Industrial Security Testbeds

Open-Source Platforms for ICS Security Training and Research

OT Security Learning Series

Document 750 | February 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Industrial security testbeds provide controlled environments for learning, researching, and testing security techniques on Industrial Control Systems (ICS) without risking production systems. These platforms range from fully virtual solutions to physical hardware setups, enabling hands-on experience with real industrial protocols and attack scenarios.

Understanding ICS security requires practical experience with industrial protocols, control systems, and attack techniques. However, access to real industrial equipment is often limited due to:

- **High costs** – Industrial PLCs and SCADA systems are expensive
- **Safety concerns** – Testing on production systems can cause physical damage
- **Availability** – Industrial environments are not easily accessible for training
- **Complexity** – Setting up realistic environments requires specialized knowledge

Security testbeds address these challenges by providing safe, accessible, and often free platforms for developing ICS security skills.

2 Testbed Categories

Industrial security testbeds can be categorized based on their deployment model:

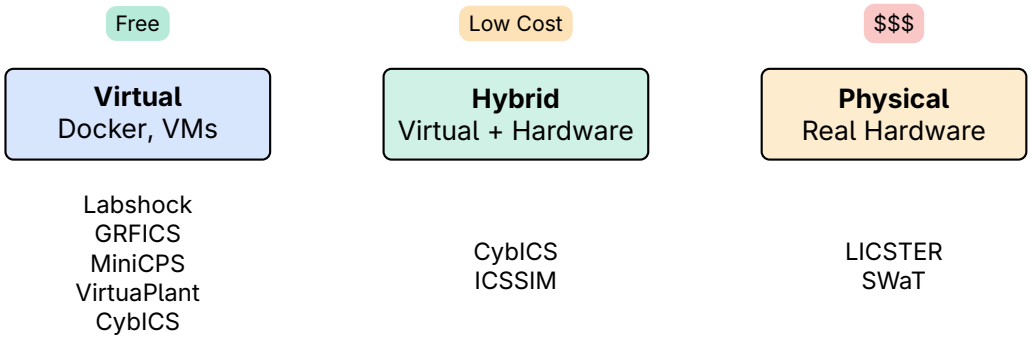

Figure 1: Testbed deployment categories and cost implications

2.1 Virtual Testbeds

Virtual testbeds run entirely in software using Docker containers or virtual machines. They offer:

- Zero hardware cost
- Quick deployment and teardown

- Easy sharing and reproducibility
- Limited physical process realism

2.2 Physical Testbeds

Physical testbeds use real hardware components and provide:

- Realistic timing and behavior
- Experience with actual industrial equipment
- Better understanding of physical consequences
- Higher cost and maintenance requirements

2.3 Hybrid Testbeds

Hybrid solutions combine virtual environments with optional physical hardware integration, offering flexibility between cost and realism.

3 Testbed Comparison

The following table compares major open-source ICS security testbeds:

Testbed	License	Cost	Type	Protocols
CybICS	MIT	Free	Virtual/Physic	Modbus, OPC-UA, S7comm, DNP3, EtherNet/IP
Labshock	Proprietary	Free (limited)	Virtual	Modbus, S7comm
GRFICSv3	GPL	Free	Virtual	Modbus, EtherNet/IP
LICSTER	MIT	€500	Physical	Modbus
MiniCPS	MIT	Free	Virtual	Modbus, EtherNet/IP
VirtuaPlant	MIT	Free	Virtual	Modbus
DVCP	Academic	Free	Virtual	Custom
ICSSIM	Open Source	Free	Virtual	Modbus, DNP3

Table 1: Testbed comparison overview

4 Detailed Testbed Descriptions

4.1 CybICS

Key Point

CybICS is a comprehensive open-source training platform for ICS security with support for multiple industrial protocols and flexible deployment options.

Repository: https://github.com/mniedermaier/CybICS

Key Features:

- Physical process simulation (gas pressure control system)
- Multiple protocol support: Modbus TCP, OPC-UA, S7comm, DNP3, EtherNet/IP
- 13+ hands-on training modules
- Integrated CTF challenges
- Web interface with real-time statistics and network monitoring
- Browser-based VNC access to Kali Linux and engineering workstation

Deployment Options:

- **Virtual:** Docker Compose environment
- **Physical:** Raspberry Pi + STM32 microcontroller setup

Use Cases: Education, penetration testing training, security research, CTF competitions.

4.2 Labshock

Repository: https://github.com/zakharb/labshock

> **Warning**
>
> Labshock is proprietary software with a limited free tier. It is not fully open source. The free version has restrictions on features and usage.

Key Features:

- Practical OT security laboratory environment
- Real industrial protocols and telemetry
- Built-in ELK Stack for log analysis
- Pentest Fury offensive module for ICS/OT networks
- Pre-configured Kibana dashboards

Requirements:

- Minimum: CPU 2 cores, 2GB RAM, 10GB storage
- Recommended: CPU 4 cores, 8GB RAM, 20GB storage
- Docker installation required

Use Cases: Universities, OT Red/Blue teams, SIEM rule development and testing.

4.3 GRFICS (Graphical Realism Framework for ICS)

Repository: https://github.com/Fortiphyd/GRFICSv2 (v2)
Repository: https://github.com/mrideout/GRFICSv3 (v3)

Information

GRFICS uses Unity 3D game engine graphics to visualize the physical impact of cyber attacks on industrial processes, making it easier to understand attack consequences.

Architecture (GRFICSv2):

- 3D simulation VM (Unity-based visualization)
- Soft PLC VM (OpenPLC)
- HMI VM (AdvancedHMI)
- pfSense firewall VM
- Workstation VM (attack platform)

GRFICSv3 Changes:

- Removed pfSense VM
- Upgraded workstation to Ubuntu 20.04 with pre-installed attack tools
- Merged ICS and DMZ networks

Simulated Process: Chemical reactor with mixing tank, maintaining safe operation parameters.

Attack Scenarios: Command injection, man-in-the-middle, buffer overflows.

4.4 LICSTER (Low-cost ICS Security Testbed)

Repository: https://github.com/thainnos/LICSTER

Warning

LICSTER requires purchasing physical hardware (approximately €500) but provides the most realistic hands-on experience with actual industrial components.

Hardware Components:

- Multiple Raspberry Pi boards
- Physical I/O modules
- Network switches
- Optional 3D-printed enclosure

Features:

- Real hardware for realistic timing behavior

- Pre-built attack scenarios (DoS, flooding, replay)
- Ready-to-use SD card images
- Detailed assembly instructions

Target Audience: Students, researchers, and anyone wanting hands-on experience with physical ICS components.

4.5 MiniCPS

Repository: https://github.com/scy-phy/minicps

MiniCPS is a framework for Cyber-Physical Systems real-time simulation built on top of Mininet.

Features:

- Physical process simulation
- Control device emulation
- Network emulation using Mininet
- Support for Modbus/TCP and EtherNet/IP
- Python 3.6 based

Use Cases: Academic research, network security experiments, CPS simulation.

4.6 VirtuaPlant

Repository: https://github.com/jseidl/virtuaplant

VirtuaPlant adds real-world control logic to basic PLC simulators, combined with a 2D physics engine for visualization.

Features:

- GUI visualization of control processes
- Written entirely in Python
- Modular design for different plant types
- Initial release: bottle-filling factory with Modbus

Tip

VirtuaPlant is archived but remains a useful learning resource for understanding basic ICS concepts and Modbus protocol interactions.

4.7 DVCP (Damn Vulnerable Chemical Process)

Repository (TE): https://github.com/satejnik/DVCP-TE
Repository (VAM): https://github.com/satejnik/DVCP-VAM

DVCP provides realistic chemical process simulations for studying cyber-physical attacks.

Variants:

- **DVCP-TE:** Tennessee Eastman process model
- **DVCP-VAM:** Vinyl Acetate Monomer process model

Requirements:

- MATLAB/Simulink
- Process models written in C-code

Availability: Free for universities, students, and research institutions.

4.8 ICSSIM

Repository: https://github.com/AlirezaDehlaghi/ICSSIM

ICSSIM enables building virtual ICS security testbeds using Docker container technology.

Features:

- Runs on separate private OS kernels
- Realistic network emulation
- Customizable to specific needs
- Can simulate various processes (e.g., bottle filling)

5 Selecting a Testbed

Consider the following factors when choosing a testbed:

Factor	Recommendation
Budget: $0	CybICS, Labshock, GRFICS, MiniCPS, VirtuaPlant
Multiple protocols	CybICS (5 protocols), ICSSIM
3D visualization	GRFICS (Unity-based)
Physical realism	LICSTER (hardware), CybICS (hybrid option)
CTF training	CybICS (built-in challenges)
Chemical processes	DVCP-TE, DVCP-VAM
Academic research	MiniCPS, DVCP, SWaT datasets
Quick start	Labshock, CybICS (Docker)

Table 2: Testbed selection guide by use case

6 Additional Resources

6.1 Curated Lists

- **Awesome ICS Security** – Comprehensive resource list
  https://github.com/hslatman/awesome-industrial-control-system-security
- **ICS Security Tools** – Testbed and tool collection
  https://github.com/ITI/ICS-Security-Tools

6.2 Datasets

For machine learning and detection research, several testbeds provide datasets:

- **SWaT Dataset** – Secure Water Treatment attack data (iTrust)
- **HAI Dataset** – HIL-based Augmented ICS Security Dataset
  https://github.com/icsdataset/hai

7 Summary

Key Takeaways

- **Virtual testbeds** (Labshock, GRFICS, MiniCPS) offer zero-cost entry into ICS security training
- **CybICS** provides the most comprehensive protocol coverage with flexible deployment
- **LICSTER** offers the most realistic experience with actual hardware (€500)
- **GRFICS** excels at visualizing attack impact through 3D simulation
- **Most testbeds are open-source** with MIT or GPL licenses (Labshock is proprietary with limited free tier)
- Choose based on your budget, required protocols, and learning objectives

8 Further Reading

Standards and Guidelines

- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443** – Industrial Automation and Control Systems Security
  https://webstore.iec.ch/publication/7029

Resources

- **SANS ICS Security** – Training and resources
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

- **CISA ICS Resources** – Government guidance
  https://www.cisa.gov/topics/industrial-control-systems

Research Papers

- Formby, D. and Rad, R. – *Lowering the Barriers to Industrial Control System Security with GRFICS*
- Antonioli, D. et al. – *MiniCPS: A Toolkit for Security Research on CPS Networks*
- Sauer, F., Niedermaier, M. et al. – *LICSTER: A Low-cost ICS Security Testbed for Education and Research* (2019)

Part of the OT Security Learning Series