Knowledge Gaps in Curricular Guidance for ICS Security

Ida Ngambeki
Purdue University
West Lafayette, USA
ingambek@purdue.edu

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

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

Abstract—Industrial Control Systems are an essential mechanism to manage complex computer systems necessary for modern life. These include everything from water treatment and transportation to energy systems and manufacturing. These systems are becoming increasingly integrated and more complex, and they are being used to manage even more of the elements that make our everyday lives possible. They are therefore becoming both more attractive to cyber criminals and more vulnerable to cyber-attacks. More attention needs to be paid to increasing resources and capability in industrial cybersecurity (ICSS). A major element of this is to significantly improve both the quality and availability of education in this area. The process of development of these educational initiatives is aided by curriculum guidance documents. Of necessity ICSS has largely evolved in industrial settings. This exploratory study examines the curricular guidance available for ICSS research and compares it to industry requirements to identify gaps in curricular guidance. Specifically, this paper looks at the three leading guiding documents, the NICE Cybersecurity Workforce Framework, the Joint Task Force on Cybersecurity Education curriculum guidance, and the NSA CAE knowledge units. These are then compared to requirements identified from ICSS related job postings. We found that the primary cybersecurity curriculum guidance documents do not sufficiently address industry requirements for ICSS.

Keywords—Industrial Cybersecurity, Industrial Control Systems, Curriculum Guidance, Workforce Development

I. Introduction

A. Importance of Industrial Cybersecurity (ICSS)

Computerized systems increasingly influence and control the physical world in which humanity resides. While this confluence may seem natural to those who, in roughly a decade, have become accustomed to unlocking their cars from key fobs and answering their door from their cell phone, the systems that control the electric grid, gas pipelines, and manufacturing facilities, were conceived under different circumstances -- literally separated from cybersecurity by decades.

In the early 2000s cybersecurity enthusiasts began to investigate industrial environments and PLCs. The evolution of the integration of cybersecurity and operational technology can be demonstrated in various ways. One of these is by tracking the prevalence of ICSS presentations at security conferences. The first publicly-identifiable "hacker" presentation on industrial control systems (ICS) occurred in 2003 at the Brumcon conference in Birmingham, England [1]. It was entitled, "How Safe is Glass of Water?" By 2019 numerous conferences around the world had come to specialize in industrial cybersecurity. These include, SCADA Security Scientific Symposium (S4 [2]), ICS Cyber Security Conference [3], Stockholm International Summit on Cyber Security in SCADA and Industrial Control Systems [4]). Other conferences such as BlackHat, Defcon, and PacSec frequently cover the topic from a variety of perspectives. Some of the most significant presentations, such as those by Larsen [5] and Krotofil [6], addressed how adversaries might plan to cause specific types of physical damage via cyber-attack.

A second way to track the evolution of ICSS is with vulnerability disclosures. In 2004, at a North Atlantic Treaty Organization (NATO) conference, a pair of professors from the University of Missouri - Rolla, provided the first public disclosure of a PLC vulnerability [7]. Since then, researchers have disclosed over 1,500 vulnerabilities affecting industrial environments, including PLCs, HMIs, industrial network switches, and variable frequency drives (VFDs) [8]. Among the most concerning vulnerabilities are that the most commonly deployed industrial protocols such as Modbus and Common Industrial Protocol (also known as Ethernet/IP) do not support authentication. This means that any device on the network can communicate with a PLC allowing it to manipulate the way the process operates [9-10].

A third marker of the evolution of ICSS is by tracking the attacks affecting industrial environments. In 2009, Stuxnet became the first attested attack to intentionally cause physical consequence by manipulating an industrial environment. This worm targeted centrifuges at Iran's Natanz uranium enrichment facility [11]. Nearly six years later, in 2015, the world experienced its first confirmed power outage due to cyber-attack. Attackers infected dispatcher workstations, which they then used to disconnect electricity service in Western Ukraine [12]. Then, in 2017, malware targeting a safety system in a Saudi Arabian oil refinery shut down the facility [13]. In addition, numerous security incidents have affected ICS without explicitly targeting them. These include the Wannacry ransomware, which halted manufacturing at a Honda plant in June 2017 [14], and the NotPetya ransomware, which stopped pharmaceutical production at a Merck facility the same month [15]. In May 2021 Colonial Pipeline chose to shut down its refined products pipeline in

the Northeastern United States due to a ransomware incident [16].

B. Research Aim

Our hypothesis is that existing cybersecurity curricular guidance is inadequate to address the significant needs of industrial environments. The intent of this paper is to present the results of our exploratory research. We write to a primary audience of cybersecurity educators. These individuals are well-developed in the consensus fundamentals of cybersecurity, and have designed and delivered a variety of courses on topics within the accepted body of knowledge. We believe this audience is familiar with high profile events in industrial cybersecurity such as Stuxnet, the Ukraine power outages of 2015 and 2016, and the 2021 Colonial Pipeline ransomware. The paper seeks to move beyond general observations about weaknesses in technological and procedural countermeasures in ICS, and instead, look at the broad challenge of intentionally producing professionals with the requisite competencies to enter not just the field of cybersecurity, or just the field of industrial automation, but the field of industrial cybersecurity.

C. Definitions

The first order is to ensure a common understanding of terminology as we employ it in this paper.

Industrial automation is the engineering field that deals with the creation and application of technologies that perform industrial processes with minimal optimal levels of human oversight and intervention (adapted from [17]).

Industrial processes involve the use of machinery and equipment in a series of steps that create physical goods, usually in bulk quantities. Examples include, but are not limited to control of motors, temperatures, pressures, levels, and flows (adapted from [18]).

Operational technology (OT) encompasses the communications and control systems used to automate, manipulate, and acquire information about industrial processes. The term is generally used to contrast with information technology (IT), which deals with data rather than industrial processes. It is an umbrella term used for various technologies that support "operations," such as SCADA Energy Management System. This term can be more inclusive than industrial control systems (ICS) control systems and can include market systems that interface directly through technology with operational assets (adapted from [19].

Information technology (IT) encompasses the computers, networking equipment, and software used to control data and provide information in support of decision making (adapted from [20]).

Industrial control system (ICS) refers to the equipment that enables industrial automation, such as, but not limited to programmable controllers, sensors, actuators, human machine interfaces, SCADA servers, and engineering laptops. The term differs only slightly from OT in that OT incorporates a larger focus on networking technologies (adapted from [21]).

Industrial cybersecurity is the term-of-art we prefer to describe efforts to ensure the safety, reliability, controllability, and functionality of industrial control systems and operational technology in the face of vulnerabilities in and threats to computerized systems and networks.

Content standard/guidance is a deliberate effort to describe what topics education and training offerings should include. This is distinct from program standard/guidance which describes how a program of study should be structured.

II. Existing Cybersecurity Education Frameworks

As a point of departure for our exploration, we identified three leading efforts where cybersecurity educators might turn to find content guidance relative to cybersecurity in ICS and OT: CSEC 17, NICE framework, and the NSA CAE knowledge units. We briefly examine each of these in turn.

A. CSEC 2017

The Joint Task Force on Cybersecurity Education is composed of notable academic organizations: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information, Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). Each of these academic and professional organizations seeks to further the state of science for computer-based fields, and are the publication and presentation outlets for thousands of scholars around the globe. In 2017, the Joint Task Force published its landmark report "Cybersecurity Curricula 2017", which sought to define and formalize "cybersecurity" as its own academic discipline [22]. The Joint Task force went to significant effort to involve interested individuals from around the world in workshops and online surveys. The document is remarkable in its description of the effort, and its provision of more than 300 names of individuals who participated in its creation. The report lists eight knowledge areas, each composed of knowledge units, essentials, and learning outcomes, which it intends to collectively "represent the full body of knowledge within the field of cybersecurity".

With reference to industrial cybersecurity the CSEC 2017 is fairly brief in its treatment.

- The term "industrial control systems", appears as a Topic under the Knowledge Area "System Security". The Description / Curricular Guidance field for this topic simply states "This Topic includes SCADA".
- The term "cyber-physical system administration" appears as a topic under the Knowledge Area "Organizational Security". The Description / Curricular Guidance field for this topic defines cyber-physical systems and gives examples of what might be included in that topic.

We can see that the authors and contributors to this effort were inconsistent about what terminology to use, and the area into which the concepts best fit. In addition, they provided limited content guidance on the topic.

B. NIST NICE Framework

The National Initiative for Cybersecurity Education (NICE) Workforce Framework is an effort led by the U.S. National Institute of Standards and Technology (NIST) to categorize and describe cybersecurity job functions [23]. It was first published in 2012 with the latest revision released in 2020. It is intended to provide a description of the knowledge, skills, and abilities needed to perform cybersecurity work.

A review of the Framework shows little attention to ICS – as the term does not appear within the document. The term "SCADA", which stands for supervisory control and data acquisition – a particular application of industrial control – is used three times. Of the occurrences, two are in parenthetical references, and the third is a general reference:

- Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access
- Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)
- Knowledge of general Supervisory control and data acquisition (SCADA) system components

The Framework maps these statements to the Specialist, Target Developer, and Threat/Warning Analyst work roles. Interestingly, none of these roles correspond to individuals assigned to actually protect or defend operational ICS that ultimately provide critical services such as electricity or drinking water.

C. NSA CAE Knowledge Units

In 2014, the National Security Agency adopted a "knowledge units" approach for post-secondary schools in the United States to demonstrate their compliance with its content standards [24]. Under this shift, the NSA created an optional Knowledge Unit for Industrial Control Systems (ICS), with the following intent statement:

"The intent of the Industrial Control Systems Knowledge Unit is to provide students with an understanding of the basics of industrial control systems, where they are likely to be found, and vulnerabilities they are likely to have."

The statement of intent seems to target a student whose primary role will not deal with ICS – it provides basics and focuses on the "likely." The knowledge unit includes five outcomes:

- Describe the use and application of PLCs in automation.
- Describe the components and applications of industrial control systems.
- Explain various control schemes and their differences
- Demonstrate the ability to understand, evaluate and implement security functionality across an industrial network.
- Understand and compare the basics of the most used protocols.

Four of these five outcomes seem reasonable for a student who only needs peripheral awareness of ICS – they lack specificity and do not address the differences associated with securing OT vs IT environments. Based on the statement of intent, one would expect to see an outcome dealing with industries and processes which employ ICS, but such an outcome is not provided. Objective 4 is among the most complex and demanding of all objectives contained within the 2020 knowledge units: it requires demonstration of understanding, evaluation, and implementation of security across a contextual space to which most universities have limited access; it seems to surpass the scope of the statement of intent, and appears inconsistent with the nature of the other objectives within the same knowledge unit.

The KU includes a list of nine topics:

- SCADA Firewalls
- Hardware Components
- Programmable Logic Controllers (PLCs)
- Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL)
- Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25)
- Types of ICSs (e.g., power distribution systems, manufacturing)
- Models of ICS systems (time driven vs. event driven)
- Common Vulnerabilities in Critical Infrastructure Systems
- Ladder Logic

While these topics do not seem unreasonable, they leave questions about why they were chosen and how they are organized. For example: Why is the first topic SCADA firewalls? Are these useful than non-SCADA firewalls? To what does "hardware components" refer? Why does the protocol list not include HART or EtherNet/IP? Doesn't "Critical Infrastructure Systems" merit its own entry? Is ladder logic (included) a higher priority than function block logic (not included)? In addition to a more-intuitive structure, it would be reasonable to include ICS-oriented defensive techniques, as well as specific ICS-related security guidance and regulatory requirements among the topics.

III. METHOD

This research attempts to define a set of knowledge, skills, and abilities required for ICSS from an industry perspective. We therefore have three research questions: 1) What are some of the job titles related to industrial cybersecurity? 2) What are the knowledge and skills required for ICSS? 3) Do the NICE Framework, the CSEC 2017 and the NSA CAE KUs adequately address ICSS requirements?

Noting that the intended end of curricular guidance is often the creation of students prepared to enter the workforce, the exploratory approach chosen was to examine ICS-related cybersecurity job postings. From these, job roles and associated knowledge items were extracted using content analysis. A selection of the five most widely used job boards in technology was used as the sampling frame. Searches on various job boards included such keywords as "Operational Technology (OT) security", "Industrial Control Systems cybersecurity", "SCADA Security". Only jobs posted within the last six months were included to ensure that the requirements were up to date. All duplicate posts were removed from the sample. This resulted in a sampling of 27 job postings with 10 unique job titles (see Table 1). Job postings found were combined into a single work role if their tasks, skills, and responsibilities seemed to overlap. A coding scheme was developed to analyze the job postings. The job requirements were coded as *Knowledge, Skills, and Tasks*. The statements were then further coded into specific knowledge/task/skills statements (see Table 2).

It is important to note that this exploratory method assumes that the market accurately understands and expresses its needs. It also assumes that the individuals comparing and compiling the list can recognize key concepts and terminology and appropriately group them together. Interestingly, this method does not appear to have been directly used in aforementioned curricular guidance efforts from the Joint Task Force, NIST, or the NSA.

IV. RESULTS AND DISCUSSION

The first research question identified job roles related to ICSS. Of the 495 cybersecurity job postings sampled 27 were unique to ICSS and 10 unique job titles emerged.

TABLE I. JOB DESCRIPTIONS IN ICSS

Title	Description
Manager, Cybersecurity (OT/ICS)	Directs and oversees the work of industrial cybersecurity for all phases of the plant, product and system life cycles. The manager interfaces continuously with operations, IT, and cybersecurity personnel.
Industrial Cybersecurity Engineer (OT/ICS)	Works within the engineering department to design and create systems, processes and procedures that maintain the safety, reliability, controllability, and security of industrial systems in the face of intentional and incidental cyber events. Interfaces with Chief Information Security Officer, plant managers and industrial cybersecurity technicians
Industrial Cyber Security Technician	Works among plant operations personnel to assure safety, reliability, functionality and cybersecurity of industrial control systems during installation, monitoring, troubleshooting, and restoration of industrial process operations.
Industrial Cybersecurity Analyst	Works among enterprise cybersecurity personnel to contextualize and synthesize threats, vulnerabilities and consequences relevant to industrial environments to provide strategic, tactical, and operational decision makers with perspective, options, and recommendations.
OT/ICS Cybersecurity Specialist	Works among enterprise cybersecurity personnel to contextualize and synthesize threats, vulnerabilities and consequences relevant to industrial environments to provide strategic, tactical, and operational decision makers with perspective, options, and recommendations.
Cybersecurity OT/ICS Senior Associate	Work with clients to design and review operations technology and ensure appropriate security controls.
Network Security Engineer (OT/ICS)	Secure and manage OT environments and network security services.
SCADA/ICS Cybersecurity Solutions Architect	Development of secure architecture and design patterns for industrial control systems, SCADA, and other grid/operational technology environments.
Industrial Cybersecurity Researcher	Works to increase detailed knowledge about ways an industrial cyber-physical system may be compromised, and advance novel ways they may be protected.
ICS/OT Consultant	Helps clients assess and strengthen ICS/OT security capability and work to continually improve assessment methodologies

The second research question concerns the skills and knowledge required for ICSS. A content analysis revealed 25 knowledge statements, 16 task statements, 6 skills statements, and a selection of certifications.

TABLE II. KNOWLEDGE, SKILLS, TASKS FOR ICSS

K1	Knowledge of IT/OT network communication protocols, e.g. TCP/IP, UDP, DNP3, Modbus, IEC 61850, OPC, OPC UA, HART, Foundation Fieldbus, PROFINET	T1	Project management including prioritizing efforts, understanding requirements per effort, obtaining and managing budget, building the team, and running and improving the program

K2	Knowledge of PLC, RTU, DCS, SIS, MES, Historians, HMI, SCADA systems	T2	Maintain ICS device asset inventory
K3	Knowledge of Windows/UNIX platforms	T3	Review architecture of ICS networks
K4	Knowledge in leading end-to-end solutions – strategy, design, development, testing, training, implementation	T4	Update ICS software and firmware
K5	Knowledge in deploying/supporting a variety of cybersecurity practices and technologies, I.e. risk assessments, compliance assessments, vulnerability assessments, antivirus software, firewalls, IDS/IPS, deep packet inspection, SIEM, centralized alert logging/monitoring in ICS environments	T5	Maintain backups of control software
K6	Knowledge in maintaining and managing compliance requirements, global and regional OT policies, standards, and procedures e.g. NIST SP 800-82, IEC 62443, NERC CIP	T6	Maintain awareness of evolving threat environments
K7	Knowledge of applications development, script writing, computer code, virtual machines	T7	Securely implement process control equipment
K8	Knowledge of ethical and social issues and responsibilities in ICS	T8	Implement emerging developments in ICS
K9	Knowledge of OT terminology and culture	T9	Dissect analytical requests, collect and synthesize information
K10	Knowledge of network security standards	T10	Analyze threats, vulnerabilities to ICS systems
K11	Knowledge in security control frameworks such as IEC-62443, IACS Cybersecurity standard, NIST CSF, 20 Critical Controls, or ISO 27002	T11	Propose and design analytical products
K12	Knowledge in troubleshooting system integration issues	T12	Maintain a library of standardized security and privacy responses to common inquiries/audits
K13	Knowledge in developing/implementing a disaster recovery plan	T13	Maintain current knowledge of security and privacy regulations
K14	Knowledge in collecting, analyzing, and escalation of security events and knowing what response, if any, is needed (e.g., when critical systems, sensitive data/information is compromised)	T14	Ensure compliance with corporate security standards
K15	Knowledge of policies, processes, and controls standardized by cybersecurity regulatory institutions and frameworks, such as the Center for Internet Security (CIS), NIST, security frameworks such as NIST 800-53 NIST 800-171, NIST 800-82, ISO 2700x, IEC/ISA 62443	T15	Build and manage client relationships
K16	Knowledge in cyber vulnerability assessments, such as pen-testing, real activations, or tabletop IR plan exercises	T16	Design and implement enterprise networks
K17	Knowledge with Windows, active directory, group policy, DNS, encryption, patch management, anti-virus software, system configuration management	S1	Organizational and project management skills.
K18	Knowledge in networking constructs, such as LAN, WAN, VPN, routers, firewalls, servers, IDS/IPS, SIEM, DLP, TCP/IP	S2	Technical writing; writing progress reports, final deliverable reports, etc, communication skills (written, verbal, presentation, facilitation)
K19	Knowledge in developing policy and policy recommendations for networks of IT/OT and systems cyber security and compliance controls	S3	Install, manage, troubleshoot a computer network, apply telecom principles to design and configure a network
K20	Knowledge in types of security architectures and cloud virtualizations	S4	Ability to function in teams
K21	Knowledge of requirements for human safety and the availability/security of operating environment	S5	Problem solving
K22	Knowledge of cloud based security	S6	System administration in an ICS environment
K23	Knowledge of identity and access management		
K24	Knowledge of applied cryptography		
K25	Knowledge of programming languages		

The third research question asks whether the NICE Framework, the CSEC 2017 and the NSA CAE KUs adequately address ICSS requirements. The three curriculum guidance documents analyzed provide very different levels of treatment of ICS and industrial cybersecurity. None provide the level or breadth of detail demonstrated by the industrial requirements though there is minor overlap. Based on the analysis provided above, it is our conclusion that industrial automation and control systems are not adequately represented in leading cybersecurity content guidance. We propose three interrelated reasons for this:

- Industrial automation has been a separate field of endeavor and study from computer science and information systems.
- Individuals who provided content guidance for these efforts were generally not experts in ICS or industrial cybersecurity.
- Core cybersecurity terminology and definitions apply to both types of systems, but the way they should be applied can differ greatly.

V. Conclusion

This paper has shown that current leading efforts to guide curriculum content for industrial cybersecurity exhibit significant gaps. In consideration of these gaps and the growing importance of ICSS we propose the establishment of a set of standards that can serve as curriculum guidance for ICSS or an addendum to the NICE Framework, the CSEC 2017 and the NSA CAE KUs to better address the lack.

Reference

[1] Barnes, A. (2003). 'We have your water supply, and printers' – Brumcon report. https://www.theregister.co.uk/2003/10/20/we_have_your_water_supply/, accessed February 2021.

[2] S4 Events (n.d.). https://s4xevents.com/, accessed February 2021.

[3] ICS Cybersecurity Conference (n.d.) https://www.icscybersecurityconference.com/

[4] Stockholm international summit on Cyber Security in SCADA and Industrial Control Systems (n.d.). https://cs3sthlm.se/, accessed February 2021.

[5] Larsen, J. (2015). Physical Damage 101: Bread and Butter Attacks. https://www.blackhat.com/docs/us-15/materials/us-15-Larsen-Remote-Physical-Damage-101-Bread-And-Butter-Attacks.pdf, accessed February 2021

[6] Krotofil, M. (2015). Damn Vulnerable Chemical Processes. https://www.slideshare.net/phdays/damn-vulnerable-chemical-process, accessed February 2021.

[7] Miller, A., Erickson, K. (2004). Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity. http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.214.6366, accessed February 2021.

[8] McBride, S. (2016). Overload: Critical Lessons from 15 Years of ICS Vulnerabilities. https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html, accessed February 2021.

[9] Batke, B., Wiberg, J., Dubé, D. (2015). CIP Security Phase 1 Secure Transport for EtherNet/IP. https://docplayer.net/11561418-Cip-security-phase-1-secure-transport-for-ethernet-ip.html, accessed February 2021

[10] Benbenishti, L. (2017). SCADA MODBUS Protocol Vulnerabilities. https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/, accessed February 2021, accessed February 2021.

[11] Langner, R. (2013). To Kill a Centrifuge. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, accessed February 2021.

[12] Whitehead, D., Owens, K. Gammel, D., and Smith J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, pp. 1-8. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8090056&isnumber=8089819, accessed February 2021.

[13] Greenberg, A. (2019). Sandworm. Anchor Books. ISBN 9780525564638

[14] Tajitsu, N., (2017). Honda halts Japan car plant after WannaCry virus hits computer network. https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI, accessed February 2021.

[15] O'Neill, P. (2017). NotPetya ransomware cost Merck more than $310 million. https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/, accessed February 2021.

[16] Morrison, S, "How a major oil pipeline got held for ransom" Vox, 2021. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

[17] International Society of Automation (n.d). "What is automation?" https://www.isa.org/about-isa/what-is-automation

[18] National ResearchCouncil (1995). Unit Manufacturing Processes: Issues and Opportunities in Research. The National Academies Press. Washington, DC. https://doi.org/10.17226/4827.

[19] O'Neil, L., Assante, M., Tobey, D., Conway, T., Vanderhorts, T., Januszewski, J., Leo, R., Perman, K. (2013). Developing Secure Power Systems Professional Competence: Alignment and Gaps in Development Programs for Phase 2 of the Secure Power Systems Professional project. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-22653.pdf, accessed February 2021.

[20] National Institute of Standards and Technology Computer Security Resource Center Glossary entry for "Information Technology" https://csrc.nist.gov/glossary/term/information_technology

[21] National Institute of Standards and Technology, Computer Security Resource Center Glossary entry for "ICS" https://csrc.nist.gov/glossary/term/ICS

[22] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E., Kaza, S., Levy, Y., Parrish, A. (2017). Cybersecurity Curricula 2017:Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf, accessed February 2021.

[23] Newhouse W., Keith S., Scribner B. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology, Washington, DC. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, accessed February 2020.

[24] Conklin W, Cline R, Roosa T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors, 47th Hawaii International Conference on System Sciences, Waikoloa, HI, pp. 2006-2014.