MUNI
C4E

KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems

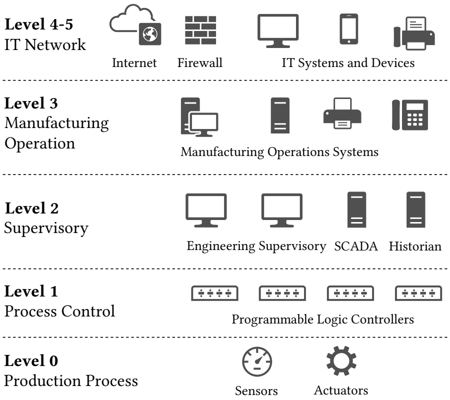
Pavel Čeleda, Jan Vykopal, Valdemar Švábenský, Karel Slavíček
celeda@ics.muni.cz

Institute of Computer Science, Masaryk University

March 14, 2020 @ SIGCSE'20, Portland, Oregon, USA

Industrial Control Systems (ICS)

- Provide **vital services** – electricity, water treatment, transportation, ...
- Used to be isolated but became **connected** with IT systems and even to the Internet.
- This connection has reduced costs and **enabled new services**.
- However, ICS assets became vulnerable to **new cyber threats**.



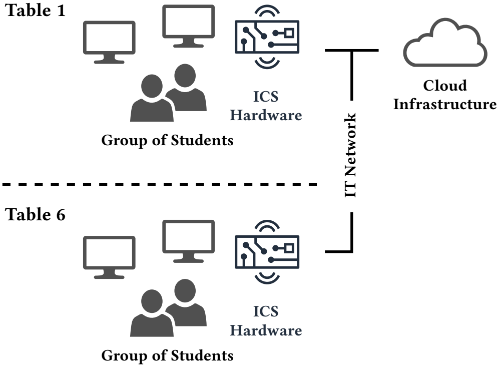
University Cybersecurity Courses

- **Fall short** in covering ICS security.
- Traditionally focus on exploiting and defending **IT assets**.
- If they feature a hands-on part, they **use virtual labs** or testbeds composed from standard IT components (desktops, servers, switches, and routers).

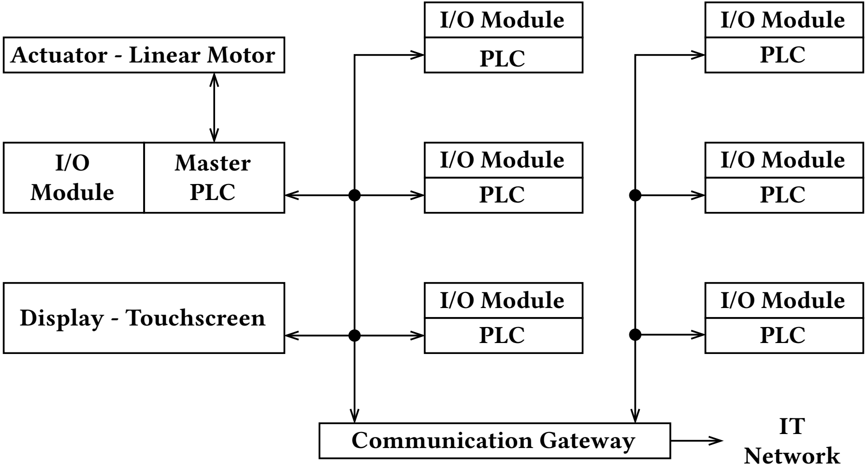
Goal of This Paper

- Share experience with the **design and acquisition of KYPO4INDUSTRY testbed** (K4I).
- Describe a **course syllabus** to deliver cybersecurity training in a simulated industrial environment to computer science students.

KYPO4INDUSTRY Testbed – K4I

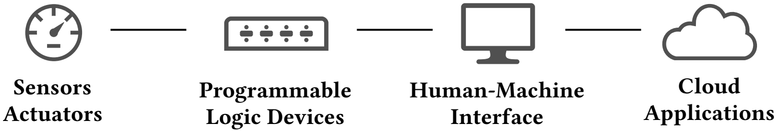


Hardware Components



Software Components

- Central testbed **controller** (virtual appliance).
- **Docker repository** for containers run at programmable logic controllers (PLC).
- **PLCs** running fully-fledged operating system (Raspbian).
- **Open-source** building blocks (PLC → Raspberry Pi).



Sensors Actuators

Programmable Logic Devices

Human-Machine Interface

Cloud Applications

ICS Cybersecurity Course at K4I Testbed

- Goal of the course: provide **undergraduate** students with an **awareness of threats** within the ICS domain via **hands-on experience**.
- Primary JTF curriculum[1] Knowledge Area covered: **System Security**, with Knowledge Units:
  - Common System Architectures,
  - System Thinking, and
  - System Control.
- Also exercises communication, presentation skills, and time management.

[1] https://cybered.hosting.acm.org/wp/

Course Format

- Spans the whole semester (**13 weeks**).
- Taught as **flipped classroom** format.
- 2-hour long **weekly lab sessions**.
- **Homework** assignments.
- Hands-on **semester project** – creating an ICS cybersecurity training game.

Course Schedule and Structure

Week	Class content	Student homework task (% of the grade)	Instructor tasks
1	Motivation, real attacks, legal issues	Prepare a presentation about an ICS attack (5%)	–
2	Student presentations of chosen attacks	Read this paper and some of the references	Grade the presentations
3	Hands-on labs on ICS testbed familiarization	Write an ICS security threat landscape report (5%)	–
4	Threat discussion, demo on ICS testbed	Write a short survey of CTF games in ICS (5%)	Grade the reports
5	Merge surveys, introduce game concepts	Select threats for your game	Grade the surveys
6	Threat modeling, storyline, consultation	Write a game draft	Check the game drafts
7	Preparing ICS part, educational objectives	Add learning outcomes and prerequisites	Check the game drafts
8	Preparing ICS and IT part	Prepare an alpha version of the game	Deploy the games
9	Dry run of the games with peers	Improve the game, submit bug reports (5%)	Review bug reports
10	Bug presentations, game improvement	Improve the game	–
11	Documentation, automation, deployment	Submit the game for presentation (50%)	Deploy the games
12	Public run of the games	Write a reflection from the public run (5%)	Oversee the event
13	Final reflections	Fix any issues that emerged in the public run (15%)	Grade the games

Experience and Lessons Learned

- Testbed components (PLCs, sensors, actuators) are **available off the shelf**.
- However, building a hardware setup that will replicate ICS in a laboratory environment is **challenging**.
- Students need a lot of guidance on how to create games with the **ICS component**.
- Otherwise, they will create games with the **traditional IT component** and do not fully exploit the capabilities of the ICS testbed.

Conclusions

- KYPO4INDUSTRY is a testbed for **teaching ICS cybersecurity in a hands-on way**.
- A novel course employs the testbed:
  - students learn about **ICS threats**,
  - develop an **educational cyber game**, and
  - exercise their **soft skills** during multiple public presentations.

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ