Analyzing Adversarial Kinetics in Industrial Production Lines

Dmytro Kryhin

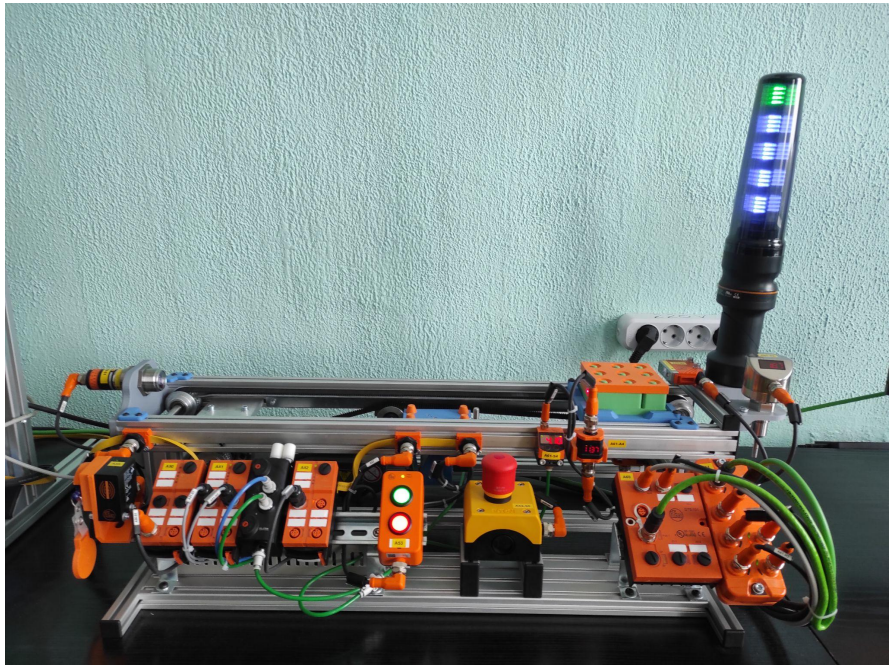
Abstract

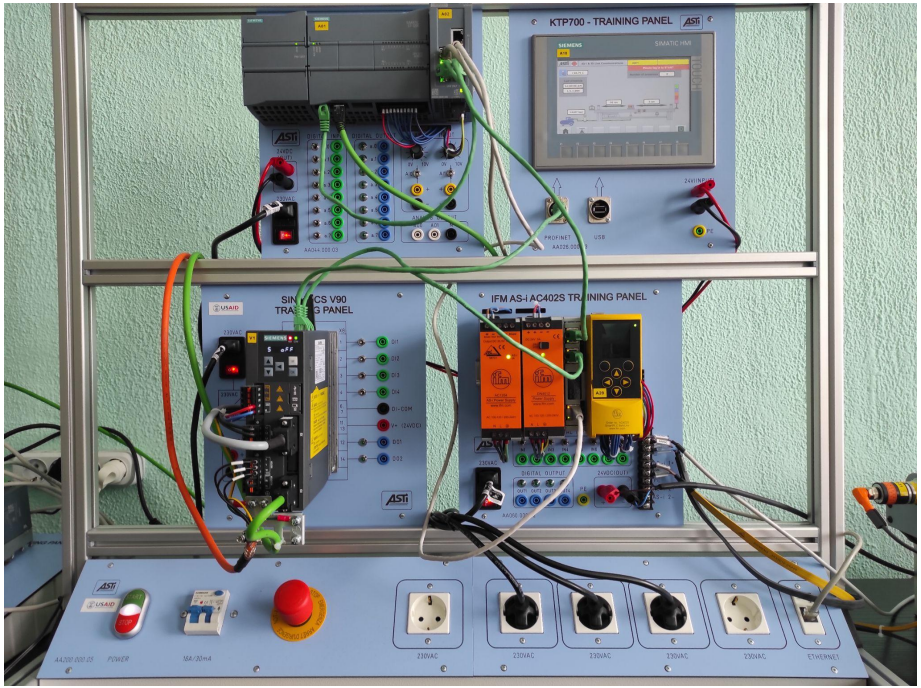
This presentation explores the work conducted in the ICS (Industrial Control Systems) security lab in NTUU Igor Sikorsky KPI , focusing on the E-Pneumatic Training System. It consists of an overview of the key components of the lab research system, discussion on the role of sensors and actuators in the operation of critical components. Additionally, we will discuss why cyberattacks on ICS are particularly dangerous, emphasizing the potential for kinetic impacts and the severe consequences that such attacks can have on real-world systems. Through this exploration, we aim to underscore the importance of robust security measures in protecting industrial environments from cyber threats.

IFM Sensors and Communications Training System

- E-Pneumatic Training System is one of the best examples of productivity and innovation for sequence logic control.
- Used in academic and industrial courses.

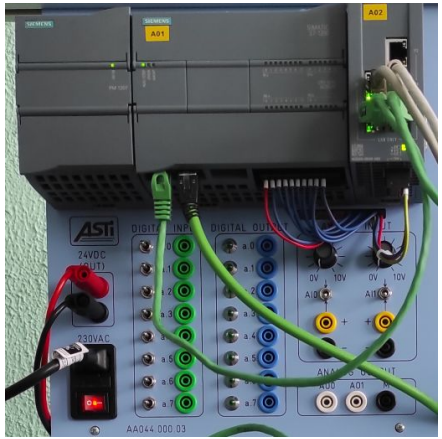
The Lab



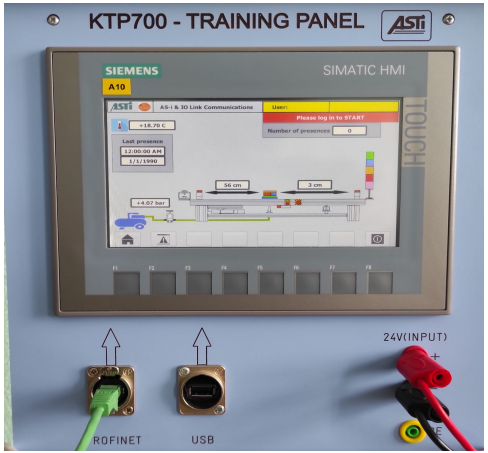


Modules

- SIMATIC S7-1200 CPU 1215C
- SIMATIC NET CSM 1277
- SIMATIC S7-1200 Power Supply Module PM1207



- SIMATIC KTP700

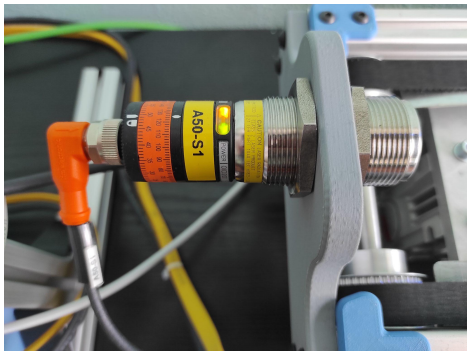


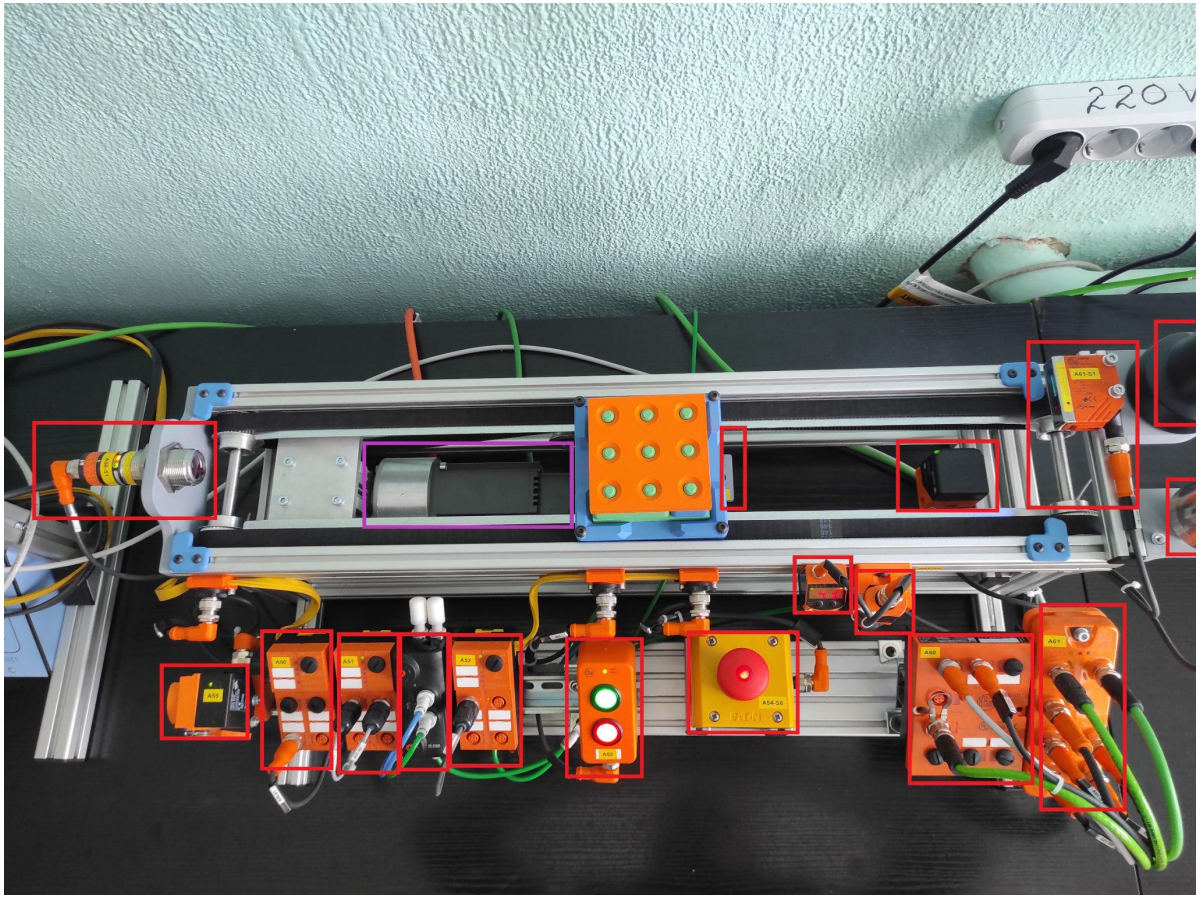
- SINAMICS V90 Training Panel
- SIMOTICS S-1FL6 Servomotor

- IFM Smart PLC Safeline AC40
- IFM Power Supply 30.5V/4A, 24V/5A

The Sensors

- Temperature transmitter
- Pressure sensor
- Photoelectronic distance sensors
- Signal Lamp
- RFID evaluation unit
- Evaluation system for analogue signals
- AL1100 IO-LINK master (PROFINET)
- AS-Interface gateway with failsafe PLC
- AS-Interface Airbox
- RFID r/w heads
- E-STOP module
- AC2388 pushbutton module
- AC5225 ClassicLine module with qmt




220V