Test bed description for Cyber4OT dataset

Krzysztof Cabaj*, Sebastian Plamowski**, Patryk Chaber**, Maciej Ławryńczuk**, Piotr Marusak**, Robert Nebeluk**, Andrzej Wojtulewicz**, Krzysztof Zarzycki**

Warsaw University of Technology,
Faculty of Electronics and Information Technology,
ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
*Institute of Computer Science
**Institute of Control and Computation Engineering
Krzysztof.Cabaj@pw.edu.pl, Sebastian.Plamowski@pw.edu.pl,
Patryk.Chaber@pw.edu.pl, Maciej.Lawrynczuk@pw.edu.pl, Piotr.Marusak@pw.edu.pl,
Robert.Nebeluk@pw.edu.pl, Andrzej.Wojtulewicz@pw.edu.pl,
Krzysztof.Zarzycki@pw.edu.pl,

Abbreviations

HMI	Human Machine Interface
ICS	Industrial Control System
IP	Internet Protocol
IT	Information Technology
OT	Operational Technology
PLC	Programmable Logic Controller
PWM	Pulse Width Modulation
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol

Test bed description

Laboratory test beds are built to mimic industrial control systems [1]. They have different objectives, e.g., evaluating selected communication standards or devices, testing vulnerabilities, and developing security mechanisms. Usually, however, these test beds are not universal, aimed deeply at a particular domain property. In our case, we develop a universal approach in which it would be possible to conduct tests of hardware resilience, communication protocols, and the control algorithms themselves. In addition, we are interested in the interface between IT and OT networks in the context of a cyber-chain attack. The developed system offers the possibility to assess vulnerability and results of attacks from the Internet in a complete cyber kill chain scheme, with end-to-end attack capabilities on network devices, communication protocols, controllers, software algorithms, and actuators. The test bed has been designed using good practices for developing Industrial Control System (ICS) [2] and focuses on factors relevant to safety [3]. Namely, our test bed has been developed taking into account several requirements:

1. The system structure should be built using commercially available components and as realistic and similar to modern industry solutions as possible.

2. The system should have a hierarchical structure with several subordinate sections and one master section.

3. Each section should have an independent visualization HMI and SCADA system for the controlled process.

4. The master section should be able to collect data from all subordinate branches for further archiving in SCADA.

5. Communication between devices should be carried out using as many protocols as possible to evaluate them from the point of view of vulnerability to attacks.

6. The key issue is to use different controlled processes and control algorithms to study the vulnerability and resilience in different configurations.

7. Remote access should be provided to the environment. Such a connection corresponds to the connection of the OT network infrastructure with the business network, which is widely practiced in industry.

The test bed has been built with a three-layer division into IT, process control and OT networks, as shown in Fig. 1. Our laboratory test bed has the same architecture shown in Fig. 2. A typical OT network's main task is process control. The workstation is enhanced with local and master computer stations with SCADA MAPS software to collect and archive data. The master iQ-R Programmable Logic Controller (PLC) from Mitsubishi Electric is responsible for managing data from slave controllers and controlling the high-speed magnetic levitation process. The slave controllers perform their local control tasks: the FX5U PLC controller from Mitsubishi Electric controls the heating-cooling station and binary control is provided by the S7–1200 PLC controller from Siemens to the FESTO station. Monitoring and diagnostics of the facilities can be performed on local HMI panels. Process data are also transferred to the iQ–R master controller. Various protocols can be used, i.e., SLMP, Profinet, Melsoft, Ethernet Simple, Modbus TCP/IP, Modbus RTU, Simens S7, marked with appropriate lines on the station diagram in Fig. 2. Communication between different devices is done using all implemented protocols. Data are exchanged through registers or individual data bits. A MAPS SCADA system collects and stores production data for further analysis. It allows real-time data collection from one or more remote locations and enables process control.

Three control processes are used: high-speed magnetic levitation process (Maglev), MPS FESTO workstation (Factory) and thermal stand (Heating-cooling). Maglev and Heating-cooling processes are continuous, while the Factory is binary, providing a wide range of feasible vulnerability-related tests.

The Maglev system is nonlinear, open-loop, unstable, time-varying, and frictionless. The basic principle of Maglev operation is to apply the voltage to an electromagnet to keep a ferromagnetic sphere levitated. The controller maintains the equilibrium state of two forces (the gravitational and electromagnetic) to keep the sphere at a desired distance from the magnet. The process is extremely fast; the controller's sample time should be as short as 1 ms.

The Factory mimics the industrial processing of parts. The workstation used has binary controls. Control is performed using valves (coils on the valves) that supply air to the actuators that set them in motion. On/off type valves are used. The measurement is performed by sensors confirming the position of the item being transported (binary signal).

In the heating-cooling, the user influences the temperature distribution in the facility through controllable fans and heaters. The test bed can be controlled via an automation system using the Modbus communication protocol. The thermal stand has six manipulated variables: Pulse Width Modulation (PWM) signals that control the fans. The process has seven measured output variables: temperatures in different parts of the system. The temperature sensors communicate internally using the OneWire bus, while current and voltage measurements use dedicated electronic devices. All inputs and output signals are available via the Modbus protocol.

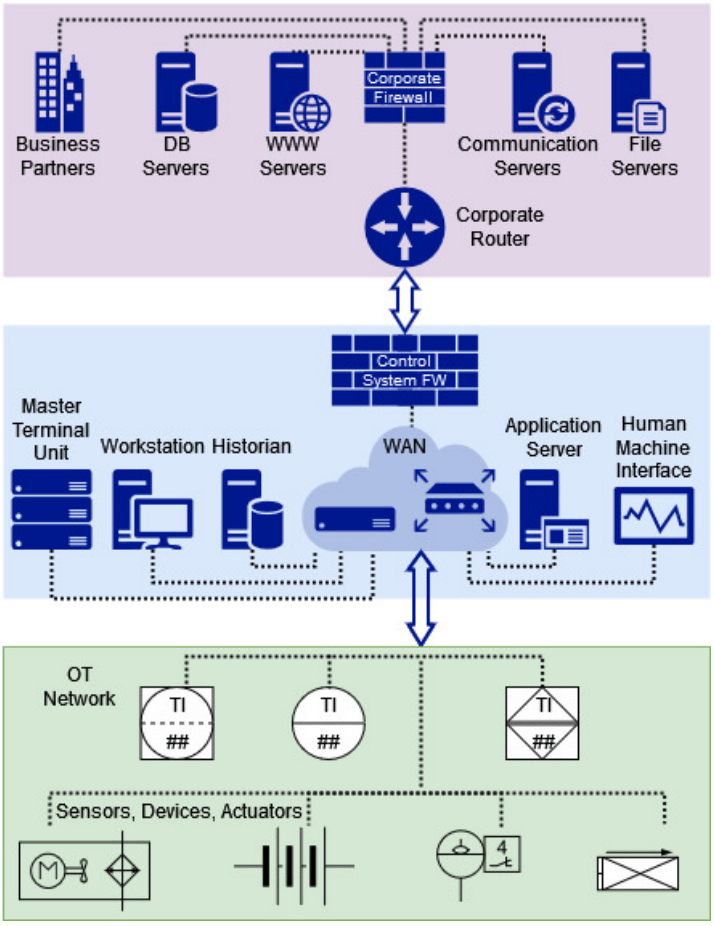

Figure 1: Three-layer structure.

Static addresses have been adopted throughout the workstation to communicate with all devices. A detailed list of addresses is shown below:

- 192.168.127. 6 – SCADA MAPS system,
- 192.168.127.10 – S7-1200 V3,
- 192.168.127.11 – S7-1200 V4,
- 192.168.127.13 – Siemens KTP Basic HMI,
- 192.168.127.20 – PLC1 (FX5U),
- 192.168.127.21 – PLC2 (FX5U),
- 192.168.127.23 – Mitsubishi GOT1 HMI,
- 192.168.127.24 – Mitsubishi GOT2 HMI,
- 192.168.127.30 – iQR (standard),
- 192.168.127.31 – iQR (Profinet),
- 192.168.127.33 – Mitsubishi GOT3 HMI,
- 192.168.127.100 – Industrial switch.

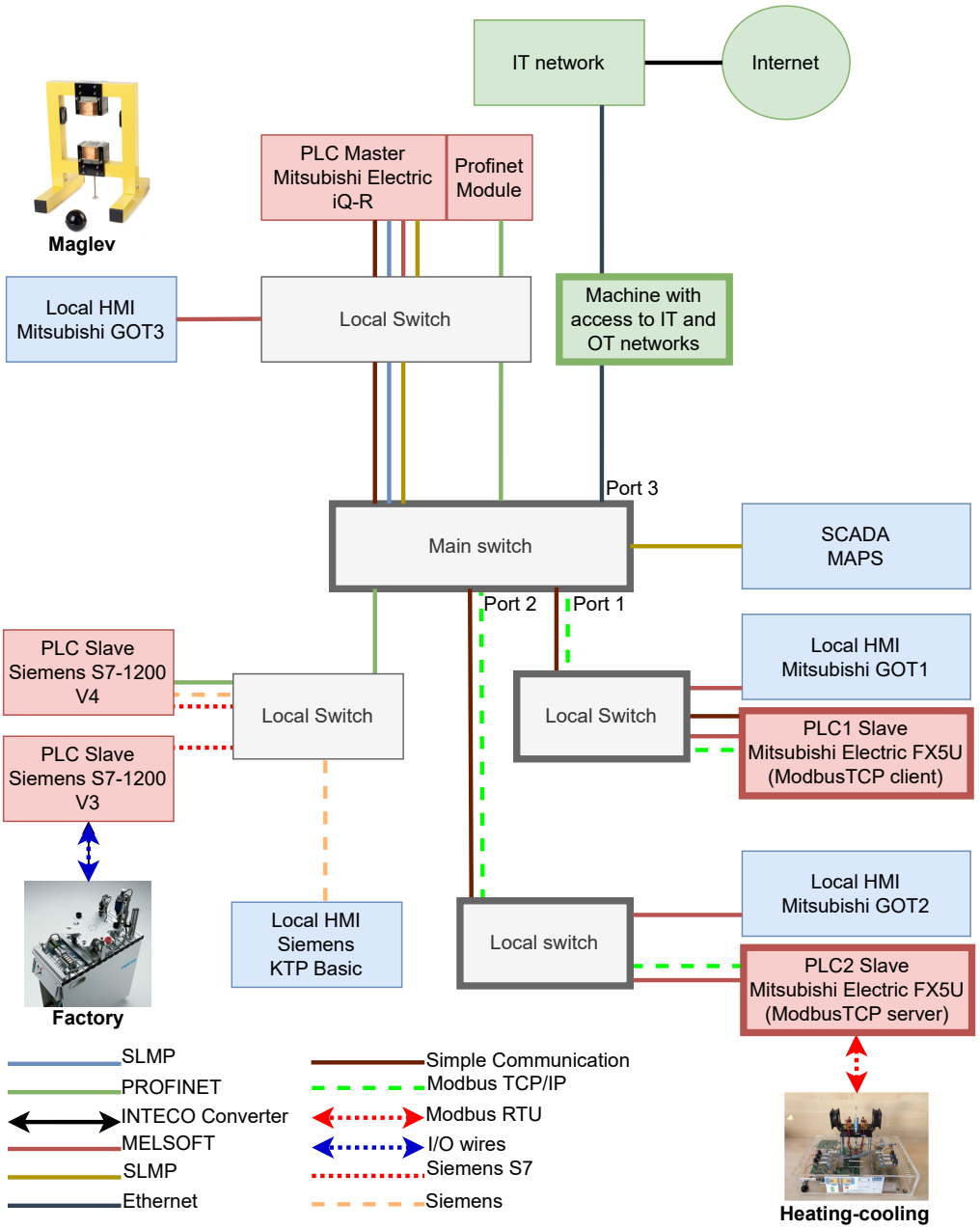

Figure 2: The laboratory test bed diagram.

References

[1] Mauro Conti, Denis Donadel, and Federico Turrin. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, 23:2248–2294, 2021.

[2] Uchenna P. Daniel Ani, Jeremy M. Watson, Benjamin Green, Barnaby Craggs, and Jason R. C. Nurse. Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. *Journal of Cyber Security Technology*, 5:71–119, 2021.

[3] Benjamin Green, Richard Derbyshire, William Knowles, James Boorman, Pierre Ciholas, Daniel Prince, and David Hutchison. ICS testbed Tetris: Practical building blocks towards a cyber security resource. In *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20)*. USENIX Association, August 2020.