Pedagogical Approaches for Cyber-Physical System Education

Jenny Marie Highfield

Catherine Teehan, Yulia Cherdantseva, Amir Javed
School of Computer Science & Informatics, Cardiff University

Introduction

The workshop proposed looks to evaluate the use of pedagogical approaches such as Challenge-based Learning (CBL), Project-based Learning (PBL), Story-based Learning (SBL), and Game-based Learning (GBL), for the education of Cyber-physical Systems (CPS).

Cyber-physical Systems are behind the Operational Technology (OT) used within Critical National Infrastructure (CNI), with many systems being built pre-Internet in the 1960s. This means that they were not built with network security in mind, and therefore rely on an 'air-gap' to be secure. [4]

Research question: How can existing pedagogical approaches be applied to the education of Cyber-physical System Security, to raise awareness of CPS security and CNI vulnerabilities and mitigation strategies?

Problem statement and aim

Cyber-physical System (CPS) education is traditionally done on the job, and so has not previously included security awareness, as many systems were kept air-gapped. Due to advancements in technology, these systems are becoming increasingly connected, whether through replacement parts with added network capability, or by connection to newer parts such as Industrial Internet of Things (IIoT) devices. This introduces vulnerabilities. [3]

Industry has seen an uptake in courses for CPS Security education using hardware artefacts. This research looks to determine a formal approach of using these hardware artefacts for education, co-created with educators.

Existing pedagogical approaches

Challenge-based Learning (CBL) is an experimental learning method where students can address real-world challenges [2] such as the United Nations' seventeen sustainable development goals (SDG) [6] of which securing CNI would contribute towards.

Project-based Learning (PBL) facilitates active exploration of a topic, collaboration, and the creation of tangible outcomes, such as prototypes [1]. One example of learning through PBL is the creation of prototype OT testbeds.

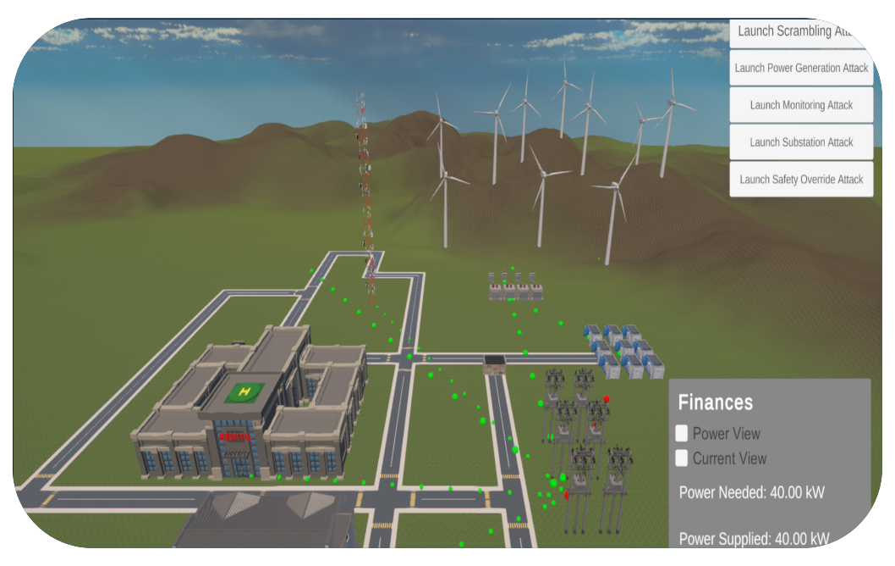
Story-based Learning (SBL) could be used to teach about vulnerabilities to CNI through an interactive narrative where the user makes active decisions to solve problems in a scenario. They could play the part of a nuclear engineer during a power outage.

Game-based Learning (GBL) such as the use of serious games [7] can be used to teach about the cascading effects of a cyberattack on CNI. This might involve a board game where malicious actors and system defenders compete to attack and defend CNI.

Educator workshop outline

The educator workshop's purpose is to gauge current teachings of CPS and CNI, to confirm interest from school teachers and FE and HE educators, and assess interest in adopting the proposed methods. The workshop will outline and demonstrate pedagogical approaches for CPS education, with a focus on cybersecurity.

Traditional methods are being assessed in this study, however, the pedagogical approaches being refined and defined in this study are **Hardware-based Learning (HwBL)** and **Testbed-based Learning (TbBL)**, using OT testbeds and CNI demonstrators.



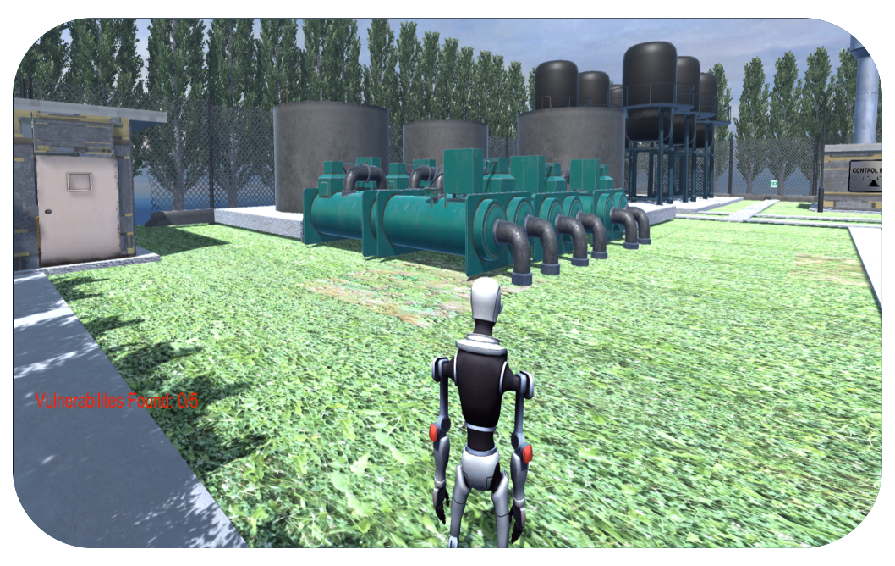


Figure 1: CNI Digital Demonstrator | Figure 2: CPS Education Serious Game

Introducing Testbed-based Learning (TbBL) – a pedagogical approach that uses OT testbeds and aligns with the "hardware approach" [5], which is referred to as Hardware-based Learning (HwBL) for the purpose of this study.

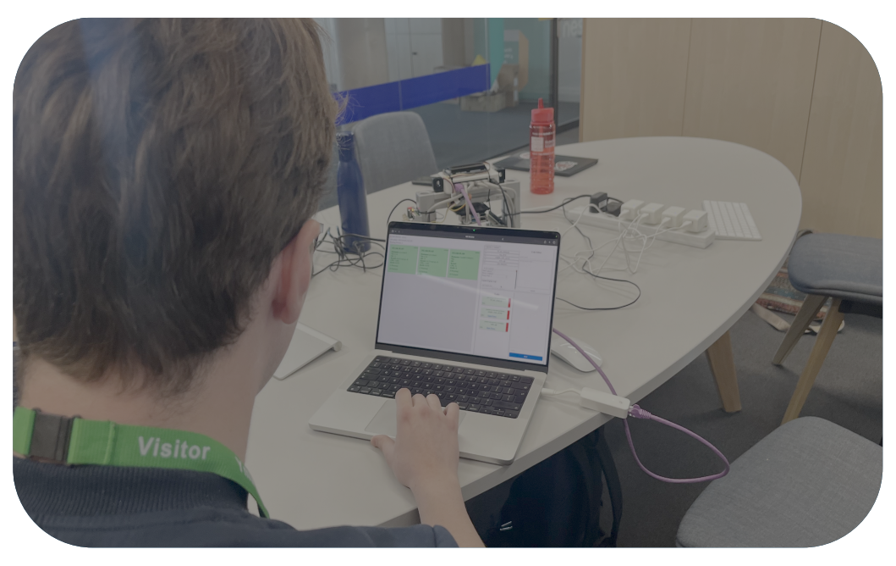
Current education mapping

This project sees the mapping of current education in this area, across levels: School, Further Education (FE), Higher Education (HE), and Continuous Professional Development/ Education (CPD/CPE). The aim of this mapping is to address gaps to be shared with the educator community. Existing research can be found in Bibliography (QR code).

Cyber-physical artefacts

OT testbeds mimic the electronic workings of a Cyber-physical Systems (CPS), including Programmable Logic Controllers (PLCs), and field devices such as sensors and actuators.

CNI demonstrators are physical or digital models that look like the system and act like the system, but the logic might not mimic the actual system.



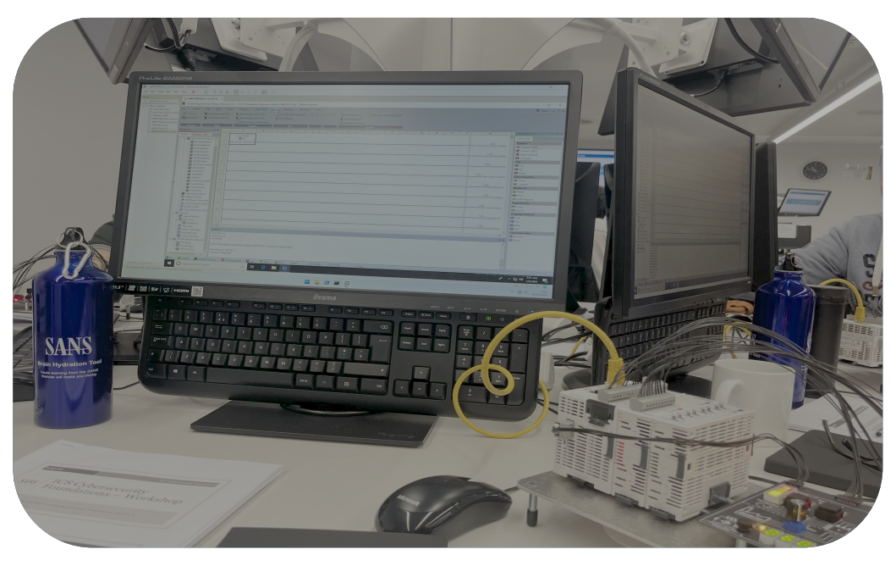


Figure 3: Prototype OT Testbed | Figure 4: SANS ICS Course

Research question: How do digital and physical artefacts for CPS and CNI education map to existing pedagogical approaches, and how should **Testbed-based Learning (TbBL)** approach be formally defined?

Get in contact:
highfieldjm@cardiff.ac.uk
ORCID: 0000-0002-5747-6347
ORCA: 21489

Co-creation with educators

Co-creation will be used for the development of the educational framework and pedagogical approach for teaching CPS security and CNI vulnerability and mitigation awareness. This will include:

The curriculum framework

- Themes
- Topics
- Learning outcomes

The educational resource pack

- Schemes of work
- Lesson plans
- Workbooks

References

[1] Thomas Armstrong. *The Power of the Adolescent Brain: Strategies for Teaching Middle and High School Students*. Alexandria, VA: ASCD, 2016. ISBN: 9781416621874.

[2] Scott Beattie. *Challenge-Based Learning: Engaging with Students Through Interactivity*. Springer Texts in Education. Singapore: Springer, 2024. ISBN: 978-9819601974. URL: https://doi.org/10.1007/978-981-96019-7-4.

[3] Clint Bodungen et al. *Hacking exposed industrial control systems: ICS and SCADA security secrets & solutions*. Columbus, OH: McGraw-Hill Education, 2016.

[4] Charles J Brooks and Philip A Craig Jr. *Practical industrial cybersecurity: ICS, industry 4.0, and IIoT*. en. Nashville, TN: John Wiley & Sons, 2022.

[5] Teachers Institute. *The Hardware Approach to Educational Technology: Tools That Transform Learning*. Teachers Institute. Dec. 2023. (Visited on 06/14/2025).

[6] United Nations. *Sustainable Development Goals*. Accessed: 2025-06-14. 2015. URL: https://sdgs.un.org/goals.

[7] Matthew Whitby et al. *Serious Games Cookbook: A beginner's guide to using and designing serious games*. University of Warwick Press, 2024. ISBN: 9781911675136. DOI: 10.31273/978-1-911675-13-6. URL: https://doi.org/10.31273/978-1-911675-13-6.