Lab 2 - OpenPLC Ladder Logic Lab

CPE 524 - 01

System Security

Fall 2023

Students: Maanav Patel, Nicholas Tan, Wesley Kwok

Lab Due: 12/14/2023

Instructor: Dr. Beard

1. Give an overview of the verification logic you used to ensure that your traffic light system is functioning correctly.

   The verification logic went through a few checks that were applied to each iteration/state. For example we had an individual verification case for the combination of lights (Main Green + Side Red, Main Yellow + Side Red, Main Red + Side Green, Main Red + Side Yellow). This also ensured that there weren't multiple lights on from either side at a time, as well as to make sure there weren't cars going from both directions. This essentially verified the combinatorial logic, and then we had to consider sequential logic of the system, or the order of the lights for example. For this, we used the functionality that allowed you to check a boolean expression based off of the previous clock cycle. Using this, we were able to construct logic such as if the main green light was previously True, and then if in the N+1 cycle the main green light was False, this means that the Main Yellow light should now be true. This helps to check against the case where light changes directly from green to red.

2. If you had implemented a Trojan, what would you have done? Just briefly describe a concept for a trigger and payload.

   Based on Wesley's and Maanav's experience from the Hardware trojans in CPE 426, we were able to devise a few ways to conceal the trigger and payload for our ladder logic traffic system. First off, our first idea was to layer multiple levels of coils and gates on top of one another, as to make them difficult to view, though this may also make it difficult to design a trojan as its functionality will be tough to dissect. Another idea was to hide logic under a comment box which could check conditions such as the current lights and the combination of inputs, and use that to increment a counter. Once that counter reached the desired value (for example 10), it would trigger the payload. A simple yet effective payload would be to set both lights to green and watch all cars crash into each other, though this may be caught quickly by verification. One key concept we learned from CPE 426 was the art of obfuscation, and as such we could also expand our system into additional states, and conceal a trigger in one of the states by modifying one of the state names in a lower layer, but then replacing the upper layer with the coil which looks like it's correct. Also, if we implemented a timer, this could hinder our opponent's ability to use the verification tool effectively.

3. Assuming the jankiness of the verification part of the assignment was fixed and we had time to do the Trojan implementation and hunt, do you think this lab has educational value? I.e. do you think you learned something about industrial programming and about formal verification from completing this lab? What could be improved?

    If the jankiness was fixed, I think the lab would definitely still be interesting (though I feel like there would be a bit of overlap with the Hardware Security class for the trojans bit). Learning about industrial programming is definitely something novel for most non-CPE majors, though I feel like the learning curve is definitely steeper for CS / SE majors that usually don't touch this sort of stuff, so organizing groups into good splits of majors would definitely be a good idea (so that way the assignment has somewhat uniform difficulty between groups). Doing a small precursor lab that introduces students to OpenPLC and allows them to get familiar with industrial programming might also be useful if time permits within the schedule, as jumping directly into it for this lab was a little daunting.

    In terms of other ideas, we're wondering if there are other interesting potential lab ideas for the class - it would also be interesting to have a few more labs but have each of them be a little shorter (so that way we could jump around between topics some more).