Paper ID #26902

Work in Progress: Layering Cybersecurity on Domain Engineering Instruction

Dr. Rhonda Kay Gaede, University of Alabama, Huntsville

Rhonda Kay Gaede is an associate professor of electrical and computer engineering, the University of Alabama in Huntsville. Her research interests include computer architecture, VLSI design, and cyber security. She has a PhD degree in electrical engineering from the University of Texas at Austin. She is a member of IEEE (computer society), ASEE and ACM. Contact her at gaeder@uah.edu.

Dr. Thomas Morris, University of Alabama, Huntsville
Mr. Rishabh Das
Prof. Yu Lei
Dr. Thiago Alves, University of Alabama, Huntsville

Thiago Alves received his B.S. degree in electrical engineering from the ”Pontifícia Universidade Católica” (PUC) in 2013, his MsE degree from the University of Alabama in Huntsville (UAH) in 2018 and his Ph.D. degree also from UAH in 2019. He was the recipient of the Best Senior Design Award from PUC University Electrical Engineering Department in 2013. In 2014 he created OpenPLC, the world's first open source industrial controller. OpenPLC is being used as a valuable tool for control system research and education. The OpenPLC project has contributions from several universities and private companies, such as Johns Hopkins and FreeWave Technologies. In 2017 Thiago won first place in CSAW, the world's largest student-run cybersecurity competition, with his innovative embedded security solution for OpenPLC. In 2019 Thiago was awarded as 2019 outstanding ECE graduate student by UAH. Currently Thiago is an Advisory Specialist Master at Deloitte. His research interests include cybersecurity for SCADA systems, industrial controllers and embedded systems.

Dr. Hongyu Zhou, University of Alabama, Huntsville

Hongyu Zhou is an Assistant Professor in Civil and Environmental Engineering at the University of Alabama in Huntsville (UAH). Dr. Zhou received his PhD in Civil Engineering from Arizona State University in 2013 and bachelor's degree in Civil Engineering from Tongji University in 2010. His research interests include materials and designs for energy-efficient buildings, integrated design, hazard mitigation, and cyber-physical systems. Dr. Zhou is a member of the American Society of Civil Engineers (ASCE) and American Concrete Institute (ACI). He has an active role in several technical committees. He is a founding member and Chair elected for the ASCE SEI Committee on Bioinspired Structures and Co-Chair of the Advanced Structures and Materials Committee of ASCE Aerospace Division (ASD).

Dr. Farbod Fahimi, University of Alabama, Huntsville

Dr. Fahimi has over 10 years of research experience in dynamic modeling, system identification, linear and nonlinear controls, with applications to robotic system and autonomous vehicles. He received a PhD degree in Mechanical Engineering on dynamic modeling of flexible multi-body systems in 1999. He has graduated 8 Masters students, and has offered several senior design projects. He is currently supervising several full time and part time graduate students. He has taught several undergraduate and graduate level courses such as Dynamics, Vibrations, System Dynamics, Elasticity, Finite Element Method, Introduction to Robotics, and Advanced Robotics. He has authored a graduate level text book titles: Autonomous Robots; Modeling, Path Planning, and Control.

Work-in-Progress: Layering Cybersecurity on Domain Engineering Instruction

Abstract

The grand challenge to secure cyberspace includes securing industrial control systems. These systems monitor and control physical processes such as nuclear power plants, gas pipelines, dams, electrical power distribution and are susceptible to cyber threats. However, many of the engineers responsible for designing, operating, and maintaining these systems do not have an appreciation of, nor understand, these threats. Conversely, cyber security professionals, having studied computer engineering, computer science, or information systems understand cybersecurity principles and threat vectors, but not the implications of the threats on the industrial control systems. There is a need for cross pollination between the two groups. We have developed a two week module on cybersecurity of industrial control systems that was first delivered to a civil engineering senior design class (Fall 2017). We subsequently expanded our reach by offering the instruction as an extra credit opportunity for a large enrollment mechanical/aerospace engineering class at the sophomore level and a chemical engineering class at the senior level (Spring 2018). Surveys administered pre- and post-instruction show significant increases in the level of appreciation students have for the challenges presented by our increasingly connected world.

1.0 Motivation

Structural dynamics and earthquake engineering, precision manufacturing, chemical refining, and electric power generation are examples of critical infrastructure that use Industrial Control Systems (ICS), also known as Supervisory Control and Data Acquisition Systems (SCADA), to monitor and control physical processes. ICS are cyber physical systems which collect data from sensors monitoring physical processes and use it to control the process via networked electronic control of actuators, switches, and valves. Protecting these ICS, and others like them, from cyber-attacks is a national priority [1].

The ICS used throughout critical infrastructure are often designed, built, operated, and maintained by engineers from domains related to the physical process being controlled. For example, chemical engineers design refineries, civil engineers design structures, and mechanical engineers design industrial robots. Cybersecurity personnel are tasked with designing, maintaining, and operating cybersecurity controls for the ICS. Cybersecurity is a critical concern for these systems. Exploited systems can cause financial and physical damage. The lack of knowledge overlap between the domain engineers and the cybersecurity personnel leads to misunderstandings and ultimately slows the adoption of security controls for these critical systems. This work is a step towards creating larger populations of domain engineers with cybersecurity awareness in the hope that awareness can lead to expertise.

2.0 Methodology

We have developed a two week module on cybersecurity of ICS for delivery to domain engineering students outside of the ECE department. Two weeks was deemed to be the maximum amount of time that these classes could devote to material that was not considered core domain engineering content. Students in the Electrical and Computer Engineering department can take multiple elective cybersecurity courses that are part of a new BS in Cybersecurity. This two week module has both lecture and lab components. Participating students were surveyed pre-and post-instruction to capture their awareness of the importance of cybersecurity and for subject matter knowledge gained. These modules were offered in two semesters, fall 2017 and spring 2018. The lectures used were the same both times but the lab experience was customized to the target audience: civil engineers in the fall of 2017 and mechanical, aerospace, and chemical engineers in the spring of 2018. All of the teaching materials are available at http://ece.uah.edu/~gaede/capacity_building/teaching/. We are not aware of any other institution that has offered this type of instruction. If such instruction exists, we can use it to strengthen our offering.

Lecture 1

The lecture material begins with the definition of cyber security. It then introduces the usage of embedded systems in the ICS that are used in dam control and monitoring, power substations, water distribution systems, oil/gas distribution systems, and petrochemical refineries. In each of these industrial control systems, the instructor helps the students to identify/understand the roles of the embedded computers and their place in the set of computers, networked data communications and graphical user interfaces that monitor and control industrial processes called SCADA (Supervisory Control and Data Acquisition).

SCADA systems consist of: the physical system (sensors and actuators), wired or wireless connection, programmable logic controller (PLC), enterprise network/Internet, and the human machine interface. At this point, the instructor presents a live demonstration of a SCADA water temperature control system. Following the demo, the instructor introduces four types of cyber security attacks: interruption, interception, modification, and injection and introduces the CIA triad of Confidentiality, Integrity, and Availability.

Lecture 2

In this lecture, the instructor goes into detail on the four major attack vectors: Interruption, Interception, Modification and Injection and demonstrates their impact on the CIA. Real cyber incidents such as Stuxnet [4], Maroochy [5], Black energy [6] and New York Dam [7] incidents are used to correlate the attack vectors and their effects. Finally, students are provided brief descriptions of risk analysis, vulnerability timeline and defense-in-depth.

Laboratory Sessions

The lab session of are hands-on using a simulator, ladder logic, and scripting. Students both inject attacks and develop countermeasures to defeat the attacks. The simulators allow the students to understand the behavior of a SCADA system during normal/abnormal conditions. Control algorithms like ON/OFF and PID control are also demonstrated. Students are provided a brief practical course on ladder logic development and three distinct attack vectors (Bad input in the HMI, volumetric denial of service and injection attack) are implemented using custom scripts, Low-orbit-ion-cannon and Radzio Modbus. The countermeasures of each attack are enforced using IPTables and by sanitizing the ladder logic program. Cyber-security awareness and impact of good programming practices is highlighted during the entirety of the coursework.

Fall 2017

We first offered the cyber-security instruction as a two week module for the civil (CE) engineering senior design class. Each week had one class of lecture and one class for lab activities. For these civil engineers, the lab used a water tank simulator. This simulator is a high-fidelity virtual copy of a laboratory scale water tank. It has a reservoir, an overhead tank, a level sensor, a pump and a manual valve. The pump is used to transfer water from the reservoir to an overhead tank and the level is reported real-time by the level sensor. The manual valve connects the overhead tank to the reservoir and water from the overhead tank is circulated back to the reservoir when the valve is open. The control logic (manual or auto) is implemented using a virtual copy of OpenPLC [2]. In auto mode, the programmable logic controller (PLC) controls the pump and keeps the level of the water between two user-defined set-points. Manual mode offers complete control to the operator. The IEC 61131-3 compliant controller OpenPLC [2] uses the MODBUS protocol to communicate to the human machine interface (HMI).

Spring 2018

We wanted to reach a larger audience and reached out to the Chemical and Mechanical and Aerospace Engineering departments. They opted for giving extra credit to students willing to attend extra sessions. For mechanical (ME), aerospace (AE), and chemical (CHE) engineering students, we used a heat exchanger simulator for the labs. It is a virtual copy of a straight tube heat exchanger system. The simulator has two pipelines connected to a chamber of tubes. Four sensors are used to measure the temperature of the hot and cold water going in and out of the heat exchanger. Based on the operator set-point and the reading of the sensors, the flow of the cold and hot water of the exchanger is controlled by the PLC using a proportional-integral-derivative PID control algorithm. Pressure and mass flow sensors on each pipeline monitor the real-time state of the system. The heat exchanger can operate only in auto mode and it has four distinct parameters (set-point, proportional gain, integral gain and differential gain) that can be modified by an operator from the human machine interface.

3.0 Results

Fall 2017

The instruction was delivered to 22 civil engineering (CE) students. Surveys using the set of questions shown in Table 1 were administered both pre-and post- instruction. Note that the number of responses post-instruction was smaller than pre-instruction. This is likely due to the fact that there was no requirement linked to the completion of the post-instruction survey and that students did these on their own time. The pre-instruction surveys were completed in the classroom prior to instruction. There were notable changes in the recognition of the importance of cybersecurity. Figure 1 shows the level of agreement (Agree or Strongly Agree) with Q2. The change from pre- to post-instruction ranges from 19.05% to 23.81%. For Strongly Agree only (Figure 2), the change is more dramatic, ranging from 40.66% to 59.71%. There was also an increase in the recognition of the presence of SCADA in civil engineering systems (Figure 3). For the systems other than traffic light controllers, the changes ranged from 11.36% to 25.64%. The decrease of -5.86% for traffic light control is an anomaly. We can continue to use this question and look for trends.

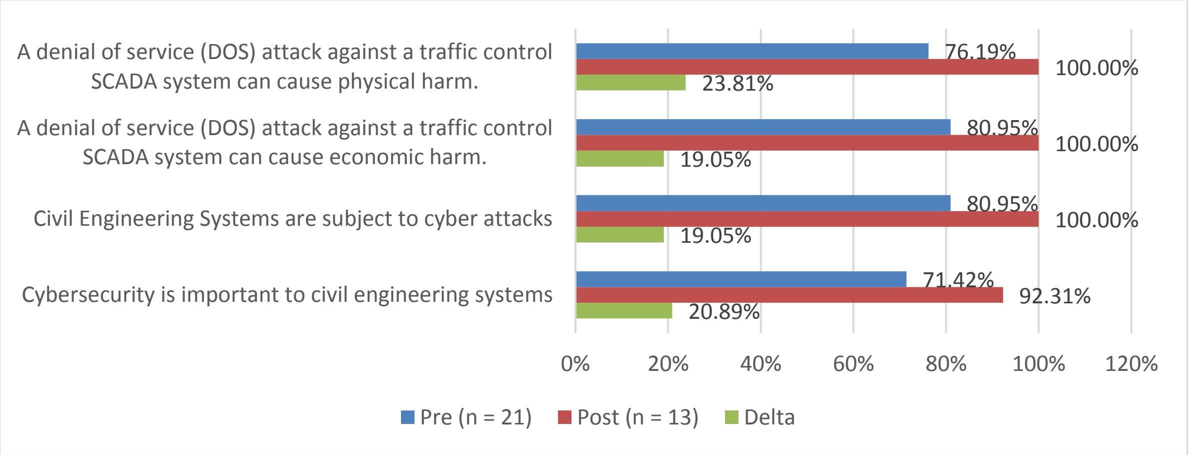

Figure 1. Fall 2017 CE Cybersecurity Importance – Agree or Strongly Agree

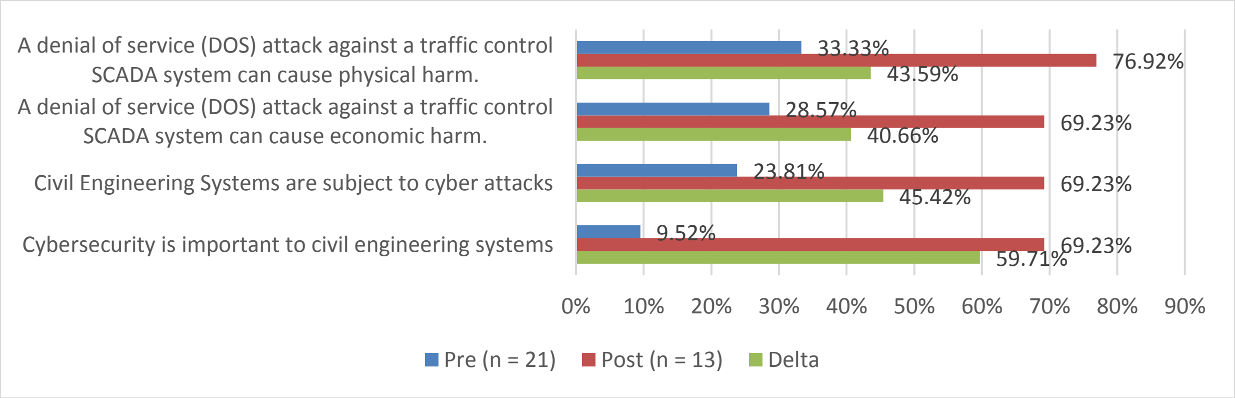

Figure 2. Fall 2017 CE Cybersecurity Importance – Strongly Agree

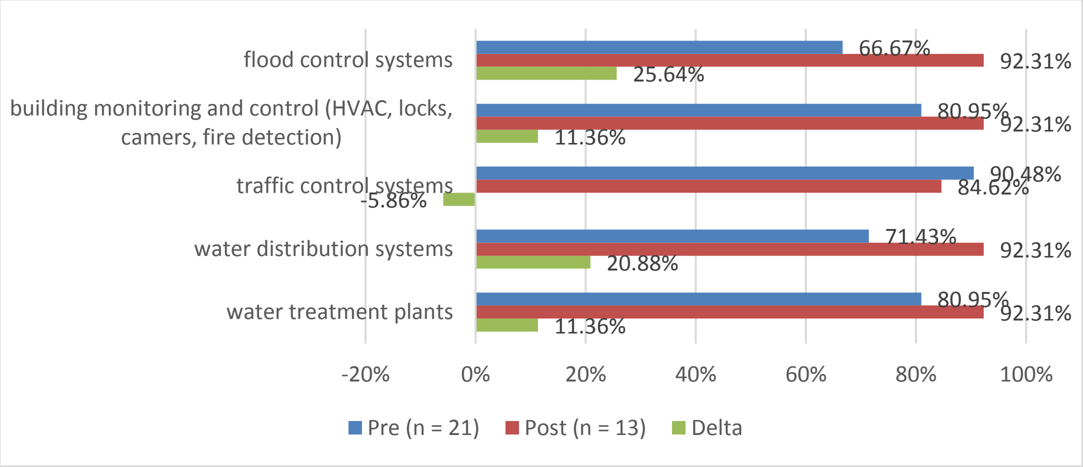

Figure 3. Fall 2017 CE Recognition of SCADA Systems

Table 1: Fall 2017 Survey Questions

Q2 Please indicate your level of agreement with the following statements: 1) Cybersecurity is important to civil engineering systems, 2) Civil Engineering systems are subject to cyber-attacks, 3) A denial of service (DOS) attack against a traffic control SCADA system can cause economic harm, 4) A denial of service (DOS) attack against a traffic control SCADA system can cause physical harm Responses: Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree.
Q5 Supervisory Control and Data Acquisition (SCADA) is 1), the ability to remotely monitor and control a physical system, 2) the ability to control a physical system, 3) only the ability to remotely monitor a physical system, 4) all of the above, 5) none of the above
Q3 Which civil engineering systems use SCADA? (you may select more than one) 1), water treatment plants, 2) water distribution systems, 3) traffic control systems, 4) building monitoring and control (HVAC, locks, cameras, fire detection), 5) flood control systems, 6) None of the above
Q4 Confidentiality is important for water treatment plant SCADA communications. 1) True, 2) Neither true nor false, 3) False
Q6 A denial of service attack is an example of what kind of attack? 1) Confidentiality, 2) availability, 3) integrity, 4) none of the above, 5) all of the above
Q7 An attacker may be able to inject falsified control packets into a dam control system, closing the water intake. This is an example of a threat to: 1) Confidentiality, 2) availability, 3) integrity, 4) all of the above, 5) none of the above
Q8 Which attack has the potential to cause the most economic harm? 1) a DOS attack against traffic control that disables traffic lights across a large area, 2) a power outage from an attack against the water inlet of a hydroelectric dam, 3) an attack that causes flood control gates to open during a flood, 4) a control injection that opens locks at a prison

Q9 Which attack has the potential to cause the most physical harm? 1) a DOS attack against traffic control that disables traffic lights across a large area, 2) a power outage from an attack against the water inlet of a hydroelectric dam, 3) an attack that causes flood control gates to open during a flood, 4)a control injection that opens locks at a prison
Q10 A vulnerability is a flaw that enables a cyber-attack. 1), True, 2) Neither true nor false, 3) False
Q13 A threat is the potential for an actor to exploit a vulnerability. 1) True, 2) Neither true nor false, 3) False
Q11 Risk is the likelihood of attack combined with the potential impact (harm). 1) True, 2) Neither true nor false, 3) False

Spring 2018

The instruction was delivered to 40 students enrolled either in Process Safety & Toxicology or Principles of Measurement & Instrumentation. Surveys using the set of questions shown in Table 2 were administered both pre-and post- instruction. As in the previous semester, there were notable changes. Figures 4, 5, and 6 show results for mechanical & aerospace engineering students while Figures 7, 8, and 9 show results for chemical engineering students.

There were notable changes in the recognition of the importance of cybersecurity for mechanical and aerospace engineering students. Figure 4 shows the level of agreement (Agree or Strongly Agree) with Q3. The change from pre-instruction to post-instruction ranges from -1.27% to 14.74%. The negative number for “Mechanical/Aerospace Engineering Systems are subject to cyber-attacks” is an anomaly that is not statistically significant. For Strongly Agree only as shown in Figure 5, the change is more dramatic, ranging from 17.47% to 36.42%. There was also an increase in the recognition of the presence of SCADA in mechanical and aerospace engineering systems as shown in Figure 6. The changes ranged from 10.74% to 37.47%.

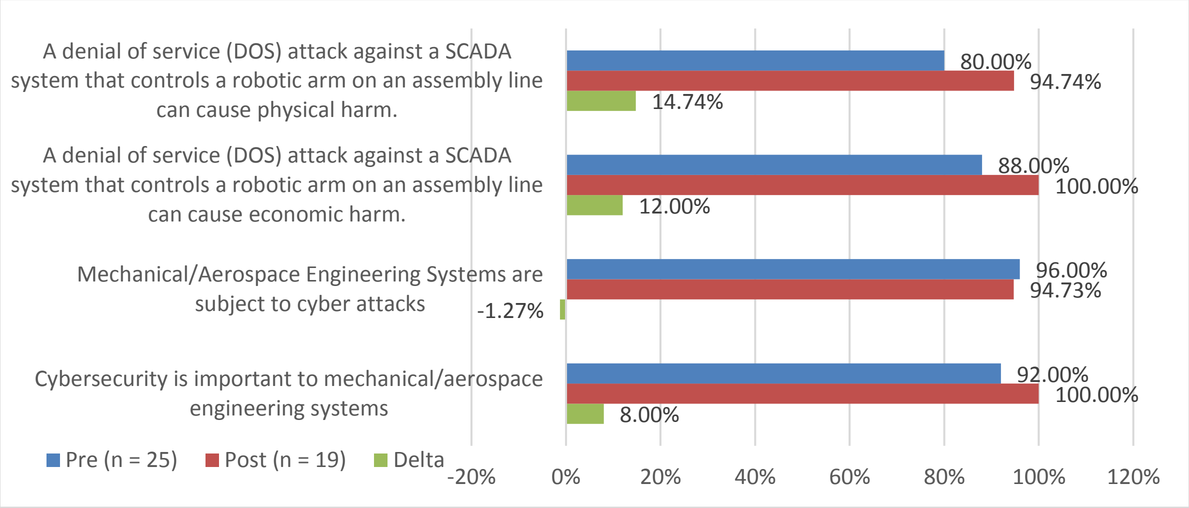

Figure 4. Spring 2018 ME/AE Cybersecurity Importance - Agree or Strongly Agree

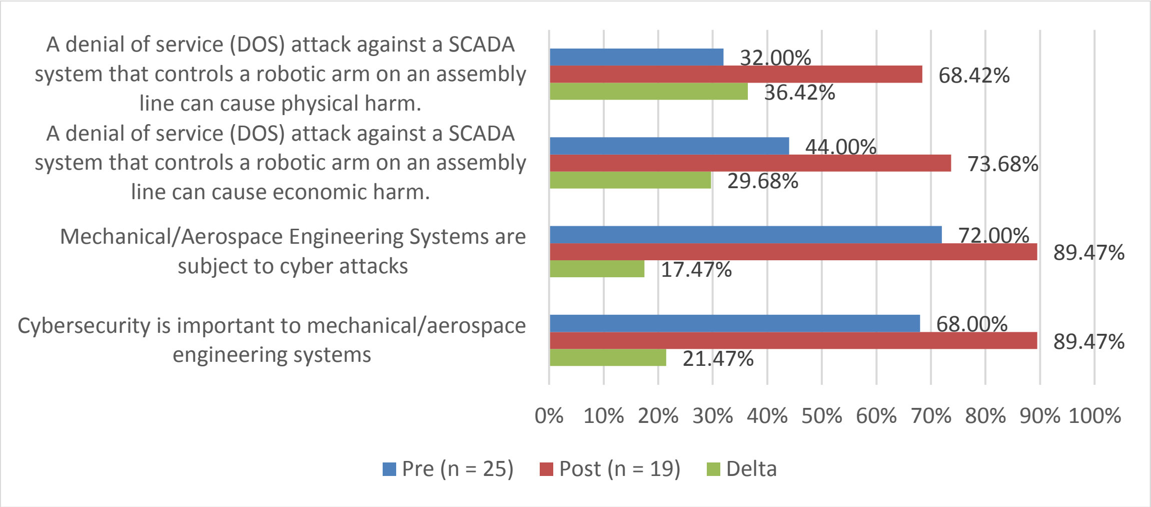

Figure 5. Spring 2018 ME/AE Cybersecurity Importance - Strongly Agree

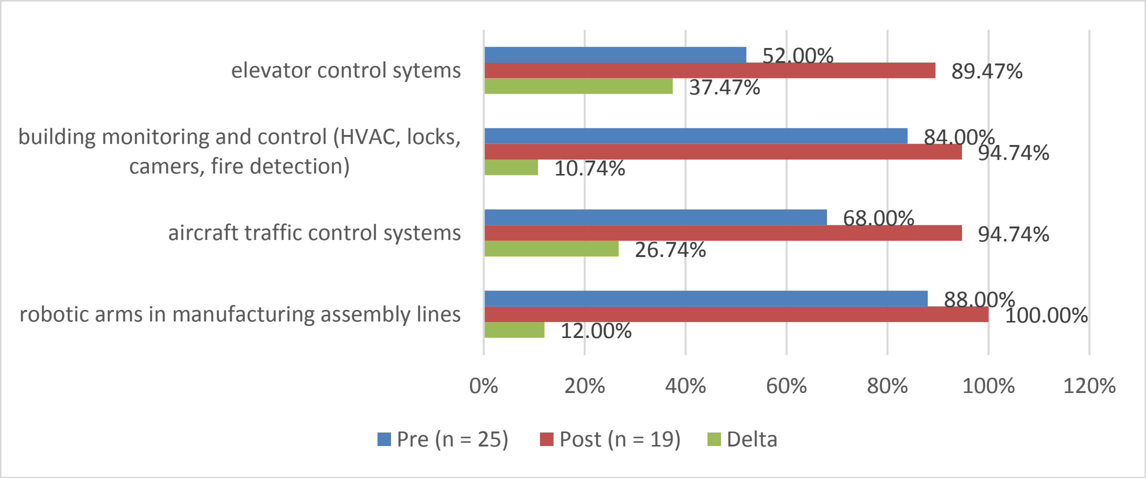

Figure 6. Spring 2018 ME/AE Recognition of SCADA Systems

There were changes in the recognition of the importance of cybersecurity for chemical engineering students. Figure 7 shows the level of agreement (Agree or Strongly Agree) with Q4. The change from pre-instruction to post-instruction ranges from 0% to 16.67%. In the cases of 0% change, there was no improvement to be had as the pre-instruction numbers were 100%. For Strongly Agree only as shown in Figure 8, the change is sizeable, ranging from 19.04% to 33.33%, with the exception of "A denial of service (DOS) attack against a distillation tower SCADA system can cause economic harm" at 4.76%. There was also an increase in the recognition of the presence of SCADA in chemical engineering systems as shown in Figure 9. The changes ranged from 8.33% to 25%.

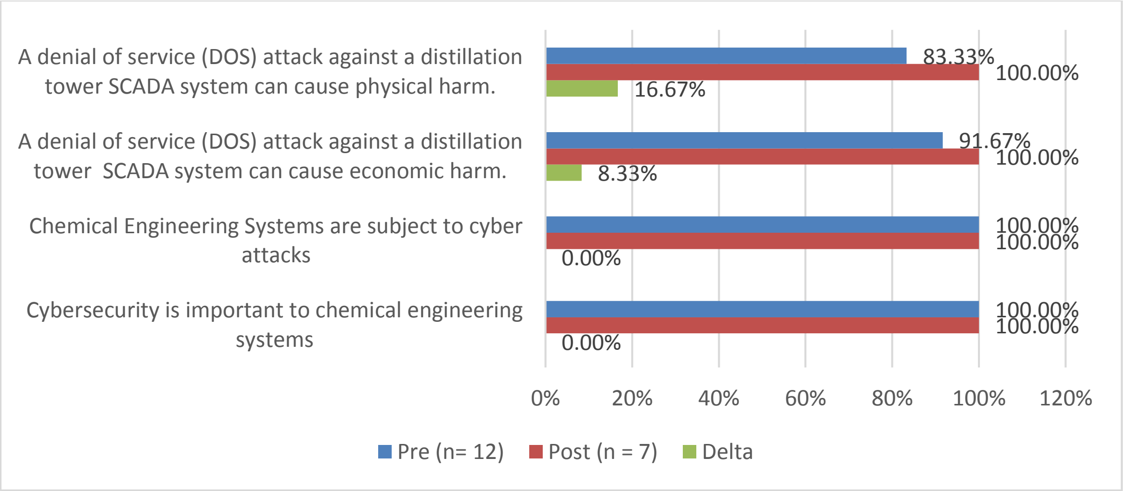

Figure 7. Spring 2018 CHE Cybersecurity Importance - Agree or Strongly Agree

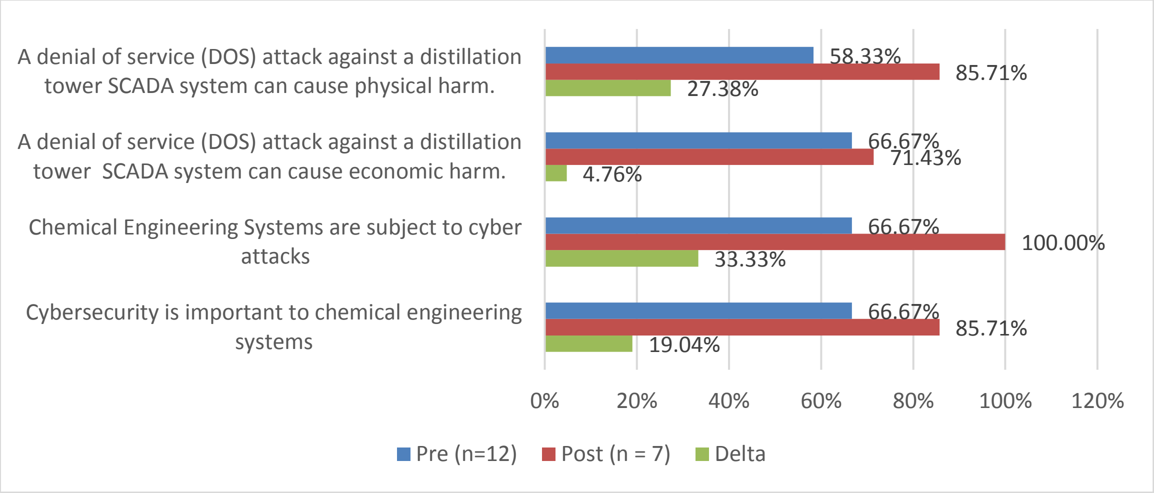

Figure 8. Spring 2018 CHE Cybersecurity Importance - Strongly Agree

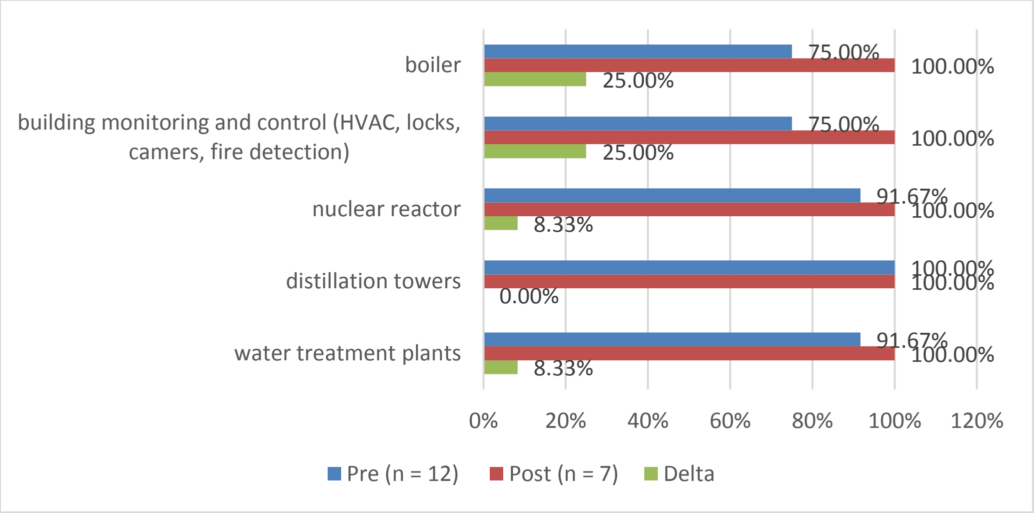

Figure 9. CHE Recognition of SCADA Systems

Table 2. Spring 2018 Survey Questions

Questions for all respondents:

Q2 What is your major? 1) Aerospace Engineering, 2) Chemical Engineering, 3) Mechanical Engineering
Q5 Supervisory Control and Data Acquisition (SCADA) is 1) the ability to remotely monitor and control a physical system, 2) the ability to control a physical system, 3) only the ability to remotely monitor a physical system
Q8 Confidentiality is important for SCADA communications. 1) True, 2) Neither true nor false, 3) False
Q9 A denial of service attack is an example of what kind of attack? 1) confidentiality, 2) availability, 3) integrity, 4) none of the above, 5) all of the above
Q10 An attacker may be able to inject falsified control packets into a HVAC, causing a spurious fire alarm. This is an example of a threat to: 1) confidentiality, 2) availability, 3) integrity, 4) all of the above, 5) none of the above
Q15 A vulnerability is a flaw that enables a cyber-attack. 1) True, 2) Neither true nor false, 3) False
Q16 A threat is the potential for an actor to exploit a vulnerability. 1) True, 2) Neither true nor false, 3) False
Q17 Risk is the likelihood of attack combined with the potential impact (harm). 1) True, 2) Neither true nor false, 3) False
Q18 Cybersecurity is important during which system life cycle phases (Check all that apply) 1) Design, 2) Maintenance, 3) End-of-Life, 4) Production

Questions for respondents with major of Aerospace or Mechanical Engineering:

Q3 Please indicate your level of agreement with the following statements: 1) Cybersecurity is important to mechanical/aerospace engineering systems, 2) Mechanical/Aerospace Engineering systems are subject to cyber-attacks, 3) A denial of service (DOS) attack against a SCADA system that controls a robotic arm can cause economic harm, 4) A denial of service (DOS) attack against a SCADA system that controls a robotic arm can cause physical harm Responses: Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree.
Q6 Which mechanical/aerospace engineering systems use SCADA? (you may select more than one) 1) robotic arms in manufacturing assembly lines. 2) aircraft traffic control systems, 3) building monitoring and control (HVAC, locks, cameras, fire detection), 4) elevator control systems
Q11 Which attack has the potential to cause economic harm? (select all that apply) 1) a DOS attack against air traffic control that causes outages across a large area, 2) a power outage from an attack against the water inlet of a hydroelectric dam, 3) an attack that causes robotic arms to malfunction on an assembly line, 4) a control injection that opens locks at a prison
Q13 Which attack has the potential to cause physical harm? (select all that apply) 1) a DOS attack against air traffic control that causes outages across a large area, 2) a power outage from an attack against the water inlet of a hydroelectric dam, 3) an attack

that causes robotic arms to malfunction on an assembly line, 4) a control injection that opens locks at a prison

Q19 What level of awareness about cybersecurity do mechanical/aerospace engineering graduates need to have? Please explain your answer.

Questions for respondents with major of Chemical Engineering:

Q4 Please indicate your level of agreement with the following statements:

1) Cybersecurity is important to chemical engineering systems, 2) Chemical Engineering systems are subject to cyber-attacks, 3) A denial of service (DOS) attack against a distillation tower SCADA system can cause economic harm, 4) A denial of service (DOS) attack against a distillation tower SCADA system can cause physical harm

Responses: Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree.

Q7 Which chemical engineering systems use SCADA? (you may select more than one)

1), water treatment plants, 2) distillation towers, 3) nuclear reactor, 4) building monitoring and control (HVAC, locks, cameras, fire detection), 5) boiler, 6) None of the above

Q12 Which attack has the potential to cause economic harm? (select all that apply)

1) a DOS attack against traffic control that disables traffic lights across a large area, 2) a power outage from an attack against a nuclear reactor, 3) an attack that causes flood control gates to open during a flood, 4)a control injection that opens locks at a prison

Q14 Which attack has the potential to cause physical harm? (select all that apply)

1) a DOS attack against traffic control that disables traffic lights across a large area, 2) a power outage from an attack against a nuclear reactor, 3) an attack that causes flood control gates to open during a flood, 4) a control injection that opens locks at a prison

Q20 What level of awareness about cybersecurity do chemical engineering graduates need to have? Please explain your answer.

For spring of 2018, we added open-ended questions Q19 and Q20 asking the respondents to identify the level of cybersecurity awareness needed in their domain. Word clouds for the ME and AE responses looked similar pre- and post-instruction. The CHE word clouds (Figure 10) did not. In the post-instruction word cloud, the words need cyber security clearly emerge.

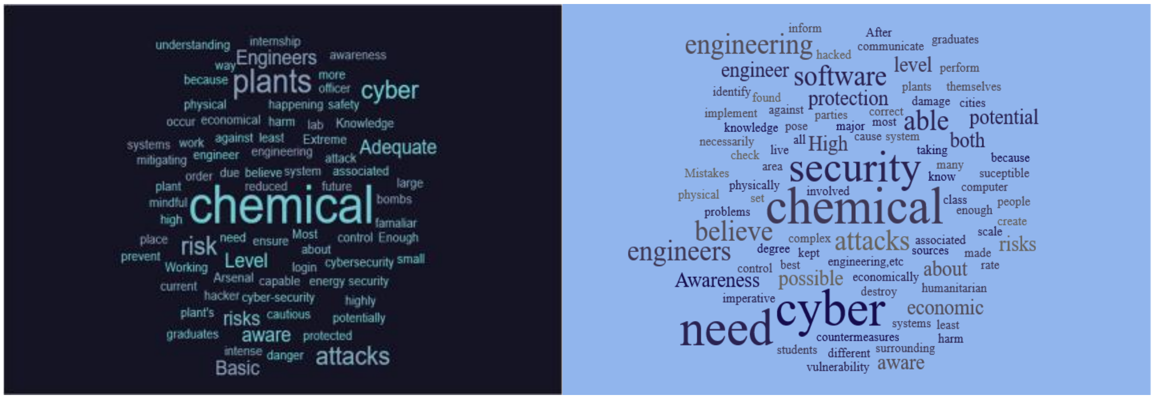

Figure 10 CHE Awareness Need (left) Pre- and (right) Post- Instruction

4.0 Future Work

We have offered the cybersecurity instruction in the fall of 2018 and again in the spring of 2019. For the 2019 offering, we expanded our reach to the EE senior design class. We will continue with these various populations for the foreseeable future to get some longitudinal data. We plan to conduct focus groups in addition to administering surveys to gain additional insight. We have decided that, in addition to the awareness and recognition pieces of the instruction, we would also like to assess more of the cybersecurity content retention. To that end, we have modified our survey to include more questions about cybersecurity subject matter. Since the survey was significantly modified in the fall of 2018, we plan to report on it in a separate publication. We also continue to pursue additional simulation models such as a robotic arm for use in the laboratory sessions and share our virtual systems with other institutions. We may expand our reach to include industrial engineering students as well.

5.0 Conclusion

We developed a two week module on cybersecurity of industrial control systems and delivered it to aerospace, chemical, civil, and mechanical engineering students both as part of an established course and as an outside enrichment opportunity. Survey data collected from the first two semesters of supplemental cybersecurity instruction indicates that it is effective in making domain engineering students aware that cybersecurity is important to systems they design. The data is both quantitative and qualitative in nature. We plan both to continue and expand this work.

References

[1] Obama, B. (2013). Improving critical infrastructure cybersecurity. Executive Order, Office of the Press Secretary, 12.

[2] Alves T., Buratto, M., de Souza, F., Rodrigues, T., "OpenPLC: An open source alternative to automation," in 2014 IEEE Global Humanitarian Technology Conference (GHTC), pp.585-589, Oct. 2014, doi: 10.1109/GHTC.2014.6970342

[3] K. Zetter, "An Unprecedented Look at STUXNET, the World's First Digital Weapon," Wired Magazine, November 3, 2014. [Online]. Available: Wired, http://wired.com. [Accessed April 28, 2019].

[4] N. Sayfayn and S. Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, MIT Management Sloan School, Working Paper CISL #2017-09, May 2017.

[5] US Department of Homeland Security – Cyber Infrastructure, "Cyber-Attack Against Ukrainian Critical Infrastructure," February 25, 2016, Revised August 23, 2018 [Accessed April 28, 2019]

[6] D. Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," The Wall Street Journal, December 20, 2015, [Online} Available: Wall Street Journal, https://www.wsj.com, [Accessed April 28, 2019]