Engineering Educators Bringing the World Together

2025 ASEE Annual Conference & Exposition

Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025

ASEE

Paper ID #48088

Integrating Cyber-Physical Security Training to the Electrical Engineering Program via Experiential Learning

Sangshin Park, University of Utah

Since 2022, he has been with University of Utah, Salt Lake City, UT, where he is currently pursuing an Ph.D at the Computer Science Department. His research interests include Cyber-Physical System, Edge Computing and ML/AI for Cybersecurity ensuring Resilience.

Dr. Reza Kamali, California State University San Marcos

Dr. Reza Kamali-Sarvestani is a Professor of Electrical and Computer Engineering at California State University San Marcos. He received his B.S. degree in Electrical Engineering from Shiraz University Iran, and M.S.E, Ph.D. degree in Electrical

Hamed Nademi

is an Assistant Professor of Electrical Engineering at California State University-San Marcos (CSUSM). Prior to joining CSUSM, Dr. Nademi served as an Assistant Professor at the New Mexico State University and prior to that he was Research Scientist at Rensselaer Polytechnic Institute (RPI), Troy, NY. He worked as PI/Co-PI with industry-sponsored projects granted by New York State Energy Research & Development Authority (NYSERDA) together with utility companies focusing on control schemes development, autonomous digital power grids and transportation electrification. Dr. Nademi has been a PI on the DOE Marine Energy and Wind Energy competitions and CO-PI of the NSF-funded AI-Assisted Wind Farm Control and ONR-sponsored Marine Energy project over the last three years. He worked with SIEMENS AG, and ABB Inc. as a R&D scientist where he was involved in the development of medium-voltage industrial grid and off-grid applications. He has authored more than 70 published scientific papers and holds seven patents on energy conversion circuits and controls.

Manish Parashar, The University of Utah

Manish Parashar is the Chief AI Officer at the University of Utah. He is also the Director of the Scientific Computing and Imaging (SCI) Institute, Chair in Computational Science and Engineering, and Presidential Professor at the Kahlert School of Computing. Manish's expertise is in high-performance parallel and distributed computing and cyberinfrastructure. Manish is the founding chair of the IEEE Technical Community on High Performance Computing (TCHPC) and is a Fellow of AAAS, ACM, and IEEE.

Prof. Jairo Giraldo, University of Utah

Dr. Jairo Giraldo received a B.Sc. degree in Electronic Engineering from the National University of Colombia in 2010 and an M.Sc. and Ph.D. degree from the University of the Andes, Colombia in 2012 and 2015, respectively. Dr. Giraldo is currently a Research Assistant Professor at the Department of Electrical and Computer Engineering at the University of Utah. His research is centered around the security and privacy of cyber-physical systems using tools from control theory, optimization, and machine learning, with applications in power systems resilience.

Work in Progress: Integrating Cyber-Physical Security Training to the Electrical Engineering Program via Experiential Learning

Abstract

As industries worldwide embrace the next wave of innovation, the integration of technologies like cyber-physical systems (CPS) and the Internet of Things (IoT) is becoming a key driver of change, with applications ranging from autonomous vehicles to large-scale critical infrastructures. Unfortunately, the increasing use of communication networks to monitor and control these systems has increased their vulnerabilities to cyber threats, posing significant risks that can cause economic losses and even lead to loss of lives. To prepare future electrical engineers for these emerging challenges, it is essential to include cyber-physical security modules with experiential learning in their education. These modules should help students develop the expertise to secure CPS integrated with IoT devices against cyber threats by equipping them with theoretical and practical tools to analyze system vulnerabilities and design defense measures. With these skills, students will be better positioned to face real-world challenges and ensure the resilience and safety of these interconnected systems in our increasingly connected world.

In this work in progress, an experiential learning framework composed of an embedded development kit and a set of laboratory experiments is proposed, allowing students to learn foundational principles related to cyber-physical systems security through hands-on experimentation. The embedded development kit integrates real wired and wireless communication networks with industrial protocols such as Modbus/TCP, a real-world programmable logic controller (PLC), models of real-world applications such as submarine position control and a DC motor speed control, and multiple I/O connections to integrate IoT devices and other external physical systems. The laboratory material spans multiple areas including principles of system modeling, feedback control systems and controller design, networking and IoT, deep packet inspection, attack detection, localization, and mitigation, and digital systems, among others. The proposed experiential learning material has been integrated into existing courses and enabled the students to learn a variety of skills that are not typically included in EE education.

1 Introduction

In the modern era, the integration of Cyber-Physical Systems (CPS) and the Internet of Things (IoT) has emerged as a transformative force across a wide range of industries. With these technologies, sectors such as energy, healthcare, transportation, communication and manufacturing are undergoing a revolution [1], as they create interconnected environments that can make autonomous decisions and respond in real-time [2]. As an example, IoT devices have enabled the automation of homes, industries, and public services, leading to greater operational efficiency and better quality of life. In a similar way [3], CPS integrates computational and physical elements to supply intelligent solutions for critical infrastructure, such as smart grids, automated industrial processes, and advanced healthcare systems. In addition to bringing unprecedented opportunities, these advancements also present significant security challenges. As CPS and IoT ecosystems become more interconnected, they are more susceptible to cyber threats [4], from data breaches to large-scale disruptions of operations. A vulnerability can have far-reaching consequences, including economic losses, public safety compromises, and even life-threatening consequences [5]. A cyber-attack on critical infrastructures, such as the power grid or the healthcare system, can disrupt essential services, underscoring the urgent need for robust cybersecurity measures [6]. CPS and IoT are becoming increasingly crucial components of critical systems, which makes it imperative for future engineers to possess the skills and knowledge to secure these technologies. In traditional engineering curricula, systems design and functionality are often emphasized on a theoretical level without addressing the dynamic and evolving nature of cybersecurity threats. In order to bridge this gap, cybersecurity education must be integrated into electrical engineering (EE) programs, both theoretically and practically [7, 8]. It has been proven that experiential learning methods, including hands-on labs, virtual testbeds, and real-life case studies, can effectively assist students in analyzing vulnerabilities, designing defense strategies, and implementing resilient systems [9].

There are several challenges associated with developing a comprehensive cybersecurity curriculum. CPS and IoT security are interdisciplinary fields that require knowledge from computer science, networking, and communication systems. Secondly, limited resources such as high costs associated with specialized infrastructure and tools, can hinder educational module development [10]. Third, curricula must continually be updated in order to remain relevant and effective as new technologies and threats emerge. To tackle these challenges, educational strategies must be innovative, leveraging partnerships between industry and academia, scalable virtual environments, and collaborative learning models [11].

This work in progress presents a low-cost and flexible embedded development kit and a series of hands-on laboratory modules designed to teach the foundational principles of CPS and IoT security. Real-world components such as programmable logic controllers (PLCs), IoT devices, and industrial protocols such as Modbus/TCP are included in the development kit. Using these tools, students can explore system modeling, feedback control systems, deep packet inspections, and attack mitigations, developing skills that are rarely taught in conventional EE courses. The proposed experiential learning approach aligns with the overarching objective of producing engineers who are proficient in technical design as well as able to address the cybersecurity challenges of modern CPS and IoT systems. The laboratory modules are designed to be adaptable, allowing instructors to tailor the content to specific course objectives. The developed content will be integrated into different courses of different levels such as sensors and systems, wireless communications, and control systems, without affecting their core content. The cyber-security modules will modify only the way the laboratories are conducted introducing the different cybersecurity principles to the main topics of the course. For instance, a control system course will shift to include lab experiments where cyber vulnerabilities are introduced while the focus remains on designing adequate feedback controllers.

2 Background and Related Work

In recent years, advancements in educational practices have been required due to the quick growth of monitoring, control, and IoT devices in day-to-day systems as well as large-scale critical infrastructures. Despite the importance of CPS/IoT security for applications ranging from industrial automation to critical infrastructure, it is often underrepresented in traditional engineering programs [12]. Some institutions offer specialized courses focused on hands-on learning [13], such as sensor integration, data transmission, and security protocols using Raspberry Pi and Arduino platforms. The development of applications that incorporate real-world scenarios, such as securing industrial protocols, has shown promise in bridging the gap between theory and practice. It should be noted that some embedded systems programs have integrated cybersecurity concepts directly into their programs [14], focusing on topics like network vulnerabilities, intrusion detection, and secure design. In industrial control systems, educational modules [15] allow students to gain a deeper understanding of the relationship between process control and cybersecurity, preparing them for real-world challenges. CPS/IoT security requires experiential learning, which has been demonstrated to be effective in teaching technical subjects. A virtual lab or environment provides students with hands-on experience in identifying vulnerabilities, implementing defense mechanisms, and responding to cyber threats. For example, DeterLab [11] provides controlled environments in which concepts related to IoT and network security can be explored. There has also been a growing interest in blended and use-case-based approaches. As an example, programs that use tools such as Shodan [16] to study Industrial IoT devices offer students an opportunity to practice cybersecurity. Through this active learning framework, not only are technical skills enhanced, but also critical thinking and problem-solving abilities are fostered, which are essential in addressing the complexity of CPS/IoT systems. Similarly, incorporating concepts such as user-centered design and secure architecture into these programs will prepare students to be able to tackle real-world cybersecurity issues [17].

3 Experiential Learning in CPS/IoT Security

The proposed experiential learning in CPS/IoT Security framework summarized in Fig. 1 has been designed to allow students to learn the main principles of cyber security in cyber-physical systems and IoT through hands-on experimentation. It consists of the following main components: i) Embedded development kit (EDK), which consists of a low-cost hardware component that allows performing a wide variety of experiments; ii) lab modules, that are designed to complement existing curricula of different courses and that are designed to allow students to learn the fundamental and advanced concepts of CPS security; iii) Industry partners that provide unique insights about existing relevant problems that help tailor the lab materials. The hands-on experimentation combined with real-world scenarios in this

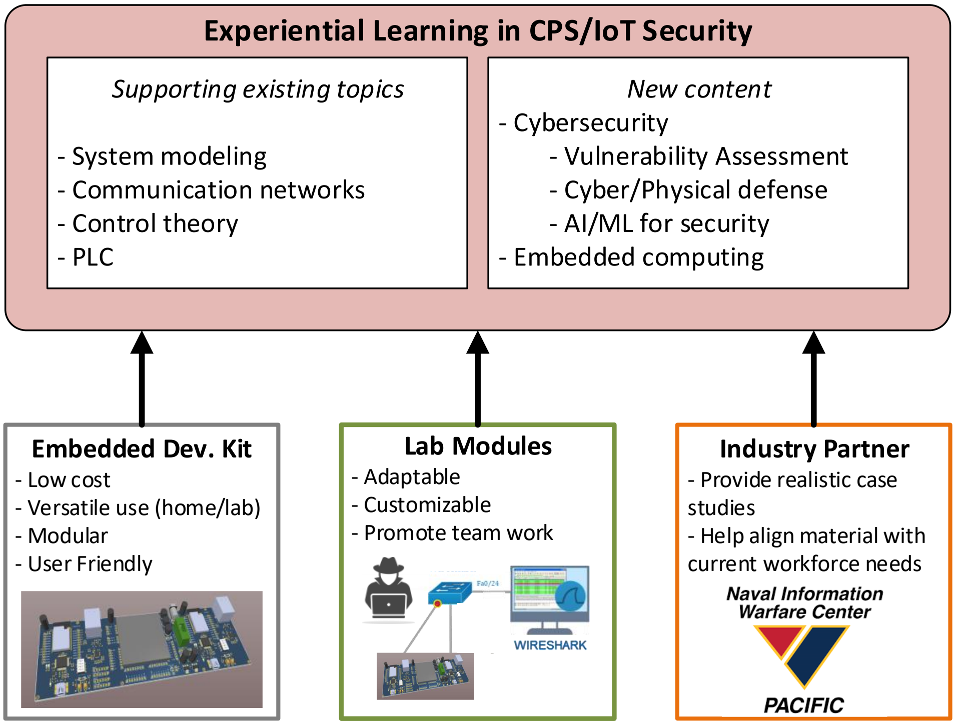


Figure 1: General description of the proposed experiential learning in CPS/IoT Security

approach will equip students with the skills to address emerging cybersecurity threats while nurturing a workforce that can seamlessly transition to the workplace.

A key advantage of the proposed experiential learning framework is that it can be easily incorporated into existing curriculums in EE and CS. Developing modules for CPS/IoT security allows seamless integration with existing academic courses at the undergraduate and graduate levels. Key strategies include incremental modules that can be integrated on CPS/IoT security can be introduced at different academic levels, starting with basic system modeling and networking courses and progressing to advanced threat analysis and secure system design courses. Capstone projects can be expanded into course projects that apply students' theoretical knowledge and practical skills to real-world problems, such as protecting a smart grid or countering cyberattacks on industrial control systems. Multidisciplinary collaboration provides a holistic understanding of CPS/IoT security, the modules encourage collaboration across engineering, computational science, and information technology disciplines. Incorporating these modules into current curricula can enhance student engagement and learning outcomes while ensuring that the material remains relevant within the rapidly evolving technological environment.

3.1 Embedded Development Kit for Hands-on Experimentation

In this study, the embedded development kit provides a platform for teaching and experimenting with cybersecurity concepts in the IoT and CPS context. The proposed embedded development kit is easily adaptable and low-cost, making it accessible to all students and also allowing working in a laboratory setup on campus or from home. As shown in Fig. 2, we illustrate the end-to-end workflow of the embedded development kit for CPS/IoT security. Through the integration of real-world hardware components, communication networks, and user interfaces, it simulates realistic industrial and critical infrastructure scenarios, which facilitates a deeper understanding of the security principles of CPS and IoT. An embedded development kit emulates a real-world CPS environment by integrating several interconnected components.

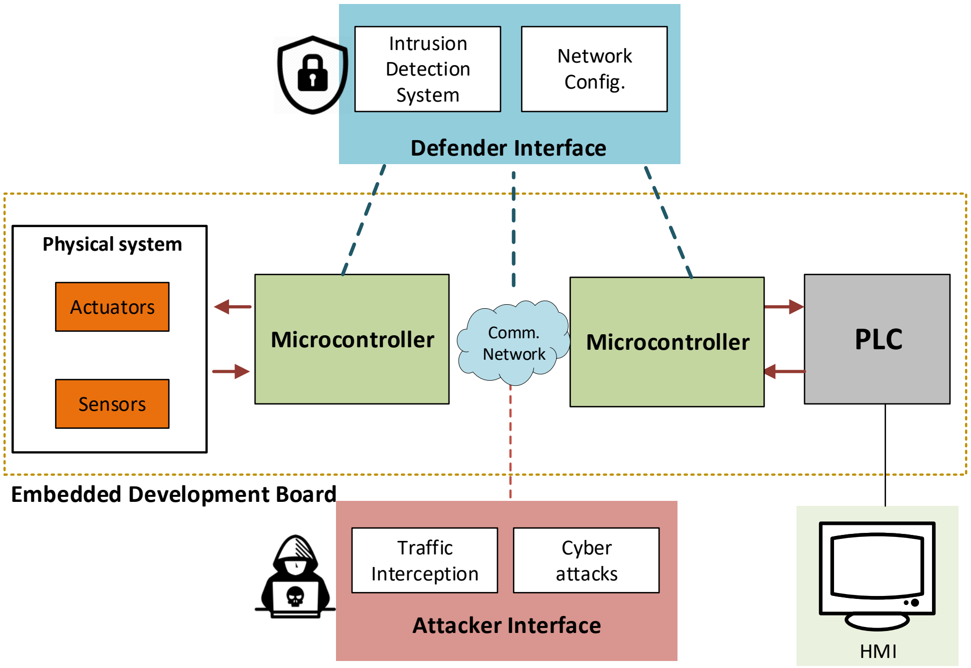


Figure 2: End-to-end Workflow of the Embedded Development Kit for CPS/IoT Security

Physical system consists of actuators and sensors that interface directly with the microcontrollers. As motors and valves are simulated with actuators, temperature, pressure, and position are measured with sensors. For an understanding of feedback loops and control systems, these components provide real-world interactions. Two microcontrollers serve as the primary computational nodes. A sensor sends data to the actuators, and the actuators respond to those commands. Through the use of microcontrollers communicating over a shared communication network, students have the opportunity to study distributed control systems and vulnerabilities associated with them. As a result of its integration with microcontrollers, the PLCs add a layer of industrial relevance to the platform. Using this software, you can manage complex control logic and mimic real-world industrial configurations. As well as interacting with the human-machine interface (HMI), this component also allows students to monitor and interact with the system. Using a communication network that simulates industrial protocols, microcontrollers and PLCs communicate with each other. Using this network, traffic interceptions, cyberattacks, and mitigation strategies can be demonstrated. Tools such as an intrusion detection system (IDS) and network configuration modules are included in the defender interface. Through these tools, students can monitor network traffic, identify anomalies, and implement security measures in order to protect their computer networks. In order to foster a comprehensive understanding of cybersecurity, the development kit includes an attacker interface that allows students to simulate traffic interception and execute cyberattacks such as denial-of-service (DoS) and packet spoofing without requiring advanced programming skills. This will allow students from multiple backgrounds to benefit from these tools and observe the impact of cyber attacks in physical systems. Using this controlled environment, defensive strategies can be tested to identify system vulnerabilities and countermeasures.

This embedded development kit provides a versatile and interactive learning environment that includes the following features. By using the intrusion detection and network configuration tools, students can simulate attacks on the system and implement defenses. Through this functionality, they can gain a better understanding of cybersecurity measures in CPS and IoT environments. By monitoring real-time data from the physical system and interacting with the control processes, the HMI provides insight into the operation of the system and potential security threats. Through interaction with sensors, actuators, and microcontrollers, students gain practical experience in designing, implementing, and troubleshooting CPS/IoT applications. Industrial protocols familiarize students with the standards used in modern CPS/IoT systems, enhancing their readiness for employment in industry. An interdisciplinary approach to problem-solving is fostered by the platform, which brings together knowledge from EE, CS, and cybersecurity. This development kit is modular and reconfigurable, making it an invaluable tool for teaching CPS/IoT security due to its adaptability for a variety of educational and research purposes. During this hands-on experience, students examine vulnerabilities in systems, build robust defenses, and ensure critical infrastructure resilience.

Embedded Development Kit Implementation Details

In order for students to gain a deeper understanding of CPS and IoT security, the embedded development kit has been configured so that students can use the kit and learn from it directly. Microcontrollers such as ESP32 are used in this system because of their high-performance, low-cost, wireless communication capabilities, and versatility when it comes to handling industrial protocols. In our initial testing scenario, we have emulated a DC motor speed control, where a controller aims to take the speed of the motor to a desired setpoint by controlling the input current. For simplicity, the DC motor is modeled using differential equations that run in an ESP32 microcontroller, namely, the system ESP32. The motor speed information is then sent through a wireless network to another ESP32, namely the controller ESP32, using an industrial communication protocol, Modbus TCP/IP. The controller ESP32 is connected to a Velocio ACE PLC and executes a PID control logic to take the speed to a desired setpoint. To close the feedback loop, the control command computed by the PLC is then sent to the controller ESP32, which then transmits it via wireless to the system ESP32 to update the dynamic model. Additionally, the Velocio PLC is integrated with HMI software such that students can monitor system behavior as well as observe the impact of security threats at any time.

Having a system that emulates a real physical scenario integrated with back-and-forth real industrial communications allows students to analyze network security using tools such as

Wireshark packet monitoring to examine Modbus Master-Slave communications and detect anomalies. Also, students can design and launch their own attacks to observe the impact they could have on a physical system. The penetration testing process provides students with the opportunity to simulate unauthorized packet injections, which further reinforces their understanding of CPS vulnerabilities and mitigation strategies. In our initial tests, 3 students were able to observe the network traffic exchange between the physical system and the controller, gain a better understanding of how an industrial protocol such as Modbus TCP/IP works, and launch real sensor attacks that caused the controller to compute wrong actions that ended up causing the motor to operate in an undesired setpoint. Currently, we are implementing some of the developed modules in an existing PLC course to gather more information about the student's experience.

Due to its modular design, this kit is scalable for large-scale classroom deployments or remote (hybrid) learning environments with an average cost range of $80 to $150 per unit. As a result of combining physical hardware, industrial protocols, and cybersecurity modules, this framework offers students a comprehensive curriculum that prepares them for real-world scenarios that arise when securing CPS and IoT systems.

3.2 Laboratory Modules

The laboratory modules in this work provide students with practical hands-on experience in systems and control, networking, and cybersecurity. Using an embedded development kit, these modules integrate theoretical foundations with practical experimentation, enhancing learning outcomes and preparing students for real-world challenges.

- **System modeling and Control** Modules on systems and control introduce students to system modeling, feedback control systems, and their applications to CPS and IoT. Through PLCs, sensors, and actuators, students explore fundamental concepts, such as system modeling, stability, and dynamic response. Proportional-Integral-Derivative (PID) control algorithms are implemented for simulated processes, such as a DC motor. Experimenting with physical parameters allows students to learn how control actions can affect system performance and stability. Throughout this module, the interactions between cyber and physical systems are emphasized, allowing students to gain a comprehensive understanding of CPS operation.

- **Networking** The networking module provides students with an understanding of communication networks within CPS/IoT environments. As students work with real-world industrial communication protocols, they can monitor and configure communication networks for data transfer between IoT devices, microcontrollers, and PLCs. Analyze network traffic, including packet flow, protocol behavior, and performance, using tools such as Wireshark. The effect of network disruptions on system performance, including latency and data integrity, can be observed by simulating disruptions and monitoring their impact. Using hands-on activities, students learn networking principles while also gaining a deeper understanding of the critical role secured and reliable communication plays in CPS/IoT systems.

- **Cybersecurity** The cybersecurity module introduces students to fundamental principles of IoT/CPS security, emphasizing identifying potential threats and mitigating them. Through guided experiments, students can investigate common vulnerabilities in communication networks and authentication of devices as part of a threat analysis. By using the attacker interface provided in the embedded development kit, we simulate cyberattacks including ARP spoofing and false data injection attacks. But also, we need to ensure that communication channels are secured and the integrity of the system is protected by using defense strategies such as IDS and packet encryption.

3.3 Industry Partners

Industry collaboration is integral to experiential learning, bridging the gap between academic and professional learning. For example, organizations such as Naval Information Warfare Center Pacific (NIWC Pacific) have provided specialized insights into industry needs and challenges to help define real-world examples and case studies that can be part of the program. Industry partners can submit authentic scenarios relating to cybersecurity challenges they are facing today, such as securing industrial control systems ensuring IoT device integrity in critical infrastructure. Using case studies, students are able to develop problem-solving skills and practical knowledge by tackling real-world challenges. Access to industry resources can be done by partnership which provides advanced tools, testbeds, and datasets that simulate realistic industrial environments, which enriches the learning process. Students gain insight into industry practices, tools, and methodologies through internships, workshops, and guest lectures. As a result of direct interaction with industry experts, students graduate more prepared to join the workforce and contribute effectively to their organizations.

4 Assessment and Evaluation of Educational Outcomes

Assessment and evaluation of educational outcomes in CPS education require multi-dimensional approaches, especially when targeting diverse student populations like lower-division undergraduates at California State University San Marcos. Our ongoing project, focused on teaching cyber-physical lessons related to wireless network security, employs a mixed-methods approach. This includes pre-lesson surveys to gauge student interest and inform curriculum design, alongside ongoing performance assessments within the lessons themselves. This formative approach allows for iterative improvements throughout the project lifecycle. By considering both quantitative survey results and qualitative observations within the learning environment, we aim to measure the effectiveness of our teaching methodologies and their impact on student learning.

Methods for assessing student engagement and learning gains in our CPS lessons centered around wireless network security included a pre-lesson survey designed to capture initial interest levels and prior experiences (see Appendice). This survey was conducted on 18 students who participated in a lower-division course related to this work. The survey was completed by students voluntarily and provided valuable insights into student perceptions and helped tailor the lessons to their specific needs. For instance, when asked, ”Would you be interested in learning about the latest threats and vulnerabilities in wireless networks?”, a combined 94% of students expressed interest (75% ”yes” and 19% ”maybe”). Similarly, 87% indicated they were ”very” or ”somewhat interested” in the technical details of wireless network protocols. This high level of initial interest provided a strong foundation for engagement. Furthermore, 69% of students reported having experienced a Wi-Fi network issue or security breach, suggesting a personal connection to the subject matter. These results underscore the relevance of the curriculum and motivate the students to learn more.

A specific experiential learning assessment mechanism employed in our project involved hands-on activities simulating real-world wireless network vulnerabilities. This allowed students to apply theoretical knowledge in a practical setting, fostering deeper understanding and skill development. The survey also revealed interesting preferences regarding technology: 69% of students expressed the most interest in hardware, with the remainder split between networking and AI, and surprisingly 0% for software. This preference for hardware influenced the design of our experiential learning activities, which focused on physical devices and network configurations. Finally, an overwhelming 94% of students indicated they would ”yes” or ”somewhat” consider taking a course or participating in a research project related to wireless security, demonstrating a strong potential for continued engagement in this critical field.

Feedback mechanisms and continual improvement processes are integral to the success of our CPS education project. The pre-lesson survey not only assessed initial interest but also provided a baseline for measuring changes in student attitudes and knowledge throughout the lessons. We are collecting ongoing feedback from students through informal discussions and observations during the experiential activities. This qualitative data, combined with the quantitative survey results, informs iterative improvements to the curriculum and teaching methods. For instance, the strong interest in hardware prompted us to incorporate more hands-on activities involving physical network devices.

By incorporating these assessment strategies, we can effectively evaluate the impact of our cyber-physical lessons on both lower-division (undergraduate) students at California State University San Marcos and upper-division (graduate) students at the University of Utah. The combination of pre-lesson surveys, experiential learning assessments, and ongoing feedback mechanisms allows for a comprehensive understanding of student engagement, learning gains, and areas for improvement. This iterative process ensures that our curriculum remains relevant, engaging, and effective in preparing students for the challenges of securing cyber-physical systems.

5 Conclusion and Future Directions

As discussed in this paper, experiential learning approaches are crucial to cybersecurity education for CPS and IoT. Using laboratory modules and an embedded development kit, we demonstrate a holistic educational framework that bridges the gap between theoretical understanding and practical application. Key insights and contributions include comprehensive curriculum design that can be part of the proposed modules, CPS/IoT security concepts will be seamlessly incorporated into existing EE and CS curricula, so students can progress from foundational principles to advanced applications over the course of their education. Experiential learning can be integrated by the embedded development kit into the curriculum, students have the opportunity to interact with real-world industrial protocols, implement control algorithms, evaluate cybersecurity threats, and develop mitigation strategies.

Industry collaboration can be the key part. The alignment of educational content with industry needs is a critical function of partnerships with organizations such as NIWC Pacific. Incorporating real-world case studies and leveraging industry resources, this program prepares employees for the workplace and bridges the gap between academic learning and professional practice. Bringing together EE, CS, and cybersecurity concepts allows students to address complex CPS and IoT security challenges through a multidisciplinary approach. As a result of these contributions, this work not only enriches the educational landscape, but also addresses the growing demand for skilled professionals capable of safeguarding critical infrastructure.

It is increasingly important to explore new technologies and methodologies to enhance the security and resilience of CPS/IoT systems due to the constant evolution of cybersecurity threats. The following areas offer promising opportunities for future research and development.

Attack detection can be combined by machine learning (ML) and artificial intelligence (AI), anomalies can be detected in real-time, which includes threats that were previously unseen. A system that detects intrusions can be made more accurate and faster using deep learning (DL) techniques. Threat mitigation is implemented by AI-driven defensive strategies to detect and respond to cyberattacks, such as dynamic reconfiguration of systems and proactive defense mechanisms such as moving targets. Behavioral analysis can be analyzed by patterns in network traffic and system behavior, AI/ML can discover potential vulnerabilities. The investigation of methods for improving the resilience of CPS/IoT architectures against cyberattacks, including fault-tolerant design and redundancy mechanisms. This can make more resilient system design possible. In order to secure large-scale IoT networks, multiple communication protocols and devices need to be accommodated. A cost-effective approach to implementing advanced security measures in resource-constrained environments. In this case, scalable security solutions should be explored.

The foundational contributions of this research can be incorporated into future research to advance CPS/IoT security, enabling professionals and systems to combat ever-evolving threats. A rapidly transforming technological landscape calls for continued innovation as a means of safeguarding critical infrastructure and ensuring the reliability and resilience of interconnected systems.

Acknowledgement

This work is supported by the Office of Naval Research (ONR) under Grant Number N000142312240.

References

[1] S. Park and H. Lee, “Deep learning approach to optical camera communication receiver design,” in *2021 IEEE Region 10 Symposium (TENSYMP)*, 2021, pp. 1–5.

[2] J. Sánchez, A. Mallorquí, A. Briones, A. Zaballos, and G. Corral, "An integral pedagogical strategy for teaching and learning iot cybersecurity," *Sensors*, vol. 20, no. 14, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/14/3970

[3] I. Delgado, E. Sancristobal, S. Martin, and A. Robles-Gómez, "Exploring iot vulnerabilities in a comprehensive remote cybersecurity laboratory," *Sensors*, vol. 23, no. 22, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/22/9279

[4] R. Raval, A. Maskus, B. Saltmiras, M. Dunn, P. J. Hawrylak, and J. Hale, "Competitive learning environment for cyber-physical system security experimentation," in *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, 2018, pp. 211–218.

[5] J. Rajamäki, "Industry-university collaboration on iot cyber security education: Academic course: "resilience of internet of things and cyber-physical systems"," in *2018 IEEE Global Engineering Education Conference (EDUCON)*, 2018, pp. 1969–1977.

[6] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7–17, 2017.

[7] S. Park, R. Kamali-Sarvestani, J. Giraldo, H. Nademi, and M. Parvania, "Importance of cyber-physical security training in electrical engineering education," in *2024 ASEE Annual Conference & Exposition*. Portland, Oregon: ASEE Conferences, June 2024.

[8] L. Xu, D. Huang, and W.-T. Tsai, "Cloud-based virtual laboratory for network security education," *IEEE Transactions on Education*, vol. 57, no. 3, pp. 145–150, 2014.

[9] V. Gonzalez, O. Perez, and R. Romero, "Cybersecurity in ece curriculum, an expanded collaboration program to disseminate real security experiences in cyber-physical systems," in *2023 IEEE Frontiers in Education Conference (FIE)*, 2023, pp. 1–4.

[10] C. Konstantinou, "Cyber-physical systems security education through hands-on lab exercises," *IEEE Design & Test*, vol. 37, no. 6, pp. 47–55, 2020.

[11] J. Mirkovic and T. Benzel, "Teaching cybersecurity with deterlab," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 73–76, 2012.

[12] A. R. Rao, "A three-year retrospective on offering an embedded systems course with a focus on cybersecurity," in *2020 IEEE Integrated STEM Education Conference (ISEC)*, 2020, pp. 1–8.

[13] A. R. Rao, D. Clarke, M. Bhadiyadra, and S. Phadke, "Development of an embedded system course to teach the internet-of-things," in *2018 IEEE Integrated STEM Education Conference (ISEC)*, 2018, pp. 154–160.

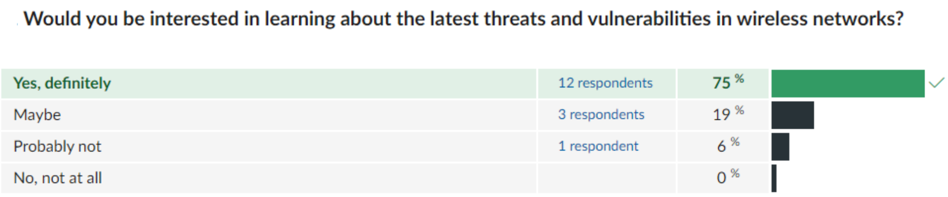
[14] J.-M. Thiriet and S. Mocanu, "A course in cyber-security, with orientations towards cyber-physical systems," in *2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)*, 2019, pp. 1–4.

[15] C. Foreman, M. Turner, and K. Perusich, "Educational modules in industrial control systems for critical infrastructure cyber security," in *2015 ASEE Annual Conference & Exposition*, 2015.

[16] A. Tundis, E. M. Modo Nga, and M. Mühlhäuser, "An exploratory analysis on the impact of shodan scanning tool on the network attacks," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3465481.3469197

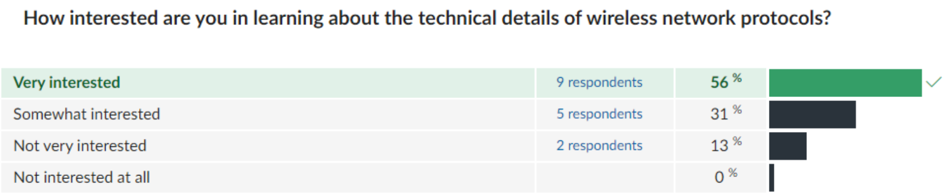
[17] C. Gough, C. Mann, C. Ficke, M. Namukasa, M. Carroll, and T. OConnor, "Remote controlled cyber: Toward engaging and educating a diverse cybersecurity workforce," in *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, ser. SIGCSE 2024. New York, NY, USA: Association for Computing Machinery, 2024, p. 394–400. [Online]. Available: https://doi.org/10.1145/3626252.3630917

Appendix



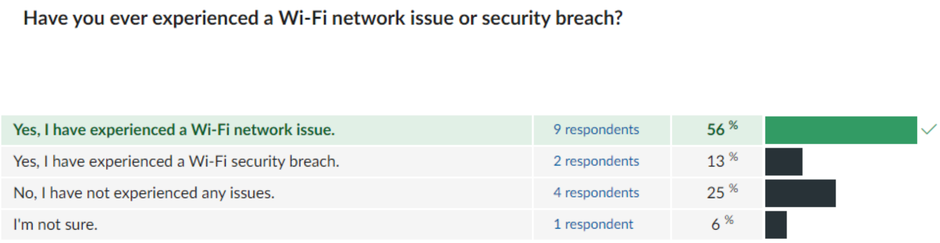
Would you be interested in learning about the latest threats and vulnerabilities in wireless networks?

Yes, definitely	12 respondents	**75 %**	✓
Maybe	3 respondents	19 %	
Probably not	1 respondent	6 %	
No, not at all		0 %	



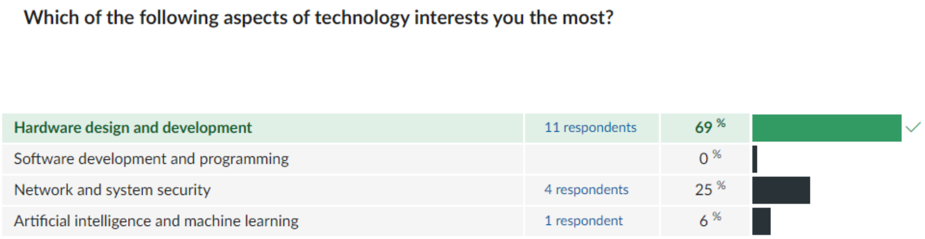
How interested are you in learning about the technical details of wireless network protocols?

Very interested	9 respondents	**56 %**	✓
Somewhat interested	5 respondents	31 %	
Not very interested	2 respondents	13 %	
Not interested at all		0 %	



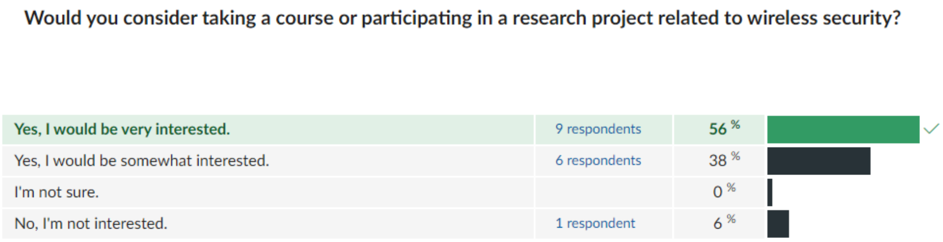
Have you ever experienced a Wi-Fi network issue or security breach?

Yes, I have experienced a Wi-Fi network issue.	9 respondents	**56 %**	✓
Yes, I have experienced a Wi-Fi security breach.	2 respondents	13 %	
No, I have not experienced any issues.	4 respondents	25 %	
I'm not sure.	1 respondent	6 %	



Which of the following aspects of technology interests you the most?

Hardware design and development	11 respondents	**69 %**	✓
Software development and programming		0 %	
Network and system security	4 respondents	25 %	
Artificial intelligence and machine learning	1 respondent	6 %	



Would you consider taking a course or participating in a research project related to wireless security?

Yes, I would be very interested.	9 respondents	**56 %**	✓
Yes, I would be somewhat interested.	6 respondents	38 %	
I'm not sure.		0 %	
No, I'm not interested.	1 respondent	6 %	