

Milestone Progress Evaluation

Milestone 2

1. Project title, names, and email addresses of team members

Basic CPS Attack and Defense testbed

Karla Daley — kdaley2024@my.fit.edu

Zach Lavoie — zlavoie2023@my.fit.edu

2. Faculty Advisor

Dr. Sneha Sudhakaran - ssudhakaran@fit.edu

3. Client or user

Dr. Sneha Sudhakaran - Department of Electrical Engineering and Computer Science at Florida Institute of Technology

4. Progress of current Milestone

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%

5. Discussion of each accomplished task and obstacles

Task 1: All three PLCs were set up with their inputs and outputs connected to the trainer for testing. One obstacle we faced was that the Modicon PLC was not able to connect to the software over the network because the Modbus RTU-to-TCP module was causing interference with the connection. For programming purposes, toward the end of the milestone, we were able to get a mini USB cable and use that method to program the Modicon PLC for now. This will allow us to continue working with the PLC until we can solve the issue with the RTU-to-TCP module. This obstacle will be addressed in the next milestone. The Allen-Bradley PLC successfully demonstrated the testbed setup so that we could observe a physical outcome after an attack. As for reflashing the second computer and allowing it to see the PLCs over the network, Kali Linux was installed. Kali Linux had better driver support, so no additional configuration was needed for it to detect the network, unlike Windows, which required additional driver setup.

Task 2: The potentiometer was the sensor used to connect to the PLCs. For the Allen-Bradley PLC, we used both the potentiometer built into the trainer and a separate physical potentiometer with a dial. Both were successfully connected and tested. The potentiometer on the Allen-Bradley PLC was used to represent the water level of a tank. In CCW, the software used for the Allen-Bradley PLC, turning the potentiometer fully to the right produced a reading of about 4090, which represented 100% tank capacity. Turning it fully to the left produced a reading of 0, which represented 0% tank capacity. The value was scaled in the program so that the potentiometer reading could be displayed as the percentage of water in

the tank. Both potentiometers connected to the Allen-Bradley PLC were also visible in the logging system that was created. Each potentiometer was represented by a global variable in CCW, and whenever the value changed, the change could also be seen in the logging system at a sampling rate of every 100th of a second. We ran a test where logging information was captured while changes were made to both potentiometers. When we reviewed the logged data, we were able to see the values of the variables changing and those changes being recorded on each line of the log.

Task 3: The Siemens PLC was added to the testbed with its inputs and outputs connected to the trainer. As more PLCs and network connections were added, the short Ethernet cables we had were no longer sufficient, so we created longer Ethernet cables using CAT6 cable and RJ45 connectors. The STEP 7 software was acquired later in the milestone because communication with Siemens and the waiting period posed a challenge. We were eventually able to obtain a 21-day trial of the software, and we currently have multiple versions available to use once the first trial expires. However, this may become a challenge once all of the available trials have been used and the full version of the software is required. We are currently working with our client/advisor to determine a long-term solution for obtaining the software. Even with this challenge, we were able to successfully set up STEP 7, and the Siemens PLC was detected in the software through the network switch. The PLC was also programmed, and changes made to the inputs and outputs were successfully reflected on the trainer.

6. Contribution of each team member to the current Milestone

Karla Daley: I finished setting up the connection between the Allen-Bradley PLC and the software and programmed each input with its corresponding output so that the changes could be reflected on the trainer. For the sensors, we were able to demonstrate connectivity for the PLCs. Currently, the Allen-Bradley PLC has a potentiometer that represents a water tank and its water level, and I programmed this in the CCW software so that the PLC could read and display the changing value. I also created ferrule-ended wires to be used for the positive and negative power connections. For the Siemens PLC, I set up the inputs and outputs to connect with the trainer. I then downloaded the STEP 7 software and set it up to create the logic program. For the Modicon PLC, I added it to the testbed and configured its inputs and outputs to connect to the trainer. I connected both the Siemens and Modicon PLCs to the terminal blocks so they could receive power from the positive and negative power distribution groups.

Zach Lavoie: I completed the network configuration in the STEP 7 software to ensure that the software was able to detect and communicate with the Siemens PLC over the network. I also assigned static IP addresses to all connected PLCs. In addition, I terminated Ethernet cables using CAT6 wiring and RJ45 connectors for use throughout the testbed and created RS485 cables to support serial communication connections where needed. For the software side of the project, I created a modular logging framework written in Python. The framework consists of several modules, each collecting and logging different types of data. The main program can be started to run all the modules together, collect their data, and save the information in appropriate formats, such as storing network traffic in a PCAP file. Once the main logging program is stopped, all of the generated log files are saved and compressed into a timestamped archive so that the information from each test can be reviewed later. I also created a second framework for the attack engine. This provides a modular way to store attack scripts and their documentation, and to execute saved attacks when needed. New attacks can be added by placing them into an existing category directory or by creating a new category directory for a different type of attack. This allows the same attacks to be stored, organized, and repeatedly tested from the attack computer.

7. Plan for the next Milestone

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

8. Discussion of each planned task for the next Milestone

Task 1: We will finish connecting the Modicon PLC to the historian through the data adapter and complete the program so that it can use the sensors and outputs that are already connected to the PLC.

Task 2: We will set up a test where the attack engine can target the historian and create an observable effect on the PLCs connected to the network.

Task 3: Using the new mockup, we will demonstrate a physical attack on the hardware and sensors and observe how the changes affect the power plant system as a whole.

Task 4: We will create a mockup of a small power plant or power distribution hub. The setup will consist of multiple Allen-Bradley PLCs communicating with each other, along with physical switches, dials, lights, and voltage sensors. Multiple Allen-Bradley PLCs will be connected, with one main PLC responsible for the system's main calculations.

9. Date(s) of meeting(s) with Client during the current milestone

10/13/26

10/19/26

10. Client feedback on the current milestone

See Faculty Advisor Feedback below.

11. Date(s) of meeting(s) with Faculty Advisor during the current milestone

10/13/26

10/19/26

12. Faculty Advisor feedback on each task for the current Milestone

Task 1: **Set up Modicon PLC and simulate attack**

Task 2: create three different test bed setup as Allen Bradley , Modicon and Seimens are currently connected

Task 3: Check with IT for network connectivity for three different testbed

Faculty Advisor Signature:  Date: 10/25/2026