Network Attacks on Cyber–Physical Systems Project-Based Learning Activity

Paul J. Frontera and Erick J. Rodríguez-Seda

***Abstract*—*Contribution:* This article presents a project-based learning (PBL) activity for use in the instruction of network attacks on cyber–physical systems. Student learning is analyzed to determine the project's contribution to learning outcome attainment.**

***Background:* The literature contains a significant amount of research on the benefits of PBL as a technique that enhances student attainment of learning outcomes. However, minimal published work currently exists on the use of PBL activities in cybersecurity of control systems curricula.**

***Intended Outcomes:* The proposed activity is intended to facilitate student attainment of cybersecurity curriculum learning outcomes and for use in assessing student learning.**

***Application Design:* A group PBL method is selected to develop student teamwork in addition to attaining technical learning outcomes. Project design seeks to minimize laboratory costs while providing flexibility for future enhancement.**

***Findings:* Analysis of the proposed activity shows that students are able to attain specified learning outcomes at or above expectations and are engaged while completing the activity.**

***Index Terms*—Cyber–physical systems (CPS), cybersecurity, engineering, networked control systems, project-based learning (PBL).**

I. Introduction

USE OF project-based learning (PBL) methods in undergraduate education have expanded over the past decade. Bédard *et al.* [1], Ríos *et al.* [2], and Kokotsaki *et al.* [3] described the value of PBL activities to develop student understanding of material. This article describes a PBL activity that facilitates student investigation of cyber threats to a networked cyber–physical system (CPS) and analyzes student attainment of learning outcomes based on cybersecurity program criteria.

The term CPS colloquially refers to a system that integrates computing, communication, and control technologies to regulate the performance of a physical process [4]. A typical CPS is comprised of multiple spatially distributed nodes (e.g., sensors, actuators, computers, and controllers) that share information (e.g., commands and measurement signals) with the aim of regulating some physical quantity [5]. CPSs are often referred to as networked CPSs when different nodes are integrated via a common communication network.

PBL techniques are shown useful to introduce students to the challenges associated with the design and operation of a CPS. A number of authors (e.g., [6]–[9]) present virtual CPS PBL activities. Other authors (e.g., [10]) present physical CPS PBL activities. However, the literature lacks depth in CPS PBL activities designed to inform students on CPS security concerns outside of specialty industrial control systems (ICS) [11], [12].

The presented PBL activity is performed by United States Naval Academy (USNA) second-year undergraduate cybersecurity program students in the Cyber Operations major. The activity introduces students to the detailed consequences of interrupting or modifying the control of a physical process while stoking student creativity to potential defensive measures. Each student team designs and implements a controller to position a single-link robotic arm, investigates system response to instructor initiated cyber attacks, and proposes approaches to defend the CPS. Students first simulate the CPS using a MATLAB Simulink model and then implement their software solution on a provided hardware testbed. Testbed details are provided in [5].

II. Introductory Course on the Control of CPSs

The USNA Cyber Operations major provides students fundamental technical understanding of computer architecture, programming, data structures, networks, cryptography, and forensics. Additionally, students are exposed to policy, law, and ethics of conducting cyberspace operations. Enrolled students are required to complete a control systems engineering course geared toward CPSs during the spring semester of their second year. The course, named Cyber Systems Engineering, introduces students to the control of CPSs and the vulnerabilities and cyber threats these systems face.

The course focuses on the interplay between the physical and cyber domains and covers several topics, including modeling of physical systems, transfer functions, stability, embedded systems, programming, actuators and sensors, classical control, cyber security, and communications, among others. A complete list of topics in chronological order is given in Table I. The syllabus follows a structure of two 50-min lectures and 110-min hands-on laboratory sessions per week for a total of 16 weeks. The sessions are devoted to teaching engineering and cyber fundamentals with hands-on projects distributed across all 16 weeks. Students in the

Manuscript received November 25, 2019; revised June 1, 2020; accepted July 27, 2020. Date of publication September 1, 2020; date of current version May 5, 2021. This work was supported in part by the Center for Cyber Security Studies at USNA under Gift Fund 87050. *(Corresponding author: Paul J. Frontera.)*

The authors are with the Weapons, Robotics, and Control Engineering Department, United States Naval Academy, Annapolis, MD 21401 USA (e-mail: frontera@usna.edu; rodrigue@usna.edu).

Digital Object Identifier 10.1109/TE.2020.3014268

TABLE I
CYBER SYSTEMS ENGINEERING TOPICS

Topics	Lecture Hours	Lab Hours
Intro to CPSs and Mechatronics	1	–
Industrial Control Systems and SCADA Systems	2	–
Modeling of Physical Systems	1	2
Laplace Transform and Transfer Functions	2	2
Time System Response and Stability	2	2
PID Control	2	2
Sensors and Actuators	3	2
Embedded Systems and Microcontrollers	2	3
Communications	2	2
Mid-Term Control Experiment Project	–	8
Controller Area Network (CAN)	1	–
Networked Control Systems (NCS)	1	2
Cyber Attack Models	2	1
Attack Detection and Resilient Control	1	–
Final PBL Activity	–	10

course are assumed to have some familiarity with computer programming, physics, and calculus but no prior experience with electrical systems, robotics, communications, dynamics, or differential equations.

A. Learning Outcomes

The course adopted the learning outcomes established by ABET for Cybersecurity programs in November 2018. ABET, a leading international organization that accredits computer and engineering undergraduate education programs, including the Cyber Operations major at USNA, under the Cybersecurity criteria, has defined the following set of student learning outcomes [13]. All graduates of the program should have the ability to:

- O1) analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions;
- O2) design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline;
- O3) communicate effectively in a variety of professional contexts;
- O4) recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles;
- O5) function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline;
- O6) apply security principles and practices to maintain operations in the presence of risks and threats.

The course also adapted two additional set of outcomes suggested by the Cyber Physical Systems Virtual Organization (CPS-VO) during their first international workshop on CPS education [14] to better reflect the hybrid nature of the course, i.e., the intersection between control in the physical domain and cyberspace. In addition to learning outcomes O1–O6, a graduate of the program should have an ability to:

- O7) design and conduct simulations and tests of a CPS and analyze results;
- O8) understand how design decisions in the cyber domain affect the physical domain and vice versa.

All outcomes are regularly assessed throughout the course via homework assignments, laboratory activities, and written exams.

B. Teaching of Cyber Threats and Cyber Security in CPSs

In contrast to traditional mechatronics and control engineering courses and PBL exercises [15]–[21], the Cyber Systems Engineering course not only introduces students to the design, synthesis, control, and analysis of CPSs but also to the execution, protection, and evaluation of network-based attacks. Throughout the semester, with an in-depth focus during the course's final month, students are: 1) lectured on the operation and consequences of cyber attacks on control systems; 2) presented with measures to prevent, detect, and recover from such attacks; and 3) asked to discuss current related events, news, and technologies. The course culminates with a final PBL activity that provides students an opportunity to design and launch network-based attacks on a controller area network (CAN) connected robotic system and evaluate the impacts. The project is designed to reinforce all course learning outcomes from Section II-A, except for learning outcome O4.

III. NETWORKED CPS TESTBED PBL ACTIVITY

The course culminates with a PBL activity designed to both enable and assess student achievement of the learning outcomes detailed in the previous section. The PBL activity follows a guided approach, where specific tasks and milestones are used to guide students through the project [22]. According to [21], [23], and [24], research shows that following a guided approach for introductory engineering and computer science courses can be more effective in learning than unguided instructions. The PBL activity presented herein provides students an opportunity to witness the physical effects of cyber threats on a networked control system and to explore creative protective and mitigation measures in a structured scheme. Examples of similar guided PBL activities focused on other topics of engineering and computer science education include [20], [21], and [25]–[27].

The networked CPS testbed introduced in [5] and shown in Fig. 1 is used to facilitate the PBL activity. The testbed consists of three NXP LPC1768 microcontrollers that are connected using a CAN bus to position a single-link robotic arm. The mbed OS microcontrollers (μC) shown in Fig. 1 are programmed using C++ and used to prepare the students for follow-on major courses. A preferred microcontroller/programming language combination could be substituted to meet other program's objectives.

The testbed arrangement is selected to represent a networked control system that has actuation, process observation, and control law implementation physically separated. Fig. 2 provides a functional block diagram detailing the network connections. The single-link actuator process provides the student with visual feedback. This process was selected for its low-cost implementation (approx. $400 per unit), robustness to

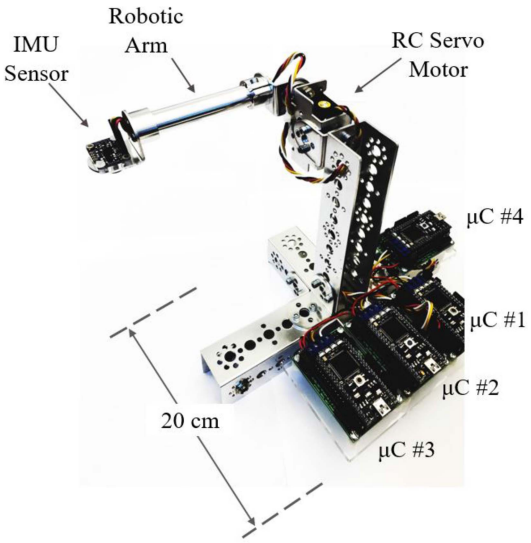

Fig. 1. Networked CPS testbed.

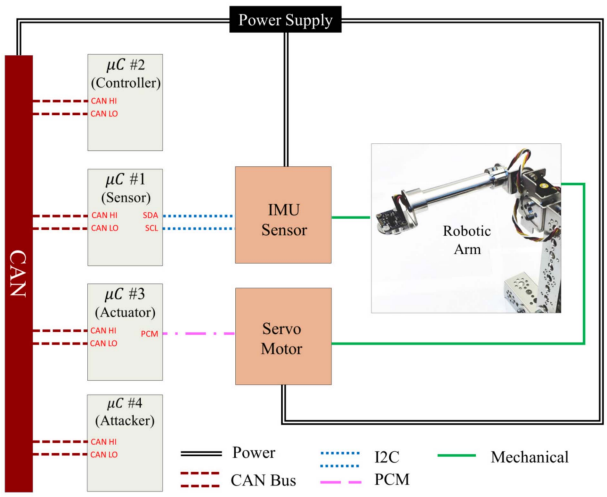

Fig. 2. Networked CPS functional block diagram.

student implementation errors, reproducibility and repeatability of experiments, and consistency among units. Additionally, the testbed's compact size and portability make it suitable for any type of classroom.

A fourth microcontroller attached to the CAN bus, shown in Fig. 1, allows for the student to inject a cyber attack on the control network. The cyber attack is inserted using a dedicated microcontroller to facilitate instructor verification that the CPS testbed is properly functioning prior to the insertion of a cyber attack.

Compiled instructor-written code is provided to the students for the sensor (μC#1) and actuator (μC#3) microcontrollers. This ensures student focus on controller design and cyber attack development. The PBL activity could be expanded to require students to develop code to accomplish these functions as necessitated by learning outcomes. Students are required to develop code to accomplish the controller (μC#2) and cyber attack (μC#4) functions.

A. Cyber Attacks

In order to investigate the implementation and effects of cyber attacks, students are asked to execute two types of deceptive data attacks on the networked CPS launched from the fourth microcontroller: 1) a stealth attack and 2) a replay attack [28]. Both attacks assume that the attacker has access to the physical components or to the communication network.

1) Stealth Attack: A stealth attack is one in which the attacker modifies sensor data being reported to the controller by injecting a small error. The error signal is typically designed to be undetected by conventional fault and false data detectors. The attacker does not need to know the dynamics of the plant and, as shown in [29], even small errors can bring the system to an unsafe state.

2) Replay Attack: A replay attack is one in which the attacker injects previously recorded sensor data from a stable operating state into the control system [30], [31]. This type of attack can easily elude conventional fault detectors given that the attack signal has the same statistical characteristics of a normal signal. Different from other replay attack models [28], the one implemented in the PBL activity does not simultaneously report false control data to the actuator.

Similar to a stealth attack, a replay attack does not require knowledge of the dynamics of the plant. However, the effects of a replay attack can be more significant given that a replay attack breaks the feedback loop.

B. MATLAB Simulation

Students begin the PBL activity by first simulating the system using MATLAB Simulink software. A Simulink custom library is provided to the students with blocks that mimic the functionality of each microcontroller, the servo actuator, the inertial measuring unit, the CAN bus, and robot arm. The simulation is included to aid in student visualization of the connections between each testbed component as shown in Fig. 2.

Students are asked to design and implement a proportional–integral (PI) controller to regulate the position of the robotic arm steady at 0 rad while meeting desired performance specifications. The simulated controller is tested under receipt of process information of varied noise and for disturbance rejection capability. Fig. 3 shows an example of the simulation exercise where students are asked to compare the closed-loop response of the system under different measurement noises. The noise is modeled as a Gaussian distribution with zero mean and a standard deviation of σ rad. It can be observed in the simulation how an increase in noise affects the performance of the closed-loop CPS. The simulation exercise also explores the effect of two-step disturbances at 10 and 20 s to test the capabilities of the PI controller to recover after external disturbances. By comparing the same controller under different scenarios, the student gains an appreciation for system response under different nominal conditions.

The MATLAB simulation is performed to increase student understanding of networked control system implementation and establish expectations for proper system functionality prior

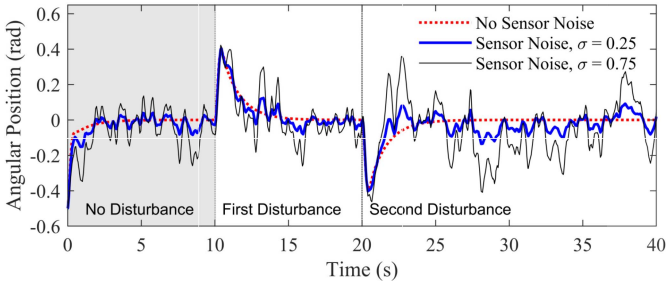

Fig. 3. Comparison of PI closed-loop system response with and without sensor measurement noise. A positive and a negative disturbance are applied at 10 and 20 s, respectively. The noise follows a Gaussian distribution with zero mean and a standard deviation of σ rad.

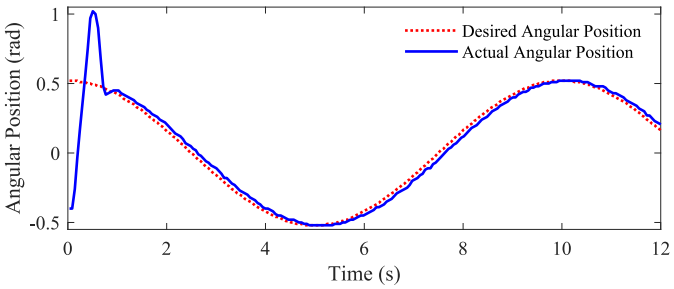

Fig. 4. Sine wave trajectory tracking using a PI controller. The dotted line represents the desired sine wave trajectory, while the solid line illustrates the system response.

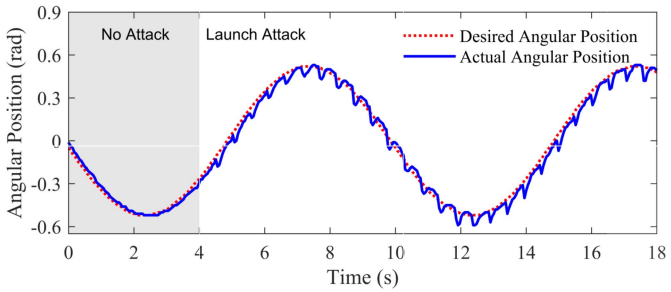

Fig. 5. Response of the networked CPS to a stealth attack. The dotted line represents the desired sine wave trajectory, while the solid line illustrates the system response.

to implementing the networked CPS with hardware. Students additionally simulate cyber attacks on the system of varied magnitude and frequency to gain familiarity with the anticipated CPS response under attack.

C. Physical Implementation

Networked control system implementation for the testbed CPS requires students to consider how the ideas presented in lecture and simulation are realized in hardware. Students are given a series of tasks to complete the physical implementation. The first task asks students to read arm angle position transmitted on the CAN bus from μC#1. This effort introduces students to implementation of CAN bus messaging while simultaneously emphasizing the fundamental difference between networked control systems and control systems implemented during prior course activities. Basic C++ instructions for CAN implementation are provided as guidelines but required code development is left to the students.

Once able to read the measured arm position, students implement the messaging required to position the arm at the desired angle. A control law is not immediately implemented since an RC servo motor is used to position the arm. The servo motor internal feedback control system is capable of holding the arm in an ordered position.

Students are then required to design and implement a PI controller on a microcontroller. This process forces student consideration of control loop frequency. Students also need to iteratively evaluate the time response of the system and redesign the gains of their PI controller in order to meet performance specifications, that is, an overshoot of less than 10% and a settling time between 2 and 3 s. After selecting PI gains and verifying performance meets required specifications, students are able to physically experience controller response and disturbance rejection by simply tilting the testbed base.

After completion of the step response portion of the activity, students are tasked with modifying their control code to track a sine wave of 10-s period in real time as shown in Fig. 4. A sine wave is used instead of a step response to increase perceptibly of the replay cyber attack.

Following the implementation of the PI controller, the PBL activity focus shifts to demonstrating cyber attacks on the networked control system. A stealth cyber attack is inserted using μC #4 by injecting false measurements using the sensor microcontroller (μC #1) CAN identification number. Students are tasked with developing and validating the code for different predefined frequencies and amplitudes of sensor error signals. Fig. 5 shows a representative response to a stealth attack that injects a 0.5 rad error every 0.5 s. Note that the control system's performance is degraded, yet the system remains stable for this frequency and magnitude of the network-based attack.

Students are then asked to implement a replay attack by recording 9.5 s of system measurements and then overwriting the actual sensor measurement on the CAN bus using the CAN identification number of the sensor microcontroller (μC #1). The signal must be repeated every 9.5 s, resulting in a slighter larger frequency and gradually building a larger error (i.e., a larger phase shift). This results in system instability with the arm position being driven into the mechanical limits of travel as seen in Fig. 6(b). The tasks challenges students to consider time scheduling in their code implementation.

Throughout the experimental part of the PBL activity, students are advised to save all data that they might consider necessary for analysis. As part of the group report, they are asked to demonstrate that their control and attack designs met the performance specifications. Students are advised to use plots and metrics taught during previous lectures to assess and justify their results.

Finally, the PBL activity culminates by asking students to provide potential approaches to mitigate cyber attacks to networked CPSs. This aspect of the PBL activity does not provide the student with any guidance beyond posing the question. Students are expected to use insight from implementing the testbed CPS code to inform potential mitigation efforts.

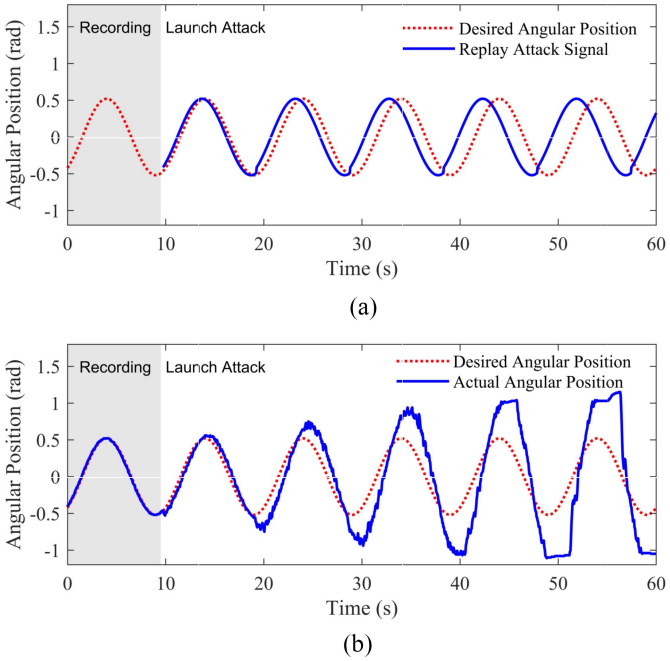

Fig. 6. Response of the networked CPS to a replay attack. (a) Replayed signal. (b) Response of the system to replay attack.

At the end of both the simulation and physical implementations of the project, students need to show correct functionality of their design to instructors.

IV. Learning Outcomes Assessment

This section presents the metrics used to assess the effectiveness of the PBL activity in reinforcing course learning outcomes.

A. Assessment System

Two different evaluations were used to assess the learning outcome achievement: 1) an individual assessment given before and after the project and 2) a group project report submitted at the end of the activity.

1) Individual Pre- and Post-Assessment: The individual assessment consisted of six multiple choice questions evaluating learning outcomes O1, O3, O6, O7, and O8. The questions asked students to:

- Q1) identify a computing solution to a control system performance problem;
- Q2) define and use correctly cybersecurity-based terminology;
- Q3) answer a cybersecurity-related question, specific to CAN-connected systems;
- Q4) compute and analyze different performances metrics for a simulated CPS;
- Q5) identify cyber threats that may affect the physical response of a control system;
- Q6) identify the effects of physical disturbances on a CPS.

The mapping of the questions with the learning outcomes is given in Section IV-B.

The assessment was provided twice as an online Google form, before (preassessment) and after (post-assessment) the PBL activity, with about three to four weeks in between and distributed to all students via e-mail. Students were asked to fill out the form individually within one week of release and were allowed to use class notes, as necessary. They were told that completion of the pre- and post-assessments counted as 5% of their PBL activity grade, regardless of the correctness of their response. A total of 87 students out of 96 enrolled in the course completed the preassessment, while a total of 86 students completed the post-assessment. The intention of the individual assessment was to gauge any learning outcome improvement before and after the execution of the project. All questions were evaluated quantitatively and graded based on a scale from 0 to 4, where scores of 0, 2, and 4 implied not meeting expectations, meeting expectations, and exceeding expectations, respectively. Samples of two different multiple-choice-type questions used for learning outcomes O1 and O6, along with their assessment rubric, are given in Table II.

2) Group Learning Assessment: Each group, composed of three to four students, was required to submit a written project report. Guidelines of what type of results to include were provided to all students, but the discussion, interpretation, and analysis of results were left open. Based on specific sections of the report, instructors qualitatively evaluated learning outcomes O2, O3, O5, and O6 using the same rubric as in the individual assessments; where a scale from 0 to 4 was used. For instance, outcome O2 was scored based on how well the group's implementation of the networked PI controller met the design criteria (refer to Section III-C and Table II for specifics on the task). A group's implementation that failed to meet specifications was given a null score. A group that showed a performance that met specifications but provided no analysis or discussion of results was given a score of 2. A group whose implementation met the design specifications and was well discussed and documented was given a score of 4.

Other outcomes were evaluated similarly. Outcome O3 was scored based on the professionalism, organization, presentation, and correct use of terminology in the report. Outcome O5 was assessed by evaluating how effectively the group completed each task of the PBL activity, including the launching of cyber attacks. Finally, outcome O6 was assessed based on the discussion and analysis provided by the group on potential resilience measures against replay attacks on the CPS (refer to Table II for more details). A total of 28 groups submitted reports.

B. Assessment Results

Results for the individual examination, both pre- and post-assessment, as well as for the group report are given in Table III. The post-assessment and the group report metrics scored an average of 2.51 or more indicating that students met the expectations established by the program's learning outcomes. More importantly, there was a 0.40 to 0.97 points of increase between pre- and post-assessment results across all evaluated outcomes except for outcomes O1 and O8 (Question Q6) for which the difference was negligible. The increase indicates the enhancement of learning outcomes O3, O6, O7, and O8 (Question Q5) after the completion of the PBL activity.

TABLE II
SAMPLE OF RUBRIC FOR LEARNING OUTCOMES O1, O2, AND O6

Outcome	Individual Assessment Question or Group Report Task	Rubric Score		
		0	2	4
O1	Individual Assessment Question Q1: *Given the plot (omitted herein) of a CPS response, what control or programming actions can you take to reduce the transient error and settling time?*	Wrong Actions	One Correct Action	Two Correct Actions
O2	Group Report Task: *Document implementation of PI Controller based on performance criteria. Evaluate if the design met the requirements using plots, computations, and discussion as necessary.*	Did not meet criteria	Met criteria	Met criteria, well discussed
O6	Individual Assessment Question Q3: *When using CAN Bus to interconnect components of a CPS, CAN data messages carry an ID number that uniquely identifies the sender. This approach is very secure and makes CAN Bus based systems impossible to hack. Is the last statement true or false?*	Chose True	–	Chose False
	Group Report Task: *Discuss resilient control solutions to protect CPS against replay attacks.*	Wrong and vague response	Correct, but vaguely discussed	Correct and sound justification

TABLE III
MEAN SCORES FOR THE INDIVIDUAL ASSESSMENT AND GROUP REPORT[a]

Learning Outcomes	Individual Pre/Post-Assessment			Group Report
	Question	Pre	Post	
O1	Q1	3.07 (1.01)	3.05 (1.04)	–
O2	–	–	–	3.54 (0.42)
O3	Q2	2.26 (1.94)	2.85 (1.73)	3.75 (0.44)
O5	–	–	–	3.59 (0.23)
O6	Q3	1.81 (2.00)	2.78 (1.85)	3.14 (0.97)
O7	Q4	2.10 (1.40)	2.51 (1.30)	–
O8	Q5	2.51 (1.49)	2.91 (1.21)	–
	Q6	3.67 (1.10)	3.76 (0.95)	–

[a]A score of 0 defines not meeting expectations, 2 defines meeting expectations, and 4 defines exceeding expectations. The standard deviation for the scores is provided in parenthesis.

Furthermore, outcomes assessed using the group report and associated with engineering design, experimentation, and computing practices (i.e., O2, O3, and O5) scored relative high values (i.e., above 3.54).

C. Students and Instructors Perception of PBL Activity

Student opinion on the PBL experience was formally collected using a required comment section on the group report. Overall, student collective opinion was positive; praising the repeatability of experiments and ease of use of the testbed despite their lack of prior experience with it. Students enjoyed being able to launch cyber attacks on a physical system and visually observe and assess the effects of the attacks on a tangible process. Some common student feedback include:

1) "the project was challenging yet enjoyable";
2) "the lab was fun and tied together many of the concepts from lectures";
3) "we were able to put in practice the majority of the concepts from the course";
4) "include more detailed instructions";
5) "increase the time given in class to complete the lab."

From the instructors' perspective, the PBL activity offered a simple yet comprehensive experiment for students to demonstrate the majority of the course's core topics. The activity was also relatively efficient to supervise: the response of the system under disturbances and cyber attacks was consistent among stations and trials facilitating the supervision, trouble shooting, and grading of students' performance. Furthermore, the activity was rewarding from a pedagogical viewpoint given the improvement in the learning outcome assessments and the engagement showcased by students.

D. Future PBL Activity and Testbed Development

The presented PBL activity can be further developed to reflect modern Ethernet networked control systems. By shifting from using only the CAN bus networking protocol, students could be exposed to attack and defense of TCP/IP networked CPS. Minor alterations to the testbed hardware would allow for linking multiple units through either wired or wireless connections. This approach would facilitate student introduction to how modern control networks can be remotely manipulated and viable defensive actions.

The CPS testbed presented in [5] can be altered to lower the per unit cost by using different microcontrollers. Additionally, students possessing prior knowledge of other programming languages may benefit from using a microcontroller other than the mbed OS microcontrollers presented in [5].

Other course learning outcomes could be accommodated through altering the specific activities students are required to perform. For example, students could be required to generate code to access the inertial measuring unit if the experience with inter-integrated circuit (I^2C) serial communications is desired. Additionally, students could be required to experimentally implement and validate the defensive measures they were asked to formulate in order to prevent an unknown instructor inserted cyber attack.

V. CONCLUSION

The presented PBL activity was used to enhance and assess the learning of network attacks on CPS by second-year undergraduate students. Learning effectiveness was assessed through a combination of measuring individual student knowledge before and after activity performance and through instructor evaluation of group reports. Students demonstrated a positive improvement toward the obtainment of course learning outcomes. The presented PBL activity can be adapted to

meet other program's learning outcomes for network attack on CPS.

ACKNOWLEDGMENT

The authors would like to thank Joseph Bradshaw and Daniel Rhodes for their support in developing the testbed and LCDR Yasmin Odunukwe for helping to administer the PBL activity and collect the data.

REFERENCES

[1] D. Bédard, C. Lison, D. Dalle, D. Côté, and N. Boutin, "Problem-based and project-based learning in engineering and medicine: Determinants of students-engagement and persistance," *Interdiscip. J. Probl. Based Learn.*, vol. 6, no. 2, p. 8, Aug. 2012.

[2] I. d. l. Ríos, A. Cazorla, J. M. Díaz-Puente, and J. L. Yagüe, "Project-based learning in engineering higher education: Two decades of teaching competences in real environments," *Procedia Soc. Behav. Sci.*, vol. 2, no. 2, pp. 1368–1378, 2010.

[3] D. Kokotsaki, V. Menzies, and A. Wiggins, "Project-based learning: A review of the literature," *Improving Schools*, vol. 19, no. 3, pp. 267–277, Nov. 2016.

[4] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.

[5] E. J. Rodríguez-Seda, P. J. Frontera, and J. Bradshaw, "A networked cyber-physical system testbed for undergraduate education," in *Proc. Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2018, pp. 3007–3012.

[6] P. J. Mosterman, "The towers of hanoi as a cyber-physical system education case study," in *Proc. Workshop Cyber-Phys. Syst. Educ. CPS Week*, Philadelphia, PA, USA, Apr. 2013, pp. 1–4.

[7] J. C. Jensen, E. A. Lee, and S. A. Seshia, "Virtualizing cyber-physical systems: Bringing CPS to online education," in *Proc. Workshop Cyber-Phys. Syst. Educ. CPS Week*, Philadelphia, PA, USA, Apr. 2013, pp. 4–11.

[8] D. P. Möller, D. Sitzmann, and H. Vakilzadian, "Cyber-physical remote access lab: Analysis and design of embedded systems," in *Proc. IEEE Int. Conf. Electron. Inf. Technol.*, Dekalb, IL, USA, May 2015, pp. 540–545.

[9] S. Adyanthaya *et al.*, "xCPS: A tool to explore cyber physical systems," in *Proc. Workshop Embedded Cyber Phys. Syst. Educ.*, Amsterdam, The Netherlands, 2015, pp. 1–8.

[10] T. L. A. Crenshaw, "Using robots and contract learning to teach cyber-physical systems to undergraduates," *IEEE Trans. Educ.*, vol. 56, no. 1, pp. 116–120, Feb. 2013.

[11] G. A. Francia, III, G. Randall, and J. Snellen, "Pedagogical resources for industrial control systems security: Design, implementation, conveyance, and evaluation," *J. Cybersecurity Educ. Res. Pract.*, vol. 2017, no. 1, p. 14, 2017.

[12] G. Richards, "Laboratory exercises to accompany industrial control and embedded systems security curriculum modules," in *Proc. CyberSecurity Educ. Res. Pract.*, May 2019, pp. 185–213.

[13] *Criteria for Accrediting Computing Programs, 2019–2020*. Accessed: Nov. 15, 2019. [Online]. Available: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2019–2020/

[14] *First Workshop on Cyber-Physical Systems Education (CPS-ED 2013)*. Accessed: Nov. 15, 2019. [Online]. Available: https://cps-vo.org/group/edu/workshop

[15] D. Hristu-Varsakelis and W. Levine, "An undergraduate laboratory for networked digital control systems," *IEEE Contr. Syst. Mag.*, vol. 25, no. 1, pp. 60–62, Feb. 2005.

[16] P. J. Martin, "An interdisciplinary controls curriculum for cyber-physical systems education," in *Proc. Workshop Cyber Phys. Syst. Educ. CPS Week*, Philadelphia, PA, USA, Apr. 2013, p. 3.

[17] H. Hassan, C. Domanguez, J. Martanez, A. Perles, J. Capella, and J. Albaladejo, "A multidisciplinary PBL robot control project in automation and electronic engineering," *IEEE Trans. Educ.*, vol. 58, no. 3, pp. 167–172, Aug. 2015.

[18] M. Törngren and E. Herzog, "Towards integration of CPS and systems engineering in education," in *Proc. Workshop Embedded Cyber Phys. Syst. Educ.*, 2016, pp. 1–5.

[19] R. Plateaux, O. Penas, J. Choley, F. Mhenni, M. Hammadi, and F. Louni, "Evolution from mechatronics to cyber physical systems: An educational point of view," in *Proc. Int. Conf. Res. Educ. Mechatron.*, Jun. 2016, pp. 360–366.

[20] M. Garduno-Aparicio, J. Rodriguez, G. Macias-Bobadilla, and S. Thenozhi, "A multidisciplinary industrial robot approach for teaching mechatronics-related courses," *IEEE Trans. Educ.*, vol. 61, no. 1, pp. 55–62, Feb. 2018.

[21] I. Calvo, I. Cabanes, J. Quesada, and O. Barambones, "A multidisciplinary PBL approach for teaching industrial informatics and robotics in engineering," *IEEE Trans. Educ.*, vol. 61, no. 1, pp. 21–28, Feb. 2018.

[22] J. Heywood, *Engineering Education: Research and Development in Curriculum and Instruction*. Piscataway, NJ, USA: IEEE Press, 2005.

[23] P. A. Kirschner, J. Sweller, and R. E. Clark, "Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching," *Educ. Psychol.*, vol. 41, no. 2, pp. 75–86, 2016.

[24] T. J. Bayer, "Effects of guided project-based learning activities on students' attitudes toward statistics in an introductory statistics course," Ph.D. dissertation, STEM Educ., Old Dominion Univ., Norfolk, VA, USA, Dec. 2016.

[25] J. Macías-Guarasa, J. M. Montero, R. San-Segundo, Á. Araujo, and O. Nieto-Taladriz, "A project-based learning approach to design electronic systems curricula," *IEEE Trans. Educ.*, vol. 49, no. 3, pp. 389–397, Aug. 2006.

[26] N. Hosseinzadeh and M. R. Hesamzadeh, "Application of project-based learning (PBL) to the teaching of electrical power systems engineering," *IEEE Trans. Educ.*, vol. 55, no. 4, pp. 495–501, Nov. 2012.

[27] D. de Matos Magnus, L. F. B. Carbonera, L. L. Pfitscher, F. A. Farret, D. P. Bernardon, and A. A. Tavares, "An educational laboratory approach for hybrid project-based learning of synchronous machine stability and control: A case study," *IEEE Trans. Educ.*, vol. 63, no. 1, pp. 48–55, Feb. 2020.

[28] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 110–127, Feb. 2015.

[29] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.

[30] B. Croteau *et al.*, "Cross-level detection framework for attacks on cyber-physical systems," *J. Hardw. Syst. Secur.*, vol. 1, no. 4, pp. 356–369, Dec. 2017.

[31] T. Severson *et al.*, "Trust-based framework for resilience to sensor-targeted attacks in cyber-physical systems," in *Proc. IEEE Amer. Control Conf.*, Jun. 2018, pp. 6499–6505.

Paul J. Frontera received the B.S. degree in systems engineering from the United States Naval Academy, Annapolis, MD, USA, in 1996, the M.S. degree in aerospace engineering from the University of Maryland at College Park, College Park, MD, USA, in 2002, and the Ph.D. degree in mechanical engineering from Naval Postgraduate School, Monterey, CA, USA, in 2016.

He is currently an Assistant Professor with the Department of Weapons, Robotics, and Control Engineering, United States Naval Academy. His current research interests include estimation, optimal control, and autonomous underwater vehicle control and trajectory planning.

Erick J. Rodríguez-Seda received the B.S. degree in electrical engineering from the University of Puerto Rico, Mayagüez, Puerto Rico, in 2004, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Illinois at Urbana–Champaign, Urbana, IL, USA, in 2007 and 2011, respectively.

He is currently an Associate Professor with the Department of Weapons, Robotics, and Control Engineering, United States Naval Academy, Annapolis, MD, USA. From 2011 to 2013, he was a Postdoctoral Research Associate with the University of Texas at Dallas, Richardson, TX, USA. His current research interests include networked control, collision avoidance, and control of cyber–physical systems.