2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023

The Harbor of Engineering
Education for 130 Years

ASEE

Paper ID #37919

Board 244: CyberSecurity for Advanced Manufacturing Organizations

Tony Hills, Northwest State Community College

Tony Hills is a Professor of Information Technology in the STEM department at Northwest State Community College. He has thirty years of experience in the Information Technology field both as a practitioner and as a teacher. His area of expertise is system administration and cybersecurity, but he also has experience in computer programming. Topics that he has taught include computer hardware, operating systems, data networking, cybersecurity, cloud computing, database management and computer programming. Tony Hills has earned a Master of Business and Organizational Leadership degree from Defiance College and a Master of Cybersecurity and Information Assurance degree from Western Governors University.

Cybersecurity for Advanced Manufacturing Organizations

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 need for cybersecurity, and that information technology (IT) technicians know about the special needs and requirements present in manufacturing environments. This approach has been successfully implemented in an introductory course at Boise State University [2].

The convergence of IT and OT technology 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 [3] [4] [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 them usable in an instructor lead face-to-face course, a remote distance learning course or any combination of the two. They can be used to supplement existing training or be the focus of the training. The project material can be used as part of a traditional academic course or for 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 contains learning objectives, and links to Internet sites that a student may visit to gain more knowledge. The overview contains lab details such as a network diagram showing system connections and IP addresses assigned to the systems. The overview contains a list of all usernames and passwords that a student may need as they complete the material.

PowerPoint presentations are included and can be used directly by the student and/or optionally used as a lecture resource by the instructor. Pre-recorded videos based on the presentations are included in the project. These videos can be used to facilitate remote learning or as a way for a student to review a face-to-face lecture.

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 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.

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 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.

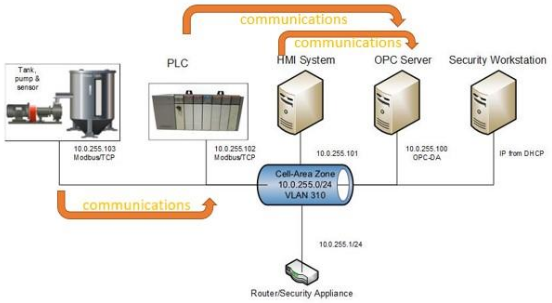

Figure 1

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. The PLC monitors the water level sensor and notes when the water level falls to a preset low level. 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/low water levels. Any changes on the HMI system are first sent to the OPC server which then informs the PLC that a change has been requested.

Training

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

Acknowledgments

This project was made possible through support from the U.S. National Science Foundation award # 1800929. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the NSF.

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

[3] 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.*

[4] 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.

[5] 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.

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