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

The Harbor of Engineering
Education for 130 Years

ASEE

Paper ID #40234

Hands-on Lab Exercises for Onsite and Remote Education Delivery in a CPS Communication Systems Course Using ISAAC

Dr. Ananth Jillepalli, Washington State University

https://www.linkedin.com/in/ajillepalli

Austin Ryan Gress, University of Idaho

Previous Sr Electrical Engineering student at the University of Idaho, Go Vandals! Studied with an emphasis on power system generation and management. Aspirations for Systems Engineering that focuses on power system integrity, quality, and security. Aimed with a desire to keep our electric grids safe and reliable and give students the resources they need to do the same.

Romulo Bainy
Yacine Chakhchoukh
Daniel Conte de Leon
Dr. Herbert L. Hess, University of Idaho

Herb Hess is Professor of Electrical Engineering at the University of Idaho. He received the PhD Degree from the University of Wisconsin-Madison in 1993. His research and teaching interests are in power electronics, electric machines and drives, electric

Dr. Brian K. Johnson P.E., University of Idaho

Brian K. Johnson received his Ph.D. in electrical engineering from the University of Wisconsin-Madison in 1992. Currently, he is a Distinguished Professor and Schweitzer Engineering Laboratories Endowed Chair in Power Engineering in the Department of Elec

Hari Challa

Hands-on Lab Exercises for Onsite and Remote Education Delivery in a CPS Communication Systems Course

Ananth A. Jillepalli, Hari Challa, Austin Gress, Rômulo G. Bainy,
Yacine Chakhchoukh, Daniel Conte de Leon, Herbert Hess, Brian K. Johnson
University of Idaho
[ajillepalli, challa, gres6121, romulo, yacinec, dcontedeleon, hhess, bjohnson]@uidaho.edu

Abstract:

The number of job positions in the operational technologies (OT) communications domain of Cyber Physical Systems (CPS) organizations has been increasing worldwide in the last 5 years. There exists a skills gap in the current CPS workforce. That gap has reached a critical level, especially for skills in the communication domain of CPS organizations. The use of hands-on exercises is known to be a practice that helps alleviate skills gap in students and in trainees. Incorporating hands-on exercises in a degree program will mitigate skills gap in graduates. While the graduates can help fill increasingly vacant positions in the communications domain of CPS organizations, it is also important to provide continuing education resources for working professionals. One of our course design priorities is to maximize access, outreach to the CPS workforce and to minimize potential damage caused by another pandemic-like societal disruption. As such, facilitating equity of access to quality hands-on educational materials across both remote and onsite learners is one of our important objectives. We created lab exercises for enabling hands-on learning in a CPS communication systems course for on-campus and remote learners.

Our hands-on exercises include tutorials in the following topics: 1) unmanaged and managed switch-based communication networks; 2) telemetry, component configuration and actuation workflows for communication using multiple OT protocols operating over Ethernet and over serial connections; 3) cybersecurity of communication devices in a CPS organization e.g., configuring gateways; and 4) commissioning i.e., testing et validation of communication devices in a CPS organization. Our exercises work uniformly and seamlessly for both onsite and remote learners. Creating uniform, seamless materials for both onsite and remote students required exploration of secure, easy-to-use network schemes that meet the requirements of a university network security policies. We discussed the challenges faced in our efforts. We present a case study where the described hands-on exercises are used in a joint listed senior/graduate level course at a public research university in the US. The case study course is cross listed for both Computer Science (CS) and Electrical Engineering (EE) majors. We present the results of an informal user experience survey for the students who performed our hands-on exercises.

I. Introduction:

Critical infrastructure organizations have been experiencing a technological transition for their devices from Industrial Control Systems (ICS) to CPS [1]. The transition is opening previously unavailable or limited networking capabilities to improve operational capabilities and efficiencies for industrial systems and infrastructure such as the power grid [1]. Expanded use of networked

communications in turn is increasing the attack vectors for the organizations, especially from outside actors [2]. As a result of the transition and the accompanying change in attack vectors, organizations need engineers skilled in configuring, operating, and maintaining their CPS devices. The CPS devices are often separated into Operational Technology (OT) networks, where timeliness and reliability of data communication is often critical [3]. The skills gap for OT communications and security engineers in a CPS organization is a known fact [4]. In addition, engineers specializing in the physical aspects of CPS often lack exposure to the cyber aspects in their education. Hands-on exercises are known to be effective instruments to train engineers to address skill gaps [5].

Education and training is needed for both full-time students located on college campuses and part-time students working full time in industry, often located far from a college campus.

II. Related Work and Problem:

There are not many open-source resources or literature items in the realm of hands-on educational exercises for CPS-OT communications and security systems. Such a lack of open-source materials is not surprising, given that OT networks and CPS devices are emerging technologies of recent decades. Here we list some auxiliary works that can be considered as outlier related works.

Dr. Konstantinou et al. have developed hands-on lab exercises for CPS security [6]. However, in this work, only 1 out of 6 hands-on activities is related to OT-CPS communication and security. All the other activities are related to the traditional IT enterprise networking communication and security such as buffer overflow, side channel attacks, performance counters, and multi-part computations.

The Escal Institute of Advanced Technologies (SANS Institute) has a 6-day intensive bootcamp for ICS/SCADA security topics. The bootcamp seems to focus partly on OT-CPS communication systems security [7]. Several CPS device vendors have their own vendor-specific training bootcamps as well. Problems associated with bootcamps is that they are:

1. Expensive, e.g., $8500 per student for 6 days [7]
2. Non-immersive, i.e., bootcamp instructors go through a high concentration of topics in a short time, leading to memory retention issues.

Therefore, the problem we face is that there are no immersive, relatively inexpensive, open-source resources for creating hands-on activities tailored for OT-CPS communications and security. In addition, the hands-on activities need to be securely available to both students located on-campus, and off-campus.

III. Solution, Setup, and Infrastructure:

With input from industry professionals working in the CPS field, we created eight hands-on activities i.e., "labs" that deal with multiple concepts associated with OT-CPS devices, ranging

from network protocols, quality of service, to HMI, commissioning, and general CPS cybersecurity maintenance. Most of these labs were prototyped through capstone senior design projects.

Figures 1, 2, and 3 show the baseline setup of our lab infrastructure for some hands-on activities. To be consistent with practices in industry, devices in Figures 1, 2, and 3 are connected using either serial, or USB, or Ethernet cables. Several of the devices in our lab are sourced from one specific vendor, which is Schweitzer Engineering Labs (SEL). The hands-on exercises are modular enough to allow deployment with devices manufactured by any vendor. To replicate our setup, devices required, and their approximate costs can be found in Table 1.
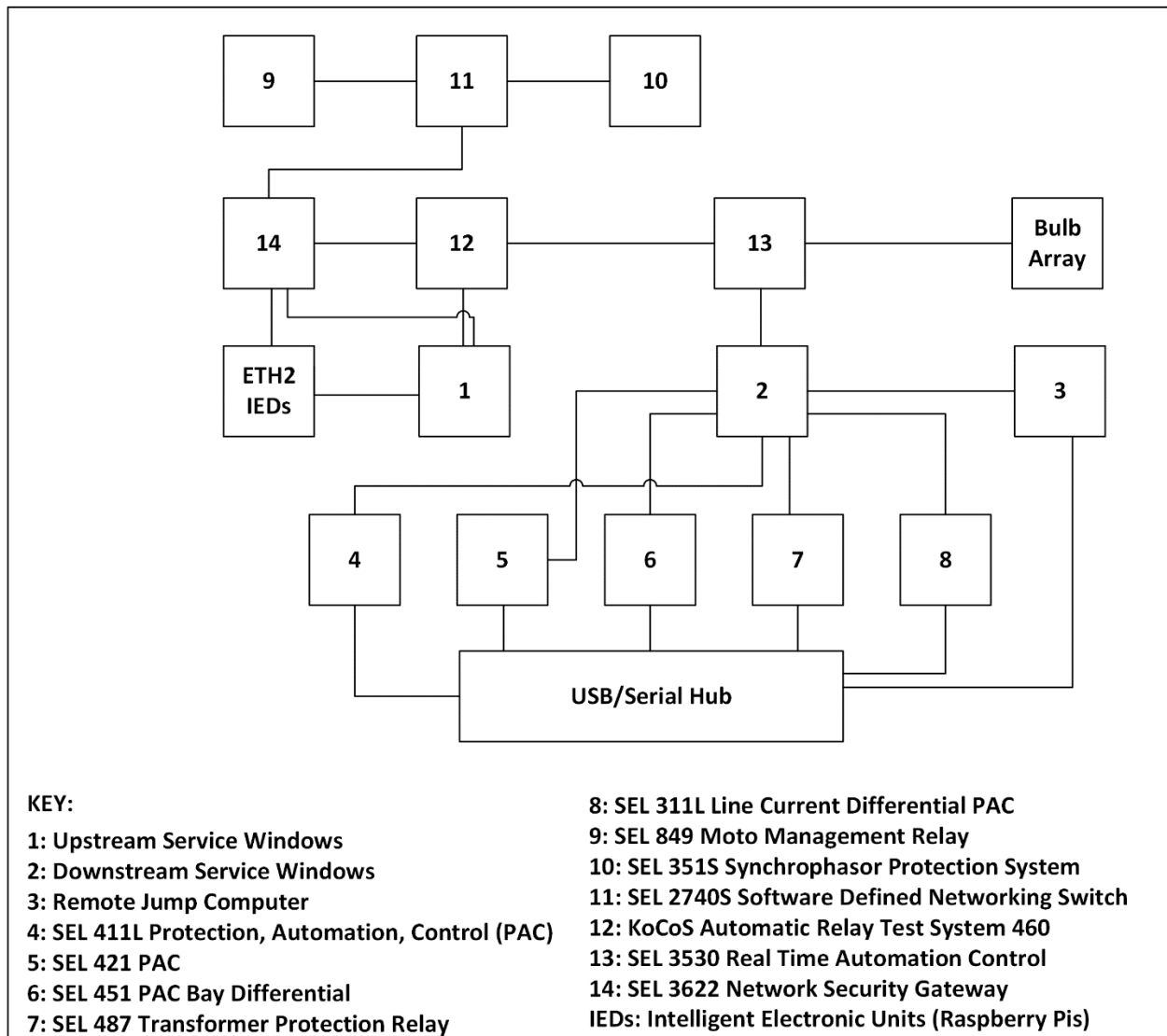
Table 1: Devices and materials required and their approximate costs.

Item	Price
Line Differential Protection, Automation, and Control System: SEL 411L [8]	$11,170
Transmission Protection, Automation, and Control System: SEL 421 [9]	$9,100
Substation Protection, Automation, and Bay Control System: SEL 451 [10]	$5,220
Transformer Protection Relay: SEL 487 [11]	$8,860
Line Current Protection and Automation System: SEL 311L [12]	$6,920
Motor Management Relay: SEL 849 [13]	$924
Power Protection System: SEL 351S [14]	$3,490
Software Defined Network Compatible Switch: SEL 2740S [15]	$4,950
Network Security Gateway: SEL 3622 [16]	$1,060
Real Time Automation Controller: SEL 3530 [17]	$3,740
Automatic Relay Test system: KoCoS ARTES 460 [18]	$37,600
Raspberry Pi [19] (2 needed, 2 backup)	$250
Cables and other general supplies [20]	$750
Total	**$94,034**

Prices seen in Table 1 are retail prices. Non-profit educational institutions may receive a discount when purchasing devices. The authors make no claims or guarantees about possibility of receiving discounts.

The 'Bulb Array' item represents an array of light bulbs that can be connected to represent dc systems, single-phase ac systems, or three phase ac systems. The bulb array allows students to observe real-time results of actions performed by their control system, such as normal operation, opening or closing circuit breakers, etc.

In our setup, off-campus/remote students can send in commands or perform actions synchronously with the CPS equipment via Remote Desktop Protocol (RDP). We have a mobile tripod-mounted camera in the room which allows remote students to watch the result of their actions on the lab infrastructure. Since the tripod-mounted camera is mobile, a lab assistant can move the camera around to show various effects of actions e.g., activating breakers, triggering specific phase bulbs, and so on.

KEY:

1: Upstream Service Windows
2: Downstream Service Windows
3: Remote Jump Computer
4: SEL 411L Protection, Automation, Control (PAC)
5: SEL 421 PAC
6: SEL 451 PAC Bay Differential
7: SEL 487 Transformer Protection Relay

8: SEL 311L Line Current Differential PAC
9: SEL 849 Moto Management Relay
10: SEL 351S Synchrophasor Protection System
11: SEL 2740S Software Defined Networking Switch
12: KoCoS Automatic Relay Test System 460
13: SEL 3530 Real Time Automation Control
14: SEL 3622 Network Security Gateway
IEDs: Intelligent Electronic Units (Raspberry Pis)

LAB INFRASTRUCTURE SETUP DIAGRAM

Figure 1: An abstract of baseline setup of lab instructure for some hands-on activities

To prevent unauthorized access and use, we isolate the infrastructure from the campus Internet via network segmentation. Remote users of the lab can access the infrastructure using a jump computer. To access the jump computer, a user would need valid university organizational

credentials and be a part of specific Virtual Private Network (VPN) group that is flushed and recreated for each course offering.

IV. Hands-on Exercises:

We have released reference manuals for our hands-on activities in a GitHub repository [21]. The manuals include specific setup and connection diagrams and detailed instructions about the processes involved in conducting the hands-on activities. The manuals have been released under a
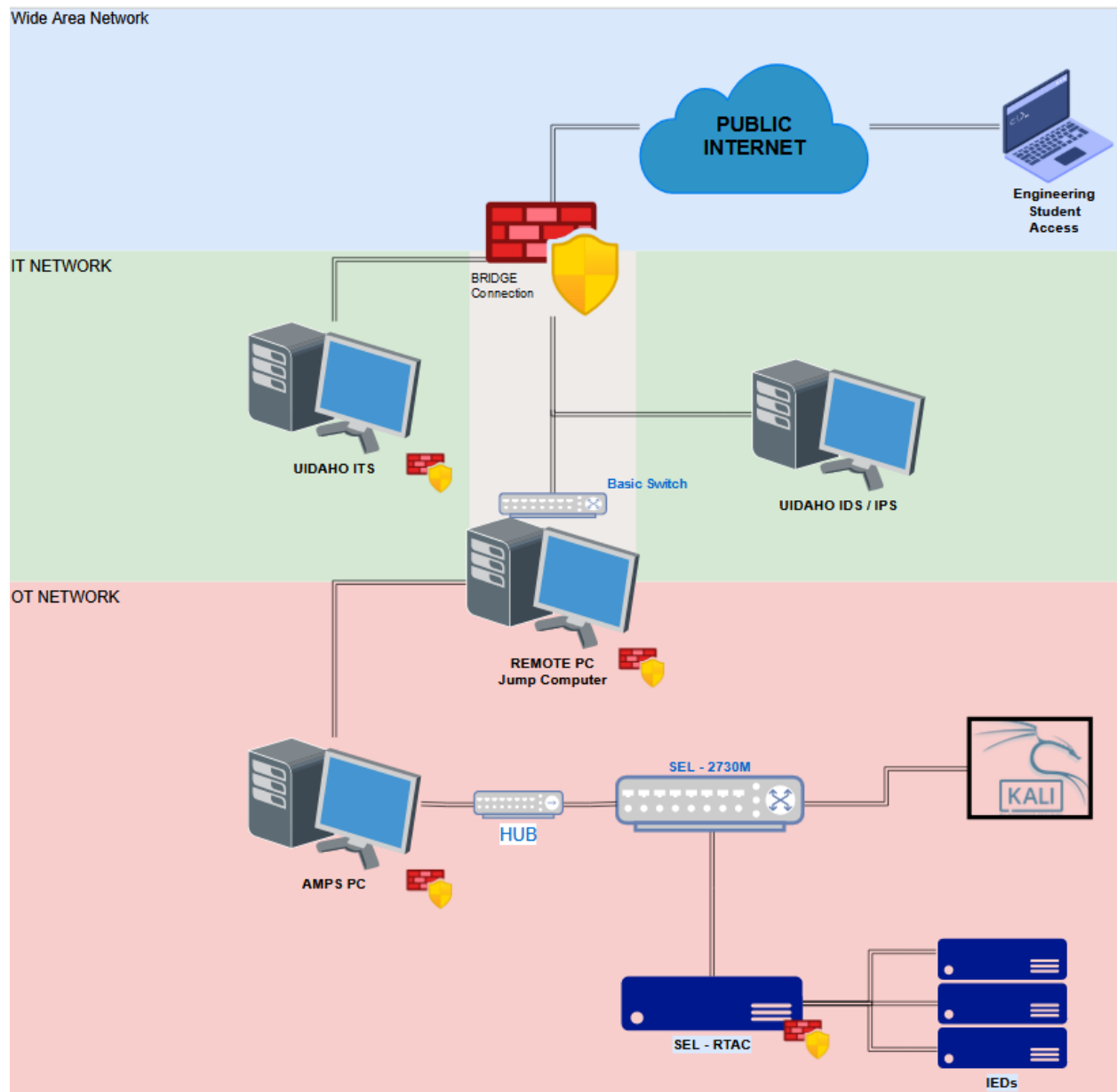

Figure 2: Visualized baseline setup of lab infrastructure for some hands-on activities

A list of our hands-on activities are as follows:

Activity 1. Introduce Intelligent Electronic Devices (IEDs)
   a. Connect to an IED
   b. Learn interface software
   c. Communicate with an IED
Activity 2. Introduce Remote Terminal Units (RTUs)
   a. Connect to and communicate with an RTU
   b. Establish connectivity and data transactions between RTU and IEDs
Activity 3. Introduce Human Machine Interfaces (HMIs)
   a. Get acquainted with HMI functions and characteristics
   b. Create a custom HMI using Schweitzer Engineering Labs (SEL) diagram builder
Activity 4. Commissioning and actuating a new device into an existing CPS system
   a. Commission and actuate SEL 351
   b. Complete installation guide by following reference manuals
Activity 5. OT Network establishment, configuration, and maintenance
   a. Configure and deploy SEL 3622: a network security gateway
   b. Password management, proxy access points, and direct access points
Activity 6. OT-Network data communications
   a. Connecting system with six managed ethernet switches to IEDs
   b. Conduct network stress, congestion tests using Ostinato comparing unmanaged and managed switches
   c. Observe network performance using Wireshark
Activity 7. Quality of service determination for OT-Networks
   a. Create a loop network connection and run two experiments with physical failure of network cable: one with Rapid Spanning Tree Protocol (RSTP) and another with no RSTP
   b. For each experiment measure: packet loss, throughput, latency, jitter, and spanning tree convergence time
Activity 8. Commission an automation controller and establish a connection from the automation controller to a downstream relay
   a. Three phase output producing test system to bulb array: KoCoS ARTES 460
   b. Automation Controller: SEL 3530
   c. Downstream relay device options: SEL 849, 421, 451, 311, 487, 3530 and KoCoS ARTES 460
   d. Protocol options available: DNP3, Modbus, Goose, Serial or Ethernet
Activity 9. Introduce standard CPS-OT network security practices and learn penetration testing (pen-testing) to identify security gaps to better secure CPS-OT networks
   a. Practice defense in depth strategy elements
   b. Network reconnaissance via mapping routes, ports, and packet sniffing
   c. Identify security gaps i.e. insecure ports, routes, unencrypted packets, etc.

d. Fix identified security gaps via network hardening and segmentation i.e. MAC filtering, Virtual Local Area Network (VLAN) and firewall configuration, etc.

e. Optional: practice virtualized network deployment and maintenance via VMWare Workstation, SecurityOnion, etc.

V. Case Study:

We tested the effectiveness of hands-on activities numbers 6, 7, and 8 in a 3-credit semester course at a public, high-research, doctoral-granting university in the United States. The course was offered to senior undergraduate and graduate students, cross-listed for both Electrical Engineering and Computer Science programs. Activities 6 and 7 were prototyped by a senior design capstone project team and have been used in the course several times with access limited to on-campus students. The most recent offering of the course added access for off-campus students taking courses remotely as well as adding exercise 6.

Exercises 1 through 5 were prototyped by a second senior design team and will be fully integrated into the course the next time it is offered.
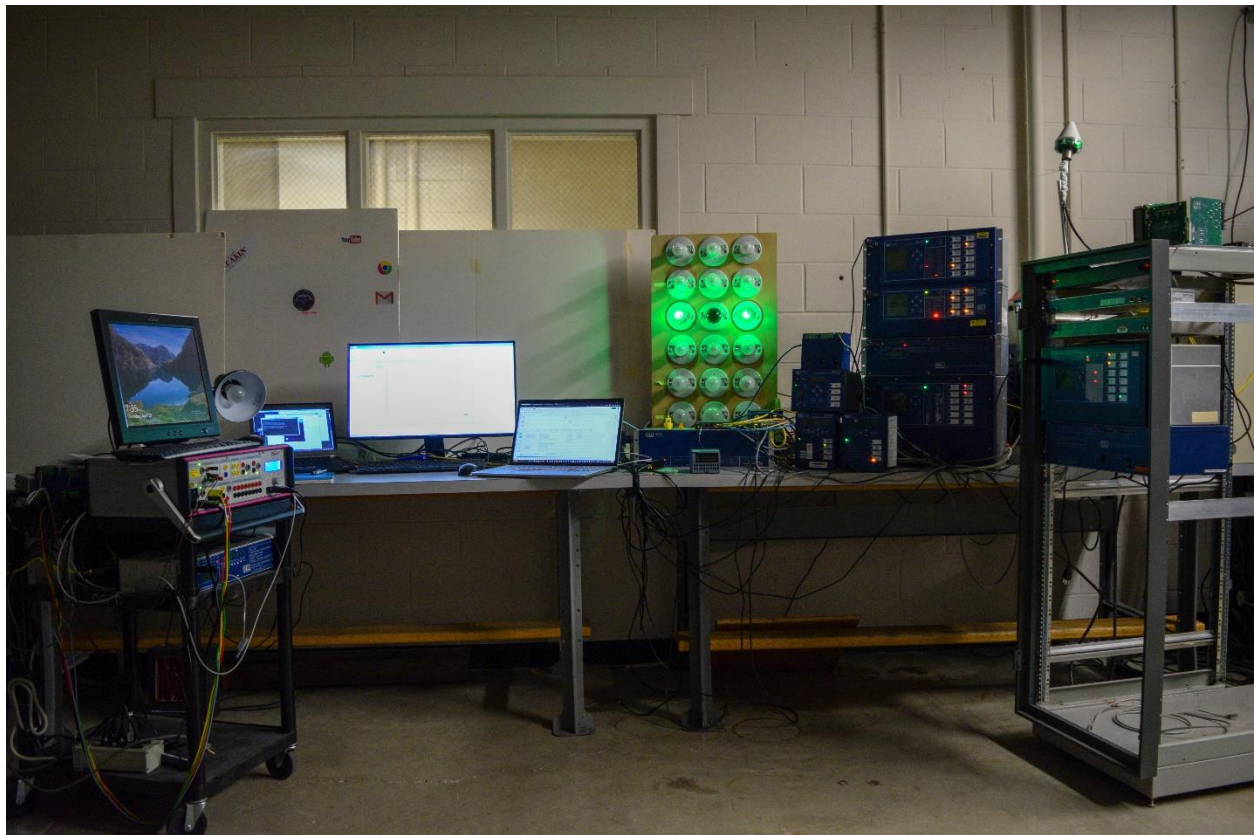

Figure 3: A photo of the baseline setup of lab infrastructure for some hands-on activities

In the most recent offering of the course, students were granted the ability to choose between hands-on activities 7 and 8 after completing exercise 6. Despite needing to complete only one of 7 or 8 for the course, we observed self-initiated interest from several students to do both the activities. Within activity number 8, students had the ability to choose which downstream relay devices to configure to communicate with the automation controller. In addition, the students were given the option to choose which communication protocol to configure in the automation controller and the relay devices for data transfers. Upon completion of the requirements for the lab exercises, many of the students requested the option to repeat the exercises with other communication protocols. The end of course review comments related to hands-on exercises were very positive.

VI. Conclusion:

We discussed the problem of lacking open-source, cost-efficient, and immersive hands-on activities for OT-CPS device commissioning and maintenance. We presented our solution: 8 hands-on lab exercises dealing with various aspects of OT-CPS device ecosystem that anybody can repurpose for non-profit educational endeavors. We have also discussed one potential deployment structure to help facilitate the execution of our hands-on activities. Our deployment structure includes discussions about specific implementation devices and their approximate costs.

VII.   References

[1] A. A. Jillepalli, D. C. De Leon, J. Alves-Foss, C. L. Jeffery and F. T. Sheldon, "A Formal Model and Verification for HESTIA: An Automated, Adversary-Aware Risk Assessment Process for Cyber Infrastructure," in IEEE Access, vol. 10, pp. 83755-83792, 2022, doi: 10.1109/ACCESS.2022.3197195.

[2] A. A. Jillepalli et al., "METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security," 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), Nantucket, MA, USA, 2018, pp. 95-102, doi: 10.1109/MALWARE.2018.8659367.

[3] Cisco, "How do OT and IT Differ?", [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

[4] A. Ribeiro, "OT security skills gap is a major challenge for industrial, manufacturing organizations", Industrial Cyber. [Online]. Available: https://industrialcyber.co/news/ot-security-skills-gap-is-a-major-challenge-for-industrial-manufacturing-organizations/

[5] S. Steiner, A. Jillepalli, and D. C. De Leon. "A survey of cloud-hosted, publicly available, cyber-ranges for educational institutions", J. Comput. Sci. Coll. 38, 1 (November 2022), 68–77.

[6] C. Konstantinou, "Cyber-Physical Systems Security Education Through Hands-on Lab Exercises," in IEEE Design & Test, vol. 37, no. 6, pp. 47-55, Dec. 2020, doi: 10.1109/MDAT.2020.3005365.

[7] J. Searle, "ICS410: ICS/SCADA Security Essentials", The SANS Institute, [Online]. Available: https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

[8] SEL-411L. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/411L/

[9] SEL-421. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/421/

[10] SEL-451. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/451/

[11] SEL-487E. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/487E/

[12] SEL-311L. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/311L/

[13] SEL-849. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/849/

[14] SEL-351S. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/351S/

[15] SEL-2740S. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/2740S/

[16] SEL-3622. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/3622/

[17] SEL-3530. Schweitzer Engineering Lab. [Online]. Available: https://selinc.com/products/3530/

[18] KoCos ARTES 460. TEquipment. [Online]. Available: https://www.tequipment.net/KoCos/ARTES-460-II/Secondary-Injection-Test-Equipment/

[19] Raspberry Pi Model 2. [Online]. Available: https://www.amazon.com/Raspberry-Pi-Model-Desktop-Linux/dp/B00T2U7R7I/

[20] Cables and general supplies. Amazon. [Online]. Available: https://www.amazon.com/stores/page/5A234098-933E-4E05-8826-1431B7662F88

[21] The Idaho CPA SCADA Cybersecurity systems group at University of Idaho. GitHub. [Online]. Available: https://github.com/MPS-ISAAC

[22] CC BY-NC-SA 4.0. Creative Commons. [Online]. Available: https://creativecommons.org/licenses/by-nc-sa/4.0/

VIII.   Appendix A: Detailed Baseline Setup Diagram