Zach Lavoie, Karla Daley

CPS Attack and Defense Testbed

Semester 1 August 31 2026

Project Goals

01 Create a Testbed for Industrial Programmable Logic Controllers (PLC)

02 Simulate Internal Threats to These Systems

03 Simulate External Threats to These Systems

04 Observe how attacks affect real PLC hardware

05 Detect abnormal behavior using monitoring tools

Motivation

- PLCs control real physical systems.
- Cybersecurity labs often focus only on software/network attacks.
- Our project connects hardware-level PLC control with software-level cyber security monitoring.
- The testbed provides a safe, hands-on learning environment.

Motivation - Why?

- Shows how cyber attacks affect physical controllers.
- Helps users understand PLC vulnerabilities.
- Supports cybersecurity education.
- Supports forensic research
- Supports future industrial control system security work

Approach (Key Features of the System)

Model Threats to PLCs:

- Model threats to modern PLCs
- Show where current systems can fail
- Support multiple PLC brands
- Use multiple industrial protocols
- Compare behavior across different PLC platforms

Approach (Key Features of the System)

Plug and Play Framework:

- Add and remove PLC hardware
- Test known and unknown protocols
- Connect PLCs to demo switches, readouts, and sensors

Testing of Physical and Cyber Elements:

- Observe both network effects and physical hardware effects
- Safely simulate production-like environments

Approach (Key Features of the System)

Complete Activity Monitoring:

- Record network traffic
- Analyze industrial protocols
- Log sensor readouts
- Track current PLC states
- Compare normal and abnormal activity
- Save results for later review

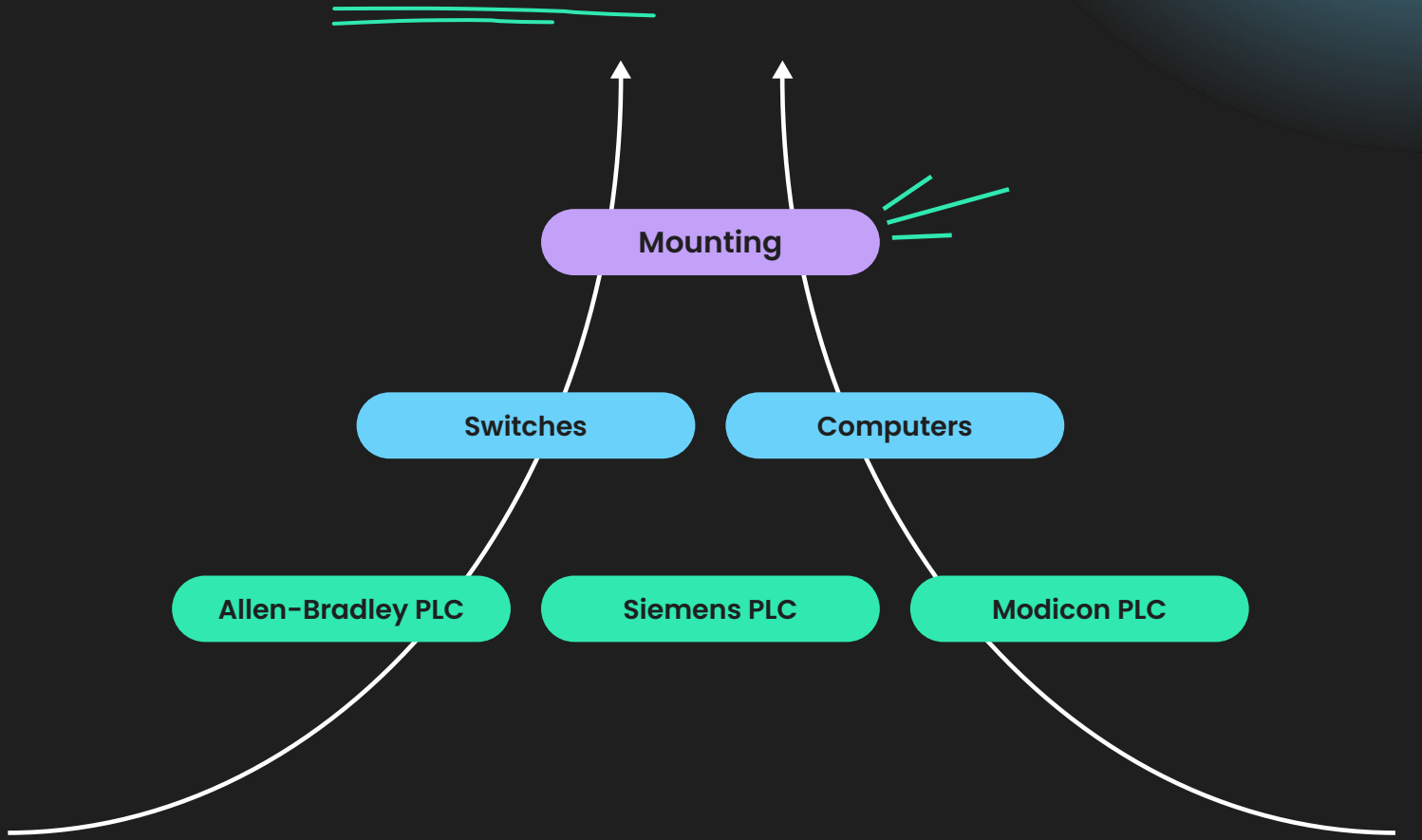
Novel Features/Functionalities

- Plug-and-play hardware support
- Repeatable attack tests
- Consistent test environment
- Comparable results across PLC brands
- Hardware sensor interception module

Algorithms and Tools

- **Front-End:** HTML, CSS, JavaScript
- **Back-End:** Python, JavaScript, Java
- **Hosting:** GitHub Pages, Docker
- **Logging:** Scapy, Wireshark, Burp Suite
- **Testing:** Python test scripts
- **Collaboration:** GitHub, Google Suite, SMS, Email
- **PLC Tools:** Studio 5000 / RSLogix, Siemens TIA Portal, Schneider EcoStruxure
- **Protocols:** EtherNet/IP, PROFINET, Modbus TCP

Hardware


Mounting
Switches
Computers
Allen-Bradley PLC
Siemens PLC
Modicon PLC

Hardware

- Allen-Bradley PLC
- Siemens PLC
- Schneider Modicon PLC
- D-Link switch
- TP-Link switch
- EGSMTPC mini computer
- 3D-printed housing
- DIN rail mounting

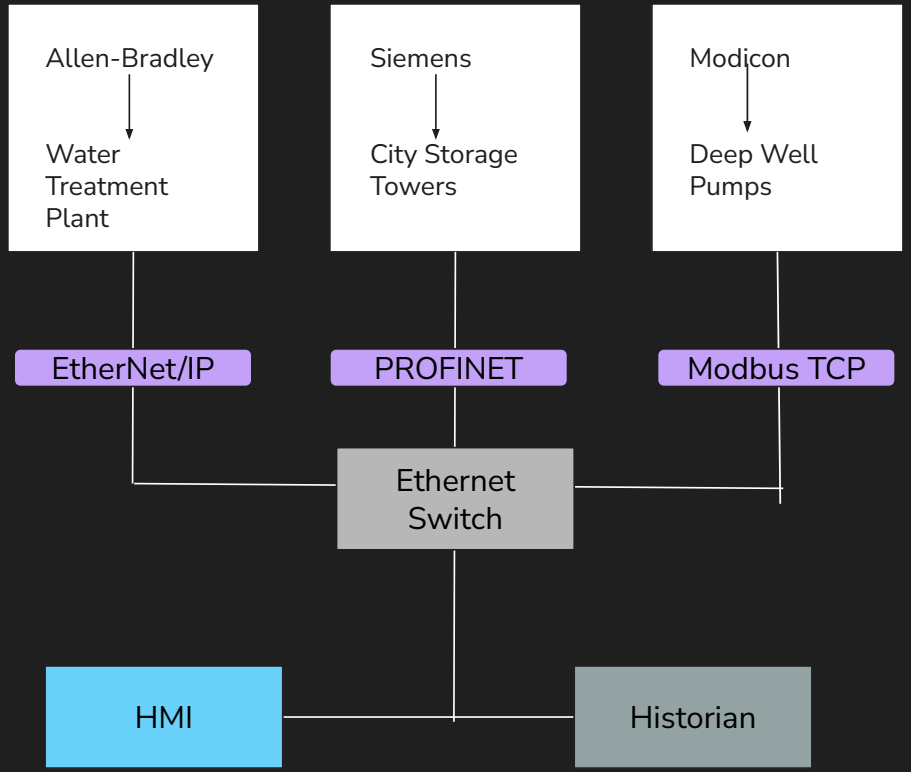
Technical Challenges

- Multi-vendor PLC communication
- HMI, historian, and network integration
- Bridging hardware/sensor security and network security
- Different PLC programming environments
- Different industrial protocols
- Correlating sensor data, PLC states, HMI output, historian logs, and network traffic

Milestones

Milestone 1

- Configure Allen-Bradley, Siemens, and Modicon PLCs
- Set up Ethernet switch and IP addressing
- Research EtherNet/IP, PROFINET, and Modbus TCP
- Create basic PLC-to-historian demo
- Select collaboration tools
- Create requirement document
- Create design document
- Create test plan



Milestones

Milestone 2

- Implement one internal attack vector
- Demo and test internal attack
- Connect sensors to all three PLCs
- Test PLC sensor communication
- Observe PLC state changes
- Begin logging sensor, PLC, historian, and network data

Milestone 3

- Implement second attack vector
- Demo and test external attack
- Implement ESP32 hardware attack vector
- Demo and test ESP32-based sensor manipulation
- Log PLC, sensor, HMI, historian, and network response
- Prepare final demo and documentation

Task Matrix for Milestone 1

Task	Zach	Karla
Compare and select Technical Tools	Network/protocol tools for EtherNet/IP, PROFINET, Modbus TCP; Ethernet switch/network configuration tools	PLC programming/configuration tools for Allen-Bradley, Siemens, and Modicon; historian/HMI-related tools
“Hello World” demos	Set up software/network side of PLC connection-chain demo; verify PLC communication over the switch	Set up hardware side of connection-chain demo; configure PLC and verify basic PLC input/output operation
Resolve Technical Challenges	Configure PLC network protocols, IP addressing, switch connections, and communication between PLCs and historian/HMI computer	Configure the three PLCs; understand digital/analog I/O and how sensors connect and operate

=

Task Matrix for Milestone 1

Compare and select Collaboration Tools	GitHub/version control and communication tools	Documents/presentations, Whiteboard/Sticky Notes, and task organization
Requirement Document	Write **50%**	Write **50%**
Design Document	Write **50%** — network architecture, protocols, IP addressing, switch connections	Write **50%** — PLC setup, I/O mappings, sensors, historian/HMI configuration
Test Plan	Write **50%** — network connectivity, protocol communication, historian/HMI tests	Write **50%** — PLC operation, I/O, sensor, hardware tests

=

Questions?