# INDUSTRIAL SIMULATION ENVIRONMENT WITH OPEN PLC

DAMIAN ATLSS, CHARLOTTE GLUTTING

Cybersecurity Exam

# AGENDA OVERVIEW

01

OUR GOALS

02

DESIGN INDUSTRY CASE

03

INDUSTRY COMPONENTS SIMULATION

04

INFRASTRUCTURE SETUP

05

PROJECT SIMULATION

06

CYBERATTACKS

07

RESULTS

08

SOURCES

# OUR GOALS

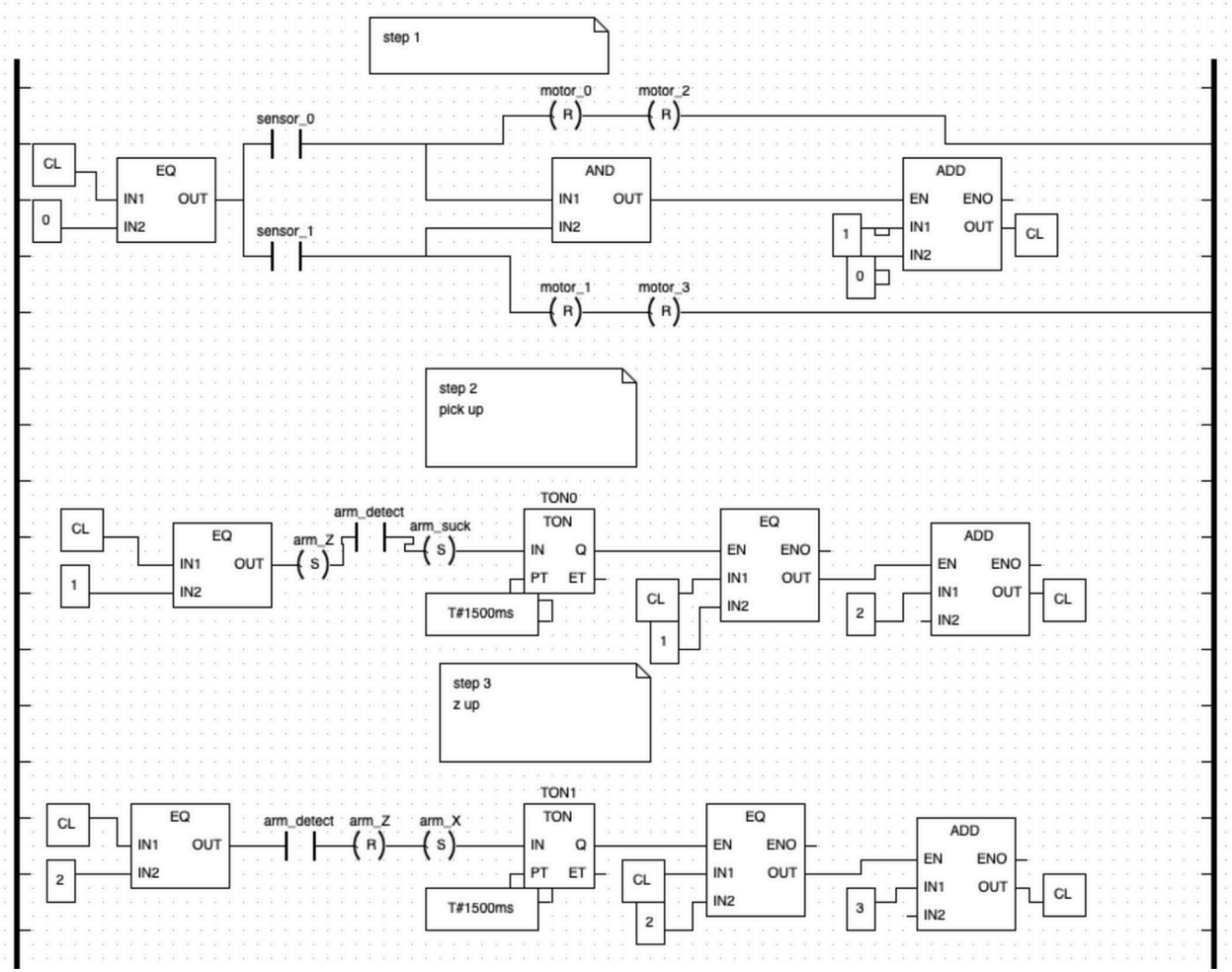
- **Simulation of Industrial Environment and Components**:
  - Design and implement a mini-industrial infrastructure to simulate an assembly station.
  - Integrate components like OpenPLC, Factory I/O, and ScadaBR.

- **Containerization with Docker**:
  - Use Docker to containerize the simulation to ensure isolation and portability.

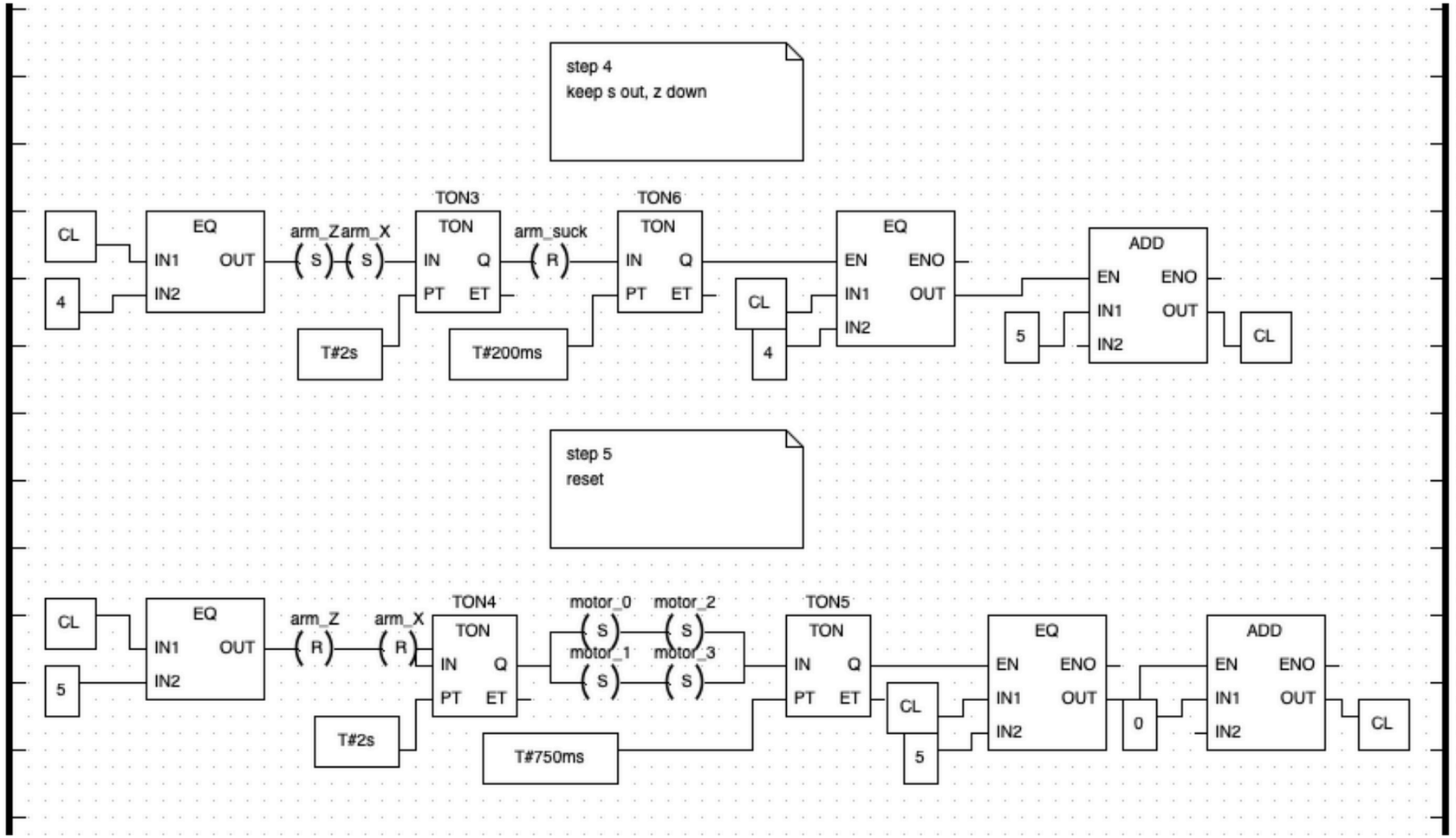
- **Automation with Terraform**:
  - Implement Terraform to automate the provisioning of the infrastructure and enable reproducibility across different deployments.

- **Security Evaluation**:
  - Evaluate the security of the simulated industrial environment by performing various cyberattacks.

# DESIGN INDUSTRY CASE



# DESIGN INDUSTRY CASE



# INDUSTRY COMPONENTS SIMULATION

## OPEN PLC

- Open-source platform for Programmable Logic Controllers (PLCs).
- Designed for simulating and controlling industrial automation components.
- **OpenPLC Runtime**: Executes PLC programs and handles real-time industrial control and simulation.
- **OpenPLC Editor**: Provides a user-friendly interface to create and edit PLC programs.

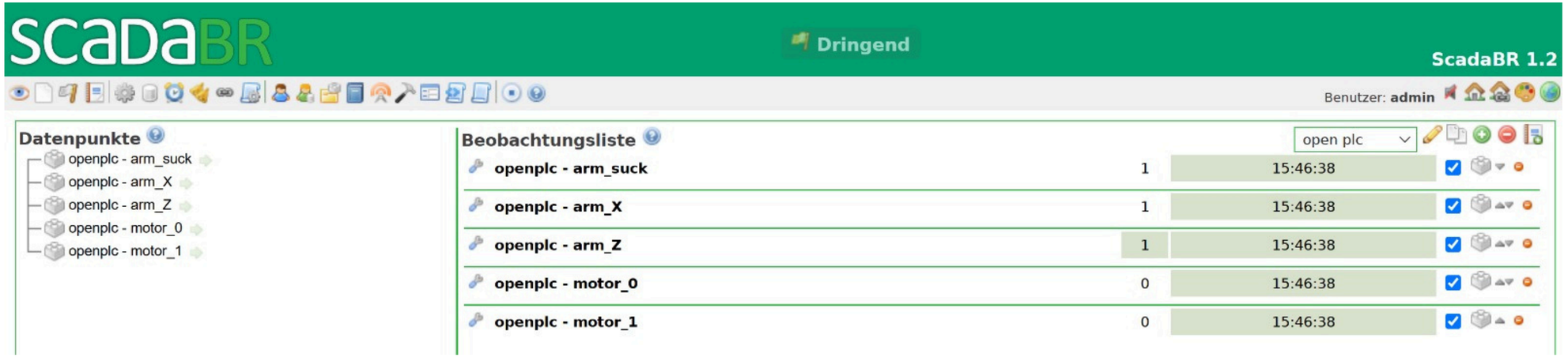
## FACTORY I/O

- Provides a dynamic 3D simulation environment for testing PLC programs.
- Complements OpenPLC for a full simulation and control workflow.

# INDUSTRY COMPONENTS SIMULATION

## SCADA BR

- Open-source Supervisory Control and Data Acquisition (SCADA).
- Serves as the Human-Machine Interface (HMI) for monitoring and controlling industrial processes.
- Provides a user-friendly interface to monitor real-time data.



# INFRASTRUCTURE SETUP

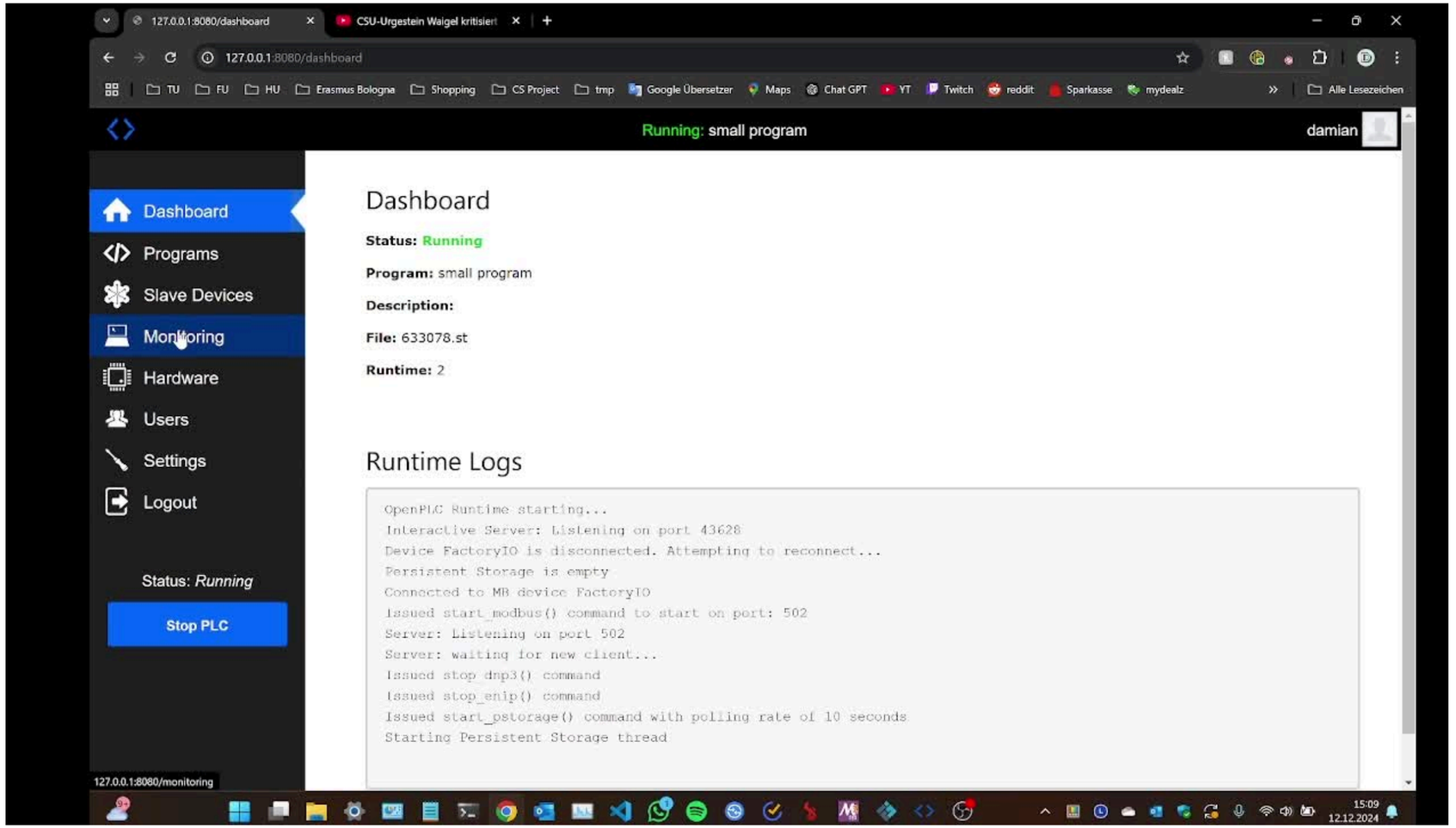
## CONTAINERIZATION AND NETWERK


- Provides isolated containers for applications and their dependencies.
- Network ensures containers can communicate with each other.
- Use Cases in Our Project: Running OpenPLC Runtime and ScadaBR and simulating cyberattacks.

## INFRASTRUCTURE AS CODE


- For automating resource management.
- Used to provision Docker components.
- Simplifies Docker infrastructure management.
- Enhances scalability and reproducibility of our project environments.

# PROJECT SIMULATION



# CYBERATTACKS

- **DDoS (Distributed Denial of Service)**:
  - Overwhelms the OpenPLC system with excessive traffic to cause disruptions in normal operations and make it unresponsive to legitimate requests.

- **HTTP Flood**:
  - Targets the OpenPLC web interface by simulating a large number of login attempts to prevent legitimate users from accessing the system.

- **MITM (Man-in-the-Middle)**:
  - Intercepts and manipulates communication between OpenPLC and ScadaBR to allow attackers to alter data or inject malicious commands without detection.

- **Modbus Flooding**:
  - Exploits the Modbus communication protocol by sending a flood of illegitimate requests to the OpenPLC system to disrupt its ability to process valid commands and responses.

# RESULTS

- **Simulation Success**:
  - Successfully simulated an assembly station integrating OpenPLC, Factory I/O, and ScadaBR.
  - Utilized two versions of OpenPLC: one running locally and another in Docker containers.

- **Containerization with Docker achieved**:
  - Docker used to containerize all components, ensuring isolation and portability.
  - Docker networking enabled seamless communication between OpenPLC and ScadaBR.

- **Automation achieved**:
  - Terraform fully automated infrastructure provisioning, ensuring consistency and reproducibility.

- **Security Testing Outcome**:
  - Conducted DDoS, HTTP Flood, MITM, and Modbus Flooding attacks.
  - Attacks were unsuccessful because of their simple nature and  to robust network configurations.

# SOURCES


- https://docs.factoryio.com, 13.12.24.
- https://github.com/ScadaBR, 13.12.24.
- https://docs.docker.com/get-started/docker-overview/, 13.12.24.
- https://docs.docker.com/engine/network/, 13.12.24.
- https://www.cloudflare.com/de-de/learning/ddos/ddos-attack-tools/how-to-ddos/, 13.12.24.
- https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack.com, 13.12.24.
- https://dl.acm.org/doi/pdf/10.5555/2667510.2667517, 13.12.24.
- https://autonomylogic.com/docs/openplc-overview/, 13.12.24.
- https://www.terraform.io/, 13.12.24.

# THANK YOU FOR YOUR ATTENTION

Cybersecurity Exam