Dan Otieno

CPE 459/559 – 01.

RGB LED Assignment.

Due Date: 02/13/2024.

REPORT QUESTIONS.

A. (60 points) Upload a video of your project running. Show the following in your video (All videos uploaded as separate files in Canvas):

1. Manual mode operation.

(a) (15 points) show that button presses change the color of the LED.

(b) (15 points) show that HMI count increases after the button presses

2. Automatic mode operation.

(a) (15 points) show that HMI count loops automatically from 0-7 and restarts.

(b) (15 points) show that the physical LED color changes approximately every 1 second.

B. (20 points) Assume causing the LED to flash RED is a signal to an operator that the system was in an alarm state, how might an attacker cause the RGB LED to flash RED by manipulating the color0-color7 variables and changing the mode.

Response: The attacker might take certain steps to manipulate the system such that they cause the LED to flash red. They would start by seeking details about the specific system software used (or hardware, in some cases). Once they have that information, they may attempt to gain access to the SCADA system by finding and taking advantage of any system vulnerabilities. Next, they may locate and analyze the ladder logic used to implement the PLC functionality, where they would identify the variables and manipulate them to achieve their desired output. Once they have completed those modifications, they can deploy the changes back to the system by sending the commands to the PLC or reconfiguring the SCADA software. An example of modification would be to manipulate the data packets between the HMI and the PLC such that they set the LEDs to flash red in auto mode, but also disable the other colors.

C. (20 points) If you power off the ScadaBR HMI VM while the PLC program is running does the PLC program and LED circuit continue to operate? Which if any functionality is lost?

Response: Yes, the PLC program and LED circuit will continue to operate with the HMI turned off, because PLCs can continue to run the system independently of the HMI, particularly where the PLC program is downloaded into the PLC CPU. During this lab, we used the OpenPLC online interface, and even with ScadaBR uninvolved, once the program was loaded, I was still able to execute the commands and monitor the outputs from the PLC. However, there may be loss of some functionalities without the HMI. For instance, we cannot remotely monitor and control the PLC without the HMI. If the HMI is off, there may also be inaccuracies in the system reporting, and if required, routine maintenance or troubleshooting may be affected, as these are typically handled remotely through the HMI.