Creating a Concept Map for ICS Security – A Delphi Study

1st Ida Ngambeki
Department of Computer and Information Technology
Purdue University
West Lafayette, USA
ingambek@purdue.edu

2nd Eugene Spafford
Department of Computer Science
Purdue University
West Lafayette, USA
spaf@purdue.edu

3rd Subia Ansari
Deparment of Computer and Information Technology
Purdue University
West Lafayette, USA
ansari0@purdue.edu

4th Isslam Alhasan
Deparment of Computer and Information Technology
Purdue University
West Lafayette, USA
ialhasan@purdue.edu

5th Marlo Basil-Camino
Deparment of Computer and Information Technology
Purdue University
West Lafayette, USA
mcamino@purdue.edu

6th Douglas Rapp
Department of Computer Science
Purdue University
West Lafayette, USA
rapp1@purdue.edu

***Abstract*— This Research Full Paper presents the results of a Delphi study. Industrial Control Systems (ICS) is a term used to describe highly integrated and mutually dependent systems made up of a complex network of hundreds of thousands of interconnected control systems. These systems usually incorporate different mass production and distribution elements to accomplish an industrial purpose. These highly integrated and mutually dependent systems have been deployed to manage, monitor, and control industrial infrastructure to provide essential services, such as electricity, energy, chemical, food and beverage, water, gas, oil, and traffic control systems. As these internet-connected systems and technologies continue to grow globally, the risks and threats of ICS cyberattacks' are rapidly increasing. If left susceptible to cyberattacks, any significant stoppage or interruption can cause real-world damages, considerable loss, and undesirable events. ICS security, the process of keeping these systems secure, is becoming a challenging priority for industrial organizations. A recent study conducted by the Center for Strategic International Studies (CSIS) showed that across eight countries of I.T. decision-makers, 82% of employers reported a cybersecurity skills shortage, and 71% believe this talent gap poses direct and observable harm to their organization. A report by (ISC)2 found that there is a vast ICS cybersecurity workforce gap, and the cybersecurity workforce needs to grow 89% to meet industry needs in the United States and 145% to close the skills gap worldwide. The major factor driving the market is the increasing number of complex cyber-attacks on ICS systems, requiring a high demand for trained and skilled professionals in the ICS cybersecurity field. In 2016, a CSIS survey of IT employers found that only 23% believed education curriculums were fully training students to join the cybersecurity industry. Likewise, in 2018, ISACA found that 61% of institutes believe that fewer than half of those filling cybersecurity positions were qualified for the job. The current education curriculum lacks essential cybersecurity programs and degrees. It does not provide a strong foundation for building the role-specific knowledge necessary to meet the needs of the cybersecurity workforce. This deficiency needs to be urgently addressed through the creation of multiple, flexible programs in industrial control systems security. One of the first steps in this development is to identify the most critical knowledge, skills, and abilities necessary to become proficient in ICS security. This paper reports on a Delphi study designed to identify these foundational concepts and create a concept map based on the findings. This study used the Delphi method to develop the concept map. A selection of 25 experts in ICS security from academia, industry, and government were contacted and asked to outline a list of core knowledge areas. The researchers developed a summary of the experts' opinions. Two more rounds of input and feedback were solicited from the panel of experts. This paper describes the process and the resulting concept map describing the landscape of ICS cybersecurity.**

Keywords—ICS Security, Delphi Study, Concept Map

I. Introduction

The security of Industrial Control Systems (ICS) is becoming a growing concern as these systems are now connected to external networks and the internet, which increases system vulnerability and imposes a direct threat to our manufacturing, energy and utility, healthcare, and transportation industries. The increasing volume of cyber threats has completely dominated ICS and is why building a secure and dependable defense mechanism against all types of cybersecurity threats is imperative. Fortinet has released a report and indicated that 9 out of 10 organizations surveyed had at least one breach in the past year, with half reporting that they had more than 3 to 10 breaches [1]. ICS targeted cyberattacks are on

the rise and are considered very costly and affect organizations' productivity, property, and revenue; thus should be regarded as a high priority. These attacks can also threaten national economies and security, for example the 2021 ransomware attack on the Colonial Pipeline caused national gas shortages. ICS security solutions enable organizations to ensure system continuity and protection from cybercrime threats and malicious threat actors to combat this ongoing situation. A recent study conducted by the Center for Strategic International Studies (CSIS) indicated that 82% of employers in various companies reported a cybersecurity skills shortage, and 71% believe that this talent gap poses direct and observable harm to their organization [2].The primary factor driving the market is the growing number of constantly evolving complex cyber-attacks on ICS systems, thus requiring a high demand for trained and skilled professionals in the ICS cybersecurity field. Kaspersky conducted a survey and found that most companies (77%) considered ICS/OT cybersecurity a major priority and a high level of importance, a percentage that is about one-third greater than that in the previous year [3]. These numbers emphasize the important need for awareness, comprehensive education, improved cybersecurity curriculum in educational institutions, and the training of the ICS workforce to better strengthen our ICS security strategies.

$(ISC)^2$ released a report and indicated that there is a huge ICS cybersecurity workforce gap, meaning the difference between the number of trained professionals and the available capacity. To meet industry needs and close the skills gap, the cybersecurity workforce needs to grow 89% in the United States and 145% worldwide [4]. To better secure and protect against the rising numbers of cybersecurity threats, many industrial organizations face challenges training and preparing their existing employees and finding individuals with the skills necessary to perform the job. There is a worldwide cybersecurity skills shortage, and as the workforce gap continues to grow, it is putting companies at higher risk. A top factor behind this growing skills gap is the lack of a well-defined career path for becoming a cybersecurity professional [5]. Also, most job positions require hands-on experience, something many cybersecurity talents do not have. Educational institutions should consider adopting a curriculum that encompasses hands-on experience to gain the necessary knowledge to succeed in the industry and fill this severe shortage. Typical cybersecurity job posts do not require a formal cybersecurity education path; in fact, most require experience and a diverse set of skills such as “ability to learn new technologies,” “quick learner,” and “team player.” Additionally, job postings usually state the degree requirement is “a degree in a related field.” Plain and simple: the industry did not create a clear, consistent career path for future cybersecurity professionals [6]. Educational institutions, starting from elementary, should be encouraged to develop interests in STEM topics. These students should be exposed to cybersecurity topics to bring in those interested students and offer guidance, recommendations, funding, and guaranteed admissions at higher educational universities. Furthermore, companies need to invest in their employees and upskill their talents. Providing additional training, suggesting related courses, and pushing for certifications are a few strategies companies and businesses can focus on to reprioritize their cybersecurity needs to help further close this gap. Also, changing their approach to creating a job role encourages those with the necessary knowledge to apply for cybersecurity positions. Companies have to consider that most candidates do not have the necessary experience requirements and are most likely starting at the beginning and have a mountain to climb. Those students who do not yet check all of the boxes of a cybersecurity job posting may become the ideal employee who fits the role with gained experience. Focusing on enhancing our cybersecurity educational curriculum, encouraging employers to train their staff, and changing our approach in job descriptions can help close the cybersecurity talent pipeline.

Identify applicable funding agency here. If none, delete this text box.

II. Literature Review

A. Standards in Information Security

When it comes to information security, there is certainly no lack of professional standards and frameworks. A quick internet search will result in a list of numerous frameworks for almost any industry. With the rise of advanced manufacturing, the industrial internet of things (IIoT), and concern for critical infrastructure, several security standards for industrial control systems (ICS) have been developed with the potential for more on the horizon as shown in Fig.1. With all of these standards, it is apparent that a considerable amount of time, effort, and thought has gone into defining those things that we must do to address information security.

But now the question has become how do we identify and create the skills required to comply with the multitude of information security standards that currently exist? So far, the effort in this area has resulted in only one major framework; the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. And while the value of the NICE Framework should not be understated, there are only three references to ICS (SCADA specifically) in the entire framework [7].

B. ICS Security Education Landscape

The need for skilled practitioners in ICS security is clearly indicated by the proliferation of standards however there is currently little data that quantitatively defines the skill deficit. However, what is known is that recent studies by $(ISC)^2$ indicate that the overall cybersecurity workforce needs to grow 89% in orders to effectively defend the critical assets of existing organizations [8].

Information Security Frameworks		ICS Inclusive Frameworks
ISO IEC 27001/ISO 270021	FedRAMP	
NIST Cybersecurity Framework	HIPAA	
IASME Governance	GDPR	IIC PUB G4 V1
SOC 2	FISMA	CPNI
CIS	NY DFS	NERC CIP
NIST 800-53	NERC CIP	ANSI
COBIT	SCAP	NIST 800-181
COSO	ANSI	
TC CYBER	NIST SP 800-12	
HITRUST CSF	NIST SP 800-14	
CISQ	NIST SP 800-26	

Fig. 1. Common Information Security Standards.

Despite the lack of a comprehensive skills framework for ICS security and because of industry demand for these skills, education providers have clearly recognized the need and reacted accordingly. ICS security education providers are diverse and have emerged in some non-traditional places. However, they are very few in number. Our search could only identify those listed below. They are broken down into five main categories with corresponding examples below:

- External corporate education providers e.g. SANS, Verve, Tonex
- Certifying organizations e.g. ISC2, ISA, GIAC (note that GIAC is the certifying arm of SANS)
- Higher Education e.g. Dunwoody College of Technology, Whatcom Community College, Wake Technical Community College, Clark State, Wichita State University, Wilmington University, Savannah Tech, Louisiana Tech, Millersville University, Mid-State Tech, Bossier Parish Community College, ITI Technical college, University of Wisconsin Plattsville, Northern Iowa Community College, Lee College
- Industry e.g. Rockwell Automation, Schneider, Honeywell (limited), Yokogawa
- Government e.g. Sandia National Laboratories, Idaho National Labs, Cybersecurity Infrastructure Security Agency (DHS)

In addition to identifying who is providing education in ICS security, we can furthermore identify the type of education being provided. These are broken down into:

- ICS Security Corporate Education – ICS security corporate education aims to develop the competency and capability of an individual employee with the added value of also increasing the capability of the company.
- ICS Security Certifications – ICS security certifications are more workforce oriented with the intent to validate a set of skills of an employee.
- ICS Security Degrees – ICS security degrees prepare an individual to enter the ICS Security career field by giving them a broad foundational knowledge of the subject.

C. Areas of Research

Research within the subject of ICS security education is limited. In reviewing the literature on this subject, two research themes or concentration areas were revealed. The first concentrated area of research deals with ICS security teaching methodology. Researchers in this area explore the advantages and effectiveness of educating using test beds and labs [9, 10]. Other research in this concentration is focused on educating through scenarios [11], simulations [12], and projects [13]. Another significant area of current research in ICS security is in the application of gamification and gamification methodology in education [14, 15].

The second theme is more closely related to this paper in that it deals with educational subjects, subject frameworks, and workforce development in ICS security education applications. Research focuses on ICS Security education from a curriculum and instruction [16] and the incorporation of ICS security education into existing education tracks [17]. Additionally, within this research theme is an emerging body of work on establishing an ICS security education standard or framework within the United States [18] and internationally [19]. However, none of these has established a common body of research that defines ICS security. We seek to address that through this study.

III. Methodology

The Delphi technique seeks to obtain consensus on the opinions of experts, termed panel members, through a series of structured questionnaires. As part of the process, the responses from each round are fed back in summarized form to the participants who are then given an opportunity to respond again to the emerging data. The Delphi is therefore an iterative multi-stage process designed to combine opinion into group consensus. In this paper, the researchers report on the first round of a three round Delphi study with 25 participants.

A. Target Population and Sampling

The target population of this study was the existing community of practice in Industrial Cyber Security, who were recruited via email. The participants' emails were obtained via snowball sampling, through an existing ICS community of practice listserv, of which the researchers were members, and a recruitment email was sent out to the listserv. The people sending the email did not have any authority over the individuals that were recruited; the people completing the study were voluntary members of a community of practice in that, they were professionals who volunteered their time because of their interest in the topic. The listserv was available to members of the community of practice and the research team, the research team sent the emails.

B. Data Collection

Prior to creating the initial content mapping for education in Industrial Control Systems, an understanding of the current state of ICS education across the country was needed. By using search engines and keywords (e.g. “industrial control system majors”, “SCADA security certification”, “Operational Technology Security education”, etc.), twenty-seven certifications, modules, and college-sponsored programs were identified as either fully

specializing or integrating OT/ICS/SCADA security into their curriculum. As mentioned prior, the number of resources dedicated to educating workers in OT/ICS/SCADA security is limited, and this is evident when benchmarking the current education programs that exist. A minority of the programs found fully specialized in OT/ICS/SCADA security, and the majority of them had one-three classes specializing in OT/ICS/SCAFA security in part of a broader automation, engineering, or cybersecurity program. In addition to researching current academic programs, job postings on Indeed and LinkedIn were analyzed in order to determine additional skillsets that are required for industry work for OT/ICS/SCADA security that were not previously covered in the various program descriptions found. With both the academic program resources and job postings discovered, a rough outline of the various skillsets required for ICS security was developed. These were used to create a draft concept map. This was reviewed by two sets of experts in academia and government. This map was then disseminated to the Delphi panel.

The participants were sent a recruitment email for the Delphi study, which contained a link to an initial draft of a concept map diagram created by the research team. This link led the participants to a web-page consisting of the concept map, which could be edited by the participants online anonymously without logging in. The participants were asked to provide feedback on the concept map diagram and modify it, if they see the need to do so. Then, participants were allowed to email their comments or diagrams, whichever they chose to do, to the research team. This feedback was analyzed by the researchers and consolidated into one final concept.

The study is expected to have three total iterations overall. The first round, on which this paper reports, consists of the research team sending an initial concept map draft for an initial round of feedback from industry professionals, through email. These professionals were to submit their feedback in the form of comments, modifications, new versions to the research team through email. The researchers also held a one-hour feedback session with the panel, during which the elements of the concept map were discussed. Based on this first round feedback, the research team created a revised version of the concept map. This study reports the results obtained from the first round of feedback.

IV. RESULTS

Based on the feedback from the panel of experts, the draft concept map was revised (Figure 2).

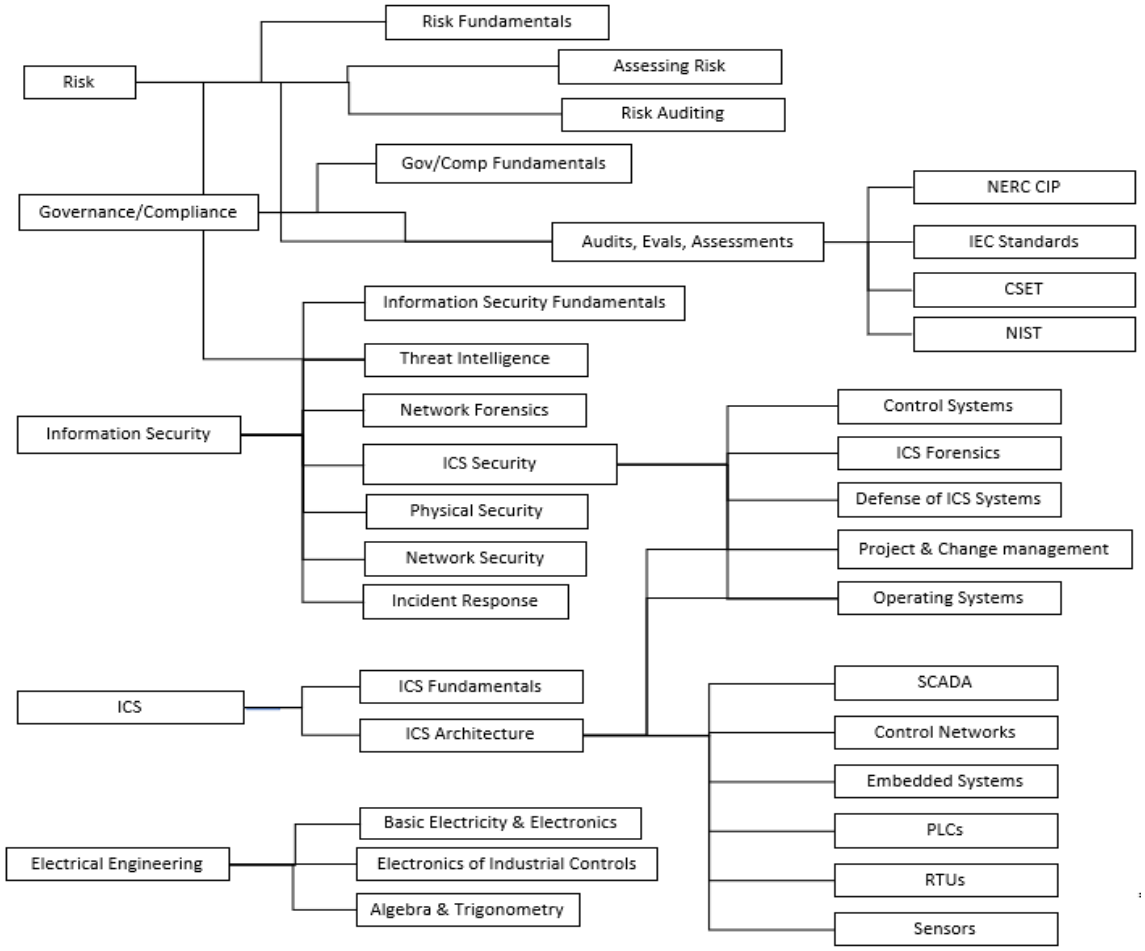

Fig. 2. ICS Security Concept Map

As indicated by the diagram, the team determined that an ICS industry professional would need knowledge in five broader topics: Risk management, governance and compliance, information security, ICS specific skills, and electrical engineering. Descriptions for the five broader areas of knowledge, as well as any specific skillsets identified are as follows:

- Risk management: The skills needed to recognize, avoid, report, and remove threats to a system, and prioritization of risks based on potential adverse impacts they may have [20].
  - *Risk fundamentals*: identifying risks as any form of threat, obstacle, or hinderance that make stop, slow, or threaten processes or information in a system [21].
  - *Assessing risk*: determining potential risks, their probability of happening, and their potential impact [21].
  - *Risk auditing*: risk examination and documentation of the effectiveness of risk responses [22].

- Governance and compliance: Understanding the formal framework that provides structure for an institution to accomplish business goals [23]. Governance and compliance also include knowledge about rules, standards, and laws, as indicated from local to international jurisdiction, and from internationally recognized institutions (e.g., NIST or IEC standards).
  - *Governance/compliance fundamentals:* understanding the standard practices that allows an organization to achieve its goals and objectives [24].
  - *Audits, evaluations, assessments:* examination and documentation of internal and external processes and measuring their effect on reaching an objective or goal.
    - *NERC CIP:* North American Electronic Reliability Corporation standards titled Critical Infrastructure Projection [25].
    - *IEC Standards:* International Electrotechnical Commission standards, e.g., IEC 38500 [26].
    - *CSET:* Cybersecurity Evaluation Tool, product of the NHS that "assists organizations in protecting their key national cyber assets" [27].
    - *NIST:* National Institution of Standards and Technology standards on Governance, Risk, and Compliance (GRC).

- Information security: includes knowledge and skills regarding the processes and tools used to protect sensitive information and systems from modification, disruption, destruction, and inspection [28].
  - *Information security fundamentals:* understanding rudimentary theoretical principles regard infosec, e.g., the CIA triad, and how it applies in a given system.
  - *Threat intelligence:* the collection, examination, and analysis of information regarding cyber threats [29].
  - *Network forensics:* collection and investigation of data in network traffic and traffic patterns captured in transit between devices [30].
  - *ICS Security:* the safekeeping and securing of an industrial control system and the components in its processes
    - *Control systems:* used to monitor industrial processes and instrumentation, getting data from remote sensors through a series of connections [31].
    - *ICS forensics:* collection and investigation of data and traffic captured in transport in between devices in an ICS setting
    - *Defense of ICS systems:* the tools and techniques used to counteract cyber threats to an ICS system
    - *Project & change management:* skills relating to managing a project team and the processes that coincide with accomplishing project goals, and the skills relating to managing change in internal or external processes.
    - *Operating systems:* familiarity with various operating systems and how to work with them in an ICS setting.
  - *Physical security:* includes physical protections and hardware that prevent cyber threats, e.g., locks, CCTV, and other physical measures restricting access.
  - *Network security:* includes security measures that prevent cyber threats in a virtual setting; includes software, network analysis tools, and other virtual security systems.
  - *Incident response:* the methodology and application of responding to any sort of cyber incident, whether it be a cyber-attack, data breach, natural disaster, etc.
- Industrial control system: specific skills include skills relating to general ICS processes. ICS is defined by NIST as a broad category of control systems that provide instrumentation and analysis used in industrial process control [32].
  - *ICS fundamentals:* understanding of rudimentary theory, principles, and practice of industrial control systems.
  - *ICS architecture:* understanding of the components and instrumentation of architecture in an ICS setting, and how proper architecture can improve the security of the system

        - *SCADA:* supervisory control and data acquisition; systems of software that control industrial processes, monitor and gather data in real time, interacts with instrumentation, and records data and events [33].
        - *Control networks:* the different application of tools and software that allow user input to monitor and adjust an ICS
        - *Embedded systems:* the individual components and instruments that perform specialized tasks in an ICS system
        - *PLC:* programmable logic controller; devices that are adapted to control industrial machinery, including robotic devices, assembly lines, etc. [34].
        - *RTU:* remote terminal unit; a device used to remotely monitor and control systems and instruments in an automated system
        - *Sensors:* the different tools and instruments that determine metrics and statuses of different components in an ICS system
- Electrical engineering: as defined by IEEE, electrical engineering encompasses the skills and application of electricity, electronics, and electromagnetism [35].
    - *Basic electricity & electronics:* understanding of fundamental electrical components, including resistors, capacitors, inductors, transformers, diodes, transistors, etc.
    - *Electronics of industrial controls:* understanding the basic electrical components and how they are applied in an industrial control system setting

Algebra & trigonometry: the universal application of the two schools of mathematics to electronics abroad

The skills learned in each of the five broader schools are not mutually exclusive and overlap of knowledge between disciplines was noted. For example, information security overlaps many skills with risk, governance and compliance, and ICS disciplines.

V. Discussion

This concept map represents the first-round response from a panel of experts. The objective of this study was to build and describe a consensus around the concept areas in ICS security. This is necessary because although ICS security is a longstanding field, because these systems have been siloed and isolated, the field has been siloed and isolated. The potential for networking introduced by developing technologies and needs has produced a requirement for a more consolidated approach to the field. This consensus is expected to form the basis of other efforts. For example new programs in ICS security can use this mapping to build their offerings; existing programs could use this concept map to assess the depth and breadth of their coverage; this map could be used to develop a common set of outcome expectations for programs in ICS security; and the map can form the basis of a common foundation for paradigm and theory-building in ICS security education.

By necessity decisions needed to be made about the nature and structure of the map. Since the primary goal of the community of practice was to contribute to the development of educational standards, the map took on a form that researchers felt would be most useful for those attempting to build programs in ICS security. Other approaches that focus on a practitioner perspective, a compliance perspective, or a knowledge base perspective are of course possible and provide their own forms of utility.

VI. Conlusion

This paper reports on the first round of a Delphi Study to delineate the knowledge area in ICS Security. ICS Security experts belonging to a community of practice were consulted. 25 experts from industry, academia, and government helped define the knowledge area in ICS Security and create a concept map. The concept map lays out five broad areas in ICS security viz. risk management, governance and compliance, information security, electrical engineering, and ICS specific skills.

VII. Limitations and Future work

This study only reports on the first round of a Delphi Study. Future work will include completing two more rounds. This study is also limited to experts in one country (USA) belonging to a single community of practice. The draft concept map viewed by the panel was constructed from a survey of existing ICS security programs in the USA. The researchers also did not collect any information on the specific expertise or industries represented by the panel. Future work could potentially expand both the program review and the panel beyond one country. Future work will also survey the panel for expertise to make sure that all sectors of industrial control systems are represented.

Acknowledgment

The authors would like to acknowledge the Industrial Control Systems Community of Practice for sharing their expertise on Industrial Control Systems. The authors would also like to acknowledge the Hub and Spoke Project headed by the Critical infrastructure Resilience Institute at the University of Illinois Urbana-Champaign in collaboration with Purdue University with funding from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency.

References

[1] Fortinet, Inc. “2020 State of Operational Technology and Cybersecurity Report,” 710343-0-0-EN, Jun. 2020. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf.

[2] Cybersecurity and Infrastructure Security Agency. 2016.

[3] W. Schwab and M. Poujol, "The State of Industrial Cybersecurity 2018," Kaspersky Industrial CyberSecurity, Jun. 2018. Accessed: Apr. 29, 2021. [Online]. Available: https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/

[4] (ISC)^2, "Cybersecurity Professionals Stand Up to a Pandemic," 2020. [Online]. Available: https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

[5] C. Alessandro, "Cyber Skills Gap, is it a lack of talent problem?," LinkedIn, Jan. 2021. https://www.linkedin.com/pulse/cyber-skills-gap-lack-talent-problem-alessandro-civati/ (accessed Apr. 29, 2021).

[6] P. Sue, "Cybersecurity Predictions for 2019," IT Business Edge, Jan. 2019. https://www.itbusinessedge.com/networking/cybersecurity-predictions-for-2019/ (accessed Apr. 29, 2021).

[7] National Institute of Standards and Technology Special Publication 800-181, Natl. Inst. Stand. illermo. Spec. Publ. 800-181, 144 pages (August 2017)

[8] (ISC)2 Cybersecurity Workforce Study, 2020

[9] Sauer, Felix, et al. "LICSTER -- A Low-Cost ICS Security Testbed for Education and Research." 2019, doi:10.14236/ewic/icscsr19.1.

[10] Morelli, Umberto, et al. "An Open and Flexible CyberSecurity Training Laboratory in IT/OT Infrastructures." Computer Security, Springer International Publishing, Cham, 2020, pp. 140–155. Lecture Notes in Computer Science.

[11] Francia, Guillermo. "Scenario-Based Learning Approach to Industrial Control Systems Security Training." Proceedings of the International Conference on Security and Management (SAM), 2018, pp. 111–116.

[12] Reutimann, Brandt R. Applications of Simulation in the Evaluation of SCADA and ICS Security, 2020.

[13] Nguyen, Thuy D, and Gondree, Mark A. "Teaching Industrial Control System Security Using Collaborative Projects." Security of Industrial Control Systems and Cyber Physical Systems (2016): 16-30. Web.

[14] Antonioli, Daniele, et al. "Gamifying Education and Research on ICS Security: Design, Implementation and Results of S3." 2017.

[15] Yonemura, Keiichi, et al. "Practical Security Education on Combination of OT and ICT Using Gamification Method at KOSEN." Smart Industry & Smart Education, Springer International Publishing, Cham, 2018, pp. 344–353. Lecture Notes in Networks and Systems.

[16] R T Albert. "SCADA Cybersecurity Education from a Curriculum and Instruction Perspective." Proceedings of the International Conference on Security and Management (SAM), 2014, p. 1.

[17] Alnsour, Rawan, and Hamdan, Basil. "Incorporating SCADA Cybersecurity in Undergraduate Engineering Technology & Information Technology Education." 2020 Intermountain Engineering, Technology and Computing (IETC), 2020, pp. 1–4.

[18] S. McBride and J. Slay "Towards Standards-Based Industrial Control Systems Security Education in The United States", 2020. https://industrialcyberforce.org/wp- content/uploads/2020/07/Towards-Standards-based-ICS-Security-Education-in-the-United-States.pdf.

[19] S. McBride and J. Slay "Criteria for International Industrial Cybersecurity Education and Training Standards". 2020. https://industrialcyberforce.org/wp-content/uploads/2020/07/Criteria-for-International-ICS-Security-Education-Standards.pdf

[20] C. Ericka, "Cybersecurity risk management explained." https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-risk-management-explained (accessed Apr. 30, 2021).

[21] I. Horvath, "Risk Analysis Definition - Understanding the Fundamentals of Risk Analysis," *Invensis Learning Blog*, Nov. 12, 2020. https://www.invensislearning.com/blog/risk-analysis-definition/ (accessed Apr. 30, 2021).

[22] P. Wootton, "Risk audit," *ProjectManagement*, Feb. 2020. https://www.projectmanagement.com/contentPages/wiki.cfm?ID=346698&thisPageURL=/wikis/346698/Risk-audit#_=_ (accessed Apr. 30, 2021).

[23] K. Lindoris, "What is IT governance? A formal way to align IT & business strategy," *CIO*, Jul. 2017. *https://www.cio.com/article/2438931/governanceit-governance-definition-and-solutions.html* (accessed Apr. 30, 2021).

[24] S. L. Mitchell, "GRC360: A framework to help organisations drive principled performance," *Int J Discl Gov*, vol. 4, no. 4, pp. 279–296, Nov. 2007, doi: 10.1057/palgrave.jdg.2050066.

[25] NERC, "CIP Standards," *NERC.com*. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed Apr. 30, 2021).

[26] ISO/IEC, "ISO/IEC 38500:2015 | Information technology - Governance of IT for the organization," International Standard, Feb. 2015. Accessed: Apr. 30, 2021. [Online]. Available: https://webstore.iec.ch/publication/21828.

[27] CISA Cyber-Infrastructure, "Cyber Security Evalutation Tool (CSET)," *CISA*. https://cset.inl.gov/SitePages/Home.aspx (accessed Apr. 30, 2021).

[28] CISCO, "What Is Information Security (InfoSec)?," *CISCO*. https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html (accessed Apr. 30, 2021).

[29] Intel & Analysis Working Group, "What is Cyber Threat Intelligence?," *CIS*, Oct. 26, 2015. https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/ (accessed Apr. 30, 2021).

[30] J. Mounteer, "Network Forensics 101," *NYSTEC*. https://www.nystec.com/insights/network-forensics-101/ (accessed Apr. 30, 2021).

[31] C. Brook, "What is ICS Security?," *Data Insider*. https://digitalguardian.com/blog/what-ics-security (accessed Apr. 30, 2021).

[32] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, NIST SP 800-82r1, May 2013. doi: 10.6028/NIST.SP.800-82r1.

[33] Inductive Automation, "What is SCADA?," *Inductive Automation*, Sep. 2018. https://inductiveautomation.com/resources/article/what-is-scada (accessed Apr. 30, 2021).

[34] W. Bolton, "Chapter 1 - Programmable Logic Controllers," in *Programmable Logic Controllers (Sixth Edition)*, W. Bolton, Ed. Boston: Newnes, 2015, pp. 1–22.

[35] Summer Institute, "What is Electrical Engineering Anyway?," *TryEngineering*, Jun. 2018. https://tryengineeringinstitute.ieee.org/what-is-electrical-engineering-anyway/ (accessed Apr. 30, 2021).