

Zach Lavoie, Karla Daley

CPS Attack and Defense Testbed

Semester 1

October 26

2026

Milestone 2 Completion Matrix

Task	Completion %	Karla	Zach	To do
1. Demo internal network attacks	100%	50%	50%	0%
2. Set up sensor connection to all 3 PLCs	100%	50%	50%	0%
3. Finish setting up the Siemens PLC	100%	50%	50%	0%

Milestone 2 Tasks – Internal Attack

- Connected all three PLCs to the trainer for input/output testing
- Installed Kali Linux on the second computer for network access
- Allen-Bradley demonstrated an observable physical response on the trainer
- Created a modular Python logging framework for test data and PCAP capture
- Created a modular attack engine for storing and repeatedly running attack scripts

Milestone 2 Tasks – Sensor Connection

- Connected and tested potentiometers as sensors on the PLC testbed
- Used the Allen-Bradley potentiometer to represent water tank level
- Scaled the potentiometer from approximately 0–4090 to 0–100% tank capacity
- Verified sensor value changes in CCW
- Logged potentiometer changes every 0.01 seconds for later analysis

Milestone 2 Tasks – Siemens PLC & Step7

- Added the Siemens PLC to the testbed and connected it to the trainer
- Obtained and configured STEP 7 software
- Detected the Siemens PLC through the network switch
- Programmed Siemens inputs and outputs and verified changes on the trainer
- Created longer CAT6 Ethernet cables with RJ45 connectors for the expanded testbed

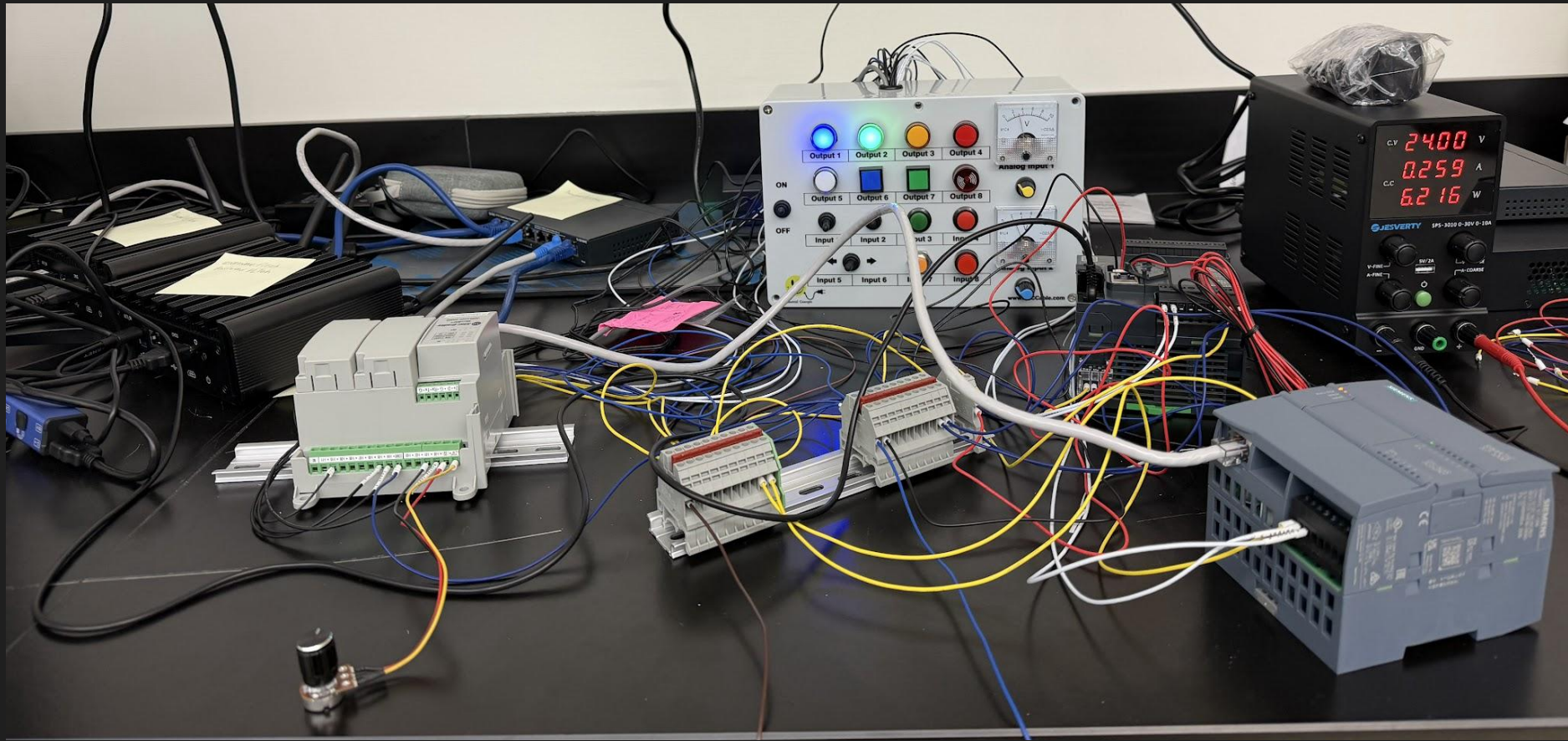
Resolved Technical Challenges

- Obtained Siemens STEP 7 access

Remaining Technical Challenges

- Network Connection for Modicon PLC with the RTU to TCP conversion

Milestone 2 Setup



Logging

```
Command Prompt
Microsoft Windows [Version 10.0.26200.9711]
(c) Microsoft Corporation. All rights reserved.

C:\Users\FloridaTech\Desktop\Logging>source .env\Scripts\activate.bat
'source' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\FloridaTech\Desktop\Logging>source .env\Scripts\activate
'source' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\FloridaTech\Desktop\Logging>.env\Scripts\activate.bat

(.env) C:\Users\FloridaTech\Desktop\Logging>python3 loggingStart.py
Connecting to PLC at 192.168.1.30...
Global tag lookup: status=Success, count=25
Discovered 25 tags from 192.168.1.30
modules.systemInfo: wrote systemInfo.json

Stopping logging modules...
modules.allenBradlyTags: wrote plcTags.jsonl
modules.netTraffic: wrote traffic.pcap
Created archive after interruption: C:\Users\FloridaTech\Desktop\Logging\archives\logs_20261025_193330.zip

(.env) C:\Users\FloridaTech\Desktop\Logging>
```

Logging

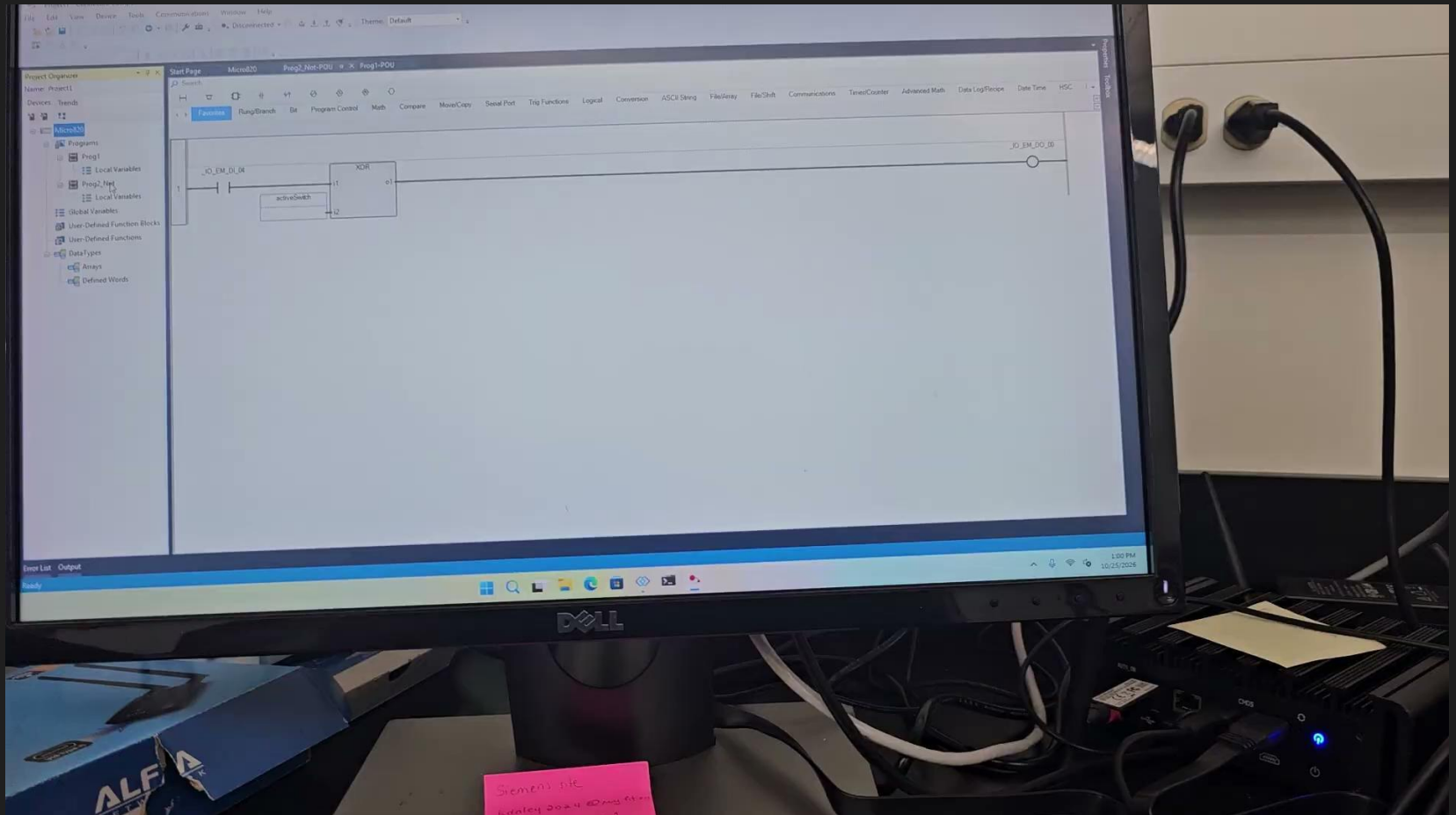
The screenshot displays three overlapping windows on a desktop background of a rocky landscape.

plcTags.jsonl (top-left): A JSON log file showing a series of events. Each event is an object with fields: "event", "plcIp", "tag", "tagCount", "timestamp", and "value". The events include "connected", "initial", and "event" for various tags like "IO_EM_AI_00", "IO_EM_AI_01", "IO_EM_AI_02", "IO_EM_AI_03", "IO_EM_AI_04", "IO_EM_AI_05", "IO_EM_AI_06", "IO_EM_AI_07", "IO_EM_AI_08", and "IO_EM_AI_09".

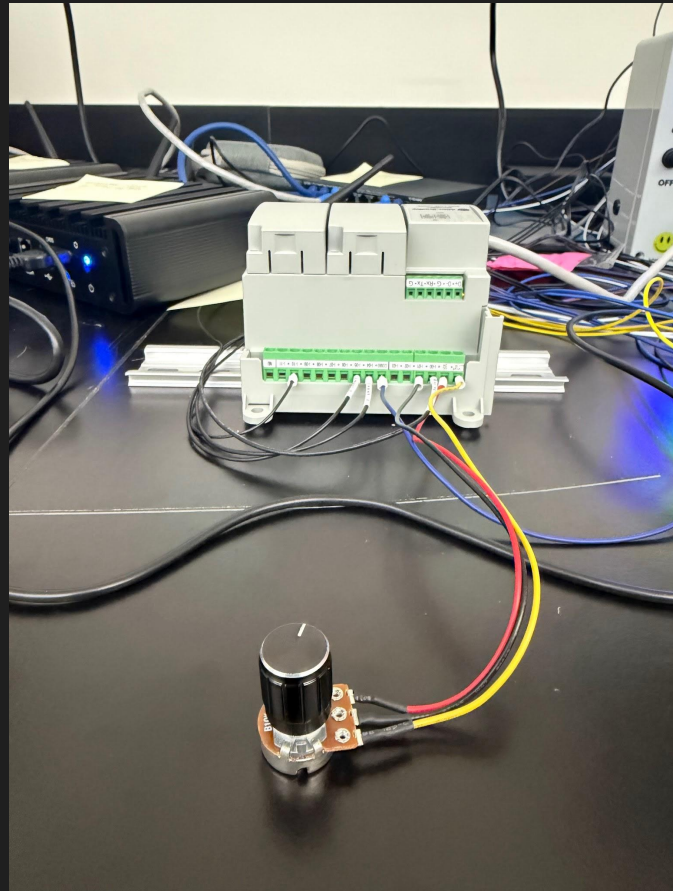
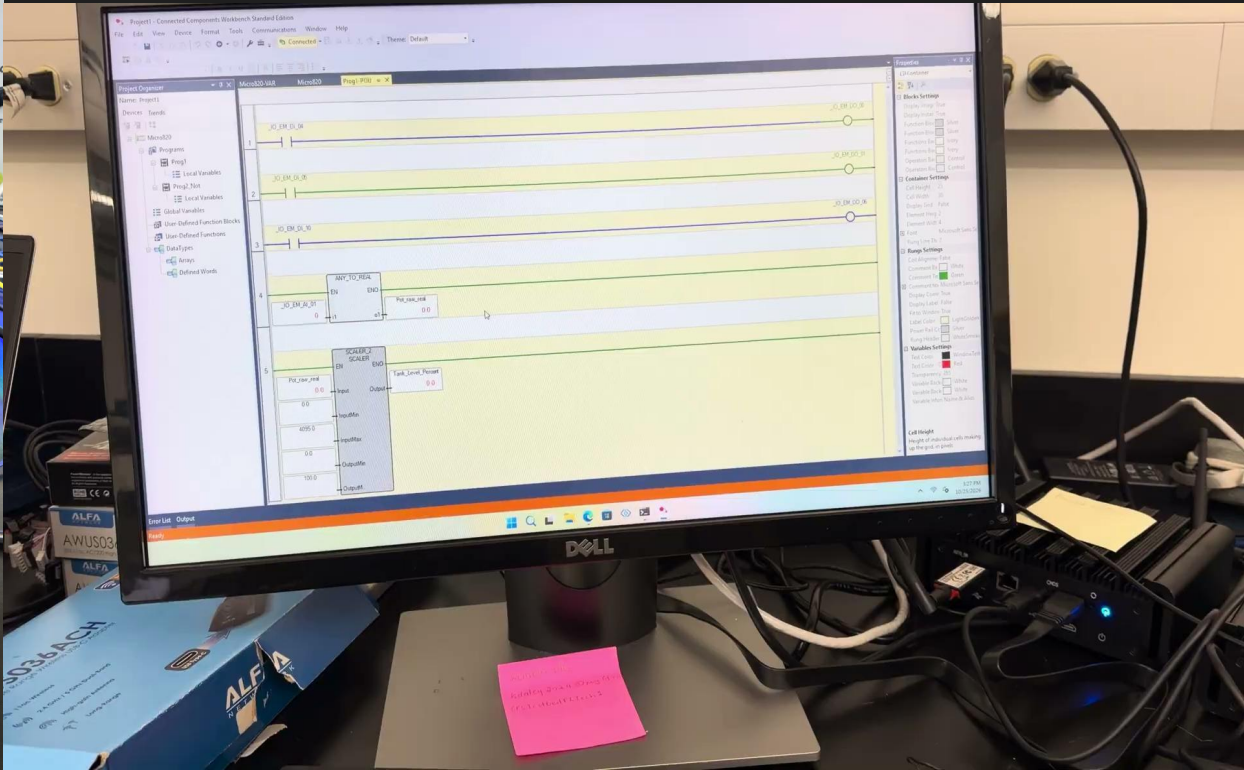
systemInfo.json (bottom-left): A JSON file containing system information. Fields include "architecture" (AMD64), "cpuCount" (4), "disk" (freeBytes: 37645160448, totalBytes: 126902857728, usedBytes: 89257697280), "homeDirectory" (C:\Users\FloridaTech), "hostname" (DESKTOP-880ISL), "macAddress" (9c:ef:d5:f7:57:cc), "networkAddresses" (10.152.11.147, 192.168.1.20, fe80::7759:c6f3:ebf7:4ef1, fe80::f0cb:27ff:8c92:eeae), "operatingSystem" (Windows), "operatingSystemRelease" (11), "operatingSystemVersion" (10.0.26200), "optionalInformation" (bootTime: 2026-10-25T16:48:17.556288+00:00, cpuCountLogical: 4).

traffic.pcap (right): A network traffic capture tool window. It shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1) is a TCP packet from 192.168.1.30 to 192.168.1.20, Seq=0, Ack=1, Win=2048, Len=0, MSS=1460. The packet details pane on the right shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

Internal Attack Demo



Allen Bradley Sensor Demo



Milestone 3 Task Matrix

Task	Karla	Zach
Complete Modicon PLC Integration	Program the Modicon PLC using the Software	Ensure the Modicon PLC can be detected and accessed over the network and through the software
Implement and Demonstrate External Attack	Configure the PLCs so the physical effects of the attack can be observed	Set up and demonstrate the external attack
Implement and Demonstrate Hardware Attack	Set up and demonstrate the hardware attack	Ensure the historian and logging system detect and record the hardware attack
Develop Allen-Bradley-Based Power Plant Test Platform	Set up sensors and wiring connections to represent components of a power plant	Network the power plant mockup so the PLCs can communicate with each other and with the historian



Questions?