Open Access License Notice

A Vertically Integrated Pathway for Infusing Engineering Technicians with Industrial Cybersecurity Competencies

Sean McBride
Idaho State University
Pocatello, USA
SeanMcBride@isu.edu

Corey Schou
Idaho State University
Pocatello, USA
Schou@iri.isu.edu

Jill Slay
University of South Australia
Mawson Lakes, Australia
Jill.Slay@unisa.edu.au

Abstract—This paper describes an effort to establish a vertically integrated pathway to identify and develop industrial control systems cybersecurity talent that extends from middle school to graduate degrees, leveraging the unique strengths of career and technical education. Educators and administrators seeking to ignite student interest in cybersecurity at a young age, and to provide a clear curriculum pathway to meet employer needs in the field of industrial cybersecurity may find this effort of use.

Keywords—industrial control systems, cybersecurity, training, education, career and technical education, engineering technology, technicians

I. Introduction

A key critique of cybersecurity education in 2021 is that it does not account for the educational and training pathways of many engineering technicians [1]. These professionals frequently come from two-year technology programs, and develop professionally by spending significant time within industrial operations on the plant floor. As their career progresses, they may become field engineers, and eventually managers. A review of the Accreditation Board for Engineering and Technology (now ABET) web site shows 89 accredited technology programs in the United States that produce electrical engineering technicians [2].

While ad-hoc lifelong learning and professional training offered by commercial providers such as SANS [3] help address this challenge, we assert that critical cyber-physical infrastructures such as electric generating facilities, water provisioning systems, and oil refineries will benefit most from incorporating robust cybersecurity education and training into the formalized pathways that technical professionals frequently follow.

In this paper we propose a vertically integrated pathway to address this challenge, based on the experience of Idaho State University (ISU).

Work supported in part by a scholarship from La Trobe University

II. Idaho State University's Involvement in Cybersecurity Education

As noted in [4] Idaho State University has a distinctive, if little known, history in cybersecurity education, beginning at the foundation of the field, and extending to a specialized focus on critical infrastructure and industrial control systems.

- In 1988 a group of cybersecurity professionals meeting at Idaho State University formalized plans to create the International Information Systems Security Certification Consortium $(ISC)^2$ – the world's leading professional cybersecurity certification body – which has certified 150,000 cybersecurity professionals [5].
- In the 1990s ISU held educational standards development sessions to create the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and Committee on National Security Systems (CNSS) training guidance [6].
- These NSTISSC and CNSS instructions became the content criteria for designating schools as Centers of Academic Excellence in Information Assurance (now Cybersecurity) [7, 8].
- In 1996, ISU helped found the Colloquium for Information Systems Security Education (CISSE) [9, 10].
- In 2003, ISU was among the first seven schools in the USA to be designated Centers of Academic Excellence (CAE) in Information Assurance [11].
- In 2014, recognizing growing need, ISU became one of just two CAEs to qualify with a focus on Industrial Control Systems and SCADA Security [12].

III. Southeast Idaho as a Talent Hotbed for Industrial Cybersecurity

The Idaho National Laboratory (INL) is the most significant cybersecurity employer in the state of Idaho, with more than 150 employees dedicated to the field. These employees work primarily in Idaho Falls, just a 45-minute

drive from the ISU main campus in Pocatello, and immediately adjacent to the ISU remote campus known as University Place. A brief review of INL's history in industrial cybersecurity provides important context for the integrated pathway we describe:

- In 2003, the Idaho National Laboratory, relying on several ISU graduates, became a principal location of the Department of Energy's National SCADA Testbed effort to secure industrial control systems [13-4].
- From 2009 to 2015, the Idaho National Laboratory ran significant portions of the Department of Homeland Security's Industrial Control Systems Computer Incident Response Team (ICS-CERT) [15].
- In 2011, the New York Times ran an article which suggested that the INL had been involved in developing the famous Stuxnet computer virus that the US Government used to disrupt a nuclear weapons uranium enrichment plant in Iran [16], indicating its reputation as a leader in the field, and implying its involvement in broader government-sponsored cyber operations.
- In 2016, the INL published its Consequence Driven Cyber Informed Engineering (CCE) methodology for integrating engineering principles into security reviews of the nation's most critical industrial control system infrastructures [17-18].

Building on these accomplishments, the INL anticipates increasing its cybersecurity workforce over the next several years. In addition, employers from across the United States recruit from the Idaho Falls area, often allowing employees to work remotely.

As the nearest public university, ISU desires to 1) create a pathway for industrial cybersecurity talent to meet demand from INL and 2) create an exemplar curriculum and industry/academic relationship to display how the curriculum can be applied to industry problems worldwide. In 2015, Idaho State University's College of Technology became the first public school in the country to offer a Degree in Industrial Cybersecurity [19]. The foundation of ISU's pathway development effort consists of vertical integration facilitated through career and technical education (CTE).

IV. Vertical Integration

Vertical integration refers to intentionally coordinated relationships among stakeholders from different stages of the educational process, as shown in Table I. These relationships – spanning institutional boundaries – allow faculty to clearly indicate the next steps an interested student may consider.

TABLE I. Stages of a Vertically Integrated Program

	Institution Type	**Faculty Role**	**Vertical Integration Actions**
Stage 1	Middle/High School	STEM related instructor	• Co-teach at college summer camp • Invite college instructorto visit classroom • Incorporate college program content
Stage 2	Technical College	Program Coordinator	• Co-teach with HS instructor at summer camp • Serve on HS advisory committee • Lead hands-on experiences in HS classrooms • Provide program tours • Invite employer to visit • Invite employer to advisory committee
Stage 3	University	Major Faculty Advisor	• Articulate with college programs • Coordinate scholarshipsfor desired pathways • Introduce to student to graduate faculty
Stage 4	Employer	Hiring Manager	• Support summer camp with funds or other contributions • Participate on college program advisory committee • Visit college classroom • Provide internships • Hire graduates
Stage 5	Graduate School	Graduate Supervisor	• Meet promising undergraduates • Coordinate course offerings (times, locations, topics) with local employers

Speaking from the authors' empirical observation as students, graduate students, professionals, and instructors, the prevailing formalized educational model focuses on what a student learns within each stage – and often within a particular component of the stage – without intentional focus

on transition between stages. Let's consider a hypothetical case of how improved vertical integration could benefit a middle school student, Alice.

In a required math class, Alice learns of a hands-on STEM summer camp opportunity from her teacher, who hands out a promotional flyer. Alice attends the camp, where she meets a high school teacher (helping run the camp) who encourages Alice to take the teacher's class as an elective. Even though two years go by, Alice sees the same teacher in the hall, and decides to sign up for her class. There, Alice participates in a hands-on activity brought to the school by a technical college instructor, who leaves behind contact information and promotional materials. The high school teacher coordinates a field trip to tour the college program. Alice attends the tour, likes what she sees, and enrolls.

During the college program, Alice hears from various employers who come to speak and seek new hires. She ends up interning with one of these employers. The employer recognizes Alice's great potential, and offers her a full-time job. She chooses instead to stay in school believing that a bachelor degree will serve her better in the long run. Her instructor points out which upper division classes will ensure employability. While taking these classes, her faculty advisor at the bachelor level offers to introduce Alice to a graduate-level faculty friend at another institution. Simultaneously, the company with which Alice first interned, offers her a full-time job at a higher wage, and describes its educational benefit that will pay for her to take a part time Master's Degree. Alice takes the job and signs up for online Master's classes.

In this scenario (summarized in Fig. 1), it was the vertical integration (in addition to appropriate instruction), that ensured Alice obtained a job, the employer obtained an employee, and the graduate program continued advancing employee value.

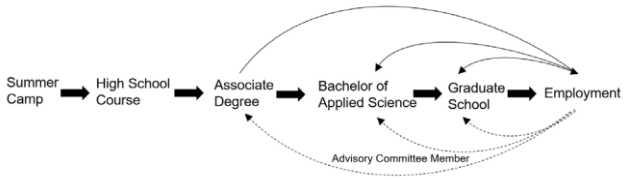

Fig. 1. Vertically integrated pathway from student perspective

V. The Role of Career and Technical Education

Career and Technical Education (CTE) refers to educational approaches that openly incorporate hands-on methods, emphasizing the link to employable competencies [20]. In Idaho, candidacy for becoming a CTE instructor requires not a degree, but years of professional experience in the field. Industry professionals and hiring managers who have an interest in producing strong entry-level employees help guide program curriculum by participating on advisory committees [21]. CTE instructors exist at both secondary and post-secondary levels. Most post-secondary degree programs offer Associate's Degrees, and are accredited by the same accrediting bodies as many academic programs. For example, ABET accredits both technical 2-year programs, and bachelor programs in engineering and technology fields, including cybersecurity [22].

Idaho State University has a unique strength in that it's College of Technology is a technical college embedded within the university structure – see Fig. 2. This allows the school to offer hands-on programs and laboratory learning experiences often missing from purely academic university programs. Literature explains that such hands-on experience is desirable for cybersecurity, and particularly desirable for cyber-physical systems [23-25].

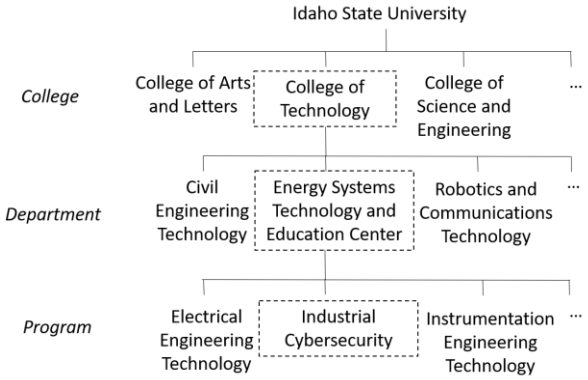

Fig. 2. ISU Organizational Structure

While most high school and college students have used a computer that controls information and have some sense of security (at least how passwords work) far fewer have used a programmable logic controller (PLC) that controls production in an industrial facility – like those used in Idaho to process raw potatoes into dehydrated mashed potatoes in a bag. It may be difficult to commence a career securing devices that one has never before seen, let alone never handled and experienced.

ISU's Energy Systems Technology and Education Center (ESTEC) within the College of Technology has the mission of creating hands-on technicians and field engineers that work in power plants, water treatment facilities, and manufacturing facilities [26]. ESTEC has instructional laboratory space designed to produce technicians in mechanical engineering, electrical engineering, instrumentation engineering, and nuclear operations.

VI. Raspberry PIs and Dehydrated Potatoes

Content for vertical integration revolves around ESET 181: IT-OT Fundamentals (IT refers to information technology, and OT refers to operational technologies – used to operate industrial control systems). The premise of this project-based course is that students design and build a notional industrial control system based on the needs of a real local potato processing firm – Basic American Foods (BAF). Students read local press articles explaining that BAF is closing one facility in favor of increasing automation at another. They visit the BAF website to see the products the firm produces.

Through a series of 43 hands-on learning activities, students rely on a credit-card sized computing platform known as the Raspberry Pi to explore and experience: IT-OT environments, computing & operating systems, coding, basic process control, web technologies, supervisory control and data acquisition (SCADA), networking, industrial networks, the IT-OT gap, network monitoring, security, and the future of OT. At the end of the semester, the students present their project, which combines the elements named above. This provides students with an exciting view of what their future holds.

A. Engaging Middle School and High School Students

ISU's ESTEC organizes an annual "Ignite Their Future" summer camp for middle school and high school students held on campus [27]. The objective of the camp is to excite students about a career in a STEM-related field. In 2019, the camp included 12 strands, and served more than 100 students.

Middle school and high school teachers sign up to co-teach strands with ESTEC instructors. The week before the camp, the teachers sit with ESTEC instructors to learn the material and create/update lesson plans. The teachers earn continuing professional education (CPE) hours, and the camp offers them a stipend for their support.

Through their participation in the camp, middle school and high school teachers have now set foot in the ESTEC buildings, and had positive experiences with college instructors. This increases their confidence in the system, and the likelihood of them mentioning the camp to their students. Next year they may sign up to co-teach a different strand.

Content for the "Build a Raspberry Pi Computer" strand is taken directly from the IT-OT Fundamentals course. While the way it is taught to middle schoolers differs from the way it is taught to undergraduate students, re-use of content offers certain convenience.

Middle school students will now have visited ESTEC classrooms – many years before attending a program there, hopefully influencing their attitude about attending college.

B. Engaging High School Students

ESTEC pays special attention to relationships with specific high school CTE instructors. The Association for Career and Technical Education claims that over 90% of high school students across the US are part of CTE [15]. This is a fantastic opportunity to identify interested students, and point them towards next steps.

ISU's Industrial Cybersecurity program has developed a relationship with several high school CTE instructors in its region. The college instructor visits these high school instructors and their students three or four times each year. During these visits, the instructor delivers a hands-on learning activity taken directly from the ESET 181 course.

We have found that most students are easily engaged in a simple cybersecurity exercise using Raspberry Pis (RPis) – which the college instructor brings to the high school classroom. The RPis are configured with secure shell (SSH) open and default credentials. Students warm up learning some basic Linux commands, including how to make a directory and create a file. They connect a network cable to their neighbor's RPi, and find their IP address. They use their smartphones to find the default SSH password credentials. They SSH to the other computer, and examine the contents of the file the other student made. They then leave their own file on their neighbors' computer. Students are surprised to learn that the other person has no immediate indication that someone else is reading and leaving files. The exercise ends with a digital arms race where one student from each pair represents the USA and one represents Russia. The instructor tells the students that whoever types the following command fastest will win the race and turn off the other person's computer: `sudo shutdown now`. Students yell in excitement or disappointment as half the screens go dark.

The college instructor then leads a debrief in which he asks the students to describe what lessons they learned from the exercise. "How to hack", says one. "Not to let anyone know your IP address", says another. "Change your default password", claims a third. These sincere responses offer a fantastic opportunity to engage in conversation about ethics, networks, and security, respectively.

Normally, one or two students will have previous knowledge of Linux. Occasionally, a student will have previous exposure to security tools such as those included with the Kali distribution. The instructor may wish to pay special attention to these students and chat with them after class. The instructor leaves behind promotional materials and offers to set up a program tour for anyone interested.

Through this hands-on experience, high school students have actually seen a college instructor, and likely learned something from him or her. They now know how to find additional information, and can ask their high school instructor any questions they may have.

It is worthwhile for the college instructor to offer to serve on the high school instructor's advisory committee. As many high school CTE students go on for more education rather than enter the workforce directly, the college instructor offers an important perspective.

As a next step for vertical integration with high schools, ISU's College of Technology plans to adjust the ESET 181 course for a high school audience, and pilot the course for dual credit with a high school instructor. Ideally the course would also qualify as a university general education course – providing additional incentive for high school students to enroll.

C. Pathway to Bachelor

In Fall 2019, the State of Idaho created a Bachelor of Applied Science in Cyber-Physical Systems Engineering Technology (BASCPS) at ISU. This pathway lays out the year 3 and 4 upper division classes for students who already have Associate degrees in the following fields, from any of Idaho's six technical colleges:

- Instrumentation Engineering Technology
- Electrical Engineering Technology
- Mechanical Engineering Technology
- Nuclear Operations Technology
- Information Technology Systems
- Robotics and Communications Systems
- Diesel Onsite Power Technology

Year three of the program – which runs under a cohort model – earns the student an Intermediate Technical Certificate in Industrial Cybersecurity, and includes the courses shown in the table below. Depending on the Associate Degree the student has earned, they may substitute electives for the Industrial Operations or IT courses. The Industrial Cybersecurity courses are offered at the upper division level.

Industrial Operations	**IT**	**Industrial Cybersecurity**
Engineering Technology	IT-OT Fundamentals	Secure Systems Design
Energy Systems	Networking	Risk Management
Digital Control		Network Security
		Critical Infrastructure Defense
		Professional Certification
		Capstone

Year 4 of the program covers remaining general education requirements and the following upper division courses, to prepare a well-rounded professional: Technical Writing, Individual and Organizational Behavior, Project Management, Operations and Production Management, Information Assurance, Informatics & Analytics.

D. Graduate Options

Currently Idaho State University offers two options for graduate students. First is National Information Assurance Training and Education Center (NIATEC) – a full time NSF Scholarship for Service program, where students earn a Master of Business Administration degree in preparation for leadership-level employment within the federal government. Students who have graduated with the BASCPS are well positioned for NIATEC because they 1) have previously developed an employable skill set; 2) have rounded out that skill set with management and communications courses; 3) have significant previous exposure to cybersecurity.

E. A Cycle of Vertical Integration

As the cybersecurity industry grows in Southeast Idaho, ISU's graduates who have worked for diverse government entities (often in the Washington, DC area) since 2005, are now returning – many to find employment at the Idaho National Laboratory. They now serve as program advisors, guest lecturers, adjunct faculty, and hiring managers – turning vertical integration into a virtuous cycle.

VII. Future Work and Conclusions

Vertical integration leveraging career and technical education appears a promising pathway for developing the unique combination of hands-on and academic competencies required to protect industrial infrastructures. While not all schools benefit from the CTE alignment present at Idaho State University, there is no intrinsic reason forward-thinking academic institutions cannot develop similar relationships and alignment.

Of course, successful vertical integration for industrial cybersecurity requires quality instructional capabilities, including appropriate pedagogical models, student learning outcomes, curricula design, and laboratories for hands-on instructional interventions. Future work will discuss our efforts to develop these aspects of an effective program.

We recognize that industrial cybersecurity is a global concern, and anticipate value in exporting this vertically integrated curricular pathway model to educational environments in other countries. Future work will need to examine its applicability in alternate educational systems.

References

[1] Ngambeki, I., McBride, S., and Slay, J., "Knowledge Gaps in Curricular Guidance for ICS Security" Colloquium for Information Systems Security Education, 2021.

[2] ABET, Accredited Programs,[Online]. https://amspub.abet.org/aps/category-search?disciplines=25&degreeLevels=A&countries=US. accessed June 19, 2020

[3] SANS, Industrial Control Systems, [Online]. https://ics.sans.org/, accessed June 19, 2020

[4] Idaho State University, "ISU's Corey Schou inducted 2019 Cyber Security Hall of Fame", Idaho State Journal. [Online]. https://www.idahostatejournal.com/community/isu-s-corey-schou-inducted-2019-cyber-security-hall-of-fame/article_c52c1de4-24d5-5202-a847-66c18daac447.html

[5] $(ISC)^2$, About, [Online]. https://www.isc2.org/About

[6] National Institute of Standards and Technology, National Computer Security Conference, (16th) Proceedings, p. 462, 1993. [Online]. https://books.google.com/books?id=vQEHUD51YNEC, accessed June 29, 2020.

[7] Bishop, M., & Taylor, C. "A Critical Analysis of the Centers of Academic Excellence Program", 2009. [Online]. https://cisse.info/resources/archives/category/12-papers?download=125:s01p04-2009

[8] Spafford, E. "An Anniversary of Continuing Excellence", 2019. [Online]. https://www.cerias.purdue.edu/site/blog/2019/05/

[9] CISSE, 23 Colloquium for Information Systems Security Education. 2019. [Online]. https://cisse.info/pdf/2019/23rd%20Colloquium%20-20Program%20&%20Agenda.pdf

[10] CISSE, Cybersecurity Education Innovation for the 21st Century, [Online]. https://cisse.info/journal/index.php/cisse/about, accessed June 17, 2020

[11] Celebrating 20 Years with the Centers of Academic Excellence in Cyber Defense, 2019. [Online]. https://www.caecommunity.org/sites/default/files/CAE_Book_Version_1.6-2.pdf

[12] NSA, CAE Designated Institutions. [Online]. Retrieved from: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm. June 17, 2020

[13] U.S. Department of Energy, National SCADA Test Bed, [Online]. https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed, accessed June 17, 2020

[14] D. Kuipers, Idaho National Laboratory National SCADA Test Bed, (2010). https://permanent.fdlp.gov/lps103348/scada_test_bed_4.pdf, accessed June 17, 2020.

[15] Idaho National Laboratory, Control Systems Cyber Security, [Online]. https://inl.gov/research-programs/control-systems-cyber-security/, accessed June 22, 2020.

[16] Broad, W.J., Markoff, J. Sanger, D., "Stuxnet worm used against Iran was Tested in Israel", New York Times, 2011.

[17] Idaho National Laboratory, "Consequence-driven Cyber-Informed Engineering (CCE)", 2016. [Online]. https://inl.gov/wp-content/uploads/2020/01/DOE_OSTI_CCEconcept-Paper.pdf, accessed July 1, 2020.

[18] Idaho National Laboratory "Consequence-driven Cyber-informed Engineering", [Online]. https://inl.gov/cce/, accessed July 1, 2020.

[19] Idaho Career and Technical Education, Technical Advisory Committees, [Online]. https://cte.idaho.gov/educators/technical-advisory-committees/

[20] Association for Career and Technical Education, "What is CTE?" [Online]. https://www.acteonline.org/why-cte/what-is-cte/, accessed June 17, 2020

[21] Idaho Career and Technical Education, Technical Advisory Committees, [Online]. https://cte.idaho.gov/educators/technical-advisory-committees/, June 17, 2020.

[22] ABET, "What Programs Does ABET Accredit?" [Online]. https://www.abet.org/accreditation/what-is-accreditation/what-programs-does-abet-accredit/. Accessed June 22, 2020

[23] Conklin, W., Cline, R., & Roosa, T. "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors", 2014. [Online]. https://ieeexplore.ieee.org/document/6758852, accessed June 22, 2020.

[24] National Academies of Sciences, Engineering and Medicine. "A 21st Century Cyber-Physical Systems Education", Washington, DC: The National Academies Press. 2016. https://doi.org/10.17226/23686. [Online]. https://www.nap.edu/catalog/23686/a-21st-century-cyber-physical-systems-education, accessed June 22, 2020.

[25] Sitnikova, E., Foo, E., Vaughn, R., "The Power of Hands-On Exercises in SCADA Cyber Security Education", 2013. [Online]. https://link.springer.com/content/pdf/10.1007%2F978-3-642-39377-8_9.pdf

[26] Idaho State University, Energy System Technology & Education Center (ESTEC) [Online]. https://www.isu.edu/estec/, accessed June 19, 2020

[27] Idaho State University, Ignite Their Future Summer Camp Series, [Online]. https://cetrain.isu.edu/enrollment/course/ignite-their-future-summer-camp-series/, accessed June 19, 2020

APPENDIX: ESET 181 INFORMATION TECHNOLOGY OPERATIONAL TECHNOLOGY (IT-OT) FUNDAMENTALS ABBREVIATED SYLLABUS

A. Course Description

Establishes fundamental understanding of information technologies for industrial control systems professionals. Topics include: operating systems, databases, programming, and virtualization. Establishes fundamental understanding of operational technologies for IT professionals. Topics include: PLCs, SCADA, HMIs, process diagrams.

B. Course Objectives

Upon successful completion of this course, students will be able to:

- Describe operational technologies such as SCADA, HMI, PLC engineering laptop, and common ICS network communication protocols
- Describe common roles and responsibilities that deal with IT and OT within industrial environments
- Explain common information technologies used in OT, including: computer hardware, operating systems, programming, applications, networks, databases, and virtualization
- Build and interact with an elementary SCADA system
- Identify common cybersecurity concerns within industrial environments

C. Required Materials

Computer/Laptop
Web browser
University network account

Electronic components for Raspberry Pi
Plenty of male to female jumpers
One set of colored LEDs (RBG)
Adafruit DHT 11 sensor

Raspberry Pi
Model 4
Mini HDMI to HDMI adapter
32 GB MicroSD card with NOOBS

D. Weekly Schedule

Topic 1: Introduction to IT-OTFundamentals
Identify Computer Components
Rack a Server
Create Process Flow Block Diagram
Design SCADA Interface

Topic 2: Raspberry PiComputing Platform
Explore BIOS/UEFI
Make Bootable USB
Register RPi on ISU DeviceNet
Navigate Command Line
Update and upgrade Linux
Explore password files
Add user and manage permissions

Topic 3: Coding
Use Turtle Python library to make a shape
Use Turtle to make a spiral of spirals
Use Turtle to make an interactive spiral shape
Review and modify pre-written code

Topic 4: Cyber-Physical Systems
Connect LED
Connect Temperature Sensor
Create six light traffic control system
Investigate leading ICS vendors

Topic 5: Web Technologies
HTML source within your Browser
Create a Web Page Folder

Topic 5: Web Technologies
Explore Web Hosting Options Folder
Explore DNS Data Folder
Control LED from Web page

Topic 6: Supervisory Control
Turn On/Off LED using Node-RED
Display Temperature trend using Node-RED

Topic 7: Intro to Networking
Explore Network Settings on RPi
Network Pi's Together
Assign static IP address to your RPi

Topic 8: Industrial Networking
Draw a network diagram
Configure Cisco switch in packet tracer
Describe industrial switch

Topic 9: IT-OT Gap
Create skit demonstrating IT-OT gap

Topic 10: Network Monitoring
Use Nmap to scan a network
Install and use TCPDUMP
IoT fingerprinting
Explore ICS network monitoring solutions

Topic 11: Security
Create asset inventory
Review and improve network architecture
Add security to Node-RED on RPi

Topic 11: Security
Configure Firewall in Packet Tracer
Test Firewall in Packet Tracer

Topic 12: Future of OT
Create VM in AWS cloud
Control RPi LED from your phone
Current events briefing