

# **Project Plan**

## **Basic Cyber Physical System Attack and Defense Testbed**

**Team Members:** Karla Daley, [kdaley2024@my.fit.edu](mailto:kdaley2024@my.fit.edu)

Zach Lavoie, [zlavoie2023@my.fit.edu](mailto:zlavoie2023@my.fit.edu)

**Faculty Advisor:** Sneha Sudhakaran, [ssudhakaran@fit.edu](mailto:ssudhakaran@fit.edu)

**Client:** Sneha Sudhakaran, College of Engineering and Science

**[Date\(s\) of Meeting\(s\) with the Client for Developing this Plan](#)**

## **Project Goals**

Create a testbed for Industrial Programmable Logic Controllers (PLC) to simulate internal and external threats to these systems.

## **Project Motivation**

The motivation for this project is the need for a safe, hands-on environment that connects hardware-level industrial control with software-level cybersecurity monitoring and defense. PLCs are used to control real physical systems in industries such as manufacturing, water treatment, energy, transportation, and critical infrastructure. However, many cybersecurity labs focus primarily on software, networks, or simulated attacks, without demonstrating how those attacks affect real industrial hardware and physical processes.

The project supports cybersecurity education, forensic research, and future work in industrial control system security.

The testbed allows students and researchers to safely study how cyberattacks affect physical controllers and how defense tools can detect abnormal behavior.

## Approach (key features of the system)

**Model threats to PLCs:** This testbed will allow users to see how threat actors approach modern industrial Programmable Logic Controllers. Watching this behavior helps users better understand where current systems fail & how they can be improved to achieve higher reliability & greater tolerance to attack.

**Compatibility with multiple PLC brands:** In modern production environments, no single PLC brand is used everywhere. To make this testbed practical, the user will be able to use multiple controllers & protocols simultaneously to model possible networks.

**Plug & Play framework:** With multiple brands of Programmable Logic Controllers operating on different protocols, configuration overhead must be managed. These users will be able to add new PLCs to known & even unknown protocols, allowing new hardware to be brought in & tested.

**Test both physical & cyber elements:** The user will be able to set up Programmable Logic Controllers in a working configuration. They will be connected to physical demo switches, readouts, & sensors, enabling safe simulation of actual production environments. This setup allows for observation of exactly what an attack does to both the network & more than that, the actual industrial machinery being targeted.

**Complete activity monitoring:** To enable a comprehensive study of the results of this test bench, meticulous logs of all activity will be recorded for the user to review. These will include all network traffic, protocol analysis, & reported sensor readouts with current PLC states.

## Novel Features/Functionalities

**Plug & Play framework hardware support:** The user will be able to add & remove hardware from the testbed, allowing for numerous configurations across protocols & companies to be tested in the same environment.

Each supported PLC will include documented:

- network configuration
- protocol configuration
- HMI configuration
- historian configuration
- I/O mappings
- sensor connections
- setup/testing procedures

**Repeatable Tests:** The user will be able to create attack scripts & use them to simulate the exact same attack as many times as needed to fully understand its mechanics. Once an attack script is made, it can be documented & saved to be played at any time, including in different hardware configurations.

A test can contain:

- test configuration
- PLC and protocol used
- normal system state
- attack method
- expected behavior
- observed PLC state
- HMI response
- network capture
- historian/log output
- reset procedure

That means the same experiment could eventually be run against Allen-Bradley + EtherNet/IP, Siemens + PROFINET & Modicon + Modbus TCP to compare behavior.

**Consistent & Comparable Test Environment:** The user will have access to a consistent test environment, regardless of which Programmable Logic Controllers are deployed. This allows the saved attack scripts to keep working & for them to yield comparable results. If the only thing that changed was the hardware or protocol, the user can see the advantages & disadvantages of different configurations.

### **Hardware Sensor Interception Module:**

Physical Sensor/Switch → Interception Module → PLC Input

The module allows the team to selectively interrupt or alter the signal before it reaches the PLC while leaving the industrial PLC hardware untouched.

**Push Button → Relay → PLC Digital Input**

controlled by:

**Arduino Nano / ESP32**

This demonstrates a hardware-level denial-of-service/sensor manipulation.



# Algorithms and Tools

**Front-End:** HTML, CSS, JavaScript.

**Back-End:** Python, JavaScript, Java.

**Hosting & Deployment:** GitHub Pages, JS, Docker.

**Logging:** Scapy, Wireshark, Burp Suite

**Testing & Debugging:** Python test scripts

**Collaboration & Organization:** GitHub (version control), Sticky Notes & Whiteboard, SMS, email (communication).

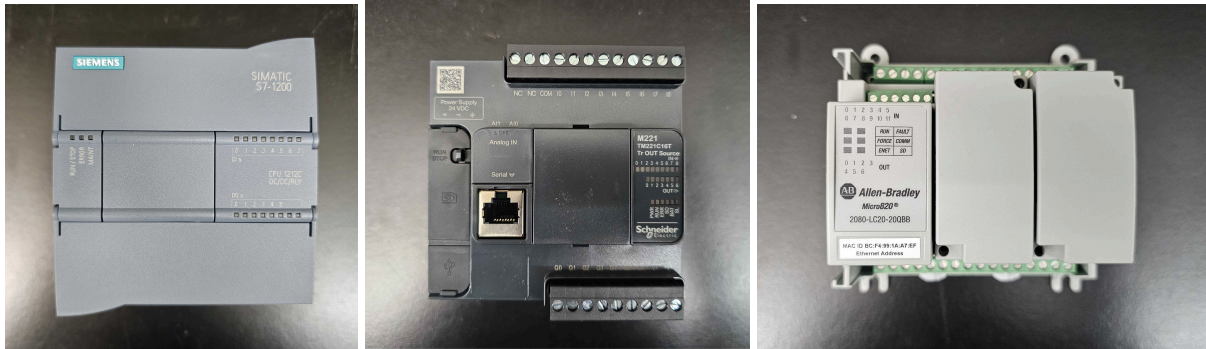
**PLC Programming & Configuration:** Studio 5000 / RSLogix for Allen-Bradley, Siemens TIA Portal / STEP 7, Schneider EcoStruxure Machine Expert Basic / SoMachine Basic.

**Industrial Communication Protocols:** EtherNet/IP, PROFINET, Modbus TCP.

**PLC Control Logic:** Ladder Logic, Boolean logic, timers, threshold detection, state-based control, alarm conditions, and sensor-state evaluation.

# Hardware

**Programmable Logic Controllers:** Siemens PLC, Schnieder Electric PLC, Allen-Bradly PLC



**Switches:** D-Link Switch, tp-Link Switch



**Computers:** EGSMTPC mini computer



**Mounting:** 3D Printed housing, DIN rail

# Technical Challenge

## **Challenge 1 — Multi-Vendor PLC Communication**

We need to integrate PLCs from Allen-Bradley, Siemens, and Modicon that use different programming environments and industrial communication protocols. The team currently has limited experience configuring EtherNet/IP, PROFINET, and Modbus TCP simultaneously in a single system.

## **Challenge 2 — HMI, Historian, and Network Integration**

We need to determine how to create an HMI and historian that can receive and display information from multiple PLC platforms while also capturing and analyzing traffic.

## **Challenge 3 — Bridging Hardware/Sensor Security and Network Security**

We need to determine how to safely, reversibly, and measurably perform physical manipulation of sensors and PLC I/O while correlating these physical events with PLC states, HMI output, historian records, and network traffic.

## **Milestone 1 (Sep 28): Initial Setup and Technical Evaluation**

### **Compare and select technical tools**

PLCs have already been selected

### **Small ("hello world") demo(s)**

Prepare a bare bone system of each PLC device talking to the Historian.

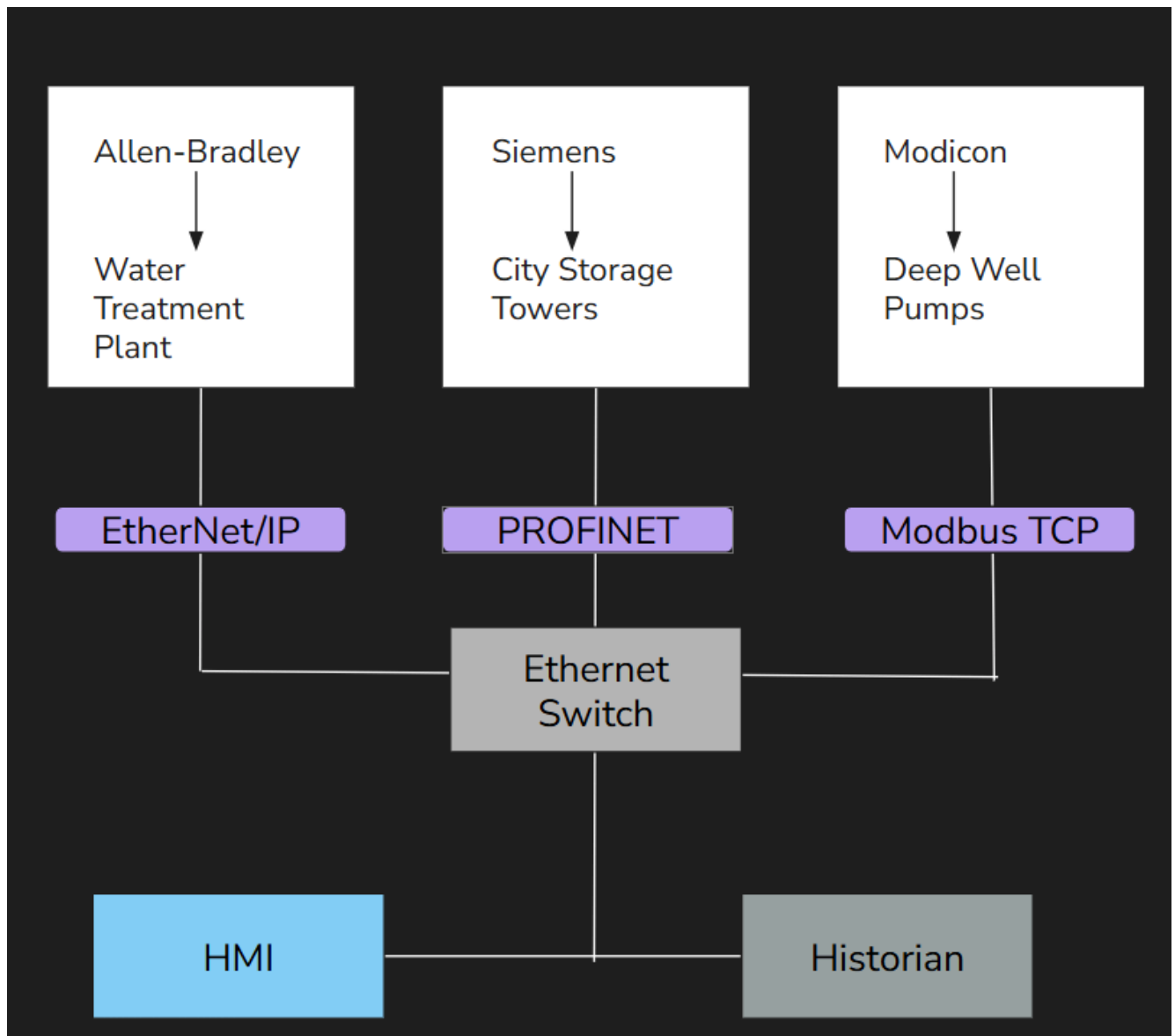
### **Compare and select collaboration tools for software development, documents/presentations, communication, task calendar**

Google Suite will be utilized, GitHub

### **Create Requirement Document**

### **Create Design Document**

### **Create Test Plan**



## **Milestone 2 (Oct 26): Feature Implementation and Testing**

- Implement, demo and test one attack vector - Internal
- Implement, demo and test Sensors that are connected to the three PLCs

## **Milestone 3 (Nov 23): Final Implementation and Launch Prep**

- Implement, demo and test second attack vector - External.
- Implement, demo and test Hardware attack vector using an ESP32



## Task Matrix for Milestone 1

| Task                                          | Zach                                                                                                                          | Karla                                                                                                    |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Compare and select Technical Tools</b>     | 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 |
| <b>“Hello World” demos</b>                    | 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 |
| <b>Resolve Technical Challenges</b>           | 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              |
| <b>Compare and select Collaboration Tools</b> | GitHub/version control and communication tools                                                                                | Documents/presentations, Whiteboard/Sticky Notes, and task organization                                  |
| <b>Requirement Document</b>                   | Write <b>50%</b>                                                                                                              | Write <b>50%</b>                                                                                         |
| <b>Design Document</b>                        | Write <b>50%</b> — network architecture, protocols, IP addressing, switch connections                                         | Write <b>50%</b> — PLC setup, I/O mappings, sensors, historian/HMI configuration                         |
| <b>Test Plan</b>                              | Write <b>50%</b> — network connectivity, protocol communication, historian/HMI tests                                          | Write <b>50%</b> — PLC operation, I/O, sensor, hardware tests                                            |

Faculty: Sneha Sudhakaran  
Date: 08/31/2026

