

Driving Factors Behind Adopting Virtual Testbeds for ICS Cybersecurity Education.

Taiwo Peter Akinremi
akinretp@mail.uc.edu
University of Cincinnati
Cincinnati, Ohio, USA

Joel Kwesi Appiah
appiahjk@mail.uc.edu
University of Cincinnati
Cincinnati, Ohio, USA

Amir Reza Asadi
asadiaa@mail.uc.edu
University of Cincinnati
Cincinnati, Ohio, USA

Opetunde Ibitoye
ibitoyoo@mail.uc.edu
University of Cincinnati
Cincinnati, Ohio, USA

Saheed Popoola
saheed.popoola@uc.edu
University of Cincinnati
Cincinnati, Ohio, USA

Abstract

The widespread adoption of industrial control systems (ICS) has created a knowledge gap and the need for a skilled ICS cybersecurity workforce to address this gap. A major challenge is the cost and resources required to train new professionals. In response, scholars have increasingly explored the use of virtual cybersecurity testbeds. However, the application of these test beds in ICS cybersecurity education remains a relatively underexplored area, despite its promising potential. This study employs a systematic literature review to identify the key factors driving the adoption of virtual cybersecurity testbeds for educational purposes. The findings indicate that the most frequently cited drivers are hands-on experience and the critical importance of ICS cybersecurity, simulation capabilities, opportunities for attack experimentation, attack automation, and ICS-specific knowledge and skills, availability of open-source and educational resources, and cost-effectiveness. Furthermore, the results reveal that virtual cybersecurity testbeds are currently used more for research than for teaching. Nonetheless, they hold significant promise for supporting learners in understanding ICS cybersecurity concepts and challenges. Finally, this study outlines the opportunities cybersecurity testbeds offer to instructors, academics, and practitioners, and highlights their potential to facilitate learning about the complexities and critical scenarios inherent in the ICS domain.

CCS Concepts

• ICS Cybersecurity, Virtual Cybersecurity Testbed;

Keywords

Industrial Control Systems, ICS Cybersecurity Education, Industrial control system, virtual testbeds, cybersecurity education

1 Introduction

The Industrial Control System (ICS) is an interconnected system that is deployed to control industrial processes in critical sectors such as defense, energy, wastewater management, agriculture, transportation, aviation, defense, agriculture, energy, healthcare, and manufacturing. This infrastructure enables predictive maintenance, real-time data monitoring, and process optimization. [36]. However, advanced cybercriminals have targeted ICS systems for various purposes such as system reconnaissance, disturbance, and disruption [22][2]. The increasing target of cyber attacks on ICS demonstrates the need for cybersecurity education in ICS that will introduce professionals, researchers, and students to ICS cybersecurity [18].

The lack of easy access to the cybersecurity educational materials of the ICS impedes how quickly individuals can be trained on the skills necessary to defend against cyber attacks that target industry control systems [18].

Industrial Control Systems (ICS) present unique educational and research challenges that significantly limit hands-on learning opportunities [17]. First, ICS implementations are owned and operated by private industrial companies that limit access to their systems due to proprietary concerns and the mission-critical nature of their operations. These systems are typically designed for specific industrial processes and objectives, making them unavailable for educational or research purposes [17]. Second, any unauthorized modifications or experimental activities on operational ICS could compromise system integrity, disrupt critical infrastructure operations, or impact public safety consequences that industrial operators cannot afford to risk [14]. Third, organizations strictly control access to their ICS environments to maintain cybersecurity principles of confidentiality, integrity, and availability, as these systems often control vital infrastructure such as power grids, water treatment facilities, and manufacturing processes. Fourth, developing ICS environments requires substantial financial investment and specialized infrastructure that most educational institutions cannot justify or afford [2]. Finally, ICS implementation and management demand highly specialized knowledge spanning both operational technology (OT) and information technology (IT) domains, expertise that remains scarce and often concentrated within industry rather than academia.

To address these challenges, cybersecurity testbeds have emerged as a mechanism that allows industry professionals and academia to replicate industrial control systems to investigate cyber attacks, assess vulnerability, and test security solutions [3]. For example, research by Al-Hawawreh and Sitnikova (2020) highlights the use of cybersecurity testbeds to assess the robustness of security controls, analyze attack landscapes, and extract threat intelligence in IIoT networks [3]. Furthermore, studies by Siboni et al.(2018) and Berhanu et al.(2013) demonstrated the application of testbeds to test, detect vulnerabilities, and evaluate resilience against cyber threats in industrial settings [33],[5].

Although the virtual cybersecurity testbed serves as an alternative environment for experimentation, its use for teaching ICS cybersecurity education is limited. In particular, researchers have used virtual cybersecurity testbeds to investigate vulnerabilities in industrial control systems, performing known attacks to exploit

vulnerabilities while testing intrusion detection systems. This is due to the benefits of virtual cybersecurity testbeds in terms of low-cost setup, ease of maintenance, and accessibility[9],[39]. Since virtual cybersecurity testbeds have gained popularity among academia and industry for conducting research and testing ICS vulnerabilities [10][32], their application to teaching ICS cybersecurity education remains unknown. This study is a review of existing seminal work to examine factors influencing virtual cybersecurity testbeds to teach ICS cybersecurity education. The study aims to answer this research question: **What factors influence the use of virtual cybersecurity testbeds for ICS cybersecurity education?**

2 Related work

The existing literature has explored virtual cybersecurity testbeds to investigate ICS vulnerabilities and support the management of ICS security. Koganti et al. (2017) designed a virtual testbed to support the ICS security management of the power grid distribution system. Their work highlighted the use of the virtual cybersecurity testbed as a potential platform to assess security threats and advance cybersecurity research [19]. Likewise, Robles Durazno et al. (2021) implemented a Virtual Napier Water Treatment System (VNWTS), a virtual testbed utilized to analyze the cybersecurity of a water treatment system. VNWTS contains virtual representations of real-world components such as sensors, actuators, PLCs (Siemens S7-1500), SCADA systems, and Human-Machine Interfaces (HMIs). Their work experimented with different cyber attacks specifically targeting operational technology to improve its cybersecurity posture [9].

Xie et al. (2018) implemented a Virtual Tennessee-Eastman Testbed (VTET) for chemical industrial processes, mainly for research purposes. VTET was used to simulate different cyberattacks, demonstrating its capability for cybersecurity testing and cyber threat evaluation [39]. In addition, Wolsing et al. (2023) focus on a virtual testbed of Extra-Large Unmanned Underwater Vehicles (XLUUVs). The virtual testbed was used to integrate IT and OT components, which allowed researchers to analyze cyber risks associated with technology used in the maritime domain [38]. Existing studies have focused on the implementation of virtual cybersecurity testbeds for cybersecurity research, which allow researchers to experiment and conduct security testing and vulnerability exploitation. From understanding when the study is conducted, there is no study that has reviewed factors that influence the virtual cybersecurity testbed used for ICS cybersecurity education. This study, therefore, attempts to address this gap and synthesize all the elements that influence virtual cybersecurity use to advance ICS cybersecurity education, to provide educators and researchers with the importance of virtual cybersecurity testbeds towards teaching ICS cybersecurity education.

3 Methodology

This study adopted Kitchenham's literature review guidelines [16] to conduct the systematic literature. Kitchenham's guideline was followed to select and analyze the primary studies included in the study.

3.1 Search Process

The authors identified relevant keywords "virtual cybersecurity testbed", "virtual testbed", "industrial control systems", "ICS", "cybersecurity education" based on the research question and existing work [18] [10]. These keywords were used to formulate the search query. After multiple revisions, a final search query was developed and applied to three databases; IEEE Digital Library, ACM Digital Library, and Scopus Digital Library. The search conducted on March 14, 2025, returns 246 articles. Of these articles, 112 come from the IEEE database, 128 from the ACM database, and 6 articles came from the Scopus database. Table 1 shows a detailed breakdown of the number of articles generated by the queries in each of the three databases.

The titles and abstracts of these articles were retrieved from the databases and uploaded to Rayyan software for further processing and analysis. Rayyan Software [27] is an online tool for systematic literature review that allows duplicate detection, inclusion, and exclusion of articles. A total of 35 possible duplicate articles were detected. The author reviewed possible duplicate articles by checking similarity scores, the title of the article, the journal, the types of publication, and the abstract of the article. This informs the author whether to keep both articles or one of the articles. Where the proceeding years and versions differ, the author kept both articles. Of the 35, 8 duplicated articles were removed. The inclusion and exclusion criteria were then applied to a total of 238 article titles and abstracts.

Table 1: Search Keywords

Database	Search Query	Articles
ACM	AllField:("virtual cybersecurity testbed") OR AllField:("virtual testbed") AND AllField:(Industrial Control Systems) OR AllField:(ICS) AND AllField:("cybersecurity education")	128
IEEE	("All Metadata": "virtual cybersecurity Testbed") OR ("All Metadata": "virtual testbed") AND ("All Metadata": "Industrial Control Systems") OR ("All Metadata": ICS) AND ("All Metadata": "cybersecurity education")	112
Scopus	ALL ("virtual cybersecurity testbed") OR ALL ("virtual testbed") AND ALL (industrial AND control AND systems) OR ALL (ics) AND ALL ("cybersecurity education")	6

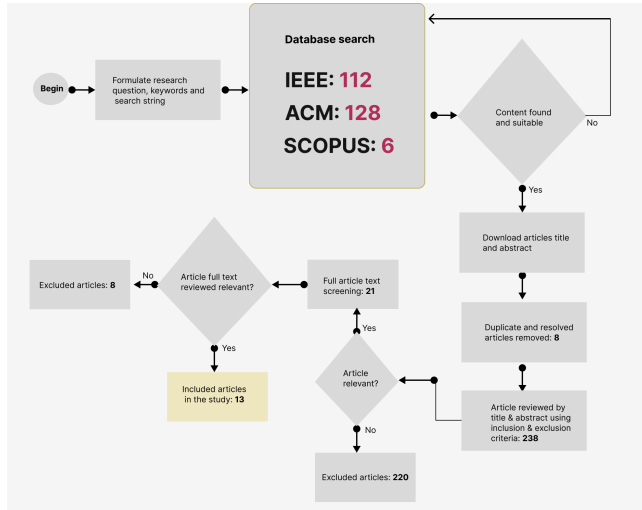
3.2 Inclusion and Exclusion Criteria

In line with the SLR protocol guidelines [16], the study defined the following inclusion and exclusion criteria as shown in Table 2.

Table 2: Inclusion and Exclusion Criteria

Inclusion	Exclusion
Journal and conference-related papers	Paper focuses on other types of cybersecurity testbeds.
Virtual cybersecurity testbed focusing on teaching ICS cybersecurity education)	Paper focuses on a virtual cybersecurity testbed for research purposes only.
Virtual testbed focusing on teaching cybersecurity education of Industrial Control System or ICS	Article that focuses on cybersecurity testbed outside ICS cybersecurity.
Paper written in English Language	Paper published in another language.
	Paper that was published with only an abstract.
	Survey and systematic literature review (SLRs)
	Other published papers that are not journals and conferences, such as posters, textbooks, handbooks, and slides.

Figure 1 illustrates the screening process that was used in this study. During the title and abstract screening process, 220 articles were excluded. The remaining articles undergo full-text review using the inclusion and exclusion criteria. Of the 21 articles, 13 articles were found relevant to answering the research question and were therefore included in the study.

**Figure 1: Review process for inclusion and exclusion of primary studies**

To ensure the quality of the included articles, the selected articles were reviewed multiple times on different days. The quality review process was guided by the question: To what extent is each selected article relevant to answer the research question? Among the 13 articles assessed, 11 articles were noted as having a focus, while 2 articles were deemed to have some focus. This process confirms that the 13 selected articles are suitable and were used in the study.

3.3 Data Extraction and Analysis

A data extraction form was used to extract data from the primary studies to answer the research question. The use of a structured data extraction form ensures consistency, reduces bias, and facilitates confidence in the data extraction process [21].

Table 3: Data Extraction Form

Field	Attributes	Description
A1	Author	Primary study citation
B1	Year	What year is the primary study published?
C1	Testbed Name	What is the name of the Virtual Cybersecurity Testbed?
D1	Open Source	Does the primary study use open source tools for the virtual cybersecurity testbed?
E1	Hands-On Experience	Does the article encourage practical usage?
F1	ICS Cybersecurity	Does the virtual cybersecurity testbed focus on ICS cybersecurity?
G1	Teach ICS Cybersecurity	Is the virtual cybersecurity testbed used to teach ICS cybersecurity?
H1	Target Learners	Who are the target learners in the primary study?
I1	Dataset Generation	Is the testbed used for dataset generation?
J1	Safety	Is the virtual testbed used for safety reasons?
K1	Simulation	Is the testbed used for the simulation of Industrial Control Systems?
L1	Cost	Does cost facilitate the use of virtual cybersecurity testbeds?
M1	Attack	Is the virtual testbed used for studying attacks or attack automation?
N1	Demand for ICS Knowledge and Skills	Does demand for ICS knowledge and skills facilitate the use of virtual cybersecurity testbeds?
O1	Reproducibility	Does the virtual cybersecurity testbed facilitate reproducibility?
P1	Interactive Learning	Is the virtual cybersecurity testbed used for interactive learning?
Q1	Learning Evaluation	Does the virtual cybersecurity testbed help with learning evaluation?
R1	Scalability	Does the virtual cybersecurity testbed allow scalability?
S1	Remote Possibility	Does the virtual cybersecurity testbed facilitate remote connection or logins?
T1	Educational Resource	Does the virtual cybersecurity testbed enable production of educational resources?

The application of the data extraction form is recognized in systematic literature reviews and analyses due to its effectiveness in maintaining uniformity and minimizing errors during data extraction [7]. The details of the extraction form are illustrated in Table 3. A1, B1, and C1 provide an overview of the primary studies while fields C1, D1, E1, F1, G1, H1, I1, J1, K1, L1, M1, N1, O1, P1, Q1, R1, S1, and T1 focus on answering the research question. These fields help to extract data that provides insight into the factors that influence the use of virtual cybersecurity testbeds to teach ICS cybersecurity.

The author, guided by the research question, reviewed the full text and therefore extracted relevant data from the selected primary studies, similar to the process found in [28]. To improve the quality and validity of the extracted data, the author performs a two-step quality validation. The author, after one week, again read the full text of the selected primary studies to ensure that appropriate data is extracted from the primary studies. After this process, the author discussed the extraction process and the extracted data with another researcher to further enhance the quality of the data to answer the research question. The author then used a descriptive analysis method to analyze and summarize the extracted data.

4 Results

This study presents the results of the data extracted from 13 primary studies, as shown in Table 4. Figure 2 shows the distribution of the factors that influenced the use of virtual cybersecurity testbeds for ICS cybersecurity education. 100% of the primary studies mentioned hands-on, while emphasizing the importance of ICS cybersecurity. This is followed by 92.3% of the primary studies mentioning simulation, 84.6% of the primary studies highlight attack and attack automation, as well as ICS knowledge and skill. In addition, 76.9% of the primary studies mentioned open source and educational resources, while 69.2% emphasized factors like cost. Furthermore, 38.5% of the primary studies stated that teaching ICS cybersecurity, safety, and interactive learning as factors that drive the use of virtual cybersecurity testbed. Likewise, 23.1% of the primary studies mentioned the generation, reproducibility, evaluation of learning, scalability, and remote possibility of the data sets as factors that drive the adoption of virtual cybersecurity.

Table 4: Factors Influencing the Use of Virtual Cybersecurity Testbeds for ICS Cybersecurity Education

Factors	Citations
Open Source	[11], [13], [25], [34], [18], [6], [20], [15], [35], [1]
Hands-On Experience	[11], [13], [25], [31], [24], [34], [18], [6], [4], [20], [15], [35], [1]
ICS Cybersecurity	[11], [13], [25], [31], [24], [34], [18], [6], [4], [20], [15], [35], [1]
Teach ICS Cybersecurity	[13], [25], [34], [18], [1]
Dataset Generation	[25], [24], [35]
Safety	[11], [25], [31], [24], [15], [35]
Simulation	[11], [13], [25], [31], [24], [34], [18], [6], [4], [20], [15], [1]
Cost	[11], [13], [25], [31], [24], [34], [18], [6], [35]
Attack/Attack Automation	[11], [13], [25], [31], [24], [18], [6], [4], [15], [35], [1]
ICS Knowledge and Skills	[11], [25], [31], [24], [34], [18], [6], [4], [15], [35], [1]
Reproducibility	[31], [34], [18]
Interactive Learning	[31], [4], [20], [15], [1]
Learning Evaluation	[13], [20], [15]
Scalability	[24], [18], [20]
Remote Possibility	[20], [15], [1]
Educational Resource	[31], [24], [34], [18], [6], [4], [20], [15], [35], [1]

Based on the findings, the study observed multiple factors that contribute to the use of virtual cybersecurity testbeds for ICS cybersecurity education. Hands-on experience facilitates the deployment of virtual cybersecurity testbeds that allow ICS cybersecurity learners to practice learning about industrial control systems. According to [8], hands-on learning is an effective method of gaining cybersecurity experience that allows learners to practice. The virtual cybersecurity testbed bridges the gap of access to a real-life system due to the possibilities of ICS system failure, system operation failure, and confidentiality that strictly prohibits such system availability for students to practice.

The need to simulate industrial control systems facilitates the use of virtual cybersecurity testbeds because the testbeds make it possible to use available tools and software to simulate a specific system. The ability to simulate makes it possible to conduct ICS research [37]. Another factor is the understanding of attacks and attack simulation. Since it is not possible to carry out an attack on a real system, the use of a virtual environment allows the possibilities of understanding the behavior of known attacks or simulating cyber attacks against industrial control systems [23, 37]. This has contributed to the deployment of virtual cybersecurity testbeds. As industries continue to deploy ICS for different reasons, the demand for ICS-skilled professionals has also increased. This factor facilitates the deployment of virtual cybersecurity testbeds to up-skill individuals interested in learning to safeguard industrial control systems [12]. However, becoming an ICS cybersecurity professional requires extensive knowledge of the ICS background and in-depth practical experience.

Another factor that makes the use of virtual cybersecurity testbeds promising is the availability of open source. Open source tools are leveraged to build a virtualized environment that enables the learning of ICS operations and their security [10]. Examples of such open-source tools as observed in the primary studies include GRFICS, Python, and Kali Linux. Many of the primary studies indicate the importance of creating educational materials on industrial control systems cybersecurity. As observed, this is why virtual cybersecurity testbeds have been leveraged to create educational materials to learn about ICS cybersecurity education. Likewise, the need to teach cybersecurity of ICS was observed in primary studies as a factor because it is necessary to go beyond just creating educational materials for ICS cybersecurity.

Furthermore, this study observed that cost contributes as a driver of the virtual cybersecurity testbed. The result aligns with [30], portraying a virtual cybersecurity testbed to be a cheaper method of implementing an ICS. ICS hardware and software are very expensive and not affordable; hence, the move to using open source, free tools to simulate and build a virtual environment, which does not require expensive hardware components.

Safety is a critical part of an industrial environment. The wrong input can lead to a catastrophic incident and loss of life. The critical nature of industrial control systems prevents them from being used for learning opportunities. As a result, led to the creation of virtual cybersecurity testbed, a safe environment that allows instructors, academics, and practitioners to spin virtual instances of an ICS environment for learning purposes. This environment has allowed the generation of a dataset to understand ICS patterns and behavior [29] that were initially not possible. The ability to

generate data makes it possible to apply the concept of machine learning techniques, allowing the student to practice using machine learning techniques to safeguard critical infrastructure [26]. And to develop an early warning system that could detect and prevent attack incidents against ICS systems.

Interactive learning was another factor driving the use of virtualized environments such as the virtual cybersecurity testbed. This enables participants to collaborate, share, and work together on realistic ICS scenarios, which, as a result, would lead to a better experience and outcome. The ability to reproduce similar ICS education materials for different sets of learners is seen to have shifted the attention to a virtual cybersecurity testbed. The same goes for the demand for remote provision that allows students to log in to participate in the learning environment. In addition, the virtual cybersecurity testbed allows the instructor to evaluate the learning as the student progresses in learning ICS cybersecurity. In addition, the scalability factor enables scaling whereby instructors can easily add resources in terms of virtual instances, and increase the number of learners that can participate or learn about ICS cybersecurity education continues to drive the use of virtual cybersecurity testbeds.

As depicted in Figure 3, the representation of the primary study highlights the intent of the virtual cybersecurity testbed. It demonstrates 100% focus on ICS cybersecurity, while 38.5% focus on using a virtual cybersecurity testbed for teaching ICS cybersecurity. Likewise, Figure 4 shows the target learners for a virtual cybersecurity testbed. Based on the literature, these learners span a broad range, including primary and secondary school students, university students, researchers, and ICT professionals.

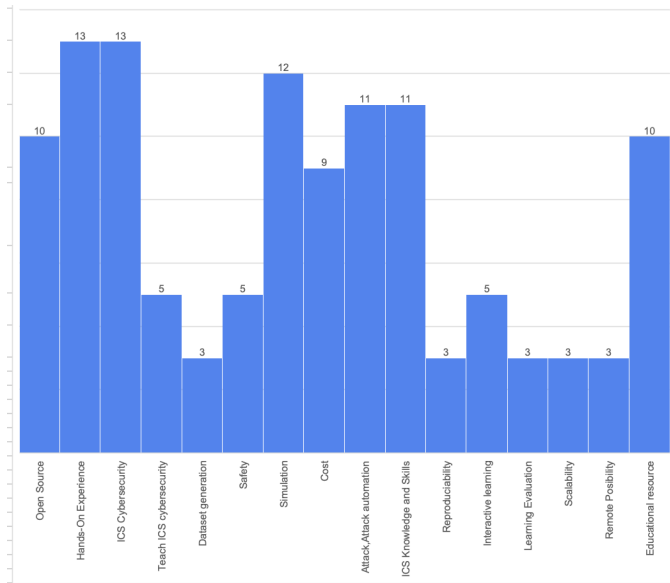


Figure 2: The overview of factors that influence the use of virtual cybersecurity testbed to understand and to teach ICS cybersecurity

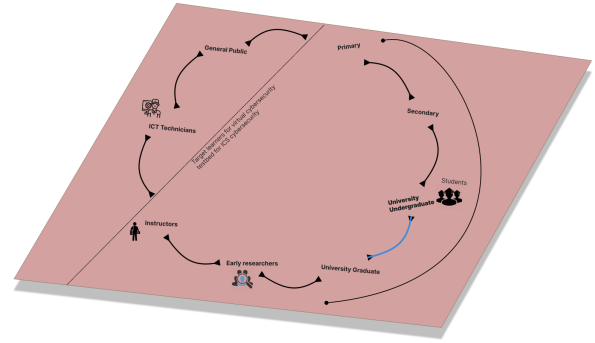


Figure 3: Target learners for the application of virtual cybersecurity in teaching ICS cybersecurity.

5 Discussion

The study identifies various factors that influence the adoption of a virtual cybersecurity testbed for ICS cybersecurity. Likewise, it shows that virtual cybersecurity testbeds are used to target different learners when it comes to ICS cybersecurity. In addition, it gives insight into how virtual cybersecurity testbeds are used to teach ICS cybersecurity.

The emphasis on hands-on experience from all the primary studies reinforces that experiential learning is critical for ICS cybersecurity education, which necessitates interactive approaches compared to the traditional method of learning. The prevalence of open-source implementations suggests that virtual cybersecurity testbed adoption helps to address the cost barrier that may hinder institutions in setting up an environment for learning ICS education. In addition, the result shows that virtual cybersecurity can be used by different learners; therefore, the testbed design should be flexible and tailored for different learners. In addition, the limited emphasis on reproducibility and remote accessibility represents a significant opportunity and research gaps due to educational shifts as a result of the COVID-19 pandemic and research rigor demands; future virtual cybersecurity testbed development should prioritize these capabilities.

Virtual cybersecurity testbeds continue to be used by academics and practitioners for cybersecurity education, simply by using them for research, simulation, and testing different types of industrial control systems. However, its use to teach ICS cybersecurity is low compared to using it for other purposes, such as research, simulation, and testing, as illustrated in Figure 3.

This study demonstrates that virtual cybersecurity testbeds can be used to implement ICS cybersecurity education that targets different types of learners. Figure 4 illustrates the applicability of the virtual cybersecurity testbed to help students and early researchers learn and be equipped with ICS knowledge and skills. Likewise, it can be used to up-skill ICT technicians and the general public interested in learning the operation of ICS. Therefore, this study encourages setting up a virtual cybersecurity testbed for teaching cybersecurity on industrial control systems as well as developing a cybersecurity program for industrial control systems.

6 Limitations

In this study, three databases of publications were used as data sources. The selection of the three digital libraries took into account their appeal in ICS cybersecurity and the relevance of the data to answer the research question. Another source of limitation is the data extraction process. However, the author ensured a rigorous process through the use of inclusion and exclusion criteria to extract relevant data from primary studies and quality review through peer discussion.

7 Conclusion and Future Works

The findings indicate that virtual cybersecurity testbeds create a unique opportunity for education by providing hands-on experience in simulating and analyzing attacks on critical infrastructure, an essential skill for learners. This suggests that virtual cybersecurity testbeds are vital tools for advancing ICS cybersecurity education. This study would inform instructors and academicians about the potential of virtual cybersecurity testbeds, especially their application for designing an ICS cybersecurity course. Likewise, it encourages academicians not to limit the use of virtual cybersecurity testbed to only research or simulation of the ICS system, but to use it to teach ICS cybersecurity targeting various learners. Consequently, these factors illustrate that virtual cybersecurity testbeds are an essential resource to build the next generation of ICS cybersecurity professionals capable of defending and protecting critical infrastructure. Based on these findings, several directions for future work emerge. First, further research should investigate ICS testbeds in teaching ICS cybersecurity courses, focusing on technical and governance aspects. Second, develop metrics to evaluate the virtual cybersecurity testbed in teaching an ICS cybersecurity course. Third, there is a need to develop reproducible, openly accessible educational materials that leverage virtual testbeds for diverse ICS learning contexts. Third, universities and colleges are encouraged to establish virtualized environments to support hands-on ICS cybersecurity training. Fourth, a virtual cybersecurity testbed should be used to equip K-12 students and teachers on the security of industrial control systems. Finally, future studies should explore effective learning evaluation mechanisms to assess and improve the pedagogical impact of virtual cybersecurity testbeds. Collectively, these efforts can help cultivate the next generation of ICS cybersecurity professionals capable of defending and protecting critical infrastructure.

References

- [1] Stanislav Abaimov, Joseph Gardiner, Emmanouil Samanis, Jacob Williams, Marios Samanis, Feras Shahbi, and Awais Rashid. 2024. Capture The Industrial Flag: Lessons from hosting an ICS cybersecurity exercise. In *Proceedings of the 10th ACM Cyber-Physical System Security Workshop*. 98–106.
- [2] Taiwo Akinremi, Joel Appiah, Amir Asadi, Opetunde Ibitoye, Hansinie Jayathilake, and Hazem Said. 2025. Systematic Literature Review of Cybersecurity Testbeds for Industrial Internet of Things. In *Proceedings of the 2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*.
- [3] Muna Al-Hawawreh and Elena Sitnikova. 2020. Developing a security testbed for industrial internet of things. *IEEE Internet of Things Journal* 8, 7 (2020), 5558–5573.
- [4] Rawan Alnsour and Basil Hamdan. 2020. Incorporating SCADA Cybersecurity in Undergraduate Engineering Technology & Information Technology Education. In *2020 Intermountain Engineering, Technology and Computing (IETC)*. IEEE, 1–4.
- [5] Yared Berhanu, Habtamu Abie, and Mohamed Hamdi. 2013. A testbed for adaptive security for IoT in eHealth. In *Proceedings of the International Workshop on Adaptive Security*. 1–8.
- [6] Pavel Čeleda, Jan Vykopal, Valdemar Švábenský, and Karel Slaviček. 2020. Kyp04industry: A testbed for teaching cybersecurity of industrial control systems. In *Proceedings of the 51st acm technical symposium on computer science education*. 1026–1032.
- [7] Jacqueline Chandler, Miranda Cumpston, Tianjing Li, Matthew J Page, and VJHW Welch. 2019. *Cochrane handbook for systematic reviews of interventions*. Hoboken: Wiley (2019).
- [8] Daniel Conte de Leon, Christopher E Goes, Michael A Haney, and Axel W Krings. 2018. ADLES: Specifying, deploying, and sharing hands-on cyber-exercises. *Computers & Security* 74 (2018), 12–40.
- [9] Andres Robles Durazno, Naghmeh Moradpoor, James McWhinnie, and Jorge Porcel-Bustamante. 2021. VNWS: A Virtual Water Chlorination Process for Cybersecurity Analysis of Industrial Control Systems. In *2021 14th International Conference on Security of Information and Networks (SIN)*, Vol. 1. IEEE, 1–7.
- [10] Conrad Ekisa, Diarmuid Ó Briain, and Yvonne Kavanagh. 2021. An open-source testbed to visualise ics cybersecurity weaknesses and remediation strategies—a research agenda proposal. In *2021 32nd Irish Signals and Systems Conference (ISSC)*. IEEE, 1–6.
- [11] Conrad Ekisa, Diarmuid Ó Briain, and Yvonne Kavanagh. 2022. Vicsort-a virtualised ics open-source research testbed. In *2022 Cyber Research Conference-Ireland (Cyber-RCI)*. IEEE, 1–8.
- [12] Conrad Ekisa, Diarmuid Ó Briain, and Yvonne Kavanagh. 2024. Modelling and Simulating Advanced Cyber-threats to Industrial Control Systems with an Emulated Testbed. In *2024 35th Irish Signals and Systems Conference (ISSC)*. IEEE, 1–6.
- [13] Magdalena Glas, Manfred Vielberth, and Guenther Pernul. 2023. Train as you fight: Evaluating authentic cybersecurity training in cyber ranges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–19.
- [14] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. 2015. A survey of industrial control system testbeds. In *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings*. Springer, 11–26.
- [15] Konstantinos Karampidis, Spyros Panagiotakis, Manos Vasilakis, Agapi Tsironi Lamari, Evangelos Markakis, and Giorgos Papadourakis. 2023. Digital Training for Cybersecurity in Industrial Fields via virtual labs and Capture-The-Flag challenges. In *2023 32nd Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEIE)*. IEEE, 1–6.
- [16] Staffs Keele and others. 2007. Guidelines for performing systematic literature reviews in software engineering.
- [17] Minseo Kim, Seungho Jeon, Jake Cho, and Seonghyeon Gong. 2024. Data-Driven ICS Network Simulation for Synthetic Data Generation. *Electronics* 13, 10 (2024), 1920.
- [18] Matthew J Kirkland, Stu Steiner, and Daniel Conte de Leon. 2021. vWaterLabs: Design and characteristics of a virtual testbed for water-focused ICS cybersecurity education. *Journal of Computing Sciences in Colleges* 36, 8 (2021), 33–42.
- [19] Venkata S Koganti, Mohammad Ashrafuzzaman, Ananth A Jillepalli, and Frederick T Sheldon. 2017. A virtual testbed for security management of industrial control systems. In *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*. IEEE, 85–90.
- [20] Karel Kuchar, Petr Blazek, and Radek Fudjak. 2023. From Playground to Battleground: Cyber Range Training for Industrial Cybersecurity Education. In *Proceedings of the 2023 13th International Conference on Communication and Network Security*. 209–214.
- [21] Alessandro Liberati, Douglas G Altman, Jennifer Tetzlaff, Cynthia Mulrow, Peter C Gøtzsche, John PA Ioannidis, Mike Clarke, Philip J Devereaux, Jos Kleijnen, and David Moher. 2009. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Annals of internal medicine* 151, 4 (2009), W–65.
- [22] Chenyang Liu, Yazeed Alrowaili, Neetesh Saxena, and Charalambos Konstantinou. 2021. Cyber risks to critical smart grid assets of industrial control systems. *Energies* 14, 17 (2021), 5501.
- [23] Daniel L Marino, Chathurika S Wickramasinghe, Vivek Kumar Singh, Jake Gentle, Craig Rieger, and Milos Manic. 2021. The virtualized cyber-physical testbed for machine learning anomaly detection: A wind powered grid case study. *IEEE Access* 9 (2021), 159475–159494.
- [24] Petr Matoušek and Ondřej Ryšavý. 2021. Teaching ICS security in blended classroom environment. In *2021 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEIE)*. IEEE, 1–6.
- [25] Colman McGuan, Chansu Yu, and Qin Lin. 2023. Towards low-barrier cybersecurity research and education for industrial control systems. In *2023 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 1–6.
- [26] Mohammad Noorizadeh, Mohammad Shakerpour, Nader Meskin, Devrim Unal, and Khashayar Khorasani. 2021. A cyber-security methodology for a cyber-physical industrial control system testbed. *IEEE Access* 9 (2021), 16239–16253.
- [27] Mourad Ouzzani, Hossam Hammady, Zbys Fedorowicz, and Ahmed Elmagarmid. 2016. Rayyan—a web and mobile app for systematic reviews. *Systematic reviews* 5 (2016), 1–10.
- [28] José Pereira dos Reis, Fernando Brito e Abreu, Glauco de Figueiredo Carneiro, and Craig Anslow. 2022. Code smells detection and visualization: a systematic literature review. *Archives of Computational Methods in Engineering* 29, 1 (2022), 47–94.

- [29] Ondrej Pospisil, Petr Blazek, Karel Kuchar, Radek Fujdiak, and Jiri Misurec. 2021. Application perspective on cybersecurity testbed for industrial control systems. *Sensors* 21, 23 (2021), 8119.
- [30] Andres Robles-Durazno, Naghmeh Moradpoor, James McWhinnie, Gordon Russell, and Jorge Porcel-Bustamante. 2021. Implementation and evaluation of physical, hybrid, and virtual testbeds for cybersecurity analysis of industrial control systems. *Symmetry* 13, 3 (2021), 519.
- [31] Fatemeh Sarshartehrani, Anthony Lee, Mohamed Azab, Trenton Watkins, and Denis Gračanin. 2024. Towards immersive cybersecurity workforce development for mission-critical IoT Systems. In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 0176–0182.
- [32] HM Shamsuzzaman, MD Mosleuzzaman, A Mia, and A Nandi. 2024. Cybersecurity Risk Mitigation in Industrial Control Systems Analyzing Physical Hybrid And Virtual Test Bed Applications. *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems* 1, 01 (2024), 19–39.
- [33] Shachar Siboni, Vinay Sachidananda, Yair Meidan, Michael Bohadana, Yael Mathov, Suhas Bhairav, Asaf Shabtai, and Yuval Elovici. 2018. Security testbed for Internet-of-Things devices. *IEEE transactions on reliability* 68, 1 (2018), 23–44.
- [34] Stu Steiner, Matthew J Kirkland, and Daniel Conte de Leon. 2021. Vwaterlabs: Developing hands-on laboratories for water-focused industrial control systems cybersecurity education. *Journal of Computing Sciences in Colleges* 36, 10 (2021), 24–29.
- [35] Jay Thom, Tapadhir Das, Bibek Shrestha, Shamik Sengupta, and Engin Arslan. 2021. Casting a wide net: An internet of things testbed for cybersecurity education and research. In *2021 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*. IEEE, 1–8.
- [36] Thavavel Vaiyapuri, Zohra Sbai, Haya Alaskar, and Nourah Ali Alaseem. 2021. Deep learning approaches for intrusion detection in IIoT networks—opportunities and future directions. *International Journal of Advanced Computer Science and Applications* 12, 4 (2021).
- [37] Yunfei Wang, Zhengdao Zhang, and Linbo Xie. 2018. A semi-physical simulation testbed for cybersecurity. In *2018 37th Chinese Control Conference (CCC)*. IEEE, 6423–6428.
- [38] Konrad Wolsing, Antoine Saillard, Elmar Padilla, and Jan Bauer. 2023. Xlab-UUV—a virtual testbed for extra-large uncrewed underwater vehicles. In *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. IEEE, 1–6.
- [39] Yaobin Xie, Wei Wang, Faren Wang, and Rui Chang. 2018. VTET: A virtual industrial control system testbed for cyber security research. In *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 1–7.