Importance of Cyber-Physical Security Training in Electrical Engineering Education

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/Cloud Computing and ML/DL for Communication Networks / CyberSecurity ensuring Power System Resilience.

Dr. Reza Kamali-Sarvestani, California State University, San Marcos

Dr. Reza Kamali-Sarvestani is the Founding Associate Professor of Electrical Engineering at California State University San Marcos. He earned his B.S. in Electrical Engineering from Shiraz University in Iran, and his M.S.E. and Ph.D. in Electrical and Computer Engineering from the University of Alabama in Huntsville. As an active participant in IEEE and ASEE, his research has received funding from the National Science Foundation (NSF), the Office of Naval Research (ONR), and various industry partners.

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 and he is an Associate Editor at the ACM Transactions on Privacy and Security. 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.

Dr. Hamed Nademi, California State University, San Marcos

Dr. Hamed Nademi is an Assistant Professor of Electrical Engineering at California State University-San Marcos (CSUSM). He worked as PI/Co-PI with industry-sponsored projects granted by New York State together with utility companies focusing on control solutions, 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-driven 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. He is a Senior Member of the IEEE.

Dr. Masood Parvania, University of Utah

Dr. Masood Parvania is currently the Roger P. Webb Endowed Professor and an Associate Professor at the Department of Electrical and Computer Engineering at the University of Utah. His research interests include the operation, economics and resilience of power and energy systems, modeling and integration of distributed energy resources, and modeling and operation of interdependent critical infrastructures. Dr. Parvania serves as an Associate Editor for the IEEE Transactions on Power Systems, and the IEEE Power Engineering Letters. He is the Chair of the IEEE Power and Energy Society (PES) Utah Chapter, and previously served as the Chair of the IEEE PES Bulk Power System Operation Subcommittee, and the IEEE PES Reliability, Risk and Probability Application (RRPA) Subcommittee.

Importance of Cyber-Physical Security Training in Electrical Engineering Education

Abstract In today's rapidly evolving technology, the integration of emerging topics and addition of new skills such as cyber-physical systems (CPS) and the Internet of Things (IoT), have become increasingly prevalent. These systems, ranging from smart grids to control systems, are foundational to the next wave of innovation in industries worldwide. As such, the inclusion of a cyber-physical security course module within an electrical engineering program is not just beneficial, but essential. This module would equip students with the necessary knowledge and skills to design, analyze, and secure CPS integrated with IoT devices against potential cyber threats. By understanding the vulnerabilities inherent to these systems and the techniques to counteract them, future electrical engineers will be better prepared to tackle real-world challenges, ensuring the resilience and safety of integrated systems in an interconnected world.

Incorporating modules related to cyber-physical systems, IoT devices, and their cybersecurity into electrical engineering courses requires a multidimensional approach, considering the convergence of hardware and software in such systems. Firstly, foundational knowledge in both control/embedded systems and cybersecurity should be established. These modules can begin with an introduction to the principles and architectures of CPS integrated with IoT devices, followed by an exploration of real-world applications like smart grids, control systems such as Programmable Logic controllers (PLC), and power systems such as motor controls. Next, practical labs can be introduced, allowing students to work with hardware platforms like Raspberry Pi or Arduino, alongside software tools to simulate and test CPS interactions. Emphasizing the significance of security, part of these modules can be dedicated to understanding vulnerabilities, threat modeling, and mitigation techniques specific to CPS. Finally, integrating case studies, hands-on testing environments, and guest lectures from industry experts can provide students with insights into real-world challenges and solutions, ensuring a holistic and applied learning experience. Collaboration with needs knowers in application security systems can also facilitate cross-disciplinary learning, further enriching the educational experience.

1. Introduction

The Internet of Things (IoT) represents a paradigm shift in the way that we interact and harness technology. IoT devices are nowadays embedded in our daily lives including home appliances, industries, transportation systems and healthcare domain, generating various amounts of data and enabling real-time communication between physical objects and the digital world. This interconnectivity introduces unprecedented opportunities for efficiency and innovation but it also exposes systems to multitude of cybersecurity threats. The integration of cybersecurity is not

only relevant for traditional critical infrastructures such as the power grid or water treatment plants, but absolutely necessary for the reliability of IoT devices and their interconnected ecosystem. In today's ever-evolving technology landscape, one undeniable reality stands out for the pervasive computing of the IoT. There is a growing imperative to incorporate cybersecurity training for both cyber-physical systems (CPS) and IoT technologies into EE education. As technologies like smart grids, control systems, and IoT devices become increasingly integral to industrial innovation, it is essential to educate future engineers on designing, analyzing, and securing these systems against cyber threats. Recognizing and addressing vulnerabilities in interconnected smart grid systems and IoT networks is crucial for maintaining security and effectiveness. Ensuring the security and IoT networks is paramount, as vulnerabilities in these interconnected systems can have far-reaching consequences. To meet this demand, various innovative approaches and tools have been developed and implemented to enhance CPS and IoT security training.

Various kinds of approaches and tools have been developed and implemented to enhance CPS-IoT security training which include: CPSA Tool Development [1] which is specifically designed to educate and train in cybersecurity, with focusing on the impact of cyber-attacks on physical power systems. This tool allows for attack modeling, simulating communication network protocols and detecting malicious activities in smart grids. However, the complexity of real-world CPS limits the effectiveness of its simulation results. Another initiative is the Collaborative Program at the University of Texas at El Paso [2], which is a partnership with the US Army's DEVCOM. This program integrates cybersecurity into the Electrical and Computer Engineering's normal curriculum. It involves new courses, modifications to existing ones, and capstone design projects. Despite its comprehensive approach, limitations include scalability to other institutions, dependency on external funding or cooperation, and the uncertainty regarding its long-term impact on students who are participating in the collaborative program. Additionally, Smart Grid Cybersecurity Education Platform [3] focuses on re-educating the power sector workforce through hands-on, active learning, and project-based approaches. Initial results have shown positive outcomes. However, there are concerns regarding the need for continuous updates, scalability, and the challenge of effective simulation of real-world threats in real-time. The Interdisciplinary Approach in Pittsburgh [4] shed light on the deficiency in existing education models for smart grid advancement, emphasizing the need for a holistic interdisciplinary approach that integrates cybersecurity, policy, economics, and technical skills. Nevertheless, the absence of empirical data on the workforce and the regional constraints of the study pose certain limitations. IoT Integration in Saudi Arabia [5] focuses on Saudi Arabia's Vision 2030 that explores incorporating IoT technologies into the EE curriculum, including practical workshops on Arduino and IoT. Although this study is limited in exploration of broader educational methods and specific regional focus. IoT Curriculum in STEM Education [6] conducts a multiple literature review to assess IoT curriculum, pedagogy, and assessment in STEM education. It reviews 60 articles, focusing on effective educational practices for implementing IoT curriculum but acknowledges limitations due to the evolving nature of IoT

technologies. CPS/IoT Infusion in Undergraduate EE Education [7] discusses enhancing undergraduate programs by integrating CPS and IoT. It proposes vertically integrated learning modules across four-year curriculum with an emphasis on project-based learning. Initially, positive feedback was received but this study has potential limitations including possible biases in student feedback, and implementing comprehensive curriculum changes. The IoT in CS Education [8] discusses the incorporation of IoT content into Computer Science (CS) education. They focus on enhancing educator's ability to integrate IoT into their curriculum by exploring new contents and teaching methods. It emphasizes the necessity of updating CS curriculum and discovering effective IoT teaching methods, while acknowledging the potential limitations in fully covering the rapidly evolving IoT technologies. IoT Education: Case Greenhouse Maintenance [9] examines an experimental course that combines problem-based and project-based learning which focuses on students developing IoT device prototypes for an urban rooftop greenhouse. They aimed to enhance learning effects through personal interest, competence, teamwork, and collaborative software skills. This work has potential challenges such as dependence on specific resources like a greenhouse and student engagement level of projects will be varied. IoT Hands-on Activities in Secondary Education [10] assesses the impact of IoT-based activities on STEM learning and career orientation among secondary school students. They involved students participating in a summer school, engaging in hands-on IoT activities. Results showed positive responses and increased interest in STEM fields and careers. Limitations of this study include a small sample size, short duration, and potential bias in self-reported data.

Overall, these initiatives aim to bridge the gap between traditional EE education and the rapidly evolving world of CPS and IoT technology. While each of these approaches has its unique focus and limitations, they collectively contribute to addressing the challenges posed by cybersecurity and IoT integration into EE education. However, the challenges identified in the aforementioned approaches include the difficulty of simulating real-world complexities, scalability and funding dependency, and difficulty to perform relevant studiesa about the impact of cybersecurity education in workforce development. For these reasons, there are still significant challenges and inherent limitations to overcome in order to ensure EE education is able to integrate CPS and IoT security in their curriculum for either undergraduate and graduate levels.

In this work in progress, novel CPS/IoT security education modules for EE are being defined accompanied with the description of a low-cost, accessible, and scalable embedded development kit. The proposed modules will address interdisciplinary topics necessary to understand the main cyber threats that CPS and IoT systems face, implement conventional cyber security measures specific for CPS and IoT systems, and tackle problems important for industry applications, while the embedded development kit will foster hands-on experimentation to build the necessary skills to close the existing workforce gap. Two case studies will be completed performed, California State University San Marcos will implement the modules into their existing undergraduate

curriculum while University of Utah will create three individual courses that will be part of graduate curriculum in EE. The project is being developed.

2. Problem Formulation and need of the survey

2.1. Challenges for cyber physical systems education in EE

The challenges facing cyber-physical systems (CPS) security education within Electrical Engineering (EE) encompass a spectrum of issues stemming from the growing integration of IoT devices, outdated curricula, and a deficiency in hands-on training. The proliferation of IoT devices across various sectors introduces unprecedented complexity to traditional EE education, requiring a paradigm shift in instructional approaches. However, many EE curricula struggle to keep pace with the rapid advancements in CPS and IoT technologies, resulting in outdated educational content that fails to adequately address current industry needs. Additionally, hands-on training, crucial for understanding the practical implications of securing interconnected systems, is often lacking in conventional lecture settings. This deficiency inhibits students from gaining essential practical skills in identifying and mitigating cybersecurity risks within CPS and IoT environments, leaving them unprepared to tackle real-world challenges in the field. As a result, there is an urgent need for innovative educational strategies that prioritize experiential learning and reflect the evolving demands of the cybersecurity landscape within EE programs.

On the other hand, the cybersecurity industry is grappling with a significant workforce gap, a dilemma exacerbated by the rapid evolution of digital transformation and the increasing sophistication of cyber threats. As highlighted in a report by Federal News Network [11] despite ongoing efforts, it still presents formidable challenges in resolving this pressing issue. Forbes [12] underscores the severity of the situation in its analysis, pointing out the widening talent gap and its implications for organizations worldwide in 2022. With the demand for skilled cybersecurity professionals surpassing the available talent pool, organizations are left vulnerable to cyberattacks, risking sensitive data breaches and financial losses. Furthermore, the shortage persists despite extensive recruitment initiatives, as reported by CSO [13], with the cybersecurity workforce deficit reaching a staggering. These statistics underscore the urgency for comprehensive strategies to address the shortage and fortify defenses against evolving cyber threats. The cybersecurity Workforce Study [14] provides deeper insights into the complexities of the workforce gap, shedding light on the multifaced challenges by the cybersecurity industry. The study emphasizes the critical need for collaborative efforts from government agencies, educational institutions, and private sector organizations to bridge the gap and cultivate a robust cybersecurity workforce. Addressing these gap requires interdisciplinary and translational approaches, such as expanding cybersecurity education and training programs, promoting diversity and inclusion within the field, and fostering mentorship opportunities for aspiring professionals. By addressing the root of the workforce shortage and investing in long-term

solutions, the cybersecurity industry can better equip itself to navigate the evolving threat landscape and safeguard digital assets effectively.

2.2. Rationale of The Project Through Survey of Students

Understanding student perspectives through surveys is crucial in evaluating the need for integrating cyber-physical system (CPS) modules into electrical engineering education. Surveys serve as an effective tool for gauging student interest and potential engagement with CPS content. Students' engagement directly influences enrollment, retention, graduation, and future employment outcomes. Student feedback plays an important role in shaping curriculum development to meet their needs and expectations. To accurately assess the demand for CPS modules, quantitative surveys were employed in this paper. Quantitative surveys provided statistical insights into students interest levels and their understanding of the relevance of CPS in their future careers. These surveys were designed to explore students awareness of CPS, their perception of its importance in the current technological landscape, and the potential impact on their career readiness. Our surveys helped identify gaps in existing curricula and guide our project in developing CPS modules that are both academically challenging and aligned with industry needs. The use of CPS to develop modules for Programmable Logic Controllers was one of the decisions that we made to be industry relevant in our project.

Analysis of Surveys at the University of Utah and California State University San Marcos

The current educational landscape in cyber-physical systems (CPS) presents a complex yet critical scenario, particularly in the field of electrical engineering. The appendix of this paper provides the pie-charts of surveying Electrical engineering students at the University of Utah and California State University San Marcos regarding CPS in their engineering pathway. The charts helped us to quantitatively measure the effect of CPS and plan the educational modules and projects based on students' interests. In these surveys, 9 EE students from California State University San Marcos and 13 EE students from the University of Utah were randomly selected to answer the survey questions.

The data reveals major facts: while a significant (45%) of students are not aware of CPS and 41% of students are just somewhat aware of it. An overwhelming 95% acknowledge its importance. This extends to their desire to learn CPS topics while 68% have not learned about CPS but express a keen interest in doing so. Students mentioned that the perceived relevance of CPS to all areas of electrical engineering is notably high (68%), underscoring its integral role in the field. Furthermore, the majority of students (73%) believe that knowledge in CPS would enhance their skills, innovation capabilities, and security awareness, which is essential in the rapidly evolving technological landscape. However, there seems to be a perceived gap in industry expertise, with 77% of students uncertain or affirming the existence of such a gap. This perception could potentially influence their career choices and academic pathways.

From an academic standpoint, the data suggests that integrating CPS into the curriculum could have substantial impacts on enrollment, retention, and graduation rates. A notable 59% of students feel that the rapidly evolving nature of CPS, insufficient resources, and lack of qualified instructors are challenging. Yet, there is a strong interest in engaging with this field through projects and courses. Specifically, 32% are interested in related projects, 9% in courses, and a significant 50% see the value in a combination of both. This interest could be leveraged to increase student engagement and retention. In terms of career aspirations, 68% are considering a CPS-related career, though 32% remain unsure, indicating the need for more informative and practical exposure to the field. The potential impact of CPS training on students sense of belonging is substantial, with 77% believing it would increase their sense of belonging to a moderate or significant extent. Lastly, 64% think such training would influence their likelihood of completing their electrical engineering degree, and 77% show interest in related capstone projects. These insights suggest that integrating CPS more comprehensively into the electrical engineering curriculum could not only enhance student knowledge and skills but also positively influence their academic journey and career prospects.

3. Cyber-Physical Systems Security Education in EE

Three different courses are being designed to provide education and training in CPS and IoT security. Each course is divided in different modules that are accompanied by a wide variety of hands-on experiments to allow students to clearly understand different concepts and apply them in realistic scenarios. The following is a summary of the three courses and the embedded development kit for hands-on experimentation:

- **Fundamentals of Cyber-Physical Systems Security and IoT for Electrical and Computer Engineering**

This class introduces the core principles and characteristics of cyber-physical system security enabling students to understand the interdependence between cyber, physical, and control components integrated to manage their operation. Students will learn how emerging technologies such as IoT devices enable the operation of physical systems. Furthermore, students will learn theoretical foundations for modeling and control of cyber-physical systems along with the fundamental principles of communication networks and packet inspection for industrial-level operations and IoT device integration. Students will be able to comprehend the different vulnerabilities that emerge in cyber-physical systems and how attacks in cyber components affect the physical system. Furthermore, students will develop adversarial thinking, which is the ability to embody the technological capabilities, unconventional perspectives, and strategic reasoning of hackers, through lectures and experimental applications. Hands-on experimentation will allow students to use multiple modeling tools to characterize a physical process (e.g., second-order DC motor), and then utilize the embedded development kits (see Fig. 1) to implement these models and test different feedback controllers. Using the communication interfaces in the development

kits, students will capture communication traffic and implement several cyber attacks including port mapping and ARP poisoning. Students will be able to analyze network traffic, launch cyber attacks, and observe the impact of these attacks on the operation of the physical system. Block diagram of the laboratory experiment is illustrated in Figure No.1.

- **Preventive and Proactive Cyber-Physical Security**

In this course, the students will learn and implement a variety of security mechanisms. Students will be capable of understanding the costs, benefits, and limitations of security mechanisms depending on the application, starting with best practices of IT network security, and then including more sophisticated defense mechanisms. Particularly, students will learn the basic principles of machine learning and AI to develop supervised and unsupervised applications for the detection and localization of cyber attacks using cyber and physical data. Students will be exposed to emerging proactive security mechanisms such as moving-target defense, security-by-design, attack mitigation, and automatic recovery. The students will use the embedded development kits to implement basic preventive security strategies such as firewalls and network access control in IoT devices. Students will capture network traffic and then use SNORT for basic packet inspection. Then, students will use a data set from testbeds and partner utilities to develop machine learning and AI tools to analyze and test various anomaly detection strategies, including signature-based and physics-based methods, to detect the studied cyber attacks. The data set will include normal operation of the system as well as predefined attack scenarios.

- **Advanced Capstone Project**

In the Advanced Capstone course, the students will form teams and will be assigned projects of relevance for industrial applications, such as autonomous vehicles, water treatment plants, and the power grid. Each team would have to apply the different tools obtained in the other two classes to model the target system, identify vulnerabilities, launch cyber attacks, and then implement defense strategies according to the system-specific characteristics. Students will be able to face realistic scenarios, determine the best possible defenses, and then implement them through the embedded development kits. A professor will guide the entire process. Industry partners will provide insights and feedback to the students throughout the definition and development of the project.

- **Embedded Development Kit:**

The general architecture of the embedded development kit is described in Fig. 1. The process is designed for end-to-end control of a physical system (e.g., a DC motor) using a PID (Proportional-Integral-Derivative) controller within a PLC (Programmable Logic Controller). Microcontrollers with communication capabilities are used to enable the WiFi communication

between the PLC and actuators/sensors from the physical system. A picture of the test setup is provided in Fig. 2.

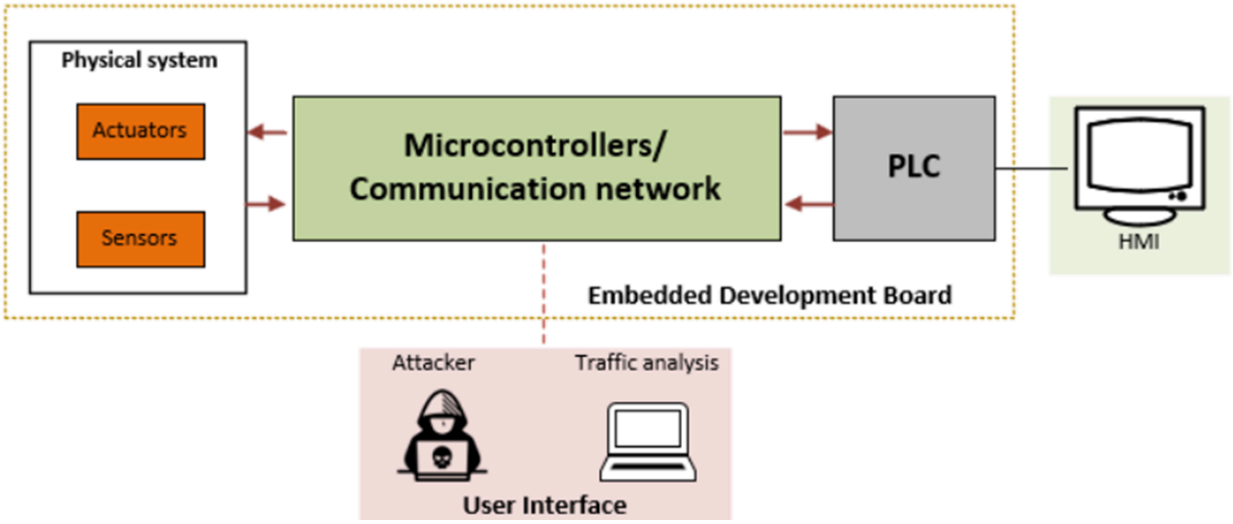


Figure 1: General architecture of the embedded development kit

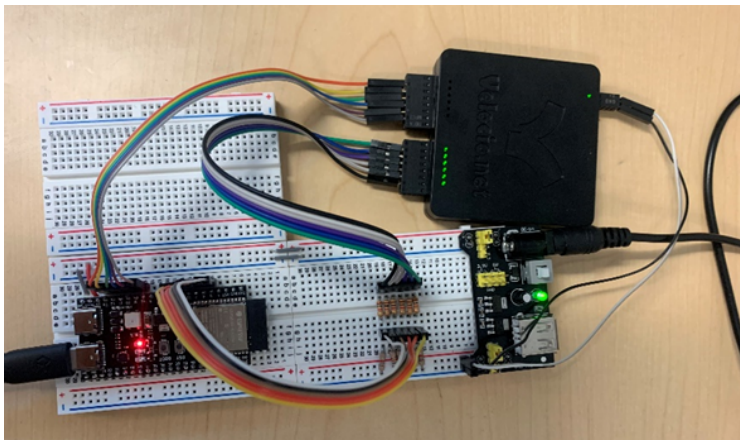


Figure 2. Test setup that interconnects the PLC and WiFi for Cyber-Physical systems attack.

The initial tests conducted with the embedded development kit shows its potential in facilitating the students to understand the real effects of cyber attacks within an educational context. The setup utilized Modbus communication between IoT devices, both equipped microcontrollers, to exchange binary bit information. This allowed students to grasp the fundamentals of Modbus master-slave communication, where one device initiates communication (Modbus Master), and the other (Modbus Slave) responds, making it a valuable learning experience in networking

principles. Also, Wireshark program provides a visual representation of network activities, making it a valuable tool for understanding the mechanism of ARP Spoofing attacks.

Furthermore, the experimentation includes simulations of cyberattacks, specifically ARP Spoofing and False Data Injection attacks, to highlight the importance of cybersecurity in real-world applications. ARP Spoofing, a technique in which an attacker manipulates the Address Resolution Protocol (ARP) to link their MAC address with a legitimate device's IP address, was employed to demonstrate unauthorized access and interception of network packets. Using Wireshark, we can observe the ARP Request and ARP Response packets during network communication and notice the sudden appearance of forged ARP Responses during an ARP Spoofing attack. This manipulation of ARP packets effectively allows the attacker to intercept and control network traffic, demonstrating the unauthorized access and interception of packets. Additionally, the False Data Injection attack, a consequence of ARP Spoofing, shows the ability to manipulate and deceive data being sent or received by victim devices. These cyber attacks prove the critical need for cybersecurity education and awareness, emphasizing the role of the embedded development kit in helping students comprehend the practical implications of such threats.

3.1. Case Study: California State University San Marcos (Undergraduate-level modules)

Integrating CPS security education into existing courses

The modules that conform the course material introduced above along with the embedded development kit are being integrated into the EE undergraduate courses at CSUSM. The integration of cyber-physical systems (CPS) into electrical engineering education represents a step toward enhancing student enrollment, retention, graduation rates, and future employment opportunities. Cyber-physical systems are increasingly widespread in various sectors, including manufacturing, healthcare, and transportation [15]. By embedding CPS-focused modules into the curriculum, educational institutions can offer a more relevant and attractive program to prospective students. This relevancy is crucial in a technological landscape where the demand for skilled professionals in CPS is rapidly growing. Furthermore, the practical and interdisciplinary nature of CPS can increase student engagement, which is a significant factor in student retention and success in higher education [16].

The inclusion of CPS modules in electrical engineering courses also promotes a deeper understanding of contemporary engineering challenges and solutions. The synergy between computational and physical elements in CPS requires a unique set of skills that traditional electrical engineering programs may not sufficiently provide [17]. By incorporating CPS modules in this project, students are better prepared for the complexities of modern engineering tasks, improving their problem-solving skills and technical knowledge. This comprehensive skill set not only contributes to higher graduation rates due to increased student competence and confidence but also makes graduates more competitive in the job market. Three modules of CPS

are being developed and added to existing courses of Clinics of Electrical Engineering I, Electric Power and Renewable Energy, and Communication Systems and Circuits. This helps to provide CPS education in entry, transitory, and mastery level of Electrical Engineering education.

Employers are increasingly seeking candidates with a robust understanding of CPS, as these systems play a crucial role in advancing technological innovation and efficiency. The future landscape of employment in engineering underscores the necessity of CPS education. The U.S. Bureau of Labor Statistics (2023) projects a steady increase in engineering jobs emphasizing the integration of computing and physical systems [18]. By equipping students with CPS knowledge and skills, the program of Electrical Engineering at California State University San Marcos directly contributes to their future employability in a dynamic and evolving job market. Moreover, CPS education fosters critical thinking, creativity, and collaborative skills, which are essential in addressing the interdisciplinary and complex problems of the 21st century [19]. Thus, the addition of CPS modules in electrical engineering education is not only beneficial but imperative for preparing students to meet the demands and challenges of their future professional careers.

Conclusions

This research emphasizes the importance of understanding student perspectives through surveys to effectively integrate CPS modules into electrical engineering education. The findings reveal a clear demand for CPS knowledge among students, highlighting its relevance to their future careers and the engineering field at large. By responding to these educational needs, universities can better prepare students for the challenges of the 21st-century technological landscape, ultimately contributing to their success and the advancement of the engineering profession. The projects and course modules being developed by California State University San Marcos and the University of Utah serve as models for other institutions aiming to enhance their engineering programs and better serve their students and society.

References

[1] S. Neetesh, K. Vasilis, and K. Neeraj, “Cyber-physical smart grid security tool for education and training purposes,” *in International Workshops: Realigning Cyber Security Education*, 2017

[2] V. Gonzalez, O. Perez, and R. Romero, "Collaboration program to disseminate cybersecurity in the ECE curriculum," *in 2022 IEEE Frontiers in Education Conference (FIE)*, October 2022

[3] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, “Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application,” *in 2014 IEEE Frontiers in Education Conference (FIE)*, pp. 1–9

[4] A. Velagapudi, K. Kelly-Pitou, D. W. Tipper, and G. Reed, “Updating the Smart Grid Workforce Education and Training Process: An Interdisciplinary Approach,” *in 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb. 2019

[5] Fahd Alharbi “Integrating internet of things in electrical engineering education,” *International Journal of Electrical Engineering & Education*, Feb. 2020

[6] P. Abichandani, V. Sivakumar, D. Lobo, C. Iaboni, and P. Shekhar, “Internet-of-things curriculum, pedagogy, and assessment for stem education: A review of literature,” *IEEE Access*, vol. 10, pp. 351–369, 2022

[7] L. Hong, L. Keel and C. McCurry, “Work-in-Progress: Enhance Undergraduate Electrical Engineering Education with CPS/IoT Infusion,” *in ASEE Annual Conference,* July 2021

[8] B. Burd, L. Barker, M. Divitini, J. Guerra, F. Perez, I. Russell, B. Siever, L. Tudor, M. McCarthy and I. Pollock “The Internet of Things in CS Education: Updating Curricula and Exploring Pedagogy.” *In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, ITiCSE 2018, Association for Computing Machinery (ACM), July 2018

[9] H. Mäenpää, S. Tarkoma, S. Varjonen and A. Vihavainen, ``Blending problem- and project-based learning in Internet of Things education: Case greenhouse maintenance," *in SIGCSE '15: Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, February 2015, pp. 398–403

[10] D. Glaroudis, A. Iossifides, N. Spyropoulou, I. D. Zaharakis, and A. D. Kameas, ‘‘STEM learning and career orientation via IoT handson activities in secondary education,’’ *in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 480–485

[11]https://federalnewsnetwork.com/federal-report/2023/12/wil-2024-bring-some-resolutions-for-the-cyber-workforce-problem/

[12]https://www.forbes.com/sites/forbestechcouncil/2022/01/28/the-widening-cybersecurity-talent-gap-and-its-ramifications-in-2022/?sh=2f3f70bc5398

[13]https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html

[14]https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

[15] E. A. Lee, “Cyber physical systems: Design challenges,” *in 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363–369.

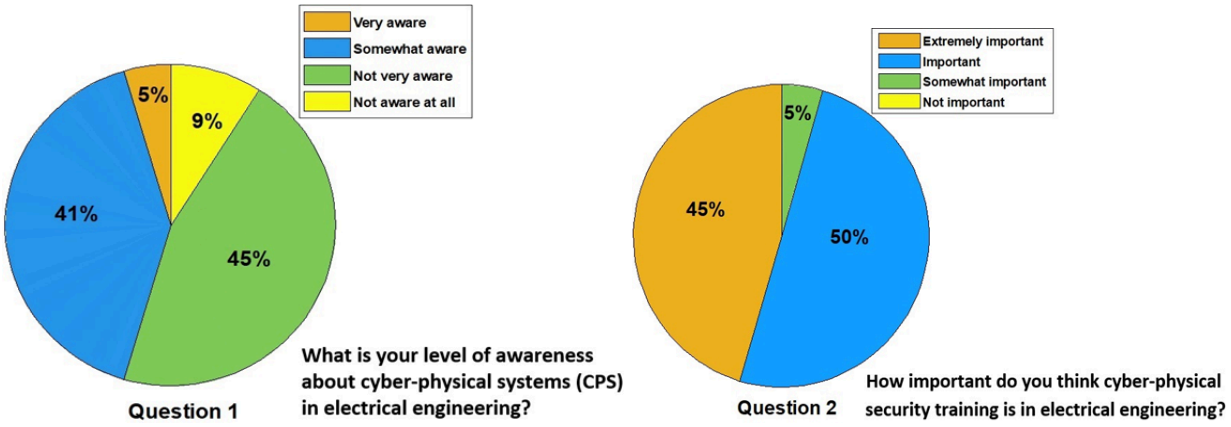
[16] J. M. Braxton " Review of Leaving College: Rethinking the Causes and Cures of Student Attrition," *Journal of College Student Development*, Volume 60, January 2019, pp. 129-134

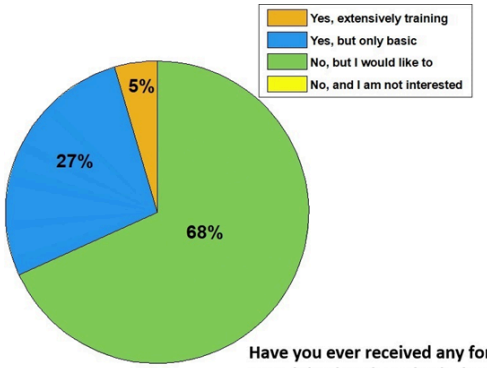
[17] R. Rajkumar, L. Lee, I. Sha, and J. A. Stankovic, “Cyber-physical systems: the next computing revolution,” *in Proceedings of the 47th design automation conference*, 2010, pp. 731–736.

[18]https://www.bls.gov/ooh/architecture-and-engineering/electrical-and-electronics-engineers.htm

[19]https://nap.nationalacademies.org/catalog/10999/the-engineer-of-2020-visions-of-engineering-in-the-new

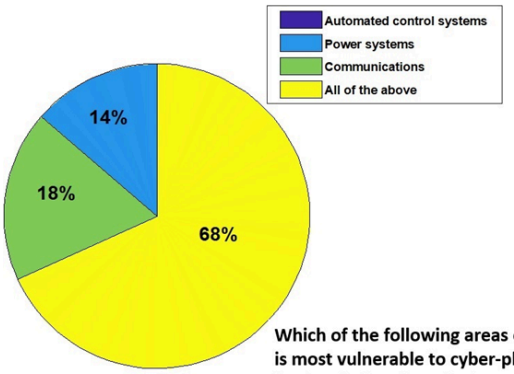
Appendix





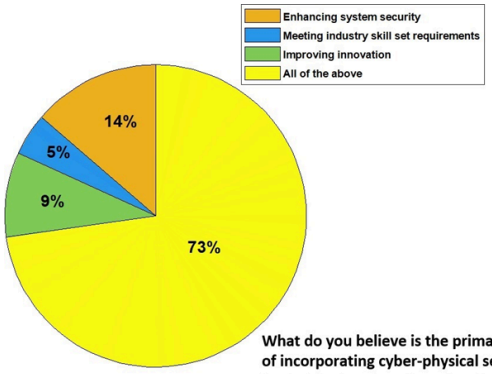
Question 3

Have you ever received any formal education or training in cyber-physical security?



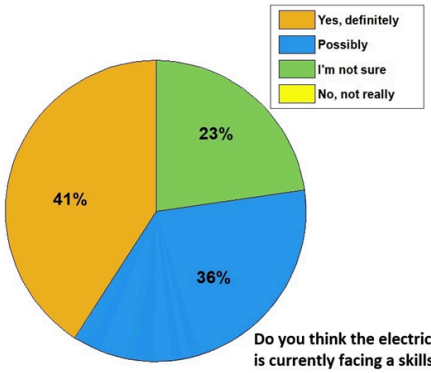
Question 4

Which of the following areas do you believe is most vulnerable to cyber-physical threats in electrical engineering?



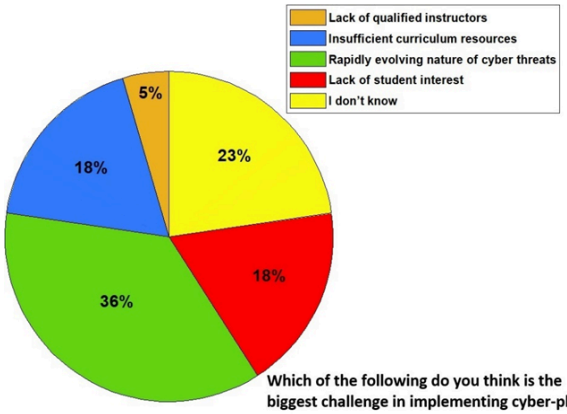
Question 5

What do you believe is the primary benefit of incorporating cyber-physical security training in electrical engineering education?



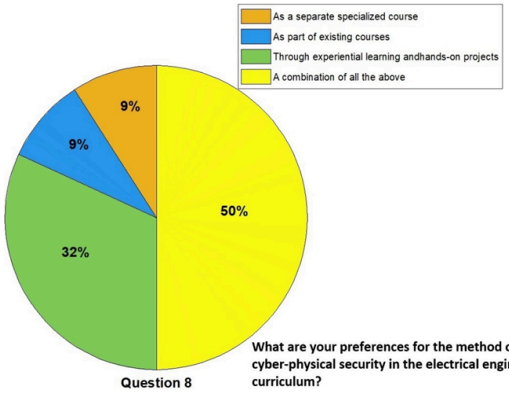
Question 6

Do you think the electrical engineering industry is currently facing a skills gap in terms of cyber-physical security expertise?



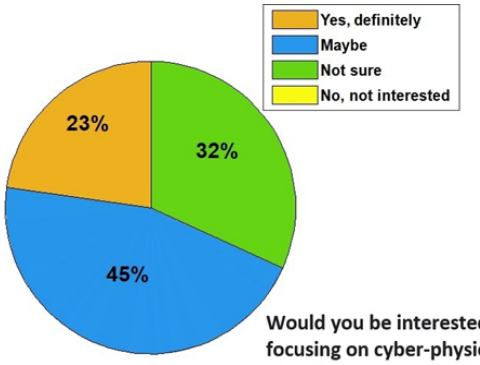
Question 7

Which of the following do you think is the biggest challenge in implementing cyber-physical security training in electrical engineering education?



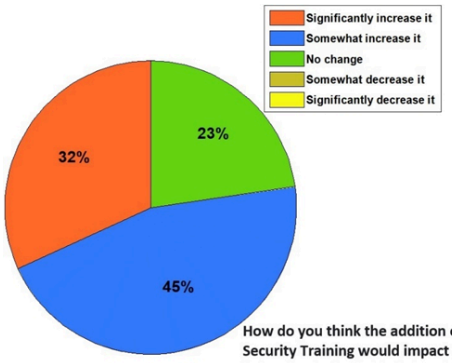
Question 8

What are your preferences for the method of learning cyber-physical security in the electrical engineering curriculum?



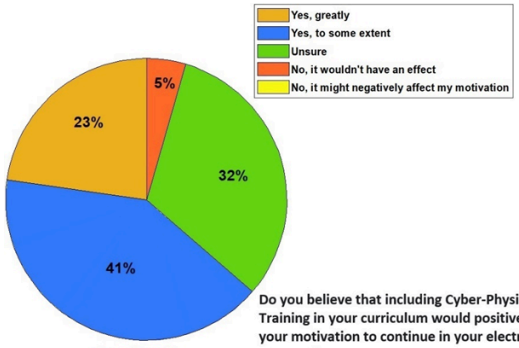
Question 9

Would you be interested in a career path focusing on cyber-physical security within electrical engineering?



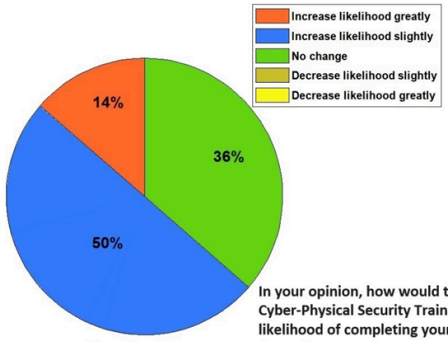
Question 10

How do you think the addition of Cyber-Physical Security Training would impact your sense of belonging in the field of electrical engineering?



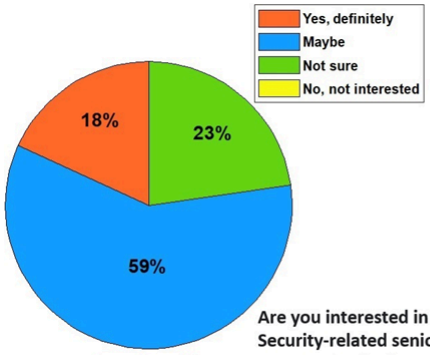
Question 11

Do you believe that including Cyber-Physical Security Training in your curriculum would positively affect your motivation to continue in your electrical engineering program?



Question 12

In your opinion, how would the integration of Cyber-Physical Security Training influence your likelihood of completing your electrical engineering degree?



Question 13

Are you interested in doing a Cyber-Physical Security-related senior capstone project toward your graduation?