

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository: <https://orca.cardiff.ac.uk/id/eprint/182786/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Highfield, Jenny , Franklin, Harry, Dartey, Adowa, Deverson, Alexander and Teehan, Catherine 2025. Pedagogical approaches for cyber-physical system education: critical national infrastructure vulnerability and mitigation awareness for long term cyber resilience. Presented at: 18th annual International Conference of Education, Research and Innovation, Seville, Spain, 10-12 November 2025. ICERI2025 Proceedings. IATED, pp. 8749-8758. 10.21125/iceri.2025.2469

Publishers page: <http://dx.doi.org/10.21125/iceri.2025.2469>

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



PEDAGOGICAL APPROACHES FOR CYBER-PHYSICAL SYSTEM EDUCATION: CRITICAL NATIONAL INFRASTRUCTURE VULNERABILITY AND MITIGATION AWARENESS FOR LONG TERM CYBER RESILIENCE

J. Highfield, H. Franklin, A. Dartey, A. Deverson, C. Teehan

Cardiff University (UNITED KINGDOM)

Abstract

This paper discusses pedagogical approaches used for Cyber-Physical System (CPS) education, through the use of physical and virtual artefacts. These include testbeds, virtual twins, simulations, serious games, and both physical and digital cyber demonstrators. Virtualisation tools, such as cyber ranges and game engines will also be discussed. Cybersecurity research into CPS vulnerabilities related to the Industrial Control Systems (ICS) behind Critical National Infrastructure (CNI) is typically conducted using replica systems, rather than the actual systems, to avoid real-world risks.

In educational contexts, these surrogate systems are used at different levels. Virtual twins and testbeds are better suited for technical instruction, while serious games, demonstrators, and simulations are better suited for conceptual education. The background research identifies research gaps: while research into the use of testbeds for education exists, there is a lack of research into Game-based Learning (GBL) and Simulation-based Learning (SBL) for CPS education. To address the research gap, this paper presents studies on the application of pedagogical approaches using digital artefacts: a GBL tool to teach Industrial Control System (ICS) security concepts, aligned with the Digital Competence Framework (DCF), to support early-stage cybersecurity literacy in schools; and SBL digital demonstrators that visualise cascading effects of cyber-attacks on CNI for a wide range of stakeholders.

Findings highlight the value of interactive, scenario-driven tools in cybersecurity education, with eighty percent of participants (n=8) in one study reporting increased knowledge of cybersecurity vulnerabilities of renewable energy infrastructure. Following on from these digital artefact studies, research will be conducted into the effectiveness of applying existing pedagogical methods to CPS education using physical artefacts, specifically testbeds. The continuation of this research looks to integrate CNI concepts into mainstream education through the Creative Curriculum for Wales using physical and digital artefacts. The studies discussed in this paper provide early evidence that CPS artefacts are not only effective educational tools, but critical components in shaping a new educational framework. This research represents foundational steps toward long-term cyber resilience, as education in this area contributes to the development of more informed and responsible digital citizens.

Keywords: Cybersecurity, cyber-physical systems, industrial control systems, operational technology, critical national infrastructure, education, pedagogy, problem-based learning, game-based learning, serious games, cyber demonstrator, testbed-based learning, testbed, CPS, ICS, OT, CNI, GBL, SBL, TbBL.

1 INTRODUCTION

Historically, training for hands-on industrial roles was delivered primarily through vocational education or on-the-job experience. Many systems were previously air gapped as discussed in Section 1.1.2, so cybersecurity awareness was not necessary for industrial technicians or engineers. However, as Cyber-Physical Systems (CPS) have become more interconnected, new vulnerabilities have emerged, making cybersecurity education increasingly essential for those responsible for operating and maintaining these systems.

1.1 Introduction to Cyber-Physical Systems

Cyber-Physical Systems (CPS) are behind the automation of a range of technologies, including smart factories using sensors and robotics for manufacturing, traffic management systems such as rail signalling and road traffic lights, smart meters that allow for real time monitoring and managing of utility supplies, and remote patient monitoring in healthcare.

1.1.1 Critical National Infrastructure

The systems that we rely on for the day-to-day functioning of society are known as Critical National Infrastructure (CNI), and there are thirteen main sectors: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water. Data Infrastructure (such as datacentres) was added as a sub-section of communications in September 2024 and is commonly referred to as the new fourteenth sector.

1.1.2 Operational Technology

The scope of this study includes CPS that utilise control loops, these systems are grouped together as Operational Technology (OT), and include Industrial Control Systems (ICS), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) Systems and the Industrial Internet of Things (IIoT). A simple control loop can be illustrated by a heating system with a thermostat, with sensors detecting a change in temperature, and actuators being the mechanisms that open or close valves regulating the flow of water.

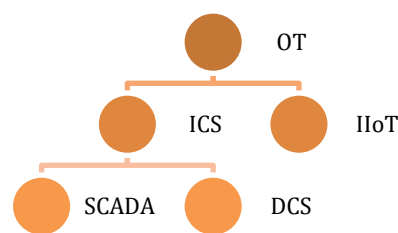


Figure 1: OT Tree Diagram

There are four generations of OT: monolithic, distributed, networked, and web-based or IIoT systems. Monolithic systems were built pre-Internet and so were not built with network security in mind. This means they are reliant on an 'air-gap'—no network connection to other systems—to be secure. However, this became an issue when new parts with the same serial number started being manufactured with added network capabilities that the industrial engineers might not have been aware of [1].

These systems need to stay operational as downtime can be costly to businesses and catastrophic for critical national infrastructure, such as the systems behind nuclear power plants, for example. Patches that update the systems and fix known vulnerabilities require time to be downloaded and installed and will need to be installed through an external connection, whether through an external drive, networked connection or temporarily attached device. This can lead to vulnerabilities, and risk further downtime in the case that the patch causes the system to crash. This leaves many SCADA systems vulnerable to known exploits.

1.1.3 Increased connectivity and emerging vulnerabilities

One significant example of a known vulnerability being exploited was the computer worm: Stuxnet. It infiltrated an Iranian nuclear facility in 2009 through the use of a USB flash drive. The Iranian nuclear facilities were air-gapped, and so a physical connection to the system was required for the intrusion. The worm exploited vulnerabilities in software (Siemens Step7) which communicate and control Programmable Logic Controllers (PLCs)—the brain of a control loop, where the decisions are made. It was able to manipulate the centrifuges causing them to spin at speeds too fast or too slow and provide false feedback data to operators to delay detection and response to the attack. Stuxnet destroyed approximately one-thousand centrifuges and caused significant disruption of operations [2].

With the rapid adoption of Internet of Things (IoT) devices for their convenience, there has been a lag in cybersecurity adoptions for the use and management of these devices, including the IIoT devices purposefully added to OT architectures [3]. This purposefully breaches the air-gap that monolithic systems rely on to remain secure. This allows for generic network exploits against the system as they have network connectivity now, which allows access to potentially unpatched systems [1].

1.2 Cyber-Physical System Education

The convergence of Information Technology (IT) and Operational Technology (OT) has led to a need for cybersecurity education that is tailored specifically to Cyber-Physical Systems (CPS). As these systems become increasingly interconnected, they are exposed to a wider range of vulnerabilities—not only technical, but also human and systemic. The risks posed to Critical National Infrastructure (CNI), such as energy grids and transportation networks, necessitate a broad-based educational response to build long-term cyber resilience.

The on-the-job or vocational training mentioned in section 1 often focusing on safety, efficiency, and mechanical reliability rather than digital security. This was sufficient in earlier generations of OT environments that were air-gapped and isolated from external networks. However, with the integration of Industrial Internet of Things (IIoT) devices and increased remote connectivity, there is now a need to train these professionals in cybersecurity principles specific to OT environments.

Education for CPS is required not only for the on-site industrial technicians and engineers, but also for research engineers involved in system development. As a result, robotics has become an established topic within computer science education and research [4]. While robotics research can be carried out on the sole piece of equipment being developed (such as a standalone robot), the CPS security research relevant to this project looks at complex systems of controllers, field devices (such as sensors and actuators), human machine interfaces (HMI), and most importantly the devices' linked networks.

1.2.1 Technical instruction

When it comes to technical instruction and cybersecurity research, to avoid risks of downtime or damage to the real-world systems, or incidents that could result in death (such as traffic control systems failing), surrogate systems are used. These can be physical, virtual, or hybrid in form.

- **Testbeds** are hardware-based representative systems that emulate the functionality of real-world industrial environments [5].
- **Digital twins** are virtual models that may have bi-directional (and sometimes mono-directional) communication with the real-world system predominantly used for research [6].
- **Virtual twins** are standalone digital representations used predominantly for education, with no live connection to a physical system [7].

These artefacts should be authentic and so should closely mimic the hardware and software used in the original system. For full virtualisation, the network needs to be replicated. This is done via Software Defined Networking (SDN) using cyber ranges [5]. Cyber ranges are computers used to simulate realistic scenarios including clients, servers and networks for training for cybersecurity training, testing and research.

1.2.2 Conceptual education

For conceptual education, didactic artefacts such as simulations, cyber demonstrators (Simulation-based Learning [8]), and serious games [9] (Game-based Learning) can be used. In contrast to digital and virtual twins, which receive sensor data from either real or virtual sensors, simulations tend to be more abstract, using historical datasets or synthetic data [10].

1.3 Pedagogical research in CPS education

While there is a growing body of research for cybersecurity education more broadly, fewer studies have focused specifically on research backed pedagogical approaches suitable for Cyber-Physical Systems (CPS) cybersecurity education. Although some general approaches can be adapted to CPS contexts, there remains a gap in literature addressing the unique technical and conceptual challenges these systems present.

1.3.1 Educational frameworks and guidance

The Cyber Security Body of Knowledge (CyBOK) includes a dedicated CPS knowledge area [11], outlining the fundamental concepts, threats, and mitigation techniques specific to the domain. This document offers a strong theoretical foundation but does not prescribe pedagogical delivery methods. The T-CHAT framework [12], by contrast, focuses explicitly on the educational design of CPS engineering. It integrates technical knowledge, human factors, assessment, and tool support, providing an adaptable structure for CPS curriculum development.

1.3.2 Testbeds for technical instruction

There are several academic papers outlining the specification for CPS testbeds for education, including researchers from Mississippi State University [13], Masaryk University [14], and the University of New Orleans [15]. However, while these papers mention that the testbeds will be used for pedagogy, there is no discussion. In contrast, The Department of Weapons and Systems Engineering (W&SE) at the United States Naval Academy [16], outline a networked CPS testbed for undergraduate education which includes the system design, and a pedagogical discussion including learning outcomes, and a Project-based Learning (PjBL) activity.

Project-based Learning (PjBL) is a student-led, educator-facilitated approach to learning [17]. The W&SE outline a testbed and propose a PjBL activity where they put into practice 1) the concepts discussed throughout the course, 2) to identify and understand the hardware being used, 3) to programme a microcontroller for the design of control systems, 4) To learn how to use controller area networks (CAN) in a control system, and 5) to run experiments on the system to evaluate the effects of disturbances and cyber threats on the performance of the system. [16]

Continuing from the research at W&SE, Fontera lead pedagogical research on a PjBL activity regarding network attacks on CPS, this time through the Weapons, Robotics and Control Engineering Department (WRC) of the United States Navy Academy. [18] Students investigate the implementation and effects of two cyberattacks, 1) a stealth attack and 2) a replay attack, both on a CPS testbed.

Konstantinou of Florida State University outlines hands-on lab exercises for CPS security education [19]. Their paper outlines six lab exercises: 1) demonstrate a CPS process-aware attack, 2) practice basic exploitation techniques using Kali Linux, 3) programme a buffer overflow vulnerability, 4) leverage hardware performance counters for anomaly detection, 5) test cache-timing attacks on AES-based (advanced encryption standard) servers, 6) provide a solution to the security multiparty set intersection problem (MPSI).

Harish et al. [20] outline a 'cyberthon' with three phases: 1) web application security testing against vulnerabilities aligned to the OWASP Top 10 [21], when to report vulnerabilities according to standards, and open-source intelligence (OSINT); 2) legally gaining evidence, and social engineering and physical security; and 3) a role play session of a cyber-physical incident where students interact with a CPS testbed that shows a crisis scenario, followed by a debrief session.

In their paper, Aydin et al. [22] discuss a PBL curriculum for production and programming of industrial automation training. Students were put into groups and asked to create a virtual company and design logos, they then had team meetings to assign tasks and plan their work as a team. The project utilises a conveyor testbed that can separate long plastic, short plastic, long metal and short metal from one another. Students were given an example application for controlling the testbed and asked to develop their own designs and programmes for the testbed.

Tharot et al. [23] outlined a gamification approach to teaching cybersecurity in CPS, including the following concepts: 1) PLC fundamental training, 2) security scenario design, 3) process setup, 4) ludic scenario design, and 5) process deployment for teaching. In a role-play scenario, participants play either an automation specialist, forensic investigator, team manager, hacker or assistant in a man in the middle (MITM) scenario.

Bristol University run Capture the Flag (CTF) competitions for ICS cybersecurity education using CPS testbeds. In their first paper on the topic, Abaimov et al. [24] outline six activities for participants: 1) reconnaissance, 2) forensics, 3) exploitation of IT vulnerabilities, 4) OT protocol exploitation, 5) OT logic analysis, and 6) physical security such as lockpicking.

Continuing from the first CTF paper [24], Gardiner et al. [25] outlined a blueprint for ICS-focussed CTF competitions using CPS testbeds. This included challenges from a second CTF, where the challenge topics were as follows: 1) OT trivia, 2) PLC forensics and analysis of OT PCAP (packet captures of

network data) and Historian logs, 3) asset discovery, 4) honeypots, 5) process comprehension regarding ladder logic, 6) process manipulation, 7) red team (hacking) challenges, 8) lockpicking, 9) man in the middle (MITM) attacks, 10) reverse engineering of S7COMM-PLUS packets.

1.3.3 Virtualisation for technical instruction

In a collaboration between National Instruments and University of California, Berkeley a massive open online course (MOOC) for the course: Introduction to Embedded Systems. The paper outlines a virtual environment for the education of CPS and discusses the benefits of the system compared to teaching using hardware. Benefits include cost savings, and grading via simulation [26].

The Institute for Nuclear Waste Disposal, Karlsruhe Institute of Technology propose an adaptive learning environment for Industry 4.0 competencies based on a learning factory and its immersive digital twin (virtual twin by this paper's definition) [19]. The paper outlines examples of how the Virtual Learning Platform (VLP) can be used, discussing PjBL and using simulation as a teaching method (defined as SBL in this paper).

Prohaska et al. [7] evaluated the use of virtual twins in a control systems course, with the aim of answering, 1) "Do virtual twins increase learning success?", 2) "Do virtual twins increase student satisfaction?", and 3) "Do virtual twins affect time spent on self-study by students". The study found that virtual twins have a positive impact on satisfaction and learning success.

1.3.4 Demonstrators for conceptual education

Cyber demonstrators are a form of Simulation-based Learning (SBL), and while simulations for the purpose of this paper are digital, the simulation in SBL relates to educational scenarios. SBL allows students to explore concepts without real-world consequences [8]. Two examples of demonstrators for the conceptual education of CNI include works by Vörös et al. [27] and Rössler et al. [28]. Both papers outline the technical setup of a model railway demonstrators for educational purposes.

2 METHODOLOGY

This study adopted a qualitative, user-focused approach to evaluate the effectiveness of digital artefacts in Cyber-Physical System (CPS) education. The research was conducted through three parallel user studies aligned to two pedagogical approaches: Game-Based Learning (GBL) and Simulation-Based Learning (SBL). The objective was to assess how interactive digital tools can support cybersecurity education and raise awareness of vulnerabilities in Critical National Infrastructure (CNI).

Each study used a bespoke artefact built in the Unity game engine:

- A serious game (GBL) focused on Industrial Control System (ICS) security concepts for early-stage learners.
- A renewable energy digital cyber demonstrator (SBL) visualising cyber-attack cascades in a wind farm control network.
- A rail infrastructure digital cyber demonstrator (SBL) simulating a targeted attack on rail signalling and operator communication systems.

The methodology across the studies followed similar structures:

2.1 Participants

Participants were recruited through convenience sampling, targeting university students and adult learners with varying levels of cybersecurity knowledge. The sample sizes were as follows:

- CPS Serious Game: 4 participants
- Renewable energy SBL: 8 participants
- Rail infrastructure SBL: 6 participants

In all three studies, participants were adults. Plans for subsequent testing with younger learners, particularly for the GBL artefact aligned with the Digital Competence Framework (DCF), are under development.

2.2 Study design

The studies were exploratory and primarily qualitative, designed to:

- Observe user engagement with the artefacts.
- Identify learning outcomes related to CPS security concepts.
- Evaluate usability and clarity of information presented.

Each session began with a short briefing, followed by a hands-on experience with the artefact. Participants then completed evaluation tasks or reflection activities depending on the artefact's design.

2.3 Data collection

Structured evaluation methods included Likert-scale surveys and task performance observations. Unstructured data was gathered through open-ended questionnaires, post-session discussions, and free-text feedback. Observational notes were taken during sessions to record behaviours, misunderstandings, and levels of engagement.

2.4 Data analysis

Qualitative feedback was coded thematically to identify recurring patterns in user experience and conceptual understanding. Quantitative elements (e.g., Likert responses) were analysed using simple descriptive statistics due to small sample sizes. No inferential statistics were applied at this stage, in line with the exploratory nature of the studies.

2.5 Ethical considerations

All participants were informed of the nature of the study and consent was obtained. No personal data was collected. The studies were reviewed under Cardiff University's internal ethical procedures for student-led research projects.

3 RESULTS

This section presents findings from three exploratory studies using digital artefacts to teach cybersecurity concepts relevant to Cyber-Physical Systems (CPS) and Critical National Infrastructure (CNI). The studies focused on evaluating learner engagement, conceptual understanding, and perceived educational value. Results are presented per study, with attention to both quantitative metrics and qualitative feedback.

3.1 Serious Game for ICS Security Education

Four participants played a Serious Game [9] that introduces learners to security risks in Industrial Control Systems. The game was designed to align with the Digital Competence Framework (DCF) [29] and features scenario-driven gameplay reflecting real-world industrial vulnerabilities.



Figure 2: CPS Security Serious Game by Adwoa Dartey

3.1.1 Key findings

Feedback from participants was gathered through semi-structured interviews and was collected on the game environment, camera movement, player movement, popups, mini quiz and final quiz. Participants described the game environment as “visually engaging” and “immersive”. The camera movement had mixed reviews, as 50% (n=4) of participants found the third person perspective difficult to control. However, the game popups were seen as informative and accessible.

3.2 Renewable Energy Cyber Digital Demonstrator

This study used a Simulation-based Learning (SBL) digital demonstrator to simulate and compare the varying effects of different cyberattacks on a wind farm. The goal was to communicate the interdependencies in renewable infrastructure and raise awareness of potential cascading effects across sectors of CNI.



Figure 3: Renewable Energy Digital Cyber Demonstrator by Harry Franklin

3.2.1 Key findings

From observing participants using the system it was found that 100% of participants (n=8) successfully navigated through all stages of using the cyber digital demonstrator. Through a survey, 80% of participants reported increased knowledge of cybersecurity vulnerabilities of renewable energy infrastructure, and 70% of participants reported learning about the cascading effects of attacks on the wider power grid.

3.3 Rail Infrastructure Cyber Digital Demonstrator

This demonstrator simulated a cyber-attack on rail signalling infrastructure, visualising the operational impact on a train control network.

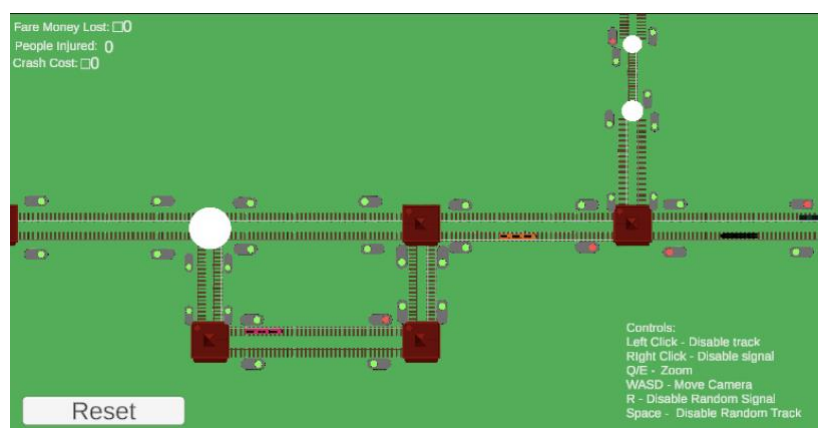


Figure 4: Rail Infrastructure Digital Cyber Demonstrator by Nathan Blundell

3.3.1 Key findings

Through a survey it was found that the projects main objective was met. When asked how useful the cyber digital demonstrator was at showing the cascading effects on a rail network the average score was 7.5/10 (n=6). Participants were also asked if they liked the virtual design of the demonstrator and the score was 6.6/10. Finally, the score was 8.8/10 for the cyber digital demonstrator's portrayal of a working rail network.

3.4 Cross-Study Observations

Across all three studies, common themes emerged:

- Both GBL and SBL are efficient for the education of CPS using digital artefacts.
- Participants valued visually driven explanations of complex systems.
- All participants reported learning about CPS security and CNI vulnerability awareness.

These findings demonstrate the value of artefact-driven learning for conceptual and technical education in CPS cybersecurity. Although all testing was conducted with adult participants, the feedback suggests these artefacts could be suitable for adaptation to younger audiences, pending further development and testing.

4 CONCLUSIONS

This paper explored the pedagogical use of digital artefacts for Cyber-Physical System (CPS) and Critical National Infrastructure (CNI) cybersecurity education, with a focus on Game-Based Learning (GBL) and Simulation-Based Learning (SBL). Across the three user studies, interactive and scenario-driven digital tools were found to be effective in raising awareness of vulnerabilities and fostering early-stage cybersecurity literacy. The results indicate that these methods can help demystify complex systems and make abstract concepts more accessible to both technical and non-technical audiences.

However, while digital artefacts such as simulations and games are suitable for conceptual education, there remains a clear gap in pedagogical frameworks tailored to physical artefacts—particularly testbeds—which are essential for technical instruction in CPS cybersecurity. Existing approaches including the use of PjBL often fall short in addressing the unique challenges of teaching cybersecurity in Operational Technology (OT) environments.

To address this, we propose Testbed-Based Learning (TbBL) as a new pedagogical approach that combines the structured, scenario-driven benefits of Simulation-Based Learning with the realism and complexity of hardware-based testbeds. TbBL aims to support learners in developing practical skills and systemic understanding of CPS vulnerabilities and mitigations in a safe, controlled environment.

Future work will explore the implementation and evaluation of TbBL within the context of testbed use in schools and vocational training environments. This ongoing research aims to support the integration of CNI cybersecurity concepts into the Creative Curriculum for Wales [30], building a long-term foundation for cyber resilience through education.

ACKNOWLEDGEMENTS

The authors would like to thank Nathan Blundell for his contribution to the development and evaluation of the rail infrastructure digital demonstrator, which formed the basis of one of the case studies presented in this paper. We would also like to thank Dr Yulia Cherdantseva, Dr Amir Javed and Dr Andrew Hood for their broader academic support and guidance. Finally, we acknowledge the student participants who took part in the user studies across the three digital artefact projects. Their engagement and feedback were invaluable to the research.

REFERENCES

- [1] C. Baylon, R. Brunt and D. Livings, "Cyber Security at Civil Nuclear Facilities Understanding the Risks," Chatham House, London, England, 2015.
- [2] K. Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*, New York: Broadway Books, Crown Publishing, 2014.
- [3] S. Babar, P. Mahalle, A. Stango, N. Prasad and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," in *Third International Conference, CNSA 2010, Proceedings*, Chennai, India, 2010.
- [4] M. Ryalat , N. Almtireen, G. Al-refai, H. Elmoaqet and N. Rawashdeh, "Research and Education in Robotics: A Comprehensive Review, Trends, Challenges, and Future Directions," *Journal of Sensor and Actuator Networks*, vol. 14, no. 76, 2025.
- [5] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou and M. A. Ferrag, "Cyber Ranges and TestBeds for Education, Training, and Research," *Applied Sciences*, vol. 11, no. 4, p. 1809, 2021.
- [6] NCSC, "Digital twins: secure design and development," 02 09 2024. [Online]. Available: <https://www.ncsc.gov.uk/pdfs/blog-post/digital-twins-secure-design-development.pdf>. [Accessed 01 09 2025].
- [7] S. Prohaska and L. Kennes, "Evaluating the Use of Virtual Twins in a Control Systems Course," in *IEEE 2nd German Education Conference (GECon)*, Berlin, Germany, 2023.
- [8] M. E. Gredler, "Games and Simulations and Their Relationships to Learning," in *D. H. Jonassen (Ed.), Handbook of research on educational communications and technology*, Lawrence Erlbaum Associates Publishers, 2004, p. 571–581.
- [9] M. Whitby, F. Mao, K. Stawarz, S. Marrero and J. L. Walton, *Serious Games Cookbook: A beginner's guide to using and designing serious games*, Warwick, UK: University of Warwick Press, 2024.
- [10] Z. Lei, . H. Zhou, W. Hu, G.-P. Liu, S. Guan and . X. Feng, "From Virtual Simulation to Digital Twins in Online Laboratories," in *2021 40th Chinese Control Conference (CCC)*, Shanghai, China, 2021.
- [11] A. Cardenas, "CyBOK," 01 07 2021. [Online]. Available: https://www.cybok.org/media/downloads/Cyber_Physical_Systems-v1.0.1.pdf. [Accessed 15 08 2025].
- [12] E. Mäkiö, F. Azmat, B. Ahmed, R. Harrison and A. W. Columbo, "T-CHAT educational framework for teaching cyber-physical system engineering," *European Journal of Engineering Education*, vol. 47, no. 4, pp. 606-635, 2021.
- [13] T. Morris, R. Vaughn and Y. . S. Dandass, "A testbed for SCADA control system cybersecurity research and pedagogy," in *CSIIRW '11: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge Tennessee USA, 2011.
- [14] P. Čeleda, J. Vykopal, V. Švábenský and K. Slavíček, "KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems," in *SIGCSE '20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, Portland, OR, USA, 2020.
- [15] I. Ahmed, V. Roussev , W. Johnson, S. Senthivel and S. Sudhakaran, "A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy," in *ICSS '16: Proceedings of the 2nd Annual Industrial Control System Security Workshop*, Los Angeles CA USA, 2016.
- [16] E. J. Rodríguez-Seda, P. J. Frontera and J. Bradshaw, "A Networked Cyber-Physical System Testbed for Undergraduate Education," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, USA, 2018.
- [17] S. Bell, "Project-Based Learning for the 21st Century: Skills for the Future," *The Clearing House*, vol. 83, p. 39–43, 2010.

- [18] P. J. Frontera and E. J. Rodríguez-Seda, "Network Attacks on Cyber-Physical Systems Project-Based Learning Activity," *IEEE Transactions on Education*, vol. 64, no. 2, pp. 110-116, 2021.
- [19] C. Konstantinou, "Cyber-Physical Systems Security Education Through Hands-on Lab Exercises," *IEEE Design & Test*, vol. 37, no. 6, pp. 47 - 55, 2020.
- [20] A. V. Harish, K. Tam and K. Jones, "Generating training events for building cyber-physical security skills," *The Computer Journal*, vol. 68, no. 5, p. 445-459, 2025.
- [21] OWASP , "OWASP Top 10," Material for MkDocs, 31 03 2021. [Online]. Available: <https://owasp.org/Top10/>. [Accessed 2025 09 01].
- [22] İ. Aydın and V. Bulut, "Production and programming of industrial automation training set with project based learning curriculum," *Journal of Educational Technology & Online Learning*, vol. 7, no. 4, pp. 413-426, 2024.
- [23] K. Tharot, A. Riela and J.-M. Thir, "A Gamification Approach to Teaching Cybersecurity in CPS," *Procedia CIRP*, vol. 128, pp. 799-803, 2024.
- [24] S. Abaimov, J. Gardiner, E. Samanis, J. Williams, M. Samanis, F. Shahbi and A. Rashid, "Capture The Industrial Flag: Lessons from hosting an ICS cybersecurity exercise," in *CPSS '24: Proceedings of the 10th ACM Cyber-Physical System Security Workshop*, Singapore, 2024.
- [25] J. Gardiner, S. Abaimov, J. Williams, F. Shahbi, K. Anastasakis, P. D. Chowdhury, E. Winston, M. Sameen, E. Samanis and A. Rashid, "'If You Build it, They will Come' - A Blueprint for ICS-focused Capture-The-Flag Competitions," in *CPSIoTSec'24: Proceedings of the Sixth Workshop on CPS&IoT Security and Privacy*, Salt Lake City UT USA, 2024.
- [26] J. C. Jensen, E. A. Lee and S. A. Seshia, "Virtualizing Cyber-Physical Systems: Bringing CPS to Online Education," in *Proceedings of the First Workshop on Cyber-Physical Systems Education (CPS-Ed 2013) at Cyber Physical Systems Week (CPSWeek 2013)*, Philadelphia, Pennsylvania, 2013.
- [27] A. e. a. Vörös, M. Búr, I. Ráth, . Á. Horváth, . Z. Micskei, L. Balogh, B. Hegyi, B. Horváth, Z. Mázló and D. Varró , "MoDeS3: Model-Based Demonstrator for Smart and Safe Cyber-Physical Systems," in *NASA Formal Methods*, Newport News, VA, USA, 2018.
- [28] P. Rössler, . R. Höller, . F. Schrön, C. Reisner and E. Ewers, "A Model Railway based Demonstrator for Safety-Critical Systems," in *Proceedings of the 12th European Workshop on Microelectronics Education (EWME)*, Braunschweig, Germany, 2018.
- [29] Hwb, "Digital Competence Framework (DCF)," 01 09 2016. [Online]. Available: <https://hwb.gov.wales/curriculum-for-wales/cross-curricular-skills-frameworks/digital-competence-framework-dcf/>. [Accessed 01 09 2025].
- [30] Hwb, "Curriculum for Wales," 01 09 2022. [Online]. Available: <https://hwb.gov.wales/curriculum-for-wales>. [Accessed 01 09 2025].