et al. NMC horizon report: 2017 higher education edition. The New Media Consortium, 2017.

[14] Shi, Yinghui, et al. "Examining interactive whiteboard-based instruction on the academic self-efficacy, academic press and achievement of college students." Open Learning: The Journal of Open, Distance and e-Learning 33.2 (2018): 115-130.

[15] Hall, Steven R., et al. "Adoption of active learning in a lecture-based engineering class." 32nd Annual frontiers in education. Vol. 1. IEEE, 2002.

[16] Kolb, David A. Experiential learning: Experience as the source of learning and development. FT press, 2014.

[17] Felder, Richard M., and Rebecca Brent. "Active learning: An introduction." ASQ higher education brief 2.4 (2009): 1-5.

[18] Felder, Richard M., and Rebecca Brent. "Cooperative learning." Active learning: Models from the analytical sciences 970 (2007): 34-53.

[19] Bergmann, Jonathan, and Aaron Sams. Flipped learning: Gateway to student engagement. International Society for Technology in Education, 2014.

[20] Keselman, Alla. "Supporting inquiry learning by promoting normative understanding of multivariable causality." Journal of Research in Science Teaching 40.9 (2003): 898-921.

[21] English, Mary C., and Anastasia Kitsantas. "Supporting student self-regulated learning in problem-and project-based learning." Interdisciplinary journal of problem-based learning 7.2 (2013): 6.

[22] Deterding, Sebastian, et al. "From game design elements to gamefulness: defining" gamification"." Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments. 2011.

[23] Lalley, J., and R. Miller. "The learning pyramid: Does it point teachers in the right direction." Education 128.1 (2007): 16.
[24] Reigeluth, Charles M. "Instructional design: What is it and why is it." Instructional-design theories and models: An overview of their current status 1 (1983): 3-36.
[25] Spector, J. Michael. Foundations of educational technology: Integrative approaches and interdisciplinary perspectives. Routledge, 2015.
[26] Huang, Ronghuai, J. Michael Spector, and Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.
[27] Brown, Abbie H., and Timothy D. Green. The essentials of instructional design: Connecting fundamental principles with process and practice. Routledge, 2015.
[28] Faruque, MD Omar, et al. "Real-time simulation technologies for power systems design, testing, and analysis." IEEE Power and Energy Technology Systems Journal 2.2 (2015): 63-73.
[29] Popovici, Katalin, and Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.
[30] Poudel, Shiva, Zhen Ni, and Naresh Malla. "Real-time cyber physical system testbed for power system security and control." International Journal of Electrical Power & Energy Systems 90 (2017): 124-133.
[31] "SCALABLE and OPAL-RT Innovate Cyber-Physical Solution." Scalable Network Technologies, 5 July 2017, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.