

## Industrial Control Systems (ICS) Testbed for Cybersecurity Monitoring and Ethical Hacking

**Problem:** Industrial control systems (ICS) provide vital services, such as electricity, water treatment, automotive manufacturing, and transportation. Although these systems were formerly isolated, they became connected with information technology (IT) systems and to the Internet. This connectivity of processes in the cyberspace and the physical world has reduced costs and enabled new services. However, the ICS assets now became vulnerable to new threats and ever-evolving cyber threat landscape. In order to make these systems more secure, it takes research, which is, however, difficult to conduct on productive systems since they often have to operate twenty-four-seven. Testbeds are mostly very expensive, or they are based on simulations with no real-world physical process. We address this issue in this project.

**Objective:** Modeling and design of an ICS system for cybersecurity monitoring and penetration testing

Penetration testing is a process to test the cybersecurity of an IT or operational technology (OT) networks. In this project, students develop a low-cost ICS testbed, which enables cybersecurity experts and researchers to try out their ideas and algorithms and gain experience with an ICS system before applying their penetration testing strategies on a real-world ICS system where unexpected impact could be catastrophic.

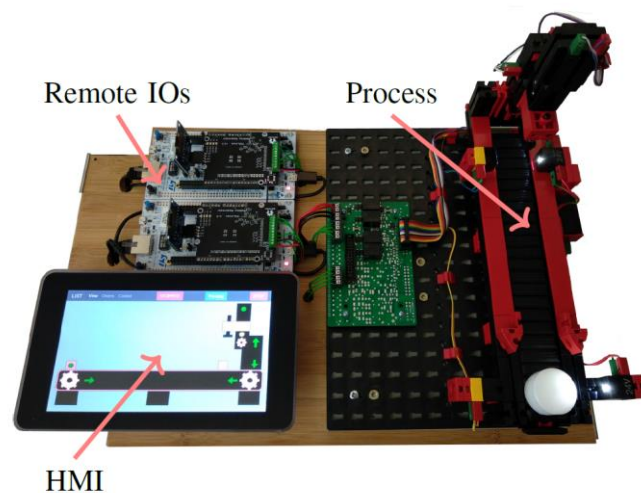


Figure: [LICSTER ICS Testbed](#)

**Project Scope:**

The proposed ICS testbed provides the necessary component of an ICS system for cybersecurity penetration testing and hacking with an emphasis on being low-cost and the use of open source software and tools. Below are the main features of the prototype:

- a) It has a real-world physical process controlled by an ICS, which enables to demonstrate and analyze the impacts of cyberattacks on a real industrial control systems.
- b) The components are open-source and free as much as possible. This allows a wide range of further research.
- c) It is cost-efficient due to use of low-cost embedded systems hardware to substitute expensive industrial program logic controller (PLC) and human machine interface (HMI).