Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 00 (2023) 000–000

www.elsevier.com/locate/procedia

56th CIRP Conference on Manufacturing Systems, CIRP CMS ‘23, South Africa

A Cybersecurity Training Concept for Cyber-physical Manufacturing Systems

Kanthanet Tharot[a,b], Quoc Bao Duong[a], Andreas Riel[a], Jean-Marc Thiriet[b]

[a]*Univ. Grenoble Alpes, CNRS, Grenoble INP, G-SCOP, 46 Avenue Félix Viallet, 38000 Grenoble, France*
[b]*Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-Lab, 11 rue des Mathemathiques, 38402 Saint-Martin-d'Hères, France*

* Corresponding author. Tel. +33476825156: *E-mail address:* kanthanet.tharot@grenoble-inp.fr

Abstract

Networked manufacturing systems based on traditional Industrial Control Systems (ICS) are particularly exposed to cyberattacks. Mostly based on Programmable Logic Controllers (PLCs), they have been designed to isolate manufacturing environments without connection to cyber-infrastructures such as cloud, connectivity with offices, and other manufacturing sites. Hence, low cybersecurity protection levels make such ICS interesting for malicious cyber-attackers. Thus, resilience to such attacks through cybersecurity has become one of the most significant concerns of Industry 4.0. While the technical aspects of cybersecurity for manufacturing systems are increasingly researched, there are few published works on effective methods to train cybersecurity for manufacturing systems. This paper proposes a cybersecurity training concept that builds on teaching cybersecurity in an interactive role-based approach within a teaching factory environment. Both attack and defense strategies can be explored, and student learning performance evaluated. The concept has been implemented to show its feasibility and potential to outperform traditional classroom-based training methods.

Keywords: Learning factory; Industry 4.0; Serious Game; Cybersecurity training.

1. Introduction

Nowadays, cyber-security is a critical issue in many activities. In the past, the main issues about cyber-security were the confidentiality and integrity of data. These data were circumscribed in IT (Information Technology), and the potential risks only impacted the digital (cyber) world. The general computing in everyday life and everywhere, IoT, connected objects, autonomous vehicles, and Industry 4.0, with potential cyber-security impacts in the physical world, leads to the need to train people to use and behave correctly in this digital environment. We should focus more specifically on manufacturing systems within Industry 4.0 [1]. In that case, the global interconnection of manufacturing systems with supervision systems imposes the deployment of cyber-security policies and mechanisms at the various steps of the company, this policy should take account of the specificities of the Industrial environment. The update policy, for instance, is a very tricky aspect of manufacturing systems: for some critical or specific software, it cannot be envisaged to update this software without taking some time to "test" the excellent quality and functioning of the new update, for example a software controlling a drone [2].

Initially, it is worth discussing the automation of traditional IT and ICS. According to the National Institute of Standards and Technology (NIST) [3], an ICS is defined as "the combination of control components (electrical, mechanical, hydraulic, pneumatic, etc.) that act together to achieve an industrial objective (manufacturing, transportation of matter and energy, etc.)". From the perspective of security properties and control, classic IT prioritizes confidentiality, integrity, and availability, whereas ICS prioritizes availability [4]. ICS is generally focused on time-critical responses, such as process incidents that may impact the environment, safety, or production.

To provide clarity, according to the Gartner glossary , IT [5] encompasses software, hardware, communications technologies, and related services. Operational technology (OT) [6] refers to hardware and software that detects or causes a change through the direct monitoring and/or control of industrial equipment, assets, processes, and events.

Generally speaking, people in the field of Automation in charge of this type of process are not advanced in IT and need to be educated and trained in cyber-security[7]. Our global work aims to propose a framework for training people in cyber-security in the industrial environment. Based on serious games, this training should be attractive enough for employees and pedagogically sufficient to reach the target to sensitize or train the people.

Our interest is a cyber-security approach for cyber-physical manufacturing systems. Our target is people with an automation (automatic, electronics) background and some IT know-how, particularly in the field of PLC (Programmable Logic Controller) and industrial networks. Depending on the time allocated to the training, on the pre-requisites of the trainees, we can envisage different types of trainings.

Studying some attack scenarios intensely, especially in the field of automation, may be pertinent. Some examples are the explosion of a Siberian gas pipeline caused by a trojan which reset pumps and valve settings in 1982 in the former Soviet Union, the Maroochy shire sewage spill in 2000 in Australia, the ransomware attack against oil distribution company Colonial Pipeline in the USA in 2021 [1].

At this first stage of our work, we propose in the present paper our global approach. We illustrate and focus on the PLC configuration and programming as well as the communication aspects, which are the first steps. The next section shows the challenges of ICS training. The third section deals with the research question and methodology. The fourth section proposes the first experimentation we have done for the training of PLC using a simulation tool. A questionnaire was sent to the trainees, which is described in the fifth section. The last section emphasizes some developments in a lab towards cyber-security and concludes this article.

Abbreviations

ASI	Actuator-Sensor Interface
CAN	Control Area Network
CIS	Critical security controls
CDAs	Critical Digital Assets
CS	Cybersecurity
CSIRT	Cybersecurity Incident Response Team
CST	Cybersecurity Team
FW	Firewall
IDS	Intrusion Detection System
IO	Inputs-Outputs
IT	Information Technology
ICS	Industrial Control System
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SME	Small and medium enterprise
TCP-IP	Transport Control Protocol Internet Protocol

2. Industrial Control System Training challenges

Some Studies [8] on digital manufacturing training during the Covid-19 is challenging face-to-face training. Using the core technology in Industry 4.0 [8], [9], such as additive manufacturing (3D printing), Internet of Things (IoT), Augmented Reality (AR), and the digital twin, to train two groups of engineer students and industrial trainees to provide a practical learning experience on turbine systems. The method of designing, developing, and 3D modelling/printing is fascinating to attract students and trainees evaluated by pre and post-survey of the impact learning experience.

In digital transformation based IoT- training by Kuhn et al. [10], there are a variety of training methods available, including an annual competition, theoretical teaching techniques, a model factory, embedded teaching through a case study, and hands-on training from the factory. However, we have yet to identify a holistic approach that is flexible enough to accommodate various learning styles and paths. Our proposed IoT training concept uses gamification and action-based learning from practical experience, allowing students to create their own applications and implement them on a low-cost microcontroller. Moreover, the training should encourage practical application, linking the educational environment with industry practice and collaboration. Apart from digitalization transformation in SMEs, Hulla et al. [11] showed through interviews with 40 experts from SMEs, larger companies, and consultants that skill gaps in strategy/roadmap, digital skills, and state-of-the-art in digital technologies have to be filled. According to them, essential success factors for relevant training approaches include:

- Competency-orientation for training content and priorities.
- Experiential learning character through hands-on training by “learning-by-doing”.
- Maturity-based training adequate to each company's digital maturity.

- Interrelationships and context (collaboration with customers and teams).
- State-of-the-art compliance (successful use cases).

Low-cost solutions in SMEs shall be addressed as well in terms of limited resource requirements for the training.

When it comes to more focused CS training, a review of the literature from Gkioulos et al. [12], shows that game-based methods can improve team skills, engage the user, and foster adaptability, scalability. They defined types of CS training as of table 1:

Table 1 Cybersecurity training types as of [12]–[14]

Type of CS training	Trainees	Description
Awareness training	All employees	Improved knowledge and understanding of integrated safety and security risks
Technical training	System engineers and CST	To boost the safety and security personnel's skills and qualifications
Specialized CS training	CST and CSIRT	Improved based on critical digital assets (CDAs) of nuclear facilities
Incident response and Recovery training	CSIRT and System engineers	Incident handing, incident monitoring, recovery, and reconfiguration

Beyond the CS training types in table 1, Gupta et al. [13] provide a more detailed justification of the particular CS training needs in the sectors of Nuclear Power Plant (NPP) security. According to them, integrated safety and security training should include awareness and technical training. The goal and outcome of the first should be to provide a general better understanding of safety and security (S&S) risks, as all personnel should bear some responsibility for S&S. Technical training should be used to complement current skills and qualifications and to define individuals' roles better. The main areas where technical training should have an impact are security testing, and the effects of security controls on safety. Lee et al. [14] conduct and define the Cybersecurity Team (CST) and Cybersecurity Incident Response Team (CSIRT) are both undergoing specialized cybersecurity training. The CST is currently focused on utilizing a test-bed built with CDAs specifically in nuclear facilities. Meanwhile, the CSIRT is tasked with detecting and analyzing cybersecurity incidents that may occur within nuclear facilities. Additionally, Hendrix et al. [15] conducted an in-depth survey of serious games for cybersecurity education. Fifteen games from industry and fourteen from academia were identified as used for training various target groups, from children to industry professionals.

Gaming and simulation techniques have long been used in the military for training and evaluation due to their effectiveness in training people and teams to make strategic decisions and plan in complex system with various variables. By providing students with positive learning experiences, interactive educational games can help to bridge this gap. Since the 1950s and 1960s, serious games have been utilized in business and management training. Serious games that combine gaming and learning allow users practice decision-making in complex systems [16]. Furthermore, the benefits of serious games for attracting students' attention and supporting them in memorizing what they have learned [17].

Industrial control and automation are complex subjects, including mathematics, logic programming, sensors, actuators, and electrical/mechanical components. Magalhães et al. [18] developed virtual systems, which are graphical computer models of dynamic systems. Thus, the advantage of these virtual systems was that they saved costs while still assuring environmental safety. A video game with rendered graphics and audio, connectivity, and attraction can enhance "situation awareness" and prepare users for learning in the real environment. Since 2008, Real Games has collaborated with the CReSTIC laboratory at Reims University to develop two serious games: HOME I/O and FACTORY I/O [19]. Home I/O is a real-time simulation software of a smart house and its surroundings that focuses on control and STEM (Science, Technology, Engineering, and Math) education. FACTORY I/O is a new 3D factory simulation software generation for learning automation technology. At this stage, we have worked with HOME I/O.

3. Research questions and Methodology

Based on the ICS training challenges, we have derived the following research questions (RQs):

- RQ1: What is an approach to training on PLC based ICS?
- RQ2: What specific contents/tools should be obtained on PLC based ICS?
- RQ3: What is the impact of simulation tools on PLC based ICS?

In Figure 1, we present an overview of our proposed training concept at the macro-level. The left column contains the lab contents, while the right column lists the corresponding training environments.

Initially, trainees will learn PLC fundamentals in a traditional classroom setting, where theoretical concepts will be presented without any practical lab work. Subsequently, the practical lab section will involve three techniques: guidance for lab content, the use of a simulation tool, and experiments with a physical PLC.

As trainees delve deeper into the PLC communication subject, they will encounter a complex environment that simulates a real-world industrial setting. This environment will be divided into three techniques: class, simulation, and lab.

The underlying hypothesis of our training concept is that traditional classroom training becomes inadequate as learners progress towards studying the setup of PLC-controlled processes and their cybersecurity. In a future article, we will explore this hypothesis and its impact on the blue parts of Figure 1. For now, this work focuses solely on the experimentation of the green parts.

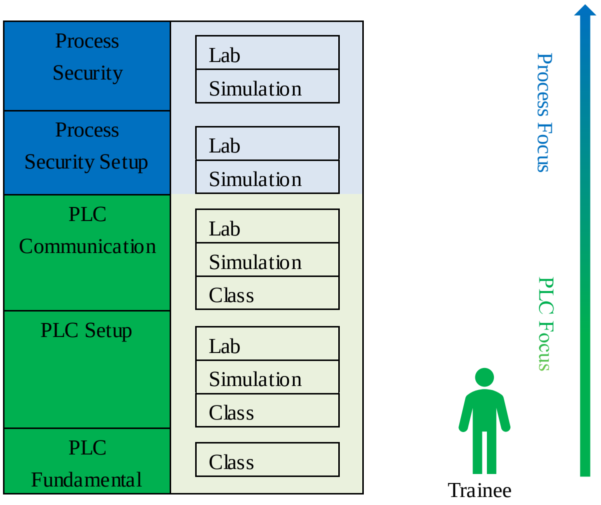

Fig. 1 A PLC cyber-security training concept

Next, collecting data on user feedback can help to evaluate the training's program content, delivery methods, accessibility, usability, and such improvement suggestions [12]. Thus, proposing the questionnaire allows us to analyze the need to prepare improvements in future research. Designing a questionnaire that motivates learners to respond is challenging. It requires being precise, concise, and still broad enough in order to get as much information on the training experience as possible. The questionnaire's focus is on questions which can cover four areas: attributes, behavior, attitudes, and beliefs [20]. In design, a questionnaire has four purposes: to collect data from respondents, provide structure for interviews, offer a standard format for recording answers and processing the collected data [21]. The sequence of questions in a questionnaire is an essential aspect of questionnaire design as well. Thus, how can one drive the respondents to go through all questions, and make them willing to answer all questions. Sreejesh et al. [21] propose the appropriate sequence of steps as follows: lead-in questions, qualifying questions, warm-up questions, specific questions, and demographics questions.

As mentioned, these procedures are some questions we have proposed to our respondents in this table 2:

Table 2 Questionnaire on lab's design

Topic	Question	Sequence type	Response format
Lab design	- How many hours did you spend in this lab?	Lead-in	Opened
	- Is it sufficient for your expectations?	Qualifying	Binary
	- How clear were the lab objectives, in your opinion?	Warm-up	Ranking
	- Did the structure and sequence of the lectures make sense?	Specific	Ranking
	- What change would make that better?	Specific	Opened

4. A first experimentation of the use of HOME I/O

To trial the fundamental part of the training concept, we proposed an experiment to 20 students with some prior PLC knowledge. The training environment was a large-scale implementation platform of the Hardware-in-the-Loop (HIL) system at G-ICS lab (GreEn-ER Industrial Control systems Sandbox), an industrial control systems research and teaching lab. G-ICS platform [22] is built upon the HIL architecture with more than 100 industrial devices (controller, protection relays, remote terminal units and industrial HMIs) from various industrial vendors such as Stormshield firewalls and Cisco CyberVision IDS. On the research side, some PhD students are working on intrusion detection as demonstrators. On the training side, this platform is used for electrical engineers' training and an advanced topic on master's degree.

For our initial experiment, we utilized a legitimate PLC joined to an emulation card, which can replicate any process. This card has an inserted Linux operating system, a network interface controller (NIC), digital and analog inputs-outputs, and a variety of LEDs and switches. The emulation card can interact with other installation devices, and the input-output interfaces permit a direct physical connection between the PLC and the emulation card. This allows for remote programming of PLCs and confirmation on the emulated system prior to sending the programmed PLC directly to the client's facility. The experimental content of the practical lab is referred to as the "SCADA project: Study of the Modbus protocol + HOME I/O." This project necessitates fundamental knowledge of PLCs, programming, supervisory software, and industrial CAN hardware. The objective of this project is to simulate a real-world scenario for students, allowing them to implement an industrial control supervision system. The lab is divided into 12-hour sessions and 4 hours each objective, as demonstrated in Table 3:

Table 3 SCADA project: Study of the Modbus protocol + HOME I/O content

Objectives	Practical task	Duration
1. Understanding the communication between PLC, HMI/SCADA, and HOME I/O	- The SCADA Modbus and HOME I/O, implementation of the PLC, programming PLC	4 hours
2. Implement and observe communication flows	- Test and validate a project on PLCs, emulation card, real games API, and HOME I/O	4 hours
3. Analyze the flows, optimize the communication	- Using HMI to control HOME I/O through PLC, analyzing by the Wireshark network monitoring	4 hours

As mentioned in table 3, the students work in a real industrial environment with a group of two on an industrial platform, including one Schneider's PLC, one HMI, two emulation cards, a switch and two remote units.

Figure 2 shows this lab's procedure as table 3 objectives on the data transmission chain from Home I/O to PLC, which will suffer several transformations. The overall process is presented:

1. Sensor value calibration is needed to ensure a maximal transmission accuracy of the process floating number represented values to the analog electrical inputs of the PLC. (Objective 1,2)
2. Starting in reverse order from the PLC digital input converted into analog electronic board. (Objective 1,2)
3. Calibration precisely converts the effective voltage range into 10 bits input format. They are automatically converted from the floating values in the process simulation software using the min and max values indicated in the GICS Engine IO interface. (Objective 1,2)
4. Receiving IP from the electronic board using an API real game adjusting controlling the digital IO inside the HOME I/O by using Wireshark to observe the communication. (Objective 1,2,3)

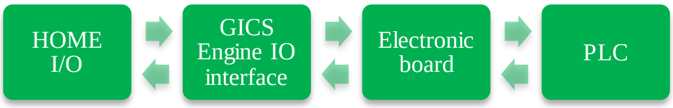

Fig. 2 Information transmission chain from process simulator to PLC

5. Discussion on the results from questionnaires

Table 2, the lab's design can lead all respondents to finish the questionnaire efficiently. Thus, the heart of the questionnaire is detailed and practical, with some evidence response to be analysed. On RQ1, A training approach on PLC-based ICS, it is important to focus on the fundamental of PLCs, industrial communication protocols, and innovative practical implementation. An innovative teaching methodology can be utilized to simplify complex subjects that may be difficult to learn in a traditional classroom setting. In addition, 77% of participants in this study offered feedback on a pedagogical schedule and content that did not meet their expectations. It is difficult to cover all the necessary content effectively in a 12-hour timeframe. Providing a clear guideline with structure and revising the lab content can improve the situation. On RQ2, there is a demand for improving the practical part of teaching of network communication between PLC, HOME I/O, HMI, and the emulation card, which provides an orientation for how theoretical and practical contents can be explored. In addition, all simulation tools, such HOME I/O, unity pro, GICS Tester let trainees understand more about the complex subjects. However, a clear guideline on each program must be provided to save time constraints. On RQ3, the list of questions has been compiled as follows:

Q1: The simulation (HOME I/O, unity pro, GICS Tester) helps you understand better?

Q2: How efficient are the physical PLC and GICS card (emulation card) you used?

Q3: What is the gap between simulation and the physical world?

Q4: Where are the gaps between simulation and practical training?

Q5: The simulation benefited you because...

Answers can be summarized as follows:

- Positive perception of simulation tools.
- The pedagogical sequence, in terms of which content needs to be taught before another one, needs to be investigated, in particular when both theoretical and practical parts are mixed.
- The use of simulation tools was considered very useful, however the long lead-times due to quite complex setup procedures compromised the training experience.
- A visual representation of the relationship of the PLC, HOME I/O, and the emulation cards was desired.
- A demonstrator showing how the PLC, HOME I/O, and the emulation cards are working together would have been highly appreciated.
- Simulation allows to circumvent hardware tool issues.
- Simulation tools take the fear of breaking anything when trying things out for experimental learning.
- Less theoretical class for more simulation and practical labs are desired. Classes should be more focused on preparing the students for using the tools in the lab.

Generally, the results show a positive impact of the training using simulation tools, PLC, and industrial network communication. All the students are in favor of re-iterating this PLC training experiment, however with some improvements mainly on the clear guidance on simulation and hardware tools, hardware fixing, and enjoyable learning scenarios. The fact that the learning cycles span over three different environments (classroom, simulation, lab) challenge the partitioning of the learning content and related training documentation.

6. Conclusion and future works

This article proposes a training concept for PLC-based ICS with a focus on Cyber-security. The key characteristic of this concept is that it mixes the three different training environments, classroom, simulation, and laboratory. Moreover, it proposes a ludic approach to teaching the setup, operation, and attack & defense of ICs.

In the small-scale student experiment presented in this article, we identified some particular challenges in implementing such a concept, in particular with respect to the repartition of teaching scope, content, and materials on the three different environments. While the use of simulation and real lab equipment has been much appreciated by students, the partly long setup times, as well as configuration and hardware issues hampered the training experience in the practical environments.

In the next step, we will implement the entire concept in terms of proposing ludic CS training scenarios to students without any prior CS knowledge and experience. This is planned to a be core education element of the Asean-Factori 4.0 project [23], where both university standas and people from industry need to be upskilled for Industry 4.0 skills in PLC-based ICS. We will compare the effectiveness of teaching PLC and CS knowledge and skills in a combination of classroom, simulation, and lab environments with respect to classical classroom teaching. Serios games will play a major role in this analysis, driven by both physical ICS hardware, and simulation facilities.

Acknowledgments

This paper is partly based on a project co-funded by the ERASMUS+ Program of the European Union: Asean Factori 4.0, Across South East Asian Nations: From Automation and Control Training to the Overall Roll-out of Industry 4.0, 609854-EPP-1-2019-1-FR-EPPKA2-CBHE-JP.

Thanks to Asst. Prof. Stephane Mocanu on a G-ICS lab platform (GreEn-ER Industrial Control systems Sandbox) to allow us to experiment on this article.

References

[1] P. Matoušek, "Security of Smart Grid Communication," Brno University of Technology, Brno, 2021. Accessed: Jan. 30, 2023. [Online]. Available: https://www.fit.vut.cz/research/publication/12593/.en

[2] T. D. Tran, J.-M. Thiriet, N. Marchand, and A. El Mrabti, "A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category," *J Intell Robot Syst*, vol. 104, no. 1, p. 4, 2022, doi: 10.1007/s10846-021-01512-0.

[3] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015. doi: 10.6028/NIST.SP.800-82R2.

[4] STEVE. MUSTARD, *Industrial Cybersecurity : Case Studies and Best Practices*. INSTRUMENT SOCIETY OF AME, 2022.

[5] "Definition of Information Technology (IT) ," *Gartner Information Technology Glossary*. https://www.gartner.com/en/information-technology/glossary/it-information-technology (accessed May 01, 2023).

[6] "Definition of Operational Technology (OT) ," *Gartner Information Technology Glossary*. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (accessed May 01, 2023).

[7] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015. doi: 10.6028/NIST.SP.800-82r2.

[8] S. Keaveney, L. Athanasopoulou, V. Siatras, P. Stavropoulos, D. Mourtzis, and D. P. Dowling, "Development and Implementation of a Digital Manufacturing Demonstrator for Engineering Education," *Procedia CIRP*, vol. 104, pp. 1674–1679, Jan. 2021, doi: 10.1016/J.PROCIR.2021.11.282.

[9] H. Images Inc and A. Stock Photo, "Global Industry 4.0 Survey: Building the digital enterprise," 2016. Accessed: May 01, 2023. [Online]. Available: www.pwc.com/industry40

[10] C. Kuhn and D. Lucke, "Supporting the Digital Transformation: A Low-Threshold Approach for Manufacturing Related Higher Education and Employee Training," *Procedia CIRP*, vol. 104, pp. 647–652, Jan. 2021, doi: 10.1016/J.PROCIR.2021.11.109.

[11] M. Hulla, P. Herstätter, M. Wolf, and C. Ramsauer, "Towards digitalization in production in SMEs – A qualitative study of challenges, competencies and requirements for trainings," *Procedia CIRP*, vol. 104, pp. 887–892, Jan. 2021, doi: 10.1016/J.PROCIR.2021.11.149.

[12] V. Gkioulos and N. Chowdhury, "Cyber security training for critical infrastructure protection: A literature review," *Comput Sci Rev*, vol. 40, p. 100361, May 2021, doi: 10.1016/J.COSREV.2021.100361.

[13] D. Gupta, E. Bajramovic, H. Hoppe, and A. Ciriello, "The need for integrated cybersecurity and safety training," *Journal of Nuclear Engineering and Radiation Science*, vol. 4, no. 4, Oct. 2018, doi: 10.1115/1.4040372/366333.

[14] J.-W. Lee, J.-G. Song, and C.-K. Lee, *Study on Nuclear Facility Cyber Security Awareness and Training Programs*. 2016.

[15] M. Hendrix, A. Al-Sherbaz, and V. Bloom, "Game Based Cyber Security Training: are Serious Games suitable for cyber security training?," *International Journal of Serious Games*, vol. 3, no. 1, 2016, doi: 10.17083/ijsg.v%vi%i.107.

[16] D. M. Qualters, J. Isaacs, T. Cullinane, J. Laird, and A. McDonald, "A Game Approach to Teach Environmentally Benign Manufacturing in the Supply Chain," *International Journal for the Scholarship of Teaching and Learning*, vol. 2, no. 2, Jul. 2008, doi: 10.20429/IJSOTL.2008.020214.

[17] H. M. Neck and P. G. Greene, "Entrepreneurship Education: Known Worlds and New Frontiers," *Journal of Small Business Management*, vol. 49, no. 1, pp. 55–70, Nov. 2011, doi: 10.1111/j.1540-627X.2010.00314.x.

[18] A. P. de Magalhães, B. Riera, and B. Vigário, "When control education is the name of the game," *Computer Games as Educational and Management Tools: Uses and Approaches*, pp. 185–205, 2011, doi: 10.4018/978-1-60960-569-8.CH012.

[19] B. Riera and B. Vigário, "HOME I/O and FACTORY I/O: a virtual house and a virtual plant for control education," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9144–9149, Jul. 2017, doi: 10.1016/J.IFACOL.2017.08.1719.

[20] S. Lydeard, "The Questionnaire as a Research Tool," *Fam Pract*, vol. 8, no. 1, pp. 84–91, Mar. 1991, doi: 10.1093/FAMPRA/8.1.84.

[21] S. Sreejesh, S. Mohapatra, and M. R. Anusree, "Questionnaire Design," *Business Research Methods*, pp. 143–159, 2014, doi: 10.1007/978-3-319-00539-3_5.

[22] M. Puys, P. H. Thevenon, S. Mocanu, M. Gallissot, and C. Sivelle, "SCADA cybersecurity awareness and teaching with Hardware-In-The-Loop platforms," *J Wirel Mob Netw Ubiquitous Comput Dependable Appl*, vol. 13, no. 1, pp. 4–32, Mar. 2022, doi: 10.22667/JOWUA.2022.03.31.004.

[23] K. Thourn, B. Kim, V. Vai, S. Am, J.-M. Thiriet, and H. Yahoui, "Curricula Improvement of Undergraduate Program in Electrical Engineering Department at ITC Under ASEAN Factori 4.0 Project," in *Conf ICA-SYMP-2023*, Bangkok, 2023.