A Gamification Approach to Teaching Cybersecurity in CPS

Kanthanet Tharot, Andreas Riel, Jean-Marc Thiriet

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 128 (2024) 799–803

www.elsevier.com/locate/procedia

34th CIRP Design Conference

A Gamification Approach to Teaching Cybersecurity in CPS

Kanthanet Tharot[a,b], 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. E-mail address: kanthanet.tharot@grenoble-inp.fr

Abstract

With the implementation of the Industrial Internet of Things (IIoT) in modern manufacturing environments, Cybersecurity has become an outstanding challenge in the design and daily operation of networked Industrial Control Systems (ICS). While Cybersecurity is an expert domain on its own, designers and operators of such Cyber-physical Systems (CPS) need to acquire at least a fundamental understanding of Cybersecurity concepts in order to contribute to the integration of such concepts both in design and operational processes. The fact that such Cybersecurity concepts have been originally established in the Information Technology (IT) domain makes knowledge transfer to stakeholders in the mostly mechanical and Operational Technology (OT) an educational challenge on its own. This paper proposes a ludic approach to teaching fundamental Cybersecurity concepts to stakeholders without any or only little prior IT knowledge. The key methodology relies on designing game scenarios that help convey Cybersecurity terminology and concept knowledge in a ludic form before letting students actually apply them in a physical CPS environment. While this basic idea is not new, the originality of our proposed approach lies in the novel combination of existing, validated Cybersecurity teaching resources to design and implement such scenarios, and in complementing those with learning on real CPS environments. The feasibility of our approach has been demonstrated in a case-study that has delivered very promising results with respect to the potential power and effectiveness of our method.

Keywords: Cybersecurity education ; ICS cybersecurity ; Design education

1. Introduction

In the ever-changing manufacturing industry today, the use of the Industrial Internet of Things (IIoT) has led to many advancements and opportunities [1]. However, with them, also comes the important issue of cybersecurity in the design and operation of networked Industrial Control Systems (ICS) [2]. Cybersecurity has become a crucial area, demanding the attention of designers and operators of Cyber-Physical Systems (CPS) in order to ensure the integrity and security of these interconnected systems [3] .

In the field of industrial cybersecurity, it is crucial to address the distinct priorities that exist between IT (Information Technology) [4] and OT (Operational Technology) [5]. These two domains have different focuses and requirements when it comes to protecting critical infrastructure and preventing cyber threats.

To address this challenge, this paper proposes a ludic approach to teaching fundamental cybersecurity concepts to participants with little or no prior IT knowledge. We have designed five role-play based-scenarios and initially implemented them with students from different backgrounds. By engaging students in interactive and immersive game-based scenarios, they are able to grasp and internalize cybersecurity principles before applying them in a physical CPS environment.

While the idea of using games for educational purposes is not new, the originality of this proposed approach relies on the innovative combination of existing [6], validated cybersecurity teaching resources to design and implement game scenarios [7].

10.1016/j.procir.2024.06.039

This approach is further strengthened by complementing these scenarios with real CPS learning experiences, providing students with practical exposure to cybersecurity challenges in industrial settings.

The feasibility and effectiveness of this approach have been proven through role-play based-scenarios. These scenarios have shown promising results by combining game-based learning with real-world ICS environments, implementing the ludic approach to industrial cybersecurity. This innovative method offers an engaging and effective way to educate participants about cybersecurity concepts [8] and enables them to explore the subject further and apply it to their specific situation.

Thus, we have derived the following research questions (RQs):

- How to design ludic scenarios for teaching cybersecurity principles to learners without any prior cybersecurity knowledge?
- How to deploy such ludic scenarios in ICS environments?

In the upcoming sections of this paper, we examine the gamification method that we propose for teaching cybersecurity in CPS in a greater depth. Additionally, we describe the training methodology. Next, we present the experimental role-play scenarios that we use in order to introduce student groups to ICS cybersecurity concepts. Moreover, we elaborate on a more thorough explanation of the game instructions and analyze the results using pre- and post-questionnaires. Lastly, we summarize this concept and present some future perspectives.

Nomenclature

CPS	Cyber-Physical System
ICS	Industrial Control System
IIOT	Industrial Internet of Things
IT	Information Technology
MitM	Man-in-the-middle
OT	Operational Technology
PLC	Programmable Logic Controller

2. Related Works

In recent years, the use of gamification has gained significant attention as an effective approach for teaching cybersecurity concepts in the context of ICS. Gamification offers a unique and engaging learning experience that enhances user motivation [9], knowledge retention, and practical application of cybersecurity principles. This section briefly introduces the area based on a few outstanding works:

2.1. Gamification in Cybersecurity Education

Gamification involves the application of game design elements and principles in non-game contexts, such as education [10]. It has been widely recognized as an innovative [8] and effective approach to enhance learning outcomes in various domains, including cybersecurity. Gamification provides a motivating and interactive learning environment that encourages active participation, problem-solving, and skill development [11].

2.2. Application of Gamification in Industrial Control Systems

Gamification has been applied in various contexts, such as ICS on the shop floor [12] and in education [10], to teach and reinforce cybersecurity concepts. By simulating realistic scenarios and challenges, gamified platforms provide hands-on experiences that enable learners to develop practical skills and a deep understanding of cybersecurity principles specific to ICS environments.

2.3. Design Principles for Gamified Cybersecurity Education

Effective gamification of cybersecurity education in ICS requires careful consideration of design principles to ensure optimal learning outcomes [13]. These principles involve using meaningful stories [8], clear goals, feedback systems [7], progressive challenges, and rewards to motivate learners and create a sense of accomplishment.

2.4. Assessment and Evaluation of Gamified Cybersecurity Education

To ensure the effectiveness of gamified cybersecurity education in ICS, assessment and evaluation play a crucial role [7]. Various methods, such as performance-based assessments, self-assessments, and feedback mechanisms, can be employed to measure learners' progress [14], identify areas for improvement, and provide personalized learning experiences.

3. Methodology

In our comprehensive methodology, we initiated the training process by providing a solid foundation in PLC through basic training. This initial step served as a building block for the development of our training program, which focuses on PLC-based ICS and places a strong emphasis on cybersecurity. Our program incorporates three distinct training environments, namely the classroom, simulation, and laboratory [15], to ensure a well-rounded and immersive learning experience for participants.

Our approach, as depicted in Fig. 1, revolves around an interactive and hands-on teaching methodology. We strive to equip learners with the necessary knowledge and skills to effectively set up [16], operate, and attacks & defenses of ICS systems. To achieve this, we have focused our efforts on the creation of engaging security scenarios that will serve as effective teaching tools. These scenarios have been designed with a playful approach, keeping in mind the importance of maintaining student engagement throughout the training process.

In addition to scenario development, we have been conducting experiments using gamification techniques. By incorporating elements of game design and mechanics, we aim to enhance the overall training experience and ensure that learners remain fully engaged and motivated. Through these gamified experiments, we can evaluate the effectiveness of our training program and make any necessary adjustments to optimize its impact.

Furthermore, we have delved into the intricate process of setting up and deploying the training program for teaching purposes. This step involves careful consideration and validation of the entire concept, ensuring its practicality and suitability for real-world implementation. By following a systematic approach, we have outlined the following procedures:

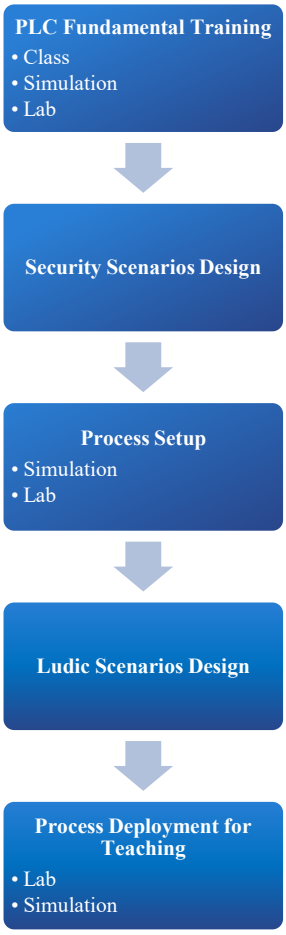

Fig. 1 The cybersecurity training concepts based-ICS [15], [16]

- Comprehensive PLC fundamental training to provide learners with a solid understanding of the underlying principles [15].
- Designing and developing security scenarios that encompass a wide range of potential cyber threats and challenges.
- Setting up the necessary processes and infrastructure to create a conductive learning environment [16].
- Devising ludic scenarios that combine educational elements with a playful approach, further enhancing learner engagement.
- Finally, deploying the training program for teaching purposes, allowing learners to gain practical experience and apply their newfound knowledge in a controlled and supportive environment.

By following these steps, our objective is to create a ludic approach for teaching in the field of industrial cybersecurity and ultimately deploy and validate this concept for teaching purposes.

4. Scenario Design

In the immersive role-play scenario depicted in Fig. 2, participants have the opportunity to explore the exciting field of cybersecurity in ICS.

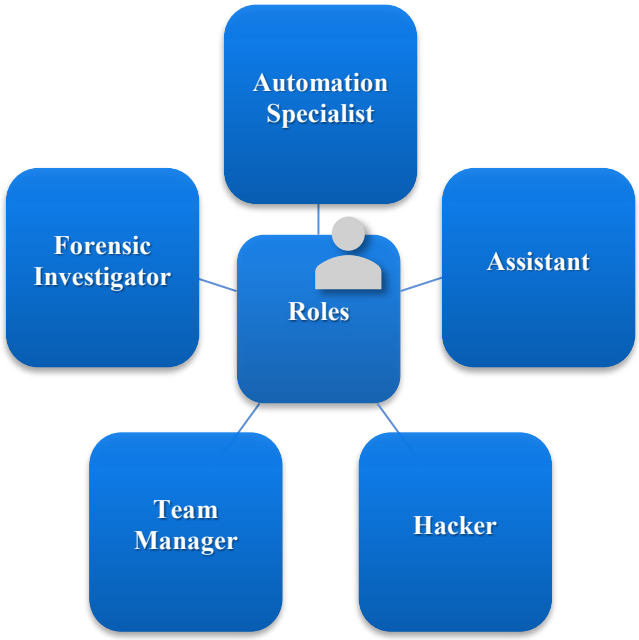

Fig. 2 Role-play scenarios based-gamification

Through interactive activities and by assuming different roles, participants will develop a comprehensive understanding of the vulnerabilities of PLC systems and learn effective measures to protect ICS from cyber threats. There are five roles as follows in the Table 1:

Table 1. Comparative analysis of each role

Role	Main Focus	Learning Outcome
Automation Specialist	Configuring a simulated ICS environment, enhancing password security	Gained hands-on experience in securing ICS components against cyber threats
Assistant (Red Team)	Cracking passwords in web-based scenarios on the picoCTF platform	Appreciated the significance of strong password security and the potential risks associated with weak passwords
Hacker	Attacking the Siemens PLC system, employing man-in-the-middle (MitM) techniques, manipulating microcontrollers	Enhanced knowledge in attacking techniques, developed effective communication and reporting skills
Team Manager	Overseeing the entire audit process, documenting each step	Gained practical experience in reporting and effectively communicating audit findings
Forensic Investigator	Understanding recognized frameworks of STRIDE and MITRE ATT&CK	Developed practical skills in investigating and mitigating security breaches in ICSs

Our decision to focus on the Man-in-the-Middle (MitM) scenario, as well as the roles we have chosen to explore, are grounded in real-world cybersecurity incidents and are reflective of the industrial production line platform at our platform. In order to provide a more tangible and practical understanding of such incidents, we have conducted a series of

experiments on our platform, simulating MitM attacks. These types of attacks are not only common, but also carry significant weight in the realm of industrial cybersecurity, as the infamous Stuxnet incident has shown us. In the pursuit of a deeper comprehension of the cybersecurity landscape, we've selected roles that represent a wide spectrum of responsibilities and perspectives.

By introducing detailed scenarios about MitM attacks, we strive to deliver an in-depth understanding of these threats, their possible effects, and the required countermeasures. Moreover, collaboration criteria in Table 2 for these roles involve clear communication, mutual respect, understanding of individual role responsibilities, and ability to work together toward common objectives. This emphasis improves the practical relevance of our training, particularly in the hacker role, and aligns with our objective of establishing an effective and realistic learning environment.

Table 2. Role interactions and collaborations based-MitM

Role	Interaction	Collaboration
Automation Specialist	Sets up and configures the ICS environment. Designs and implements security measures	Collaborates with other roles to ensure the security of the ICS environment
Assistant (Red Team)	Learns how to crack passwords, gains practical experience in password cracking	Collaborates with the Hacker by understanding and potentially exposing weak spots in the system
Hacker	Attacks the ICS system, employs MitM techniques, and manipulates microcontrollers to analyze vulnerabilities	Collaborates with forensic investigators to understand the effects and implications of the attack
Team Manager	Oversees the audit process, records the time taken and techniques employed	Collaborates with all roles, provides oversight, and ensures effective communication and documentation of processes
Forensic Investigator	Uses the frameworks to identify and analyze security threats	Collaborates with the Hacker to understand the attack and develops mitigation strategies

The selection of the roles such as Automation Specialist, Assistant, Hacker, Team Manager, and Forensic Investigator is guided by the requirements of a practical platform within a production line environment. Each of these roles serves a specific function necessary for the operation, security, and management of the production line. The Automation Specialist is responsible for overseeing and maintaining the automated systems within the production line. The Assistant supports the specialist and the team in their tasks. The Hacker role is crucial for simulating potential cybersecurity threats, providing valuable insights into vulnerabilities and areas for improvement. The Team Manager ensures smooth collaboration and efficient workflow among the team members. Finally, the Forensic Investigator examines incidents to determine causes and potential solutions, using the frameworks of MITRE ATT&CK and STRIDE.

5. Game instruction, evaluation, and result

During the immersive game instruction session in Table 3 for industrial cybersecurity, participants are engaged in a series of role-play tasks.

Table 3. Cybersecurity role-play session activities

Activity	Description	Duration
Pre-survey	Gathering initial information, pre-requisites, and expectations of learners	
Role-Play Tasks for Learning	The main activity of the session involved role-playing scenarios related to industrial cybersecurity. The participants engaged in various tasks, including an introduction (5 minutes), scenario overview (10 minutes), role-play scenarios (30 minutes), documentation and reporting (10 minutes), and wrap-up and reflection (5 minutes)	1 hour
Post-survey	Gathering feedback and assessing effectiveness of the session	

We have implemented this game with a total of 51 students from Thailand and France. The participants have had diverse educational backgrounds, as Table 4 below:

Table 4. Participant educational background

Participant Background	Number of Participants (n)
Bachelor's degree in Computer Engineering from Mae Fah Luang University, Chiang Rai, Thailand	26
Master's Degree in Computer Engineering from Mae Fah Luang University, Chiang Rai, Thailand	2
Master in microelectronics integration of embedded real-time systems from UGA - UFR PhITEM, Grenoble, France	23

Upon analyzing the results of the questionnaires, it was found that 90.2% of participants (n=51) expressed their willingness to recommend the serious game to others. This indicates a high level of satisfaction and endorsement for the game. Furthermore, the overall experiences with the serious game received positive feedback, with 29.4% of participants providing an excellent score (5 out of 5) and 58.8% providing a good score (4 out of 5). In Table 5 following, we analyse feedback per role:

Table 5. Role-Based Feedback based gamification

Role	Feedback
Automation Specialists (n=7)	Positive feedback on the usefulness for programming and learning about cybersecurity. Valued the opportunity to work with real programs and equipment. Found the emphasis on timeliness in ICS environments effective
Assistant (Red Team) (n=12)	Enjoyed cracking passwords and were competitive. However, their focus seemed to be solely on the IT domain
Hacker (n=13)	Appreciation for learning about ICS through serious games. Some participants felt they lacked the necessary knowledge to fully understand the activities
Team Manager (n=10)	Found the game helpful in gaining knowledge and improving skills in managing teams and dealing with cybersecurity incidents
Forensic Investigator (n=9)	Positive feedback on their learning and acquisition of knowledge in mitigation strategies. Expressed a desire for more engaging activities

6. Conclusion, limitations, outlook

In conclusion, the gamification approach has emerged as a promising method for teaching cybersecurity in ICSs. By applying game design elements and principles, gamified scenarios applied in ICS environments provide engaging and interactive learning experiences that enhance learners' understanding and practical application of cybersecurity concepts specific to ICS environments.

The evaluation of this concept using pre- and post-questionnaires provided valuable insights into the effectiveness of the immersive game instruction session for industrial cybersecurity. The overwhelmingly positive feedback and high recommendation rate from participants demonstrate the session's success in enhancing participants' understanding and skills in the field.

The role-play tasks enabled participants to engage in hands-on activities and simulate real-world scenarios, developing practical skills and knowledge in industrial cybersecurity. The session covered key topics including ICS security, password cracking, ethical hacking, and forensic investigation.

However, it is important to note the limitations of this work. The one-hour duration may have limited exploration and practice in some areas. The session's effectiveness may vary depending on participants' prior knowledge and experience in industrial cybersecurity. Customization and adaptation may be needed to meet the specific needs of different participants and learning outcomes.

While our focus in this study was primarily on role-playing games, we recognize the value of incorporating more visual aids and gamification elements. Feedback suggests that these elements could offer a more tangible understanding of our approach. As part of our future work, we aim to expand the use of such features to further enhance the learning experience in cybersecurity education.

Enhancements to the industrial cybersecurity program include adding more role-play scenarios and hands-on activities, incorporating real-world case studies, and collecting ongoing feedback. Future work will assess the long-term impact of the program, update content regularly, and re-evaluate the effectiveness of the training methods, including the incorporation of more scenarios based on the latest developments in recognized cybersecurity monitoring frameworks like MITRE ATT&CK.

Acknowledgements

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.

References

[1] O. Peter, A. Pradhan, and C. Mbohwa, “Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies,” *Procedia Comput Sci*, vol. 217, pp. 856–865, Jan. 2023, doi: 10.1016/J.PROCS.2022.12.282.

[2] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” *Comput Secur*, vol. 89, p. 101677, 2020, doi: https://doi.org/10.1016/j.cose.2019.101677.

[3] M. R. Asghar, Q. Hu, and S. Zeadally, “Cybersecurity in industrial control systems: Issues, technologies, and challenges,” *Computer Networks*, vol. 165, p. 106946, Dec. 2019, doi: 10.1016/J.COMNET.2019.106946.

[4] “Definition of Information Technology (IT) ,” Gartner Information Technology Glossary. Accessed: May 01, 2023. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/it-information-technology

[5] “Definition of Operational Technology (OT) ,” Gartner Information Technology Glossary. Accessed: May 01, 2023. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[6] 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, Mar. 2016, doi: 10.17083/ijsg.v3i1.107.

[7] S. Kulshrestha, S. Agrawal, D. Gaurav, M. Chaturvedi, S. Sharma, and R. Bose, “Development and Validation of Serious Games for Teaching Cybersecurity,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12945 LNCS, Springer Science and Business Media Deutschland GmbH, 2021, pp. 247–262. doi: 10.1007/978-3-030-88272-3_18.

[8] A. Arora and A. Mendhekar, “Innovative Techniques for Student Engagement in Cybersecurity Education,” in *Data Management, Analytics and Innovation*, N. Sharma, A. Chakrabarti, V. E. Balas, and J. Martinovic, Eds., Singapore: Springer Singapore, 2021, pp. 395–406.

[9] C. Dichev and D. Dicheva, “Gamifying education: what is known, what is believed and what remains uncertain: a critical review,” *International Journal of Educational Technology in Higher Education*, vol. 14, no. 1, p. 9, Dec. 2017, doi: 10.1186/s41239-017-0042-5.

[10] D. Dicheva, C. Dichev, G. Agre, and G. Angelova, “Gamification in Education: A Systematic Mapping Study,” *J. Educ. Technol. Soc.*, 2015.

[11] G. Bassi, S. Fabbri, and A. Vaccarelli, “Cybersecurity Education: a Gamification Approach,” *Conference Proceedings. The Future of Education 2023*, Jun. 2023.

[12] R. Sochor, J. Schenk, K. Fink, and J. Berger, “Gamification in industrial shopfloor – development of a method for classification and selection of suitable game elements in diverse production and logistics environments,” *Procedia CIRP*, vol. 100, pp. 157–162, Jan. 2021, doi: 10.1016/J.PROCIR.2021.05.024.

[13] Z. Batzos *et al.*, “Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview,” *Authorea Preprints*, Oct. 2023, doi: 10.36227/TECHRXIV.22650952.V1.

[14] A. De Gloria, F. Bellotti, and R. Berta, “Serious Games for education and training,” *International Journal of Serious Games*, vol. 1, no. 1, Feb. 2014, doi: 10.17083/IJSG.V1I1.11.

[15] K. Tharot, Q. B. Duong, A. Riel, and J. M. Thiriet, “A Cybersecurity Training Concept for Cyber-physical Manufacturing Systems,” *Procedia CIRP*, vol. 120, pp. 1375–1380, Jan. 2023, doi: 10.1016/J.PROCIR.2023.09.179.

[16] K. Tharot, Q. B. Duong, A. Riel, and J. M. Thiriet, “A Low-Cost Environment for Teaching Fundamental Cybersecurity Concepts in CPS,” *Communications in Computer and Information Science*, vol. 1890 CCIS, pp. 356–365, 2023, doi: 10.1007/978-3-031-42307-9_25.