Open Access License Notice

Cyber-physical Shooting Gallery: Gamification to Address the IT-OT Gap in Cybersecurity Education

Tiffany Fuhrmann
Dept. of Computer Science
University of Idaho
Idaho Falls, Idaho, USA
0000-0003-0196-4787

Taegan Williams
Dept. of Computer Science
University of Idaho
Idaho Falls, Idaho, USA
0000-0003-0434-1040

Dr. Michael Haney
Dept. of Computer Science
University of Idaho
Idaho Falls, Idaho, USA
0000-0003-2359-2478

***Abstract*—While much has been written on the dire need for workers who understand both the IT and OT core concepts necessary to protect the cyber-physical systems of critical infrastructure, practical and specific recommendations for how to meet this need through education and workforce training are lacking. Many of the available programs for teaching cybersecurity of physical systems rely on virtual simulations and students may not encounter relevant physical equipment until they are in the workplace. RADICL's Cyber-physical Shooting Gallery is a critical missing piece toward a comprehensive system to develop the competent workforce the nation needs. Through a series of cyber-physical capture-the-flag challenges that integrate the Purdue ICS Model with the MITRE ATT&CK framework, the Cyber-physical Shooting Gallery provides an accessible educational model for cyber-physical security education and training.**

Keywords—Cyber-physical systems, gamification, OT CTF, cybersecurity, pedagogy, critical infrastructure, Purdue Model, MITRE ATT&CK, PLCs, Raspberry Pi, Arduino, electronics, industrial cybersecurity, workforce development

I. INTRODUCTION: BUILDING A PURPLE UNICORN

In May of 2022, the Idaho National Laboratory's Industrial Cybersecurity Community of Practice (ICSCOP) held an education and training workshop titled 'Developing Industrial Cyber Personnel Instead of Chasing Purple Unicorns'. Researchers, government officials, and industrial leaders spoke on the pressing and difficult problem of finding the "purple unicorn"–namely, workers who can bridge the skills, education, and cultural divide between information technology (IT) that is largely centered on data and operational technology (OT) that is the world of monitoring and controlling physical systems. Indeed, as of 2018, over a decade after Stuxnet and years after the world watched cyberattacks bring down Ukraine's power grid, there were only two programs out of the more than 200 National Centers for Academic Excellence in Cyber Defense (NCAE-CD) that qualified with an Industrial Control Systems focus [1]. According to Ralph Ley, manager of Workforce Development and Training at Idaho National Laboratory, "If cybersecurity is among the top national security concerns faced by the nation, industrial cybersecurity must be the single most critical overlooked educational topic" [2].

Standard programs in cybersecurity typically have very little if any exposure to "getting your hands dirty" with real physical equipment. Likewise, technical and vocational training programs traditionally have little emphasis on cybersecurity training. This gap needs to be addressed from both directions, both in education and in the workplace. In recent years, several virtual simulations have been developed to teach security of cyber-physical systems and critical infrastructure [3], [4]. While these simulation games have been well-received with students and provide important multidisciplinary experience with complexity that is not otherwise available, they lack actual interaction with the physical components themselves. As Dr. Sean McBride, a leader in researching and advocating for improvements in ICS cyber-physical education, says, "It may be difficult to commence a career securing devices that one has never before seen, let alone never handled and experienced" [5].

There have been recent efforts to address this need for hands-on training in ICS cybersecurity. LICSTER is a low-cost, open source testbed developed by researchers at the Hochschule Augsburg in Germany that uses a model conveyor belt and punching machine to demonstrate a series of attack scenarios [6]. KYPO4INDUSTRY is an ICS training laboratory in the Czech Republic that includes a simulated industrial environment for courses that require the students to study attacks and develop their own game scenarios [7]. This paper presents the RADICL Cyber-physical Shooting Gallery which aims to provide an engaging, replicable platform for students to gain hands-on experience with the security challenges of real cyber-physical systems.

II. DEVELOPING A CYBER-PHYSICAL EDUCATIONAL ENVIRONMENT

A. RADICL

The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) is a hands-on educational and research computing laboratory that has been evolving to meet the needs of new cybersecurity challenges since its creation at the University of Idaho in 2004 [8], [9]. Funding

from the state of Idaho and grants from NSF have enabled it to develop an isolated and controlled environment for students and researchers to engage in realistic attack and defense scenarios working with actual malware in real-time, while also creating data sets for additional research and learning. Adding the additional capability for hands-on cyber-physical attack and defense will make RADICL a unique environment poised to help fill the IT-OT gap in current cybersecurity education.

B. Cyber-physical Shooting Gallery

The Cyber-physical Shooting Gallery consists of a series of small-scale platforms hung on the walls around the laboratory, providing targets with real physical responses as students attempt attack and defense techniques. The goal is to provide a reconfigurable introductory platform for studying the security of cyber-physical systems. The challenges are designed with a low bar and high ceiling, enabling students and workers to become more comfortable with the crossover between IT and OT and begin to understand the threat model of industrial control systems (ICS). The platforms provide a progression of challenge for students to gain experience with a variety of physical systems and their controls, the logic of the cyber kill chain as applied to cyber-physical systems, the significance of network segmentation and the Purdue ICS Model, and some of the relevant methods of attack and defense.

C. The Gaming Platform

a) Standardized: Each platform in the Cyber-physical Shooting Gallery is self-contained on a 16” by 32” metal pegboard that can be hung on a wall or set up on a table with a stand. The top half of the platforms are standardized to enable a streamlined process for creating new OT challenges and to provide some familiarity for students as they work through the challenges. The authors have also developed a template for planning the attack surface and designs for new platforms, making it possible for others to more easily contribute a design for a new cyber-physical challenge.

Standard with each platform:

- Small monitor with remote control
- Keyboard with touchpad (wireless)
- PoE 5-port Switch (4 PoE ports, 1 ethernet port for uplink)
- Din rails and Din rail mounts
- 2 Raspberry Pis
- 1 Arduino or other microcontroller
- 1 PLC (Controllino mini, Controllino maxi, Click Koyo, or other advanced industrial model)
- 1 optocoupler multi-channel relay
- Surge protector (three outlet, two usb)
- Industrial signal light tower with alarm (green to signify when the system is active, yellow when the system is under attack, and red for a successful system breach)
- Breadboard
- Ethernet and various power cables
- POE splitters
- Room for additional cyber-physical device(s)
- QR code to link to documentation such as device manuals and hints

b) Reconfigurable: The lower half of the board is reserved for a unique cyber-physical system that students can attempt to attack and see a real-world physical response. For the prototype example, this was simply a badge reader and light bulb. Once students manage to access the system, they attempt to find a way to gain authorization to light the bulb. Both the physical system itself and the pathway to attacking the system are reconfigurable.

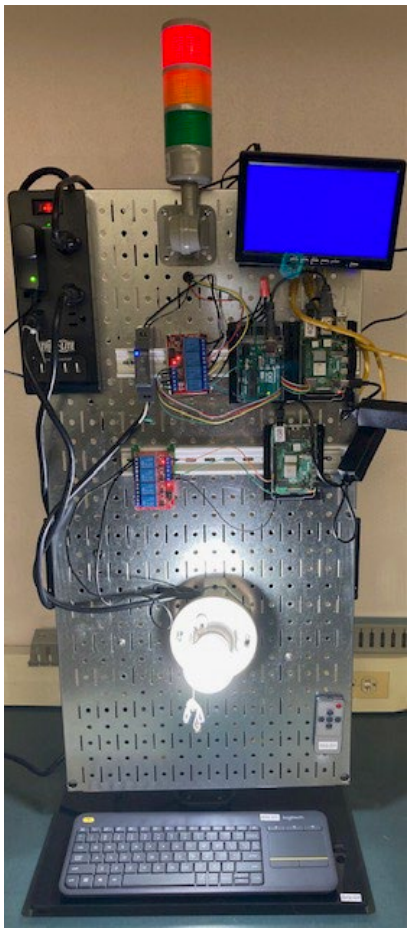

Fig. 1. Cyber-Physical Shooting Gallery Platform Prototype

In the prototype scenario (Fig. 1), the student may begin by identifying a gateway to the system which is represented by a small web server on one of the Raspberry Pis. The gateway web page offers a simple description of the system

and an innocuous looking login prompt. However, by viewing the source code for this homepage, the attacker may discover HTML comments which include the default username and password to log in, a scenario that is unfortunately not unlike the real world. Once logged in, the attacker is then presented with a simplified Human-Machine Interface (HMI) which offers control of the light bulb, or an administration page which allows the user to add arbitrary badge reader credentials. These vulnerabilities then allow the attacker to place their own physical badge number into the authorization database, or bypass the badge reader and simply turn the light bulb on or off electronically. The scenario is extensible by adding routines for blinking or dimming the light bulb to match various patterns or set-points. These routines may be pre-loaded and selected by the attacker or customized through a programmable "engineering workstation" interface that is hosted on the internal Raspberry Pi. As such, a variety of real-world examples can be modeled using very basic electronic devices.

Another board has a printed silhouette of a city at night, backlit by LEDs, and connected to a small model power substation. The model power substation consists of an Arduino Mega running "ground truth" data that is read by the PLC as voltage (randomly generated between 200 and 240, representing a set point of 220V) and frequency (randomly generated between 58 and 62, representing a set point of 60Hz). If players are able to take control of the system, they can shut off the power for the entire city by "tripping" a breaker via an HMI. This platform also consists of a simple gateway device, in this case using an SSH-based VPN with easily guessable login credentials (e.g. "admin" and "password").

Other stations might include a coffee maker that serves as a model nuclear power plant, a model factory conveyor belt, a wind turbine, or any number of systems of relays and logic controllers, servos and motors, pumps and valves, and sensors and actuators representing the diversity of physical systems. The stations share a common model for making logical sense of the system and a common flow to make reconfiguration manageable. The architecture includes the essential elements of cyber-enabled IT systems (e.g. web servers, VPNs), engineering systems and basic HMIs, programmable logic controllers, and physical elements.

c) QR code: The purpose of the QR code is to provide a system of orientation, giving the students introductory information for each platform. The QR code links to an internal documentation server and may provide a detailed diagram of the components on the board, hints about other resources, or the story-line of the company or industry that the platform is representing. Since our environment is isolated from the wireless network for security reasons, the QR code may also provide a non-clickable image of a link to a website hosted by the platform for the students to access from within the room on our isolated network. This system of orientation can be reconfigured as well, establishing attack scenarios at varying degrees of complexity and expertise. Introductory versions of each board may be suitable for beginners with a slimmed-down scenario and basic tutorial-style walk-through. More advanced versions may offer different attack pathways and fewer hints with more complex versions of the digital system components. Additional challenge can also be introduced by requiring students to attempt to cover their tracks as they modify a system, perhaps by shutting off the alarm lights and sound, or by modifying supervisory controls to appear normal while actually under attack.

D. Integrating MITRE ATT&CK and the Purdue ICS Model

a) Architecture: The Cyber-physical Shooting Gallery is intentionally built to both logically and visually represent the Purdue Model for ICS Security (Fig. 2), a well-known model for network segmentation in industrial control systems developed from the original Purdue Enterprise Reference Architecture (PERA) [10], [11]. The top portion of the board, which represents levels 4 and 5 of the Purdue Model, includes the network switch and a Raspberry Pi hosting a shell server, web server, and/or auxiliary services. The middle of the board, representing levels 2 and 3, contains a second Raspberry Pi or other microprocessor which monitors lower levels and manages human machine interfaces (HMI). The programmable logic controllers and the platform-specific cyber-physical components represent levels 1 and 0 at the bottom of the board. Across different platforms, this model can be simplified or additional virtualization can be added to further explore the segmentation of networks. Fig. 3 shows the layered network and path students will use to take control of the physical system.

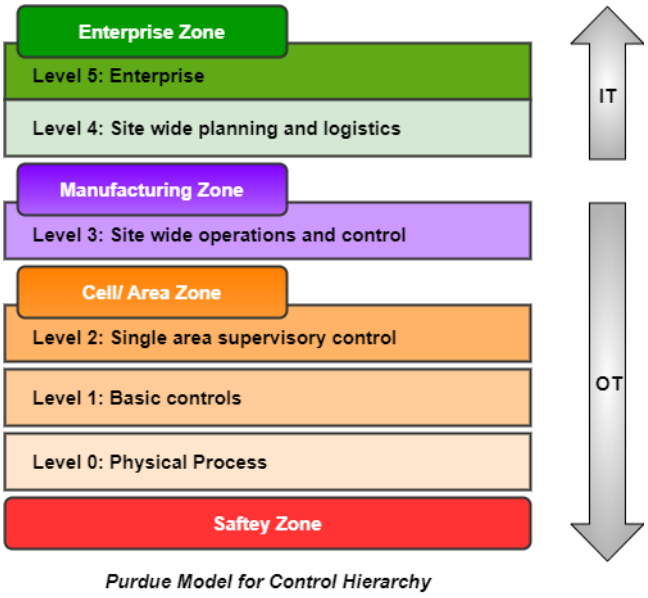

Fig. 2. Purdue Model

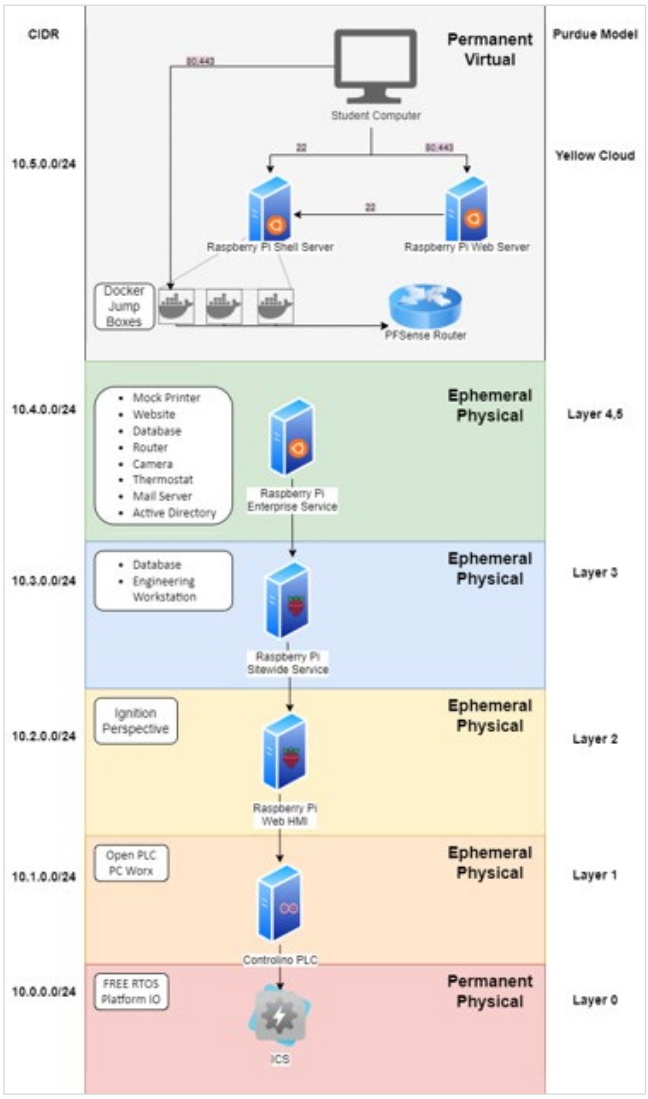

Fig. 3. Cyber-Physical Shooting Gallery Architecture

The Purdue Model advocates a strict air gap between the control network and the enterprise or business levels which have access to external networks. While the Cyber-physical Shooting Gallery platforms are not air-gapped, this is both a useful training and research tool and an accurate representation of the reality of most ICS environments [12], [13]. The Dragos Annual Report in 2021 revealed that 70% of ICS/OT environments were not properly air-gapped, a situation that has worsened during the pandemic due to increases in remote working.

b) MITRE ATT&CK and the Game Map: MITRE released their ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) for ICS in 2020 as a response to the growing need for understanding adversary behavior specific to industrial control systems [11]. The ATT&CK framework has proven both popular and helpful to defenders and systems engineers by helping to articulate and quantify common attacker techniques and tactics. Students will be introduced to this framework as well as the ICS Kill Chain [14], which covers the seven high level goals that attackers progress through during an attack. In the deployment of the Cyber-physical Shooting Gallery, these frameworks will be used by both designers and students in conjunction with the Purdue Model to explore the threat model for each platform. The students will be able to follow along with a virtual "Game Map" progressing through the stages of the ICS Kill Chain, allowing them to make clear connections between the physical platform at each of the layers, the defenses used between layers, and these conceptual models, thus reinforcing their understanding and retention of these critical concepts.

E. Next Steps: Expansion Pack

a) Advanced Reconfiguration: While the initial Cyber-physical Shooting Gallery platforms are intentionally built to be accessible and not overly complicated, there are plans for more advanced versions. One part of RADICL will contain the single-board platforms with a range of challenges, varying in both the physical element and difficulty levels, while another room will have the space for more elaborate, multi-board designs. This could potentially be a place for multi-player attack and defense scenarios, like a reversible conveyor belt with each team attempting to keep the factory running in their favor. That is, as a robotic arm drops items such as small wooden blocks on the middle of the belt from above, attackers work to force the belt to move those blocks into catch bins on their side of the belt. Scenarios can be built to allow for attackers to discover ways to control the belt motion and speed as well as lock out the opposing players. More complicated platforms can be designed with integrated layers of physical systems, and disjoint cyber systems that represent more complex and realistic critical infrastructure elements.

b) Expertise exchange: The potential for expertise exchange is integral to the development of increasing challenge and complexity, as well as closing the divide between academic education and the needs of the actual workforce. The Cyber-physical Shooting Gallery is seen as an environment both for education for students and training exercises for current ICS workers. The crossover of expertise between cybersecurity students and workers with OT expertise will advance more relevant exercises and a refined curriculum that is beneficial to both groups.

c) OT Capture-the-Flag or stand-alone: RADICL is meant to be a highly flexible environment and the Cyber-physical Shooting Gallery as a keystone element of the laboratory is no exception. In addition to being used for stand-alone challenges and an introduction to security issues in cyber-physical systems, the platforms can also be used for OT-based Capture the Flag competitions using the community-supported code base for Carnegie Mellon's PicoCTF capture the flag program [15]. Students will be able to compete in an OT-CTF to take control of systems all around the room, earning points based on the levels of difficulty as well as stealth and level of penetration. This engagingly chaotic scene allows students to earn points based on the physical state of each system in a way that is agnostic to the specific method the student used to attack the system,

overcoming the shortcomings of some traditional CTFs that may not credit students for correct answers using the wrong spelling or case. The points awarded in an OT CTF are purely based on the physical state of a system (e.g. whether a light bulb is lit or not, or the set speed on a motor). Using local or cloud servers, the services that make the CTF possible can also make the experience portable. The platforms are kept manageable in size and are able to be mounted on a stand so they can travel to schools, career fairs, and workplace training events.

d) Multi-disciplinary geo-political and cultural scenarios: RADICL currently works in an isolated network and makes use of real (would-be routable) IP addresses. This allows for scenarios that better mimic the types of attacks and network traffic associated with significant nation-states and other persistent threat actors. By using real IPs and basic static routing tables, defenders are able to take advantage of tools such as geoIP lookup databases and gain a sense of where an adversary may be based, how widely distributed an attack may be, etc. The Cyber-physical Shooting Gallery template can eventually be used in a multi-disciplinary way to simulate geo-political and culturally-informed scenarios that can be used to study the pattern of attacks on critical infrastructure that have been increasing in recent years.

III. CONCLUSION

The education and workforce development necessary to meet the global needs for securing critical infrastructure and other cyber-physical systems will require a multi-faceted and coordinated approach. Fortunately, the intrinsically hands-on nature of cyber-physical education is very well suited to early education. Our experience with summer cybersecurity camps for middle and high school students for the past six years has shown that students respond enthusiastically to opportunities to build and program their own circuits with Raspberry Pis and simple sensors and actuators. The opportunity to build and creatively design physical projects pulls in a wider range of students than more narrowly focused coding programs. McBride [5] advocates a coordinated and vertically integrated pathway beginning with such early school camps and clubs and building through technical schools, universities, and employers.

There are many roadblocks to overcome, including cultural and educational barriers between workers in IT and OT [16], the sparsity of current dedicated programs for ICS cybersecurity, and financial hurdles to recruiting the necessary expertise for teaching these skills. However, there is momentum building toward addressing these issues. There have been recent efforts to develop comprehensive ICS cybersecurity curricular guidance [17], [18], to develop project-based, hands-on ICS tasks [19], [20], to develop open-source training materials for operational technicians [21], and to develop multidisciplinary certificates or degrees that bridge computer science, industrial technology, and engineering [22], [23].

This paper presents a novel approach to deploying a scalable and repeatable platform for engaging students in adversarial thinking about cyber-physical systems. The RADICL Cyber-physical Shooting Gallery is intended to fill an entry-level role in developing comfort with the interplay between cybersecurity and physical systems in an engaging and non-threatening way. It can provide a key bridge between jeopardy-style CTFs and virtual simulations and larger scale test-bed challenges [24], [25], hopefully de-mystifying the field and enticing more students into the joys and challenges of working with cyber-physical systems.

REFERENCES

[1] S. McBride, and J. Slay, "Towards standards-based industrial control systems security education in the United States," unpublished. *industrialcyberforce.org*, 2020. [Online]. Available: https://industrialcyberforce.org/wp-content/uploads/2020/08/Towards-Standards-based-ICS-Security-Education-in-the-United-States.pdf.

[2] R. Ley, "NICE ENewsletter Winter 2021-22 Government Spotlight." NIST, Jan. 2022. [Online].

[3] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review*, vol. 40, pp. 1-20, 2021.

[4] T. R. McJunkin *et al*., "Multidisciplinary game-based approach for generating student enthusiasm for addressing critical infrastructure challenges," in 2016 ASEE Annual Conference & Exposition. New Orleans, Louisiana: ASEE Conferences, Jun. 2016.

[5] S. McBride, C. Schou, J. Slay, "A vertically integrated pathway for infusing engineering technicians with industrial cybersecurity competencies," in *Journal of The Colloquium for Information Systems Security Education*, vol. 9, no. 1, p. 8, 2022.

[6] F. Sauer, M. Niedermaier, S. Kießling, and D. Merli, "LICSTER—A low-cost ICS security testbed for education and research," in Proc. 6th Int. Symp. ICS SCADA Cyber Security Res., 2019, pp. 1–10.

[7] P. Čeleda, J. Vykopal, V. Švábenský, K. Slavíček, "KYPO4INDUSTRY: A testbed for teaching cybersecurity of industrial control systems," in Proc. 51st ACM Tech. Symp. Comput.Sci. Educ., 2020, pp. 1026–1032.

[8] S. Caltagirone, P. Ortman, S. Melton, D. Manz, K. King, and P. W. Oman, "Design and implementation of a multi-use attack-defend computer security lab," in Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS-39), vol. 9. Kauai, Hawaii, U.S.A.: IEEE Computer Society, January 2006, p. 220c.

[9] D. Conte de Leon, C. E. Goes, M. Haney, A.W. Krings, "ADLES: Specifying, deploying, and sharing hands-on cyber-exercises," *Computers and Security*, vol. 74, May, 12-40, 2018.

[10] T. Williams, "The Purdue Enterprise Reference Architecture," *Computers in Industry*, vol. 24, no. 2, pp. 559-564, 1994.

[11] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK for industrial control systems: Design and philosophy," MITRE, 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

[12] E. Byres, "The air gap: SCADA's enduring security myth," *Communications of the ACM*, vol. 56, no. 8, pp. 29–31, Aug. 2013.

[13] Dragos, "ICS cybersecurity year in review 2021," Hanover, MD, 2022. [Online]. Available: https://cdn.cyberscoop.com/2021-ics-ot-cybersecurity-year-in-review-report.pdf.

[14] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," SANS Inst., North Bethesda, MD, USA, Tech. Rep. 36297, Oct. 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/industrialcontrolsystem-cyber-kill-chain-36297.

[15] P. Chapman, J. Burket and D. Brumley, "PicoCTF: A Game-Based Computer Security Competition for High School Students," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[16] S. McBride, J. Slay, C. Schou, "A security workforce to bridge the IT-OT gap," [Online]. Available: https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf.

[17] I. Ngambeki, S. McBride, and J. Slay, "Knowledge gaps in curricular guidance for ICS security," in *Colloquium for Information Systems Security Education*, vol. 9, no. 1, p. 6, 2022.

[18] P. Marwedel, T. Mitra, M. E. Grimheden, and H. A. Andrade, "Survey on education for cyber-physical systems," *IEEE Design & Test*, vol. 37, no. 6, pp. 56-70, 2020.

[19] E. Mäkiö, E. Yablochnikov, AW. Colombo, J. Mäkiö, R. Harrison, "Applying task-centric holistic teaching approach in education of industrial cyber physical systems," *IEEE Conference on Industrial cyber-physical Systems*, vol. 1, pp. 359-364, 2020.

[20] J. Maekioe, E. Maekioe-Marusik, E. Yablochnikov, "Taskcentric holistic agile approach on teaching cyber physical systems engineering," IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, pp. 6608–6614, 2016.

[21] K. Karampidis, S. Panagiotakis, M. Vasilakis, E. K. Markakis and G. Papadourakis, "Industrial cyberSecurity 4.0: Preparing the operational technicians for industry 4.0," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1-6, 2019.

[22] B. Hamdan and R. A. Nsour, "Curriculum development for teaching cybersecurity of industrial control systems & critical infrastructure," 2022 Intermountain Engineering, Technology and Computing (IETC), pp. 1-5, 2022.

[23] D. Oliver and M. Haney, "Curriculum development for teaching critical infrastructure protection," *Journal of The Colloquium for Information System Security Education (CISSE)*, vol. 5, no. 2, p. 18, March 2018.

[24] IA. Oyewumi, "ISAAC: The Idaho cyber-physical system smart grid cybersecurity testbed". Diss. University of Idaho, 2019.

[25] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, N. O. Tippenhauer, "Gamifying ICS security training and research: Design,implementation, and results of S3," in Proc. Workshop Cyber-Phys. Syst. Secur. Privacy, pp. 93–102, Nov. 2017.