Driving Factors Behind Adopting Virtual Testbeds for ICS Cybersecurity Education

Taiwo Peter Akinremi, Joel Appiah, Amir Reza Asadi ,Opetunde Ibitoye,
Saheed Popoola, University of Cincinnati

next
lives
here

University of
CINCINNATI




16 critical infrastructure sectors







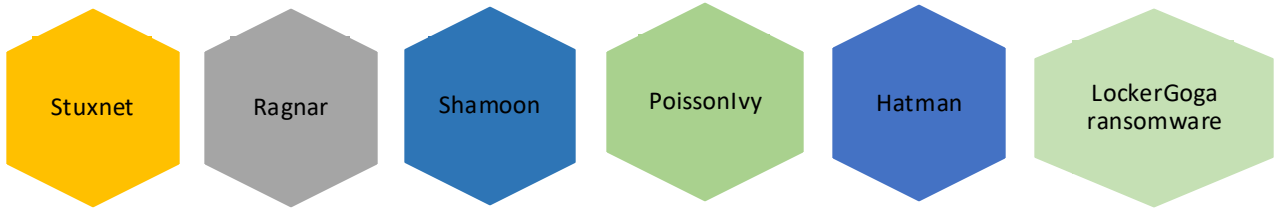




Background

ICS cybersecurity education is at low compared to the rapid increase of cyber threats on Industrial controls systems that control our critical industrial processes

- Cyber attacks target ICS system



- The potential gains attracted illicit cyber-related activities

Motivation

- Industrial Control Systems (ICS) present unique educational and research challenges that significantly limit hands-on learning opportunities.

- Although the virtual cybersecurity testbed serves as an alter-native environment for experimentation, there IS ICS training gap caused by restricted access to real ICS environments.

next lives here

- ICS systems are owned and privately owned
- Unavailable for training
- Strict confidentiality
- Resource intensive

University of CINCINNATI

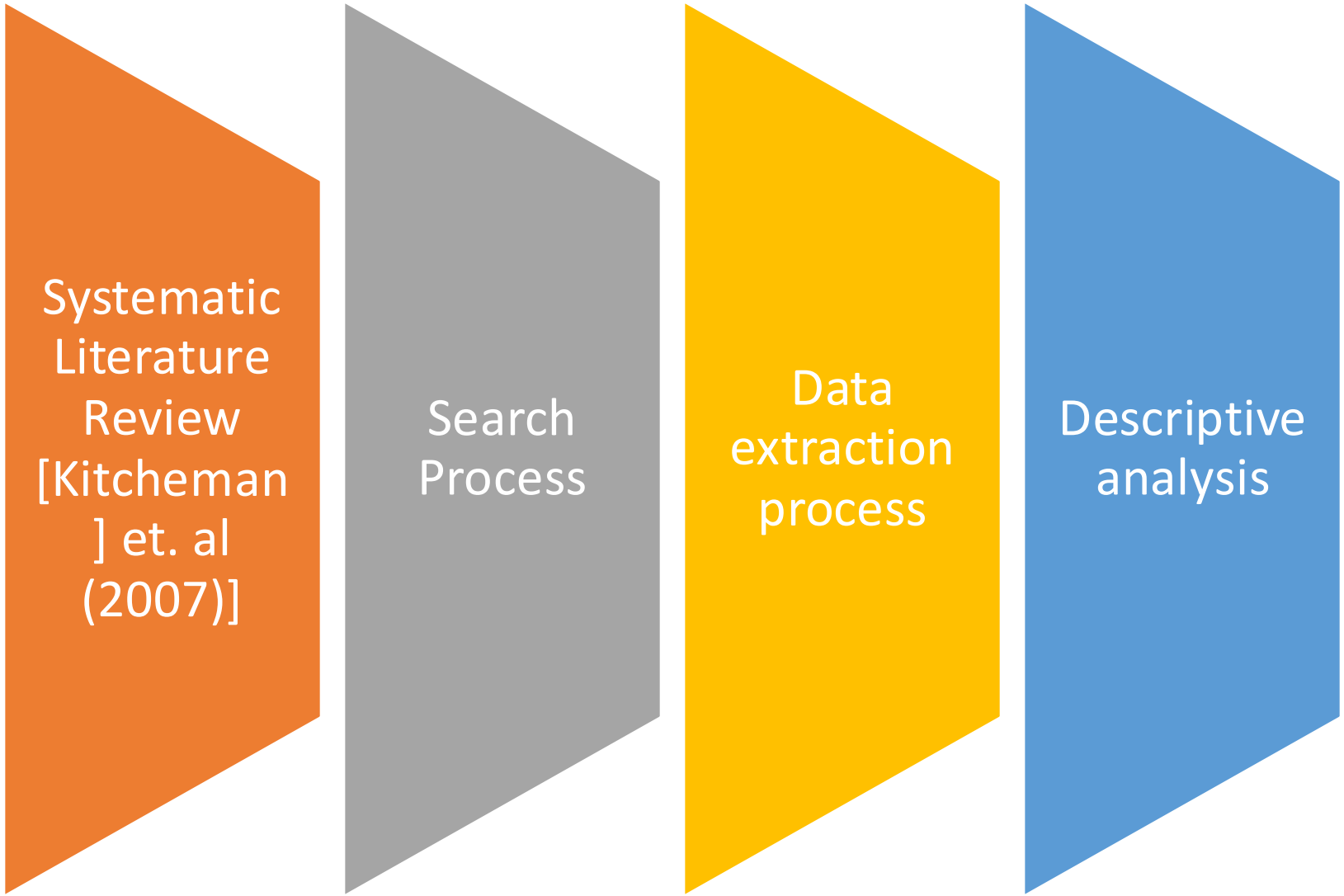
Research question

- What factors influence the use of virtual cybersecurity testbeds for ICS cybersecurity education?

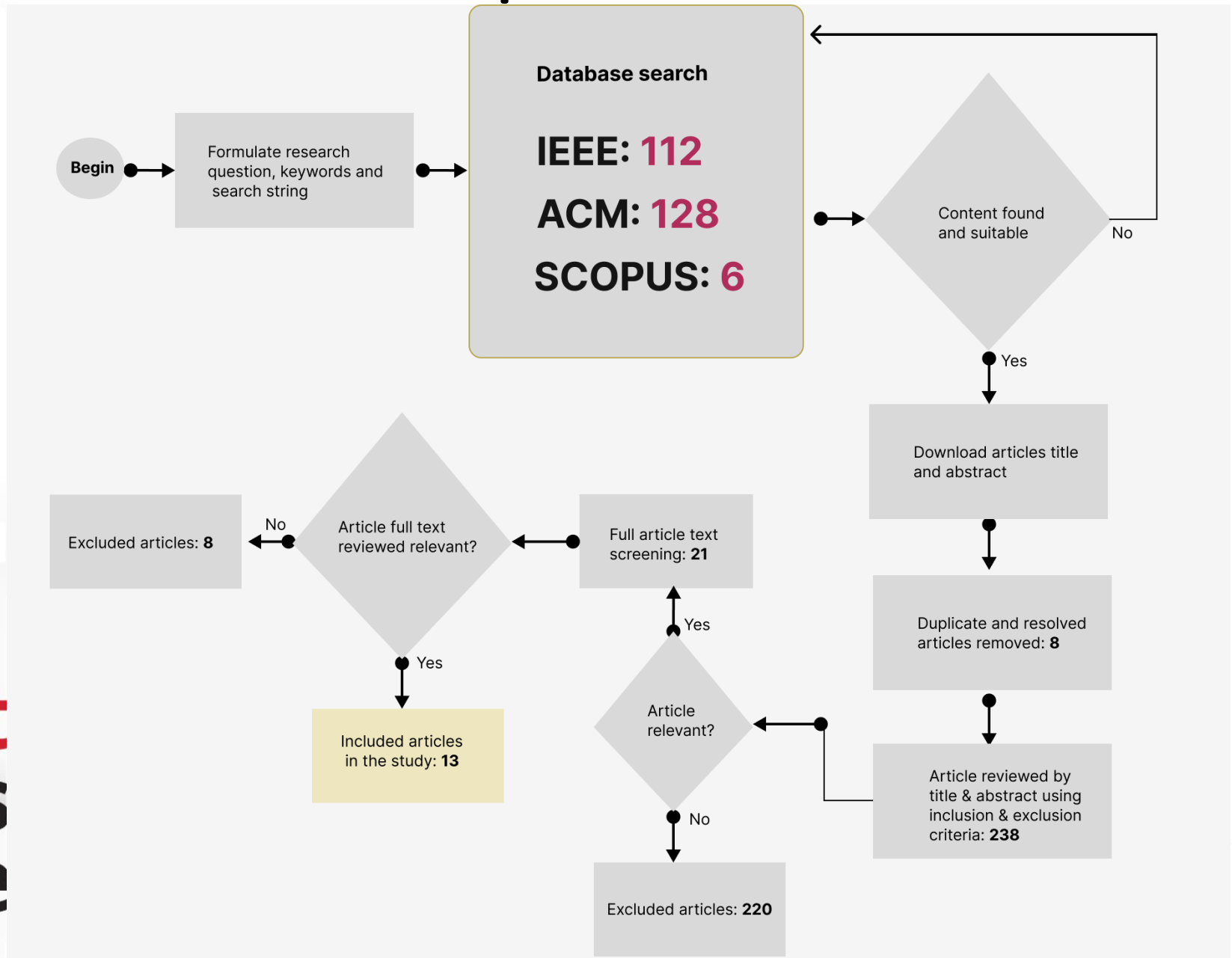
next lives here

University of CINCINNATI

Research Method



Data collection process



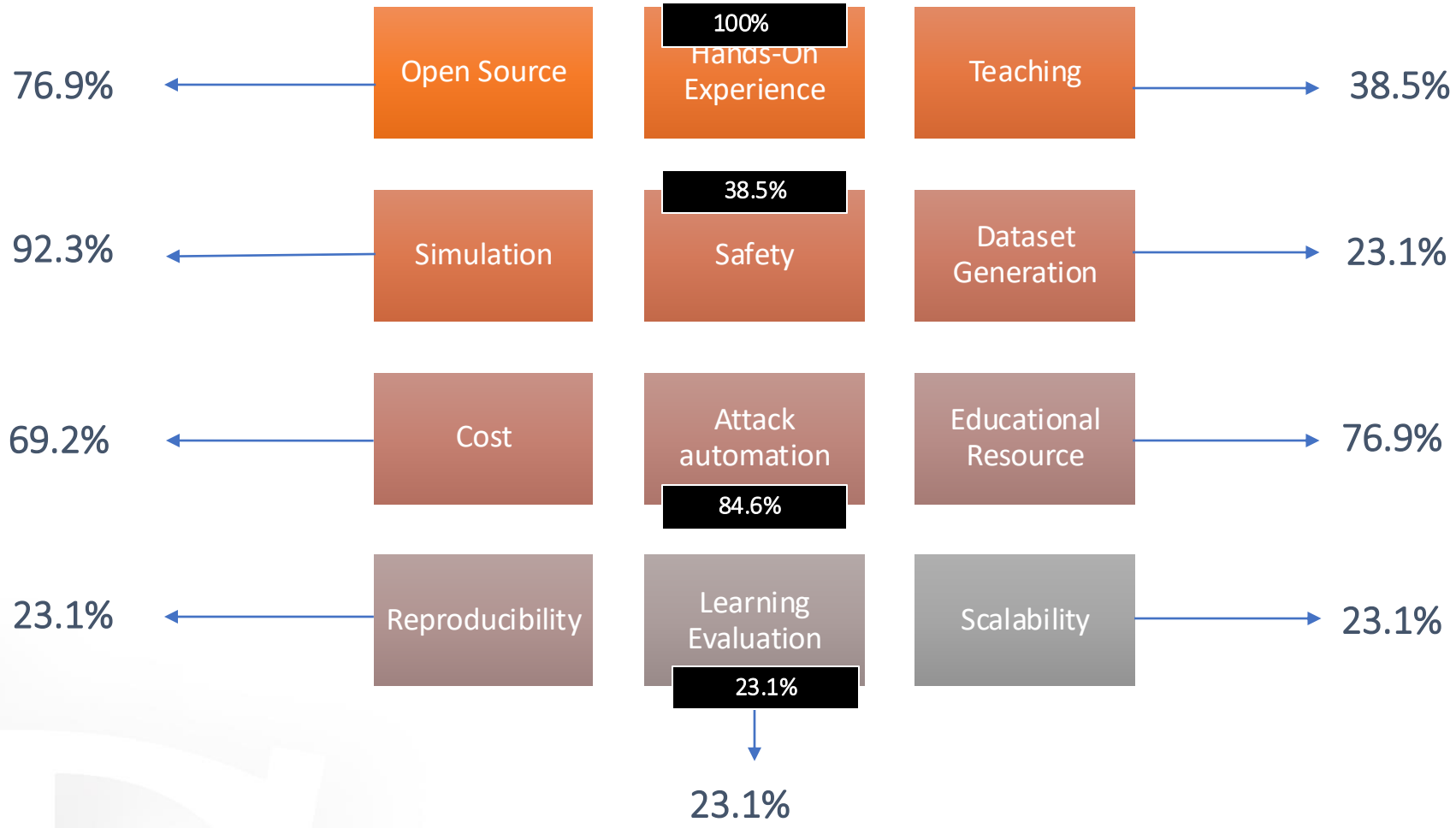
next lives here

University of CINCINNATI

Result

next
lives
here

University of
CINCINNATI

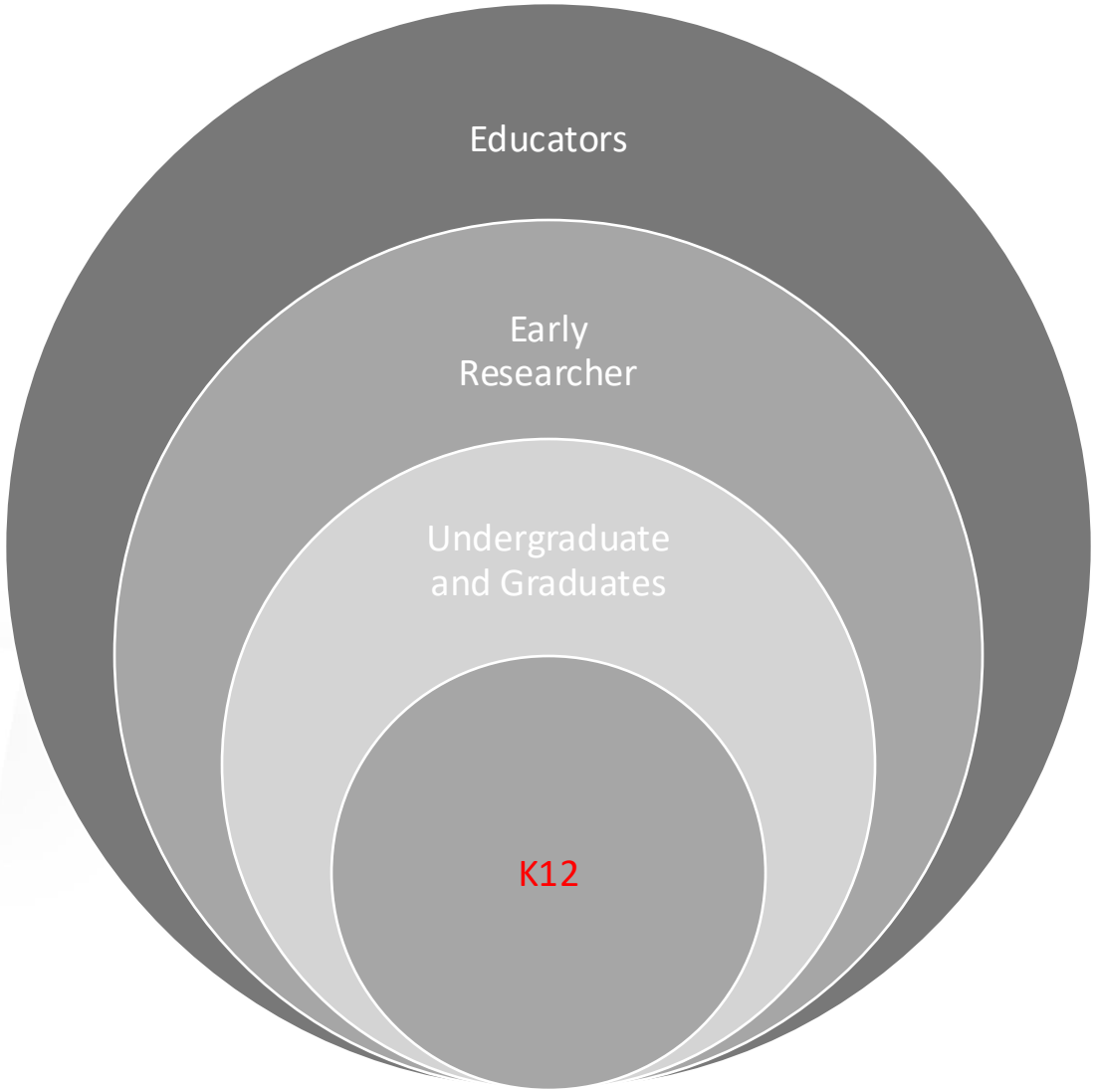


next lives here

Based on the results, the study observed multiple factors that contribute to the use of virtual cybersecurity testbeds for ICS cyber-security education.

University of CINCINNATI

Users of Virtual cybersecurity testbeds.



next lives here

University of CINCINNATI

Findings

The study shows ICS testbed are useful for practitioners and educators alike.

virtual testbeds offers accessible, safe, and cost-effective educational environments

next lives here

CINCINNATI

What can be done with virtual cybersecurity testbed?

INSTRUCTORS

- Teach ICS Cybersecurity
- Cost effectiveness
- Remote Possibility
- Educational Resource

LEARNERS

- Hands-On Experience
- Interactive Learning
- ICS Knowledge and Skills
- Learning Evaluation

EDUCATIONAL BENEFITS

- Open Source
- Reproducibility
- Dataset Generation
- Scalability

APPLICATION

- ICS Cybersecurity
- Safety
- Attack/Attack Automation
- Simulation

next lives here

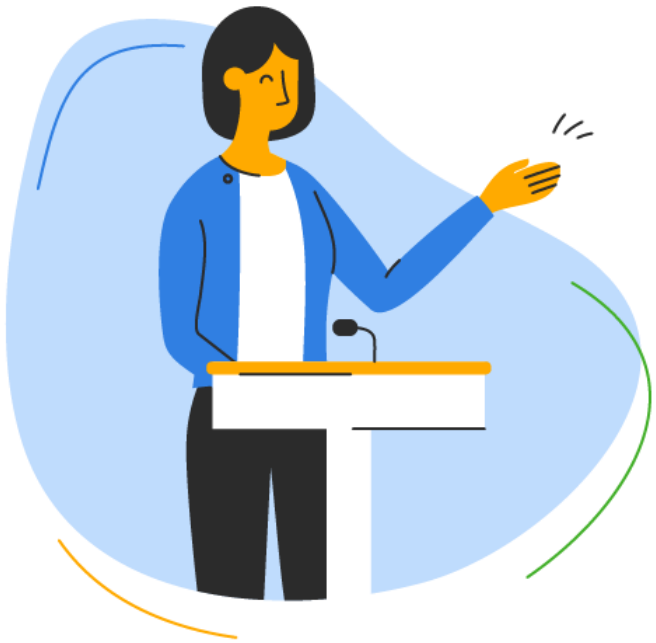
University of CINCINNATI

Contributions

- The paper identify and categorize factors for adoption of ICS cybersecurity testbeds in education.
- Guides educators and researchers on design priorities hands-on, open-source, cost-effective ICS testbed

Summary

- Industrial Control Systems (ICS) present unique educational and research challenges that significantly limit hands-on learning
- virtual testbeds offers accessible, safe, and cost-effective educational environments
- Educators and researchers needs to collaborate and design hands-on, open-source, cost-effective ICS testbed



Thank You!

next
lives
here

University of
CINCINNATI

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. 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.
3. 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.
4. 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.
5. Andres Robles-Durazno, Naghmeh Moradpoor, James McWhinnie, Gordon Rus-sell, 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.