Northwest State Community College

Cybersecurity for Advanced Manufacturing

Summary, results and lessons learned

Tony Hills
7-31-2024

Abstract

Advanced manufacturing organizations have historically suffered from poor cyber-security defenses. Some of the reason for this is a lack of security awareness among the engineering technicians responsible for day-to-day maintenance and operations. In addition, information technology personnel who have security knowledge are not aware of the unique challenges posed by advanced manufacturing technology.

We believe that providing free, accessible, training material presented using technology typically found in advanced manufacturing will increase cyber-security awareness among both groups. To prove this, we have created virtual training scenarios designed to increase general security knowledge among engineering technicians. These training scenarios can also be used to increase awareness of advanced manufacturing technology in information technology workers. To accompany our scenarios, we have created a virtual industrial control environment. This virtual industrial control system can be used without safety concerns or expensive specialized industrial hardware. This virtual industrial control environment can be used remotely, anywhere and at any time. The virtual scenarios can be used with or without guided instruction as they include videos, presentations, labs, and other material intended to facilitate both synchronous and asynchronous learning.

Our material has been used in classes at multiple educational institutions. The scenarios have been used in four-year universities, two-year community colleges and a high school. We have assessed student learning for twenty-eight students, in four courses. Our assessment shows that students completing the scenarios can apply the concepts being taught in the scenarios.

Funding for this project has been provided by an NSF ATE grant.

Introduction

Manufacturing organizations are increasingly relying on technology to increase productivity and remain competitive. This technology is often implemented by operational technology (OT) technicians whose focus is more on system performance and reliability than on following good cybersecurity practices. Partially because of this IBM Security's X-Force Threat Intelligence Index for 2022 states that manufacturing made up most of the cybersecurity attacks they were asked to remediate in 2021 [1].

One way to mitigate against cybersecurity risk is to make sure that OT technicians are aware of the need for cybersecurity, and that information technology (IT) technicians know about the special needs and requirements present in manufacturing systems. This convergence of IT and OT is known as Industry 4.0.

The need for more awareness regarding Industry 4.0 has been the focus of multiple studies conducted over the last several years [2] [3] [4]. This project teaches basic OT knowledge and basic IT knowledge. As is being done at Boise State University, this project stresses basic cybersecurity concepts and skills that are important to both OT and IT technicians [5].

An economical, safe, and efficient way of training students both in person and remotely is to use an online virtual environment [6]. This project combines Internet accessible written materials, videos and a virtual industrial control system (ICS). All materials are available free of charge and the virtual ICS can be downloaded and run locally or used as cloud hosted service.

The training scenarios included in this project have successfully been taught to high school students, two-year college students, four-year college students and professionals currently working in advanced manufacturing organizations. The training has been delivered as remote independent learning and in a traditional instructor led lecture format. Collected assessment data has shown that students' knowledge of the learning outcomes has increased because of the training.

Scenarios

The scenarios created as a part of this project are designed to be used in multiple environments. The scenarios include material that make in usable in an instructor lead face-to-face course, a remote distance learning course or any combination of the two. The scenarios could be used to supplement existing training or be the focus of the training. The scenarios can be used as part of a traditional academic course or for any type of short-term training. The scenarios can be used individually or together.

Each scenario includes a written overview that describes the purpose of the scenario. The overview also contains learning objectives, a network diagram showing important system details such as IP addressing, usernames or passwords that may be needed, and links to Internet sites that a student can visit for more information on the topic.

Each scenario includes a presentation which can be reviewed by the student and used as a lecture resource by the instructor. Each scenario includes a video covering the presentation which can be used for remote learning or student review.

The primary focus of each scenario is a lab which allows students to use the virtual ICS to get hands on experience. The labs include detailed step by step instructions which are suitable for either independent

student use or in an instructor led classroom environment. Each scenario includes an optional lab sheet containing questions students can be required to answer. All the lab sheets come with instructor material that includes grading rubrics and answers to the questions asked on the lab sheets. This makes the material easy to use in a traditional academic course and, because the lab sheets are optional, also suitable for use in short-term training.

The project currently has multiple scenarios available, and more are planned in the future. Scenarios exist covering basic topics such as network monitoring and how and why to use specific security software. Scenarios also exist which cover more advanced topics such as firewall configuration and the proper use of intrusion detection devices. There is a recommended order that the scenarios should be taught in, but they can be used independently of one another if only specifics topics are needed.

The recommended starting scenario is one covering network monitoring. Specifically, students are taught how to use the free and open-source packet analyzer software Wireshark®. This scenario teaches students the purpose of network monitoring software, how to use Wireshark and some of the problems that they may encounter when attempting to monitor the network. The lab for the scenario walks the students through the process of capturing network traffic and then filtering the results to make processing the data easier. The students observe unencrypted HTTP web traffic and encrypted HTTPS web traffic. This allows them to observe the way in which encryption protects network communication.

One of the scenarios covers the basic use and theory of the popular open-source network scanning software Nmap. The Nmap software is specifically designed to map networks. The process of network mapping involves discovering what hosts are running on a network, what the network addresses of those hosts are, what services the hosts offer, and the versions of software being used to provide those services. The lab that goes with this scenario walks the students thorough the use of Nmap starting with basic host discovery techniques and ending with using Nmap to perform advanced script-based vulnerability scans. The lab includes a challenge section in which the students must use what they have learned to find hosts with specific characteristics.

Another introductory scenario included in the project is one covering the free and open-source security tool Metasploit®. Metasploit is a framework tool that allows the easy creation and use of modules designed to test and exploit security fundamentals. Students are taught the purpose of Metasploit, terminology commonly used in Metasploit and basic Metasploit usage. When doing the lab for this scenario students use Metasploit to first find a vulnerability on the HMI system running in the ICS then they exploit that vulnerability and remotely take over the system. This lab contains a challenge section in which students are tasked with remotely shutting down the HMI system using Metasploit.

The project includes a scenario covering ICS basics. In this scenario students are first taught about the history of ICS network protocols. This topic leads into specific training on three commonly used industrial protocols, Modbus® TCP/IP, PROFINET®, S7®, and Ethernet/IP™. When completing the lab for this scenario students must capture and analyze data between systems using first the Modbus TCP/IP protocol and then the S7 protocol. Students must analyze the data at the bit level to determine the status of equipment running on the ICS being monitored.

The Zoning scenario teaches students the importance of carefully segmenting an industrial network into multiple zones. This scenario uses the Purdue model to show categories of devices and recommendations on how they should be separated. The students are taught virtual local area network

(VLAN) concepts and how they can use VLANs to implement zoning in an industrial environment. Students use the lab for this scenario to observe how network zoning greatly mitigates the risk associated with certain network vulnerabilities.

The project includes a scenario covering the basics concepts used in virtual private networks (VPN). Students are taught that a VPN encrypts data which enforces data privacy. Students learn that using a VPN is an important part of establishing secure remote access to an ICS. This scenario also introduces students to firewall use and concepts. In the lab for this scenario students demonstrate how easily workstations can be compromised if unsecured remote access is allowed. Students then configure a VPN and firewall so that only secured remote access is available. Students are asked to compromise a workstation where only secured remote access is allowed and find that they are unable to.

One of the project's scenarios focuses on intrusion detection/intrusion prevention systems (IDS/IPS). In this scenario, students learn that IDS/IPS systems monitor networks and devices for signs of malicious activity. Particular attention is given to the fact that an IDS only generates alerts and an IPS attempts to block suspicious activity. When doing the lab for this scenario students will configure and use both an IDS and an IPS. They will generate potentially malicious activity and observe that the IDS system creates an alert when the traffic is detected while the IPS system blocks the activity.

A scenario exists which covers the basic concepts behind system hardening. This scenario teaches students that following security best practices can make even the most insecure system more secure. Conversely, they learn that not following security best practices can make an inherently secure system insecure. In the lab associated with this scenario students demonstrate the risks associated with choosing poor passwords, not disabling unnecessary services and other easily correctable security vulnerabilities.

Virtual Industrial Control System

A significant part of this project has been the creation of a virtualized industrial Control system (ICS). An industrial control system is a collection of all the physical devices, software and protocols needed to carry out an industrial process. The industrial control system used in this project was made virtual to increase system accessibility, decrease system cost and eliminate student safety concerns. Because the system is virtual it can be accessed remotely or downloaded and run locally, which increases availability. Since the system is virtual no expensive physical hardware is required, which reduces cost. No live electrical circuits or potentially harmful moving parts are present in our virtual environment, and this makes the system safe.

Typical industrial control systems are made up of multiple devices communicating with one another. Some devices that are usually present in an industrial control system are sensors, actuators, motors, programable logic controllers (PLC), open platform computing servers (OPC) and human machine interface systems (HMI). All these devices are present in this project's industrial control system. This is illustrated in Figure 1.

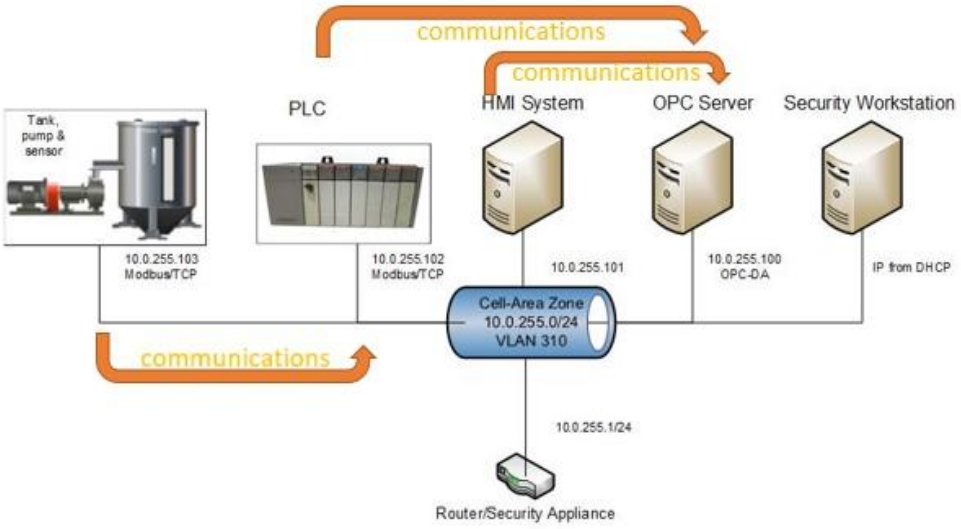


Figure 1

The ICS being used in this project is simulating a simple water-cooling system that might be used in a typical industrial environment. Cooling water is stored in a water tank. Water from the water tank is consumed as the equipment is cooled. When the water level falls to a preset low level the PLC notes this by monitoring the water level sensor. The PLC then activates the water pump. The water pump runs until the PLC and sensor combination determine that the water level has reached a preset high level. The PLC then deactivates the water pump. The OPC server collects data from the PLC and stores it in an easily processed format. The HMI reads the data from the OPC server and displays it on the HMI in a graphical, user-friendly format that can be easily interpreted by system operators. System operators can use the HMI to control the system by changing the system power state, resetting the system, or changing the high or low water levels. Any changes made on the HMI system are first sent to the OPC server which then informs the PLC that a change has been requested.

The tank, pump, sensor, and PLC in this project's ICS are being simulated using the open source pymodbus Python module and some custom coding [7]. The PLC stores, monitors and controls system power status, pump power status, current water level in the tank, high water level and low water level as shown in Figure 2. The PLC is installed on one virtual machine and the tank, pump and sensor are installed on a separate virtual machine. Both virtual machines are running a lightweight distribution of Arch Linux to decrease system requirements and keep costs down. All communications between these two virtual machines occurs using TCP/IP and the Modbus industrial data communications protocol. The PLC virtual machine communicates with the OPC server using TCP/IP and the Modbus industrial data communications protocol.

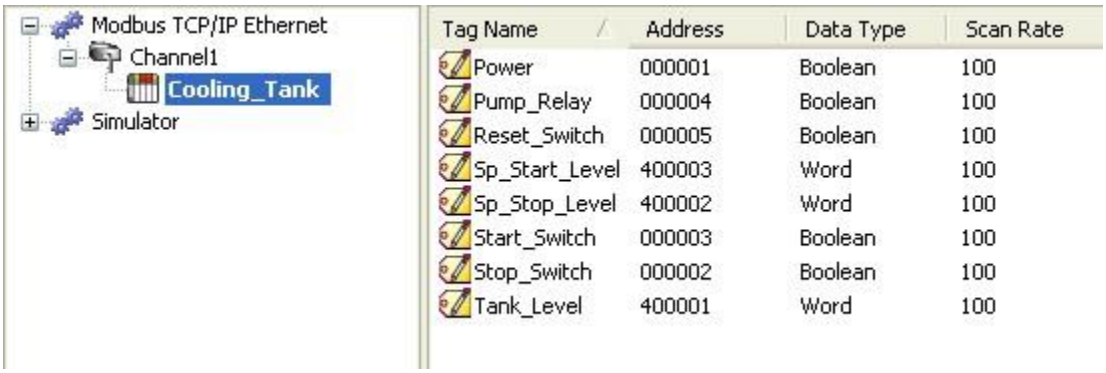


Figure 2

This project's ICS includes an OPC server. The purpose of an OPC server is to collect data from industrial devices which often communicate using proprietary protocols. An OPC server converts data collected from the industrial devices into a standardized format. The converted data can then more easily be shared with other systems such as HMI devices or databases used to log historical data. The OPC server used in this project is an older evaluation copy of Kepware®. The operating system used for the base virtual machine supporting the OPC server is running Microsoft Windows XP®. Both the OPC server and operating system are intentionally several versions old. This was done to mirror what is present in industry. Industry often is reluctant to upgrade software and equipment due to cost and time constraints. The OPC server communicates with the PLC using TCP/IP and the Modbus industrial data communications protocol. The OPC server communicates with the HMI system using the OPC-DA protocol.

The HMI system being used in the ICS was developed using the free software AdvancedHMI® [8]. This software was chosen because it was free, met the requirements of the project and could be modified using the standard Microsoft .NET® application programming interface (API) and tools. The operating system chosen for the HMI system was Microsoft Windows XP.

Initial development on the virtual ICS was done using the VMWare® hypervisor. A hypervisor is a category of software that allows the creation and management of virtual computers. VMWare was chosen since the ICS was specifically intended to be hosted on the Ohio Cyber Range using the NETLAB+® platform. The NETLAB+ platform uses the VMWare hypervisor. After development of the first scenario was complete it was decided that the virtual ICS would reach a wider audience if it was available on multiple ICS platforms. Because of this decision the ICS has been converted to, and is available for VMWare, Microsoft Hyper-V®, and Oracle VirtualBox® platforms.

The complete ICS and be downloaded free of charge from https://nl.northweststate.edu/camo. Programs used to develop the ICS and notes on how to configure them can be downloaded from the same location.

Training

The scenarios created by this project have been used in multiple training sessions. The training has been incorporated into traditional academic classroom environments. The training has been presented in both seminar and short-term training formats. The training has been delivered to professionals currently working in industry, high school students and students in both two-year and four-year colleges. The

training has been delivered as a face-to-face lecture, as online, independent learning and as hybrid training. The hybrid training included both face-to-face and distance-learning/online components.

A total of 28 students from 4 different classes were given a survey intended to evaluate the learning they achieved in the course. The questions asked students to report their knowledge on general operational technology before taking the class and then after taking the class. The survey also asked students to report their knowledge of cybersecurity concepts before and after completing the class. The students reported an increase of 78% improvement in general operational technology knowledge and 92% increase in their knowledge of cybersecurity.

Surveys were given to students completing any of the scenarios which contained the following questions:

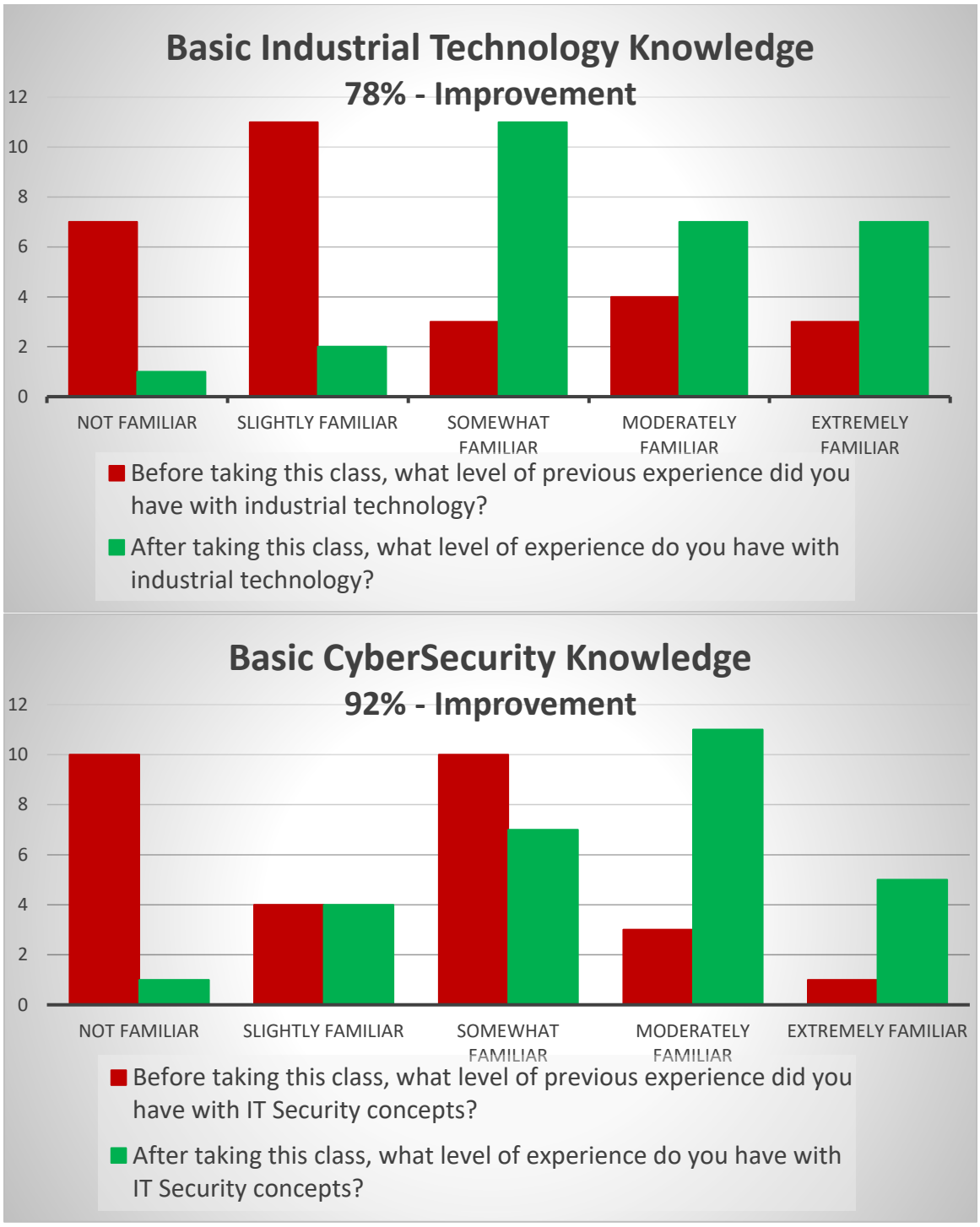
- Before taking this class, what level of previous experience did you have with industrial technology such as Programmable Logic Controllers (PLC), Modbus protocol, Human Machine Interfaces (HMI)?
- After taking this class, what level of experience do you have with industrial technology such as Programmable Logic Controllers (PLC), Modbus protocol, Human Machine Interfaces (HMI)?
- Before taking this class, what level of previous experience did you have with IT Security concepts such as packet capture (Wireshark), network scanning (NMAP) and Virtual Private Network (VPN) technology?
- After taking this class, what level of experience do you have with IT Security concepts such as packet capture (Wireshark), network scanning (NMAP) and Virtual Private Network (VPN) technology?

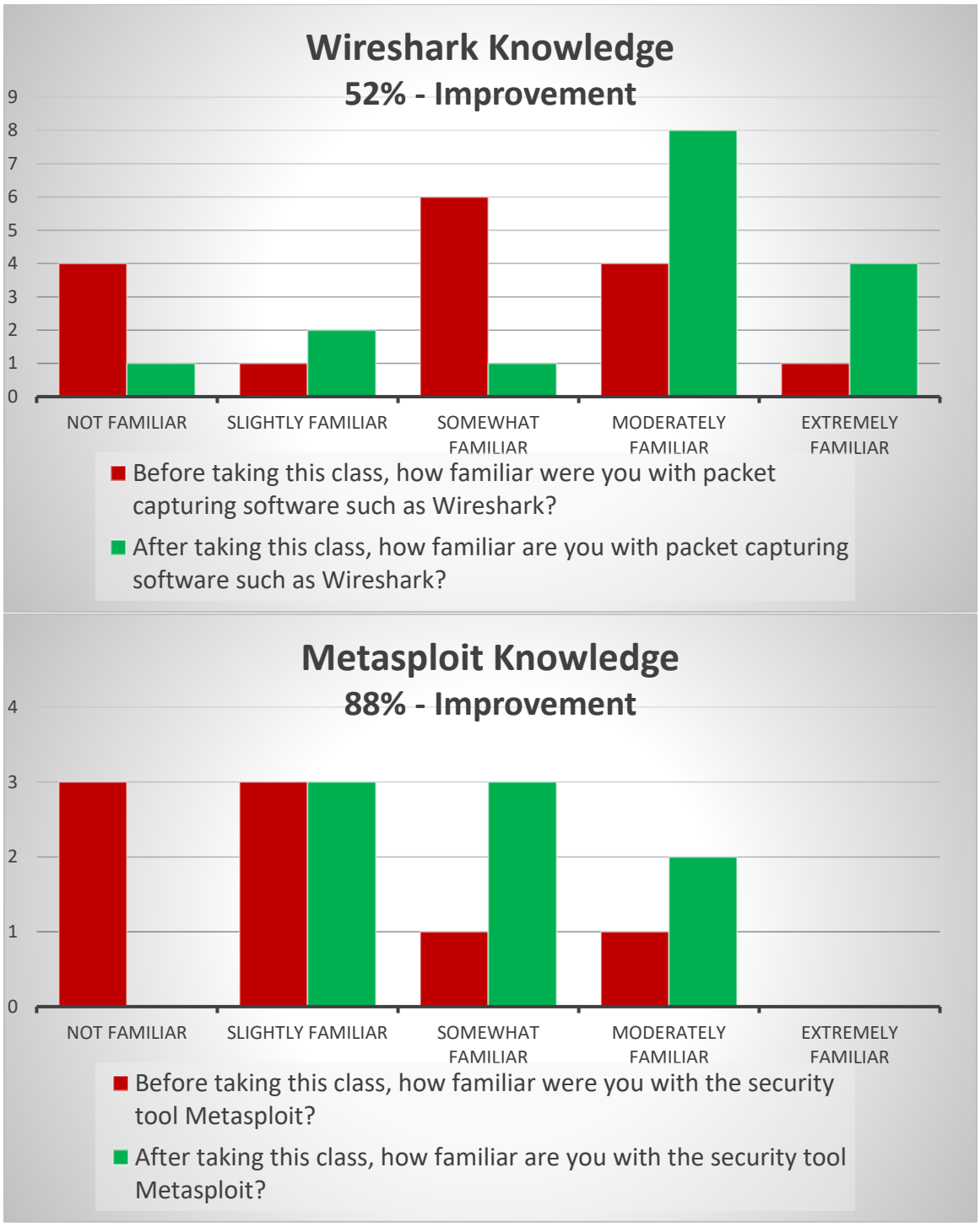
Each specific scenario completed also has a set of associated questions associated with them. For example, the following questions are associated with the Industrial Control System (ICS) Basics Scenario:

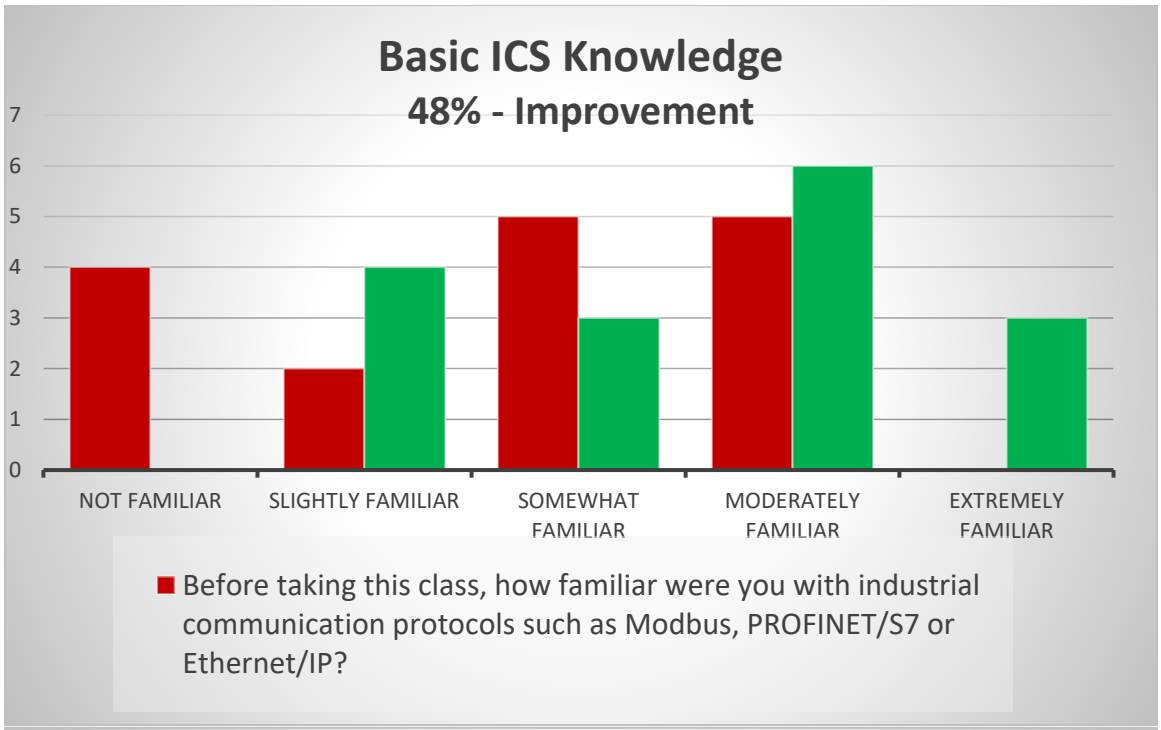
- Before taking this class, how familiar were you with industrial communication protocols such as Modbus, PROFINET/S7 or Ethernet/IP?
- After taking this class, how familiar are you with industrial communication protocols such as Modbus, PROFINET/S7 or Ethernet/IP?

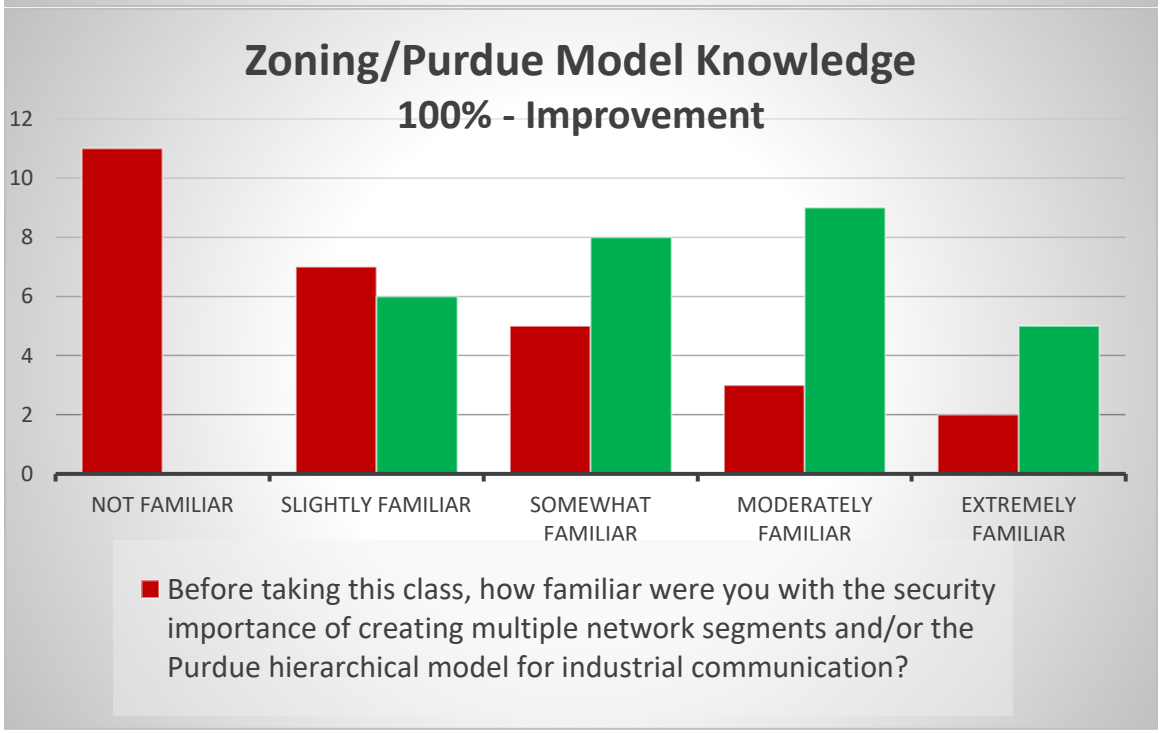
The answers to each question were in 5-level Likert format. The surveys were delivered using Google Forms and the assessment tools built into the Sakai Learning Management System.

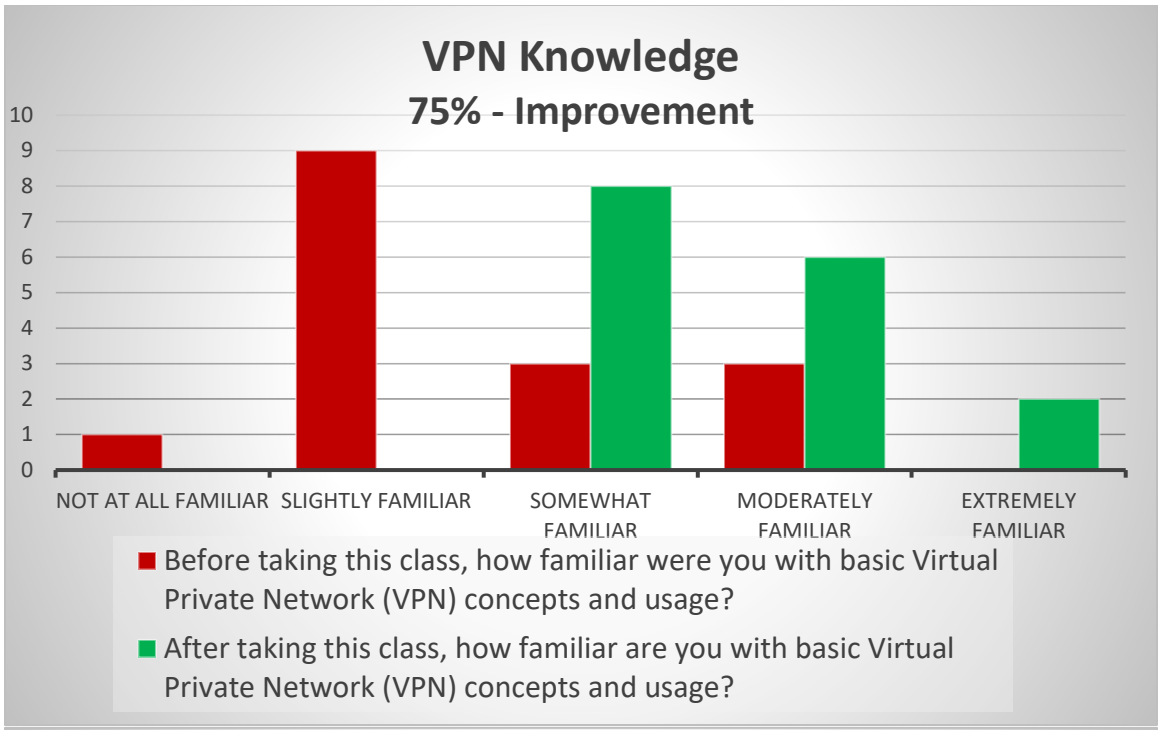
The results of the survey are shown below:

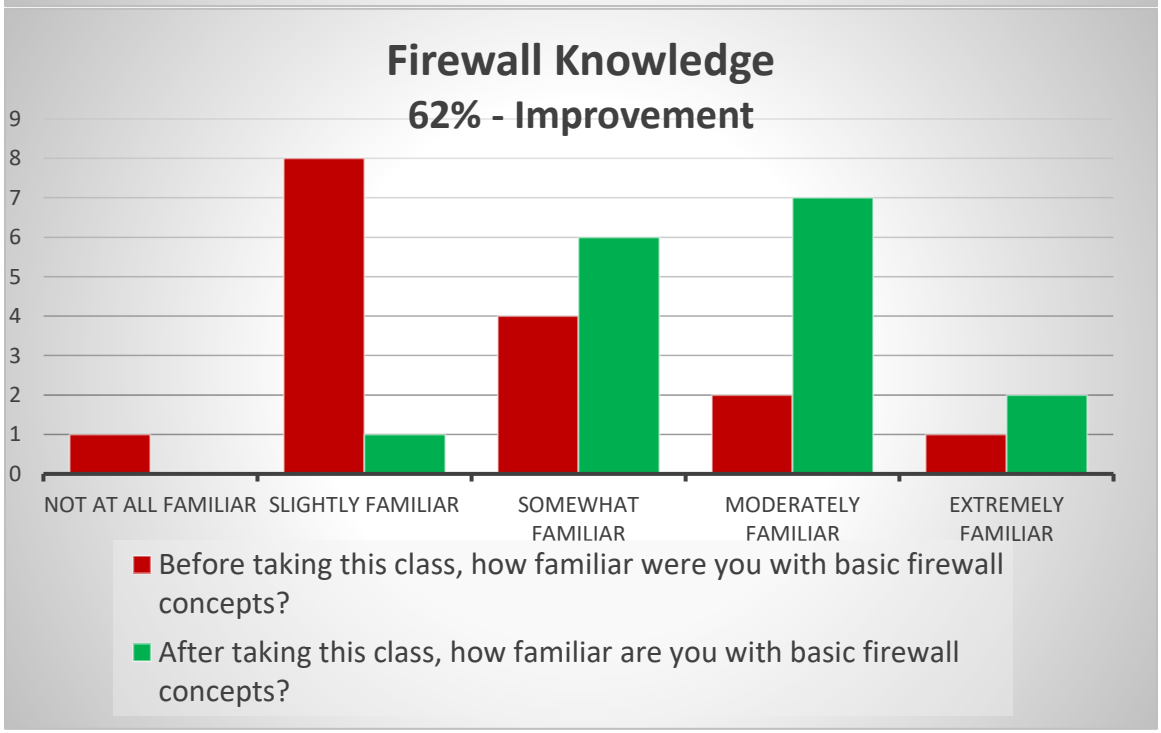

Basic Industrial Technology Knowledge
78% - Improvement
12
10
8
6
4
2
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, what level of previous experience did you have with industrial technology?
After taking this class, what level of experience do you have with industrial technology?
Basic CyberSecurity Knowledge
92% - Improvement
12
10
8
6
4
2
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, what level of previous experience did you have with IT Security concepts?
After taking this class, what level of experience do you have with IT Security concepts?

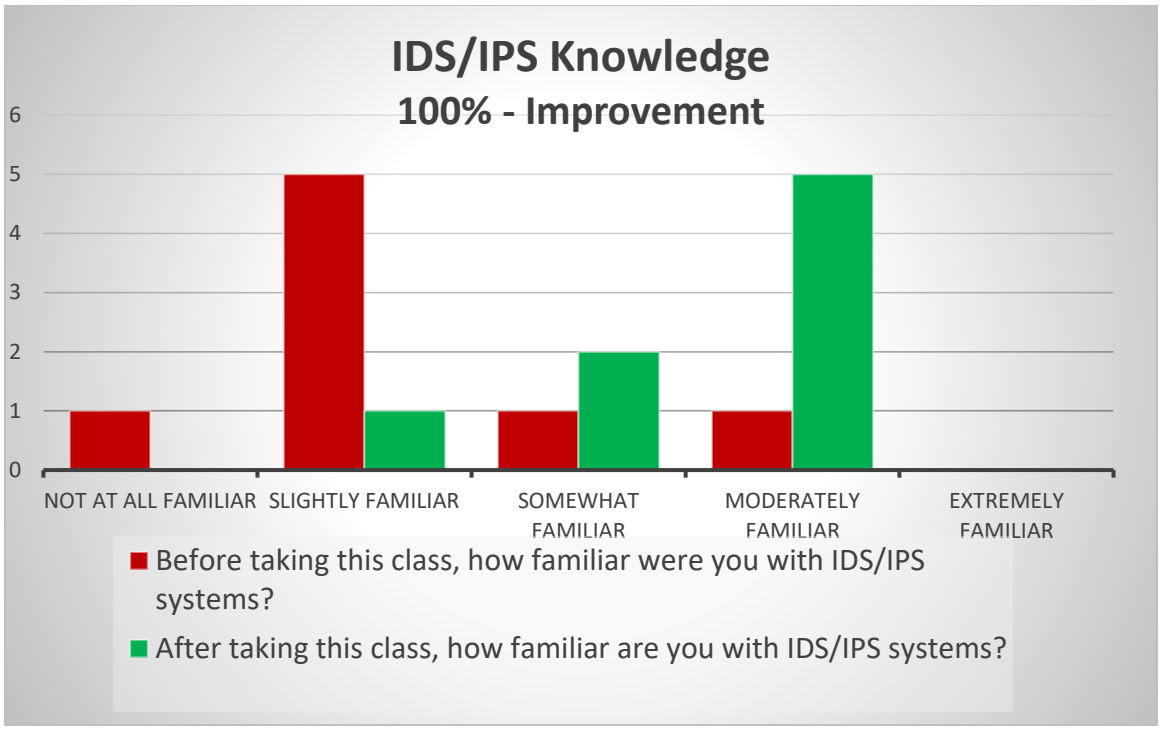

Wireshark Knowledge
52% - Improvement
9
8
7
6
5
4
3
2
1
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with packet capturing software such as Wireshark?
After taking this class, how familiar are you with packet capturing software such as Wireshark?
Metasploit Knowledge
88% - Improvement
4
3
2
1
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with the security tool Metasploit?
After taking this class, how familiar are you with the security tool Metasploit?


Basic ICS Knowledge
48% - Improvement
7
6
5
4
3
2
1
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with industrial communication protocols such as Modbus, PROFINET/S7 or Ethernet/IP?


Zoning/Purdue Model Knowledge
100% - Improvement
12
10
8
6
4
2
0
NOT FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with the security importance of creating multiple network segments and/or the Purdue hierarchical model for industrial communication?


VPN Knowledge
75% - Improvement
10
9
8
7
6
5
4
3
2
1
0
NOT AT ALL FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with basic Virtual Private Network (VPN) concepts and usage?
After taking this class, how familiar are you with basic Virtual Private Network (VPN) concepts and usage?


Firewall Knowledge
62% - Improvement
9
8
7
6
5
4
3
2
1
0
NOT AT ALL FAMILIAR
SLIGHTLY FAMILIAR
SOMEWHAT FAMILIAR
MODERATELY FAMILIAR
EXTREMELY FAMILIAR
Before taking this class, how familiar were you with basic firewall concepts?
After taking this class, how familiar are you with basic firewall concepts?



Lessons Learned

There have been many lessons learned while completing this project.

One thing a project like this should do is prepare the assessment and evaluation material very early in the process. When this project was created the team started with only a general idea of what would be assessed. The team started the project with scenario design. After the creation of several scenarios the evaluation questions were prepared, and the surveys generated. All the completed scenarios had already been put into a learning management system (LMS) so they could be delivered to students. This meant that the LMS material needed to be reworked to add the survey material. In addition, the team quickly found that the assessment material would benefit from frequent revisions as data was collected. Not having the assessment material available early in the process meant that the assessment questions were not as refined as they could have been.

A second evaluation and assessment lesson learned is that if surveys are being given to traditional college students some mechanism needs to be put into place to ensure that the students complete the survey. The first survey that was given was given to a non-credit class of working industrial control technicians. This survey was given at the end of class and the instructor stressed its importance. All the students taking the course completed the survey. The second set of surveys was given to a regular college class. The class instructor was the Primary Investigator on the project and the survey's importance was stressed. Most students completed the survey in that class. The remainder of the surveys were given in traditional college classes taught by instructors with little connection to the project. These surveys had very poor returns. Should a project like this be undertaken again a grade would be attached to the completion of the survey and this would be clearly communicated in the notes given to instructors who will be using the scenarios in any of their classes.

Acknowledgments

This project was made possible through support from the U.S. National Science Foundation award # 1800929.

References

[1] C. Singleton, C. DeBeck, J. Chung, D. McMillen, S. Craig, S. Moore, C. Hammond, J. Dwyer, M. Frydrych, O. Villadsen, R. Emerson, G.-V. Jorudan, V. Onut, S. Carruthers, A. Laurie, M. Alvarez, S. Wuttke, G. Prassions, J. Zorabedian, M. Mayne, L. Kessem, I. Gallagher and A. Eitan, "X-Force Threat Intelligence Index 2022," IBM Corporation, Armonk, NY, 2022.

[2] J. Ekong, V. Chauhan, J. Osedeme, S. Niknam and R. Nguyen, "A framework for Industry 4.0 workforce training through project-based and experiential learning approaches," *ASEE Annual Conference.*

[3] P. Ferreira, A. Aharair, S. H. Bonilla and J. B. Sacomano, "Maker Smart Education: Methodology and Technologies to Train New Engineers in Line with Industry 4.0.," *Journal of Engineering Science & Technology Review,* vol. 15, no. 1, pp. 185-190, 2022.

[4] M. Kuttolamadom, J. Wang, D. Griffith and C. Greer, "Educating the Workforce in Cyber & Smart Manufacturing for Industry 4.0," *ASEE Annual Conference 2020,* 2020.

[5] S. M. Loo and L. Babinkostova, "Cyber-Physical Systems Security Introductory Course for STEM Students," *ASEE 2020 Annual Conference,* 2020.

[6] B. Jenkins, "Development of A Remote-Access, Simulator-Enabled, Team-Friendly Lab for an Electric Machines Course," *ASEE 2022 Annual Conference,* 2022.

[7] "PyModbus - A Python Modbus Stack," 28 07 2024. [Online]. Available: https://github.com/pymodbus-dev/pymodbus. [Accessed 31 07 2024].

[8] "AdvancedHMI Software," AdvancedHMI, [Online]. Available: https://www.advancedhmi.com/index.php?main_page=page&id=14&chapter=0. [Accessed 31 07 2024].