Institut für Steuerungs- und Regelungssysteme
Professur für Vernetzte Sichere Automatisierungstechnik
Univ.-Prof. Dr.-Ing. Mike Barth
Fritz-Haber-Weg 1 (Geb. 30.33), 76131 Karlsruhe

Ladder Logic and War Games: Teaching Materials for PLCs Under Siege

Bachelor- or Masterthesis

System security in computer science offers a wealth of challenges (known as wargames like Figure 1) for learning purposes. Similar opportunities should also be created for dealing with security in industrial plants.

Motivation

Programmable Logic Controllers (PLCs), the digital workhorses of industrial automation, were never originally designed with cybersecurity in mind — yet they now sit at the intersection of IT and OT, often exposed to risks from both worlds.
Cyberattacks on critical infrastructure are no longer hypothetical. From Stuxnet to ransomware targeting manufacturing plants, the need for professionals who understand both operational technology and cybersecurity is more urgent than ever. However, teaching these concepts in an engaging, hands-on way remains a challenge.

Figure 1: overthewire.org

This thesis aims to design realistic, modular Red Team (attack) and Blue Team (defense) tasks on PLC systems, so that students can actively explore the vulnerabilities, defensive strategies, and real-world implications of cyber incidents — without crashing an actual factory.
In short: Why just lecture about ladder logic and firewalls when you can simulate an industrial siege and train future defenders on the front lines?

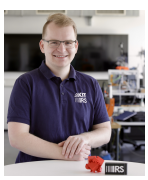
Goals

- Analyze suitable PLCs vulnerabilities, threat vectors, and typical attacker behavior for teaching purposes
- Design modular and realistic Red Team attack scenarios and corresponding Blue Team defense tasks
- Create repeatable and scalable teaching framework, allowing instructors to deploy the scenarios in labs or classrooms with minimal setup effort
- Evaluate developed scenarios with students or peers

Figure 2: Programmable Logic Controller

Interests and Helpful Prior Knowledge

- Interest in Cybersecurity and Ethical Hacking (Prior exposure to Red Team/Blue Team concepts or tools (e.g., Wireshark, Metasploit, or Snort) is helpful)
- Basic Understanding of PLCs and automation architectures
- Completion of IT/OT security seminar or willingness to work through it during the thesis



Supervisor
Marwin Madsen, M. Sc.
Build. 30.33, Room 110
Phone: 0721/608-42642
marwin.madsen@kit.edu

Thesis: Bachelor or Master
Date of Announcement: 08.08.2025
Tags: *Security Lab, Industrial Control Systems, Teaching*