

# Programmable Logic Controllers (PLCs)

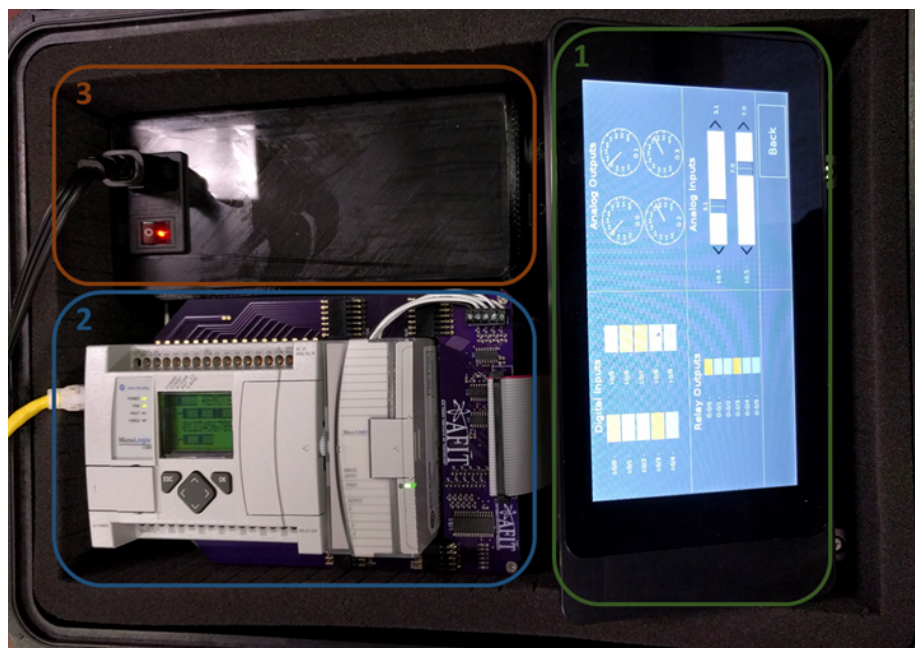
## Lab #0 Setup

### Intro

In this lab you will setup the PLC training kit you have received. This process includes understanding how to connect to the kit, program the PLC, and test the hardware using the IO\_Test example project.

### Kit Contents

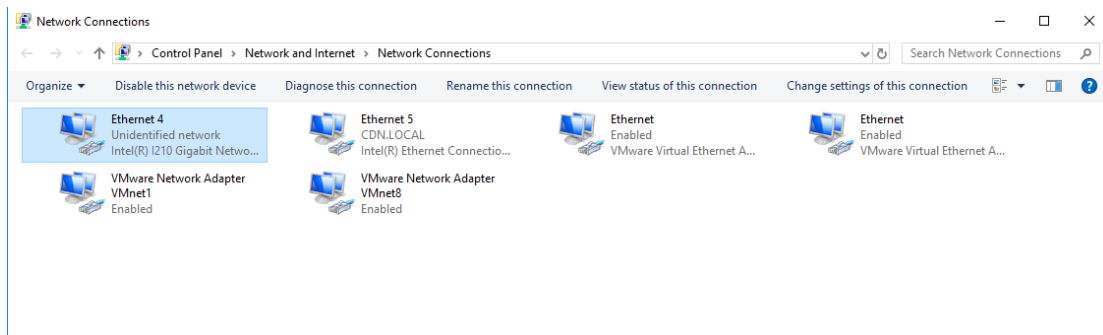
**WARNING!!! DO NOT REMOVE THE SYSTEM FROM THE PELICAN CASE.**



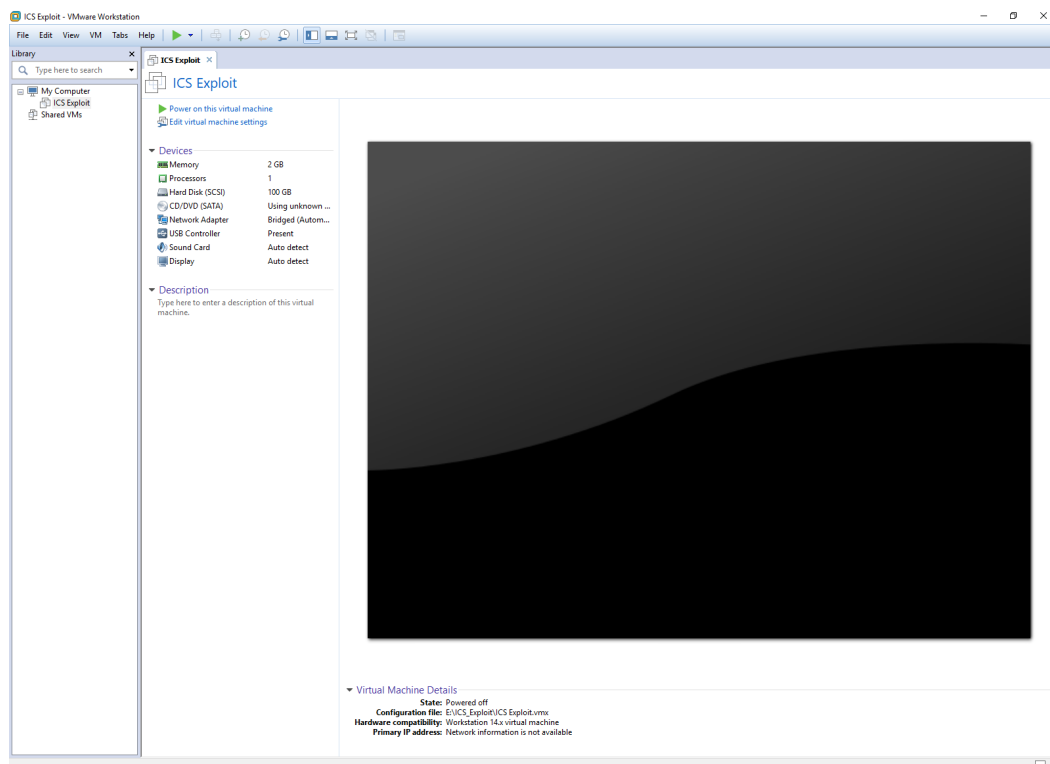
1. Raspberry PI touchscreen - hardware-in-the-loop simulator.
2. MicroLogix 1100 - Programmable Logic Controller.
3. Power.

## Lab Procedure

1. Open your PLC kit (**do not remove contents from Pelican case**).
2. Use the power cord from an unused monitor to power the kit.
3. Connect the **PLC's Ethernet** to an **empty Ethernet port on your computer**.
4. Check the name of the network interface that you used. In this picture it is the **I210 Gigabit Network**.



5. Open VMware Workstation



6. Enter the Virtual Network Editor. Select **VMnet0** and remove the **Bridged >> Automatic** setting. Either select a specific interface or switch it to **Host-only**.

The screenshot shows the 'Virtual Network Editor' window. At the top, there is a table listing several virtual networks. Below the table are buttons for 'Add Network...', 'Remove Network', and 'Rename Network...'. The 'VMnet Information' section is expanded, showing three radio button options: 'Bridged (connect VMs directly to the external network)', 'NAT (shared host's IP address with VMs)', and 'Host-only (connect VMs internally in a private network)'. The 'Host-only' option is selected. Below these options are checkboxes for 'Connect a host virtual adapter to this network' and 'Use local DHCP service to distribute IP address to VMs'. At the bottom, there are input fields for 'Subnet IP' and 'Subnet mask', and a row of buttons: 'Restore Defaults', 'OK', 'Cancel', 'Apply', and 'Help'.

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Custom	-	-	-	192.168.78.0
VMnet1	Host-only	-	Connected	Enabled	192.168.1.0
VMnet2	Custom	-	-	-	192.168.24.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.237.0
VMnet3	Host-only	-	Connected	Enabled	192.168.64.0

Buttons: Add Network..., Remove Network, Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

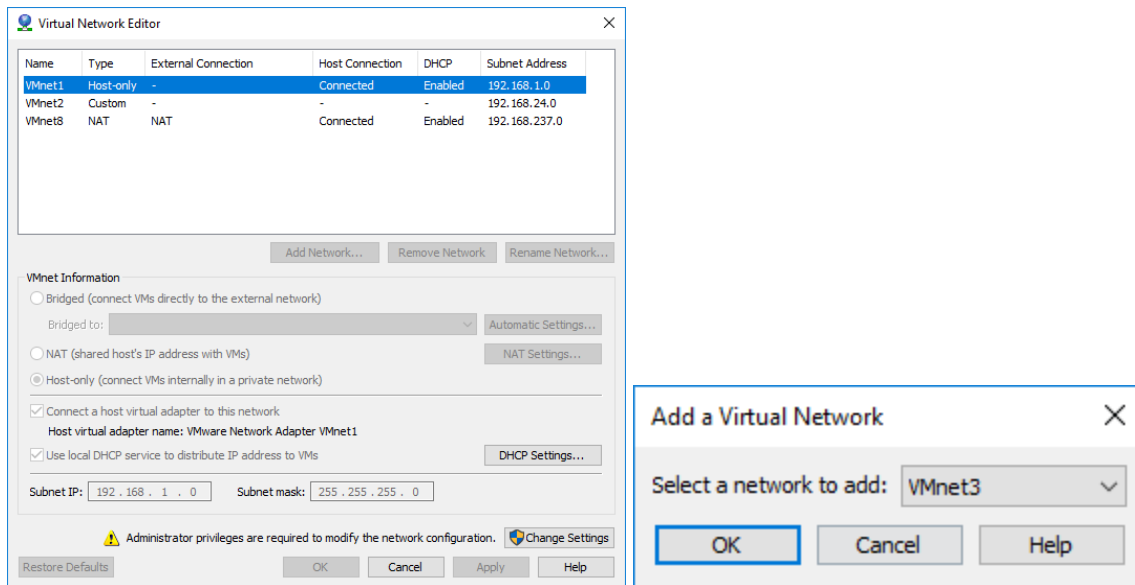
☐ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet0

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

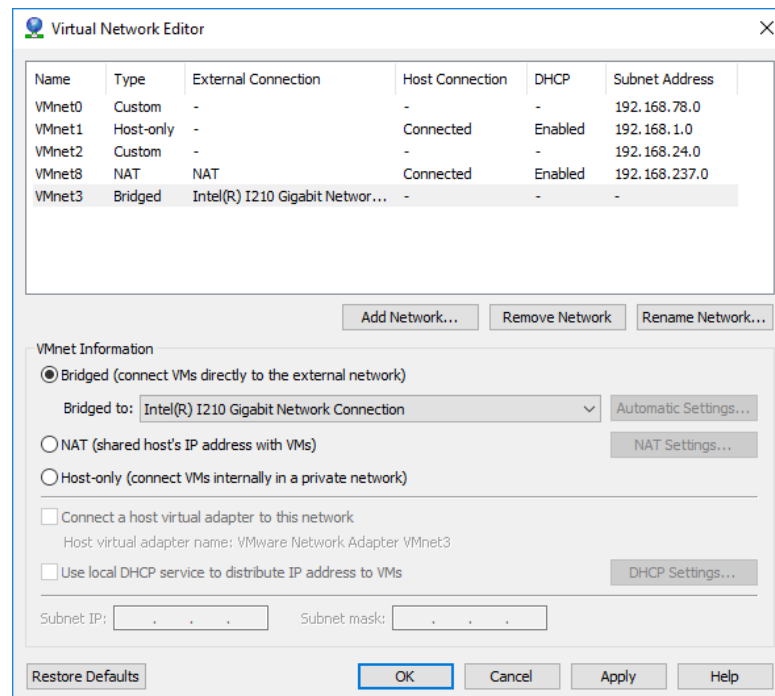
Subnet IP: 192 . 168 . 78 . 0 Subnet mask: 255 . 255 . 255 . 0

Buttons: Restore Defaults, OK, Cancel, Apply, Help

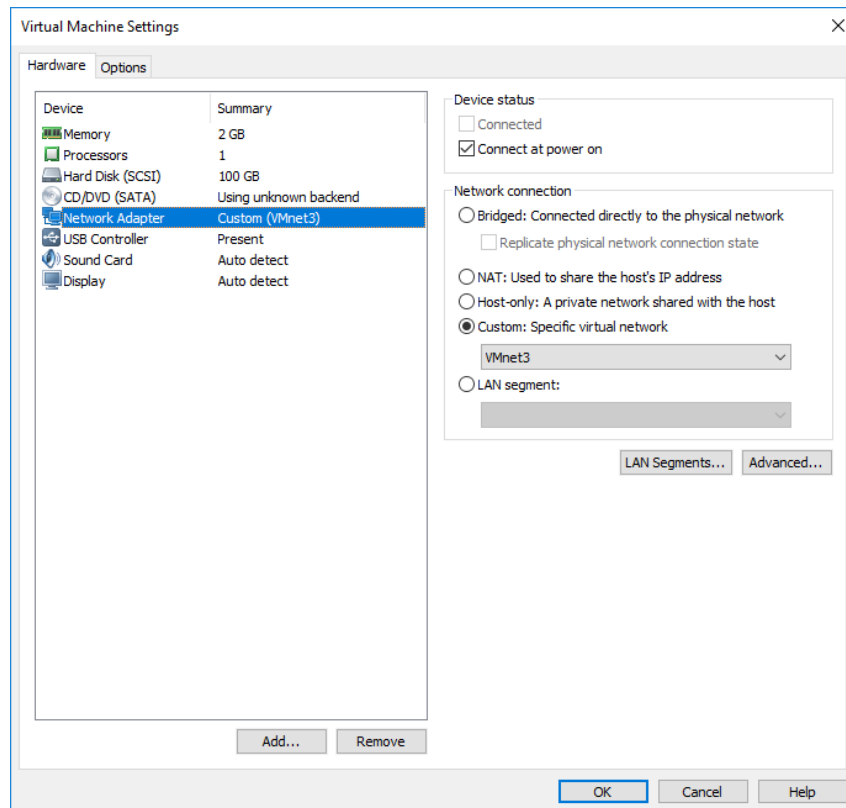
7. Click **Change Settings** and then **Add Network**. Note the name of the new network (**VMnet3** in this example).



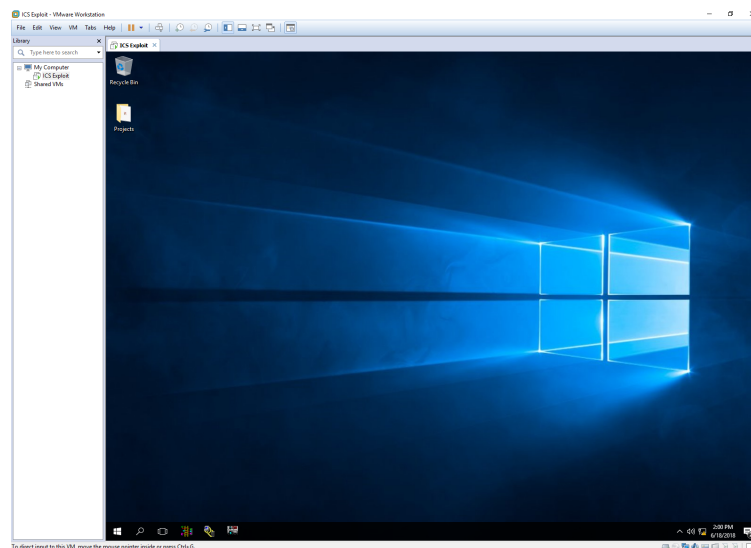
8. Select the network you added (**VMnet3** in this example), set it to **Bridged** mode, and select the interface the PLC is connected to.



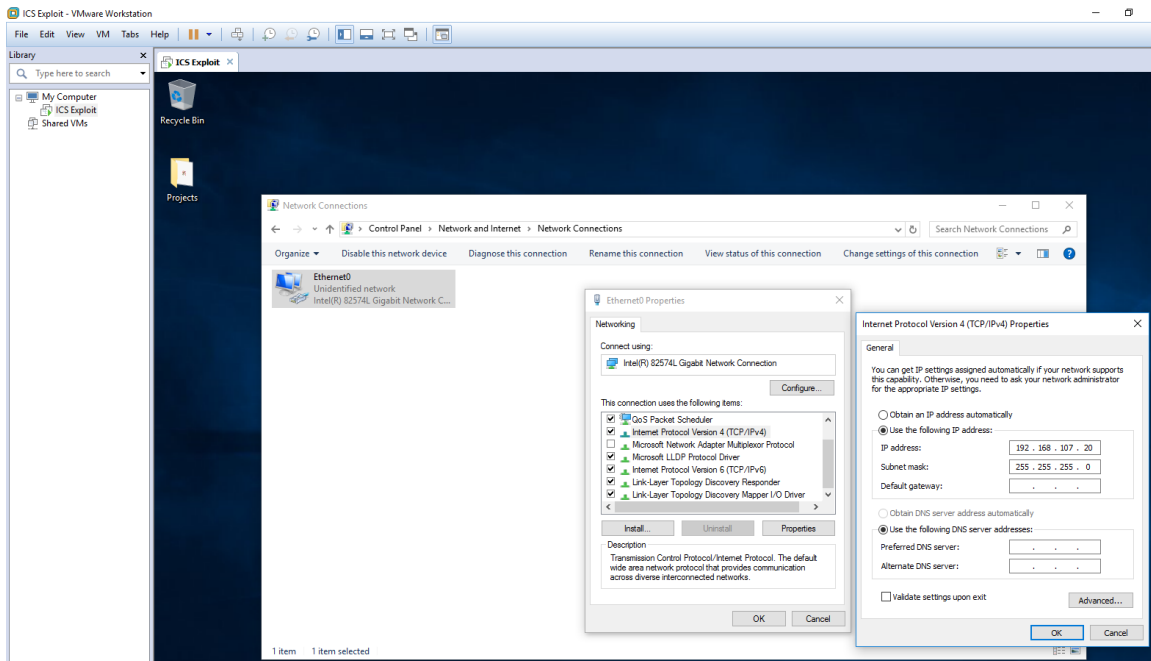
9. Select the ICS Exploit VM and click **Edit virtual machine settings**.
10. Under **Netork Adapter**, select **Custom** and select the network you created earlier (**VMnet3** in this example).



11. Start the VM



12. In the VM, check the IP address and, if necessary, set it to a non-conflicting IP in the **192.168.107.\*** subnet. E.g., **192.168.107.42**.



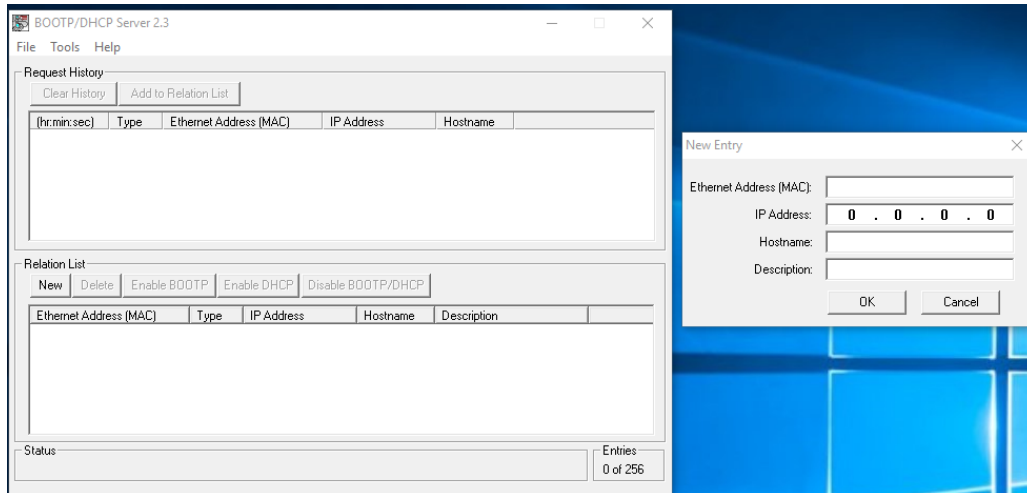
13. Find your PLC's current IP address.



14. If your PLC does not have an IP address assigned, create a new relation in the BOOTP/DHCP Server. You can follow this tutorial for additional details:

<https://www.youtube.com/watch?v=ErdkGziBkmA>

We recommend using **192.168.107.3** for the IP address. This IP was used for development and will allow you to skip a few steps during the lab.



15. Use **ping** to verify connectivity with the PLC.

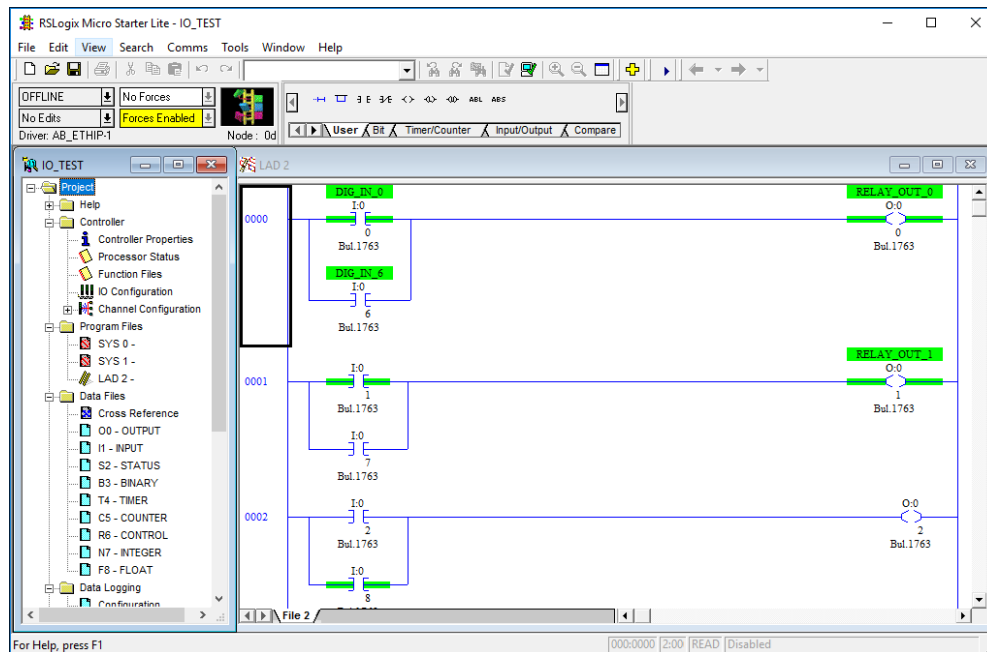
```
C:\Users\User>ping 192.168.107.3

Pinging 192.168.107.3 with 32 bytes of data:
Reply from 192.168.107.3: bytes=32 time=2ms TTL=128
Reply from 192.168.107.3: bytes=32 time=2ms TTL=128
Reply from 192.168.107.3: bytes=32 time=2ms TTL=128
Reply from 192.168.107.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.107.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\User>
```

16. Start RSLogix Micro and open **Desktop\Projects\IO\_Test**.

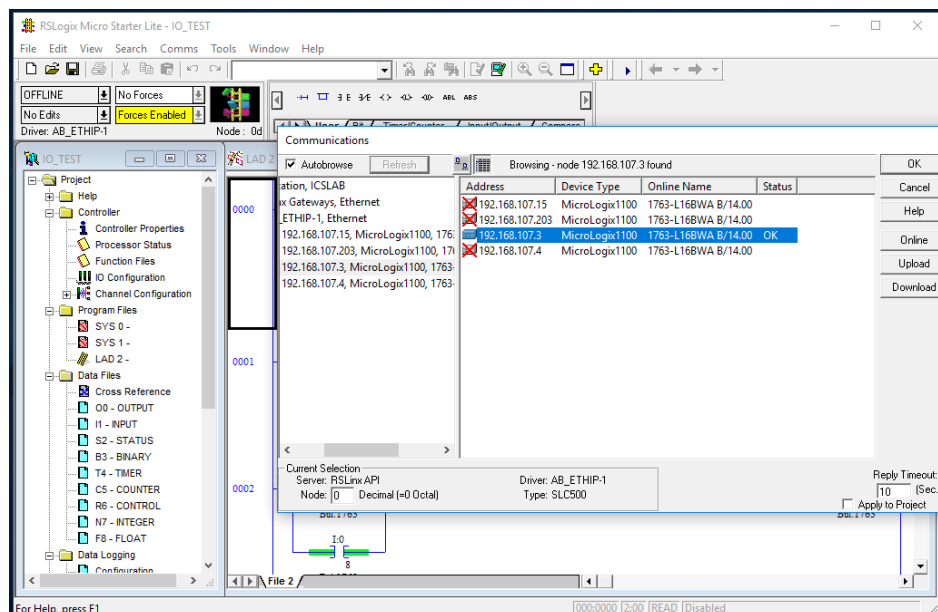


17. Open the **Comms >> System Comms** menu.

18. Select the IP of your PLC.

19. **Download** the program, clicking through the numerous, pointless and annoying pop ups.

**Note:** In this program, “download” means write the program to the PLC. This naming scheme is backwards and annoying.





20. Run the **IO\_Test** application on the **Raspberry Pi**. This application is used to test the inputs and outputs of the PLC. The IO\_Test ladder logic program copies the state of the Digital Inputs to the Relay Outputs. It also copies the voltage from the Analog Inputs to the Analog Outputs. Use this to verify that all IO is working.

**Note:** the labels in this application match the addressing scheme used by RSLogix Micro. Pay close attention to the difference between 'I' and 'Q' for inputs. I:0\_4 is analog input 1 (IV1). I:0\_4 is digital input 4.

21. While in **Online** mode with the PLC, compare the ladder logic interface to the Touchscreen to gain an understanding of the logic and hardware. Additionally you can check the status of the digital inputs and outputs on the PLC under the IO\_STATUS option.

